

CloudEngine S5700, S6700
V600R023C00

CloudEngine S5700, S6700 产品文档

发布日期 2023-12-04



版权所有 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目录

- 目录 1
- 1 配置 8
 - 1.1 典型配置案例 8
 - 1.1.1 快速配置指南 8
 - 1.1.1.1 开始 8
 - 1.1.1.2 小型园区组网场景 9
 - 1.1.1.2.1 小型园区组网图 9
 - 1.1.1.2.2 数据规划 10
 - 1.1.1.2.3 快速配置小型园区 11
 - 1.1.1.2.3.1 登录设备（以交换机为例） 12
 - 1.1.1.2.3.2 配置管理 IP 和 Telnet 12
 - 1.1.1.2.3.3 配置接口与 VLAN 13
 - 1.1.1.2.3.4 配置 DHCP 17
 - 1.1.1.2.3.5 配置核心交换机路由 19
 - 1.1.1.2.3.6 配置出口路由器 19
 - 1.1.1.2.3.7 配置 DHCP Snooping 和 IPSG 20
 - 1.1.1.2.3.8 业务验证 21
 - 1.1.1.2.3.9 保存配置 22
 - 1.1.1.3 中小园区组网场景 22
 - 1.1.1.3.1 中小园区组网图 22
 - 1.1.1.3.2 数据规划 23
 - 1.1.1.3.3 快速配置中小园区 25
 - 1.1.1.3.3.1 登录设备（以交换机为例） 25
 - 1.1.1.3.3.2 配置管理 IP 和 Telnet 26
 - 1.1.1.3.3.3 配置网络互连互通 27
 - 1.1.1.3.3.4 配置 DHCP 33
 - 1.1.1.3.3.5 配置 OSPF 36
 - 1.1.1.3.3.6 配置可靠性和负载分担 37
 - 1.1.1.3.3.7 配置链路聚合 38
 - 1.1.1.3.3.8 配置限速 39
 - 1.1.1.3.3.9 配置映射内网服务器和公网多出口 40
 - 1.1.1.3.3.10 业务验证和保存配置 44

1.1.2 园区网络综合配置案例	45
1.1.2.1 园区内基础网络连通部署案例	45
1.1.2.1.1 基础网络连通性部署要点	46
1.1.2.1.2 两层和三层网络架构部署差异说明	47
1.1.2.1.3 集群/堆叠通用部署	48
1.1.2.1.4 独立 AC 方案：核心交换机做有线无线用户网关.....	62
1.1.2.1.5 独立 AC 方案：汇聚交换机做有线无线用户网关.....	92
1.1.2.1.6 独立 AC 方案：核心交换机做有线用户网关，AC 做无线用户网关	123
1.1.2.1.7 独立 AC 方案：汇聚交换机做有线用户网关，AC 做无线用户网关	154
1.1.2.2 有线无线用户接入认证部署案例	185
1.1.2.2.1 用户接入认证部署要点和说明	185
1.1.2.2.2 独立 AC 方案：核心交换机做有线用户网关和认证点，AC 做无线用户网关和认证点，NAC	186
1.1.2.2.3 独立 AC 方案：汇聚交换机做有线用户网关和认证点，AC 做无线用户网关和认证点，NAC	224
1.1.2.2.4 认证点在接入设备的认证部署配置示例	272
1.1.2.3 智能极简园区网络部署案例（小行星部署案例）	290
1.1.2.4 环网接入 VRRP 网关配置案例.....	299
1.1.2.5 集中式网关部署方式的 VXLAN 配置案例	336
1.1.3 交换机与防火墙对接上网配置案例	356
1.1.3.1 二层交换机与防火墙对接上网配置案例	356
1.1.3.2 三层交换机与防火墙对接上网配置案例	365
1.1.4 交换机与路由器对接上网配置案例	370
1.1.4.1 二层交换机与路由器对接上网配置案例	370
1.1.4.2 三层交换机与路由器对接上网配置案例	376
1.1.5 特性典型配置案例.....	380
1.1.5.1 特性典型配置案例的说明	381
1.1.5.2 基础配置	381
1.1.5.2.1 首次登录设备.....	382
1.1.5.2.1.1 举例：配置用户通过 Console 口首次登录设备	382
1.1.5.2.2 登录设备命令行界面.....	385
1.1.5.2.2.1 举例：配置用户通过 Telnet 登录设备	385
1.1.5.2.2.2 举例：配置用户通过 STelnet 登录设备	388
1.1.5.2.2.3 举例：配置用户通过 Console 口登录设备	393
1.1.5.2.2.4 举例：配置基于 ACL 规则和 RADIUS 认证限制 Telnet 登录设备	396
1.1.5.2.2.5 举例：配置通过 STelnet 登录设备示例（基于 RADIUS 认证）	401

1.1.5.2.3 登录设备 Web 界面	406
1.1.5.2.3.1 举例：通过 HTTPS 登录 Web 界面（默认证书）	406
1.1.5.2.4 文件系统管理	408
1.1.5.2.4.1 举例：本地文件操作	409
1.1.5.2.4.2 举例：配置设备作为 FTP 服务器	410
1.1.5.2.4.3 举例：配置设备作为 SFTP 服务器	414
1.1.5.2.4.4 举例：配置设备作为 TFTP 客户端	417
1.1.5.2.4.5 举例：配置设备作为 FTP 客户端	419
1.1.5.2.4.6 举例：配置设备作为 SFTP 客户端	421
1.1.5.2.4.7 举例：配置设备作为 SCP 客户端	429
1.1.5.3 接口管理	432
1.1.5.3.1 以太网接口	433
1.1.5.3.1.1 举例：配置以太网接口速率和双工模式	433
1.1.5.3.1.2 举例：配置以太网接口的二层模式切换	435
1.1.5.3.2 端口隔离	437
1.1.5.3.2.1 举例：配置二层端口隔离	437
1.1.5.4 系统管理	439
1.1.5.4.1 SNMP	439
1.1.5.4.1.1 举例：配置设备使用 SNMPv1 与网管通信	440
1.1.5.4.1.2 举例：配置设备使用 SNMPv2c 与网管通信	442
1.1.5.4.1.3 举例：配置设备使用 SNMPv3 USM 用户与网管通信	447
1.1.5.4.2 升级维护	452
1.1.5.4.2.1 举例：新设备升级	452
1.1.5.5 虚拟化	455
1.1.5.5.1 堆叠	455
1.1.5.5.1.1 举例：组建堆叠	456
1.1.5.6 以太网交换	461
1.1.5.6.1 MAC	461
1.1.5.6.1.1 举例：配置静态 MAC 表项	461
1.1.5.6.1.2 举例：配置黑洞 MAC 表项	463
1.1.5.6.1.3 举例：配置基于接口的 MAC 地址限制	465
1.1.5.6.1.4 举例：配置基于 VLAN 的 MAC 地址限制	467
1.1.5.6.2 Eth-Trunk	469
1.1.5.6.2.1 举例：配置手工模式 Eth-Trunk	469

1.1.5.6.2.2 举例：配置静态 LACP 模式 Eth-Trunk	471
1.1.5.6.2.3 举例：配置 Eth-Trunk 接口流量本地优先转发示例（集群/堆叠）	475
1.1.5.6.3 VLAN	480
1.1.5.6.3.1 举例：配置 VLANIF 接口实现不同 VLAN 间的互通（同设备）	481
1.1.5.6.3.2 举例：配置基于接口划分 VLAN，实现同一 VLAN 内的互通（跨设备）	482
1.1.5.6.3.3 举例：配置基于接口划分 VLAN，实现不同 VLAN 内的互通（接入层设备作为网关）	487
1.1.5.6.3.4 举例：配置基于接口划分 VLAN，实现不同 VLAN 内的互通（汇聚层设备作为网关）	493
1.1.5.6.3.5 举例：配置基于 MAC 地址划分 VLAN	497
1.1.5.6.3.6 举例：配置基于子网划分 VLAN	500
1.1.5.6.3.7 举例：配置 VLAN 聚合	502
1.1.5.6.3.8 举例：配置 MUX VLAN（级联设备）	507
1.1.5.6.3.9 举例：配置基本 QinQ	513
1.1.5.6.3.10 举例：配置基于 VLAN ID 的灵活 QinQ	516
1.1.5.6.3.11 举例：配置基于 MQC 的灵活 QinQ	518
1.1.5.6.4 STP/RSTP/MSTP	523
1.1.5.6.4.1 举例：配置 STP 功能	523
1.1.5.6.4.2 举例：配置 RSTP 功能	526
1.1.5.6.4.3 举例：配置 MSTP 功能	530
1.1.5.6.4.4 举例：配置 MSTP+VRRP 组合组网	539
1.1.5.6.5 VBST	552
1.1.5.6.5.1 举例：配置 VBST 基本功能	553
1.1.5.7 IP 地址与服务	561
1.1.5.7.1 ARP 安全	561
1.1.5.7.1.1 举例：配置 ARP 安全功能	562
1.1.5.7.1.2 举例：配置防止 ARP 中间人攻击	566
1.1.5.7.2 DHCPv4	569
1.1.5.7.2.1 举例：配置基于接口地址池的 DHCPv4 服务器	570
1.1.5.7.2.2 举例：配置基于全局地址池的 DHCPv4 服务器（使用三层以太网接口）	574
1.1.5.7.2.3 举例：配置 DHCPv4 客户端	579
1.1.5.7.2.4 举例：配置 DHCPv4 中继	582
1.1.5.7.2.5 举例：配置 VRRP 组网中的 DHCPv4 服务器	586
1.1.5.7.3 DHCP Snooping	595
1.1.5.7.3.1 举例：配置 DHCP Snooping 的攻击防范功能示例	595
1.1.5.7.4 ACL	600

1.1.5.7.4.1 举例：使用基本 ACL 限制 FTP 访问权限	600
1.1.5.7.4.2 举例：使用高级 ACL 限制用户在特定时间访问特定服务器的权限	602
1.1.5.7.4.3 举例：使用二层 ACL 禁止特定用户上网	607
1.1.5.7.4.4 举例：配置特定时间段允许个别用户上网	610
1.1.5.7.4.5 举例：使用高级 ACL 限制不同网段的用户互访	614
1.1.5.7.4.6 举例：使用基本 ACL 限制内网主机访问外网网站	618
1.1.5.7.4.7 举例：使用高级 ACL 限制外网用户访问内网中服务器的权限	622
1.1.5.8 IP 路由	626
1.1.5.8.1 IPv4 静态路由	626
1.1.5.8.1.1 举例：IPv4 静态路由实现路由负载分担	626
1.1.5.8.1.2 举例：IPv4 静态路由实现主备备份	632
1.1.5.9 VPN	638
1.1.5.9.1 IPv4 L3VPN	638
1.1.5.9.1.1 举例：配置本地 IPv4 L3VPN 互访	639
1.1.5.9.1.2 举例：配置基本 IPv4 L3VPN over MPLS 场景	644
1.1.5.9.1.3 举例：配置 Hub and Spoke 示例（Hub-PE 和 Hub-CE 双链路接入）	663
1.1.5.9.1.4 举例：配置 L3VPN+VRRP 综合场景	676
1.1.5.9.1.5 举例：配置企业使用路由策略控制 L3VPN 分支间用户互访场景	695
1.1.5.9.2 IPv6 L3VPN	707
1.1.5.9.2.1 举例：配置基本 IPv6 L3VPN over MPLS 场景	707
1.1.5.9.2.2 举例：配置 IPv6 L3VPN over MPLS Hub and Spoke（IPv6）场景	723
1.1.5.10 网络切片	737
1.1.5.10.1 举例：配置 EVPN L3VPNv4 over SRv6 BE 网络切片示例（静态配置）	737
1.1.5.10.2 举例：配置 VLAN 切片示例	755
1.1.5.11 可靠性	764
1.1.5.11.1 VRRP	764
1.1.5.11.1.1 举例：配置 VRRP 网络传输组播数据	764
1.1.5.11.2 M-LAG	783
1.1.5.11.2.1 举例：配置 M-LAG 双归接入二层网络（根桥方式）	783
1.1.5.11.2.2 举例：配置 M-LAG 双归接入三层网络（V-STP 方式）	792
1.1.5.11.2.3 举例：配置动态路由接入 M-LAG（V-STP 方式）	803
1.1.5.11.2.4 举例：配置多级 M-LAG 互联（V-STP 方式）	813
1.1.5.11.2.5 举例：配置 M-LAG 设备作为 DHCPv4 中继（插入 Option82 选项的子选项）	831
1.1.5.11.2.6 举例：配置 M-LAG 设备作为 DHCPv4 中继（Option82 选项携带回程地址信息）	837

1.1.5.12 用户接入与认证	844
1.1.5.12.1 AAA	844
1.1.5.12.1.1 举例：配置 AAA 本地认证和授权	844
1.1.5.12.1.2 举例：配置 HWTACACS 认证、授权和计费	847
1.1.5.12.1.3 举例：配置 RADIUS 认证、授权和计费	851
1.1.5.12.2 NAC	855
1.1.5.12.2.1 举例：配置 802.1X 认证（AAA 采用 RADIUS 方式）	855
1.1.5.12.2.2 举例：配置 802.1X 认证（AAA 采用本地认证）	859
1.1.5.13 安全	863
1.1.5.13.1 IPSP	863
1.1.5.13.1.1 举例：基于接口配置静态绑定表的 IPSP	863
1.1.5.13.1.2 举例：基于 VLAN 配置静态绑定表的 IPSP	865
1.1.5.13.1.3 举例：配置 IPSP 防止 DHCP 动态主机私自更改 IP 地址	868
1.1.5.13.1.4 举例：基于 VLAN 配置动态绑定表的 IPSP	872
1.1.5.13.2 端口安全	875
1.1.5.13.2.1 举例：配置端口安全	875
1.1.5.14 QoS	877
1.1.5.14.1 流量统计	877
1.1.5.14.1.1 举例：配置基于 MQC 的流量统计	877
1.1.5.14.2 流量监管、流量整形和接口限速	880
1.1.5.14.2.1 举例：配置基于 DiffServ 域优先级映射的流量整形	880
1.1.5.14.2.2 举例：配置基于信任 802.1p 优先级的流量整形	883
1.1.5.14.2.3 举例：配置流量监管实现接口限速	887
1.1.5.14.2.4 举例：配置一级 CAR 的流量监管（MQC 方式）	888
1.1.5.14.3 拥塞管理	895
1.1.5.14.3.1 举例：配置拥塞管理	895
1.1.5.14.3.2 举例：配置拥塞避免和拥塞管理综合示例（PQ+WDRR 调度和 WRED 模板）	899
1.1.5.15 系统监控	904
1.1.5.15.1 镜像	904
1.1.5.15.1.1 举例：配置本地端口镜像（N:1）	904
1.1.5.15.1.2 举例：配置本地端口镜像（1:1）	906
1.1.5.15.1.3 举例：配置本地端口镜像（1:N，通过单个观察端口方式配置）	908
1.1.5.15.1.4 举例：配置本地端口镜像（1:N，通过观察端口组方式配置）	910
1.1.5.15.1.5 举例：配置本地端口镜像（M:N）	912

- 1.1.5.15.1.6 举例：配置本地基于 MQC 的流镜像 915
- 1.1.5.15.1.7 举例：配置本地 VLAN 镜像 917
- 1.1.5.15.2 NetStream.....919
 - 1.1.5.15.2.1 举例：配置原始流统计信息的输出功能 919
 - 1.1.5.15.2.2 举例：配置灵活流统计信息的输出功能.....923

1 配置

[典型配置案例](#)

[CLI 配置指南](#)

[Web 配置指南](#)

[安全加固与维护](#)

1.1 典型配置案例

[快速配置指南](#)

[园区网络综合配置案例](#)

[交换机与防火墙对接上网配置案例](#)

[交换机与路由器对接上网配置案例](#)

[特性典型配置案例](#)

1.1.1 快速配置指南

[开始](#)

[小型园区组网场景](#)

[中小园区组网场景](#)

1.1.1.1 开始

本文档帮助您首次登录及快速配置华为 S 系列交换机。更多业务配置，请查阅《交换机配置指南》。

说明

本文适用于交换机 V600R022C10 及更高版本。可以在用户视图下执行 **display version** 命令查看设备的版本信息。

在开始数据配置之前，请您首先完成如下工作：

1. 完成交换机的安装、上电。
2. 获取以下常用联系方式信息，并打印和张贴在您的工作台附近。

华为企业业务技术支持热线电话（400-822-9999）。

负责贵单位网络建设和服务的代理商的联系电话。

3. 访问华为企业技术支持网站（<http://support.huawei.com/enterprise>）并注册一个用户账号，以获取更多的便利，浏览或下载更有价值的产品文档、案例、公告等信息，并可获得订阅和推送方面的支持。

1.1.1.2 小型园区组网场景

[小型园区组网图](#)

[数据规划](#)

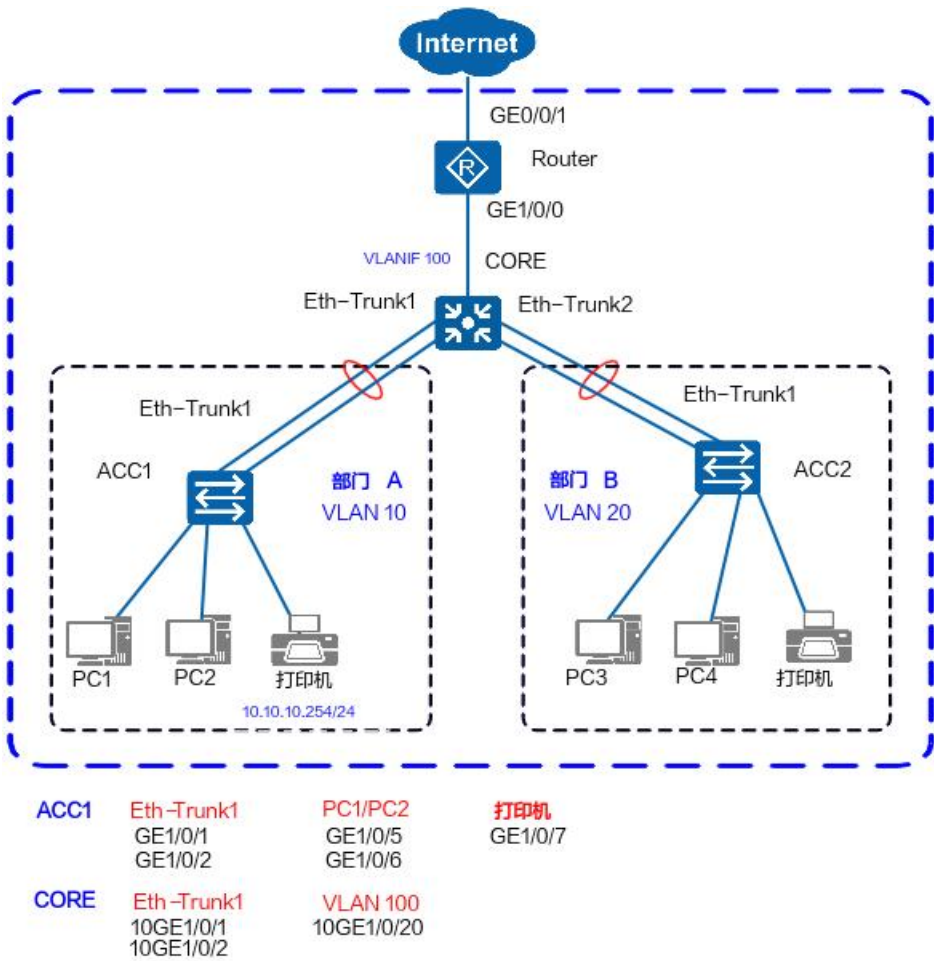
[快速配置小型园区](#)

1.1.1.2.1 小型园区组网图

说明

本举例中的接入交换机 ACC1、ACC2 以 V600R022C10 版本的 S5735-L-V2 为例、核心交换机 CORE 以 V600R022C10 版本的 S8700-4 为例、出口路由器 Router 以 AR651 V300R022C10 为例。

图 1 小型园区组网图



在小型园区中，S5735-L-V2 通常部署在网络的接入层，S8700-4 通常部署在网络的核心，出口路由器一般选用 AR 系列路由器。

接入交换机与核心交换机通过 Eth-Trunk 组网保证可靠性。

每个部门业务划分到一个 VLAN 中，部门间的业务在 CORE 上通过 VLANIF 三层互通。

核心交换机作为 DHCP Server，为园区用户分配 IP 地址。

接入交换机上配置 DHCP Snooping 功能，防止内网用户私接小路由器分配 IP 地址；同时配置 IPSG 功能，防止内网用户私自更改 IP 地址。

1.1.1.2.2 数据规划

在配置之前，需按照下面的表格准备好数据。以下数据将在本文后续章节使用。

操作	准备项	数据	说明
配置管理 IP 和 Telnet	管理 IP 地址	10.10.1.1/24	管理 IP 用于登录交换机。
	管理 VLAN	VLAN 5	交换机管理口是 MEth0/0/0。 对于没有管理口的交换机建议使用 VLANIF 接口进行带内管理。
配置接口和 VLAN	Eth-Trunk 类型	静态 LACP	Eth-Trunk 链路有手工负载分担和静态 LACP 两种工作模式。
	端口类型	连接交换机的端口建议设置为 trunk，连接 PC 的端口设置为 access。	trunk 类型端口一般用于连接交换机。 access 类型端口一般用于连接 PC。 hybrid 类型端口是通用端口，既可以用来连接交换机，也可用来连接 PC。
	VLAN ID	ACC1: VLAN 10 ACC2: VLAN 20 CORE: VLAN 100、VLAN 10、VLAN 20	交换机有缺省 VLAN 1。 为二层隔离部门 A 和部门 B，将部门 A 划分到 VLAN 10 中，部门 B 划分到 VLAN 20 中。 CORE 通过 VLANIF 100 连接出口路由器。
配置 DHCP	DHCP Server	CORE	在园区核心交换机 CORE 上部署 DHCP Server。
	地址池	VLAN 10: ip pool 10 VLAN 20: ip pool 20	部门 A 的终端从 ip pool 10 中获取 IP 地址。 部门 B 的终端从 ip pool 20 中获取 IP 地址。
	地址分配方式	基于全局地址池	无
配置核心交换机路由	IP 地址	CORE: VLANIF 100 10.10.100.1/24 VLANIF 10 10.10.10.1/24 VLANIF 20 10.10.20.1/24	VLANIF100 是 CORE 与园区出口路由器对接的 IP 地址，用于园区内部用户访问 Internet。CORE 上需要配置一条缺省路由由下一跳指向出口路由器。 在 CORE 上配置 VLANIF 10、VLANIF 20 的 IP 地址后，部门 A 与部门 B 之间可以通过 CORE 互访。

操作	准备项	数据	说明
配置出口路由器	公网接口及其 IP 地址	GE0/0/1: 1.1.1.2/30	GE0/0/1 为出口路由器连接 Internet 的接口，一般称为公网接口。
	公网网关	1.1.1.1/30	该地址是与出口路由器对接的运营商设备的 IP 地址，出口路由器上需要配置一条缺省路由指向该地址，用于指导内网流量转发至 Internet。
	DNS 地址	8.8.8.8	DNS 服务器用于将域名解析成 IP 地址。
	内网接口及其 IP 地址	GE1/0/0: 10.10.100.2/24	GE1/0/0 为出口路由器连接内网的接口。
配置 DHCP Snooping 和 IPSG	信任接口	Eth-Trunk1	无

1.1.1.2.3 快速配置小型园区

您可以按照下列流程配置各设备的数据，连通园区内用户，并使园区内用户可访问外网。



登录设备（以交换机为例）

配置管理 IP 和 Telnet

配置接口与 VLAN

配置 DHCP

配置核心交换机路由

配置出口路由器

配置 DHCP Snooping 和 IPSG

业务验证

保存配置

1.1.1.2.3.1 登录设备（以交换机为例）

1. 请使用 Console 通信电缆（产品随设备附带）连接交换机与 PC。将 Console 通信电缆的 DB9（孔）插头插入 PC 机的串口（COM）中，再将 RJ-45 插头端插入设备的 Console 口中。若 PC 无串口，需要使用 USB 接口转串口的转接线。
2. 在 PC 上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。
连接的接口请根据实际情况进行选择。例如，在 Windows 系统中，可以通过在“设备管理器”中查看端口信息，选择连接的接口。交换机上的通信参数如表 1 所示。

表 1 交换机 Console 口缺省值

参数	缺省值
传输速率	9600bit/s
流控方式	不进行流控
校验方式	不进行校验
停止位	1
数据位	8

3. 在 PC 的终端仿真软件界面按 **Connect** 键，直到出现如下信息，提示用户设置登录密码。

```
Login authentication
Username:admin1
Password:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2023-02-26 20:10:05+08:00.
```

完成 Console 登录密码设置后，用户便可以配置交换机，需要帮助可随时键入“?”。

1.1.1.2.3.2 配置管理 IP 和 Telnet

配置设备管理 IP 地址后，可以通过管理 IP 远程登录设备，下面以交换机 CORE 为例说明配置管理 IP 和 Telnet 的方法。

1. 配置管理 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] vlan 5           //创建交换机管理 VLAN 5
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5
[HUAWEI-vlanif5] ip address 10.10.1.1 24
[HUAWEI-vlanif5] quit
```

2. 将管理接口加入到管理 VLAN 。

```
[HUAWEI] interface 10GE 1/0/8    //假设连接网管的接口为 10GE 1/0/8，非直连，中间有二层设备
[HUAWEI-10GE1/0/8] port link-type trunk
[HUAWEI-10GE1/0/8] port trunk allow-pass vlan 5
[HUAWEI-10GE1/0/8] quit
```

3. 配置 Telnet。

```
[HUAWEI] telnet server enable    //Telnet 出厂时是关闭的
[HUAWEI] telnet server-source -i vlanif 5
Warning: Telnet server source configuration will take effect in the next login. Continue? [Y/N]: Y
[HUAWEI] user-interface vty 0 4    //Telnet 常用于设备管理员登录，推荐使用 AAA 认证
[HUAWEI-ui-vty0-4] protocol inbound telnet // 缺省情况下，用户界面支持所有协议类型，包括 SSH 和 Telnet。
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin1 password irreversible-cipher Helloworld@6789 //配置管理员 Telnet 登录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin1 privilege level 3    //将管理员的账号权限设置为 3（最高）
[HUAWEI-aaa] local-user admin1 service-type telnet
```

说明

使用 Telnet 协议存在安全风险，建议使用安全级别更高的 STelnet 登录设备，详细配置可根据设备版本参见相应的《配置指南-基础配置》。

4. 在维护终端上 Telnet 到交换机。出现用户视图的命令行提示符表示登录成功。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1 //输入交换机管理 IP，并回车

Login authentication
Username:admin1          //输入用户名和密码
Password:
Info: The max number of VTY users is 5, and the number
      of current VTY users on line is 1.
      The current login time is 2023-02-06 18:33:18+00:00.
<HUAWEI>                //用户视图命令行提示符
```

1.1.1.2.3.3 配置接口与 VLAN

配置接入层交换机

1. 以接入交换机 ACC1 为例，创建 ACC1 的业务 VLAN 10。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname ACC1           //修改设备名称为 ACC1
[ACC1] vlan batch 10             //批量创建 VLAN
```

2. 配置 ACC1 连接 CORE 的 Eth-Trunk1，透传部门 A 的 VLAN。

```
[ACC1] interface eth-trunk 1
[ACC1-Eth-Trunk1] port link-type trunk           //配置为 trunk 模式，用于透传 VLAN。
[ACC1-Eth-Trunk1] port trunk allow-pass vlan 10 //配置 Eth-Trunk1 透传 ACC1 上的业务 VLAN
[ACC1-Eth-Trunk1] mode lacp-static              //配置 Eth-Trunk1 为 lacp-static 模式
[ACC1-Eth-Trunk1] quit
[ACC1] interface GE 1/0/1                       //将成员接口加入 Eth-Trunk1
[ACC1-GE1/0/1] eth-Trunk 1
[ACC1-GE1/0/1] quit
[ACC1] interface GE 1/0/2
[ACC1-GE1/0/2] eth-Trunk 1
[ACC1-GE1/0/2] quit
```

3. 配置 ACC1 连接用户的接口，使用户加入 VLAN，并将接口配置成边缘端口。

```
[ACC1] interface GE 1/0/5           //配置连接 PC1 的接口
[ACC1-GE1/0/5] port link-type access
[ACC1-GE1/0/5] port default vlan 10
[ACC1-GE1/0/5] stp edged-port enable
[ACC1-GE1/0/5] quit
[ACC1] interface GE 1/0/6           //配置连接 PC2 的接口
[ACC1-GE1/0/6] port link-type access
[ACC1-GE1/0/6] port default vlan 10
[ACC1-GE1/0/6] stp edged-port enable
[ACC1-GE1/0/6] quit
[ACC1] interface GE 1/0/7           //配置连接打印机的接口
[ACC1-GE1/0/7] port link-type access
[ACC1-GE1/0/7] port default vlan 10
[ACC1-GE1/0/7] stp edged-port enable
[ACC1-GE1/0/7] quit
```

说明

如果把 ACC1 下接入的用户都加入 VLAN 10，为了配置简单，也可以 ACC1 上不配置 VLAN，而是把 CORE 的 Eth-Trunk1 以 access 方式加入 VLAN 10，这样 Eth-Trunk1 接入的用户全部属于 VLAN 10。

4. 配置 BPDU 保护功能，加强网络的稳定性。

```
[ACC1] stp bpdu-protection
```

配置核心层交换机

1. 批量创建 CORE 与 ACC1、ACC2 以及园区出口路由器互通的 VLAN。


```
<HUAWEI> system-view
[HUAWEI] sysname CORE           //修改设备名称为 CORE
[CORE] vlan batch 10 20 100     //批量创建 VLAN
```

2. 配置下行接口和 VLANIF 接口，VLANIF 接口用于部门 A 与部门 B 之间互访。以 CORE 连接 ACC1 的 Eth-Trunk1 为例。

```
[CORE] interface eth-trunk 1
[Core-Eth-Trunk1] port link-type trunk      //配置为 trunk 模式，用于透传 VLAN
[Core-Eth-Trunk1] port trunk allow-pass vlan 10 //配置 Eth-Trunk1 透传 ACC1 上的业务 VLAN
[Core-Eth-Trunk1] mode lacp-static          //配置为 lacp-static 模式
[Core-Eth-Trunk1] quit
[CORE] interface 10GE 1/0/1      //将成员接口加入 Eth-Trunk1
[Core-10GE1/0/1] eth-trunk 1
[Core-10GE1/0/1] quit
[CORE] interface 10GE 1/0/2
[Core-10GE1/0/2] eth-trunk 1
[Core-10GE1/0/2] quit
[CORE] interface Vlanif 10       //配置 VLANIF，使部门 A 与部门 B 之间三层互通
[Core-Vlanif10] ip address 10.10.10.1 24
[Core-Vlanif10] quit
[CORE] interface Vlanif 20       //配置 VLANIF，使部门 B 与部门 A 之间三层互通
[Core-Vlanif20] ip address 10.10.20.1 24
[Core-Vlanif20] quit
```

3. 配置上行接口和 VLANIF 接口，使园区网络与 Internet 互通。

```
[CORE] interface 10GE 1/0/20
[Core-10GE1/0/20] port link-type access     //配置为 access 模式
[Core-10GE1/0/20] port default vlan 100
[Core-10GE1/0/20] quit
[CORE] interface Vlanif 100      //配置 VLANIF，使 CORE 与路由器之间三层互通
[Core-Vlanif100] ip address 10.10.100.1 24
[Core-Vlanif100] quit
```

4. 完成接口和 VLAN 的配置后，可以通过以下命令查看配置结果，显示信息说明可选择对应设备版本查阅《命令参考》。

执行 **display eth-trunk** 命令检查 ACC1 上的 Eth-Trunk 接口配置结果。可以看到，ACC1 上接口 GE1/0/1 和 GE1/0/2 加入了 Eth-Trunk 1。

```
[ACC1] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1           WorkingMode: lacp-static
Preempt Delay: Disabled   Hash arithmetic: According to SA-XOR-DA
System Priority: 32768    System ID: 00e0-fc12-6704
```

Least Active-linknumber: 1 Max Active-linknumber: 8

Operate status: up Number Of Up Port In Trunk: 1

ActorPortName Status PortType PortPri PortNo PortKey PortState Weight

GE1/0/1 Selected 1000M 32768 2 289 10111100 1

GE1/0/2 Selected 1000M 32768 3 289 10100010 1

Partner:-----

ActorPortName SysPri SystemID PortPri PortNo PortKey PortState

GE1/0/1 32768 00e0-fc12-2212 32768 2 289 10111100

GE1/0/2 32768 00e0-fc12-2212 32768 3 289 10111100

执行 **display vlan** 命令检查 ACC1 上的 VLAN 配置结果。可以看到，ACC1 上，接口 GE1/0/5~GE1/0/7 以 Untagged 方式加入 VLAN 10，Eth-Trunk 1 以 Tagged 方式加入 VLAN 10。

[ACC1] **display vlan**

The total number of VLANs is : 1

U: Up; D: Down; TG: Tagged; UT: Untagged;

MP: Vlan-mapping; ST: Vlan-stacking;

#: ProtocolTransparent-vlan; *: Management-vlan;

VID Type Ports

10 common UT:GE1/0/5(U) GE1/0/6(U) GE1/0/7(U)

TG:Eth-Trunk1(U)

VID Status Property MAC-LRN Statistics Description

10 enable default enable disable VLAN 0010

执行 **display eth-trunk** 命令检查 CORE 上 Eth-Trunk 接口配置结果。可以看到，CORE 上，接口 10GE1/0/1 和 10GE1/0/2 加入了 Eth-Trunk 1。

[CORE] **display eth-trunk 1**

Eth-Trunk1's state information is:

Local:

LAG ID: 1 WorkingMode: **lACP-static**

Preempt Delay: Disabled Hash arithmetic: According to SA-XOR-DA

System Priority: 32768 System ID: 00e0-fc12-6703

Least Active-linknumber: 1 Max Active-linknumber: 8

Operate status: up Number Of Up Port In Trunk: 1

-

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight

10GE1/0/1	Selected 1000M	32768	2	289	10111100	1	

10GE1/0/2	Selected 1000M	32768	3	289	10100010	1	

Partner:

-

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState

10GE1/0/1	32768	00e0-fc12-2211	32768	2	289	10111100

10GE1/0/2	32768	00e0-fc12-2211	32768	3	289	10111100

执行 **display vlan** 命令检查 CORE 上 VLAN 配置结果。可以看到，CORE 上，接口 Eth-Trunk1、Eth-Trunk2 分别以 Tagged 方式加入 VLAN 10 和 VLAN 20；10GE1/0/20 以 Tagged 方式加入 VLAN 100。

[CORE] **display vlan**

The total number of VLANs is : 3

-

U: Up; D: Down; TG: Tagged; UT: Untagged;

MP: Vlan-mapping; ST: Vlan-stacking;

#: ProtocolTransparent-vlan; *: Management-vlan;

VID Type Ports

-

10 common TG:Eth-Trunk1(U)

20 common TG:Eth-Trunk2(U)

100 common TG:10GE1/0/20(U)

VID	Status	Property	MAC-LRN	Statistics	Description

-

10	enable	default	enable	disable	VLAN 0010

20	enable	default	enable	disable	VLAN 0020

100	enable	default	enable	disable	VLAN 0100

1.1.1.2.3.4 配置 DHCP

在 CORE 上配置 DHCP Server，使部门 A（VLAN10）和部门 B（VLAN20）的用户都能获取到正确的 IP 地址。

以下以部门 A 为例，说明 DHCP Server 的配置步骤。

说明

本文以基于全局地址池的 DHCP Server 举例。还可以配置基于接口地址池的 DHCP Server，详细操作可根据设备版本参见《配置指南-IP 地址与服务》。

1. 创建全局地址池，配置出口网关、租期（采用缺省值 1 天，不需配置）并配置为打印机（MAC 地址为 a-b-c）分配固定的 IP 地址 10.10.10.254。

```
<CORE> system-view
[CORE] dhcp enable
[CORE] ip pool 10
[CORE-ip-pool-10] network 10.10.10.0 mask 24 //配置部门 A 的用户可分配的地址池范围
[CORE-ip-pool-10] gateway-list 10.10.10.1 //配置部门 A 的用户的网关地址
[CORE-ip-pool-10] static-bind ip-address 10.10.10.254 mac-address a-b-c //配置为打印机分配固定的 IP 地址
[CORE-ip-pool-10] quit
```

2. 配置部门 A 的用户从全局地址池获取 IP 地址。

```
[CORE] interface vlanif 10
[CORE-Vlanif10] dhcp select global //配置部门 A 的用户从全局地址池获取 IP 地址
[CORE-Vlanif10] quit
```

3. 使用 **display ip pool** 命令，分别查看全局地址池 10 的配置和使用信息。

```
[CORE] display ip pool name 10
Pool-name      : 10
Pool-No        : 0
Lease          : 1 Days 0 Hours 0 Minutes
Domain-name    : -
DNS-server0    : -
NBNS-server0   : -
Netbios-type   : -
Position       : Local      Status       : Unlocked
Gateway-0      : 10.10.10.1
Network        : 10.10.10.0
Mask           : 255.255.255.0
VPN instance   : --

-----
Start      End      Total Used Idle(Expired) Conflict Disable
-----
10.10.10.1 10.10.10.254 253   4    249(0)    0     0
-----
```

说明

在 DHCP 服务器配置完成后，需要设置终端电脑网卡为自动获取地址，这样终端才能正常从 DHCP 服务器获取到地址，正常上网。

配置完动态分配地址之后，刚开电脑获取地址的时间比较长，这是因为对于开启了生成树协议的交换机，每当有电脑接入之后导致生成树重新收敛，所以需要的时间比较长；通过关闭接口的生成树协议或者把连接终端的交换机接口配置为边缘端口即可解决。

下面以 ACC1 为例，说明配置步骤。

关闭接口的生成树协议

```
[ACC1] interface GE 1/0/5
[ACC1-GE1/0/5] stp disable //undo stp enable 命令也可完成该功能
```

配置连接终端设备的交换机接口为边缘端口

```
[ACC1] interface GE 1/0/5
[ACC1-GE1/0/5] stp edged-port enable
[ACC1-GE1/0/5] quit
```

以上两种方法选择一种进行配置，终端电脑刚开机获取地址速度慢的问题就可以有效解决。

1.1.1.2.3.5 配置核心交换机路由

1. 在 CORE 上配置一条到园区出口网关的缺省静态路由，使内网数据可以发到出口路由器。

```
[CORE] ip route-static 0.0.0.0 0 10.10.100.2
```

2. 在 CORE 上使用 `display ip routing-table` 命令查看 IP 路由表。能够查看到有一条下一跳地址为 10.10.100.2 的缺省静态路由，表示静态路由配置完成。三条直连路由是链路发现自动生成。

```
[CORE] display ip routing-table
Route Flags: R – relay, D – download to fib
-----
Routing Tables: Public
Destinations : 5      Routes : 5
Destination/Mask  Proto  Pre  Cost   Flags NextHop   Interface
0.0.0.0/0         Static 60   0       RD 10.10.100.2  Vlanif100
10.10.10.0/24     Direct 0     0       D 10.10.10.1   Vlanif10
10.10.10.1/32     Direct 0     0       D 127.0.0.1    Vlanif10
10.10.20.0/24     Direct 0     0       D 10.10.20.1   Vlanif20
10.10.20.1/32     Direct 0     0       D 127.0.0.1    Vlanif20
10.10.100.0/24    Direct 0     0       D 10.10.100.1  Vlanif100
10.10.100.1/32    Direct 0     0       D 127.0.0.1    Vlanif100
```

1.1.1.2.3.6 配置出口路由器

说明

在配置出口路由器之前需要准备如下数据：公网接口的 IP 地址：1.1.1.2/30，公网网关地址：1.1.1.1，DNS 地址：8.8.8.8，这些参数在申请宽带的时候由运营商提供，实际网络中请以运营商提供的数据为准。

1. 配置出口路由器内网接口和公网接口的 IP 地址。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] ip address 1.1.1.2 30
[Router] interface GigabitEthernet 1/0/0
[Router-GigabitEthernet1/0/0] ip address 10.10.100.2 24
```

2. 配置允许上网的 acl，将所有允许访问 Internet 的用户网段写入该 acl。

```
[Router] acl 2000
[Router-acl-basic-2000] rule permit source 10.10.10.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 10.10.20.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 10.10.100.0 0.0.0.255
```

3. 在连接公网的接口配置 NAT 转换实现内网用户访问 Internet。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 2000
```

4. 配置到内网的明细路由和到公网的静态缺省路由。

```
[Router] ip route-static 10.10.10.0 255.255.255.0 10.10.100.1
[Router] ip route-static 10.10.20.0 255.255.255.0 10.10.100.1
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

5. 配置 DNS 地址解析功能，DNS 服务器地址为运营商给的。

```
[Router] dns resolve
[Router] dns server 8.8.8.8
```

1.1.1.2.3.7 配置 DHCP Snooping 和 IPSG

配置了 DHCP 功能之后，部门内用户主机可以自动获取地址。但是为了防止员工在内网私自接一个小路由器并开启 DHCP 自动分配地址的功能，导致内网合法用户获取到了私接的小路由器分配的地址而不能正常上网，还需要配置 DHCP Snooping 功能。

以下以部门 A 为例，说明 DHCP Snooping 的配置过程。

1. 在接入交换机 ACC1 上开启 DHCP Snooping 功能。

```
<ACC1> system-view
[ACC1] dhcp enable //使能 DHCP 功能
[ACC1] dhcp snooping enable //使能 DHCP Snooping 功能
```

2. 在连接 DHCP 服务器的接口上使能 DHCP Snooping 功能，并将此接口配置为信任接口。

```
[ACC1] interface eth-trunk 1
[ACC1-Eth-Trunk1] dhcp snooping enable //使能 DHCP Snooping 功能
[ACC1-Eth-Trunk1] dhcp snooping trusted //配置为信任接口
[ACC1-Eth-Trunk1] quit
```

3. 在连接终端的接口上使能 DHCP Snooping 功能。

```
[ACC1] interface GE 1/0/5 //配置连接 PC1 的接口
```

```
[ACC1-GE1/0/5] dhcp snooping enable
[ACC1-GE1/0/5] quit
[ACC1] interface GE 1/0/6           //配置连接 PC2 的接口
[ACC1-GE1/0/6] dhcp snooping enable
[ACC1-GE1/0/6] quit
[ACC1] interface GE 1/0/7           //配置连接打印机的接口
[ACC1-GE1/0/7] dhcp snooping enable
[ACC1-GE1/0/7] quit
```

完成上述配置之后，部门 A 的用户就可以从合法的 DHCP 服务器获取 IP 地址，内网私接的小路由器分配地址不会干扰到内网正常用户。

为了防止部门内用户私自更改 IP 地址后攻击网络，在接入交换机开启 DHCP Snooping 功能后，还需要开启 IP 报文检查功能，具体配置以 ACC1 为例。

4. 在接入交换机 ACC1 上开启 VLAN10 的 IP 报文检查功能。

```
[ACC1] vlan 10
[ACC1-vlan10] ipv4 source check user-bind enable //使能 IP 报文检查功能
[ACC1-vlan10] quit
```

这样 ACC1 从 VLAN10 收到报文后会将报文与动态绑定表的表项进行匹配，放行匹配的报文，丢弃不匹配的报文。如果不想对整个 VLAN 收到的报文进行检查，可以只在连接某个终端的接口上开启 IP 报文检查功能。

关于交换机防止内网私接小路由器（仿冒 DHCP 服务器）以及防止用户私自更改 IP 地址的具体说明及详细配置，请参考《配置指南-IP 地址与服务》中“DHCP Snooping 配置>配置 DHCP Snooping 的基本功能及配置举例”和《配置指南-安全》中“IPSG 配置>配置 IPSG 及配置举例”。

1.1.1.2.3.8 业务验证

1. 部门内部选两台 PC 进行 ping 测试，验证部门内部二层互通是否正常。以部门 A 为例，PC1 和 PC2 是通过 ACC1 实现二层互通的。如果 PC1 和 PC2 之间互 ping 测试正常则说明二层互通正常。

```
<PC1> ping 10.10.10.100    //假设 PC2 通过 DHCP 自动获取的 IP 地址为 10.10.10.100
PING 10.10.10.100 data bytes, press CTRL_C to break
  Reply from 10.10.10.100 : bytes=56 Sequence=1 ttl=253 time=62 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=2 ttl=253 time=16 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=3 ttl=253 time=62 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=4 ttl=253 time=94 ms
  Reply from 10.10.10.100 : bytes=56 Sequence=5 ttl=253 time=63 ms

--- 10.10.10.100 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received    //能 Ping 通，说明 PC1 与 PC2 之间二层互通正常
```

2. 从两个部门内各选一台 PC 进行 ping 测试，验证部门之间通过 VLANIF 实现三层互通是否正常。部门 A 和部门 B 之间的用户是通过 CORE 上的 VLANIF 实现三层互通的。如果 PC1 和 PC3 之间互 ping 测试正常则说明两个部门之间通过 VLANIF 实现三层互通正常。ping 测试命令与步骤 1 类似。

3. 每个部门各选一台 PC 进行 ping 公网地址测试，验证公司内网用户访问 Internet 是否正常。以部门 A 为例，一般可以通过在 PC1 上 ping 公网网关地址（即与出口路由器对接的运营商设备的 IP 地址）来验证是否可以访问 Internet，如果 ping 测试正常则说明内网用户访问 Internet 正常。ping 测试命令与步骤 1 类似。

1.1.1.2.3.9 保存配置

通过命令行配置的数据是临时性的。如果不保存，交换机重启后这些配置都会丢失。

如果要使当前配置在交换机重启后仍然有效，需要将当前配置保存为配置文件。

1. 保存配置。（以 CORE 举例）

```
<CORE> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0..
Save the configuration successfully.
```

1.1.1.3 中小园区组网场景

[中小园区组网图](#)

[数据规划](#)

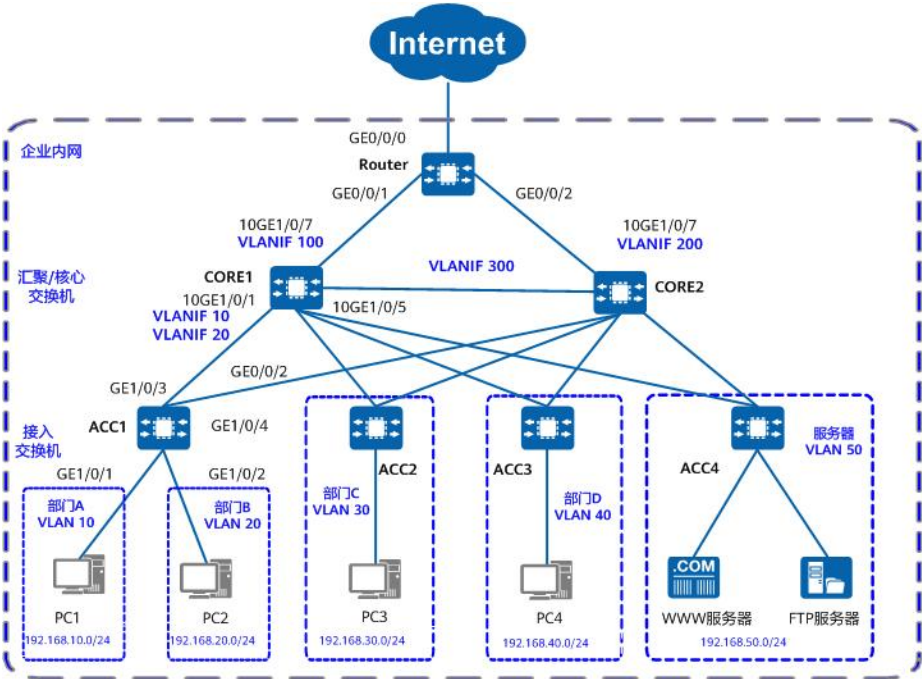
[快速配置中小园区](#)

1.1.1.3.1 中小园区组网图

说明

本举例中的接入交换机 ACC1、ACC2、ACC3、ACC4 以 V600R022C10 版本的 S5735-L-V2 为例、核心/汇聚交换机 CORE1 和 CORE2 以 V600R022C10 版本的 S8700-4 为例、出口路由器 Router 以 AR651 V300R022C10 为例。

图 1 中小园区组网图



在中小园区中，S5735-L-V2 通常部署在网络的接入层，S8700-4 通常部署在网络的核心，出口路由器一般选用 AR 系列路由器。

核心交换机配置 VRRP 保证网络可靠性，配置负载分担有效利用资源。

每个部门业务划分到一个 VLAN 中，部门间的业务在 CORE 上通过 VLANIF 三层互通。

核心交换机作为 DHCP Server，为园区用户分配 IP 地址。

接入交换机上配置 DHCP Snooping 功能，防止内网用户私接小路由器分配 IP 地址；同时配置 IP 报文检查功能，防止内网用户私自更改 IP 地址。

1.1.1.3.2 数据规划

在配置之前，需按照下面的表格准备好数据。以下数据将在本文后续章节使用。

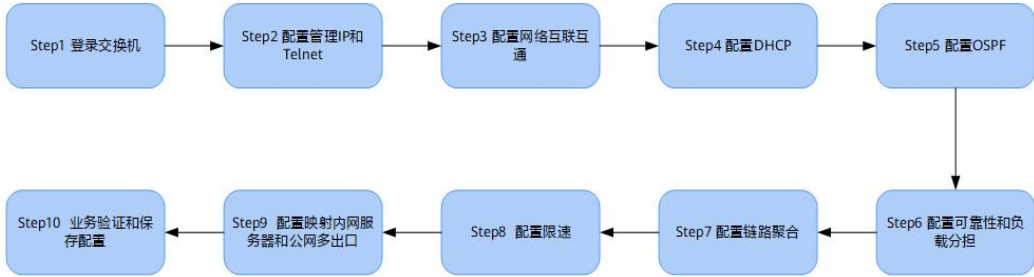
操作	准备项	数据	说明
配置管理 IP 和 Telnet	管理 IP 地址	10.10.1.1/24	管理 IP 用于登录交换机。
	管理 VLAN	VLAN 5	框式和盒式交换机管理口都是 MEth0/0/0。 对于没有管理口的交换机建议使用 VLANIF 接口进行带内管理。
配置接口和 VLAN	端口类型	连接交换机的端口建议设置为 trunk，连接 PC 的端口设置为 access。	trunk 类型端口一般用于连接交换机。 access 类型端口一般用于连接 PC。 hybrid 类型端口是通用端口，既可以用来连接交换机，也可用来连接 PC。
	VLAN ID	ACC1: VLAN 10 20 CORE1: VLAN 10、20、30、40、50、100、300	交换机有缺省 VLAN1。

操作	准备项	数据	说明
			为二层隔离部门 A 和部门 B，将部门 A 划分到 VLAN 10 中，部门 B 划分到 VLAN 20 中，将部门 C 划分到 VLAN 30 中，将部门 D 划分到 VLAN 40 中。 CORE1 通过 VLANIF100 连接出口路由器。
配置 DHCP	DHCP Server	CORE1、CORE2	在 CORE1、CORE2 上部署 DHCP Server。
	地址池	VLAN 10: ip pool 10 VLAN 20: ip pool 20	部门 A 的终端从 ip pool 10 中获取 IP 地址。 部门 B 的终端从 ip pool 20 中获取 IP 地址。
	地址分配方式	基于全局地址池	无
配置核心交换机	IP 地址	CORE1: VLANIF100 172.16.1.1/24 VLANIF300 172.16.3.1/24 VLANIF10 192.168.10.1/24 VLANIF20 192.168.20.1/24	VLANIF100 用于 CORE1 与园区出口路由器对接。 VLANIF300 用于 CORE1 与 CORE2 对接。 CORE1 上需要配置一条主用路由，下一跳指向出口路由器； 一条备用路由，下一跳指向 CORE2。 在 CORE1 上配置 VLANIF10、VLANIF20 的 IP 地址后， 部门 A 与部门 B 之间可以通过 CORE1 互访。
	链路聚合	—	Eth-Trunk 链路聚合有手工负载分担和静态 LACP 两种工作模式。
配置出口路由器	公网接口及 IP 地址	GE0/0/0: 1.1.1.2/30	GE0/0/0 为出口路由器连接 Internet 的接口，一般称为公网接口。
	公网网关	1.1.1.1/30	该地址是与出口路由器对接的运营商设备的 IP 地址，出口路由器上需要配置一条缺省路由指向该地址，用于指导内网流量转发至 Internet。
	DNS 地址	8.8.8.8	DNS 服务器用于将域名解析成 IP 地址。
	内网接口及 IP 地址	GE0/0/1: 172.16.1.2/24 GE0/0/2: 172.16.2.2/24	GE0/0/1、GE0/0/2 为出口路由器连接内网的接口，GE0/0/1 连接主设备，GE0/0/2 连接备设备。
配置 DHCP Snooping 和 IPSG	信任接口	GE1/0/3 GE1/0/4	配置信任接口后，用户只会接收从信任接口进入的 DHCP 报文，防止内网私接小路由器为主机分配 IP 地址。

操作	准备项	数据	说明
配置内网服务器	FTP 服务器 WWW 服务器	FTP 服务器： 192.168.50.10 WWW 服务器： 192.168.50.20	1、出口路由器会通过 NAT 实现服务器公网地址和私网地址之间的映射。 2、外网用户可以通过访问公网地址访问服务器。

1.1.1.3.3 快速配置中小园区

您可以按照下列流程配置各个设备的数据，连通园区内用户，并使园区内用户可访问外网。



[登录设备（以交换机为例）](#)

[配置管理 IP 和 Telnet](#)

[配置网络互连互通](#)

[配置 DHCP](#)

[配置 OSPF](#)

[配置可靠性和负载分担](#)

[配置链路聚合](#)

[配置限速](#)

[配置映射内网服务器和公网多出口](#)

[业务验证和保存配置](#)

1.1.1.3.3.1 登录设备（以交换机为例）

1. 请使用 Console 通信电缆（产品随设备附带）连接交换机与 PC。
2. 在 PC 上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。
连接的接口请根据实际情况进行选择。例如，在 Windows 系统中，可以通过在“设备管理器”中查看端口信息，选择连接的接口。交换机上的通信参数如[表 1](#)所示。

表 1 交换机 Console 口缺省值

参数	缺省值
传输速率	9600bit/s
流控方式	不进行流控
校验方式	不进行校验
停止位	1
数据位	8

3. 在 PC 的终端仿真软件界面按 **Connect** 键，直到出现如下信息，提示用户设置登录密码。

```
Login authentication
Username:admin1
Password:
Info: The max number of VTY users is 20, and the number
      of current VTY users on line is 1.
      The current login time is 2023-02-26 10:10:05+08:00.
```

完成 Console 登录密码设置后，用户便可以配置交换机，需要帮助可随时键入“?”。

1.1.1.3.3.2 配置管理 IP 和 Telnet

配置设备管理 IP 地址后，可以通过管理 IP 远程登录设备，下面以交换机 CORE1 为例说明配置管理 IP 和 Telnet 的方法。

1. 配置管理 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] vlan 5           //创建交换机管理 VLAN 5
[HUAWEI-VLAN5] management-vlan
[HUAWEI-VLAN5] quit
[HUAWEI] interface vlanif 5   //创建交换机管理 VLAN 的 VLANIF 接口
[HUAWEI-vlanif5] ip address 10.10.1.1 24 //配置 VLANIF 接口 IP 地址
[HUAWEI-vlanif5] quit
```

2. 将管理接口加入到管理 VLAN 。

```
[HUAWEI] interface 10GE 1/0/8   //假设连接网管的接口为 10GE 1/0/8，非直连，中间有二层设备
[HUAWEI-10GE1/0/8] port link-type trunk
[HUAWEI-10GE1/0/8] port trunk allow-pass vlan 5
[HUAWEI-10GE1/0/8] quit
```

3. 配置 Telnet。

```
[HUAWEI] telnet server enable   //Telnet 出厂时是关闭的，需要打开
[HUAWEI] telnet server-source -i vlanif 5
```

```
Warning: Telnet server source configuration will take effect in the next login. Continue? [Y/N]: Y
[HUAWEI] user-interface vty 0 4 //Telnet 常用于设备管理员登录，推荐使用 AAA 认证
[HUAWEI-ui-vty0-4] protocol inbound telnet //缺省情况下，用户界面支持所有协议类型，包括 SSH 和 Telnet。
[HUAWEI-ui-vty0-4] authentication-mode aaa
[HUAWEI-ui-vty0-4] idle-timeout 15
[HUAWEI-ui-vty0-4] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin1 password irreversible-cipher Helloworld@6789 //配置管理员 Telnet 登
录交换机的用户名和密码。用户名不区分大小写，密码区分大小写
[HUAWEI-aaa] local-user admin1 privilege level 3 //将管理员的账号权限设置为 3（最高）
[HUAWEI-aaa] local-user admin1 service-type telnet
[HUAWEI-aaa] quit
```

说明

使用 Telnet 协议存在安全风险，建议使用安全级别更高的 STelnet 登录设备，详细配置可根据设备版本参见相应的《配置指南-基础配置》。

- 在维护终端上 Telnet 到交换机。出现用户视图的命令行提示符表示登录成功。

```
C:\Documents and Settings\Administrator> telnet 10.10.1.1 //输入交换机管理 IP，并回车

Login authentication

Username:admin1 //输入用户名和密码
Password:
Info: The max number of VTY users is 5, and the number
of current VTY users on line is 1.
The current login time is 2023-05-06 18:33:18+00:00.
<HUAWEI> //用户视图命令行提示符
```

1.1.1.3.3.3 配置网络互连互通

配置接入层交换机

- 以接入交换机 ACC1 为例，创建 ACC1 的业务 VLAN 10 和 20。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1 //修改设备名称为 ACC1
[ACC1] vlan batch 10 20 //批量创建 VLAN
```

- 配置 ACC1 连接 CORE1 和 CORE2 的 GE1/0/3 和 GE1/0/4，透传部门 A 和部门 B 的 VLAN。

```
[ACC1] interface GE 1/0/3
[ACC1-GE1/0/3] port link-type trunk //配置为 trunk 模式，用于透传 VLAN。
[ACC1-GE1/0/3] port trunk allow-pass vlan 10 20 //配置 GE1/0/3 透传 ACC1 上的业务 VLAN
```

```
[ACC1-GE1/0/3] quit
[ACC1] interface GE 1/0/4
[ACC1-GE1/0/4] port link-type trunk //配置为 trunk 模式，用于透传 VLAN。
[ACC1-GE1/0/4] port trunk allow-pass vlan 10 20 //配置 GE1/0/4 透传 ACC1 上的业务 VLAN
[ACC1-GE1/0/4] quit
```

3. 配置 ACC1 连接用户的接口，使各部门加入 VLAN。

```
[ACC1] interface GE 1/0/1 //配置连接部门 A 的接口
[ACC1-GE1/0/1] port link-type access
[ACC1-GE1/0/1] port default vlan 10
[ACC1-GE1/0/1] quit
[ACC1] interface GE 1/0/2 //配置连接部门 B 的接口
[ACC1-GE1/0/2] port link-type access
[ACC1-GE1/0/2] port default vlan 20
[ACC1-GE1/0/2] quit
```

4. 配置 BPDU 保护功能，加强网络的稳定性。

```
[ACC1] stp bpdu-protection
```

说明

如果把 ACC1 下接入的用户都加入 VLAN 10，为了配置简单，也可以 ACC1 上不配置 VLAN，而把 CORE1、CORE2 与 ACC1 直接相连的接口以 access 方式加入 VLAN10，这样通过 ACC1 接入的用户全部属于 VLAN10。

配置汇聚/核心层交换机

1. 以汇聚/核心交换机 CORE1 为例，创建其与接入交换机、备份设备以及园区出口路由器互通的 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname CORE1 //修改设备名称为 CORE1
[CORE1] vlan batch 10 20 30 40 50 100 300 //批量创建 VLAN
```

2. 配置用户侧的接口 VLAN 和 VLANIF，VLANIF 接口用于部门之间互访。以 CORE1 连接 ACC1 的 10GE1/0/1 接口为例，其他接口不再赘述。

```
[CORE1] interface 10GE 1/0/1
[CORE1-10GE1/0/1] port link-type trunk //配置为 trunk 模式，用于透传 VLAN
[CORE1-10GE1/0/1] port trunk allow-pass vlan 10 20 //配置 10GE1/0/1 透传 ACC1 上的业务 VLAN
[CORE1-10GE1/0/1] quit
[CORE1] interface Vlanif 10 //配置 VLANIF10，使部门之间三层互通
[CORE1-Vlanif10] ip address 192.168.10.1 24
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20 //配置 VLANIF20，使部门之间三层互通
[CORE1-Vlanif20] ip address 192.168.20.1 24
[CORE1-Vlanif20] quit
```

3. 配置连接出口路由器的接口 VLAN 和 VLANIF。

```
[CORE1] interface 10GE 1/0/7
[CORE1-10GE1/0/7] port link-type access //配置为 access 模式
[CORE1-10GE1/0/7] port default vlan 100
[CORE1-10GE1/0/7] quit
[CORE1] interface Vlanif 100 //配置 VLANIF，使 CORE1 与路由器之间三层互通
[CORE1-Vlanif100] ip address 172.16.1.1 24
[CORE1-Vlanif100] quit
```

4. 配置两个核心交换机直连的接口 VLAN 和 VLANIF。

```
[CORE1] interface 10GE 1/0/5
[CORE1-10GE1/0/5] port link-type access //配置为 access 模式
[CORE1-10GE1/0/5] port default vlan 300
[CORE1-10GE1/0/5] quit
[CORE1] interface Vlanif 300
[CORE1-Vlanif300] ip address 172.16.3.1 24
[CORE1-Vlanif300] quit
```

查看配置结果

- 完成接口和 VLAN 的配置后，可以通过以下命令查看配置结果，显示信息说明可根据不同设备版本查阅相应的《命令参考》。

执行 **display vlan** 命令检查 ACC1 上的 VLAN 配置结果。

```
[ACC1] display vlan
The total number of VLANs is : 2
-----
-
U: Up;      D: Down;    TG: Tagged;    UT: Untagged;
MP: Vlan-mapping;      ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
-----
-
VID Type  Ports
-----
-
10 common UT: GE0/0/1(U) TG:GE0/0/3(U) GE0/0/4(U)
20 common UT: GE0/0/2(U) TG:GE0/0/3(U) GE0/0/4(U) //可以看到，ACC1 上，下行接口已与业务
VLAN 相对应，上行接口透传所有业务 VLAN。
VID Status Property  MAC-LRN Statistics Description
-----
-
10 enable default    enable disable  VLAN 0010
```

```
20 enable default    enable disable  VLAN 0020
```

执行 **display vlan** 命令检查 CORE1 上的 VLAN 配置结果。

```
[CORE1] display vlan
```

```
The total number of VLANs is : 7
```

```
-----
```

```
-
```

```
U: Up;      D: Down;    TG: Tagged;    UT: Untagged;
```

```
MP: Vlan-mapping;      ST: Vlan-stacking;
```

```
#: ProtocolTransparent-vlan;  *: Management-vlan;
```

```
-----
```

```
-
```

```
VID Type  Ports
```

```
-----
```

```
-
```

```
10 common TG:10GE1/0/1(U)
```

```
20 common TG:10GE1/0/1(U)
```

```
30 common TG:10GE1/0/2(U)
```

```
40 common TG:10GE1/0/3(U)
```

```
50 common TG:10GE1/0/4(U)
```

```
100 common TG:10GE1/0/7(U)
```

```
300 common UT:10GE1/0/5(U)           //可以看到，CORE1 上，与各接入交换机相连的接口已加入接入交换机对应的业务 VLAN。
```

```
VID Status Property  MAC-LRN Statistics Description
```

```
-----
```

```
-
```

```
10 enable default    enable disable  VLAN 0010
```

```
20 enable default    enable disable  VLAN 0020
```

```
30 enable default    enable disable  VLAN 0030
```

```
40 enable default    enable disable  VLAN 0040
```

```
50 enable default    enable disable  VLAN 0050
```

```
100 enable default    enable disable  VLAN 0100
```

```
300 enable default    enable disable  VLAN 0300
```

配置出口路由器的接口地址

1. 配置连接内网的接口地址。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname Router           //修改设备名称为 Router
```

```
[Router] interface GigabitEthernet 0/0/1
```

```
[Router-GigabitEthernet0/0/1] ip address 172.16.1.2 24 //配置与主设备互连的接口地址
```

```
[Router-GigabitEthernet0/0/1] quit
```



```
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] ip address 172.16.2.2 24 //配置与备设备互连的接口地址
[Router-GigabitEthernet0/0/2] quit
```

2. 配置连接公网的接口地址。

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] ip address 1.1.1.2 30 //配置路由器连接公网的接口地址
[Router-GigabitEthernet0/0/0] quit
```

（可选）配置静态路由实现网络互通

若配置动态路由，此步骤则不需配置。

1. 分别在 CORE1 和 CORE2 上面配置一条缺省静态路由指向出口路由器及其备份路由。

```
[CORE1] ip route-static 0.0.0.0 0.0.0.0 172.16.1.2 //CORE1 指向出口路由器的缺省静态路由
[CORE1] ip route-static 0.0.0.0 0.0.0.0 172.16.3.2 preference 70 //CORE1 指向 CORE2 的备份静态路由
[CORE2] ip route-static 0.0.0.0 0.0.0.0 172.16.2.2
[CORE2] ip route-static 0.0.0.0 0.0.0.0 172.16.3.1 preference 70
```

2. 在出口路由器配置一条缺省静态路由指向运营商。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

3. 在出口路由器配置到内网的主备路由，主路由下一跳指向 CORE1，备路由下一跳指向 CORE2。

```
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.1.1
[Router] ip route-static 192.168.10.0 255.255.255.0 172.16.2.1 preference 70 //配置到达 VLAN10 网段指向
备设备的备路由
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.1.1
[Router] ip route-static 192.168.20.0 255.255.255.0 172.16.2.1 preference 70 //配置到达 VLAN20 网段指向
备设备的备路由
```

配置 VRRP 主备备份实现虚拟网关冗余

正常情况下内网用户流量都上送到 CORE1 进行处理，只有当 CORE1 出故障之后，VRRP 备份组切换 CORE2 为主设备，内网用户流量上送到 CORE2。

1. 配置示例：在 CORE1 和 CORE2 上创建 VRRP 备份组 1 和 2，配置 CORE1 的优先级为 120，抢占延时为 20 秒，作为 VLAN10 和 VLAN20 的 Master 设备。

```
[CORE1] interface Vlanif 10
[CORE1-Vlanif10] vrrp vrid 1 virtual-ip 192.168.10.3 //配置 VRRP group 1 的虚地址
[CORE1-Vlanif10] vrrp vrid 1 priority 120 //配置 CORE1 的优先级为 120
[CORE1-Vlanif10] vrrp vrid 1 preempt-mode timer delay 20
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20
```

```
[CORE1-Vlanif20] vrrp vrid 2 virtual-ip 192.168.20.3 //配置 VRRP group 2 的虚地址
[CORE1-Vlanif20] vrrp vrid 2 priority 120
[CORE1-Vlanif20] vrrp vrid 2 preempt-mode timer delay 20
[CORE1-Vlanif20] quit
```

2. CORE2 的优先级为缺省值，作为 VLAN10 和 VLAN20 的 Backup 设备。

```
[CORE2] interface Vlanif 10
[CORE2-Vlanif10] vrrp vrid 1 virtual-ip 192.168.10.3
[CORE2-Vlanif10] quit
[CORE2] interface Vlanif 20
[CORE2-Vlanif20] vrrp vrid 2 virtual-ip 192.168.20.3
[CORE2-Vlanif20] quit
```

说明

由于 CORE1、CORE2 和 ACC1 之间物理成环，实际链路不成环，而交换机默认是开启 stp 功能的。为了避免影响 CORE1 和 CORE2 之间 VRRP 主备备份的状态，在此需要关闭接入交换机连接上行链路接口的 stp 功能，具体配置命令如下：

```
[ACC1] interface GE 1/0/3
[ACC1-GE1/0/3] stp disable //配置关闭 ACC1 上行链路接口的 stp 功能
[ACC1-GE1/0/3] quit
[ACC1] interface GE 1/0/4
[ACC1-GE1/0/4] stp disable
[ACC1-GE1/0/4] quit
```

如果确保网络中没有环路的话也可以直接关闭整机的 stp 功能，配置命令如下：

```
[ACC1] stp disable
Warning:The global STP state will be changed. Continue? [Y/N] y
```

配置出口路由器实现内网共享上网

1. 配置允许上网的 ACL。以 VLAN 10 和 20 的用户为例：

```
[Router] acl 2000
[Router-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255 //配置允许 VLAN 10 的用户上网
[Router-acl-basic-2000] rule permit source 192.168.20.0 0.0.0.255 //配置允许 VLAN 20 的用户上网
[Router-acl-basic-2000] rule permit source 172.16.1.0 0.0.0.255
[Router-acl-basic-2000] rule permit source 172.16.2.0 0.0.0.255
[Router-acl-basic-2000] quit
```

2. 在连接公网的接口配置 NAT 转换实现内网上网。

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] nat outbound 2000
[Router-GigabitEthernet0/0/0] quit
```

3. 配置 DNS 地址解析功能，DNS 服务器地址为运营商指定。

```
[Router] dns resolve
[Router] dns server 8.8.8.8
```

4. 做完上述配置之后，给内网 VLAN10 的用户配置静态地址，网关设置为 192.168.10.3 即可以实现上网。

1.1.1.3.3.4 配置 DHCP

配置 DHCP 服务器

网络管理员为每个终端配置固定的 IP 地址，当网络规模逐渐增大，为终端手工配置地址变得繁琐和难以管理。为减轻管理负担，管理员决定所有终端用户全部改为自动从 DHCP 服务器获取地址，除了个别必须固定地址的终端。

配置核心交换机作为 DHCP Server，使所有部门的用户都能动态获取到正确的 IP 地址。以下以 CORE1 作为主用 DHCP Server，以部门 A 为例，说明 DHCP Server 的配置步骤。

说明

本文以基于全局地址池的 DHCP Server 为例。还可以配置基于接口地址池的 DHCP Server，详细操作请根据设备版本参见相应的《配置指南-IP 地址与服务》。

VRRP 组网环境下，为防止主备切换而产生 IP 地址冲突的问题，因此在配置 DHCP 服务器时，主设备分配地址段的前一半地址，备设备分配地址段的后一半地址。

1. 配置 CORE1 作为主用 DHCP 服务器，分配地址段的前一半地址。

```
<CORE1> system-view
[CORE1] dhcp enable
[CORE1] ip pool 10
[CORE1-ip-pool-10] gateway-list 192.168.10.3 //配置网关地址
[CORE1-ip-pool-10] network 192.168.10.0 mask 24 //配置可分配的 IP 地址范围
[CORE1-ip-pool-10] excluded-ip-address 192.168.10.128 192.168.10.254 //配置排除地址段后一半地址
[CORE1-ip-pool-10] lease day 0 hour 20 minute 0 //配置租期
[CORE1-ip-pool-10] dns-list 8.8.8.8 //配置 DNS 服务器地址
[CORE1-ip-pool-10] quit
```

2. 配置 CORE2 作为备用 DHCP 服务器，分配地址段的后一半地址。

```
<CORE2> system-view
[CORE2] dhcp enable
[CORE2] ip pool 10
[CORE2-ip-pool-10] gateway-list 192.168.10.3
[CORE2-ip-pool-10] network 192.168.10.0 mask 24
[CORE2-ip-pool-10] excluded-ip-address 192.168.10.1 192.168.10.2
[CORE2-ip-pool-10] excluded-ip-address 192.168.10.4 192.168.10.127
[CORE2-ip-pool-10] lease day 0 hour 20 minute 0
```

```
[CORE2-ip-pool-10] dns-list 8.8.8.8
[CORE2-ip-pool-10] quit
```

对 VLAN20 配置 DHCP 动态分配地址方式同上。

3. 配置部门 A 的用户从全局地址池获取 IP 地址。

```
[CORE1] interface vlanif 10
[CORE1-Vlanif10] dhcp select global //配置部门 A 的用户从全局地址池获取 IP 地址
[CORE1-Vlanif10] quit
[CORE2] interface vlanif 10
[CORE2-Vlanif10] dhcp select global
[CORE2-Vlanif10] quit
```

4. 使用 display ip pool 命令，查看全局地址池 10 的配置和使用情况。

```
[CORE1] display ip pool name 10
Pool-name      : 10
Pool-No       : 0
Lease         : 0 Days 20 Hours 0 Minutes
Domain-name    : -
DNS-server0   : 8.8.8.8
NBNS-server0  : -
Netbios-type   : -
Position      : Local      Status      : Unlocked
Gateway-0     : 192.168.10.3
Network       : 192.168.10.0
Mask          : 255.255.255.0
VPN instance   : --

-----
      Start      End    Total Used Idle(Expired) Conflict Disable
-----
192.168.10.1 192.168.10.254 253   1   125(0)      0    127
```

说明

在 DHCP 服务器配置完成后，需要设置终端电脑网卡为自动获取地址，这样终端才能正常从 DHCP 服务器获取到地址，正常上网。

配置完动态分配地址之后，刚开电脑获取地址的时间比较长，这是因为对于开启了生成树协议的交换机，每当有电脑接入之后导致生成树重新计算收敛，所以需要的时间比较长；通过关闭接口的生成树协议或者把连接终端的交换机接口配置为边缘端口即可解决。

下面以 ACC1 为例，说明配置步骤。

关闭接口的生成树协议

```
[ACC1] interface GE 1/0/1
[ACC1-GE1/0/1] stp disable //undo stp enable 命令也可完成该功能
[ACC1-GE1/0/1] quit
```

配置连接终端设备的交换机接口为边缘端口

```
[ACC1] interface GE 1/0/1
[ACC1-GE1/0/1] stp edged-port enable
[ACC1-GE1/0/1] quit
```

以上两种方法选择一种进行配置，终端电脑刚开机获取地址速度慢的问题就可以有效解决。

配置 DHCP Snooping 和 IPSG

配置了 DHCP 功能之后，部门内用户主机可以自动获取地址。但是为了防止员工在内网私自接一个小路由器（仿冒 DHCP 服务器）并开启 DHCP 自动分配地址的功能，导致内网合法用户获取到了私接的小路由器分配的地址而不能正常上网，还需要配置 DHCP Snooping 功能。

以下以部门 A 为例，说明 DHCP Snooping 的配置过程。

1. 在接入交换机 ACC1 上开启 DHCP Snooping 功能。

```
<ACC1> system-view
[ACC1] dhcp enable //使能 DHCP 功能
[ACC1] dhcp snooping enable //使能 DHCP Snooping 功能
```

2. 在连接终端的接口上使能 DHCP Snooping 功能。

```
[ACC1] interface GE 1/0/1 //配置连接部门 A 的接口
[ACC1-GE1/0/1] dhcp snooping enable
[ACC1-GE1/0/1] quit
[ACC1] interface GE 1/0/2 //配置连接部门 B 的接口
[ACC1-GE1/0/2] dhcp snooping enable
[ACC1-GE1/0/2] quit
```

3. 在连接 DHCP 服务器的接口上使能 DHCP Snooping 功能，并将此接口配置为信任接口。

```
[ACC1] interface GE 1/0/3 //配置连接 CORE1 的接口
[ACC1-GE1/0/3] dhcp snooping enable //使能 DHCP Snooping 功能
[ACC1-GE1/0/3] dhcp snooping trusted //配置为信任接口
[ACC1-GE1/0/3] quit
[ACC1] interface GE 1/0/4 //配置连接 CORE2 的接口
[ACC1-GE1/0/4] dhcp snooping enable
[ACC1-GE1/0/4] dhcp snooping trusted
[ACC1-GE1/0/4] quit
```

完成上述配置之后，部门 A 的用户就可以从合法的 DHCP 服务器获取 IP 地址，内网私接的小路由器分配地址不会干扰到内网正常用户。

为了防止部门内用户私自更改 IP 地址后攻击网络，在接入交换机开启 DHCP Snooping 功能后，还需要开启 IP 报文检查功能，具体配置以 ACC1 为例。

4. 在接入交换机 ACC1 上开启 VLAN10 的 IP 报文检查功能。

```
[ACC1] vlan 10
[ACC1-vlan10] ipv4 source check user-bind enable //使能 IP 报文检查功能
```

```
[ACC1-vlan10] quit
```

这样 ACC1 从 VLAN10 收到报文后会将报文与动态绑定表的表项进行匹配，放行匹配的报文，丢弃不匹配的报文。如果不想对整个 VLAN 收到的报文进行检查，可以只在连接某个终端的接口上开启 IP 报文检查功能。

关于交换机防止内网私接小路由器（仿冒 DHCP 服务器）以及防止用户私自更改 IP 地址的具体说明及详细配置，请根据设备版本参考相应的《配置指南-IP 业务与服务》中“DHCP Snooping 配置”和《配置指南-安全》中“IPSG 配置”。

1.1.1.3.3.5 配置 OSPF

说明

由于内网互联使用的是静态路由，在链路出现故障之后需要管理员手动配置新的静态路由，造成网络长时间中断，影响业务。为了减少这种故障的发生，使用动态路由协议是一种不错的选择。动态路由有自己的算法，在链路出现故障之后动态路由根据自己的算法及时把流量切换到正常的链路，等到故障恢复之后流量又切过来。下面以动态路由协议 OSPF 为例进行配置：

1. 删除两台汇聚/核心交换机的静态路由配置。

```
[CORE1] undo ip route-static all  
[CORE2] undo ip route-static all
```

2. 删除出口路由器到内网的静态路由，保留到公网的缺省路由。

```
[Router] undo ip route-static 192.168.10.0 24  
[Router] undo ip route-static 192.168.20.0 24
```

3. CORE1 的 OSPF 配置。

```
[CORE1] ospf 100 router-id 2.2.2.2  
[CORE1-ospf-100] area 0  
[CORE1-ospf-100-area-0.0.0.0] network 172.16.1.0 0.0.0.255  
[CORE1-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255  
[CORE1-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255  
[CORE1-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255  
[CORE1-ospf-100-area-0.0.0.0] quit  
[CORE1-ospf-100] quit
```

4. CORE2 的 OSPF 配置。

```
[CORE2] ospf 100 router-id 3.3.3.3  
[CORE2-ospf-100] area 0  
[CORE2-ospf-100-area-0.0.0.0] network 172.16.2.0 0.0.0.255  
[CORE2-ospf-100-area-0.0.0.0] network 172.16.3.0 0.0.0.255  
[CORE2-ospf-100-area-0.0.0.0] network 192.168.10.0 0.0.0.255  
[CORE2-ospf-100-area-0.0.0.0] network 192.168.20.0 0.0.0.255  
[CORE2-ospf-100-area-0.0.0.0] quit  
[CORE2-ospf-100] quit
```

5. 出口路由器的 OSPF 配置，为了连接内网和公网需要配置指向公网的静态缺省路由，在 OSPF 进程需要引入缺省路由，同时需要配置一条缺省静态路由指向运营商。

```
[Router] ospf 100 router-id 1.1.1.1
[Router-ospf-100] default-route-advertise always
[Router-ospf-100] area 0
[Router-ospf-100-area-0.0.0.0] network 172.16.1.0 0.0.0.255
[Router-ospf-100-area-0.0.0.0] network 172.16.2.0 0.0.0.255
[Router-ospf-100-area-0.0.0.0] quit
[Router-ospf-100] quit
[Router] ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

关于交换机 OSPF 更详细配置说明及具体的配置命令，请根据设备版本参考相应《配置指南-IP 路由》中的“OSPF 配置”。

1.1.1.3.3.6 配置可靠性和负载分担

配置 VRRP 联动接口检测链路

说明

当 CORE1 到出口路由器的链路出现故障后，流量会通过 CORE1 到 CORE2 的互联链路经由 CORE2 到达出口路由器，此时就增加了互联链路负担，对互联链路的稳定性和带宽负载要求都很高。现网环境中一般希望主设备的上行接口出现故障的时候可以实现主备的快速切换，通过配置 VRRP 与接口状态联动功能可以实现此快速切换。在 VRRP 备份组中配置对上行接口进行检测，当检测到接口 down 了，设备会通过降低优先级来实现主备切换。

VRRP 联动接口监视上行链路。

```
[CORE1] interface Vlanif 10
[CORE1-Vlanif10] vrrp vrid 1 track interface 10GE 1/0/7 reduced 100 //配置 VRRP 与上行接口状态联动监视接口功能
[CORE1-Vlanif10] quit
[CORE1] interface Vlanif 20
[CORE1-Vlanif20] vrrp vrid 2 track interface 10GE 1/0/7 reduced 100
[CORE1-Vlanif20] quit
```

配置负载分担

说明

随着业务的增长，经由 CORE1 的链路带宽占用率太高，但是经过 CORE2 的链路是闲置的，这样不但可靠性不好而且浪费资源，有效利用左右两边两条链路显得尤为重要。把 VRRP 主备份配置为负载分担，一些 VLAN 以 CORE1 为主设备，另一些 VLAN 以 CORE2 为主设备，不同 VLAN 的流量被分配到了左右两条链路上，有效的利用现网资源。此处 CORE1 继续作为 VLAN10 的主设备，修改 CORE2 的优先级使其成为 VLAN20 的主设备。

1. 首先删除 CORE1 上面 VRRP 备份组 2 的优先级和抢占延时配置。

```
[CORE1] interface Vlanif 20
```

```
[CORE1-Vlanif20] undo vrrp vrid 2 preempt-mode timer delay
[CORE1-Vlanif20] undo vrrp vrid 2 priority
[CORE1-Vlanif20] quit
```

- 配置 CORE2 为 VLAN20 的主设备，抢占延时为 20S。

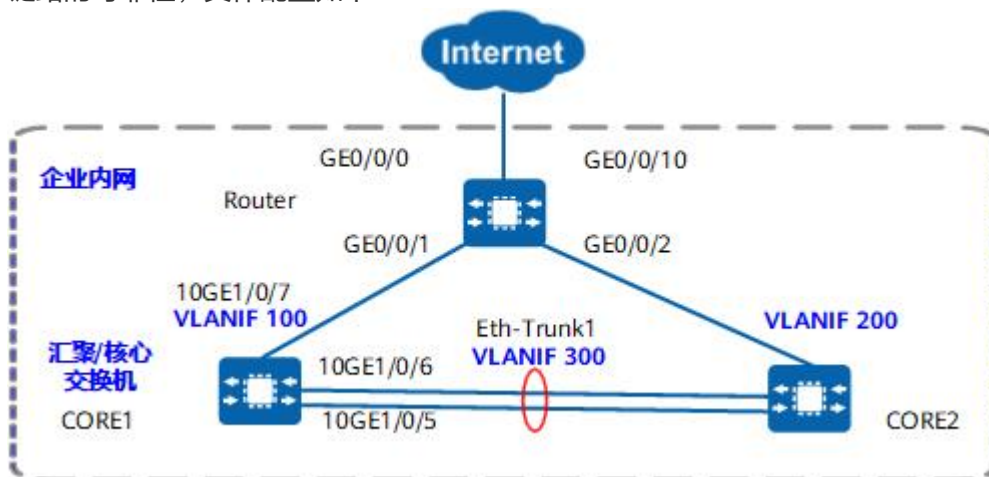
```
[CORE2] interface Vlanif 20
[CORE2-Vlanif20] vrrp vrid 2 priority 120
[CORE2-Vlanif20] vrrp vrid 2 preempt-mode timer delay 20
```

- 配置 VRRP 备份组联动上行接口监视上行链路情况。

```
[CORE2-Vlanif20] vrrp vrid 2 track interface 10GE 1/0/8 reduced 100
[CORE2-Vlanif20] quit
```

1.1.1.3.3.7 配置链路聚合

当 CORE1 或者 CORE2 的上行发生故障时，流量经过 CORE1 和 CORE2 互联的链路，但是单条链路有可能带宽不够，因而造成数据丢失。为了增加带宽，把多条物理链路捆绑为一条逻辑链路，增加带宽的同时提高了链路的可靠性，具体配置如下：



- 恢复接口默认配置（如果接口是默认配置，请直接进行配置即可），将接口恢复为默认配置的步骤和命令如下：

```
[CORE1] interface 10GE 1/0/5
[CORE1-10GE1/0/5] display this
#
interface 10GE1/0/5
port link-type access
port default vlan 300
#
return
[CORE1-10GE1/0/5] undo port default vlan
[CORE1-10GE1/0/5] undo port link-type
```

- 可以通过命令把接口恢复为初始配置，恢复之后接口被关闭了，需要手动 undo shutdown 来开启：

```
[CORE1-10GE1/0/5] clear configuration this
```



```
Warning: All configurations of the interface will be cleared, and its state will be shutdown. Continue?
[Y/N] :y
Info: Total 2 command(s) executed, 2 successful, 0 failed.
[CORE1-10GE1/0/5] undo shutdown
[CORE1-10GE1/0/5] quit
```

3. 配置链路聚合，配置的步骤和命令如下：

方式一：配置手工负载分担方式的链路聚合

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] trunkport 10GE 1/0/5 to 1/0/6
[CORE1-Eth-Trunk1] port link-type access
[CORE1-Eth-Trunk1] port default vlan 300
[CORE1-Eth-Trunk1] quit
```

方式二：配置 LACP 模式的链路聚合

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] mode lacp-static
[CORE1-Eth-Trunk1] trunkport 10GE 1/0/5 to 1/0/6
[CORE1-Eth-Trunk1] port link-type access
[CORE1-Eth-Trunk1] port default vlan 300
[CORE1-Eth-Trunk1] quit
```

在 CORE1 上配置系统优先级为 100，使其成为 LACP 主动端

```
[CORE1] lacp priority 100
```

在 CORE1 上配置活动接口上限阈值为 2

```
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] max bandwidth-affected-linknumber 2
[CORE1-Eth-Trunk1] quit
```

在 CORE1 上配置接口优先级确定活动链路（配置 10GE1/0/5 和 10GE1/0/6 为活动链路）

```
[CORE1] interface 10GE 1/0/5
[CORE1-10GE1/0/5] lacp priority 100
[CORE1-10GE1/0/5] quit
[CORE1] interface 10GE 1/0/6
[CORE1-10GE1/0/6] lacp priority 100
[CORE1-10GE1/0/6] quit
```

CORE2 的配置同上，只是无需配置系统优先级，使用系统默认的优先级即可。

关于交换机链路聚合的详细说明及具体配置命令，请根据设备版本参考相应《配置指南-以太网交换》。

1.1.1.3.3.8 配置限速

基于 IP 地址限速

由于交换机配置每 IP 限速不是很方便而且需要消耗大量的硬件 ACL 资源，所以只能在 AR 路由器上配置每 IP 限速。

由于带宽有限，不能影响正常办公，需要限制内网每个 IP 地址上传和下载的网速不能超过 512kbit/s，在出口路由器连接内网交换机的物理接口做每 IP 限速。

1. 在 GigabitEthernet0/0/1 接口对 192.168.10.0 和 192.168.20.0 的网段做每 IP 限速，限制为 512Kbit/s，配置每 IP 限速需要注意是在 LAN 侧接口配置的。因为大多数情况下 WAN 侧接口做了 NAT 无法识别内网的 IP 地址，在 LAN 侧配置每 IP 限速时 inbound 方向对应 source 地址，限制上传速度，outbound 对应 destination 地址，限制下载速度。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] qos car inbound source-ip-address range 192.168.10.1 to 192.168.10.254
per-address cir 512
[Router-GigabitEthernet0/0/1] qos car outbound destination-ip-address range 192.168.10.1 to
192.168.10.254 per-address cir 512
[Router-GigabitEthernet0/0/1] qos car inbound source-ip-address range 192.168.20.1 to 192.168.20.254
per-address cir 512
[Router-GigabitEthernet0/0/1] qos car outbound destination-ip-address range 192.168.20.1 to
192.168.20.254 per-address cir 512
[Router-GigabitEthernet0/0/1] quit
```

接口 GigabitEthernet0/0/2 及其他网段做基于 IP 限速的方式同上。

基于网段总流量限速

随着业务的增长，为了给部门 A 留有足够的带宽，需要对部门 B 进行网速限速，要求部门 B 访问互联网的网速不能超过 2M，下载的网速不能超过 4M。

1. 在出口路由器使用 ACL 匹配部门 B 的网段数据流。

```
[Router] acl 2222
[Router-acl-basic-2222] rule permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2222] quit
```

2. 在出口路由器 LAN 侧接口配置对访问互联网的流量和下载的流量进行限速。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] qos car inbound acl 2222 cir 2048
[Router-GigabitEthernet0/0/1] qos car outbound acl 2222 cir 4096
[Router-GigabitEthernet0/0/1] quit
```

接口 GigabitEthernet0/0/2 及其他网段做限速的方式同上。

关于 AR 路由器每 IP 限速更多的配置说明及详细配置命令，请根据设备版本参考相应《配置指南-QoS》中的“流量监管、流量整形和接口限速配置”。

1.1.1.3.3.9 配置映射内网服务器和公网多出口

配置映射内网服务器

随着业务的发展，内网的 WWW 服务器和 FTP 文件服务器不能仅限于内网用户访问，对外也要提供服务，公网和内网用户都要通过公网地址来访问服务器提供的服务。

1. 配置内网服务器，使公网用户通过公网地址访问内网服务器。

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] nat server protocol tcp global current-interface www inside 192.168.50.20
www
Warning:The port 80 is well-known port. If you continue it may cause function failure.
Are you sure to continue?[Y/N]:y
[Router-GigabitEthernet0/0/0] nat server protocol tcp global current-interface ftp inside 192.168.50.10 ftp
[Router-GigabitEthernet0/0/0] quit
```

2. 由于 FTP 是一个多通道协议，需要在出口路由器使能 ALG 功能。

```
[Router] nat alg ftp enable
```

3. 配置内网用户使用公网地址访问内网服务器。

```
[Router] acl 3333
[Router-acl-adv-3333] rule permit ip source 192.168.10.0 0.0.0.255 destination 203.0.113.0 0.0.0.0
[Router-acl-adv-3333] rule permit ip source 192.168.20.0 0.0.0.255 destination 203.0.113.0 0.0.0.0
[Router-acl-adv-3333] quit
```

4. 在内网接口做 NAT 转换。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat outbound 3333
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 3333
[Router-GigabitEthernet0/0/2] quit
```

5. 分别在内网接口下面做内部服务器映射。

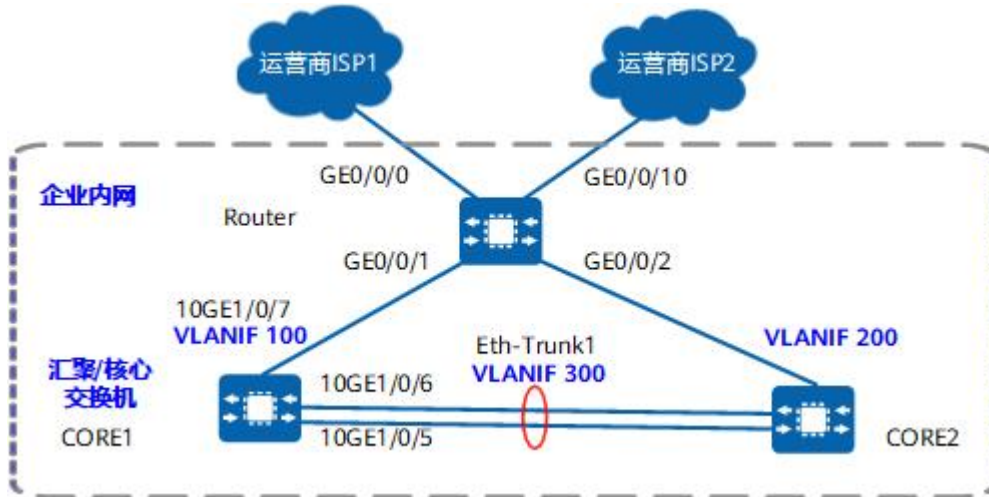
```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] nat server protocol tcp global interface GigabitEthernet 0/0/0 www inside
192.168.50.20 www
[Router-GigabitEthernet0/0/1] nat server protocol tcp global interface GigabitEthernet 0/0/0 ftp inside
192.168.50.10 ftp
[Router-GigabitEthernet0/0/1] quit
```

内网接口 GigabitEthernet0/0/2 的配置同上。

关于 AR 路由器配置内网服务器映射的详细说明和具体配置命令，请根据设备版本参考相应《配置指南—NAT 配置》。

配置公网多出口

刚开始企业在运营商只申请了一条链路，随着业务的发展，一条链路不能满足企业的网络带宽，需要在原有链路的基础上再申请一条链路，由原来的单出口改为双出口，对内网不同的网段进行控制让其走指定的链路上网。



配置 GigabitEthernet0/0/10 通过 PPPoE 拨号上网。

配置策略路由实现不同网段通过不同运营商上网。

1. 配置需要进行 NAT 的 ACL。

```
[Router] acl 2015
[Router-acl-basic-2015] rule permit source 192.168.10.0 0.0.0.255
[Router-acl-basic-2015] rule permit source 192.168.20.0 0.0.0.255
[Router-acl-basic-2015] quit
```

2. 配置拨号访问控制列表。

```
[Router] dialer-rule
[Router-dialer-rule] dialer-rule 1 ip permit
[Router-dialer-rule] quit
```

3. 配置拨号接口。

```
[Router] interface Dialer 0
[Router-Dialer0] ip address ppp-negotiate
[Router-Dialer0] ppp chap user Router
[Router-Dialer0] ppp chap password cipher Router@123
[Router-Dialer0] dialer user user
[Router-Dialer0] dialer bundle 1
[Router-Dialer0] dialer-group 1
[Router-Dialer0] ppp ipcp dns request
[Router-Dialer0] ppp ipcp dns admit-any
[Router-Dialer0] quit
```

4. 配置使用接口 IP 地址进行 NAT 转换。

```
[Router] interface Dialer 0
[Router-Dialer0] nat outbound 2015
[Router-Dialer0] quit
```

5. 配置 TCP 最大报文段长度为 1200，如果使用默认的 1460 可能会出现访问网站慢的情况。

```
[Router] interface Dialer 0
[Router-Dialer0] tcp adjust-mss 1200
[Router-Dialer0] quit
```

6. 在连接运营商线路的物理接口启用 PPPoE 功能。

```
[Router] interface GigabitEthernet 0/0/10
[Router-GigabitEthernet0/0/10] pppoe-client dial-bundle-number 1
[Router-GigabitEthernet0/0/10] quit
```

7. 配置到公网的缺省静态路由，指定出接口为 Dialer 0。

```
[Router] ip route-static 0.0.0.0 0 Dialer 0
```

8. 配置 ACL 匹配数据流，需要把内网互访的数据流不要做重定向。

```
[Router] acl 3000
[Router-acl-adv-3000] rule permit ip source 192.168.10.0 0.0.0.255 destination 192.168.20.0 0.0.0.255
[Router-acl-adv-3000] rule permit ip source 192.168.20.0 0.0.0.255 destination 192.168.10.0 0.0.0.255
[Router-acl-adv-3000] quit
[Router] acl 3001
[Router-acl-adv-3001] rule permit ip source 192.168.10.0 0.0.0.255
[Router-acl-adv-3001] quit
[Router] acl 3002
[Router-acl-adv-3002] rule permit ip source 192.168.20.0 0.0.0.255
[Router-acl-adv-3002] quit
```

9. 配置流分类 c0、c1 和 c2，分别匹配 ACL3000、ACL3001 和 ACL3002。

```
[Router] traffic classifier c0
[Router-classifier-c0] if-match acl 3000
[Router-classifier-c0] quit
[Router] traffic classifier c1
[Router-classifier-c1] if-match acl 3001
[Router-classifier-c1] quit
[Router] traffic classifier c2
[Router-classifier-c2] if-match acl 3002
[Router-classifier-c2] quit
```

10. 配置流行为，对内网互访的数据流不做重定向操作，对内网 192.168.10.0 网段的数据重定向到下一跳 1.1.1.1，对内网 192.168.20.0 网段的数据重定向到出接口 Dialer0。

```
[Router] traffic behavior b0
[Router-behavior-b0] permit
[Router-behavior-b0] quit
[Router] traffic behavior b1
[Router-behavior-b1] redirect ip-nextthop 1.1.1.1
[Router-behavior-b1] quit
[Router] traffic behavior b2
```

```
[Router-behavior-b2] redirect interface Dialer 0
[Router-behavior-b2] quit
```

11. 配置流策略，分别将流分类和流行为组合起来。

```
[Router] traffic policy test
[Router-trafficpolicy-test] classifier c0 behavior b0
[Router-trafficpolicy-test] classifier c1 behavior b1
[Router-trafficpolicy-test] classifier c2 behavior b2
[Router-trafficpolicy-test] quit
```

12. 将流策略应用到出口路由器互联内网交换机的接口。

```
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] traffic-policy test inbound
[Router-GigabitEthernet0/0/1] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] traffic-policy test inbound
[Router-GigabitEthernet0/0/2] quit
```

配置完策略路由之后，内网 192.168.10.0 网段的数据访问互联网走的是 GigabitEthernet0/0/0 接口，而 192.168.20.0 网段的数据访问互联网走的是 GigabitEthernet0/0/10 接口，通过 PPPoE 拨号上网。

关于 AR 路由器策略路由的详细配置说明及具体配置命令，请根据设备版本参考相应《配置指南》中的“路由策略配置”。

1.1.1.3.3.10 业务验证和保存配置

业务验证

- 从两个部门内各选一台 PC 进行 ping 测试，验证部门之间通过 VLANIF 实现三层互通是否正常。以部门 A 和部门 B 为例，PC1 和 PC2 是通过 CORE1（或 CORE2）实现三层互通的。如果 PC1 和 PC2 之间互 ping 测试正常则说明三层互通正常。

```
<PC1> ping 192.168.20.254      //假设 PC2 通过 DHCP 自动获取的 IP 地址为 192.168.20.254
PING 192.168.20.254 data bytes, press CTRL_C to break
  Reply from 192.168.20.254 : bytes=56 Sequence=1 ttl=253 time=62 ms
  Reply from 192.168.20.254 : bytes=56 Sequence=2 ttl=253 time=16 ms
  Reply from 192.168.20.254 : bytes=56 Sequence=3 ttl=253 time=62 ms
  Reply from 192.168.20.254 : bytes=56 Sequence=4 ttl=253 time=94 ms
  Reply from 192.168.20.254 : bytes=56 Sequence=5 ttl=253 time=63 ms

--- 192.168.20.254 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received    //能 Ping 通，说明 PC1 与 PC2 之间三层互通正常
```

2. 部门内部选两台 PC 进行 ping 测试，验证部门内部二层互通是否正常。部门 A 的用户是通过 ACC1 实现二层互通的。如果部门 A 的用户之间互 ping 测试正常则说明部门 A 内二层互通正常。ping 测试命令与步骤 1 类似。
3. 每个部门各选一台 PC 进行 ping 公网地址测试，验证公司内网用户访问 Internet 是否正常。以部门 A 为例，一般可以通过在 PC1 上 ping 公网网关地址（即与出口路由器对接的运营商设备的 IP 地址）来验证是否可以访问 Internet，如果 ping 测试正常则说明内网用户访问 Internet 正常。ping 测试命令与步骤 1 类似。

保存配置

通过命令行配置的数据是临时性的。如果不保存，交换机重启后这些配置都会丢失。

如果要使当前配置在交换机重启后仍然有效，需要将当前配置保存为配置文件。

以 CORE1 为例：

```
<CORE1> save
The current configuration will be written to the device.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0..
Save the configuration successfully.
```

1.1.2 园区网络综合配置案例

[园区内基础网络连通部署案例](#)

[有线无线用户接入认证部署案例](#)

[智能极简园区网络部署案例（小行星部署案例）](#)

[环网接入 VRRP 网关配置案例](#)

[集中式网关部署方式的 VXLAN 配置案例](#)

1.1.2.1 园区内基础网络连通部署案例

[基础网络连通性部署要点](#)

[两层和三层网络架构部署差异说明](#)

[集群/堆叠通用部署](#)

[独立 AC 方案：核心交换机做有线无线用户网关](#)

[独立 AC 方案：汇聚交换机做有线无线用户网关](#)

独立 AC 方案：核心交换机做有线用户网关，AC 做无线用户网关

独立 AC 方案：汇聚交换机做有线用户网关，AC 做无线用户网关

1.1.2.1.1 基础网络连通性部署要点

网络连通性部署旨在打通园区网络核心层、汇聚层、接入层设备间的二三层通信，实现有线、无线用户接入园区网络以及用户间的互访，是园区网络建设的基础。

根据园区网络的业务、规模的不同，园区内基础网络连通性部署有以下要点：

表 1 基础网络连通性部署要点

部署要点	说明	场景推荐
确定使用两层还是三层网络架构	两层网络架构包括核心层、接入层。 三层网络架构包括核心层、汇聚层和接入层。 具体请参见《 两层和三层网络架构部署差异说明 》的说明。	对于规模较小的网络，通常采用组网简单，网元数量少，网络故障点少的两层网络架构。 对于规模比较大的网络，通常采用组网复杂，网元数量多，故障点也多的三层网络架构。 实际应用中，当传输距离较短，且核心层有足够多的接口能直接连接接入层的情况下，往往也采用两层网络架构。一来可以节省总体成本，二来能减轻维护负担，网络状况也更易监控。
确定网络中设备是否组建集群/堆叠	通过网络部署集群/堆叠，提供网络的可靠性。在组建网络时，建议优先完成 集群/堆叠通用部署 。	为提升网络可靠性，建议核心层设备部署集群、汇聚层设备部署堆叠。 用户接入较多场景中，可以在接入层部署堆叠扩充端口数量。
确定组网中网关的位置（即二三层分界点）	一般在网关以下部署二层交换业务，网关以上部署三层路由业务。	建议根据网络规模进行选择，规模较小，核心交换机做网关，规模较大时，可以使用汇聚交换机做网关。
确定独立 AC 旁挂组网还是直连组网	AC 旁挂组网指的是 AC 旁挂在核心交换机或汇聚交换机旁边，实现对 AP 的管理。 AC 直连组网是指 AC 下直接接入 AP 或接入交换机，同时扮演 AC 和汇聚交换机功能，AP 的数据业务和管理业务都由 AC 集中转发和处理。	希望对现有网络改造小，通常建议使用 AC 旁挂组网；中小型规模的新建组网，通常使用 AC 直连组网简化网络架构。
确定独立 AC 无线数据采用直接转发还是隧道转发	直接转发模式下，AP 的业务报文不会进行 CAPWAP 封装，而是直接转发给上层网络。	隧道转发适用于需要集中管理控制业务数据的场景，直接转发适用于报文转发效率要求高的场景。 当无线用户网关部署在交换机上时，如果不需要部署业务随行，无线数据推荐采用直接转发方式；如果需要部署业务随行，无线数据推荐采用隧道转发方式。 当无线用户网关部署在独立 AC 上时，无线数据推荐采用隧道转发方式。

部署说明

网络组网架构分为两层和三层，二层架构比三层架构少了汇聚层，本章节中均使用三层组网架构进行举例。部署的差异见 [两层和三层网络架构部署差异说明](#)。

交换机部署集群/堆叠功能后，多台交换机从逻辑上就虚拟成了一台交换设备，配置及组网都变得更加简单。部署案例见 [集群/堆叠通用部署](#)。

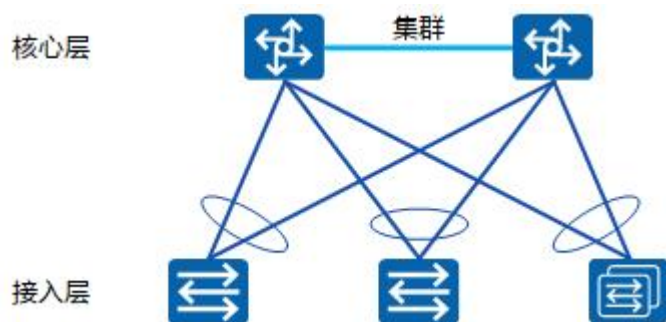
1.1.2.1.2 两层和三层网络架构部署差异说明

园区网络的物理架构推荐采用树形组网，不仅便于部署和管理，还具有良好的扩展性。树形组网通常采用分层架构，园区网络的层次一般包括终端层、接入层、汇聚层和核心层等。针对接入层、汇聚层和核心层的层次结构，在实际应用中，我们可以根据网络规模和业务的需要，灵活选择两层或三层网络架构。

两层网络架构

如[图 1](#)所示，两层网络架构包括核心层、接入层。

图 1 二层架构组网图



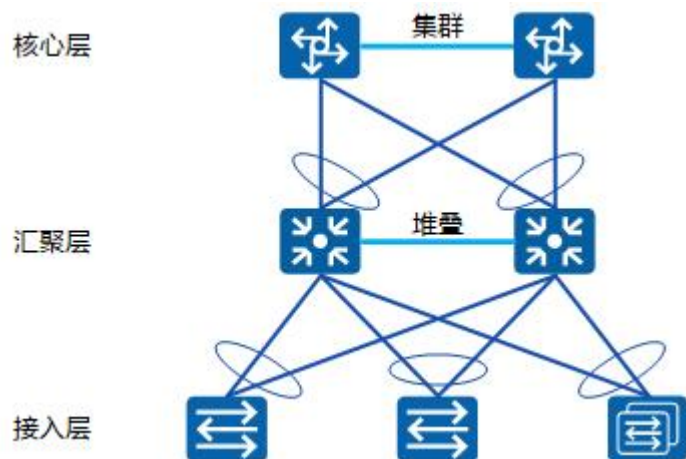
为了保证网络设备级和链路级可靠性，核心层和接入层推荐双机集群/堆叠，核心层和接入层之间推荐采用 Eth-Trunk 组网。当接入层单机即可满足下连终端的接入密度时，接入层也可采用单机组网。

集群/堆叠+Eth-Trunk 组网是一种无环组网，配置简单，不需要复杂的环网协议和可靠性协议（如 RSTP、MSTP、RRPP 等）。该组网保证了网络设备级和链路级可靠性的同时，亦简化了网络拓扑，减少了部署和维护工作量。

三层网络架构

如[图 2](#)所示，三层网络架构包括核心层、汇聚层、接入层。

图 2 三层架构组网图



为了保证网络设备级和链路级可靠性，核心层、汇聚层和接入层推荐双机集群/堆叠，接入层和汇聚层之间、汇聚层和核心层之间推荐采用 Eth-Trunk 组网。当接入层单机即可满足下联终端的接入密度时，接入层也可采用单机组网。

部署差异

三层网络架构与二层网络架构的差异在于汇聚层。汇聚层用来连接核心层和接入层，处于中间位置。汇聚层交换机是多台接入层交换机的汇聚点，能够处理来自接入层设备的所有通信量，并提供到核心层的上行链路。

两种网络架构的选取主要取决于以下几点：

1. 网络规模。例如网元的数量，主要涉及投资成本的问题。
2. 网络复杂度。主要涉及后期网络维护的成本，以及故障定位的简易程度。网络越复杂，故障点越多，那么定位故障的难度就越大，维护成本就越高。
3. 传输距离问题。忽略不同传输介质的差异，三层网络架构比二层网络架构能够覆盖更大的网络。

总体来看，两层网络架构的组网简单，网元数量少，网络故障点少，适用于规模较小的园区；三层网络架构的组网复杂，网元数量多，故障点也多，适用于规模比较大的园区。

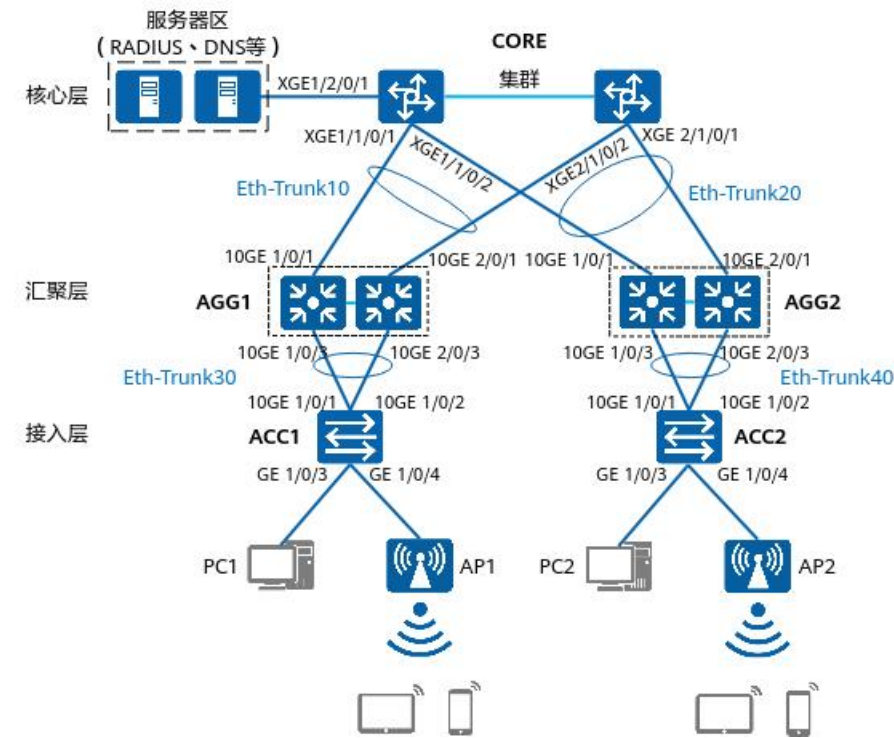
在实际应用中，很多时候会采用二层网络架构。在传输距离较短，且核心层有足够多的接口能直接连接接入层的情况下，汇聚层是可以被省略的，这样的做法比较常见。一来可以节省总体成本，二来能减轻维护负担，网络状况也更易监控。

1.1.2.1.3 集群/堆叠通用部署

案例描述

核心层使用两台框式交换机组建集群，汇聚层使用两台盒式交换机组建堆叠，核心层的集群与汇聚层的堆叠使用 Eth-Trunk 相连。

图 1 园区基础网络组网图



设备要求和版本

位置	设备要求	本案例使用的设备	本案例使用的版本
核心层	支持集群功能的框式交换机	S12700E-8	V200R022C10
汇聚层	支持堆叠功能的盒式交换机	S6730-H-V2	V600R022C10
接入层	-	S5735-L-V2	V600R022C10

说明

不同款型的设备，堆叠、集群的连线方式和支持情况是有差异的，可以使用[堆叠助手](#)或查询堆叠支持情况、集群支持情况获取各款型的详细信息。

部署思路

步骤	部署思路	涉及设备
1	配置核心交换机集群和多主检测功能	核心层交换机
2	配置汇聚交换机堆叠和双主检测功能	汇聚层交换机
3	配置交换机上下行 Eth-Trunk	核心层交换机、汇聚层交换机、接入层交换机

数据规划

表 1 集群软硬件配置规划

项目	数据详情
集群方式	业务口集群
交换机台数	2 台
每台交换机硬件配置	主控板：2 块 MPUE 业务板型号：2 块 LST7X24BX6E0，出于可靠性考虑建议配置 2 块单板，配置 1 块单板也可以组建集群 集群线缆：4 根 3m SFP+ AOC 光线缆
集群主	集群 ID 为 1 的框为集群主
集群优先级	集群 ID 为 1 的框，集群优先级为 150 集群 ID 为 2 的框，集群优先级使用缺省值 1
多主检测	两台集群交换机之间使用单独的线缆，通过直连方式进行多主检测。线缆连接的接口为 XGE1/1/0/10 和 XGE2/1/0/10。

表 2 堆叠软硬件配置规划

项目	数据详情
堆叠方式	业务口堆叠
交换机台数	2 台
每台交换机硬件配置	堆叠口：10GE 业务口 10GE 1/0/2 和 10GE 1/0/4 连线方式：环形连线 堆叠线缆：2 根 3m SFP+ AOC 光线缆
堆叠主	两台交换机的堆叠 ID 分别修改为 1 和 2，堆叠 ID 为 1 的交换机为堆叠主
堆叠优先级	堆叠 ID 为 1 的交换机，堆叠优先级为 150 堆叠 ID 为 2 的交换机，堆叠优先级为 100
双主检测	两台堆叠交换机之间使用单独的线缆，通过直连方式进行双主检测。线缆连接的接口为 10GE 1/0/10 和 10GE 2/0/10。

表 3 集群和堆叠接口对接规划

项目	端口号
集群下行连接堆叠的接口	与 AGG1 相连的接口使用 Eth-Trunk 10，物理成员口为 XGE 1/1/0/1 和 XGE 2/1/0/2 与 AGG2 相连的接口使用 Eth-Trunk 20，物理成员口为 XGE 1/1/0/2 和 XGE 2/1/0/1

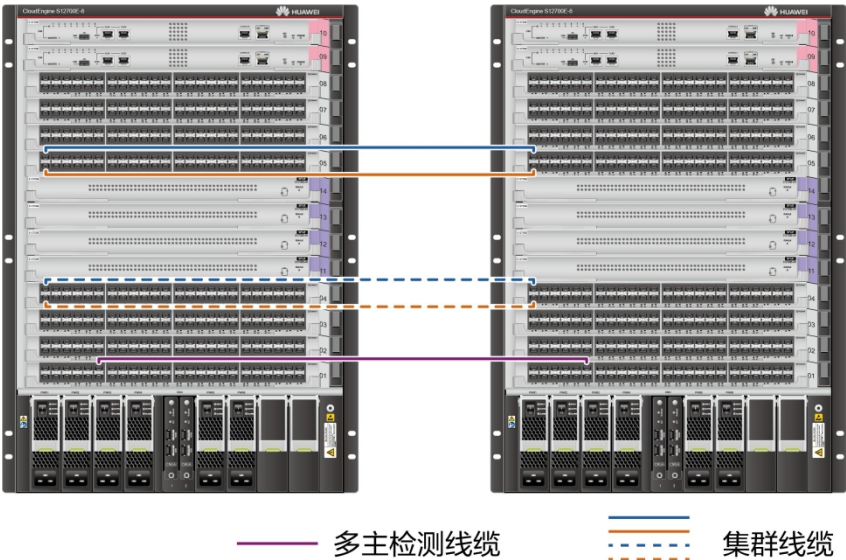
表 3 集群和堆叠接口对接规划

项目	端口号
堆叠 AGG1 上行连接集群的接口	Eth-Trunk 10，物理成员口为 10GE 1/0/1 和 10GE 2/0/1
堆叠 AGG2 上行连接集群的接口	Eth-Trunk 20，物理成员口为 10GE 1/0/1 和 10GE 2/0/1
堆叠 AGG1 下行连接 ACC1 的接口	Eth-Trunk 30，物理成员口为 10GE 1/0/3 和 10GE 2/0/3
堆叠 AGG2 下行连接 ACC2 的接口	Eth-Trunk 40，物理成员口为 10GE 1/0/3 和 10GE 2/0/3
ACC1 上行连接堆叠 AGG1 的接口	Eth-Trunk 30，物理成员口为 10GE 1/0/1 和 10GE 1/0/2
ACC2 上行连接堆叠 AGG2 的接口	Eth-Trunk 40，物理成员口为 10GE 1/0/1 和 10GE 1/0/2

配置步骤

1. 搭建集群环境
- a. 交换机下电，安装用于集群业务板并根据下面连线图连线集群线缆和多主检测线缆。

图 2 集群线缆连线图



说明

出于可靠性考虑，推荐按照下面方式进行连线：

一块业务板上建议至少有两个物理成员端口加入到一个逻辑集群端口。

上行端口和配置多主检测的端口所在业务板建议属于非组建集群的业务板。

b. 为两台交换机上电，按照数据规划分别对两台框式交换机进行配置。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch1
[Switch1] set css id 1
[Switch1] set css priority 150 //框 1 的集群优先级配置为 150
[Switch1] interface css-port 1
[Switch1-css-port1] port interface xgigabitethernet 4/0/1 to xgigabitethernet 4/0/2 enable
[Switch1-css-port1] quit
[Switch1] interface css-port 2
[Switch1-css-port2] port interface xgigabitethernet 5/0/1 to xgigabitethernet 5/0/2 enable
[Switch1-css-port2] quit
[Switch1] display css status saved //查看集群配置是否正确
CSS port media-type: SFP+
Current Id   Saved Id   CSS Enable  CSS Mode   Priority   Master force
-----
-----
1           1           Off         LPU        150       Off

[Switch1] css enable //集群配置确认正确后，使能集群，重启设备，为保证框 ID 成为主交换机，先重启 Switch1
Warning: The CSS configuration will take effect only after the system is rebooted. The next CSS
mode is CSS card. Reboot now? [Y/N]:y

<HUAWEI> system-view
[HUAWEI] sysname Switch2
[Switch2] set css id 2 //框 2 的集群优先级使用缺省值，不需要配置。
[Switch2] interface css-port 1
[Switch2-css-port1] port interface xgigabitethernet 4/0/1 to xgigabitethernet 4/0/2 enable
[Switch2-css-port1] quit
[Switch2] interface css-port 2
[Switch2-css-port2] port interface xgigabitethernet 5/0/1 to xgigabitethernet 5/0/2 enable
[Switch2-css-port2] quit
[Switch2] display css status saved //查看集群配置是否正确
CSS port media-type: SFP+
Current Id   Saved Id   CSS Enable  CSS Mode   Priority   Master Force
-----
-----
1           2           Off         LPU        1         Off

[Switch2] css enable //集群配置确认正确后，使能集群，重启设备
Warning: The CSS configuration will take effect only after the system is rebooted. The next CSS
mode is CSS card. Reboot now? [Y/N]:y
```

c. 交换机重启后，查看集群是否组建成功。

#通过交换机框上主控板的集群指示灯查看集群状态。

Switch1 主控板上 ACT 灯绿色常亮，表示该主控板为集群系统主用主控板，Switch1 为主交换机。

Switch2 主控板上 ACT 灯绿色闪烁，表示该主控板为集群系统备用主控板，Switch2 为备交换机。

#通过任意主控板上的 Console 口登录集群系统，使用命令行查看集群组建是否成功。
根据集群优先级，优先级大的 Switch1 会成为集群系统的主框，执行命令 **display device** 查看设备状态时，集群系统名为 Switch1。

```
<Switch1> display device
Chassis 1 (Master Switch)
S12700E-8's Device status:
Slot Sub Type      Online Power Register Status Role
-----
1  - LST7X24BX6E0 Present PowerOn Registered Normal NA
2  - LST7X24BX6E0 Present PowerOn Registered Normal NA
3  - - Present PowerOn Unregistered - NA
9  - LST7MPUE0000 Present PowerOn Registered Normal Master
10 - LST7MPUE0000 Present PowerOn Registered Normal Slave
PWR1 - - Present PowerOn Registered Normal NA
CMU1 - EH1D200CMU00 Present PowerOn Registered Normal Master
FAN1 - - Present PowerOn Registered Normal NA
FAN2 - - Present PowerOn Registered Normal NA
Chassis 2 (Standby Switch)
S12700E-8's Device status:
Slot Sub Type      Online Power Register Status Role
-----
1  - LST7X24BX6E0 Present PowerOn Registered Normal NA
2  - LST7X24BX6E0 Present PowerOn Registered Normal NA
3  - - Present PowerOn Unregistered - NA
9  - LST7MPUE0000 Present PowerOn Registered Normal Master
10 - LST7MPUE0000 Present PowerOn Registered Normal Slave
PWR1 - - Present PowerOn Registered Normal NA
CMU2 - EH1D200CMU00 Present - Unregistered - NA
FAN1 - - Present PowerOn Registered Normal NA
FAN2 - - Present PowerOn Registered Normal NA
<Switch1> display css status
CSS Enable switch On
Chassis Id CSS Enable CSS Status CSS Mode Priority Master Force
-----
1 On Master LPU 150 Off
2 On Standby LPU 1 Off
<Switch1> display css channel all //查看集群链路拓扑是否与硬件连接一致
```



```
CSS link-down-delay: 500ms
```

```

                Chassis 1      ||      Chassis 2
=====
=====
Num [CSS port]  [LPU Port]    ||  [LPU Port]    [CSS port]
1  1/1  XGigabitEthernet1/4/0/1  XGigabitEthernet2/4/0/1  2/1
2  1/1  XGigabitEthernet1/4/0/2  XGigabitEthernet2/4/0/2  2/1
3  1/2  XGigabitEthernet1/5/0/1  XGigabitEthernet2/5/0/1  2/2
4  1/2  XGigabitEthernet1/5/0/2  XGigabitEthernet2/5/0/2  2/2
                Chassis 2      ||      Chassis 1
=====
=====
Num [CSS port]  [LPU Port]    ||  [LPU Port]    [CSS port]
1  2/1  XGigabitEthernet2/4/0/1  XGigabitEthernet1/4/0/1  1/1
2  2/1  XGigabitEthernet2/4/0/2  XGigabitEthernet1/4/0/2  1/1
3  2/2  XGigabitEthernet2/5/0/1  XGigabitEthernet1/5/0/1  1/2
4  2/2  XGigabitEthernet2/5/0/2  XGigabitEthernet1/5/0/2  1/2
<Switch1> system-view
[Switch1] sysname CORE //为便于记忆,修改集群系统的设备名

```

d. 集群组建完成，配置多主检测。

集群组建完成后，为防止集群故障分裂导致多主影响业务，在两台交换机直接连接一条线缆，用于多主检测。线缆对应的接口分别为 XGE1/1/0/10 和 XGE2/1/0/10，如图 2 所示。

```

[CORE] interface xgigabitethernet 1/1/0/10
[CORE-XGigabitEthernet1/1/0/10] mad detect mode direct
Warning: This command will block the port, and no other configuration running on this port is
recommended. Continue?[Y/N]:y [CORE-XGigabitEthernet1/1/0/10] quit
[CORE] interface xgigabitethernet 2/1/0/10
[CORE-XGigabitEthernet2/1/0/10] mad detect mode direct
Warning: This command will block the port, and no other configuration running on this port is
recommended. Continue?[Y/N]:y [CORE-XGigabitEthernet2/1/0/10] return
<CORE> display mad verbose //查看多主检测配置
Current MAD domain: 0
Current MAD status: Detect
Mad direct detect interfaces configured:
XGigabitEthernet1/1/0/10
XGigabitEthernet2/1/0/10
Mad relay detect interfaces configured:
Excluded ports(configurable):
Excluded ports(can not be configured):

```

2. 搭建堆叠环境

这里以搭建堆叠 AGG1 为例，AGG2 的搭建和配置过程与 AGG1 相同。

- a. 按照数据规划分别对两台盒式交换机进行配置。

说明

如果使用专用堆叠线缆堆叠，此步配置可以省略。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch1
[Switch1] stack
[Switch1-satck] stack member 1 priority 150
[Switch1-satck] quit
[Switch1] interface Stack-Port 1/1
[Switch1-Stack-Port1/1] port member-group interface 10GE 1/0/2 10GE 1/0/4
[Switch1-Stack-Port1/1] quit
<Switch1> save //堆叠相关的配置不需要保存，会自动写入 flash。为防止其他配置丢失，这里建议执行 save
命令进行保存
The current configuration will be written to flash:/vrpcfg.zip.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0.....
Save the configuration successfully.
<HUAWEI> system-view
[HUAWEI] sysname Switch2
[Switch2] stack
[Switch2-satck] stack member 1 priority 100
[Switch2-satck] stack member 1 renumber 2
[Switch2-satck] quit
[Switch2] interface Stack-Port 1/1
[Switch2-Stack-Port1/1] port member-group interface 10GE 1/0/2 10GE 1/0/4
[Switch2-Stack-Port1/1] quit
<Switch2> save //堆叠相关的配置不需要保存，会自动写入 flash。为防止其他配置丢失，这里建议执行 save
命令进行保存
The current configuration will be written to flash:/vrpcfg.zip.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 0.....
Save the configuration successfully.
```

- b. 交换机下电，根据下面连线图连线堆叠线缆和双主检测线缆。

[图 3](#) 使用的是 S6730-H28X6CZ-V2 设备，堆叠接口和步骤 1 中配置的接口保持一致。

图 3 堆叠线缆连线图



c. 交换机重启后，查看堆叠是否组建成功。

```
<Switch1> display stack configuration //堆叠组建成功，switch1 是堆叠主
Oper      : Operation
Conf      : Configuration
*         : Offline configuration
#         : Media mismatch or absence

Attribute Configuration:
-----
MemberID   Domain      Priority  DelayTime
Oper(Conf) Oper(Conf)  Oper(Conf) Oper(Conf)
-----
1(1)       10(10)       150(150)  0(0)
2(2)       10(10)       100(100)  0(0)
-----

Stack-Port Configuration:
-----
-----
Stack-Port  Member Ports
-----
-----
Stack-Port1/1  10GE1/1/0/2    10GE1/1/0/4
Stack-Port2/1  10GE2/1/0/2    10GE2/1/0/4
-----
-----

Stack-Global Configuration:
-----
-----
AuthMode      Password
-----
-----
hmac-sha256    *****
-----
-----

<Switch1> system-view
```

```
[Switch1] sysname AGG1 //为便于记忆，修改堆叠系统的设备名
```

d. 堆叠组建完成，配置双主检测。

堆叠组建完成后，为防止堆叠故障分裂导致多主影响业务，在两台交换机直接连接一条线缆，用于双主检测。线缆对应的接口分别为 10GE 1/0/10 和 10GE 2/0/10，如图 3 所示。

```
[AGG1] interface 10ge 1/0/10
[AGG1-10GE1/0/10] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue? [Y/N]: y
[AGG1-10GE1/0/10] quit
[AGG1] interface 10ge 2/0/10
[AGG1-10GE2/0/10] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue? [Y/N]: y
[AGG1-10GE2/0/10] return
<AGG1> display dual-active //查看双主检测配置
Stack domainID: 10
Dual-active status: Normal
Dual-active detect mode: Direct
Dual-active direct detect interfaces configured:
10GE1/0/10    up (Physical) up (Protocol) 10 (PeerDomain)
10GE2/0/10    up (Physical) up (Protocol) 10 (PeerDomain)
Dual-active relay detect interfaces configured:
--
Excluded ports(configurable):
--
Excluded ports(can not be configured):
```

3. 配置集群和堆叠之间的 Eth-Trunk 接口，以及堆叠和接入层交换机之间的 Eth-Trunk 接口。

a. 在集群上配置 Eth-Trunk 接口。

```
<CORE> system-view
[CORE] interface eth-trunk 10 //创建与 AGG1 相连的 Eth-Trunk 接口
[CORE-Eth-Trunk10] mode lacp
[CORE-Eth-Trunk10] quit
[CORE] interface xgigabitethernet 1/1/0/1
[CORE-XGigabitEthernet1/1/0/1] eth-trunk 10
[CORE-XGigabitEthernet1/1/0/1] quit
[CORE] interface xgigabitethernet 2/1/0/2
[CORE-XGigabitEthernet2/1/0/2] eth-trunk 10
[CORE-XGigabitEthernet2/1/0/2] quit
[CORE] interface eth-trunk 20 //创建与 AGG2 相连的 Eth-Trunk 接口
[CORE-Eth-Trunk20] mode lacp
[CORE-Eth-Trunk20] quit
[CORE] interface xgigabitethernet 1/1/0/2
[CORE-XGigabitEthernet1/1/0/2] eth-trunk 20
```

```
[CORE-XGigabitEthernet1/1/0/2] quit
[CORE] interface xgigabitethernet 2/1/0/1
[CORE-XGigabitEthernet2/1/0/1] eth-trunk 20
[CORE-XGigabitEthernet2/1/0/1] quit
```

b. 在堆叠 AGG1 上配置 Eth-Trunk 接口。

```
<AGG1> system-view
[AGG1] interface eth-trunk 10 //创建与集群相连的 Eth-Trunk 接口
[AGG1-Eth-Trunk10] mode lacp-static
[AGG1-Eth-Trunk10] quit
[AGG1] interface 10ge 1/0/1
[AGG1-10GE1/0/1] eth-trunk 10
[AGG1-10GE1/0/1] quit
[AGG1] interface 10ge 2/0/1
[AGG1-10GE2/0/1] eth-trunk 10
[AGG1-10GE2/0/1] quit
[AGG1] interface eth-trunk 30 //创建与接入层交换机 ACC1 相连的 Eth-Trunk 接口
[AGG1-Eth-Trunk30] mode lacp-static
[AGG1-Eth-Trunk30] quit
[AGG1] interface 10ge 1/0/3
[AGG1-10GE1/0/3] eth-trunk 30
[AGG1-10GE1/0/3] quit
[AGG1] interface 10ge 2/0/3
[AGG1-10GE2/0/3] eth-trunk 30
[AGG1-10GE2/0/3] quit
```

c. 在堆叠 AGG2 上配置 Eth-Trunk 接口。

```
<AGG2> system-view
[AGG2] interface eth-trunk 20 //创建与集群相连的 Eth-Trunk 接口
[AGG2-Eth-Trunk20] mode lacp-static
[AGG2-Eth-Trunk20] quit
[AGG2] interface 10ge 1/0/1
[AGG2-10GE1/0/1] eth-trunk 20
[AGG2-10GE1/0/1] quit
[AGG2] interface 10ge 2/0/1
[AGG2-10GE2/0/1] eth-trunk 20
[AGG2-10GE2/0/1] quit
[AGG2] interface eth-trunk 40 //创建与接入层交换机 ACC2 相连的 Eth-Trunk 接口
[AGG2-Eth-Trunk40] mode lacp-static
[AGG2-Eth-Trunk40] quit
[AGG2] interface 10ge 1/0/3
[AGG2-10GE1/0/3] eth-trunk 40
[AGG2-10GE1/0/3] quit
```

```
[AGG2] interface 10ge 2/0/3
[AGG2-10GE2/0/3] eth-trunk 40
[AGG2-10GE2/0/3] quit
```

- d. 在接入层交换机 ACC1 上配置 Eth-Trunk 接口。

```
<ACC1> system-view
[ACC1] interface eth-trunk 30 //创建与堆叠 AGG1 相连的 Eth-Trunk 接口
[ACC1-Eth-Trunk30] mode lacp-static
[ACC1-Eth-Trunk30] quit
[ACC1] interface 10ge 1/0/1
[ACC1-10GE1/0/1] eth-trunk 30
[ACC1-10GE1/0/1] quit
[ACC1] interface 10ge 1/0/2
[ACC1-10GE1/0/2] eth-trunk 30
[ACC1-10GE1/0/2] quit
```

- e. 在接入层交换机 ACC2 上配置 Eth-Trunk 接口。

```
<ACC2> system-view
[ACC2] interface eth-trunk 40 //创建与堆叠 AGG2 相连的 Eth-Trunk 接口
[ACC2-Eth-Trunk40] mode lacp-static
[ACC2-Eth-Trunk40] quit
[ACC2] interface 10ge 1/0/1
[ACC2-10GE1/0/1] eth-trunk 40
[ACC2-10GE1/0/1] quit
[ACC2] interface 10ge 1/0/2
[ACC2-10GE1/0/2] eth-trunk 40
[ACC2-10GE1/0/2] quit
```

配置脚本

说明

集群和堆叠的配置不记入配置文件，直接写入 Flash，所以配置文件中没有堆叠和集群相关的配置，只有多主检测/双主检测和 Eth-Trunk 接口的配置。

集群配置文件

```
#
sysname CORE
#
interface Eth-Trunk10
 mode lacp
#
interface Eth-Trunk20
```

```
mode lacp
#
interface XGigabitEthernet1/1/0/1
eth-trunk 10
#
interface XGigabitEthernet1/1/0/2
eth-trunk 20
#
interface XGigabitEthernet1/1/0/10
mad detect mode direct
#
interface XGigabitEthernet2/1/0/1
eth-trunk 20
#
interface XGigabitEthernet2/1/0/2
eth-trunk 10
#
interface XGigabitEthernet2/1/0/10
mad detect mode direct
#
return
```

AGG1 堆叠配置文件

```
#
sysname AGG1
#
interface Eth-Trunk10
mode lacp
#
interface Eth-Trunk30
mode lacp
#
interface 10GE 1/0/3
eth-trunk 30
#
interface 10GE 1/0/10
mad detect mode direct
#
interface 10GE 2/0/3
eth-trunk 30
#
interface 10GE 2/0/10
mad detect mode direct
```

```
#
interface 10GE 1/0/1
 eth-trunk 10
#
interface 10GE 2/0/1
 eth-trunk 10
#
return
```

AGG2 堆叠配置文件

```
#
sysname AGG2
#
interface Eth-Trunk20
 mode lacp
#
interface Eth-Trunk40
 mode lacp
#
interface 10GE 1/0/3
 eth-trunk 40
#
interface 10GE 1/0/10
 mad detect mode direct
#
interface 10GE 2/0/3
 eth-trunk 40
#
interface 10GE 2/0/10
 mad detect mode direct
#
interface 10GE 1/0/1
 eth-trunk 20
#
interface 10GE 2/0/1
 eth-trunk 20
#
return
```

ACC1 配置文件

```
#
sysname ACC1
#
```

```
interface Eth-Trunk30
 mode lacp
#
interface 10GE1/0/1
 eth-trunk 30
#
interface 10GE1/0/2
 eth-trunk 30
#
return
```

ACC2 配置文件

```
#
sysname ACC2
#
interface Eth-Trunk40
 mode lacp
#
interface 10GE1/0/1
 eth-trunk 40
#
interface 10GE1/0/2
 eth-trunk 40
#
return
```

1.1.2.1.4 独立 AC 方案：核心交换机做有线无线用户网关

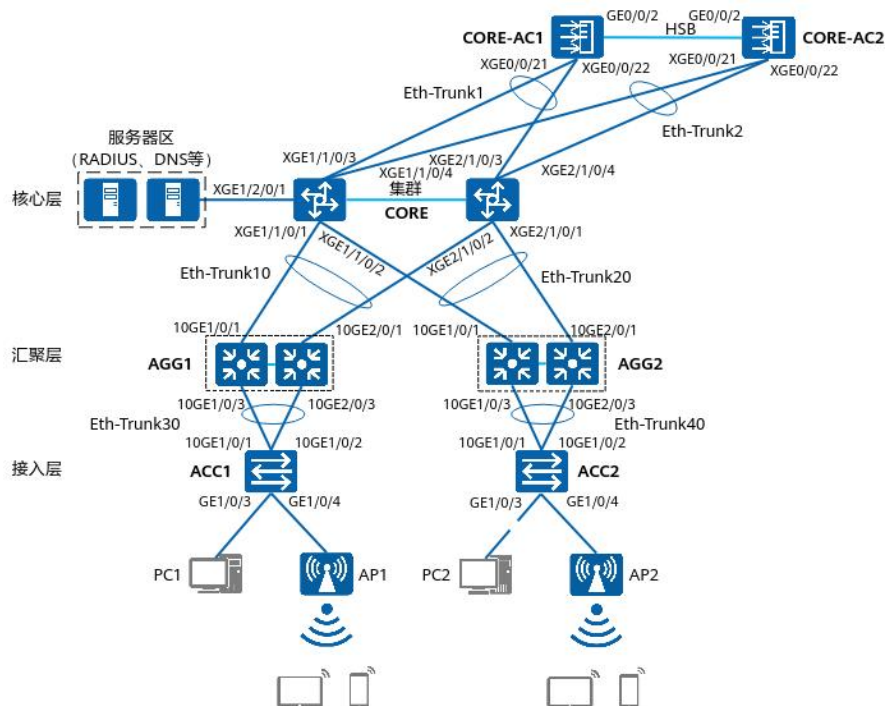
案例描述

核心层交换机组建集群，作为整个园区网络的核心，实现网络高可靠性和网络大数据量转发。独立 AC 旁挂式部署，作为网关为 AP 分配 IP 地址，统一管理全网 AP 上线。

汇聚层交换机组建堆叠，实现设备级备份的同时，也扩展了设备的端口密度和转发带宽。

本案例中，核心交换机作为全网有线无线用户的网关，负责全网用户业务的路由转发。

图 1 核心交换机做网关+独立 AC



设备要求和版本

位置	设备要求	本案例使用的设备	本案例使用的版本
核心层	—	S12700E	V200R022C10
汇聚层	—	S6730-H-V2	V600R022C10
接入层	—	S5735-L-V2	V600R022C10
AC	—	AC6805	V200R022C10
AP	—	AirEngine 8760-X1-PRO	V200R022C10

部署思路

步骤	部署思路	涉及设备
1	配置交换机集群/堆叠、多主检测功能，配置上下行 Eth-Trunk	核心交换机、汇聚交换机
2	配置交换机、AC 的接口和 VLAN，配置三层接口地址、路由，使得网络互通	核心交换机、汇聚交换机、接入交换机、AC
3	配置核心交换机和 AC 的 DHCP 功能，使交换机作为 DHCP 服务器为有线/无线用户分配 IP 地址，使 AC 作为 DHCP 服务器为 AP 分配 IP 地址	核心交换机、AC
4	配置 AC 的 VRRP+HSB 方式的备份	AC
5	配置 AC 的无线业务，实现 AP 和 STA 上线	AC

步骤	部署思路	涉及设备
6	配置 VRRP 热备份场景下的无线配置同步	AC

数据规划

表 1 核心交换机业务数据规划

项目	VLAN ID	网段
无线用户的业务 VLAN（AP1）	VLAN 30	172.16.30.0/24
	VLAN 40	172.16.40.0/24
有线用户的业务 VLAN（PC1）	VLAN 50	172.16.50.0/24
有线用户的业务 VLAN（PC2）	VLAN 60	172.16.60.0/24
连接 CORE-AC 的 VLAN	VLAN 20	192.168.20.20/24
连接服务器的 VLAN	VLAN 1000	192.168.11.254/24

表 2 CORE-AC 业务数据规划

项目	VLAN ID	网段
无线 AP 管理 VLAN	VLAN 20	172.16.20.0/24
CORE-AC1 和 CORE-AC2 的互通 VLAN	VLAN 100	172.16.100.0/24
主备 AC HSB 同步 VLAN	VLAN 200	172.16.200.0/24

表 3 CORE-AC 无线业务数据规划

项目	数据
AP 组	ap-group1
域管理模板	domain1
SSID 模板	test01、test02
VAP 模板	vap1、vap2、直接转发模式
CAPWAP 源接口和 IP 地址（CORE-AC1）	VLANIF 20: 192.168.20.1/24
CAPWAP 源接口和 IP 地址（CORE-AC2）	VLANIF 20: 192.168.20.2/24

部署注意事项

不建议使用 VLAN 1 作为管理 VLAN 或者业务 VLAN，将各端口从 VLAN 1 中退出。根据实际业务需求透传 VLAN，禁止端口透传所有 VLAN。

直接转发方式下，建议管理 VLAN 和业务 VLAN 分别使用不同的 VLAN，否则可能导致业务不通。例如，业务 VLAN 如果和管理 VLAN 相同，且交换机连接 AP 的端口配置了 PVID 为管理 VLAN，则下行到用户的报文出连接 AP 的交换机时业务 VLAN 会被终结，从而导致业务不通。

直接转发模式下，AP 的业务报文不会进行 CAPWAP 封装，而是直接转发给上层网络，所以需要 AP 与上层网络间的网络加入业务 VLAN，配置 AC 与 AP 间的网络加入管理 VLAN，才能正常传输业务报文和管理报文。

对于主备 AC 上关联的同一 AP，其 WLAN 相关的业务配置必须保持一致（如 WMM 模板、射频模板、射频、流量模板、安全模板、安全策略和 WLAN ID 等都需要保持一致），否则当 AC 的主备状态切换后，无法保证用户业务正常。

主备 AC 的型号和软件版本需完全一致。

在 VRRP 热备份场景下部署 DHCP 服务器时需要注意以下几点：

V200R019C00 及之后版本，开启 DHCP 服务器功能的接口无限制，主 AC 分配 IP 地址，备 AC 不分配，主 AC 的 IP 地址分配信息会同步到备 AC。

主备 AC 上配置的 IP 地址池必须完全一致，配置不一致会导致主备 AC 备份失败。

配置命令 `hsb-service-type dhcp hsb-group group-index`，使 DHCP 业务绑定 HSB 备份组。否则主备 AC 上的 IP 地址分配信息无法备份。

部署步骤

1. 配置核心层交换机集群和汇聚层交换机堆叠、多主检测及上下行 Eth-Trunk。

此部分配置请参考 [集群/堆叠通用部署](#)。

2. 配置核心交换机 CORE 的接口和 VLAN。

创建 VLAN。

```
[CORE] vlan batch 20 30 40 50 60 1000
```

配置与汇聚交换机 AGG1 互连的 Eth-Trunk。和汇聚交换机 AGG2 互连的配置与此类似，此处不再赘述。

```
[CORE] interface eth-trunk 10
[Core-Eth-Trunk10] description con to AGG1
[Core-Eth-Trunk10] mode lacp
[Core-Eth-Trunk10] port link-type trunk
[Core-Eth-Trunk10] undo port trunk allow-pass vlan 1
[Core-Eth-Trunk10] port trunk allow-pass vlan 20 30 40 50
[Core-Eth-Trunk10] quit
```

创建和 CORE-AC1 互连的 Eth-Trunk1 并将接口加入 Eth-Trunk。和 CORE-AC2 互连的配置与此类似，此处不再赘述。

```
[CORE] interface eth-trunk 1
[CORE-Eth-Trunk1] description con to CORE-AC1
[CORE-Eth-Trunk1] mode lacp
[CORE-Eth-Trunk1] port link-type trunk
[CORE-Eth-Trunk1] undo port trunk allow-pass vlan 1
[CORE-Eth-Trunk1] port trunk allow-pass vlan 20
[CORE-Eth-Trunk1] quit
[CORE] interface xgigabitethernet 1/1/0/3
[CORE-XGigabitEthernet1/1/0/3] eth-trunk 1
[CORE-XGigabitEthernet1/1/0/3] quit
[CORE] interface xgigabitethernet 2/1/0/3
[CORE-XGigabitEthernet2/1/0/3] eth-trunk 1
[CORE-XGigabitEthernet2/1/0/3] quit
```

将和服务区对接的接口加入 VLAN1000。

```
[CORE] interface xgigabitethernet 1/2/0/1
[CORE-XGigabitEthernet1/2/0/1] port link-type access
[CORE-XGigabitEthernet1/2/0/1] port default vlan 1000
[CORE-XGigabitEthernet1/2/0/1] quit
```

3. 配置汇聚交换机 AGG1 的接口和 VLAN。汇聚交换机 AGG2 的配置与此类似，不再赘述。

创建 VLAN。

```
[AGG1] vlan batch 20 30 40 50
```

配置与核心交换机 CORE 连接的 Eth-Trunk。

```
[AGG1] interface eth-trunk 10
[AGG1-Eth-Trunk10] description connect to CORE
[AGG1-Eth-Trunk10] mode lacp-static
[AGG1-Eth-Trunk10] port link-type trunk
[AGG1-Eth-Trunk10] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk10] port trunk allow-pass vlan 20 30 40 50
[AGG1-Eth-Trunk10] quit
[AGG1] interface 10ge 1/0/1
[AGG1-10GE1/0/1] eth-trunk 10
[AGG1-10GE1/0/1] quit
[AGG1] interface 10ge 2/0/1
[AGG1-10GE2/0/1] eth-trunk 10
[AGG1-10GE2/0/1] quit
```

配置与接入交换机 ACC1 连接的下行接口。

```
[AGG1] interface eth-trunk 30
[AGG1-Eth-Trunk30] mode lacp-static
```

```
[AGG1-Eth-Trunk30] port link-type trunk
[AGG1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk30] port trunk allow-pass vlan 20 30 40 50
[AGG1-Eth-Trunk30] port-isolate enable group 1
[AGG1-Eth-Trunk30] quit
[AGG1] interface 10ge 1/0/3
[AGG1-10GE1/0/3] eth-trunk 30
[AGG1-10GE1/0/3] quit
[AGG1] interface 10ge 2/0/3
[AGG1-10GE2/0/3] eth-trunk 30
[AGG1-10GE2/0/3] quit
```

4. 配置接入交换机 ACC1 的接口和 VLAN。接入交换机 ACC2 的配置与此类似，不再赘述。

创建 VLAN。

```
[ACC1] vlan batch 20 30 40 50
```

配置与汇聚交换机 AGG1 连接的上行接口。

```
[ACC1] interface eth-trunk 30
[ACC1-Eth-Trunk30] mode lacp-static
[ACC1-Eth-Trunk30] port link-type trunk
[ACC1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[ACC1-Eth-Trunk30] port trunk allow-pass vlan 20 30 40 50
[ACC1-Eth-Trunk30] quit
[ACC1] interface 10ge 1/0/1
[ACC1-10GE1/0/1] eth-trunk 30
[ACC1-10GE1/0/1] quit
[ACC1] interface 10ge 1/0/2
[ACC1-10GE1/0/2] eth-trunk 30
[ACC1-10GE1/0/2] quit
```

配置与用户 PC 和 AP1 连接的下行接口，并将其配置为边缘端口。

```
[ACC1] interface GE1/0/3
[ACC1-GE1/0/3] port link-type access
[ACC1-GE1/0/3] port default vlan 50
[ACC1-GE1/0/3] port-isolate enable group 1
[ACC1-GE1/0/3] stp edged-port enable
[ACC1-GE1/0/3] quit
[ACC1] interface GE1/0/4
[ACC1-GE1/0/4] port link-type trunk
[ACC1-GE1/0/4] port trunk pvid vlan 20
[ACC1-GE1/0/4] port trunk allow-pass vlan 20 30 40
[ACC1-GE1/0/4] port-isolate enable group 1
[ACC1-GE1/0/4] stp edged-port enable
[ACC1-GE1/0/4] quit
```

5. 配置 CORE-AC1 的接口和 VLAN。CORE-AC2 的配置与此类似，不再赘述。

配置与核心交换机 CORE 连接的下行接口。

```
<AC6805> system-view
[AC6805] sysname CORE-AC1
[CORE-AC1] vlan batch 20 100
[CORE-AC1] interface eth-trunk 1
[CORE-AC1-Eth-Trunk1] mode lacp
[CORE-AC1-Eth-Trunk1] port link-type trunk
[CORE-AC1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[CORE-AC1-Eth-Trunk1] port trunk allow-pass vlan 20
[CORE-AC1-Eth-Trunk1] quit
[CORE-AC1] interface xgigabitethernet0/0/21
[CORE-AC1-XGigabitEthernet0/0/21] eth-trunk 1
[CORE-AC1-XGigabitEthernet0/0/21] quit
[CORE-AC1] interface xgigabitethernet0/0/22
[CORE-AC1-XGigabitEthernet0/0/22] eth-trunk 1
[CORE-AC1-XGigabitEthernet0/0/22] quit
[CORE-AC1] interface vlanif 20
[CORE-AC1-Vlanif20] ip address 192.168.20.1 255.255.255.0
[CORE-AC1-Vlanif20] quit
```

配置 CORE-AC1 连接 CORE-AC2 的接口。

```
[CORE-AC1] interface gigabitethernet 0/0/2
[CORE-AC1-GigabitEthernet0/0/2] port link-type trunk
[CORE-AC1-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[CORE-AC1-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[CORE-AC1-GigabitEthernet0/0/2] quit
[CORE-AC1] interface vlanif 100
[CORE-AC1-Vlanif100] ip address 172.16.100.1 255.255.255.0
[CORE-AC1-Vlanif100] quit
```

6. 配置核心交换机的 DHCP 功能，使交换机作为 DHCP 服务器为有线、无线用户分配 IP 地址。

使能全局 DHCP，并配置业务 VLAN 的 DHCP Snooping 功能。

```
[CORE] dhcp enable
[CORE] dhcp snooping enable
[CORE] vlan 30
[CORE-vlan30] dhcp snooping enable
[CORE-vlan30] quit
[CORE] vlan 40
[CORE-vlan40] dhcp snooping enable
[CORE-vlan40] quit
[CORE] vlan 50
[CORE-vlan50] dhcp snooping enable
```

```
[CORE-vlan50] quit
[CORE] vlan 60
[CORE-vlan60] dhcp snooping enable
[CORE-vlan60] quit
```

创建无线业务三层接口 VLANIF30、VLANIF40 并配置通过接口地址池为 STA 分配地址。

```
[CORE] interface vlanif 30
[CORE-Vlanif30] ip address 172.16.30.1 255.255.255.0
[CORE-Vlanif30] dhcp select interface
[CORE-Vlanif30] dhcp server dns-list 192.168.11.2 //配置终端的 DNS 服务器
[CORE-Vlanif30] arp-proxy inner-sub-vlan-proxy enable //启动无线用户业务 VLAN 内 Proxy ARP 功能，
否则无线用户之间的流量通过 AC 无法完成互访。请根据实际需求判断是否需要配置该命令
[CORE-Vlanif30] quit
[CORE] interface vlanif 40
[CORE-Vlanif40] ip address 172.16.40.1 255.255.255.0
[CORE-Vlanif40] dhcp select interface
[CORE-Vlanif40] dhcp server dns-list 192.168.11.2 //配置终端的 DNS 服务器
[CORE-Vlanif40] arp-proxy inner-sub-vlan-proxy enable //启动无线用户业务 VLAN 内 Proxy ARP 功能，
否则无线用户之间的流量通过 AC 无法完成互访。请根据实际需求判断是否需要配置该命令
[CORE-Vlanif40] quit
```

创建有线业务三层接口 VLANIF50、VLANIF60 并配置通过接口地址池为有线终端分配地址。

```
[CORE] interface vlanif 50
[CORE-Vlanif50] ip address 172.16.50.1 255.255.255.0
[CORE-Vlanif50] dhcp select interface
[CORE-Vlanif50] dhcp server dns-list 192.168.11.2 //配置终端的 DNS 服务器
[CORE-Vlanif50] arp-proxy inner-sub-vlan-proxy enable //启动有线用户 VLAN 内 Proxy ARP 功能，否则
有线用户之间的流量无法互访。请根据实际需求判断是否需要配置该命令
[CORE-Vlanif50] quit
[CORE] interface vlanif 60
[CORE-Vlanif60] ip address 172.16.60.1 255.255.255.0
[CORE-Vlanif60] dhcp select interface
[CORE-Vlanif60] dhcp server dns-list 192.168.11.2 //配置终端的 DNS 服务器
[CORE-Vlanif60] arp-proxy inner-sub-vlan-proxy enable //启动有线用户 VLAN 内 Proxy ARP 功能，否则
有线用户之间的流量无法互访。请根据实际需求判断是否需要配置该命令
[CORE-Vlanif60] quit
```

创建连接 AC 的三层接口 VLANIF20。

```
[CORE] interface vlanif 20
[CORE-Vlanif20] ip address 192.168.20.20 255.255.255.0
[CORE-Vlanif20] quit
```

创建连接服务器的三层接口 VLANIF1000。

```
[CORE] interface vlanif 1000
[CORE-Vlanif1000] ip address 192.168.11.254 255.255.255.0
```

```
[CORE-Vlanif1000] quit
```

7. 配置 CORE-AC1 的 DHCP 功能，使 AC 作为 DHCP 服务器为 AP 分配 IP 地址。CORE-AC2 的配置与此类似，不再赘述。

```
[CORE-AC1] dhcp enable
[CORE-AC1] interface vlanif 20
[CORE-AC1-Vlanif20] dhcp select interface
[CORE-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.2
[CORE-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.20
[CORE-AC1-Vlanif20] quit
```

8. 配置 CORE-AC1 到有线用户和服务器区网段的路由。CORE-AC2 的配置与此类似，不再赘述。

```
[CORE-AC1] ip route-static 172.16.50.0 255.255.255.0 192.168.20.20
[CORE-AC1] ip route-static 172.16.60.0 255.255.255.0 192.168.20.20
[CORE-AC1] ip route-static 192.168.11.0 255.255.255.0 192.168.20.20
```

9. 配置 CORE-AC1 的 VRRP+HSB 方式的备份。CORE-AC2 的配置与此类似，不再赘述。

配置 VRRP 备份组的状态恢复延迟时间为 60 秒。

```
[CORE-AC1] vrrp recover-delay 60
```

在 CORE-AC1 上创建管理 VRRP 备份组，配置 CORE-AC1 在该备份组中的优先级为 120，并配置抢占时间为 1200 秒。

```
[CORE-AC1] interface vlanif 20
[CORE-AC1-Vlanif20] vrrp vrid 1 virtual-ip 192.168.20.3
[CORE-AC1-Vlanif20] vrrp vrid 1 priority 120
[CORE-AC1-Vlanif20] vrrp vrid 1 preempt-mode timer delay 1200
[CORE-AC1-Vlanif20] admin-vrrp vrid 1
[CORE-AC1-Vlanif20] quit
```

在 CORE-AC1 上创建 HSB 主备服务 0，并配置其主备通道 IP 地址和端口号。

```
[CORE-AC1] hsb-service 0
[CORE-AC1-hsb-service-0] service-ip-port local-ip 172.16.100.1 peer-ip 172.16.100.2 local-data-port
10241 peer-data-port 10241
[CORE-AC1-hsb-service-0] quit
```

在 CORE-AC1 上创建 HSB 备份组 0，并配置其绑定 HSB 主备服务 0 和管理 VRRP 备份组。

```
[CORE-AC1] hsb-group 0
[CORE-AC1-hsb-group-0] bind-service 0
[CORE-AC1-hsb-group-0] track vrrp vrid 1 interface vlanif 20
[CORE-AC1-hsb-group-0] quit
```

配置 CORE-AC1 业务绑定 HSB 备份组。

```
[CORE-AC1] hsb-service-type access-user hsb-group 0
[CORE-AC1] hsb-service-type ap hsb-group 0
[CORE-AC1] hsb-service-type dhcp hsb-group 0
```



```
[CORE-AC1] hsb-group 0
[CORE-AC1-hsb-group-0] hsb enable
[CORE-AC1-hsb-group-0] quit
```

配置完成后，在 CORE-AC1 和 CORE-AC2 上分别执行 **display vrrp** 命令，可以看到 CORE-AC1 的 State 字段的显示为 **Master**，CORE-AC2 的 State 字段的显示为 **Backup**。

```
[CORE-AC1] display vrrp
Vlanif20 | Virtual Router 1
  State : Master
  Virtual IP : 192.168.20.3
  Master IP : 192.168.20.1
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay Time : 1200s
  TimerRun : 2s
  TimerConfig : 2s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : admin-vrrp
  Backup-forward : disabled
  Track SysHealth Priority reduced : 254
  SysHealth state : UP
  Create time : 2019-11-05 15:30:25
  Last change time : 2019-11-05 15:30:31

[CORE-AC2] display vrrp
Vlanif20 | Virtual Router 1
  State : Backup
  Virtual IP : 192.168.20.3
  Master IP : 192.168.20.1
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 120
  Preempt : YES   Delay Time : 0s
  TimerRun : 2s
  TimerConfig : 2s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : admin-vrrp
  Backup-forward : disabled
  Track SysHealth Priority reduced : 254
```

```
SysHealth state : UP
Create time : 2019-11-05 11:12:13
Last change time : 2019-11-05 11:13:23
```

在 CORE-AC1 和 CORE-AC2 上查看主备服务的建立情况。可以看到 **Service State** 字段的显示为 **Connected**，说明主备服务通道已经成功建立。

```
[CORE-AC1] display hsb-service 0
```

```
Hot Standby Service Information:
```

```
-----
Local IP Address   : 172.16.100.1
Peer IP Address    : 172.16.100.2
Source Port        : 10241
Destination Port   : 10241
Keep Alive Times   : 5
Keep Alive Interval : 3
Service State      : Connected
Service Batch Modules :
Shared-key         : -
```

```
[CORE-AC2] display hsb-service 0
```

```
Hot Standby Service Information:
```

```
-----
Local IP Address   : 172.16.100.2
Peer IP Address    : 172.16.100.1
Source Port        : 10241
Destination Port   : 10241
Keep Alive Times   : 5
Keep Alive Interval : 3
Service State      : Connected
Service Batch Modules :
Shared-key         : -
```

在 CORE-AC1 和 CORE-AC2 上执行 **display hsb-group 0** 命令，查看 HSB 备份组的运行情况。

```
[CORE-AC1] display hsb-group 0
```

```
Hot Standby Group Information:
```

```
-----
HSB-group ID       : 0
Vrrp Group ID      : 1
Vrrp Interface      : Vlanif20
Service Index       : 0
Group Vrrp Status   : Master
Group Status        : Active
```

```

Group Backup Process      : Realtime
Peer Group Device Name    : AC6805
Peer Group Software Version : V200R022C10
Group Backup Modules      : Access-user
                          AP
                          DHCP

```

```
[CORE-AC2] display hsb-group 0
```

```
Hot Standby Group Information:
```

```

HSB-group ID             : 0
Vrrp Group ID            : 1
Vrrp Interface           : Vlanif20
Service Index            : 0
Group Vrrp Status        : Backup
Group Status             : Inactive
Group Backup Process      : Realtime
Peer Group Device Name    : AC6805
Peer Group Software Version : V200R022C10
Group Backup Modules      : Access-user
                          DHCP
                          AP

```

10. 在 CORE-AC1 上配置 AP 上线。

配置 AC 的源接口。

```
[CORE-AC1] capwap source interface vlanif 20
```

创建 AP 组，用于将相同配置的 AP 都加入到同一 AP 组中。

```

[CORE-AC1] wlan
[CORE-AC1-wlan-view] ap-group name ap-group1
[CORE-AC1-wlan-ap-group-ap-group1] quit

```

创建域管理模板，在域管理模板下配置 AC 的国家码并在 AP 组下引用域管理模板。

```

[CORE-AC1-wlan-view] regulatory-domain-profile name domain1
[CORE-AC1-wlan-regulate-domain-domain1] country-code cn
[CORE-AC1-wlan-regulate-domain-domain1] quit
[CORE-AC1-wlan-view] ap-group name ap-group1
[CORE-AC1-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the
radio and reset the AP. Continue?[Y/N]:y
[CORE-AC1-wlan-ap-group-ap-group1] quit

```

将目标 AP 加入 AP 组，并根据 AP 的部署位置为 AP 配置名称。

```
[CORE-AC1-wlan-view] ap auth-mode mac-auth
[CORE-AC1-wlan-view] ap-id 1 ap-mac 00e0-fc12-6660
[CORE-AC1-wlan-ap-1] ap-name area_1
[CORE-AC1-wlan-ap-1] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power
and antenna gain configurations of the radio, whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[CORE-AC1-wlan-ap-1] quit
[CORE-AC1-wlan-view] ap-id 2 ap-mac 00e0-fc12-6670
[CORE-AC1-wlan-ap-2] ap-name area_2
[CORE-AC1-wlan-ap-2] ap-group ap-group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power
and antenna gain configurations of the radio, whether to continue? [Y/N]:y
Info: This operation may take a few seconds. Please wait for a moment.. done.
[CORE-AC1-wlan-ap-2] quit
[CORE-AC1-wlan-view] quit
```

将 AP 上电后，可以查看到 AP 的“State”字段为“nor”。

```
[CORE-AC1] display ap all
Total AP information:
nor : normal      [2]
ExtraInfo : Extra information
P : insufficient power supply

-----
-----
ID  MAC      Name  Group  IP      Type      State  STA Uptime ExtraInfo
-----
-----
1   00e0-fc12-6660 area_1 ap-group1 192.168.20.41 AirEngine 8760-X1-PRO  nor  0  5M:26S -
2   00e0-fc12-6670 area_2 ap-group1 192.168.20.164 AirEngine 8760-X1-PRO  nor  0  2M:52S -
-----
-----
```

11. 在 CORE-AC1 上配置 STA 上线。

配置 WLAN 业务参数。

```
[CORE-AC1] wlan
[CORE-AC1-wlan-view] security-profile name sec1
[CORE-AC1-wlan-sec-prof-sec1] security open
[CORE-AC1-wlan-sec-prof-sec1] quit
[CORE-AC1-wlan-view] ssid-profile name ssid1
[CORE-AC1-wlan-ssid-prof-ssid1] ssid test01
[CORE-AC1-wlan-ssid-prof-ssid1] quit
[CORE-AC1-wlan-view] traffic-profile name traff1
```

```
[CORE-AC1-wlan-traffic-prof-traff1] user-isolate l2
[CORE-AC1-wlan-traffic-prof-traff1] quit
[CORE-AC1-wlan-view] security-profile name sec2
[CORE-AC1-wlan-sec-prof-sec2] security open
[CORE-AC1-wlan-sec-prof-sec2] quit
[CORE-AC1-wlan-view] ssid-profile name ssid2
[CORE-AC1-wlan-ssid-prof-ssid2] ssid test02
[CORE-AC1-wlan-ssid-prof-ssid2] quit
[CORE-AC1-wlan-view] traffic-profile name traff2
[CORE-AC1-wlan-traffic-prof-traff2] user-isolate l2
[CORE-AC1-wlan-traffic-prof-traff2] quit
```

配置 VAP 模板，配置业务数据转发模式、业务 VLAN，并应用安全模板和 SSID 模板，使能 STA 地址严格 DHCP 获取功能、IPSG 功能、动态 ARP 检测功能。

```
[CORE-AC1-wlan-view] vap-profile name vap1
[CORE-AC1-wlan-vap-prof-vap1] forward-mode direct-forward
[CORE-AC1-wlan-vap-prof-vap1] service-vlan vlan-id 30
[CORE-AC1-wlan-vap-prof-vap1] security-profile sec1
[CORE-AC1-wlan-vap-prof-vap1] ssid-profile ssid1
[CORE-AC1-wlan-vap-prof-vap1] traffic-profile traff1
[CORE-AC1-wlan-vap-prof-vap1] ip source check user-bind enable
[CORE-AC1-wlan-vap-prof-vap1] arp anti-attack check user-bind enable
[CORE-AC1-wlan-vap-prof-vap1] learn-client-address dhcp-strict
[CORE-AC1-wlan-vap-prof-vap1] quit
[CORE-AC1-wlan-view] vap-profile name vap2
[CORE-AC1-wlan-vap-prof-vap2] forward-mode direct-forward
[CORE-AC1-wlan-vap-prof-vap2] service-vlan vlan-id 40
[CORE-AC1-wlan-vap-prof-vap2] security-profile sec2
[CORE-AC1-wlan-vap-prof-vap2] ssid-profile ssid2
[CORE-AC1-wlan-vap-prof-vap2] traffic-profile traff2
[CORE-AC1-wlan-vap-prof-vap2] ip source check user-bind enable
[CORE-AC1-wlan-vap-prof-vap2] arp anti-attack check user-bind enable
[CORE-AC1-wlan-vap-prof-vap2] learn-client-address dhcp-strict
[CORE-AC1-wlan-vap-prof-vap2] quit
```

说明

由于 **ip source check user-bind enable** 命令是基于绑定表进行匹配检查的，因此

对于 DHCP 用户，需要使能 DHCP Snooping 自动生成动态绑定表。

对于静态配置 IP 的用户，需要手工配置静态绑定表。

learn-client-address dhcp-strict 命令的前置条件为：

在 VAP 模板视图下执行命令 **undo dhcp trust port** 去使能 AP 的 DHCP 信任功能。

在 VAP 模板视图下执行命令 **undo learn-client-address { ipv4 | ipv6 } disable** 使能 STA 地址学习功能。

配置 AP 组引用 VAP 模板。

```
[CORE-AC1-wlan-view] ap-group name ap-group1
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 0
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 0
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 1
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 1
[CORE-AC1-wlan-ap-group-ap-group1] quit
[CORE-AC1-wlan-view] quit
```

12. 配置 VRRP 热备份场景下的无线配置同步，将 CORE-AC1 的无线业务配置信息同步到 CORE-AC2。

配置 CORE-AC2 的源接口。

```
[CORE-AC2] capwap source interface vlanif 20
```

配置 CORE-AC1 上的无线配置同步功能。

```
[CORE-AC1] wlan
[CORE-AC1-wlan-view] master controller
[CORE-AC1-master-controller] master-redundancy peer-ip ip-address 172.16.100.2 local-ip ip-address 172.16.100.1 psk YsHsjx_202206
[CORE-AC1-master-controller] master-redundancy track-vrrp vrid 1 interface vlanif 20
[CORE-AC1-master-controller] quit
[CORE-AC1-wlan-view] quit
```

配置 CORE-AC2 上的无线配置同步功能。

```
[CORE-AC2] wlan
[CORE-AC2-wlan-view] master controller
[CORE-AC2-master-controller] master-redundancy peer-ip ip-address 172.16.100.1 local-ip ip-address 172.16.100.2 psk YsHsjx_202206
[CORE-AC2-master-controller] master-redundancy track-vrrp vrid 1 interface vlanif 20
[CORE-AC2-master-controller] quit
[CORE-AC2-wlan-view] quit
```

执行命令 **display sync-configuration status** 查看无线配置同步状态信息，**Status** 为 **cfg-mismatch**。需要在 Master AC 上手动触发无线配置同步到 Backup AC 上。等待 Backup AC 自动重启完成。

```
[CORE-AC1] display sync-configuration status
Controller role:Master/Backup/Local

-----
Controller IP Role  Device  Type          Version      Status      Last synced
-----
172.16.100.2 Backup AirEngine 8760-X1-PRO V200R022C10 cfg-mismatch(config check fail) -
```

```
Total: 1
```

```
[CORE-AC1] synchronize-configuration
```

```
Warning: This operation may reset the remote AC, synchronize configurations to it, and save all its
configurations. Whether to continue? [Y/N]:y
```

说明

手动触发无线配置同步后，Backup 会自动重启，等待 Backup AC 自动重启完成之后，再使用 **display sync-configuration status** 命令检查同步功能是否正常。

检查同步功能是否正常，如果状态为 **up**，表示无线配置同步功能正常。

```
[CORE-AC1] display sync-configuration status
```

```
Controller role:Master/Backup/Local
```

```
-----
Controller IP Role  Device  Type          Version          Status Last synced
-----
172.16.100.2 Backup AirEngine 8760-X1-PRO  V200R022C10      up    2019-11-05/19:09:14
-----
```

```
Total: 1
```

结果验证

预期结果

有线用户、无线用户均可正常接入园区网络。

验证方法

在 AC 上查看 AP 均已成功获取到 IP 地址。

```
[CORE-AC1] display ip pool interface vlanif20 used
```

```
Pool-name      : vlanif20
```

```
Pool-No       : 0
```

```
Lease         : 1 Days 0 Hours 0 Minutes
```

```
Domain-name   : -
```

```
DNS-server0   : -
```

```
NBNS-server0  : -
```

```
Netbios-type  : -
```

```
Position      : Interface
```

```
Status       : Unlocked
```

```
Gateway-0     : -
```

```
Network      : 192.168.20.0
```

```

Mask      : 255.255.255.0
Logging   : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :254   Used    :2
                  Idle     :233   Expired  :0
                  Conflict  :0     Disabled :19

```

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled

192.168.20.1	192.168.20.254	254	2	233(0)	0	19

Client-ID format as follows:

```

DHCP : mac-address          PPPoE : mac-address
IPSec : user-id/portnumber/vrf  PPP  : interface index
L2TP  : cpu-slot/session-id    SSL-VPN : user-id/session-id

```

Index	IP	Client-ID	Type	Left	Status
40	192.168.20.41	00e0-fc12-6660	DHCP	72528	Used
163	192.168.20.164	00e0-fc12-6670	DHCP	72813	Used

在核心交换机上查看有线用户均已成功获取到 IP 地址。

[CORE] display ip pool interface vlanif50 used

```

Pool-name      : Vlanif50
Pool-No        : 2
Lease          : 1 Days 0 Hours 0 Minutes
Domain-name    : -
DNS-server0    : 192.168.11.2
NBNS-server0   : -
Netbios-type   : -
Position       : Interface
Status         : Unlocked
Gateway-0      : -
Network        : 172.16.50.0

```


Mask : 255.255.255.0
VPN instance : --
Logging : Disable
Conflicted address recycle interval: --
Address Statistic: Total :254 Used :1
Idle :253 Expired :0
Conflict :0 Disabled :0

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled

172.16.50.1	172.16.50.254	254	1	253(0)	0	0

Client-ID format as follows:

DHCP : mac-address PPPoE : mac-address
IPSec : user-id/portnumber/vrf PPP : interface index
L2TP : cpu-slot/session-id SSL-VPN : user-id/session-id

Index	IP	Client-ID	Type	Left	Status
109	172.16.50.110	00e0-fc12-3344	DHCP	48538	Used

[CORE] display ip pool interface vlanif60 used

Pool-name : Vlanif60
Pool-No : 3
Lease : 1 Days 0 Hours 0 Minutes
Domain-name : --
DNS-server0 : 192.168.11.2
NBNS-server0 : --
Netbios-type : --
Position : Interface
Status : Unlocked
Gateway-0 : --
Network : 172.16.60.0

```

Mask      : 255.255.255.0
VPN instance  : --
Logging    : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :254   Used    :1
                  Idle     :253   Expired  :0
                  Conflict  :0     Disabled :0

```

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled

172.16.60.1	172.16.60.254	254	1	253(0)	0	0

Client-ID format as follows:

```

DHCP : mac-address          PPPoE : mac-address
IPSec : user-id/portnumber/vrf  PPP  : interface index
L2TP  : cpu-slot/session-id    SSL-VPN : user-id/session-id

```

Index	IP	Client-ID	Type	Left	Status
236	172.16.60.237	00e0-fc12-3377	DHCP	48050	Used

有线、无线用户可以实现互访。

在 AP1 上可以 Ping 通服务器区设备。

```
<area_1> ping 192.168.11.1
```

```
PING 192.168.11.1: 56 data bytes, press CTRL_C to break
```

```
Reply from 192.168.11.1: bytes=56 Sequence=1 ttl=63 time=1 ms
```

```
Reply from 192.168.11.1: bytes=56 Sequence=2 ttl=63 time=1 ms
```

```
Reply from 192.168.11.1: bytes=56 Sequence=3 ttl=63 time=1 ms
```

```
Reply from 192.168.11.1: bytes=56 Sequence=4 ttl=63 time=1 ms
```

```
Reply from 192.168.11.1: bytes=56 Sequence=5 ttl=63 time=1 ms
```

```
--- 192.168.11.1 ping statistics ---
```

```

5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/1/1 ms

```

AP1 下有无线用户接入后，在 CORE-AC1 上可以查看到接入的无线用户信息。

```
[CORE-AC1] display station ssid test01
```

```
Rf/WLAN: Radio ID/WLAN ID
```

```
Rx/Tx: link receive rate/link transmit rate(Mbps)
```

```

-----
STA MAC      AP ID Ap name Rf/WLAN Band Type Rx/Tx  RSSI VLAN IP address
-----

```

```

00e0-fc12-3388 2  area_2 1/1  5G  11ac 173/144  -38 30  172.16.30.180
-----

```

```
Total: 1 2.4G: 0 5G: 1
```

在 PC1 上可以 Ping 通连接 AP1 的用户。

```
C:\Users>ping 172.16.30.168
```

```
Pinging 172.16.30.168 with 32 bytes of data:
```

```
Reply from 172.16.30.168: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.168: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.168: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.168: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 172.16.30.168:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

配置文件

CORE 的配置文件

```

#
vlan batch 20 30 40 50 60 1000
#
dhcp enable
#
dhcp snooping enable
#

```

```
vlan 30
  dhcp snooping enable
vlan 40
  dhcp snooping enable
vlan 50
  dhcp snooping enable
vlan 60
  dhcp snooping enable
#
interface Vlanif20
  ip address 192.168.20.20 255.255.255.0
#
interface Vlanif30
  ip address 172.16.30.1 255.255.255.0
  arp-proxy inner-sub-vlan-proxy enable
  dhcp select interface
  dhcp server dns-list 192.168.11.2
#
interface Vlanif40
  ip address 172.16.40.1 255.255.255.0
  arp-proxy inner-sub-vlan-proxy enable
  dhcp select interface
  dhcp server dns-list 192.168.11.2
#
interface Vlanif50
  ip address 172.16.50.1 255.255.255.0
  arp-proxy inner-sub-vlan-proxy enable
  dhcp select interface
  dhcp server dns-list 192.168.11.2
#
interface Vlanif60
  ip address 172.16.60.1 255.255.255.0
  arp-proxy inner-sub-vlan-proxy enable
  dhcp select interface
  dhcp server dns-list 192.168.11.2
#
interface Vlanif1000
  ip address 192.168.11.1 255.255.255.0
#
interface Eth-Trunk1
  description con to CORE-AC1
  port link-type trunk
  undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 20
mode lacp
#
interface Eth-Trunk2
description con to CORE-AC2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20
mode lacp
#
interface Eth-Trunk10
description con to AGG1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40 50
mode lacp
#
interface Eth-Trunk20
description con to AGG2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40 60
mode lacp
#
interface XGigabitEthernet1/1/0/1
eth-trunk 10
#
interface XGigabitEthernet1/1/0/2
eth-trunk 20
#
interface XGigabitEthernet1/1/0/3
eth-trunk 1
#
interface XGigabitEthernet1/1/0/4
eth-trunk 2
#
interface XGigabitEthernet1/1/0/10
mad detect mode direct
#
interface XGigabitEthernet1/2/0/1
port link-type access
port default vlan 1000
#
```

```
interface XGigabitEthernet2/1/0/1
 eth-trunk 20
#
interface XGigabitEthernet2/1/0/2
 eth-trunk 10
#
interface XGigabitEthernet2/1/0/3
 eth-trunk 1
#
interface XGigabitEthernet2/1/0/4
 eth-trunk 2
#
interface XGigabitEthernet2/1/0/10
 mad detect mode direct
#
return
```

AGG1 的配置文件

```
#
vlan batch 20 30 40 50
#
interface Eth-Trunk10
 description connect to CORE
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20 30 40 50
 mode lacp-static
#
interface Eth-Trunk30
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20 30 40 50
 mode lacp-static
 port-isolate enable group 1
#
interface 10GE1/0/3
 eth-trunk 30
#
interface 10GE2/0/3
 eth-trunk 30
#
interface 10GE1/0/1
 eth-trunk 10
```

```
#  
interface 10GE2/0/1  
  eth-trunk 10  
#  
return
```

AGG2 的配置文件

```
#  
vlan batch 20 30 40 60  
#  
interface Eth-Trunk20  
  description connect to CORE  
  port link-type trunk  
  undo port trunk allow-pass vlan 1  
  port trunk allow-pass vlan 20 30 40 60  
  mode lacp-static  
#  
interface Eth-trunk40  
  port link-type trunk  
  undo port trunk allow-pass vlan 1  
  port trunk allow-pass vlan 20 30 40 60  
  mode lacp-static  
  port-isolate enable group 1  
#  
interface 10GE1/0/3  
  eth-trunk 40  
#  
interface 10GE2/0/3  
  eth-trunk 40  
#  
interface 10GE1/0/1  
  eth-trunk 20  
#  
interface 10GE2/0/1  
  eth-trunk 20  
#  
return
```

ACC1 的配置文件

```
#  
vlan batch 20 30 40 50  
#  
interface Eth-Trunk30  
  port link-type trunk
```

```
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40 50
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 30
#
interface 10GE1/0/2
eth-trunk 30
#
interface GE1/0/3
port link-type access
port default vlan 50
stp edged-port enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type trunk
port trunk pvid vlan 20
port trunk allow-pass vlan 20 30 40
stp edged-port enable
port-isolate enable group 1
#
return
```

ACC2 的配置文件

```
#
vlan batch 20 30 40 60
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40 60
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 40
#
interface 10GE1/0/2
eth-trunk 40
#
interface GE1/0/3
port link-type access
```



```
port default vlan 60
stp edged-port enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type trunk
port trunk pvid vlan 20
port trunk allow-pass vlan 20 30 40
stp edged-port enable
port-isolate enable group 1
#
return
```

CORE-AC1 的配置文件

```
#
sysname CORE-AC1
#
vrrp recover-delay 60
#
vlan batch 20 100
#
dhcp enable
#
interface Vlanif20
ip address 192.168.20.1 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
admin-vrrp vrid 1
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
dhcp select interface
dhcp server excluded-ip-address 192.168.20.2
dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif100
ip address 172.16.100.1 255.255.255.0
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20
mode lacp
#
interface GigabitEthernet0/0/2
```

```
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/21
eth-trunk 1
#
interface XGigabitEthernet0/0/22
eth-trunk 1
#
ip route-static 172.16.50.0 255.255.255.0 192.168.20.20
ip route-static 172.16.60.0 255.255.255.0 192.168.20.20
ip route-static 192.168.11.0 255.255.255.0 192.168.20.20
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.100.1 peer-ip 172.16.100.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff1
user-isolate l2
traffic-profile name traff2
user-isolate l2
security-profile name sec1
security open
security-profile name sec2
security open
ssid-profile name ssid1
ssid test01
ssid-profile name ssid2
ssid test02
```

```

vap-profile name vap1
forward-mode direct-forward
service-vlan vlan-id 30
ssid-profile ssid1
security-profile sec1
traffic-profile traff1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name vap2
forward-mode direct-forward
service-vlan vlan-id 40
ssid-profile ssid2
security-profile sec2
traffic-profile traff2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
master controller
master-redundancy track-vrrp vrid 1 interface Vlanif20
master-redundancy peer-ip ip-address 172.16.100.2 local-ip ip-address 172.16.100.1
psk %^%#5Vh&+;LCyDdLEV1gGJuP}9l(9W&u!+uHt";5T#yM%^%#
#
return

```

CORE-AC2 的配置文件

```

#
sysname CORE-AC2

```

```
#
vrrp recover-delay 60
#
vlan batch 20 100
#
dhcp enable
#
interface Vlanif20
 ip address 192.168.20.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.20.3
 admin-vrrp vrid 1
 dhcp select interface
 dhcp server excluded-ip-address 192.168.20.1
 dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif100
 ip address 172.16.100.2 255.255.255.0
#
interface Eth-Trunk2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20
 mode lacp
#
interface GigabitEthernet0/0/2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/21
 eth-trunk 2
#
interface XGigabitEthernet0/0/22
 eth-trunk 2
#
ip route-static 172.16.50.0 255.255.255.0 192.168.20.20
ip route-static 172.16.60.0 255.255.255.0 192.168.20.20
ip route-static 192.168.11.0 255.255.255.0 192.168.20.20
#
capwap source interface vlanif20
#
hsb-service 0
 service-ip-port local-ip 172.16.100.2 peer-ip 172.16.100.1 local-data-port 10241 peer-data-port 10241
```

```
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable

#
hsb-service-type access-user hsb-group 0

#
hsb-service-type dhcp hsb-group 0

#
hsb-service-type ap hsb-group 0

#
wlan
traffic-profile name traff1
user-isolate l2
traffic-profile name traff2
user-isolate l2
security-profile name sec1
security-profile name sec2
ssid-profile name ssid1
ssid test01
ssid-profile name ssid2
ssid test02
vap-profile name vap1
forward-mode direct-forward
service-vlan vlan-id 30
ssid-profile ssid1
security-profile sec1
traffic-profile traff1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name vap2
forward-mode direct-forward
service-vlan vlan-id 40
ssid-profile ssid2
security-profile sec2
traffic-profile traff2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
```

```
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
master controller
master-redundancy track-vrrp vrid 1 interface Vlanif20
master-redundancy peer-ip ip-address 172.16.100.1 local-ip ip-address 172.16.100.2
psk %^%#QKK0'nRL%0U`y32S6bOSB40e=FJE^Lbs7.A]x)QQ%^%#
#
return
```

1.1.2.1.5 独立 AC 方案：汇聚交换机做有线无线用户网关

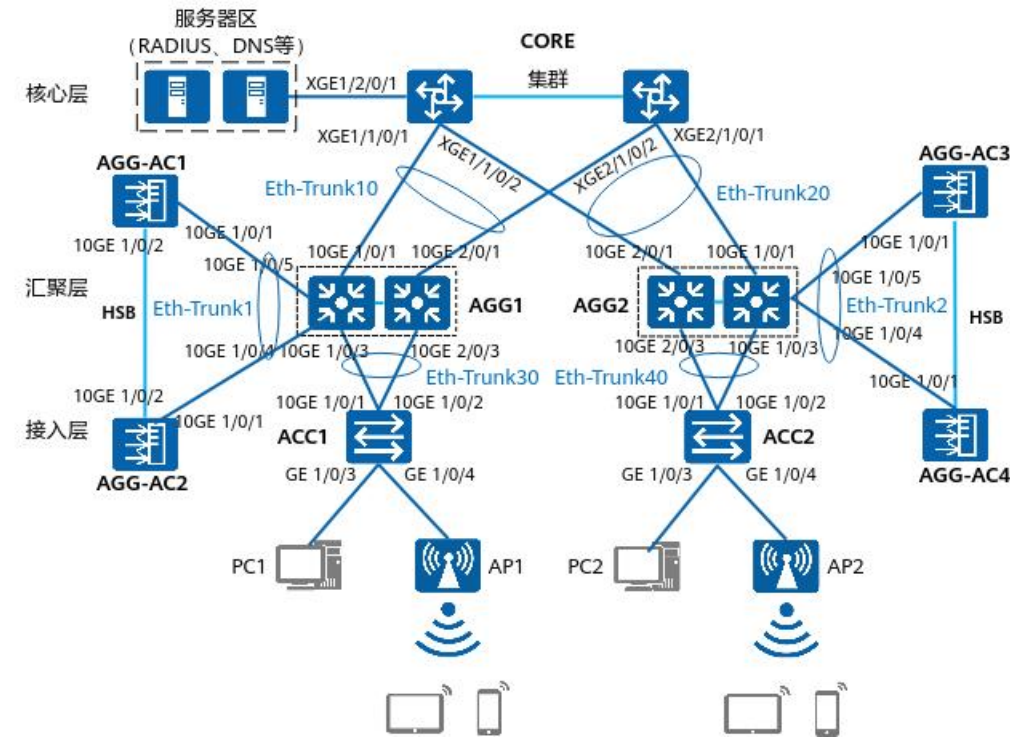
案例描述

核心层交换机组建集群，作为整个园区网络的核心，实现网络高可靠性和网络大数据量转发。

汇聚层交换机组建堆叠，实现设备级备份的同时，也扩展了设备的端口密度和转发带宽。独立 AC 旁挂式部署，统一管理全网 AP 上线。

本案例中，汇聚交换机作为全网有线无线用户的网关，负责全网用户业务的路由转发。

图 1 汇聚交换机做网关+独立 AC



设备要求和版本

位置	设备要求	本案例使用的设备	本案例使用的版本
核心层	–	S12700E	V200R022C10
汇聚层	–	S6730-H-V2	V600R022C10
接入层	–	S5735-L-V2	V600R022C10
AC	–	AC6805	V200R022C10
AP	–	AirEngine 8760-X1-PRO	V200R022C10

部署思路

步骤	部署思路	涉及设备
1	配置交换机的集群/堆叠功能，配置上下行 Eth-Trunk	核心交换机、汇聚交换机
2	配置交换机、AC 的接口和 VLAN，配置三层接口地址、路由，使得网络互通	核心交换机、汇聚交换机、接入交换机
3	配置汇聚交换机和 AC 的 DHCP 功能，使交换机和 AC 分别作为 DHCP 服务器为有线/无线用户和 AP 分配 IP 地址	汇聚交换机、AC
4	配置 AC 的 VRRP+HSB 方式的备份	AC

步骤	部署思路	涉及设备
5	配置 AC 的无线业务，实现 AP 和 STA 上线	AC
6	配置 VRRP 热备份场景下的无线配置同步	AC

数据规划

表 1 核心交换机业务数据规划

项目	VLAN ID	网段
连接 AGG1 的网段	VLAN 70	172.16.70.0/24
连接 AGG2 的网段	VLAN 80	172.16.80.0/24
连接服务器的网段	VLAN 1000	192.168.11.254/24

表 2 汇聚交换机业务数据规划

设备	项目	VLAN ID	网段
AGG1	无线用户的业务 VLAN	VLAN 30	172.16.30.0/24
		VLAN 31	172.16.31.0/24
	有线用户的业务 VLAN	VLAN 50	172.16.50.0/24
	连接 CORE 的网段	VLAN 70	172.16.70.0/24
	连接 AGG-AC 的网段	VLAN 20	172.16.20.0/24
AGG2	无线用户的业务 VLAN	VLAN 40	172.16.40.0/24
		VLAN 41	172.16.41.0/24
	有线用户的业务 VLAN	VLAN 60	172.16.60.0/24
	连接 CORE 的网段	VLAN 80	172.16.80.0/24
	连接 AGG-AC 的网段	VLAN 20	172.16.20.0/24

表 3 AGG-AC 业务数据规划

设备	项目	VLAN ID	网段
AGG-AC1、AGG-AC2	AP 管理 VLAN	VLAN 20	192.168.20.0/24
	连接 CORE 的网段	VLAN 70	172.16.70.0/24

表 3 AGG-AC 业务数据规划

设备	项目	VLAN ID	网段
AGG-AC3、AGG-AC4	主备 AC HSB 同步 VLAN	VLAN 200	172.16.200.0/24
	AP 管理 VLAN	VLAN 21	192.168.21.0/24
	连接 CORE 的网段	VLAN 80	172.16.80.0/24
	主备 AC HSB 同步 VLAN	VLAN 200	172.16.200.0/24

表 4 AGG-AC 无线业务数据规划

项目	数据
AP 组	ap-group1、ap-group2
域管理模板	domain1
SSID 模板	ssid1、ssid2
VAP 模板	vap1、vap2、直接转发模式

配置注意事项

- 不建议使用 VLAN 1 作为管理 VLAN 或者业务 VLAN，将各端口从 VLAN 1 中退出。根据实际业务需求透传 VLAN，禁止端口透传所有 VLAN。
- 直接转发方式下，建议管理 VLAN 和业务 VLAN 分别使用不同的 VLAN，否则可能导致业务不通。例如，业务 VLAN 如果和管理 VLAN 相同，且交换机连接 AP 的端口配置了 PVID 为管理 VLAN，则下行到用户的报文出连接 AP 的交换机时业务 VLAN 会被终结，从而导致业务不通。
- 直接转发模式下，AP 的业务报文不会进行 CAPWAP 封装，而是直接转发给上层网络，所以需要 AP 与上层网络间的网络加入业务 VLAN，配置 AC 与 AP 间的网络加入管理 VLAN，才能正常传输业务报文和管理报文。
- 对于主备 AC 上关联的同一 AP，其 WLAN 相关的业务配置必须保持一致（如 WMM 模板、射频模板、射频、流量模板、安全模板、安全策略和 WLAN ID 等都需要保持一致），否则当 AC 的主备状态切换后，无法保证用户业务正常。
- 主备 AC 的型号和软件版本需完全一致。
- 在 VRRP 热备份场景下部署 DHCP 服务器时需要注意以下几点：
- V200R019C00 及之后版本，开启 DHCP 服务器功能的接口无限制，主 AC 分配 IP 地址，备 AC 不分配，主 AC 的 IP 地址分配信息会同步到备 AC。
 - 主备 AC 上配置的 IP 地址池必须完全一致，配置不一致会导致主备 AC 备份失败。
 - 配置命令 `hsb-service-type dhcp hsb-group group-index`，使 DHCP 业务绑定 HSB 备份组。否则主备 AC 上的 IP 地址分配信息无法备份。

配置步骤

1. 配置核心层交换机集群和汇聚层交换机堆叠、多主检测及上下行 Eth-Trunk。

此部分配置请参考 [集群/堆叠通用部署](#)。

2. 配置核心交换机 CORE 的接口和 VLAN。

创建 VLAN。

```
[CORE] vlan batch 70 80 1000
```

配置与汇聚交换机 AGG1 互连的 Eth-Trunk。和汇聚交换机 AGG2 互连的配置与此类似，此处不再赘述。

```
[CORE] interface eth-trunk 10
[Core-Eth-Trunk10] description connect to AGG1
[Core-Eth-Trunk10] mode lacp
[Core-Eth-Trunk10] port link-type trunk
[Core-Eth-Trunk10] port trunk allow-pass vlan 70
[Core-Eth-Trunk10] undo port trunk allow-pass vlan 1
[Core-Eth-Trunk10] quit
```

将和服务器对接的接口加入 VLAN1000。

```
[CORE] interface xgigabitethernet 1/2/0/1
[Core-XGigabitEthernet1/2/0/1] port link-type access
[Core-XGigabitEthernet1/2/0/1] port default vlan 1000
[Core-XGigabitEthernet1/2/0/1] quit
```

创建连接汇聚交换机 AGG1 的三层接口 VLANIF70。

```
[CORE] interface vlanif 70
[Core-Vlanif70] ip address 172.16.70.1 255.255.255.0
[Core-Vlanif70] quit
```

创建连接汇聚交换机 AGG2 的三层接口 VLANIF80。

```
[CORE] interface vlanif 80
[Core-Vlanif80] ip address 172.16.80.1 255.255.255.0
[Core-Vlanif80] quit
```

创建连接服务器的三层接口 VLANIF1000。

```
[CORE] interface vlanif 1000
[Core-Vlanif1000] ip address 192.168.11.254 255.255.255.0
[Core-Vlanif1000] quit
```

3. 配置汇聚交换机 AGG1 的接口和 VLAN。汇聚交换机 AGG2 的配置与此类似，不再赘述。

创建 VLAN。

```
[AGG1] vlan batch 20 30 31 50 70
```

配置与核心交换机 CORE 连接的 Eth-Trunk。

```
[AGG1] interface eth-trunk 10
```

```
[AGG1-Eth-Trunk10] description connect to CORE
[AGG1-Eth-Trunk10] mode lacp-static
[AGG1-Eth-Trunk10] port link-type trunk
[AGG1-Eth-Trunk10] port trunk allow-pass vlan 70
[AGG1-Eth-Trunk10] quit
[AGG1] interface 10ge 1/0/1
[AGG1-10GE1/0/1] eth-trunk 10
[AGG1-10GE1/0/1] quit
[AGG1] interface 10ge 2/0/1
[AGG1-10GE2/0/1] eth-trunk 10
[AGG1-10GE2/0/1] quit
```

创建和 AGG-AC1 互连的 Eth-Trunk1 并将接口加入 Eth-Trunk。

```
[AGG1] interface eth-trunk 1
[AGG1-Eth-Trunk1] description con to AC
[AGG1-Eth-Trunk1] mode lacp-static
[AGG1-Eth-Trunk1] port link-type trunk
[AGG1-Eth-Trunk1] port trunk allow-pass vlan 20
[AGG1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk1] quit
[AGG1] interface 10ge 1/0/4
[AGG1-10GE1/0/4] eth-trunk 1
[AGG1-10GE1/0/4] quit
[AGG1] interface 10ge 1/0/5
[AGG1-10GE1/0/5] eth-trunk 1
[AGG1-10GE1/0/5] quit
```

创建连接核心交换机 CORE 的三层接口 VLANIF70。

```
[AGG1] interface Vlanif 70
[AGG1-Vlanif70] ip address 172.16.70.2 255.255.255.0
[AGG1-Vlanif70] quit
```

创建连接 AC 的三层接口 VLANIF20。

```
[CORE] interface vlanif 20
[CORE-Vlanif20] ip address 192.168.20.20 255.255.255.0
[CORE-Vlanif20] quit
```

配置与接入交换机 ACC1 连接的下行接口。

```
[AGG1] interface eth-trunk 30
[AGG1-Eth-Trunk30] port link-type trunk
[AGG1-Eth-Trunk30] port trunk allow-pass vlan 20 30 31 50
[AGG1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk30] quit
[AGG1] interface 10ge 1/0/3
[AGG1-10GE1/0/3] eth-trunk 30
```

```
[AGG1-10GE1/0/3] quit
[AGG1] interface 10ge 2/0/3
[AGG1-10GE2/0/3] eth-trunk 30
[AGG1-10GE2/0/3] quit
```

4. 配置 AGG-AC1 的接口和 VLAN。AGG-AC2、AGG-AC3 和 AGG-AC4 的配置与此类似，不再赘述。

创建 VLAN。

```
<AC6805> system-view
[AC6805] sysname AGG-AC1
[AGG-AC1] vlan batch 20 200
```

创建 AGG-AC1 与汇聚交换机 AGG1 互连的 Eth-Trunk，并将接口加入 Eth-Trunk。

```
[AGG-AC1] interface eth-trunk 1
[AGG-AC1-Eth-Trunk1] description connect to AGG1
[AGG-AC1-Eth-Trunk1] mode lacp
[AGG-AC1-Eth-Trunk1] port link-type trunk
[AGG-AC1-Eth-Trunk1] port trunk allow-pass vlan 20
[AGG-AC1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[AGG-AC1-Eth-Trunk1] quit
[AGG-AC1] interface 10ge 1/0/1
[AGG-AC1-10GE1/0/1] eth-trunk 1
[AGG-AC1-10GE1/0/1] quit
```

配置 AGG-AC1 链接 AGG-AC2 的接口。

```
[AGG-AC1] interface 10ge 1/0/2
[AGG-AC1-10GE1/0/2] port link-type trunk
[AGG-AC1-10GE1/0/2] port trunk allow-pass vlan 200
[AGG-AC1-10GE1/0/2] undo port trunk allow-pass vlan 1
[AGG-AC1-10GE1/0/2] quit
[AGG-AC1] interface vlanif 200
[AGG-AC1-Vlanif200] ip address 172.16.200.1 255.255.255.0
[AGG-AC1-Vlanif200] quit
```

5. 配置接入交换机 ACC1 的接口和 VLAN。接入交换机 ACC2 的配置与此类似，不再赘述。

创建 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1
[ACC1] vlan batch 20 30 31 50
```

配置与汇聚交换机 AGG1 连接的上行接口。

```
[ACC1] interface eth-trunk 30
[ACC1-Eth-Trunk30] mode lacp-static
[ACC1-Eth-Trunk30] port link-type trunk
```

```
[ACC1-Eth-Trunk30] port trunk allow-pass vlan 20 30 31 50
[ACC1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[ACC1-Eth-Trunk30] quit
[ACC1] interface 10ge 1/0/1
[ACC1-10GE1/0/1] eth-trunk 30
[ACC1-10GE1/0/1] quit
[ACC1] interface 10ge 1/0/2
[ACC1-10GE1/0/2] eth-trunk 30
[ACC1-10GE1/0/2] quit
```

配置与 PC1 和 AP1 连接的下行接口，并将连接 PC1 和 AP1 的端口配置为边缘端口。

```
[ACC1] interface GE 1/0/3
[ACC1-GE1/0/3] port link-type access
[ACC1-GE1/0/3] port default vlan 50
[ACC1-GE1/0/3] port-isolate enable group 1
[ACC1-GE1/0/3] stp edged-port enable
[ACC1-GE1/0/3] quit
[ACC1] interface GE 1/0/4
[ACC1-GE1/0/4] port link-type trunk
[ACC1-GE1/0/4] port trunk pvid vlan 20
[ACC1-GE1/0/4] port trunk allow-pass vlan 20 30 31
[ACC1-GE1/0/4] port-isolate enable group 1
[ACC1-GE1/0/4] stp edged-port enable
[ACC1-GE1/0/4] quit
```

6. 配置汇聚交换机 AGG1 的 DHCP 功能，使得交换机作为 DHCP 服务器为有线、无线用户分配 IP 地址。汇聚交换机 AGG2 的配置与此类似，不再赘述。

使能全局 DHCP 功能，并配置业务 VLAN 的 DHCP Snooping 功能。

```
[AGG1] dhcp enable
[AGG1] dhcp snooping enable
[AGG1] vlan 30
[AGG1-vlan30] dhcp snooping enable
[AGG1-vlan30] quit
[AGG1] vlan 31
[AGG1-vlan31] dhcp snooping enable
[AGG1-vlan31] quit
[AGG1] vlan 50
[AGG1-vlan50] dhcp snooping enable
[AGG1-vlan50] quit
```

创建无线业务三层接口 VLANIF30 并通过接口地址池为 STA 分配地址。

```
[AGG1] interface Vlanif 30
[AGG1-Vlanif30] ip address 172.16.30.1 255.255.255.0
[AGG1-Vlanif30] dhcp select interface
```

```
[AGG1-Vlanif30] dhcp server dns-list 192.168.11.1 //配置终端的 DNS 服务器
[AGG1-Vlanif30] arp proxy intra-vlan enable //开启 VLAN 内 ARP 代理
[AGG1-Vlanif30] quit
```

创建无线业务三层接口 VLANIF31 并通过接口地址池为 STA 分配地址。

```
[AGG1] interface Vlanif 31
[AGG1-Vlanif31] ip address 172.16.31.1 255.255.255.0
[AGG1-Vlanif31] dhcp select interface
[AGG1-Vlanif31] dhcp server dns-list 192.168.11.1 //配置终端的 DNS 服务器
[AGG1-Vlanif31] arp proxy intra-vlan enable //开启 VLAN 内 ARP 代理
[AGG1-Vlanif31] quit
```

创建有线业务三层接口 VLANIF50 并配置通过接口地址池为有线终端分配地址。

```
[AGG1] interface Vlanif 50
[AGG1-Vlanif50] ip address 172.16.50.1 255.255.255.0
[AGG1-Vlanif50] dhcp select interface
[AGG1-Vlanif50] dhcp server dns-list 192.168.11.1 //配置终端的 DNS 服务器
[AGG1-Vlanif50] arp proxy intra-vlan enable //开启 VLAN 内 ARP 代理
[AGG1-Vlanif50] quit
```

7. 配置核心交换机和汇聚交换机的路由功能，实现三层网络互通。

在核心交换机 CORE 上配置 OSPF 功能。

```
[CORE] ospf 1 router-id 1.1.1.1
[CORE-ospf-1] area 0
[CORE-ospf-1-area-0.0.0.0] network 172.16.70.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] network 172.16.80.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] network 192.168.11.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] quit
```

在汇聚交换机 AGG1 上配置 OSPF 功能。汇聚交换机 AGG2 的配置与此类似，不再赘述。

```
[AGG1] ospf 1 router-id 2.2.2.2
[AGG1-ospf-1] area 0
[AGG1-ospf-1-area-0.0.0.0] network 172.16.70.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 172.16.30.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 172.16.31.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 172.16.50.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] quit
[AGG1-ospf-1] area 1
[AGG1-ospf-1-area-0.0.0.1] network 192.168.20.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.1] quit
[CORE-ospf-1] quit
```

在 AGG-AC1 配置上配置 OSPF 功能。

```
[AGG-AC1] ospf 1 router-id 3.3.3.3
```

```
[AGG-AC1-ospf-1] area 1
[AGG-AC1-ospf-1-area-0.0.0.1] network 192.168.20.0 0.0.0.255
[AGG-AC1-ospf-1-area-0.0.0.1] quit
[AGG-AC1-ospf-1] quit
```

8. 配置 AGG-AC1 的 DHCP 功能，使 AC 作为 DHCP 服务器为 AP 分配 IP 地址。AGG-AC3 的配置与此类似，不再赘述。

```
[AGG-AC1] dhcp enable
[AGG-AC1] interface Vlanif 20
[AGG-AC1-Vlanif20] ip address 172.16.20.1 255.255.255.0
[AGG-AC1-Vlanif20] dhcp select interface
[AGG-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.2
[AGG-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.20
[AGG-AC1-Vlanif20] quit
```

9. 配置 AGG-AC1 的 VRRP+HSB 方式的备份。AGG-AC2 配置与此类似，不再赘述。

配置 VRRP 备份组的状态恢复延迟时间为 60 秒。

```
[AGG-AC1] vrrp recover-delay 60
```

在 AGG-AC1 上创建管理 VRRP 备份组，配置 AGG-AC1 在该备份组中的优先级为 120，并配置抢占时间为 1200 秒。

```
[AGG-AC1] interface vlanif 20
[AGG-AC1-Vlanif20] vrrp vrid 1 virtual-ip 192.168.20.3
[AGG-AC1-Vlanif20] vrrp vrid 1 priority 120
[AGG-AC1-Vlanif20] vrrp vrid 1 preempt-mode timer delay 1200
[AGG-AC1-Vlanif20] quit
```

在 AGG-AC1 上创建 HSB 主备服务 0，并配置其主备通道 IP 地址和端口号。

```
[AGG-AC1] hsb-service 0
[AGG-AC1-hsb-service-0] service-ip-port local-ip 172.16.200.1 peer-ip 172.16.200.2 local-data-port
10241 peer-data-port 10241
[AGG-AC1-hsb-service-0] quit
```

在 AGG-AC1 上创建 HSB 备份组 0，并配置其绑定 HSB 主备服务 0 和管理 VRRP 备份组。

```
[AGG-AC1] hsb-group 0
[AGG-AC1-hsb-group-0] bind-service 0
[AGG-AC1-hsb-group-0] track vrrp vrid 1 interface vlanif 20
[AGG-AC1-hsb-group-0] quit
```

配置 AGG-AC1 业务绑定 HSB 备份组。

```
[AGG-AC1] hsb-service-type access-user hsb-group 0
[AGG-AC1] hsb-service-type ap hsb-group 0
[AGG-AC1] hsb-group 0
[AGG-AC1-hsb-group-0] hsb enable
[AGG-AC1-hsb-group-0] quit
```

配置完成后，在 AGG-AC1 和 AGG-AC2 上分别执行 **display vrrp** 命令，可以看到 AGG-AC1 的 State 字段的显示为 **Master**，AGG-AC2 的 State 字段的显示为 **Backup**。

[AGG-AC1] **display vrrp**

Vlanif20 | Virtual Router 1
State : **Master**
Virtual IP : 192.168.20.3
Master IP : 192.168.20.3
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES Delay Time : 1200 s
TimerRun : 2 s
TimerConfig : 2 s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : admin-vrrp
Backup-forward : disabled
Track SysHealth Priority reduced : 254
SysHealth state : UP
Create time : 2019-11-30 14:23:11
Last change time : 2019-11-30 14:23:17

[AGG-AC2] **display vrrp**

Vlanif20 | Virtual Router 1
State : **Backup**
Virtual IP : 192.168.20.3
Master IP : 192.168.20.2
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 0
Preempt : YES Delay Time : 1200 s
TimerRun : 2 s
TimerConfig : 2 s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : admin-vrrp
Backup-forward : disabled
Track SysHealth Priority reduced : 254
SysHealth state : UP
Create time : 2019-11-30 07:15:11
Last change time : 2019-11-30 14:23:17

在 AGG-AC1 和 AGG-AC2 上查看主备服务的建立情况。可以看到 **Service State** 字段的显示为 **Connected**，说明主备服务通道已经成功建立。

```
[AGG-AC1] display hsb-service 0
```

Hot Standby Service Information:

```
-----  
Local IP Address    : 172.16.200.1  
Peer IP Address     : 172.16.200.2  
Source Port         : 10241  
Destination Port    : 10241  
Keep Alive Times    : 5  
Keep Alive Interval : 3  
Service State       : Connected  
Service Batch Modules :  
Shared-key          : -  
-----
```

```
[AGG-AC2] display hsb-service 0
```

Hot Standby Service Information:

```
-----  
Local IP Address    : 172.16.200.2  
Peer IP Address     : 172.16.200.1  
Source Port         : 10241  
Destination Port    : 10241  
Keep Alive Times    : 5  
Keep Alive Interval : 3  
Service State       : Connected  
Service Batch Modules :  
Shared-key          : -  
-----
```

在 AGG-AC1 和 AGG-AC2 上执行 **display hsb-group 0** 命令，查看 HSB 备份组的运行情况。

```
[AGG-AC1] display hsb-group 0
```

Hot Standby Group Information:

```
-----  
HSB-group ID        : 0  
Vrrp Group ID       : 1  
Vrrp Interface       : Vlanif20  
Service Index        : 0  
Group Vrrp Status    : Master  
Group Status         : Active  
Group Backup Process  : Realtime  
Peer Group Device Name : AC6805  
Peer Group Software Version : V200R022C10  
Group Backup Modules  : Access-user  
-----
```

AP

```
[AGG-AC2] display hsb-group 0
```

Hot Standby Group Information:

```

HSB-group ID      : 0
Vrrp Group ID     : 1
Vrrp Interface    : Vlanif20
Service Index     : 0
Group Vrrp Status : Backup
Group Status      : Active
Group Backup Process : Realtime
Peer Group Device Name : AC6805
Peer Group Software Version : V200R022C10
Group Backup Modules : Access-user

```

AP

10. 配置 AGG-AC1 的无线业务，实现 AP1 上线。AGG-AC2 的配置与此类似，不再赘述。

配置 AC 的源接口。

```
[AGG-AC1] capwap source interface vlanif 20
```

#创建 AP 组，用于将相同配置的 AP 都加入到同一 AP 组中。

```

[AGG-AC1] wlan
[AGG-AC1-wlan-view] ap-group name ap-group1
[AGG-AC1-wlan-ap-group-ap-group1] quit

```

创建域管理模板，在域管理模板下配置 AC 的国家码并在 AP 组下引用域管理模板。

```

[AGG-AC1-wlan-view] regulatory-domain-profile name domain1
[AGG-AC1-wlan-regulate-domain-domain1] country-code cn
[AGG-AC1-wlan-regulate-domain-domain1] quit
[AGG-AC1-wlan-view] ap-group name ap-group1
[AGG-AC1-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the
radio and reset the AP. Continue?[Y/N]:y
[AGG-AC1-wlan-ap-group-ap-group1] quit

```

将 AP1 加入 AP 组 ap-group1，并根据 AP 的部署位置为 AP 配置名称。

```

[AGG-AC1-wlan-view] ap auth-mode mac-auth
[AGG-AC1-wlan-view] ap-id 1 ap-mac 00e0-fc12-3300
[AGG-AC1-wlan-ap-1] ap-name area_1
Warning: The AP name of more than 31 characters does not take effect for APs in versions earlier than
V200R009C00.
Warning: This operation may cause AP reset. Continue? [Y/N]:y

```

```
[AGG-AC1-wlan-ap-1] ap-group ap-group1
```

Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, whether to continue? [Y/N]:y

Info: This operation may take a few seconds. Please wait for a moment.. done.

```
[AGG-AC1-wlan-ap-1] quit
```

```
[AGG-AC1-wlan-view] quit
```

将 AP1 上电后，可以查看到 AP1 的“State”字段为“nor”。

```
[AGG-AC1] display ap all
```

Info: This operation may take a few seconds. Please wait for a moment.done.

Total AP information:

```
nor : normal      [1]
```

```
-----
ID  MAC      Name  Group  IP      Type      State STA Uptime
-----
1   00e0-fc12-3300 area_1 ap-group1 192.168.20.254 AirEngine 8760-X1-PRO  nor  0  2M:44S
-----
```

Total AP information:

```
nor : normal      [1]
```

ExtraInfo : Extra information

```
P   : insufficient power supply
```

```
-----
ID  MAC      Name  Group  IP      Type      State STA Uptime  ExtraInfo
-----
1   00e0-fc12-4400 area_1 ap-group1 192.168.20.148 AirEngine 8760-X1-PRO nor  0  1H:19M:18S -
-----
```

11. 在 AGG-AC1 上配置 STA 上线。

配置 WLAN 业务参数，创建安全模板、SSID 模板和流量模板。

```
[AGG-AC1] wlan
```

```
[AGG-AC1-wlan-view] security-profile name sec1
```

```
[AGG-AC1-wlan-sec-prof-sec1] quit
```

```
[AGG-AC1-wlan-view] ssid-profile name ssid1
```

```
[AGG-AC1-wlan-ssid-prof-ssid1] ssid test01
```

```
[AGG-AC1-wlan-ssid-prof-test01] quit
```

```
[AGG-AC1-wlan-view] traffic-profile name traff1
```

```
[AGG-AC1-wlan-traffic-prof-traff1] user-isolate l2
```

```
[AGG-AC1-wlan-traffic-prof-test01] quit
[AGG-AC1-wlan-view] security-profile name sec2
[AGG-AC1-wlan-sec-prof-sec2] quit
[AGG-AC1-wlan-view] ssid-profile name ssid2
[AGG-AC1-wlan-ssid-prof-ssid2] ssid test02
[AGG-AC1-wlan-ssid-prof-test02] quit
[AGG-AC1-wlan-view] traffic-profile name traff2
[AGG-AC1-wlan-traffic-prof-traff2] user-isolate l2
[AGG-AC1-wlan-traffic-prof-traff2] quit
```

配置 WLAN-VAP 模板，配置业务数据转发模式、业务 VLAN，并应用安全模板和 SSID 模板，使能 IPSG 功能动态 ARP 检测功能和 STA 地址严格 DHCP 获取功能。

```
[AGG-AC1-wlan-view] vap-profile name vap1
[AGG-AC1-wlan-vap-prof-test01] forward-mode direct-forward
[AGG-AC1-wlan-vap-prof-test01] service-vlan vlan-id 30
[AGG-AC1-wlan-vap-prof-test01] security-profile sec1
[AGG-AC1-wlan-vap-prof-test01] ssid-profile ssid1
[AGG-AC1-wlan-vap-prof-test01] traffic-profile traff1
[AGG-AC1-wlan-vap-prof-test01] ip source check user-bind enable
[AGG-AC1-wlan-vap-prof-test01] arp anti-attack check user-bind enable
[AGG-AC1-wlan-vap-prof-test01] learn-client-address dhcp-strict
[AGG-AC1-wlan-vap-prof-test01] quit
[AGG-AC1-wlan-view] vap-profile name vap2
[AGG-AC1-wlan-vap-prof-test02] forward-mode direct-forward
[AGG-AC1-wlan-vap-prof-test02] service-vlan vlan-id 31
[AGG-AC1-wlan-vap-prof-test02] security-profile sec2
[AGG-AC1-wlan-vap-prof-test02] ssid-profile ssid2
[AGG-AC1-wlan-vap-prof-test02] traffic-profile traff2
[AGG-AC1-wlan-vap-prof-test02] ip source check user-bind enable
[AGG-AC1-wlan-vap-prof-test02] arp anti-attack check user-bind enable
[AGG-AC1-wlan-vap-prof-test02] learn-client-address dhcp-strict
[AGG-AC1-wlan-vap-prof-test02] quit
```

说明

由于 **ip source check user-bind enable** 命令是基于绑定表进行匹配检查的，因此

对于 DHCP 用户，需要使能 DHCP Snooping 自动生成动态绑定表。

对于静态配置 IP 的用户，需要手工配置静态绑定表。

learn-client-address dhcp-strict 命令的前置条件为：

在 VAP 模板视图下执行命令 **undo dhcp trust port** 去使能 AP 的 DHCP 信任功能。

在 VAP 模板视图下执行命令 **undo learn-client-address { ipv4 | ipv6 } disable** 使能 STA 地址学习功能。

配置 AP 组引用 VAP 模板。

```
[AGG-AC1-wlan-view] ap-group name ap-group1
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 0
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 0
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 1
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 1
[AGG-AC1-wlan-ap-group-ap-group1] quit
[AGG-AC1-wlan-view] quit
```

结果验证

预期结果

有线用户、无线用户均可正常接入园区网络。

验证方法

以汇聚交换机 AGG1 和 AGG-AC1 为例，汇聚交换机 AGG2 和 AGG-AC3 上的验证方法与此类似，不再赘述。

在 AGG-AC1 上查看 AP 已成功获取到 IP 地址。

```
[AGG-AC1] display ip pool interface vlanif20 used
Pool-name      : Vlanif20
Pool-No        : 0
Lease          : 1 Days 0 Hours 0 Minutes
Domain-name    : -
DNS-server0    : -
NBNS-server0   : -
Netbios-type   : -
Position       : Interface
Status         : Unlocked
Gateway-0      : -
Network        : 192.168.20.0
Mask           : 255.255.255.0
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total    :254    Used    :1
                   Idle     :251    Expired  :0
                   Conflict  :0      Disabled :2
```

Network section							
Start	End	Total	Used	Idle(Expired)	Conflict	Disabled	

192.168.20.1 192.168.20.254 254 1 251(0) 0 2

Client-ID format as follows:

DHCP : mac-address PPPoE : mac-address

IPSec : user-id/portnumber/vrf PPP : interface index

L2TP : cpu-slot/session-id SSL-VPN : user-id/session-id

Index	IP	Client-ID	Type	Left	Status
147	192.168.20.148	00e0-fc12-4400	DHCP	80426	Used

在汇聚交换机 AGG1 上查看有线 用户均已成功获取到 IP 地址。

[AGG1] display ip pool interface vlanif50 used

Pool-name : Vlanif50

Pool-No : 2

Lease : 1 Days 0 Hours 0 Minutes

Domain-name : -

DNS-server0 : 192.168.11.1

NBNS-server0 : -

Netbios-type : -

Position : Interface

Status : Unlocked

Gateway-0 : -

Network : 172.16.50.0

Mask : 255.255.255.0

VPN instance : --

Logging : Disable

Conflicted address recycle interval: -

Address Statistic: Total :254 Used :1

Idle :254 Expired :0

Conflict :0 Disabled :0

Network section

StartEndTotalUsedIdle(Expired)ConflictDisabled

```
172.16.50.1 172.16.50.254 254 0 254(0) 0 0
```

有线、无线用户可以实现互访。

在 AP1 上可以 Ping 通服务器区设备。

```
<area_1> ping 192.168.11.1
PING 192.168.11.1: 56 data bytes, press CTRL_C to break
  Reply from 192.168.11.1: bytes=56 Sequence=1 ttl=63 time=1 ms
  Reply from 192.168.11.1: bytes=56 Sequence=2 ttl=63 time=1 ms
  Reply from 192.168.11.1: bytes=56 Sequence=3 ttl=63 time=1 ms
  Reply from 192.168.11.1: bytes=56 Sequence=4 ttl=63 time=1 ms
  Reply from 192.168.11.1: bytes=56 Sequence=5 ttl=63 time=1 ms

--- 192.168.11.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 1/1/1 ms
```

AP1 下有无线用户接入后，在 AGG-AC1 上可以查看到接入的无线用户信息。

```
[AGG-AC1] display station ssid test01
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)

-----
-----
STA MAC      AP ID Ap name Rf/WLAN Band Type Rx/Tx  RSSI VLAN IP address
-----
-----
00e0-fc12-5555 1 area_1 0/1 2.4G 11n 24/1 -38 30 172.16.30.180
-----
-----
Total: 1 2.4G: 1 5G: 0
```

在 PC1 上可以 Ping 通 AP1 的无线用户。

```
C:\Users>ping 172.16.30.180

Pinging 172.16.30.180 with 32 bytes of data:
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.30.180:
```

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

配置文件

CORE 的配置文件

```
#
sysname CORE
#
vlan batch 70 80 1000
#
interface Vlanif70
 ip address 172.16.70.1 255.255.255.0
#
interface Vlanif80
 ip address 172.16.80.1 255.255.255.0
#
interface Vlanif1000
 ip address 192.168.11.254 255.255.255.0
#
interface Eth-Trunk10
 description connect to AGG1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 70
 mode lacp
#
interface Eth-Trunk20
 description connect to AGG2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 80
 mode lacp
#
interface XGigabitEthernet1/1/0/1
 eth-trunk 10
#
interface XGigabitEthernet1/1/0/2
 eth-trunk 20
#
interface XGigabitEthernet1/1/0/10
```



```
mad detect mode direct
#
interface XGigabitEthernet1/2/0/1
port link-type access
port default vlan 1000
#
interface XGigabitEthernet2/1/0/1
eth-trunk 20
#
interface XGigabitEthernet2/1/0/2
eth-trunk 10
#
interface XGigabitEthernet2/1/0/10
mad detect mode direct
#
ospf 1 router-id 1.1.1.1
area 0.0.0.0
network 172.16.70.0 0.0.0.255
network 172.16.80.0 0.0.0.255
network 192.168.11.0 0.0.0.255
#
return
```

AGG-AC1 的配置文件

```
#
sysname AGG-AC1
#
vrrp recover-delay 60
#
vlan batch 20 200
#
dhcp enable
#
dhcp snooping enable
#
interface vlanif 20
ip address 192.168.20.1 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
dhcp select interface
dhcp server excluded-ip-address 192.168.20.2
dhcp server excluded-ip-address 192.168.20.20
```

```
#
interface vlanif 200
 ip address 172.16.200.1 255.255.255.0
#
interface eth-trunk 1
 description connect to AGG1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20
 mode lacp
#
interface 10GE 1/0/1
 eth-trunk 1
#
interface 10GE 1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
 undo port trunk allow-pass vlan 1
#
ospf 1 router-id 3.3.3.3
 area 0.0.0.1
  network 192.168.20.0 0.0.0.255
#
capwap source interface vlanif20
#
hsb-service 0
 service-ip-port local-ip 172.16.200.1 peer-ip 172.16.200.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
 track vrrp vrid 1 interface Vlanif20
 bind-service 0
 hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
 traffic-profile name traff1
  user-isolate l2
 traffic-profile name traff2
  user-isolate l2
 security-profile name sec1
```

```
security-profile name sec2
ssid-profile name ssid1
  ssid test01
ssid-profile name ssid2
  ssid test02
vap-profile name vap1
  forward-mode direct-forward
  service-vlan vlan-id 30
  ssid-profile ssid1
  security-profile sec1
  traffic-profile traff1
  ip source check user-bind enable
  arp anti-attack check user-bind enable
  learn-client-address dhcp-strict
vap-profile name vap2
  forward-mode direct-forward
  service-vlan vlan-id 40
  ssid-profile ssid2
  security-profile sec2
  traffic-profile traff2
  ip source check user-bind enable
  arp anti-attack check user-bind enable
  learn-client-address dhcp-strict
ap-group name ap-group1
  regulatory-domain-profile domain1
radio 0
  vap-profile vap1 wlan 1
  vap-profile vap2 wlan 2
radio 1
  vap-profile vap1 wlan 1
  vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
  ap-name area_1
  ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
  ap-name area_2
  ap-group ap-group1
#
```

AGG-AC2 的配置文件

```
#
sysname AGG-AC2
#
```

```
vrrp recover-delay 60
#
vlan batch 20 200
#
interface vlanif 20
ip address 192.168.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
#
interface vlanif 200
ip address 172.16.200.1 255.255.255.0
#
interface eth-trunk 1
description connect to AGG1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20
mode lacp
#
interface 10GE 1/0/1
eth-trunk 1
#
interface 10GE 1/0/2
port link-type trunk
port trunk allow-pass vlan 200
undo port trunk allow-pass vlan 1
#
hsb-service 0
service-ip-port local-ip 172.16.200.2 peer-ip 172.16.200.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type ap hsb-group 0
#
```

AGG-AC3 的配置文件

```
#
```

```
sysname AGG-AC3
#
vrrp recover-delay 60
#
vlan batch 21 200
#
dhcp enable
#
dhcp snooping enable
#
interface vlanif 21
 ip address 192.168.21.1 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.21.3
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 1200
 dhcp select interface
 dhcp server excluded-ip-address 192.168.21.2
 dhcp server excluded-ip-address 192.168.21.20
#
interface vlanif 201
 ip address 172.16.201.1 255.255.255.0
#
interface eth-trunk 1
 description connect to AGG2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 21
 mode lacp
#
interface 10GE 1/0/1
 eth-trunk 1
#
interface 10GE 1/0/2
 port link-type trunk
 port trunk allow-pass vlan 201
 undo port trunk allow-pass vlan 1
#
ospf 1 router-id 4.4.4.4
 area 0.0.0.2
  network 192.168.21.0 0.0.0.255
#
capwap source interface vlanif21
#
```

```
hsb-service 0
service-ip-port local-ip 172.16.201.1 peer-ip 172.16.201.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif21
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff1
user-isolate l2
traffic-profile name traff2
user-isolate l2
security-profile name sec1
security-profile name sec2
ssid-profile name ssid3
ssid test03
ssid-profile name ssid4
ssid test04
vap-profile name vap1
forward-mode direct-forward
service-vlan vlan-id 40
ssid-profile ssid3
security-profile sec1
traffic-profile traff1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name vap2
forward-mode direct-forward
service-vlan vlan-id 41
ssid-profile ssid2
security-profile sec2
traffic-profile traff2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
ap-group name ap-group1
regulatory-domain-profile domain1
```

```
radio 0
 vap-profile vap1 wlan 1
 vap-profile vap2 wlan 2
radio 1
 vap-profile vap1 wlan 1
 vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
 ap-name area_1
 ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
 ap-name area_2
 ap-group ap-group1
#
```

AGG-AC4 的配置文件

```
#
sysname AGG-AC4
#
vrrp recover-delay 60
#
vlan batch 21 200
#
interface vlanif 21
 ip address 192.168.21.2 255.255.255.0
 vrrp vrid 1 virtual-ip 192.168.21.3
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt-mode timer delay 1200
#
interface vlanif 201
 ip address 172.16.201.1 255.255.255.0
#
interface eth-trunk 1
 description connect to AGG2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 21
 mode lacp
#
interface 10GE 1/0/1
 eth-trunk 1
#
interface 10GE 1/0/2
 port link-type trunk
```

```
port trunk allow-pass vlan 200
undo port trunk allow-pass vlan 1
#
hsb-service 0
service-ip-port local-ip 172.16.201.2 peer-ip 172.16.201.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif21
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type ap hsb-group 0
#
```

AGG1 的配置文件

```
#
sysname AGG1
#
vlan batch 20 30 to 31 50 70
#
dhcp enable
#
dhcp snooping enable
#
vlan 30
dhcp snooping enable
vlan 31
dhcp snooping enable
vlan 50
dhcp snooping enable
#
interface Vlanif20
ip address 192.168.20.20 255.255.255.0
#
interface Vlanif30
ip address 172.16.30.1 255.255.255.0
arp proxy intra-vlan enable
dhcp select interface
dhcp server dns-list 192.168.11.1
#
interface Vlanif31
```



```
ip address 172.16.31.1 255.255.255.0
arp proxy intra-vlan enable
dhcp select interface
dhcp server dns-list 192.168.11.1
#
interface Vlanif50
ip address 172.16.50.1 255.255.255.0
arp proxy intra-vlan enable
dhcp select interface
dhcp server dns-list 192.168.11.1
#
interface Vlanif70
ip address 172.16.70.2 255.255.255.0
#
interface Eth-Trunk1
description con to AC
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20
mode lacp-static
#
interface Eth-Trunk10
description con to CORE
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 70
mode lacp-static
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 to 31 50
mode lacp-static
port-isolate enable group 1
#
interface 10GE 1/0/3
eth-trunk 30
#
interface 10GE 1/0/4
eth-trunk 1
#
interface 10GE 1/0/5
eth-trunk 1
```

```
#
interface 10GE 2/0/3
 eth-trunk 30
#
interface 10GE 1/0/1
 eth-trunk 10
#
interface 10GE 2/0/1
 eth-trunk 10
#
return
```

AGG2 的配置文件

```
#
sysname AGG2
#
vlan batch 21 40 to 41 60 80
#
dhcp enable
#
dhcp snooping enable
#
vlan 40
 dhcp snooping enable
vlan 41
 dhcp snooping enable
vlan 60
 dhcp snooping enable
#
interface Vlanif21
 ip address 192.168.21.20 255.255.255.0
#
interface Vlanif40
 ip address 172.16.40.1 255.255.255.0
 arp proxy intra-vlan enable
 dhcp select interface
 dhcp server dns-list 192.168.11.1
#
interface Vlanif41
 ip address 172.16.41.1 255.255.255.0
 arp proxy intra-vlan enable
 dhcp select interface
 dhcp server dns-list 192.168.11.1
```

```
#
interface Vlanif60
ip address 172.16.60.1 255.255.255.0
arp proxy intra-vlan enable
dhcp select interface
dhcp server dns-list 192.168.11.1
#
interface Vlanif80
ip address 172.16.80.2 255.255.255.0
#
interface Eth-Trunk1
description con to AC
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21
mode lacp-static
#
interface Eth-Trunk10
description con to CORE
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 80
mode lacp-static
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 40 to 41 60
mode lacp-static
port-isolate enable group 1
#
interface 10GE 1/0/3
eth-trunk 40
#
interface 10GE 1/0/4
eth-trunk 2
#
interface 10GE 1/0/5
eth-trunk 2
#
interface 10GE 2/0/3
eth-trunk 40
#
```

```
interface 10GE 1/0/1
 eth-trunk 20
#
interface 10GE 2/0/1
 eth-trunk 20
#
return
```

ACC1 的配置文件

```
#
sysname ACC1
#
vlan batch 20 50
#
interface Eth-Trunk30
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20 50
 mode lacp-static
#
interface 10GE1/0/1
 eth-trunk 30
#
interface 10GE1/0/2
 eth-trunk 30
#
interface GE1/0/3
 port link-type access
 port default vlan 50
 stp edged-port enable
 port-isolate enable group 1
#
interface GE1/0/4
 port link-type access
 port default vlan 20
 stp edged-port enable
 port-isolate enable group 1
#
return
```

ACC2 的配置文件

```
#
sysname ACC2
#
```

```
vlan batch 21 60
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 60
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 40
#
interface 10GE1/0/2
eth-trunk 40
#
interface GE1/0/3
port link-type access
port default vlan 60
stp edged-port enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type access
port default vlan 21
stp edged-port enable
port-isolate enable group 1
#
return
```

1.1.2.1.6 独立 AC 方案：核心交换机做有线用户网关，AC 做无线用户网关

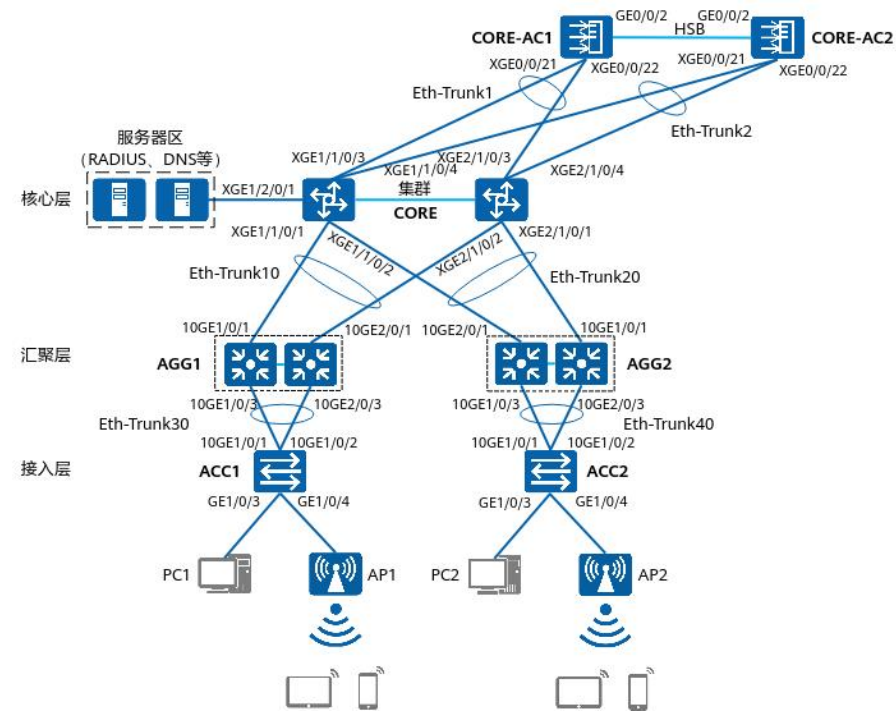
案例描述

核心层交换机组建集群，作为整个园区网络的核心，实现网络高可靠性和网络大数据量转发。独立 AC 旁挂式部署，作为网关为 AP 和无线用户分配 IP 地址，统一管理全网 AP 和无线用户上线。

汇聚层交换机组建堆叠，实现设备级备份的同时，也扩展了设备的端口密度和转发带宽。

本案例中，核心交换机作为全网有线用户的网关，独立 AC 作为全网无线用户的网关。

图 1 核心交换机做有线用户网关+独立 AC 做无线用户网关



设备要求和版本

位置	设备要求	本案例使用的设备	本案例使用的版本
核心层	–	S12700E	V200R022C10
汇聚层	–	S6730-H-V2	V600R022C10
接入层	–	S5735-L-V2	V600R022C10
AC	–	AC6805	V200R022C10
AP	–	AirEngine 8760-X1-PRO	V200R022C10

部署思路

步骤	部署思路	涉及设备
1	配置交换机集群/堆叠、多主检测功能，配置上下行 Eth-Trunk	核心交换机、汇聚交换机
2	配置交换机、AC 的接口和 VLAN，配置三层接口地址、路由，使得网络互通	核心交换机、汇聚交换机、接入交换机、AC
3	配置核心交换机和 AC 的 DHCP 功能，使交换机和 AC 分别作为 DHCP 服务器为有线、AP/无线用户分配 IP 地址	核心交换机、AC
4	配置 AC 的 VRRP+HSB 方式的备份	AC
5	配置 AC 的无线业务，实现 AP 和 STA 上线	AC

步骤	部署思路	涉及设备
6	配置 VRRP 热备份场景下的无线配置同步	AC

数据规划

表 1 核心交换机业务数据规划

项目	VLAN ID	网段
无线用户的业务 VLAN（AP1）	VLAN 30	172.16.30.0/24
	VLAN 40	172.16.40.0/24
有线用户的业务 VLAN（PC1）	VLAN 50	172.16.50.0/24
有线用户的业务 VLAN（PC2）	VLAN 60	172.16.60.0/24
连接 CORE-AC 的 VLAN	VLAN 20	192.168.20.20/24
连接服务器的 VLAN	VLAN 1000	192.168.11.254/24

表 2 CORE-AC 业务数据规划

项目	VLAN ID	网段
无线 AP 管理 VLAN	VLAN 20	172.16.20.0/24
CORE-AC1 和 CORE-AC2 的互通 VLAN	VLAN 100	172.16.100.0/24
主备 AC HSB 同步 VLAN	VLAN 200	172.16.200.0/24

表 3 CORE-AC 无线业务数据规划

项目	数据
AP 组	ap-group1
域管理模板	domain1
SSID 模板	Employee、Guest
VAP 模板	vap1、vap2、隧道转发方式
CAPWAP 源接口和 IP 地址（CORE-AC1）	VLANIF 20: 192.168.20.1/24
CAPWAP 源接口和 IP 地址（CORE-AC2）	VLANIF 20: 192.168.20.2/24

部署注意事项

不建议使用 VLAN 1 作为业务 VLAN，将各端口从 VLAN1 中退出。根据实际业务需求透传 VLAN，禁止端口透传所有 VLAN。

隧道转发方式下，管理 VLAN 和业务 VLAN 不能配置为同一 VLAN，否则会导致 MAC 漂移，报文转发出错。并且 AP 和 AC 之间只能放通管理 VLAN，不能放通业务 VLAN

隧道转发模式下，AP 的业务报文会封装在 CAPWAP 数据隧道中进行传输，先发送给 AC，然后由 AC 再转发到上层网络，所以只要配置 AC 与 AP 间的网络加入管理 VLAN，AC 与上层网络间的网络加入业务 VLAN，就能正常传输业务报文和管理报文。

对于主备 AC 上关联的同一 AP，其 WLAN 相关的业务配置必须保持一致（如 WMM 模板、射频模板、射频、流量模板、安全模板、安全策略和 WLAN ID 等都需要保持一致），否则当 AC 的主备状态切换后，无法保证用户业务正常。

主备 AC 的型号和软件版本需完全一致。

在 VRRP 热备份场景下部署 DHCP 服务器时需要注意以下几点：

V200R019C00 及之后版本，开启 DHCP 服务器功能的接口无限制，主 AC 分配 IP 地址，备 AC 不分配，主 AC 的 IP 地址分配信息会同步到备 AC。

主备 AC 上配置的 IP 地址池必须完全一致，配置不一致会导致主备 AC 备份失败。

配置命令 `hsb-service-type dhcp hsb-group group-index`，使 DHCP 业务绑定 HSB 备份组。否则主备 AC 上的 IP 地址分配信息无法备份。

部署步骤

1. 配置核心层交换机集群和汇聚层交换机堆叠、多主检测及上下行 Eth-Trunk。

此部分配置请参考 [集群/堆叠通用部署](#)。

2. 配置核心交换机 CORE 的接口和 VLAN。

创建 VLAN。

```
[CORE] vlan batch 20 30 40 50 60 1000
```

配置和汇聚交换机 AGG1 互连的 Eth-Trunk10。和汇聚交换机 AGG2 互连的配置与此类似，此处不再赘述。

```
[CORE] interface eth-trunk 10
[Core-Eth-Trunk10] description con to AGG1
[Core-Eth-Trunk10] mode lacp
[Core-Eth-Trunk10] port link-type trunk
[Core-Eth-Trunk10] undo port trunk allow-pass vlan 1
[Core-Eth-Trunk10] port trunk allow-pass vlan 20 50
[Core-Eth-Trunk10] quit
```

创建和 CORE-AC1 互连的 Eth-Trunk1 并将接口加入 Eth-Trunk。和 CORE-AC2 互连的配置与此类似，此处不再赘述。


```
[CORE] interface eth-trunk 1
[Core-Eth-Trunk1] description con to CORE-AC1
[Core-Eth-Trunk1] mode lacp
[Core-Eth-Trunk1] port link-type trunk
[Core-Eth-Trunk1] undo port trunk allow-pass vlan 1
[Core-Eth-Trunk1] port trunk allow-pass vlan 20 30 40
[Core-Eth-Trunk1] quit
[Core] interface xgigabitethernet 1/1/0/3
[Core-XGigabitEthernet1/1/0/3] eth-trunk 1
[Core-XGigabitEthernet1/1/0/3] quit
[Core] interface xgigabitethernet 2/1/0/3
[Core-XGigabitEthernet2/1/0/3] eth-trunk 1
[Core-XGigabitEthernet2/1/0/3] quit
```

将和 iMaster NCE-Campus 对接的接口加入 VLAN1000。

```
[CORE] interface xgigabitethernet 1/2/0/1
[Core-XGigabitEthernet1/2/0/1] port link-type access
[Core-XGigabitEthernet1/2/0/1] port default vlan 1000
[Core-XGigabitEthernet1/2/0/1] quit
```

3. 配置汇聚交换机 AGG1 的接口和 VLAN。汇聚交换机 AGG2 的配置与此类似，不再赘述。

创建 VLAN。

```
[AGG1] vlan batch 20 50
```

配置与核心交换机 CORE 连接的 Eth-Trunk。

```
[AGG1] interface eth-trunk 10
[AGG1-Eth-Trunk10] description connect to CORE
[AGG1-Eth-Trunk10] mode lacp-static
[AGG1-Eth-Trunk10] port link-type trunk
[AGG1-Eth-Trunk10] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk10] port trunk allow-pass vlan 20 50
[AGG1-Eth-Trunk10] quit
[AGG1] interface 10ge 1/0/1
[AGG1-10GE1/0/1] eth-trunk 10
[AGG1-10GE1/0/1] quit
[AGG1] interface 10ge 2/0/1
[AGG1-10GE2/0/1] eth-trunk 10
[AGG1-10GE2/0/1] quit
```

配置与接入交换机 ACC1 连接的下行接口。

```
[AGG1] interface eth-trunk 30
[AGG1-Eth-Trunk30] mode lacp-static
[AGG1-Eth-Trunk30] port link-type trunk
[AGG1-Eth-Trunk30] undo port trunk allow-pass vlan 1
```

```
[AGG1-Eth-Trunk30] port trunk allow-pass vlan 20 50
[AGG1-Eth-Trunk30] port-isolate enable group 1
[AGG1-Eth-Trunk30] quit
[AGG1] interface 10ge 1/0/3
[AGG1-10GE1/0/3] eth-trunk 30
[AGG1-10GE1/0/3] quit
[AGG1] interface 10ge 2/0/3
[AGG1-10GE2/0/3] eth-trunk 30
[AGG1-10GE2/0/3] quit
```

4. 配置接入交换机 ACC1 的接口和 VLAN。接入交换机 ACC2 的配置与此类似，不再赘述。

创建 VLAN。

```
[ACC1] vlan batch 20 50
```

配置与汇聚交换机 AGG1 连接的上行接口。

```
[ACC1] interface eth-trunk 30
[ACC1-Eth-Trunk30] mode lacp-static
[ACC1-Eth-Trunk30] port link-type trunk
[ACC1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[ACC1-Eth-Trunk30] port trunk allow-pass vlan 20 50
[ACC1-Eth-Trunk30] quit
[ACC1] interface 10ge 1/0/1
[ACC1-10GE1/0/1] eth-trunk 30
[ACC1-10GE1/0/1] quit
[ACC1] interface 10ge 1/0/2
[ACC1-10GE1/0/2] eth-trunk 30
[ACC1-10GE1/0/2] quit
```

配置与用户 PC1 和 AP1 连接的下行接口，并将连接 PC1 和 AP1 的端口配置为边缘端口。

```
[ACC1] interface ge 1/0/3
[ACC1-GE1/0/3] port link-type access
[ACC1-GE1/0/3] port default vlan 50
[ACC1-GE1/0/3] port-isolate enable group 1
[ACC1-GE1/0/3] stp edged-port enable
[ACC1-GE1/0/3] quit
[ACC1] interface ge 1/0/4
[ACC1-GE1/0/4] port link-type access
[ACC1-GE1/0/4] port default vlan 20
[ACC1-GE1/0/4] port-isolate enable group 1
[ACC1-GE1/0/4] stp edged-port enable
[ACC1-GE1/0/4] quit
```

5. 配置 CORE-AC1 的接口和 VLAN。CORE-AC2 的配置与此类似，不再赘述。

配置与核心交换机连接的接口。

```
<AC6805> system-view
[AC6805] sysname CORE-AC1
[CORE-AC1] vlan batch 20 30 40 100
[CORE-AC1] interface eth-trunk 1
[CORE-AC1-Eth-Trunk1] mode lacp
[CORE-AC1-Eth-Trunk1] port link-type trunk
[CORE-AC1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[CORE-AC1-Eth-Trunk1] port trunk allow-pass vlan 20 30 40
[CORE-AC1-Eth-Trunk1] quit
[CORE-AC1] interface xgigabitethernet 0/0/21
[CORE-AC1-XGigabitEthernet0/0/21] eth-trunk 1
[CORE-AC1-XGigabitEthernet0/0/21] quit
[CORE-AC1] interface xgigabitethernet 0/0/22
[CORE-AC1-XGigabitEthernet0/0/22] eth-trunk 1
[CORE-AC1-XGigabitEthernet0/0/22] quit
```

配置 CORE-AC1 连接 CORE-AC2 的接口。

```
[CORE-AC1] interface gigabitethernet 0/0/2
[CORE-AC1-GigabitEthernet0/0/2] port link-type trunk
[CORE-AC1-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[CORE-AC1-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[CORE-AC1-GigabitEthernet0/0/2] quit
[CORE-AC1] interface vlanif 100
[CORE-AC1-Vlanif100] ip address 172.16.100.1 255.255.255.0
[CORE-AC1-Vlanif100] quit
```

6. 配置核心交换机的 DHCP 功能，使交换机作为 DHCP 服务器为有线用户分配 IP 地址。

使能全局 DHCP，并配置业务 VLAN 的 DHCP Snooping 功能。

```
[CORE] dhcp enable
[CORE] dhcp snooping enable
[CORE] vlan 50
[CORE-vlan50] dhcp snooping enable
[CORE-vlan50] quit
[CORE] vlan 60
[CORE-vlan60] dhcp snooping enable
[CORE-vlan60] quit
```

创建有线业务三层接口 VLANIF50、VLANIF60 并配置通过接口地址池为有线终端分配地址。

```
[CORE] interface vlanif 50
[CORE-Vlanif50] ip address 172.16.50.1 255.255.255.0
[CORE-Vlanif50] dhcp select interface
[CORE-Vlanif50] dhcp server dns-list 192.168.100.2 //配置终端的 DNS 服务器
[CORE-Vlanif50] arp-proxy inner-sub-vlan-proxy enable //启动有线用户 VLAN 内 Proxy ARP 功能，否则
有线用户之间的流量无法互访。请根据实际需求判断是否需要配置该命令
```

```
[CORE-Vlanif50] quit
[CORE] interface vlanif 60
[CORE-Vlanif60] ip address 172.16.60.1 255.255.255.0
[CORE-Vlanif60] dhcp select interface
[CORE-Vlanif60] dhcp server dns-list 192.168.100.2 //配置终端的 DNS 服务器
[CORE-Vlanif60] arp-proxy inner-sub-vlan-proxy enable //启动有线用户 VLAN 内 Proxy ARP 功能，否则
有线用户之间的流量无法互访。请根据实际需求判断是否需要配置该命令
[CORE-Vlanif60] quit
```

创建连接 AC 的三层接口。

```
[CORE] interface vlanif 20
[CORE-Vlanif20] ip address 192.168.20.20 255.255.255.0
[CORE-Vlanif20] quit
[CORE] interface vlanif 30
[CORE-Vlanif30] ip address 172.16.30.3 255.255.255.0
[CORE-Vlanif30] quit
[CORE] interface vlanif 40
[CORE-Vlanif40] ip address 172.16.40.3 255.255.255.0
[CORE-Vlanif40] quit
```

创建连接服务器的三层接口 VLANIF1000。

```
[CORE] interface vlanif 1000
[CORE-Vlanif1000] ip address 192.168.100.1 255.255.255.0
[CORE-Vlanif1000] quit
```

7. 配置 CORE-AC1 的 DHCP 功能，使 AC 作为 DHCP 服务器为 AP 和无线用户分配 IP 地址。
CORE-AC2 的配置与此类似，不再赘述。

使能全局 DHCP，并配置业务 VLAN 的 DHCP Snooping 功能。

```
[CORE-AC1] dhcp enable
[CORE-AC1] dhcp snooping enable
[CORE-AC1] vlan 30
[CORE-AC1-vlan30] dhcp snooping enable
[CORE-AC1-vlan30] quit
[CORE-AC1] vlan 40
[CORE-AC1-vlan40] dhcp snooping enable
[CORE-AC1-vlan40] quit
```

创建无线管理接口 VLANIF20 并通过接口地址池为 AP 分配地址。

```
[CORE-AC1] interface vlanif 20
[CORE-AC1-Vlanif20] dhcp select interface
[CORE-AC1-Vlanif20] ip address 192.168.20.1 255.255.255.0
[CORE-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.2
[CORE-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.20
[CORE-AC1-Vlanif20] quit
```

创建有线业务三层接口 VLANIF30、VLANIF40 并配置通过接口地址池为无线终端分配地址。

```
[CORE-AC1] interface vlanif 30
[CORE-AC1-Vlanif30] ip address 172.16.30.1 255.255.255.0
[CORE-AC1-Vlanif30] dhcp select interface
[CORE-AC1-Vlanif30] dhcp server excluded-ip-address 172.16.30.2 172.16.30.3
[CORE-AC1-Vlanif30] dhcp server dns-list 192.168.100.2 //配置终端的 DNS 服务器
[CORE-AC1-Vlanif30] arp-proxy inner-sub-vlan-proxy enable //启动无线用户业务 VLAN 内 Proxy ARP 功能，否则无线用户之间的流量通过 AC 无法完成互访。请根据实际需求判断是否需要配置该命令
[CORE-AC1-Vlanif30] quit
[CORE-AC1] interface vlanif 40
[CORE-AC1-Vlanif40] ip address 172.16.40.1 255.255.255.0
[CORE-AC1-Vlanif40] dhcp select interface
[CORE-AC1-Vlanif40] dhcp server excluded-ip-address 172.16.40.2 172.16.40.3
[CORE-AC1-Vlanif40] dhcp server dns-list 192.168.100.2 //配置终端的 DNS 服务器
[CORE-AC1-Vlanif40] arp-proxy inner-sub-vlan-proxy enable //启动无线用户业务 VLAN 内 Proxy ARP 功能，否则无线用户之间的流量通过 AC 无法完成互访。请根据实际需求判断是否需要配置该命令
[CORE-AC1-Vlanif40] quit
```

8. 配置 CORE-AC1 的缺省路由。CORE-AC2 的配置与此类似，不再赘述。

```
[CORE-AC1] ip route-static 0.0.0.0 0.0.0.0 192.168.20.20
```

9. 配置 CORE-AC1 的 VRRP+HSB 方式的备份。CORE-AC2 的配置与此类似，不再赘述。

配置 VRRP 备份组的状态恢复延迟时间为 60 秒。

```
[CORE-AC1] vrrp recover-delay 60
```

在 CORE-AC1 上创建管理 VRRP 备份组，配置 CORE-AC1 在该备份组中的优先级为 120，并配置抢占时间为 1200 秒。

```
[CORE-AC1] interface vlanif 20
[CORE-AC1-Vlanif20] vrrp vrid 1 virtual-ip 192.168.20.3
[CORE-AC1-Vlanif20] vrrp vrid 1 priority 120
[CORE-AC1-Vlanif20] vrrp vrid 1 preempt-mode timer delay 1200
[CORE-AC1-Vlanif20] admin-vrrp vrid 1
[CORE-AC1-Vlanif20] quit
```

在 CORE-AC1 上创建 HSB 主备服务 0，并配置其主备通道 IP 地址和端口号。

```
[CORE-AC1] hsb-service 0
[CORE-AC1-hsb-service-0] service-ip-port local-ip 172.16.100.1 peer-ip 172.16.100.2 local-data-port 10241 peer-data-port 10241
[CORE-AC1-hsb-service-0] quit
```

在 CORE-AC1 上创建 HSB 备份组 0，并配置其绑定 HSB 主备服务 0 和管理 VRRP 备份组。

```
[CORE-AC1] hsb-group 0
[CORE-AC1-hsb-group-0] bind-service 0
[CORE-AC1-hsb-group-0] track vrrp vrid 1 interface vlanif 20
```

```
[CORE-AC1-hsb-group-0] quit
```

配置 CORE-AC1 业务绑定 HSB 备份组。

```
[CORE-AC1] hsb-service-type access-user hsb-group 0
```

```
[CORE-AC1] hsb-service-type ap hsb-group 0
```

```
[CORE-AC1] hsb-service-type dhcp hsb-group 0
```

```
[CORE-AC1] hsb-group 0
```

```
[CORE-AC1-hsb-group-0] hsb enable
```

```
[CORE-AC1-hsb-group-0] quit
```

配置完成后，在 CORE-AC1 和 CORE-AC2 上分别执行 **display vrrp** 命令，可以看到 CORE-AC1 的 State 字段的显示为 **Master**，CORE-AC2 的 State 字段的显示为 **Backup**。

```
[CORE-AC1] display vrrp
```

```
Vlanif20 | Virtual Router 1
```

```
State : Master
```

```
Virtual IP : 192.168.20.3
```

```
Master IP : 192.168.20.1
```

```
PriorityRun : 120
```

```
PriorityConfig : 120
```

```
MasterPriority : 120
```

```
Preempt : YES Delay Time : 1200s
```

```
TimerRun : 2s
```

```
TimerConfig : 2s
```

```
Auth type : NONE
```

```
Virtual MAC : 0000-5e00-0101
```

```
Check TTL : YES
```

```
Config type : admin-vrrp
```

```
Backup-forward : disabled
```

```
Track SysHealth Priority reduced : 254
```

```
SysHealth state : UP
```

```
Create time : 2019-11-05 15:30:25
```

```
Last change time : 2019-11-05 15:30:31
```

```
[CORE-AC2] display vrrp
```

```
Vlanif20 | Virtual Router 1
```

```
State : Backup
```

```
Virtual IP : 192.168.20.3
```

```
Master IP : 192.168.20.1
```

```
PriorityRun : 100
```

```
PriorityConfig : 100
```

```
MasterPriority : 120
```

```
Preempt : YES Delay Time : 0s
```

```
TimerRun : 2s
```

```
TimerConfig : 2s
```

```
Auth type : NONE
```

```

Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : admin-vrrp
Backup-forward : disabled
Track SysHealth Priority reduced : 254
SysHealth state : UP
Create time : 2019-11-05 11:12:13
Last change time : 2019-11-05 11:13:23

```

在 CORE-AC1 和 CORE-AC2 上查看主备服务的建立情况。可以看到 **Service State** 字段的显示为 **Connected**，说明主备服务通道已经成功建立。

```
[CORE-AC1] display hsb-service 0
```

```
Hot Standby Service Information:
```

```

-----
Local IP Address   : 172.16.100.1
Peer IP Address    : 172.16.100.2
Source Port        : 10241
Destination Port    : 10241
Keep Alive Times    : 5
Keep Alive Interval : 3
Service State      : Connected
Service Batch Modules :
Shared-key          : -

```

```
[CORE-AC2] display hsb-service 0
```

```
Hot Standby Service Information:
```

```

-----
Local IP Address   : 172.16.100.2
Peer IP Address    : 172.16.100.1
Source Port        : 10241
Destination Port    : 10241
Keep Alive Times    : 5
Keep Alive Interval : 3
Service State      : Connected
Service Batch Modules :
Shared-key          : -

```

在 CORE-AC1 和 CORE-AC2 上执行 **display hsb-group 0** 命令，查看 HSB 备份组的运行情况。

```
[CORE-AC1] display hsb-group 0
```

```
Hot Standby Group Information:
```

```

-----
HSB-group ID       : 0

```

```

Vrrp Group ID      : 1
Vrrp Interface     : Vlanif20
Service Index      : 0
Group Vrrp Status   : Master
Group Status        : Active
Group Backup Process : Realtime
Peer Group Device Name : AC6805
Peer Group Software Version : V200R022C10
Group Backup Modules : Access-user
                    AP
                    DHCP

```

[CORE-AC2] **display hsb-group 0**

Hot Standby Group Information:

```

HSB-group ID       : 0
Vrrp Group ID      : 1
Vrrp Interface     : Vlanif20
Service Index      : 0
Group Vrrp Status   : Backup
Group Status        : Inactive
Group Backup Process : Realtime
Peer Group Device Name : AC6805
Peer Group Software Version : V200R022C10
Group Backup Modules : Access-user
                    DHCP
                    AP

```

10. 在 CORE-AC1 上配置 AP 上线。

配置 AC 的源接口。

```
[CORE-AC1] capwap source interface vlanif 20 //VLAN20 是无线 AP 的管理 VLAN
```

创建 AP 组，用于将相同配置的 AP 都加入到同一 AP 组中。

```

[CORE-AC1] wlan
[CORE-AC1-wlan-view] ap-group name ap-group1
[CORE-AC1-wlan-ap-group-ap-group1] quit

```

创建域管理模板，在域管理模板下配置 AC 的国家码并在 AP 组下引用域管理模板。

```

[CORE-AC1-wlan-view] regulatory-domain-profile name domain1
[CORE-AC1-wlan-regulate-domain-domain1] country-code cn
[CORE-AC1-wlan-regulate-domain-domain1] quit
[CORE-AC1-wlan-view] ap-group name ap-group1
[CORE-AC1-wlan-ap-group-ap-group1] regulatory-domain-profile domain1

```


Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y

[CORE-AC1-wlan-ap-group-ap-group1] quit

将目标 AP 加入 AP 组，并根据 AP 的部署位置为 AP 配置名称。

[CORE-AC1-wlan-view] ap auth-mode mac-auth

[CORE-AC1-wlan-view] ap-id 1 ap-mac 00e0-fc12-6660

[CORE-AC1-wlan-ap-1] ap-name area_1

[CORE-AC1-wlan-ap-1] ap-group ap-group1

Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, whether to continue? [Y/N]:y

Info: This operation may take a few seconds. Please wait for a moment.. done.

[CORE-AC1-wlan-ap-1] quit

[CORE-AC1-wlan-view] ap-id 2 ap-mac 00e0-fc12-6670

[CORE-AC1-wlan-ap-2] ap-name area_2

[CORE-AC1-wlan-ap-2] ap-group ap-group1

Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, whether to continue? [Y/N]:y

Info: This operation may take a few seconds. Please wait for a moment.. done.

[CORE-AC1-wlan-ap-2] quit

[CORE-AC1-wlan-view] quit

将 AP 上电后，可以查看到 AP 的“State”字段为“nor”。

[CORE-AC1] display ap all

Total AP information:

nor : normal [2]

ExtraInfo : Extra information

P : insufficient power supply

```

-----
ID   MAC       Name  Group  IP        Type           State STA Uptime ExtraInfo
-----
1    00e0-fc12-6660 area_1 ap-group1 192.168.20.41 AirEngine 8760-X1-PRO   nor  0 5M:26S -
2    00e0-fc12-6670 area_2 ap-group1 192.168.20.164 AirEngine 8760-X1-PRO   nor  0 2M:52S -
-----

```

11. 在 CORE-AC1 上配置 STA 上线。

配置 WLAN 业务参数。

[CORE-AC1] wlan

[CORE-AC1-wlan-view] security-profile name sec1

[CORE-AC1-wlan-sec-prof-sec1] security open

[CORE-AC1-wlan-sec-prof-sec1] quit

```
[CORE-AC1-wlan-view] ssid-profile name ssid1
[CORE-AC1-wlan-ssid-prof-ssid1] ssid Employee
[CORE-AC1-wlan-ssid-prof-ssid1] quit
[CORE-AC1-wlan-view] traffic-profile name traff
[CORE-AC1-wlan-traffic-prof-traff] user-isolate l2
[CORE-AC1-wlan-traffic-prof-traff] quit
[CORE-AC1-wlan-view] security-profile name sec2
[CORE-AC1-wlan-sec-prof-sec2] security open
[CORE-AC1-wlan-sec-prof-sec2] quit
[CORE-AC1-wlan-view] ssid-profile name ssid2
[CORE-AC1-wlan-ssid-prof-ssid2] ssid Guest
[CORE-AC1-wlan-ssid-prof-ssid2] quit
```

配置 WLAN-VAP 模板，配置业务数据转发模式、业务 VLAN，并应用安全模板和 SSID 模板，使能 STA 地址严格 DHCP 获取功能、IPSG 功能动态 ARP 检测功能。

```
[CORE-AC1-wlan-view] vap-profile name vap1
[CORE-AC1-wlan-vap-prof-vap1] forward-mode tunnel
[CORE-AC1-wlan-vap-prof-vap1] service-vlan vlan-id 30
[CORE-AC1-wlan-vap-prof-vap1] security-profile sec1
[CORE-AC1-wlan-vap-prof-vap1] ssid-profile ssid1
[CORE-AC1-wlan-vap-prof-vap1] traffic-profile traff
[CORE-AC1-wlan-vap-prof-vap1] ip source check user-bind enable
[CORE-AC1-wlan-vap-prof-vap1] arp anti-attack check user-bind enable
[CORE-AC1-wlan-vap-prof-vap1] learn-client-address dhcp-strict
[CORE-AC1-wlan-vap-prof-vap1] quit
[CORE-AC1-wlan-view] vap-profile name vap2
[CORE-AC1-wlan-vap-prof-vap2] forward-mode tunnel
[CORE-AC1-wlan-vap-prof-vap2] service-vlan vlan-id 40
[CORE-AC1-wlan-vap-prof-vap2] security-profile sec2
[CORE-AC1-wlan-vap-prof-vap2] ssid-profile ssid2
[CORE-AC1-wlan-vap-prof-vap2] traffic-profile traff
[CORE-AC1-wlan-vap-prof-vap2] ip source check user-bind enable
[CORE-AC1-wlan-vap-prof-vap2] arp anti-attack check user-bind enable
[CORE-AC1-wlan-vap-prof-vap2] learn-client-address dhcp-strict
[CORE-AC1-wlan-vap-prof-vap2] quit
```

说明

由于 **ip source check user-bind enable** 命令是基于绑定表进行匹配检查的，因此

对于 DHCP 用户，需要使能 DHCP Snooping 自动生成动态绑定表。

对于静态配置 IP 的用户，需要手工配置静态绑定表。

learn-client-address dhcp-strict 命令的前置条件为：

在 VAP 模板视图下执行命令 **undo dhcp trust port** 去使能 AP 的 DHCP 信任功能。

在 VAP 模板视图下执行命令 `undo learn-client-address { ipv4 | ipv6 } disable` 使能 STA 地址学习功能。

配置 AP 组引用 VAP 模板。

```
[CORE-AC1-wlan-view] ap-group name ap-group1
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 0
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 0
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 1
[CORE-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 1
[CORE-AC1-wlan-ap-group-ap-group2] quit
[CORE-AC1-wlan-view] quit
```

12. 配置 VRRP 热备份场景下的无线配置同步，将 CORE-AC1 的无线业务配置信息同步到 CORE-AC2。

配置 CORE-AC2 的源接口。

```
[CORE-AC2] capwap source interface vlanif 20
```

配置 CORE-AC1 上的无线配置同步功能。

```
[CORE-AC1] wlan
[CORE-AC1-wlan-view] master controller
[CORE-AC1-master-controller] master-redundancy peer-ip ip-address 172.16.100.2 local-ip ip-address 172.16.100.1 psk YsHsjx_202206
[CORE-AC1-master-controller] master-redundancy track-vrrp vrid 1 interface vlanif 20
[CORE-AC1-master-controller] quit
[CORE-AC1-wlan-view] quit
```

配置 CORE-AC2 上的无线配置同步功能。

```
[CORE-AC2] wlan
[CORE-AC2-wlan-view] master controller
[CORE-AC2-master-controller] master-redundancy peer-ip ip-address 172.16.100.1 local-ip ip-address 172.16.100.2 psk YsHsjx_202206
[CORE-AC2-master-controller] master-redundancy track-vrrp vrid 1 interface vlanif 20
[CORE-AC2-master-controller] quit
[CORE-AC2-wlan-view] quit
```

执行命令 `display sync-configuration status` 查看无线配置同步状态信息，Status 为 `cfg-mismatch`。需要在 Master AC 上手动触发无线配置同步到 Backup AC 上。等待 Backup AC 自动重启完成。

```
[CORE-AC1] display sync-configuration status
Controller role:Master/Backup/Local
```


Controller IP	Role	Device	Type	Version	Status	Last synced


```
172.16.100.2 Backup AirEngine 8760-X1-PRO V200R022C10 cfg-mismatch(config check fail) -
```

```
Total: 1
```

```
[CORE-AC1] synchronize-configuration
```

```
Warning: This operation may reset the remote AC, synchronize configurations to it, and save all its configurations. Whether to continue? [Y/N]:y
```

说明

手动触发无线配置同步后，Backup 会自动重启，等待 Backup AC 自动重启完成之后，再使用 **display sync-configuration status** 命令检查同步功能是否正常。

检查同步功能是否正常，如果状态为 **up**，表示无线配置同步功能正常。

```
[CORE-AC1] display sync-configuration status
```

```
Controller role:Master/Backup/Local
```

```
-----
Controller IP Role Device Type Version Status Last synced
-----
172.16.100.2 Backup AirEngine 8760-X1-PRO V200R022C10 up 2019-11-05/19:09:14
-----
```

```
Total: 1
```

结果验证

预期结果

有线用户、无线用户均可正常接入园区网络。

验证方法

在 AC 上查看 AP 均已成功获取到 IP 地址。

```
[CORE-AC1] display ip pool interface vlanif20 used
```

```
Pool-name : vlanif20
```

```
Pool-No : 0
```

```
Lease : 1 Days 0 Hours 0 Minutes
```

```
Domain-name : -
```

```
DNS-server0 : -
```

```
NBNS-server0 : -
```

```
Netbios-type : -
```

```
Position : Interface
```

```
Status : Unlocked
```

```
Gateway-0      : -
Network        : 192.168.20.0
Mask           : 255.255.255.0
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total    :254    Used      :2
                  Idle      :233    Expired    :0
                  Conflict   :0      Disabled   :19

-----

Network section
  Start      End      Total  Used Idle(Expired) Conflict Disabled
-----
192.168.20.1 192.168.20.254 254    2    233(0)    0    19
-----

Client-ID format as follows:
DHCP  : mac-address          PPPoE  : mac-address
IPSec : user-id/portnumber/vrf  PPP   : interface index
L2TP  : cpu-slot/session-id    SSL-VPN : user-id/session-id
-----

Index      IP      Client-ID  Type    Left  Status
-----
40  192.168.20.41    00e0-fc12-6660  DHCP    72528  Used
163 192.168.20.164    00e0-fc12-6670  DHCP    72813  Used
-----
```

在核心交换机上查看有线用户均已成功获取到 IP 地址。

```
[CORE] display ip pool interface vlanif50 used
Pool-name      : Vlanif50
Pool-No        : 2
Lease          : 1 Days 0 Hours 0 Minutes
Domain-name    : -
DNS-server0    : 192.168.100.2
NBNS-server0   : -
Netbios-type   : -
Position       : Interface
Status         : Unlocked
```

```
Gateway-0      : -
Network        : 172.16.50.0
Mask           : 255.255.255.0
VPN instance   : --
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total    :254    Used      :1
                  Idle      :253    Expired    :0
                  Conflict   :0      Disabled   :0

-----

Network section
  Start      End      Total  Used Idle(Expired) Conflict Disabled
-----
172.16.50.1 172.16.50.254 254   1   253(0)   0   0

-----

Client-ID format as follows:
DHCP : mac-address          PPPoE : mac-address
IPSec : user-id/portnumber/vrf  PPP  : interface index
L2TP  : cpu-slot/session-id    SSL-VPN : user-id/session-id

-----

Index      IP      Client-ID  Type    Left  Status
-----
109 172.16.50.110    00e0-fc12-3344  DHCP    84875  Used

-----

[CORE] display ip pool interface vlanif60 used
Pool-name   : Vlanif60
Pool-No     : 3
Lease       : 1 Days 0 Hours 0 Minutes
Domain-name : -
DNS-server0 : 192.168.100.2
NBNS-server0 : -
Netbios-type : -
Position    : Interface
Status      : Unlocked
```

```

Gateway-0      : -
Network        : 172.16.60.0
Mask           : 255.255.255.0
VPN instance   : --
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :254   Used    :1
                  Idle     :253   Expired  :0
                  Conflict  :0     Disabled :0

```

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled

172.16.60.1	172.16.60.254	254	1	253(0)	0	0

Client-ID format as follows:

```

DHCP : mac-address          PPPoE : mac-address
IPSec : user-id/portnumber/vrf  PPP  : interface index
L2TP  : cpu-slot/session-id    SSL-VPN : user-id/session-id

```

Index	IP	Client-ID	Type	Left	Status
236	172.16.60.237	00e0-fc12-3377	DHCP	84434	Used

有线、无线用户可以实现互访。

在 AP1 上可以 Ping 通服务器区设备。

```
<area_1> ping 192.168.100.2
```

```
PING 192.168.100.1: 56 data bytes, press CTRL_C to break
```

```
Reply from 192.168.100.2: bytes=56 Sequence=1 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=2 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=3 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=4 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=5 ttl=63 time=1 ms
```

```

--- 192.168.100.2 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
round-trip min/avg/max = 1/1/1 ms

```

AP1 下有无线用户接入后，在 CORE-AC1 上可以查看到接入的无线用户信息。

```
[CORE-AC1] display station ssid Employee
```

```
Rf/WLAN: Radio ID/WLAN ID
```

```
Rx/Tx: link receive rate/link transmit rate(Mbps)
```

```

-----
STA MAC      AP ID Ap name Rf/WLAN Band Type Rx/Tx  RSSI VLAN IP address
-----

```

```

00e0-fc12-3388 1 area_1 1/1 5G 11ac 173/115 -38 30 172.16.30.180
-----

```

```
Total: 1 2.4G: 0 5G: 1
```

在 PC1 上可以 Ping 通连接 AP1 的无线用户。

```
C:\Users>ping 172.16.30.180
```

```
Pinging 172.16.30.180 with 32 bytes of data:
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 172.16.30.180:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

配置文件

CORE 的配置文件

```

#
sysname CORE
#
vlan batch 20 30 40 50 60 1000
#

```



```
dhcp enable
#
dhcp snooping enable
#
vlan 50
    dhcp snooping enable
vlan 60
    dhcp snooping enable
#
interface Vlanif20
    ip address 192.168.20.20 255.255.255.0
#
interface Vlanif30
    ip address 172.16.30.3 255.255.255.0
#
interface Vlanif40
    ip address 172.16.40.3 255.255.255.0
#
interface Vlanif50
    ip address 172.16.50.1 255.255.255.0
    arp-proxy inner-sub-vlan-proxy enable
    dhcp select interface
    dhcp server dns-list 192.168.100.2
#
interface Vlanif60
    ip address 172.16.60.1 255.255.255.0
    arp-proxy inner-sub-vlan-proxy enable
    dhcp select interface
    dhcp server dns-list 192.168.100.2
#
interface Vlanif1000
    ip address 192.168.100.1 255.255.255.0
#
interface Eth-Trunk1
    description con to CORE-AC1
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 20 30 40
    mode lacp
#
interface Eth-Trunk2
    description con to CORE-AC2
    port link-type trunk
```

```
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40
mode lacp
#
interface Eth-Trunk10
description con to AGG1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
mode lacp
#
interface Eth-Trunk20
description con to AGG2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 60
mode lacp
#
interface XGigabitEthernet1/1/0/1
eth-trunk 10
#
interface XGigabitEthernet1/1/0/2
eth-trunk 20
#
interface XGigabitEthernet1/1/0/3
eth-trunk 1
#
interface XGigabitEthernet1/1/0/4
eth-trunk 2
#
interface XGigabitEthernet1/1/0/10
mad detect mode direct
#
interface XGigabitEthernet1/2/0/1
port link-type access
port default vlan 1000
#
interface XGigabitEthernet2/1/0/1
eth-trunk 20
#
interface XGigabitEthernet2/1/0/2
eth-trunk 10
#
```

```
interface XGigabitEthernet2/1/0/3
 eth-trunk 1
#
interface XGigabitEthernet2/1/0/4
 eth-trunk 2
#
interface XGigabitEthernet2/1/0/10
 mad detect mode direct
#
return
```

AGG1 的配置文件

```
#
sysname AGG1
#
vlan batch 20 50
#
interface Eth-Trunk10
 description connect to CORE
 port link-type trunk
 port trunk allow-pass vlan 20 50
 mode lacp-static
#
interface Eth-Trunk30
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20 50
 mode lacp-static
 port-isolate enable group 1
#
interface 10GE1/0/3
 eth-trunk 30
#
interface 10GE2/0/3
 eth-trunk 30
#
interface 10GE1/0/1
 eth-trunk 10
#
interface 10GE2/0/1
 eth-trunk 10
#
return
```

AGG2 的配置文件

```
#
sysname AGG2
#
vlan batch 20 60
#
interface Eth-Trunk20
description connect to CORE
port link-type trunk
port trunk allow-pass vlan 20 60
mode lacp-static
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 60
mode lacp-static
port-isolate enable group 1
#
interface 10GE1/0/3
eth-trunk 40
#
interface 10GE2/0/3
eth-trunk 40
#
interface 10GE1/0/1
eth-trunk 20
#
interface 10GE2/0/1
eth-trunk 20
#
return
```

ACC1 的配置文件

```
#
sysname ACC1
#
vlan batch 20 50
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
```

```
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 30
#
interface 10GE1/0/2
eth-trunk 30
#
interface GE1/0/3
port link-type access
port default vlan 50
stp edged-port enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type access
port default vlan 20
stp edged-port enable
port-isolate enable group 1
#
return
```

ACC2 的配置文件

```
#
sysname ACC2
#
vlan batch 20 60
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 60
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 40
#
interface 10GE1/0/2
eth-trunk 40
#
interface GE1/0/3
port link-type access
port default vlan 60
```

```
stp edged-port enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type access
port default vlan 20
stp edged-port enable
port-isolate enable group 1
#
return
```

CORE-AC1 的配置文件

```
#
sysname CORE-AC1
#
vrp recover-delay 60
#
vlan batch 20 30 40 100
#
dhcp enable
#
dhcp snooping enable
#
vlan 30
dhcp snooping enable
vlan 40
dhcp snooping enable
#
interface Vlanif20
ip address 192.168.20.1 255.255.255.0
vrp vrid 1 virtual-ip 192.168.20.3
admin-vrrp vrid 1
vrp vrid 1 priority 120
vrp vrid 1 preempt-mode timer delay 1200
dhcp select interface
dhcp server excluded-ip-address 192.168.20.2
dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif30
ip address 172.16.30.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.30.2 172.16.30.3
```

```
dhcp server dns-list 192.168.100.2
#
interface Vlanif40
ip address 172.16.40.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.40.2 172.16.40.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif100
ip address 172.16.100.1 255.255.255.0
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40
mode lacp
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/21
eth-trunk 1
#
interface XGigabitEthernet0/0/22
eth-trunk 1
#
ip route-static 0.0.0.0 0.0.0.0 192.168.20.20
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.100.1 peer-ip 172.16.100.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
```

```
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
  user-isolate l2
security-profile name sec1
  security open
security-profile name sec2
  security open
ssid-profile name ssid1
  ssid Employee
ssid-profile name ssid2
  ssid Guest
vap-profile name vap1
  forward-mode tunnel
  service-vlan vlan-id 30
  ssid-profile ssid1
  security-profile sec1
  traffic-profile traff
  ip source check user-bind enable
  arp anti-attack check user-bind enable
  learn-client-address dhcp-strict
vap-profile name vap2
  forward-mode tunnel
  service-vlan vlan-id 40
  ssid-profile ssid2
  security-profile sec2
  traffic-profile traff
  ip source check user-bind enable
  arp anti-attack check user-bind enable
  learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
  regulatory-domain-profile domain1
radio 0
  vap-profile vap1 wlan 1
  vap-profile vap2 wlan 2
radio 1
  vap-profile vap1 wlan 1
  vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
```



```
ap-name area_1
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
master controller
master-redundancy track-vrrp vrid 1 interface Vlanif20
master-redundancy peer-ip ip-address 172.16.100.2 local-ip ip-address 172.16.100.1
psk %^%#5Vh&+;LCyDdLEV1gGJuP}9l(9W&u!+uHt";5T#yM%^%#
#
return
```

CORE-AC2 的配置文件

```
#
sysname CORE-AC2
#
vrrp recover-delay 60
#
vlan batch 20 30 40 100
#
dhcp enable
#
dhcp snooping enable
#
vlan 30
dhcp snooping enable
vlan 40
dhcp snooping enable
#
interface Vlanif20
ip address 192.168.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
admin-vrrp vrid 1
dhcp select interface
dhcp server excluded-ip-address 192.168.20.1
dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif30
ip address 172.16.30.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.30.1
dhcp server excluded-ip-address 172.16.30.3
```

```
dhcp server dns-list 192.168.100.2
#
interface Vlanif40
ip address 172.16.40.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.40.1
dhcp server excluded-ip-address 172.16.40.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif100
ip address 172.16.100.2 255.255.255.0
#
interface Eth-Trunk2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40
mode lacp
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/21
eth-trunk 2
#
interface XGigabitEthernet0/0/22
eth-trunk 2
#
ip route-static 0.0.0.0 0.0.0.0 192.168.20.20
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.100.2 peer-ip 172.16.100.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
```

```
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
    user-isolate l2
security-profile name sec1
security-profile name sec2
ssid-profile name ssid1
    ssid Employee
ssid-profile name ssid2
    ssid Guest
vap-profile name vap1
    forward-mode tunnel
    service-vlan vlan-id 30
    ssid-profile ssid1
    security-profile sec1
    traffic-profile traff
    ip source check user-bind enable
    arp anti-attack check user-bind enable
    learn-client-address dhcp-strict
vap-profile name vap2
    forward-mode tunnel
    service-vlan vlan-id 40
    ssid-profile ssid2
    security-profile sec2
    traffic-profile traff
    ip source check user-bind enable
    arp anti-attack check user-bind enable
    learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
    regulatory-domain-profile domain1
radio 0
    vap-profile vap1 wlan 1
    vap-profile vap2 wlan 2
radio 1
    vap-profile vap1 wlan 1
    vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
```

```
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
master controller
master-redundancy track-vrrp vrid 1 interface Vlanif20
master-redundancy peer-ip ip-address 172.16.100.1 local-ip ip-address 172.16.100.2
psk %^%#QKK0'nRL%0U`y32S6bOSB40e=FJE^Lbs7.A]x)QQ%^%#
#
return
```

1.1.2.1.7 独立 AC 方案：汇聚交换机做有线用户网关，AC 做无线用户网关

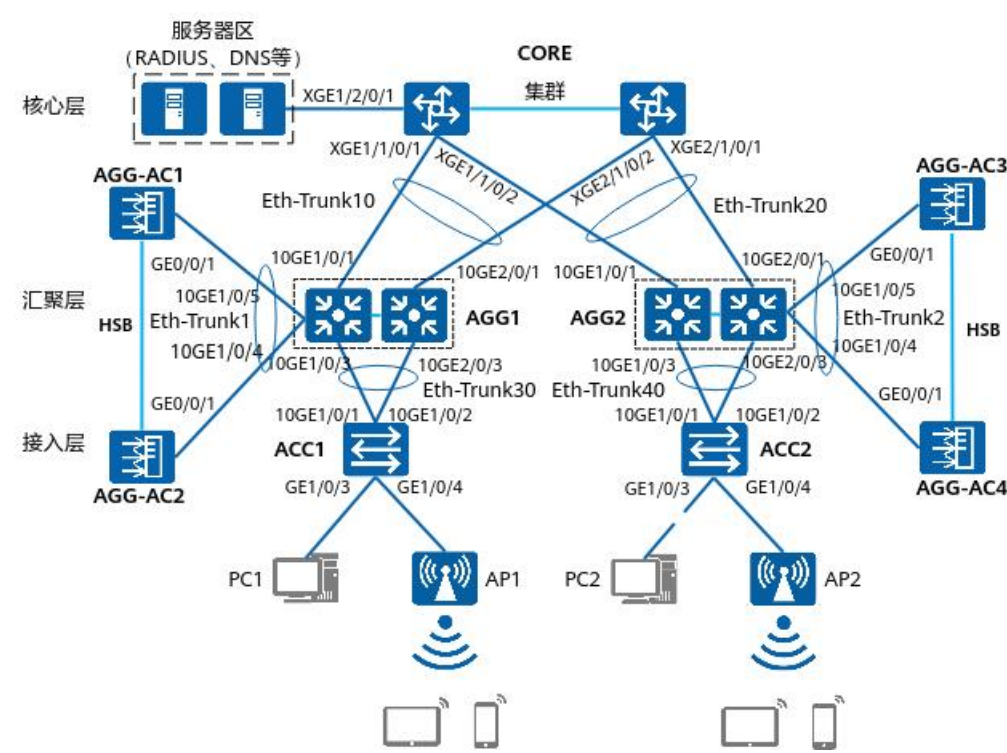
核心层交换机组建集群，作为整个园区网络的核心，实现网络高可靠性和网络大数据量转发。

汇聚层交换机组建堆叠，实现设备级备份的同时，也扩展了设备的端口密度和转发带宽。

独立 AC 旁挂式部署，作为 DHCP 服务器为 AP 分配 IP 地址，管理全网 AP 上线。

本案例中，汇聚交换机和 AC 分别作为全网有线、无线用户的网关，负责全网用户业务的路由转发。

图 1 汇聚交换机做有线用户网关+独立 AC 做无线用户网关



设备要求和版本

位置	设备要求	本案例使用的设备	本案例使用的版本
核心层	—	S12700E	V200R022C10

位置	设备要求	本案例使用的设备	本案例使用的版本
汇聚层	–	S6730-H-V2	V600R022C10
接入层	–	S5735-L-V2	V600R022C10
AC	–	AC6805	V200R022C10
AP	–	AirEngine 8760-X1-PRO	V200R022C10

部署思路

步骤	部署思路	涉及设备
1	配置交换机的集群/堆叠功能，配置上下行 Eth-Trunk	核心交换机、汇聚交换机
2	配置交换机、AC 的接口和 VLAN，配置三层接口地址、路由，使得网络互通	核心交换机、汇聚交换机、接入交换机
3	配置汇聚交换机和 AC 的 DHCP 功能，使交换机和 AC 分别作为 DHCP 服务器为有线、AP/无线用户分配 IP 地址	汇聚交换机、AC
4	配置 AC 的 VRRP+HSB 方式的备份	AC
5	配置 AC 的无线业务，实现 AP 和 STA 上线	AC
6	配置 VRRP 热备份场景下的无线配置同步	AC

数据规划

表 1 核心交换机业务数据规划

项目	VLAN ID	网段
连接 AGG1 的网段	VLAN 70	172.16.70.0/24
连接 AGG2 的网段	VLAN 80	172.16.80.0/24
连接服务器的网段	VLAN 1000	192.168.100.0/24

表 2 汇聚交换机业务数据规划

设备	项目	VLAN ID	网段
AGG1	有线用户的业务 VLAN	VLAN 50	172.16.50.0/24
	连接 CORE 的网段	VLAN 70	172.16.70.0/24

表 2 汇聚交换机业务数据规划

设备	项目	VLAN ID	网段
	连接 AGG-AC 的网段	VLAN 20	172.16.20.0/24
AGG2	有线用户的业务 VLAN	VLAN 60	172.16.60.0/24
	连接 CORE 的网段	VLAN 80	172.16.80.0/24
	连接 AGG-AC 的网段	VLAN 21	172.16.21.0/24

表 3 AC 业务数据规划

设备	项目	VLAN ID	网段
AGG-AC1、AGG-AC2	AP 管理 VLAN	VLAN 20	192.168.20.0/24
	无线用户的业务 VLAN	VLAN 30	172.16.30.0/24
		VLAN 31	172.16.31.0/24
	有线用户的业务 VLAN	VLAN 50	172.16.50.0/24
	连接 CORE 的网段	VLAN 70	172.16.70.0/24
	主备 AC HSB 同步 VLAN	VLAN 200	172.16.200.0/24
AGG-AC3、AGG-AC4	AP 管理 VLAN	VLAN 21	192.168.21.0/24
	无线用户的业务 VLAN	VLAN 40	172.16.40.0/24
		VLAN 41	172.16.41.0/24
	有线用户的业务 VLAN	VLAN 60	172.16.60.0/24
	连接 CORE 的网段	VLAN 80	172.16.80.0/24
	主备 AC HSB 同步 VLAN	VLAN 200	172.16.200.0/24

表 4 AGG-AC 无线业务数据规划

项目	数据
AP 组	ap-group1、ap-group2
域管理模板	domain1
SSID 模板	ssid1、ssid2
VAP 模板	vap1、vap2、隧道转发方式

配置注意事项

不建议使用 VLAN 1 作为业务 VLAN，将各端口从 VLAN1 中退出。根据实际业务需求透传 VLAN，禁止端口透传所有 VLAN。

隧道转发方式下，管理 VLAN 和业务 VLAN 不能配置为同一 VLAN，否则会导致 MAC 漂移，报文转发出错。并且 AP 和 AC 之间只能放通管理 VLAN，不能放通业务 VLAN。

隧道转发模式下，AP 的业务报文会封装在 CAPWAP 数据隧道中进行传输，先发送给 AC，然后由 AC 再转发到上层网络，所以只要配置 AC 与 AP 间的网络加入管理 VLAN，AC 与上层网络间的网络加入业务 VLAN，就能正常传输业务报文和管理报文。

对于主备 AC 上关联的同一 AP，其 WLAN 相关的业务配置必须保持一致（如 WMM 模板、射频模板、射频、流量模板、安全模板、安全策略和 WLAN ID 等都需要保持一致），否则当 AC 的主备状态切换后，无法保证用户业务正常。

主备 AC 的型号和软件版本需完全一致。

在 VRRP 热备份场景下部署 DHCP 服务器时需要注意以下几点：

V200R019C00 及之后版本，开启 DHCP 服务器功能的接口无限制，主 AC 分配 IP 地址，备 AC 不分配，主 AC 的 IP 地址分配信息会同步到备 AC。

主备 AC 上配置的 IP 地址池必须完全一致，配置不一致会导致主备 AC 备份失败。

配置命令 `hsb-service-type dhcp hsb-group group-index`，使 DHCP 业务绑定 HSB 备份组。否则主备 AC 上的 IP 地址分配信息无法备份。

配置步骤

1. 配置核心层交换机集群和汇聚层交换机堆叠、多主检测及上下行 Eth-Trunk。

此部分配置请参考 [集群/堆叠通用部署](#)。

2. 配置核心交换机 CORE 的接口和 VLAN。

创建 VLAN。

```
[CORE] vlan batch 70 80 1000
```

配置和汇聚交换机 AGG1 互连的 Eth-Trunk10。和汇聚交换机 AGG2 互连的配置与此类似，此处不再赘述。

```
[CORE] interface eth-trunk 10
[Core-Eth-Trunk10] description connect to AGG1
[Core-Eth-Trunk10] mode lacp
[Core-Eth-Trunk10] port link-type trunk
[Core-Eth-Trunk10] port trunk allow-pass vlan 70
[Core-Eth-Trunk10] undo port trunk allow-pass vlan 1
[Core-Eth-Trunk10] quit
```

将和服务器对接的接口加入 VLAN1000。

```
[CORE] interface xgigabitethernet 1/2/0/1
```

```
[CORE-XGigabitEthernet1/2/0/1] port link-type access
[CORE-XGigabitEthernet1/2/0/1] port default vlan 1000
[CORE-XGigabitEthernet1/2/0/1] quit
```

创建连接汇聚交换机 AGG1 的三层接口 VLANIF70。

```
[CORE] interface vlanif 70
[CORE-Vlanif70] ip address 172.16.70.1 255.255.255.0
[CORE-Vlanif70] quit
```

创建连接汇聚交换机 AGG2 的三层接口 VLANIF80。

```
[CORE] interface vlanif 80
[CORE-Vlanif80] ip address 172.16.80.1 255.255.255.0
[CORE-Vlanif80] quit
```

创建连接服务器的三层接口 VLANIF1000。

```
[CORE] interface vlanif 1000
[CORE-Vlanif1000] ip address 192.168.100.1 255.255.255.0
[CORE-Vlanif1000] quit
```

3. 配置汇聚交换机 AGG1 的接口和 VLAN。汇聚交换机 AGG2 的配置与此类似，不再赘述。

创建 VLAN。

```
<AGG1> system-view
[AGG1] vlan batch 20 30 31 50 70
```

配置与核心交换机 CORE 连接的 Eth-Trunk。

```
[AGG1] interface eth-trunk 10
[AGG1-Eth-Trunk10] description connect to CORE
[AGG1-Eth-Trunk10] mode lacp-static
[AGG1-Eth-Trunk10] port link-type trunk
[AGG1-Eth-Trunk10] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk10] port trunk allow-pass vlan 70
[AGG1-Eth-Trunk10] quit
[AGG1] interface 10GE 1/0/1
[AGG1-10GE1/0/1] eth-trunk 10
[AGG1-10GE1/0/1] quit
[AGG1] interface 10GE 2/0/1
[AGG1-10GE2/0/1] eth-trunk 10
[AGG1-10GE2/0/1] quit
```

创建和 AGG-AC1 互连的 Eth-Trunk1 并将接口加入 Eth-Trunk。

```
[AGG1] interface eth-trunk 1
[AGG1-Eth-Trunk1] description connect to AC
[AGG1-Eth-Trunk1] mode lacp-static
[AGG1-Eth-Trunk1] port link-type trunk
[AGG1-Eth-Trunk1] port trunk allow-pass vlan 20 30 31
```



```
[AGG1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk1] quit
[AGG1] interface 10GE 1/0/4
[AGG1-10GigabitEthernet1/0/4] eth-trunk 1
[AGG1-10GigabitEthernet1/0/4] quit
[AGG1] interface 10GE 1/0/5
[AGG1-10GigabitEthernet1/0/5] eth-trunk 1
[AGG1-10GigabitEthernet1/0/5] quit
```

创建连接核心交换机 CORE 的三层接口 VLANIF70。

```
[AGG1] interface Vlanif 70
[AGG1-Vlanif70] ip address 172.16.70.2 255.255.255.0
[AGG1-Vlanif70] quit
```

创建连接 AC 的三层接口 VLANIF20。

```
[CORE] interface vlanif 20
[CORE-Vlanif20] ip address 192.168.20.20 255.255.255.0
[CORE-Vlanif20] quit
```

配置与接入交换机 ACC1 连接的下行接口。

```
[AGG1] interface eth-trunk 30
[AGG1-Eth-Trunk30] mode lacp-static
[AGG1-Eth-Trunk30] port link-type trunk
[AGG1-Eth-Trunk30] port trunk allow-pass vlan 20 50
[AGG1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[AGG1-Eth-Trunk30] quit
[AGG1] interface 10GE 1/0/3
[AGG1-10GE1/0/3] eth-trunk 30
[AGG1-10GE1/0/3] quit
[AGG1] interface 10GE 2/0/3
[AGG1-10GE2/0/3] eth-trunk 30
[AGG1-10GE2/0/3] quit
```

4. 配置 AGG-AC1 的接口和 VLAN。AGG-AC2、AGG-AC3 和 AGG-AC4 的配置与此类似，不再赘述。

创建 VLAN。

```
<AC6805> system-view
[AC6805] sysname AGG-AC1
[AGG-AC1] vlan batch 20 30 31 200
```

创建 AGG-AC1 与汇聚交换机 AGG1 互连的 Eth-Trunk，并将接口加入 Eth-Trunk。

```
[AGG-AC1] interface eth-trunk 1
[AGG-AC1-Eth-Trunk1] description connect to AGG1
[AGG-AC1-Eth-Trunk1] mode lacp-static
```

```
[AGG-AC1-Eth-Trunk1] port link-type trunk
[AGG-AC1-Eth-Trunk1] port trunk allow-pass vlan 20 30 31
[AGG-AC1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[AGG-AC1-Eth-Trunk1] quit
[AGG-AC1] interface gigabitethernet 0/0/1
[AGG-AC1-GigabitEthernet0/0/1] eth-trunk 1
[AGG-AC1-GigabitEthernet0/0/1] quit
[AGG-AC1] interface gigabitethernet 0/0/2
[AGG-AC1-GigabitEthernet0/0/2] eth-trunk 1
[AGG-AC1-GigabitEthernet0/0/2] quit
```

配置 AGG-AC1 链接 AGG-AC2 的接口。

```
[AGG-AC1] interface gigabitethernet 0/0/2
[AGG-AC1-GigabitEthernet0/0/2] port link-type trunk
[AGG-AC1-GigabitEthernet0/0/2] port trunk allow-pass vlan 200
[AGG-AC1-GigabitEthernet0/0/2] undo port trunk allow-pass vlan 1
[AGG-AC1-GigabitEthernet0/0/2] quit
[AGG-AC1] interface vlanif 200
[AGG-AC1-Vlanif200] ip address 172.16.200.1 255.255.255.0
[AGG-AC1-Vlanif200] quit
```

5. 配置接入交换机 ACC1 的接口和 VLAN。接入交换机 ACC2 的配置与此类似，不再赘述。

创建 VLAN。

```
<ACC1> system-view
[ACC1] vlan batch 20 50
```

配置与汇聚交换机 AGG1 连接的上行接口。

```
[ACC1] interface eth-trunk 30
[ACC1-Eth-Trunk30] mode lacp-static
[ACC1-Eth-Trunk30] port link-type trunk
[ACC1-Eth-Trunk30] port trunk allow-pass vlan 20 50
[ACC1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[ACC1-Eth-Trunk30] quit
[ACC1] interface 10GE 1/0/1
[ACC1-10GE1/0/1] eth-trunk 30
[ACC1-10GE1/0/1] quit
[ACC1] interface 10GE 1/0/2
[ACC1-10GE1/0/2] eth-trunk 30
[ACC1-10GE1/0/2] quit
```

配置与 PC1 和 AP1 连接的下行接口，并将连接 PC1 和 AP1 的端口配置为边缘端口。

```
[ACC1] interface GE 1/0/3
[ACC1-GE1/0/3] port link-type access
[ACC1-GE1/0/3] port default vlan 50
```

```
[ACC1-GE1/0/3] port-isolate enable group 1
[ACC1-GE1/0/3] stp edged-port enable
[ACC1-GE1/0/3] quit
[ACC1] interface GE 1/0/4
[ACC1-GE1/0/4] port link-type trunk
[ACC1-GE1/0/4] port trunk pvid vlan 20
[ACC1-GE1/0/4] port trunk allow-pass vlan 20
[ACC1-GE1/0/4] port-isolate enable group 1
[ACC1-GE1/0/4] stp edged-port enable
[ACC1-GE1/0/4] quit
```

6. 配置汇聚交换机 AGG1 的 DHCP 功能，使得交换机作为 DHCP 服务器为有线、无线用户分配 IP 地址。汇聚交换机 AGG2 的配置与此类似，不再赘述。

使能全局 DHCP 功能，并配置业务 VLAN 的 DHCP Snooping 功能。

```
[AGG1] dhcp enable
[AGG1] dhcp snooping enable
[AGG1] vlan 50
[AGG1-vlan50] dhcp snooping enable
[AGG1-vlan50] quit
```

创建有线业务三层接口 VLANIF50 并配置通过接口地址池为有线终端分配地址。

```
[AGG1] interface Vlanif 50
[AGG1-Vlanif50] ip address 172.16.50.1 255.255.255.0
[AGG1-Vlanif50] dhcp select interface
[AGG1-Vlanif50] dhcp server dns-list 192.168.100.2 //配置终端的 DNS 服务器
[AGG1-Vlanif50] arp proxy intra-vlan enable //开启 VLAN 内 ARP 代理
[AGG1-Vlanif50] quit
```

7. 配置核心交换机和汇聚交换机的路由功能，实现三层网络互通。

在核心交换机 CORE 上配置 OSPF 功能。

```
[CORE] ospf 1 router-id 1.1.1.1
[CORE-ospf-1] area 0
[CORE-ospf-1-area-0.0.0.0] network 172.16.70.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] network 172.16.80.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] network 192.168.100.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] quit
```

在汇聚交换机 AGG1 上配置 OSPF 功能。汇聚交换机 AGG2 的配置与此类似，不再赘述。

```
[AGG1] ospf 1 router-id 2.2.2.2
[AGG1-ospf-1] area 0
[AGG1-ospf-1-area-0.0.0.0] network 172.16.70.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 172.16.50.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] quit
[AGG1-ospf-1] area 1
```

```
[AGG1-ospf-1-area-0.0.0.1] network 192.168.20.0 0.0.0.255
[AGG1-ospf-1-area-0.0.0.1] quit
[CORE-ospf-1] quit
```

在 AGG-AC1 上配置 OSPF 功能。

```
[AGG-AC1] ospf 1 router-id 3.3.3.3
[AGG-AC1-ospf-1] area 1
[AGG-AC1-ospf-1-area-0.0.0.1] network 192.168.20.0 0.0.0.255
[AGG-AC1-ospf-1-area-0.0.0.1] network 172.16.30.0 0.0.0.255
[AGG-AC1-ospf-1-area-0.0.0.1] network 172.16.31.0 0.0.0.255
[AGG-AC1-ospf-1-area-0.0.0.1] quit
[AGG-AC1-ospf-1] quit
```

8. 配置 AGG-AC1 的 DHCP 功能。AGG-AC3 的配置与此类似，不再赘述。

创建无线业务三层接口 VLANIF20 并通过接口地址池为 AP 分配 IP 地址。

```
[AGG-AC1] dhcp enable
[AGG-AC1] interface Vlanif 20
[AGG-AC1-Vlanif20] ip address 172.16.20.1 255.255.255.0
[AGG-AC1-Vlanif20] dhcp select interface
[AGG-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.2
[AGG-AC1-Vlanif20] dhcp server excluded-ip-address 192.168.20.20
[AGG-AC1-Vlanif20] quit
```

创建无线业务三层接口 VLANIF30 并通过接口地址池为 STA 分配地址。

```
[AGG-AC1] interface Vlanif 30
[AGG-AC1-Vlanif30] ip address 172.16.30.1 255.255.255.0
[AGG-AC1-Vlanif30] dhcp select interface
[AGG-AC1-Vlanif30] dhcp server dns-list 192.168.100.2 //配置终端的 DNS 服务器
[AGG-AC1-Vlanif30] arp-proxy inner-sub-vlan-proxy enable //开启 VLAN 内 ARP 代理
[AGG-AC1-Vlanif30] quit
```

创建无线业务三层接口 VLANIF31 并通过接口地址池为 STA 分配地址。

```
[AGG-AC1] interface Vlanif 31
[AGG-AC1-Vlanif31] ip address 172.16.31.1 255.255.255.0
[AGG-AC1-Vlanif31] dhcp select interface
[AGG-AC1-Vlanif31] dhcp server dns-list 192.168.100.2 //配置终端的 DNS 服务器
[AGG-AC1-Vlanif31] arp-proxy inner-sub-vlan-proxy enable //开启 VLAN 内 ARP 代理
[AGG-AC1-Vlanif31] quit
```

9. 配置 AGG-AC1 的 VRRP+HSB 方式的备份。AGG-AC2 配置与此类似，不再赘述。

配置 VRRP 备份组的状态恢复延迟时间为 60 秒。

```
[AGG-AC1] vrrp recover-delay 60
```

在 AGG-AC1 上创建管理 VRRP 备份组，配置 AGG-AC1 在该备份组中的优先级为 120，并配置抢占时间为 1200 秒。

```
[AGG-AC1] interface vlanif 20
[AGG-AC1-Vlanif20] vrrp vrid 1 virtual-ip 192.168.20.3
[AGG-AC1-Vlanif20] vrrp vrid 1 priority 120
[AGG-AC1-Vlanif20] vrrp vrid 1 preempt-mode timer delay 1200
[AGG-AC1-Vlanif20] admin-vrrp vrid 1
[AGG-AC1-Vlanif20] quit
```

在 AGG-AC1 上创建 HSB 主备服务 0，并配置其主备通道 IP 地址和端口号。

```
[AGG-AC1] hsb-service 0
[AGG-AC1-hsb-service-0] service-ip-port local-ip 172.16.200.1 peer-ip 172.16.200.2 local-data-port
10241 peer-data-port 10241
[AGG-AC1-hsb-service-0] quit
```

在 AGG-AC1 上创建 HSB 备份组 0，并配置其绑定 HSB 主备服务 0 和管理 VRRP 备份组。

```
[AGG-AC1] hsb-group 0
[AGG-AC1-hsb-group-0] bind-service 0
[AGG-AC1-hsb-group-0] track vrrp vrid 1 interface vlanif 20
[AGG-AC1-hsb-group-0] quit
```

配置 AGG-AC1 业务绑定 HSB 备份组。

```
[AGG-AC1] hsb-service-type access-user hsb-group 0
[AGG-AC1] hsb-service-type ap hsb-group 0
[AGG-AC1] hsb-service-type dhcp hsb-group 0
[AGG-AC1] hsb-group 0
[AGG-AC1-hsb-group-0] hsb enable
[AGG-AC1-hsb-group-0] quit
```

配置完成后，在 AGG-AC1 和 AGG-AC2 上分别执行 **display vrrp** 命令，可以看到 AGG-AC1 的 State 字段的显示为 **Master**，AGG-AC2 的 State 字段的显示为 **Backup**。

```
[AGG-AC1] display vrrp
Vlanif20 | Virtual Router 1
  State : Master
  Virtual IP : 192.168.20.3
  Master IP : 192.168.20.3
  PriorityRun : 120
  PriorityConfig : 120
  MasterPriority : 120
  Preempt : YES   Delay Time : 1200s
  TimerRun : 2s
  TimerConfig : 2s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : admin-vrrp
```

```
Backup-forward : disabled
Track SysHealth Priority reduced : 254
SysHealth state : UP
Create time : 2019-11-30 14:23:11
Last change time : 2019-11-30 14:23:17
```

[AGG-AC2] display vrrp

```
Vlanif20 | Virtual Router 1
State : Backup
Virtual IP : 192.168.20.3
Master IP : 192.168.20.2
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 0
Preempt : YES Delay Time : 1200s
TimerRun : 2s
TimerConfig : 2s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : admin-vrrp
Backup-forward : disabled
Track SysHealth Priority reduced : 254
SysHealth state : UP
Create time : 2019-11-30 07:15:11
Last change time : 2019-11-30 14:23:17
```

在 AGG-AC1 和 AGG-AC2 上查看主备服务的建立情况。可以看到 **Service State** 字段的显示为 **Connected**，说明主备服务通道已经成功建立。

[AGG-AC1] display hsb-service 0

Hot Standby Service Information:

```
-----
Local IP Address   : 172.16.200.1
Peer IP Address    : 172.16.200.2
Source Port        : 10241
Destination Port   : 10241
Keep Alive Times    : 5
Keep Alive Interval : 3
Service State       : Connected
Service Batch Modules :
Shared-key          : -
-----
```

[AGG-AC2] display hsb-service 0

Hot Standby Service Information:

```

-----
Local IP Address      : 172.16.200.2
Peer IP Address       : 172.16.200.1
Source Port           : 10241
Destination Port      : 10241
Keep Alive Times      : 5
Keep Alive Interval   : 3
Service State         : Connected
Service Batch Modules :
Shared-key             : -
-----

```

在 AGG-AC1 和 AGG-AC2 上执行 **display hsb-group 0** 命令，查看 HSB 备份组的运行情况。

[AGG-AC1] **display hsb-group 0**

Hot Standby Group Information:

```

-----
HSB-group ID          : 0
Vrrp Group ID         : 1
Vrrp Interface        : Vlanif20
Service Index         : 0
Group Vrrp Status     : Master
Group Status          : Active
Group Backup Process   : Realtime
Peer Group Device Name : AC6805
Peer Group Software Version : V200R022C10
Group Backup Modules   : Access-user
                        AP
-----

```

[AGG-AC2] **display hsb-group 0**

Hot Standby Group Information:

```

-----
HSB-group ID          : 0
Vrrp Group ID         : 1
Vrrp Interface        : Vlanif20
Service Index         : 0
Group Vrrp Status     : Backup
Group Status          : Active
Group Backup Process   : Realtime
Peer Group Device Name : AC6805
Peer Group Software Version : V200R022C10
Group Backup Modules   : Access-user
                        AP
-----

```

10. 配置 AGG-AC1 的无线业务，实现 AP1 上线。AGG-AC2 的配置与此类似，不再赘述。

配置 AC 的源接口。

```
[AGG-AC1] capwap source interface vlanif 20
```

#创建 AP 组，用于将相同配置的 AP 都加入到同一 AP 组中。

```
[AGG-AC1] wlan
```

```
[AGG-AC1-wlan-view] ap-group name ap-group1
```

```
[AGG-AC1-wlan-ap-group-ap-group1] quit
```

创建域管理模板，在域管理模板下配置 AC 的国家码并在 AP 组下引用域管理模板。

```
[AGG-AC1-wlan-view] regulatory-domain-profile name domain1
```

```
[AGG-AC1-wlan-regulate-domain-domain1] country-code cn
```

```
[AGG-AC1-wlan-regulate-domain-domain1] quit
```

```
[AGG-AC1-wlan-view] ap-group name ap-group1
```

```
[AGG-AC1-wlan-ap-group-ap-group1] regulatory-domain-profile domain1
```

Warning: Modifying the country code will clear channel, power and antenna gain configurations of the radio and reset the AP. Continue?[Y/N]:y

```
[AGG-AC1-wlan-ap-group-ap-group1] quit
```

将 AP1 加入 AP 组 ap-group1，并根据 AP 的部署位置为 AP 配置名称。

```
[AGG-AC1-wlan-view] ap auth-mode mac-auth
```

```
[AGG-AC1-wlan-view] ap-id 1 ap-mac 00e0-fc12-3300
```

```
[AGG-AC1-wlan-ap-1] ap-name area_1
```

Warning: The AP name of more than 31 characters does not take effect for APs in versions earlier than V200R009C00.

Warning: This operation may cause AP reset. Continue? [Y/N]:y

```
[AGG-AC1-wlan-ap-1] ap-group ap-group1
```

Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configurations of the radio, whether to continue? [Y/N]:y

Info: This operation may take a few seconds. Please wait for a moment.. done.

```
[AGG-AC1-wlan-ap-1] quit
```

```
[AGG-AC1-wlan-view] quit
```

将 AP1 上电后，可以查看到 AP1 的“State”字段为“nor”。

```
[AGG-AC1] display ap all
```

Total AP information:

nor : normal [1]

ExtraInfo : Extra information

P : insufficient power supply

```
-----
ID  MAC      Name  Group  IP      Type      State  STA Uptime  ExtraInfo
-----
```



```
1 00e0-fc12-4400 area_1 ap-group1 192.168.20.148 AirEngine 8760-X1-PRO nor 0 1H:19M:18S
-
-----
-----
```

11. 在 AGG-AC1 上配置 STA 上线。

配置 WLAN 业务参数，创建安全模板、SSID 模板和流量模板。

```
[AGG-AC1] wlan
[AGG-AC1-wlan-view] security-profile name sec1
[AGG-AC1-wlan-sec-prof-sec1] security open
[AGG-AC1-wlan-sec-prof-sec1] quit
[AGG-AC1-wlan-view] ssid-profile name ssid1
[AGG-AC1-wlan-ssid-prof-ssid1] ssid test01
[AGG-AC1-wlan-ssid-prof-test01] quit
[AGG-AC1-wlan-view] traffic-profile name traff1
[AGG-AC1-wlan-traffic-prof-traff1] user-isolate l2
[AGG-AC1-wlan-traffic-prof-test01] quit
[AGG-AC1-wlan-view] security-profile name sec2
[AGG-AC1-wlan-sec-prof-sec2] security open
[AGG-AC1-wlan-sec-prof-sec2] quit
[AGG-AC1-wlan-view] ssid-profile name ssid2
[AGG-AC1-wlan-ssid-prof-ssid2] ssid test02
[AGG-AC1-wlan-ssid-prof-test02] quit
[AGG-AC1-wlan-view] traffic-profile name traff2
[AGG-AC1-wlan-traffic-prof-traff2] user-isolate l2
[AGG-AC1-wlan-traffic-prof-traff2] quit
```

配置 WLAN-VAP 模板，配置业务数据转发模式、业务 VLAN，并应用安全模板和 SSID 模板，使能 IPSG 功能动态 ARP 检测功能和 STA 地址严格 DHCP 获取功能。

```
[AGG-AC1-wlan-view] vap-profile name test01
[AGG-AC1-wlan-vap-prof-test01] forward-mode tunnel
[AGG-AC1-wlan-vap-prof-test01] service-vlan vlan-id 30
[AGG-AC1-wlan-vap-prof-test01] security-profile sec1
[AGG-AC1-wlan-vap-prof-test01] ssid-profile ssid1
[AGG-AC1-wlan-vap-prof-test01] traffic-profile traff1
[AGG-AC1-wlan-vap-prof-test01] ip source check user-bind enable
[AGG-AC1-wlan-vap-prof-test01] arp anti-attack check user-bind enable
[AGG-AC1-wlan-vap-prof-test01] learn-client-address dhcp-strict
[AGG-AC1-wlan-vap-prof-test01] quit
[AGG-AC1-wlan-view] vap-profile name test02
[AGG-AC1-wlan-vap-prof-test02] forward-mode tunnel
[AGG-AC1-wlan-vap-prof-test02] service-vlan vlan-id 31
[AGG-AC1-wlan-vap-prof-test02] security-profile sec2
```

```
[AGG-AC1-wlan-vap-prof-test02] ssid-profile ssid2
[AGG-AC1-wlan-vap-prof-test02] traffic-profile traff2
[AGG-AC1-wlan-vap-prof-test02] ip source check user-bind enable
[AGG-AC1-wlan-vap-prof-test02] arp anti-attack check user-bind enable
[AGG-AC1-wlan-vap-prof-test02] learn-client-address dhcp-strict
[AGG-AC1-wlan-vap-prof-test02] quit
```

说明

由于 **ip source check user-bind enable** 命令是基于绑定表进行匹配检查的，因此

对于 DHCP 用户，需要使能 DHCP Snooping 自动生成动态绑定表。

对于静态配置 IP 的用户，需要手工配置静态绑定表。

learn-client-address dhcp-strict 命令的前置条件为：

在 VAP 模板视图下执行命令 **undo dhcp trust port** 去使能 AP 的 DHCP 信任功能。

在 VAP 模板视图下执行命令 **undo learn-client-address { ipv4 | ipv6 } disable** 使能 STA 地址学习功能。

配置 AP 组引用 VAP 模板。

```
[AGG-AC1-wlan-view] ap-group name ap-group1
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 0
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 0
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap1 wlan 1 radio 1
[AGG-AC1-wlan-ap-group-ap-group1] vap-profile vap2 wlan 2 radio 1
[AGG-AC1-wlan-ap-group-ap-group1] quit
[AGG-AC1-wlan-view] quit
```

结果验证

预期结果

有线用户、无线用户均可正常接入园区网络。

验证方法

以汇聚交换机 AGG1 和 AGG-AC1 为例，汇聚交换机 AGG2 和 AGG-AC2 上的验证方法与此类似，不再赘述。

在 AGG-AC1 上查看 AP 已成功获取到 IP 地址。

```
[AGG-AC1] display ip pool interface vlanif20 used
Pool-name      : Vlanif20
Pool-No        : 0
Lease           : 1 Days 0 Hours 0 Minutes
Domain-name     : -
DNS-server0    : -
NBNS-server0   : -
Netbios-type    : -
```

```

Position      : Interface
Status        : Unlocked
Gateway-0     : -
Network       : 192.168.20.0
Mask          : 255.255.255.0
Logging       : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :254   Used    :1
                  Idle     :251   Expired  :0
                  Conflict  :0     Disabled :2

```

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled

192.168.20.1	192.168.20.254	254	1	251(0)	0	2

Client-ID format as follows:

```

DHCP  : mac-address          PPPoE  : mac-address
IPSec : user-id/portnumber/vrf  PPP   : interface index
L2TP  : cpu-slot/session-id    SSL-VPN : user-id/session-id

```

Index	IP	Client-ID	Type	Left	Status
147	192.168.20.148	00e0-fc12-4400	DHCP	80426	Used

在汇聚交换机上查看有线用户均已成功获取到 IP 地址。

[AGG1] **display ip pool interface vlanif50 used**

```

Pool-name      : Vlanif50
Pool-No        : 2
Lease          : 1 Days 0 Hours 0 Minutes
Domain-name    : -
DNS-server0    : 192.168.100.2
NBNS-server0   : -
Netbios-type   : -
Position       : Interface

```

```

Status      : Unlocked
Gateway-0   : -
Network     : 172.16.50.0
Mask        : 255.255.255.0
VPN instance : --
Logging     : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :254   Used    :1
                  Idle     :254   Expired   :0
                  Conflict  :0     Disabled  :0

```

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled
172.16.50.1	172.16.50.216	254	0	254(0)	0	0

有线、无线用户可以实现互访。

在 AP1 上可以 Ping 通服务器区设备。

```
<area_1> ping 192.168.100.2
```

```
PING 192.168.100.2: 56 data bytes, press CTRL_C to break
```

```
Reply from 192.168.100.2: bytes=56 Sequence=1 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=2 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=3 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=4 ttl=63 time=1 ms
```

```
Reply from 192.168.100.2: bytes=56 Sequence=5 ttl=63 time=1 ms
```

```
--- 192.168.100.2 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 1/1/1 ms
```

AP1 下有无线用户接入后，在 AGG-AC1 上可以查看到接入的无线用户信息。

```
[AGG-AC1] display station ssid test01
```

```
Rf/WLAN: Radio ID/WLAN ID
```

```
Rx/Tx: link receive rate/link transmit rate(Mbps)
```

STA MAC	AP ID	Ap name	Rf/WLAN	Band	Type	Rx/Tx	RSSI	VLAN	IP address

00e0-fc12-3388	2	area_2	1/1	5G	11ac	117/115	-71	30	172.16.30.180

Total: 1 2.4G: 0 5G: 1									

在 PC1 上可以 Ping 通连接 AP1 的用户。

```
C:\Users>ping 172.16.30.180
```

```
Pinging 172.16.30.180 with 32 bytes of data:
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Reply from 172.16.30.180: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 172.16.30.180:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

配置文件

CORE 的配置文件

```
#
sysname CORE
#
vlan batch 70 80 1000
#
interface Vlanif70
 ip address 172.16.70.1 255.255.255.0
#
interface Vlanif80
 ip address 172.16.80.1 255.255.255.0
#
interface Vlanif1000
 ip address 192.168.100.1 255.255.255.0
#
interface Eth-Trunk10
 description connect to AGG1
 port link-type trunk
 undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 70
mode lacp
#
interface Eth-Trunk20
description connect to AGG2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 80
mode lacp
#
interface XGigabitEthernet1/1/0/1
eth-trunk 10
#
interface XGigabitEthernet1/1/0/2
eth-trunk 20
#
interface XGigabitEthernet1/1/0/10
mad detect mode direct
#
interface XGigabitEthernet1/2/0/1
port link-type access
port default vlan 1000
#
interface XGigabitEthernet2/1/0/1
eth-trunk 20
#
interface XGigabitEthernet2/1/0/2
eth-trunk 10
#
interface XGigabitEthernet2/1/0/10
mad detect mode direct
#
ospf 1 router-id 1.1.1.1
area 0.0.0.0
network 172.16.70.0 0.0.0.255
network 172.16.80.0 0.0.0.255
network 192.168.100.0 0.0.0.255
#
return
```

AGG-AC1 的配置文件

```
#
sysname AGG-AC1
```

```
#
vrrp recover-delay 60
#
vlan batch 20 30 to 31 200
#
dhcp enable
#
dhcp snooping enable
#
vlan 30
    dhcp snooping enable
vlan 31
    dhcp snooping enable
#
interface Vlanif20
    ip address 192.168.20.1 255.255.255.0
    vrrp vrid 1 virtual-ip 192.168.20.3
    admin-vrrp vrid 1
    vrrp vrid 1 priority 120
    vrrp vrid 1 preempt-mode timer delay 1200
    dhcp select interface
    dhcp server excluded-ip-address 192.168.20.2
    dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif30
    ip address 172.16.30.1 255.255.255.0
    arp-proxy inner-sub-vlan-proxy enable
    dhcp select interface
    dhcp server dns-list 192.168.100.2
#
interface Vlanif31
    ip address 172.16.31.1 255.255.255.0
    arp-proxy inner-sub-vlan-proxy enable
    dhcp select interface
    dhcp server dns-list 192.168.100.2
#
interface Vlanif200
    ip address 172.16.200.1 255.255.255.0
#
interface Eth-Trunk 1
    description connect to AGG1
    port link-type trunk
    undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 20
mode lacp
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 200
#
ospf 1 router-id 3.3.3.3
area 0.0.0.1
network 192.168.20.0 0.0.0.255
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.200.1 peer-ip 172.16.200.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff1
user-isolate l2
traffic-profile name traff2
user-isolate l2
security-profile name sec1
security open
security-profile name sec2
security open
ssid-profile name ssid1
ssid test01
ssid-profile name ssid2
```



```
ssid test02
vap-profile name test01
forward-mode tunnel
service-vlan vlan-id 30
ssid-profile ssid1
security-profile sec1
traffic-profile traff1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name test02
forward-mode tunnel
service-vlan vlan-id 40
ssid-profile ssid2
security-profile sec2
traffic-profile traff2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
#
```

AGG-AC2 的配置文件

```
#
sysname AGG-AC2
#
vrrp recover-delay 60
#
vlan batch 20 200
#
```

```
interface vlanif20
ip address 192.168.20.2 255.255.255.0
admin-vrrp vrid 1
vrrp vrid 1 virtual-ip 192.168.20.3
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
#
interface vlanif200
ip address 172.16.200.1 255.255.255.0
#
interface eth-trunk 1
description connect to AGG1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20
mode lacp
#
interface gigabitethernet 0/0/1
eth-trunk 1
#
interface gigabitethernet 0/0/2
port link-type trunk
port trunk allow-pass vlan 200
undo port trunk allow-pass vlan 1
#
hsb-service 0
service-ip-port local-ip 172.16.200.2 peer-ip 172.16.200.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
```

AGG-AC3 的配置文件

```
#
sysname AGG-AC3
```

```
#
vrrp recover-delay 60
#
vlan batch 21 200
#
dhcp enable
#
dhcp snooping enable
#
vlan 40
    dhcp snooping enable
vlan 41
    dhcp snooping enable
#
interface vlanif21
    ip address 192.168.21.1 255.255.255.0
    admin-vrrp vrid 1
    vrrp vrid 1 virtual-ip 192.168.21.3
    vrrp vrid 1 priority 120
    vrrp vrid 1 preempt-mode timer delay 1200
    dhcp select interface
    dhcp server excluded-ip-address 192.168.21.2
    dhcp server excluded-ip-address 192.168.21.20
#
interface Vlanif40
    ip address 172.16.40.1 255.255.255.0
    arp-proxy inner-sub-vlan-proxy enable
    dhcp select interface
    dhcp server dns-list 192.168.100.2
#
interface Vlanif41
    ip address 172.16.41.1 255.255.255.0
    arp-proxy inner-sub-vlan-proxy enable
    dhcp select interface
    dhcp server dns-list 192.168.100.2
#
interface vlanif201
    ip address 172.16.201.1 255.255.255.0
#
interface eth-trunk 1
    description connect to AGG2
    port link-type trunk
    undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 21
mode lacp
#
interface gigabitethernet 0/0/1
eth-trunk 1
#
interface gigabitethernet 0/0/2
port link-type trunk
port trunk allow-pass vlan 201
undo port trunk allow-pass vlan 1
#
ospf 1 router-id 4.4.4.4
area 0.0.0.2
network 192.168.21.0 0.0.0.255
#
capwap source interface vlanif21
#
hsb-service 0
service-ip-port local-ip 172.16.201.1 peer-ip 172.16.201.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif21
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff1
user-isolate l2
traffic-profile name traff2
user-isolate l2
security-profile name sec1
security-profile name sec2
ssid-profile name ssid3
ssid test03
ssid-profile name ssid4
ssid test04
vap-profile name test01
```

```
forward-mode tunnel
service-vlan vlan-id 40
ssid-profile ssid3
security-profile sec1
traffic-profile traff1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name test02
forward-mode tunnel
service-vlan vlan-id 41
ssid-profile ssid2
security-profile sec2
traffic-profile traff2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
#
```

AGG-AC4 的配置文件

```
#
sysname AGG-AC4
#
vrrp recover-delay 60
#
vlan batch 21 200
#
interface vlanif21
ip address 192.168.21.2 255.255.255.0
```

```
admin-vrrp vrid 1
vrrp vrid 1 virtual-ip 192.168.21.3
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
#
interface vlanif201
ip address 172.16.201.1 255.255.255.0
#
interface eth-trunk 1
description connect to AGG2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21
mode lacp
#
interface gigabitethernet 0/0/1
eth-trunk 1
#
interface gigabitethernet 0/0/2
port link-type trunk
port trunk allow-pass vlan 200
undo port trunk allow-pass vlan 1
#
hsb-service 0
service-ip-port local-ip 172.16.201.2 peer-ip 172.16.201.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif21
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
```

AGG1 的配置文件

```
#
sysname AGG1
#
vlan batch 20 50 70
```

```
#
dhcp enable

#
dhcp snooping enable

#
vlan 50
    dhcp snooping enable

#
interface Vlanif20
    ip address 192.168.20.20 255.255.255.0

#
interface Vlanif50
    ip address 172.16.50.1 255.255.255.0
    arp proxy intra-vlan enable
    dhcp select interface
    dhcp server dns-list 192.168.100.2

#
interface Vlanif70
    ip address 172.16.70.2 255.255.255.0

#
interface Eth-Trunk1
    description con to AC
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 20
    mode lacp-static

#
interface Eth-Trunk10
    description connect to CORE
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 70
    mode lacp-static

#
interface Eth-Trunk30
    port link-type trunk
    undo port trunk allow-pass vlan 1
    port trunk allow-pass vlan 20 30 to 31 50
    mode lacp-static

#
interface 10GE1/0/3
    eth-trunk 30

#
```

```
interface 10GE1/0/4
 eth-trunk 1
#
interface 10GE1/0/5
 eth-trunk 1
#
interface 10GE2/0/3
 eth-trunk 30
#
interface 10GE1/0/1
 eth-trunk 10
#
interface 10GE2/0/1
 eth-trunk 10
#
return
```

AGG2 的配置文件

```
#
sysname AGG2
#
vlan batch 21 60 80
#
dhcp enable
#
dhcp snooping enable
#
vlan 60
 dhcp snooping enable
#
interface Vlanif21
 ip address 192.168.21.20 255.255.255.0
#
interface Vlanif60
 ip address 172.16.60.1 255.255.255.0
 arp proxy intra-vlan enable
 dhcp select interface
 dhcp server dns-list 192.168.100.2
#
interface Vlanif80
 ip address 172.16.80.2 255.255.255.0
#
interface Eth-Trunk1
```



```
description con to AC
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21
mode lacp-static
#
interface Eth-Trunk10
description connect to CORE
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 80
mode lacp-static
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 40 to 41 60
mode lacp-static
port-isolate enable group 1
#
interface 10GE1/0/3
eth-trunk 40
#
interface 10GE1/0/4
eth-trunk 2
#
interface 10GE1/0/5
eth-trunk 2
#
interface 10GE2/0/3
eth-trunk 40
#
interface 10GE1/0/1
eth-trunk 20
#
interface 10GE2/0/1
eth-trunk 20
#
return
```

ACC1 的配置文件

```
#
sysname ACC1
```

```
#
vlan batch 20 50
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 30
#
interface 10GE1/0/2
eth-trunk 30
#
interface GE1/0/3
port link-type access
port default vlan 50
stp edged-port enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type access
port default vlan 20
stp edged-port enable
port-isolate enable group 1
#
return
```

ACC2 的配置文件

```
#
sysname ACC2
#
vlan batch 21 60
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 60
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 30
```

```
#
interface 10GE1/0/2
 eth-trunk 30
#
interface GE1/0/3
 port link-type access
 port default vlan 60
 stp edged-port enable
 port-isolate enable group 1
#
interface GE1/0/4
 port link-type access
 port default vlan 21
 stp edged-port enable
 port-isolate enable group 1
#
return
```

1.1.2.2 有线无线用户接入认证部署案例

用户接入认证部署要点和说明

独立 AC 方案：核心交换机做有线用户网关和认证点，AC 做无线用户网关和认证点，NAC

独立 AC 方案：汇聚交换机做有线用户网关和认证点，AC 做无线用户网关和认证点，NAC

认证点在接入设备的认证部署配置示例

1.1.2.2.1 用户接入认证部署要点和说明

用户接入认证部署的目的是解决用户认证和策略管控两大问题。这其中涉及到几个关键节点设备：

认证点：负责用户准入认证的设备或者节点。

准入执行点（接入点）：负责执行是否允许终端准入的设备或者节点。

组策略执行点：负责执行业务随行组策略的设备或者节点。

传统接入控制方案采用 NAC 认证+ACL 策略控制，园区网络中通常会定义认证控制点这一个设备角色，对接入园区网络的用户终端进行准入认证和策略控制。华为的接入控制方案在传统 NAC 方案基础上新增策略联动和业务随行功能后，对园区网络接入控制中的设备角色做了更精细化的分工。

认证控制点：负责用户接入认证，与认证服务器进行交互，完成认证、授权、计费。在策略联动方案中，认证控制点与认证执行点间会建立 CAPWAP 隧道，交互用户认证请求，同步用户表项等。

认证执行点：在策略联动方案中，负责对接入用户进行准入控制，用户认证通过后，才允许访问网络；同时，会向认证控制点透传用户认证报文。用户授权的策略也可以通过认证控制点下发到认证执行点，但需要手工配置。

策略执行点：即执行管控策略的设备。一般认证控制点即为策略执行点，比如传统 NAC 认证+ACL 策略的接入控制方案中，用户认证通过后，认证服务器可以授权 ACL 给用户，认证控制点根据用户授权的 ACL 信息，对用户访问网络进行策略控制。

本章节介绍典型的用户接入认证部署案例，采用独立 AC 部署方案，主要根据认证点位置差异以及策略管控方案差异来划分。

表 1 用户接入认证部署要点和说明

部署要点	说明	场景推荐
AC 部署方案	采用独立 AC 部署方案。	选择独立 AC 方案，可以将有线、无线用户网关都部署在交换机上，也可以将有线用户网关部署在交换机上，无线用户网关部署在独立 AC 上。用户接入认证部署案例中的独立 AC 方案，以无线用户的网关和认证点都部署在独立 AC 为例。
有线无线认证点	一般来讲，认证点位置通常同用户网关位置。	独立 AC 方案中建议将有线用户网关部署在交换机上，无线用户网关部署在独立 AC 上。
策略管控	策略管控方案包括 NAC、业务随行和策略联动。	NAC 可以应用在所有需要认证的场景中。 业务随行一般应用在园区接入场景，主要用于实现基于帐号、终端类型和接入方式的权限控制，与用户在何处登录无关，权限随行。 策略联动一般应用在大型园区，接入层设备数量众多且位置分布广的场景中，若在每个接入层设备上部署 NAC 认证和用户访问策略，工作量巨大且策略调整不灵活。通过部署策略联动（汇聚层交换机或核心交换机做认证控制点，接入交换机配做认证执行点），一方面能够避免接入用户未认证就在接入层互通、另一方面能够获取用户在接入设备上线的接口、用户所属 VLAN 等信息便于维护管理。

1.1.2.2.2 独立 AC 方案：核心交换机做有线用户网关和认证点，AC 做无线用户网关和认证点，NAC

案例描述

核心层交换机组建集群，作为整个园区网络的核心，实现网络高可靠性和网络大数据量转发。独立 AC 旁挂式部署，作为网关为 AP 和无线用户分配 IP 地址，统一管理全网 AP 和无线用户上线。

汇聚层交换机组建堆叠，实现设备级备份的同时，也扩展了设备的端口密度和转发带宽。
本案例中，核心交换机作为全网有线用户的网关和认证点，独立 AC 作为全网无线用户的网关和认证点，有线用户和无线用户必须认证成功才能接入网络。其中：

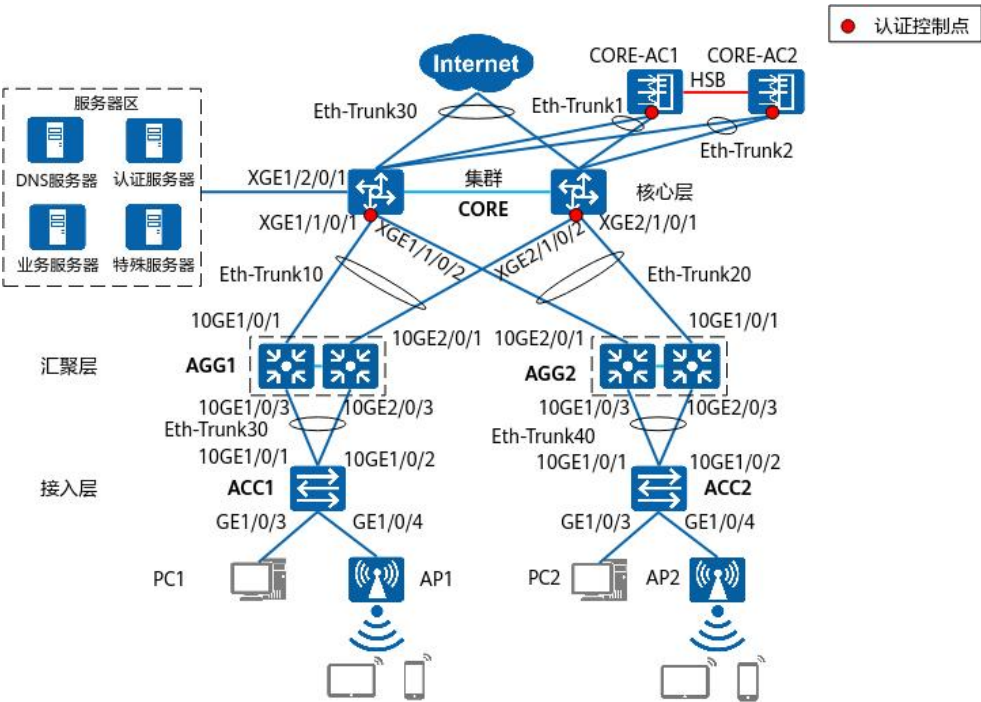
用户角色包括员工（接入方式包括有线和无线）和访客（仅能通过无线接入），员工使用 802.1X 认证，访客使用 MAC 优先的 Portal 认证。

iMaster NCE-Campus 作为认证服务器和用户业务数据源服务器，采用集中式认证服务器部署方案。

iMaster NCE-Campus 对认证成功的用户授权 ACL 策略，用于管控不同角色的用户的网络访问权限。

汇聚和接入层交换机配置端口隔离，用于管控用户的二层流量。

图 1 核心交换机做有线用户的网关和认证点 + 独立 AC 做无线用户的网关和认证点组网图



设备要求和版本

位置	设备要求	本案例使用的设备	本案例使用的版本
认证服务器	—	iMaster NCE-Campus	V300R022C10SPC100
核心层	—	S12700E	V200R022C10
汇聚层	—	S6730-H-V2	V600R022C10
接入层	—	S5735-L-V2	V600R022C10
AC	—	AC6805	V200R022C10
AP	—	AirEngine 8760-X1-PRO	V200R022C10

部署思路

步骤	部署思路
配置基础网络互通	1. 请参见 独立 AC 方案：核心交换机做有线用户网关，AC 做无线用户网关 。
配置核心交换机和 AC	2. 配置 AAA 参数，包括 RADIUS 服务器模板、AAA 方案和认证域，用于指定交换机以及 AC 与 RADIUS 服务器的对接参数。
	3. 配置免认证资源以及员工和访客认证成功后的网络访问权限。
	4. 配置员工使用 802.1X 认证。
	5. （仅涉及 AC）配置访客使用 MAC 优先的 Portal 认证。
配置汇聚和接入交换机	6. 配置 802.1X 认证报文二层透明传输功能。
配置 iMaster NCE-Campus	7. 添加与 iMaster NCE-Campus 对接的设备，指定 RADIUS 认证参数和 Portal 认证参数。
	8. 添加用户组和用户帐号。
	9. 开启 MAC 优先的 Portal 认证。
	10. 配置员工和访客认证成功后的网络访问权限。

数据规划

表 1 基础网络连通数据规划

项目	VLAN ID	网段
核心交换机与 AC 之间的互通 VLAN	VLAN 20（AP 的管理 VLAN）	192.168.20.0/24
	VLAN 30（无线员工的业务 VLAN）	172.16.30.0/24
	VLAN 40（访客的业务 VLAN）	172.16.40.0/24
有线用户的业务 VLAN（AGG1 侧）	VLAN 50	172.16.50.0/24
有线用户的业务 VLAN（AGG2 侧）	VLAN 60	172.16.60.0/24
CORE-AC1 和 CORE-AC2 之间的互通 VLAN	VLAN 100	172.16.100.0/24
核心交换机与服务器之间的互通 VLAN	VLAN 1000	192.168.100.0/24

表 2 AC 无线业务数据规划

项目	员工	访客
流量模板	traff: 用户隔离模式为二层隔离三层互通	
安全模板	sec1: WPA/WPA2-802.1X 认证	sec2: 开放认证 (缺省的安全策略)
SSID 模板	ssid1: Employee	ssid2: Guest
AP 组	ap-group1	
域管理模板	domain1	
业务数据转发模式	隧道转发模式	
业务 VLAN	VLAN 30	VLAN 40
VAP 模板	vap1	vap2

表 3 核心交换机和 AC 认证业务数据规划

项目	数据
AAA 方案	认证方案 auth: RADIUS 认证 计费方案 acco: RADIUS 计费
RADIUS 服务器	RADIUS 服务器模板名称: tem_rad 认证、计费和授权服务器的 IP 地址: 192.168.100.10 认证服务器的端口号: 1812 计费服务器的端口号: 1813 认证计费密钥: YsHsjx_202206 授权密钥: YsHsjx_202206 计费周期: 15 分钟
Portal 服务器	Portal 服务器模板名称: tem_portal Portal 服务器的 IP 地址: 192.168.100.10 端口号: 50200 Portal 服务器共享密钥: YsHsjx_202206 Portal 服务器探测功能: 已开启
802.1X 接入模板	名称: d1 认证方式: EAP

表 3 核心交换机和 AC 认证业务数据规划

项目	数据
Portal 接入模板	名称：web1
MAC 接入模板	名称：mac1
免认证资源	DNS 服务器，IP 地址为 192.168.100.2。
用户认证成功后的网络访问权限	员工：Internet、DNS 服务器、业务服务器、其他员工 访客：Internet、DNS 服务器、其他访客 业务服务器的 IP 地址为 192.168.100.3，特殊服务器的 IP 地址为 192.168.100.100，园区出口的 IP 地址为 172.16.3.1。

表 4 iMaster NCE–Campus 业务数据规划

项目	数据
用户帐号	员工：user1/YsHsjx_202206、user2/YsHsjx_202206 访客：guest4/YsHsjx_202206
设备的 IP 地址	核心交换机：192.168.100.1 AC：192.168.20.1（备设备 IP 地址：192.168.20.2）
RADIUS 认证参数	设备系列：Huawei Engine 认证计费密钥：YsHsjx_202206 授权密钥：YsHsjx_202206 实时计费周期(分钟)：15
Portal 认证参数	Portal 密钥：YsHsjx_202206 终端 IP 地址列表：172.16.30.0/24;172.16.40.0/24

部署注意事项

不建议使用 VLAN 1 作为业务 VLAN，将各端口从 VLAN1 中退出。根据实际业务需求透传 VLAN，禁止端口透传所有 VLAN。

隧道转发方式下，管理 VLAN 和业务 VLAN 不能配置为同一 VLAN，否则会导致 MAC 漂移，报文转发出错。并且 AP 和 AC 之间只能放通管理 VLAN，不能放通业务 VLAN

隧道转发模式下，AP 的业务报文会封装在 CAPWAP 数据隧道中进行传输，先发送给 AC，然后由 AC 再转发到上层网络，所以只要配置 AC 与 AP 间的网络加入管理 VLAN，AC 与上层网络间的网络加入业务 VLAN，就能正常传输业务报文和管理报文。

对于主备 AC 上关联的同一 AP，其 WLAN 相关的业务配置必须保持一致（如 WMM 模板、射频模板、射频、流量模板、安全模板、安全策略和 WLAN ID 等都需要保持一致），否则当 AC 的主备状态切换后，无法保证用户业务正常。

主备 AC 的型号和软件版本需完全一致。

在 VRRP 热备份场景下部署 DHCP 服务器时需要注意以下几点：

V200R019C00 及之后版本，开启 DHCP 服务器功能的接口无限制，主 AC 分配 IP 地址，备 AC 不分配，主 AC 的 IP 地址分配信息会同步到备 AC。

主备 AC 上配置的 IP 地址池必须完全一致，配置不一致会导致主备 AC 备份失败。

配置命令 `hsb-service-type dhcp hsb-group group-index`，使 DHCP 业务绑定 HSB 备份组。否则主备 AC 上的 IP 地址分配信息无法备份。

配置过程中的 RADIUS 认证计费密钥、授权密钥和 Portal 密钥，交换机侧与服务器侧必须要配置一致。

交换机默认放行发往 RADIUS 服务器和 Portal 服务器的报文，不需要针对其配置免认证规则。

802.1X 认证场景中，如果使能 802.1X 认证的交换机和用户之间存在二层交换机，则需要在二层交换机上配置 802.1X 认证报文二层透明传输功能，否则用户无法认证成功。

部署步骤

1. 基础网络连通部署，请参见 [独立 AC 方案：核心交换机做有线用户网关，AC 做无线用户网关](#)。

配置 CORE 连接 Internet 的网段。

```
<CORE> system-view
[CORE] interface Eth-Trunk 30
[CORE-Eth-Trunk30] mode lacp
[CORE-Eth-Trunk30] description con to Internet
[CORE-Eth-Trunk30] trunkport xgigabitethernet 1/1/0/5
[CORE-Eth-Trunk30] trunkport xgigabitethernet 2/1/0/5
[CORE-Eth-Trunk30] undo portswitch
[CORE-Eth-Trunk30] ip address 172.16.3.1 24
[CORE-Eth-Trunk30] quit
```

2. 配置核心交换机的认证业务数据。

- a. 配置 AAA 参数。

配置 RADIUS 服务器模板“tem_rad”，指定核心交换机与 RADIUS 服务器的对接参数，包括 RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号以及认证计费密钥。

```
[CORE] radius-server template tem_rad
[CORE-radius-tem_rad] radius-server authentication 192.168.100.10 1812
[CORE-radius-tem_rad] radius-server accounting 192.168.100.10 1813
[CORE-radius-tem_rad] radius-server shared-key cipher YsHsjx_202206
[CORE-radius-tem_rad] quit
```

配置 RADIUS 授权服务器和授权密钥。

```
[CORE] radius-server authorization 192.168.100.10 shared-key cipher YsHsjx_202206
```

配置 AAA 认证和计费方案，指定认证和计费方式为 RADIUS，计费周期为 15 分钟。

```
[CORE] aaa
[CORE-aaa] authentication-scheme auth
[CORE-aaa-authen-auth] authentication-mode radius
[CORE-aaa-authen-auth] quit
[CORE-aaa] accounting-scheme acco
[CORE-aaa-accounting-acco] accounting-mode radius
[CORE-aaa-accounting-acco] accounting realtime 15
[CORE-aaa-accounting-acco] quit
```

配置认证域 “huawei.com”，在域下绑定 AAA 方案和 RADIUS 服务器模板。

```
[CORE-aaa] domain huawei.com
[CORE-aaa-domain-huawei.com] authentication-scheme auth
[CORE-aaa-domain-huawei.com] accounting-scheme acco
[CORE-aaa-domain-huawei.com] radius-server tem_rad
[CORE-aaa-domain-huawei.com] quit
[CORE-aaa] quit
```

b. 配置免认证资源以及员工认证成功后的网络访问权限。

配置免认证资源：放通到 DNS 服务器的报文和 AP 管理 VLAN 的报文。

```
[CORE] free-rule-template name default_free_rule
[CORE-free-rule-default_free_rule] free-rule 1 destination ip 192.168.100.2 mask 32
[CORE-free-rule-default_free_rule] free-rule 2 source vlan 20
[CORE-free-rule-default_free_rule] quit
```

配置员工认证成功后的网络访问权限：员工认证成功之后可以访问 Internet、DNS 服务器和业务服务器，员工之间可以互访。

```
[CORE] acl 3001
[CORE-acl-adv-3001] rule 1 permit ip destination 172.16.3.0 0.0.0.255 //员工认证成功后可以访问 Internet
[CORE-acl-adv-3001] rule 2 permit ip destination 192.168.100.2 0.0.0.0 //员工认证成功后可以访问 DNS 服务器
[CORE-acl-adv-3001] rule 3 permit ip destination 192.168.100.3 0.0.0.0 //员工认证成功后可以访问业务服务器
[CORE-acl-adv-3001] rule 4 permit ip destination 172.16.30.0 0.0.0.255 //允许员工之间互访
[CORE-acl-adv-3001] rule 5 permit ip destination 172.16.50.0 0.0.0.255 //允许员工之间互访
[CORE-acl-adv-3001] rule 6 permit ip destination 172.16.60.0 0.0.0.255 //允许员工之间互访
[CORE-acl-adv-3001] rule 7 deny ip destination any
[CORE-acl-adv-3001] quit
```

c. 配置员工使用 802.1X 认证。

配置 802.1X 接入模板。802.1X 接入模板默认采用 EAP 认证方式，请确保 RADIUS 服务器支持 EAP 协议，否则无法处理 802.1X 认证请求。

```
[CORE] dot1x-access-profile name d1
[CORE-dot1x-access-profile-d1] quit
```

配置员工使用的认证模板。

```
[CORE] authentication-profile name p1
[CORE-authen-profile-p1] dot1x-access-profile d1
[CORE-authen-profile-p1] access-domain huawei.com force //配置认证域 huawei.com 为强制认证域
[CORE-authen-profile-p1] quit
```

在下行接口配置有线接入的员工使用 802.1X 认证。

```
[CORE] interface eth-trunk 10
[CORE-Eth-Trunk10] authentication-profile p1
[CORE-Eth-Trunk10] quit
[CORE] interface eth-trunk 20
[CORE-Eth-Trunk20] authentication-profile p1
[CORE-Eth-Trunk20] quit
```

3. 配置 AC 的认证业务数据。此处以 CORE-AC1 为例，CORE-AC2 与之类似，不再赘述。

a. 配置 AAA 参数。

配置 RADIUS 服务器模板“tem_rad”，指定 AC 与 RADIUS 服务器的对接参数，包括 RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号以及认证计费密钥。

```
<CORE-AC1> system-view
[CORE-AC1] radius-server template tem_rad
[CORE-AC1-radius-tem_rad] radius-server authentication 192.168.100.10 1812
[CORE-AC1-radius-tem_rad] radius-server accounting 192.168.100.10 1813
[CORE-AC1-radius-tem_rad] radius-server shared-key cipher YsHsjx_202206
[CORE-AC1-radius-tem_rad] quit
```

配置 RADIUS 授权服务器和授权密钥。

```
[CORE-AC1] radius-server authorization 192.168.100.10 shared-key cipher YsHsjx_202206
```

配置 AAA 认证和计费方案，指定认证和计费方式为 RADIUS，计费周期为 15 分钟。

```
[CORE-AC1] aaa
[CORE-AC1-aaa] authentication-scheme auth
[CORE-AC1-aaa-authen-auth] authentication-mode radius
[CORE-AC1-aaa-authen-auth] quit
[CORE-aaa] accounting-scheme acco
[CORE-AC1-aaa-accounting-acco] accounting-mode radius
```

```
[CORE-AC1-aaa-accounting-acco] accounting realtime 15
[CORE-AC1-aaa-accounting-acco] quit
```

- b. 配置免认证资源以及用户认证成功后的网络访问权限。

配置免认证资源：放通到 DNS 服务器的报文。

```
[CORE-AC1] free-rule-template name default_free_rule
[CORE-AC1-free-rule-default_free_rule] free-rule 1 destination ip 192.168.100.2 mask 32
[CORE-AC1-free-rule-default_free_rule] quit
```

配置员工认证成功后的网络访问权限：员工认证成功之后可以访问 Internet、DNS 服务器和业务服务器，员工之间可以互访。

说明

对于无线用户，由于 ACL 规则被下发到 AP 上执行，因此必须放通无线用户能访问的所有网段的地址，包括无线用户所在网段的地址，否则无线用户即使能够认证成功，但所有报文在 AP 上均会被丢弃。

```
[CORE-AC1] acl 3001
[CORE-AC1-acl-adv-3001] rule 1 permit ip destination 172.16.3.0 0.0.0.255
[CORE-AC1-acl-adv-3001] rule 2 permit ip destination 192.168.100.2 0.0.0.0
[CORE-AC1-acl-adv-3001] rule 3 permit ip destination 192.168.100.3 0.0.0.0
[CORE-AC1-acl-adv-3001] rule 4 permit ip destination 172.16.30.0 0.0.0.255
[CORE-AC1-acl-adv-3001] rule 5 permit ip destination 172.16.50.0 0.0.0.255
[CORE-AC1-acl-adv-3001] rule 6 permit ip destination 172.16.60.0 0.0.0.255
[CORE-AC1-acl-adv-3001] rule 7 deny ip destination any
[CORE-AC1-acl-adv-3001] quit
```

配置访客认证成功后的网络访问权限：访客认证成功之后可以访问 Internet 和 DNS 服务器，访客之间可以互访。

```
[CORE-AC1] acl 3002
[CORE-AC1-acl-adv-3002] rule 1 permit ip destination 172.16.3.0 0.0.0.255 //访客认证成功后可以访问 Internet
[CORE-AC1-acl-adv-3002] rule 2 permit ip destination 192.168.100.2 0.0.0.0 //访客认证成功后可以访问 DNS 服务器
[CORE-AC1-acl-adv-3002] rule 3 permit ip destination 172.16.40.0 0.0.0.255 //允许访客之间互访
[CORE-AC1-acl-adv-3002] rule 4 deny ip destination any
[CORE-AC1-acl-adv-3002] quit
```

- c. 配置员工使用 802.1X 认证。

配置 802.1X 接入模板。802.1X 接入模板默认采用 EAP 认证方式，请确保 RADIUS 服务器支持 EAP 协议，否则无法处理 802.1X 认证请求。

```
[CORE-AC1] dot1x-access-profile name d1
[CORE-AC1-dot1x-access-profile-d1] quit
```

配置员工使用的认证模板。

```
[CORE-AC1] authentication-profile name p1
[CORE-AC1-authen-profile-p1] dot1x-access-profile d1
[CORE-AC1-authen-profile-p1] free-rule-template default_free_rule
[CORE-AC1-authen-profile-p1] authentication-scheme auth
[CORE-AC1-authen-profile-p1] accounting-scheme acco
[CORE-AC1-authen-profile-p1] radius-server tem_rad
[CORE-AC1-authen-profile-p1] quit
```

配置无线接入的员工的安全策略。

```
[CORE-AC1] wlan
[CORE-AC1-wlan] security-profile name sec1
[CORE-AC1-wlan-sec-prof-sec1] security wpa2 dot1x aes
Warning: This action may cause service interruption. Continue?[Y/N]y
[CORE-AC1-wlan-sec-prof-sec1] quit
```

配置无线接入的员工使用 802.1X 认证。

```
[CORE-AC1-wlan-view] vap-profile name vap1
[CORE-AC1-wlan-vap-prof-vap1] authentication-profile p1
Warning: This action may cause service interruption. Continue?[Y/N]y
[CORE-AC1-wlan-vap-prof-vap1] quit
[CORE-AC1-wlan-view] quit
```

d. 配置访客使用 MAC 优先的 Portal 认证。

配置 Portal 服务器模板。指定 AC 与 Portal 服务器的对接参数，包括 Portal 服务器的 IP 地址、端口号、Portal 共享密钥以及 Portal 页面的 URL。

```
[CORE-AC1] web-auth-server tem_portal
[CORE-AC1-web-auth-server-tem_portal] server-ip 192.168.100.10
[CORE-AC1-web-auth-server-tem_portal] port 50200
[CORE-AC1-web-auth-server-tem_portal] shared-key cipher YsHsjx_202206
[CORE-AC1-web-auth-server-tem_portal] url http://192.168.100.10:8080/portal
[CORE-AC1-web-auth-server-tem_portal] server-detect interval 100 max-times 5 critical-num
0 action log //使能 Portal 服务器探测功能，使管理员能够实时掌握网络中 Portal 服务器的状态，保证在
Portal 服务器故障时，用户仍然能够正常访问网络。探测周期 interval 不能小于 15s，建议配置为 100s
[CORE-AC1-web-auth-server-tem_portal] quit
```

配置 Portal 接入模板。

```
[CORE-AC1] portal-access-profile name web1
[CORE-AC1-portal-acces-profile-web1] web-auth-server tem_portal direct
[CORE-AC1-portal-acces-profile-web1] quit
```

配置 MAC 接入模板。

```
[CORE-AC1] mac-access-profile name mac1
[CORE-AC1-mac-access-profile-mac1] quit
```

配置访客使用的认证模板。

```
[CORE-AC1] authentication-profile name p2
[CORE-AC1-authen-profile-p2] portal-access-profile web1
[CORE-AC1-authen-profile-p2] mac-access-profile mac1
[CORE-AC1-authen-profile-p2] free-rule-template default_free_rule
[CORE-AC1-authen-profile-p2] authentication-scheme auth
[CORE-AC1-authen-profile-p2] accounting-scheme acco
[CORE-AC1-authen-profile-p2] radius-server tem_rad
[CORE-AC1-authen-profile-p2] quit
```

配置访客使用 MAC 优先的 Portal 认证。

```
[CORE-AC1] wlan
[CORE-AC1-wlan-view] vap-profile name vap2
[CORE-AC1-wlan-vap-prof-vap2] authentication-profile p2
Warning: This action may cause service interruption. Continue?[Y/N]y
[CORE-AC1-wlan-vap-prof-vap2] quit
[CORE-AC1-wlan-view] quit
```

4. 在汇聚和接入交换机上配置 802.1X 认证报文二层透明传输功能。此处以接入交换机 ACC1 为例，其他交换机的配置与之类似，不再赘述。

802.1X 认证报文经过的所有接口都需要配置该功能。对于不支持 `bpdu enable` 命令的交换机，接口下仅需配置 `l2protocol-tunnel user-defined-protocol 802.1x enable` 命令即可。

```
<ACC1> system-view
[ACC1] l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 0180-c200-0003 group-mac
0100-0000-0002
[ACC1] interface Eth-Trunk 30
[ACC1-Eth-Trunk30] l2protocol-tunnel user-defined-protocol 802.1x enable
[ACC1-Eth-Trunk30] quit
[ACC1] interface ge 1/0/3
[ACC1-GE1/0/3] l2protocol-tunnel user-defined-protocol 802.1x enable
[ACC1-GE1/0/3] quit
[ACC1] interface ge 1/0/4
[ACC1-GE1/0/4] l2protocol-tunnel user-defined-protocol 802.1x enable
[ACC1-GE1/0/4] quit
```

5. 登录 iMaster NCE-Campus，添加与 iMaster NCE-Campus 对接的设备，指定 RADIUS 认证参数和 Portal 认证参数。

选择“准入 > 准入资源 > 准入设备”，单击“创建”，添加设备。

添加 AC 设备的步骤如[图 2](#)。核心交换机的添加步骤与之类似，相关配置参数见[表 5](#)。

图 2 添加 AC 设备

*设备名称:

AC

描述:

*IP地址:

192.168.20.1

备份IP:

192.168.20.2

?

设备系列:

Huawei Engine

▼

RADIUS认证参数:

CoA类型:

默认CoA

No CoA

Port Bounce

Reauth

?

CoA端口:

?

准入设备模板:

...

*认证计费密钥:

.....

?

*确认认证计费密钥:

.....

*授权密钥:

.....

?

*确认授权密钥:

.....

*计费周期(分钟):

15

?

自定义MAC认证密码:

Service-Type属性值设置:

Portal认证参数:

Portal协议:

Huawei Portal(Portal2.0)

▼

Portal在线用户同步:

?

Portal心跳检验:

?

认证组件列表:

名称

▼

*Portal密钥:

.....

?

*确认Portal密钥:

.....

URL密钥:

?

确认URL密钥:

终端IP地址列表:

172.16.30.0/24
172.16.40.0/24

?

*Portal认证端口:

2000

?

Service-Type属性值设置:

HWTACACS认证参数:

表 5 iMaster NCE–Campus 与核心交换机和 AC 联动的参数设置

iMaster NCE–Campus 上的参数	核心交换机的参数取值	AC 的参数取值
设备名称	CORE	AC
IP 地址	192.168.100.1	192.168.20.1
RADIUS 认证参数	勾选	
备份 IP	–	192.168.20.2
设备系列	Huawei Engine	
认证计费密钥	YsHsjx_202206	
授权密钥	YsHsjx_202206	
计费周期(分钟)	15	
Portal 认证参数	–	勾选
Portal 协议		Huawei Portal (Portal2.0)
Portal 密钥		YsHsjx_202206
终端 IP 地址列表		172.16.30.0/24;172.16.40.0/24
Portal 心跳检测		勾选
Portal 认证端口		2000

6. 添加用户组和用户账号。此处以创建员工组以及员工账号为例，访客组以及访客账号与之类似，不再赘述。

选择“准入 > 准入资源 > 用户管理”。

增加名称为“employee”的用户组，并将单个用户“user1”、“user2”添加到该用户组。增加名称为“guest”的用户组，并将单个用户“guest4”添加到该用户组。[图 3](#)为用户 user1 的创建方式，user2 和 guest4 的创建方式与之类似。

图 3 创建用户

用户 | MAC帐号 | PPSK | 用户操作日志

基本信息

*用户名:

user1

*密码:

*确认密码:

角色:

名称

最大接入终端数:

0

过期时间:

下次登录修改密码:

允许登录方式:

☐ Portal

☒ 802.1X & Portal 2.0

☐ HWTACACS

进行Portal2.0认证需要同时勾选Portal及802.1X & Portal 2.0。进行HACA认证需要勾选Portal。

请输入关键字

用户自定义字段

启用

停用

转移

删除

创建

☐	用户名	用户组	角色	描述	邮箱	联系电话	过期时间	停用状态	操作
☐	user1	ROOT\employee					--	已启用	

7. 启用 MAC 优先的 Portal 认证

- a. 选择“准入 > 准入策略 > 用户在线控制”。设置 Portal 免认证策略，使能支持 Portal 免认证，并设置免认证时间为 1 小时。
- b. 将 Portal 免认证策略，分配给用户组“guest”。

图 4 设置 Portal 免认证策略

创建Portal免认证策略

*名称:

MAC优先Portal免认证

描述:

支持Portal免认证:

*Portal免认证时间:

1

小时

取消

确定

☐	名称	描述	支持Portal免认证	Portal免认证时间	操作
☒	MAC优先Portal免认证		是	1 小时	

分配给用户组

分配给用户

请输入名称

☐ 名称

描述

操作

☐ ROOT\guest

共1条

10 条/页

8. 配置员工和访客认证成功后的网络访问权限。

- a. 选择“准入 > 准入策略 > 认证授权”，单击“授权结果”页签，单击“创建”，分别添加员工和访客授权 ACL。
- ACL 编号与认证控制设备配置一致。

图 5 添加员工和访客授权 ACL

准入 / 准入策略 / 认证授权

认证规则 | 授权规则 | 授权结果 | 策略元素

创建

*名称:

ACL3001

描述:

策略

设备管理业务:

VIP用户:

仅支持AP、LSW

ACL:

3001

...

支持AP、LSW、AR，仅支持有ACL编号的ACL，不支持编号为编号段的ACL。

认证规则 | 授权规则 | 授权结果 | 策略元素

创建

*名称:

ACL3002

描述:

策略

设备管理业务:

VIP用户:

仅支持AP、LSW

ACL:

3002

...

支持AP、LSW、AR，仅支持有ACL编号的ACL，不支持编号为编号段的ACL。

表 6 员工和访客的授权结果

名称	授权参数: ACL 号/AAA 用户组
ACL3001	3001

表 6 员工和访客的授权结果

名称	授权参数: ACL 号/AAA 用户组
ACL3002	3002

b. 选择“准入 > 准入策略 > 认证授权”，单击“授权规则”，关联授权结果，指定员工和访客认证通过后允许访问的资源。

图 6 为有线员工的授权规则，无线员工和访客授权规则配置方法与之类似，配置参数见表 7。

图 6 有线员工的授权规则

创建授权规则

基本信息

*名称:

员工授权规则-有线

描述:

认证方式:

用户接入认证

MAC认证

设备管理认证

启用Portal-HACA协议:

?

接入方式:

WIFI

有线

蜂窝网络

?

用户信息

用户组信息匹配:

*用户组:

ROOT\employee

...

授权结果

*授权结果:

ACL3001

...

表 7 员工和访客的授权规则

名称	授权条件: 用户组	授权结果
员工授权规则-有线	employee	ACL3001
员工授权规则-无线	employee	ACL3001
访客授权规则	guest	ACL3002

预期结果

1. 员工或访客认证成功之前或是认证失败时，可以访问免认证资源，但无法访问认证后域资源。
2. 员工和访客分别选择正确的接入方式，并输入正确的用户名和密码之后，可以认证成功并接入网络。

- 3. 员工或访客认证成功之后，可以访问免认证资源，也可以访问认证后域资源，但无法访问认证后域禁止访问的资源。
- 4. 员工之间可以互访，员工与访客之间无法互访。

 说明

访客第一次接入网络，通过移动终端连接无线局域网 **Guest**，在浏览器中输入 **http://192.168.100.10:8080/portal**，进行 Portal 认证，在弹出的重定向页面中输入用户名和密码即可认证成功。访客断开网络，如果在 1 小时内重新接入 **Guest**，能够触发 MAC 优先的 Portal 认证，可以直接接入网络，无需再次输入用户名和密码。

结果验证

- 1. 员工或访客认证成功之前或是认证失败时，可以访问免认证资源，但无法访问认证后域资源。此处仅以通过有线方式接入的员工为例进行验证。

在 PC1 上输入错误的用户名和密码，然后在 CORE 执行 **display access-user** 命令查看在线用户信息。此时可以发现 user1 已上线，但处于预认证状态（**Pre-authen**），即未认证或认证失败状态。

```
[CORE] display access-user
-----
UserID  Username      IP address      MAC              Status
-----
114337  user1           172.16.50.110   00e0-fc12-3344   Pre-authen
-----
Total: 1, printed: 1
```

在 PC1 上 Ping 免认证资源（DNS 服务器：192.168.100.2），能够 Ping 通。

```
C:\Users\*****>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:
Reply from 192.168.100.2: bytes=32 time<1ms TTL=253
Reply from 192.168.100.2: bytes=32 time<1ms TTL=253
Reply from 192.168.100.2: bytes=32 time<1ms TTL=253
Reply from 192.168.100.2: bytes=32 time<1ms TTL=253

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\*****>
```

在 PC1 上 Ping 认证后域（园区出口：172.16.3.1），无法 Ping 通。

```
C:\Users\*****>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.

Ping statistics for 172.16.3.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\*****>
```

2. 员工和访客分别选择正确的接入方式，并输入正确的用户名和密码之后，可以认证成功并接入网络。

在 PC1 上输入正确的用户名和密码，再通过 Employee 和 Guest 分别接入一个无线用户，然后在 CORE 和 CORE-AC1 上执行 **display access-user** 命令查看在线用户信息。此时可以发现 user1、user2 和 guest4 均处于认证成功状态（**Success**）。

```
[CORE] display access-user

-----
UserID  Username      IP address      MAC             Status
-----
115318  user1          172.16.50.110   00e0-fc12-3344  Success
-----

Total: 1, printed: 1
[CORE-AC1] display access-user

-----
UserID  Username      IP address      MAC             Status
-----
16401   guest4        172.16.40.210   00e0-fc12-3355  Success
32788   user2         172.16.30.165   00e0-fc12-3366  Success
-----

Total: 2, printed: 2
```

在 CORE 上执行 **display access-user username user1 detail** 命令，可以查看 user1 的详细认证信息和授权信息。

[CORE] display access-user username user1 detail

Basic:

```
User ID           : 115318
User name         : user1
Domain-name       : huawei.com
User MAC          : 00e0-fc12-3344
User IP address   : 172.16.50.110
User vpn-instance : -
User IPv6 address : FE80::E9AA:9FE9:95F9:C499
User IPv6 link local address : FE80::E9AA:9FE9:95F9:C499
User access Interface : Eth-Trunk10
User vlan event    : Success
QinQVlan/UserVlan : 0/50
User vlan source   : user request
User access time   : 2019/11/26 11:08:16
User accounting session ID : CORE002100000000506e****0304276
User access type   : 802.1x
Terminal Device Type : Data Terminal
Dynamic ACL ID(Effective) : 3001
```

AAA:

```
User authentication type : 802.1x authentication
Current authentication method : RADIUS
Current authorization method : -
Current accounting method : RADIUS
```

Total: 1, printed: 1

在 CORE-AC1 上执行 **display access-user username user2 detail** 和 **display access-user username guest4 detail** 命令，可以查看 user2 和 guest4 的详细认证信息和授权信息。

[CORE-AC1] display access-user username user2 detail

Basic:

```
User ID           : 32788
User name         : user2
User MAC          : 00e0-fc12-3366
User IP address   : 172.16.30.165
User vpn-instance : -
User IPv6 address : -
User access Interface : Wlan-Dbss17496
User vlan event    : Success
```

```

QinQVlan/UserVlan      : 0/30
User vlan source        : user request
User access time        : 2019/11/26 21:22:53
User accounting session ID : CORE-AC00000000000030f0****0200014
User accounting mult session ID : AC853DA6A42038CADA5E441A5DDD9****690329A
User access type        : 802.1x
AP name                 : area_1
Radio ID                : 0
AP MAC                  : 00e0-fc12-6660
SSID                    : Employee
Online time             : 494(s)
Dynamic ACL ID(Effective) : 3001
User Group Priority      : 0

```

AAA:

```

User authentication type : 802.1x authentication
Current authentication method : RADIUS
Current authorization method : -
Current accounting method : RADIUS

```

Total: 1, printed: 1

[CORE-AC1] **display access-user username guest4 detail**

Basic:

```

User ID                : 16401
User name              : guest4
User MAC               : 00e0-fc12-3355
User IP address        : 172.16.40.210
User vpn-instance      : -
User IPv6 address      : -
User access Interface  : Wlan-Dbss17497
User vlan event        : Success
QinQVlan/UserVlan      : 0/40
User vlan source        : user request
User access time        : 2019/11/26 21:25:05
User accounting session ID : CORE-AC000000000000401c****0100011
User accounting mult session ID : AC853DA6A42064B0A6A3F913FFFFFF****FFFFFFF
User access type        : WEB
AP name                 : area_1
Radio ID                : 0
AP MAC                  : 00e0-fc12-6660
SSID                    : Guest

```

```

Online time           : 421(s)
Web-server IP address : 192.168.100.10
Dynamic ACL ID(Effective) : 3002
User Group Priority    : 0

```

AAA:

```

User authentication type : WEB authentication
Current authentication method : RADIUS
Current authorization method : -
Current accounting method : RADIUS

```

Total: 1, printed: 1

3. 员工或访客认证成功之后，可以访问免认证资源，也可以访问认证后域资源，但无法访问认证后域禁止访问的资源。此处仅以有线员工为例进行验证。

在 PC1 上 Ping 免认证资源（DNS 服务器：192.168.100.2），能够 Ping 通。

```

C:\Users\*****>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:
Reply from 192.168.100.2: bytes=32 time=1ms TTL=253
Reply from 192.168.100.2: bytes=32 time=1ms TTL=253
Reply from 192.168.100.2: bytes=32 time=1ms TTL=253
Reply from 192.168.100.2: bytes=32 time=1ms TTL=253

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\*****>

```

在 PC1 上 Ping 业务服务器（192.168.100.3），能够 Ping 通。

```

C:\Users\*****>ping 192.168.100.3

Pinging 192.168.100.3 with 32 bytes of data:
Reply from 192.168.100.3: bytes=32 time=1ms TTL=253
Reply from 192.168.100.3: bytes=32 time=1ms TTL=253
Reply from 192.168.100.3: bytes=32 time=1ms TTL=253
Reply from 192.168.100.3: bytes=32 time=1ms TTL=253

Ping statistics for 192.168.100.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

```



```
Approximate round trip times in milli-seconds:  
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

```
C:\Users\*****>
```

在 PC1 上 Ping 认证后域（园区出口：172.16.3.1），能够 Ping 通。

```
C:\Users\*****>ping 172.16.3.1
```

```
Pinging 172.16.3.1 with 32 bytes of data:  
Reply from 172.16.3.1: bytes=32 time<1ms TTL=254  
Reply from 172.16.3.1: bytes=32 time<1ms TTL=254  
Reply from 172.16.3.1: bytes=32 time<1ms TTL=254  
Reply from 172.16.3.1: bytes=32 time<1ms TTL=254  
  
Ping statistics for 172.16.3.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\Users\*****>
```

在 PC1 上 Ping 认证后域禁止访问的资源（特殊服务器：192.168.100.100），无法 Ping 通。

```
C:\Users\*****>ping 192.168.100.100
```

```
Pinging 192.168.100.100 with 32 bytes of data:  
Request time out.  
Request time out.  
Request time out.  
Request time out.  
  
Ping statistics for 192.168.100.100:  
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
  
C:\Users\*****>
```

4. 员工之间可以互访，员工与访客之间无法互访。

在 PC1 上 Ping 无线员工 user2，能够 Ping 通。

```
C:\Users\*****>ping 172.16.30.165
```

```
Pinging 172.16.30.165 with 32 bytes of data:  
Reply from 172.16.30.165: bytes=32 time=175ms TTL=62  
Reply from 172.16.30.165: bytes=32 time=60ms TTL=62  
Reply from 172.16.30.165: bytes=32 time=81ms TTL=62
```

```
Reply from 172.16.30.165: bytes=32 time=102ms TTL=62

Ping statistics for 172.16.30.165:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 60ms, Maximum = 175ms, Average = 104ms

C:\Users\*****>
```

在 PC1 上 Ping 无线访客 guest4，无法 Ping 通。

```
C:\Users\*****>ping 172.16.40.210

Pinging 172.16.40.210 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.

Ping statistics for 172.16.40.210:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\*****>
```

配置文件

CORE 的配置文件

```
#
sysname CORE
#
vlan batch 20 30 40 50 60 1000
#
authentication-profile name p1
dot1x-access-profile d1
free-rule-template default_free_rule
access-domain huawei.com force
#
dhcp enable
#
dhcp snooping enable
#
radius-server template tem_rad
radius-server shared-key cipher %^%#P&%q-,!CC~Ng<^1w;LT:NQj&B.*@a~V.Zi+<pA0H%^%#
```

```
radius-server authentication 192.168.100.10 1812 weight 80
radius-server accounting 192.168.100.10 1813 weight 80
radius-server authorization 192.168.100.10 shared-key
cipher %^%#x`c[=x{ot~7c@T@8fMb'+IGz74$gT6:Kc/DZ1K5Z%^%#
#
acl number 3001
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 192.168.100.3 0
rule 4 permit ip destination 172.16.30.0 0.0.0.255
rule 5 permit ip destination 172.16.50.0 0.0.0.255
rule 6 permit ip destination 172.16.60.0 0.0.0.255
rule 7 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
free-rule 2 source vlan 20
#
vlan 50
dhcp snooping enable
vlan 60
dhcp snooping enable
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
domain huawei.com
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
interface Vlanif20
ip address 192.168.20.20 255.255.255.0
#
interface Vlanif30
ip address 172.16.30.3 255.255.255.0
#
interface Vlanif40
ip address 172.16.40.3 255.255.255.0
#
```

```
interface Vlanif50
ip address 172.16.50.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server dns-list 192.168.100.2
#
interface Vlanif60
ip address 172.16.60.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server dns-list 192.168.100.2
#
interface Vlanif1000
ip address 192.168.100.1 255.255.255.0
#
interface Eth-Trunk1
description con to CORE-AC1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40
mode lacp
#
interface Eth-Trunk2
description con to CORE-AC2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40
mode lacp
#
interface Eth-Trunk10
description con to AGG1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
authentication-profile p1
mode lacp
#
interface Eth-Trunk20
description con to AGG2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 60
authentication-profile p1
```

```
mode lacp
#
interface Eth-Trunk30
description con to Internet
undo portswitch
ip address 172.16.3.1 255.255.255.0
mode lacp
#
interface XGigabitEthernet1/1/0/1
eth-trunk 10
#
interface XGigabitEthernet1/1/0/2
eth-trunk 20
#
interface XGigabitEthernet1/1/0/3
eth-trunk 1
#
interface XGigabitEthernet1/1/0/4
eth-trunk 2
#
interface XGigabitEthernet1/1/0/5
eth-trunk 30
#
interface XGigabitEthernet1/2/0/1
port link-type access
port default vlan 1000
#
interface XGigabitEthernet2/1/0/1
eth-trunk 20
#
interface XGigabitEthernet2/1/0/2
eth-trunk 10
#
interface XGigabitEthernet2/1/0/3
eth-trunk 1
#
interface XGigabitEthernet2/1/0/4
eth-trunk 2
#
interface XGigabitEthernet2/1/0/5
eth-trunk 30
#
dot1x-access-profile name d1
```

```
#  
return
```

CORE-AC1 的配置文件

```
#  
sysname CORE-AC1  
#  
vrrp recover-delay 60  
#  
vlan batch 20 30 40 100  
#  
authentication-profile name p1  
dot1x-access-profile d1  
free-rule-template default_free_rule  
authentication-scheme auth  
accounting-scheme acco  
radius-server tem_rad  
authentication-profile name p2  
mac-access-profile mac1  
portal-access-profile web1  
free-rule-template default_free_rule  
authentication-scheme auth  
accounting-scheme acco  
radius-server tem_rad  
#  
dhcp enable  
#  
dhcp snooping enable  
#  
vlan 30  
    dhcp snooping enable  
vlan 40  
    dhcp snooping enable  
#  
radius-server template tem_rad  
radius-server shared-key cipher %^%#!XJ(Vgk2'$xrU{5H..g"f)`<ELF*e${j}(A>B~f<%%^%#  
radius-server authentication 192.168.100.10 1812 weight 80  
radius-server accounting 192.168.100.10 1813 weight 80  
radius-server authorization 192.168.100.10 shared-key  
cipher %^%#Kc8XWx+M%F{rpFQ:w[v>Ay]0A*xcqV{@CP0}M3<*%^%#  
#  
acl number 3001  
    rule 1 permit ip destination 172.16.3.0 0.0.0.255
```

```
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 192.168.100.3 0
rule 4 permit ip destination 172.16.30.0 0.0.0.255
rule 5 permit ip destination 172.16.50.0 0.0.0.255
rule 6 permit ip destination 172.16.60.0 0.0.0.255
rule 7 deny ip
acl number 3002
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 172.16.40.0 0.0.0.255
rule 4 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
#
web-auth-server tem_portal
server-ip 192.168.100.10
port 50200
shared-key cipher %^%#pn3AB{kK:VEVrIUe=YR2a3^q@l<~,7&Pxc&hP|^;%^%#
url http://192.168.100.10:8080/portal
server-detect interval 100 max-times 5 action log
#
portal-access-profile name web1
web-auth-server tem_portal direct
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
#
interface Vlanif20
ip address 192.168.20.1 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
admin-vrrp vrid 1
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
dhcp select interface
dhcp server excluded-ip-address 192.168.20.2
dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif30
```

```
ip address 172.16.30.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.30.2 172.16.30.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif40
ip address 172.16.40.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.40.2 172.16.40.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif100
ip address 172.16.100.1 255.255.255.0
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40
mode lacp
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/21
eth-trunk 1
#
interface XGigabitEthernet0/0/22
eth-trunk 1
#
ip route-static 0.0.0.0 0.0.0.0 192.168.20.20
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.100.1 peer-ip 172.16.100.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
```



```
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
user-isolate l2
security-profile name sec1
security wpa2 dot1x aes
security-profile name sec2
ssid-profile name ssid1
ssid Employee
ssid-profile name ssid2
ssid Guest
vap-profile name vap1
forward-mode tunnel
service-vlan vlan-id 30
ssid-profile ssid1
security-profile sec1
traffic-profile traff
authentication-profile p1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name vap2
forward-mode tunnel
service-vlan vlan-id 40
ssid-profile ssid2
security-profile sec2
traffic-profile traff
authentication-profile p2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
```

```

vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
master controller
master-redundancy track-vrrp vrid 1 interface Vlanif20
master-redundancy peer-ip ip-address 172.16.100.2 local-ip ip-address 172.16.100.1
psk %^%#5Vh&+;LCyDdLEV1gGJuP}9l(9W&u!+uHt";5T#yM%^%#
#
dot1x-access-profile name d1
#
mac-access-profile name mac1
#
return

```

CORE-AC2 的配置文件

```

#
sysname CORE-AC2
#
vrrp recover-delay 60
#
vlan batch 20 30 40 100
#
authentication-profile name p1
dot1x-access-profile d1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
authentication-profile name p2
mac-access-profile mac1
portal-access-profile web1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#

```

```
dhcp enable
#
dhcp snooping enable
#
vlan 30
    dhcp snooping enable
vlan 40
    dhcp snooping enable
#
radius-server template tem_rad
    radius-server shared-key cipher %^%#!XJ(Vgk2'$xrU{5H..g"f)`<ELF*e${j}(A>B~f<%%^%#
    radius-server authentication 192.168.100.10 1812 weight 80
    radius-server accounting 192.168.100.10 1813 weight 80
    radius-server authorization 192.168.100.10 shared-key
    cipher %^%#Kc8XWx+M%F{rpFQ:w[v>Ay]0A*xcqV{@CP0}M3<*%^%#
#
acl number 3001
    rule 1 permit ip destination 172.16.3.0 0.0.0.255
    rule 2 permit ip destination 192.168.100.2 0
    rule 3 permit ip destination 192.168.100.3 0
    rule 4 permit ip destination 172.16.30.0 0.0.0.255
    rule 5 permit ip destination 172.16.50.0 0.0.0.255
    rule 6 permit ip destination 172.16.60.0 0.0.0.255
    rule 7 deny ip
acl number 3002
    rule 1 permit ip destination 172.16.3.0 0.0.0.255
    rule 2 permit ip destination 192.168.100.2 0
    rule 3 permit ip destination 172.16.40.0 0.0.0.255
    rule 4 deny ip
#
free-rule-template name default_free_rule
    free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
#
web-auth-server tem_portal
    server-ip 192.168.100.10
    port 50200
    shared-key cipher %^%#pn3AB{kK:VEVrIUe=YR2a3^q@|<~,7&Pxc&hP|^;%%^%#
    url http://192.168.100.10:8080/portal
    server-detect interval 100 max-times 5 action log
#
portal-access-profile name web1
    web-auth-server tem_portal direct
#
```

```
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
#
interface Vlanif20
ip address 192.168.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
admin-vrrp vrid 1
dhcp select interface
dhcp server excluded-ip-address 192.168.20.1
dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif30
ip address 172.16.30.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.30.1
dhcp server excluded-ip-address 172.16.30.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif40
ip address 172.16.40.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.40.1
dhcp server excluded-ip-address 172.16.40.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif100
ip address 172.16.100.2 255.255.255.0
#
interface Eth-Trunk2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 40
mode lacp
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 100
#
interface XGigabitEthernet0/0/21
eth-trunk 2
#
interface XGigabitEthernet0/0/22
eth-trunk 2
#
ip route-static 0.0.0.0 0.0.0.0 192.168.20.20
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.100.2 peer-ip 172.16.100.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
user-isolate l2
security-profile name sec1
security wpa2 dot1x aes
security-profile name sec2
ssid-profile name ssid1
ssid Employee
ssid-profile name ssid2
ssid Guest
vap-profile name vap1
forward-mode tunnel
service-vlan vlan-id 30
ssid-profile ssid1
security-profile sec1
traffic-profile traff
authentication-profile p1
```

```

ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name vap2
forward-mode tunnel
service-vlan vlan-id 40
ssid-profile ssid2
security-profile sec2
traffic-profile traff
authentication-profile p2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group1
master controller
master-redundancy track-vrrp vrid 1 interface Vlanif20
master-redundancy peer-ip ip-address 172.16.100.1 local-ip ip-address 172.16.100.2
psk%^%#QKK0'nRL%0U`y32S6bOSB40e=FJE^Lbs7.A]x)QQ%^%#
#
dot1x-access-profile name d1
#
mac-access-profile name mac1
#
return

```

AGG1 的配置文件

```

#
sysname AGG1
#

```

```
vlan batch 20 50
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
#
interface Eth-Trunk10
description connect to CORE
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
l2protocol-tunnel user-defined-protocol 802.1x enable
mode lacp
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
l2protocol-tunnel user-defined-protocol 802.1x enable
mode lacp
port-isolate enable group 1
#
interface 10GE1/0/3
eth-trunk 30
#
interface 10GE2/0/3
eth-trunk 30
#
interface 10GE1/0/1
eth-trunk 10
#
interface 10GE2/0/1
eth-trunk 10
#
return
```

AGG2 的配置文件

```
#
sysname AGG2
#
vlan batch 20 60
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
```

```
#
interface Eth-Trunk20
description connect to CORE
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 60
l2protocol-tunnel user-defined-protocol 802.1x enable
mode lacp
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 60
l2protocol-tunnel user-defined-protocol 802.1x enable
mode lacp
port-isolate enable group 1
#
interface 10GE1/0/3
eth-trunk 40
#
interface 10GE2/0/3
eth-trunk 40
#
interface 10GE1/0/1
eth-trunk 20
#
interface 10GE2/0/1
eth-trunk 20
#
return
```

ACC1 的配置文件

```
#
sysname ACC1
#
vlan batch 20 50
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
```



```
port trunk allow-pass vlan 20 50
l2protocol-tunnel user-defined-protocol 802.1x enable
mode lacp
#
interface 10GE1/0/1
eth-trunk 30
#
interface 10GE1/0/2
eth-trunk 30
#
interface GE1/0/3
port link-type access
port default vlan 50
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type access
port default vlan 20
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
return
```

ACC2 的配置文件

```
#
sysname ACC2
#
vlan batch 20 60
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 0180-c200-0003 group-mac 0100-0000-0002
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 60
l2protocol-tunnel user-defined-protocol 802.1x enable
mode lacp
#
interface 10GE1/0/1
```

```
eth-trunk 40
#
interface 10GE1/0/2
eth-trunk 40
#
interface GE1/0/3
port link-type access
port default vlan 60
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
interface GE1/0/4
port link-type access
port default vlan 20
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
return
```

1.1.2.2.3 独立 AC 方案：汇聚交换机做有线用户网关和认证点，AC 做无线用户网关和认证点，NAC

案例描述

核心层交换机组建集群，作为整个园区网络的核心，实现网络高可靠性和网络大数据量转发。

汇聚层交换机组建堆叠，实现设备级备份的同时，也扩展了设备的端口密度和转发带宽。独立 AC 旁挂式部署，统一管理全网 AP 上线。

本案例中，汇聚交换机作为全网有线的网关，同时汇聚交换机还是全网有线用户的认证点，独立 AC 作为无线用户的网关，以及全网无线用户的认证点，有线和无线用户必须认证成功才能接入网络。其中：

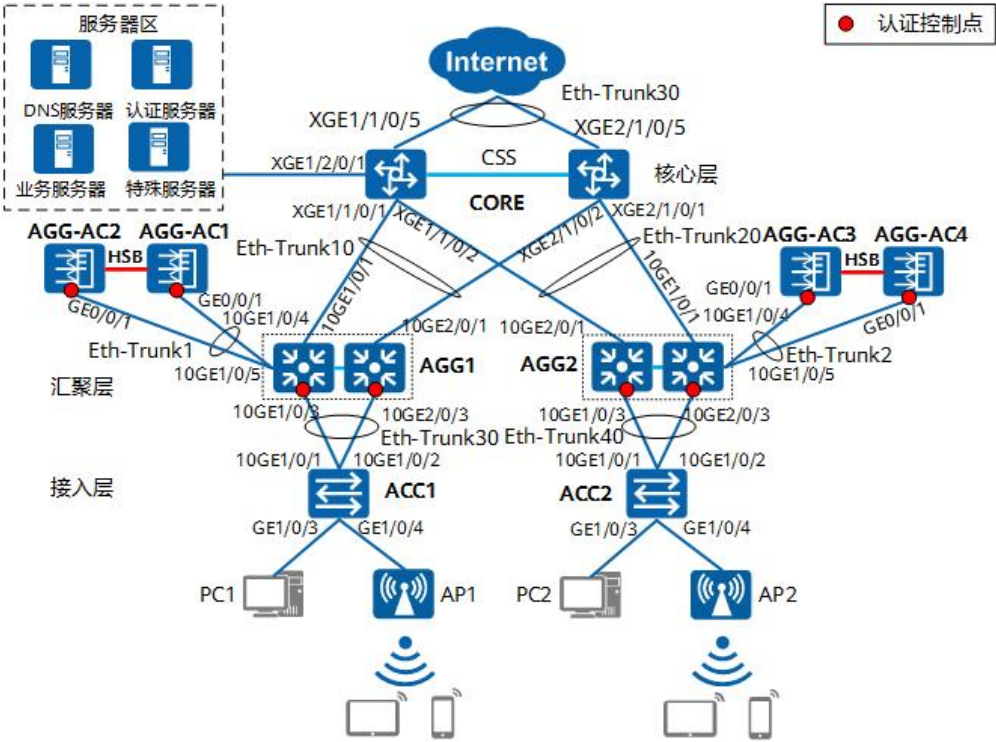
用户角色包括员工（接入方式包括有线和无线）和访客（仅能通过无线接入），员工使用 802.1X 认证，访客使用 MAC 优先的 Portal 认证。

iMaster NCE-Campus 作为认证服务器和用户业务数据源服务器，采用集中式认证服务器部署方案。

iMaster NCE-Campus 对认证成功的用户授权 ACL 策略，用于管控不同角色的用户的网络访问权限。

接入层交换机配置端口隔离，用于管控用户的二层流量。

图 1 汇聚交换机做有线用户的网关和认证点 + 独立 AC 做无线用户的网关和认证点组网图



设备要求和版本

位置	设备要求	本案例使用的设备	本案例使用的版本
认证服务器	—	iMaster NCE–Campus	V300R022C10SPC100
核心层	—	S12700E	V200R022C10
汇聚层	—	S6730–H–V2	V600R022C10
接入层	—	S5735–L–V2	
AC	—	AC9700–M1	V200R022C10
AP	—	AirEngine 8760–X1–PRO	

部署思路

步骤	部署思路
配置基础网络互通	1. 请参见 独立 AC 方案：汇聚交换机做有线用户网关，AC 做无线用户网关 。
配置汇聚交换机和 AC	2. 配置 AAA 参数，包括 RADIUS 服务器模板、AAA 方案和认证域，用于指定交换机与 RADIUS 服务器的对接参数。
	3. 配置免认证资源以及员工和访客认证成功后的网络访问权限。
	4. 配置员工使用 802.1X 认证。

步骤	部署思路
	5. （仅涉及 AC）配置访客使用 MAC 优先的 Portal 认证。
配置接入交换机	6. 配置 802.1X 认证报文二层透明传输功能。
配置 iMaster NCE-Campus	7. 添加与 iMaster NCE-Campus 对接的设备，指定 RADIUS 认证参数和 Portal 认证参数。
	8. 添加用户组和用户帐号。
	9. 开启 MAC 优先的 Portal 认证。
	10. 配置员工和访客认证成功后的网络访问权限。

数据规划

表 1 核心交换机业务数据规划

项目	VLAN ID	网段
连接 Internet 的网段	—	172.16.3.0/24
连接 AGG1 的网段	VLAN 70	172.16.70.0/24
连接 AGG2 的网段	VLAN 80	172.16.80.0/24
连接服务器的网段	VLAN 1000	192.168.100.0/24

表 2 汇聚交换机业务数据规划

设备	项目	VLAN ID	网段
AGG1	AP 的管理 VLAN	VLAN 20	192.168.20.0/24
	无线用户的业务 VLAN	VLAN 30（Employee）	172.16.30.0/24
		VLAN 31（Guest）	172.16.31.0/24
	有线用户的业务 VLAN	VLAN 50	172.16.50.0/24
	连接 CORE 的网段	VLAN 70	172.16.70.0/24
AGG2	AP 的管理 VLAN	VLAN 21	192.168.21.0/24
	无线用户的业务 VLAN	VLAN 40（Employee）	172.16.40.0/24
		VLAN 41（Guest）	172.16.41.0/24
	有线用户的业务 VLAN	VLAN 60	172.16.60.0/24

表 2 汇聚交换机业务数据规划

设备	项目	VLAN ID	网段
	连接 CORE 的网段	VLAN 80	172.16.80.0/24

表 3 AC 无线业务数据规划

项目	员工	访客
流量模板	traff: 用户隔离模式为二层隔离三层互通	
安全模板	sec1: WPA/WPA2-802.1X 认证	sec2: 开放认证（缺省的安全策略）
SSID 模板	ssid1: Employee	ssid2: Guest
AP 组	ap-group1、ap-group2	
域管理模板	domain1	
业务数据转发模式	隧道转发模式	
VAP 模板	vap1	vap2

表 4 汇聚交换机和 AC 认证业务数据规划

项目	数据
AAA 方案	认证方案 auth: RADIUS 认证 计费方案 acco: RADIUS 计费
RADIUS 服务器	RADIUS 服务器模板名称: tem_rad 认证、计费和授权服务器的 IP 地址: 192.168.100.10 认证服务器的端口号: 1812 计费服务器的端口号: 1813 认证计费密钥: YsHsjx_202206 授权密钥: YsHsjx_202206 计费周期: 15 分钟
Portal 服务器	Portal 服务器模板名称: tem_portal Portal 服务器的 IP 地址: 192.168.100.10 端口号: 50200 Portal 服务器共享密钥: YsHsjx_202206 Portal 服务器探测功能: 已开启

表 4 汇聚交换机和 AC 认证业务数据规划

项目	数据
802.1X 接入模板	名称：d1 认证方式：EAP
Portal 接入模板	名称：web1
MAC 接入模板	名称：mac1
免认证资源	DNS 服务器，IP 地址为 192.168.100.2。
用户认证成功后的网络访问权限	员工：Internet、DNS 服务器、业务服务器、其他员工 访客：Internet、DNS 服务器、其他访客 业务服务器的 IP 地址为 192.168.100.3，特殊服务器的 IP 地址为 192.168.100.100，园区出口的 IP 地址为 172.16.3.1。

表 5 iMaster NCE-Campus 业务数据规划

项目	数据
用户帐号	员工：user1/YsHsjx_202206、user2/YsHsjx_202206 访客：guest4/YsHsjx_202206
设备的 IP 地址	AGG1：172.16.70.2 AGG2：172.16.80.2 AGG-AC1：192.168.20.1（备设备 IP 地址：192.168.20.2） AGG-AC3：192.168.21.1（备设备 IP 地址：192.168.21.2）
RADIUS 认证参数	设备系列：Huawei Engine 认证计费密钥：YsHsjx_202206 授权密钥：YsHsjx_202206 实时计费周期(分钟)：15
Portal 认证参数	Portal 密钥：YsHsjx_202206 接入终端 IP 地址列表（AGG-AC1）： 172.16.30.0/24;172.16.31.0/24 接入终端 IP 地址列表（AGG-AC3）： 172.16.40.0/24;172.16.41.0/24

配置注意事项

不建议使用 VLAN 1 作为管理 VLAN 或者业务 VLAN，将各端口从 VLAN 1 中退出。根据实际业务需求透传 VLAN，禁止端口透传所有 VLAN。

直接转发方式下，建议管理 VLAN 和业务 VLAN 分别使用不同的 VLAN，否则可能导致业务不通。例如，业务 VLAN 如果和管理 VLAN 相同，且交换机连接 AP 的端口配置了 PVID 为管理 VLAN，则下行到用户的报文出连接 AP 的交换机时业务 VLAN 会被终结，从而导致业务不通。

直接转发模式下，AP 的业务报文不会进行 CAPWAP 封装，而是直接转发给上层网络，所以需要 AP 与上层网络间的网络加入业务 VLAN，配置 AC 与 AP 间的网络加入管理 VLAN，才能正常传输业务报文和管理报文。

对于主备 AC 上关联的同一 AP，其 WLAN 相关的业务配置必须保持一致（如 WMM 模板、射频模板、射频、流量模板、安全模板、安全策略和 WLAN ID 等都需要保持一致），否则当 AC 的主备状态切换后，无法保证用户业务正常。

主备 AC 的型号和软件版本需完全一致。

在 VRRP 热备份场景下部署 DHCP 服务器时需要注意以下几点：

V200R019C00 及之后版本，开启 DHCP 服务器功能的接口无限制，主 AC 分配 IP 地址，备 AC 不分配，主 AC 的 IP 地址分配信息会同步到备 AC。

主备 AC 上配置的 IP 地址池必须完全一致，配置不一致会导致主备 AC 备份失败。

配置命令 `hsb-service-type dhcp hsb-group group-index`，使 DHCP 业务绑定 HSB 备份组。否则主备 AC 上的 IP 地址分配信息无法备份。

部署步骤

1. 基础网络连通部署，请参见 [独立 AC 方案：汇聚交换机做有线用户网关，AC 做无线用户网关](#)。

配置 CORE 连接 Internet 的网段。

```
<CORE> system-view
[CORE] interface Eth-Trunk 30
[CORE-Eth-Trunk30] mode lacp
[CORE-Eth-Trunk30] description con to Internet
[CORE-Eth-Trunk30] trunkport xgigabitethernet 1/1/0/5
[CORE-Eth-Trunk30] trunkport xgigabitethernet 2/1/0/5
[CORE-Eth-Trunk30] undo portswitch
[CORE-Eth-Trunk30] ip address 172.16.3.1 24
[CORE-Eth-Trunk30] quit
[CORE] ospf
[CORE-ospf-1] area 0
[CORE-ospf-1-area-0.0.0.0] network 172.16.3.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] quit
[CORE-ospf-1] quit
```

2. 配置汇聚交换机的认证业务数据。此处以 AGG1 为例，AGG2 与之类似，不再赘述。

a. 配置 AAA 参数。

配置 RADIUS 服务器模板 “tem_rad”，指定汇聚交换机与 RADIUS 服务器的对接参数，包括 RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号以及认证计费密钥。

```
<AGG1> system-view
[AGG1] radius-server template tem_rad
[AGG1-radius-tem_rad] radius-server authentication 192.168.100.10 1812
[AGG1-radius-tem_rad] radius-server accounting 192.168.100.10 1813
[AGG1-radius-tem_rad] radius-server shared-key cipher YsHsjx_202206
[AGG1-radius-tem_rad] quit
```

配置 RADIUS 授权服务器和授权密钥。

```
[AGG1] radius-server authorization 192.168.100.10 shared-key cipher YsHsjx_202206
```

配置 AAA 认证和计费方案，指定认证和计费方式为 RADIUS，计费周期为 15 分钟。

```
[AGG1] aaa
[AGG1-aaa] authentication-scheme auth
[AGG1-aaa-authen-auth] authentication-mode radius
[AGG1-aaa-authen-auth] quit
[AGG1-aaa] accounting-scheme acco
[AGG1-aaa-accounting-acco] accounting-mode radius
[AGG1-aaa-accounting-acco] accounting realtime 15
[AGG1-aaa-accounting-acco] quit
```

配置认证域 “huawei.com”，在域下绑定 AAA 方案和 RADIUS 服务器模板。

```
[AGG1-aaa] domain huawei.com
[AGG1-aaa-domain-huawei.com] authentication-scheme auth
[AGG1-aaa-domain-huawei.com] accounting-scheme acco
[AGG1-aaa-domain-huawei.com] radius-server tem_rad
[AGG1-aaa-domain-huawei.com] quit
[AGG1-aaa] quit
```

b. 配置免认证资源以及员工认证成功后的网络访问权限。

配置免认证资源：放通到 DNS 服务器的报文和 AP 管理 VLAN 的报文。

```
[AGG1] free-rule-template name default_free_rule
[AGG1-free-rule-default_free_rule] free-rule 1 destination ip 192.168.100.2 mask 32
[AGG1-free-rule-default_free_rule] free-rule 2 source vlan 20
[AGG1-free-rule-default_free_rule] quit
```

配置员工认证成功后的网络访问权限：员工认证成功之后可以访问 Internet、DNS 服务器和业务服务器，员工之间可以互访。

```
[AGG1] acl 3001
[AGG1-acl-adv-3001] rule 1 permit ip destination 172.16.3.0 0.0.0.255 //员工认证成功后可以访问
Internet
```



```
[AGG1-acl-adv-3001] rule 2 permit ip destination 192.168.100.2 0.0.0.0 //员工认证成功后可以访问
DNS 服务器
[AGG1-acl-adv-3001] rule 3 permit ip destination 192.168.100.3 0.0.0.0 //员工认证成功后可以访问业
务服务器
[AGG1-acl-adv-3001] rule 4 permit ip destination 172.16.30.0 0.0.0.255 //允许员工之间互访
[AGG1-acl-adv-3001] rule 5 permit ip destination 172.16.40.0 0.0.0.255 //允许员工之间互访
[AGG1-acl-adv-3001] rule 6 permit ip destination 172.16.50.0 0.0.0.255 //允许员工之间互访
[AGG1-acl-adv-3001] rule 7 permit ip destination 172.16.60.0 0.0.0.255 //允许员工之间互访
[AGG1-acl-adv-3001] rule 8 deny ip destination any
[AGG1-acl-adv-3001] quit
```

c. 配置员工使用 802.1X 认证。

配置 802.1X 接入模板。802.1X 接入模板默认采用 EAP 认证方式，请确保 RADIUS 服务器支持 EAP 协议，否则无法处理 802.1X 认证请求。

```
[AGG1] dot1x-access-profile name d1
[AGG1-dot1x-access-profile-d1] quit
```

配置员工使用的认证模板。

```
[AGG1] authentication-profile name p1
[AGG1-authen-profile-p1] dot1x-access-profile d1
[AGG1-authen-profile-p1] access-domain huawei.com force //配置认证域 huawei.com 为强制认证
域
[AGG1-authen-profile-p1] quit
```

在下行接口配置有线接入的员工使用 802.1X 认证。

```
[AGG1] interface Eth-Trunk 30
[AGG1-Eth-Trunk30] authentication-profile p1
[AGG1-Eth-Trunk30] quit
```

3. 配置 AC 的认证业务数据。此处以 AGG-AC1 为例，其他 AC 的配置与之类似，不再赘述。

a. 配置 AAA 参数。

配置 RADIUS 服务器模板 “tem_rad”，指定 AC 与 RADIUS 服务器的对接参数，包括 RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号以及认证计费密钥。

```
<AGG-AC1> system-view
[AGG-AC1] radius-server template tem_rad
[AGG-AC1-radius-tem_rad] radius-server authentication 192.168.100.10 1812
[AGG-AC1-radius-tem_rad] radius-server accounting 192.168.100.10 1813
[AGG-AC1-radius-tem_rad] radius-server shared-key cipher YsHsjx_202206
[AGG-AC1-radius-tem_rad] quit
```

配置 RADIUS 授权服务器和授权密钥。

```
[AGG-AC1] radius-server authorization 192.168.100.10 shared-key cipher YsHsjx_202206
```

配置 AAA 认证和计费方案，指定认证和计费方式为 RADIUS，计费周期为 15 分钟。

```
[AGG-AC1] aaa
[AGG-AC1-aaa] authentication-scheme auth
[AGG-AC1-aaa-authen-auth] authentication-mode radius
[AGG-AC1-aaa-authen-auth] quit
[AGG-AC1-aaa] accounting-scheme acco
[AGG-AC1-aaa-accounting-acco] accounting-mode radius
[AGG-AC1-aaa-accounting-acco] accounting realtime 15
[AGG-AC1-aaa-accounting-acco] quit
```

b. 配置免认证资源以及用户认证成功后的网络访问权限。

配置免认证资源：放通到 DNS 服务器的报文。

```
[AGG-AC1] free-rule-template name default_free_rule
[AGG-AC1-free-rule-default_free_rule] free-rule 1 destination ip 192.168.100.2 mask 32
[AGG-AC1-free-rule-default_free_rule] quit
```

配置员工认证成功后的网络访问权限：员工认证成功之后可以访问 Internet、DNS 服务器和业务服务器，员工之间可以互访。

说明

对于无线用户，由于 ACL 规则被下发到 AP 上执行，因此必须放通无线用户能访问的所有网段的地址，包括无线用户所在网段的地址，否则无线用户即使能够认证成功，但所有报文在 AP 上均会被丢弃。

```
[AGG-AC1] acl 3001
[AGG-AC1-acl-adv-3001] rule 1 permit ip destination 172.16.3.0 0.0.0.255
[AGG-AC1-acl-adv-3001] rule 2 permit ip destination 192.168.100.2 0.0.0.0
[AGG-AC1-acl-adv-3001] rule 3 permit ip destination 192.168.100.3 0.0.0.0
[AGG-AC1-acl-adv-3001] rule 4 permit ip destination 172.16.30.0 0.0.0.255
[AGG-AC1-acl-adv-3001] rule 5 permit ip destination 172.16.40.0 0.0.0.255
[AGG-AC1-acl-adv-3001] rule 6 permit ip destination 172.16.50.0 0.0.0.255
[AGG-AC1-acl-adv-3001] rule 7 permit ip destination 172.16.60.0 0.0.0.255
[AGG-AC1-acl-adv-3001] rule 8 deny ip destination any
[AGG-AC1-acl-adv-3001] quit
```

配置访客认证成功后的网络访问权限：访客认证成功之后可以访问 Internet 和 DNS 服务器，访客之间可以互访。

```
[AGG-AC1] acl 3002
[AGG-AC1-acl-adv-3002] rule 1 permit ip destination 172.16.3.0 0.0.0.255 //访客认证成功后可以访问 Internet
[AGG-AC1-acl-adv-3002] rule 2 permit ip destination 192.168.100.2 0.0.0.0 //访客认证成功后可以访问 DNS 服务器
[AGG-AC1-acl-adv-3002] rule 3 permit ip destination 172.16.31.0 0.0.0.255 //允许访客之间互访
[AGG-AC1-acl-adv-3002] rule 4 permit ip destination 172.16.41.0 0.0.0.255 //允许访客之间互访
[AGG-AC1-acl-adv-3002] rule 5 deny ip destination any
```

```
[AGG-AC1-acl-adv-3002] quit
```

c. 配置员工使用 802.1X 认证。

配置 802.1X 接入模板。802.1X 接入模板默认采用 EAP 认证方式，请确保 RADIUS 服务器支持 EAP 协议，否则无法处理 802.1X 认证请求。

```
[AGG-AC1] dot1x-access-profile name d1
[AGG-AC1-dot1x-access-profile-d1] quit
```

配置员工使用的认证模板。

```
[AGG-AC1] authentication-profile name p1
[AGG-AC1-authen-profile-p1] dot1x-access-profile d1
[AGG-AC1-authen-profile-p1] free-rule-template default_free_rule
[AGG-AC1-authen-profile-p1] authentication-scheme auth
[AGG-AC1-authen-profile-p1] accounting-scheme acco
[AGG-AC1-authen-profile-p1] radius-server tem_rad
[AGG-AC1-authen-profile-p1] quit
```

配置无线接入的员工的安全策略。

```
[AGG-AC1] wlan
[AGG-AC1-wlan] security-profile name sec1
[AGG-AC1-wlan-sec-prof-sec1] security wpa2 dot1x aes
Warning: This action may cause service interruption. Continue?[Y/N]y
[AGG-AC1-wlan-sec-prof-sec1] quit
```

配置无线接入的员工使用 802.1X 认证。

```
[AGG-AC1-wlan-view] vap-profile name vap1
[AGG-AC1-wlan-vap-prof-vap1] authentication-profile p1
Warning: This action may cause service interruption. Continue?[Y/N]y
[AGG-AC1-wlan-vap-prof-vap1] quit
[AGG-AC1-wlan-view] quit
```

d. 配置访客使用 MAC 优先的 Portal 认证。

配置 Portal 服务器模板。指定 AC 与 Portal 服务器的对接参数，包括 Portal 服务器的 IP 地址、端口号、Portal 共享密钥以及 Portal 页面的 URL。

```
[AGG-AC1] web-auth-server tem_portal
[AGG-AC1-web-auth-server-tem_portal] server-ip 192.168.100.10
[AGG-AC1-web-auth-server-tem_portal] port 50200
[AGG-AC1-web-auth-server-tem_portal] shared-key cipher YsHsjx_202206
[AGG-AC1-web-auth-server-tem_portal] url http://192.168.100.10:8080/portal
[AGG-AC1-web-auth-server-tem_portal] server-detect interval 100 max-times 5 critical-num 0
action log //使能 Portal 服务器探测功能，使管理员能够实时掌握网络中 Portal 服务器的状态，保证在 Portal
服务器故障时，用户仍然能够正常访问网络。探测周期 interval 不能小于 15s，建议配置为 100s
[AGG-AC1-web-auth-server-tem_portal] quit
```

配置 Portal 接入模板。

```
[AGG-AC1] portal-access-profile name web1
[AGG-AC1-portal-access-profile-web1] web-auth-server tem_portal direct
[AGG-AC1-portal-access-profile-web1] quit
```

配置 MAC 接入模板。

```
[AGG-AC1] mac-access-profile name mac1
[AGG-AC1-mac-access-profile-mac1] quit
```

配置访客使用的认证模板。

```
[AGG-AC1] authentication-profile name p2
[AGG-AC1-authen-profile-p2] portal-access-profile web1
[AGG-AC1-authen-profile-p2] mac-access-profile mac1
[AGG-AC1-authen-profile-p2] free-rule-template default_free_rule
[AGG-AC1-authen-profile-p2] authentication-scheme auth
[AGG-AC1-authen-profile-p2] accounting-scheme acco
[AGG-AC1-authen-profile-p2] radius-server tem_rad
[AGG-AC1-authen-profile-p2] quit
```

配置访客使用 MAC 优先的 Portal 认证。

```
[AGG-AC1] wlan
[AGG-AC1-wlan-view] vap-profile name vap2
[AGG-AC1-wlan-vap-prof-vap2] authentication-profile p2
Warning: This action may cause service interruption. Continue?[Y/N]y
[AGG-AC1-wlan-vap-prof-vap2] quit
[AGG-AC1-wlan-view] quit
```

4. 在接入交换机上配置 802.1X 认证报文二层透明传输功能。此处以 ACC1 为例，ACC2 的配置与之类似，不再赘述。

802.1X 认证报文经过的所有接口都需要配置该功能。对于不支持 **bpdu enable** 命令的交换机，接口下仅需配置 **l2protocol-tunnel user-defined-protocol 802.1x enable** 命令即可。

```
<ACC1> system-view
[ACC1] l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 00e0-fc02-0003 group-mac 00e0-fc00-0002
[ACC1] interface Eth-Trunk 30
[ACC1-Eth-Trunk30] l2protocol-tunnel user-defined-protocol 802.1x enable
[ACC1-Eth-Trunk30] quit
[ACC1] interface gigabitethernet 1/0/3
[ACC1-GigabitEthernet1/0/3] l2protocol-tunnel user-defined-protocol 802.1x enable
[ACC1-GigabitEthernet1/0/3] quit
[ACC1] interface gigabitethernet 1/0/4
[ACC1-GigabitEthernet1/0/4] l2protocol-tunnel user-defined-protocol 802.1x enable
[ACC1-GigabitEthernet1/0/4] quit
```

5. 登录 iMaster NCE–Campus，添加与 iMaster NCE–Campus 对接的设备，指定 RADIUS 认证参数和 Portal 认证参数。

选择“准入 > 准入资源 > 准入设备”，单击“创建”，添加设备。

添加 AC 设备的步骤如图 2。汇聚交换机的添加步骤与之类似，相关配置参数见表 6。

图 2 添加 AC 设备

*设备名称:

AC

描述:

*IP地址:

192.168.20.1

备份IP:

192.168.20.2

?

设备系列:

Huawei Engine

▼

RADIUS认证参数:

CoA类型:

默认CoA

No CoA

Port Bounce

Reauth

?

CoA端口:

?

准入设备模板:

...

*认证计费密钥:

.....

?

*确认认证计费密钥:

.....

*授权密钥:

.....

?

*确认授权密钥:

.....

*计费周期(分钟):

15

?

自定义MAC认证密码:

Service-Type属性值设置:

Portal认证参数:

Portal协议:

Huawei Portal(Portal2.0)

Portal在线用户同步:

Portal心跳检验:

认证组件列表:

名称

*Portal密钥:

.....

*确认Portal密钥:

.....

URL密钥:

确认URL密钥:

终端IP地址列表:

172.16.30.0/24
172.16.40.0/24

*Portal认证端口:

2000

Service-Type属性值设置:

HWTACACS认证参数:

表 6 iMaster NCE–Campus 与汇聚交换机和 AC 联动的参数设置

iMaster NCE–Campus 上的参数	汇聚交换机的参数取值	AC 的参数取值
名称、IP 地址	AGG1: 172.16.70.2 AGG2: 172.16.80.2	AGG-AC1: 192.168.20.1 (备设备 IP 地址: 192.168.20.2) AGG-AC3: 192.168.21.1 (备设备 IP 地址: 192.168.21.2)
RADIUS 认证参数	勾选	
设备系列	Huawei Engine	
认证计费密钥	YsHsjx_202206	
授权密钥	YsHsjx_202206	
实时计费周期(分钟)	15	
Portal 认证参数	–	勾选
Portal 协议		Huawei Portal (Portal2.0)
Portal 密钥		YsHsjx_202206

表 6 iMaster NCE–Campus 与汇聚交换机和 AC 联动的参数设置

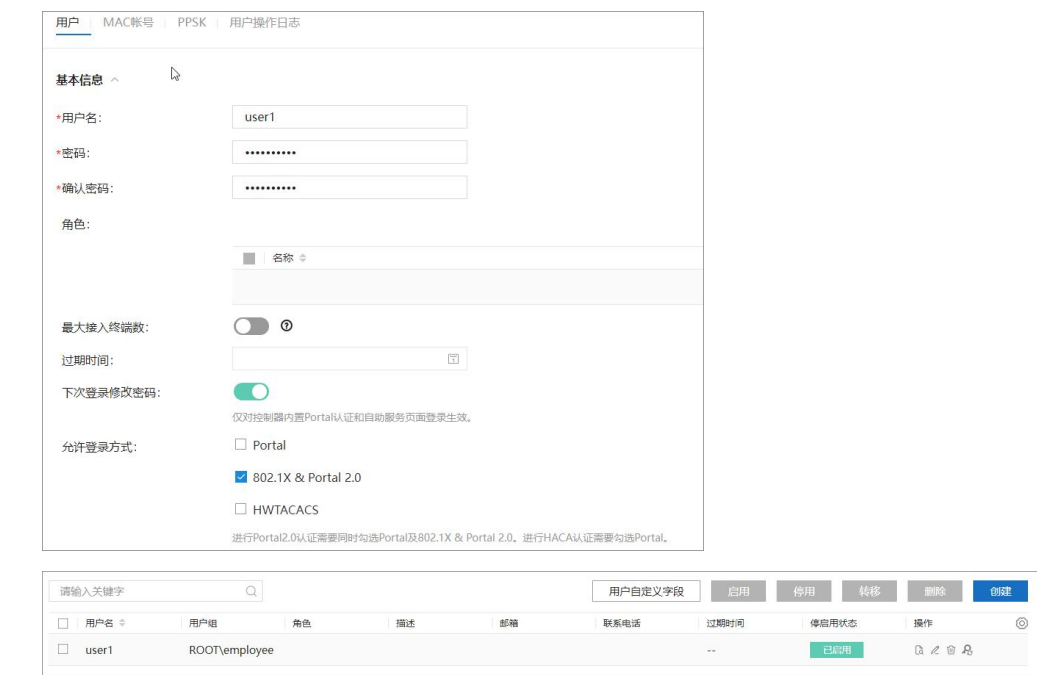
iMaster NCE–Campus 上的参数	汇聚交换机的参数取值	AC 的参数取值
终端 IP 地址列表		AGG-AC1: 172.16.30.0/24;172.16.31.0/24 AGG-AC3: 172.16.40.0/24;172.16.41.0/24
Portal 心跳检验		勾选
Portal 认证端口		2000

6. 添加用户组和用户账号。此处以创建员工组以及员工账号为例，访客组以及访客账号与之类似，不再赘述。

选择“准入 > 准入资源 > 用户管理”。

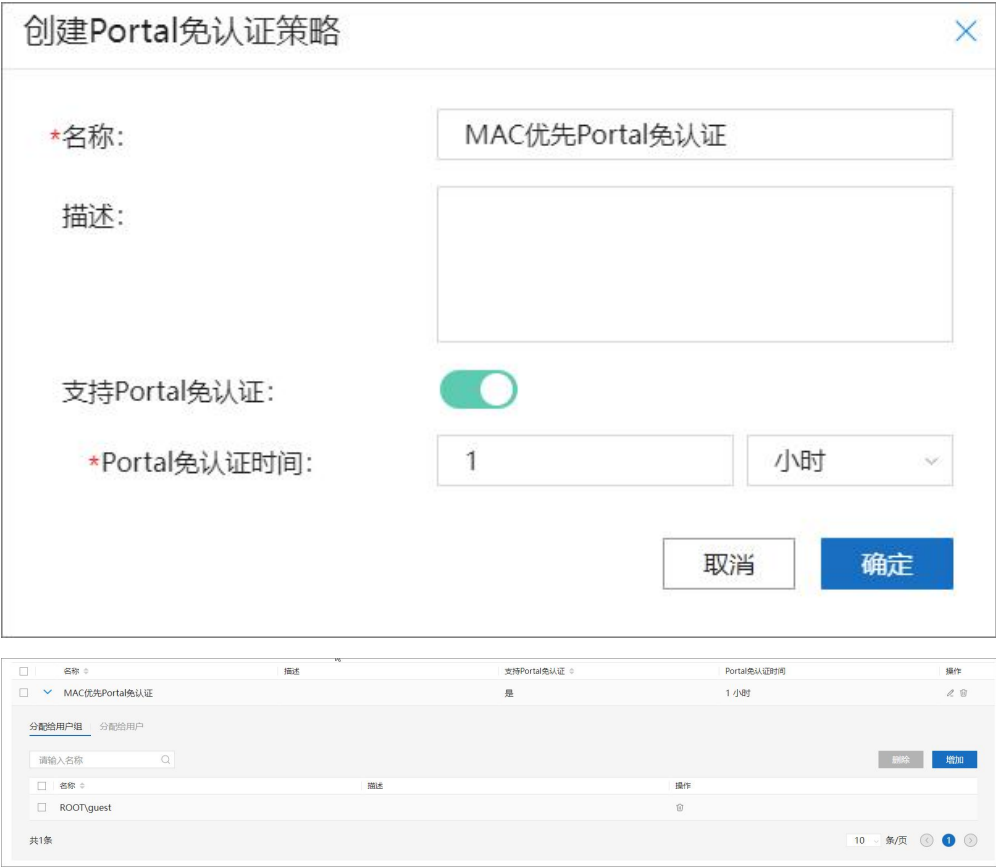
增加名称为“employee”的用户组，并将单个用户“user1”、“user2”添加到该用户组。增加名称为“guest”的用户组，并将单个用户“guest4”添加到该用户组。[图 3](#)为用户 user1 的创建方式，user2 和 guest4 的创建方式与之类似。

图 3 创建用户



7. 启用 MAC 优先的 Portal 认证
- a. 选择“准入 > 准入策略 > 用户在线控制”。设置 Portal 免认证策略，使能支持 Portal 免认证，并设置免认证时间为 1 小时。
 - b. 将 Portal 免认证策略，分配给用户组“guest”。

图 4 设置 Portal 免认证策略



8. 配置员工和访客认证成功后的网络访问权限。

- a. 选择“准入 > 准入策略 > 认证授权”，单击“授权结果”页签，单击“创建”，分别添加员工和访客授权 ACL。

ACL 编号与认证控制设备配置一致。

图 5 添加员工和访客授权 ACL



认证规则

授权规则

授权结果

策略元素

创建

*名称:

ACL3002

描述:

策略

设备管理业务:

VIP用户:

仅支持AP、LSW

ACL:

3002

...

支持AP、LSW、AR，仅支持有ACL编号的ACL，不支持编号为编号段的ACL。

表 7 员工和访客的授权结果

名称	授权参数: ACL 号/AAA 用户组
员工认证后域	3001
访客认证后域	3002

b. 选择“准入 > 准入策略 > 认证授权”，单击“授权规则”，关联授权结果，指定员工和访客认证通过后允许访问的资源。

图 6 为有线员工的授权规则，无线员工和访客授权规则配置方法与之类似，配置参数见表 8。

图 6 有线员工的授权规则

创建授权规则

基本信息

*名称:

员工授权规则-有线

描述:

认证方式:

用户接入认证

MAC认证

设备管理认证

启用Portal-HACA协议:

?

接入方式:

WIFI

有线

蜂窝网络

?

用户信息

用户组信息匹配:

*用户组:

ROOT\employee

...

授权结果

*授权结果:

ACL3001

表 8 员工和访客的授权规则

名称	授权条件：用户组	授权结果
员工授权规则-有线	employee	ACL3001
员工授权规则-无线	employee	ACL3001
访客授权规则	guest	ACL3002

预期结果

1. 员工和访客分别选择正确的接入方式，并输入正确的用户名和密码之后，可以认证成功并接入网络。
2. 员工或访客认证成功之后，可以访问免认证资源，也可以访问认证后域资源，但无法访问认证后域禁止访问的资源。
3. 员工之间可以互访，员工与访客之间无法互访。

说明

访客第一次接入网络，通过移动终端连接无线局域网 **Guest**，在浏览器中输入 **http://192.168.100.10:8080/portal**，进行 Portal 认证，在弹出的重定向页面中输入用户名和密码即可认证成功。访客断开网络，如果在 1 小时内重新接入 **Guest**，能够触发 MAC 优先的 Portal 认证，可以直接接入网络，无需再次输入用户名和密码。

结果验证

1. 员工和访客分别选择正确的接入方式，并输入正确的用户名和密码之后，可以认证成功并接入网络。

在 PC1 上输入正确的用户名和密码，再通过 **Employee** 和 **Guest** 分别接入一个无线用户，然后在 AGG1 和 AGG-AC1 上执行 **display access-user** 命令查看在线用户信息。此时可以发现 user1、user2 和 guest4 均处于认证成功状态（**Success**）。

```
[AGG1] display access-user
-----
UserID  Username      IP address      MAC              Status
-----
32792   user1             172.16.50.216   00e0-fc12-3344   Success
-----
Total: 1, printed: 1
```

```
[AGG-AC1] display access-user
```

```
-----
UserID  Username      IP address      MAC             Status
-----
16434  user2        172.16.30.97    00e0-fc12-3366  Success
32809  guest4       172.16.31.165   00e0-fc12-3355  Success
-----
```

```
Total: 2, printed: 2
```

在 AGG1 上执行 **display access-user username user1 detail** 命令，可以查看 user1 的详细认证信息和授权信息。

```
[AGG1] display access-user username user1 detail
```

```
Basic:
```

```
User ID           : 32792
User name          : user1
Domain-name        : huawei.com
User MAC           : 00e0-fc12-3344
User IP address    : 172.16.50.216
User vpn-instance  : -
User IPv6 address   : FE80::E9AA:9FE9:95F9:C499
User IPv6 link local address : FE80::E9AA:9FE9:95F9:C499
User access Interface : Eth-Trunk10
User vlan event     : Success
QinQVlan/UserVlan   : 0/50
User vlan source    : user request
User access time     : 2019/12/30 10:01:33
User accounting session ID : AGG000180000000050ef****0200018
User access type     : 802.1x
Terminal Device Type : Data Terminal
Dynamic ACL ID(Effective) : 3001
```

```
AAA:
```

```
User authentication type : 802.1x authentication
Current authentication method : RADIUS
Current authorization method : -
Current accounting method : RADIUS
```

```
-----
Total: 1, printed: 1
```

在 AGG-AC1 上执行 **display access-user username user2 detail** 和 **display access-user username guest4 detail** 命令，可以查看 user2 和 guest4 的详细认证信息和授权信息。

[AGG-AC1] **display access-user username user2 detail**

Basic:

User ID : 16434
User name : user2
User MAC : 00e0-fc12-3366
User IP address : 172.16.30.97
User vpn-instance : -
User IPv6 address : -
User access Interface : Wlan-Dbss17498
User vlan event : Success
QinQVlan/UserVlan : 0/30
User vlan source : user request
User access time : 2019/12/30 10:02:55
User accounting session ID : AC2000000000000308d****0100032
User accounting mult session ID : AC853DA6A42038CADA5E441A5E09C****B2526E4
User access type : 802.1x
AP name : area_1
Radio ID : 1
AP MAC : 00e0-fc12-4400
SSID : Employee
Online time : 115(s)
Dynamic ACL ID(Effective) : 3001
User Group Priority : 0

AAA:

User authentication type : 802.1x authentication
Current authentication method : RADIUS
Current authorization method : -
Current accounting method : RADIUS

Total: 1, printed: 1

[AGG-AC1] **display access-user username guest4 detail**

Basic:

User ID : 32809
User name : guest4
User MAC : 00e0-fc12-3355
User IP address : 172.16.31.165

```

User vpn-instance      : -
User IPv6 address      : -
User access Interface  : Wlan-Dbss17497
User vlan event        : Success
QinQVlan/UserVlan     : 0/31
User vlan source       : user request
User access time       : 2019/12/30 09:52:57
User accounting session ID : AC200000000000031dd****0200029
User accounting mult session ID : AC853DA6A42064B0A6A3F913FFFFFF****FFFFFFF
User access type       : WEB
AP name                : area_1
Radio ID               : 0
AP MAC                 : 00e0-fc12-4400
SSID                   : Guest
Online time            : 764(s)
Web-server IP address  : 192.168.100.10
Dynamic ACL ID(Effective) : 3002
User Group Priority     : 0

```

AAA:

```

User authentication type : WEB authentication
Current authentication method : RADIUS
Current authorization method : -
Current accounting method : RADIUS

```

Total: 1, printed: 1

2. 员工或访客认证成功之后，可以访问免认证资源，也可以访问认证后域资源，但无法访问认证后域禁止访问的资源。此处仅以有线员工为例进行验证。

在 PC1 上 Ping 免认证资源（DNS 服务器：192.168.100.2），能够 Ping 通。

```

C:\Users\*****>ping 192.168.100.2

Pinging 192.168.100.2 with 32 bytes of data:
Reply from 192.168.100.2: bytes=32 time=1ms TTL=252
Reply from 192.168.100.2: bytes=32 time=1ms TTL=252
Reply from 192.168.100.2: bytes=32 time=1ms TTL=252
Reply from 192.168.100.2: bytes=32 time=1ms TTL=252

Ping statistics for 192.168.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

```

```
C:\Users\*****>
```

在 PC1 上 Ping 业务服务器（192.168.100.3），能够 Ping 通。

```
C:\Users\*****>ping 192.168.100.3
```

Pinging 192.168.100.3 with 32 bytes of data:

Reply from 192.168.100.3: bytes=32 time=1ms TTL=252

Reply from 192.168.100.3: bytes=32 time=1ms TTL=252

Reply from 192.168.100.3: bytes=32 time=1ms TTL=252

Reply from 192.168.100.3: bytes=32 time=1ms TTL=252

Ping statistics for 192.168.100.3:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 1ms, Maximum = 1ms, Average = 1ms

```
C:\Users\*****>
```

在 PC1 上 Ping 认证后域（园区出口：172.16.3.1），能够 Ping 通。

```
C:\Users\*****>ping 172.16.3.1
```

Pinging 172.16.3.1 with 32 bytes of data:

Reply from 172.16.3.1: bytes=32 time<1ms TTL=253

Reply from 172.16.3.1: bytes=32 time<1ms TTL=253

Reply from 172.16.3.1: bytes=32 time<1ms TTL=253

Reply from 172.16.3.1: bytes=32 time<1ms TTL=253

Ping statistics for 172.16.3.1:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

```
C:\Users\*****>
```

在 PC1 上 Ping 认证后域禁止访问的资源（特殊服务器：192.168.100.100），无法 Ping 通。

```
C:\Users\*****>ping 192.168.100.100
```

Pinging 192.168.100.100 with 32 bytes of data:

Request time out.

Request time out.

Request time out.

Request time out.

```
Ping statistics for 192.168.100.100:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\*****>
```

3. 员工之间可以互访，员工与访客之间无法互访。

在 PC1 上 Ping 无线员工 user2，能够 Ping 通。

```
C:\Users\*****>ping 172.16.30.97

Pinging 172.16.30.97 with 32 bytes of data:
Reply from 172.16.30.97: bytes=32 time=131ms TTL=62
Reply from 172.16.30.97: bytes=32 time=39ms TTL=62
Reply from 172.16.30.97: bytes=32 time=169ms TTL=62
Reply from 172.16.30.97: bytes=32 time=93ms TTL=62

Ping statistics for 172.16.30.97:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 39ms, Maximum = 169ms, Average = 108ms

C:\Users\*****>
```

在 PC1 上 Ping 无线访客 guest4，无法 Ping 通。

```
C:\Users\*****>ping 172.16.31.165

Pinging 172.16.31.165 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.

Ping statistics for 172.16.31.165:
  Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\*****>
```

配置文件

CORE 的配置文件

```
#
sysname CORE
```

```
#
vlan batch 70 80 1000
#
interface Vlanif70
 ip address 172.16.70.1 255.255.255.0
#
interface Vlanif80
 ip address 172.16.80.1 255.255.255.0
#
interface Vlanif1000
 ip address 192.168.100.1 255.255.255.0
#
interface Eth-Trunk10
 description connect to AGG1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 70
 mode lacp
#
interface Eth-Trunk20
 description connect to AGG2
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 80
 mode lacp
#
interface Eth-Trunk30
 undo portswitch
 description connect to Internet
 ip address 172.16.3.1 255.255.255.0
 mode lacp
#
interface XGigabitEthernet1/1/0/1
 eth-trunk 10
#
interface XGigabitEthernet1/1/0/2
 eth-trunk 20
#
interface XGigabitEthernet1/1/0/5
 eth-trunk 30
#
interface XGigabitEthernet1/1/0/10
 mad detect mode direct
```



```
#
interface XGigabitEthernet1/2/0/1
 port link-type access
 port default vlan 1000
#
interface XGigabitEthernet2/1/0/1
 eth-trunk 20
#
interface XGigabitEthernet2/1/0/2
 eth-trunk 10
#
interface XGigabitEthernet2/1/0/5
 eth-trunk 30
#
interface XGigabitEthernet2/1/0/10
 mad detect mode direct
#
ospf 1 router-id 1.1.1.1
 area 0.0.0.0
  network 172.16.3.0 0.0.0.255
  network 172.16.70.0 0.0.0.255
  network 172.16.80.0 0.0.0.255
  network 192.168.100.0 0.0.0.255
#
return
```

AGG1 的配置文件

```
#
sysname AGG1
#
vlan batch 20 30 to 31 50 70
#
authentication-profile name p1
 dot1x-access-profile d1
 free-rule-template default_free_rule
 access-domain huawei.com force
#
dhcp enable
#
dhcp snooping enable
#
radius-server template tem_rad
 radius-server shared-key cipher %^%#~jZ]F$6t6!/K%~9Ow$"Vb,+LFnrEI>q<\'1!^JD7%^%#
```

```
radius-server authentication 192.168.100.10 1812 weight 80
radius-server accounting 192.168.100.10 1813 weight 80
radius-server authorization 192.168.100.10 shared-key
cipher %^%#GH(%~#au`G.f/IA~"P%l]^Z4L*yVj"/w"2uWP\'%^%#
#
acl number 3001
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 192.168.100.3 0
rule 4 permit ip destination 172.16.30.0 0.0.0.255
rule 5 permit ip destination 172.16.40.0 0.0.0.255
rule 6 permit ip destination 172.16.50.0 0.0.0.255
rule 7 permit ip destination 172.16.60.0 0.0.0.255
rule 8 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
free-rule 2 source vlan 20
#
vlan 50
dhcp snooping enable
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
domain huawei.com
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
interface Vlanif20
ip address 192.168.20.20 255.255.255.0
#
interface Vlanif30
ip address 172.16.30.3 255.255.255.0
#
interface Vlanif31
ip address 172.16.31.3 255.255.255.0
#
interface Vlanif50
```

```
ip address 172.16.50.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server dns-list 192.168.100.2
#
interface Vlanif70
ip address 172.16.70.2 255.255.255.0
#
interface Eth-Trunk1
description con to AC
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 to 31
mode lacp
#
interface Eth-Trunk10
description connect to CORE
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 70
mode lacp
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
authentication-profile p1
mode lacp
#
interface 10GigabitEthernet1/0/3
eth-trunk 30
#
interface 10GigabitEthernet1/0/4
eth-trunk 1
#
interface 10GigabitEthernet1/0/10
mad detect mode direct
#
interface 10GigabitEthernet1/0/5
eth-trunk 1
#
interface 10GigabitEthernet2/0/3
eth-trunk 30
```

```
#
interface 10GigabitEthernet1/0/1
 eth-trunk 10
#
interface 10GigabitEthernet2/0/1
 eth-trunk 10
#
interface 10GigabitEthernet2/0/10
 mad detect mode direct
#
ospf 1 router-id 2.2.2.2
 area 0.0.0.0
  network 172.16.30.0 0.0.0.255
  network 172.16.31.0 0.0.0.255
  network 172.16.50.0 0.0.0.255
  network 172.16.70.0 0.0.0.255
#
dot1x-access-profile name d1
#
return
```

AGG2 的配置文件

```
#
sysname AGG2
#
vlan batch 21 40 to 41 60 80
#
authentication-profile name p1
 dot1x-access-profile d1
 free-rule-template default_free_rule
 access-domain huawei.com force
#
dhcp enable
#
dhcp snooping enable
#
radius-server template tem_rad
 radius-server shared-key cipher %^%#~jZ}F$6t6/!K%~9Ow$"Vb,+LFnrEI>q<\!^JD7%^%#
 radius-server authentication 192.168.100.10 1812 weight 80
 radius-server accounting 192.168.100.10 1813 weight 80
 radius-server authorization 192.168.100.10 shared-key
 cipher %^%#GH(%~#au`G.f/IA~"P%]]^Z4L*yVj"/w"2uWP\'%^%#
#
```

```
acl number 3001
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 192.168.100.3 0
rule 4 permit ip destination 172.16.30.0 0.0.0.255
rule 5 permit ip destination 172.16.40.0 0.0.0.255
rule 6 permit ip destination 172.16.50.0 0.0.0.255
rule 7 permit ip destination 172.16.60.0 0.0.0.255
rule 8 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
free-rule 2 source vlan 21
#
vlan 60
dhcp snooping enable
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
domain huawei.com
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
interface Vlanif21
ip address 192.168.21.20 255.255.255.0
#
interface Vlanif40
ip address 172.16.40.3 255.255.255.0
#
interface Vlanif41
ip address 172.16.41.3 255.255.255.0
#
interface Vlanif60
ip address 172.16.60.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server dns-list 192.168.100.2
#
```

```
interface Vlanif80
ip address 172.16.80.2 255.255.255.0
#
interface Eth-Trunk2
description con to AC
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 40 to 41
mode lacp
#
interface Eth-Trunk10
description connect to CORE
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 80
mode lacp
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 60
authentication-profile p1
mode lacp
#
interface 10GigabitEthernet1/0/3
eth-trunk 40
#
interface 10GigabitEthernet1/0/4
eth-trunk 2
#
interface 10GigabitEthernet1/0/5
eth-trunk 2
#
interface 10GigabitEthernet1/0/10
mad detect mode direct
#
interface 10GigabitEthernet2/0/3
eth-trunk 40
#
interface 10GigabitEthernet2/0/10
mad detect mode direct
#
interface 10GigabitEthernet1/0/1
```

```
eth-trunk 20
#
interface 10GigabitEthernet2/0/1
eth-trunk 20
#
ospf 1 router-id 7.7.7.7
area 0.0.0.0
network 172.16.40.0 0.0.0.255
network 172.16.41.0 0.0.0.255
network 172.16.60.0 0.0.0.255
network 172.16.80.0 0.0.0.255
#
dot1x-access-profile name d1
#
return
```

AGG-AC1 的配置文件

```
#
sysname AGG-AC1
#
vrrp recover-delay 60
#
vlan batch 20 30 to 31 200
#
authentication-profile name p1
dot1x-access-profile d1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
authentication-profile name p2
mac-access-profile mac1
portal-access-profile web1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
dhcp enable
#
dhcp snooping enable
#
vlan 30
```

```
dhcp snooping enable
vlan 31
dhcp snooping enable
#
radius-server template tem_rad
radius-server shared-key cipher %^%#}q]hRf*~x5o]fjF<R#EEFXy0MI=L4)Tw]%+Nk)ET%^%#
radius-server authentication 192.168.100.10 1812 weight 80
radius-server accounting 192.168.100.10 1813 weight 80
radius-server authorization 192.168.100.10 shared-key cipher %^%#j7U//99!v(-n+\HtWgD60K@2IFc-
I$3F)3K]ar/O%^%#
#
acl number 3001
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 192.168.100.3 0
rule 4 permit ip destination 172.16.30.0 0.0.0.255
rule 5 permit ip destination 172.16.40.0 0.0.0.255
rule 6 permit ip destination 172.16.50.0 0.0.0.255
rule 7 permit ip destination 172.16.60.0 0.0.0.255
rule 8 deny ip
acl number 3002
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 172.16.31.0 0.0.0.255
rule 4 permit ip destination 172.16.41.0 0.0.0.255
rule 5 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
#
web-auth-server tem_portal
server-ip 192.168.100.10
port 50200
shared-key cipher %^%#@Un19tIB1FQ\p%US,S54+gEh'8@qzSQ&BGXJ$niV%^%#
url http://192.168.100.10:8080/portal
server-detect interval 100 max-times 5 action log
#
portal-access-profile name web1
web-auth-server tem_portal direct
#
aaa
authentication-scheme auth
authentication-mode radius
```



```
accounting-scheme acco
accounting-mode radius
accounting realtime 15
#
interface Vlanif20
ip address 192.168.20.1 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
admin-vrrp vrid 1
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
dhcp select interface
dhcp server excluded-ip-address 192.168.20.2
dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif30
ip address 172.16.30.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.30.2 172.16.30.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif31
ip address 172.16.31.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.31.2 172.16.31.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif200
ip address 172.16.200.1 255.255.255.0
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 to 31
mode lacp
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 200
#
ospf 1 router-id 3.3.3.3
area 0.0.0.0
network 172.16.30.0 0.0.0.255
network 172.16.31.0 0.0.0.255
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.200.1 peer-ip 172.16.200.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
user-isolate l2
security-profile name sec1
security wpa2 dot1x aes
security-profile name sec2
ssid-profile name ssid1
ssid Employee
ssid-profile name ssid2
ssid Guest
vap-profile name vap1
forward-mode tunnel
service-vlan vlan-id 30
ssid-profile ssid1
security-profile sec1
traffic-profile traff
authentication-profile p1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
```

```
vap-profile name vap2
forward-mode tunnel
service-vlan vlan-id 31
ssid-profile ssid2
security-profile sec2
traffic-profile traff
authentication-profile p2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
provision-ap
#
dot1x-access-profile name d1
#
mac-access-profile name mac1
#
return
```

AGG-AC2 的配置文件

```
#
sysname AGG-AC2
#
vrrp recover-delay 60
#
vlan batch 20 30 to 31 200
#
authentication-profile name p1
dot1x-access-profile d1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
```

```
radius-server tem_rad
authentication-profile name p2
mac-access-profile mac1
portal-access-profile web1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
dhcp enable
#
dhcp snooping enable
#
vlan 30
  dhcp snooping enable
vlan 31
  dhcp snooping enable
#
radius-server template tem_rad
radius-server shared-key cipher %^%#}q]hRf*~x5o]fjF<R#EEFXy0MI=L4)Tw]%^+Nk)ET%^%#
radius-server authentication 192.168.100.10 1812 weight 80
radius-server accounting 192.168.100.10 1813 weight 80
radius-server authorization 192.168.100.10 shared-key cipher %^%#j7U//99!v(-n+\HtWgD60K@2IFc-
I$3F)3K]ar/O%^%#
#
acl number 3001
  rule 1 permit ip destination 172.16.3.0 0.0.0.255
  rule 2 permit ip destination 192.168.100.2 0
  rule 3 permit ip destination 192.168.100.3 0
  rule 4 permit ip destination 172.16.30.0 0.0.0.255
  rule 5 permit ip destination 172.16.40.0 0.0.0.255
  rule 6 permit ip destination 172.16.50.0 0.0.0.255
  rule 7 permit ip destination 172.16.60.0 0.0.0.255
  rule 8 deny ip
acl number 3002
  rule 1 permit ip destination 172.16.3.0 0.0.0.255
  rule 2 permit ip destination 192.168.100.2 0
  rule 3 permit ip destination 172.16.31.0 0.0.0.255
  rule 4 permit ip destination 172.16.41.0 0.0.0.255
  rule 5 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
```

```
#
web-auth-server tem_portal
server-ip 192.168.100.10
port 50200
shared-key cipher %^%#@Un19tIB1FQ\p%US,S54+gEh'8@qzSQ&BGXJ$niV%^%#
url http://192.168.100.10:8080/portal
server-detect interval 100 max-times 5 action log
#
portal-access-profile name web1
web-auth-server tem_portal direct
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
#
interface Vlanif20
ip address 192.168.20.2 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.20.3
admin-vrrp vrid 1
dhcp select interface
dhcp server excluded-ip-address 192.168.20.1
dhcp server excluded-ip-address 192.168.20.20
#
interface Vlanif30
ip address 172.16.30.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.30.1
dhcp server excluded-ip-address 172.16.30.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif31
ip address 172.16.31.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.31.1
dhcp server excluded-ip-address 172.16.31.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif200
```

```
ip address 172.16.200.2 255.255.255.0
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30 to 31
mode lacp
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 200
#
ospf 1 router-id 3.3.3.3
area 0.0.0.0
network 172.16.30.0 0.0.0.255
network 172.16.31.0 0.0.0.255
#
capwap source interface vlanif20
#
hsb-service 0
service-ip-port local-ip 172.16.200.2 peer-ip 172.16.200.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif20
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
user-isolate l2
security-profile name sec1
security wpa2 dot1x aes
security-profile name sec2
```

```
ssid-profile name ssid1
ssid Employee
ssid-profile name ssid2
ssid Guest
vap-profile name vap1
forward-mode tunnel
service-vlan vlan-id 30
ssid-profile ssid1
security-profile sec1
traffic-profile traff
authentication-profile p1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name vap2
forward-mode tunnel
service-vlan vlan-id 31
ssid-profile ssid2
security-profile sec2
traffic-profile traff
authentication-profile p2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group1
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 1 type-id 30 ap-mac 00e0-fc12-6660 ap-sn 2102355547W0E3000316
ap-name area_1
ap-group ap-group1
provision-ap
#
dot1x-access-profile name d1
#
mac-access-profile name mac1
#
```

```
return
```

AGG-AC3 的配置文件

```
#
sysname AGG-AC3
#
vrrp recover-delay 60
#
vlan batch 21 40 to 41 201
#
authentication-profile name p1
dot1x-access-profile d1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
authentication-profile name p2
mac-access-profile mac1
portal-access-profile web1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
dhcp enable
#
dhcp snooping enable
#
vlan 40
dhcp snooping enable
vlan 41
dhcp snooping enable
#
radius-server template tem_rad
radius-server shared-key cipher %^%#}q]hRf*~x5o]fjF<R#EEFXy0MI=L4)Tw]%+Nk)ET%^%#
radius-server authentication 192.168.100.10 1812 weight 80
radius-server accounting 192.168.100.10 1813 weight 80
radius-server authorization 192.168.100.10 shared-key cipher %^%#j7U//99!v(-n+\\HtWgD60K@2IFc-
I$3F)3K]ar/O%^%#
#
acl number 3001
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
```



```
rule 3 permit ip destination 192.168.100.3 0
rule 4 permit ip destination 172.16.30.0 0.0.0.255
rule 5 permit ip destination 172.16.40.0 0.0.0.255
rule 6 permit ip destination 172.16.50.0 0.0.0.255
rule 7 permit ip destination 172.16.60.0 0.0.0.255
rule 8 deny ip
acl number 3002
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 172.16.31.0 0.0.0.255
rule 4 permit ip destination 172.16.41.0 0.0.0.255
rule 5 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
#
web-auth-server tem_portal
server-ip 192.168.100.10
port 50200
shared-key cipher %^%#@Un19tIB1FQ\p%US,S54+gEh'8@qzSQ&BGXJ$niV%^%#
url http://192.168.100.10:8080/portal
server-detect interval 100 max-times 5 action log
#
portal-access-profile name web1
web-auth-server tem_portal direct
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
#
interface Vlanif21
ip address 192.168.21.1 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.21.3
admin-vrrp vrid 1
vrrp vrid 1 priority 120
vrrp vrid 1 preempt-mode timer delay 1200
dhcp select interface
dhcp server excluded-ip-address 192.168.21.2
dhcp server excluded-ip-address 192.168.21.20
#
```

```
interface Vlanif40
ip address 172.16.40.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.40.2 172.16.40.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif41
ip address 172.16.41.1 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.41.2 172.16.41.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif201
ip address 172.16.201.1 255.255.255.0
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 40 to 41
mode lacp
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 201
#
ospf 1 router-id 3.3.3.3
area 0.0.0.0
network 172.16.40.0 0.0.0.255
network 172.16.41.0 0.0.0.255
#
capwap source interface vlanif21
#
hsb-service 0
service-ip-port local-ip 172.16.201.1 peer-ip 172.16.201.2 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif21
```

```
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
user-isolate l2
security-profile name sec1
security wpa2 dot1x aes
security-profile name sec2
ssid-profile name ssid1
ssid Employee
ssid-profile name ssid2
ssid Guest
vap-profile name vap1
forward-mode tunnel
service-vlan vlan-id 40
ssid-profile ssid1
security-profile sec1
traffic-profile traff
authentication-profile p1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
vap-profile name vap2
forward-mode tunnel
service-vlan vlan-id 41
ssid-profile ssid2
security-profile sec2
traffic-profile traff
authentication-profile p2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group2
regulatory-domain-profile domain1
radio 0
```

```

vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group2
provision-ap
#
dot1x-access-profile name d1
#
mac-access-profile name mac1
#
return
```

AGG-AC4 的配置文件

```

#
sysname AGG-AC4
#
vrrp recover-delay 60
#
vlan batch 21 40 to 41 201
#
authentication-profile name p1
dot1x-access-profile d1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
authentication-profile name p2
mac-access-profile mac1
portal-access-profile web1
free-rule-template default_free_rule
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
dhcp enable
#
dhcp snooping enable
#
vlan 40
```

```
dhcp snooping enable
vlan 41
dhcp snooping enable
#
radius-server template tem_rad
radius-server shared-key cipher %^%#}q]hRf*~x5o]fjF<R#EEFXy0MI=L4)Tw]%+Nk)ET%^%#
radius-server authentication 192.168.100.10 1812 weight 80
radius-server accounting 192.168.100.10 1813 weight 80
radius-server authorization 192.168.100.10 shared-key cipher %^%#j7U//99!v(-n+\HtWgD60K@2IFc-
I$3F)3K]ar/O%^%#
#
acl number 3001
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 192.168.100.3 0
rule 4 permit ip destination 172.16.30.0 0.0.0.255
rule 5 permit ip destination 172.16.40.0 0.0.0.255
rule 6 permit ip destination 172.16.50.0 0.0.0.255
rule 7 permit ip destination 172.16.60.0 0.0.0.255
rule 8 deny ip
acl number 3002
rule 1 permit ip destination 172.16.3.0 0.0.0.255
rule 2 permit ip destination 192.168.100.2 0
rule 3 permit ip destination 172.16.31.0 0.0.0.255
rule 4 permit ip destination 172.16.41.0 0.0.0.255
rule 5 deny ip
#
free-rule-template name default_free_rule
free-rule 1 destination ip 192.168.100.2 mask 255.255.255.255
#
web-auth-server tem_portal
server-ip 192.168.100.10
port 50200
shared-key cipher %^%#@Un19tIB1FQ\p%US,S54+gEh'8@qzSQ&BGXJ$niV%^%#
url http://192.168.100.10:8080/portal
server-detect interval 100 max-times 5 action log
#
portal-access-profile name web1
web-auth-server tem_portal direct
#
aaa
authentication-scheme auth
authentication-mode radius
```

```
accounting-scheme acco
accounting-mode radius
accounting realtime 15
#
interface Vlanif21
ip address 192.168.21.2 255.255.255.0
vrrp vrid 1 virtual-ip 192.168.21.3
admin-vrrp vrid 1
dhcp select interface
dhcp server excluded-ip-address 192.168.21.1
dhcp server excluded-ip-address 192.168.21.20
#
interface Vlanif40
ip address 172.16.40.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.40.1
dhcp server excluded-ip-address 172.16.40.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif41
ip address 172.16.41.2 255.255.255.0
arp-proxy inner-sub-vlan-proxy enable
dhcp select interface
dhcp server excluded-ip-address 172.16.41.1
dhcp server excluded-ip-address 172.16.41.3
dhcp server dns-list 192.168.100.2
#
interface Vlanif201
ip address 172.16.201.2 255.255.255.0
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 40 to 41
mode lacp
#
interface GigabitEthernet0/0/1
eth-trunk 1
#
interface GigabitEthernet0/0/2
port link-type trunk
undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 201
#
ospf 1 router-id 3.3.3.3
area 0.0.0.0
network 172.16.40.0 0.0.0.255
network 172.16.41.0 0.0.0.255
#
capwap source interface vlanif21
#
hsb-service 0
service-ip-port local-ip 172.16.201.2 peer-ip 172.16.201.1 local-data-port 10241 peer-data-port 10241
#
hsb-group 0
track vrrp vrid 1 interface Vlanif21
bind-service 0
hsb enable
#
hsb-service-type access-user hsb-group 0
#
hsb-service-type dhcp hsb-group 0
#
hsb-service-type ap hsb-group 0
#
wlan
traffic-profile name traff
user-isolate l2
security-profile name sec1
security wpa2 dot1x aes
security-profile name sec2
ssid-profile name ssid1
ssid Employee
ssid-profile name ssid2
ssid Guest
vap-profile name vap1
forward-mode tunnel
service-vlan vlan-id 40
ssid-profile ssid1
security-profile sec1
traffic-profile traff
authentication-profile p1
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
```

```
vap-profile name vap2
forward-mode tunnel
service-vlan vlan-id 41
ssid-profile ssid2
security-profile sec2
traffic-profile traff
authentication-profile p2
ip source check user-bind enable
arp anti-attack check user-bind enable
learn-client-address dhcp-strict
regulatory-domain-profile name domain1
ap-group name ap-group2
regulatory-domain-profile domain1
radio 0
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
radio 1
vap-profile vap1 wlan 1
vap-profile vap2 wlan 2
ap-id 2 type-id 56 ap-mac 00e0-fc12-6670 ap-sn 21500829352SGA900583
ap-name area_2
ap-group ap-group2
provision-ap
#
dot1x-access-profile name d1
#
mac-access-profile name mac1
#
return
```

ACC1 的配置文件

```
#
sysname ACC1
#
vlan batch 20 50
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 00e0-fc02-0003 group-mac 00e0-fc00-0002
#
interface Eth-Trunk30
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 50
l2protocol-tunnel user-defined-protocol 802.1x enable
```



```
mode lacp
#
interface 10GigabitEthernet1/0/1
eth-trunk 30
#
interface 10GigabitEthernet1/0/2
eth-trunk 30
#
interface GigabitEthernet1/0/3
port link-type access
port default vlan 50
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
interface GigabitEthernet1/0/4
port link-type access
port default vlan 20
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
return
```

ACC2 的配置文件

```
#
sysname ACC2
#
vlan batch 21 60
#
l2protocol-tunnel user-defined-protocol 802.1x protocol-mac 00e0-fc02-0003 group-mac 00e0-fc00-0002
#
interface Eth-Trunk40
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 21 60
l2protocol-tunnel user-defined-protocol 802.1x enable
mode lacp
#
interface 10GigabitEthernet1/0/1
eth-trunk 40
#
interface 10GigabitEthernet1/0/2
```

```
eth-trunk 40
#
interface GigabitEthernet1/0/3
port link-type access
port default vlan 60
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
interface GigabitEthernet1/0/4
port link-type access
port default vlan 21
stp edged-port enable
l2protocol-tunnel user-defined-protocol 802.1x enable
port-isolate enable group 1
#
return
```

1.1.2.2.4 认证点在接入设备的认证部署配置示例

简介

本场景旨在打通小型园区网络核心层、汇聚层与接入层设备间的二三层通信，同时在接入层设备上部署 802.1X 认证，用户需通过认证后才能接入园区网络及用户间互访。

组网需求

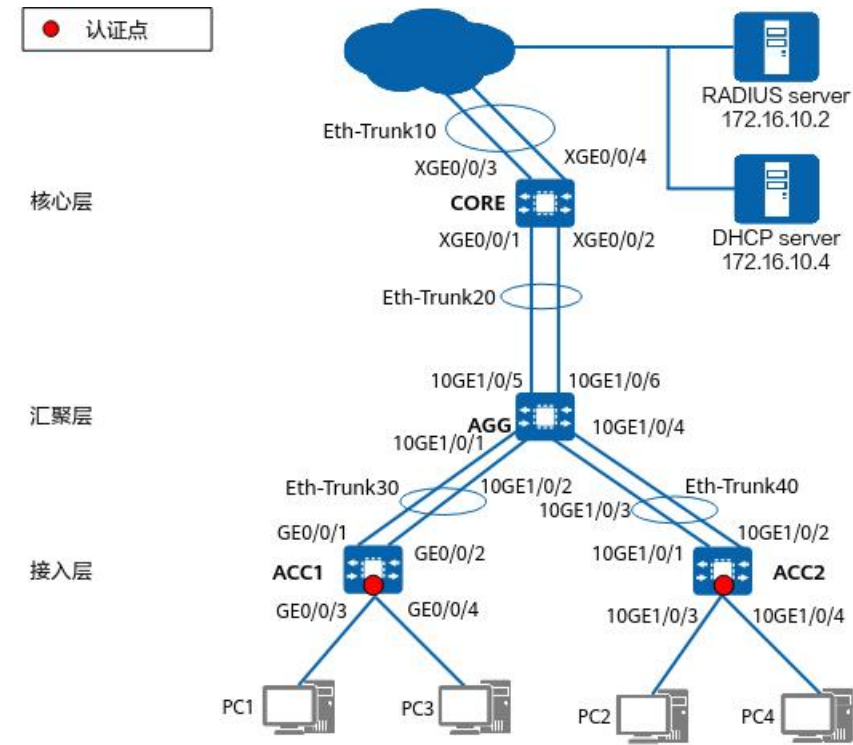
如[图 1](#)所示，园区网络自上而下分为核心层-汇聚层-接入层，其中：

汇聚交换机作为用户网关，负责用户业务的路由转发。

接入交换机作为用户认证点，用户必须 802.1X 认证成功才能接入网络。

各层网络设备之间通过 Eth-Trunk 连接，提高网络可靠性。

图 1 认证点在接入设备的认证部署配置示例基本组网图



数据规划

表 1 VLAN 规划表

设备	规划类型	规划取值	说明
核心交换机 CORE	–	VLAN 70	连接 AGG。
汇聚交换机 AGG	–	VLAN 60	ACC1 的业务 VLAN。
	–	VLAN 50	ACC2 的业务 VLAN。

表 2 IP 地址规划表

设备	规划类型	规划取值	说明（可选）
核心交换机 CORE	XGE0/0/1	VLANIF 70: 172.16.70.1/24	连接 AGG 的接口。
	XGE0/0/2		
	XGE0/0/3	172.16.10.0/24	连接 Internet 的网段。
	XGE0/0/4		
汇聚交换机 AGG	10GE1/0/1	VLANIF 60: 172.16.60.0/24	连接 ACC1 的网段。
	10GE1/0/2		
	10GE1/0/3	VLANIF 50: 172.16.50.0/24	连接 ACC2 的网段。
	10GE1/0/4		

表 2 IP 地址规划表

设备	规划类型	规划取值	说明（可选）
	10GE1/0/5	VLANIF 70: 172.16.70.2/24	连接 CORE 的接口。
	10GE1/0/6		

配置注意事项

不建议使用 VLAN 1 作为管理 VLAN 或者业务 VLAN，并将各端口从 VLAN 1 中退出。根据实际业务需求透传 VLAN，禁止端口透传所有 VLAN。

配置过程中的 RADIUS 认证计费密钥、授权密钥，交换机侧与服务器侧必须要配置一致。本案列仅展示交换机侧配置，RADIUS 服务器侧配置需参照具体服务器指南进行配置。

交换机默认放行发往 RADIUS 服务器的报文，不需要针对其配置免认证规则。

802.1X 认证场景中，如果使能 802.1X 认证的交换机和用户之间存在二层交换机，则需要在二层交换机上配置 802.1X 认证报文二层透明传输功能，否则用户无法认证成功。

适用产品和版本

表 3 适用的产品和版本

产品/子系列	设备主机名	版本
S12700	CORE	V200R019C00 及之后版本。
S8700	AGG、ACC2	V600R021C10 及之后版本。
S5731-S	ACC1	V200R019C10 及之后版本。

配置思路

表 4 二层接入认证 Eth-Trunk 级联配置思路

步骤	配置思路	涉及产品
1	配置交换机的接口和 VLAN，使得二层网络互通。	核心交换机（CORE）、汇聚交换机（AGG）、接入交换机（ACC1、ACC2）。
2	配置交换机的 VLANIF 接口及其 IP 地址。	核心交换机（CORE）、汇聚交换机（AGG）。

表 4 二层接入认证 Eth-Trunk 级联配置思路

步骤	配置思路	涉及产品
3	配置交换机的 DHCP 中继功能，使得交换机作为 DHCP 中继来转发 DHCP 客户端和 DHCP 服务器之间的 DHCP 报文。	汇聚交换机（AGG）。
4	配置交换机的路由功能，使得三层网络互通。	核心交换机（CORE）、汇聚交换机（AGG）。
5	配置 AAA，包括：RADIUS 服务器模板、AAA 方案和认证域，用来指定用户使用 RADIUS 进行认证、授权和计费，以及设备与 RADIUS 服务器对接的各项参数。	接入交换机（ACC1、ACC2）。
6	配置免认证资源、认证后域，保证用户在认证各阶段都有相应的网络访问权限。	接入交换机（ACC1、ACC2）。
7	配置用户使用 802.1X 认证。	接入交换机（ACC1、ACC2）。

操作步骤

- 1. 配置交换机的接口和 VLAN。
 - a. 配置核心交换 CORE 的接口和 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname CORE
[CORE] vlan batch 70
[CORE] interface eth-trunk 20
[CORE-Eth-Trunk20] description connect to AGG
[CORE-Eth-Trunk20] mode lacp
[CORE-Eth-Trunk20] port link-type trunk
[CORE-Eth-Trunk20] port trunk allow-pass vlan 70
[CORE-Eth-Trunk20] undo port trunk allow-pass vlan 1
[CORE-Eth-Trunk20] quit
[CORE] interface xgigabitethernet 0/0/1
[CORE-XGigabitEthernet0/0/1] eth-trunk 20
[CORE-XGigabitEthernet0/0/1] quit
[CORE] interface xgigabitethernet 0/0/2
[CORE-XGigabitEthernet0/0/2] eth-trunk 20
[CORE-XGigabitEthernet0/0/2] quit
[CORE] interface eth-trunk 10
[CORE-Eth-Trunk10] undo portswitch
[CORE-Eth-Trunk10] description connect to Internet
[CORE-Eth-Trunk10] trunkport xgigabitethernet 0/0/3
```

```
[CORE-Eth-Trunk10] trunkport xgigabitethernet 0/0/4
[CORE-Eth-Trunk10] mode lacp
[CORE-Eth-Trunk10] ip address 172.16.10.3 24
[CORE-Eth-Trunk10] quit
```

b. 配置汇聚交换机 AGG 的接口和 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname AGG
[AGG] vlan batch 50 60 70
[AGG] interface eth-trunk 20
[AGG-Eth-Trunk20] description connect to CORE
[AGG-Eth-Trunk20] mode lacp-static
[AGG-Eth-Trunk20] port link-type trunk
[AGG-Eth-Trunk20] port trunk allow-pass vlan 70
[AGG-Eth-Trunk20] undo port trunk allow-pass vlan 1
[AGG-Eth-Trunk20] quit
[AGG] interface 10GE 1/0/5
[AGG-10GE1/0/5] eth-trunk 20
[AGG-10GE1/0/5] quit
[AGG] interface 10GE 1/0/6
[AGG-10GE1/0/6] eth-trunk 20
[AGG-10GE1/0/6] quit
[AGG] interface eth-trunk 30
[AGG-Eth-Trunk30] description connect to ACC1
[AGG-Eth-Trunk30] mode lacp-static
[AGG-Eth-Trunk30] port link-type trunk
[AGG-Eth-Trunk30] port trunk allow-pass vlan 60
[AGG-Eth-Trunk30] undo port trunk allow-pass vlan 1
[AGG-Eth-Trunk30] quit
[AGG] interface 10GE 1/0/1
[AGG-10GE1/0/1] eth-trunk 30
[AGG-10GE1/0/1] quit
[AGG] interface 10GE 1/0/2
[AGG-10GE1/0/2] eth-trunk 30
[AGG-10GE1/0/2] quit
[AGG] interface eth-trunk 40
[AGG-Eth-Trunk40] description connect to ACC2
[AGG-Eth-Trunk40] mode lacp-static
[AGG-Eth-Trunk40] port link-type trunk
[AGG-Eth-Trunk40] port trunk allow-pass vlan 50
[AGG-Eth-Trunk40] undo port trunk allow-pass vlan 1
[AGG-Eth-Trunk40] quit
[AGG] interface 10GE 1/0/3
```

```
[AGG-10GE1/0/3] eth-trunk 40
[AGG-10GE1/0/3] quit
[AGG] interface 10GE 1/0/4
[AGG-10GE1/0/4] eth-trunk 40
[AGG-10GE1/0/4] quit
```

c. 配置接入交换机 ACC1 的接口和 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1
[ACC1] vlan batch 60
[ACC1] interface eth-Trunk 30
[ACC1-Eth-Trunk30] description connect to AGG
[ACC1-Eth-Trunk30] mode lacp
[ACC1-Eth-Trunk30] port link-type trunk
[ACC1-Eth-Trunk30] port trunk allow-pass vlan 60
[ACC1-Eth-Trunk30] undo port trunk allow-pass vlan 1
[ACC1-Eth-Trunk30] quit
[ACC1] interface gigabitethernet 0/0/1
[ACC1-GigabitEthernet0/0/1] eth-trunk 30
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface gigabitethernet 0/0/2
[ACC1-GigabitEthernet0/0/2] eth-trunk 30
[ACC1-GigabitEthernet0/0/2] quit
[ACC1] interface gigabitethernet 0/0/3
[ACC1-GigabitEthernet0/0/3] port link-type access
[ACC1-GigabitEthernet0/0/3] port default vlan 60
[ACC1-GigabitEthernet0/0/3] stp edged-port enable
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface gigabitethernet 0/0/4
[ACC1-GigabitEthernet0/0/4] port link-type access
[ACC1-GigabitEthernet0/0/4] port default vlan 60
[ACC1-GigabitEthernet0/0/4] stp edged-port enable
[ACC1-GigabitEthernet0/0/4] quit
```

d. 配置接入交换机 ACC2 的接口和 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC2
[ACC2] vlan batch 50
[ACC2] interface eth-Trunk 40
[ACC2-Eth-Trunk40] description connect to AGG
[ACC2-Eth-Trunk40] mode lacp-static
[ACC2-Eth-Trunk40] port link-type trunk
[ACC2-Eth-Trunk40] port trunk allow-pass vlan 50
```

```
[ACC2-Eth-Trunk40] undo port trunk allow-pass vlan 1
[ACC2-Eth-Trunk40] quit
[ACC2] interface 10GE 1/0/1
[ACC2-10GE1/0/1] eth-trunk 40
[ACC2-10GE1/0/1] quit
[ACC2] interface 10GE 1/0/2
[ACC2-10GE1/0/2] eth-trunk 40
[ACC2-10GE1/0/2] quit
[ACC2] interface 10GE 1/0/3
[ACC2-10GE1/0/3] port link-type access
[ACC2-10GE1/0/3] port default vlan 50
[ACC2-10GE1/0/3] stp edged-port enable
[ACC2-10GE1/0/3] quit
[ACC2] interface 10GE 1/0/4
[ACC2-10GE1/0/4] port link-type access
[ACC2-10GE1/0/4] port default vlan 50
[ACC2-10GE1/0/4] stp edged-port enable
[ACC2-10GE1/0/4] quit
```

2. 配置交换机的 VLANIF 接口及其 IP 地址。

a. 配置核心交换机的 VLANIF 接口及其 IP 地址。

创建连接汇聚交换机 AGG 的三层接口 VLANIF 70。

```
[CORE] interface vlanif 70
[CORE-Vlanif70] ip address 172.16.70.1 255.255.255.0
[CORE-Vlanif70] quit
```

b. 配置汇聚交换机的 VLANIF 接口及其 IP 地址。

创建连接接入交换机的三层接口 VLANIF 50、VLANIF 60。

```
[AGG] interface vlanif 60
[AGG-Vlanif60] ip address 172.16.60.1 255.255.255.0
[AGG-Vlanif60] quit
[AGG] interface vlanif 50
[AGG-Vlanif50] ip address 172.16.50.1 255.255.255.0
[AGG-Vlanif50] quit
```

创建连接核心交换机 CORE 的三层接口 VLANIF 70。

```
[AGG] interface vlanif 70
[AGG-Vlanif70] ip address 172.16.70.2 255.255.255.0
[AGG-Vlanif70] quit
```

3. 配置汇聚交换机 AGG 的 DHCP 中继功能，使得交换机作为 DHCP 中继转发 DHCP 客户端和 DHCP 服务器之间的 DHCP 报文。

在汇聚层交换机 AGG 的接口 VLANIF50 与 VLANIF60 下使能 DHCP 中继功能，并配置 DHCP 服务器的 IP 地址。

```
[AGG] dhcp enable
[AGG] interface vlanif 50
[AGG-Vlanif50] dhcp select relay
[AGG-Vlanif50] dhcp relay server-ip 172.16.10.4
[AGG-Vlanif50] quit
[AGG] interface vlanif 60
[AGG-Vlanif60] dhcp select relay
[AGG-Vlanif60] dhcp relay server-ip 172.16.10.4
[AGG-Vlanif60] quit
```

4. 配置交换机的路由功能，实现三层网络互通。实际配置中可以按需求配置路由协议，本案例中使用 OSPF 路由协议。

在核心交换机 CORE 上配置 OSPF 功能。

```
[CORE] ospf 1 router-id 1.1.1.1
[CORE-ospf-1] area 0
[CORE-ospf-1-area-0.0.0.0] network 172.16.70.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] network 172.16.10.0 0.0.0.255
[CORE-ospf-1-area-0.0.0.0] quit
[CORE-ospf-1] quit
```

在汇聚交换机 AGG 配置 OSPF 功能。

```
[AGG] ospf 1 router-id 2.2.2.2
[AGG-ospf-1] area 0
[AGG-ospf-1-area-0.0.0.0] network 172.16.70.0 0.0.0.255
[AGG-ospf-1-area-0.0.0.0] network 172.16.50.0 0.0.0.255
[AGG-ospf-1-area-0.0.0.0] network 172.16.60.0 0.0.0.255
[AGG-ospf-1-area-0.0.0.0] quit
[AGG-ospf-1] quit
```

5. 配置接入交换机的 DHCP Snooping 信任接口，保护用户从合法的 DHCP 服务器获取 IP 地址。

在接入交换机 ACC1 上配置 DHCP Snooping 信任接口，接入交换机 ACC2 的配置与此类似，不再赘述。

```
[ACC1] dhcp enable
[ACC1] dhcp snooping enable
[ACC1] vlan 60
[ACC1-vlan60] dhcp snooping enable
[ACC1-vlan60] dhcp snooping trusted interface Eth-Trunk 30
[ACC1-vlan60] quit
```

6. 配置接入交换机 ACC1 上的 AAA 参数。接入交换机 ACC2 的配置与此类似，不再赘述。

配置 RADIUS 服务器模板“tem_rad”，指定接入交换机与 RADIUS 服务器的对接参数，包括 RADIUS 认证服务器和 RADIUS 计费服务器的 IP 地址、端口号以及认证计费密钥。

```
[ACC1] radius-server template tem_rad
[ACC1-radius-tem_rad] radius-server authentication 172.16.10.2 1812
[ACC1-radius-tem_rad] radius-server accounting 172.16.10.2 1813
[ACC1-radius-tem_rad] radius-server shared-key cipher YsHsjx_202206
[ACC1-radius-tem_rad] quit
```

配置 RADIUS 授权服务器和授权密钥。

```
[ACC1] radius-server authorization 172.16.10.2 shared-key cipher YsHsjx_202206
```

配置 AAA 认证和计费方案，指定认证和计费方式为 RADIUS，计费周期为 15 分钟。

```
[ACC1] aaa
[ACC1-aaa] authentication-scheme auth
[ACC1-aaa-authen-auth] authentication-mode radius
[ACC1-aaa-authen-auth] quit
[ACC1-aaa] accounting-scheme acco
[ACC1-aaa-accounting-acco] accounting-mode radius
[ACC1-aaa-accounting-acco] accounting realtime 15
[ACC1-aaa-accounting-acco] quit
```

配置认证域“huawei.com”，在域下绑定 AAA 方案和 RADIUS 服务器模板。

```
[ACC1-aaa] domain huawei.com
[ACC1-aaa-domain-huawei.com] authentication-scheme auth
[ACC1-aaa-domain-huawei.com] accounting-scheme acco
[ACC1-aaa-domain-huawei.com] radius-server tem_rad
[ACC1-aaa-domain-huawei.com] quit
[ACC1-aaa] quit
```

7. 配置接入交换机 ACC1 上的免认证资源、认证后域。接入交换机 ACC2 的配置与此类似，不再赘述。

配置免认证资源：放通到 DNS 服务器的报文。

```
[ACC1] free-rule-template name default_free_rule
[ACC1-free-rule-default_free_rule] free-rule 1 destination ip 172.16.10.1 mask 32
[ACC1-free-rule-default_free_rule] quit
```

配置认证后域：ACL 3001 管控用户认证成功后的网络访问权限。

```
[ACC1] acl 3001
[ACC1-acl4-advance-3001] rule 1 permit ip destination 172.16.10.0 0.0.0.255
[ACC1-acl4-advance-3001] rule 2 permit ip destination 172.16.50.0 0.0.0.255
[ACC1-acl4-advance-3001] rule 3 permit ip destination 172.16.60.0 0.0.0.255
[ACC1-acl4-advance-3001] rule 4 deny ip destination any
[ACC1-acl4-advance-3001] quit
```

8. 配置接入交换机 ACC1 上的 802.1X 认证。接入交换机 ACC2 的配置与此类似，不再赘述。

配置 802.1X 接入模板。802.1X 接入模板默认采用 EAP 认证方式，请确保 RADIUS 服务器支持 EAP 协议，否则无法处理 802.1X 认证请求。

```
[ACC1] dot1x-access-profile name d1
```

```
[ACC1-dot1x-access-profile-d1] quit
```

配置用户使用的认证模板。

```
[ACC1] authentication-profile name p1
[ACC1-authen-profile-p1] dot1x-access-profile d1
[ACC1-authen-profile-p1] access-domain huawei.com force
[ACC1-authen-profile-p1] authentication event authen-server-up action re-authen
[ACC1-authen-profile-p1] quit
```

在下行接口上，配置接入用户使用 802.1X 认证。

```
[ACC1] interface gigabitethernet 0/0/3
[ACC1-GigabitEthernet0/0/3] authentication-profile p1
[ACC1-GigabitEthernet0/0/3] quit
[ACC1] interface gigabitethernet 0/0/4
[ACC1-GigabitEthernet0/0/4] authentication-profile p1
[ACC1-GigabitEthernet0/0/4] quit
```

检查配置结果

1. 用户认证成功之前或者认证失败时，可以访问免认证资源，但无法访问认证后域资源。

在 PC1 上输入错误的用户名和密码，然后在 ACC1 上执行 **display access-user** 查看在线用户信息。此时可以发现 user1 已上线，但处于预认证状态（**Pre-authen**），即未认证或认证失败状态。

```
[ACC1] display access-user
process 0:
-----
-----
UserID Username          IP address      MAC             Status
-----
-----
16457 user1              172.16.60.43   00e0-fc12-3344 Pre-authen
-----
-----
Total: 1, printed: 1
```

在 PC1 上 Ping 免认证资源（DNS 服务器：172.16.10.1），能够 Ping 通。

```
C:\Users>ping 172.16.10.1

Pinging 172.16.10.1 with 32 bytes of data:
Reply from 172.16.10.1: bytes=32 time<1ms TTL=128
Reply from 172.16.10.1: bytes=32 time<1ms TTL=128
Reply from 172.16.10.1: bytes=32 time<1ms TTL=128
Reply from 172.16.10.1: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.10.1:
```

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 0ms, Maximum = 0ms, Average = 0ms

在 PC1 上 Ping 认证后域（园区出口：172.16.10.3），无法 Ping 通。

```
C:\Users>ping 172.16.10.3

Pinging 172.16.10.3 with 32 bytes of data:
Request time out.
Request time out.
Request time out.
Request time out.
Request time out.
Ping statistics for 172.16.10.3:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss)
```

2. 用户认证成功后，可以访问认证后域资源。

在汇聚交换机 AGG 上执行 **display ip pool interface vlanif60 used** 命令，查看用户均已成功获取到 IP 地址。

```
[AGG] display ip pool interface vlanif60 used

Pool-name      : Vlanif60
Pool-No       : 1
Lease          : 1 Days 0 Hours 0 Minutes
Domain-name    : -
DNS-server0    : 172.16.10.1
NBNS-server0   : -
Netbios-type   : -
Position       : Interface
Status         : Unlocked
Gateway-0      : -
Network        : 172.16.60.0
Mask           : 255.255.255.0
VPN instance   : --
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :254   Used   :2
                   Idle    :252   Expired :0
                   Conflict :0     Disabled :0

-----
-
Network section
  Start      End      Total  Used Idle(Expired) Conflict Disabled
```

```
-----
172.16.60.1 172.16.60.254 254 2 252(0) 0 0
-----
```

Client-ID format as follows:

```
DHCP : mac-address      PPPoE : mac-address
IPSec : user-id/portnumber/vrf  PPP : interface index
L2TP : cpu-slot/session-id     SSL-VPN : user-id/session-id
-----
```

```
-----
Index      IP      Client-ID  Type    Left  Status
-----
42 172.16.60.43      00e0-fc12-3344 DHCP    86380 Used
173 172.16.60.174     00e0-fc12-4400 DHCP    85890 Used
-----
```

在 PC1 上执行 **ping 172.16.60.174** 命令，查看 PC1 已连通 PC3。

```
C:\Users>ping 172.16.60.174
```

Pinging 172.16.60.174 with 32 bytes of data:

Reply from 172.16.60.174: bytes=32 time<1ms TTL=128

Reply from 172.16.60.174: bytes=32 time<1ms TTL=128

Reply from 172.16.60.174: bytes=32 time<1ms TTL=128

Reply from 172.16.60.174: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.60.174:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 0ms, Maximum = 0ms, Average = 0ms

在接入交换机 ACC1 执行 **display access-user** 命令查看在线用户信息。

```
[ACC1] display access-user
```

Total: 2

```
-----
UserID  Username      IP address      MAC              Status
-----
16457   user1         172.16.60.43    00e0-fc12-3344   Success
16463   user2         172.16.60.174    00e0-fc12-4400   Success
-----
```

配置脚本

CORE 的配置脚本

```
#
sysname CORE
#
vlan batch 70
#
interface eth-trunk 20
description connect to AGG
mode lacp
port link-type trunk
port trunk allow-pass vlan 70
undo port trunk allow-pass vlan 1
#
interface xgigabitethernet 0/0/1
eth-trunk 20
#
interface xgigabitethernet 0/0/2
eth-trunk 20
#
interface eth-trunk 10
undo portswitch
description connect to Internet
trunkport xgigabitethernet 0/0/3
trunkport xgigabitethernet 0/0/4
mode lacp
ip address 172.16.10.3 24
#
interface vlanif 70
ip address 172.16.70.1 255.255.255.0
#
ospf 1 router-id 1.1.1.1
area 0
network 172.16.70.0 0.0.0.255
network 172.16.10.0 0.0.0.255
#
return
```

AGG 的配置脚本

```
#
sysname AGG
#
vlan batch 50 60 70
#
interface eth-trunk 20
description connect to CORE
mode lacp-static
port link-type trunk
port trunk allow-pass vlan 70
undo port trunk allow-pass vlan 1
#
interface 10GE 1/0/5
eth-trunk 20
#
interface 10GE 1/0/6
eth-trunk 20
#
interface eth-trunk 30
description connect to ACC1
mode lacp-static
port link-type trunk
port trunk allow-pass vlan 60
undo port trunk allow-pass vlan 1
#
interface 10GE 1/0/1
eth-trunk 30
#
interface 10GE 1/0/2
eth-trunk 30
#
interface eth-trunk 40
description connect to ACC2
mode lacp-static
port link-type trunk
port trunk allow-pass vlan 50
undo port trunk allow-pass vlan 1
#
interface 10GE 1/0/3
eth-trunk 40
#
interface 10GE 1/0/4
```

```
eth-trunk 40
#
interface vlanif 60
 ip address 172.16.60.1 255.255.255.0
#
interface vlanif 50
 ip address 172.16.50.1 255.255.255.0
#
interface vlanif 70
 ip address 172.16.70.2 255.255.255.0
#
dhcp enable
#
interface vlanif 50
 dhcp select relay
 dhcp relay server-ip 172.16.10.4
#
interface vlanif 60
 dhcp select relay
 dhcp relay server-ip 172.16.10.4
#
ospf 1 router-id 2.2.2.2
 area 0
  network 172.16.70.0 0.0.0.255
  network 172.16.50.0 0.0.0.255
  network 172.16.60.0 0.0.0.255
#
return
```

ACC1 的配置脚本

```
#
sysname ACC1
#
vlan batch 60
#
interface eth-Trunk 30
 description connect to AGG
 mode lacp
 port link-type trunk
 port trunk allow-pass vlan 60
 undo port trunk allow-pass vlan 1
#
interface gigabitethernet 0/0/1
```



```
eth-trunk 30
#
interface gigabitethernet 0/0/2
eth-trunk 30
#
interface gigabitethernet 0/0/3
port link-type access
port default vlan 60
stp edged-port enable
#
interface gigabitethernet 0/0/4
port link-type access
port default vlan 60
stp edged-port enable
#
dhcp enable
#
dhcp snooping enable
#
vlan 60
dhcp snooping enable
dhcp snooping trusted interface Eth-Trunk 30
#
radius-server template tem_rad
radius-server authentication 172.16.10.2 1812
radius-server accounting 172.16.10.2 1813
radius-server shared-key
cipher %+%##!!!!!!"!!!!$!!!!*!!!!ZonC2XJ]_A]N&P!y16vPj_Uy9)u)C(uV/Z*!!!!2jp5!!!!>!!!!`6iHP{C#&HAcVY08({:
4]*A%,$y+NJ>E9=@UDI<%+%#
#
radius-server authorization 172.16.10.2 shared-key
cipher %+%##!!!!!!"!!!!$!!!!*!!!!ZonC2XJ]_A!^$C:%n#~KaX8E66].pBb\^nM!!!!2jp5!!!!>!!!!GI3OQ[gk[I#n({0dZ"V
(Cvgj)QG[+'oB,D"YP`'A%+%#
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
domain huawei.com
authentication-scheme auth
accounting-scheme acco
```

```
radius-server tem_rad
#
free-rule-template name default_free_rule
free-rule 1 destination ip 172.16.10.1 mask 32
#
acl 3001
rule 1 permit ip destination 172.16.10.0 0.0.0.255
rule 2 permit ip destination 172.16.50.0 0.0.0.255
rule 3 permit ip destination 172.16.60.0 0.0.0.255
rule 4 deny ip destination any
#
dot1x-access-profile name d1
#
authentication-profile name p1
dot1x-access-profile d1
access-domain huawei.com force
authentication event authen-server-up action re-authen
#
interface gigabitethernet 0/0/3
authentication-profile p1
#
interface gigabitethernet 0/0/4
authentication-profile p1
#
return
```

ACC2 的配置脚本

```
#
sysname ACC2
#
vlan batch 50
#
interface eth-Trunk 40
description connect to AGG
mode lacp-static
port link-type trunk
port trunk allow-pass vlan 50
undo port trunk allow-pass vlan 1
#
interface 10GE 1/0/1
eth-trunk 40
#
interface 10GE 1/0/2
```

```
eth-trunk 40
#
interface 10GE 1/0/3
port link-type access
port default vlan 50
stp edged-port enable
#
interface 10GE 1/0/4
port link-type access
port default vlan 50
stp edged-port enable
#
dhcp enable
#
dhcp snooping enable
#
vlan 50
dhcp snooping enable
dhcp snooping trusted interface Eth-Trunk 40
#
radius-server template tem_rad
radius-server authentication 172.16.10.2 1812
radius-server accounting 172.16.10.2 1813
radius-server shared-key
cipher %+%##!!!!!!"!!!!$!!!!*!!!!ZonC2XJ]_A]N&P!y16vPj_Uy9)u)C(uV/Z*!!!!2jp5!!!!>!!!!`6iHP{C#&HAcVY08({:
4]*A%,$y+NJ>E9=@UDI<%+%#
#
radius-server authorization 172.16.10.2 shared-key
cipher %+%##!!!!!!"!!!!$!!!!*!!!!ZonC2XJ]_A!^$C:%n#~KaX8E66].pBb\^nM!!!!2jp5!!!!>!!!!GI3OQ[gk[l#n({0dZ"V
(Cvgj)QG[+'oB,D"YP`A%+%#
#
aaa
authentication-scheme auth
authentication-mode radius
accounting-scheme acco
accounting-mode radius
accounting realtime 15
domain huawei.com
authentication-scheme auth
accounting-scheme acco
radius-server tem_rad
#
free-rule-template name default_free_rule
```

```
free-rule 1 destination ip 172.16.10.1 mask 32
#
acl 3001
rule 1 permit ip destination 172.16.10.0 0.0.0.255
rule 2 permit ip destination 172.16.50.0 0.0.0.255
rule 3 permit ip destination 172.16.60.0 0.0.0.255
rule 4 deny ip destination any
#
dot1x-access-profile name d1
#
authentication-profile name p1
dot1x-access-profile d1
access-domain huawei.com force
authentication event authen-server-up action re-authen
#
interface gigabitethernet 0/0/3
authentication-profile p1
#
interface gigabitethernet 0/0/4
authentication-profile p1
#
return
```

1.1.2.3 智能极简园区网络部署案例（小行星部署案例）

简介

传统园区网络架构面临着以下三个挑战：

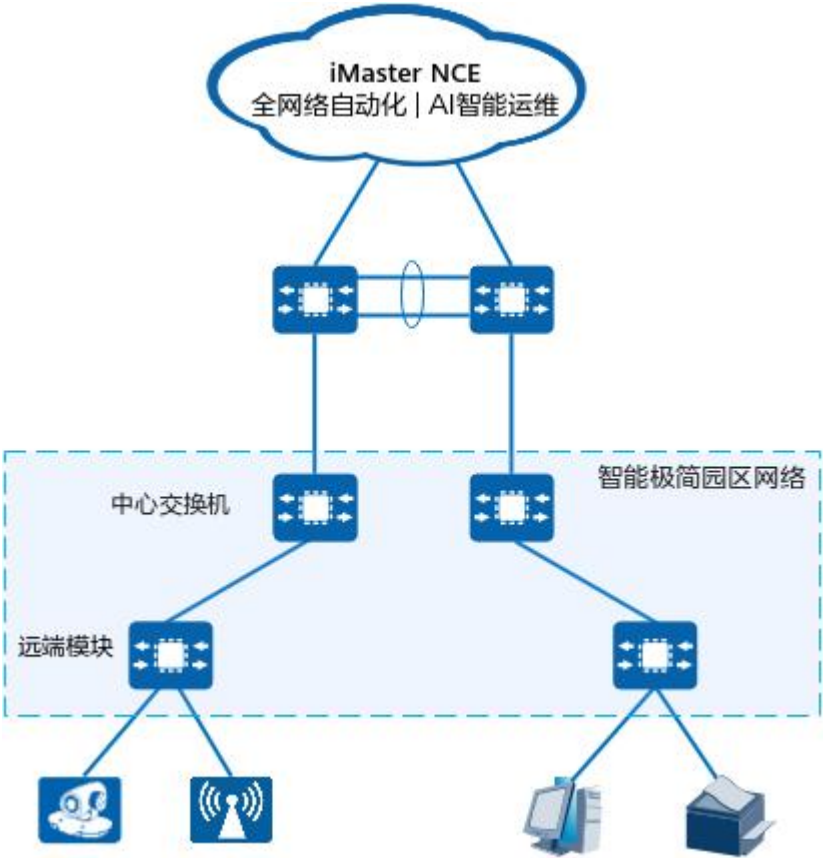
成本高：互联网、物联网的发展催生出越来越多的新型终端，网络经常需要扩展以接入更多的终端。当前的网络部署方式，交换机部署在楼层弱电间，连接接入点的网线通常埋在墙体中。如果扩展接入更多的终端，需要施工改造，重新布线，成本较高。

带宽低：远程办公、线上教学模式等业务的快速发展对网络带宽的要求越来越高，双绞线不足以满足带宽的不停演进。

管理难：园区多网融合成为趋势，网络越来越复杂，这使得网络管理变得愈发困难。

为解决上述问题，华为推出了全新的智能极简园区网络方案（也称为小行星方案）。如[图 1](#)所示，它由中心交换机，以及分布在各个办公室、敏捷岛、教室等信息点的远端模块组成，让网络的部署、运营更加高效。

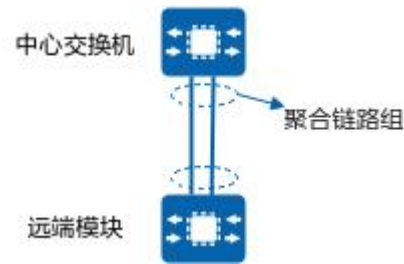
图 1 智能极简园区网络



远端模块即插即用，组网方便快捷，可以根据实际应用场景选择合适的线缆类型连接中心交换机和远端模块，网线、光纤、光电混合缆均支持该组网。使用光电混合缆能够实现中心交换机对远端模块的远程供电，实现断电不断网。

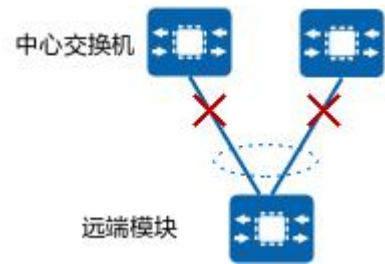
远端模块的上行接口可采用单链路或双链路对接中心交换机。如果是单链路，完成上电即组建成功。如果是双链路，如[图 双链路场景组建智能极简网络](#)所示，两条链路应该对接同一个中心交换机和远端模块，远端模块的两个上行接口自动组建链路聚合组，中心交换机侧需要手动将两个端口组建链路聚合组。

图 2 双链路场景组建智能极简园区网络



如[图 异常双链路场景](#)所示，对于中心交换机未组建链路聚合组、两条链路对接不同中心交换机等异常双链路场景，中心交换机会自动检测并触发告警和 Error-Down。

图 3 异常双链路场景

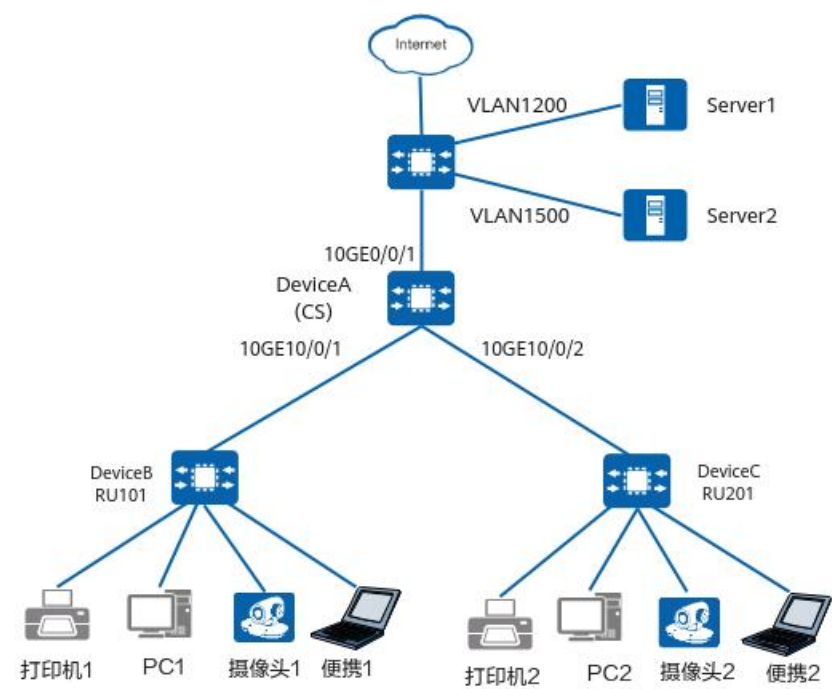


组网需求

某企业新建一栋办公大楼，有若干间办公室，每间办公室部署若干个摄像头、便携、PC、打印机。其中便携可能会在几个办公室之间移动使用，要求便携无论在哪个办公室使用，均只能访问特定部门的服务器（不同部门的便携只访问本部门的服务器。比如，便携 1 只能访问 Server1，便携 2 只能访问 Server2 ），组网如图 1。

交换机摆放方案：办公楼弱电间部署中心交换机（图中的 DeviceA），每间办公室弱电箱部署一个远端模块（图中的 RUn，n 为办公室房间号）。中心交换机通过光电混合缆和远端模块连接，并通过 PoE 给远端模块供电。每间办公室的远端模块通过网线下挂摄像头、便携、PC、打印机，8 口远端模块使用 4 个下行接口，其他下行接口预留给未来终端扩展。

图 4 办公大楼远端模块部署组网



数据规划

表 1 终端数据规划

终端	供电方式	VLAN	MAC 地址
摄像头 1	PoE	1100	00e0-fc76-1230
便携 1	本地供电	1200	00e0-fc76-1240
PC1	本地供电	1300	00e0-fc76-1250
打印机 1	本地供电	1400	00e0-fc76-1260
摄像头 2	PoE	1100	00e0-fc76-2230
便携 2	本地供电	1500	00e0-fc76-2240
PC2	本地供电	1300	00e0-fc76-2250

表 1 终端数据规划

终端	供电方式	VLAN	MAC 地址
打印机 2	本地供电	1400	00e0-fc76-2260

适用产品和版本

表 2 交换机适用的产品和版本

系列	产品	版本
S12700E	S12700E-4、S12700E-8、S12700E-12	从 V200R021C10 版本开始支持
S12700	S12704、S12708、S12712	从 V200R021C10 版本开始支持
S8700	S8700-4、S8700-6、S8700-10	从 V600R022C10 版本开始支持
S7700	S7706、S7712	从 V200R021C10 版本开始支持
S6700	S6730-H、S6730S-H、S6730-S、S6730S-S、S6735-S、S6720-EI、S6720S-EI	从 V200R021C10 版本开始支持
	S6730-H-V2	从 V600R022C10 版本开始支持
S5700	S5732-H	从 V200R021C10 版本开始支持
	S5731-H	从 V200R021C10 版本开始支持
	S5731S-H、S5731-S、S5731S-S、S5736-S、S5735S-H、S5735-S、S5735S-S、S5735-S-I、S5720I-SI、S5735-L、S5735S-L、S5735-L1、S5735S-L1、S5735-L-I、S5720-LI、S5720S-LI、S5720I-SI	从 V200R021C10 版本开始支持
	S5732-H-V2	从 V600R022C10 版本开始支持
	S5735-L-V2、S5735-S-V2、S5735I-L-V2、S5735I-S-V2、S5735I-L-V2	从 V600R022C10 版本开始支持
	S5755-H	从 V600R023C00 版本开始支持

表 2 交换机适用的产品和版本

系列	产品	版本
S5500	S5535-L-V2、S5535-S-V2	从 V600R023C00 版本开始支持
S500、S300	S500、S300	从 V200R021C10 版本开始支持

表 3 远端模块适用的产品和版本

远端模块型号	版本
S5731-L4P2HW-RUA S5731S-L4P2HW-RUA S5731-L4P2HT-RUA S5731S-L4P2HT-RUA S5731-L8P2HT-RUA S5731S-L8P2HT-RUA S5731-L8P2HT-RUA S5731S-L8P2HT-RUA S5731-L4P2ST-RUA S5731S-L4P2ST-RUA S5731-L8P2ST-RUA S5731S-L8P2ST-RUA S5731-L4T2S-RUA S5731S-L4T2S-RUA S5731-L4T2ST-RUA S5731S-L4T2ST-RUA S5731-L8T2ST-RUA S5731S-L8T2ST-RUA	从 V200R021C10 版本开始支持

配置思路

表 4 小行星部署方案配置思路

步骤	配置思路
1	将中心交换机与远端模块相连，远端模块即插即用上线。
2	在中心交换机 DeviceA 上绑定互联口，配置远端模块端口隔离。
3	在中心交换机 DeviceA 上配置终端 MAC 地址与 VLAN 关联。
4	在中心交换机 DeviceA 上配置与远端模块互联的接口，并将 VLAN1100、VLAN1200、VLAN1300、VLAN1400、VLAN1500 加入互联口，便于终端上线。

操作步骤

1. 将远端模块的上行接口连接到中心交换机，查看远端模块上线。

检查远端模块状态，状态为 Normal 表示正常。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] display remote-unit
```

ESN	ID	Type	ConnectInterface	Status	VersionMatch	Name
219801176801XXXXXXXXX	-	S5731-L8P2HT-RUA	10GE10/0/1	Normal	NO	-
219801176802XXXXXXXXX	-	S5731-L8P2HT-RUA	10GE10/0/2	Normal	NO	-

```
Total: 2, printed: 2
```

2. 配置互联口、配置远端模块端口隔离。

绑定互联口。

```
[DeviceA] remote-unit 0
[DeviceA-remote-unit-0] name RU101
[DeviceA-remote-unit-0] description RU101_10GE10/0/1
[DeviceA-remote-unit-0] bind interface 10GE 10/0/1
[DeviceA-remote-unit-0] quit
[DeviceA] remote-unit 1
[DeviceA-remote-unit-1] name RU201
[DeviceA-remote-unit-1] description RU201_10GE10/0/2
[DeviceA-remote-unit-1] bind interface 10GE 10/0/2
[DeviceA-remote-unit-1] quit
```

在远端模块全局视图下配置端口隔离，并下发到远端模块。

```
[DeviceA] remote-unit
[DeviceA-remote-unit] isolate enable
[DeviceA-remote-unit] commit all
[DeviceA-remote-unit] quit
```

3. 创建 VLAN 并配置接口允许通过的 VLAN。将 VLAN1100、VLAN1200、VLAN1300、VLAN1400、VLAN1500 加入互联口 10GE10/0/1、10GE10/0/2。

```
[DeviceA] vlan batch 1100 1200 1300 1400 1500
[DeviceA] interface 10GE 10/0/1
[DeviceA-10GE10/0/1] description to_RU101
[DeviceA-10GE10/0/1] port link-type hybrid
[DeviceA-10GE10/0/1] port hybrid pvid vlan 1300
```

```
[DeviceA-10GE10/0/1] port hybrid untagged vlan 1100 1200 1300 1400 1500
[DeviceA-10GE10/0/1] quit
[DeviceA] interface 10GE 10/0/2
[DeviceA-10GE10/0/2] description to_RU201
[DeviceA-10GE10/0/2] port link-type hybrid
[DeviceA-10GE10/0/2] port hybrid pvid vlan 1300
[DeviceA-10GE10/0/2] port hybrid untagged vlan 1100 1200 1300 1400 1500
[DeviceA-10GE10/0/2] quit
```

配置终端 MAC 地址与 VLAN 关联。

```
[DeviceA] vlan 1100
[DeviceA-vlan1100] mac-vlan mac-address 00e0-fc76-1230
[DeviceA-vlan1100] mac-vlan mac-address 00e0-fc76-2230
[DeviceA-vlan1100] quit
[DeviceA] vlan 1200
[DeviceA-vlan1200] mac-vlan mac-address 00e0-fc76-1240
[DeviceA-vlan1200] quit
[DeviceA] vlan 1500
[DeviceA-vlan1500] mac-vlan mac-address 00e0-fc76-2240
[DeviceA-vlan1500] quit
[DeviceA] vlan 1400
[DeviceA-vlan1400] mac-vlan mac-address 00e0-fc76-1260
[DeviceA-vlan1400] mac-vlan mac-address 00e0-fc76-2260
[DeviceA-vlan1400] quit
[DeviceA] interface 10GE 10/0/1
[DeviceA-10GE10/0/1] mac-vlan enable
[DeviceA-10GE10/0/1] quit
[DeviceA] interface 10GE 10/0/2
[DeviceA-10GE10/0/2] mac-vlan enable
[DeviceA-10GE10/0/2] quit
```

4. 配置中心交换机上行口放通 vlan。

```
[DeviceA] interface 10GE 0/0/1
[DeviceA-10GE0/0/1] port link-type trunk
[DeviceA-10GE0/0/1] port trunk allow-pass vlan 1100 1200 1300 1400 1500
[DeviceA-10GE0/0/1] quit
```

检查配置结果

检查远端模块状态，此时可以看到配置的远端模块 ID、别名。

```
[DeviceA] display remote-unit
```

ESN	ID	Type	ConnectInterface	Status	VersionMatch	Name	

219801176801XXXXXXXXX	0	S5731-L8P2HT-RUA	10GE10/0/1	Normal	NO	-	
219801176802XXXXXXXXX	1	S5731-L8P2HT-RUA	10GE10/0/2	Normal	NO	-	

Total: 2, printed: 2							

在任意视图下执行 **display mac-vlan mac-address all** 命令，查看基于 MAC 划分 VLAN 的配置。

[DeviceA] display mac-vlan mac-address all

MAC Address	MASK	VLAN	Priority
00e0-fc76-1230	ffff-ffff-ffff	1100	0
00e0-fc76-2230	ffff-ffff-ffff	1100	0
00e0-fc76-1240	ffff-ffff-ffff	1200	0
00e0-fc76-1260	ffff-ffff-ffff	1400	0
00e0-fc76-2260	ffff-ffff-ffff	1400	0
00e0-fc76-2240	ffff-ffff-ffff	1500	0

Total MAC VLAN address count: 6

终端接入后，检查终端的 MAC 表。

[DeviceA] display mac-address

MAC Address	VLAN/VSI/BD	Learned-From	Type
00e0-fc76-1230	1100/-/-	10GE10/0/1	dynamic
00e0-fc76-1240	1200/-/-	10GE10/0/1	dynamic
00e0-fc76-1250	1300/-/-	10GE10/0/1	dynamic
00e0-fc76-1260	1400/-/-	10GE10/0/1	dynamic
00e0-fc76-2230	1100/-/-	10GE10/0/2	dynamic
00e0-fc76-2240	1500/-/-	10GE10/0/2	dynamic
00e0-fc76-2250	1300/-/-	10GE10/0/2	dynamic
00e0-fc76-2260	1400/-/-	10GE10/0/2	dynamic

Total items displayed = 8

配置脚本

DeviceA

```
#
```

```
sysname DeviceA

#
vlan batch 1100 1200 1300 1400 1500
#
vlan 1100
 mac-vlan mac-address 00e0-fc76-1230
 mac-vlan mac-address 00e0-fc76-2230
vlan 1200
 mac-vlan mac-address 00e0-fc76-1240
vlan 1400
 mac-vlan mac-address 00e0-fc76-1260
 mac-vlan mac-address 00e0-fc76-2260
vlan 1500
 mac-vlan mac-address 00e0-fc76-2240
#
interface 10GE 10/0/1
 description to_RU101
 port link-type hybrid
 port hybrid pvid vlan 1300
 port hybrid untagged vlan 1100 1200 1300 1400 1500
 mac-vlan enable
#
interface 10GE 10/0/2
 description to_RU201
 port link-type hybrid
 port hybrid pvid vlan 1300
 port hybrid untagged vlan 1100 1200 1300 1400 1500
 mac-vlan enable
#
interface 10GE 0/0/1
 port link-type trunk
 port trunk allow-pass vlan 1100 1200 1300 1400 1500
#
remote-unit
 isolate enable
 commit all
#
remote-unit 0
 description RU101_10GE10/0/1
 name RU101
 bind interface 10GE10/0/1
remote-unit 1
 description RU201_10GE10/0/2
```

```
name RU201
bind interface 10GE10/0/2
#
```

1.1.2.4 环网接入 VRRP 网关配置案例

简介

在二层网络中，一旦网络存在环路就会造成报文在环路内不断循环和增生，产生广播风暴。在广播风暴的情况下，所有的有效带宽都被大量占用，导致网络变得不可用。应用二层环网技术，通过选择性地阻塞网络冗余链路，可以对环形网络形成逻辑环路进行破坏，达到消除环路的目的。但是网络的快速普及和相关应用的日益深入，各种增值业务（如 IPTV、视频会议等）已经开始广泛部署，基础网络的可靠性日益成为用户关注的焦点，能够保证网络传输不中断对于用户非常重要。VRRP 的出现很好地解决了这个问题。VRRP 能够在不改变组网的情况下，将多台设备组成一个虚拟设备，通过配置虚拟设备的 IP 地址为缺省网关，实现缺省网关的备份。当网关设备发生故障时，VRRP 机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。

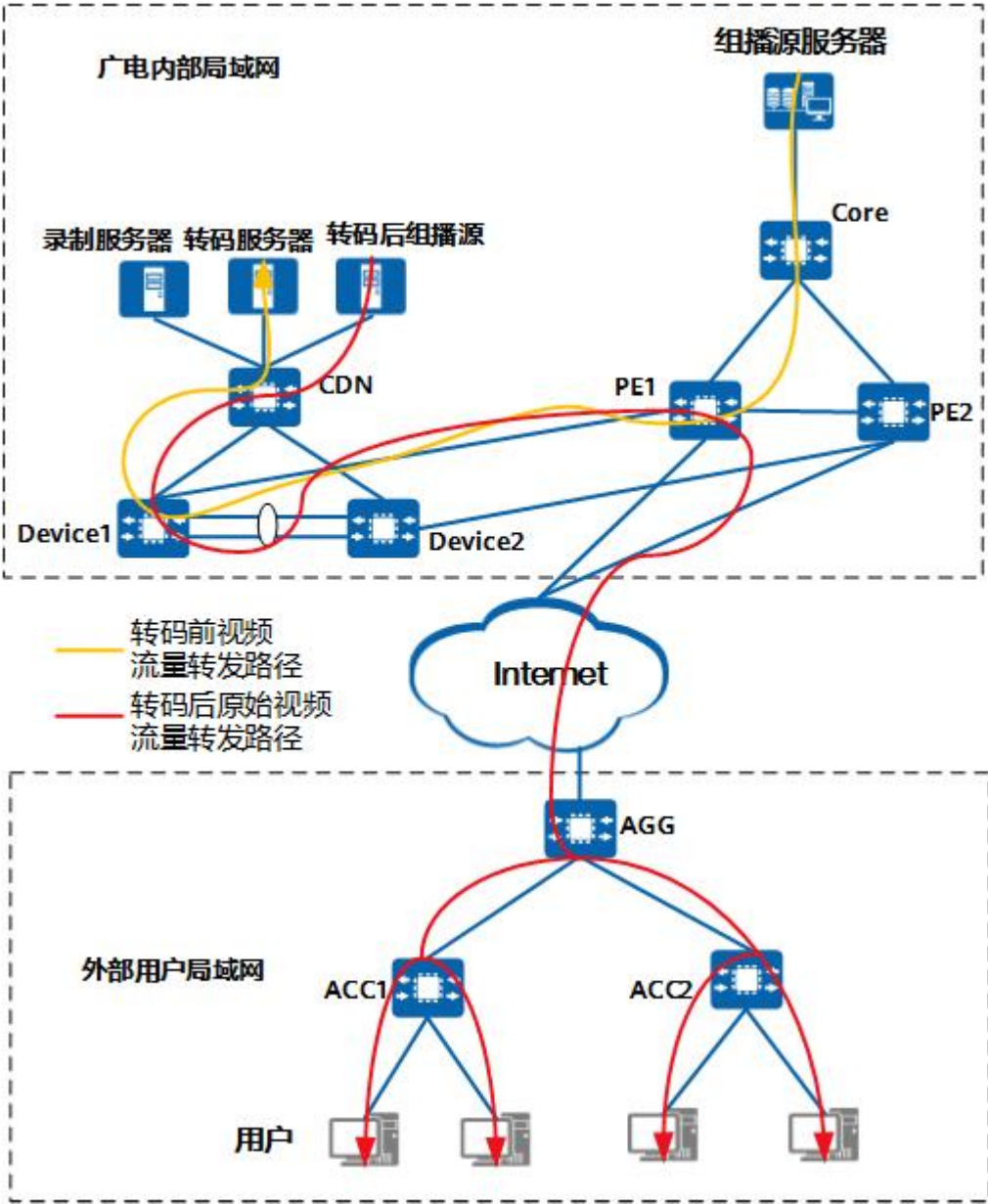
如图 1 所示是某个地区 IPTV 基本组网图。为了保证直播流的质量，组播源服务器发送的直播流需要先转发到转码服务器进行转码，然后由转码服务器再转发给用户。转码服务器通过环网双机备份的方式接入 IPTV 组网，提高网络可靠性。

组播源服务器发送的组播流正常转发路径是：Core->PE1->Device1->CDN->转码服务器。

转码服务器转换后的组播流正常转发路径是：转码服务器->CDN->Device1->PE1->AGG->ACC1 和 ACC2。

录制服务器到用户单播流正常转发路径是：录制服务器->CDN->Device1->PE1->AGG->ACC1 和 ACC2。

图 1 环网接入 VRRP 网关场景视频流量转发路径



组网需求

如图 2 所示为某地区 IPTV 组网图，用户可以点播直播节目，也可以回看电视节目。具体需求如下：

组播源服务器发送的组播直播流，先转发到 CDN 服务器转码录制后，再转发给用户。

用户也可以通过单播方式回看电视节目。

通过部署二、三层组播和 IGMP Snooping 功能，实现组播流转发。

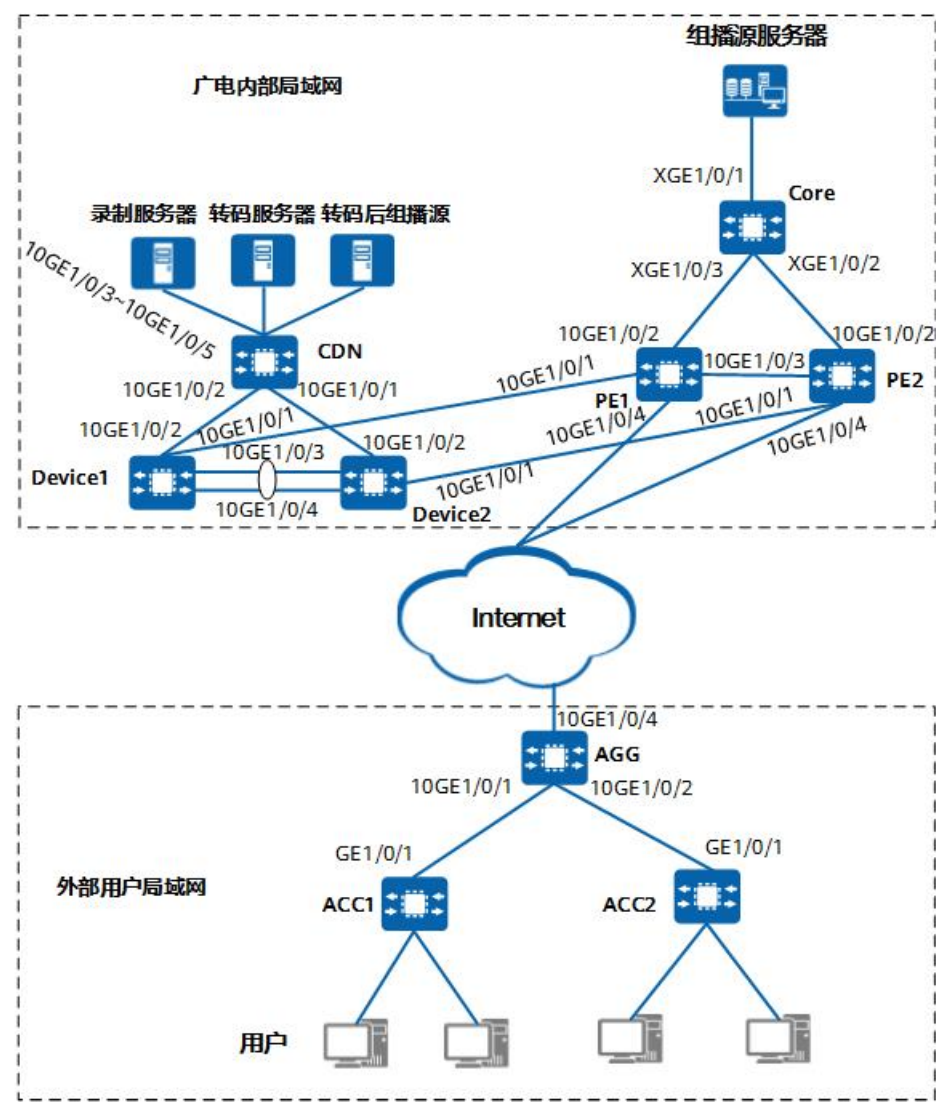
通过 OSPF 协议实现三层流量互通。Device1、Device2 与 PE1、PE2 通过 OSPF 1 区域 1 建立邻居关系，Core 与 PE1、PE2 通过 OSPF 1 区域 0 建立邻居关系。

CDN、Device1 和 Device2 部署 MSTP 破坏协议，在 Device1 和 Device2 上配置 VRRP 备份组。其中，Device1 上配置较高优先级和 20 秒抢占延时，作为 Master 设备承担流量转发；Device2 上配置较低优先级，作为备用设备，实现网关冗余备份，提高网络可靠性。

为保证接入安全，Device1 和 Device2 通过流策略限制组播源服务器的接入。

本举例中 Core 以 S12700 为例，PE1、PE2、AGG、CDN、Device1、Device2 以 S8700-6 为例，ACC1、ACC2 以 S5735-L 为例。

图 2 环网接入 VRRP 网关场景 IPTV 基本组网图



数据规划

表 1 VLAN 规划表

规划类型	规划取值	说明
VLAN	33	ACC1 下挂用户所属的 VLAN。
	34	ACC2 下挂用户所属的 VLAN。
	88	用户回看节目使用的 VLAN。
	301	Device1 和 Device2 使用的 VLAN。
	400	组播直播流转码后使用的 VLAN。
	530	组播直播流未转码前使用的 VLAN。

表 2 IP 地址规划表

设备	规划类型	规划取值	说明
Core	XGE1/0/1	10.6.1.3/24	连接组播源服务器的三层接口。
	XGE1/0/2	10.7.1.3/24	连接 PE2 的三层接口。
	XGE1/0/3	10.8.1.2/24	连接 PE1 的三层接口。
	LoopBack0	10.0.0.3/24	—
PE1	10GE1/0/2	10.12.1.1/24	连接 Core 的三层接口。
	10GE1/0/3	10.60.1.1/24	连接 PE2 的三层接口。
	Vlanif10	10.1.1.1/24，对应物理接口是 10GE1/0/1	连接 Device1 的接口。
	Vlanif11	10.11.1.1/24，对应物理接口是 10GE1/0/4	连接外部网络的接口。
	LoopBack0	10.0.0.1/24	—
PE2	10GE1/0/2	10.20.1.2/24	连接 Core 的三层接口。
	10GE1/0/3	10.60.1.2/24	连接 PE1 的三层接口。
	Vlanif10	10.1.2.1/24，对应物理接口是 10GE1/0/1	连接 Device2 的接口。
	Vlanif22	10.22.1.2/24，对应物理接口是 10GE1/0/4	连接外部网络的接口。
	LoopBack0	10.0.0.2/24	—
AGG	Vlanif13	10.11.1.8/24，对应物理接口是 10GE1/0/4	连接视频网络出口的接口。
	Vlanif33	10.33.1.8/24，对应物理接口是 10GE1/0/1	连接 ACC1 的接口。
	Vlanif34	10.34.1.8/24，对应物理接口是 10GE1/0/2	连接 ACC2 的接口。
	LoopBack0	10.0.0.4/24	—
Device1	Vlanif10	10.1.1.2/24，对应物理接口是 10GE1/0/1	连接 PE1 的接口。
	Vlanif88	10.88.1.7/24，对应物理接口是 10GE1/0/2	用于与录制服务器通信。

表 2 IP 地址规划表

设备	规划类型	规划取值	说明
	Vlanif301	10.31.1.1/24，对应物理接口是 10GE1/0/3 和 10GE1/0/4	连接 Device2 的接口。10GE1/0/3 和 10GE1/0/4 绑定为 Eth-Trunk1。
	Vlanif400	10.4.1.2/24，对应物理接口是 10GE1/0/2	用于与转码后的服务器通信。
	Vlanif530	10.5.1.2/24，对应物理接口是 10GE1/0/2	用于与转码前的服务器通信。
Device2	Vlanif10	10.1.2.2/24，对应物理接口是 10GE1/0/1	连接 PE2 的接口。
	Vlanif88	10.88.1.5/24，对应物理接口是 10GE1/0/2	用于与录制服务器通信。
	Vlanif301	10.31.1.2/24，对应物理接口是 10GE1/0/3 和 10GE1/0/4	连接 Device1 的接口。10GE1/0/3 和 10GE1/0/4 绑定为 Eth-Trunk1。
	Vlanif400	10.4.1.3/24，对应物理接口是 10GE1/0/2	用于与转码后的服务器通信。
	Vlanif530	10.5.1.3/24，对应物理接口是 10GE1/0/2	用于与转码前的服务器通信。

适用产品和版本

表 3 适用的产品和版本

产品/子系列	版本
S5735-L	从 V200R019C00 版本开始支持
S12700	从 V200R019C00 版本开始支持
S8700	从 V600R021C10 版本开始支持

配置思路

表 4 环网接入 VRRP 网关组网配置思路

步骤	配置思路
1	在 ACC、AGG、PE、Device、CDN 设备上创建 VLAN 并配置各接口所属 VLAN。

表 4 环网接入 VRRP 网关组网配置思路

步骤	配置思路
2	在 Device1、Device2、CDN 设备上配置 MSTP 破坏功能，破坏二层环路。
3	在 Core、PE、AGG、Device 设备上配置各 VLANIF 接口的 IP 地址。
4	在 Device1、Device2 设备上配置 VRRP 功能，实现网关备份。
5	在 Core、PE、Device 设备上配置 OSPF 功能，实现三层互通。
6	在 Core、PE、AGG、Device 设备上配置三层组播功能。
7	在 ACC、Device 设备上配置 IGMP Snooping 二层组播功能。
8	在 Device1、Device2 设备上配置流策略，控制组播源的接入。

操作步骤

1. 创建 VLAN 并配置各接口所属 VLAN。

在 ACC1 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1
[ACC1] vlan batch 33
[ACC1] interface GE 1/0/1
[ACC1-GE1/0/1] description ACC1***to***AGG
[ACC1-GE1/0/1] port link-type trunk
[ACC1-GE1/0/1] port trunk allow-pass vlan 33
[ACC1-GE1/0/1] quit
[ACC1] interface GE 1/0/2
[ACC1-GE1/0/2] port link-type access
[ACC1-GE1/0/2] port default vlan 33
[ACC1-GE1/0/2] quit
[ACC1] interface GE 1/0/3
[ACC1-GE1/0/3] port link-type access
[ACC1-GE1/0/3] port default vlan 33
[ACC1-GE1/0/3] quit
```

在 ACC2 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC2
[ACC2] vlan batch 34
[ACC2] interface GE 1/0/1
[ACC2-GE1/0/1] description ACC2***to***AGG
```

```
[ACC2-GE1/0/1] port link-type trunk
[ACC2-GE1/0/1] port trunk allow-pass vlan 34
[ACC2-GE1/0/1] quit
[ACC2] interface GE 1/0/2
[ACC2-GE1/0/2] port link-type access
[ACC2-GE1/0/2] port default vlan 34
[ACC2-GE1/0/2] quit
[ACC2] interface GE 1/0/3
[ACC2-GE1/0/3] port link-type access
[ACC2-GE1/0/3] port default vlan 34
[ACC2-GE1/0/3] quit
```

在 AGG 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname AGG
[AGG] vlan batch 11 22 33 to 34
[AGG] interface 10GE 1/0/1
[AGG-10GE1/0/1] description AGG***to***ACC1
[AGG-10GE1/0/1] port link-type trunk
[AGG-10GE1/0/1] port trunk allow-pass vlan 33
[AGG-10GE1/0/1] quit
[AGG] interface 10GE 1/0/2
[AGG-10GE1/0/2] description AGG***to***ACC2
[AGG-10GE1/0/2] port link-type trunk
[AGG-10GE1/0/2] port trunk allow-pass vlan 34
[AGG-10GE1/0/2] quit
[AGG] interface 10GE 1/0/4
[AGG-10GE1/0/4] description AGG***to***PE1
[AGG-10GE1/0/4] port link-type trunk
[AGG-10GE1/0/4] port trunk allow-pass vlan 11
[AGG-10GE1/0/4] quit
[AGG] interface 10GE 1/0/5
[AGG-10GE1/0/5] description AGG***to***PE2
[AGG-10GE1/0/5] port link-type trunk
[AGG-10GE1/0/5] port trunk allow-pass vlan 22
[AGG-10GE1/0/5] quit
```

在 PE1 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] vlan batch 10 to 11
[PE1] interface 10GE 1/0/1
[PE1-10GE1/0/1] description PE1***to***Device1
```

```
[PE1-10GE1/0/1] port link-type access
[PE1-10GE1/0/1] port default vlan 10
[PE1-10GE1/0/1] quit
[PE1] interface 10GE 1/0/4
[PE1-10GE1/0/4] description PE1****to***AGG
[PE1-10GE1/0/4] port link-type trunk
[PE1-10GE1/0/4] port trunk allow-pass vlan 11
[PE1-10GE1/0/4] quit
```

在 PE2 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] vlan batch 10 22
[PE2] interface 10GE 1/0/1
[PE2-10GE1/0/1] description PE2****to***Device2
[PE2-10GE1/0/1] port link-type access
[PE2-10GE1/0/1] port default vlan 10
[PE2-10GE1/0/1] quit
[PE2] interface 10GE 1/0/4
[PE2-10GE1/0/4] description PE2****to***AGG
[PE2-10GE1/0/4] port link-type trunk
[PE2-10GE1/0/4] port trunk allow-pass vlan 22
[PE2-10GE1/0/4] quit
```

在 Device1 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname Device1
[Device1] vlan batch 10 88 301 400 530
[Device1] interface eth-trunk1
[Device1-Eth-Trunk1] description Device1****to***Device2
[Device1-Eth-Trunk1] port link-type trunk
[Device1-Eth-Trunk1] port trunk allow-pass vlan 88 301 400 530
[Device1-Eth-Trunk1] quit
[Device1] interface 10GE 1/0/3
[Device1-10GE1/0/3] eth-trunk 1
[Device1-10GE1/0/3] quit
[Device1] interface 10GE 1/0/4
[Device1-10GE1/0/4] eth-trunk 1
[Device1-10GE1/0/4] quit
[Device1] interface 10GE 1/0/1
[Device1-10GE1/0/1] description Device1****to***PE1
[Device1-10GE1/0/1] port link-type access
[Device1-10GE1/0/1] port default vlan 10
```

```
[Device1-10GE1/0/1] quit
[Device1] interface 10GE 1/0/2
[Device1-10GE1/0/2] description Device1***to***CDN
[Device1-10GE1/0/2] port link-type trunk
[Device1-10GE1/0/2] port trunk allow-pass vlan 88 301 400 530
[Device1-10GE1/0/2] quit
```

在 Device2 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname Device2
[Device2] vlan batch 10 88 301 400 530
[Device2] interface eth-trunk1
[Device2-Eth-Trunk1] description Device1***to***Device2
[Device2-Eth-Trunk1] port link-type trunk
[Device2-Eth-Trunk1] port trunk allow-pass vlan 88 301 400 530
[Device2-Eth-Trunk1] quit
[Device2] interface 10GE 1/0/3
[Device2-10GE1/0/3] eth-trunk 1
[Device2-10GE1/0/3] quit
[Device2] interface 10GE 1/0/4
[Device2-10GE1/0/4] eth-trunk 1
[Device2-10GE1/0/4] quit
[Device2] interface 10GE 1/0/1
[Device2-10GE1/0/1] description Device2***to***PE2
[Device2-10GE1/0/1] port link-type access
[Device2-10GE1/0/1] port default vlan 10
[Device2-10GE1/0/1] quit
[Device2] interface 10GE 1/0/2
[Device2-10GE1/0/2] description Device2***to***CDN
[Device2-10GE1/0/2] port link-type trunk
[Device2-10GE1/0/2] port trunk allow-pass vlan 88 301 400 530
[Device2-10GE1/0/2] quit
```

在 CDN 上创建 VLAN，并将接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname CDN
[CDN] vlan batch 88 301 400 530
[CDN] interface 10GE 1/0/1
[CDN-10GE1/0/1] description CDN***to***Device2
[CDN-10GE1/0/1] port link-type trunk
[CDN-10GE1/0/1] port trunk allow-pass vlan 88 301 400 530
[CDN-10GE1/0/1] quit
[CDN] interface 10GE 1/0/2
```

```

[CDN-10GE1/0/2] description CDN***to***Device1
[CDN-10GE1/0/2] port link-type trunk
[CDN-10GE1/0/2] port trunk allow-pass vlan 88 301 400 530
[CDN-10GE1/0/2] quit
[CDN] interface 10GE 1/0/3
[CDN-10GE1/0/3] description CDN***to***HMS-Server
[CDN-10GE1/0/3] port link-type access
[CDN-10GE1/0/3] port default vlan 88
[CDN-10GE1/0/3] quit
[CDN] interface 10GE 1/0/4
[CDN-10GE1/0/4] description CDN***to***MRF-IN
[CDN-10GE1/0/4] port link-type access
[CDN-10GE1/0/4] port default vlan 400
[CDN-10GE1/0/4] quit
[CDN] interface 10GE 1/0/5
[CDN-10GE1/0/5] description CDN***to***MRF-OUT
[CDN-10GE1/0/5] port link-type access
[CDN-10GE1/0/5] port default vlan 530
[CDN-10GE1/0/5] quit

```

2. 配置 STP。Device1、Device2 和 CDN 组成二层环路，通过 MSTP 进行破坏。

在 Device1 配置 MSTP 域并使能 STP 功能。

```

[Device1] stp region-configuration
[Device1-mst-region] region-name IPTV
[Device1-mst-region] instance 1 vlan 530
[Device1-mst-region] instance 2 vlan 88 301 400
[Device1-mst-region] quit
[Device1] stp instance 1 root primary
[Device1] stp instance 2 root secondary
[Device1] stp enable //缺省情况下，设备全局和接口下都已使能 STP 功能。下面仅需要将不需要参与 STP 计算的接口去使能 STP 功能。
[Device1] interface 10GE 1/0/1
[Device1-10GE1/0/1] stp disable
[Device1-10GE1/0/1] quit

```

在 Device2 配置 MSTP 域并使能 STP 功能。

```

[Device2] stp region-configuration
[Device2-mst-region] region-name IPTV
[Device2-mst-region] instance 1 vlan 530
[Device2-mst-region] instance 2 vlan 88 301 400
[Device2-mst-region] quit
[Device2] stp instance 1 root secondary
[Device2] stp instance 2 root primary

```

```
[Device2] stp enable //缺省情况下，设备全局和接口下都已使能 STP 功能。下面仅需要将不需要参与 STP 计算的接口去使能 STP 功能。
```

```
[Device2] interface 10GE 1/0/1
```

```
[Device2-10GE1/0/1] stp disable
```

```
[Device2-10GE1/0/1] quit
```

在 CDN 配置 MSTP 域并使能 STP 功能。

```
[CDN] stp region-configuration
```

```
[CDN-mst-region] region-name IPTV
```

```
[CDN-mst-region] instance 1 vlan 530
```

```
[CDN-mst-region] instance 2 vlan 88 301 400
```

```
[CDN-mst-region] quit
```

```
[CDN] stp enable //缺省情况下，设备全局和接口下都已使能 STP 功能。下面仅需要将不需要参与 STP 计算的接口去使能 STP 功能。
```

```
[CDN] interface 10GE 1/0/3
```

```
[CDN-10GE1/0/3] stp disable
```

```
[CDN-10GE1/0/3] quit
```

```
[CDN] interface 10GE 1/0/4
```

```
[CDN-10GE1/0/4] stp disable
```

```
[CDN-10GE1/0/4] quit
```

```
[CDN] interface 10GE 1/0/5
```

```
[CDN-10GE1/0/5] stp disable
```

```
[CDN-10GE1/0/5] quit
```

3. 配置各接口的 IP 地址。

在 Core 配置接口的 IP 地址。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname Core
```

```
[Core] interface XGE 1/0/1
```

```
[Core-XGE1/0/1] undo portswitch
```

```
[Core-XGE1/0/1] description Core***to***Sever
```

```
[Core-XGE1/0/1] ip address 10.6.1.3 255.255.255.0
```

```
[Core-XGE1/0/1] quit
```

```
[Core] interface XGE 1/0/2
```

```
[Core-XGE1/0/2] undo portswitch
```

```
[Core-XGE1/0/2] description Core***to***PE2
```

```
[Core-XGE1/0/2] ip address 10.7.1.3 255.255.255.0
```

```
[Core-XGE1/0/2] quit
```

```
[Core] interface XGE 1/0/3
```

```
[Core-XGE1/0/3] undo portswitch
```

```
[Core-XGE1/0/3] description Core***to***PE1
```

```
[Core-XGE1/0/3] ip address 10.8.1.2 255.255.255.0
```

```
[Core-XGE1/0/3] quit
```

```
[Core] interface LoopBack0
[Core-LoopBack0] ip address 10.0.0.3 255.255.255.255
[Core-LoopBack0] quit
```

在 PE1 配置接口的 IP 地址。

```
[PE1] interface vlanif 10
[PE1-Vlanif10] description to***Device1
[PE1-Vlanif10] ip address 10.1.1.1 255.255.255.0
[PE1-Vlanif10] quit
[PE1] interface vlanif 11
[PE1-Vlanif11] description to***Internet
[PE1-Vlanif11] ip address 10.11.1.1 255.255.255.0
[PE1-Vlanif11] quit
[PE1] interface 10GE 1/0/2
[PE1-10GE1/0/2] undo portswitch
[PE1-10GE1/0/2] description PE1***to***Core
[PE1-10GE1/0/2] ip address 10.12.1.1 255.255.255.0
[PE1-10GE1/0/2] quit
[PE1] interface 10GE 1/0/3
[PE1-10GE1/0/3] undo portswitch
[PE1-10GE1/0/3] description PE1***to***PE2
[PE1-10GE1/0/3] ip address 10.60.1.1 255.255.255.0
[PE1-10GE1/0/3] quit
[PE1] interface LoopBack0
[PE1-LoopBack0] ip address 10.0.0.1 255.255.255.255
[PE1-LoopBack0] quit
```

在 PE2 配置接口的 IP 地址。

```
[PE2] interface vlanif 10
[PE2-Vlanif10] description to***Device2
[PE2-Vlanif10] ip address 10.1.2.1 255.255.255.0
[PE2-Vlanif10] quit
[PE2] interface vlanif 22
[PE2-Vlanif22] description to***Internet
[PE2-Vlanif22] ip address 10.22.1.2 255.255.255.0
[PE2-Vlanif22] quit
[PE2] interface 10GE 1/0/2
[PE2-10GE1/0/2] undo portswitch
[PE2-10GE1/0/2] description PE2***to***Core
[PE2-10GE1/0/2] ip address 10.20.1.2 255.255.255.0
[PE2-10GE1/0/2] quit
[PE2] interface 10GE 1/0/3
[PE2-10GE1/0/3] undo portswitch
```



```
[PE2-10GE1/0/3] description PE2***to***PE1
[PE2-10GE1/0/3] ip address 10.60.1.2 255.255.255.0
[PE2-10GE1/0/3] quit
[PE2] interface LoopBack0
[PE2-LoopBack0] ip address 10.0.0.2 255.255.255.255
[PE2-LoopBack0] quit
```

在 AGG 配置接口的 IP 地址。

```
[AGG] interface vlanif 13
[AGG-Vlanif11] description to***Internet
[AGG-Vlanif11] ip address 10.11.1.8 255.255.255.0
[AGG-Vlanif11] quit
[AGG] interface vlanif 33
[AGG-Vlanif33] description to***ACC1
[AGG-Vlanif33] ip address 10.33.1.8 255.255.255.0
[AGG-Vlanif33] quit
[AGG] interface vlanif 34
[AGG-Vlanif34] description to***ACC2
[AGG-Vlanif34] ip address 10.34.1.8 255.255.255.0
[AGG-Vlanif34] quit
[AGG] interface LoopBack0
[AGG-LoopBack0] ip address 10.0.0.4 255.255.255.255
[AGG-LoopBack0] quit
```

在 Device1 配置接口的 IP 地址。

```
[Device1] interface vlanif 10
[Device1-Vlanif10] description to***PE1
[Device1-Vlanif10] ip address 10.1.1.2 255.255.255.0
[Device1-Vlanif10] quit
[Device1] interface vlanif 88
[Device1-Vlanif88] description to***HMS
[Device1-Vlanif88] ip address 10.88.1.7 255.255.255.0
[Device1-Vlanif88] quit
[Device1] interface vlanif 301
[Device1-Vlanif301] description to***Device2
[Device1-Vlanif301] ip address 10.31.1.1 255.255.255.0
[Device1-Vlanif301] quit
[Device1] interface vlanif 400
[Device1-Vlanif400] description to***MRF IN
[Device1-Vlanif400] ip address 10.4.1.2 255.255.255.0
[Device1-Vlanif400] quit
[Device1] interface vlanif 530
[Device1-Vlanif530] description to***MRF OUT
```

```
[Device1-Vlanif530] ip address 10.5.1.2 255.255.255.0
[Device1-Vlanif530] quit
```

在 Device2 配置接口的 IP 地址。

```
[Device2] interface vlanif 10
[Device2-Vlanif10] description to***PE2
[Device2-Vlanif10] ip address 10.1.2.2 255.255.255.0
[Device2-Vlanif10] quit
[Device2] interface vlanif 88
[Device2-Vlanif88] description to***HMS
[Device2-Vlanif88] ip address 10.88.1.5 255.255.255.0
[Device2-Vlanif88] quit
[Device2] interface vlanif 301
[Device2-Vlanif301] description to***Device2
[Device2-Vlanif301] ip address 10.31.1.2 255.255.255.0
[Device2-Vlanif301] quit
[Device2] interface vlanif 400
[Device2-Vlanif400] description to***MRF IN
[Device2-Vlanif400] ip address 10.4.1.3 255.255.255.0
[Device2-Vlanif400] quit
[Device2] interface vlanif 530
[Device2-Vlanif530] description to***MRF OUT
[Device2-Vlanif530] ip address 10.5.1.3 255.255.255.0
[Device2-Vlanif530] quit
```

4. 配置 VRRP 功能。

在 Device1 配置 VRRP 备份功能。

```
[Device1] interface vlanif 88
[Device1-Vlanif88] vrrp vrid 2 virtual-ip 10.88.1.100
[Device1-Vlanif88] vrrp vrid 2 priority 120
[Device1-Vlanif88] vrrp vrid 2 preempt-mode timer delay 20
[Device1-Vlanif88] vrrp vrid 2 track interface 10GE1/0/1 reduced 100
[Device1-Vlanif88] quit
[Device1] interface vlanif 400
[Device1-Vlanif400] vrrp vrid 40 virtual-ip 10.4.1.10
[Device1-Vlanif400] vrrp vrid 40 priority 120
[Device1-Vlanif400] quit
[Device1] interface vlanif 530
[Device1-Vlanif530] vrrp vrid 53 virtual-ip 10.5.1.10
[Device1-Vlanif530] vrrp vrid 53 priority 120
[Device1-Vlanif530] quit
```

在 Device2 配置 VRRP 备份功能。

```
[Device2] interface vlanif 88
[Device2-Vlanif88] vrrp vrid 2 virtual-ip 10.88.1.100
[Device2-Vlanif88] quit
[Device2] interface vlanif 400
[Device2-Vlanif400] vrrp vrid 40 virtual-ip 10.4.1.10
[Device2-Vlanif400] quit
[Device2] interface vlanif 530
[Device2-Vlanif530] vrrp vrid 53 virtual-ip 10.5.1.10
[Device2-Vlanif530] quit
```

5. 配置 OSPF 功能。

在 Core 配置 OSPF 功能。

```
[Core] ospf 1
[Core-ospf-1] area 0
[Core-ospf-1-area-0.0.0.0] quit
[Core-ospf-1] quit
[Core] interface XGE 1/0/1
[Core-XGE1/0/1] ospf enable 1 area 0.0.0.0
[Core-10GE1/0/1] quit
[Core] interface XGE 1/0/2
[Core-XGE1/0/2] ospf enable 1 area 0.0.0.0
[Core-XGE1/0/2] quit
[Core] interface XGE 1/0/3
[Core-XGE1/0/3] ospf enable 1 area 0.0.0.0
[Core-XGE1/0/3] quit
[Core] interface LoopBack0
[Core-LoopBack0] ospf enable 1 area 0.0.0.0
[Core-LoopBack0] quit
```

在 PE1 配置 OSPF 功能。通过 Internet 网络保证 PE1 与 AGG 路由可达。

```
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] area 1
[PE1-ospf-1-area-0.0.0.1] nssa
[PE1-ospf-1-area-0.0.0.1] quit
[PE1-ospf-1] quit
[PE1] interface vlanif10
[PE1-Vlanif10] ospf enable 1 area 0.0.0.1
[PE1-Vlanif10] quit
[PE1] interface 10GE 1/0/2
[PE1-10GE1/0/2] ospf enable 1 area 0.0.0.0
[PE1-10GE1/0/2] quit
```

```
[PE1] interface 10GE 1/0/3
[PE1-10GE1/0/3] ospf enable 1 area 0.0.0.0
[PE1-10GE1/0/3] quit
[PE1] interface LoopBack0
[PE1-LoopBack0] ospf enable 1 area 0.0.0.0
[PE1-LoopBack0] quit
```

在 PE2 配置 OSPF 功能。通过 Internet 网络保证 PE2 与 AGG 路由可达。

```
[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] area 1
[PE2-ospf-1-area-0.0.0.1] nssa
[PE2-ospf-1-area-0.0.0.1] quit
[PE2-ospf-1] quit
[PE2] interface vlanif10
[PE2-Vlanif10] ospf enable 1 area 0.0.0.1
[PE2-Vlanif10] quit
[PE2] interface 10GE 1/0/2
[PE2-10GE1/0/2] ospf enable 1 area 0.0.0.0
[PE2-10GE1/0/2] quit
[PE2] interface 10GE 1/0/3
[PE2-10GE1/0/3] ospf enable 1 area 0.0.0.0
[PE2-10GE1/0/3] quit
[PE2] interface LoopBack0
[PE2-LoopBack0] ospf enable 1 area 0.0.0.0
[PE2-LoopBack0] quit
```

在 Device1 配置 OSPF 功能。

```
[Device1] interface vlanif10
[Device1-Vlanif10] ospf enable 1 area 0.0.0.1
[Device1-Vlanif10] quit
[Device1] interface vlanif301
[Device1-Vlanif301] ospf network-type p2p
[Device1-Vlanif301] ospf timer hello 1
[Device1-Vlanif301] quit
[Device1] ospf 1 router-id 192.168.1.1
[Device1-ospf-1] default-route-advertise
[Device1-ospf-1] silent-interface Vlanif88
[Device1-ospf-1] silent-interface Vlanif530
[Device1-ospf-1] silent-interface Vlanif400
[Device1-ospf-1] area 1
[Device1-ospf-1-area-0.0.0.1] network 10.5.1.0 0.0.0.255
```

```
[Device1-ospf-1-area-0.0.0.1] network 10.1.1.0 0.0.0.255
[Device1-ospf-1-area-0.0.0.1] network 10.31.1.0 0.0.0.255
[Device1-ospf-1-area-0.0.0.1] network 10.88.1.0 0.0.0.255
[Device1-ospf-1-area-0.0.0.1] nssa
[Device1-ospf-1-area-0.0.0.1] quit
[Device1-ospf-1] quit
```

在 Device2 配置 OSPF 功能。

```
[Device2] interface vlanif10
[Device2-Vlanif10] ospf enable 1 area 0.0.0.1
[Device2-Vlanif10] quit
[Device2] interface vlanif301
[Device2-Vlanif301] ospf network-type p2p
[Device2-Vlanif301] ospf timer hello 1
[Device2-Vlanif301] quit
[Device2] ospf 1 router-id 192.168.1.2
[Device2-ospf-1] default-route-advertise
[Device2-ospf-1] silent-interface Vlanif88
[Device2-ospf-1] silent-interface Vlanif530
[Device2-ospf-1] silent-interface Vlanif400
[Device2-ospf-1] area 1
[Device2-ospf-1-area-0.0.0.1] network 10.5.1.0 0.0.0.255
[Device2-ospf-1-area-0.0.0.1] network 10.1.1.0 0.0.0.255
[Device2-ospf-1-area-0.0.0.1] network 10.31.1.0 0.0.0.255
[Device2-ospf-1-area-0.0.0.1] network 10.88.1.0 0.0.0.255
[Device2-ospf-1-area-0.0.0.1] nssa
[Device2-ospf-1-area-0.0.0.1] quit
[Device2-ospf-1] quit
```

6. 配置三层组播功能。

在 Core 配置三层组播功能。

```
[Core] multicast routing-enable
[Core] pim
[Core-pim] static-rp 10.0.0.2
[Core-pim] quit
[Core] interface XGE 1/0/1
[Core-XGE1/0/1] pim sm
[Core-XGE1/0/1] quit
[Core] interface XGE 1/0/2
[Core-XGE1/0/2] pim sm
[Core-XGE1/0/2] quit
[Core] interface XGE 1/0/3
[Core-XGE1/0/3] pim sm
```

```
[Core-XGE1/0/3] quit
```

在 PE1 配置三层组播功能。

```
[PE1] multicast routing-enable
[PE1] pim
[PE1-pim] c-bsr LoopBack0
[PE1-pim] c-rp LoopBack0
[PE1-pim] static-rp 10.0.0.2
[PE1-pim] quit
[PE1] interface vlanif10
[PE1-Vlanif10] pim sm
[PE1-Vlanif10] quit
[PE1] interface vlanif11
[PE1-Vlanif11] pim sm
[PE1-Vlanif11] quit
[PE1] interface 10GE 1/0/2
[PE1-10GE1/0/2] pim sm
[PE1-10GE1/0/2] quit
[PE1] interface 10GE 1/0/3
[PE1-10GE1/0/3] pim sm
[PE1-10GE1/0/3] quit
[PE1] interface LoopBack0
[PE1-LoopBack0] pim sm
[PE1-LoopBack0] quit
```

在 PE2 配置三层组播功能。

```
[PE2] multicast routing-enable
[PE2] pim
[PE2-pim] static-rp 10.0.0.2
[PE2-pim] quit
[PE2] interface vlanif10
[PE2-Vlanif10] pim sm
[PE2-Vlanif10] quit
[PE2] interface vlanif22
[PE2-Vlanif22] pim sm
[PE2-Vlanif22] quit
[PE2] interface 10GE 1/0/2
[PE2-10GE1/0/2] pim sm
[PE2-10GE1/0/2] quit
[PE2] interface 10GE 1/0/3
[PE2-10GE1/0/3] pim sm
[PE2-10GE1/0/3] quit
[PE2] interface LoopBack0
```

```
[PE2-LoopBack0] pim sm
[PE2-LoopBack0] quit
```

在 AGG 配置三层组播功能。

```
[AGG] multicast routing-enable
[AGG] pim
[AGG-pim] static-rp 10.0.0.2
[AGG-pim] quit
[AGG] interface vlanif13
[AGG-Vlanif11] pim sm
[AGG-Vlanif11] quit
[AGG] interface vlanif33
[AGG-Vlanif33] pim sm
[AGG-Vlanif33] igmp enable //与用户相连，需要使能 IGMP 功能
[AGG-Vlanif33] quit
[AGG] interface vlanif34
[AGG-Vlanif34] pim sm
[AGG-Vlanif34] igmp enable
[AGG-Vlanif34] quit
```

在 Device1 配置三层组播功能。

```
[Device1] multicast routing-enable
[Device1] pim
[Device1-pim] static-rp 10.0.0.1
[Device1-pim] quit
[Device1] interface vlanif10
[Device1-Vlanif10] pim sm
[Device1-Vlanif10] quit
[Device1] interface vlanif301
[Device1-Vlanif301] pim sm
[Device1-Vlanif301] quit
[Device1] interface vlanif400
[Device1-Vlanif400] pim hello-option dr-priority 100 //调整优先级，保证组播流量优先从 Device1 转发
[Device1-Vlanif400] pim sm
[Device1-Vlanif400] igmp enable
[Device1-Vlanif400] quit
[Device1] interface vlanif530
[Device1-Vlanif530] pim sm
[Device1-Vlanif530] pim hello-option dr-priority 100
[Device1-Vlanif530] igmp enable //与解码服务器相连，需要使能 IGMP 功能
[Device1-Vlanif530] quit
```

在 Device2 配置三层组播功能。

```
[Device2] multicast routing-enable
[Device2] pim
[Device2-pim] static-rp 10.0.0.1
[Device2-pim] quit
[Device2] interface vlanif10
[Device2-Vlanif10] pim sm
[Device2-Vlanif10] quit
[Device2] interface vlanif301
[Device2-Vlanif301] pim sm
[Device2-Vlanif301] quit
[Device2] interface vlanif400
[Device2-Vlanif400] pim sm
[Device2-Vlanif400] igmp enable
[Device2-Vlanif400] quit
[Device2] interface vlanif530
[Device2-Vlanif530] pim sm
[Device2-Vlanif530] igmp enable
[Device2-Vlanif530] quit
```

7. 配置 IGMP Snooping 二层组播功能。

在 ACC1 上使能 IGMP Snooping 功能。

```
[ACC1] igmp-snooping enable
[ACC1] vlan 33
[ACC1-vlan33] igmp-snooping enable
[ACC1-vlan33] multicast drop-unknown
[ACC1-vlan33] quit
```

在 ACC2 上使能 IGMP Snooping 功能。

```
[ACC2] igmp-snooping enable
[ACC2] vlan 34
[ACC2-vlan34] igmp-snooping enable
[ACC2-vlan34] multicast drop-unknown
[ACC2-vlan34] quit
```

在 Device1 上使能 IGMP Snooping 功能。

```
[Device1] igmp-snooping enable
[Device1] vlan 301
[Device1-vlan301] igmp-snooping enable
[Device1-vlan301] quit
[Device1] vlan 530
[Device1-vlan530] igmp-snooping enable
[Device1-vlan530] quit
```


在 Device2 上使能 IGMP Snooping 功能。

```
[Device2] igmp-snooping enable
[Device2] vlan 301
[Device2-vlan301] igmp-snooping enable
[Device2-vlan301] quit
[Device2] vlan 530
[Device2-vlan530] igmp-snooping enable
[Device2-vlan530] quit
```

8. 配置流策略限制组播源接入。

在 Device1 上配置流策略。

```
[Device1] acl number 3000
[Device1-acl-adv-3000] description ***ACL FOR IPTV_Service_IN***
[Device1-acl-adv-3000] rule 1 permit ip source 10.66.1.1 0.0.0.255 destination 10.4.1.1 0.0.0.127
[Device1-acl-adv-3000] quit
[Device1] acl number 3998
[Device1-acl-adv-3998] description ***ACL FOR Multicast Remark***
[Device1-acl-adv-3998] rule 5 permit ip source 10.5.1.80 0.0.0.15
[Device1-acl-adv-3998] quit
[Device1] traffic classifier IPTV_Service_IN
[Device1-classifier-IPTV_Service_IN] if-match acl 3000
[Device1-classifier-IPTV_Service_IN] quit
[Device1] traffic classifier IPTV_Multicast_Remark
[Device1-classifier-IPTV_Multicast_Remark] if-match acl 3998
[Device1-classifier-IPTV_Multicast_Remark] quit
[Device1] traffic behavior IPTV_Service_IN
[Device1-behavior-IPTV_Service_IN] permit
[Device1-behavior-IPTV_Service_IN] quit
[Device1] traffic behavior IPTV_Multicast_Remark
[Device1-behavior-IPTV_Multicast_Remark] permit
[Device1-behavior-IPTV_Multicast_Remark] remark dscp af41
[Device1-behavior-IPTV_Multicast_Remark] quit
[Device1] traffic policy IPTV_Service_IN
[Device1-trafficpolicy-IPTV_Service_IN] classifier IPTV_Service_IN behavior IPTV_Service_IN
[Device1-trafficpolicy-IPTV_Service_IN] quit
[Device1] traffic policy IPTV_Multicast_Remark
[Device1-trafficpolicy-IPTV_Multicast_Remark] classifier IPTV_Multicast_Remark behavior
IPTV_Multicast_Remark
[Device1-trafficpolicy-IPTV_Multicast_Remark] quit
[Device1] interface 10GE 1/0/1
[Device1-10GE1/0/1] traffic-policy IPTV_Service_IN inbound
[Device1-10GE1/0/1] quit
```

```
[Device1] interface 10GE 1/0/2
[Device1-10GE1/0/2] traffic-policy IPTV_Multicast_Remark inbound
[Device1-10GE1/0/2] quit
```

在 Device2 上配置流策略。

```
[Device2] acl number 3000
[Device2-acl-adv-3000] description ***ACL FOR IPTV_Service_IN***
[Device2-acl-adv-3000] rule 1 permit ip source 10.66.1.1 0.0.0.255 destination 10.4.1.1 0.0.0.127
[Device2-acl-adv-3000] quit
[Device2] acl number 3998
[Device2-acl-adv-3998] description ***ACL FOR Multicast Remark***
[Device2-acl-adv-3998] rule 5 permit ip source 10.5.1.80 0.0.0.15
[Device2-acl-adv-3998] quit
[Device2] traffic classifier IPTV_Service_IN
[Device2-classifier-IPTV_Service_IN] if-match acl 3000
[Device2-classifier-IPTV_Service_IN] quit
[Device2] traffic classifier IPTV_Multicast_Remark
[Device2-classifier-IPTV_Multicast_Remark] if-match acl 3998
[Device2-classifier-IPTV_Multicast_Remark] quit
[Device2] traffic behavior IPTV_Service_IN
[Device2-behavior-IPTV_Service_IN] permit
[Device2-behavior-IPTV_Service_IN] quit
[Device2] traffic behavior IPTV_Multicast_Remark
[Device2-behavior-IPTV_Multicast_Remark] permit
[Device2-behavior-IPTV_Multicast_Remark] remark dscp af41
[Device2-behavior-IPTV_Multicast_Remark] quit
[Device2] traffic policy IPTV_Service_IN
[Device2-trafficpolicy-IPTV_Service_IN] classifier IPTV_Service_IN behavior IPTV_Service_IN
[Device2-trafficpolicy-IPTV_Service_IN] quit
[Device2] traffic policy IPTV_Multicast_Remark
[Device2-trafficpolicy-IPTV_Multicast_Remark] classifier IPTV_Multicast_Remark behavior
IPTV_Multicast_Remark
[Device2-trafficpolicy-IPTV_Multicast_Remark] quit
[Device2] interface 10GE 1/0/1
[Device2-10GE1/0/1] traffic-policy IPTV_Service_IN inbound
[Device2-10GE1/0/1] quit
[Device2] interface 10GE 1/0/2
[Device2-10GE1/0/2] traffic-policy IPTV_Multicast_Remark inbound
[Device2-10GE1/0/2] quit
```

检查配置结果

1. 执行 **display pim neighbor** 命令，验证 Core、PE1、PE2 和 AGG 上可以正常生成 PIM 邻居信息。

[Core] display pim neighbor

VPN-Instance: public net

Total Number of Neighbors = 2

Neighbor	Interface	Uptime	Expires	Dr-Priority	BFD-Session
10.12.1.1	XGE1/0/3	01:09:01	00:01:43	1	N
10.20.1.2	XGE1/0/2	01:06:30	00:01:39	1	N

[PE1] display pim neighbor

VPN-Instance: public net

Total Number of Neighbors = 4

Neighbor	Interface	Uptime	Expires	Dr-Priority	BFD-Session
10.8.1.2	10GE1/0/2	01:10:48	00:01:27	1	N
10.60.1.2	10GE1/0/3	01:08:06	00:01:40	1	N
10.1.1.2	Vlanif10	00:39:38	00:01:21	1	N
10.11.1.8	Vlanif11	01:05:16	00:01:30	1	N

[PE2] display pim neighbor

VPN-Instance: public net

Total Number of Neighbors = 4

Neighbor	Interface	Uptime	Expires	Dr-Priority	BFD-Session
10.7.1.3	10GE1/0/2	01:11:32	00:01:42	1	N
10.60.1.1	10GE1/0/3	01:11:18	00:01:27	1	N
10.1.2.2	Vlanif10	00:41:06	00:01:39	1	N
10.22.1.8	Vlanif22	01:08:28	00:01:42	1	N

[AGG] display pim neighbor

VPN-Instance: public net

Total Number of Neighbors = 2

Neighbor	Interface	Uptime	Expires	Dr-Priority	BFD-Session
10.11.1.1	Vlanif11	01:09:30	00:01:20	1	N
10.22.1.2	Vlanif22	01:08:34	00:01:18	1	N

2. 执行 **display igmp-snooping port-info** 命令，验证用户发送 IGMP Report 报文后，ACC1 和 ACC2 上可以正常生成组播组成员端口信息。

[ACC1] display igmp-snooping port-info

Flag: S:Static D:Dynamic M:Ssm-mapping

A:Active P:Protocol T:Trill

(Source, Group) Port Flag

-

VLAN 33, 1 Entry(s)

```

(*, 225.1.1.1) GE1/0/2      -D-
                      GE1/0/3      -D-
                      2 port(s) include

```

```

-----
-
[ACC2] display igmp-snooping port-info

```

```

-----
Flag: S:Static   D:Dynamic   M:Ssm-mapping
      A:Active   P:Protocol   T:Trill
      (Source, Group) Port      Flag

```

```

-----
-
VLAN 34, 1 Entry(s)
      (*, 225.1.1.1) GE1/0/2      -D-
                      GE1/0/3      -D-
                      2 port(s) include

```

3. 执行 **display pim routing-table** 命令，组播源发送组播报文，解码服务器发送组播组加入报文后，Device1 和 PE1 上可以正常生成组播路由表。

```

[Device1] display pim routing-table

```

```

VPN-Instance: public net
Total 1 (*, G) entry; 0 (S, G) entry

```

```

(*, 225.0.0.1)
  RP: 10.0.0.1
  Protocol: pim-sm, Flag: WC
  UpTime: 00:06:50
  Upstream interface: Vlanif10
    Upstream neighbor: 10.1.1.1
    RPF prime neighbor: 10.1.1.1
  Downstream interface(s) information:
    Total number of downstreams: 1
      1: Vlanif530
        Protocol: igmp, UpTime: 00:01:42, Expires: -

```

```

[PE1] display pim routing-table

```

```

VPN-Instance: public net
Total 1 (*, G) entry; 0 (S, G) entry

```

```

(*, 225.0.0.1)
  RP: 10.0.0.1 (local)
  Protocol: pim-sm, Flag: WC

```

```
UpTime: 00:12:46
Upstream interface: Register
  Upstream neighbor: NULL
  RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
  1: Vlanif10
    Protocol: pim-sm, UpTime: 00:08:59, Expires: 00:02:31
```

配置脚本

Core 的配置脚本

```
#
sysname Core
#
multicast routing-enable
#
interface XGE1/0/1
undo portswitch
description Core***to***Sever
ip address 10.6.1.3 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.0
#
interface XGE1/0/2
undo portswitch
description Core***to***PE2
ip address 10.7.1.3 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.0
#
interface XGE1/0/3
undo portswitch
description Core***to***PE1
ip address 10.8.1.2 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.0
#
interface LoopBack0
ip address 10.0.0.3 255.255.255.255
ospf enable 1 area 0.0.0.0
#
```

```
ospf 1
 area 0.0.0.0
#
pim
 static-rp 10.0.0.2
#
return
```

PE1 的配置脚本

```
#
sysname PE1
#
vlan batch 10 to 11
#
multicast routing-enable
#
interface Vlanif10
 description to***Device1
 ip address 10.1.1.1 255.255.255.0
 pim sm
 ospf enable 1 area 0.0.0.1
#
interface Vlanif11
 description to***Internet
 ip address 10.11.1.1 255.255.255.0
 pim sm
 ospf enable 1 area 0.0.0.0
#
interface 10GE1/0/1
 description PE1***to***Device1
 port link-type access
 port default vlan 10
#
interface 10GE1/0/2
 undo portswitch
 description PE1***to***Core
 ip address 10.12.1.1 255.255.255.0
 pim sm
 ospf enable 1 area 0.0.0.0
#
interface 10GE1/0/3
 undo portswitch
```

```
description PE1***to***PE2
ip address 10.60.1.1 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.0
#
interface 10GE1/0/4
description PE1***to***AGG
port link-type trunk
port trunk allow-pass vlan 11
#
interface LoopBack0
ip address 10.0.0.1 255.255.255.255
pim sm
ospf enable 1 area 0.0.0.0
#
pim
c-bsr LoopBack0
c-rp LoopBack0
static-rp 10.0.0.2
#
return
```

PE2 的配置脚本

```
#
sysname PE2
#
vlan batch 10 22
#
multicast routing-enable
#
interface Vlanif10
description to***Device2
ip address 10.1.2.1 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.1
#
interface Vlanif22
description to***Internet
ip address 10.22.1.2 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.0
#
```

```
interface 10GE1/0/1
description PE2***to***Device2
port link-type access
port default vlan 10
#
interface 10GE1/0/2
undo portswitch
description PE2***to***Core
ip address 10.20.1.2 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.0
#
interface 10GE1/0/3
undo portswitch
description PE2***to***PE1
ip address 10.60.1.2 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.0
#
interface 10GE1/0/4
description PE2***to***AGG
port link-type trunk
port trunk allow-pass vlan 22
#
interface LoopBack0
ip address 10.0.0.2 255.255.255.255
ospf enable 1 area 0.0.0.0
#
pim
static-rp 10.0.0.2
#
return
```

Device1 的配置脚本

```
#
sysname Device1
#
vlan batch 10 88 301 400 530
#
stp instance 1 root primary
stp instance 2 root secondary
#
```



```
multicast routing-enable
#
igmp-snooping enable
#
stp region-configuration
 region-name IPTV
 instance 1 vlan 530
 instance 2 vlan 88 301 400
#
acl number 3000
 description ***ACL FOR IPTV_Service_IN***
 rule 1 permit ip source 10.66.1.1 0.0.0.255 destination 10.4.1.1 0.0.0.127
acl number 3998
 description ***ACL FOR Multicast Remark***
 rule 5 permit ip source 10.5.1.80 0.0.0.15
#
traffic classifier IPTV_Multicast_Remark operator or
 if-match acl 3998
traffic classifier IPTV_Service_IN operator or
 if-match acl 3000
#
traffic behavior IPTV_Multicast_Remark
 permit
 remark dscp af41
traffic behavior IPTV_Service_IN
 permit
#
traffic policy IPTV_Multicast_Remark match-order config
 classifier IPTV_Multicast_Remark behavior IPTV_Multicast_Remark
traffic policy IPTV_Service_IN match-order config
 classifier IPTV_Service_IN behavior IPTV_Service_IN
#
vlan 10
 description to***PE1
vlan 301
 description to***Device2
 igmp-snooping enable
vlan 400
 description ***MRF IN***
 multicast drop-unknown
 igmp-snooping enable
vlan 530
 description ***MRF OUT***
```

```
multicast drop-unknown
igmp-snooping enable
#
interface Vlanif10
description to***PE1
ip address 10.1.1.2 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.1
#
interface Vlanif88
description to***HMS
ip address 10.88.1.7 255.255.255.0
vrrp vrid 2 virtual-ip 10.88.1.100
vrrp vrid 2 priority 120
vrrp vrid 2 preempt-mode timer delay 20
vrrp vrid 2 track interface 10GE1/0/1 reduced 100
#
interface Vlanif301
description Device1***to***Device2
ip address 10.31.1.1 255.255.255.0
pim sm
ospf network-type p2p
ospf timer hello 1
#
interface Vlanif400
description to***MRF IN
ip address 10.4.1.2 255.255.255.0
vrrp vrid 40 virtual-ip 10.4.1.10
vrrp vrid 40 priority 120
pim hello-option dr-priority 100
pim sm
igmp enable
#
interface Vlanif530
description to***MRF OUT
ip address 10.5.1.2 255.255.255.0
vrrp vrid 53 virtual-ip 10.5.1.10
vrrp vrid 53 priority 120
pim hello-option dr-priority 100
pim sm
igmp enable
#
interface Eth-Trunk1
```

```
description Device1***to***Device2
port link-type trunk
port trunk allow-pass vlan 88 301 400 530
#
interface 10GE1/0/1
description Device1***to***PE1
port link-type access
port default vlan 10
stp disable
traffic-policy IPTV_Service_IN inbound
#
interface 10GE1/0/2
description Device1***to***CDN
port link-type trunk
port trunk allow-pass vlan 88 301 400 530
traffic-policy IPTV_Multicast_Remark inbound
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
eth-trunk 1
#
ospf 1 router-id 192.168.1.1
default-route-advertise
silent-interface Vlanif88
silent-interface Vlanif530
silent-interface Vlanif400
area 0.0.0.1
network 10.1.1.0 0.0.0.255
network 10.31.1.0 0.0.0.255
network 10.88.1.0 0.0.0.255
network 10.5.1.0 0.0.0.255
nssa
#
pim
static-rp 10.0.0.1
#
return
```

Device2 的配置脚本

```
#
```

```
sysname Device2
#
vlan batch 10 88 301 400 530
#
stp instance 1 root secondary
stp instance 2 root primary
#
multicast routing-enable
#
igmp-snooping enable
#
stp region-configuration
region-name IPTV
instance 1 vlan 530
instance 2 vlan 88 301 400
#
acl number 3000
description ***ACL FOR IPTV_Service_IN***
rule 1 permit ip source 10.66.1.1 0.0.0.255 destination 10.4.1.1 0.0.0.127
acl number 3998
description ***ACL FOR Multicast Remark***
rule 5 permit ip source 10.5.1.80 0.0.0.15
#
traffic classifier IPTV_Multicast_Remark operator or
if-match acl 3998
traffic classifier IPTV_Service_IN operator or
if-match acl 3000
#
traffic behavior IPTV_Multicast_Remark
permit
remark dscp af41
traffic behavior IPTV_Service_IN
permit
#
traffic policy IPTV_Multicast_Remark match-order config
classifier IPTV_Multicast_Remark behavior IPTV_Multicast_Remark
traffic policy IPTV_Service_IN match-order config
classifier IPTV_Service_IN behavior IPTV_Service_IN
#
vlan 10
description to***PE2
vlan 301
description to***Device1
```

```
igmp-snooping enable
vlan 400
description ***MRF IN***
multicast drop-unknown
igmp-snooping enable
vlan 530
description ***MRF OUT***
multicast drop-unknown
igmp-snooping enable
#
interface Vlanif10
description to***PE2
ip address 10.1.2.2 255.255.255.0
pim sm
ospf enable 1 area 0.0.0.1
#
interface Vlanif88
description to***HMS
ip address 10.88.1.5 255.255.255.0
vrrp vrid 2 virtual-ip 10.88.1.100
#
interface Vlanif301
description Device2***to***Device1
ip address 10.31.1.2 255.255.255.0
pim sm
ospf network-type p2p
ospf timer hello 1
#
interface Vlanif400
description to***MRF IN
ip address 10.4.1.3 255.255.255.0
vrrp vrid 40 virtual-ip 10.4.1.10
pim sm
igmp enable
#
interface Vlanif530
description to***MRF OUT
ip address 10.5.1.3 255.255.255.0
vrrp vrid 53 virtual-ip 10.5.1.10
pim sm
igmp enable
#
interface Eth-Trunk1
```

```
description Device2****to***Device1
port link-type trunk
port trunk allow-pass vlan 88 301 400 530
#
interface 10GE1/0/1
description Device2****to***PE2
port link-type access
port default vlan 10
stp disable
traffic-policy IPTV_Service_IN inbound
#
interface 10GE1/0/2
description Device2****to***CDN
port link-type trunk
port trunk allow-pass vlan 88 301 400 530
traffic-policy IPTV_Multicast_Remark inbound
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
eth-trunk 1
#
ospf 1 router-id 192.168.1.2
default-route-advertise
silent-interface Vlanif88
silent-interface Vlanif530
silent-interface Vlanif400
area 0.0.0.1
network 10.5.1.0 0.0.0.255
network 10.1.1.0 0.0.0.255
network 10.31.1.0 0.0.0.255
network 10.88.1.0 0.0.0.255
nssa
#
pim
static-rp 10.0.0.1
#
return
```

CDN 的配置脚本

```
#
```

```
sysname CDN
#
vlan batch 88 301 400 530
#
stp region-configuration
region-name IPTV
instance 1 vlan 530
instance 2 vlan 88 301 400
#
interface 10GE1/0/1
description CDN***to***Device2
port link-type trunk
port trunk allow-pass vlan 88 301 400 530
#
interface 10GE1/0/2
description CDN***to***Device1
port link-type trunk
port trunk allow-pass vlan 88 301 400 530
#
interface 10GE1/0/3
description CDN***to***HMS-Server
port link-type access
port default vlan 88
stp disable
#
interface 10GE1/0/4
description CDN***to***MRF-IN
port link-type access
port default vlan 400
stp disable
#
interface 10GE1/0/5
description CDN***to***MRF-OUT
port link-type access
port default vlan 530
stp disable
#
return
```

AGG 的配置脚本

```
#
sysname AGG
```

```
#
vlan batch 11 22 33 to 34
#
multicast routing-enable
#
interface Vlanif13
description to***Internet
ip address 10.11.1.8 255.255.255.0
pim sm
#
interface Vlanif33
description to***ACC1
ip address 10.33.1.8 255.255.255.0
pim sm
igmp enable
#
interface Vlanif34
description to***ACC2
ip address 10.34.1.8 255.255.255.0
pim sm
igmp enable
#
interface 10GE1/0/1
description AGG***to***ACC1
port link-type trunk
port trunk allow-pass vlan 33
#
interface 10GE1/0/2
description AGG***to***ACC2
port link-type trunk
port trunk allow-pass vlan 34
#
interface 10GE1/0/4
description AGG***to***PE1
port link-type trunk
port trunk allow-pass vlan 11
#
interface 10GE1/0/5
description AGG***to***PE2
port link-type trunk
port trunk allow-pass vlan 22
#
```



```
return
```

ACC1 的配置脚本

```
#
sysname ACC1
#
vlan batch 33
#
igmp-snooping enable
#
vlan 33
multicast drop-unknown
igmp-snooping enable
#
interface GE1/0/1
description ACC1***to***AGG
port link-type trunk
port trunk allow-pass vlan 33
#
interface GE1/0/2
port link-type access
port default vlan 33
#
interface GE1/0/3
port link-type access
port default vlan 33
#
return
```

ACC2 的配置脚本

```
#
sysname ACC2
#
vlan batch 34
#
igmp-snooping enable
#
vlan 34
multicast drop-unknown
igmp-snooping enable
#
interface GE1/0/1
```

```
description ACC2***to***AGG
port link-type trunk
port trunk allow-pass vlan 34
#
interface GE1/0/2
port link-type access
port default vlan 34
#
interface GE1/0/3
port link-type access
port default vlan 34
#
return
```

1.1.2.5 集中式网关部署方式的 VXLAN 配置案例

简介

VXLAN 是 NVO3 中的一种网络虚拟化技术，通过将虚拟机发出的数据包封装在 UDP 中，并使用物理网络的 IP、MAC 作为 outer-header 进行封装，然后在 IP 网络上传输，到达目的地后由隧道终结点解封装并将数据发送给目标虚拟机。通过 VXLAN，虚拟网络可接入大量租户，且租户可以规划自己的虚拟网络，不需要考虑物理网络 IP 地址和广播域的限制，降低了网络管理的难度。

在 VXLAN 网络中，不同 BD 间的用户需要通过 VXLAN 三层网关实现互通。其中，集中式网关是指三层网关集中部署在一台设备上，所有跨子网的流量都经过三层网关进行转发，实现流量的集中管理。

本示例实现了通过静态方式配置 VXLAN，构建集中式网关部署方式的虚拟网络。

组网需求

企业已经建成比较成熟的园区网络，但是没有专用的数据中心网络，所有的服务器分布在不同的部门，并且不具备集中放置的条件。现在用户希望在已有园区网络上构建一个虚拟网络，需求如下：

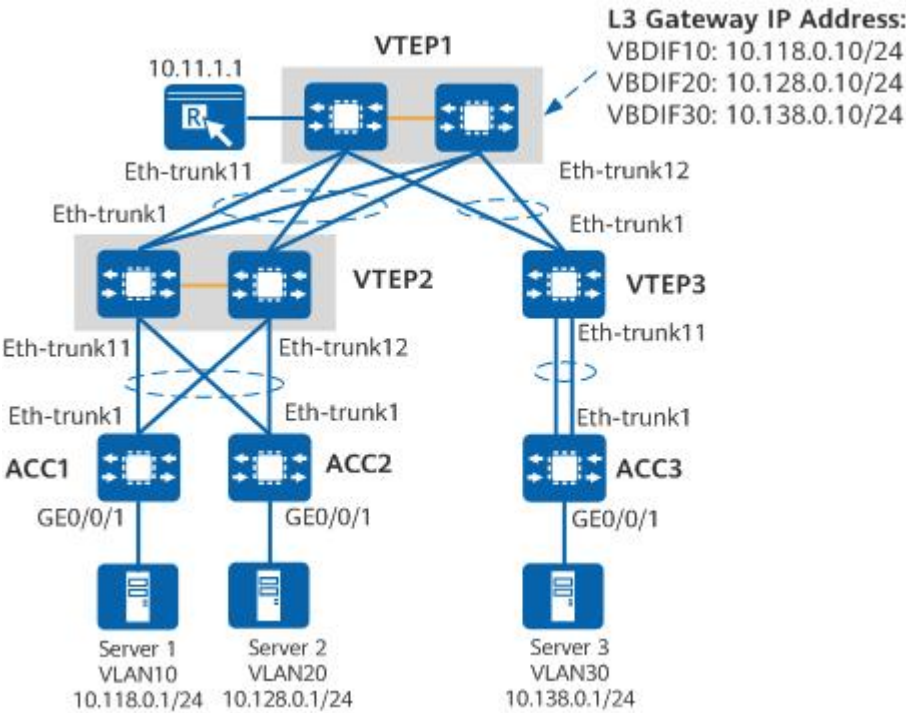
将散落在不同部门的服务器构建成一个虚拟网络，实现资源整合和业务灵活部署。

各服务器上部署着大量的 VM，不同业务的服务器之间需要实现三层互通。

服务器需要通过 MAC 认证，才能接入网络。

如图 1 所示，企业在不同的位置都拥有自己的 VM，Server1 属于 VLAN 10，Server2 属于 VLAN 20，Server3 属于 VLAN 30，现需要通过 VXLAN 隧道实现不同业务的服务器之间的三层互通。

图 1 集中式网关部署方式的 VXLAN 配置组网图



数据规划

表 1 部署 VXLAN 隧道相关数据

设备	VXLAN 隧道	BD	VNI	Source IP	Peer IP
VTEP1	VTEP1—>VTEP2	10	10	10.200.200.1	10.200.200.10
		20	20		
	VTEP1—>VTEP3	30	30	10.200.200.1	10.200.200.20
VTEP2	VTEP2—>VTEP1	10	10	10.200.200.10	10.200.200.1
		20	20		
VTEP3	VTEP3—>VTEP1	30	30	10.200.200.20	10.200.200.1

适用产品和版本

表 2 适用的产品和版本

产品/子系列	设备主机名	版本
S8700-6	VTEP1、VTEP2	V600R021C10 及之后版本
S6730-H-V2	VTEP3	V200R020C00 及之后版本
S5735-S-V2	ACC1、ACC3	V200R019C00 及之后版本

表 2 适用的产品和版本

产品/子系列	设备主机名	版本
S5735-L-V2	ACC2	V200R019C00 及之后版本

配置思路

表 3 VXLAN 集中式网关部署方式的虚拟网络配置思路

步骤	配置思路	涉及产品
1	组建集群。	两台 S8700-6，组建集群，并命名为 VTEP2；两台 S8700-6，组建集群，并命名为 VTEP1。
2	配置核心交换机与汇聚交换机之间的路由。	核心交换机（VTEP1）、汇聚交换机（VTEP2、VTEP3）。
3	配置 VLAN 接入，配置 VXLAN 业务接入点。	接入交换机（ACC1~ACC3）、汇聚交换机（VTEP2、VTEP3）。
4	配置 MAC 认证。其中，AAA 采用 RADIUS 认证。	汇聚交换机（VTEP2、VTEP3）。
5	配置 VXLAN 隧道。	核心交换机（VTEP1）、汇聚交换机（VTEP2、VTEP3）。
6	配置 VXLAN 三层网关。	核心交换机（VTEP1）。

操作步骤

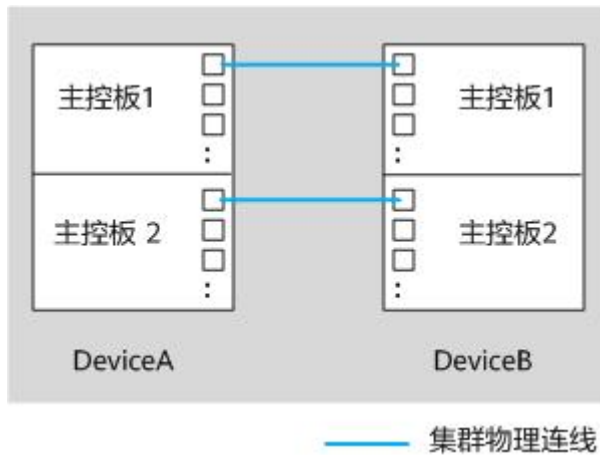
1. 组建集群

这里以 VTEP2 组建集群为例。VTEP1 组建集群的过程，与 VTEP2 组建集群的过程类似，因此不再赘述。

a. 连接集群线缆

VTEP2 采用两台 S8700-6 组建集群。分别将两台设备命名为 DeviceA 和 DeviceB。如图 2 所示，连接 DeviceA 和 DeviceB 之间的集群线缆。

图 2 集群连接示意图



b. 配置集群参数

配置 DeviceA 的集群成员 ID 为 1，优先级为 150，Domain ID 为 10。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] css
[DeviceA-css] css member 1
[DeviceA-css] css priority 150
[DeviceA-css] css domain 10
[DeviceA-css] quit
```

配置 DeviceB 的集群成员 ID 为 2，优先级为 100，Domain ID 为 10。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] css
[DeviceB-css] css member 2
[DeviceB-css] css priority 100
[DeviceB-css] css domain 10
[DeviceB-css] quit
```

c. 配置 Stack-Port 端口

建议在配置 Stack-Port 端口前，手动备份当前配置文件。

建议在配置 Stack-Port 端口前，先 **shutdown** 待加入的成员端口，避免端口因产生 CRC 错包而导致 Error-Down。配置过程省略。

在 DeviceA 上创建 Stack-Port 端口，将成员端口加入 Stack-Port 端口。

```
[DeviceA] interface stack-port 1
[DeviceA-Stack-Port1] port member-group interface 10ge 5/0/1 10ge 6/0/1
[DeviceA-Stack-Port1] quit
[DeviceA] quit
```

在 DeviceB 上创建 Stack-Port 端口，将成员端口加入 Stack-Port 端口。

```
[DeviceB] interface stack-port 1
[DeviceB-Stack-Port1] port member-group interface 10ge 5/0/1 10ge 6/0/1
[DeviceB-Stack-Port1] quit
[DeviceB] quit
```

undo shutdown 之前被关闭的成员端口，配置过程省略。

d. 保存配置并开启设备集群功能

保存 DeviceA 的配置并开启集群功能。先开启规划为主设备的 DeviceA 的集群功能。这样 DeviceA 可以先完成重启，从而优先成为主设备。为了使后面的配置易于理解，将主设备 DeviceA 的名称修改为 VTEP2。

```
<DeviceA> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
<DeviceA> system-view
[DeviceA] sysname VTEP2
[VTEP2] css
[VTEP2-css] css enable
Warning: Make sure that one or more dual-active detection methods are configured
once the conversion is complete and the device enters the CSS or stack mode. Switches
working in different forward modes cannot set up a CSS or stack.
Current configuration will be converted to the next startup saved-configuration
file of CSS or stack mode.
System will reboot. Continue? [Y/N]: y      //开启集群功能后，设备会自动重启。
```

保存 DeviceB 的配置并开启集群功能。

```
<DeviceB> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
<DeviceB> system-view
[DeviceB] css
[DeviceB-css] css enable
Warning: Make sure that one or more dual-active detection methods are configured
once the conversion is complete and the device enters the CSS or stack mode. Switches
working in different forward modes cannot set up a CSS or stack.
Current configuration will be converted to the next startup saved-configuration
file of CSS or stack mode.
System will reboot. Continue? [Y/N]: y      //开启集群功能后，设备会自动重启。
```

2. 配置核心交换机与汇聚交换机之间的路由

a. 配置核心交换机

配置各接口的 IP 地址。配置 OSPF 时，注意需要发布设备上的 Loopback 接口地址。

```
<VTEP1> system-view
[VTEP1] interface loopback 0
[VTEP1-LoopBack0] ip address 10.200.200.1 255.255.255.255
[VTEP1-LoopBack0] quit
[VTEP1] vlan batch 10 11 20 30 100 200
[VTEP1] interface vlanif 11
[VTEP1-Vlanif11] ip address 10.11.1.2 255.255.255.0
[VTEP1-Vlanif11] quit
```

```
[VTEP1] interface vlanif 100
[VTEP1-Vlanif100] ip address 10.1.100.1 255.255.255.252
[VTEP1-Vlanif100] quit
[VTEP1] interface vlanif 200
[VTEP1-Vlanif200] ip address 10.1.200.1 255.255.255.252
[VTEP1] interface eth-trunk 11
[VTEP1-Eth-Trunk11] description TO-VTEP2
[VTEP1-Eth-Trunk11] port link-type trunk
[VTEP1-Eth-Trunk11] undo port trunk allow-pass vlan 1
[VTEP1-Eth-Trunk11] port trunk allow-pass vlan 100
[VTEP1-Eth-Trunk11] quit
[VTEP1] interface eth-trunk 12
[VTEP1-Eth-Trunk12] description TO-VTEP3
[VTEP1-Eth-Trunk12] port link-type trunk
[VTEP1-Eth-Trunk12] undo port trunk allow-pass vlan 1
[VTEP1-Eth-Trunk12] port trunk allow-pass vlan 200
[VTEP1-Eth-Trunk12] quit
[VTEP1] interface 10GE 1/3/0/0
[VTEP1-10GE1/3/0/0] eth-trunk 11
[VTEP1-10GE1/3/0/0] quit
[VTEP1] interface 10GE 1/3/0/1
[VTEP1-10GE1/3/0/1] port link-type access
[VTEP1-10GE1/3/0/1] port default vlan 11
[VTEP1-10GE1/3/0/1] quit
[VTEP1] interface 10GE 1/3/0/13
[VTEP1-10GE1/3/0/13] eth-trunk 11
[VTEP1-10GE1/3/0/13] quit
[VTEP1] interface 10GE 2/3/0/2
[VTEP1-10GE2/3/0/2] eth-trunk 12
[VTEP1-10GE2/3/0/2] quit
[VTEP1] interface 10GE 2/3/0/14
[VTEP1-10GE2/3/0/14] eth-trunk 12
[VTEP1-10GE2/3/0/14] quit
[VTEP1] ospf router-id 10.200.200.1
[VTEP1-ospf-1] area 0
[VTEP1-ospf-1-area-0.0.0.0] network 10.200.200.1 0.0.0.0
[VTEP1-ospf-1-area-0.0.0.0] network 10.1.100.0 0.0.0.3
[VTEP1-ospf-1-area-0.0.0.0] network 10.1.200.0 0.0.0.3
[VTEP1-ospf-1-area-0.0.0.0] quit
[VTEP1-ospf-1] quit
```

b. 配置汇聚交换机

配置汇聚交换机 VTEP2。

```
<VTEP2> system-view
[VTEP2] interface loopback 0
[VTEP2-LoopBack0] ip address 10.200.200.10 255.255.255.255
[VTEP2-LoopBack0] quit
[VTEP2] vlan batch 10 20 100
[VTEP2] interface vlanif 100
[VTEP2-Vlanif100] ip address 10.1.100.2 255.255.255.252
[VTEP2-Vlanif100] quit
[VTEP2] interface eth-trunk 1
[VTEP2-Eth-Trunk1] port link-type trunk
[VTEP2-Eth-Trunk1] undo port trunk allow-pass vlan 1
[VTEP2-Eth-Trunk1] port trunk allow-pass vlan 100
[VTEP2-Eth-Trunk1] quit
[VTEP2] interface 10GE 1/2/0/2
[VTEP2-10GE1/2/0/2] eth-trunk 1
[VTEP2-10GE1/2/0/2] quit
[VTEP2] interface 10GE 1/2/0/3
[VTEP2-10GE1/2/0/3] eth-trunk 1
[VTEP2-10GE1/2/0/3] quit
[VTEP2] ospf router-id 10.200.200.10
[VTEP2-ospf-1] area 0
[VTEP2-ospf-1-area-0.0.0.0] network 10.200.200.10 0.0.0.0
[VTEP2-ospf-1-area-0.0.0.0] network 10.1.100.0 0.0.0.3
[VTEP2-ospf-1-area-0.0.0.0] quit
[VTEP2-ospf-1] quit
```

配置汇聚交换机 VTEP3。

```
<HUAWEI> system-view
[HUAWEI] sysname VTEP3
[VTEP3] interface loopback 0
[VTEP3-LoopBack0] ip address 10.200.200.20 255.255.255.255
[VTEP3-LoopBack0] quit
[VTEP3] vlan batch 30 200
[VTEP3] interface vlanif 200
[VTEP3-Vlanif200] ip address 10.1.200.2 255.255.255.252
[VTEP3-Vlanif200] quit
[VTEP3] interface eth-trunk 1
[VTEP3-Eth-Trunk1] port link-type trunk
[VTEP3-Eth-Trunk1] undo port trunk allow-pass vlan 1
[VTEP3-Eth-Trunk1] port trunk allow-pass vlan 200
[VTEP3-Eth-Trunk1] quit
[VTEP3] interface xgigabitethernet 0/0/1
[VTEP3-XGigabitEthernet0/0/1] eth-trunk 1
```



```
[VTEP3-XGigabitEthernet0/0/1] quit
[VTEP3] interface xgigabitethernet 0/0/2
[VTEP3-XGigabitEthernet0/0/2] eth-trunk 1
[VTEP3-XGigabitEthernet0/0/2] quit
[VTEP3] ospf router-id 10.200.200.20
[VTEP3-ospf-1] area 0
[VTEP3-ospf-1-area-0.0.0.0] network 10.200.200.20 0.0.0.0
[VTEP3-ospf-1-area-0.0.0.0] network 10.1.200.0 0.0.0.3
[VTEP3-ospf-1-area-0.0.0.0] quit
[VTEP3-ospf-1] quit
```

3. 在接入交换机 ACC1~ACC3 上配置 VLAN 接入，在汇聚交换机 VTEP2、VTEP3 上配置 VXLAN 业务接入点

配置 ACC1。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC1
[ACC1] vlan batch 10
[ACC1] interface eth-trunk 1
[ACC1-Eth-Trunk1] port link-type trunk
[ACC1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[ACC1-Eth-Trunk1] port trunk allow-pass vlan 10
[ACC1-Eth-Trunk1] quit
[ACC1] interface xgigabitethernet 0/0/1
[ACC1-XGigabitEthernet0/0/1] eth-trunk 1
[ACC1-XGigabitEthernet0/0/1] quit
[ACC1] interface xgigabitethernet 0/0/2
[ACC1-XGigabitEthernet0/0/2] eth-trunk 1
[ACC1-XGigabitEthernet0/0/2] quit
[ACC1] interface gigabitethernet 0/0/1
[ACC1-GigabitEthernet0/0/1] port link-type access
[ACC1-GigabitEthernet0/0/1] port default vlan 10
[ACC1-GigabitEthernet0/0/1] quit
```

配置 ACC2。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC2
[ACC2] vlan batch 20
[ACC2] interface eth-trunk 1
[ACC2-Eth-Trunk1] port link-type trunk
[ACC2-Eth-Trunk1] undo port trunk allow-pass vlan 1
[ACC2-Eth-Trunk1] port trunk allow-pass vlan 20
[ACC2-Eth-Trunk1] quit
[ACC2] interface xgigabitethernet 0/0/1
```

```
[ACC2-XGigabitEthernet0/0/1] eth-trunk 1
[ACC2-XGigabitEthernet0/0/1] quit
[ACC2] interface xgigabitethernet 0/0/2
[ACC2-XGigabitEthernet0/0/2] eth-trunk 1
[ACC2-XGigabitEthernet0/0/2] quit
[ACC2] interface gigabitethernet 0/0/1
[ACC2-GigabitEthernet0/0/1] port link-type access
[ACC2-GigabitEthernet0/0/1] port default vlan 20
[ACC2-GigabitEthernet0/0/1] quit
```

配置 ACC3。

```
<HUAWEI> system-view
[HUAWEI] sysname ACC3
[ACC3] vlan batch 30
[ACC3] interface eth-trunk 1
[ACC3-Eth-Trunk1] port link-type trunk
[ACC3-Eth-Trunk1] undo port trunk allow-pass vlan 1
[ACC3-Eth-Trunk1] port trunk allow-pass vlan 30
[ACC3-Eth-Trunk1] quit
[ACC3] interface xgigabitethernet 0/0/1
[ACC3-XGigabitEthernet0/0/1] eth-trunk 1
[ACC3-XGigabitEthernet0/0/1] quit
[ACC3] interface xgigabitethernet 0/0/2
[ACC3-XGigabitEthernet0/0/2] eth-trunk 1
[ACC3-XGigabitEthernet0/0/2] quit
[ACC3] interface gigabitethernet 0/0/1
[ACC3-GigabitEthernet0/0/1] port link-type access
[ACC3-GigabitEthernet0/0/1] port default vlan 30
[ACC3-GigabitEthernet0/0/1] quit
```

配置 VTEP2。

```
[VTEP2] interface eth-trunk 11
[VTEP2-Eth-Trunk11] port link-type trunk
[VTEP2-Eth-Trunk11] undo port trunk allow-pass vlan 1
[VTEP2-Eth-Trunk11] port trunk allow-pass vlan 10
[VTEP2-Eth-Trunk11] quit
[VTEP2] interface 10GE 2/4/0/40
[VTEP2-10GE2/4/0/40] eth-trunk 11
[VTEP2-10GE2/4/0/40] quit
[VTEP2] interface 10GE 2/4/0/44
[VTEP2-10GE2/4/0/44] eth-trunk 11
[VTEP2-10GE2/4/0/44] quit
[VTEP2] interface eth-trunk 12
```

```
[VTEP2-Eth-Trunk12] port link-type trunk
[VTEP2-Eth-Trunk12] undo port trunk allow-pass vlan 1
[VTEP2-Eth-Trunk12] port trunk allow-pass vlan 20
[VTEP2-Eth-Trunk12] quit
[VTEP2] interface 10GE 2/4/0/41
[VTEP2-10GE2/4/0/41] eth-trunk 12
[VTEP2-10GE2/4/0/41] quit
[VTEP2] interface 10GE 2/4/0/45
[VTEP2-10GE2/4/0/45] eth-trunk 12
[VTEP2-10GE2/4/0/45] quit
```

配置 VTEP3。

```
[VTEP3] interface eth-trunk 11
[VTEP3-Eth-Trunk11] port link-type trunk
[VTEP3-Eth-Trunk11] undo port trunk allow-pass vlan 1
[VTEP3-Eth-Trunk11] port trunk allow-pass vlan 30
[VTEP3-Eth-Trunk11] quit
[VTEP3] interface xgigabitethernet 0/0/3
[VTEP3-XGigabitEthernet0/0/3] eth-trunk 11
[VTEP3-XGigabitEthernet0/0/3] quit
[VTEP3] interface xgigabitethernet 0/0/4
[VTEP3-XGigabitEthernet0/0/4] eth-trunk 11
[VTEP3-XGigabitEthernet0/0/4] quit
```

4. 配置 AAA

这里以 VTEP2 配置 AAA 为例。VTEP3 配置 AAA 的过程，与 VTEP2 配置 AAA 的过程类似，因此不再赘述。

创建并配置 RADIUS 服务器模板 “rd1”。

```
[VTEP2] radius-server template rd1
[VTEP2-radius-rd1] radius-server authentication 10.11.1.1 1812
[VTEP2-radius-rd1] radius-server shared-key cipher YsHsjx_202206789
[VTEP2-radius-rd1] quit
```

创建 AAA 认证方案 “abc” 并配置认证方式为 RADIUS。

```
[VTEP2] aaa
[VTEP2-aaa] authentication-scheme abc
[VTEP2-aaa-authen-abc] authentication-mode radius
[VTEP2-aaa-authen-abc] quit
```

创建认证域 “example.com”，并在其上绑定 AAA 认证方案 “abc” 与 RADIUS 服务器模板 “rd1”。

```
[VTEP2-aaa] domain example.com
[VTEP2-aaa-domain-example.com] authentication-scheme abc
```

```
[VTEP2-aaa-domain-example.com] radius-server rd1
[VTEP2-aaa-domain-example.com] quit
[VTEP2-aaa] quit
```

测试用户是否能够通过 RADIUS 模板的认证。（已在 RADIUS 服务器上配置了测试用户 test1，用户密码 YsHsjx_202206）

```
[VTEP2] test-aaa test1 YsHsjx_202206 radius-template rd1
Info: Account test succeeded.
```

5. 配置 MAC 认证

这里以 VTEP2 配置 MAC 认证为例。VTEP3 配置 MAC 认证的过程，与 VTEP2 配置 MAC 认证的过程类似，因此不再赘述。

配置 MAC 接入模板 “m1”。

```
[VTEP2] mac-access-profile name m1
[VTEP2-mac-access-profile-m1] quit
```

配置认证模板 “p1”，并在其上绑定 MAC 接入模板 “m1”、指定认证模板下用户的强制认证域为 “example.com”、指定用户接入模式为多用户单独认证接入模式、最大接入用户数为 100。

```
[VTEP2] authentication-profile name p1
[VTEP2-authen-profile-p1] mac-access-profile m1
[VTEP2-authen-profile-p1] access-domain example.com
[VTEP2-authen-profile-p1] authentication mode multi-authen max-user 100
[VTEP2-authen-profile-p1] quit
```

在接口 Eth-Trunk11 和 Eth-Trunk12 上绑定认证模板 “p1”，开启 MAC 认证。

```
[VTEP2] interface eth-trunk 11
[VTEP2-Eth-Trunk11] authentication-profile p1
[VTEP2-Eth-Trunk11] quit
[VTEP2] interface eth-trunk 12
[VTEP2-Eth-Trunk12] authentication-profile p1
[VTEP2-Eth-Trunk12] quit
```

6. 配置 VXLAN 隧道

配置 VTEP1。

```
[VTEP1] bridge-domain 10
[VTEP1-bd10] vxlan vni 10
[VTEP1-bd10] l2 binding vlan 10
[VTEP1-bd10] quit
[VTEP1] bridge-domain 20
[VTEP1-bd20] vxlan vni 20
[VTEP1-bd20] l2 binding vlan 20
[VTEP1-bd20] quit
[VTEP1] bridge-domain 30
```

```
[VTEP1-bd30] vxlan vni 30
[VTEP1-bd30] l2 binding vlan 30
[VTEP1-bd30] quit
[VTEP1] interface nve 1
[VTEP1-Nve1] source 10.200.200.1
[VTEP1-Nve1] vni 10 head-end peer-list 10.200.200.10
[VTEP1-Nve1] vni 10 head-end peer-list 10.200.200.20
[VTEP1-Nve1] vni 20 head-end peer-list 10.200.200.10
[VTEP1-Nve1] vni 20 head-end peer-list 10.200.200.20
[VTEP1-Nve1] vni 30 head-end peer-list 10.200.200.10
[VTEP1-Nve1] vni 30 head-end peer-list 10.200.200.20
[VTEP1-Nve1] quit
```

配置 VTEP2。

```
[VTEP2] bridge-domain 10
[VTEP2-bd10] vxlan vni 10
[VTEP2-bd10] l2 binding vlan 10
[VTEP2-bd10] quit
[VTEP2] bridge-domain 20
[VTEP2-bd20] vxlan vni 20
[VTEP2-bd20] l2 binding vlan 20
[VTEP2-bd20] quit
[VTEP2] bridge-domain 30
[VTEP2-bd30] vxlan vni 30
[VTEP2-bd30] l2 binding vlan 30
[VTEP2-bd30] quit
[VTEP2] interface nve 1
[VTEP2-Nve1] source 10.200.200.10
[VTEP2-Nve1] vni 10 head-end peer-list 10.200.200.1
[VTEP2-Nve1] vni 20 head-end peer-list 10.200.200.1
[VTEP2-Nve1] vni 30 head-end peer-list 10.200.200.1
[VTEP2-Nve1] quit
```

配置 VTEP3。

```
[VTEP3] bridge-domain 10
[VTEP3-bd10] vxlan vni 10
[VTEP3-bd10] l2 binding vlan 10
[VTEP3-bd10] quit
[VTEP3] bridge-domain 20
[VTEP3-bd20] vxlan vni 20
[VTEP3-bd20] l2 binding vlan 20
[VTEP3-bd20] quit
[VTEP3] bridge-domain 30
```

```
[VTEP3-bd30] vxlan vni 30
[VTEP3-bd30] l2 binding vlan 30
[VTEP3-bd30] quit
[VTEP3] interface nve 1
[VTEP3-Nve1] source 10.200.200.20
[VTEP3-Nve1] vni 10 head-end peer-list 10.200.200.1
[VTEP3-Nve1] vni 20 head-end peer-list 10.200.200.1
[VTEP3-Nve1] vni 30 head-end peer-list 10.200.200.1
[VTEP3-Nve1] quit
```

7. 配置 VXLAN 三层网关

配置 VTEP1。

```
[VTEP1] interface vbdif 10
[VTEP1-Vbdif1] ip address 10.118.0.10 255.255.255.0
[VTEP1-Vbdif1] quit
[VTEP1] interface vbdif 20
[VTEP1-Vbdif2] ip address 10.128.0.10 255.255.255.0
[VTEP1-Vbdif2] quit
[VTEP1] interface vbdif 30
[VTEP1-Vbdif3] ip address 10.138.0.10 255.255.255.0
[VTEP1-Vbdif3] quit
```

检查配置结果

上述配置成功后，在 VTEP1、VTEP2、VTEP3 上执行 **display vxlan tunnel** 命令可查看到 VXLAN 隧道的信息；执行 **display vxlan vni** 命令可查看到 VNI 的状态是 Up。以 VTEP1 的显示为例。

```
[VTEP1] display vxlan tunnel
Number of vxlan tunnel : 2
Tunnel ID   Source           Destination      State Type   Uptime
-----
4026531841  10.200.200.1     10.200.200.10   up   static  0035h21m
4026531842  10.200.200.1     10.200.200.20   up   static  0036h21m
[VTEP1] display vxlan vni
Number of vxlan vni : 3
VNI         BD-ID           State
-----
10          10              up
20          20              up
30          30              up
```

配置完成后，不同区域的服务器（Server1 ~ Server3）之间通过 VXLAN 网关可以互通。

配置脚本

VTEP1 的配置脚本。

```
#
sysname VTEP1
#
vlan batch 10 11 20 30 100 200
#
bridge-domain 10
l2 binding vlan 10
vxlan vni 10
#
bridge-domain 20
l2 binding vlan 20
vxlan vni 20
#
bridge-domain 30
l2 binding vlan 30
vxlan vni 30
#
interface Vbdif10
ip address 10.118.0.10 255.255.255.0
#
interface Vbdif20
ip address 10.128.0.10 255.255.255.0
#
interface Vbdif30
ip address 10.138.0.10 255.255.255.0
#
interface Vlanif11
ip address 10.11.1.2 255.255.255.0
#
interface Vlanif100
ip address 10.1.100.1 255.255.255.252
#
interface Vlanif200
ip address 10.1.200.1 255.255.255.252
#
interface Eth-Trunk11
description TO-VTEP2
port link-type trunk
undo port trunk allow-pass vlan 1
```

```
port trunk allow-pass vlan 100
#
interface Eth-Trunk12
description TO-VTEP3
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 200
#
interface 10GE1/3/0/0
eth-trunk 11
#
interface 10GE1/3/0/1
port default vlan 11
#
interface 10GE1/3/0/13
eth-trunk 11
#
interface 10GE2/3/0/2
eth-trunk 12
#
interface 10GE2/3/0/14
eth-trunk 12
#
interface LoopBack0
ip address 10.200.200.1 255.255.255.255
#
interface Nve1
source 10.200.200.1
vni 10 head-end peer-list 10.200.200.10
vni 10 head-end peer-list 10.200.200.20
vni 20 head-end peer-list 10.200.200.10
vni 20 head-end peer-list 10.200.200.20
vni 30 head-end peer-list 10.200.200.10
vni 30 head-end peer-list 10.200.200.20
#
ospf 1 router-id 10.200.200.1
area 0.0.0.0
network 10.1.100.0 0.0.0.3
network 10.1.200.0 0.0.0.3
network 10.200.200.1 0.0.0.0
#
return
```


VTEP2 的配置脚本。

```
#
sysname VTEP2
#
authentication-profile name p1
  mac-access-profile m1
  access-domain example.com
  authentication mode multi-authen max-user 100
#
vlan batch 10 20 100
#
aaa
  authentication-scheme abc
  authentication-mode radius
  domain example.com
  authentication-scheme abc
  radius-server rd1
#
bridge-domain 10
  l2 binding vlan 10
  vxlan vni 10
#
bridge-domain 20
  l2 binding vlan 20
  vxlan vni 20
#
bridge-domain 30
  l2 binding vlan 30
  vxlan vni 30
#
radius-server template rd1
  radius-server shared-key
  cipher %+%##!!!!!!!"!!!!!!!"*!!!!SKvr$[Fs.3t@/5k|BENhEu>W(3~XG!!D;!!!!2jp5!!!!!!A!!!!3"pK8qv!]9M#(4$jGWvQ
  F/R[CNe/+:W^jk8HUe&W%+%#
  radius-server authentication 10.11.1.1 1812 weight 80
#
mac-access-profile name m1
#
interface Vlanif100
  ip address 10.1.100.2 255.255.255.252
#
interface Eth-Trunk1
```

```
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
#
interface Eth-Trunk11
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10
authentication-profile p1
#
interface Eth-Trunk12
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20
authentication-profile p1
#
interface 10GE1/2/0/2
eth-trunk 1
#
interface 10GE1/2/0/3
eth-trunk 1
#
interface 10GE2/4/0/40
eth-trunk 11
device transceiver 1000BASE-X
#
interface 10GE2/4/0/41
eth-trunk 12
device transceiver 1000BASE-X
#
interface 10GE2/4/0/42
eth-trunk 1
device transceiver 10GBASE-FIBER
#
interface 10GE2/4/0/44
eth-trunk 11
#
interface 10GE2/4/0/45
eth-trunk 12
#
interface LoopBack0
ip address 10.200.200.10 255.255.255.255
#
```

```
interface Nve1
 source 10.200.200.10
 vni 10 head-end peer-list 10.200.200.1
 vni 20 head-end peer-list 10.200.200.1
 vni 30 head-end peer-list 10.200.200.1
#
ospf 1 router-id 10.200.200.10
 area 0.0.0.0
  network 10.1.100.0 0.0.0.3
  network 10.200.200.10 0.0.0.0
#
return
```

VTEP3 的配置脚本。

```
#
sysname VTEP3
#
authentication-profile name p1
 mac-access-profile m1
 access-domain example.com
 authentication mode multi-authen max-user 100
#
vlan batch 30 200
#
aaa
 authentication-scheme abc
 authentication-mode radius
 domain example.com
 authentication-scheme abc
 radius-server rd1
#
bridge-domain 10
 l2 binding vlan 10
 vxlan vni 10
#
bridge-domain 20
 l2 binding vlan 20
 vxlan vni 20
#
bridge-domain 30
 l2 binding vlan 30
 vxlan vni 30
#
```

```
radius-server rd1
radius-server shared-key
cipher %+%##!!!!!!!"!!!!!!*!!!!SKvr$[[Fs.3t@/5k|BENhEu>W(3~-XG!!D;!!!!2jp5!!!!!!A!!!!3"pK8qv!}9M#(4$jGWvQ
F/R[CNe/+:W^jk8HUe&W%+%#
radius-server authentication 10.11.1.1 1812 weight 80
#
mac-access-profile name m1
#
interface Vlanif200
ip address 10.1.200.2 255.255.255.252
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 200
#
interface Eth-Trunk11
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 30
authentication-profile p1
#
interface XGigabitEthernet0/0/1
eth-trunk 1
#
interface XGigabitEthernet0/0/2
eth-trunk 1
#
interface XGigabitEthernet0/0/3
eth-trunk 11
#
interface XGigabitEthernet0/0/4
eth-trunk 11
#
interface LoopBack0
ip address 10.200.200.20 255.255.255.255
#
interface Nve1
source 10.200.200.20
vni 10 head-end peer-list 10.200.200.1
vni 20 head-end peer-list 10.200.200.1
vni 30 head-end peer-list 10.200.200.1
#
```

```
ospf 1 router-id 10.200.200.20
area 0.0.0.0
 network 10.1.200.0 0.0.0.3
 network 10.200.200.20 0.0.0.0
#
return
```

ACC1 的配置脚本。

```
#
sysname ACC1
#
vlan batch 10
#
interface Eth-Trunk1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 10
#
interface GigabitEthernet0/0/1
 port link-type access
 port default vlan 10
#
interface XGigabitEthernet0/0/1
 eth-trunk 1
#
interface XGigabitEthernet0/0/2
 eth-trunk 1
#
return
```

ACC2 的配置脚本。

```
#
sysname ACC2
#
vlan batch 20
#
interface Eth-Trunk1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 20
#
interface GigabitEthernet0/0/1
 port link-type access
```

```
port default vlan 20
#
interface XGigabitEthernet0/0/1
eth-trunk 1
#
interface XGigabitEthernet0/0/2
eth-trunk 1
#
return
```

ACC3 的配置脚本。

```
#
sysname ACC3
#
vlan batch 30
#
interface Eth-Trunk1
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 30
#
interface GigabitEthernet0/0/1
port link-type access
port default vlan 30
#
interface XGigabitEthernet0/0/1
eth-trunk 1
#
interface XGigabitEthernet0/0/2
eth-trunk 1
#
return
```

1.1.3 交换机与防火墙对接上网配置案例

[二层交换机与防火墙对接上网配置案例](#)

[三层交换机与防火墙对接上网配置案例](#)

1.1.3.1 二层交换机与防火墙对接上网配置案例

二层交换机简介

二层交换机指的是仅能够进行二层转发，不能进行三层转发的交换机。也就是说仅支持二层特性，不支持路由等三层特性的交换机。

二层交换机一般部署在接入层，不能作为用户的网关。

配置注意事项

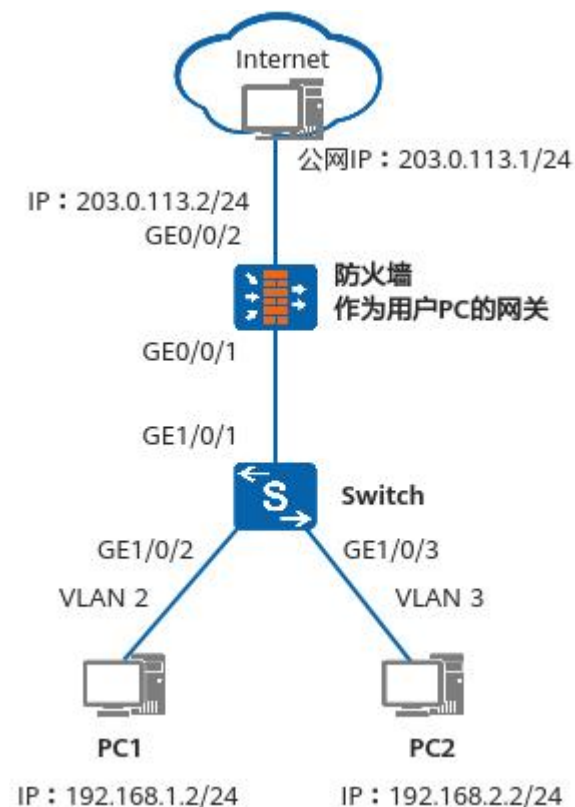
本举例中的交换机配置适用于 S 系列交换机所有产品的所有 V600 版本。

本举例中的防火墙配置以 USG6655E V600R007C00 为例，其他防火墙的配置方法可根据设备版本参见相应的《配置指南-基础配置》。

组网需求

如图 1 所示，某公司拥有多个部门且位于不同网段，各部门均有访问 Internet 的需求。现要求用户通过二层交换机和防火墙访问外部网络，且要求防火墙作为用户的网关。

图 1 二层交换机与防火墙对接上网组网图



配置思路

采用如下思路进行配置：

1. 配置交换机基于接口划分 VLAN，实现二层转发。
2. 配置防火墙作为用户的网关，通过子接口或 VLANIF 接口实现跨网段的三层转发。
3. 配置防火墙作为 DHCP 服务器，为用户 PC 分配 IP 地址。
4. 开启防火墙域间安全策略，使不同域的报文可以相互转发。

5. 配置防火墙 PAT 功能，使内网用户可以访问外部网络。

操作步骤

1. 配置交换机

配置下行连接用户的接口。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 2 3
[Switch] interface GE 1/0/2
[Switch-GE1/0/2] port default vlan 2
[Switch-GE1/0/2] quit
[Switch] interface GE 1/0/3
[Switch-GE1/0/3] port default vlan 3
[Switch-GE1/0/3] quit
```

配置上行连接防火墙的接口。

```
[Switch] interface GE 1/0/1
[Switch-GE1/0/1] port link-type trunk
[Switch-GE1/0/1] port trunk allow-pass vlan 2 3
[Switch-GE1/0/1] quit
```

2. 配置防火墙

防火墙的配置有两种方式，配置子接口或者配置 VLANIF 接口，两种方式选择其一即可。

配置防火墙通过子接口终结 VLAN，实现跨网段的三层转发。

配置终结子接口。

```
<USG6600E> system-view
[USG6600E] interface GigabitEthernet 0/0/1.1
[USG6600E-GigabitEthernet0/0/1.1] vlan-type dot1q 2
[USG6600E-GigabitEthernet0/0/1.1] ip address 192.168.1.1 24
[USG6600E-GigabitEthernet0/0/1.1] quit
[USG6600E] interface GigabitEthernet 0/0/1.2
[USG6600E-GigabitEthernet0/0/1.2] vlan-type dot1q 3
[USG6600E-GigabitEthernet0/0/1.2] ip address 192.168.2.1 24
[USG6600E-GigabitEthernet0/0/1.2] quit
```

配置 DHCP 功能，为内网用户分配 IP 地址并指定 DNS 服务器地址。

```
[USG6600E] dhcp enable
[USG6600E] interface GigabitEthernet 0/0/1.1
[USG6600E-GigabitEthernet0/0/1.1] dhcp select interface
[USG6600E-GigabitEthernet0/0/1.1] dhcp server dns-list 114.114.114.114 223.5.5.5 //配置的 DNS-List 114.114.114.114 是公用的 DNS 服务器地址，是不区分运营商的。在实际应用中，请根据运营商分配的 DNS 进行配置
```



```
[USG6600E-GigabitEthernet0/0/1.1] quit
[USG6600E] interface GigabitEthernet 0/0/1.2
[USG6600E-GigabitEthernet0/0/1.2] dhcp select interface
[USG6600E-GigabitEthernet0/0/1.2] dhcp server dns-list 114.114.114.114 223.5.5.5
[USG6600E-GigabitEthernet0/0/1.2] quit
```

配置公网接口的 IP 地址和静态路由。

```
[USG6600E] interface GigabitEthernet 0/0/2
[USG6600E-GigabitEthernet0/0/2] ip address 203.0.113.2 255.255.255.0
[USG6600E-GigabitEthernet0/0/2] quit
[USG6600E] ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
```

配置安全区域。

```
[USG6600E] firewall zone trust
[USG6600E-zone-trust] add interface GigabitEthernet 0/0/1
[USG6600E-zone-trust] add interface GigabitEthernet 0/0/1.1
[USG6600E-zone-trust] add interface GigabitEthernet 0/0/1.2
[USG6600E-zone-trust] quit
[USG6600E] firewall zone untrust
[USG6600E-zone-untrust] add interface GigabitEthernet 0/0/2
[USG6600E-zone-untrust] quit
```

配置安全策略，允许域间互访。

```
[USG6600E] security-policy
[USG6600E-policy-security] rule name policy1
[USG6600E-policy-security-rule-policy1] source-zone trust
[USG6600E-policy-security-rule-policy1] destination-zone untrust
[USG6600E-policy-security-rule-policy1] source-address 192.168.0.0 mask 255.255.0.0
[USG6600E-policy-security-rule-policy1] action permit
[USG6600E-policy-security-rule-policy1] quit
[USG6600E-policy-security] quit
```

配置 PAT 地址池，开启允许端口地址转换。

```
[USG6600E] nat address-group addressgroup1
[USG6600E-address-group-addressgroup1] mode pat
[USG6600E-address-group-addressgroup1] route enable
[USG6600E-address-group-addressgroup1] section 0 203.0.113.2 203.0.113.2
[USG6600E-address-group-addressgroup1] quit
```

配置源 PAT 策略，实现私网指定网段访问公网时自动进行源地址转换。

```
[USG6600E] nat-policy
[USG6600E-policy-nat] rule name policy_nat1
[USG6600E-policy-nat-rule-policy_nat1] source-zone trust
[USG6600E-policy-nat-rule-policy_nat1] destination-zone untrust
```

```
[USG6600E-policy-nat-rule-policy_nat1] source-address 192.168.0.0 mask 255.255.0.0
[USG6600E-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[USG6600E-policy-nat-rule-policy_nat1] quit
[USG6600E-policy-nat] quit
[USG6600E] quit
```

配置防火墙通过配置 VLANIF 接口，实现跨网段的三层转发。

配置 VLANIF 接口。

```
<USG6600E> system-view
[USG6600E] vlan batch 2 3
[USG6600E] interface GigabitEthernet 0/0/1
[USG6600E-GigabitEthernet0/0/1] portswitch
[USG6600E-GigabitEthernet0/0/1] port link-type hybrid
[USG6600E-GigabitEthernet0/0/1] port hybrid tagged vlan 2 to 3
[USG6600E-GigabitEthernet0/0/1] quit
[USG6600E] interface vlanif 2
[USG6600E-Vlanif2] ip address 192.168.1.1 24
[USG6600E-Vlanif2] quit
[USG6600E] interface vlanif 3
[USG6600E-Vlanif3] ip address 192.168.2.1 24
[USG6600E-Vlanif3] quit
```

配置 DHCP 功能。

```
[USG6600E] dhcp enable
[USG6600E] interface vlanif 2
[USG6600E-Vlanif2] dhcp select interface
[USG6600E-Vlanif2] dhcp server dns-list 114.114.114.114 223.5.5.5
[USG6600E-Vlanif2] quit
[USG6600E] interface vlanif 3
[USG6600E-Vlanif3] dhcp select interface
[USG6600E-Vlanif3] dhcp server dns-list 114.114.114.114 223.5.5.5
[USG6600E-Vlanif3] quit
```

配置公网接口的 IP 地址和静态路由。

```
[USG6600E] interface GigabitEthernet 0/0/2
[USG6600E-GigabitEthernet0/0/2] ip address 203.0.113.2 255.255.255.0
[USG6600E-GigabitEthernet0/0/2] quit
[USG6600E] ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
```

配置安全区域。

```
[USG6600E] firewall zone trust
[USG6600E-zone-trust] add interface gigabitethernet 0/0/1
[USG6600E-zone-trust] add interface vlanif 2
[USG6600E-zone-trust] add interface vlanif 3
```

```
[USG6600E-zone-trust] quit
[USG6600E] firewall zone untrust
[USG6600E-zone-untrust] add interface gigabitethernet 0/0/2
[USG6600E-zone-untrust] quit
```

配置安全策略，允许域间互访。

```
[USG6600E] security-policy
[USG6600E-policy-security] rule name policy1
[USG6600E-policy-security-rule-policy1] source-zone trust
[USG6600E-policy-security-rule-policy1] destination-zone untrust
[USG6600E-policy-security-rule-policy1] source-address 192.168.0.0 mask 255.255.0.0
[USG6600E-policy-security-rule-policy1] action permit
[USG6600E-policy-security-rule-policy1] quit
[USG6600E-policy-security] quit
```

配置 PAT 地址池，开启允许端口地址转换。

```
[USG6600E] nat address-group addressgroup1
[USG6600E-address-group-addressgroup1] mode pat
[USG6600E-address-group-addressgroup1] route enable
[USG6600E-address-group-addressgroup1] section 0 203.0.113.2 203.0.113.2
[USG6600E-address-group-addressgroup1] quit
```

配置源 PAT 策略，实现私网指定网段访问公网时自动进行源地址转换。

```
[USG6600E] nat-policy
[USG6600E-policy-nat] rule name policy_nat1
[USG6600E-policy-nat-rule-policy_nat1] source-zone trust
[USG6600E-policy-nat-rule-policy_nat1] destination-zone untrust
[USG6600E-policy-nat-rule-policy_nat1] source-address 192.168.0.0 mask 255.255.0.0
[USG6600E-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[USG6600E-policy-nat-rule-policy_nat1] quit
[USG6600E-policy-nat] quit
[USG6600E] quit
```

3. 检查配置结果

配置 PC1 的 IP 地址为 192.168.1.2/24，网关为 192.168.1.1；PC2 的 IP 地址为 192.168.2.2/24，网关为 192.168.2.1。

配置外网 PC 的 IP 地址为 203.0.113.1/24，网关为 203.0.113.2。

配置完成后，PC1 和 PC2 都可以 Ping 通外网的 IP 203.0.113.1/24，PC1 和 PC2 都可以访问 Internet。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 2 to 3
#
interface GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
interface GE1/0/2
port default vlan 2
#
interface GE1/0/3
port default vlan 3
#
return
```

USG 的配置脚本（防火墙通过子接口进行三层转发的配置脚本）

```
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/1.1
vlan-type dot1q 2
ip address 192.168.1.1 255.255.255.0
dhcp select interface
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface GigabitEthernet0/0/1.2
vlan-type dot1q 3
ip address 192.168.2.1 255.255.255.0
dhcp select interface
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface GigabitEthernet0/0/2
ip address 203.0.113.2 255.255.255.0
#
firewall zone trust
set priority 85
add interface GigabitEthernet0/0/1
add interface GigabitEthernet0/0/1.1
add interface GigabitEthernet0/0/1.2
#
firewall zone untrust
```

```
set priority 5
add interface GigabitEthernet0/0/2
#
ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
#
nat address-group addressgroup1 0 mode pat
route enable
section 0 203.0.113.2 203.0.113.2
#
security-policy
rule name policy1
source-zone trust
destination-zone untrust
source-address 192.168.0.0 mask 255.255.0.0
action permit
#
nat-policy
rule name policy_nat1
source-zone trust
destination-zone untrust
source-address 192.168.0.0 mask 255.255.0.0
action source-nat address-group addressgroup1
#
return
```

USG 的配置脚本（防火墙通过 VLANIF 接口进行三层转发的配置脚本）

```
#
vlan batch 2 to 3
#
interface Vlanif2
ip address 192.168.1.1 255.255.255.0
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface Vlanif3
ip address 192.168.2.1 255.255.255.0
dhcp select interface
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface GigabitEthernet0/0/1
portswitch
port hybrid tagged vlan 2 to 3
#
```

```
interface GigabitEthernet0/0/2
 ip address 203.0.113.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/1
 add interface Vlanif2
 add interface Vlanif3
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/2
#
 ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
#
 nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 203.0.113.2 203.0.113.2
#
 security-policy
 rule name policy1
 source-zone trust
 destination-zone untrust
 source-address 192.168.0.0 mask 255.255.0.0
 action permit
#
 nat-policy
 rule name policy_nat1
 source-zone trust
 destination-zone untrust
 source-address 192.168.0.0 mask 255.255.0.0
 action source-nat address-group addressgroup1
#
return
```

相关信息

视频

[S 系列交换机二层交换机与防火墙对接上网](#)

1.1.3.2 三层交换机与防火墙对接上网配置案例

三层交换机简介

三层交换机是具有路由功能的交换机，由于路由属于 OSI 模型中第三层网络层的功能，所以称为三层交换机。三层交换机既可以工作在二层也可以工作在三层，可以部署在接入层，也可以部署在汇聚层，作为用户的网关。

配置注意事项

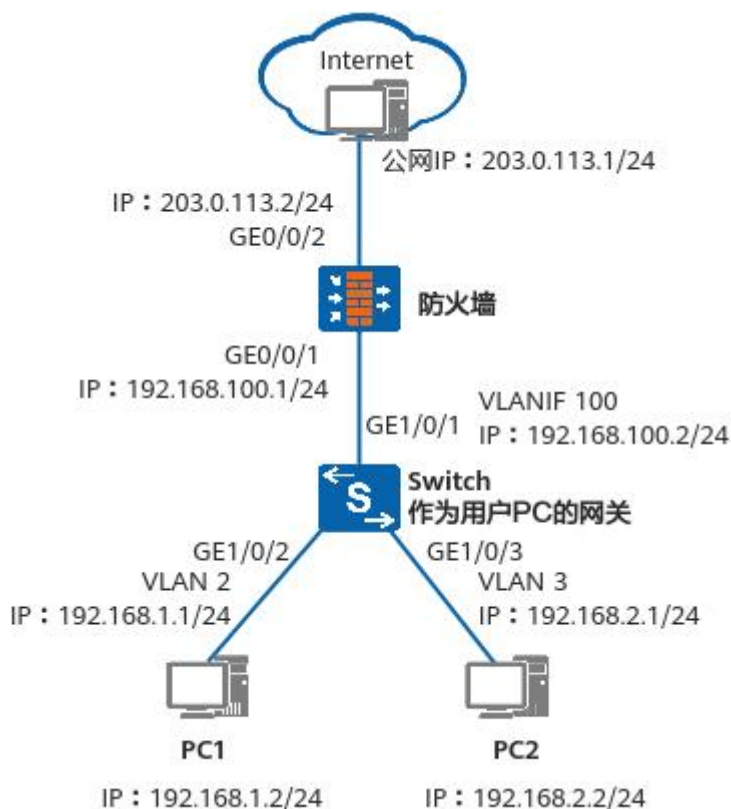
本举例中的交换机配置适用于 S 系列交换机所有产品的所有 V600 版本。

本举例中的防火墙配置以 USG6655E V600R007C00 为例，其他防火墙的配置方法可根据设备版本参见相应的《配置指南-基础配置》。

组网需求

如图 1 所示，某公司拥有多个部门且位于不同网段，各部门均有访问 Internet 的需求。现要求用户通过三层交换机和防火墙访问外部网络，且要求三层交换机作为用户的网关。

图 1 三层交换机与防火墙对接上网组网图



配置思路

采用如下思路进行配置：

1. 配置交换机作为用户的网关，通过 VLANIF 接口，实现跨网段用户互访。

2. 配置交换机作为 DHCP 服务器，为用户分配 IP 地址。
3. 开启防火墙域间安全策略，使不同域的报文可以相互转发。
4. 配置防火墙 PAT 转换功能，使用户可以访问外部网络。

操作步骤

1. 配置交换机

配置连接用户的接口和对应的 VLANIF 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 2 3
[Switch] interface GE 1/0/2
[Switch-GE1/0/2] port default vlan 2 //配置接口加入 VLAN 2
[Switch-GE1/0/2] quit
[Switch] interface GE 1/0/3
[Switch-GE1/0/3] port default vlan 3
[Switch-GE1/0/3] quit
[Switch] interface Vlanif 2
[Switch-Vlanif2] ip address 192.168.1.1 24
[Switch-Vlanif2] quit
[Switch] interface Vlanif 3
[Switch-Vlanif3] ip address 192.168.2.1 24
[Switch-Vlanif3] quit
```

配置连接防火墙的接口和对应的 VLANIF 接口。

```
[Switch] vlan batch 100
[Switch] interface GE 1/0/1
[Switch-GE1/0/1] port default vlan 100
[Switch-GE1/0/1] quit
[Switch] interface Vlanif 100
[Switch-Vlanif100] ip address 192.168.100.2 24
[Switch-Vlanif100] quit
```

配置缺省路由。

```
[Switch] ip route-static 0.0.0.0 0.0.0.0 192.168.100.1 //缺省路由的下一跳是防火墙接口的 IP 地址
192.168.100.1
```

配置 DHCP 服务器。

```
[Switch] dhcp enable
[Switch] interface Vlanif 2
[Switch-Vlanif2] dhcp select interface //DHCP 使用接口地址池的方式为用户分配 IP 地址
[Switch-Vlanif2] dhcp server dns-list 114.114.114.114 223.5.5.5 //配置的 DNS-List 114.114.114.114 是公用
的 DNS 服务器地址，是不区分运营商的。在实际应用中，请根据运营商分配的 DNS 进行配置
```



```
[Switch-Vlanif2] quit
[Switch] interface Vlanif 3
[Switch-Vlanif3] dhcp select interface
[Switch-Vlanif3] dhcp server dns-list 114.114.114.114 223.5.5.5
[Switch-Vlanif3] quit
```

2. 配置防火墙

配置连接交换机的接口对应的 IP 地址。

```
<USG6600E> system-view
[USG6600E] interface GigabitEthernet 0/0/1
[USG6600E-GigabitEthernet0/0/1] ip address 192.168.100.1 255.255.255.0
[USG6600E-GigabitEthernet0/0/1] quit
```

配置连接公网的接口对应的 IP 地址。

```
[USG6600E] interface GigabitEthernet 0/0/2
[USG6600E-GigabitEthernet0/0/2] ip address 203.0.113.2 255.255.255.0 //配置连接公网接口的 IP 地址和公
网的 IP 地址在同一网段
[USG6600E-GigabitEthernet0/0/2] quit
```

配置缺省路由和回程路由。

```
[USG6600E] ip route-static 0.0.0.0 0.0.0.0 203.0.113.1 //配置静态缺省路由的下一跳指向公网提供的 IP 地址
203.0.113.1
[USG6600E] ip route-static 192.168.0.0 255.255.0.0 192.168.100.2 //配置回程路由的下一跳就指向交换机上行
接口的 IP 地址 192.168.100.2
```

配置安全策略。

```
[USG6600E] firewall zone trust //配置 trust 域
[USG6600E-zone-trust] add interface GigabitEthernet 0/0/1
[USG6600E-zone-trust] quit
[USG6600E] firewall zone untrust //配置 untrust 域
[USG6600E-zone-untrust] add interface GigabitEthernet 0/0/2
[USG6600E-zone-untrust] quit
```

配置安全策略，允许域间互访。

```
[USG6600E] security-policy
[USG6600E-policy-security] rule name policy1
[USG6600E-policy-security-rule-policy1] source-zone trust
[USG6600E-policy-security-rule-policy1] destination-zone untrust
[USG6600E-policy-security-rule-policy1] source-address 192.168.0.0 mask 255.255.0.0
[USG6600E-policy-security-rule-policy1] action permit
[USG6600E-policy-security-rule-policy1] quit
[USG6600E-policy-security] quit
```

配置 PAT 地址池，开启允许端口地址转换。

```
[USG6600E] nat address-group addressgroup1
```

```
[USG6600E-address-group-addressgroup1] mode pat
[USG6600E-address-group-addressgroup1] route enable
[USG6600E-address-group-addressgroup1] section 0 203.0.113.2 203.0.113.2 //转换的公网 IP 地址
[USG6600E-address-group-addressgroup1] quit
```

配置源 PAT 策略，实现私网指定网段访问公网时自动进行源地址转换。

```
[USG6600E] nat-policy
[USG6600E-policy-nat] rule name policy_nat1
[USG6600E-policy-nat-rule-policy_nat1] source-zone trust
[USG6600E-policy-nat-rule-policy_nat1] destination-zone untrust
[USG6600E-policy-nat-rule-policy_nat1] source-address 192.168.0.0 mask 255.255.0.0 //允许进行 PAT
转换的源 IP 地址
[USG6600E-policy-nat-rule-policy_nat1] action source-nat address-group addressgroup1
[USG6600E-policy-nat-rule-policy_nat1] quit
[USG6600E-policy-nat] quit
[USG6600E] quit
```

3. 检查配置结果

配置 PC1 的 IP 地址为 192.168.1.2/24，网关为 192.168.1.1；PC2 的 IP 地址为 192.168.2.2/24，网关为 192.168.2.1。

配置外网 PC 的 IP 地址为 203.0.113.1/24，网关为 203.0.113.2。

配置完成后，PC1 和 PC2 都可以 Ping 通外网的 IP 203.0.113.1/24，PC1 和 PC2 都可以访问 Internet。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 2 to 3 100
#
dhcp enable
#
interface Vlanif2
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface Vlanif3
 ip address 192.168.2.1 255.255.255.0
 dhcp select interface
 dhcp server dns-list 114.114.114.114 223.5.5.5
```

```
#
interface Vlanif100
 ip address 192.168.100.2 255.255.255.0
#
interface GE1/0/1
 port default vlan 100
#
interface GE1/0/2
 port default vlan 2
#
interface GE1/0/3
 port default vlan 3
#
ip route-static 0.0.0.0 0.0.0.0 192.168.100.1
#
return
```

USG 的配置脚本

```
#
interface GigabitEthernet0/0/1
 ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet0/0/2
 ip address 203.0.113.2 255.255.255.0
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/1
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/2
#
ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
ip route-static 192.168.0.0 255.255.0.0 192.168.100.2
#
nat address-group addressgroup1 0
 mode pat
 route enable
 section 0 203.0.113.2 203.0.113.2
#
security-policy
 rule name policy1
```

```
source-zone trust
destination-zone untrust
source-address 192.168.0.0 mask 255.255.0.0
action permit
#
nat-policy
rule name policy_nat1
source-zone trust
destination-zone untrust
source-address 192.168.0.0 mask 255.255.0.0
action natsource-nat address-group addressgroup1
#
return
```

1.1.4 交换机与路由器对接上网配置案例

[二层交换机与路由器对接上网配置案例](#)

[三层交换机与路由器对接上网配置案例](#)

1.1.4.1 二层交换机与路由器对接上网配置案例

二层交换机简介

二层交换机指的是仅能够进行二层转发，不能进行三层转发的交换机，即仅支持二层特性，不支持路由等三层特性的交换机。

二层交换机一般部署在接入层，不作为网关。

配置注意事项

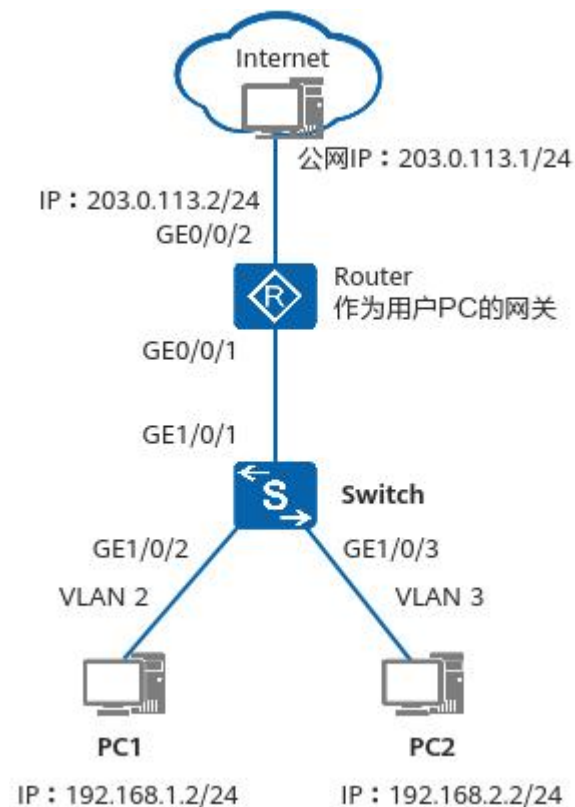
本举例中的交换机配置适用于 S 系列交换机所有产品的所有 V600 版本。

本举例中的路由器配置以 AR651 V300R022C10 为例，其他路由器的配置方法请参见对应的产品文档。

组网需求

如[图 1](#)所示，某公司拥有多个部门且位于不同网段，各部门均有访问 Internet 的需求。现要求用户通过二层交换机和路由器访问外部网络，且要求路由器作为用户的网关。

图 1 二层交换机与路由器对接上网组网图



配置思路

采用如下思路进行配置：

1. 配置二层交换机基于接口划分 VLAN，实现二层转发。
2. 配置路由器作为用户的网关，通过子接口或 VLANIF 接口实现跨网段的三层转发。
3. 配置路由器作为 DHCP 服务器，为用户 PC 分配 IP 地址。
4. 配置路由器 NAT 功能，使内网用户可以访问外部网络。

操作步骤

1. 配置交换机

配置下行连接用户的接口。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 2 3
[Switch] interface GE 1/0/2
[Switch-GE1/0/2] port default vlan 2 //配置接口加入 VLAN 2
[Switch-GE1/0/2] quit
[Switch] interface GE 1/0/3
[Switch-GE1/0/3] port default vlan 3
[Switch-GE1/0/3] quit
```

配置上行连接路由器的接口。

```
[Switch] interface GE 1/0/1
[Switch-GE1/0/1] port link-type trunk
[Switch-GE1/0/1] port trunk allow-pass vlan 2 3 //配置接口以 trunk 方式透传 VLAN 2 和 VLAN 3
[Switch-GE1/0/1] quit
```

2. 配置路由器

路由器的配置有两种方式，配置子接口进行通信或者配置 VLANIF 接口进行通信，两种方式选择其一即可。

方式一：配置路由器通过子接口终结 VLAN，实现跨网段的三层转发。

配置终结子接口。

```
<HUAWEI> system-view
[HUAWEI] sysname Router
[Router] vlan batch 2 3
[Router] interface GigabitEthernet 0/0/1.1
[Router-GigabitEthernet0/0/1.1] dot1q termination vid 2
[Router-GigabitEthernet0/0/1.1] ip address 192.168.1.1 24
[Router-GigabitEthernet0/0/1.1] arp broadcast enable
[Router-GigabitEthernet0/0/1.1] quit
[Router] interface GigabitEthernet 0/0/1.2
[Router-GigabitEthernet0/0/1.2] dot1q termination vid 3
[Router-GigabitEthernet0/0/1.2] ip address 192.168.2.1 24
[Router-GigabitEthernet0/0/1.2] arp broadcast enable
[Router-GigabitEthernet0/0/1.2] quit
```

配置 DHCP 功能，为内网用户分配 IP 地址和指定 DNS 服务器地址。

```
[Router] dhcp enable
[Router] interface GigabitEthernet 0/0/1.1
[Router-GigabitEthernet0/0/1.1] dhcp select interface //DHCP 使用接口地址池的方式为内网用户分配 IP 地址
[Router-GigabitEthernet0/0/1.1] dhcp server dns-list 114.114.114.114 223.5.5.5 //配置的 DNS-List
114.114.114.114 是公用的 DNS 服务器地址，是不区分运营商的。在实际应用中，请根据运营商分配的 DNS 进行配置
[Router-GigabitEthernet0/0/1.1] quit
[Router] interface GigabitEthernet 0/0/1.2
[Router-GigabitEthernet0/0/1.2] dhcp select interface
[Router-GigabitEthernet0/0/1.2] dhcp server dns-list 114.114.114.114 223.5.5.5
[Router-GigabitEthernet0/0/1.2] quit
```

配置公网接口的 IP 地址和静态路由。

```
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] ip address 203.0.113.2 255.255.255.0 //配置连接公网的接口 GE0/0/2 的 IP 地址 203.0.113.2
[Router-GigabitEthernet0/0/2] quit
```

```
[Router] ip route-static 0.0.0.0 0.0.0.0 203.0.113.1 //配置静态缺省路由的下一跳指向公网提供的 IP 地址
203.0.113.1
```

配置 NAT 功能，使内网用户可以访问外网。

```
[Router] acl number 2001
[Router-acl-basic-2001] rule 5 permit source 192.168.0.0 0.0.255.255 //NAT 转换只对源 IP 地址是
192.168.0.0/16 网段的生效，并在接口 GE0/0/2 的出方向进行转换
[Router-acl-basic-2001] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 2001
[Router-GigabitEthernet0/0/2] quit
```

方式二：配置路由器通过配置 VLANIF 接口，实现跨网段的三层转发。

配置 VLANIF 接口。

```
[Router] vlan batch 2 3
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] portswitch //将以太网接口从三层模式切换到二层模式。如果接口已经是二层
模式，跳过该步骤
[Router-GigabitEthernet0/0/1] port link-type trunk
[Router-GigabitEthernet0/0/1] port trunk allow-pass vlan 2 3
[Router-GigabitEthernet0/0/1] quit
[Router] interface vlanif 2
[Router-Vlanif2] ip address 192.168.1.1 24 //配置 VLANIF2 的 IP 地址作为 PC1 的网关
[Router-Vlanif2] quit
[Router] interface vlanif 3
[Router-Vlanif3] ip address 192.168.2.1 24 //配置 VLANIF3 的 IP 地址作为 PC2 的网关
[Router-Vlanif3] quit
```

配置 DHCP 功能，为内网用户分配 IP 地址并指定 DNS 服务器地址。

```
[Router] dhcp enable
[Router] interface vlanif 2
[Router-Vlanif2] dhcp select interface
[Router-Vlanif2] dhcp server dns-list 114.114.114.114 223.5.5.5 //配置的 DNS-List 114.114.114.114 是
公用的 DNS 服务器地址，是不区分运营商的。在实际应用中，请根据运营商分配的 DNS 进行配置
[Router-Vlanif2] quit
[Router] interface vlanif 3
[Router-Vlanif3] dhcp select interface
[Router-Vlanif3] dhcp server dns-list 114.114.114.114 223.5.5.5
[Router-Vlanif3] quit
```

配置公网接口的 IP 地址和静态路由。

```
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] ip address 203.0.113.2 255.255.255.0
[Router-GigabitEthernet0/0/2] quit
```

```
[Router] ip route-static 0.0.0.0 0.0.0.0 203.0.113.1 //配置静态缺省路由的下一跳指向公网提供的 IP 地址
203.0.113.1
```

配置 NAT 功能，使内网用户可以访问外网。

```
[Router] acl number 2001
[Router-acl-basic-2001] rule 5 permit source 192.168.0.0 0.0.255.255 //NAT 转换只对源 IP 地址是
192.168.0.0/16 网段的生效，并在接口 GE0/0/2 的出方向进行转换
[Router-acl-basic-2001] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 2001
[Router-GigabitEthernet0/0/2] quit
```

3. 检查配置结果

- a. 配置 PC1 的 IP 地址为 192.168.1.2/24，网关为 192.168.1.1
- b. 配置 PC2 的 IP 地址为 192.168.2.2/24，网关为 192.168.2.1。
- c. 配置外网 PC 的 IP 地址为 203.0.113.1/24，网关为 203.0.113.2。
- d. 配置完成后，PC1 和 PC2 都可以 Ping 通外网的 IP 203.0.113.1/24，PC1 和 PC2 都可以访问 Internet。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 2 to 3
#
interface GE 1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
interface GE 1/0/2
port default vlan 2
#
interface GE 1/0/3
port default vlan 3
#
return
```

Router 的配置脚本（路由器通过子接口进行三层转发的配置脚本）

```
#
sysname Router
```



```
#
vlan batch 2 to 3
#
dhcp enable
#
acl number 2001
 rule 5 permit source 192.168.0.0 0.0.255.255
#
interface GigabitEthernet0/0/1
#
interface GigabitEthernet0/0/1.1
 dot1q termination vid 2
 ip address 192.168.1.1 255.255.255.0
 arp broadcast enable
 dhcp select interface
 dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface GigabitEthernet0/0/1.2
 dot1q termination vid 3
 ip address 192.168.2.1 255.255.255.0
 arp broadcast enable
 dhcp select interface
 dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface GigabitEthernet0/0/2
 ip address 203.0.113.2 255.255.255.0
 nat outbound 2001
#
ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
#
return
```

Router 的配置脚本（路由器通过 VLANIF 接口进行三层转发的配置脚本）

```
#
sysname Router
#
vlan batch 2 to 3
#
dhcp enable
#
acl number 2001
 rule 5 permit source 192.168.0.0 0.0.255.255
#
```

```
interface Vlanif2
ip address 192.168.1.1 255.255.255.0
dhcp select interface
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface Vlanif3
ip address 192.168.2.1 255.255.255.0
dhcp select interface
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface GigabitEthernet0/0/1
portswitch
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
interface GigabitEthernet0/0/2
ip address 203.0.113.2 255.255.255.0
nat outbound 2001
#
ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
#
return
```

相关信息

视频

[S 系列交换机二层交换机与路由器对接上网](#)

1.1.4.2 三层交换机与路由器对接上网配置案例

三层交换机简介

三层交换机是具有路由功能的交换机，由于路由属于 OSI 模型中第三层网络层的功能，所以称为三层交换机。三层交换机既可以工作在二层也可以工作在三层，可以部署在接入层，也可以部署在汇聚层，作为用户的网关。

配置注意事项

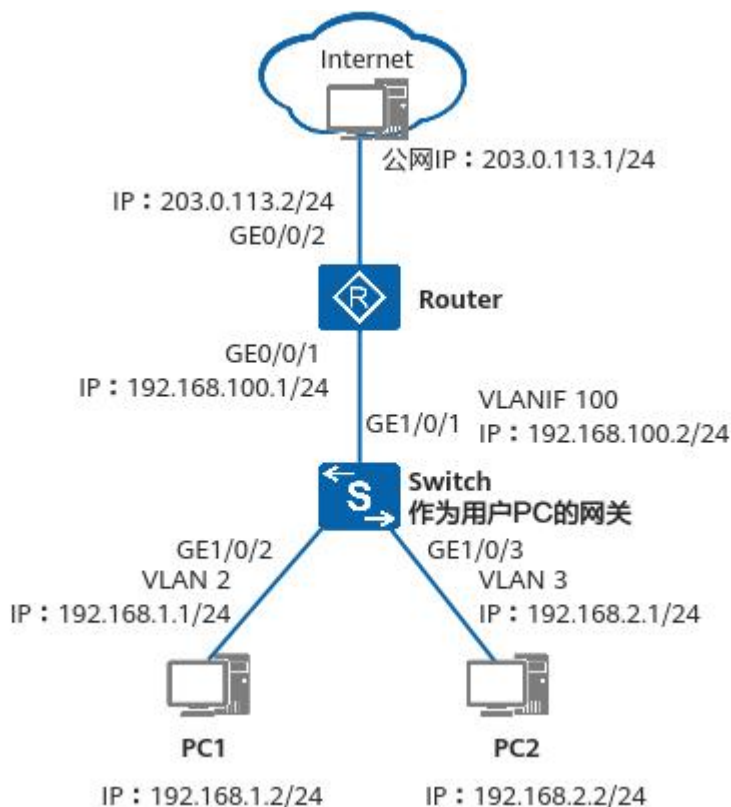
本举例中的交换机配置适用于 S 系列交换机所有产品的所有 V600 版本。

本举例中的路由器配置以 AR651 V300R022C10 为例，其他路由器的配置方法请参见对应的产品文档。

组网需求

如图 1 所示，某公司拥有多个部门且位于不同网段，各部门均有访问 Internet 的需求。现要求用户通过三层交换机和路由器访问外部网络，且要求三层交换机作为用户的网关。

图 1 三层交换机与路由器对接上网组网图



配置思路

采用如下思路进行配置：

1. 配置交换机作为用户的网关，通过 VLANIF 接口，实现跨网段用户互访。
2. 配置交换机作为 DHCP 服务器，为用户分配 IP 地址。
3. 配置路由器通过 NAT 转换，使用户可以访问外部网络。

操作步骤

1. 配置交换机

配置连接用户的接口和对应的 VLANIF 接口。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 2 3
[Switch] interface GE 1/0/2
[Switch-GE1/0/2] port default vlan 2 //配置接口加入 VLAN 2
[Switch-GE1/0/2] quit
[Switch] interface GE 1/0/3
[Switch-GE1/0/3] port default vlan 3
```

```
[Switch-GE1/0/3] quit
[Switch] interface Vlanif 2
[Switch-Vlanif2] ip address 192.168.1.1 24
[Switch-Vlanif2] quit
[Switch] interface Vlanif 3
[Switch-Vlanif3] ip address 192.168.2.1 24
[Switch-Vlanif3] quit
```

配置连接路由器的接口和对应的 VLANIF 接口。

```
[Switch] vlan batch 100
[Switch] interface GE 1/0/1
[Switch-GE1/0/1] port default vlan 100
[Switch-GE1/0/1] quit
[Switch] interface Vlanif 100
[Switch-Vlanif100] ip address 192.168.100.2 24
[Switch-Vlanif100] quit
```

配置缺省路由。

```
[Switch] ip route-static 0.0.0.0 0.0.0.0 192.168.100.1 //缺省路由的下一跳是路由器接口的 IP 地址
192.168.100.1
```

配置 DHCP 服务器。

```
[Switch] dhcp enable
[Switch] interface Vlanif 2
[Switch-Vlanif2] dhcp select interface //DHCP 使用接口地址池的方式为用户分配 IP 地址
[Switch-Vlanif2] dhcp server dns-list 114.114.114.114 223.5.5.5 //配置的 DNS-List 114.114.114.114 是公用
的 DNS 服务器地址，是不区分运营商的。在实际应用中，请根据运营商分配的 DNS 进行配置
[Switch-Vlanif2] quit
[Switch] interface Vlanif 3
[Switch-Vlanif3] dhcp select interface
[Switch-Vlanif3] dhcp server dns-list 114.114.114.114 223.5.5.5
[Switch-Vlanif3] quit
```

2. 配置路由器

配置连接交换机的接口对应的 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname Router
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] ip address 192.168.100.1 255.255.255.0 //配置的 IP 地址 192.168.100.1 为交
换机缺省路由的下一跳 IP 地址
[Router-GigabitEthernet0/0/1] quit
```

配置连接公网的接口对应的 IP 地址。

```
[Router] interface GigabitEthernet 0/0/2
```

```
[Router-GigabitEthernet0/0/2] ip address 203.0.113.2 255.255.255.0 //配置连接公网接口的 IP 地址和公网的 IP 地址在同一网段
[Router-GigabitEthernet0/0/2] quit
```

配置缺省路由和回程路由。

```
[Router] ip route-static 0.0.0.0 0.0.0.0 203.0.113.1 //配置静态缺省路由的下一跳指向公网提供的 IP 地址 203.0.113.1
[Router] ip route-static 192.168.0.0 255.255.0.0 192.168.100.2 //配置回程路由的下一跳就指向交换机上行接口的 IP 地址 192.168.100.2
```

配置 NAT 功能，使内网用户可以访问外网。

```
[Router] acl number 2001
[Router-acl-basic-2001] rule 5 permit source 192.168.0.0 0.0.255.255 //NAT 转换只对源 IP 地址是 192.168.0.0/16 网段的生效，并在接口 GE0/0/2 的出方向进行转换
[Router-acl-basic-2001] quit
[Router] interface GigabitEthernet 0/0/2
[Router-GigabitEthernet0/0/2] nat outbound 2001
[Router-GigabitEthernet0/0/2] quit
```

3. 检查配置结果

- a. 配置 PC1 的 IP 地址为 192.168.1.2/24，网关为 192.168.1.1。
- b. 配置 PC2 的 IP 地址为 192.168.2.2/24，网关为 192.168.2.1。
- c. 配置外网 PC 的 IP 地址为 203.0.113.1/24，网关为 203.0.113.2。
- d. 配置完成后，PC1 和 PC2 都可以 Ping 通外网的 IP 203.0.113.1/24，PC1 和 PC2 都可以访问 Internet。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 2 to 3 100
#
dhcp enable
#
interface Vlanif2
ip address 192.168.1.1 255.255.255.0
dhcp select interface
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface Vlanif3
```

```
ip address 192.168.2.1 255.255.255.0
dhcp select interface
dhcp server dns-list 114.114.114.114 223.5.5.5
#
interface Vlanif100
ip address 192.168.100.2 255.255.255.0
#
interface GE 1/0/1
port default vlan 100
#
interface GE 1/0/2
port default vlan 2
#
interface GE 1/0/3
port default vlan 3
#
ip route-static 0.0.0.0 0.0.0.0 192.168.100.1
#
return
```

Router 的配置脚本

```
#
sysname Router
#
acl number 2001
rule 5 permit source 192.168.0.0 0.0.255.255
#
interface GigabitEthernet0/0/1
ip address 192.168.100.1 255.255.255.0
#
interface GigabitEthernet0/0/2
ip address 203.0.113.2 255.255.255.0
nat outbound 2001
#
ip route-static 0.0.0.0 0.0.0.0 203.0.113.1
ip route-static 192.168.0.0 255.255.0.0 192.168.100.2
#
return
```

1.1.5 特性典型配置案例

[特性典型配置案例的说明](#)

[基础配置](#)

[接口管理](#)[系统管理](#)[虚拟化](#)[以太网交换](#)[IP 地址与服务](#)[IP 路由](#)[VPN](#)[网络切片](#)[可靠性](#)[用户接入与认证](#)[安全](#)[QoS](#)[系统监控](#)

1.1.5.1 特性典型配置案例的说明

特性典型配置案例以特定款型和特定版本为例进行写作，本手册以 V600R023C00 版本为例，适用于通过命令行配置的交换机。各版本各款型间的命令格式或者配置方式可能存在差异，您可以根据用户使用的款型和版本，参见对应的产品文档。

1.1.5.2 基础配置

[首次登录设备](#)[登录设备命令行界面](#)[登录设备 Web 界面](#)[文件系统管理](#)

1.1.5.2.1 首次登录设备

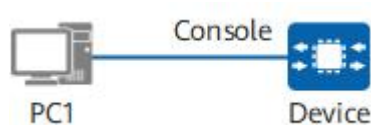
举例：配置用户通过 Console 口首次登录设备

1.1.5.2.1.1 举例：配置用户通过 Console 口首次登录设备

组网需求

当设备第一次上电，需要对此设备进行配置和管理时，可以通过 Console 口登录。如[图 配置 Console 口首次登录设备组网图](#)，设备的 Console 口与用户侧主机 PC1 相连，要求用户通过 Console 口登录设备。

图 1 配置 Console 口首次登录设备组网图



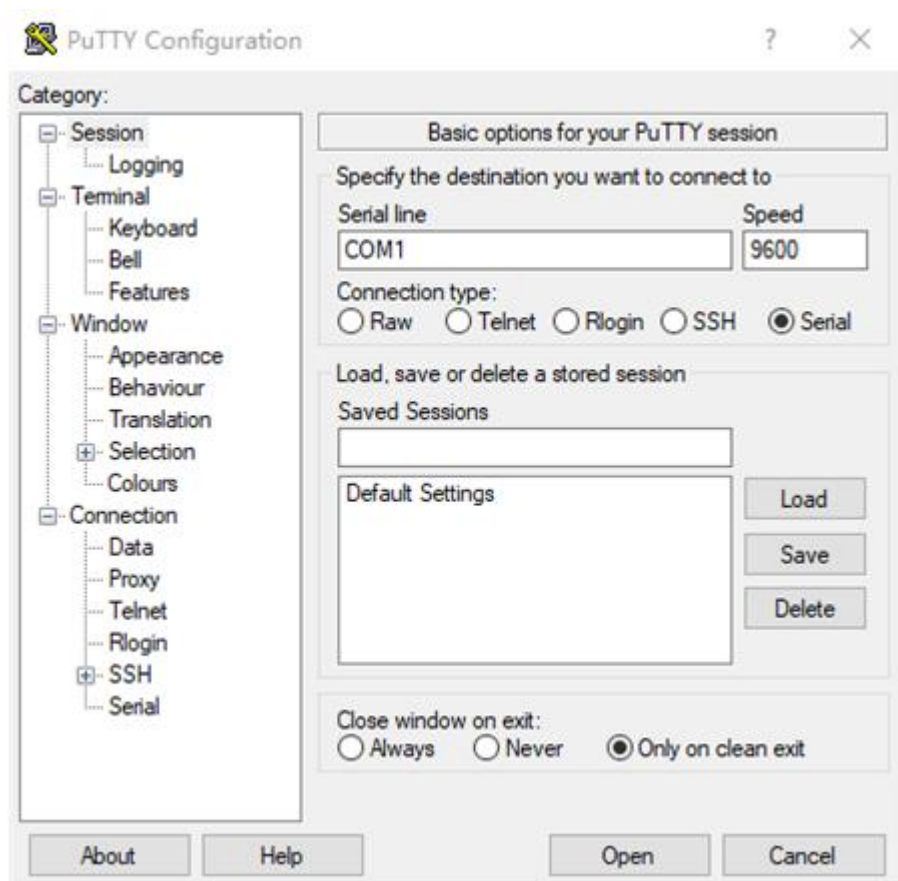
配置思路

1. 通过 Console 口登录设备。
2. 对设备进行基本配置。

操作步骤

1. 将 Console 通信电缆的 DB9（孔）插头插入 PC 机的串口（COM）中，再将 RJ-45 插头端插入设备的 Console 口中。
2. 在 PC 上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。（此处使用第三方软件 PuTTY 为例进行介绍）
 - a. 如[图 新建连接](#)所示，单击“Session”，新建连接。

图 2 新建连接



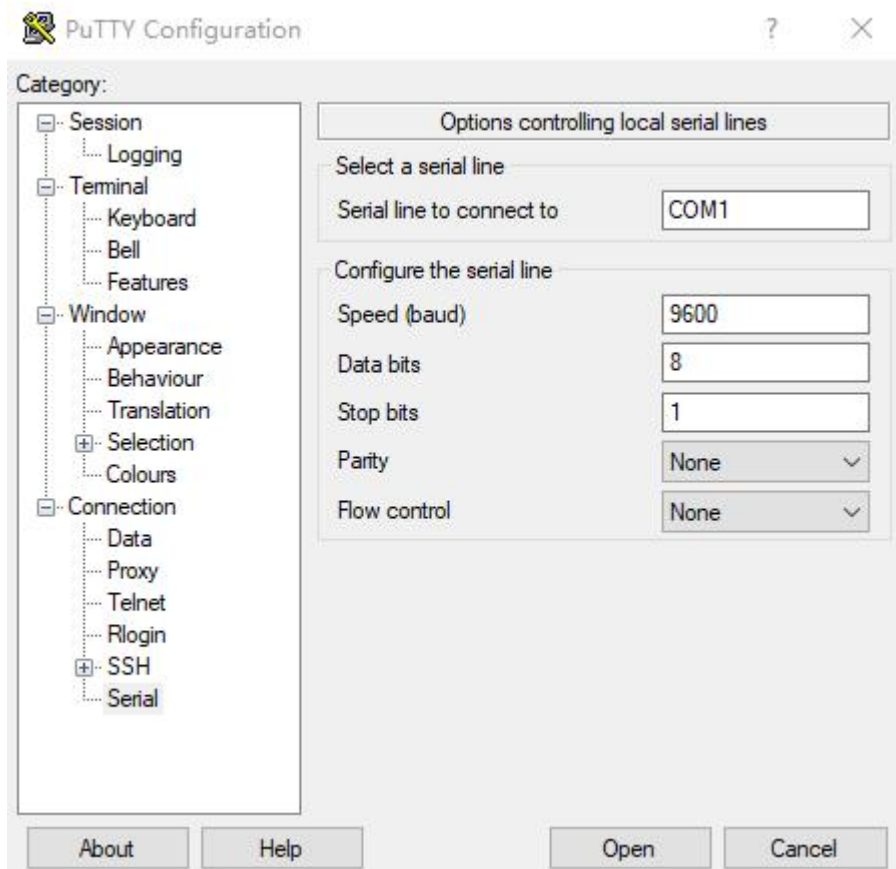
- b. 如图 [设置连接的接口以及通信参数](#) 所示，单击“Serial”，设置连接的接口以及通信参数。
- 连接的接口请根据实际情况进行选择。例如，在 Windows 系统中，可以通过在“设备管理器”中查看端口信息，选择连接的接口。
 - 设置终端软件的通信参数需与设备的缺省值保持一致，分别为：传输速率为 9600bit/s、8 位数据位、1 位停止位、无校验和无流控。
 - 单击“Open”。

说明

因为 PC 端可能会存在多个连接接口，这里需要选择的是连接 Console 线缆的那个接口。一般情况下，选择的接口是 COM1。

若修改了设备的串口通信参数值，需要在 PC 端更换通信参数值与设备的串口通信参数值一致后，重新连接。

图 3 设置连接的接口以及通信参数



3. Enter 键，直到系统出现如下显示，提示用户先设置登录密码，然后再登录。（以下显示信息仅为示意）

User interface con0 is available

Please Press ENTER.

Please configure the login password (8-16)

Enter Password:

Confirm Password: //设置 Console 口登录密码

Info: Save the password now. Please wait for a moment.

Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of terminal users online is 2.

The current login time is 2020-06-30 18:15:10+08:00

<HUAWEI>

说明

第一次通过 Console 口登录设备时，须设置登录密码。登录成功后，串口的权限为默认的管理员权限。

密码为字符串形式，区分大小写，长度范围是 8~16。输入的密码至少包含两种类型字符，包括大写字母、小写字母、数字及特殊字符。特殊字符不包括“？”和空格。

采用交互方式输入的密码不会在终端屏幕上显示出来。

为充分保证设备安全，请用户定期修改密码。

检查配置结果

完成以上配置后，用户可以键入命令，对设备进行配置，如果需要帮助可以随时键入“?”。

1.1.5.2.2 登录设备命令行界面

举例：[配置用户通过 Telnet 登录设备](#)

举例：[配置用户通过 STelnet 登录设备](#)

举例：[配置用户通过 Console 口登录设备](#)

举例：[配置基于 ACL 规则和 RADIUS 认证限制 Telnet 登录设备](#)

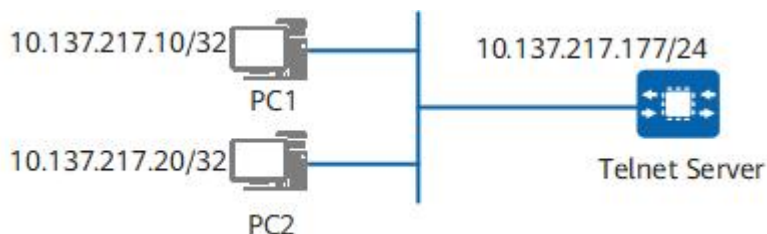
举例：[配置通过 STelnet 登录设备示例（基于 RADIUS 认证）](#)

1.1.5.2.2.1 举例：配置用户通过 Telnet 登录设备

组网需求

如[图 1](#)所示，用户希望简单方便的配置和管理设备。在服务器端配置 Telnet 用户使用 AAA 验证登录，并配置 ACL 策略，保证只有符合 ACL 策略的用户才能登录设备。

图 1 配置通过 Telnet 登录设备组网图



配置思路

采用如下的思路进行配置：

1. 配置 Telnet 方式登录设备，以实现远程维护网络设备。
2. 配置 ACL 策略，保证只有符合 ACL 策略的用户才能登录设备。
3. 配置管理员的用户名和密码，并配置 AAA 认证策略，保证只有认证通过的用户才能登录设备。

配置注意事项

当网络所处环境不够安全时，我们建议选择安全的密码认证方式/加密认证算法/协议。安全的举例请参见：[配置用户通过 STelnet 登录设备](#)。

操作步骤

1. 在用户视图下执行命令 **install feature-software WEAKEA** 安装弱安全算法/协议特性包（WEAKEA）。

2. 配置 Telnet 服务器的管理网口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname Telnet Server
[Telnet Server] interface meth 0/0/0
[Telnet Server-MEth0/0/0] ip address 10.137.217.177 255.255.255.0
[Telnet Server-MEth0/0/0] quit
```

3. 配置服务器的端口号以及使能服务器功能。

```
[Telnet Server] telnet server enable
[Telnet Server] telnet server port 1025
[Telnet Server] telnet server-source all-interface
```

4. 配置 VTY 用户界面的相关参数。

配置 VTY 用户界面的最大个数。

```
[Telnet Server] user-interface maximum-vty 8
```

配置允许用户登录设备的主机地址。

```
[Telnet Server] acl 2001
[Telnet Server-acl4-basic-2001] rule permit source 10.137.217.10 0
[Telnet Server-acl4-basic-2001] rule deny source 10.137.217.20 0
[Telnet Server-acl4-basic-2001] quit
[Telnet Server] user-interface vty 0 7
[Telnet Server-ui-vty0-7] acl 2001 inbound
```

配置 VTY 用户界面的终端属性。

```
[Telnet Server-ui-vty0-7] shell
[Telnet Server-ui-vty0-7] idle-timeout 20
[Telnet Server-ui-vty0-7] screen-length 30
[Telnet Server-ui-vty0-7] history-command max-size 20
[Telnet Server-ui-vty0-7] protocol inbound telnet
```

配置 VTY 用户界面的用户验证方式。

```
[Telnet Server-ui-vty0-7] authentication-mode aaa
[Telnet Server-ui-vty0-7] quit
```

5. 配置登录用户的相关信息。

配置登录验证方式。

```
[Telnet Server] aaa
[Telnet Server-aaa] local-user admin1234 password
Please configure the login password (8-128)
```

It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.

Please enter password:

Please confirm password:

Info: Add a new user.

[Telnet Server-aaa] **local-user admin1234 service-type telnet**

[Telnet Server-aaa] **local-user admin1234 privilege level 3**

[Telnet Server-aaa] **quit**

检查配置结果

进入 PC1 的 Windows 的命令行提示符，执行相关命令，通过 Telnet 方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.137.217.177 1025
```

输入 Enter 键后，在登录窗口输入 AAA 验证方式配置的登录用户名和密码，验证通过后，出现用户视图的命令行提示符，至此用户成功登录设备。

```
Username:admin1234
```

```
Password:
```

```
Info: The max number of VTY users is 8, the number of current VTY users online is 1, and total number of terminal users online is 1.
```

```
<Telnet Server>
```

配置脚本

```
#
sysname Telnet Server
#
telnet server enable
telnet server-source all-interface
telnet server port 1025
#
acl number 2001
rule 5 permit source 10.137.217.10 0
rule 10 deny source 10.137.217.20 0
#
aaa
local-user admin1234 password irreversible-cipher
$1d$g8wLJ`LjL!$CyE(V{3qg5DdU:PM[6=6O$UF-.fQ,Q}>^)OBzgoU$
local-user admin1234 service-type telnet
local-user admin1234 privilege level 3
#
interface MEth0/0/0
```

```
ip address 10.137.217.177 255.255.255.0
#
user-interface maximum-vty 8
#
user-interface vty 0 7
acl 2001 inbound
authentication-mode aaa
history-command max-size 20
idle-timeout 20 0
screen-length 30
#
return
```

1.1.5.2.2.2 举例：配置用户通过 STelnet 登录设备

组网需求

如图 1 所示，在作为 SSH 服务器的设备上使能 STelnet 服务器功能后，SSH 客户端 PC 可以通过不同的认证方式登录 SSH 服务器，这里以 RSA 认证方式为例介绍客户端通过 STelnet 登录服务器的配置过程。为了提升系统安全性，防止非法用户登录到 SSH 服务器，用户可以在 SSH 服务器上配置 ACL 规则。

图 1 配置用户通过 STelnet 登录设备组网图



配置思路

采用如下的思路配置 SSH 用户通过 STelnet 登录设备：

1. 配置 SSH 服务器的管理网口 IP 地址。
2. 在 SSH 服务器端生成本地密钥对。
3. 配置 SSH 服务器的 VTY 用户界面。
4. 创建本地用户，并配置服务类型。
5. 创建 SSH 用户，并配置认证方式。
6. SSH 客户端根据配置的 SSH 用户认证类型创建相应的密钥对，并将公钥拷贝至 SSH 服务器。
7. SSH 服务器端编辑公钥，并将编辑好的公钥分配给用户。
8. 使能 SSH 服务器的 STelnet 功能，配置 SSH 用户的服务类型为 STelnet。
9. 在 SSH 服务器上配置允许 STelnet 客户端登录的 ACL 规则。

10. 配置客户端登录软件的参数，STelnet 至服务器。

数据准备

为完成此配置示例，需准备如下数据：

说明

为了保证更好的安全性，建议使用 3072 位及以上的 RSA 密钥对。

SSH 客户端已安装 OpenSSH 软件。

SSH 服务器的管理网口 IP 地址为 10.248.103.194/24。

本地用户的认证方式为 password，用户名为“admin123”，密码为“YsHsjx_202206”。

SSH 用户的认证方式为 RSA。

配置基本的 ACL 2000，允许 10.248.103.0/24 网段的客户端合法接入 SSH 服务器。

操作步骤

1. 配置 SSH 服务器的管理网口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH Server
[SSH Server] interface meth 0/0/0
[SSH Server-MEth0/0/0] ip address 10.248.103.194 255.255.255.0
[SSH Server-MEth0/0/0] quit
```

2. 在 SSH 服务器端生成本地密钥对。

```
[SSH Server] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

3. 配置 SSH 服务器的 VTY 用户界面。

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

说明

若配置登录协议为 SSH，则设备将自动禁止 Telnet 功能。

4. 在服务器端创建本地用户，并配置用户服务方式。

```
[SSH Server] aaa
```

```
[SSH Server-aaa] local-user admin123 password
```

Please configure the login password (8-128)

It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.

Please enter password:

Please confirm password:

Info: Add a new user.

```
[SSH Server-aaa] local-user admin123 service-type ssh
```

```
[SSH Server-aaa] local-user admin123 privilege level 3
```

```
[SSH Server-aaa] quit
```

5. 在服务器端创建 SSH 用户，并配置认证方式。

```
[SSH Server] ssh user admin123
```

```
[SSH Server] ssh user admin123 authentication-type rsa
```

6. 配置 SSH 服务器的公钥算法、加密算法、密钥交换算法列表、HMAC 认证算法和最小密钥长度。

```
[SSH Server] ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
```

```
[SSH Server] ssh server hmac sha2_256 sha2_512
```

```
[SSH Server] ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
```

```
[SSH Server] ssh server publickey rsa_sha2_256 rsa_sha2_512
```

```
[SSH Server] ssh server dh-exchange min-len 3072
```

7. SSH 客户端使用 OpenSSH 创建 RSA 密钥对，并将密钥对中的公钥拷贝至 SSH 服务器。

进入 Windows 的命令行提示符，创建 RSA 密钥对，并保存到本地 id_rsa.pub 文件中（以下内容仅为示例）。

```
C:\Users\User1>ssh-keygen -t rsa
```

Generating public/private rsa key pair.

Enter file in which to save the key (C:\Users\User1\.ssh\id_rsa):

Enter passphrase (empty for no passphrase):

Enter same passphrase again:

Your identification has been saved in C:\Users\User1\.ssh\id_rsa.

Your public key has been saved in C:\Users\User1\.ssh\id_rsa.pub.

The key fingerprint is:

SHA256:c43yubJjCUjY3JqH0aVZwJFM3gWJcH4YI5+4HUDAlqo

The key's randomart image is:

```
+----[RSA 3072]-----+
```

```
|..o==B=.o. |
```

```
|o. O=*+. |
```

```
|o. +.oB=o |
```

```
|..=o=o o |
```

```
|. *.S o. |
```

```
|E =o =. |
```

```
|...o |
```



```
|   = .   |
|   ..+.  |
+-----[SHA256]-----+
```

8. SSH 服务器编辑 SSH 客户端 OpenSSH 生成的公钥，并将编辑后的公钥分配给 SSH 用户。

```
[SSH Server] rsa peer-public-key rsa01 encoding-type openssh
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-public-key-rsa-key-code] ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQACg5Ag490i6ilB7QuCVb35B8RJEh1DIYB88h2p1qjdh7qdMQv
8rpJaVAgQWxwzKZO0Xdfuz4ReGQzTCSf7Det7Ajicddw3qi+6P8hRqZj6MPdLg/o3RN4aPCfr/LFWCwqJ
3gWGHIOC7qqjRk+6pySVoiWcSk5/elBkU7WVkcSWrt4qFXJV373OCesKcEVeDvAa1Tvx6L3LQroBqUO
0EXzDgOthPCmOqiqvS5h3JipzqVsesdSKjelnooCQzSOv5eePpBcFclvU6wFiLIZ5vnf6YtypgTVzHuje/sh4
xM7luuon7AYXKHT8NpO9jd9zA/lKaRPXyDtei1O1Bt/5lxnn
[SSH Server-rsa-public-key-rsa-key-code] public-key-code end
[SSH Server-key-code] peer-public-key end
[SSH Server] ssh user admin123 assign rsa-key rsa01
```

9. 使能 STelnet 功能，并配置用户的服务类型为 STelnet。

```
[SSH Server] stelnet server enable
[SSH Server] ssh server-source all-interface
[SSH Server] ssh user admin123 service-type stelnet
```

10. 配置 ACL 规则。

```
[SSH Server] acl 2000
[SSH Server-acl4-basic-2000] rule permit source 10.248.103.0 24
[SSH Server-acl4-basic-2000] quit
[SSH Server] ssh server acl 2000
```

检查配置结果

客户端通过 OpenSSH 软件登录 SSH 服务器。进入 Windows 的命令行提示符，执行 OpenSSH 命令，通过 STelnet 方式访问设备。

```
C:\Users\User1>ssh admin123@10.248.103.194
Enter passphrase for key 'C:\Users\User1\.ssh\id_rsa':
Info: The max number of VTY users is 21, the number of current VTY users online is 4, and total number of
terminal users online is 4.

The current login time is 2020-12-15 15:58:03.
<SSH Server>
```

配置脚本

```
#
```

```
sysname SSH Server
#
acl number 2000
 rule 5 permit source 10.248.103.0 0.0.0.255
#
rsa peer-public-key rsa01 encoding-type openssh
 public-key-code begin
  ssh-rsa
 AAAAB3NzaC1yc2EAAAADAQABAAQACg5Ag490i6ilB7QuCVb35B8RJEh1DIYB88h2p1qjdh7qdMQv8rpJaV
 AgQWxwzKZO0XdFuz4ReGQzTCSf7Det7Ajjcddw3qi+6P8hRqZj6MPdLg/o3RN4aPCfr/LFWCwqJ3gWGHIOC7
 qqjRk+6pySVoiWcSk5/elBkU7WVvk/cSWrt4qFXJV373OCesKcEVeDvAa1Tvx6L3LQroBqUO0EXzDgOthPCmOq
 iqvS5h3JipzqVsesdSKjelnooCQzSOv5eePpBcFclvU6wFiLIZ5vnf6YtypgTVzHuje/sh4xM7luon7AYXKHT8NpO
 9jd9zA/lKaRPXyDtei1O1Bt/5lxnn rsa-key
 public-key-code end
 peer-public-key end
#
aaa
 local-user admin123 password irreversible-cipher
 $1d$+,JS+))\2$KVNj(.3`_5x0FCKGv}H&.kUTI`Ff&H*eBqO.ua>)$
 local-user admin123 service-type terminal ssh
 local-user admin123 privilege level 3
#
interface MEth0/0/0
 ip address 10.248.103.194 255.255.255.0
#
stelnet server enable
ssh user admin123
ssh user admin123 authentication-type rsa
ssh user admin123 assign rsa-key rsa01
ssh user admin123 service-type stelnet
ssh server-source all-interface
ssh server acl 2000
#
ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh server hmac sha2_256 sha2_512
ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh server publickey rsa_sha2_256 rsa_sha2_512
ssh server dh-exchange min-len 3072
#
user-interface vty 0 4
 authentication-mode aaa
 protocol inbound ssh
#
```

return

1.1.5.2.2.3 举例：配置用户通过 Console 口登录设备

组网需求

当用户无法进行远程登录设备时，可通过 Console 口进行本地登录。使用 Console 口登录设备时需要密码认证，为了防止非法用户登录设备，修改 Console 用户界面的认证方式为 AAA 认证。

图 1 配置通过 Console 口登录设备组网图



配置思路

采用如下的思路配置通过 Console 口登录设备：

1. 使用终端仿真软件通过 Console 口登录设备。
2. 配置 Console 用户界面的认证方式。

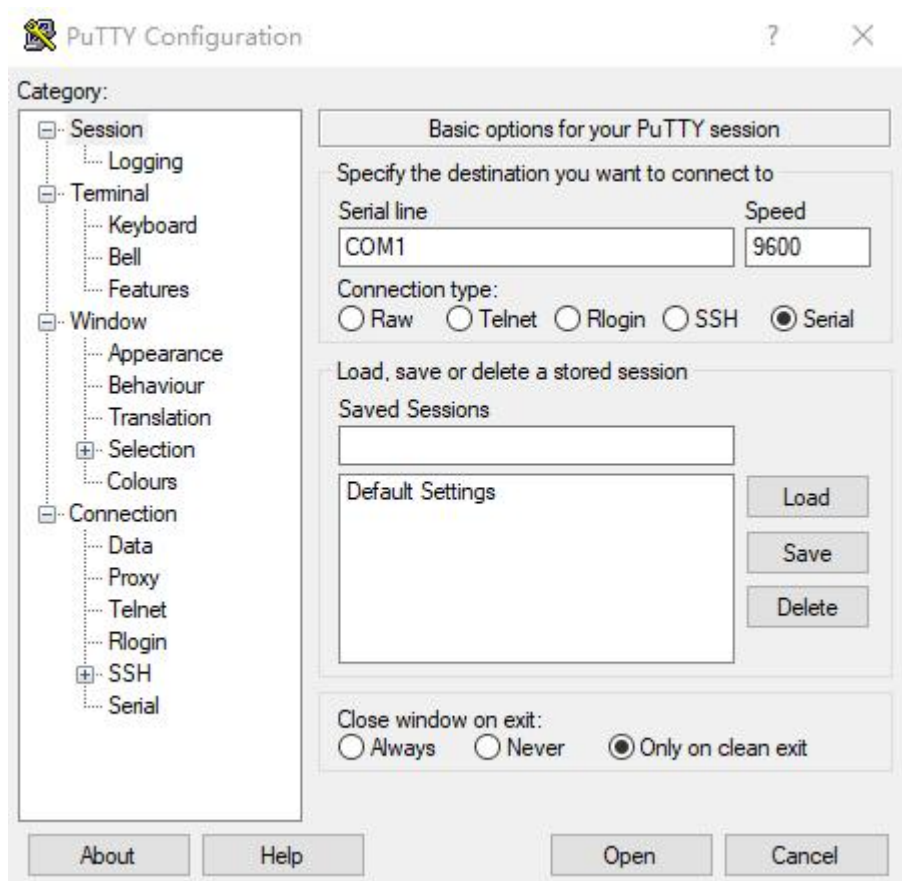
说明

如果系统不带终端仿真软件，请您准备第三方终端仿真软件，使用方法请参照该软件的使用指导或联机帮助。

操作步骤

1. 将 Console 通信电缆的 DB9（孔）插头插入 PC 机的串口（COM）中，再将 RJ-45 插头端插入设备的 Console 口中。如果终端（PC 端）上没有 DB9 串口，可通过 DB9 串口转 USB 的转接线，将 USB 口连接到终端上。
2. 在 PC 上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。（此处使用第三方软件 PuTTY 为例进行介绍）
 - a. 如[图 2](#)所示，单击“Session”，新建连接。

图 2 新建连接



b. 如图 3 所示，单击“Serial”，设置连接的接口以及通信参数。

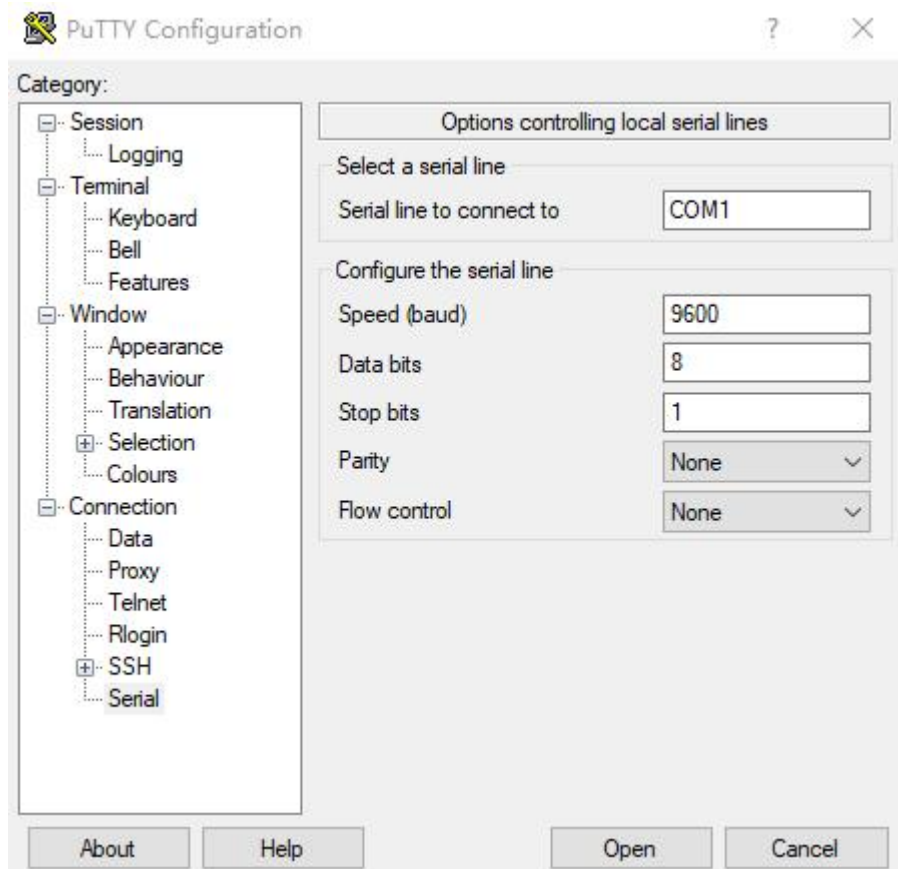
- i. 连接的接口请根据实际情况进行选择。例如，在 Windows 系统中，可以通过在“设备管理器”中查看端口信息，选择连接的接口。
- ii. 设置终端软件的通信参数需与设备的缺省值保持一致，分别为：传输速率为 9600bit/s、8 位数据位、1 位停止位、无校验和无流控。
- iii. 单击“Open”。

说明

因为 PC 端可能会存在多个连接接口，这里需要选择的是连接 Console 线缆的那个接口。一般情况下，选择的接口是 COM1。

若修改了设备的串口通信参数值，需要在 PC 端更换通信参数值与设备的串口通信参数值一致后，重新连接。

图 3 设置连接的接口以及通信参数



3. 按 Enter 键，直到系统出现如下显示，提示用户输入密码。（AAA 认证时，提示输入用户名和密码，以下显示信息仅为示意）

Login authentication

Password:

进入设备后，用户可以键入命令，对设备进行配置，需要帮助可以随时键入“?”。

4. 配置 Console 用户界面的认证方式

```
<HUAWEI> system-view
[HUAWEI] user-interface console 0
[HUAWEI-ui-console0] authentication-mode aaa
[HUAWEI-ui-console0] user privilege level 3
[HUAWEI-ui-console0] quit
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin1234 password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters,
uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
[HUAWEI-aaa] local-user admin1234 privilege level 3
```

```
[HUAWEI-aaa] local-user admin1234 service-type terminal
```

检查配置结果

执行以上操作后，用户使用 Console 用户界面重新登录设备时，需要输入用户名 admin1234，认证密码 YsHsjx_202206 才能通过身份验证，成功登录设备。

```
Username:admin1234
```

```
Password:
```

```
<HUAWEI>
```

配置脚本

```
#
aaa
 local-user admin1234 password irreversible-cipher
 $1d$g8wLJ`LjLI$CyE(V{3qg5DdU:PM[6=6O$UF-.fQ,Q}>^)OBzgoU$
 local-user admin1234 service-type terminal
 local-user admin1234 privilege level 3
#
user-interface con 0
 authentication-mode aaa
#
return
```

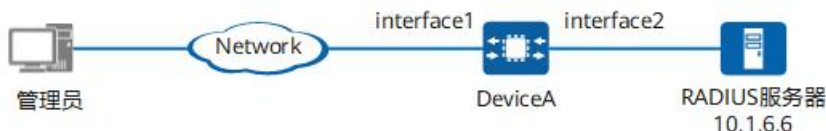
1.1.5.2.2.4 举例：配置基于 ACL 规则和 RADIUS 认证限制 Telnet 登录设备

组网需求

网络管理员希望能够对设备进行远程管理与维护，同时对网络的安全性要求较高，希望网络不受未经授权访问的干扰。可以通过配置基于 ACL 规则以及 RADIUS 认证的 Telnet 登录方式满足用户的需求。

如图 [基于 ACL 规则和 RADIUS 认证限制 Telnet 登录设备组网图](#) 所示，DeviceA 为 Telnet 服务器，网络管理员和 DeviceA 之间、DeviceA 与 RADIUS 服务器之间路由可达。RADIUS 服务器的 IP 地址为 10.1.6.6/24，认证端口号为 1812。

图 1 基于 ACL 规则和 RADIUS 认证限制 Telnet 登录设备组网图



说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。

配置思路

采用如下的思路进行配置（基于 ACL 规则和 RADIUS 认证）：

1. 配置设备接口相关参数。
2. 配置 Telnet 协议，实现用户可以通过 Telnet 登录设备。
3. 配置 ACL 规则，保证只有满足该规则的用户才能登录设备。
4. 配置 RADIUS 协议，实现 RADIUS 认证。用户通过 Telnet 登录设备时使用 RADIUS 服务器上配置的用户名和密码，从而保证用户登录的安全性。
5. 配置 RADIUS 服务器。

配置注意事项

当网络所处环境不足够安全时，我们建议选择安全的密码认证方式/加密认证算法/协议。安全的举例请参见：[举例：配置通过 STelnet 登录设备示例（基于 RADIUS 认证）](#)

配置前请确保各设备之间路由可达。

请确保设备上配置的 RADIUS 服务器的地址、端口号和共享密钥配置正确，并且和 RADIUS 服务器上的配置保持一致。

域被配置成全局默认管理域之后，管理用户的用户名中携带该域名或者不携带域名时，会使用全局默认管理域下的 AAA 配置信息。

请确保已在 RADIUS 服务器上配置了用户。本例中假设 RADIUS 服务器上已配置了用户 `admin123@huawei.com`（用户名@域名），其密码为 `YsHsjx_202206`。

如果 RADIUS 服务器不接受包含域名的用户名，还需要配置命令 `undo radius-server user-name domain-included` 使设备向 RADIUS 服务器发送的报文中的用户名不包含域名。

操作步骤

1. 在用户视图下执行命令 `install feature-software WEAKEA` 安装弱安全算法/协议特性包（WEAKEA）。
2. 配置接口的相关参数。
配置接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface 10ge 1/0/1
```

```
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.2 255.255.255.0
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.6.2 255.255.255.0
[DeviceA-Vlanif20] quit
```

3. 配置 Telnet 登录。

配置服务器的端口号以及使能 Telnet 服务器功能。

```
[DeviceA] telnet server enable
[DeviceA] telnet server port 1025
[DeviceA] telnet server-source all-interface
```

配置 VTY 用户界面 0~4 的认证方式为 AAA 认证、支持的协议为 Telnet。

```
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] authentication-mode aaa
[DeviceA-ui-vty0-4] protocol inbound telnet
[DeviceA-ui-vty0-4] user privilege level 3
[DeviceA-ui-vty0-4] quit
```

4. 在 DeviceA 上配置 ACL 规则允许管理员登录。

```
[DeviceA] acl 2000
[DeviceA-acl4-basic-2000] rule permit source 10.137.217.10 0
[DeviceA-acl4-basic-2000] quit
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] acl 2000 inbound
[DeviceA-ui-vty0-4] quit
```

5. 配置 RADIUS 认证。

配置 RADIUS 服务器模板，实现与 RADIUS 服务器的通信。

```
[DeviceA] radius-server template 1
[DeviceA-radius-1] radius-server authentication 10.1.6.6 1812 weight 80
[DeviceA-radius-1] radius-server shared-key cipher YsHsjx_202206
[DeviceA-radius-1] quit
```

配置 AAA 认证方案，指定认证方式为 RADIUS。


```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme auth1
[DeviceA-aaa-authen-auth1] authentication-mode radius
[DeviceA-aaa-authen-auth1] quit
```

创建域，并在域下引用 AAA 认证方案及 RADIUS 服务器模板。

```
[DeviceA-aaa] domain huawei.com
[DeviceA-aaa-domain-huawei.com] authentication-scheme auth1
[DeviceA-aaa-domain-huawei.com] accounting-scheme acc1
[DeviceA-aaa-domain-huawei.com] radius-server 1
[DeviceA-aaa-domain-huawei.com] quit
[DeviceA-aaa] quit
```

配置 huawei.com 为全局默认管理域，这样管理员登录设备时就不需要输入域名。

```
[DeviceA] domain huawei.com admin
```

6. 配置 RADIUS 服务器。

配置步骤包括：添加设备、添加用户、配置授权用户级别为 3。

检查配置结果

进入管理员的 Windows 的命令行提示符，执行相关命令，通过 Telnet 方式登录设备。

```
C:\Documents and Settings\Administrator> telnet 10.1.1.2 1025
```

在登录界面根据提示输入 RADIUS 服务器上配置的用户名 **admin123** 和密码 **YsHsjx_202206**，并按 Enter 键，验证通过，用户成功通过 Telnet 登录到 DeviceA。（以下显示仅为示意）

```
Username:admin123
Password:
Info: The max number of VTY users is 8, the number of current VTY users online is 1, and total number of
terminal users online is 1.
<>
```

配置脚本

```
#
sysname DeviceA
#
acl number 2000
rule permit source 10.137.217.10 0
#
radius-server template 1
```

```
radius-server shared-key
cipher %+%##!!!!!!!"!!!!!!*!!!!SKvr$[[Fs.3t@/5k|BENhEu>W(3~XG!!D;!!!!2jp5!!!!A!!!!3"pK8qv!}9M#(4$JGWvQ
F/R[CNe/+:W^jk8HUe&W%+%#
radius-server authentication 10.1.6.6 1812 weight 80
#
aaa
authentication-scheme auth1
authentication-mode radius
accounting-scheme acc1
accounting-mode radius
domain huawei.com
authentication-scheme auth1
accounting-scheme acc1
radius-server 1
#
domain huawei.com admin
#
vlan batch 10 20
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
#
interface Vlanif20
ip address 10.1.6.2 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
#
telnet server enable
telnet server-source -i Vlanif10
telnet server port 1025
#
user-interface vty 0 4
acl 2000 inbound
authentication-mode aaa
user privilege level 3
protocol inbound telnet
#
```

```
acl number 2000
rule 5 permit source 10.137.217.10 0
#
return
```

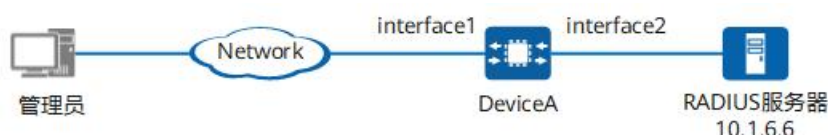
1.1.5.2.2.5 举例：配置通过 STelnet 登录设备示例（基于 RADIUS 认证）

组网需求

网络管理员希望通过安全的方式远程登录设备，同时对网络的安全性要求较高，希望网络不受未经授权访问的干扰。可以通过配置基于 RADIUS 认证的 STelnet 满足用户的需求。

如[图 通过 STelnet 登录设备（基于 RADIUS 认证）组网图](#)所示，DeviceA 为 SSH 服务器，与 RADIUS 服务器之间路由可达。RADIUS 服务器的 IP 地址为 10.1.6.6/24，认证端口号为 1812。

图 1 通过 STelnet 登录设备（基于 RADIUS 认证）组网图



说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。

配置思路

采用如下思路配置通过 STelnet 登录设备（基于 RADIUS 认证）：

1. 配置设备接口相关参数。
2. 在 SSH 服务器端生成本地密钥对，实现在服务器端和客户端进行安全地数据交互。
3. 配置 STelnet 协议，实现用户可以通过 STelnet 登录设备。
4. 配置 ACL 规则，保证只有满足该规则的用户才能登录设备。
5. 配置 RADIUS 协议，实现 RADIUS 认证。用户通过 STelnet 登录设备时使用 RADIUS 服务器上配置的用户名和密码，从而保证用户登录的安全性。
6. 配置 RADIUS 服务器。

配置注意事项

配置 STelnet 登录设备前，用户终端应该已安装 SSH 服务器登录软件。

请确保用户终端和登录的设备及 RADIUS 服务器之间均路由可达。

域被配置成全局默认管理域之后，管理用户的用户名中携带该域名或者不携带域名时，会使用全局默认管理域下的 AAA 配置信息。

请确保已在 RADIUS 服务器上配置了用户。本例中假设 RADIUS 服务器上已配置了用户 **admin123@huawei.com**（用户名@域名），其密码为 **YsHsjx_202206**。

如果 RADIUS 服务器不接受包含域名的用户名，还需要配置命令 **undo radius-server user-name domain-included** 使设备向 RADIUS 服务器发送的报文中的用户名不包含域名。

操作步骤

1. 配置接口的相关参数。

配置接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.2 255.255.255.0
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.6.2 255.255.255.0
[DeviceA-Vlanif20] quit
```

2. 配置 STelnet 登录。

在服务器端生成本地密钥对。

```
[DeviceA] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

配置 SSH 服务器的 VTY 用户界面。

```
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] authentication-mode aaa
```

```
[DeviceA-ui-vty0-4] protocol inbound ssh
[DeviceA-ui-vty0-4] user privilege level 3
[DeviceA-ui-vty0-4] quit
```

配置 SSH 服务器的公钥算法、加密算法、密钥交换算法列表、HMAC 认证算法和最小密钥长度。

```
[DeviceA] ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
[DeviceA] ssh server hmac sha2_256 sha2_512
[DeviceA] ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
[DeviceA] ssh server publickey rsa_sha2_256 rsa_sha2_512
```

在服务器端创建 SSH 用户，并配置认证方式为 Password 认证。

```
[DeviceA] ssh user admin123
[DeviceA] ssh user admin123 authentication-type password
```

说明

如果需要配置多个 SSH 用户使用 Password 认证方式，可以执行命令 **ssh authentication-type default password** 将 SSH 用户的缺省认证方式指定为 Password 认证。配置完成后，不用再对每一个 SSH 用户配置认证方式和服务类型，从而简化配置，提高效率。

使能 STelnet 功能，并配置用户的服务类型为 STelnet。

```
[DeviceA] stelnet server enable
[DeviceA] ssh server-source all-interface
[DeviceA] ssh user admin123 service-type stelnet
```

3. 在 DeviceA 上配置 ACL 规则允许管理员登录。

```
[DeviceA] acl 2000
[DeviceA-acl4-basic-2000] rule permit source 10.137.217.10 0
[DeviceA-acl4-basic-2000] quit
[DeviceA] ssh server acl 2000
```

说明

采用 ACL 方式配置 Telnet 终端服务的配置为可选配置。

4. 配置 RADIUS 认证。

配置 RADIUS 服务器模板，实现与 RADIUS 服务器的通信。

```
[DeviceA] radius-server template 1
[DeviceA-radius-1] radius-server authentication 10.1.6.6 1812 weight 80
[DeviceA-radius-1] radius-server shared-key cipher YsHsjx_202206
[DeviceA-radius-1] quit
```

配置 AAA 认证方案，指定认证方式为 RADIUS。

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme auth1
[DeviceA-aaa-authen-auth1] authentication-mode radius
[DeviceA-aaa-authen-auth1] quit
```

创建域，并在域下引用 AAA 认证方案及 RADIUS 服务器模板。

```
[DeviceA-aaa] domain huawei.com
[DeviceA-aaa-domain-huawei.com] authentication-scheme auth1
[DeviceA-aaa-domain-huawei.com] accounting-scheme acc1
[DeviceA-aaa-domain-huawei.com] radius-server 1
[DeviceA-aaa-domain-huawei.com] quit
[DeviceA-aaa] quit
```

配置 huawei.com 为全局默认管理域，这样管理员登录设备时就不需要输入域名。

```
[DeviceA] domain huawei.com admin
```

5. 配置 RADIUS 服务器。

配置步骤包括：添加设备、添加用户、配置授权用户级别为 3。

检查配置结果

客户端通过 OpenSSH 软件登录 SSH 服务器。进入 Windows 的命令行提示符，执行 OpenSSH 命令，通过 STelnet 方式访问设备。在登录界面根据提示输入 RADIUS 服务器上配置的用户名 **admin123** 和密码 **YsHsjx_202206**，并按 Enter 键，验证通过，用户成功通过 STelnet 登录到 DeviceA。（以下显示仅为示意）

```
C:\Documents and Settings\Administrator>ssh admin123@10.1.1.2
```

```
Enter passphrase for key 'C:\Users\User/.ssh/id_rsa':
```

```
Enter password:
```

```
Warning: Negotiated key exchange algorithm and identity key for server authentication are not safe. It is recommended that you disable the insecure algorithm or upgrade the client.
```

```
Warning: The initial password poses security risks.
```

```
The password needs to be changed. Change now? [Y/N]:n
```

```
Info: The max number of VTY users is 21, the number of current VTY users online is 1, and total number of terminal users online is 2.
```

```
The current login time is 2022-09-28 12:07:34.
```

```
The last login time is 2022-09-28 06:44:35 from 172.16.0.1 through SSH.
```

```
The last login failure time is 2022-09-28 11:59:21 from 172.16.0.1 through SSH. Consecutive login failures since the last successful login: 3.
```

```
<DeviceA>
```

配置脚本

```
#
sysname DeviceA
#
acl number 2000
```

```
rule 5 permit source 10.137.217.10 0
#
radius-server template 1
radius-server shared-key
cipher %+%##!!!!!!"!!!!!!*!!!!SKvr$[[Fs.3t@/5k|BENhEu>W(3~XG!!D;!!!!2jp5!!!!A!!!!3"pK8qv!}9M#(4$jGWvQ
F/R[CNe/+:W^jk8HUe&W%+%#
radius-server authentication 10.1.6.6 1812 weight 80
#
aaa
authentication-scheme auth1
authentication-mode radius
accounting-scheme acc1
accounting-mode radius
domain huawei.com
authentication-scheme auth1
accounting-scheme acc1
radius-server 1
#
domain huawei.com admin
#
vlan batch 10 20
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
#
interface Vlanif20
ip address 10.1.6.2 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
#
stelnet server enable
ssh user admin123
ssh user admin123 authentication-type password
ssh user admin123 service-type stelnet
ssh server-source all-interface
ssh server acl 2000
#
```

```
user-interface vty 0 4
authentication-mode aaa
user privilege level 3
protocol inbound ssh
#
ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh server hmac sha2_256 sha2_512
ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh server publickey rsa_sha2_256 rsa_sha2_512
ssh server dh-exchange min-len 3072
#
return
```

1.1.5.2.3 登录设备 Web 界面

举例：通过 HTTPS 登录 Web 界面（默认证书）

1.1.5.2.3.1 举例：通过 HTTPS 登录 Web 界面（默认证书）

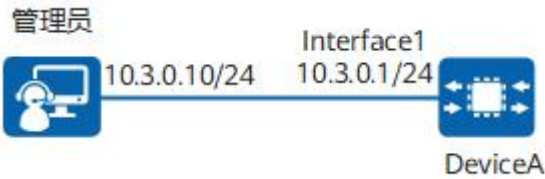
组网信息

如图 1 所示，为 DeviceA 配置一个本地帐号 admin123，允许该帐号可以通过 HTTPS 登录到 Web 界面。

图 1 通过 HTTPS（默认证书）登录 Web 界面组网图

说明

本例中 interface1 代表 Vlanif10。



数据规划

项目	数据
用户名	admin123
密码	YsHsjx_202206
服务类型	HTTPS
用户级别	3

配置思路

1. 配置所有接口都可用于访问 Web 界面。
2. 配置设备登录接口。
3. 创建本地用户帐号，用于 Web 登录设备。
4. 开启设备的 Web 服务功能。
5. 用户使用本地用户帐号和密码登录 Web 界面。

操作步骤

1. 配置所有接口都可用于访问 Web 界面。

```
<HUAWEI> system-view  
[HUAWEI] sysname DeviceA  
[DeviceA] web-manager server-source all-interface
```

2. 配置设备登录接口。

- a. 配置接口的 IP 地址。

```
[DeviceA] interface vlanif10  
[DeviceA-Vlanif10] ip address 10.3.0.1 255.255.255.0  
[DeviceA-Vlanif10] quit
```

3. 创建 Web 用户帐号。

```
[DeviceA] aaa  
[DeviceA-aaa] local-user admin123 password irreversible-cipher YsHsjx_202206  
[DeviceA-aaa] local-user admin123 service-type http  
[DeviceA-aaa] local-user admin123 privilege level 3  
[DeviceA-aaa] quit
```

4. 开启 Web 服务功能。

- a. 开启 HTTPS 服务。

```
[DeviceA] web-manager enable port 8443
```

- b. 配置 HTTP 协议强制跳转为 HTTPS 协议。

```
[DeviceA] web-manager http forward enable
```

开启该功能后，如果使用 HTTP 协议访问 Web 界面，设备会自动使用安全性更高的 HTTPS 协议进入 Web 界面。

5. 登录 Web 界面。

- a. 配置管理员 PC 的 IP 地址为 10.3.0.10/24。
- b. PC 中打开网络浏览器，输入需要登录设备的 IP 地址 “https://10.3.0.1:8443”。

c. 在登录界面中输入管理员的用户名“admin123”和密码“YsHsjx_202206”，单击“登录”。

检查配置结果

管理员通过 Web 浏览器访问设备的 Web 界面，输入用户名和密码后，检查是否成功登录设备 Web 界面。

配置脚本

```
#
sysname DeviceA
#
web-manager server-source all-interface
web-manager enable port 8443
web-manager http forward enable
#
interface Vlanif10
 ip address 10.3.0.1 255.255.255.0
#
aaa
 local-user admin123 password irreversible-cipher
 $1d$OwseVRh@LH}ZeTBm$1nH4$ab>d(N{-%0!ab48y=lc*xEUR4pVhR2"9-~,$
 local-user admin123 service-type http
 local-user admin123 privilege level 3
#
return
```

1.1.5.2.4 文件系统管理

举例：本地文件操作

举例：配置设备作为 FTP 服务器

举例：配置设备作为 SFTP 服务器

举例：配置设备作为 TFTP 客户端

举例：配置设备作为 FTP 客户端

举例：配置设备作为 SFTP 客户端

举例：配置设备作为 SCP 客户端

1.1.5.2.4.1 举例：本地文件操作

组网需求

用户通过 Console 口、Telnet 或 STelnet 方式登录设备，需要对设备上的文件进行以下操作：

查看当前目录下的文件及子目录。

创建目录 **test**，将文件 **vrpcfg.zip** 复制至 **test** 目录下，并命名为 **backup.zip**。

查看 **test** 目录下的文件。

操作步骤

1. 查看当前目录下的文件及子目录。

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] quit
<Device> dir
Directory of flash:/

Idx Attr  Size(Byte) Date      Time      FileName
 0 -rw-    889 Mar 01 2019 14:41:56 private-data.txt
 1 -rw-   6,311 Feb 17 2019 14:05:04 backup.cfg
 2 -rw-   2,393 Mar 06 2019 17:20:10 vrpcfg.zip
 3 -rw-    812 Nov 12 2019 15:43:10 hostkey
 4 drw-      - Mar 01 2019 14:41:46 compatible
 5 -rw-    540 Nov 12 2019 15:43:12 serverkey
...
670,092 KB total (569,904 KB free)
```

2. 创建目录 **test**，将文件 **vrpcfg.zip** 复制至 **test** 目录下，并命名为 **backup.zip**。

创建目录 **test**。

```
<Device> mkdir test
Info: Create directory flash:/test/.....Done.
```

复制 **vrpcfg.zip** 至 **test** 目录下，并命名为 **backup.zip**。

```
<Device> copy vrpcfg.zip flash:/test/backup.zip
Info: Are you sure to copy flash:/vrpcfg.zip to flash:/test/backup.zip?[Y/N]:y
100% complete
Info: Copied file flash:/vrpcfg.zip to flash:/test/backup.zip...Done.
```

说明

如果不指定目标文件名，则目标文件名默认为源文件名，即目标文件和源文件同名。

检查配置结果

进入 **test** 目录。

```
<Device> cd test
```

查看当前的工作路径。

```
<Device> pwd
```

```
flash:/test/
```

查看 **test** 目录下的文件。

```
<Device> dir
```

```
Directory of flash:/test/
```

Idx	Attr	Size(Byte)	Date	Time	FileName
0	-rw-	2,399	Mar 12 2012	11:16:44	backup.zip

```
670,092 KB total (569,900 KB free)
```

配置脚本

```
#  
sysname Device  
  
#  
return
```

1.1.5.2.4.2 举例：配置设备作为 FTP 服务器

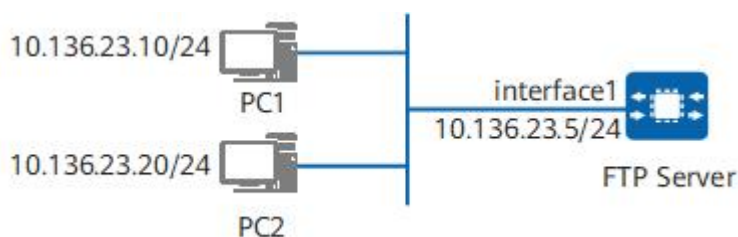
组网需求

如图 1 所示，PC1 与设备相连，10.136.23.5 是设备的 IP 地址，设备需要进行升级操作，要求将设备作为 FTP 服务器，从终端 PC1 将系统软件上传至设备，且保存当前设备的配置文件到终端进行备份。配置 ACL 策略，保证只有 PC1 才能访问 FTP 服务器。

图 1 设备作为 FTP 服务器组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下的思路配置通过 FTP 进行文件操作：

1. 配置设备的 FTP 功能及 FTP 用户信息（包括源地址、用户名及密码、用户级别、服务类型、授权目录）。
2. 配置 FTP 服务器访问权限。
3. 保存设备当前配置文件。
4. 从终端 PC1 通过 FTP 连接设备。
5. 将系统软件上传至设备以及配置文件备份至 PC1。

配置注意事项

当网络所处环境不足够安全时，我们建议选择安全的密码认证方式/加密认证算法/协议。安全的举例请参见：[配置设备作为 SFTP 服务器](#)。

操作步骤

1. 在用户视图下执行命令 **install feature-software WEAKEA** 安装弱安全算法/协议特性包（WEAKEA）。
2. 配置 FTP 服务器的 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname FTP_Server
[FTP_Server] interface 10ge 1/0/1
[SSH Server-10GE1/0/1] undo portswitch
[FTP_Server-10GE1/0/1] ip address 10.136.23.5 255.255.255.0
[FTP_Server-10GE1/0/1] quit
```

3. 配置设备的 FTP 功能及 FTP 用户信息。

```
[FTP_Server] ftp server enable
[FTP_Server] ftp server source all-interface
[FTP_Server] aaa
[FTP_Server-aaa] local-user admin1234 password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters,
uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
[FTP_Server-aaa] local-user admin1234 privilege level 3
[FTP_Server-aaa] local-user admin1234 service-type ftp
```

```
[FTP_Server-aaa] local-user admin1234 ftp-directory flash:/
[FTP_Server-aaa] quit
```

4. 配置 FTP 服务器访问权限。

```
[FTP_Server] acl number 2001
[FTP_Server-acl4-basic-2001] rule permit source 10.136.23.10 0
[FTP_Server-acl4-basic-2001] rule deny source 10.136.23.20 0
[FTP_Server-acl4-basic-2001] quit
[FTP_Server] ftp server acl 2001
[FTP_Server] quit
```

5. 保存设备当前配置文件。

```
<FTP_Server> save
```

6. 从终端 PC1 通过 FTP 连接设备，输入用户名 **admin1234** 和密码 **YsHsjx_202206**，并采用 binary 模式进行文件传输。

终端以 Windows 操作系统为例说明。

```
C:\Documents and Settings\Administrator> ftp 10.136.23.5
连接到 10.136.23.5。
220 FTP service ready.
用户 (10.136.23.5:(none)): admin1234
331 Password required for admin1234.
密码:
230 User logged in.
ftp> binary
200 Type set to I.
ftp>
```

7. 将系统软件上传至设备以及配置文件备份至终端。

上传系统软件至设备。

```
ftp> put devicesoft.cc
200 Port command okay.
150 Opening BINARY mode data connection for /devicesoft.cc
226 Transfer complete.
ftp: 发送 107973953 字节，用时 151.05Seconds 560.79Kbytes/sec.
```

备份配置文件。

```
ftp> get vrpcfg.zip
200 Port command okay.
150 Opening BINARY mode data connection for /vrpcfg.zip.
226 Transfer complete.
ftp: 收到 1257 字节，用时 0.03Seconds 40.55Kbytes/sec.
```



说明

用户在进行上传和下载操作时，需要明确客户端 FTP 的工作路径，例如 Windows 操作系统默认的 FTP 路径是 C:\Windows\System32。待上传的系统软件需要预先保存至此路径下，以及备份的配置文件也将保存在此路径下。

检查配置结果

在设备中执行 **dir** 命令，查看系统软件是否上传至设备。

```
<FTP_Server> dir
Directory of flash:/

Idx Attr   Size(Byte) Date      Time      FileName
 0 -rw-      14 Mar 13 2019 14:13:38 back_time_a
 1 drw-      - Mar 11 2019 00:58:54 logfile
 2 -rw-       4 Nov 17 2019 09:33:58 snmpnotilog.txt
 3 -rw-    11,238 Mar 12 2019 21:15:56 private-data.txt
 4 -rw-    1,257 Mar 12 2019 21:15:54 vrpcfg.zip
 5 -rw-      14 Mar 13 2019 14:13:38 back_time_b
 6 -rw- 107,973,953 Mar 13 2019 14:24:24 devicesoft.cc
 7 drw-      - Oct 31 2019 10:20:28 sysdrv
 8 drw-      - Feb 21 2019 17:16:36 compatible
 9 drw-      - Feb 09 2019 14:20:10 selftest
10 -rw-    19,174 Feb 20 2019 18:55:32 backup.cfg
11 -rw-    23,496 Oct 15 2019 20:59:36 20191015.zip
12 -rw-     588 Nov 04 2019 13:54:04 servercert.der
13 -rw-     320 Nov 04 2019 13:54:26 serverkey.der
14 drw-      - Nov 04 2019 13:58:36 security
...
670,092 KB total (569,904 KB free)
```

在终端 FTP 用户的工作路径下，可以看到 **vrpcfg.zip** 文件已保存至此路径。

配置脚本

```
#
sysname FTP_Server
#
ftp server enable
ftp serversource all-interface
ftp server acl 2001
#
acl number 2001
rule 5 permit source 10.136.23.10 0
rule 10 deny source 10.136.23.20 0
```

```
#
aaa
 local-user admin1234 password irreversible-cipher
 $1d$g8wLJ`LjL!$CyE(V{3qg5DdU:PM[6=6O$UF-.fQ,Q}>^)OBzgoU$
 local-user admin1234 privilege level 3
 local-user admin1234 ftp-directory flash:
 local-user admin1234 service-type ftp
#
interface 10GE1/0/1
 undo portswitch
 ip address 10.136.23.5 255.255.255.0
#
return
```

1.1.5.2.4.3 举例：配置设备作为 SFTP 服务器

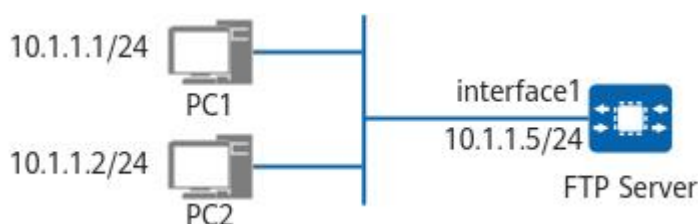
组网需求

如图 [配置通过 SFTP 进行文件操作组网图](#) 所示，终端 PC1 与设备连接，10.1.1.5 是设备的 IP 地址。用户希望在终端与设备之间进行安全的文件传输操作。将设备配置为 SSH 服务器，提供 SFTP 服务，服务器通过对客户端的认证和双向的数据加密，实现用户对安全文件传输操作的要求。配置 ACL 策略，保证只有 PC1 才能访问 SSH 服务器。

图 1 配置通过 SFTP 进行文件操作组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下的思路配置用户通过 SFTP 进行文件操作：

1. 在 SSH 服务器端生成本地密钥对及使能 SFTP 服务器功能，实现在服务器端和客户端进行安全地数据交互。
2. 配置 SSH 用户，包括认证方式、服务类型、授权目录以及用户名和密码等。
3. 配置 SSH 服务器的访问权限，实现对 SSH 用户的限制。
4. 从终端通过第三方软件 OpenSSH 实现访问 SSH 服务器。

操作步骤

1. 配置 SSH 服务器的 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname FTP_Server
[SSH Server] interface 10ge 1/0/1
[SSH Server-10GE1/0/1] undo portswitch
[SSH Server-10GE1/0/1] ip address 10.1.1.5 255.255.255.0
[SSH Server-10GE1/0/1] quit
```

2. 在服务器端生成本地密钥对，并使能 SFTP 服务器功能。

```
[SSH Server] rsa local-key-pair create
The key name will be:Host_Server
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
[SSH Server] sftp server enable
[SSH Server] ssh server-source all-interface
```

3. 配置 SSH 服务器的公钥算法、加密算法、密钥交换算法列表、HMAC 认证算法和最小密钥长度。

```
[SSH Server] ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
[SSH Server] ssh server hmac sha2_256 sha2_512
[SSH Server] ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
[SSH Server] ssh server publickey rsa_sha2_256 rsa_sha2_512
[SSH Server] ssh server dh-exchange min-len 3072
```

4. 配置 SSH 用户，包括认证方式、服务类型、授权目录以及用户名和密码等。

```
[SSH Server] ssh user client001 authentication-type password
Info: Succeeded in adding a new SSH user.
[SSH Server] ssh user client001 service-type sftp
[SSH Server] ssh user client001 sftp-directory flash:/
[SSH Server] aaa
[SSH Server-aaa] local-user client001 password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters,
uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
[SSH Server-aaa] local-user client001 privilege level 3

[SSH Server-aaa] local-user client001 privilege level 3
[SSH Server-aaa] local-user client001 service-type ssh
```

```
[SSH Server-aaa] quit
```

5. 配置 SSH 服务器的访问权限。

```
[SSH Server] acl 2001
[SSH Server-acl4-basic-2001] rule permit source 10.1.1.1 0
[SSH Server-acl4-basic-2001] rule deny source 10.1.1.2 0
[SSH Server-acl4-basic-2001] quit
[SSH Server] ssh server acl 2001
```

检查配置结果

从终端通过 OpenSSH 软件实现访问 SSH 服务器。

只有在用户终端安装了 OpenSSH 软件后，Windows 命令行提示符才能识别 OpenSSH 相关命令。

```
C:/Documents and Settings/Administrator> sftp client001@10.1.1.5
Connecting to 10.1.1.5...
The authenticity of host "10.1.1.5 (10.1.1.5)" can't be established.
DSA key fingerprint is 0d:48:82:fd:2f:52:1c:f0:c4:22:70:80:8f:7b:fd:78.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added "10.1.1.5" (DSA) to the list of known hosts.
client001@10.1.1.5's password:
sftp>
```

通过第三方软件连接设备后，进入 SFTP 视图，此时可以执行一系列文件操作。

配置脚本

```
#
sysname SSH Server
#
acl number 2001
rule 5 permit source 10.1.1.1 0
rule 10 deny source 10.1.1.2 0
#
aaa
local-user client001 password irreversible-cipher $1d$v!=.5/:(q-
$xL=\K+if"S}>k7vGP5$_ox0B@ys7.'DBHL~3*aN$
local-user client001 service-type terminal ssh
local-user client001 privilege level 3
#
interface 10GE1/0/1
undo portswitch
ip address 10.1.1.5 255.255.255.0
#
```

```
sftp server enable
ssh server-source all-interface
ssh server acl 2001
ssh user client001
ssh user client001 authentication-type password
ssh user client001 service-type sftp
ssh user client001 sftp-directory flash:
#
ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh server hmac sha2_256 sha2_512
ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh server publickey rsa_sha2_256 rsa_sha2_512
ssh server dh-exchange min-len 3072
#
return
```

1.1.5.2.4.4 举例：配置设备作为 TFTP 客户端

组网需求

如图 1 所示，远端服务器提供 TFTP Server 功能，IP 地址为 10.1.1.1/24。设备作为 TFTP 客户端，IP 地址为 10.2.1.1/24，与服务器之间的路由可达。

设备需要进行升级操作，要求：从 TFTP 服务器上下载系统软件至设备，且备份当前设备的配置文件到 TFTP 服务器。

图 1 配置通过 TFTP 访问其他设备文件组网图

说明

使用 TFTP 协议存在安全风险，建议使用 SFTP V2 或 SCP 方式进行文件操作。

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下的思路配置 TFTP 传输文件功能：

1. 在 TFTP 服务器端运行 TFTP 软件，并设置 TFTP 的工作路径。
2. 在设备上使用 TFTP 命令下载和上传文件。

配置注意事项

当网络所处环境不足够安全时，我们建议选择安全的密码认证方式/加密认证算法/协议。安全的举例请参见：[举例：配置设备作为 SCP 客户端](#)。

操作步骤

1. 在用户视图下执行命令 `install feature-software WEAKEA` 安装弱安全算法/协议特性包（WEAKEA）。
2. 在 TFTP 服务器端运行 TFTP 软件，并设置 TFTP 的工作路径。（具体操作见第三方软件帮助文档）
3. 在设备上使用 TFTP 命令下载和上传文件。

```
<HUAWEI> tftp 10.1.1.1 get devicesoft.cc
Info: Transfer file in binary mode.
Please wait for a while...
/ 107973953 bytes transferred
Info: Downloaded the file successfully.
<HUAWEI> tftp 10.1.1.1 put vrpcfg.zip
Info: Transfer file in binary mode.
Please wait for a while...
/ 100% [*****]
Info: Uploaded the file successfully.
```

检查配置结果

在设备中执行 `dir` 命令，查看系统软件是否下载至设备。

```
<HUAWEI> dir
Directory of flash:/

Idx Attr  Size(Byte) Date      Time      FileName
0 -rw-    14 Mar 13 2019 14:13:38 back_time_a
1 drw-    - Mar 11 2019 00:58:54 logfile
2 -rw-     4 Nov 17 2019 09:33:58 snmpnotilog.txt
3 -rw-   11,238 Mar 12 2019 21:15:56 private-data.txt
4 -rw-    1,257 Mar 12 2019 21:15:54 vrpcfg.zip
5 -rw-     14 Mar 13 2019 14:13:38 back_time_b
6 -rw- 107,973,953 Mar 13 2019 14:24:24 devicesoft.cc
7 drw-    - Oct 31 2019 10:20:28 sysdrv
8 drw-    - Feb 21 2019 17:16:36 compatible
9 drw-    - Feb 09 2019 14:20:10 selftest
10 -rw-   19,174 Feb 20 2019 18:55:32 backup.cfg
11 -rw-   23,496 Oct 15 2019 20:59:36 20191015.zip
```

```

12 -rw-      588 Nov 04 2019 13:54:04  servercert.der
13 -rw-      320 Nov 04 2019 13:54:26  serverkey.der
14 drw-      - Nov 04 2019 13:58:36  security
...
670,092 KB total (569,904 KB free)

```

在 TFTP 服务器的工作路径下，可以看到 `vrpcfg.zip` 文件已保存至此路径。

配置脚本

无

1.1.5.2.4.5 举例：配置设备作为 FTP 客户端

组网需求

如图 1 所示，远端服务器提供 FTP Server 功能，IP 地址为 10.1.1.1/24。设备作为 FTP 客户端，IP 地址为 10.2.1.1/24，与服务器之间的路由可达。

设备需要进行升级操作，要求：从 FTP 服务器上下载系统软件至设备，且备份当前设备的配置文件到 FTP 服务器。

图 1 配置通过 FTP 访问其他设备文件组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下的思路配置 FTP 访问其他设备文件功能：

1. 在 FTP 服务器端运行 FTP 软件，并设置 FTP 用户的相关信息。
2. 通过 FTP 与 FTP 服务器建立连接。
3. 在设备上使用 FTP 命令下载和上传文件。

配置注意事项

当网络所处环境不够安全时，我们建议选择安全的密码认证方式/加密认证算法/协议。安全的举例请参见：[配置设备作为 SFTP 客户端](#)。

操作步骤

1. 在用户视图下执行命令 **install feature-software WEAKEA** 安装弱安全算法/协议特性包（WEAKEA）。
2. 在 FTP 服务器端运行 FTP 软件，并设置 FTP 用户的相关信息。（具体操作见第三方软件帮助文档）
3. 通过 FTP 与 FTP 服务器建立连接。

```
<HUAWEI> ftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL + K to abort
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.1:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.
[ftp]
```

4. 在设备上使用 FTP 命令下载和上传文件。

```
[ftp] binary
200 Type is Image (Binary)
[ftp] get devicesoft.cc
500 Unidentified command SIZE test123.cfg
200 PORT command okay
150 "D:\FTP\test123.cfg" file ready to send (3544 bytes) in IMAGE / Binary mode
..
226 Transfer finished successfully.
FTP: 107973953 byte(s) received in 151.05 second(s) 560.79Kbyte(s)/sec.
[ftp] put vrpcfg.zip
200 PORT command okay
150 "D:\FTP\vrpcfg.zip" file ready to receive in IMAGE / Binary mode
/ 100% [*****]
226 Transfer finished successfully.
FTP: 1257 byte(s) send in 0.03 second(s) 40.55Kbyte(s)/sec.
[ftp] quit
```

检查配置结果

- # 在设备中执行 **dir** 命令，查看系统软件是否下载至设备。

```
<HUAWEI> dir
Directory of flash:/

Idx Attr  Size(Byte) Date      Time      FileName
```

```

0 -rw-      14 Mar 13 2019 14:13:38  back_time_a
1 drw-      - Mar 11 2019 00:58:54  logfile
2 -rw-      4 Nov 17 2019 09:33:58  snmpnotilog.txt
3 -rw-     11,238 Mar 12 2019 21:15:56  private-data.txt
4 -rw-     1,257 Mar 12 2019 21:15:54  vrpcfg.zip
5 -rw-      14 Mar 13 2019 14:13:38  back_time_b
6 -rw-   107,973,953 Mar 13 2019 14:24:24  devicesoft.cc
7 drw-      - Oct 31 2019 10:20:28  sysdrv
8 drw-      - Feb 21 2019 17:16:36  compatible
9 drw-      - Feb 09 2019 14:20:10  selftest
10 -rw-     19,174 Feb 20 2019 18:55:32  backup.cfg
11 -rw-    23,496 Oct 15 2019 20:59:36  20191015.zip
12 -rw-      588 Nov 04 2019 13:54:04  servercert.der
13 -rw-      320 Nov 04 2019 13:54:26  serverkey.der
14 drw-      - Nov 04 2019 13:58:36  security

```

...

670,092 KB total (569,904 KB free)

在 FTP 服务器的工作路径下，可以看到 **vrpcfg.zip** 文件已保存至此路径。

配置脚本

无

1.1.5.2.4.6 举例：配置设备作为 SFTP 客户端

组网需求

SSH 提供了在一个传统不安全的网络环境中，服务器通过对客户端的认证及双向的数据加密，为网络终端访问提供了安全的服务。通过 SFTP 方式，客户端可以安全地连接到 SSH 服务器，进行文件的安全传输。

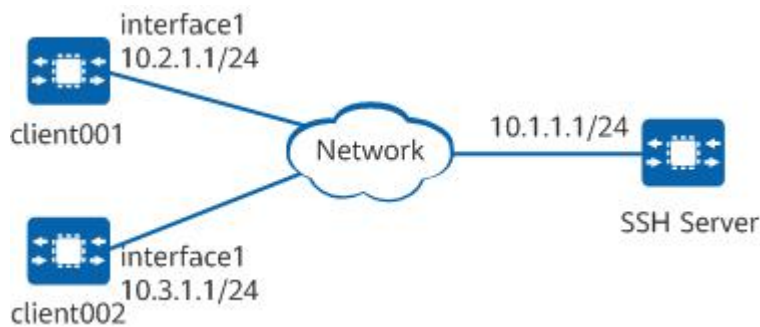
如[图 1](#)所示，SSH 服务器与客户端 client001、client002 路由可达，此例中用华为设备作为 SSH 服务器。

要求：两个客户端分别使用 password 方式和 RSA 方式与 SSH 服务器连接，实现安全访问服务器上的文件。

图 1 通过 SFTP 访问其他设备文件组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下思路配置通过 SFTP 访问其他设备文件功能：

1. 在服务器端生成本地密钥对及使能 SFTP 服务器功能，实现在服务器端和客户端进行安全地数据交互。
2. 在 SSH 服务器上配置用户 client001 和 client002，分别使用 password 和 RSA 的认证方式登录 SSH 服务器。
3. 在客户端 client002 生成本地密钥对，并将客户端生成的 RSA 公钥配置到 SSH 服务器上，实现客户端登录服务器端时，对客户端进行验证。
4. 用户 client001 和 client002 分别以 SFTP 方式登录 SSH 服务器，实现访问服务器上的文件。

操作步骤

1. 在服务器端生成本地密钥对及使能 SFTP 服务器功能。

```

<HUAWEI> system-view
[HUAWEI] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be:Host_Server
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
[SSH Server] sftp server enable
[SSH Server] ssh server-source all-interface
  
```

2. 配置 SSH 服务器的公钥算法、加密算法、密钥交换算法列表、HMAC 认证算法和最小密钥长度。

```

[SSH Server] ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
[SSH Server] ssh server hmac sha2_256 sha2_512
[SSH Server] ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
[SSH Server] ssh server publickey rsa_sha2_256 rsa_sha2_512
[SSH Server] ssh server dh-exchange min-len 3072
  
```

3. 在服务器端创建 SSH 用户。

新建用户名为 client001 的 SSH 用户，且认证方式为 password。

```

[SSH Server] ssh user client001
  
```



```
[SSH Server] ssh user client001 authentication-type password
```

```
[SSH Server] ssh user client001 service-type sftp
```

```
[SSH Server] ssh user client001 sftp-directory flash:/
```

```
[SSH Server] aaa
```

```
[SSH Server-aaa] local-user client001 password
```

Please configure the login password (8–128)

It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.

It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numerals and special characters.

Please enter password:

Please confirm password:

Info: Add a new user.

```
[SSH Server-aaa] local-user client001 service-type ssh
```

```
[SSH Server-aaa] local-user client001 privilege level 3
```

```
[SSH Server-aaa] quit
```

新建用户名为 client002 的 SSH 用户，且认证方式为 RSA。

```
[SSH Server] ssh user client002
```

```
[SSH Server] ssh user client002 authentication-type rsa
```

```
[SSH Server] ssh authorization-type default root
```

```
[SSH Server] ssh user client002 service-type sftp
```

```
[SSH Server] ssh user client002 sftp-directory flash:/
```

4. 在客户端 client001，配置加密算法、HMAC 认证算法、密钥交换算法列表、公钥算法。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname client001
```

```
[client001] ssh client cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
```

```
[client001] ssh client hmac sha2_256 sha2_512
```

```
[client001] ssh client key-exchange dh_group_exchange_sha256 dh_group16_sha512
```

```
[client001] ssh client publickey rsa_sha2_256 rsa_sha2_512
```

5. 在客户端 client002 生成本地密钥对，并将客户端生成的 RSA 公钥配置到 SSH 服务器上。

客户端生成客户端的本地密钥对。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname client002
```

```
[client002] rsa local-key-pair create
```

The key name will be: Host_Server

The range of public key size is (2048, 4096).

NOTE: Key pair generation will take a short while.

Please input the modulus [default = 3072]:3072

配置客户端 client002 的加密算法、HMAC 认证算法、密钥交换算法列表、公钥算法。

```
[client002] ssh client cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
```

```
[client002] ssh client hmac sha2_256 sha2_512
[client002] ssh client key-exchange dh_group_exchange_sha256 dh_group16_sha512
[client002] ssh client publickey rsa_sha2_256 rsa_sha2_512
```

查看客户端上生成 RSA 公钥。

```
[client002] display rsa local-key-pair public
=====
Time of key pair created : 2019-11-05 12:10:40
Key name                : Host_RSA
Key modulus              : 3072
Key type                 : RSA encryption key
=====
Key code:
3082010A
02820101
00BBB7A0 4924AF13 04F2662D 2ED43B9D 589967EB
D8A4F785 5AD1F662 13845081 0C65F6B3 88A9C415
D81C34BD 41A4B580 70DC7460 E4A5407B 9B95630F
E211F4B3 1115772D FB95D3DC 915A1858 D0DE49F7
F39DD7A7 7795F2B9 C9562E8B 598CB50F 6D39240D
B5C6F1D3 33A218D0 98C30104 F8F3A8CA 7172C95B
03AEC0A0 8A7E99F6 6C1939AA 52CC2E31 B6703278
AEE1BCD8 DC21FCA2 041C9A4C 1856A935 6894998D
FBFA88FF 1708C3A6 7E092368 ACE983D7 C8DDCDF5
26F5D4E5 16A15C5C D6D0018E 4EAFE055 B93FCB87
2BB46EFB 02C04C3B F167A417 380CD0B0 0BC59493
646CBE96 BCAF3DB7 AD0AFA0A 5D14155E D7F97DC1
32693DE5 4B103442 8E0F4DAD 2598BE5E 19
0203
010001
```

Host public key for PEM format code:

```
----- BEGIN SSH2 PUBLIC KEY -----
AAAAB3NzaC1yc2EAAAADAQABAAQAC7t6BJJK8TBPJmLS7UO51YmWfr2KT3hVrR
9mIThFCBDGX2s4ipxBXYHDS9QaS1gHDcdGDkpUB7m5VjD+IR9LMRFXct+5XT3JFa
GFjQ3kn3853Xp3eV8rnJVi6LWYy1D205JA21xvHTM6IY0JjDAQT486jKcXLJWwOu
wKCKfnp2bBk5qILMLjG2cDJ4ruG82Nwh/KIEHJpMGFapNWiUmY37+oj/FwjDpn4J
I2is6YPXyN3N9Sb11OUWoVxc1tABjk6v4FW5P8uHK7Ru+wLATDvxZ6QXOAzQsAvF
IJNkbL6WvK89t60K+gpdFBVe1/I9wTJpPeVLEDRCjg9NrSWYvi4Z
----- END SSH2 PUBLIC KEY -----
```

Public key code for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQAC7t6BJJK8TBPJmLS7UO51YmWfr2KT3hVrR9mIThFCB
DGX2s4ipxBXYHDS9QaS1gHDcdGDkpUB7m5VjD+IR9LMRFXct+5XT3JFaGFjQ3kn3853Xp3eV8rnJVi6
L
WYy1D205JA21xvHTM6IY0JjDAQT486jKcXLJWwOuwKCKfnp2bBk5qlLMLjG2cDJ4ruG82Nwh/KIEHJp
M
GFapNWiUmY37+oj/FwjDpn4Jl2is6YPXyN3N9Sb11OUWoVxc1tABjk6v4FW5P8uHK7Ru+wLATDvxZ6Q
X
OAzQsAvFIJNkbL6WvK89t60K+gpdFBVe1/l9wTJpPeVLEDRCjg9NrSWYvI4Z== rsa-key
```

将客户端上产生的 RSA 公钥配置到服务器端(上面 **display** 命令显示信息中黑体部分即为客户端产生的 RSA 公钥，将其拷贝粘贴至服务器端)。

```
[SSH Server] rsa peer-public-key rsakey001 encoding-type der
[SSH Server-rsa-public-key] public-key-code begin
[SSH Server-rsa-public-key-rsa-key-code] 3082010A
[SSH Server-rsa-public-key-rsa-key-code] 02820101
[SSH Server-rsa-public-key-rsa-key-code] 00BBB7A0 4924AF13 04F2662D 2ED43B9D 589967EB
[SSH Server-rsa-public-key-rsa-key-code] D8A4F785 5AD1F662 13845081 0C65F6B3 88A9C415
[SSH Server-rsa-public-key-rsa-key-code] D81C34BD 41A4B580 70DC7460 E4A5407B 9B95630F
[SSH Server-rsa-public-key-rsa-key-code] E211F4B3 1115772D FB95D3DC 915A1858 D0DE49F7
[SSH Server-rsa-public-key-rsa-key-code] F39DD7A7 7795F2B9 C9562E8B 598CB50F 6D39240D
[SSH Server-rsa-public-key-rsa-key-code] B5C6F1D3 33A218D0 98C30104 F8F3A8CA 7172C95B
[SSH Server-rsa-public-key-rsa-key-code] 03AEC0A0 8A7E99F6 6C1939AA 52CC2E31 B6703278
[SSH Server-rsa-public-key-rsa-key-code] AEE1BCD8 DC21FCA2 041C9A4C 1856A935 6894998D
[SSH Server-rsa-public-key-rsa-key-code] FBFA88FF 1708C3A6 7E092368 ACE983D7 C8DDCDF5
[SSH Server-rsa-public-key-rsa-key-code] 26F5D4E5 16A15C5C D6D0018E 4EAFE055 B93FCB87
[SSH Server-rsa-public-key-rsa-key-code] 2BB46EFB 02C04C3B F167A417 380CD0B0 0BC59493
[SSH Server-rsa-public-key-rsa-key-code] 646CBE96 BCAF3DB7 AD0AFA0A 5D14155E D7F97DC1
[SSH Server-rsa-public-key-rsa-key-code] 32693DE5 4B103442 8E0F4DAD 2598BE5E 19
[SSH Server-rsa-public-key-rsa-key-code] 0203
[SSH Server-rsa-public-key-v-key-code] 010001
[SSH Server-rsa-public-key-rsa-key-code] public-key-code end
[SSH Server-rsa-public-key] peer-public-key end
```

为 SSH 用户 client002 绑定 SSH 客户端的 RSA 公钥。

```
[SSH Server] ssh user client002 assign rsa-key rsakey001
```

6. SFTP 客户端连接 SSH 服务器。

第一次登录，使能 SSH 客户端首次登录功能。

使能客户端 client001 首次登录功能。

```
<HUAWEI> system-view
[HUAWEI] sysname client001
[client001] ssh client first-time enable
```

使能客户端 client002 首次登录功能。

```
[client002] ssh client first-time enable
```

SFTP 客户端 client001 用 password 认证方式连接 SSH 服务器。

```
[client001] sftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server's public key does not match the one cached before.
The server is not authenticated. Continue to access it? [Y/N]:y
The keyname:10.1.1.1 already exists. Update it? [Y/N]:n

Please input the username: client001
Enter password:
sftp-client>
```

SFTP 客户端 client002 用 RSA 认证方式连接 SSH 服务器。

```
[client002] sftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server's public key does not match the one cached before.
The server is not authenticated. Continue to access it? [Y/N]:y
The keyname:10.1.1.1 already exists. Update it? [Y/N]:n

Please input the username: client002
sftp-client>
```

检查配置结果

配置完成后，在 SSH 服务器端执行 **display ssh server status** 命令可以查看到 SFTP 服务已经使能。执行 **display ssh user-information** 命令可以查看服务器端 SSH 用户信息。

查看 SSH 状态信息。

```
[SSH Server] display ssh server status
SSH Version                : 2.0
SSH authentication timeout (Seconds) : 60
SSH authentication retries (Times)   : 3
SSH server key generating interval (Hours) : 0
SSH version 1.x compatibility      : Disable
SSH server keepalive          : Enable
SFTP IPv4 server              : Enable
SFTP IPv6 server              : Enable
STELNET IPv4 server           : Enable
```

```

STELNET IPv6 server          : Enable
SNETCONF IPv4 server        : Disable
SNETCONF IPv6 server        : Disable
SNETCONF IPv4 server port(830) : Disable
SNETCONF IPv6 server port(830) : Disable
SCP IPv4 server              : Enable
SCP IPv6 server              : Enable
SSH IPv4 server port         : 22
SSH IPv6 server port         : 22
ACL name                     : --
ACL number                   : --
ACL6 name                    : --
ACL6 number                  : --
SSH server ip-block          : Enable

```

查看 SSH 用户信息。

```
[SSH Server] display ssh user-information
```

```

-----
User Name          : client001
Authentication type : password
User public key name : --
User public key type : --
Sftp directory     : flash:
Service type       : sftp

```

```

User Name          : client002
Authentication type : rsa
User public key name : --
User public key type : --
Sftp directory     : flash:
Service type       : sftp

```

```
-----
Total 2, 2 printed
```

配置脚本

SSH 服务器上的配置脚本

```

#
sysname SSH Server
#
rsa peer-public-key rsakey001 encoding-type der
public-key-code begin
3082010A

```

```
02820101
```

```
00BBB7A0 4924AF13 04F2662D 2ED43B9D 589967EB D8A4F785 5AD1F662 13845081
0C65F6B3 88A9C415 D81C34BD 41A4B580 70DC7460 E4A5407B 9B95630F E211F4B3
1115772D FB95D3DC 915A1858 D0DE49F7 F39DD7A7 7795F2B9 C9562E8B 598CB50F
6D39240D B5C6F1D3 33A218D0 98C30104 F8F3A8CA 7172C95B 03AEC0A0 8A7E99F6
6C1939AA 52CC2E31 B6703278 AEE1BCD8 DC21FCA2 041C9A4C 1856A935 6894998D
FBFA88FF 1708C3A6 7E092368 ACE983D7 C8DDCDF5 26F5D4E5 16A15C5C D6D0018E
4EAFE055 B93FCB87 2BB46EFB 02C04C3B F167A417 380CD0B0 0BC59493 646CBE96
BCAF3DB7 AD0AFA0A 5D14155E D7F97DC1 32693DE5 4B103442 8E0F4DAD 2598BE5E
19
```

```
0203
```

```
010001
```

```
public-key-code end
```

```
peer-public-key end
```

```
#
```

```
aaa
```

```
local-user client001 password irreversible-cipher
```

```
$1d$g8wLJ`LjL!$CyE(V{3qg5DdU:PM[6=6O$UF-.fQ,Q}>^)OBzgoU$
```

```
local-user client001 service-type terminal ssh
```

```
local-user client001 privilege level 3
```

```
#
```

```
sftp server enable
```

```
ssh user client001
```

```
ssh user client001 authentication-type password
```

```
ssh user client001 service-type sftp
```

```
ssh user client001 sftp-directory flash:/
```

```
ssh user client002
```

```
ssh user client002 authentication-type rsa
```

```
ssh user client002 assign rsa-key rsakey001
```

```
ssh user client002 service-type sftp
```

```
ssh user client002 sftp-directory flash:/
```

```
#
```

```
ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
```

```
ssh server hmac sha2_256 sha2_512
```

```
ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
```

```
ssh server publickey rsa_sha2_256 rsa_sha2_512
```

```
ssh server dh-exchange min-len 3072
```

```
#
```

```
return
```

SSH 客户端 client001 的配置脚本

```
#
```

```
sysname client001
```

```
#
ssh client first-time enable
#
ssh client cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh client hmac sha2_256 sha2_512
ssh client key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh client publickey rsa_sha2_256 rsa_sha2_512
#
return
```

SSH 客户端 client002 的配置脚本

```
#
sysname client002
#
ssh client first-time enable
#
ssh client cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh client hmac sha2_256 sha2_512
ssh client key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh client publickey rsa_sha2_256 rsa_sha2_512
#
return
```

1.1.5.2.4.7 举例：配置设备作为 SCP 客户端

组网需求

与使用 SFTP 协议传输文件相比，SCP 协议可以简化用户传输文件的操作，将用户身份认证、文件传输等步骤合并，提高配置效率。

如图 1 所示，作为 SCP 客户端的设备和服务器路由可达，并从 SSH 服务器中下载文件至客户端。

图 1 配置通过 SCP 访问其他设备文件配置示例组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下的思路配置通过 SCP 访问其他设备文件：

1. 在 SSH 服务器端生成本地密钥对。
2. 在 SSH 服务器端创建 SSH 用户。
3. 在 SSH 服务器端使能 SCP 功能。
4. 从 SSH 服务器下载文件至本地。

操作步骤

1. 在服务器端生成本地密钥对。

```
<HUAWEI> system-view
[HUAWEI] sysname SSH Server
[SSH Server] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 4096).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:
```

2. 在服务器端创建 SSH 用户。

配置 VTY 用户界面。

```
[SSH Server] user-interface vty 0 4
[SSH Server-ui-vty0-4] authentication-mode aaa
[SSH Server-ui-vty0-4] protocol inbound ssh
[SSH Server-ui-vty0-4] quit
```

新建用户名为 Client 的 SSH 用户，且认证方式为 password，服务方式为 all。

```
[SSH Server] ssh user Client
[SSH Server] ssh user Client authentication-type password
[SSH Server] ssh user Client service-type all
```

为 SSH 用户 Client 配置密码。

```
[SSH Server] aaa
[SSH Server-aaa] local-user Client password
Please configure the login password (8~128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters,
uppercase letters, numerals and special characters.
Please enter password:
Please confirm password:
Info: Add a new user.
[SSH Server-aaa] local-user Client service-type ssh
[SSH Server-aaa] local-user Client privilege level 3
[SSH Server-aaa] quit
```

3. 在服务器端使能 SCP 服务。


```
[SSH Server] scp server enable
[SSH Server] ssh server-source all-interface
```

4. 在 SSH 服务器端配置公钥算法、加密算法、密钥交换算法列表、HMAC 认证算法和最小密钥长度。

```
[SSH Server] ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
[SSH Server] ssh server hmac sha2_256 sha2_512
[SSH Server] ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
[SSH Server] ssh server publickey rsa_sha2_256 rsa_sha2_512
[SSH Server] ssh server dh-exchange min-len 3072
```

5. 在客户端配置加密算法、HMAC 认证算法、密钥交换算法列表、公钥算法。

```
<HUAWEI> system-view
[HUAWEI] sysname SCP Client
[SCP Client] ssh client cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
[SCP Client] ssh client hmac sha2_256 sha2_512
[SCP Client] ssh client key-exchange dh_group_exchange_sha256 dh_group16_sha512
[SCP Client] ssh client publickey rsa_sha2_256 rsa_sha2_512
```

检查配置结果

从 SCP 客户端下载服务器上的文件。

第一次登录，使能 SSH 客户端首次登录功能。

```
<HUAWEI> system-view
[HUAWEI] sysname SCP Client
[SCP Client] ssh client first-time enable
```

使用 aes256_ctr 加密算法将文件 backup.cfg 从 IP 地址为 10.1.1.1 的远端 SSH 服务器下载至本地用户目录下。

```
[SCP Client] scp -cipher aes256_ctr Client1@10.1.1.1:backup.cfg backup.cfg
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
Continue to access it? [Y/N]:y
[Y/N]:y
The server's public key will be saved with the name 10.1.1.1. Please wait...

Enter password:
backup.cfg          100%    19174Bytes    7Kb/s
```

配置脚本

SSH 服务器上的配置脚本

```
#
sysname SSH Server
#
aaa
local-user Client password irreversible-cipher
$#z$!9S<a#>H7{7dl>%0S{AcKGC=t:zjv14LIQqHO\p.*=<x1]u;y*P`'GR3[m]$
local-user Client service-type terminal ssh
local-user Client privilege level 3
#
scp server enable
ssh user Client
ssh user Client authentication-type password
ssh user Client service-type all
ssh server-source all-interface
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
ssh server cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh server hmac sha2_256 sha2_512
ssh server key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh server publickey rsa_sha2_256 rsa_sha2_512
ssh server dh-exchange min-len 3072
#
return
```

SCP 客户端上的配置脚本

```
#
sysname SCP Client
#
ssh client first-time enable
#
ssh client cipher aes128_ctr aes256_ctr aes192_ctr aes128_gcm aes256_gcm
ssh client hmac sha2_256 sha2_512
ssh client key-exchange dh_group_exchange_sha256 dh_group16_sha512
ssh client publickey rsa_sha2_256 rsa_sha2_512
#
return
```

1.1.5.3 接口管理

以太网接口

1.1.5.3.1 以太网接口

举例：配置以太网接口速率和双工模式

举例：配置以太网接口的二三层模式切换

1.1.5.3.1.1 举例：配置以太网接口速率和双工模式

组网需求

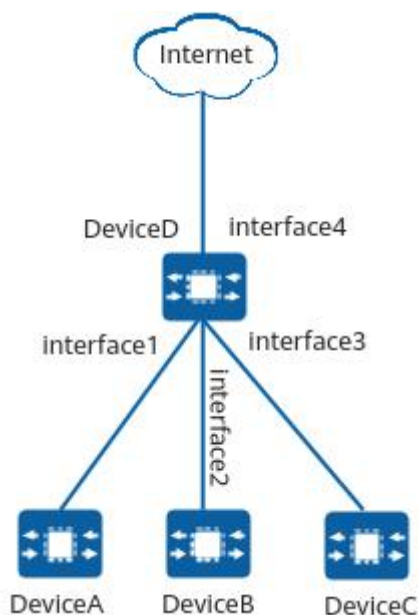
如图 1 所示，设备 DeviceA、DeviceB 和 DeviceC 分别与 DeviceD 的接口 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 相连，DeviceD 通过接口 10GE1/0/4 上行接入 Internet 网络。

由于 DeviceD 的特殊限制，接口 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 只能自协商为半双工模式，在该模式下，当业务数据流量较大时将会产生丢包现象；同时，接口 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 速率自协商为最大速率 1000Mbit/s，当 DeviceA、DeviceB 和 DeviceC 同时以 1000Mbit/s 速率对外发送数据时，就会造成出接口 10GE1/0/4 拥塞。用户希望解决数据丢包和拥塞问题。

图 1 配置非自协商模式下速率和双工模式组网图

说明

本例中 interface1、interface2、interface3 和 interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3 和 10GE1/0/4。



配置思路

配置接口工作在非自协商模式，避免影响设备接口的最终工作速率。

在非自协商模式下强制指定接口双工模式为全双工，避免发生数据丢包现象。

在非自协商模式下强制指定接口工作速率为 100Mbit/s，避免发生数据拥塞现象。

操作步骤

1. 创建端口组，并将接口 interface1、interface2 和 interface3 加入端口组。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] port-group portgroup1 //创建永久端口组 portgroup1,并进入端口组。
[DeviceD-port-group-portgroup1] group-member 10GE1/0/1 to 10GE1/0/3 //将接口 10GE1/0/1、
10GE1/0/2 和 10GE1/0/3 加入 portgroup1 中。
```

2. 批量配置接口 interface1、interface2 和 interface3 工作在非自协商模式、双工模式为全双工、工作速率为 100Mbit/s

```
[DeviceD-port-group-portgroup1] negotiation disable //批量配置接口工作在非自协商模式。
[DeviceD-port-group-portgroup1] duplex full //批量配置接口为全双工模式。
[DeviceD-port-group-portgroup1] speed 100 //批量配置接口速率为 100Mbit/s。
[DeviceD-port-group-portgroup1] quit
```

检查配置结果

在任意视图下执行命令 **display interface 10ge1/0/1**，检查接口当前工作速率及双工模式。

```
[DeviceD] display interface 10ge1/0/1
...
Port Mode:      AUTO,   Port Split/Aggregate:      -
Speed:          100,   Loopback:          NONE
Duplex:         FULL,   Negotiation:          DISABLE
Input Flow-control: DISABLE,   Output Flow-control:      DISABLE
Mdi:            -,   Fec:
...
```

由上述回显字段看出接口工作在非自协商模式，工作速率为 100Mbit/s，双工模式为全双工。

同理，对于 10GE1/0/2 和 10GE1/0/3 也可以通过执行 **display interface 10ge1/0/2** 和 **display interface 10ge1/0/3** 命令查看接口当前工作信息。

配置脚本

```
#
sysname DeviceD
#
port-group portgroup1
group-member 10GE1/0/1 to 10GE1/0/3
```

```
negotiation disable
duplex full
speed 100
#
return
```

1.1.5.3.1.2 举例：配置以太网接口的二三层模式切换

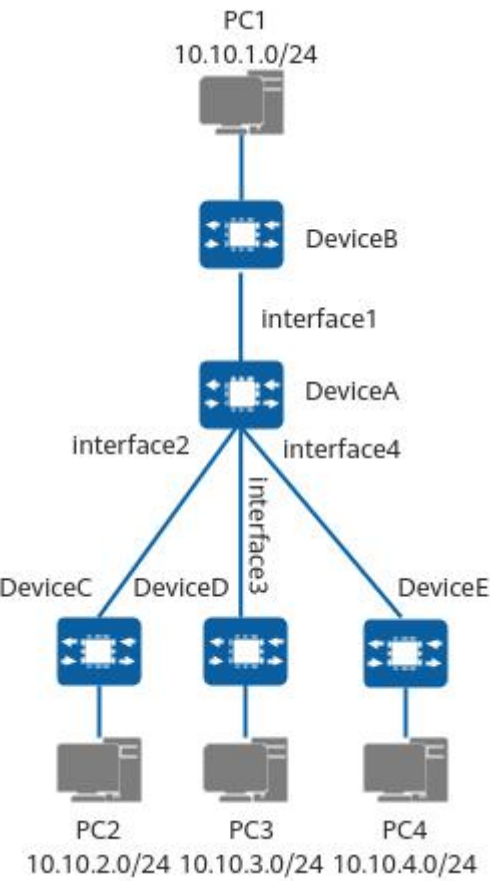
组网需求

如图 1 所示，PC1、PC2、PC3 和 PC4 分别属于不同网段，DeviceB、DeviceC、DeviceD、DeviceE 分别为这四个网段的接入层设备。用户希望使用 DeviceA 上的四个以太网物理接口作为这四个网段的网关接口。

图 1 配置二三层模式切换组网图

说明

本例中 interface1、interface2、interface3 和 interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3 和 10GE1/0/4。



配置思路

配置思路如下：

将接口的工作模式切换为三层模式。

配置三层以太网接口的 IP 地址作为网关。

操作步骤

1. 配置接口切换到三层模式

配置单个接口切换到三层模式。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] undo portswitch
[DeviceA-10GE1/0/1] quit
```

配置以太网接口批量切换到三层模式。

```
[DeviceA] undo portswitch batch 10ge 1/0/2 to 1/0/4
```

2. 配置三层接口的 IP 地址作为网关。

以配置 10GE1/0/1 接口的 IP 地址作为网关为例。10GE1/0/2、10GE1/0/3、10GE1/0/4 的配置与 10GE1/0/1 的类似，详见配置脚本。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] ip address 10.10.1.1 24
[DeviceA-10GE1/0/1] quit
```

检查配置结果

在任意视图下执行命令 **display interface 10GE 1/0/1**，检查接口当前工作速率及双工模式。

```
[DeviceA] display interface 10ge 1/0/1
...
Description:
Route Port,The Maximum Frame Length is 9216
Internet Address is 10.10.1.1/24
...
```

如果回显字段为 **Switch Port**，代表接口工作在二层模式；如果回显字段为 **Route Port**，代表接口工作在三层模式。由上述回显字段可以看出接口工作在三层模式。

配置脚本

```
#
sysname DeviceA
#
interface 10ge1/0/1
undo portswitch
ip address 10.10.1.1 255.255.255.0
```

```
#
interface 10ge1/0/2
undo portswitch
ip address 10.10.2.1 255.255.255.0
#
interface 10ge1/0/3
undo portswitch
ip address 10.10.3.1 255.255.255.0
#
interface 10ge1/0/4
undo portswitch
ip address 10.10.4.1 255.255.255.0
#
return
```

1.1.5.3.2 端口隔离

举例：配置二层端口隔离

1.1.5.3.2.1 举例：配置二层端口隔离

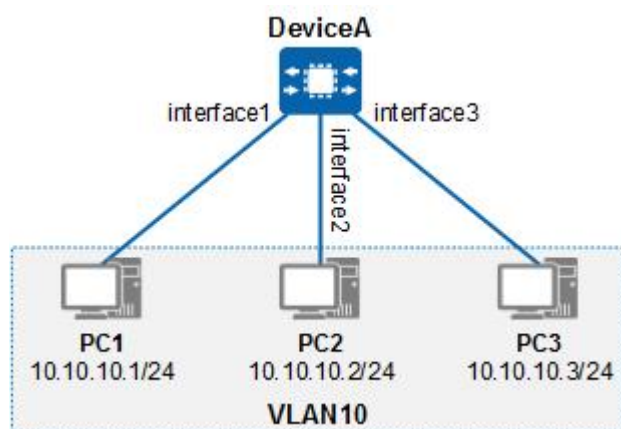
组网需求

如图 1 所示，PC1、PC2 和 PC3 同属于 VLAN10，用户希望 PC1 与 PC2 之间在 VLAN10 内不能互相访问，PC1 与 PC3 之间可以互相访问，PC2 与 PC3 之间可以互相访问。

图 1 配置二层端口隔离示例组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



配置思路

采用如下的思路配置二层端口隔离：

1. 配置接口加入 VLAN。
2. 使能端口隔离功能。

配置注意事项

根据实际接口类型自行选择是否需要执行接口切换到二层模式的步骤。

操作步骤

1. 创建 VLAN10，并将接口加入 VLAN10。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan 10
[DeviceA-vlan10] quit
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 10
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 10
[DeviceA-10GE1/0/3] quit
```

2. 配置二层端口隔离功能。

配置 10GE1/0/1 的二层端口隔离功能。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port-isolate enable group 1
[DeviceA-10GE1/0/1] quit
```

配置 10GE1/0/2 的二层端口隔离功能。

```
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] port-isolate enable group 1
[DeviceA-10GE1/0/2] quit
```


检查配置结果

PC1 和 PC2 不能互通。

PC1 和 PC3 可以互通。

PC2 和 PC3 可以互通。

配置脚本

DeviceA 的配置文件

```
#
sysname DeviceA
#
vlan batch 10
#
interface 10GE1/0/1
port default vlan 10
port-isolate enable group 1
#
interface 10GE1/0/2
port default vlan 10
port-isolate enable group 1
#
interface 10GE1/0/3
port default vlan 10
#
return
```

1.1.5.4 系统管理

[SNMP](#)

[升级维护](#)

1.1.5.4.1 SNMP

[举例：配置设备使用 SNMPv1 与网管通信](#)

[举例：配置设备使用 SNMPv2c 与网管通信](#)

[举例：配置设备使用 SNMPv3 USM 用户与网管通信](#)

1.1.5.4.1.1 举例：配置设备使用 SNMPv1 与网管通信

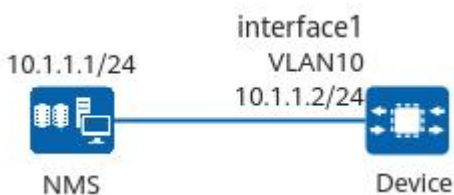
组网需求

如图 1 所示，现有网络中网管服务器对网络中的设备进行监管，由于网络规模较小，安全性较高等因素，在规划时配置设备使用 SNMPv1 版本与网管进行通信。现在新增一台设备，用户希望通过利用现有的网络资源对设备进行监管，在发生故障时能够快速对故障进行定位和排除。

图 1 配置使用 SNMPv1 与网管通信组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置注意事项

当网络所处环境不足够安全时，我们建议选择安全的 SNMPv3 协议与网管通信。

配置思路

采用如下思路配置 SNMP：

1. 配置设备的 SNMP 版本为 v1，允许版本为 v1 的网管管理设备。
2. 配置访问控制，只允许指定 IP 地址的网管读写设备指定 MIB。
3. 配置团体名，在网管上添加设备时，使用团体名进行认证。
4. 配置告警主机，并使能设备主动发送 Trap 消息的功能。
5. 在网管上添加设备，网管上使用的团体名和设备保持一致，才能正常管理设备。

操作步骤

1. 在用户视图下执行命令 `install feature-software WEAKEA` 安装弱安全算法/协议特性包（WEAKEA）。
2. 配置设备和网管站之间路由可达（略）。
3. 使能 SNMP Agent。

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] snmp-agent
```

4. 配置设备的 SNMP 版本为 v1，允许版本为 v1 的网管管理设备。

```
[Device] snmp-agent sys-info version v1 //缺省情况下仅支持 SNMPv3 版本。
```

5. 配置设备可以接收和响应网管请求报文的接口。

```
[Device] snmp-agent protocol source-interface Loopback0
```

6. 配置访问控制，只允许指定的 IP 地址的网管读写设备指定的 MIB。

配置 ACL，通过 ACL 限制仅 IP 地址为 10.1.1.1 网管能够对交换机进行访问。

```
[Device] acl 2001
[Device-acl4-basic-2001] rule permit source 10.1.1.1 0
[Device-acl4-basic-2001] rule deny
[Device-acl4-basic-2001] quit
```

配置 MIB 视图，通过 MIB 视图限制网管仅能访问指定的 MIB。

```
[Device] snmp-agent mib-view included isoview01 system //配置 MIB 视图 isoview01 能够访问 system 子树。
[Device] snmp-agent mib-view included isoview02 interfaces //配置 MIB 视图 isoview02 能够访问 interfaces 子树。
```

7. 配置团体名，在网管上添加设备时，使用团体名进行认证，并应用访问控制，使访问控制功能生效。

```
[Device] snmp-agent community read adminnms01 mib-view isoview01 acl 2001 //配置 adminnms01 对 system 子树具有只读权限。
[Device] snmp-agent community write adminnms02 mib-view isoview02 acl 2001 //配置 adminnms02 对 interfaces 子树具有读写权限。
```

8. 配置告警主机，并使能设备主动发送 Trap 消息的功能。

```
[Device] snmp-agent trap enable
Warning: All switches of SNMP trap/notification will be open. Continue? [Y/N]:y //打开设备上所有的 Trap 开关。缺省情况下仅打开了部分告警开关，可通过 display snmp-agent trap all 命令查看。
[Device] snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname adminnms01 v1
```

9. 配置网管站（NMS）。

网管的配置请根据采用的网管产品参考对应的网管配置手册。

说明

网管侧的参数配置必须和设备上保持一致，否则网管添加设备失败。

配置脚本

```
#
sysname Device
#
acl number 2001
```

```

rule 5 permit source 10.1.1.1 0
rule 10 deny
#
snmp-agent
snmp-agent local-engineid 800007DB03360102101100
snmp-agent community read
cipher %%%Pqp'RXi))y\KgEtwP9A3x2z5_FgxG1v'D/8>=G,D9<yMC^RAM_YB:F0BZIF="bHXg%IH*L"Jq'lea`S
%%mib-view isoview01 acl 2001
snmp-agent community write cipher %%%.T|&Whvyf$<Gd"I,wXi5SP_6~Nakk6<<+3H:N-
h@aJ6d,l0md%HCeAY8~>X=>xV\JKNAL=124r839v<*%%mib-view isoview02 acl 2001
snmp-agent sys-info version v1
snmp-agent target-host trap address udp-domain 10.1.1.1 params securityname
cipher %%%uq!/YZfvW4*vf[~C|.CI}UqS(vXd#wwqR~5M(rU%%%%
snmp-agent mib-view included isoview01 system
snmp-agent mib-view included isoview02 interfaces
snmp-agent trap enable
snmp-agent protocol source-interface LoopBack0
#
return

```

1.1.5.4.1.2 举例：配置设备使用 SNMPv2c 与网管通信

组网需求

如图 1 所示，在网络中，用户的两个网管和设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理设备的所有节点，网管站 NMS1 不再管理该设备。

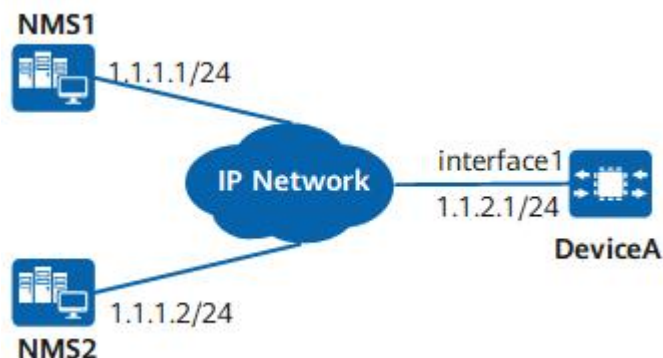
NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。由于设备发送的告警需要经过公网才能被网管接收，为了保证告警接收的可靠性，采用 Inform 方式告警。

由于网管管理员离设备较远，为了使设备出现故障时网管管理员能快速联系上设备管理员，以便对故障进行定位和排除，故要求在设备上配置设备管理员的联系方式。

图 1 配置使用 SNMPv2c 与网管通信组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置注意事项

当网络所处环境不足够安全时，我们建议选择安全的 SNMPv3 协议与网管通信。

配置思路

采用如下思路配置设备使用 SNMPv2c 与网管通信：

1. 使能 SNMP Agent。
2. 配置设备的 SNMP 版本为 SNMPv2c。
3. 配置用户访问权限，限制 NMS2 可以管理设备上的节点。
4. 配置 SNMP 接收和响应网管请求报文的源接口信息。
5. 配置设备的 Inform 告警功能，使设备产生的告警能够发送至 NMS。
6. 配置设备管理员联系方式。
7. 配置网管站（NMS2）。

操作步骤

1. 在用户视图下执行命令 **install feature-software WEAKEA** 安装弱安全算法/协议特性包（WEAKEA）。
2. 配置设备和网管站之间路由可达（略）。
3. 使能 SNMP Agent。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] snmp-agent password min-length 9
[DeviceA] snmp-agent
```

4. 配置设备的 SNMP 版本为 SNMPv2c。

```
[DeviceA] snmp-agent sys-info version v2c
```
5. 配置 SNMP 接收和响应网管请求报文的源接口信息。

```
[DeviceA] snmp-agent protocol source-interface Loopback0
```

6. 配置网管站的访问权限。

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[DeviceA] acl 2001
[DeviceA-acl4-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[DeviceA-acl4-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[DeviceA-acl4-basic-2001] quit
```

配置 MIB 视图。

```
[DeviceA] snmp-agent mib-view excluded allxthgmp 1.3.6.1.4.1.2011.6.7
```

配置团体名引用 ACL 和 MIB 视图。

```
[DeviceA] snmp-agent community write adminnms2 mib-view allxthgmp acl 2001
```

7. 配置告警功能。

```
[DeviceA] snmp-agent target-host inform address udp-domain 1.1.1.2 params securityname Huawei-1234 v2c
snmp-agent inform timeout 5 resend-times 6 pending 7
snmp-agent trap enable
snmp-agent notification-log enable
snmp-agent notification-log global-ageout 36
```

8. 配置设备管理员联系方式。

```
[DeviceA] snmp-agent sys-info contact call Operator at 010-12345678
```

9. 配置网管站（NMS2）。

网管的配置请根据采用的网管产品参考对应的网管配置手册。

检查配置结果

查看 SNMP 版本。

```
<DeviceA> display snmp-agent sys-info version
SNMP version running in the system:
    SNMPv2c SNMPv3
```

查看团体名的配置信息。

```
<DeviceA> display snmp-agent community
Community name: %@%##!!!!!!"!!!!"!!!!*!!!!PR=uJ|5'u%-
3Bw@/>NzBr/k=X0[ALT.K-:,!!!!2jp5!!!!!!U!!!!%{+ITI_[/Jh<3.<4RvQ/.Z'33]YwP
JkB^`J9g":TFqD-'B$kmL6;vyHwQ74KEfp22!!!!!!%#@%#
Group name: %@%##!!!!!!"!!!!"!!!!*!!!!PR=uJ|5'u%-
3Bw@/>NzBr/k=X0[ALT.K-:,!!!!2jp5!!!!!!U!!!!%{+ITI_[/Jh<3.<4RvQ/.Z'33]YwP
JkB^`J9g":TFqD-'B$kmL6;vyHwQ74KEfp22!!!!!!%#@%#
Acl: 2001
```

Alias name: __CommunityAliasName_01_8357

Storage-type: nonVolatile

查看 ACL 配置。

<DeviceA> **display acl 2001**

Basic ACL 2001, 2 rules

Acl's step is 5

rule 5 permit source 1.1.1.2 0 (0 times matched)

rule 6 deny source 1.1.1.1 0 (0 times matched)

查看 MIB 视图。

<DeviceA> **display snmp-agent mib-view viewname allexthgmp**

View name: allexthgmp

MIB Subtree: huaweiUtility.7

Subtree mask: FF80(Hex)

Storage-type: nonVolatile

View Type: excluded

View status: active

查看告警的目标主机。

<DeviceA> **display snmp-agent target-host**

Target-host NO. 1

Host-name : __targetHost_1_41354

IP-address : 1.1.1.2

Source interface : -

VPN instance : -

Security

name : %+%##!!!!!!"!!!!\$!!!!*!!!!%&K/U}|G\2KYm@@k}uDDU#gLLO<J"0Q'/kH!!!!2jp5!!!!<!!!!rv4VL.u
cqLA!PK/olg}.vn0tBf0m4'5^XcK!!!!%+%#

Port : 162

Type : inform

Version : v2c

Level : No authentication and privacy

NMS type : NMS

With ext vb : No

Notification filter profile name : -

Heart beat required : No

查看设备管理员联系方式。

<DeviceA> **display snmp-agent sys-info contact**

The contact person for this managed node:

call Operator at 010-12345678

配置脚本

DeviceA

```
#
sysname DeviceA
#
acl number 2001
rule 5 permit source 1.1.1.2 0
rule 6 deny source 1.1.1.1 0
#
vlan 10
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface Vlanif10
ip address 1.1.2.1 255.255.255.0
#
interface LoopBack0
ip address 10.1.1.1 255.255.255.0
#
ospf 1
area 0.0.0.0
network 1.1.2.0 0.0.0.255
#
snmp-agent
snmp-agent local-engineid 800007DB0300FDFDFD2211
snmp-agent community write cipher %@%##!!!!!!!"!!!!!!!"!!!!*!!!!PR=uJ|5'u%-
3Bw@/>NzBr/k=X0[ALT.K~:,!!!!2jp5!!!!!!U!!!!%{+ITI_[/Jh<3.<4RvQ/.Z'33]YwPJkB^`J9g":TFqD-
'B$kmL6;vyHwQ74KEFp22!!!!!!!"!!!!!!!"!!!!%@@%# mib-view allethgmp acl 2001 alias
__CommunityAliasName_01_8357
#
snmp-agent sys-info contact call Operator at 010-12345678
snmp-agent sys-info version v2c
snmp-agent password min-length 9
snmp-agent target-host host-name __targetHost_1_11752 inform address udp-domain 1.1.1.2 params
securityname
cipher %+%##!!!!!!!"!!!!!!!"!!!!*!!!!PR=uJ|5'u%<OoF8~{B=#QW("E3cky"H*I%E!!!!2jp5!!!!!!<!!!!%m9qN;K61!+'7
q>-bKZ&qJzJ3nQ\g)WWHkL!!!!!!!"!!!!%+%# v2c
#
snmp-agent mib-view excluded allethgmp huaweiUtility.7
```



```
#
snmp-agent notification-log enable
snmp-agent notification-log global-ageout 36
snmp-agent inform timeout 5
snmp-agent inform resend-times 6
snmp-agent inform pending 7
#
snmp-agent protocol source-interface LoopBack0
#
snmp-agent trap enable
#
return
```

1.1.5.4.1.3 举例：配置设备使用 SNMPv3 USM 用户与网管通信

组网需求

如图 1 所示，在网络中，用户的两个网管和设备通过公网相连，由于业务的需求，用户规划网管 NMS2 可以管理设备上的所有节点，网管站 NMS1 不再管理该设备。

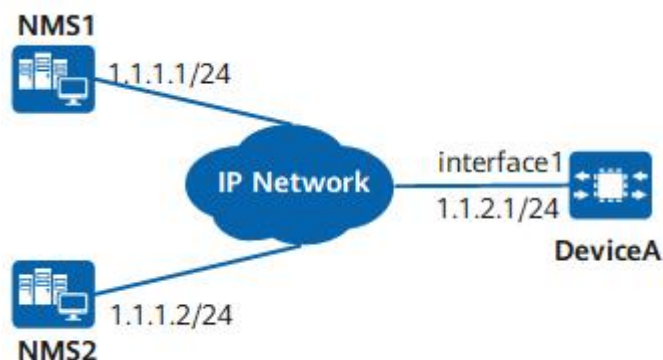
NMS2 管理设备的过程中，为了方便对告警信息进行定位，避免过多的无用告警对处理问题造成干扰，用户只允许缺省打开的模块可以发送告警至 NMS。

由于 NMS2 和设备间的数据需要穿越公网，对用户的数据进行认证和加密。由于网管管理员离设备较远，为了使设备出现故障时网管管理员能快速联系上该设备管理员，以便对故障进行快速定位和排除，故要求在设备上配置设备管理员的联系方式。

图 1 配置使用 SNMPv3 与网管通信组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下思路配置设备使用 SNMPv3 与网管通信：

1. 使能 SNMP Agent。
2. 配置设备的 SNMP 版本为 SNMPv3。
3. 配置 SNMP 接收和响应网管请求报文的源接口信息。
4. 配置用户访问权限，限制 NMS2 可以管理设备上的节点。配置对用户的数据进行认证和加密的算法分别是：sha2-256 和 aes128。
5. 配置设备的 Trap 功能，使设备产生的告警能够发送至 NMS2。
6. 配置设备管理员联系方式。
7. 配置网管站（NMS2）。

操作步骤

1. 配置设备和网管站之间路由可达（略）。
2. 使能 SNMP Agent。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] snmp-agent password min-length 10
[DeviceA] snmp-agent
```

3. 配置设备的 SNMP 版本为 SNMPv3。

```
[DeviceA] snmp-agent sys-info version v3
```

4. 配置 SNMP 接收和响应网管请求报文的源接口信息。

```
[DeviceA] snmp-agent protocol source-interface Loopback0
```

5. 配置网管站的访问权限。

配置 ACL，限制 NMS2 可以管理设备，NMS1 不允许管理设备。

```
[DeviceA] acl 2001
[DeviceA-acl4-basic-2001] rule 5 permit source 1.1.1.2 0.0.0.0
[DeviceA-acl4-basic-2001] rule 6 deny source 1.1.1.1 0.0.0.0
[DeviceA] quit
```

配置 MIB 视图。

```
[DeviceA] snmp-agent mib-view included iso iso
```

配置用户组和用户，对用户的数据进行认证和加密。

```
[DeviceA] snmp-agent group v3 admin privacy write-view iso notify-view iso read-view iso
[DeviceA] snmp-agent usm-user v3 nms2-admin group admin acl 2001
[DeviceA] snmp-agent usm-user v3 nms2-admin authentication-mode sha2-256
Please configure the authentication password (8-255)
Enter Password:
Confirm Password:
[DeviceA] snmp-agent usm-user v3 nms2-admin privacy-mode aes128
```

Please configure the privacy password (8–255)

Enter Password:

Confirm Password:

6. 配置告警功能。

```
[DeviceA] snmp-agent target-host trap address udp-domain 1.1.1.2 params securityname nms2-admin v3 privacy
```

```
[DeviceA] snmp-agent trap enable
```

7. 配置设备管理员联系方式。

```
[DeviceA] snmp-agent sys-info contact call Operator at 010-12345678
```

8. 配置网管站。

网管的配置请根据采用的网管产品参考对应的网管配置手册。

检查配置结果

查看 SNMP 版本。

```
<DeviceA> display snmp-agent sys-info version
```

SNMP version running in the system:

SNMPv3

查看用户组信息。

```
<DeviceA> display snmp-agent group admin
```

Group name: admin

Security model: USM AuthPriv

Readview: iso

Writeview: iso

Notifyview: iso

Storage-type: nonVolatile

查看用户信息。

```
<DeviceA> display snmp-agent usm-user
```

User name: nms2-admin

Engine ID: 800007DB03D0C65B951201 active

Authentication Protocol: sha2-256

Privacy Protocol: aes128

Group name: admin

Acl: 2001

State: Active

查看 ACL 配置。

```
<DeviceA> display acl 2001
```

Basic ACL 2001, 2 rules

ACL's step is 5

```
rule 5 permit ip source 1.1.1.2 0 ( 4 times matched )
rule 6 deny source 1.1.1.1 0 (0 times matched)
```

查看 MIB 视图。

```
<DeviceA> display snmp-agent mib-view viewname iso
View name: iso
  MIB Subtree: iso
  Subtree mask: 80(Hex)
  Storage-type: nonVolatile
  View Type: included
  View status: active
```

查看告警的目标主机。

```
<DeviceA> display snmp-agent target-host
Target-host NO. 1
```

```
-----
Host name           : __targetHost_1_27466
IP address          : 1.1.1.2
Source interface    : -
VPN instance        : -
Security name       : nms2-admin
Port                : 162
Type                : trap
Version             : v3
Level               : Privacy
NMS type            : NMS
With ext vb         : No
Notification filter profile name : -
Heart beat required : No
-----
```

查看设备管理员联系方式。

```
<DeviceA> display snmp-agent sys-info contact
The contact person for this managed node:
  call Operator at 010-12345678
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
acl number 2001
```

```
rule 5 permit source 1.1.1.2 0.0.0.0
rule 6 deny source 1.1.1.1 0.0.0.0
#
vlan 10
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface Vlanif10
ip address 1.1.2.1 255.255.255.0
#
interface loopback0
ip address 10.1.1.1 255.255.255.255
#
ospf 1
area 0.0.0.0
network 1.1.2.0 0.0.0.255
network 1.1.3.1 0.0.0.0
#
snmp-agent
snmp-agent local-engineid 800007DB03D0C65B951201
#
snmp-agent sys-info contact call Operator at 010-12345678
snmp-agent sys-info version v3
snmp-agent password min-length 10
snmp-agent group v3 admin privacy read-view iso write-view iso notify-view iso
snmp-agent target-host host-name __targetHost_1_27466 trap address udp-domain 1.1.1.2 params
securityname nms2-admin v3 privacy
#
snmp-agent mib-view included iso iso
snmp-agent usm-user v3 nms2-admin
snmp-agent usm-user v3 nms2-admin group admin
snmp-agent usm-user v3 nms2-admin authentication-mode sha2-256
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"PR=uJ|5'u%{Ku|VKwEyE-
uN:Pp9K`O+oLF,!!!!2jp5!!!!!!<!!!!6r!o;)ju=D<fXX.r3a`QWe'gPol7aEif^M'!!!!!!%+%#
snmp-agent usm-user v3 nms2-admin privacy-mode aes128
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"PR=uJ|5'u%B.79lwRIE3(xTzFsYNQ5iH4;X!!!!2jp5!!!!!!<!!!!A"X3:)AC815G!a6
]bVc8-wj'EK9!&V<M0HP!!!!!!%+%#
snmp-agent usm-user v3 nms2-admin acl 2001
#
snmp-agent protocol source-interface LoopBack0
#
```

```
snmp-agent trap enable
#
return
```

1.1.5.4.2 升级维护

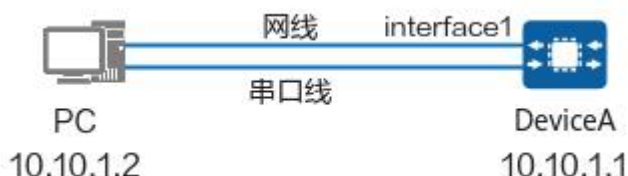
举例：新设备升级

1.1.5.4.2.1 举例：新设备升级

组网需求

通过 Console 通信电缆（串口线）和网线，将设备与 PC 直连，实现组网的搭建。Console 通信电缆与设备 Console 口相连，网线与任意以太网口相连，如[图 新设备升级组网图](#)所示。

图 1 新设备升级组网图



说明

本例中 interface1 代表 10GE1/0/1。

配置思路

1. 通过 Console 口登录设备。
2. 在 PC 端运行任一 FTP 软件，并设置 FTP 用户的相关信息。
3. 配置设备的管理 IP，使设备和 PC 直接处于同一网段。
4. 设备作为 FTP Client，从 PC 获取软件大包，并检查加载内容是否成功。
5. 设置设备下次启动使用的系统软件和补丁。
6. 重启设备。

配置注意事项

准备升级工具，即操作终端 PC、网线和串口线。

准备所需版本系统软件。

访问 [华为企业业务技术支持网站](#)，在软件下载专区选择对应的产品节点。

选择需要的软件版本。

单击软件版本对应的 *product_version.cc* 文件右侧的“下载”按钮进行下载。

准备所需版本补丁文件。

访问 [华为企业业务技术支持网站](#)，在软件下载专区选择对应的产品节点。

选择需要的软件版本。

单击软件版本对应的 *product_version.PAT* 文件右侧的“下载”按钮进行下载。

操作步骤

1. PC 通过设备 Console 口登录设备，具体操作请参见 [举例：配置用户通过 Console 口首次登录设备](#)。
2. 在用户视图下执行命令 **install feature-software WEAKEA** 安装弱安全算法/协议特性包（WEAKEA）。
3. 在 PC 端运行任一 FTP 软件。
4. 配置设备的管理 IP，使设备和 PC 之间处于同一网段，可以 ping 通。

配置设备的管理 IP。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] ip address 10.10.1.1 24
[DeviceA-10GE1/0/1] quit
```

5. 设备通过 FTP 与 PC 终端建立连接。

```
<DeviceA> ftp 10.10.1.2
Trying 10.10.1.2 ...
Press CTRL + K to abort
Connected to 10.10.1.2.
220 FTP service ready.
User(10.10.1.2:(none)):admin
331 Password required for admin.
Enter password:
230 User logged in.
[ftp]
```

6. 设备作为 FTP Client，通过 FTP 命令与 PC 实现文件传输。

```
[ftp] binary
200 Type is Image (Binary)
[ftp] get product_version.cc //加载系统软件到设备中，product_version.cc 为系统软件的文件名。
500 Unidentified command SIZE test123.cfg
200 PORT command okay
```

```

150 "D:\FTP\test123.cfg" file ready to send (3544 bytes) in IMAGE / Binary mode
..
226 Transfer finished successfully.
FTP: 107973953 byte(s) received in 151.05 second(s) 560.79Kbyte(s)/sec.
[ftp] get product_version.PAT //加载补丁文件到设备中，product_version.PAT 为系统补丁的文件名。
200 PORT command okay
150 "D:\FTP\vrpcfg.zip" file ready to receive in IMAGE / Binary mode
/ 100% [*****]
226 Transfer finished successfully.
FTP: 1257 byte(s) send in 0.03 second(s) 40.55Kbyte(s)/sec.
[ftp] quit

```

7. 检查加载内容是否成功。

```

<DeviceA> dir
Directory of flash:/

Idx Attr  Size(Byte) Date      Time      FileName
0 -rw-      14 Mar 13 2019 14:13:38 back_time_a
1 drw-      - Mar 11 2019 00:58:54 logfile
2 -rw-       4 Nov 17 2019 09:33:58 snmpnotilog.txt
3 -rw-    11,238 Mar 12 2019 21:15:56 private-data.txt
4 -rw-     1,257 Mar 12 2019 21:15:54 vrpcfg.zip
5 -rw-      14 Mar 13 2019 14:13:38 back_time_b
6 -rw- 107,973,953 Mar 13 2019 14:24:24 devicesoft.cc
7 drw-      - Oct 31 2019 10:20:28 sysdrv
8 drw-      - Feb 21 2019 17:16:36 compatible
9 drw-      - Feb 09 2019 14:20:10 selftest
10 -rw-    19,174 Feb 20 2019 18:55:32 backup.cfg
11 -rw-    23,496 Oct 15 2019 20:59:36 20191015.zip
12 -rw-     588 Nov 04 2019 13:54:04 servercert.der
13 -rw-     320 Nov 04 2019 13:54:26 serverkey.der
14 drw-      - Nov 04 2019 13:58:36 security
...
670,092 KB total (569,904 KB free)

```

8. 设置设备下次启动使用的系统软件和补丁。

单主控设备。

```

<DeviceA> startup system-software product_version.cc //设置下次启动的系统软件。
<DeviceA> startup patch product_version.PAT all //设置下次启动的补丁，如当前版本无对应补丁，则不需要执行此命令。

```

在堆叠场景。

```

<DeviceA> copy product_version.cc all#flash:
<DeviceA> startup system-software product_version.cc all //设置下次启动的系统软件。

```



```
<DeviceA> startup patch product_version.PAT all //设置下次启动的补丁，如当前版本无对应补丁，则不需要执行此命令。
```

9. 检查下次启动的启动项。（具体设备的实际回显请以设备实际显示为准。此处的回显信息仅为举例。）

```
<DeviceA> display startup
MainBoard:
  Configured startup system software:    flash:/basicsoft.cc
  Startup system software:               flash:/basicsoft.cc
  Next startup system software:          flash:/product_version.cc
  Startup saved-configuration file:      flash:/vrpcfg.zip
  Next startup saved-configuration file:  flash:/vrpcfg.zip
  Startup paf file:                      default
  Next startup paf file:                  default
  Startup patch package:                  NULL
  Next startup patch package:             NULL
```

10. 重启设备。

```
<DeviceA> reboot fast
```

检查配置结果

等候几分钟，设备重启完成，可再次进入系统。执行命令行 **display version**，可以看到设备当前的系统软件版本为新的版本，表明升级完成。

配置脚本

```
#
sysname DeviceA
#
interface 10GE1/0/1
 ip address 10.10.1.1 24
#
return
```

1.1.5.5 虚拟化

[堆叠](#)

1.1.5.5.1 堆叠

[举例：组建堆叠](#)

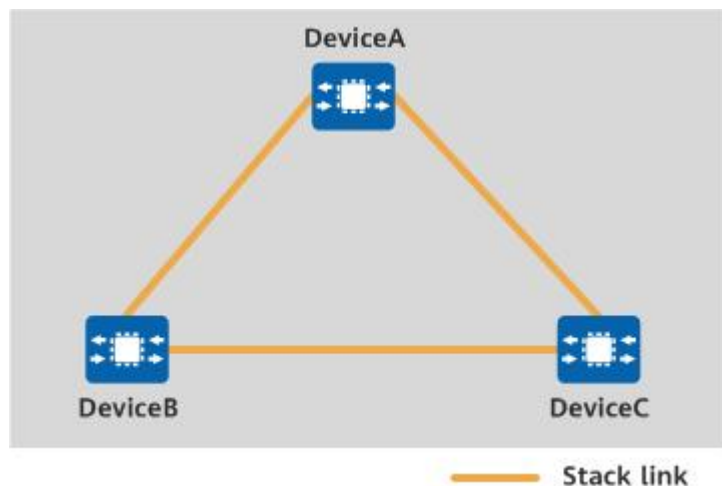
1.1.5.5.1.1 举例：组建堆叠

组网需求

在一个新建的企业网络中，要求接入设备具有充足的端口数目，并且希望网络结构简单，易于配置和管理。

如图 1 所示，DeviceA、DeviceB 和 DeviceC 三台设备组成环形堆叠系统。

图 1 组建堆叠组网图



配置思路

采用如下的思路配置：

1. 提前规划好堆叠方案。
2. 按照前期的规划，完成各台设备的堆叠配置，包括堆叠 ID、堆叠优先级、Stack-Port 端口等。完成后保存配置并将设备下电。
3. 连接设备之间的堆叠线缆并将设备上电。

说明

堆叠成员设备之间，本端设备的 Stack-Port n/1 端口必须与对端设备的 Stack-Port n/2 端口相连。

一个 Stack-Port 端口可以绑定多个物理成员端口，用来提高堆叠的可靠性和堆叠带宽；只要其中一条物理链路保持连接堆叠就不会分裂，但堆叠带宽会相应降低。

如果两端设备对应的 Stack-Port 端口内包含多个物理成员端口，对物理成员端口的连接无对应端口号的要求。

3 台或者 3 台以上成员设备组建堆叠时，为增加可靠性，建议采用环形组网，此时堆叠系统的带宽取所有 Stack-Port 端口带宽的最小值。

2 台成员设备组建堆叠时，建议每台成员设备只创建一个 Stack-Port 端口，Stack-Port 端口包含多个物理成员端口。

4. 检查堆叠组建是否成功。

操作步骤

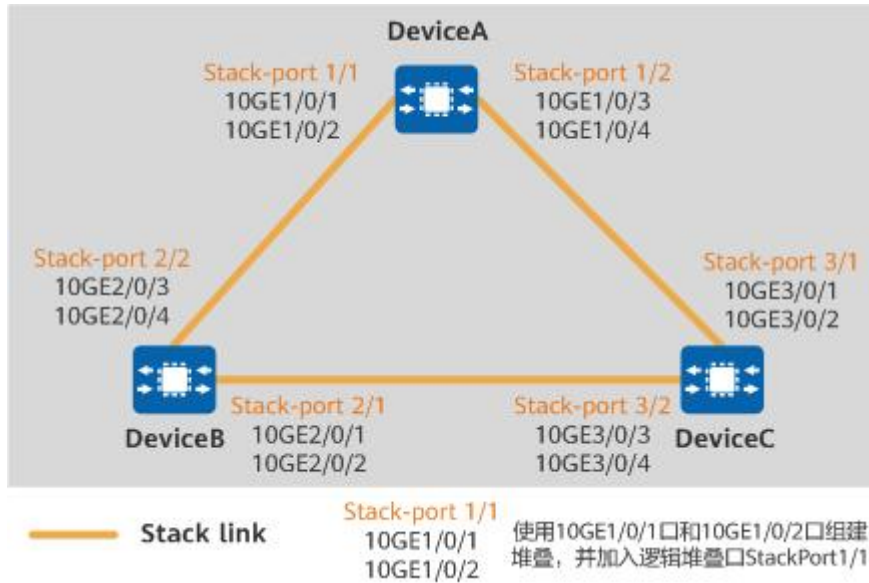
1. 提前规划堆叠方案。

规划 DeviceA 的堆叠 ID 为 1，DeviceB 的堆叠 ID 为 2，DeviceC 的堆叠 ID 为 3。

规划 DeviceA 作为主设备，其堆叠优先级最高，为 150，DeviceB 的堆叠优先级为 100，DeviceC 的堆叠优先级为 50。

规划堆叠连接拓扑为环形。成员设备间用于堆叠连接的端口如图 2 所示。

图 2 堆叠成员端口连接示意图



2. 配置堆叠参数。

配置 DeviceA 的堆叠 ID 为 1，优先级为 150。缺省情况下，设备的堆叠 ID 为 1。此处默认 DeviceA 的堆叠 ID 为 1，无需配置。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stack
[DeviceA-stack] stack member 1 priority 150
[DeviceA-stack] quit
```

配置 DeviceB 的堆叠 ID 为 2，优先级为 100。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] stack
[DeviceB-stack] stack member 1 priority 100
[DeviceB-stack] stack member 1 renumber 2
[DeviceB-stack] quit
```

#配置 DeviceC 的堆叠 ID 为 3，优先级为 50。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] stack
```

```
[DeviceC-stack] stack member 1 priority 50
[DeviceC-stack] stack member 1 renumber 3
[DeviceC-stack] quit
```

3. 配置 Stack-Port 端口。

建议在配置 Stack-Port 端口前，手动备份当前配置文件。

在 DeviceA 上创建 Stack-Port 端口，将成员端口加入 Stack-Port 端口。

```
[DeviceA] interface Stack-Port 1/1
[DeviceA-Stack-Port1/1] port member-group interface 10GE 1/0/1 10GE 1/0/2
[DeviceA-Stack-Port1/1] quit
[DeviceA] interface Stack-Port 1/2
[DeviceA-Stack-Port1/2] port member-group interface 10GE 1/0/3 10GE 1/0/4
[DeviceA-Stack-Port1/2] quit
```

在 DeviceB 上创建 Stack-Port 端口，将成员端口加入 Stack-Port 端口。

```
[DeviceB] interface Stack-Port 1/1
[DeviceB-Stack-Port1/1] port member-group interface 10GE 1/0/1 10GE 1/0/2
[DeviceB-Stack-Port1/1] quit
[DeviceB] interface Stack-Port 1/2
[DeviceB-Stack-Port1/2] port member-group interface 10GE 1/0/3 10GE 1/0/4
[DeviceB-Stack-Port1/2] quit
```

在 DeviceC 上创建 Stack-Port 端口，将成员端口加入 Stack-Port 端口。

```
[DeviceC] interface Stack-Port 1/1
[DeviceC-Stack-Port1/1] port member-group interface 10GE 1/0/1 10GE 1/0/2
[DeviceC-Stack-Port1/1] quit
[DeviceC] interface Stack-Port 1/2
[DeviceC-Stack-Port1/2] port member-group interface 10GE 1/0/3 10GE 1/0/4
[DeviceC-Stack-Port1/2] quit
```

4. 检查堆叠配置信息。

上述配置完成后，执行命令 **display stack configuration** 查看配置是否与规划的一致，如果不一致，需要修改配置。以查看 DeviceA 为例。

```
[DeviceA] display stack configuration
```

Oper : Operation

Conf : Configuration

* : Offline configuration

: Media mismatch or absence

^ : Unsaved configuration

Attribute Configuration:

```
-----
MemberID   Domain      Priority   DelayTime
Oper(Conf) Oper(Conf)  Oper(Conf) Oper(Conf)
```

```

-----
1(1)      --(10)      100(150)  0(0)
-----

```

Stack-Port Configuration:

```

-----
-
Stack-Port      Member Ports
-----
-
Stack-Port1/1   10GE1/0/1      10GE1/0/2
Stack-Port1/2   10GE1/0/3      10GE1/0/4
-----
-

```

Stack-Global Configuration:

```

-----
-
AuthMode      Password
-----
-
-
-----
-

```

5. 保存配置。

如果需要保存设备上的配置，请执行该步骤，以 DeviceA 为例。

```
[DeviceA] quit
```

```
<DeviceA> save
```

```
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
```

说明

如果设备需要使用 ZTP 空配置开局，不建议执行 **save** 命令保存配置。

6. DeviceA、DeviceB、DeviceC 下电，使用线缆连接后再上电。请按照《CLI 配置指南-虚拟化配置》中“堆叠配置”的“连接堆叠线缆并上电”进行操作。

为确保 DeviceA 成为主设备，可以先为 DeviceA 上电，DeviceA 启动后，再为 DeviceB 上电。

7. 检查堆叠是否组建成功。

通过 Console 口或管理网口登录堆叠系统，使用命令 **display stack** 查看堆叠是否组建成功。当通过管理网口登录时，需要使用主设备的 IP 地址。

```
<HUAWEI> display stack
```

MemberID	Role	MAC	Priority	DeviceType	Description

-					
1	Master	00e0-fc12-1111	255	S6730-H24X6C-V2	
2	Standby	00e0-fc12-2222	100	S6730-H24X6C-V2	
3	Slave	00e0-fc12-3333	100	S6730-H24X6C-V2	

-					

如上所示，显示三台设备的信息，表示堆叠建立成功，且主设备是堆叠 ID 为 1 的设备，即 DeviceA。
查看堆叠的拓扑信息是否与堆叠连线一致。

<DeviceA> display stack topology					
Stack Topology Type: Ring					

Stack-Port 1		Stack-Port 2			
MemberID	Status	Neighbor	Status	Neighbor	

1	up	2	up	3	
2	up	3	up	1	
3	up	1	up	2	

Stack Link:					

Stack-Port	Port	Status	PeerPort	PeerStatus	

Stack-Port1/1	10GE1/0/1	up	10GE2/0/3	up	
Stack-Port1/1	10GE1/0/2	up	10GE2/0/4	up	
Stack-Port1/2	10GE1/0/3	up	10GE3/0/1	up	
Stack-Port1/2	10GE1/0/4	up	10GE3/0/2	up	
Stack-Port2/1	10GE2/0/1	up	10GE3/0/3	up	
Stack-Port2/1	10GE2/0/2	up	10GE3/0/4	up	
Stack-Port2/2	10GE2/0/3	up	10GE1/0/1	up	
Stack-Port2/2	10GE2/0/4	up	10GE1/0/2	up	
Stack-Port3/1	10GE3/0/1	up	10GE1/0/3	up	
Stack-Port3/1	10GE3/0/2	up	10GE1/0/4	up	
Stack-Port3/2	10GE3/0/3	up	10GE2/0/1	up	
Stack-Port3/2	10GE3/0/4	up	10GE2/0/2	up	

如上所示，拓扑信息与堆叠连线一致，表示所有堆叠链路均建立成功，无异常链路。

配置脚本

堆叠功能的相关配置均保存在设备内存中，不会写入配置文件。

```
#  
sysname DeviceA  
#
```

1.1.5.6 以太网交换

MAC

Eth-Trunk

VLAN

STP/RSTP/MSTP

VBST

1.1.5.6.1 MAC

举例：配置静态 MAC 表项

举例：配置黑洞 MAC 表项

举例：配置基于接口的 MAC 地址限制

举例：配置基于 VLAN 的 MAC 地址限制

1.1.5.6.1.1 举例：配置静态 MAC 表项

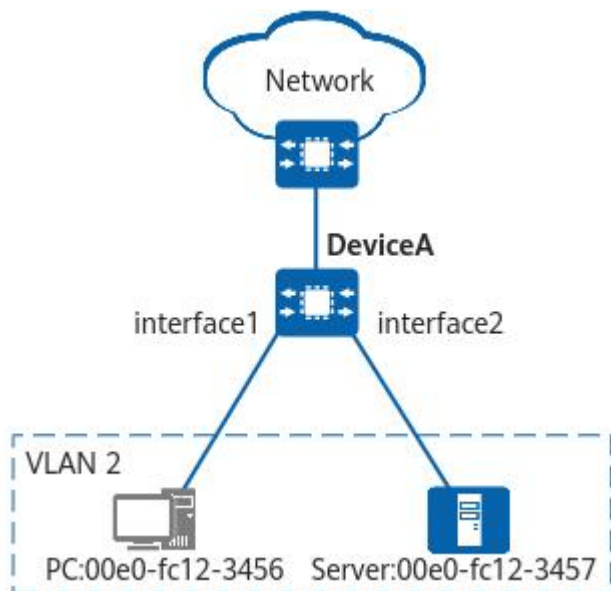
组网需求

如[图 1](#)所示，服务器通过 10GE1/0/2 接口连接设备。为避免设备在转发目的地址为服务器地址的报文时进行广播，要求在设备上设置服务器的静态 MAC 地址表项，使设备始终通过 10GE1/0/2 接口单播发送去往服务器的报文。为了保证 PC 用户和服务器的安全通信，同时把 PC 用户的 MAC 地址和接口 10GE1/0/1 静态绑定。

说明

本例中 interface1、interface2 分别代表 10GE1/0/1、10GE1/0/2。

图 1 配置静态 MAC 地址组网图



配置思路

采用如下思路配置静态 MAC：

1. 创建 VLAN，并将接口加入 VLAN，实现二层转发功能。
2. 在接口配置上服务器的静态 MAC 地址表项。

操作步骤

1. 创建 VLAN2，并将 10GE1/0/1、10GE1/0/2 加入 VLAN 2。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 2
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 2
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE] portswitch
[DeviceA-10GE] port link-type access
[DeviceA-10GE] port default vlan 2
[DeviceA-10GE] quit
```

2. 在接口 10GE1/0/1 上配置 PC 对应的静态 MAC 地址表项。

```
[DeviceA] mac-address static 00e0-fc12-3456 10ge 1/0/1 vlan 2
```

3. 在接口 10GE1/0/2 上配置 Server 对应的静态 MAC 地址表项。

```
[DeviceA] mac-address static 00e0-fc12-3457 10ge 1/0/2 vlan 2
```


检查配置结果

在任意视图下执行命令 `display mac-address static vlan vlan-id [ verbose ]`，查看基于 VLAN 配置的静态 MAC 表项。

[DeviceA] display mac-address static vlan 2

MAC Address	VLAN/VSID/BD	Learned-From	Type	Age
00e0-fc12-3456	2/-/-	10GE1/0/1	static	-
00e0-fc12-3457	2/-/-	10GE1/0/2	static	-

Total items displayed = 2

配置脚本

```
#
sysname DeviceA
#
vlan batch 2
#
interface 10GE1/0/1
port link-type access
port default vlan 2
#
interface 10GE1/0/2
port link-type access
port default vlan 2
#
mac-address static 00e0-fc12-3456 10GE1/0/1 vlan 2
mac-address static 00e0-fc12-3457 10GE1/0/2 vlan 2
#
return
```

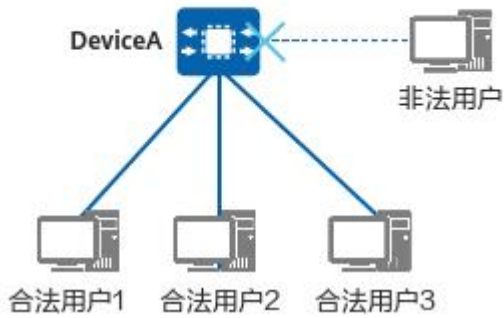
1.1.5.6.1.2 举例：配置黑洞 MAC 表项

组网需求

如图 1 所示，设备收到一个非法用户的访问，非法用户的 MAC 地址为 00e0-fc12-3456，所属 VLAN 为 VLAN 3。通过指定该 MAC 地址为黑洞 MAC，实现非法用户的过滤。

图 1 配置黑洞 MAC 地址组网图

MAC Address	VLAN ID
00e0-fc12-3456	3



配置思路

采用如下的思路配置黑洞 MAC：

1. 创建 VLAN，实现二层转发功能。
2. 添加黑洞 MAC 表，防止非法 MAC 地址攻击。

操作步骤

1. 添加黑洞 MAC 地址表项。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan 3
[DeviceA-vlan 3] quit
[DeviceA] mac-address blackhole 00e0-fc12-3456 vlan 3
```

检查配置结果

在任意视图下执行命令 `display mac-address blackhole`，查看黑洞 MAC 表项。

```
[DeviceA] display mac-address static vlan 2
-----
MAC Address  VLAN/VSI/BD          Learned-From  Type    Age
-----
00e0-fc12-3456  3/-/-          -           blackhole  -
-----
Total items displayed = 1
```

配置脚本

```
#
```

```
sysname DeviceA
#
vlan batch 3
#
mac-address blackhole 00e0-fc12-3456 vlan 3
#
return
```

1.1.5.6.1.3 举例：配置基于接口的 MAC 地址限制

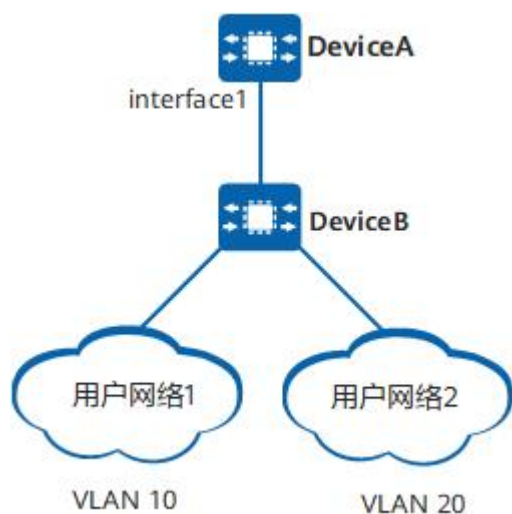
组网需求

如图 1 所示，用户网络 1 和用户网络 2 通过 DeviceB 与 DeviceA 相连，DeviceA 连接 DeviceB 的接口为 10GE1/0/1。用户网络 1 和用户网络 2 分别属于 VLAN 10 和 VLAN 20。在 DeviceA 上，为了控制接入用户数量，可以基于接口 10GE1/0/1 配置 MAC 地址限制。

图 1 配置基于接口的 MAC 地址限制组网图

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

采用如下的思路配置基于接口的 MAC 地址限制：

1. 创建 VLAN，并将接口加入到 VLAN 中，实现二层转发功能。
2. 配置基于接口的 MAC 地址限制，控制接入用户数量。

操作步骤

1. 创建 VLAN，并将接口加入到 VLAN 中。

将 10GE1/0/1 加入 VLAN 10 和 VLAN 20。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10 20
[DeviceA-10GE1/0/1] quit
```

2. 配置基于接口的 MAC 地址限制。

在接口 10GE1/0/1 上配置动态学习 MAC 地址的数量和动作：最多可以学习 100 个 MAC 地址，超过最大 MAC 地址学习数量的报文进行告警提示。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] mac-address limit maximum 100 alarm enable
[DeviceA-10GE1/0/1] quit
```

检查配置结果

在任意视图下执行命令 **display mac-address limit**，查看动态学习 MAC 地址的数量和动作是否配置成功。

```
[DeviceA] display mac-address limit
MAC Address Limit is enabled
Total MAC Address limit rule count : 1
```

Port	VLAN/VSI/SI/BD	Slot	Maximum	Action	Alarm
10GE1/0/1	--	--	100	discard	enable

配置脚本

```
#
sysname DeviceA
#
vlan batch 10 20
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10 20
mac-address limit maximum 100 alarm enable
#
```

return

1.1.5.6.1.4 举例：配置基于 VLAN 的 MAC 地址限制

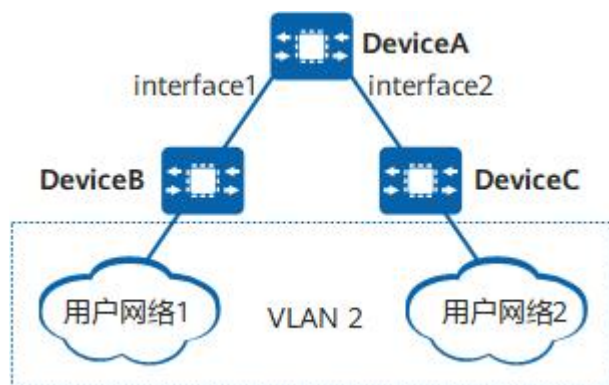
组网需求

如图 1 所示，用户网络 1 通过 DeviceB 与 DeviceA 相连，DeviceA 的接口为 10GE1/0/1。用户网络 2 通过 DeviceC 与 DeviceA 相连，DeviceA 的接口为 10GE1/0/2。10GE1/0/1、10GE1/0/2 同属于 VLAN 2。为控制接入用户数，对 VLAN 2 进行配置 MAC 地址限制。

图 1 配置基于 VLAN 的 MAC 地址限制组网图

说明

本例中 interface1、interface2 分别代表 10GE1/0/1、10GE1/0/2。



配置思路

采用如下的思路配置基于 VLAN 的 MAC 地址限制：

1. 创建 VLAN，并将接口加入到 VLAN 中，实现二层转发功能。
2. 配置基于 VLAN 的 MAC 地址限制，控制接入用户数量。

操作步骤

1. 创建 VLAN，并将接口加入到 VLAN 中。

将 10GE1/0/1、10GE1/0/2 加入 VLAN 2。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan 2
[DeviceA-vlan2] quit
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 2
  
```

```
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 2
[DeviceA-10GE1/0/2] quit
```

2. 配置基于 VLAN 的 MAC 地址限制。

在 VLAN 2 上配置动态学习 MAC 地址的数量和动作：最多可以学习 100 个 MAC 地址，超过最大 MAC 地址学习数量的报文继续转发但不加入 MAC 地址表。

```
[DeviceA] vlan 2
[DeviceA-vlan2] mac-address limit maximum 100 action forward
[DeviceA-vlan2] quit
```

检查配置结果

在任意视图下执行命令 **display mac-address limit**，查看动态学习 MAC 地址的数量和动作是否配置成功。

```
[DeviceA] display mac-address limit
MAC Address Limit is enabled
Total MAC Address limit rule count : 1
```

Port	VLAN/VSI/Sl/BD	Slot	Maximum	Action	Alarm
--	2	--	100	forward	enable

配置脚本

```
#
sysname DeviceA
#
vlan batch 2
#
vlan 2
 mac-address limit maximum 100 action forward
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
interface 10GE1/0/2
 port link-type trunk
```

```
port trunk allow-pass vlan 2
#
return
```

1.1.5.6.2 Eth-Trunk

举例：配置手工模式 Eth-Trunk

举例：配置静态 LACP 模式 Eth-Trunk

举例：配置 Eth-Trunk 接口流量本地优先转发示例（集群/堆叠）

1.1.5.6.2.1 举例：配置手工模式 Eth-Trunk

组网需求

如图 1 所示，DeviceA 和 DeviceB 之间存在多条链路，需要提供较大的带宽来实现流量负载分担，同时也希望能够提供一定的冗余度，保证数据传输和链路的可靠性。

图 1 配置手工模式 Eth-Trunk 组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 在 DeviceA 和 DeviceB 上分别创建 Eth-Trunk1 并配置为手工模式。

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] portswitch
[DeviceA-Eth-Trunk1] mode manual load-balance
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface eth-trunk 1
[DeviceB-Eth-Trunk1] portswitch
```

```
[DeviceB-Eth-Trunk1] mode manual load-balance
```

2. 向 DeviceA 和 DeviceB 的 Eth-Trunk 接口中加入成员接口。

配置 DeviceA。

```
[DeviceA-Eth-Trunk1] trunkport 10ge 1/0/1 to 1/0/3
```

```
[DeviceA-Eth-Trunk1] quit
```

配置 DeviceB。

```
[DeviceB-Eth-Trunk1] trunkport 10ge 1/0/1 to 1/0/3
```

```
[DeviceB-Eth-Trunk1] quit
```

检查配置结果

在任意视图下执行 **display eth-trunk 1** 命令，检查 Eth-Trunk 是否创建成功，及成员接口是否正确加入。

```
[DeviceA] display eth-trunk 1
```

Eth-Trunk1's state information is:

Working Mode: Normal Hash Arithmetic: profile default

Least Active-linknumber: 1 Max Bandwidth-affected-linknumber: 128

Operating Status: **up** Number of Up Ports in Trunk: 3

```
-----
PortName          Status   Weight
10GE1/0/1         Up       1
10GE1/0/2         Up       1
10GE1/0/3         Up       1
```

从以上信息看出 Eth-Trunk 1 中包含 3 个成员接口 10GE1/0/1、10GE1/0/2、10GE1/0/3，成员接口的状态都为 Up。Eth-Trunk 1 的“Operating Status”为 Up。

配置脚本

DeviceA

```
#
sysname DeviceA
#
interface Eth-Trunk1
 portswitch
#
interface 10GE1/0/1
 eth-trunk 1
#
interface 10GE1/0/2
 eth-trunk 1
#
```



```
interface 10GE1/0/3
 eth-trunk 1
#
return
```

DeviceB

```
#
sysname DeviceB
#
interface Eth-Trunk1
 portswitch
#
interface 10GE1/0/1
 eth-trunk 1
#
interface 10GE1/0/2
 eth-trunk 1
#
interface 10GE1/0/3
 eth-trunk 1
#
return
```

1.1.5.6.2.2 举例：配置静态 LACP 模式 Eth-Trunk

组网需求

如[图 1](#)所示，DeviceA 和 DeviceB 之间存在多条链路，在两台设备上配置静态 LACP 模式链路聚合组，提高两设备之间的带宽与可靠性，具体要求如下：

两条活动链路具有负载分担的能力。

两设备间的链路具有 1 条冗余备份链路，当活动链路出现故障链路时，备份链路替代故障链路，保持数据传输的可靠性。

图 1 配置静态 LACP 模式 Eth-Trunk 组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 在 DeviceA 和 DeviceB 上分别创建 Eth-Trunk1 并配置为静态 LACP 模式。

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] mode lacp-static
[DeviceA-Eth-Trunk1] quit
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface eth-trunk 1
[DeviceB-Eth-Trunk1] mode lacp-static
[DeviceB-Eth-Trunk1] quit
```

2. 向 DeviceA 和 DeviceB 的 Eth-Trunk 接口中加入成员接口。

配置 DeviceA。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] eth-trunk 1
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] eth-trunk 1
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] eth-trunk 1
[DeviceA-10GE1/0/3] quit
```

配置 DeviceB。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] eth-trunk 1
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] eth-trunk 1
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
```

```
[DeviceB-10GE1/0/3] eth-trunk 1
[DeviceB-10GE1/0/3] quit
```

3. 在 DeviceA 上配置系统优先级为 100，DeviceB 上保持缺省值，使 DeviceA 成为 LACP 主动端。

```
[DeviceA] lacp priority 100
```

4. 在 DeviceA 上配置活动接口上限阈值为 2，剩余一条作为冗余备份链路。

```
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] lacp max active-linknumber 2
[DeviceA-Eth-Trunk1] quit
```

5. 在 DeviceA 上配置接口优先级确定活动链路。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] lacp priority 100
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] lacp priority 100
[DeviceA-10GE1/0/2] quit
```

检查配置结果

查看各 Device 设备的 Eth-Trunk 信息，查看链路是否协商成功。

```
[DeviceA] display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1          Working Mode: Static
Preempt Delay: Disabled   Hash Arithmetic: profile default
System Priority: 100      System ID: xxxx-xxxx-xxxx
Least Active-linknumber: 1   Max Active-linknumber: 2
Operating Status: up       Number Of Up Ports In Trunk: 2
Timeout Period: Slow
```

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
10GE1/0/1	Selected	10GE	100	1	20289	10111100	1
10GE1/0/2	Selected	10GE	100	2	20289	10111100	1
10GE1/0/3	Unselect	10GE	32768	3	20289	10100000	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
10GE1/0/1	32768	xxxx-xxxx-xxxx	32768	4	20289	10111100
10GE1/0/2	32768	xxxx-xxxx-xxxx	32768	5	20289	10111100

10GE1/0/3 32768 xxxx-xxxx-xxxx 32768 6 20289 10100000

[DeviceB] **display eth-trunk 1**

Eth-Trunk1's state information is:

Local:

LAG ID: 1 Working Mode: **Static**

Preempt Delay: Disabled Hash Arithmetic: profile default

System Priority: 32768 System ID: xxxx-xxxx-xxxx

Least Active-linknumber: 1 Max Active-linknumber: 128

Operating Status: **up** Number Of Up Ports In Trunk: 2

Timeout Period: Slow

ActorPortName	Status	PortType	PortPri	PortNo	PortKey	PortState	Weight
10GE1/0/1	Selected	10GE	32768	4	20289	10111100	1
10GE1/0/2	Selected	10GE	32768	5	20289	10111100	1
10GE1/0/3	Unselect	10GE	32768	6	20289	10100000	1

Partner:

ActorPortName	SysPri	SystemID	PortPri	PortNo	PortKey	PortState
10GE1/0/1	100	xxxx-xxxx-xxxx	100	1	20289	10111100
10GE1/0/2	100	xxxx-xxxx-xxxx	100	2	20289	10111100
10GE1/0/3	100	xxxx-xxxx-xxxx	32768	3	20289	10100000

通过以上显示信息可以看到，DeviceA 的系统优先级为 100，高于 DeviceB 的系统优先级。Eth-Trunk 的成员接口中 **10GE1/0/1**、**10GE1/0/2** 成为活动接口，处于 “Selected” 状态，接口 **10GE1/0/3** 处于 “Unselect” 状态，同时实现冗余备份功能。

配置脚本

DeviceA

```
#
sysname DeviceA
#
lacp priority 100
#
interface Eth-Trunk1
mode lacp-static
lacp max active-linknumber 2
#
interface 10GE1/0/1
eth-trunk 1
lacp priority 100
#
```

```
interface 10GE1/0/2
 eth-trunk 1
 lacp priority 100
#
interface 10GE1/0/3
 eth-trunk 1
#
return
```

DeviceB

```
#
sysname DeviceB
#
interface Eth-Trunk1
 mode lacp-static
#
interface 10GE1/0/1
 eth-trunk 1
#
interface 10GE1/0/2
 eth-trunk 1
#
interface 10GE1/0/3
 eth-trunk 1
#
return
```

1.1.5.6.2.3 举例：配置 Eth-Trunk 接口流量本地优先转发示例（集群/堆叠）

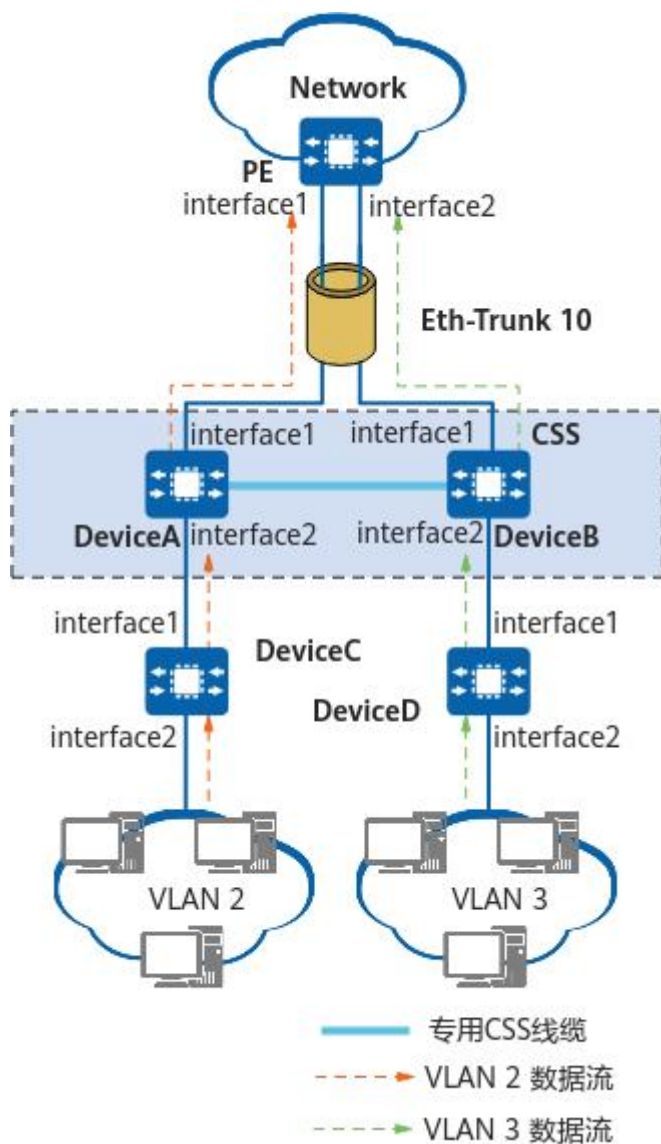
组网需求

如图 1 所示，为了增加设备的容量采用设备集群技术，将 DeviceA 和 DeviceB 通过专用的集群电缆链接起来，对外呈现为一台逻辑交换机。为了实现设备间的备份、提高可靠性，采用跨集群设备 Eth-Trunk 接口技术，将不同设备上的物理接口加入同一个 Eth-Trunk 接口。在网络无任何故障情况下，在 PE 设备上查看成员口信息时，发现 VLAN2 的数据流量会通过成员口 10GE1/0/1 和 10GE1/0/2 转发，VLAN3 的数据流量通过成员口 10GE1/0/1 和 10GE1/0/2 转发。增加了集群设备之间的带宽承载能力，也降低了流量转发效率。为了有效保证 VLAN2 的数据流量通过成员口 10GE1/0/1 转发，VLAN3 的数据流量通过成员口 10GE1/0/2 转发，可在集群/堆叠设备上使能 Eth-Trunk 接口流量本地优先转发功能。

说明

本例中 interface1、interface2 分别代表 10GE1/0/1、10GE1/0/2。

图 1 接口流量本地优先转发组网图



操作步骤

1. 创建 Eth-Trunk 接口，并配置允许通过的 VLAN。

配置集群/堆叠设备。

```
<HUAWEI> system-view
[HUAWEI] sysname CSS
[CSS] interface eth-trunk 10
[CSS-Eth-Trunk1] portswitch
[CSS-Eth-Trunk1] port link-type trunk
[CSS-Eth-Trunk1] port trunk allow-pass vlan all
```

配置汇聚设备 PE。

```
<HUAWEI> system-view
[HUAWEI] sysname PE
[PE] interface eth-trunk 10
[PE-Eth-Trunk10] portswitch
```

```
[PE-Eth-Trunk10] port link-type trunk
[PE-Eth-Trunk10] port trunk allow-pass vlan all
[PE] quit
```

2. 加入 Eth-Trunk 的成员接口。

配置集群/堆叠设备。

```
[CSS] interface 10ge 1/1/0/1
[CSS-10GE1/1/0/1] portswitch
[CSS-10GE1/1/0/1] eth-trunk 10
[CSS-10GE1/1/0/1] quit
[CSS] interface 10ge 2/1/0/1
[CSS-10GE2/1/0/1] eth-trunk 10
[CSS-10GE2/1/0/1] quit
```

配置汇聚设备 PE。

```
[PE] interface eth-trunk 10
[PE-Eth-Trunk10] portswitch
[PE-Eth-Trunk10] port link-type trunk
[PE-Eth-Trunk10] trunkport 10ge 1/0/1 to 1/0/2
[PE-Eth-Trunk10] quit
```

3. 在集群/堆叠交换机 CSS 上使能 Eth-Trunk 接口流量本地优先转发功能。

```
[CSS] interface eth-trunk 10
[CSS-Eth-Trunk10] undo local-preference disable
[CSS] quit
```

默认情况下，设备已使能 Eth-Trunk 接口流量本地优先转发功能。

4. 配置二层转发功能。

配置集群/堆叠设备。

```
[CSS] vlan batch 2 3
[CSS] interface 10ge 1/1/0/2
[CSS-10GE1/1/0/2] port link-type trunk
[CSS-10GE1/1/0/2] port trunk allow pass vlan 2
[CSS-10GE1/1/0/2] quit
[CSS] interface 10ge 2/1/0/2
[CSS-10GE2/1/0/2] port link-type trunk
[CSS-10GE2/1/0/2] port trunk allow pass vlan 2
[CSS-10GE2/1/0/2] quit
```

配置接入设备 DeviceC，配置 DeviceD 方法类似，不做赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan 2
[DeviceC] quit
```

```
[DeviceC] interface 10ge 1/0/1
[PE-Eth-Trunk10] portswitch
[DeviceC-1/0/1] port link-type trunk
[DeviceC-1/0/1] port trunk allow pass vlan 2
[DeviceC-1/0/1] quit
[DeviceC] interface 10ge 1/0/2
[PE-Eth-Trunk10] portswitch
[DeviceC-1/0/2] port link-type trunk
[DeviceC-1/0/2] port trunk allow pass vlan 2
[DeviceC-1/0/2] quit
```

检查配置结果

上述配置成功后，在任意视图下执行 **display eth-trunk membership** 命令，可以看到 Eth-Trunk 接口的成员口信息。例如：

以集群/堆叠交换机 CSS 的显示为例。

```
<CSS> display eth-trunk membership 10
Trunk ID: 10
Used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of Up Ports in Trunk = 2
Operate status: up

Interface 10GE1/1/0/4, valid, operate up, weight=1
Interface 10GE2/1/0/4, valid, operate up, weight=1
```

配置脚本

CSS

```
sysname CSS
#
vlan batch 2 3
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4094
#
interface 10GE1/1/0/2
 port link-type trunk
```



```
port trunk allow-pass vlan 2
#
interface 10GE2/1/0/2
port link-type trunk
port trunk allow-pass vlan 3
#
interface 10GE1/1/0/1
eth-trunk 10
#
interface 10GE2/1/0/1
eth-trunk 10
#
return
```

PE

```
#
sysname PE
#
interface Eth-Trunk10
port link-type trunk
port trunk allow-pass vlan 2 to 4094
#
interface 10GE1/0/1
eth-trunk 10
#
interface 10GE1/0/2
eth-trunk 10
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 2
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2
```

```
#  
return
```

DeviceD

```
#  
sysname DeviceD  
  
#  
vlan batch 3  
  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 3  
  
#  
interface 10GE1/0/2  
port link-type trunk  
port trunk allow-pass vlan 3  
  
#  
return
```

1.1.5.6.3 VLAN

举例：配置 VLANIF 接口实现不同 VLAN 间的互通（同设备）

举例：配置基于接口划分 VLAN，实现同一 VLAN 内的互通（跨设备）

举例：配置基于接口划分 VLAN，实现不同 VLAN 内的互通（接入层设备作为网关）

举例：配置基于接口划分 VLAN，实现不同 VLAN 内的互通（汇聚层设备作为网关）

举例：配置基于 MAC 地址划分 VLAN

举例：配置基于子网划分 VLAN

举例：配置 VLAN 聚合

举例：配置 MUX VLAN（级联设备）

举例：配置基本 QinQ

举例：配置基于 VLAN ID 的灵活 QinQ

举例：配置基于 MQC 的灵活 QinQ

1.1.5.6.3.1 举例：配置 VLANIF 接口实现不同 VLAN 间的互通（同设备）

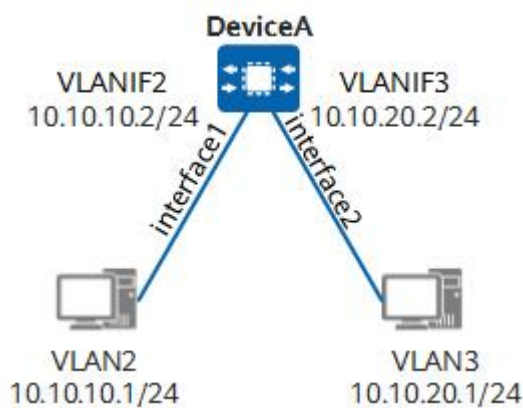
组网需求

如图 1 所示，DeviceA 下的主机被划分到不同的 VLAN 中，分别是 VLAN2 和 VLAN3，且位于不同的网段。希望实现 VLAN2 和 VLAN3 之间相互通信。

图 1 配置 VLANIF 接口实现不同 VLAN 间的互通组网图（同设备）

说明

本例中 interface1、interface2 分别代表 10GE1/0/1、10GE1/0/2。



操作步骤

1. 创建 VLAN，并配置接口加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 2 3
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 2
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 3
[DeviceA-10GE1/0/2] quit
```

2. 配置 VLANIF 接口的 IP 地址。

```
[DeviceA] interface vlanif 2
[DeviceA-Vlanif2] ip address 10.10.10.2 24
```

```
[DeviceA-Vlanif2] quit
[DeviceA] interface vlanif 3
[DeviceA-Vlanif3] ip address 10.10.20.2 24
[DeviceA-Vlanif3] quit
```

检查配置结果

在 VLAN2 中的主机上配置 IP 地址为 10.10.10.1/24，缺省网关为接口 VLANIF2 的 IP 地址 10.10.10.2/24，在 VLAN3 中的主机上配置 IP 地址为 10.10.20.1/24，缺省网关为接口 VLANIF3 的 IP 地址 10.10.20.2/24。配置完成后，VLAN2 中的主机与 VLAN3 中的主机能够相互 Ping 通。

配置脚本

```
#
sysname DeviceA
#
vlan batch 2 to 3
#
interface Vlanif2
ip address 10.10.10.2 255.255.255.0
#
interface Vlanif3
ip address 10.10.20.2 255.255.255.0
#
interface 10GE1/0/1
port default vlan 2
#
interface 10GE1/0/2
port default vlan 3
#
return
```

1.1.5.6.3.2 举例：配置基于接口划分 VLAN，实现同一 VLAN 内的互通（跨设备）

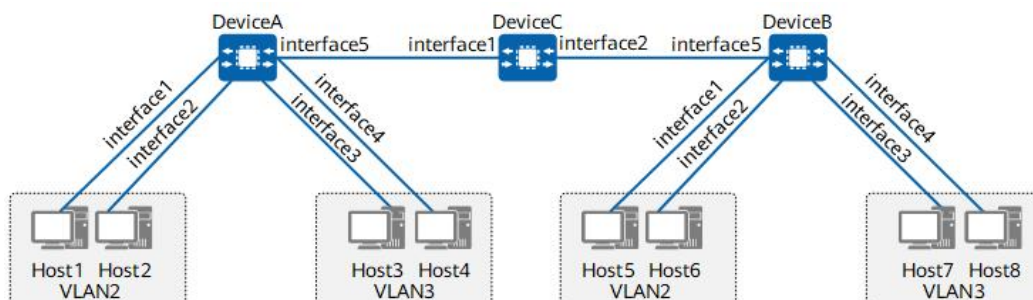
组网需求

如图 1 所示，把 Host1、Host2、Host5、Host6 划分到 VLAN2，把 Host3、Host4、Host7、Host8 划分到 VLAN3。DeviceA 与 DeviceC、DeviceC 与 DeviceB 之间相连的链路允许 VLAN2 和 VLAN3 的报文通过。希望实现 DeviceA 和 DeviceB 下属于同一 VLAN 内的主机可以直接通信，属于不同 VLAN 间的主机不能直接进行二层通信。

图 1 基于接口划分 VLAN 组网图（跨设备）

说明

本例中 interface1、interface2、interface3、interface4、interface5 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4、10GE1/0/5。



操作步骤

1. 配置 DeviceA、DeviceB 与主机相连的接口为 Access 类型的接口，并将 Host1、Host2、Host5、Host6 划分到 VLAN2，将 Host3、Host4、Host7、Host8 划分到 VLAN3。

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 2 3
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 2
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 2
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 3
[DeviceA-10GE1/0/3] quit
[DeviceA] interface 10ge 1/0/4
[DeviceA-10GE1/0/4] portswitch
[DeviceA-10GE1/0/4] port link-type access
[DeviceA-10GE1/0/4] port default vlan 3
[DeviceA-10GE1/0/4] quit
```

配置 DeviceB。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 2 3
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type access
[DeviceB-10GE1/0/1] port default vlan 2
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type access
[DeviceB-10GE1/0/2] port default vlan 2
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type access
[DeviceB-10GE1/0/3] port default vlan 3
[DeviceB-10GE1/0/3] quit
[DeviceB] interface 10ge 1/0/4
[DeviceB-10GE1/0/4] portswitch
[DeviceB-10GE1/0/4] port link-type access
[DeviceB-10GE1/0/4] port default vlan 3
[DeviceB-10GE1/0/4] quit

```

2. 配置 DeviceA 与 DeviceC、DeviceB 与 DeviceC 之间的链路为干道链路

配置 DeviceA。

```

[DeviceA] interface 10ge 1/0/5
[DeviceA-10GE1/0/5] portswitch
[DeviceA-10GE1/0/5] port link-type trunk
[DeviceA-10GE1/0/5] port trunk allow-pass vlan 2 3
[DeviceA-10GE1/0/5] quit

```

配置 DeviceB。

```

[DeviceB] interface 10ge 1/0/5
[DeviceB-10GE1/0/5] portswitch
[DeviceB-10GE1/0/5] port link-type trunk
[DeviceB-10GE1/0/5] port trunk allow-pass vlan 2 3
[DeviceB-10GE1/0/5] quit

```

配置 DeviceC。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 2 3
[DeviceC] interface 10ge 1/0/1

```

```
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] port link-type trunk
[DeviceC-10GE1/0/1] port trunk allow-pass vlan 2 3
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] port link-type trunk
[DeviceC-10GE1/0/2] port trunk allow-pass vlan 2 3
[DeviceC-10GE1/0/2] quit
```

检查配置结果

执行命令 **display vlan** 可以查看 VLAN 状态，以 DeviceA 为例：

```
[DeviceA] display vlan 2
```

```
-----
U: Up;      D: Down;    TG: Tagged;    UT: Untagged;
MP: Vlan-mapping;      ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
MAC-LRN: MAC-address learning; STAT: Statistic;
BC: Broadcast; MC: Multicast; UC: Unknown-unicast;
FWD: Forward; DSD: Discard;
-----
```

```
VID      Ports
-----
 2      UT:10GE1/0/1(U) 10GE1/0/2(U)
        TG:10GE1/0/5(U)
```

```
VID Type  Status Property MAC-LRN STAT  BC MC UC Description
-----
 2 common enable default enable disable FWD FWD FWD VLAN 0002
```

执行命令 **display port vlan**，查看 10GE1/0/5 接口上可以通过的 VLAN 信息，以 DeviceA 为例：

```
[DeviceA] display port vlan 10ge 1/0/5
```

```
Port      Link Type  PVID Trunk VLAN List      Port Description
-----
10GE1/0/5      trunk      1 1-3
```

在 DeviceA 和 DeviceB 下，属于相同 VLAN2 或相同 VLAN3 内的主机之间能够互相 Ping 通，并且 VLAN2 的主机无法 Ping 通 VLAN3 内的主机。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 2 to 3
#
interface 10GE1/0/1
port default vlan 2
#
interface 10GE1/0/2
port default vlan 2
#
interface 10GE1/0/3
port default vlan 3
#
interface 10GE1/0/4
port default vlan 3
#
interface 10GE1/0/5
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 2 to 3
#
interface 10GE1/0/1
port default vlan 2
#
interface 10GE1/0/2
port default vlan 2
#
interface 10GE1/0/3
port default vlan 3
#
interface 10GE1/0/4
port default vlan 3
#
interface 10GE1/0/5
```



```
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 2 to 3
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
return
```

1.1.5.6.3.3 举例：配置基于接口划分 VLAN，实现不同 VLAN 内的互通（接入层设备作为网关）

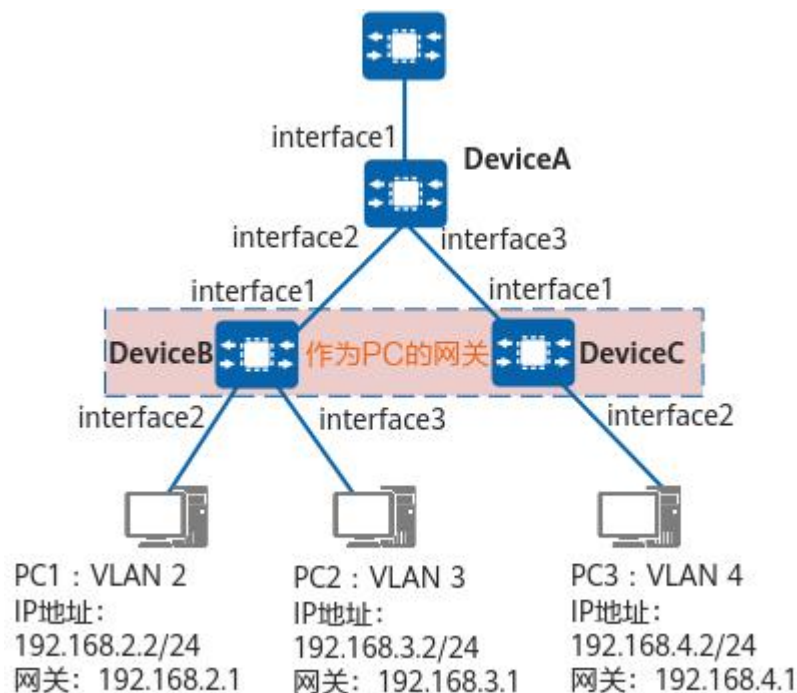
组网需求

如[图 1](#)所示，PC1 和 PC2 分别属于 VLAN 2 和 VLAN 3，通过接入层设备 DeviceB 接入汇聚层设备 DeviceA。PC3 属于 VLAN 4，通过接入层设备 DeviceC 接入汇聚层设备 DeviceA。接入层设备 DeviceB 作为 PC1 和 PC2 的网关，DeviceC 作为 PC3 的网关，通过在设备上配置静态路由，实现用户 PC 间的互访以及和上层设备的互连。

图 1 配置接入层设备作为网关组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 配置接入层设备 DeviceB。

创建 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 2 3
```

将接口加入相应 VLAN。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type access
[DeviceB-10GE1/0/2] port default vlan 2
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type access
[DeviceB-10GE1/0/3] port default vlan 3
[DeviceB-10GE1/0/3] quit
```

配置 VLANIF 接口，作为用户 PC 的网关。

```
[DeviceB] interface vlanif 2
[DeviceB-Vlanif2] ip address 192.168.2.1 24
[DeviceB-Vlanif2] quit
[DeviceB] interface vlanif 3
[DeviceB-Vlanif3] ip address 192.168.3.1 24
[DeviceB-Vlanif3] quit
```

配置 DeviceB 和 DeviceA 互连。

```
[DeviceB] vlan batch 5
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type access
[DeviceB-10GE1/0/1] port default vlan 5
[DeviceB-10GE1/0/1] quit
[DeviceB] interface Vlanif 5
[DeviceB-Vlanif5] ip address 192.168.5.2 24
[DeviceB-Vlanif5] quit
[DeviceB] ip route-static 0.0.0.0 0.0.0.0 192.168.5.1
```

2. 配置接入层设备 DeviceC。

创建 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 4
```

将接口加入相应 VLAN。

```
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] port link-type access
[DeviceC-10GE1/0/2] port default vlan 4
[DeviceC-10GE1/0/2] quit
```

配置 VLANIF 接口，作为用户 PC 的网关。

```
[DeviceC] interface vlanif 4
[DeviceC-Vlanif4] ip address 192.168.4.1 24
[DeviceC-Vlanif4] quit
```

配置 DeviceC 和 DeviceA 互连。

```
[DeviceC] vlan batch 5
[DeviceC] interface 10ge 1/0/1
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] port link-type access
[DeviceC-10GE1/0/1] port default vlan 5
[DeviceC-10GE1/0/1] quit
[DeviceC] interface Vlanif 5
[DeviceC-Vlanif5] ip address 192.168.5.2 24
[DeviceC-Vlanif5] quit
[DeviceC] ip route-static 0.0.0.0 0.0.0.0 192.168.5.1
```

3. 配置汇聚层设备 DeviceA。

创建 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 5
```

将接口加入相应 VLAN。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 5
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 5
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 5
[DeviceA-10GE1/0/3] quit
```

配置 VLANIF 接口，实现和上层设备的互连。

```
[DeviceA] interface vlanif 5
[DeviceA-Vlanif5] ip address 192.168.5.1 24
[DeviceA-Vlanif5] quit
```

配置回程明细路由，实现内网网段之间互访。

```
[DeviceA] ip route-static 192.168.2.0 255.255.255.0 192.168.5.2
[DeviceA] ip route-static 192.168.3.0 255.255.255.0 192.168.5.2
[DeviceA] ip route-static 192.168.4.0 255.255.255.0 192.168.5.3
```

配置缺省路由，实现内网网段到上层设备的访问。

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 192.168.5.4
```

检查配置结果

执行命令 **display vlan** 可以查看 VLAN 状态，以 DeviceB 为例：

```
[DeviceB] display vlan 2
```

```
-----
U: Up;      D: Down;    TG: Tagged;    UT: Untagged;
MP: Vlan-mapping;      ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
MAC-LRN: MAC-address learning; STAT: Statistic;
BC: Broadcast; MC: Multicast; UC: Unknown-unicast;
```

FWD: Forward; DSD: Discard;

VID	Ports
2	UT:10GE1/0/2(U) 10GE1/0/3(U) TG:10GE1/0/1(U)

VID	Type	Status	Property	MAC-LRN	STAT	BC	MC	UC	Description
2	common	enable	default	enable	disable	FWD	FWD	FWD	VLAN 0002

执行命令 **display port vlan**，查看接口上可以通过的 VLAN 信息，以 DeviceB 的接口 10GE1/0/1 为例：

[DeviceB] display port vlan 10ge 1/0/1				
Port	Link Type	PVID	Trunk VLAN List	Port Description
10GE1/0/1	trunk	1	2-3	

配置脚本

DeviceA

```
#
sysname DeviceA

#
vlan batch 5

#
interface Vlanif5
 ip address 192.168.5.1 255.255.255.0

#
interface 10GE1/0/1
 port link-type access
 port default vlan 5

#
interface 10GE1/0/2
 port link-type access
 port default vlan 5

#
interface 10GE1/0/3
 port link-type access
 port default vlan 5

#
ip route-static 0.0.0.0 0.0.0.0 192.168.5.4
```

```
ip route-static 192.168.2.0 255.255.255.0 192.168.5.2
ip route-static 192.168.3.0 255.255.255.0 192.168.5.2
ip route-static 192.168.4.0 255.255.255.0 192.168.5.3
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 2 to 3 5
#
#
interface Vlanif2
 ip address 192.168.2.1 255.255.255.0
#
interface Vlanif3
 ip address 192.168.3.1 255.255.255.0
#
interface Vlanif5
 ip address 192.168.5.2 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 5
#
interface 10GE1/0/2
 port link-type access
 port default vlan 2
#
interface 10GE1/0/3
 port link-type access
 port default vlan 3
#
ip route-static 0.0.0.0 0.0.0.0 192.168.5.1
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 4 to 5
```

```
#
#
interface Vlanif4
 ip address 192.168.4.1 255.255.255.0
#
interface Vlanif5
 ip address 192.168.5.3 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 5
#
interface 10GE1/0/2
 port link-type access
 port default vlan 4
#
ip route-static 0.0.0.0 0.0.0.0 192.168.5.1
#
return
```

1.1.5.6.3.4 举例：配置基于接口划分 VLAN，实现不同 VLAN 内的互通（汇聚层设备作为网关）

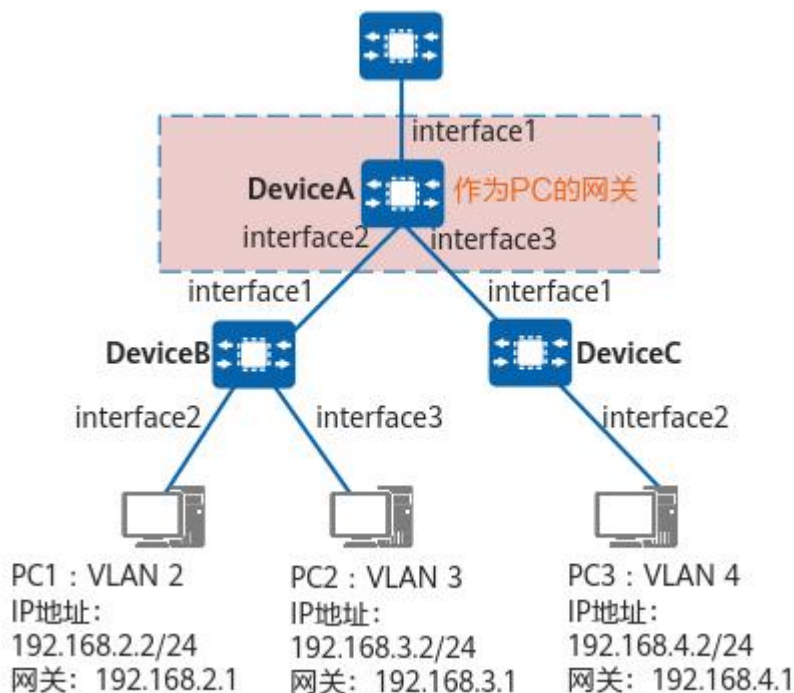
组网需求

如图 1 所示，PC1 和 PC2 分别属于 VLAN 2 和 VLAN 3，通过接入层设备 DeviceB 接入汇聚层设备 DeviceA。PC3 属于 VLAN 4，通过接入层设备 DeviceC 接入汇聚层设备 DeviceA。DeviceC 不做任何配置，当做 HUB 即插即用。汇聚层设备 DeviceA 作为 PC1、PC2 和 PC3 的网关，实现用户 PC 间的互访以及和上层设备的互连。

图 1 配置汇聚层设备作为网关组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 配置接入层设备 DeviceB。

创建 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 2 3
```

将接口加入相应 VLAN。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type access
[DeviceB-10GE1/0/2] port default vlan 2
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type access
[DeviceB-10GE1/0/3] port default vlan 3
[DeviceB-10GE1/0/3] quit
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 2 3
[DeviceB-10GE1/0/1] quit
```

2. 配置汇聚层设备 DeviceA。

创建 VLAN。


```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 2 to 5
```

将连接 DeviceB、DeviceC 的接口加入相应 VLAN。

```
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 2 3
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 4
[DeviceA-10GE1/0/3] quit
```

配置 VLANIF 接口，作为用户 PC 的网关。

```
[DeviceA] interface vlanif 2
[DeviceA-Vlanif5] ip address 192.168.2.1 24
[DeviceA-Vlanif5] quit
[DeviceA] interface vlanif 3
[DeviceA-Vlanif5] ip address 192.168.3.1 24
[DeviceA-Vlanif5] quit
[DeviceA] interface vlanif 4
[DeviceA-Vlanif5] ip address 192.168.4.1 24
[DeviceA-Vlanif5] quit
```

将连接上层设备的接口加入相应 VLAN。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 5
[DeviceA-10GE1/0/1] quit
```

配置 VLANIF 接口，实现内网网段到上层设备的访问。

```
[DeviceA] interface vlanif 5
[DeviceA-Vlanif5] ip address 192.168.5.1 24
[DeviceA-Vlanif5] quit
```

检查配置结果

执行命令 **display vlan** 可以查看 VLAN 状态，以 DeviceB 为例：

```
[DeviceB] display vlan 2
```

U: Up; D: Down; TG: Tagged; UT: Untagged;
MP: Vlan-mapping; ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
MAC-LRN: MAC-address learning; STAT: Statistic;
BC: Broadcast; MC: Multicast; UC: Unknown-unicast;
FWD: Forward; DSD: Discard;

VID	Ports
2	UT:10GE1/0/2(U) 10GE1/0/3(U) TG:10GE1/0/1(U)

VID	Type	Status	Property	MAC-LRN	STAT	BC	MC	UC	Description
2	common	enable	default	enable	disable	FWD	FWD	FWD	VLAN 0002

执行命令 **display port vlan**，查看接口上可以通过的 VLAN 信息，以 DeviceB 的接口 10GE1/0/1 为例：

[DeviceB] **display port vlan 10ge 1/0/1**

Port	Link Type	PVID	Trunk VLAN List	Port Description
10GE1/0/1	trunk	1	2-3	

配置脚本

DeviceA

```
#
sysname DeviceA

#
vlan batch 2 to 5

#
interface Vlanif2
ip address 192.168.2.1 255.255.255.0

#
interface Vlanif3
ip address 192.168.3.1 255.255.255.0

#
interface Vlanif4
ip address 192.168.4.1 255.255.255.0

#
interface Vlanif5
ip address 192.168.5.1 255.255.255.0
```

```
#
interface 10GE1/0/1
 port link-type access
 port default vlan 5
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
interface 10GE1/0/3
 port link-type access
 port default vlan 4
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 2 to 3
#
interface 10GE1/0/1

 port link-type trunk
 port trunk allow-pass vlan 2 to 3
#
interface 10GE1/0/2
 port link-type access
 port default vlan 2
#
interface 10GE1/0/3
 port link-type access
 port default vlan 3
#
return
```

1.1.5.6.3.5 举例：配置基于 MAC 地址划分 VLAN

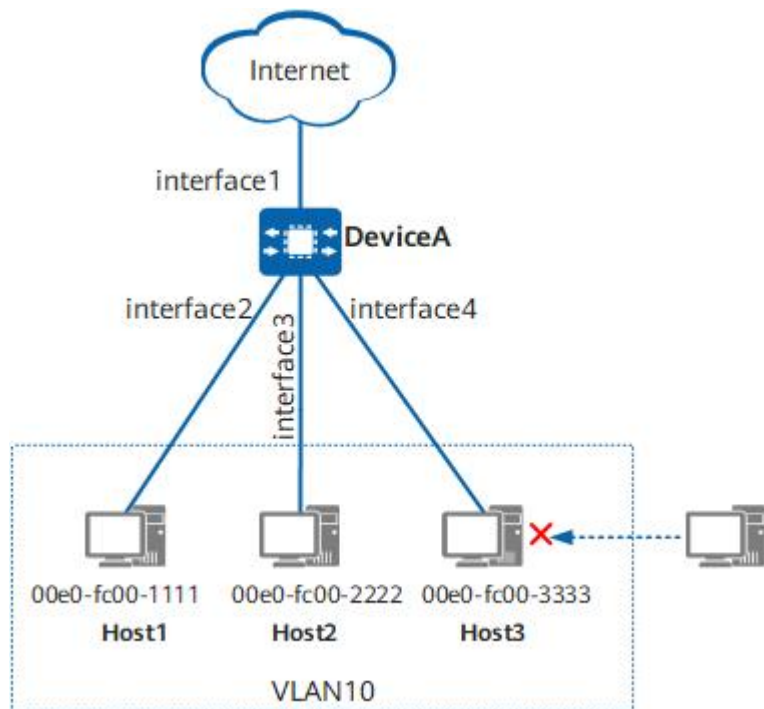
组网需求

如图 1 所示，根据主机 MAC 地址将网络内主机 Host1、Host2、Host3 划分到 VLAN10。主机之间可以互相访问且能访问 Internet。如果私自更换其他主机接入网络，则无法访问 Internet，且和其他合法主机间也无法互访。

图 1 基于 MAC 地址划分 VLAN 组网图

说明

本例中 interface1、interface2、interface3、interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4。



操作步骤

1. 创建 VLAN10，并将用户主机的 MAC 地址与 VLAN 进行关联。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan 10
[DeviceA-vlan10] mac-vlan mac-address 00e0-fc00-1111
[DeviceA-vlan10] mac-vlan mac-address 00e0-fc00-2222
[DeviceA-vlan10] mac-vlan mac-address 00e0-fc00-3333
[DeviceA-vlan10] quit
  
```

2. 配置接口加入 VLAN10，并在接口 10GE1/0/2~10GE1/0/4 上使能基于 MAC 地址划分 VLAN。

```

[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type hybrid
[DeviceA-10GE1/0/1] port hybrid tagged vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
  
```

```
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type hybrid
[DeviceA-10GE1/0/2] port hybrid untagged vlan 10
[DeviceA-10GE1/0/2] mac-vlan enable
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type hybrid
[DeviceA-10GE1/0/3] port hybrid untagged vlan 10
[DeviceA-10GE1/0/3] mac-vlan enable
[DeviceA-10GE1/0/3] quit
[DeviceA] interface 10ge 1/0/4
[DeviceA-10GE1/0/4] portswitch
[DeviceA-10GE1/0/4] port link-type hybrid
[DeviceA-10GE1/0/4] port hybrid untagged vlan 10
[DeviceA-10GE1/0/4] mac-vlan enable
[DeviceA-10GE1/0/4] quit
```

检查配置结果

执行命令 **display mac-vlan vlan 10**，查看基于 MAC 地址划分 VLAN 的信息。

```
[DeviceA] display mac-vlan vlan 10
```

```
Total MAC VLAN address count: 3
```

```
-----
MAC Address   Mask          VLAN   Priority
-----
```

```
00e0-fc00-1111 ffff-ffff-ffff 10      0
```

```
00e0-fc00-2222 ffff-ffff-ffff 10      0
```

```
00e0-fc00-3333 ffff-ffff-ffff 10      0
```

网络内合法主机 Host1、Host2、Host3 可以互访且均能访问 Internet，如果更换成其他主机不能访问。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 10
#
vlan 10
mac-vlan mac-address 00e0-fc00-1111
```

```
mac-vlan mac-address 00e0-fc00-2222
mac-vlan mac-address 00e0-fc00-3333
#
interface 10GE1/0/1
port link-type hybrid
port hybrid tagged vlan 10
#
interface 10GE1/0/2
port link-type hybrid
port hybrid untagged vlan 10
mac-vlan enable
#
interface 10GE1/0/3
port link-type hybrid
port hybrid untagged vlan 10
mac-vlan enable
#
interface 10GE1/0/4
port link-type hybrid
port hybrid untagged vlan 10
mac-vlan enable
#
return
```

1.1.5.6.3.6 举例：配置基于子网划分 VLAN

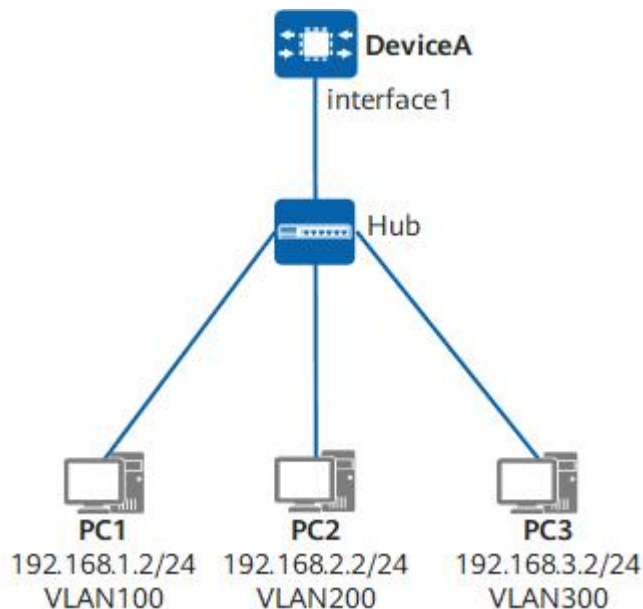
组网需求

如[图 1](#)所示，PC1、PC2、PC3 的 IP 地址网段不相同。希望将不同 IP 地址网段的 PC 划分到不同的 VLAN，即 PC1、PC2、PC3 分别划分到 VLAN100、VLAN200、VLAN300 中。

图 1 基于子网划分 VLAN 组网图

说明

本例中 interface1 代表 10GE1/0/1。



操作步骤

1. 创建 VLAN，并关联 IP 子网和 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 100 200 300
[DeviceA] vlan 100
[DeviceA-vlan100] ip-subnet-vlan 1 ip 192.168.1.2 24 priority 2
[DeviceA-vlan100] quit
[DeviceA] vlan 200
[DeviceA-vlan200] ip-subnet-vlan 1 ip 192.168.2.2 24 priority 3
[DeviceA-vlan200] quit
[DeviceA] vlan 300
[DeviceA-vlan300] ip-subnet-vlan 1 ip 192.168.3.2 24 priority 4
[DeviceA-vlan300] quit
```

2. 配置接口 10GE1/0/1 为 Hybrid 类型，接口允许 VLAN100、VLAN200、VLAN300 通过，并使能基于子网划分 VLAN 功能。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type hybrid
[DeviceA-10GE1/0/1] port hybrid untagged vlan 100
[DeviceA-10GE1/0/1] port hybrid untagged vlan 200
[DeviceA-10GE1/0/1] port hybrid untagged vlan 300
[DeviceA-10GE1/0/1] ip-subnet-vlan enable
[DeviceA-10GE1/0/1] quit
```

检查配置结果

在 DeviceA 上执行命令 `display ip-subnet-vlan vlan all`，查看设备上基于子网划分 VLAN 的信息。

```
[DeviceA] display ip-subnet-vlan vlan all
IP-subnet-VLAN count: 3          total count: 3
-----
VLAN  Index IpAddress      SubnetMask      Priority
-----
100    1 192.168.1.2    255.255.255.0    2
200    1 192.168.2.2    255.255.255.0    3
300    1 192.168.3.2    255.255.255.0    4
-----
```

配置脚本

DeviceA

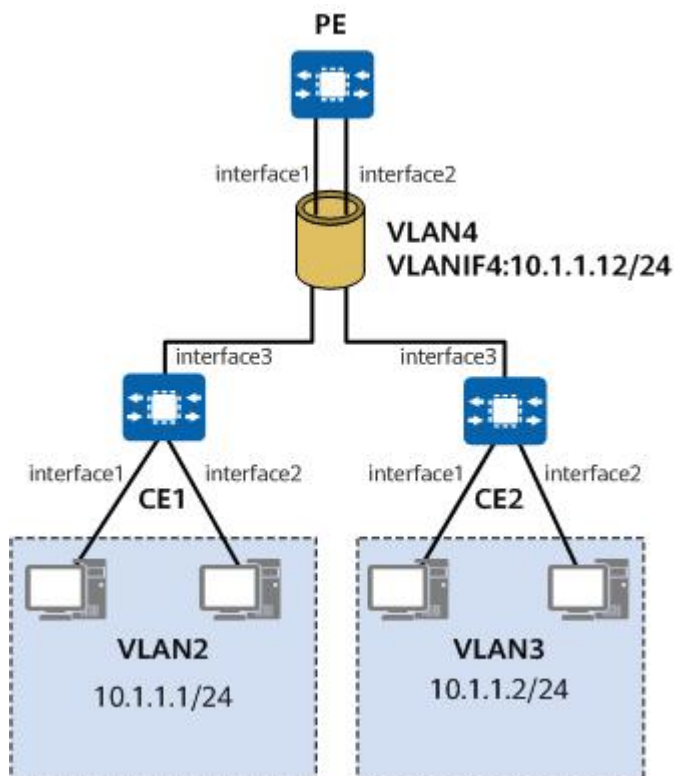
```
#
sysname DeviceA
#
vlan batch 100 200 300
#
vlan 100
 ip-subnet-vlan 1 ip 192.168.1.2 255.255.255.0 priority 2
#
vlan 200
 ip-subnet-vlan 1 ip 192.168.2.2 255.255.255.0 priority 3
#
vlan 300
 ip-subnet-vlan 1 ip 192.168.3.2 255.255.255.0 priority 4
#
interface 10GE1/0/1
 port link-type hybrid
 port hybrid untagged vlan 100
 port hybrid untagged vlan 200
 port hybrid untagged vlan 300
 ip-subnet-vlan enable
#
return
```

1.1.5.6.3.7 举例：配置 VLAN 聚合

组网需求

如图 [VLAN 间通过 VLAN 聚合通信组网图](#) 所示，VLAN2 和 VLAN3 是两个 Sub-VLAN，二者接入到 VLAN4 这个 Super-VLAN 中，VLAN2 和 VLAN3 的 PC 需要进行互通。

图 1 VLAN 间通过 VLAN 聚合通信组网图



配置思路

采用如下思路配置 VLAN 间通过 VLAN 聚合通信：

1. 在 CE 上创建 VLAN，确定用户所属的 VLAN。
2. 在 PE 上配置 VLAN 聚合。
 - a. 配置二层转发功能。
 - b. 创建 Super-VLAN，并把 Sub-VLAN 加入 Super-VLAN。
 - c. 创建 Super-VLAN 对应的 VLANIF 接口，并配置 IP 地址，作为网关地址。

数据准备

为完成此配置例，需准备如下的数据：

用户所属的 VLAN ID。

用户的 IP 地址。

CE 连接用户的接口编号。

Sub-VLAN ID、Super-VLAN ID。

Super-VLAN 对应的 VLANIF 接口编号及 IP 地址。

操作步骤

1. 在 CE 上创建 VLAN，并将二层端口加入 VLAN。

配置 CE1。

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] vlan batch 2
[CE1] interface 10ge 1/0/1
[CE1-10GE1/0/1] portswitch
[CE1-10GE1/0/1] port link-type access
[CE1-10GE1/0/1] port default vlan 2
[CE1-10GE1/0/1] quit
[CE1] interface 10ge 1/0/2
[CE1-10GE1/0/2] portswitch
[CE1-10GE1/0/2] port link-type access
[CE1-10GE1/0/2] port default vlan 2
[CE1-10GE1/0/2] quit
[CE1] interface 10ge 1/0/3
[CE1-10GE1/0/3] portswitch
[CE1-10GE1/0/3] port link-type trunk
[CE1-10GE1/0/3] port trunk allow-pass vlan 2
[CE1-10GE1/0/3] quit
```

配置 CE2。

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] vlan batch 3
[CE2] interface 10ge 1/0/1
[CE2-10GE1/0/1] portswitch
[CE2-10GE1/0/1] port link-type access
[CE2-10GE1/0/1] port default vlan 3
[CE2-10GE1/0/1] quit
[CE2] interface 10ge 1/0/2
[CE2-10GE1/0/2] portswitch
[CE2-10GE1/0/2] port link-type access
[CE2-10GE1/0/2] port default vlan 3
[CE2-10GE1/0/2] quit
[CE2] interface 10ge 1/0/3
[CE2-10GE1/0/3] portswitch
[CE2-10GE1/0/3] port link-type trunk
[CE2-10GE1/0/3] port trunk allow-pass vlan 3
[CE2-10GE1/0/3] quit
```

2. 在 PE 上配置 VLAN 聚合。

配置二层转发功能。

```
<HUAWEI> system-view
[HUAWEI] sysname PE
[PE] vlan batch 2 to 4
[PE] interface 10ge 1/0/1
[PE-10GE1/0/1] portswitch
[PE-10GE1/0/1] port link-type trunk
[PE-10GE1/0/1] port trunk allow-pass vlan 2
[PE-10GE1/0/1] quit
[PE] interface 10ge 1/0/2
[PE-10GE1/0/2] portswitch
[PE-10GE1/0/2] port link-type trunk
[PE-10GE1/0/2] port trunk allow-pass vlan 3
[PE-10GE1/0/2] quit
```

创建 Super-VLAN，并将 Sub-VLAN 加入 Super-VLAN。

```
[PE] vlan 4
[PE-vlan4] aggregate-vlan
[PE-vlan4] access-vlan 2 to 3
[PE-vlan4] quit
```

创建 Super-VLAN 对应的 VLANIF 接口，并配置 IP 地址。

```
[PE] interface vlanif 4
[PE-Vlanif4] ip address 10.1.1.12 24
```

上述配置完成后，为各 PC 配置 IP 地址，PC 的 IP 地址和 VLANIF 接口的 IP 地址应处于同一网段。配置成功后，各 VLAN 中的员工与交换机之间可以互通，但 VLAN2 和 VLAN3 中的 PC 不能互通。

3. 使能 VLAN 间 ARP 代理功能。

```
[PE-vlanif4] arp proxy inter-vlan enable
[PE-vlanif4] quit
```

4. 检查配置结果。

上述配置完成后，VLAN2 中的 PC 与 VLAN3 中的 PC 可以互通。

配置脚本

CE1 的配置文件

```
#
sysname CE1
#
vlan batch 2
#
interface 10GE1/0/1
```

```
port link-type access
port default vlan 2
#
interface 10GE1/0/2

port link-type access
port default vlan 2
#
interface 10GE1/0/3

port link-type trunk
port trunk allow-pass vlan 2
#
return
```

CE2 的配置文件

```
#
sysname CE2
#
vlan batch 3
#
interface 10GE1/0/1

port link-type access
port default vlan 3
#
interface 10GE1/0/2

port link-type access
port default vlan 3
#
interface 10GE1/0/3

port link-type trunk
port trunk allow-pass vlan 3
#
return
```

PE 的配置文件

```
#
sysname PE
#
vlan batch 2 to 4
#
vlan 4
aggregate-vlan
access-vlan 2 to 3
#
interface Vlanif4
ip address 10.1.1.12 255.255.255.0
arp proxy inter-vlan enable
#
interface 10GE1/0/1

port link-type trunk
port trunk allow-pass vlan 2
#
interface 10GE1/0/2

port link-type trunk
port trunk allow-pass vlan 3
#
return
```

1.1.5.6.3.8 举例：配置 MUX VLAN（级联设备）

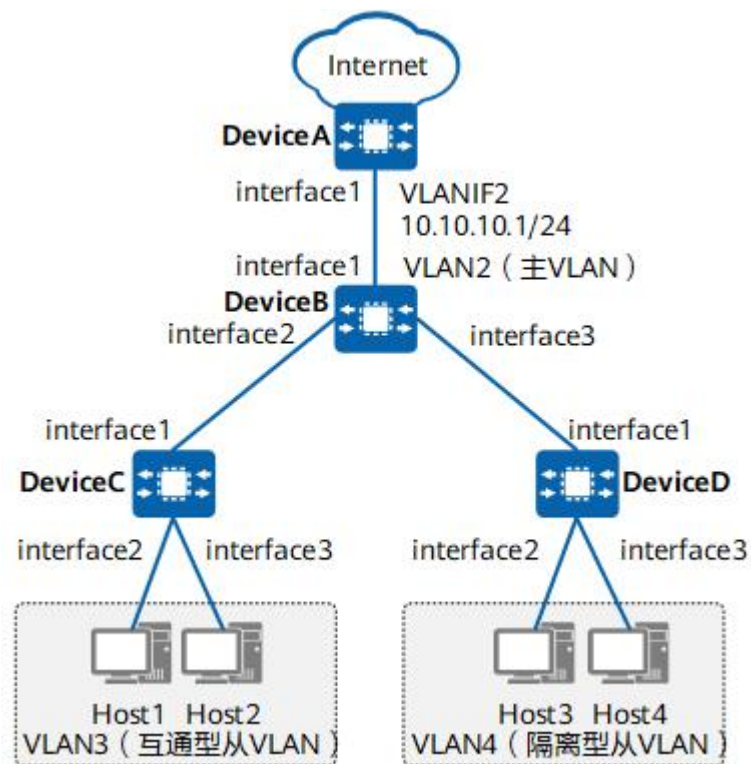
组网需求

如图 1 所示，用户希望网络内主机均可以访问 Internet，并且 VLAN3 内的主机可以互相访问，VLAN4 内的主机不能互访。

图 1 配置 MUX VLAN 组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 配置 MUX VLAN。

在 DeviceB 上创建 VLAN 2~VLAN 4，配置 VLAN 2 为主 VLAN，VLAN 3 为互通型从 VLAN，VLAN4 为隔离型从 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 2 3 4
[DeviceB] vlan 2
[DeviceB-vlan2] mux-vlan
[DeviceB-vlan2] subordinate group 3
[DeviceB-vlan2] subordinate separate 4
[DeviceB-vlan2] quit
```

在 DeviceC 上创建 VLAN 2~VLAN 4，配置 VLAN 2 为主 VLAN，VLAN 3 为互通型从 VLAN，VLAN 4 为隔离型从 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 2 3 4
[DeviceC] vlan 2
[DeviceC-vlan2] mux-vlan
[DeviceC-vlan2] subordinate group 3
[DeviceC-vlan2] subordinate separate 4
[DeviceC-vlan2] quit
```

在 DeviceD 上创建 VLAN 2~VLAN 4，配置 VLAN 2 为主 VLAN，VLAN 3 为互通型从 VLAN，VLAN 4 为隔离型从 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] vlan batch 2 3 4
[DeviceD] vlan 2
[DeviceD-vlan2] mux-vlan
[DeviceD-vlan2] subordinate group 3
[DeviceD-vlan2] subordinate separate 4
[DeviceD-vlan2] quit
```

2. 配置 DeviceB 的上行口 interface1 加入 VLAN 2，并使能 MUX VLAN 功能，配置下行口 interface2 和 interface3 允许 VLAN 2~VLAN 4 通过。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 2
[DeviceB-10GE1/0/1] port mux-vlan enable vlan 2
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 2 to 4
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type trunk
[DeviceB-10GE1/0/3] port trunk allow-pass vlan 2 to 4
[DeviceB-10GE1/0/3] quit
```

3. 配置 DeviceC 的上行口 interface1 允许 VLAN 2~VLAN 4 通过，配置下行口 interface2 和 interface3 加入 VLAN 3 并在接口下使能 MUX VLAN 功能。

```
[DeviceC] interface 10ge 1/0/1
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] port link-type trunk
[DeviceC-10GE1/0/1] port trunk allow-pass vlan 2 to 4
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] port link-type access
[DeviceC-10GE1/0/2] port default vlan 3
[DeviceC-10GE1/0/2] port mux-vlan enable vlan 3
[DeviceC-10GE1/0/2] quit
```

```
[DeviceC] interface 10ge 1/0/3
[DeviceC-10GE1/0/3] portswitch
[DeviceC-10GE1/0/3] port link-type access
[DeviceC-10GE1/0/3] port default vlan 3
[DeviceC-10GE1/0/3] port mux-vlan enable vlan 3
[DeviceC-10GE1/0/3] quit
```

4. 配置 DeviceD 的上行口 interface1 允许 VLAN 2~VLAN 4 通过，配置下行口 interface2 和 interface3 加入 VLAN 4 并在接口下使能 MUX VLAN 功能。

```
[DeviceD] interface 10ge 1/0/1
[DeviceD-10GE1/0/1] portswitch
[DeviceD-10GE1/0/1] port link-type trunk
[DeviceD-10GE1/0/1] port trunk allow-pass vlan 2 to 4
[DeviceD-10GE1/0/1] quit
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] portswitch
[DeviceD-10GE1/0/2] port link-type access
[DeviceD-10GE1/0/2] port default vlan 4
[DeviceD-10GE1/0/2] port mux-vlan enable vlan 4
[DeviceD-10GE1/0/2] quit
[DeviceD] interface 10ge 1/0/3
[DeviceD-10GE1/0/3] portswitch
[DeviceD-10GE1/0/3] port link-type access
[DeviceD-10GE1/0/3] port default vlan 4
[DeviceD-10GE1/0/3] port mux-vlan enable vlan 4
[DeviceD-10GE1/0/3] quit
```

5. 在 DeviceA 上创建 VLANIF 2，配置 IP 地址为 10.1.1.1 24，并配置接口 interface1 加入 VLAN 2。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 2
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 2
[DeviceA-10GE1/0/1] quit
[DeviceA] interface vlanif 2
[DeviceA-Vlanif2] ip address 10.1.1.1 24
[DeviceA-Vlanif2] quit
```

说明

如果 MUX VLAN 中有多个 Group VLAN，并且 Group VLAN 之间需要互通，则需要在 DeviceA 的 VLANIF 接口下执行命令 **arp proxy intra-vlan enable** 配置 VLAN 内 ARP Proxy 功能。

6. 配置网络内主机的 IP 地址，使其和 DeviceA 上 VLANIF 2 接口的 IP 地址同网段。

检查配置结果

Host1、Host2、Host3、Host4 可以访问 Internet。

Host1 和 Host2 可以互相 ping 通。

Host3 和 Host4 互相 ping 不通。

VLAN3 内主机（Host1、Host2）和 VLAN4 内主机（Host3、Host4）互相 ping 不通。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 2
#
interface Vlanif2
 ip address 10.10.10.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 2 to 4
#
vlan 2
 mux-vlan
 subordinate separate 4
 subordinate group 3
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 2
 port mux-vlan enable vlan 2
```

```
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 2 to 4
#
vlan 2
 mux-vlan
 subordinate separate 4
 subordinate group 3
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 2 to 4
#
interface 10GE1/0/2
 port default vlan 3
 port mux-vlan enable vlan 3
#
interface 10GE1/0/3
 port default vlan 3
 port mux-vlan enable vlan 3
#
return
```

DeviceD

```
#
sysname DeviceD
#
vlan batch 2 to 4
#
vlan 2
```

```

mux-vlan
subordinate separate 4
subordinate group 3
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 4
#
interface 10GE1/0/2
port default vlan 4
port mux-vlan enable vlan 4
#
interface 10GE1/0/3
port default vlan 4
port mux-vlan enable vlan 4
#
return

```

1.1.5.6.3.9 举例：配置基本 QinQ

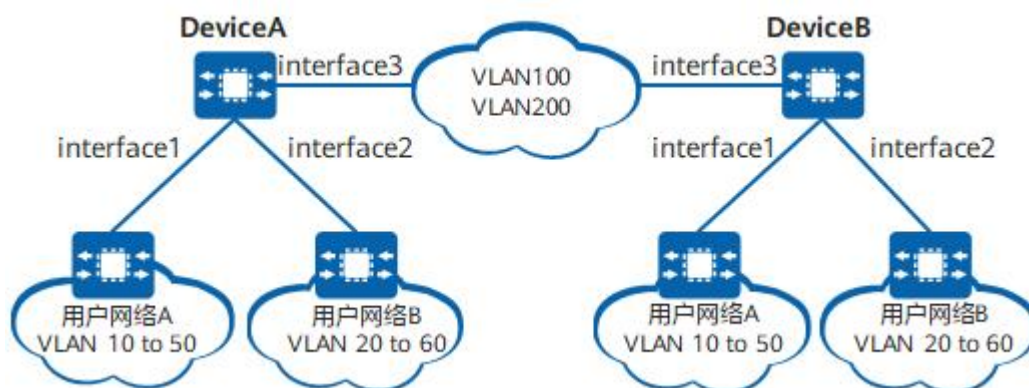
组网需求

如图 1 所示，DeviceA 和 DeviceB 下连接用户网络 A 和用户网络 B，且 DeviceA 和 DeviceB 分布在不同的地域。DeviceA 和 DeviceB 之间通过公网相连。公网划分给用户网络 A 的 VLAN 为 100，划分给用户网络 B 的 VLAN 为 200。用户希望在 DeviceA 和 DeviceB 上部署基本 QinQ 功能，实现用户网络 A 和用户网络 B 独立划分 VLAN，互不影响；不同地域间用户网络 A 内的用户能够互通，不同地域间用户网络 B 内的用户能够互通，不同地域间用户网络 A 和用户网络 B 内的用户相互隔离。

图 1 配置基本 QinQ 组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 创建 VLAN。

在 DeviceA 上创建 VLAN100 和 VLAN200

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 100 200
```

在 DeviceB 上创建 VLAN100 和 VLAN200

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 100 200
```

2. 在 DeviceA 上配置接口 10GE1/0/1、10GE1/0/2 的类型为 QinQ，10GE1/0/1 的外层 tag 为 VLAN100，10GE1/0/2 的外层 tag 为 VLAN200。DeviceB 的配置与 DeviceA 类似，不再赘述。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type dot1q-tunnel
[DeviceA-10GE1/0/1] port default vlan 100
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type dot1q-tunnel
[DeviceA-10GE1/0/2] port default vlan 200
[DeviceA-10GE1/0/2] quit
```

3. 在 DeviceA 上配置接口 10GE1/0/3 加入 VLAN100 和 VLAN200。DeviceB 的配置与 DeviceA 类似，不再赘述。

```
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 100 200
[DeviceA-10GE1/0/3] quit
```

检查配置结果

DeviceA 下用户网络 A 内的任一主机 ping 同一 VLAN 内 DeviceB 下用户网络 A 内的主机，可以 ping 通。

DeviceA 下用户网络 B 内的任一主机 ping 同一 VLAN 内 DeviceB 下用户网络 B 内的主机，可以 ping 通。

DeviceA 下用户网络 A 内的任一主机 ping 同一 VLAN 内 DeviceB 下用户网络 B 内的主机，不能 ping 通。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 100 200
#
interface 10GE1/0/1
port link-type dot1q-tunnel
port default vlan 100
#
interface 10GE1/0/2
port link-type dot1q-tunnel
port default vlan 200
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 100 200
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 100 200
#
interface 10GE1/0/1
port link-type dot1q-tunnel
port default vlan 100
#
interface 10GE1/0/2
port link-type dot1q-tunnel
port default vlan 200
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 100 200
#
return
```

1.1.5.6.3.10 举例：配置基于 VLAN ID 的灵活 QinQ

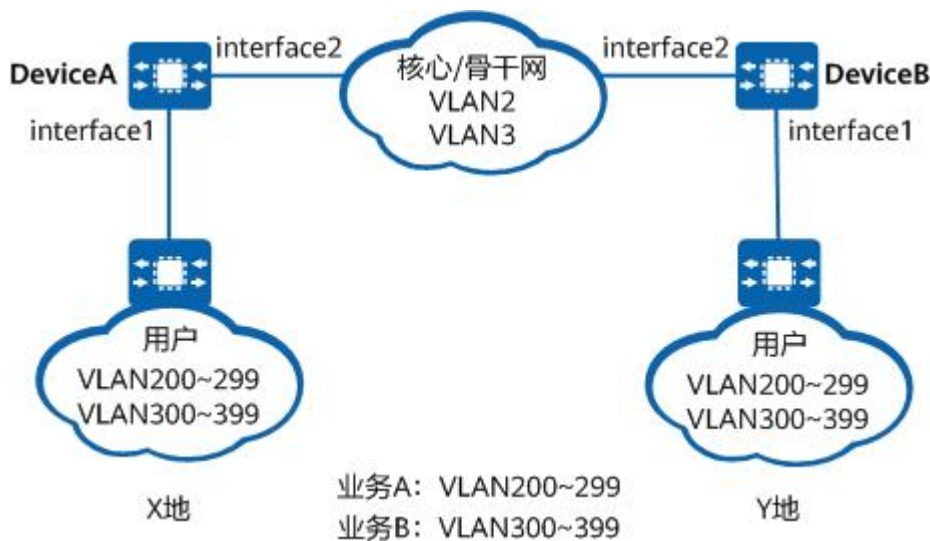
组网需求

如图 1 配置基于 VLAN ID 的灵活 QinQ 组网图所示，X 地中的用户业务中包括业务 A 和业务 B，Y 地类似。其中，两地的业务 A 属于同一 VLAN 范围，业务 B 属于同一 VLAN 范围。为了保证各业务之间的安全性和节省核心/骨干网 VLAN ID，要求两地的流量通过核心/骨干网透明传输，相同业务之间可以互通，不同业务之间相互隔离。

图 1 配置基于 VLAN ID 的灵活 QinQ 组网图

说明

本例中 interface1、interface2 分别代表 10GE1/0/1、10GE1/0/2。



操作步骤

1. 创建 VLAN

在 DeviceA 的接口 10GE1/0/1 上创建 VLAN2、VLAN3，即需要添加的外层 VLAN。DeviceB 的配置与 DeviceA 类似，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 2 3
```

2. 创建 VLAN 并将入接口加入 VLAN。

在 DeviceA 的接口 10GE1/0/1 上配置灵活 QinQ 功能。DeviceB 的配置与 DeviceA 类似，不再赘述。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type hybrid
[DeviceA-10GE1/0/1] port hybrid untagged vlan 2 3
[DeviceA-10GE1/0/1] port vlan-stacking vlan 200 to 299 stack-vlan 2
```

```
[DeviceA-10GE1/0/1] port vlan-stacking vlan 300 to 399 stack-vlan 3
[DeviceA-10GE1/0/1] quit
```

3. 配置出接口加入外层 VLAN。

在 DeviceA 上配置 10GE1/0/2 允许 VLAN2 和 VLAN3 报文通过。DeviceB 的配置与 DeviceA 类似，不再赘述。

```
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 2 3
[DeviceA-10GE1/0/2] quit
```

检查配置结果

从 X 地用户 VLAN200 ~ VLAN299 的一台 A 业务服务器 ping Y 地用户同一 VLAN 内的 A 业务服务器，可以 ping 通则表示租户内部 A 业务服务器可以互相通信。

从 X 地用户 VLAN300 ~ VLAN399 的一台 B 业务服务器 ping Y 地用户同一 VLAN 内的 B 业务服务器，可以 ping 通则表示租户内部 B 业务服务器可以互相通信。

从 X 地用户 VLAN200 ~ VLAN299 的一台 A 业务服务器 ping Y 地用户内 VLAN300 ~ VLAN399 的 B 业务服务器，不能 ping 通，则表示不同业务之间是互相隔离的。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 2 3
#
interface 10GE1/0/1
port link-type hybrid
port hybrid untagged vlan 2 3
port vlan-stacking vlan 200 to 299 stack-vlan 2
port vlan-stacking vlan 300 to 399 stack-vlan 3
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 3
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 2 3
#
interface 10GE1/0/1
port link-type hybrid
port hybrid untagged vlan 2 3
port vlan-stacking vlan 200 to 299 stack-vlan 2
port vlan-stacking vlan 300 to 399 stack-vlan 3
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 3
#
return
```

1.1.5.6.3.11 举例：配置基于 MQC 的灵活 QinQ

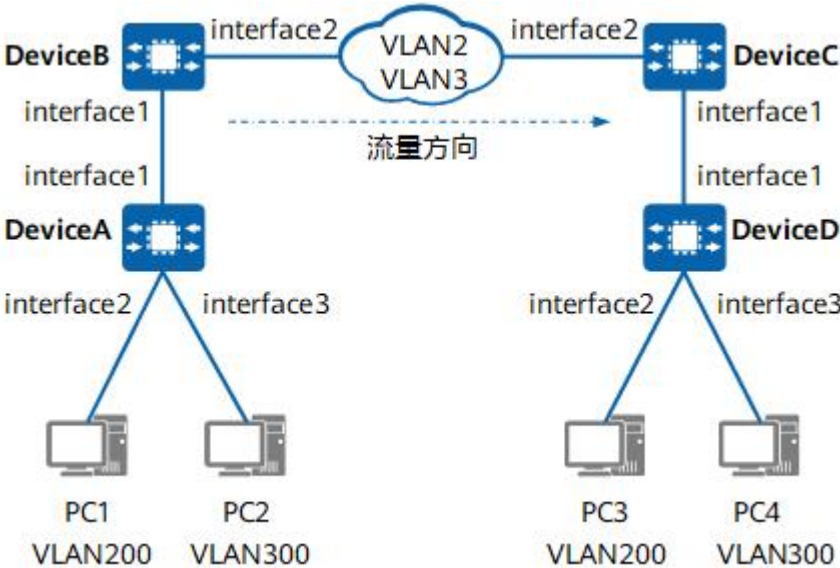
组网需求

如图 1 所示，DeviceA 下连接的 PC1 属于 VLAN200，PC2 属于 VLAN300；DeviceD 下连接的 PC3 属于 VLAN200，PC4 属于 VLAN300。PC1 与 PC3 属于同一网段，PC2 与 PC4 属于同一网段。DeviceB 与 DeviceC 之间的网络规划 VLAN2 给 PC1 和 PC3 用，规划 VLAN3 给 PC2 和 PC4 用。希望在 DeviceB 上配置基于 MQC 的灵活 QinQ 功能，实现 PC1 能够单向访问 PC3，PC2 能够单向访问 PC4。

图 1 配置基于 MQC 的灵活 QinQ 组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 创建 VLAN 并将接口加入 VLAN。

在 DeviceA 上创建 VLAN200、VLAN300，并将接口 10GE1/0/2 加入 VLAN200，10GE1/0/3 加入 VLAN300，10GE1/0/1 允许 VLAN200 和 VLAN300 的报文通过。DeviceD 的配置与 DeviceA 相同，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 200 300
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 200 300
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 200
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 300
[DeviceA-10GE1/0/3] quit
```

在 DeviceB 上创建 VLAN2、VLAN3，即需要添加的外层 VLAN；并配置接口 10GE1/0/1 和 10GE1/0/2 允许 VLAN2 和 VLAN3 报文通过。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 2 3
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 2 3
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 2 3
[DeviceB-10GE1/0/2] quit
```

在 DeviceC 上创建 VLAN2、VLAN3，并配置接口 10GE1/0/1 和 10GE1/0/2 允许 VLAN2 和 VLAN3 报文通过。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 2 3
[DeviceC] interface 10ge 1/0/1
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] port link-type hybrid
[DeviceC-10GE1/0/1] port hybrid untagged vlan 2 3
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] port link-type hybrid
[DeviceC-10GE1/0/2] port hybrid untagged vlan 2 3
[DeviceC-10GE1/0/2] quit

```

2. 配置流分类、流行为、流策略。

在 DeviceB 上配置流分类、流行为、流策略，在 VLAN200 报文的外层添加 VLAN2，在 VLAN300 报文的外层添加 VLAN3。

```

[DeviceB] traffic classifier name1
[DeviceB-classifier-name1] if-match vlan 200
[DeviceB-classifier-name1] quit
[DeviceB] traffic behavior name1
[DeviceB-behavior-name1] vlan-stacking vlan 2
[DeviceB-behavior-name1] quit
[DeviceB] traffic classifier name2
[DeviceB-classifier-name2] if-match vlan 300
[DeviceB-classifier-name2] quit
[DeviceB] traffic behavior name2
[DeviceB-behavior-name2] vlan-stacking vlan 3
[DeviceB-behavior-name2] quit
[DeviceB] traffic policy name1
[DeviceB-trafficpolicy-name1] classifier name1 behavior name1
[DeviceB-trafficpolicy-name1] classifier name2 behavior name2
[DeviceB-trafficpolicy-name1] quit

```

3. 在接口上应用流策略。

在 DeviceB 的接口 10GE1/0/1 上应用流策略。

```

[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] traffic-policy name1 inbound
[DeviceB-10GE1/0/1] quit

```

检查配置结果

配置完成后 PC1 能够访问 PC3；PC2 能够访问 PC4。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 200 300
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 200 300
#
interface 10GE1/0/2
port default vlan 200
#
interface 10GE1/0/3
port default vlan 300
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 2 to 3
#
traffic classifier name1 type or
if-match vlan 200
#
traffic classifier name2 type or
if-match vlan 300
#
traffic behavior name1
vlan-stacking vlan 2
#
traffic behavior name2
vlan-stacking vlan 3
#
traffic policy name1
classifier name1 behavior name1 precedence 5
classifier name2 behavior name2 precedence 10
#
interface 10GE1/0/1
```

```
port link-type trunk
port trunk allow-pass vlan 2 to 3
traffic-policy name1 inbound
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 2 to 3
#
interface 10GE1/0/1
port link-type hybrid
port hybrid untagged vlan 2 to 3
#
interface 10GE1/0/2
port link-type hybrid
port hybrid untagged vlan 2 to 3
#
return
```

DeviceD

```
#
sysname DeviceD
#
vlan batch 200 300
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 200 300
#
interface 10GE1/0/2
port default vlan 200
#
interface 10GE1/0/3
port default vlan 300
#
return
```

1.1.5.6.4 STP/RSTP/MSTP

举例：配置 STP 功能

举例：配置 RSTP 功能

举例：配置 MSTP 功能

举例：配置 MSTP+VRRP 组合组网

1.1.5.6.4.1 举例：配置 STP 功能

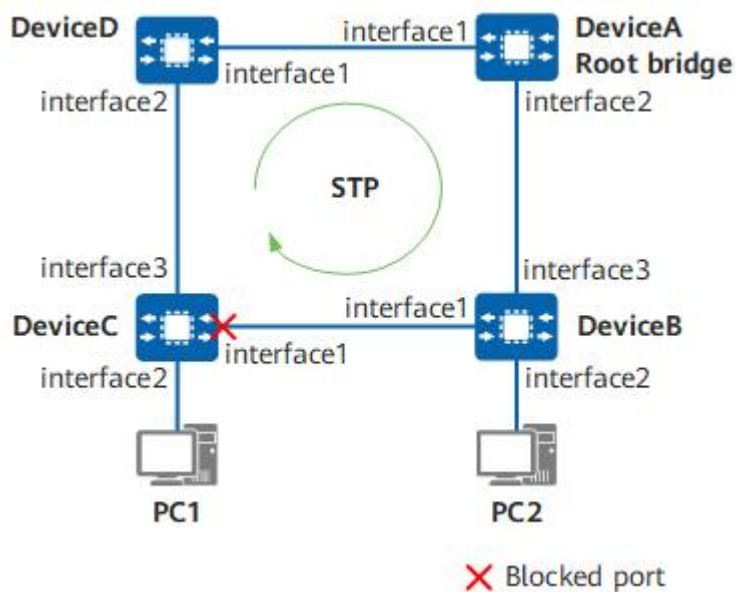
组网需求

如图 1 所示，网络中 DeviceA、DeviceB、DeviceC 和 DeviceD 之间存在环路。用户希望在网络中部署 STP，破除网络环路，从而避免广播风暴和 MAC 表振荡。

图 1 配置 STP 功能组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 配置生成树协议工作在 STP 模式。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stp mode stp
<HUAWEI> system-view
```

```
[HUAWEI] sysname DeviceB
[DeviceB] stp mode stp
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] stp mode stp
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] stp mode stp
```

2. 配置根桥和备份根桥。一般将网络中性能高、网络层次高的设备指定为根桥和备份根桥。

配置 DeviceA 为根桥。

```
[DeviceA] stp root primary
```

配置 DeviceB 为备份根桥。

```
[DeviceB] stp root secondary
```

3. 配置网络中所有设备使用相同的端口路径开销计算方法；并配置 DeviceC 上 10GE1/0/1 的端口路径开销值，实现将该端口阻塞。

配置 DeviceA 的端口路径开销的计算方法为华为私有计算方法。

```
[DeviceA] stp pathcost-standard legacy
```

配置 DeviceB 的端口路径开销的计算方法为华为私有计算方法。

```
[DeviceB] stp pathcost-standard legacy
```

配置 DeviceC 的端口路径开销的计算方法为华为私有计算方法；并配置 DeviceC 上 10GE1/0/1 的端口路径开销值为 20000，使该端口的路径开销大于其他接口，从而实现将该端口阻塞。

```
[DeviceC] stp pathcost-standard legacy
[DeviceC] interface 10ge 1/0/1
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] stp cost 20000
[DeviceC-10GE1/0/1] quit
```

配置 DeviceD 的端口路径开销的计算方法为华为私有计算方法。

```
[DeviceD] stp pathcost-standard legacy
```

4. 设备 DeviceB 和 DeviceC 与 PC 相连的端口上去使能 STP 功能。

DeviceB 的端口 10GE1/0/2 上去使能 STP 功能。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] stp disable
[DeviceB-10GE1/0/2] quit
```

DeviceC 的端口 10GE1/0/2 上去使能 STP 功能。

```
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] stp disable
```

```
[DeviceC-10GE1/0/2] quit
```

5. 启用 STP。

缺省情况下，设备上生成树协议处于使能状态，无需操作。在系统视图下执行命令 **stp enable** 可以启用 STP 功能。

检查配置结果

一段时间生成树协议计算稳定后，执行以下操作，验证配置结果。

在 DeviceA 上执行命令 **display stp brief**，查看端口角色和端口状态。根桥 DeviceA 上 10GE1/0/1 和 10GE1/0/2 为指定端口，处于 forwarding 状态。

```
[DeviceA] display stp brief
```

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	DESI	forwarding	none	2	disable
0	10GE1/0/2	DESI	forwarding	none	2	disable

在 DeviceB 上执行命令 **display stp interface brief**，查看 10GE1/0/1 的端口角色和端口状态。DeviceB 上 10GE1/0/1 为指定端口，处于 forwarding 状态。

```
[DeviceB] display stp interface 10ge 1/0/1 brief
```

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	DESI	forwarding	none	2	disable

在 DeviceC 上执行命令 **display stp brief**，查看端口角色和端口状态。DeviceC 上 10GE1/0/1 为 Alternate 端口，处于 discarding 状态；10GE1/0/3 为根端口，处于 forwarding 状态。

```
[DeviceC] display stp brief
```

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	ALTE	discarding	none	20000	disable
0	10GE1/0/3	ROOT	forwarding	none	2	disable

配置脚本

DeviceA

```
#
sysname DeviceA
#
stp mode stp
stp instance 0 root primary
stp pathcost-standard legacy
#
return
```

DeviceB

```
#
sysname DeviceB
```

```
#
stp mode stp
stp instance 0 root secondary
stp pathcost-standard legacy
#
interface 10GE1/0/2

    stp disable
#
return
```

DeviceC

```
#
sysname DeviceC
#
stp mode stp
stp pathcost-standard legacy
#
interface 10GE1/0/1
    stp instance 0 cost 20000
#
interface 10GE1/0/2
    stp disable
#
return
```

DeviceD

```
#
sysname DeviceD
#
stp mode stp
stp pathcost-standard legacy
#
return
```

1.1.5.6.4.2 举例：配置 RSTP 功能

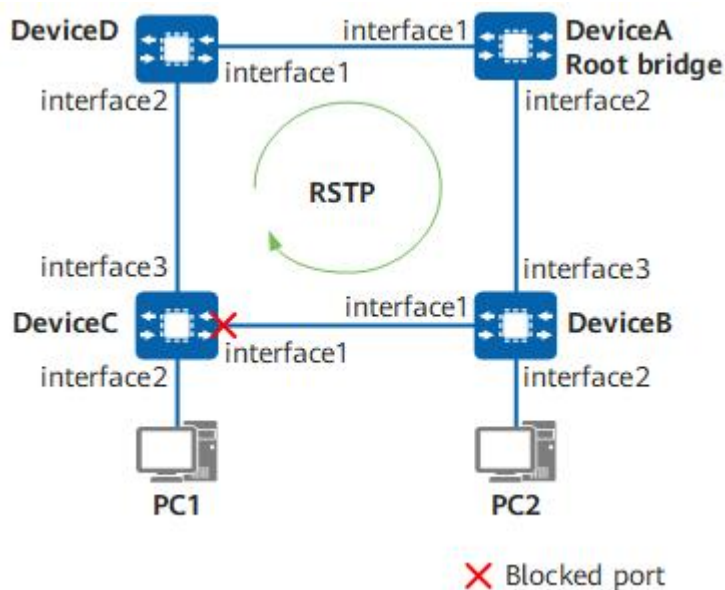
组网需求

如[图 1](#)所示，网络中 DeviceA、DeviceB、DeviceC 和 DeviceD 之间存在环路。用户希望在网络中部署 RSTP，破除网络环路，从而避免广播风暴和 MAC 表振荡。

图 1 配置 RSTP 功能组网图

说明

本例中 interface1、interface2、interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 配置生成树协议工作在 RSTP 模式。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stp mode rstp
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] stp mode rstp
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] stp mode rstp
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] stp mode rstp
```

2. 配置根桥和备份根桥。一般将网络中性能高、网络层次高的设备指定为根桥和备份根桥。

配置 DeviceA 为根桥。

```
[DeviceA] stp root primary
```

配置 DeviceB 为备份根桥。

```
[DeviceB] stp root secondary
```

3. 配置网络中所有设备使用相同的端口路径开销计算方法；并配置 DeviceC 上 10GE1/0/1 的端口路径开销值，实现将该端口阻塞。

配置 DeviceA 的端口路径开销计算方法为华为私有计算方法。

```
[DeviceA] stp pathcost-standard legacy
```

配置 DeviceB 的端口路径开销计算方法为华为私有计算方法。

```
[DeviceB] stp pathcost-standard legacy
```

配置 DeviceC 的端口路径开销计算方法为华为私有计算方法；配置 DeviceC 端口 10GE1/0/1 端口路径开销值为 20000，使该端口的路径开销大于其他接口，从而实现将该端口阻塞。

```
[DeviceC] stp pathcost-standard legacy
```

```
[DeviceC] interface 10ge 1/0/1
```

```
[DeviceC-10GE1/0/1] portswitch
```

```
[DeviceC-10GE1/0/1] stp cost 20000
```

```
[DeviceC-10GE1/0/1] quit
```

配置 DeviceD 的端口路径开销计算方法为华为私有计算方法。

```
[DeviceD] stp pathcost-standard legacy
```

4. 配置设备 DeviceB 和 DeviceC 与 PC 相连的端口为边缘端口。

DeviceB 端口 10GE1/0/2 配置为边缘端口，并配置 BPDU 保护功能。

```
[DeviceB] interface 10ge 1/0/2
```

```
[DeviceB-10GE1/0/2] portswitch
```

```
[DeviceB-10GE1/0/2] stp edged-port enable
```

```
[DeviceB-10GE1/0/2] quit
```

```
[DeviceB] stp bpdu-protection
```

DeviceC 端口 10GE1/0/2 配置为边缘端口，并配置 BPDU 保护功能。

```
[DeviceC] interface 10ge 1/0/2
```

```
[DeviceC-10GE1/0/2] portswitch
```

```
[DeviceC-10GE1/0/2] stp edged-port enable
```

```
[DeviceC-10GE1/0/2] quit
```

```
[DeviceC] stp bpdu-protection
```

5. 启用 RSTP。

缺省情况下，设备上生成树协议处于使能状态，无需操作。在系统视图下执行命令 **stp enable** 可以启用 RSTP 功能。

6. 在根桥 DeviceA 的指定端口 10GE1/0/1 和 10GE1/0/2 上配置根保护功能。

```
[DeviceA] interface 10ge 1/0/1
```

```
[DeviceA-10GE1/0/1] portswitch
```

```
[DeviceA-10GE1/0/1] stp root-protection
```

```
[DeviceA-10GE1/0/1] quit
```

```
[DeviceA] interface 10ge 1/0/2
```

```
[DeviceA-10GE1/0/2] portswitch
```

```
[DeviceA-10GE1/0/2] stp root-protection
```

```
[DeviceA-10GE1/0/2] quit
```

检查配置结果

一段时间生成树协议计算稳定后，执行以下操作，验证配置结果。

在 DeviceA 上执行命令 **display stp brief**，查看端口状态和端口的保护类型。根桥 DeviceA 的 10GE1/0/1 和 10GE1/0/2 为指定端口，并配置了根保护功能。

[DeviceA] display stp brief

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	DESI	forwarding	root	2	disable
0	10GE1/0/2	DESI	forwarding	root	2	disable

在 DeviceB 上执行命令 **display stp interface brief**，查看 10GE1/0/1 的端口角色和端口状态。DeviceB 上 10GE1/0/1 为指定端口，处于 forwarding 状态。

[DeviceB] display stp interface 10ge 1/0/1 brief

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	DESI	forwarding	none	2	disable

在 DeviceC 上执行命令 **display stp brief**，查看端口角色和端口状态。DeviceC 上 10GE1/0/1 为 Alternate 端口，处于 discarding 状态；10GE1/0/3 为根端口，处于 forwarding 状态。

[DeviceC] display stp brief

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	ALTE	discarding	none	20000	disable
0	10GE1/0/3	ROOT	forwarding	none	2	disable

配置脚本

DeviceA

```
#
sysname DeviceA
#
stp mode rstp
stp instance 0 root primary
stp pathcost-standard legacy
#
interface 10GE1/0/1
  stp root-protection
#
interface 10GE1/0/2
  stp root-protection
#
return
```

DeviceB

```
#
```

```
sysname DeviceB
#
stp mode rstp
stp bpdu-protection
stp instance 0 root secondary
stp pathcost-standard legacy
#
interface 10GE1/0/2
    stp edged-port enable
#
return
```

DeviceC

```
#
sysname DeviceC
#
stp mode rstp
stp bpdu-protection
stp pathcost-standard legacy
#
interface 10GE1/0/1
    stp instance 0 cost 20000
#
interface 10GE1/0/2
    stp edged-port enable
#
return
```

DeviceD

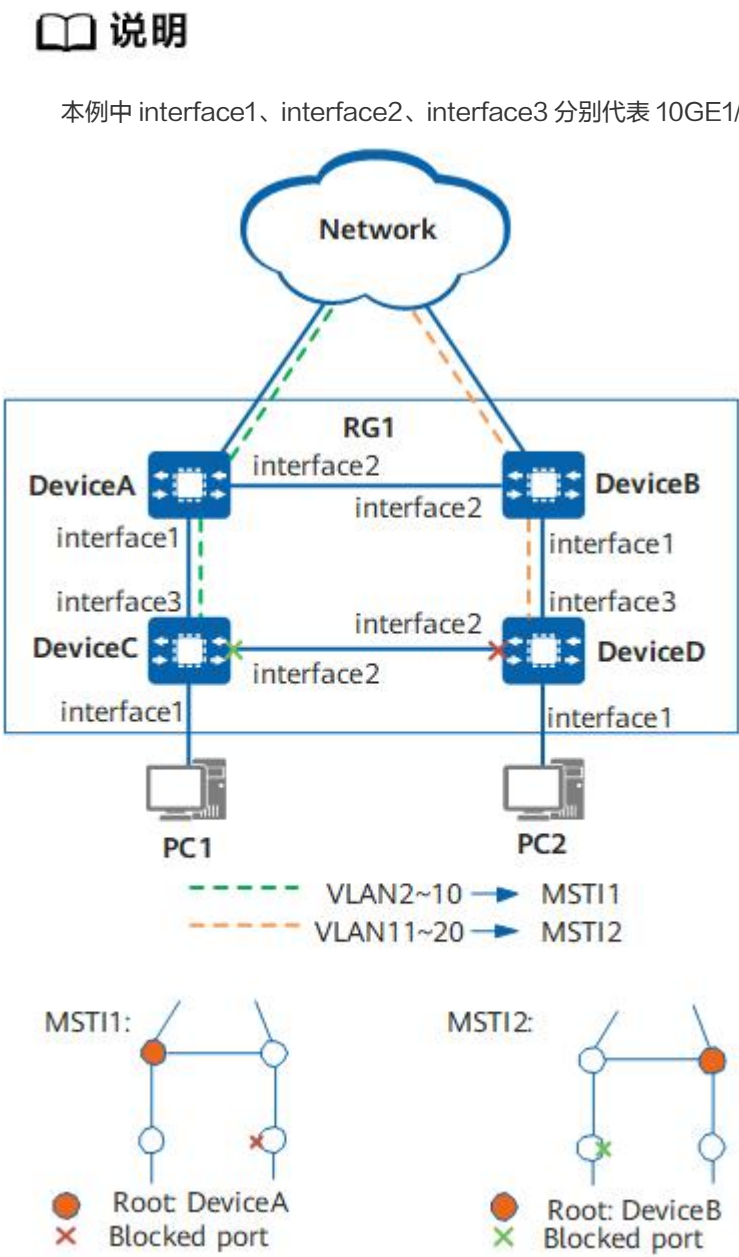
```
#
sysname DeviceD
#
stp mode rstp
stp pathcost-standard legacy
#
return
```

1.1.5.6.4.3 举例：配置 MSTP 功能

组网需求

如图 1 所示，网络中 DeviceA、DeviceB、DeviceC 和 DeviceD 之间存在环路。用户希望在网络中部署 MSTP，破除网络环路，从而避免广播风暴和 MAC 表振荡；并且实现 VLAN2~VLAN10 和 VLAN11~VLAN20 的流量负载分担。

图 1 配置 MSTP 功能组网图



操作步骤

1. 配置 DeviceA、DeviceB、DeviceC 和 DeviceD 到域名为 RG1 的域内，创建实例 MSTI1 和实例 MSTI2。

说明

当两台设备的 MST 域的域名、实例和 VLAN 的映射关系、MST 域的修订级别都相同时，这两台设备属于同一个 MST 域。

不能将同一个 VLAN 映射到多个不同的实例上。如果将一个已经和实例建立映射关系的 VLAN 又映射到另一个实例上，原来的映射关系将被取消。

在 DeviceA 上配置 MST 域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name RG1
[DeviceA-mst-region] instance 1 vlan 2 to 10
[DeviceA-mst-region] instance 2 vlan 11 to 20
[DeviceA-mst-region] quit
```

在 DeviceB 上配置 MST 域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name RG1
[DeviceB-mst-region] instance 1 vlan 2 to 10
[DeviceB-mst-region] instance 2 vlan 11 to 20
[DeviceB-mst-region] quit
```

在 DeviceC 上配置 MST 域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name RG1
[DeviceC-mst-region] instance 1 vlan 2 to 10
[DeviceC-mst-region] instance 2 vlan 11 to 20
[DeviceC-mst-region] quit
```

在 DeviceD 上配置 MST 域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] stp region-configuration
[DeviceD-mst-region] region-name RG1
[DeviceD-mst-region] instance 1 vlan 2 to 10
[DeviceD-mst-region] instance 2 vlan 11 to 20
[DeviceD-mst-region] quit
```

2. 在 MST 域 RG1 内，分别配置 MSTI1、MSTI2 的根桥和备份根桥。

配置 DeviceA 为 MSTI1 的根桥。

```
[DeviceA] stp instance 1 root primary
```

配置 DeviceB 为 MSTI1 的备份根桥。

```
[DeviceB] stp instance 1 root secondary
```

配置 DeviceB 为 MSTI2 的根桥。

```
[DeviceB] stp instance 2 root primary
```

配置 DeviceA 为 MSTI2 的备份根桥。

```
[DeviceA] stp instance 2 root secondary
```

3. 配置同一网络内所有设备的端口路径开销应使用相同的计算方法；配置实例 MSTI1 和 MSTI2 中将要被阻塞端口的路径开销值大于缺省值。

配置 DeviceA 的端口路径开销计算方法为华为计算方法。

```
[DeviceA] stp pathcost-standard legacy
```

配置 DeviceB 的端口路径开销计算方法为华为计算方法。

```
[DeviceB] stp pathcost-standard legacy
```

配置 DeviceC 的端口路径开销计算方法为华为计算方法，将端口 10GE1/0/2 在实例 MSTI2 中的路径开销值配置为 20000。

```
[DeviceC] stp pathcost-standard legacy
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] stp instance 2 cost 20000
[DeviceC-10GE1/0/2] quit
```

配置 DeviceD 的端口路径开销计算方法为华为计算方法，将端口 10GE1/0/2 在实例 MSTI1 中的路径开销值配置为 20000。

```
[DeviceD] stp pathcost-standard legacy
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] portswitch
[DeviceD-10GE1/0/2] stp instance 1 cost 20000
[DeviceD-10GE1/0/2] quit
```

4. 设备全局启用 MSTP。

缺省情况下，设备上生成树协议处于使能状态，无需操作。在系统视图下执行命令 **stp enable** 可以启用 MSTP 功能。

5. 在设备与终端相连的端口上去使能 MSTP。

在 DeviceC 端口 10GE1/0/1 上去使能 MSTP 功能。

```
[DeviceC] interface 10ge 1/0/1
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] stp disable
[DeviceC-10GE1/0/1] quit
```

在 DeviceD 端口 10GE1/0/1 上去使能 MSTP 功能。

```
[DeviceD] interface 10ge 1/0/1
[DeviceD-10GE1/0/1] portswitch
[DeviceD-10GE1/0/1] stp disable
[DeviceD-10GE1/0/1] quit
```

6. 配置保护功能，如在各实例的根桥设备的指定端口配置根保护功能。

在 DeviceA 端口 10GE1/0/1 上启动根保护。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] stp root-protection
[DeviceA-10GE1/0/1] quit
```

在 DeviceB 端口 10GE1/0/1 上启动根保护。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] stp root-protection
[DeviceB-10GE1/0/1] quit
```

7. 创建 VLAN 并将接口加入 VLAN。

在 DeviceA 上创建 VLAN2~20，并将 DeviceA 的端口 10GE1/0/1 和 10GE1/0/2 分别加入 VLAN。

```
[DeviceA] vlan batch 2 to 20
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 2 to 20
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 2 to 20
[DeviceA-10GE1/0/2] quit
```

在 DeviceB 上创建 VLAN2~20，并将 DeviceB 的端口 10GE1/0/1 和 10GE1/0/2 分别加入 VLAN。

```
[DeviceB] vlan batch 2 to 20
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 2 to 20
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 2 to 20
[DeviceB-10GE1/0/2] quit
```

在 DeviceC 上创建 VLAN2~20，并将 DeviceC 的端口 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 分别加入 VLAN。

```
[DeviceC] vlan batch 2 to 20
[DeviceC] interface 10ge 1/0/1
```



```
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] port link-type access
[DeviceC-10GE1/0/1] port default vlan 2
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] port link-type trunk
[DeviceC-10GE1/0/2] port trunk allow-pass vlan 2 to 20
[DeviceC-10GE1/0/2] quit
[DeviceC] interface 10ge 1/0/3
[DeviceC-10GE1/0/3] portswitch
[DeviceC-10GE1/0/3] port link-type trunk
[DeviceC-10GE1/0/3] port trunk allow-pass vlan 2 to 20
[DeviceC-10GE1/0/3] quit
```

在 DeviceD 上创建 VLAN2 ~ 20，并将 DeviceD 的端口 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 分别加入 VLAN。

```
[DeviceD] vlan batch 2 to 20
[DeviceD] interface 10ge 1/0/1
[DeviceD-10GE1/0/1] portswitch
[DeviceD-10GE1/0/1] port link-type access
[DeviceD-10GE1/0/1] port default vlan 11
[DeviceD-10GE1/0/1] quit
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] portswitch
[DeviceD-10GE1/0/2] port link-type trunk
[DeviceD-10GE1/0/2] port trunk allow-pass vlan 2 to 20
[DeviceD-10GE1/0/2] quit
[DeviceD] interface 10ge 1/0/3
[DeviceD-10GE1/0/3] portswitch
[DeviceD-10GE1/0/3] port link-type trunk
[DeviceD-10GE1/0/3] port trunk allow-pass vlan 2 to 20
[DeviceD-10GE1/0/3] quit
```

检查配置结果

在网络计算稳定后，执行以下操作，验证配置结果。本配置举例以实例 1 和实例 2 为例，因此不用关注实例 0 中端口的状态。

在 DeviceA 上执行命令 **display stp brief**，查看端口角色和端口状态。在 MSTI1 中，由于 DeviceA 是根桥，DeviceA 的端口 10GE1/0/2 和 10GE1/0/1 成为指定端口。在 MSTI2 中，DeviceA 的端口 10GE1/0/1 成为指定端口，端口 10GE1/0/2 成为根端口。

```
[DeviceA] display stp brief
```

MSTID	Port	Role	STP State	Protection	Cost	Edged

0	10GE1/0/1	DESI forwarding	root	2	disable
0	10GE1/0/2	DESI forwarding	none	2	disable
1	10GE1/0/1	DESI forwarding	root	2	disable
1	10GE1/0/2	DESI forwarding	none	2	disable
2	10GE1/0/1	DESI forwarding	root	2	disable
2	10GE1/0/2	ROOT forwarding	none	2	disable

在 DeviceB 上执行命令 **display stp brief**，查看端口角色和端口状态。在 MSTI2 中，由于 DeviceB 是根桥，端口 10GE1/0/1 和 10GE1/0/2 在 MSTI2 中成为指定端口。在 MSTI1 中，DeviceB 的端口 10GE1/0/1 成为指定端口，端口 10GE1/0/2 成为根端口。

[DeviceB] **display stp brief**

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	DESI forwarding	root	2	disable	
0	10GE1/0/2	ROOT forwarding	none	2	disable	
1	10GE1/0/1	DESI forwarding	root	2	disable	
1	10GE1/0/2	ROOT forwarding	none	2	disable	
2	10GE1/0/1	DESI forwarding	root	2	disable	
2	10GE1/0/2	DESI forwarding	none	2	disable	

在 DeviceC 上执行命令 **display stp interface brief**，查看端口角色和端口状态。DeviceC 的端口 10GE1/0/3 在 MSTI1 和 MSTI2 中为根端口。DeviceC 的另一个端口 10GE1/0/2，在 MSTI2 中被阻塞，在 MSTI1 中被计算为指定端口。

[DeviceC] **display stp interface 10ge 1/0/3 brief**

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/3	ROOT forwarding	none	2	disable	
1	10GE1/0/3	ROOT forwarding	none	2	disable	
2	10GE1/0/3	ROOT forwarding	none	2	disable	

[DeviceC] **display stp interface 10ge 1/0/2 brief**

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/2	DESI forwarding	none	2	disable	
1	10GE1/0/2	DESI forwarding	none	2	disable	
2	10GE1/0/2	ALTE discarding	none	20000	disable	

在 DeviceD 上执行命令 **display stp interface brief**，查看端口角色和端口状态。DeviceD 的端口 10GE1/0/3 在 MSTI1 和 MSTI2 中为根端口。DeviceD 的另一个端口 10GE1/0/2，在 MSTI1 中被阻塞，在 MSTI2 中被计算为指定端口。

[DeviceD] **display stp interface 10ge 1/0/3 brief**

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/3	ALTE discarding	none	2	disable	
1	10GE1/0/3	ROOT forwarding	none	2	disable	
2	10GE1/0/3	ROOT forwarding	none	2	disable	

[DeviceD] **display stp interface 10ge 1/0/2 brief**

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/2	ROOT forwarding	none	2	disable	

1	10GE1/0/2	ALTE discarding	none	20000	disable
2	10GE1/0/2	DESI forwarding	none	2	disable

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 2 to 20
#
stp instance 1 root primary
stp instance 2 root secondary
stp pathcost-standard legacy
#
stp region-configuration
region-name RG1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 20
stp root-protection
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 20
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 2 to 20
#
stp instance 1 root secondary
stp instance 2 root primary
stp pathcost-standard legacy
#
stp region-configuration
```

```
region-name RG1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 20
stp root-protection
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 20
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 2 to 20
#
stp pathcost-standard legacy
#
stp region-configuration
region-name RG1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
#
interface 10GE1/0/1
port link-type access
port default vlan 2
stp disable
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 20
stp instance 2 cost 20000
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 2 to 20
#
return
```

DeviceD

```
#
sysname DeviceD
#
vlan batch 2 to 20
#
stp pathcost-standard legacy
#
stp region-configuration
region-name RG1
instance 1 vlan 2 to 10
instance 2 vlan 11 to 20
#
interface 10GE1/0/1
port link-type access
port default vlan 11
stp disable
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 20
stp instance 1 cost 20000
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 2 to 20
#
return
```

1.1.5.6.4.4 举例：配置 MSTP+VRRP 组合组网

组网需求

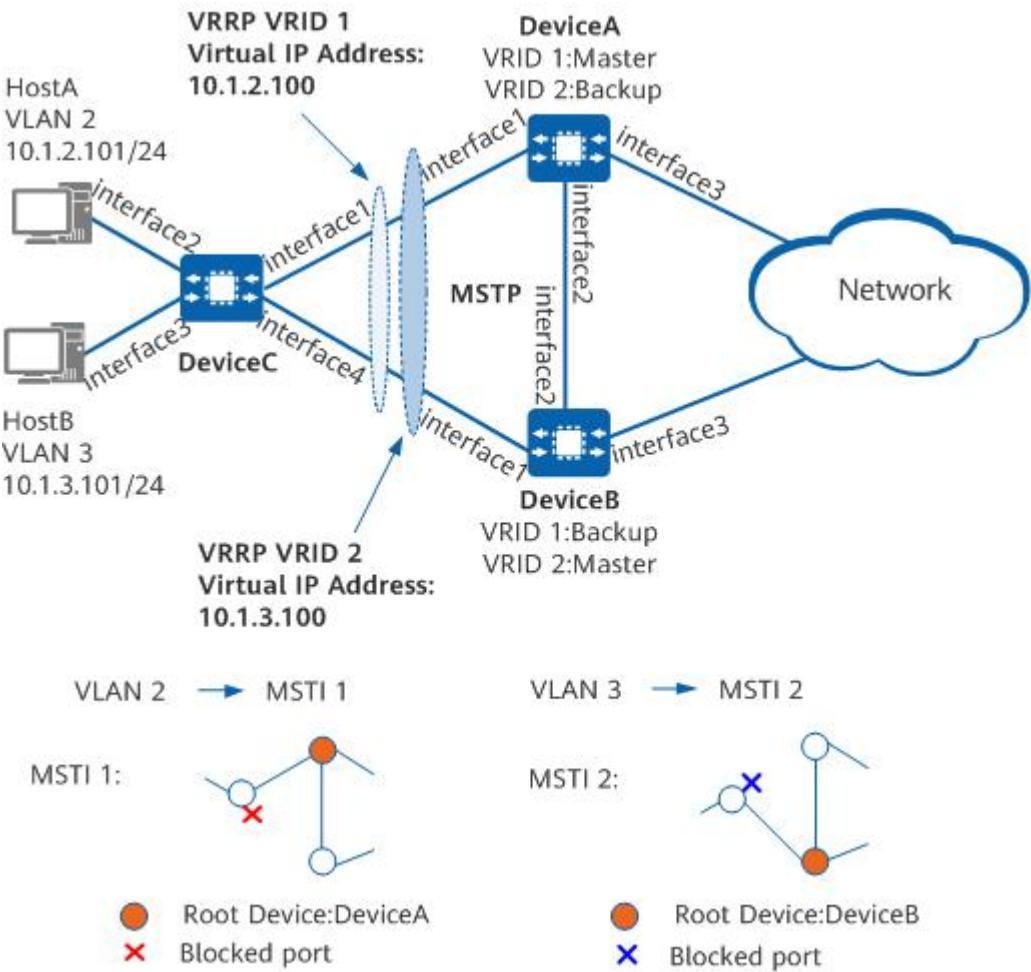
如图 1 所示，主机通过 DeviceC 接入网络，DeviceC 通过双上行连接 DeviceA 和 DeviceB 来接入 Internet。由于接入备份的需要，用户部署了冗余链路。冗余备份链路的存在导致出现环网，可能会引起广播风暴和 MAC 地址表项被破坏。用户希望在存在冗余备份链路的同时消除网络中的环路，在一条上行链路断开的时候，流量能切换到另外一条上行链路转发，还能合理利用网络带宽。

此时可以在网络中部署 MSTP 解决环路问题。MSTP 可阻塞二层网络中的冗余链路，将网络修剪成树状，达到消除环路的目的。同时在 DeviceA 和 DeviceB 上配置 VRRP，HostA 以 DeviceA 为默认网关接入 Internet，DeviceB 作为备份网关；HostB 以 DeviceB 为默认网关接入 Internet，DeviceA 作为备份网关，以实现可靠性及流量的负载分担。

图 1 配置 MSTP+VRRP 组合组网图

说明

本例中 interface1、interface2、interface3 和 interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3 和 10GE1/0/4。



设备	接口	对应的 VLANIF	IP 地址
DeviceA	interface1 和 interface2	VLANIF2	10.1.2.102/24
	interface1 和 interface2	VLANIF3	10.1.3.102/24
	interface3	VLANIF4	10.1.4.102/24
DeviceB	interface1 和 interface2	VLANIF2	10.1.2.103/24
	interface1 和 interface2	VLANIF3	10.1.3.103/24
	interface3	VLANIF5	10.1.5.103/24

配置思路

采用以下思路配置：

1. 在处于环形网络中的设备上配置 MSTP 基本功能，包括：

- a. 配置 MST 域并创建多实例，配置 VLAN2 映射到 MSTI1，VLAN3 映射到 MSTI2，实现流量的负载分担。
- b. 在 MST 域内，配置各实例的根桥与备份根桥。
- c. 配置各实例中某端口的路径开销值，实现将该端口阻塞。
- d. 使能 MSTP，实现破除环路，包括：

设备全局使能 MSTP。

除与终端设备相连的端口外，其他端口使能 MSTP。

说明

与终端相连的端口不用参与 MSTP 计算，建议将其设置为边缘端口。

2. 配置保护功能，实现对设备或链路的保护。例如：在各实例的根桥设备指定端口配置根保护功能。
3. 配置设备的二层转发功能。
4. 配置各设备端口 IP 地址及路由协议，使各设备间网络层连通。
5. 在 DeviceA 和 DeviceB 上创建 VRRP 备份组 1 和 VRRP 备份组 2，在备份组 1 中，配置 DeviceA 为 Master 设备，DeviceB 为 Backup 设备；在备份组 2 中，配置 DeviceB 为 Master 设备，DeviceA 为 Backup 设备，实现流量的负载均衡。

操作步骤

1. 配置 MSTP 基本功能

- a. 配置 DeviceA、DeviceB、DeviceC 到域名为 RG1 的域内，创建实例 MSTI1 和实例 MSTI2
配置 DeviceA 的 MST 域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stp region-configuration
[DeviceA-mst-region] region-name RG1
[DeviceA-mst-region] instance 1 vlan 2
[DeviceA-mst-region] instance 2 vlan 3
[DeviceA-mst-region] quit
```

配置 DeviceB 的 MST 域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] stp region-configuration
[DeviceB-mst-region] region-name RG1
[DeviceB-mst-region] instance 1 vlan 2
[DeviceB-mst-region] instance 2 vlan 3
[DeviceB-mst-region] quit
```

配置 DeviceC 的 MST 域。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] stp region-configuration
[DeviceC-mst-region] region-name RG1
[DeviceC-mst-region] instance 1 vlan 2
[DeviceC-mst-region] instance 2 vlan 3
[DeviceC-mst-region] quit
```

b. 在域 RG1 内，配置 MSTI1 与 MSTI2 的根桥与备份根桥

配置 MSTI1 的根桥与备份根桥

配置 DeviceA 为 MSTI1 的根桥。

```
[DeviceA] stp instance 1 root primary
```

配置 DeviceB 为 MSTI1 的备份根桥。

```
[DeviceB] stp instance 1 root secondary
```

配置 MSTI2 的根桥与备份根桥

配置 DeviceB 为 MSTI2 的根桥。

```
[DeviceB] stp instance 2 root primary
```

配置 DeviceA 为 MSTI2 的备份根桥。

```
[DeviceA] stp instance 2 root secondary
```

c. 配置实例 MSTI1 和 MSTI2 中将要被阻塞端口的路径开销值大于缺省值

说明

端口路径开销值取值范围由路径开销计算方法决定，这里选择使用华为计算方法为例，配置实例 MSTI1 和 MSTI2 中将被阻塞端口的路径开销值为 20000。

同一网络内所有设备的端口路径开销应使用相同的计算方法。

配置 DeviceA 的端口路径开销计算方法为华为计算方法。

```
[DeviceA] stp pathcost-standard legacy
```

配置 DeviceB 的端口路径开销计算方法为华为计算方法。

```
[DeviceB] stp pathcost-standard legacy
```

配置 DeviceC 的端口路径开销计算方法为华为计算方法，将端口 10GE1/0/1 在实例 MSTI2 中的路径开销值配置为 20000，将端口 10GE1/0/4 在实例 MSTI1 中的路径开销值配置为 20000。

```
[DeviceC] stp pathcost-standard legacy
[DeviceC] interface 10ge1/0/1
[DeviceC-10GE1/0/1] stp instance 2 cost 20000
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10ge1/0/4
[DeviceC-10GE1/0/4] stp instance 1 cost 20000
```



```
[DeviceC-10GE1/0/4] quit
```

d. 使能 MSTP，实现破除环路

设备全局使能 MSTP

在 DeviceA 上启动 MSTP。

```
[DeviceA] stp enable
```

在 DeviceB 上启动 MSTP。

```
[DeviceB] stp enable
```

在 DeviceC 上启动 MSTP。

```
[DeviceC] stp enable
```

将与 Host 相连的端口设置为边缘端口

配置 DeviceC 端口的 10GE1/0/2 和 10GE1/0/3 为边缘端口。

```
[DeviceC] interface 10ge1/0/2
```

```
[DeviceC-10GE1/0/2] stp edged-port enable
```

```
[DeviceC-10GE1/0/2] quit
```

```
[DeviceC] interface 10ge1/0/3
```

```
[DeviceC-10GE1/0/3] stp edged-port enable
```

```
[DeviceC-10GE1/0/3] quit
```

(可选) 配置 DeviceC 的 BPDU 保护功能。

```
[DeviceC] stp bpdu-protection
```

将与 Network 相连的端口设置为边缘端口

配置 DeviceA 端口 10GE1/0/3 为边缘端口。

```
[DeviceA] interface 10ge1/0/3
```

```
[DeviceA-10GE1/0/3] stp edged-port enable
```

```
[DeviceA-10GE1/0/3] quit
```

(可选) 配置 DeviceA 的 BPDU 保护功能。

```
[DeviceA] stp bpdu-protection
```

配置 DeviceB 端口 10GE1/0/3 为边缘端口。

```
[DeviceB] interface 10ge1/0/3
```

```
[DeviceB-10GE1/0/3] stp edged-port enable
```

```
[DeviceB-10GE1/0/3] quit
```

(可选) 配置 DeviceB 的 BPDU 保护功能。

```
[DeviceB] stp bpdu-protection
```

说明

如果与边缘端口相连的是使能了 STP 功能的网络设备，配置 BPDU 保护功能后，如果边缘端口收到 BPDU 报文，边缘端口将会被 shutdown，边缘端口属性不变。

2. 配置保护功能，如在各实例的根桥设备的指定端口配置根保护功能

在 DeviceA 端口 10GE1/0/1 上启动根保护。

```
[DeviceA] interface 10ge1/0/1
[DeviceA-10GE1/0/1] stp root-protection
[DeviceA-10GE1/0/1] quit
```

在 DeviceB 端口 10GE1/0/1 上启动根保护。

```
[DeviceB] interface 10ge1/0/1
[DeviceB-10GE1/0/1] stp root-protection
[DeviceB-10GE1/0/1] quit
```

3. 配置处于环网中的设备的二层转发功能

在设备 DeviceA、DeviceB、DeviceC 上创建 VLAN2 ~ 3

在 DeviceA 上创建 VLAN2 ~ 3。

```
[DeviceA] vlan batch 2 to 3
```

在 DeviceB 上创建 VLAN2 ~ 3。

```
[DeviceB] vlan batch 2 to 3
```

在 DeviceC 上创建 VLAN2 ~ 3。

```
[DeviceC] vlan batch 2 to 3
```

将设备上相应的端口加入 VLAN

将 DeviceA 端口 10GE1/0/1 加入 VLAN。

```
[DeviceA] interface 10ge1/0/1
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 2 to 3
[DeviceA-10GE1/0/1] quit
```

将 DeviceA 端口 10GE1/0/2 加入 VLAN。

```
[DeviceA] interface 10ge1/0/2
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 2 to 3
[DeviceA-10GE1/0/2] quit
```

将 DeviceB 端口 10GE1/0/1 加入 VLAN。

```
[DeviceB] interface 10ge1/0/1
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 2 to 3
[DeviceB-10GE1/0/1] quit
```

将 DeviceB 端口 10GE1/0/2 加入 VLAN。

```
[DeviceB] interface 10ge1/0/2
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 2 to 3
```

```
[DeviceB-10GE1/0/2] quit
```

将 DeviceC 端口 10GE1/0/1 加入 VLAN。

```
[DeviceC] interface 10ge1/0/1
[DeviceC-10GE1/0/1] port link-type trunk
[DeviceC-10GE1/0/1] port trunk allow-pass vlan 2 to 3
[DeviceC-10GE1/0/1] quit
```

将 DeviceC 端口 10GE1/0/2 加入 VLAN。

```
[DeviceC] interface 10ge1/0/2
[DeviceC-10GE1/0/2] port link-type access
[DeviceC-10GE1/0/2] port default vlan 2
[DeviceC-10GE1/0/2] quit
```

将 DeviceC 端口 10GE1/0/3 加入 VLAN。

```
[DeviceC] interface 10ge1/0/3
[DeviceC-10GE1/0/3] port link-type access
[DeviceC-10GE1/0/3] port default vlan 3
[DeviceC-10GE1/0/3] quit
```

将 DeviceC 端口 10GE1/0/4 加入 VLAN。

```
[DeviceC] interface 10ge1/0/4
[DeviceC-10GE1/0/4] port link-type trunk
[DeviceC-10GE1/0/4] port trunk allow-pass vlan 2 to 3
[DeviceC-10GE1/0/4] quit
```

4. 验证配置结果

经过以上配置，在网络计算稳定后，执行以下操作，验证配置结果。

说明

本配置举例以实例 1 和实例 2 为例，因此不用关注实例 0 中端口的状态。

在 DeviceA 上执行 **display stp brief** 命令，查看端口状态和端口的保护类型，结果如下：

```
[DeviceA] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	10GE1/0/1	DESI	FORWARDING	ROOT
0	10GE1/0/2	DESI	FORWARDING	NONE
1	10GE1/0/1	DESI	FORWARDING	ROOT
1	10GE1/0/2	DESI	FORWARDING	NONE
2	10GE1/0/1	DESI	FORWARDING	ROOT
2	10GE1/0/2	ROOT	FORWARDING	NONE

在 MSTI1 中，由于 DeviceA 是根桥，DeviceA 的端口 10GE1/0/1 和 10GE1/0/2 成为指定端口。在 MSTI2 中，DeviceA 的端口 10GE1/0/1 成为指定端口，端口 10GE1/0/2 成为根端口。

在 DeviceB 上执行 **display stp brief** 命令，结果如下：

```
[DeviceB] display stp brief
```

MSTID	Port	Role	STP State	Protection
0	10GE1/0/1	DESI	FORWARDING	ROOT
0	10GE1/0/2	ROOT	FORWARDING	NONE
1	10GE1/0/1	DESI	FORWARDING	ROOT
1	10GE1/0/2	ROOT	FORWARDING	NONE
2	10GE1/0/1	DESI	FORWARDING	ROOT
2	10GE1/0/2	DESI	FORWARDING	NONE

在 MSTI2 中，由于 DeviceB 是根桥，端口 10GE1/0/1 和 10GE1/0/2 在 MSTI2 中成为指定端口。在 MSTI1 中，DeviceB 的端口 10GE1/0/1 成为指定端口，端口 10GE1/0/2 成为根端口。

在 DeviceC 上执行 **display stp interface brief** 命令，结果如下：

[DeviceC] **display stp interface 10ge1/0/1 brief**

MSTID	Port	Role	STP State	Protection
0	10GE1/0/1	ROOT	FORWARDING	NONE
1	10GE1/0/1	ROOT	FORWARDING	NONE
2	10GE1/0/1	ALTE	DISCARDING	NONE

[DeviceC] **display stp interface 10ge1/0/4 brief**

MSTID	Port	Role	STP State	Protection
0	10GE1/0/4	ALTE	DISCARDING	NONE
1	10GE1/0/4	ALTE	DISCARDING	NONE
2	10GE1/0/4	ROOT	FORWARDING	NONE

DeviceC 的端口 10GE1/0/1 在 MSTI1 中为根端口，在 MSTI2 中被阻塞。DeviceC 的另一个端口 10GE1/0/4，在 MSTI1 中被阻塞，在 MSTI2 中为根端口。

5. 配置设备间的网络互连

配置设备各端口的 IP 地址，以 DeviceA 为例。DeviceB 的配置与 DeviceA 类似，详见配置文件。

[DeviceA] **vlan batch 4**

[DeviceA] **interface 10ge1/0/3**

[DeviceA-10GE1/0/3] **port link-type trunk**

[DeviceA-10GE1/0/3] **port trunk allow-pass vlan 4**

[DeviceA-10GE1/0/3] **quit**

[DeviceA] **interface vlanif 2**

[DeviceA-Vlanif2] **ip address 10.1.2.102 24**

[DeviceA-Vlanif2] **quit**

[DeviceA] **interface vlanif 3**

[DeviceA-Vlanif3] **ip address 10.1.3.102 24**

[DeviceA-Vlanif3] **quit**

[DeviceA] **interface vlanif 4**

[DeviceA-Vlanif4] **ip address 10.1.4.102 24**

[DeviceA-Vlanif4] **quit**

配置 DeviceA、DeviceB 和 Network 间采用 OSPF 协议进行互连。以 DeviceA 为例，DeviceB 的配置与 DeviceA 类似，详见配置文件。

[DeviceA] **ospf 1**

```
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.4.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

6. 配置 VRRP 备份组

在 DeviceA 和 DeviceB 上创建 VRRP 备份组 1，配置 DeviceA 的优先级为 120，抢占延时为 20 秒，作为 Master 设备。

```
[DeviceA] interface vlanif 2
[DeviceA-Vlanif2] vrrp vrid 1 virtual-ip 10.1.2.100
[DeviceA-Vlanif2] vrrp vrid 1 priority 120
[DeviceA-Vlanif2] vrrp vrid 1 preempt timer delay 20
[DeviceA-Vlanif2] quit
```

DeviceB 的优先级为缺省值，作为 Backup 设备。

```
[DeviceB] interface vlanif 2
[DeviceB-Vlanif2] vrrp vrid 1 virtual-ip 10.1.2.100
[DeviceB-Vlanif2] quit
```

在 DeviceA 和 DeviceB 上创建 VRRP 备份组 2，配置 DeviceB 的优先级为 120，抢占延时为 20 秒，作为 Master 设备。

```
[DeviceB] interface vlanif 3
[DeviceB-Vlanif3] vrrp vrid 2 virtual-ip 10.1.3.100
[DeviceB-Vlanif3] vrrp vrid 2 priority 120
[DeviceB-Vlanif3] vrrp vrid 2 preempt timer delay 20
[DeviceB-Vlanif3] quit
```

DeviceA 的优先级为缺省值，作为 Backup 设备。

```
[DeviceA] interface vlanif 3
[DeviceA-Vlanif3] vrrp vrid 2 virtual-ip 10.1.3.100
[DeviceA-Vlanif3] quit
```

配置主机 HostA 的缺省网关为备份组 1 的虚拟 IP 地址 10.1.2.100，配置主机 HostB 的缺省网关为备份组 2 的虚拟 IP 地址 10.1.3.100。

7. 验证配置结果

完成上述配置后，在 DeviceA 上执行 **display vrrp** 命令，可以看到 DeviceA 在备份组 1 中作为 Master 设备，在备份组 2 中作为 Backup 设备。

```
[DeviceA] display vrrp
Vlanif2 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.2.100
  Master IP : 10.1.2.102
  PriorityRun : 120
```

```
PriorityConfig : 120
MasterPriority : 120
Preempt : YES   Delay Time : 20 s
TimerRun : 1 s
TimerConfig : 1 s
Auth type : NONE
Virtual MAC : 00e0-fc12-3456
Check TTL : YES
Config type : normal-vrrp
Backup-forward : disabled
Create time : 2021-05-11 11:39:18
Last change time : 2021-05-26 11:38:58
```

Vlanif3 | Virtual Router 2

State : Backup

```
Virtual IP : 10.1.3.100
Master IP : 10.1.3.103
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt : YES   Delay Time : 0 s
TimerRun : 1 s
TimerConfig : 1 s
Auth type : NONE
Virtual MAC : 00e0-fc12-3457
Check TTL : YES
Config type : normal-vrrp
Backup-forward : disabled
Create time : 2021-05-11 11:40:18
Last change time : 2021-05-26 11:48:58
```

在 DeviceB 上执行 **display vrrp** 命令，可以看到 DeviceB 在备份组 1 中作为 Backup 设备，在备份组 2 中作为 Master 设备。

```
[DeviceB] display vrrp
```

Vlanif2 | Virtual Router 1

State : Backup

```
Virtual IP : 10.1.2.100
Master IP : 10.1.2.102
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt : YES   Delay Time : 0 s
TimerRun : 1 s
```

TimerConfig : 1 s
Auth type : NONE
Virtual MAC : 00e0-fc12-3456
Check TTL : YES
Config type : normal-vrrp
Backup-forward : disabled
Create time : 2021-05-11 11:39:18
Last change time : 2021-05-26 11:38:58

Vlanif3 | Virtual Router 2

State : Master

Virtual IP : 10.1.3.100
Master IP : 10.1.3.103
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES Delay Time : 20 s
TimerRun : 1 s
TimerConfig : 1 s
Auth type : NONE
Virtual MAC : 00e0-fc12-3457
Check TTL : YES
Config type : normal-vrrp
Backup-forward : disabled
Create time : 2021-05-11 11:40:18
Last change time : 2021-05-26 11:48:58

配置脚本

DeviceA 的配置文件

```
#  
sysname DeviceA  
#  
vlan batch 2 to 4  
#  
stp instance 1 root primary  
stp instance 2 root secondary  
stp bpdu-protection  
stp pathcost-standard legacy  
#  
stp region-configuration  
region-name RG1
```

```
instance 1 vlan 2
instance 2 vlan 3
#
interface Vlanif2
ip address 10.1.2.102 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.2.100
vrrp vrid 1 priority 120
vrrp vrid 1 preempt timer delay 20
#
interface Vlanif3
ip address 10.1.3.102 255.255.255.0
vrrp vrid 2 virtual-ip 10.1.3.100
#
interface Vlanif4
ip address 10.1.4.102 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 3
stp root-protection
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 4
stp edged-port enable
#
ospf 1
area 0.0.0.0
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
network 10.1.4.0 0.0.0.255
#
return
```

DeviceB 的配置文件

```
#
sysname DeviceB
#
vlan batch 2 to 3 5
```



```
#
stp instance 1 root secondary
stp instance 2 root primary
stp bpdu-protection
stp pathcost-standard legacy
#
stp region-configuration
region-name RG1
instance 1 vlan 2
instance 2 vlan 3
#
interface Vlanif2
ip address 10.1.2.103 255.255.255.0
vrp vrid 1 virtual-ip 10.1.2.100
#
interface Vlanif3
ip address 10.1.3.103 255.255.255.0
vrp vrid 2 virtual-ip 10.1.3.100
vrp vrid 2 priority 120
vrp vrid 2 preempt timer delay 20
#
interface Vlanif5
ip address 10.1.5.103 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 to 3
stp root-protection
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 to 3
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 5
stp edged-port enable
#
ospf 1
area 0.0.0.0
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
network 10.1.5.0 0.0.0.255
```

```
#  
return
```

DeviceC 的配置文件

```
#  
sysname DeviceC  
#  
vlan batch 2 to 3  
#  
stp bpdu-protection  
stp pathcost-standard legacy  
#  
stp region-configuration  
region-name RG1  
instance 1 vlan 2  
instance 2 vlan 3  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 2 to 3  
stp instance 2 cost 20000  
#  
interface 10GE1/0/2  
port link-type access  
port default vlan 2  
stp edged-port enable  
#  
interface 10GE1/0/3  
port link-type access  
port default vlan 3  
stp edged-port enable  
#  
interface 10GE1/0/4  
port link-type trunk  
port trunk allow-pass vlan 2 to 3  
stp instance 1 cost 20000  
#  
return
```

1.1.5.6.5 VBST

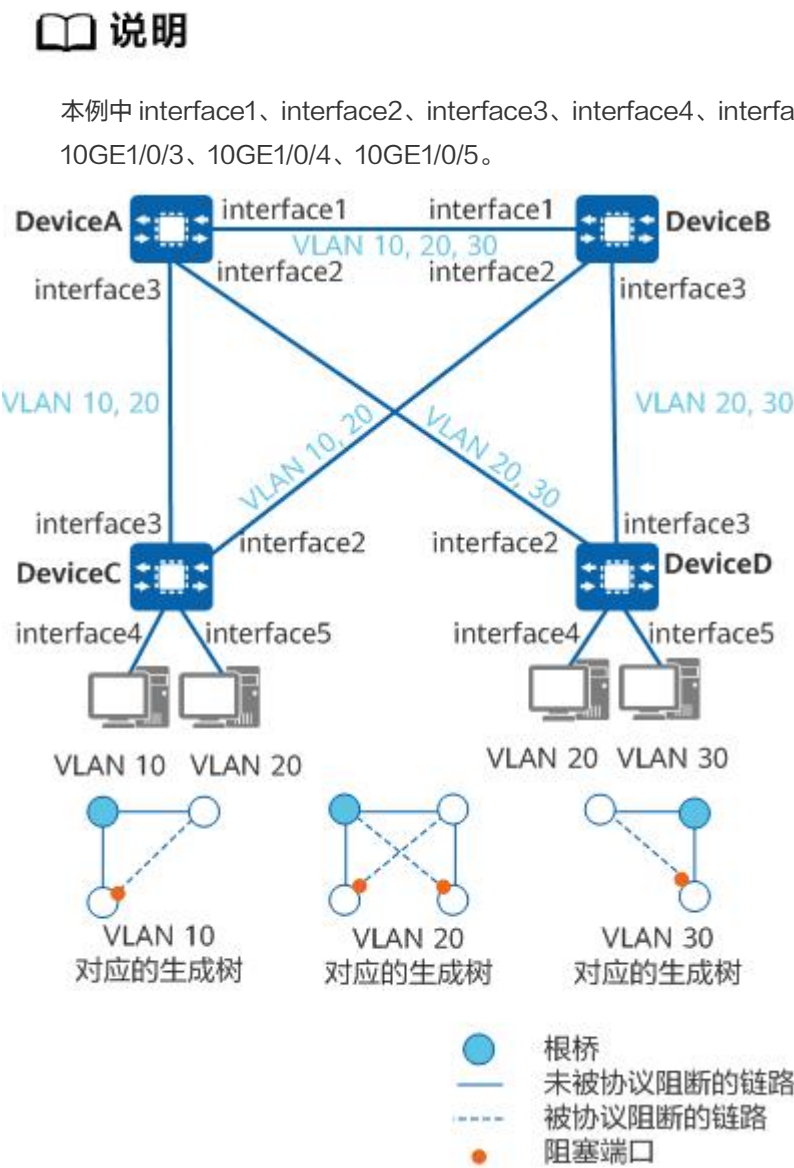
举例：配置 VBST 基本功能

1.1.5.6.5.1 举例：配置 VBST 基本功能

组网需求

如图 1 所示，设备 DeviceC 和 DeviceD 分别双归接入到 DeviceA 和 DeviceB。DeviceC 接入 VLAN 10、20 的业务流量，DeviceD 接入 VLAN 20、30 的业务流量。由于双归接入，设备间存在环形网络。用户希望部署 VBST，使各 VLAN 内的业务流量正常转发，同时希望不同 VLAN 内的业务流量能够在链路上负载分担，以提高链路利用率。

图 1 配置 VBST 功能组网图



操作步骤

1. 在设备 DeviceA、DeviceB、DeviceC 和 DeviceD 上创建 VLAN10、VLAN20 和 VLAN30。
在 DeviceA 上创建 VLAN10、VLAN20 和 VLAN30。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
```

```
[DeviceA] vlan batch 10 20 30
```

在 DeviceB 上创建 VLAN10、VLAN20 和 VLAN30。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10 20 30
```

在 DeviceC 上创建 VLAN10 和 VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 10 20
```

在 DeviceD 上创建 VLAN20 和 VLAN30。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] vlan batch 20 30
```

2. 配置接口加入 VLAN。

将 DeviceA 接口 10GE1/0/1 加入 VLAN10、VLAN20 和 VLAN30，10GE1/0/2 加入 VLAN20 和 VLAN30，10GE1/0/3 加入 VLAN10 和 VLAN20。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10 20 30
[DeviceA-10GE1/0/1] undo port trunk allow-pass vlan 1
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 20 30
[DeviceA-10GE1/0/2] undo port trunk allow-pass vlan 1
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 10 20
[DeviceA-10GE1/0/3] undo port trunk allow-pass vlan 1
[DeviceA-10GE1/0/3] quit
```

将 DeviceB 接口 10GE1/0/1 加入 VLAN10、VLAN20 和 VLAN30，10GE1/0/2 加入 VLAN10 和 VLAN20，10GE1/0/3 加入 VLAN20 和 VLAN30。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10 20 30
```

```
[DeviceB-10GE1/0/1] undo port trunk allow-pass vlan 1
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 10 20
[DeviceB-10GE1/0/2] undo port trunk allow-pass vlan 1
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type trunk
[DeviceB-10GE1/0/3] port trunk allow-pass vlan 20 30
[DeviceB-10GE1/0/3] undo port trunk allow-pass vlan 1
[DeviceB-10GE1/0/3] quit
```

将 DeviceC 接口 10GE1/0/2 加入 VLAN10 和 VLAN20, 10GE1/0/3 加入 VLAN10 和 VLAN20, 10GE1/0/4 加入 VLAN10, 10GE1/0/5 加入 VLAN20。

```
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] port link-type trunk
[DeviceC-10GE1/0/2] port trunk allow-pass vlan 10 20
[DeviceC-10GE1/0/2] undo port trunk allow-pass vlan 1
[DeviceC-10GE1/0/2] quit
[DeviceC] interface 10ge 1/0/3
[DeviceC-10GE1/0/3] portswitch
[DeviceC-10GE1/0/3] port link-type trunk
[DeviceC-10GE1/0/3] port trunk allow-pass vlan 10 20
[DeviceC-10GE1/0/3] undo port trunk allow-pass vlan 1
[DeviceC-10GE1/0/3] quit
[DeviceC] interface 10ge 1/0/4
[DeviceC-10GE1/0/4] portswitch
[DeviceC-10GE1/0/4] port link-type access
[DeviceC-10GE1/0/4] port default vlan 10
[DeviceC-10GE1/0/4] quit
[DeviceC] interface 10ge 1/0/5
[DeviceC-10GE1/0/5] portswitch
[DeviceC-10GE1/0/5] port link-type access
[DeviceC-10GE1/0/5] port default vlan 20
[DeviceC-10GE1/0/5] quit
```

将 DeviceD 接口 10GE1/0/2 加入 VLAN20 和 VLAN30, 10GE1/0/3 加入 VLAN20 和 VLAN30, 10GE1/0/4 加入 VLAN20, 10GE1/0/5 加入 VLAN30。

```
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] portswitch
```

```
[DeviceD-10GE1/0/2] port link-type trunk
[DeviceD-10GE1/0/2] port trunk allow-pass vlan 20 30
[DeviceD-10GE1/0/2] undo port trunk allow-pass vlan 1
[DeviceD-10GE1/0/2] quit
[DeviceD] interface 10ge 1/0/3
[DeviceD-10GE1/0/3] portswitch
[DeviceD-10GE1/0/3] port link-type trunk
[DeviceD-10GE1/0/3] port trunk allow-pass vlan 20 30
[DeviceD-10GE1/0/3] undo port trunk allow-pass vlan 1
[DeviceD-10GE1/0/3] quit
[DeviceD] interface 10ge 1/0/4
[DeviceD-10GE1/0/4] portswitch
[DeviceD-10GE1/0/4] port link-type access
[DeviceD-10GE1/0/4] port default vlan 20
[DeviceD-10GE1/0/4] quit
[DeviceD] interface 10ge 1/0/5
[DeviceD-10GE1/0/5] portswitch
[DeviceD-10GE1/0/5] port link-type access
[DeviceD-10GE1/0/5] port default vlan 30
[DeviceD-10GE1/0/5] quit
```

3. 配置设备的生成树协议工作在 VBST 模式。

配置 DeviceA 的工作模式为 VBST。

```
[DeviceA] stp mode vbst
```

配置 DeviceB 的工作模式为 VBST。

```
[DeviceB] stp mode vbst
```

配置 DeviceC 的工作模式为 VBST。

```
[DeviceC] stp mode vbst
```

配置 DeviceD 的工作模式为 VBST。

```
[DeviceD] stp mode vbst
```

4. 分别配置 VLAN10、VLAN20、VLAN30 的根桥和备份根桥。

配置 DeviceA 为 VLAN10 的根桥。

```
[DeviceA] stp vlan 10 root primary
```

配置 DeviceB 为 VLAN10 的备份根桥。

```
[DeviceB] stp vlan 10 root secondary
```

配置 DeviceA 为 VLAN20 的根桥。

```
[DeviceA] stp vlan 20 root primary
```

配置 DeviceB 为 VLAN20 的备份根桥。

```
[DeviceB] stp vlan 20 root secondary
```

配置 DeviceB 为 VLAN30 的根桥。

```
[DeviceB] stp vlan 30 root primary
```

配置 DeviceA 为 VLAN30 的备份根桥。

```
[DeviceA] stp vlan 30 root secondary
```

5. 配置各 VLAN 中端口的路径开销值，实现将该端口阻塞。

说明

端口路径开销值取值范围由路径开销计算方法决定，本例选择使用缺省的 IEEE 802.1t 计算方法，配置将被阻塞端口的路径开销值为 2000000。

同一网络内所有设备的端口路径开销应使用相同的计算方法。

将 DeviceC 上的端口 10GE1/0/2 在 VLAN10 中的路径开销值配置为 2000000，在 VLAN20 中的路径开销值配置为 2000000。

```
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] stp vlan 10 cost 2000000
[DeviceC-10GE1/0/2] stp vlan 20 cost 2000000
[DeviceC-10GE1/0/2] quit
```

将 DeviceD 上的端口 10GE1/0/2 在 VLAN20 中的路径开销值配置为 2000000，在 VLAN30 中的路径开销值配置为 2000000。

```
[DeviceD] interface 10ge 1/0/2
[DeviceD-10GE1/0/2] stp vlan 20 cost 2000000
[DeviceD-10GE1/0/2] stp vlan 30 cost 2000000
[DeviceD-10GE1/0/2] quit
```

6. 使能 VBST，实现破除环路。

全局使能 VBST 功能。

缺省情况下，全局 VBST 功能已使能。为确保全局 VBST 使能，可执行命令 **display stp vlan information** 查看 VBST 的使能状态。如果未使能，请在系统视图执行命令 **undo stp vlan disable** 全局使能 VBST 功能。

VLAN 使能 VBST 功能。

缺省情况下，VLAN 上的 VBST 功能处于使能状态。为确保 VLAN 的 VBST 功能使能，可执行命令 **display stp vlan *vlan-id* information** 查看 VLAN 上的 VBST 状态。如果提示该 VLAN 上 VBST 功能未使能，请在系统视图执行命令 **undo stp vlan *vlan-id* disable** 使能该 VLAN 的 VBST 功能。

检查配置结果

一段时间生成树协议计算稳定后，执行以下操作，验证配置结果。

在 DeviceA 上执行 **display stp vlan bridge local** 命令，查看 STP 工作模式。根据 Protocol 字段可以看出，STP 工作在 VBST 模式。

```
[DeviceA] display stp vlan bridge local
```

VLANID	BridgeID	HelloTime	MaxAge	ForwardDelay	Protocol
10	10.ac94-8400-df01	2	20	15	VBST
20	20.ac94-8400-df01	2	20	15	VBST
30	4126.ac94-8400-df01	2	20	15	VBST

在 DeviceA、DeviceB、DeviceC 和 DeviceD 上分别执行 **display stp vlan information brief** 命令，查看端口状态。以 DeviceA 回显为例，DeviceA 分别参加 VLAN10、VLAN20 和 VLAN30 的生成树计算。DeviceA 在 VLAN10 和 VLAN20 中都是根桥，所以在 VLAN10 中 10GE1/0/1 和 10GE1/0/3 都被选举为指定端口；在 VLAN20 中 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 都被选举为指定端口。DeviceA 在 VLAN30 中是备份根桥，所以 VLAN30 中 10GE1/0/1 被选举为根端口，10GE1/0/2 被选举为指定端口。

[DeviceA] display stp vlan information brief

VLANID	Interface	Role	STPState	Protection	Cost	Edged
10	10GE1/0/1	DESI	forwarding	none	200	disable
10	10GE1/0/3	DESI	forwarding	none	200	disable
20	10GE1/0/1	DESI	forwarding	none	200	disable
20	10GE1/0/2	DESI	forwarding	none	200	disable
20	10GE1/0/3	DESI	forwarding	none	200	disable
30	10GE1/0/1	ROOT	forwarding	none	200	disable
30	10GE1/0/2	DESI	forwarding	none	200	disable

配置脚本

DeviceA

```
#
sysname DeviceA
#
stp vlan 10 20 root primary
stp vlan 30 root secondary
#
vlan batch 10 20 30
#
stp mode vbst
#
interface 10GE1/0/1
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
```



```
port trunk allow-pass vlan 10 20 30
#
interface 10GE1/0/2
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30
#
interface 10GE1/0/3
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 20
#
return
```

DeviceB

```
#
sysname DeviceB
#
stp vlan 10 20 root secondary
stp vlan 30 root primary
#
vlan batch 10 20 30
#
stp mode vbst
#
interface 10GE1/0/1
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 20 30
#
interface 10GE1/0/2
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 20
#
interface 10GE1/0/3
portswitch
```

```
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 10 20
#
stp mode vbst
#
interface 10GE1/0/2
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 20
stp vlan 10 20 cost 2000000
#
interface 10GE1/0/3
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 10 20
#
interface 10GE1/0/4
portswitch
port default vlan 10
#
interface 10GE1/0/5
portswitch
port default vlan 20
#
return
```

DeviceD

```
#
sysname DeviceD
#
vlan batch 20 30
```

```
#
stp mode vbst
#
interface 10GE1/0/2
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30
stp vlan 20 30 cost 2000000
#
interface 10GE1/0/3
portswitch
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 20 30
#
interface 10GE1/0/4
portswitch
port default vlan 20
#
interface 10GE1/0/5
port default vlan 30
#
return
```

1.1.5.7 IP 地址与服务

[ARP 安全](#)

[DHCPv4](#)

[DHCP Snooping](#)

[ACL](#)

1.1.5.7.1 ARP 安全

[举例：配置 ARP 安全功能](#)

[举例：配置防止 ARP 中间人攻击](#)

1.1.5.7.1.1 举例：配置 ARP 安全功能

组网需求

如图 1 所示，设备通过接口 10GE1/0/3 连接一台服务器，通过接口 10GE1/0/1 和接口 10GE1/0/2 连接 VLAN10 和 VLAN20 下的四个用户主机。网络中存在的 ARP 攻击包括：

服务器可能会发送一些目的 IP 地址不可达的报文，而且这种报文相对其他普通用户主机的报文要多。

用户 HostA 遭到网络攻击者攻击后，会在网络中发送大量的伪造 ARP 攻击报文，这种报文中的源 IP 地址会不断变化。

用户 HostC 遭到网络攻击者攻击后，会构造大量的源 IP 地址固定的 ARP 报文对网络进行攻击。

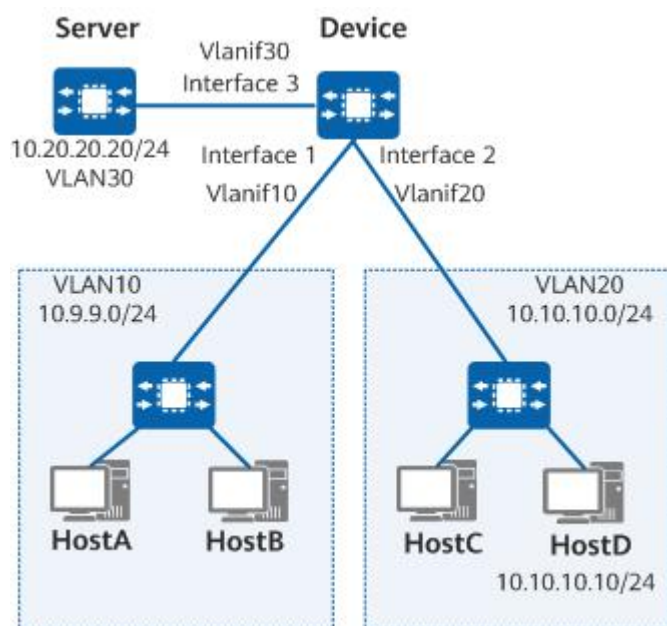
用户 HostD 可能会发送一些目的 IP 地址不可达的报文。

要求在 Device 配置 ARP 的安全功能，预防上述攻击。

图 1 配置 ARP 安全功能组网图

说明

本例中 interface1 代表 10GE1/0/1，interface2 代表 10GE1/0/2，interface3 代表 10GE1/0/3。



配置思路

采用如下的思路在 Device 上配置 ARP 安全功能：

1. 配置全局的 ARP 表项严格学习的功能，限制设备只学习自己发送的 ARP 请求报文的应答报文。
2. 基于接口配置 ARP 表项限制功能，限制接口学习 ARP 表项的最大数目，防止 ARP 表项溢出。
3. 配置 ARP 表项固化功能，防止网络攻击者通过发送伪造的 ARP 报文篡改 ARP 表项。

4. 配置 ARP 报文限速功能，限制设备 1 秒内处理 ARP 报文的数量，节省系统开销，保证用户业务不受影响。
5. 配置 ARP Miss 消息限速功能，限制设备 1 秒内处理 ARP Miss 消息的数量，节省系统开销，保证用户业务不受影响。同时需要保证设备可以正常处理服务器发出的大量此类报文，避免因丢弃服务器发出的大量此类报文而造成网络无法正常通信。

数据准备

为完成此配置例，需准备如下的数据：

基于接口配置 ARP 表项限制的阈值为 20。

配置 ARP 表项固化的固化模式为 **fixed-mac** 模式。

配置 ARP 报文限速的阈值为 15。

配置 ARP Miss 消息限速的阈值：对用户主机 HostD 的限速阈值为 30，对其他用户主机的限制阈值为 20，对服务器的限速阈值为 50。

操作步骤

1. 配置相关接口的 IP 地址和路由协议，具体的配置过程参见[配置脚本](#)。
2. 配置 ARP 表项严格学习功能。

```
<HUAWEI> system-view
[HUAWEI] sysname Device
[Device] arp learning strict
```

3. 基于接口配置 ARP 表项限制功能。

在接口 10GE1/0/1 上配置 VLAN10 的 ARP 表项限制阈值为 20。

```
[Device] interface 10ge1/0/1
[Device-10GE1/0/1] portswitch
[Device-10GE1/0/1] arp limit vlan 10 20
[Device-10GE1/0/1] quit
```

#参考接口 10GE1/0/1 的配置，配置接口 10GE1/0/2 和接口 10GE1/0/3 的 ARP 表项限制阈值。

4. 配置 ARP 表项固化功能。

```
[Device] arp anti-attack entry-check fixed-mac enable
```

5. 配置 ARP 报文限速功能。

```
[Device] arp anti-attack rate-limit source-ip maximum 15
```

6. 配置 ARP Miss 消息限速功能。

```
[Device] arp miss anti-attack rate-limit source-ip 10.10.10.10 maximum 30
[Device] arp miss anti-attack rate-limit source-ip maximum 20
[Device] arp miss anti-attack rate-limit source-ip 10.20.20.20 maximum 50
```

检查配置结果

执行命令 **display arp learning strict**，查看 ARP 表项严格学习的情况。

```
<HUAWEI> display arp learning strict
The global arp learning strict state:enable

-----

Interface          LearningStrictState
-----
-----

Total:0   Force-enable:0   Force-disable:0
```

执行命令 **display arp limit interface**，查看 10GE 1/0/1 接口上配置的 ARP 表项限制的阈值。

```
<HUAWEI> display arp limit interface 10ge1/0/1
Interface          VLAN   Limit   Learnt
-----
10GE1/0/1          10    20      0
-----

Total:1
```

执行命令 **display arp miss anti-attack rate-limit**，查看配置的 ARP Miss 消息限速的限速值。

```
<HUAWEI> display arp miss anti-attack rate-limit
Global ARP miss rate-limit : 500 (0 means no limit)

VLAN ID           Suppress Rate(pps)(0 means no limit)
-----
All                0
-----

Total: 0, spec of rate-limit configuration for VLAN is 1024.

Source IP          Suppress Rate(pps)(0 means no limit)
-----
10.10.10.10/32     30
10.20.20.20/32     50
Other              20
-----

Total: 2, spec of rate-limit configuration for Source IP is 1024.
```

执行命令 **display arp packet statistics**，查看 ARP 报文的统计信息。

```
<HUAWEI> display arp packet statistics
ARP Packets Received
Total:              154333
Learnt Count:       8
Discard For Entry Limit: 5
Discard For Speed Limit: 0
```

Discard For Proxy Suppress: 0

Discard For Other: 151597

ARP Packets Sent

Total: 0

Request: 0

Reply: 0

Gratuitous ARP: 0

ARP-Miss Message Received:

Total: 0

Discard For Speed Limit: 0

Discard For Other: 3

配置脚本

Device

```
#
sysname Device
#
vlan batch 10 20 30
#
arp learning strict
arp anti-attack entry-check fixed-mac enable
arp anti-attack rate-limit source-ip maximum 15
arp miss anti-attack rate-limit source-ip 10.10.10.10 maximum 30
arp miss anti-attack rate-limit source-ip maximum 20
arp miss anti-attack rate-limit source-ip 10.20.20.20 maximum 50
#
interface Vlanif10
 ip address 10.9.9.1 255.255.255.0
#
interface Vlanif20
 ip address 10.10.10.1 255.255.255.0
#
interface Vlanif30
 ip address 10.20.20.1 255.255.255.0
#
interface 10GE1/0/1
 arp limit vlan 10 20
#
interface 10GE1/0/2
 arp limit vlan 20 20
#
```

```
interface 10GE1/0/3
 arp limit vlan 30 20
#
return
```

1.1.5.7.1.2 举例：配置防止 ARP 中间人攻击

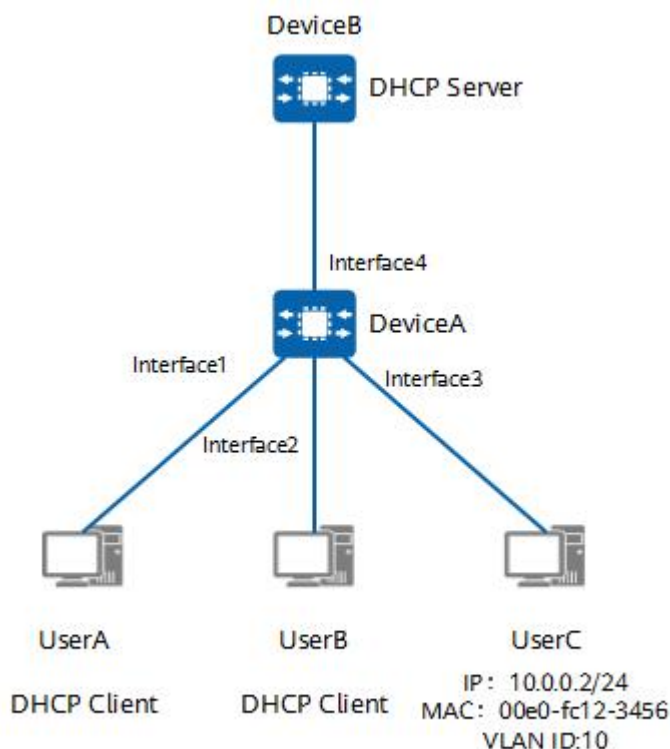
组网需求

如图 1 所示，DeviceA 通过接口 10GE1/0/4 连接 DHCP Server，通过接口 10GE1/0/1、10GE1/0/2 连接 DHCP 客户端 UserA 和 UserB，通过接口 10GE1/0/3 连接静态配置 IP 地址的用户 UserC。DeviceA 的接口 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4 都属于 VLAN10。管理员希望能够防止 ARP 中间人攻击，避免合法用户的数据被中间人窃取，同时希望能够了解当前 ARP 中间人攻击的频率和范围。

图 1 配置防止 ARP 中间人攻击组网

说明

本例中 interface1 代表 10GE1/0/1，interface2 代表 10GE1/0/2，interface3 代表 10GE1/0/3，interface4 代表 10GE1/0/4。



配置思路

1. 使能动态 ARP 检测功能，使 DeviceA 对收到的 ARP 报文对应的源 IP、源 MAC、VLAN 以及接口信息进行 DHCP Snooping 绑定表匹配检查，实现防止 ARP 中间人攻击。

2. 使能动态 ARP 检测丢弃报文告警功能，使 DeviceA 开始统计丢弃的不匹配 DHCP Snooping 绑定表的 ARP 报文数量，并在丢弃数量超过告警阈值时能以告警的方式提醒管理员，这样可以使管理员根据告警信息以及报文丢弃计数来了解当前 ARP 中间人攻击的频率和范围。
3. 配置 DHCP Snooping 功能，并配置静态绑定表，使动态 ARP 检测功能生效。

操作步骤

1. 创建 VLAN，将接口加入到 VLAN 中。

创建 VLAN10，并将接口 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4 加入 VLAN10 中。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 10
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10GE 1/0/3
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 10
[DeviceA-10GE1/0/3] quit
[DeviceA-10GE1/0/4] interface 10GE 1/0/4
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/4] quit
```

2. 使能动态 ARP 检测功能和动态 ARP 检测丢弃报文告警功能。

在接口 10GE1/0/1、10GE1/0/2、10GE1/0/3 下使能动态 ARP 检测功能和动态 ARP 检测丢弃报文告警功能。

```
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] arp anti-attack check user-bind enable
[DeviceA-10GE1/0/1] arp anti-attack check user-bind alarm enable
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] arp anti-attack check user-bind enable
[DeviceA-10GE1/0/2] arp anti-attack check user-bind alarm enable
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10GE 1/0/3
[DeviceA-10GE1/0/3] arp anti-attack check user-bind enable
```

```
[DeviceA-10GE1/0/3] arp anti-attack check user-bind alarm enable
[DeviceA-10GE1/0/3] quit
```

3. 配置 DHCP Snooping 功能。

使能 DHCP Snooping 功能，并将连接 DHCP Server 的 10GE1/0/4 接口配置为信任接口。

```
[DeviceA] dhcp enable
[DeviceA] dhcp snooping enable
[DeviceA] vlan 10
[DeviceA-vlan10] dhcp snooping enable
[DeviceA-vlan10] quit
[DeviceA] interface 10GE 1/0/4
[DeviceA-10GE1/0/4] dhcp snooping trusted
[DeviceA-10GE1/0/4] quit
```

配置静态绑定表。

```
[DeviceA] user-bind static ip-address 10.0.0.2 mac-address 00e0-fc12-3456 interface 10GE1/0/3 vlan
10
```

检查配置结果

执行命令 **display arp anti-attack configuration check user-bind**，查看各接口下动态 ARP 检测的配置信息，以 10GE1/0/1 为例。

```
[DeviceA] display arp anti-attack configuration check user-bind interface 10GE 1/0/1
interface 10GE1/0/1
  arp anti-attack check user-bind enable
  arp anti-attack check user-bind alarm enable
```

执行命令 **display arp anti-attack statistics check user-bind interface**，查看各接口下动态 ARP 检测的 ARP 报文丢弃计数，以 10GE1/0/1 为例。

```
[DeviceA] display arp anti-attack statistics check user-bind interface 10GE 1/0/1
```

```
-----
Type      View      Total Dropped  Last Dropped
-----
Interface  10GE1/0/1    966           605
-----
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 10
```

```
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.2 mac-address 00e0-fc12-3456 interface 10GE1/0/3 vlan 10
#
vlan 10
  dhcp snooping enable
#
interface 10GE1/0/1
  port link-type access
  port default vlan 10
  arp anti-attack check user-bind enable
  arp anti-attack check user-bind alarm enable
#
interface 10GE1/0/2
  port link-type access
  port default vlan 10
  arp anti-attack check user-bind enable
  arp anti-attack check user-bind alarm enable
#
interface 10GE1/0/3
  port link-type access
  port default vlan 10
  arp anti-attack check user-bind enable
  arp anti-attack check user-bind alarm enable
#
interface 10GE1/0/4
  port link-type trunk
  port trunk allow-pass vlan 10
  dhcp snooping trusted
#
return
```

1.1.5.7.2 DHCPv4

[举例：配置基于接口地址池的 DHCPv4 服务器](#)

[举例：配置基于全局地址池的 DHCPv4 服务器（使用三层以太网接口）](#)

[举例：配置 DHCPv4 客户端](#)

[举例：配置 DHCPv4 中继](#)

1.1.5.7.2.1 举例：配置基于接口地址池的 DHCPv4 服务器

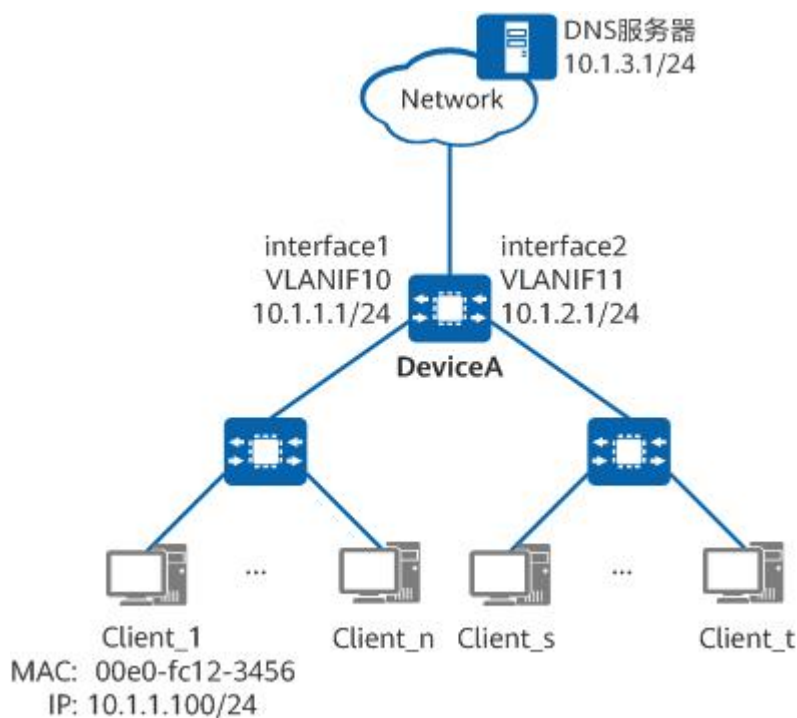
组网需求

如图 1 所示，DeviceA 作为 DHCPv4 服务器，网段 10.1.1.0/24 内 PC 为固定终端，网段 10.1.2.0/24 供终端临时接入。为方便统一管理，管理员希望终端能够自动获取 IPv4 地址和 DNS 服务器 IPv4 地址（当用户希望以域名方式访问时需要配置域名解析的 DNS 服务器）。其中一台 PC（命名为 Client_1）由于业务需要，希望使用固定 IPv4 地址为 10.1.1.100/24。

图 1 配置基于接口地址池的 DHCPv4 服务器组网图

说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

采用如下思路配置基于接口地址池的 DHCPv4 服务器：

1. 网段 10.1.1.0/24 内 PC（Client_1~Client_n）的 IPv4 地址租期配置为 30 天，并通过静态方式为 Client_1 分配固定 IPv4 地址 10.1.1.100/24。
2. 网段 10.1.2.0/24 供（Client_s~Client_t）临时接入网络，IPv4 地址租期配置为 2 天。

操作步骤

1. 使能 DHCPv4 功能

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] dhcp enable
```

2. 配置接口加入 VLAN

配置接口 10GE1/0/1 加入 VLAN10，配置接口 10GE1/0/2 加入 VLAN11。

```
[DeviceA] vlan batch 10 11
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 11
[DeviceA-10GE1/0/2] quit
```

3. 配置 VLANIF 接口的 IPv4 地址

配置接口 VLANIF10 的地址。

```
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.1 24
[DeviceA-Vlanif10] quit
```

配置接口 VLANIF11 的地址。

```
[DeviceA] interface vlanif 11
[DeviceA-Vlanif11] ip address 10.1.2.1 24
[DeviceA-Vlanif11] quit
```

4. 配置接口地址池

配置 VLANIF10 接口下的客户端从接口地址池中获取 IPv4 地址和相关网络参数。

```
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] dhcp select interface
[DeviceA-Vlanif10] dhcp server gateway-list 10.1.1.1
[DeviceA-Vlanif10] dhcp server lease day 30
[DeviceA-Vlanif10] dhcp server domain-name huawei.com
[DeviceA-Vlanif10] dhcp server dns-list 10.1.3.1
[DeviceA-Vlanif10] dhcp server static-bind ip-address 10.1.1.100 mac-address 00e0-fc12-3456
[DeviceA-Vlanif10] quit
```

配置 VLANIF11 接口下的客户端从接口地址池中获取 IPv4 地址和相关网络参数。

```
[DeviceA] interface vlanif 11
[DeviceA-Vlanif11] dhcp select interface
```

```
[DeviceA-Vlanif11] dhcp server gateway-list 10.1.2.1
[DeviceA-Vlanif11] dhcp server lease day 2
[DeviceA-Vlanif11] dhcp server domain-name huawei.com
[DeviceA-Vlanif11] dhcp server dns-list 10.1.3.1
[DeviceA-Vlanif11] quit
```

检查配置结果

在 DeviceA 上执行命令 **display ip pool** 来查看地址池的配置情况和分配情况，“Used” 字段显示已经分配出去的 IPv4 地址数量。

```
[DeviceA] display ip pool interface vlanif10
Pool-name      : Vlanif10
Pool-No        : 0
Lease          : 30 Days 0 Hours 0 Minutes
Domain-name    : huawei.com
DNS-server0    : 10.1.3.1
NBNS-server0   : -
Netbios-type   : -
Position       : Interface
Status         : Unlocked
Gateway-0      : 10.1.1.1
Network        : 10.1.1.0
Mask           : 255.255.255.0
VPN instance   : --
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total    :253    Used    :100
                  Idle      :153     Expired  :0
                  Conflict   :0       Disabled :0
```

Network section							
Start	End	Total	Used	Idle(Expired)	Conflict	Disabled	
10.1.1.1	10.1.1.254	253	100	153(0)	0	0	

```
[DeviceA] display ip pool interface vlanif11
Pool-name      : Vlanif11
Pool-No        : 1
Lease          : 2 Days 0 Hours 0 Minutes
Domain-name    : huawei.com
DNS-server0    : 10.1.3.1
```

```

NBNS-server0    : -
Netbios-type    : -
Position        : Interface
Status          : Unlocked
Gateway-0       : 10.1.2.1
Network         : 10.1.2.0
Mask            : 255.255.255.0
VPN instance    : --
Logging         : Disable
Conflicted address recycle interval: -
Address Statistic: Total    :253    Used    :3
                  Idle     :250    Expired  :0
                  Conflict  :0      Disabled :0

```

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled

10.1.2.1	10.1.1.254	253	3	250(0)	0	0

在 Client_1 上查看 IPv4 地址信息，可以看到 Client_1 已经获取到 IPv4 地址 10.1.1.100/24。

在其他 DHCPv4 客户端上查看 IPv4 地址信息，可以看到已经成功获取到 IPv4 地址。

配置脚本

DeviceA 的配置脚本

```

#
sysname DeviceA
#
vlan batch 10 11
#
dhcp enable
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
 dhcp select interface
 dhcp server gateway-list 10.1.1.1
 dhcp server static-bind ip-address 10.1.1.100 mac-address 00e0-fc12-3456
 dhcp server lease day 30 hour 0 minute 0
 dhcp server dns-list 10.1.3.1
 dhcp server domain-name huawei.com
#

```

```
interface Vlanif11
ip address 10.1.2.1 255.255.255.0
dhcp select interface
dhcp server gateway-list 10.1.2.1
dhcp server lease day 2 hour 0 minute 0
dhcp server dns-list 10.1.3.1
dhcp server domain-name huawei.com
#
interface 10GE1/0/1
port default vlan 10
#
interface 10GE1/0/2
port default vlan 11
#
return
```

1.1.5.7.2.2 举例：配置基于全局地址池的 DHCPv4 服务器（使用三层以太网接口）

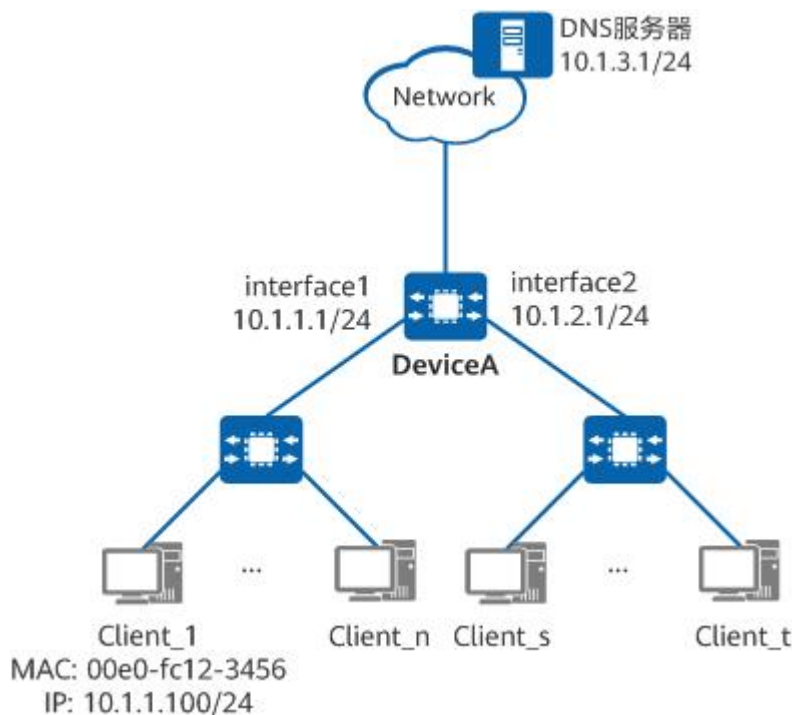
组网需求

如[图 1](#)所示，DeviceA 作为 DHCPv4 服务器，网段 10.1.1.0/24 内 PC 为固定终端，网段 10.1.2.0/24 供终端临时接入。为方便统一管理，管理员希望终端能够自动获取 IPv4 地址和 DNS 服务器 IPv4 地址（当用户希望以域名方式访问时需要配置域名解析的 DNS 服务器）。其中一台 PC（命名为 Client_1）由于业务需要，希望使用固定 IPv4 地址为 10.1.1.100/24。

图 1 配置基于全局地址池的 DHCPv4 服务器（使用三层以太网接口）组网图

说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

采用如下思路配置基于全局地址池且使用三层以太网接口的 DHCPv4 服务器：

1. 网段 10.1.1.0/24 内 PC (**Client_1** ~ **Client_n**) 的 IPv4 地址租期配置为 30 天，并通过静态方式为 **Client_1** 分配固定 IPv4 地址 10.1.1.100/24。
2. 网段 10.1.2.0/24 供 (**Client_s** ~ **Client_t**) 临时接入网络，IPv4 地址租期配置为 2 天。

操作步骤

1. 使能 DHCPv4 功能

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] dhcp enable
```

2. 配置接口的 IPv4 地址

```
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] undo portswitch
[DeviceA-10GE1/0/1] ip address 10.1.1.1 24
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] undo portswitch
[DeviceA-10GE1/0/2] ip address 10.1.2.1 24
[DeviceA-10GE1/0/2] quit
```

3. 配置全局地址池

配置地址池 pool1 的属性。

```
[DeviceA] ip pool pool1
[DeviceA-ip-pool-pool1] network 10.1.1.0 mask 24
[DeviceA-ip-pool-pool1] gateway-list 10.1.1.1
[DeviceA-ip-pool-pool1] lease day 30
[DeviceA-ip-pool-pool1] domain-name huawei.com
[DeviceA-ip-pool-pool1] dns-list 10.1.3.1
[DeviceA-ip-pool-pool1] static-bind ip-address 10.1.1.100 mac-address 00e0-fc12-3456
[DeviceA-ip-pool-pool1] quit
```

配置地址池 pool2 的属性。

```
[DeviceA] ip pool pool2
[DeviceA-ip-pool-pool2] network 10.1.2.0 mask 24
[DeviceA-ip-pool-pool2] gateway-list 10.1.2.1
[DeviceA-ip-pool-pool2] lease day 2
[DeviceA-ip-pool-pool2] domain-name huawei.com
[DeviceA-ip-pool-pool2] dns-list 10.1.3.1
[DeviceA-ip-pool-pool2] quit
```

4. 开启三层以太网接口采用全局地址池的 DHCPv4 服务器功能

```
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] dhcp select global
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] dhcp select global
[DeviceA-10GE1/0/2] quit
```

检查配置结果

在 DeviceA 上执行命令 **display ip pool** 来查看地址池的配置和分配情况，“Used” 字段显示已经分配出去的 IPv4 地址数量。

```
[DeviceA] display ip pool name pool1

Pool-name      : pool1
Pool-No        : 7
Lease          : 30 Days 0 Hours 0 Minutes
Domain-name    : huawei.com
DNS-server0    : 10.1.3.1
NBNS-server0   : -
Netbios-type   : -
Position       : Local
Status         : Unlocked
Gateway-0      : 10.1.1.1
Network        : 10.1.1.0
```

```
Mask      : 255.255.255.0
VPN instance  : --
Logging    : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :253   Used    :1
                  Idle     :252   Expired   :0
                  Conflict  :0     Disabled  :0

-----

--

Network section
  Start      End      Total   Used Idle(Expired) Conflict Disabled
-----
10.1.1.1     10.1.1.254  253    1   252(0)    0    0
-----

--

[DeviceA] display ip pool name pool2

Pool-name    : pool2
Pool-No      : 8
Lease        : 2 Days 0 Hours 0 Minutes
Domain-name   : huawei.com
DNS-server0  : 10.1.3.1
NBNS-server0 : -
Netbios-type  : -
Position     : Local
Status       : Unlocked
Gateway-0    : 10.1.2.1
Network      : 10.1.2.0
Mask         : 255.255.255.0
VPN instance  : --
Logging      : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :253   Used    :0
                  Idle     :253   Expired   :0
                  Conflict  :0     Disabled  :0

-----

--

Network section
  Start      End      Total   Used Idle(Expired) Conflict Disabled
```

```
-----  
-  
10.1.2.1 10.1.2.254 253 0 253(0) 0 0  
-----  
--
```

在 Client_1 上查看 IPv4 地址信息，可以看到 Client_1 已经获取到 IPv4 地址 10.1.1.100/24。

在其他 DHCPv4 客户端上查看 IPv4 地址信息，可以看到已经成功获取到 IPv4 地址。

配置脚本

DeviceA 的配置脚本

```
#  
sysname DeviceA  
#  
dhcp enable  
#  
ip pool pool1  
gateway-list 10.1.1.1  
network 10.1.1.0 mask 255.255.255.0  
static-bind ip-address 10.1.1.100 mac-address 00e0-fc12-3456  
lease day 30 hour 0 minute 0  
dns-list 10.1.3.1  
domain-name huawei.com  
#  
ip pool pool2  
gateway-list 10.1.2.1  
network 10.1.2.0 mask 255.255.255.0  
lease day 2 hour 0 minute 0  
dns-list 10.1.3.1  
domain-name huawei.com  
#  
interface 10GE1/0/1  
undo portswitch  
ip address 10.1.1.1 255.255.255.0  
dhcp select global  
#  
interface 10GE1/0/2  
undo portswitch  
ip address 10.1.2.1 255.255.255.0  
dhcp select global  
#  
return
```

1.1.5.7.2.3 举例：配置 DHCPv4 客户端

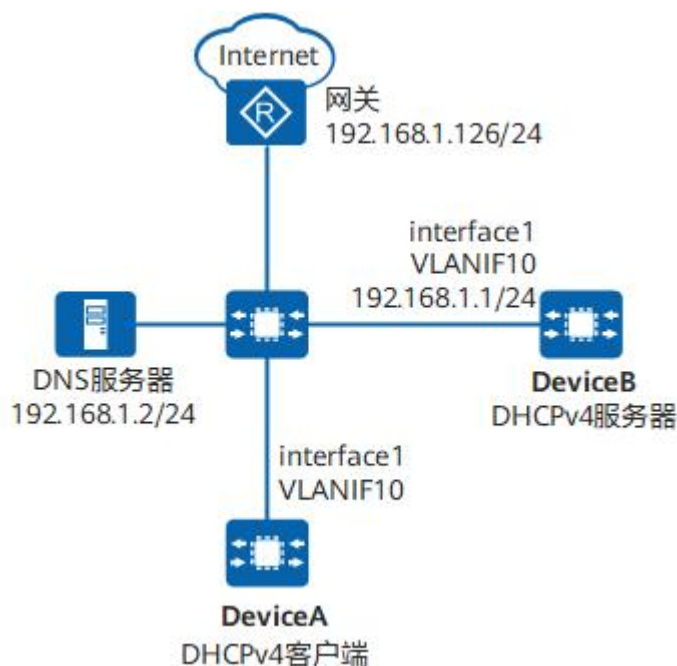
组网需求

如图 1 所示，DeviceA 作为 DHCPv4 客户端，希望从 DHCPv4 服务器（DeviceB）中动态获取 IPv4 地址、DNS 服务器、网关地址等信息。

图 1 配置 DHCPv4 客户端组网图

说明

本例中 interface1 代表 10GE1/0/1。



操作步骤

1. 在 DeviceA 上配置 DHCPv4 客户端功能

创建 VLAN10 并将 10GE1/0/1 接口加入到 VLAN10 中。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
  
```

在 VLANIF10 接口上使能 DHCPv4 客户端功能。

```

[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address dhcp-alloc
  
```

```
[DeviceA-Vlanif10] quit
```

2. 在 DeviceB 上创建 DHCPv4 服务器的全局地址池并配置网络参数

a. 使能 DHCPv4 功能。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] dhcp enable
```

b. 创建 VLAN10 并将 10GE1/0/1 接口加入到 VLAN10 中。

```
[DeviceB] vlan batch 10
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceB-10GE1/0/1] quit
```

c. 创建地址池并配置相关属性。

```
[DeviceB] ip pool pool1
[DeviceB-ip-pool-pool1] network 192.168.1.0 mask 24
[DeviceB-ip-pool-pool1] gateway-list 192.168.1.126
[DeviceB-ip-pool-pool1] dns-list 192.168.1.2
[DeviceB-ip-pool-pool1] excluded-ip-address 192.168.1.1
[DeviceB-ip-pool-pool1] excluded-ip-address 192.168.1.2
[DeviceB-ip-pool-pool1] quit
```

d. 开启接口 VLANIF10 采用全局地址池的 DHCPv4 服务器功能。

```
[DeviceB] interface vlanif 10
[DeviceB-Vlanif10] ip address 192.168.1.1 24
[DeviceB-Vlanif10] dhcp select global
[DeviceB-Vlanif10] quit
```

检查配置结果

当接口成功分配到 IPv4 地址，在 DeviceA 执行 **display dhcp client** 命令，查看 DHCPv4 客户端的状态信息。

```
[DeviceA] display dhcp client
DHCP client lease information on interface Vlanif10 :
Current machine state      : Bound
Internet address assigned via : DHCP
Physical address          : 00e0-fc12-3456
IP address                 : 192.168.1.254
Subnet mask                 : 255.255.255.0
Gateway ip address         : 192.168.1.126
```

```

DHCP server      : 192.168.1.1
Lease obtained at : 2021-09-26 20:30:39
Lease expires at  : 2021-09-27 20:30:39
Lease renews at   : 2020-09-27 08:30:39
Lease rebinds at  : 2020-09-27 17:30:39
Request option list : 1 3 6 15 28 33 44 121 184
Class identifier   : huawei xxxx
Client identifier  : 00e0-fc12-1111
DNS                : 192.168.1.2

```

在 DeviceB 上执行 **display ip pool name pool1** 命令，查看全局地址池的分配情况，“Used” 字段表示已经分配出去的 IPv4 地址数量。

```

[DeviceB] display ip pool name pool1
Pool-name      : pool1
Pool-No        : 0
Lease          : 1 Days 0 Hours 0 Minutes
Domain-name    : -
DNS-server0    : 192.168.1.2
NBNS-server0   : -
Netbios-type   : -
Position       : Local
Status         : Unlocked
Gateway-0      : 192.168.1.126
Network        : 192.168.1.0
Mask           : 255.255.255.0
VPN instance   : --
Logging        : Disable
Conflicted address recycle interval: -
Address Statistic: Total   :253   Used    :1
                  Idle     :251   Expired   :0
                  Conflict  :0     Disabled  :1

```

Network section

Start	End	Total	Used	Idle(Expired)	Conflict	Disabled

192.168.1.1	192.168.1.254	253	1	251(0)	0	1

配置脚本

DeviceA 的配置文件

```
#
sysname DeviceA
#
vlan batch 10
#
interface Vlanif10
 ip address dhcp-alloc
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

DeviceB 的配置文件

```
#
sysname DeviceB
#
vlan batch 10
#
dhcp enable
#
ip pool pool1
 gateway-list 192.168.1.126
 network 192.168.1.0 mask 255.255.255.0
 excluded-ip-address 192.168.1.1 192.168.1.2
 dns-list 192.168.1.2
#
interface Vlanif10
 ip address 192.168.1.1 255.255.255.0
 dhcp select global
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
return
```

1.1.5.7.2.4 举例：配置 DHCPv4 中继

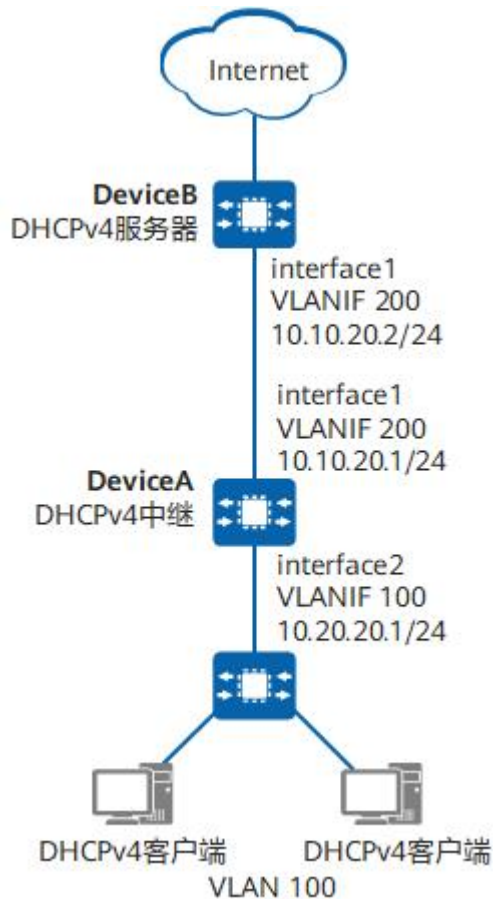
背景信息

如图 1 所示，DHCPv4 服务器与 DHCPv4 客户端不在同一网段，用户希望通过配置 DHCPv4 中继使 DHCPv4 客户端动态获取 IPv4 地址。

图 1 配置 DHCPv4 中继组网图

说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



操作步骤

1. 配置设备间的网络互连

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 100 200
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type hybrid
[DeviceA-10GE1/0/1] port hybrid pvid vlan 200
[DeviceA-10GE1/0/1] port hybrid untagged vlan 200
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
```

```
[DeviceA-10GE1/0/2] port link-type hybrid
[DeviceA-10GE1/0/2] port hybrid pvid vlan 100
[DeviceA-10GE1/0/2] port hybrid untagged vlan 100
[DeviceA-10GE1/0/2] quit
[DeviceA] interface vlanif 200
[DeviceA-Vlanif200] ip address 10.10.20.1 24
[DeviceA-Vlanif200] quit
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 200
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type hybrid
[DeviceB-10GE1/0/1] port hybrid pvid vlan 200
[DeviceB-10GE1/0/1] port hybrid untagged vlan 200
[DeviceB-10GE1/0/1] quit
[DeviceB] interface vlanif 200
[DeviceB-Vlanif200] ip address 10.10.20.2 24
[DeviceB-Vlanif200] quit
```

2. 配置 DHCPv4 中继。

在 DeviceA 的接口 VLANIF100 下使能 DHCPv4 中继功能，并配置 DHCPv4 服务器的 IPv4 地址。

```
[DeviceA] dhcp enable
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] ip address 10.20.20.1 24
[DeviceA-Vlanif100] dhcp select relay
[DeviceA-Vlanif100] dhcp relay server-ip 10.10.20.2
[DeviceA-Vlanif100] quit
```

3. 配置 DHCPv4 服务器。

在 DeviceB 上配置基于全局地址池的 DHCPv4 服务器功能。

```
[DeviceB] dhcp enable
[DeviceB] interface vlanif 200
[DeviceB-Vlanif200] dhcp select global
[DeviceB-Vlanif200] quit
[DeviceB] ip pool pool1
[DeviceB-ip-pool-pool1] network 10.20.20.0 mask 24
[DeviceB-ip-pool-pool1] gateway-list 10.20.20.1
[DeviceB-ip-pool-pool1] option121 ip-address 10.10.20.0 24 10.20.20.1
[DeviceB-ip-pool-pool1] quit
```

4. 配置路由。

在 DeviceA 上配置缺省路由。

```
[DeviceA] ip route-static 0.0.0.0 0.0.0.0 10.10.20.2
```

在 DeviceB 上配置静态路由。

```
[DeviceB] ip route-static 10.20.20.0 255.255.255.0 10.10.20.1
```

检查配置结果

在 DeviceA 上执行命令 **display dhcp relay interface vlanif 100** 命令用来查看 DHCPv4 中继的配置信息。

```
[DeviceA] display dhcp relay interface vlanif 100
```

```
Server IP address [00] : 10.10.20.2
```

```
Gateway address in use : 10.20.20.1
```

```
Gateway switch      : Disable
```

在 DHCPv4 客户端上查看 IPv4 地址信息，可以看到已经成功获取到 IPv4 地址。

配置脚本

DeviceA 的配置文件

```
#
sysname DeviceA
#
vlan batch 100 200
#
dhcp enable
#
interface Vlanif100
 ip address 10.20.20.1 255.255.255.0
 dhcp select relay
 dhcp relay server-ip 10.10.20.2
#
interface Vlanif200
 ip address 10.10.20.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type hybrid
 port hybrid pvid vlan 200
 port hybrid untagged vlan 200
#
interface 10GE1/0/2
 port link-type hybrid
```

```
port hybrid pvid vlan 100
port hybrid untagged vlan 100
#
ip route-static 0.0.0.0 0.0.0.0 10.10.20.2
#
return
```

DeviceB 的配置文件

```
#
sysname DeviceB
#
vlan batch 200
#
dhcp enable
#
ip pool pool1
gateway-list 10.20.20.1
network 10.20.20.0 mask 255.255.255.0
option121 ip-address 10.10.20.0 24 10.20.20.1
#
interface Vlanif200
ip address 10.10.20.2 255.255.255.0
dhcp select global
#
interface 10GE1/0/1
port link-type hybrid
port hybrid pvid vlan 200
port hybrid untagged vlan 200
#
ip route-static 10.20.20.0 255.255.255.0 10.10.20.1
#
return
```

1.1.5.7.2.5 举例：配置 VRRP 组网中的 DHCPv4 服务器

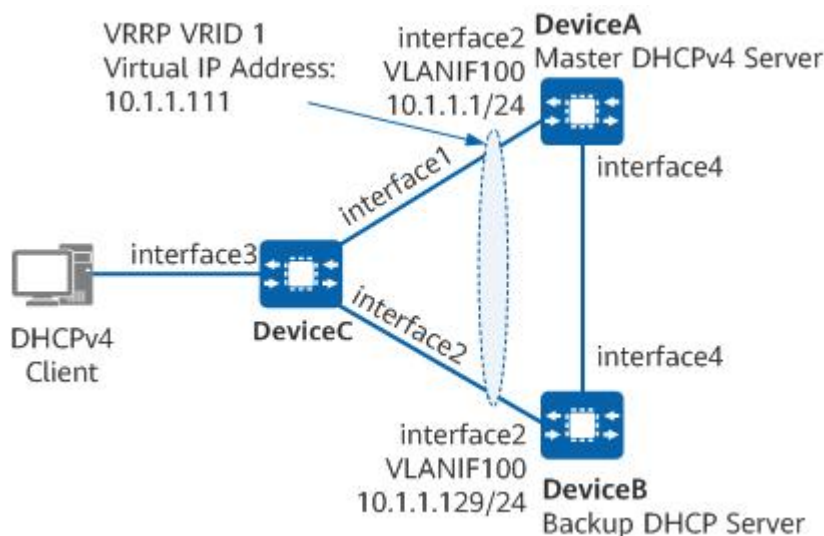
组网需求

如图 1 所示，某企业内的一台主机通过 DeviceC 双归属到 DeviceA 和 DeviceB。其中 DeviceA 为主设备，作为 DHCPv4 服务器为客户端分配 IPv4 地址。用户希望当主设备 DeviceA 故障时，客户端能够通过备设备 DeviceB 重新获取 IPv4 地址。

图 1 配置 VRRP 组网中的 DHCPv4 服务器组网图

说明

本例中 interface1, interface2, interface3 和 interface4 分别代表 10GE1/0/1, 10GE1/0/2, 10GE1/0/3 和 10GE1/0/4。



配置思路

采用如下思路配置 VRRP 组网中的 DHCPv4 服务器：

1. 配置 DeviceA 和 DeviceB 的接口 IPv4 地址，并且配置 DeviceC 的二层透传功能，使各设备间网络层连通。
2. 在 DeviceA 和 DeviceB 上配置 VRRP 备份组。其中，DeviceA 上配置较高优先级，作为 Master 设备为客户端分配 IPv4 地址；DeviceB 上配置较低优先级，作为备用设备。
3. 在 DeviceA 和 DeviceB 上创建全局地址池，并配置地址池相关属性。
4. 在 DeviceA、DeviceB 和 DeviceC 上配置破环协议，防止环路的产生（本举例以配置 STP 为例）。

操作步骤

1. 配置设备间的网络互连

配置 DeviceA 的接口 IPv4 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 100
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 100
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10GE 1/0/4
[DeviceA-10GE1/0/4] portswitch
```

```
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 100
[DeviceA-10GE1/0/4] quit
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] ip address 10.1.1.1 24
[DeviceA-Vlanif100] quit
```

配置 DeviceB 的接口 IPv4 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 100
[DeviceB] interface 10GE 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 100
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10GE 1/0/4
[DeviceB-10GE1/0/4] portswitch
[DeviceB-10GE1/0/4] port link-type trunk
[DeviceB-10GE1/0/4] port trunk allow-pass vlan 100
[DeviceB-10GE1/0/4] quit
[DeviceB] interface vlanif 100
[DeviceB-Vlanif100] ip address 10.1.1.129 24
[DeviceB-Vlanif100] quit
```

配置 DeviceC 的二层透传功能。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 100
[DeviceC] interface 10GE 1/0/1
[DeviceC-10GE1/0/1] portswitch
[DeviceC-10GE1/0/1] port link-type trunk
[DeviceC-10GE1/0/1] port trunk allow-pass vlan 100
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10GE 1/0/2
[DeviceC-10GE1/0/2] portswitch
[DeviceC-10GE1/0/2] port link-type trunk
[DeviceC-10GE1/0/2] port trunk allow-pass vlan 100
[DeviceC-10GE1/0/2] quit
[DeviceC] interface 10GE 1/0/3
[DeviceC-10GE1/0/3] portswitch
[DeviceC-10GE1/0/3] port link-type access
[DeviceC-10GE1/0/3] port default vlan 100
```

```
[DeviceC-10GE1/0/3] quit
```

2. 配置地址池

在 DeviceA 上配置地址池。使能 DHCPv4 功能，创建地址池并配置地址池范围为 10.1.1.2 ~ 10.1.1.128，使 DeviceA 的地址池范围与 DeviceB 上配置的地址池范围不重合。

说明

由于主设备上的地址池信息不能实时备份到备设备上，为防止主备切换后出现 IPv4 地址分配冲突，主设备和备设备上配置的地址池必须要互相排除。

```
[DeviceA] dhcp enable
[DeviceA] ip pool pool1
[DeviceA-ip-pool-pool1] network 10.1.1.0 mask 255.255.255.0
[DeviceA-ip-pool-pool1] gateway-list 10.1.1.111
[DeviceA-ip-pool-pool1] excluded-ip-address 10.1.1.1
[DeviceA-ip-pool-pool1] excluded-ip-address 10.1.1.129 10.1.1.254
[DeviceA-ip-pool-pool1] lease day 10
[DeviceA-ip-pool-pool1] quit
```

在 DeviceB 上配置地址池。使能 DHCPv4 功能，创建地址池并配置地址池范围为 10.1.1.130 ~ 10.1.1.254，使 DeviceB 的地址池范围与 DeviceA 上配置的地址池范围不重合。

```
[DeviceB] dhcp enable
[DeviceB] ip pool pool1
[DeviceB-ip-pool-pool1] network 10.1.1.0 mask 255.255.255.0
[DeviceB-ip-pool-pool1] gateway-list 10.1.1.111
[DeviceB-ip-pool-pool1] excluded-ip-address 10.1.1.1 10.1.1.110
[DeviceB-ip-pool-pool1] excluded-ip-address 10.1.1.112 10.1.1.129
[DeviceB-ip-pool-pool1] lease day 10
[DeviceB-ip-pool-pool1] quit
```

3. 配置 VRRP 备份组

在 DeviceA 上创建 VRRP 备份组 1，配置 DeviceA 在该备份组中的优先级为 120，并配置客户端从全局地址池中获取 IPv4 地址。

```
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[DeviceA-Vlanif100] vrrp vrid 1 priority 120
[DeviceA-Vlanif100] vrrp vrid 1 authentication-mode md5 YsH_2022
[DeviceA-Vlanif100] dhcp select global
[DeviceA-Vlanif100] quit
```

在 DeviceB 上创建 VRRP 备份组 1，配置 DeviceB 在该备份组中的优先级为缺省值 100，并配置客户端从全局地址池中获取 IPv4 地址。

```
[DeviceB] interface vlanif 100
[DeviceB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[DeviceB-Vlanif100] vrrp vrid 1 authentication-mode md5 YsH_2022
```

```
[DeviceB-Vlanif100] dhcp select global
[DeviceB-Vlanif100] quit
```

4. 配置 STP 协议

在 DeviceA 上全局使能 STP 功能，实现破除环路。

```
[DeviceA] stp enable
```

在 DeviceB 上全局使能 STP 功能，实现破除环路。

```
[DeviceB] stp enable
```

在 DeviceC 上全局使能 STP 功能，实现破除环路。

```
[DeviceC] stp enable
```

在 DeviceC 的接口 10GE1/0/3 上去使能 STP，并且将接口 10GE1/0/1 的路径开销值配置为 20000。

```
[DeviceC] interface 10GE 1/0/3
[DeviceC-10GE1/0/3] stp disable
[DeviceC-10GE1/0/3] quit
[DeviceC] interface 10GE 1/0/1
[DeviceC-10GE1/0/1] stp cost 20000
[DeviceC-10GE1/0/1] quit
```

检查配置结果

在 DeviceA 和 DeviceB 上分别执行 **display vrrp** 命令，可以看到 DeviceA 在备份组中的状态为 Master，DeviceB 在备份组中的状态为 Backup。

```
[DeviceA] display vrrp verbose
Vlanif100 | Virtual Router 1
State      : Master
Virtual IP  : 10.1.1.111
Master IP   : 10.1.1.1
PriorityRun  : 120
PriorityConfig : 120
MasterPriority : 120
Preempt     : YES Delay Time : 0s Remain : --
Hold Multiplier: 3
TimerRun    : 1s
TimerConfig : 1s
Auth Type   : MD5 Auth Key : *****
Virtual MAC  : 00e-fc00-0101
Check TTL   : YES
Config Type  : Normal
Create Time  : 2020-05-12 16:22:11
Last Change Time : 2020-05-12 16:22:11
```



```
[DeviceB] display vrrp verbose
Vlanif100 | Virtual Router 1
State      : Backup
Virtual IP  : 10.1.1.111
Master IP   : 10.1.1.1
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt     : YES Delay Time : 0s Remain : --
Hold Multiplier: 3
TimerRun    : 1s
TimerConfig : 1s
Auth Type   : MD5 Auth Key : *****
Virtual MAC  : 00e-fc00-0101
Check TTL   : YES
Config Type  : Normal
Create Time  : 2020-05-12 16:22:11
Last Change Time : 2020-05-12 16:22:11
```

在 DeviceA 和 DeviceB 上使用 **display ip pool** 命令用来查看地址池中的 IPv4 地址分配情况，可以看到作为主设备的 DeviceA 成功为 DHCPv4 客户端分配了 IPv4 地址，而作为备设备的 DeviceB 则没有为 DHCPv4 客户端分配 IPv4 地址。

```
[DeviceA] display ip pool
-----
Pool-name      : pool1
Pool-No        : 0
Lease          : 10 Days 0 Hours 0 Minutes
Position       : Local
Status         : Unlocked
Gateway-0      : 10.1.1.111
Network        : 10.1.1.0
Mask           : 255.255.255.0
VPN instance   : --
Conflicted address recycle interval: -
Address Statistic: Total    :253    Used      :1
                  Idle      :125     Expired    :0
                  Conflict   :0       Disabled   :127

IP address Statistic
Total           :253
Used            :1    Idle      :125
Expired         :0    Conflict  :0    Disabled :127
```

```
[DeviceB] display ip pool
```

```
-----
Pool-name      : pool1
Pool-No       : 0
Lease         : 10 Days 0 Hours 0 Minutes
Position      : Local
Status        : Unlocked
Gateway-0     : 10.1.1.111
Network       : 10.1.1.0
Mask          : 255.255.255.0
VPN instance   : --
Address Statistic: Total   :253   Used    :0
                  Idle     :125   Expired   :0
                  Conflict  :0     Disabled  :128
```

```
IP address Statistic
```

```
Total      :253
Used        :0   Idle      :125
Expired     :0   Conflict   :0   Disabled  :128
```

在 DeviceA 的接口 10GE1/0/2 和接口 10GE1/0/4 上执行 **shutdown** 命令，模拟 DeviceA 出现故障后，在 DeviceB 上执行 **display vrrp** 命令查看 VRRP 状态信息。可以看到 DeviceB 的状态是 Master。

```
[DeviceA] interface 10GE 1/0/2
```

```
[DeviceA-10GE1/0/2] shutdown
```

```
[DeviceA-10GE1/0/2] quit
```

```
[DeviceA] interface 10GE 1/0/4
```

```
[DeviceA-10GE1/0/4] shutdown
```

```
[DeviceA-10GE1/0/4] quit
```

```
[DeviceB] display vrrp verbose
```

```
Vlanif100 | Virtual Router 1
```

```
State      : Master
```

```
Virtual IP  : 10.1.1.111
```

```
Master IP   : 10.1.1.1
```

```
PriorityRun  : 100
```

```
PriorityConfig : 100
```

```
MasterPriority : 100
```

```
Preempt      : YES Delay Time : 0s Remain : --
```

```
Hold Multiplier: 3
```

```
TimerRun     : 1s
```

```
TimerConfig  : 1s
```

```
Auth Type    : NONE
```

```
Virtual MAC   : 00e-fc00-0101
```

Check TTL : YES
Config Type : Normal
Create Time : 2020-05-12 16:27:11
Last Change Time : 2020-05-12 16:27:11

在 DeviceB 上使用 **display ip pool** 命令用来查看全局地址池配置情况。

[DeviceB] display ip pool

```
-----  
Pool-name      : pool1  
Pool-No       : 0  
Lease         : 10 Days 0 Hours 0 Minutes  
Position      : Local  
Status        : Unlocked  
Gateway-0     : 10.1.1.111  
Network       : 10.1.1.0  
Mask          : 255.255.255.0  
VPN instance  : --  
Address Statistic: Total   :253   Used    :1  
                  Idle    :124   Expired  :0  
                  Conflict :0     Disabled :128
```

IP address Statistic

```
Total   :253  
Used    :1   Idle   :124  
Expired :0   Conflict :0   Disabled :128
```

配置脚本

DeviceA 的配置文件

```
#  
sysname DeviceA  
#  
vlan batch 100  
#  
dhcp enable  
#  
ip pool pool1  
gateway-list 10.1.1.111  
network 10.1.1.0 mask 255.255.255.0  
excluded-ip-address 10.1.1.1  
excluded-ip-address 10.1.1.129 10.1.1.254  
lease day 10 hour 0 minute 0
```

```
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 priority 120
 vrrp vrid 1 authentication-mode
md5 %+%##!!!!!!!"!!!!"!!!!*!!!!%M)\5[{0vYb}[6P0eY{3bKEQAGvMD,>,NTS!!!!2jp5!!!!9!!!!h*0u$>G#Qrhz
@F'+1JTXy!#3i=0.F!!!!!!!"%+%#
 dhcp select global
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface 10GE1/0/4
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

DeviceB 的配置文件

```
#
sysname DeviceB
#
vlan batch 100
#
dhcp enable
#
ip pool pool1
 gateway-list 10.1.1.111
 network 10.1.1.0 mask 255.255.255.0
 excluded-ip-address 10.1.1.1 10.1.1.110
 excluded-ip-address 10.1.1.112 10.1.1.129
 lease day 10 hour 0 minute 0
#
interface Vlanif100
 ip address 10.1.1.129 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.111
 vrrp vrid 1 authentication-mode
md5 %+%##!!!!!!!"!!!!"!!!!*!!!!%M)\5[{0vYb}[6P0eY{3bKEQAGvMD,>,NTS!!!!2jp5!!!!9!!!!h*0u$>G#Qrhz
@F'+1JTXy!#3i=0.F!!!!!!!"%+%#
 dhcp select global
#
```

```
interface 10GE1/0/2
port link-type trunk
port trunk allow vlan 100
#
interface 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 100
#
return
```

DeviceC 的配置文件

```
#
sysname DeviceC
#
vlan batch 100
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
stp instance 0 cost 20000
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/3
port link-type access
port default vlan 100
stp disable
#
return
```

1.1.5.7.3 DHCP Snooping

举例：配置 DHCP Snooping 的攻击防范功能示例

1.1.5.7.3.1 举例：配置 DHCP Snooping 的攻击防范功能示例

组网需求

如图 1 所示，DeviceA 与 DeviceB 是二层交换机，DeviceC 是用户网关，作为 DHCP Relay 向 DHCP 服务器转发 DHCP 报文，使得 DHCP 客户端可以从 DHCP 服务器上申请到 IP 地址等相关配置信息。

然而网络中可能会存在针对 DHCP 的攻击，例如：

DHCP Server 仿冒者攻击：在网络上随意添加一台 DHCP 服务器，它可以为客户端分配 IP 地址以及其他网络参数。如果该 DHCP 服务器为用户分配错误的 IP 地址和其他网络参数，将会对网络造成非常大的危害。

DHCP 报文泛洪攻击：若攻击者短时间内向设备发送大量的 DHCP 报文，将会对设备的性能造成巨大的冲击以致可能会导致设备无法正常工作。

仿冒 DHCP 报文攻击：如果攻击者冒充合法用户不断向 DHCP Server 发送 DHCP Request 报文来续租 IP 地址，会导致这些到期的 IP 地址无法正常回收，以致一些合法用户不能获得 IP 地址；而若攻击者仿冒合法用户的 DHCP Release 报文发往 DHCP Server，将会导致用户异常下线。

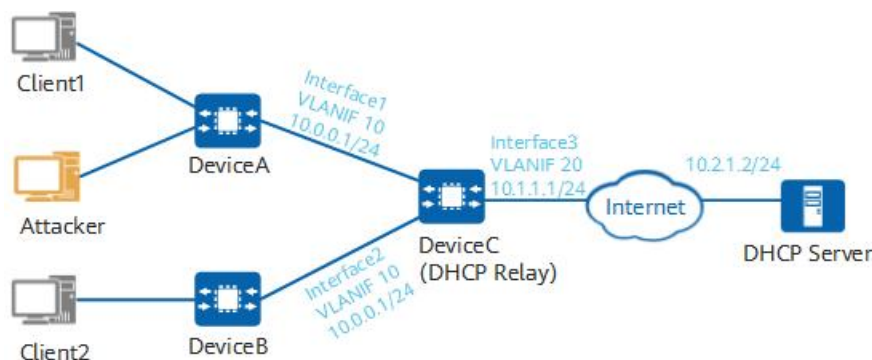
DHCP Server 服务拒绝攻击：当存在大量攻击者恶意申请 IP 地址或者某一攻击者通过不断改变 CHADDR 字段向 DHCP Server 申请 IP 地址，会导致 DHCP Server 中 IP 地址快速耗尽而不能为其他合法用户分配 IP 地址。

为了向 DHCP 用户提供更优质的服务，网络管理员可以通过配置 DHCP Snooping 功能，实现 DHCP 攻击防范。

图 1 配置 DHCP Snooping 的攻击防范功能组网图

说明

本例中 Interface1、Interface2 和 Interface3 分别代表 10GE1/0/1、10GE1/0/2 和 10GE1/0/3。



配置思路

采用如下思路配置 DHCP Snooping 攻击防范功能：

1. 配置 DHCP 中继功能，实现 DeviceC 转发不同网段的 DHCP 报文给 DHCP 服务器。
2. 配置 DHCP Snooping 的基本功能，防止 DHCP Server 仿冒者攻击。同时可以启用 ARP 与 DHCP Snooping 的联动功能，保证 DHCP 用户在异常下线时实时更新绑定表。还可以配置丢弃 GIADDR 字段非零的 DHCP 报文，防止非法用户攻击。
3. 配置 DHCP 报文上送 DHCP 报文处理单元的最大允许速率，防止 DHCP 报文泛洪攻击。同时可以启用丢弃报文告警功能，当丢弃的 DHCP 报文数达到告警阈值时产生告警信息。
4. 开启对 DHCP 报文进行绑定表匹配检查的功能，防止仿冒 DHCP 报文攻击。同时可以启用与绑定表不匹配而被丢弃的 DHCP 报文数达到阈值时产生告警信息功能。

5. 配置允许接入的最大用户数以及开启检测 DHCP Request 报文帧头源 MAC 地址与 CHADDR 字段是否一致功能，防止 DHCP Server 服务拒绝攻击。

本例仅 DeviceC 的配置。关于 DHCP 服务器的配置，本例中不予以详细介绍，只给出需要的步骤描述。

操作步骤

1. 配置 DHCP 中继功能。

配置 DHCP 中继功能。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 10 20
[DeviceC] interface 10GE 1/0/1
[DeviceC-10GE1/0/1] port link-type access
[DeviceC-10GE1/0/1] port default vlan 10
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10GE 1/0/2
[DeviceC-10GE1/0/2] port link-type access
[DeviceC-10GE1/0/2] port default vlan 10
[DeviceC-10GE1/0/2] quit
[DeviceC] interface 10GE 1/0/3
[DeviceC-10GE1/0/3] port link-type access
[DeviceC-10GE1/0/3] port default vlan 20
[DeviceC-10GE1/0/3] quit
[DeviceC] dhcp enable
[DeviceC] interface vlanif 10
[DeviceC-Vlanif10] ip address 10.0.0.1 255.255.255.0
[DeviceC-Vlanif10] dhcp select relay
[DeviceC-Vlanif10] quit
[DeviceC] interface vlanif 20
[DeviceC-Vlanif20] ip address 10.1.1.1 255.255.255.0
[DeviceC-Vlanif20] dhcp select relay
[DeviceC-Vlanif20] quit
[DeviceC] ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
```

DHCP 服务器 IP 地址配置为 10.2.1.2/24，同时配置一个 IP 地址范围为 10.0.1.0/24 的地址池，地址池中网关配置为 10.0.0.1。

2. 开启 DHCP Snooping 基本功能。

开启全局 DHCP Snooping 功能。

```
[DeviceC] dhcp snooping enable
```

开启用户侧接口的 DHCP Snooping 功能。以 10GE1/0/1 接口为例，10GE1/0/2 的配置与 10GE1/0/1 接口相同，不再赘述。

```
[DeviceC] interface 10GE 1/0/1
```

```
[DeviceC-10GE1/0/1] dhcp snooping enable
```

开启 ARP 与 DHCP Snooping 的联动功能。

```
[DeviceC-10GE1/0/1] dhcp snooping user-bind arp-detect enable
```

开启检测 DHCP Request 报文中 GIADDR 字段是否非零的功能。

```
[DeviceC-10GE1/0/1] dhcp snooping check dhcp-giaddr enable
```

3. 开启对 DHCP 报文进行绑定表匹配检查功能。

在用户侧接口进行配置。

```
[DeviceC-10GE1/0/1] dhcp snooping check dhcp-request enable
```

4. 配置接口允许接入的最大用户数并使能对 CHADDR 字段检查功能。

在用户侧接口进行配置。

```
[DeviceC-10GE1/0/1] dhcp snooping user-bind max-number 20
```

```
[DeviceC-10GE1/0/1] dhcp snooping check dhcp-chaddr enable
```

```
[DeviceC-10GE1/0/1] quit
```

5. 验证配置结果。

查看 DHCP Snooping 的配置信息。

```
[DeviceC] display dhcp snooping configuration
```

```
#
```

```
dhcp snooping enable
```

```
#
```

```
interface 10GE1/0/1
```

```
dhcp snooping enable
```

```
dhcp snooping check dhcp-giaddr enable
```

```
dhcp snooping check dhcp-request enable
```

```
dhcp snooping check dhcp-chaddr enable
```

```
dhcp snooping user-bind max-number 20
```

```
#
```

```
interface 10GE1/0/2
```

```
dhcp snooping enable
```

```
dhcp snooping check dhcp-giaddr enable
```

```
dhcp snooping check dhcp-request enable
```

```
dhcp snooping check dhcp-chaddr enable
```

```
dhcp snooping user-bind max-number 20
```

```
#
```

查看接口下的 DHCP Snooping 运行信息。可以看到 Check dhcp-giaddr、Check dhcp-chaddr 和 Check dhcp-request 字段都为 Enable。以接口 10GE1/0/1 的回显为例：

```
[DeviceC] display dhcp snooping interface 10GE 1/0/1
```

```
DHCP snooping running information for interface 10GE1/0/1 :
```



```
DHCP snooping          : Enable
Trusted interface       : No
Dhcp user max number    : 20
Current dhcp and nd user number : 0
Check dhcp-giaddr       : Enable
Check dhcp-chaddr       : Enable
Check dhcp-request      : Enable
```

配置脚本

DeviceC

```
#
sysname DeviceC
#
vlan batch 10 20
#
dhcp enable
#
dhcp snooping enable
#
interface Vlanif 10
 ip address 10.0.0.1 255.255.255.0
 dhcp select relay
#
interface Vlanif 20
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE 1/0/1
 port default vlan 10
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping user-bind max-number 20
#
interface 10GE 1/0/2
 port default vlan 10
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
 dhcp snooping check dhcp-request enable
 dhcp snooping check dhcp-chaddr enable
 dhcp snooping user-bind max-number 20
```

```
#
interface 10GE 1/0/3
 port default vlan 20
#
ip route-static 0.0.0.0 0.0.0.0 10.1.1.1
#
return
```

1.1.5.7.4 ACL

举例：使用基本 ACL 限制 FTP 访问权限

举例：使用高级 ACL 限制用户在特定时间访问特定服务器的权限

举例：使用二层 ACL 禁止特定用户上网

举例：配置特定时间段允许个别用户上网

举例：使用高级 ACL 限制不同网段的用户互访

举例：使用基本 ACL 限制内网主机访问外网网站

举例：使用高级 ACL 限制外网用户访问内网中服务器的权限

1.1.5.7.4.1 举例：使用基本 ACL 限制 FTP 访问权限

组网需求

如[图 1](#)所示，Switch 作为 FTP 服务器，对网络中的不同用户开放不同的访问权限：

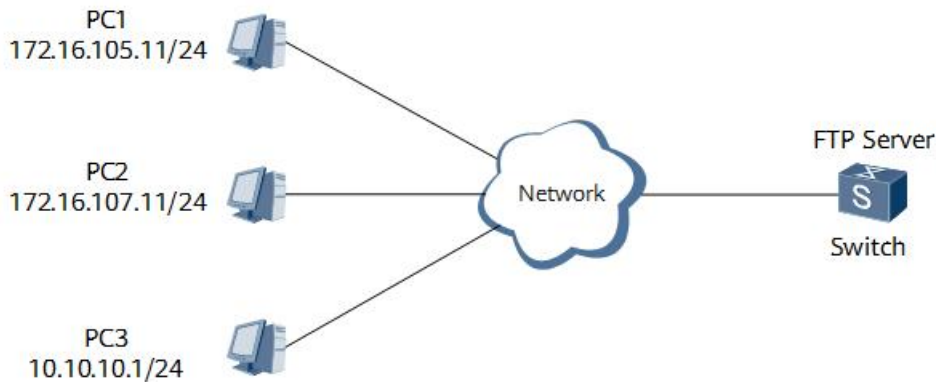
子网 1（172.16.105.11/24）的所有用户在任意时间都可以访问 FTP 服务器。

子网 2（172.16.107.11/24）的所有用户只能在某一个时间范围内访问 FTP 服务器。

其他用户不可以访问 FTP 服务器。

已知 Switch 与各个子网之间路由可达，要求在 Switch 上进行配置，实现 FTP 服务器对客户端访问权限的设置。

图 1 使用基本 ACL 限制 FTP 访问权限组网图



说明

需要先在全局视图下执行命令 **install feature-software WEAKEA** 安装弱安全算法/协议特性包（WEAKEA）后才能使用 FTP 协议。

操作步骤

1. 配置时间段。

```
<HUAWEI> system-view
[ ] sysname Switch
[Switch] time-range ftp-access from 0:0 2023/1/1 to 23:59 2023/12/31
[Switch] time-range ftp-access 14:00 to 18:00 off-day
```

2. 配置基本 ACL。

```
[Switch] acl number 2001
[Switch-acl-number-2001] rule permit source 172.16.105.0 0.0.0.255
[Switch-acl-number-2001] rule permit source 172.16.107.0 0.0.0.255 time-range ftp-access
[Switch-acl-number-2001] rule deny source any
[Switch-acl-number-2001] quit
```

3. 配置 FTP 基本功能。

```
[Switch] ftp server enable
[Switch] ftp server source -i Vlanif 10
[Switch] aaa
[Switch-aaa] local-user huawei password irreversible-cipher SetUserPassword@123
[Switch-aaa] local-user huawei privilege level 15
[Switch-aaa] local-user huawei service-type ftp
[Switch-aaa] local-user huawei ftp-directory cfcad:/
[Switch-aaa] quit
```

4. 配置 FTP 服务器访问权限。

```
[Switch] ftp server acl 2001
```

检查配置结果

在子网 1 的 PC1 (172.16.105.11/24) 上执行 **ftp 172.16.104.110** 命令，可以连接 FTP 服务器。

2023 年某个周一在子网 2 的 PC2 (172.16.107.11/24) 上执行 **ftp 172.16.104.110** 命令，不能连接 FTP 服务器；2023 年某个周六下午 15:00 在子网 2 的 PC2 (172.16.107.11/24) 上执行 **ftp 172.16.104.110** 命令，可以连接 FTP 服务器。

在 PC3 (10.10.10.1/24) 上执行 **ftp 172.16.104.110** 命令，不能连接 FTP 服务器。

配置脚本

Switch 的配置脚本

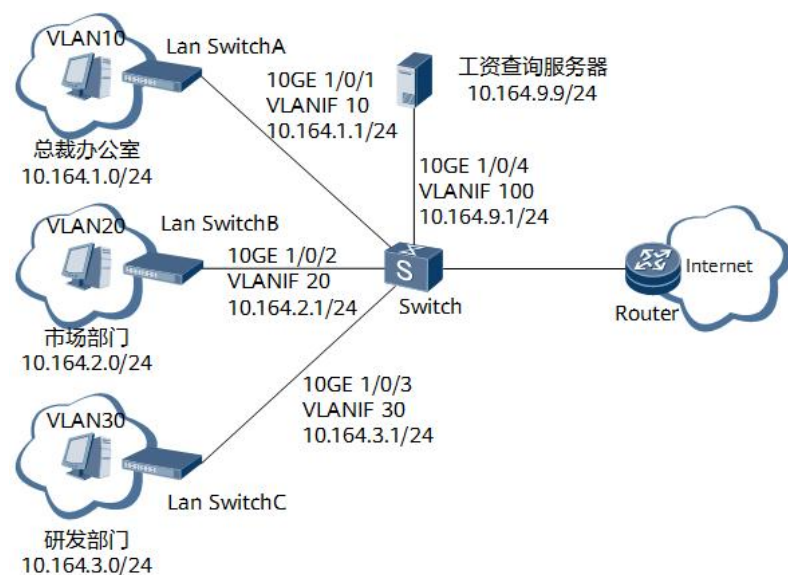
```
#
sysname Switchh
#
FTP server enable
FTP server-source -i Vlanif 10
FTP acl 2001
#
time-range ftp-access 14:00 to 18:00 off-day
time-range ftp-access from 00:00 2023/1/1 to 23:59 2023/12/31
#
acl number 2001
rule 5 permit source 172.16.105.0 0.0.0.255
rule 10 permit source 172.16.107.0 0.0.0.255 time-range ftp-access
rule 15 deny
#
aaa
local-user huawei password irreversible-cipher SetUserPassword@123
local-user huawei privilege level 15
local-user huawei ftp-directory cfcad:/
local-user huawei service-type ftp
#
return
```

1.1.5.7.4.2 举例：使用高级 ACL 限制用户在特定时间访问特定服务器的权限

组网需求

如[图 1](#)所示，某公司通过 Switch 实现各部门之间的互连。公司要求禁止研发部门和市场部门在上班时间内（8:00 至 17:30）访问工资查询服务器（IP 地址为 10.164.9.9），总裁办公室不受限制，可以随时访问。

图 1 使用高级 ACL 限制用户在特定时间访问特定服务器的权限组网图



配置思路

采用如下的思路在 Switch 上进行配置：

1. 配置时间段、高级 ACL 和基于 ACL 的流分类，使设备可以基于时间的 ACL，对用户访问服务器的报文进行过滤，从而限制不同用户在特定时间访问特定服务器的权限。
2. 配置流行为，拒绝匹配上 ACL 的报文通过。
3. 配置并应用流策略，使 ACL 和流行为生效。

操作步骤

1. 配置接口加入 VLAN，并配置 VLANIF 接口的 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20 30 100
[Switch] interface 10GE 1/0/1
[Switch-10GE1/0/1] port link-type trunk
[Switch-10GE1/0/1] port trunk allow-pass vlan 10
[Switch-10GE1/0/1] quit
[Switch] interface vlanif 10
[Switch-vlanif10] ip address 10.164.1.1 255.255.255.0
[Switch-vlanif10] quit
```

2. 配置时间段。

```
[Switch] time-range satime 8:00 to 17:30 working-day
```

3. 配置高级 ACL。

```
[Switch] acl 3002
```

```
[Switch-acl-adv-3002] rule deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-
range satime
[Switch-acl-adv-3002] quit
[Switch] acl 3003
[Switch-acl-adv-3003] rule deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0.0.0.0 time-
range satime
[Switch-acl-adv-3003] quit
```

4. 配置基于高级 ACL 的流分类。

```
[Switch] traffic classifier c_market
[Switch-classifier-c_market] if-match acl 3002
[Switch-classifier-c_market] quit
[Switch] traffic classifier c_rd
[Switch-classifier-c_rd] if-match acl 3003
[Switch-classifier-c_rd] quit
```

5. 配置流行为。

```
[Switch] traffic behavior b_market
[Switch-behavior-b_market] deny
[Switch-behavior-b_market] quit
[Switch] traffic behavior b_rd
[Switch-behavior-b_rd] deny
[Switch-behavior-b_rd] quit
```

6. 配置流策略。

```
[Switch] traffic policy p_market
[Switch-policy-p_market] classifier c_market behavior b_market
[Switch-policy-p_market] quit
[Switch] traffic policy p_rd
[Switch-policy-p_rd] classifier c_rd behavior b_rd
[Switch-policy-p_rd] quit
```

7. 应用流策略。

```
[Switch] interface 10GE 1/0/2
[Switch-10GE1/0/2] traffic-policy p_market inbound
[Switch-10GE1/0/2] quit
[Switch] interface 10GE 1/0/3
[Switch-10GE1/0/3] traffic-policy p_rd inbound
[Switch-10GE1/0/3] quit
```

检查配置结果

查看 ACL 规则的配置信息。

[Switch] **display acl all**

Total nonempty ACL number is 2

Advanced ACL 3002, 1 rule

Acl's step is 5

rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range satime (Active)(0 times matched)

Advanced ACL 3003, 1 rule

Acl's step is 5

rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime (Active)(0 times matched)

查看流分类的配置信息。

[Switch] **display traffic classifier**

User Defined Classifier Information:

Classifier: c_market

Precedence: 5

Operator: OR

Rule(s) : if-match acl 3002

Classifier: c_rd

Precedence: 5

Operator: OR

Rule(s) : if-match acl 3003 T

Total classifier number is 2

查看流策略的配置信息。

[Switch] **display traffic policy**

User Defined Traffic Policy Information:

Policy: p_market

Classifier: c_market

Operator: OR

Behavior: b_market

Deny

Policy: p_rd

Classifier: c_rd

Operator: OR

Behavior: b_rd

Deny

Total policy number is 2

查看流策略的应用信息。

```
[Switch] display traffic-policy applied-record
Total records : 2
-----
-----
Policy Type/Name          Apply Parameter          Slot State
-----
-----
p_market                  10GE1/1/0/6(IN)         1/5 fail
-----
-----
p_rd                      10GE1/1/0/7(IN)         1/5 fail
-----
-----
```

研发部门和市场部门在上班时间（ 8:00 至 17:30 ）无法访问工资查询服务器。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 10 20 30 100
#
time-range satime 08:00 to 17:30 working-day
#
acl number 3002
 rule 5 deny ip source 10.164.2.0 0.0.0.255 destination 10.164.9.9 0 time-range satime
acl number 3003
 rule 5 deny ip source 10.164.3.0 0.0.0.255 destination 10.164.9.9 0 time-range satime
#
traffic classifier c_market operator or precedence 5
 if-match acl 3002
traffic classifier c_rd operator or precedence 5
 if-match acl 3003
#
traffic behavior b_market
 deny
traffic behavior b_rd
 deny
#
```



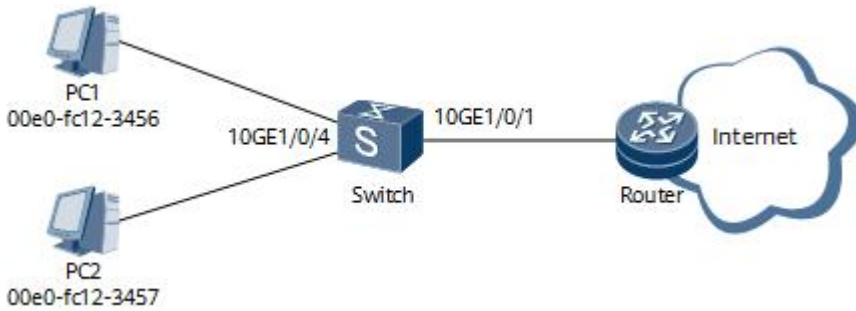
```
traffic policy p_market
mclassifier c_market behavior b_market
traffic policy p_rd
mclassifier c_rd behavior b_rd
#
interface Vlanif10
 ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
 ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
 ip address 10.164.9.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
 traffic-policy p_market inbound
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
 traffic-policy p_rd inbound
#
interface 10GE1/0/4
 port link-type trunk
 port trunk allow-pass vlan 100
#
return
```

1.1.5.7.4.3 举例：使用二层 ACL 禁止特定用户上网

组网需求

如图 1 所示，Switch 作为网关设备，下挂用户 PC，与各个子网之间路由可达。管理员发现 PC1（MAC 地址为 00e0-fc12-3456）用户是非法用户，要求禁止该用户上网。

图 1 使用二层 ACL 禁止特定用户上网组网图



配置思路

采用如下的思路在 Switch 上进行配置：

1. 配置二层 ACL 和基于 ACL 的流分类，使设备对 MAC 地址为 00e0-fc12-3456 的报文进行过滤，从而禁止该地址对应的用户上网。
2. 配置流行为，拒绝匹配上 ACL 的报文通过。
3. 配置并应用流策略，使 ACL 和流行为生效。

操作步骤

1. 配置二层 ACL。

配置符合要求的二层 ACL。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] acl 4000
[Switch-acl-L2-4000] rule deny source-mac 00e0-fc12-3456
[Switch-acl-L2-4000] quit
```

2. 配置基于二层 ACL 的流分类。

配置流分类 tc1，对匹配 ACL 4000 的报文进行分类。

```
[Switch] traffic classifier tc1
[Switch-classifier-tc1] if-match acl 4000
[Switch-classifier-tc1] quit
```

3. 配置流行为。

配置流行为 tb1，动作为拒绝报文通过。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] deny
[Switch-behavior-tb1] quit
```

4. 配置流策略。

配置流策略 tp1，将流分类 tc1 与流行为 tb1 关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

5. 应用流策略。

由于 PC1 的报文从 10GE1/0/4 进入 Switch 并流向 Internet，所以可以在接口 10GE1/0/4 的入方向应用流策略 tp1。

```
[Switch] interface 10GE 1/0/4
[Switch-10GE1/0/4] traffic-policy tp1 inbound
[Switch-10GE1/0/4] quit
```

6. 验证配置结果。

查看 ACL 规则的配置信息。

```
[Switch] display acl 4000
L2 ACL 4000, 1 rule
Acl's step is 5
rule 5 deny source-mac 00e0-fc12-3456
```

查看流分类的配置信息。

```
[Switch] display traffic classifier
User Defined Classifier Information:
Classifier: tc1
Type: OR
Rule(s) :
    if-match acl 4000

Total classifier number is 1
```

查看流策略的配置信息。

```
[Switch] display traffic policy tp1
User Defined Traffic Policy Information:
Policy: tp1
Classifier: tc1
Type: OR
Behavior: tb1
Deny
```

查看流策略的应用信息。

```
[Switch] display traffic-policy applied-record
Total record : 1

-----
Policy Type/Name:  Apply Parameter   Slot   State
```

```
-----  
tp1      10GE1/1/0/5(IN)  1/5  success  
-----
```

源 MAC 地址是 00e0-fc12-3456 的用户无法上网。

配置脚本

Switch 的配置脚本

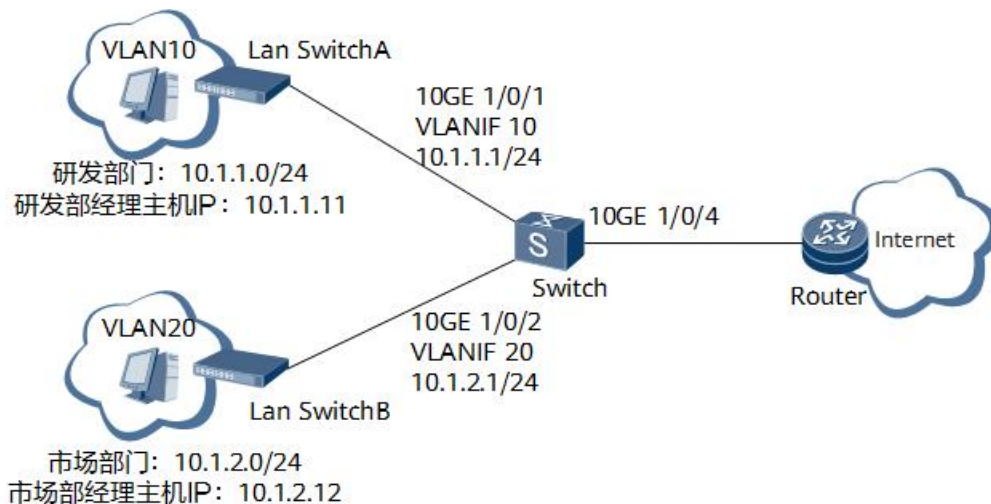
```
#  
sysname Switch  
  
#  
acl number 4000  
rule 5 deny source-mac 00e0-fc12-3456  
  
#  
traffic classifier tc1 type or  
if-match acl 4000  
  
#  
traffic behavior tb1  
deny  
  
#  
traffic policy tp1  
classifier tc1 behavior tb1 precedence 5  
  
#  
interface 10GE1/0/4  
traffic-policy tp1 inbound  
  
#  
return
```

1.1.5.7.4.4 举例：配置特定时间段允许个别用户上网

组网需求

如[图 1](#)所示，某公司通过 Switch 实现各部门之间的互连。公司要求在上班时间（周一至周五）所有员工均可以上网，但周末时间（周六和周日）仅允许各部门经理能够上网，其他用户不允许上网。

图 1 配置特定时间段允许个别用户上网组网图



配置思路

采用如下的思路在 Switch 上进行配置：

1. 配置时间段、基本 ACL 和基于 ACL 的流分类，使设备可以基于时间的 ACL，对公司用户访问外网的报文进行过滤，从而达到在特定时间段内仅允许个别用户上网的目的。
2. 配置流行为，允许匹配上 ACL 的 permit 规则的报文通过。
3. 配置并应用流策略，使 ACL 和流行为生效。

操作步骤

1. 配置接口所属的 VLAN 以及接口的 IP 地址

创建 VLAN10 和 VLAN20。

```

<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20
  
```

配置 Switch 的接口 10GE1/0/1、10GE1/0/2 为 trunk 类型接口，并分别加入 VLAN10 和 VLAN20；配置 Switch 的接口 10GE1/0/4 为 trunk 类型接口，加入 VLAN10 和 VLAN20。

```

[Switch] interface 10GE 1/0/1
[Switch-10GE1/0/1] port link-type trunk
[Switch-10GE1/0/1] port trunk allow-pass vlan 10
[Switch-10GE1/0/1] quit
[Switch] interface 10GE 1/0/2
[Switch-10GE1/0/2] port link-type trunk
[Switch-10GE1/0/2] port trunk allow-pass vlan 20
[Switch-10GE1/0/2] quit
[Switch] interface 10GE 1/0/4
[Switch-10GE1/0/4] port link-type trunk
[Switch-10GE1/0/4] port trunk allow-pass vlan 10 20
  
```

```
[Switch-10GE1/0/4] quit
```

创建 VLANIF10 和 VLANIF20，并配置各 VLANIF 接口的 IP 地址。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.1.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 10.1.2.1 24
[Switch-Vlanif20] quit
```

2. 配置时间段

配置周六至周日的周期时间段。

```
[Switch] time-range rest-time 0:00 to 23:59 off-day
```

3. 配置基本 ACL

创建基本 ACL 2001 并配置 ACL 规则，允许研发部和市场部经理主机（IP 地址为 10.1.1.11 和 10.1.2.12）在任意时间访问外网的报文通过，拒绝其他用户在周六和周日时间范围内访问外网的报文通过，即周六和周日仅允许研发部和市场部经理上网。

```
[Switch] acl 2001
[Switch-acl-basic-2001] rule permit source 10.1.1.11 0
[Switch-acl-basic-2001] rule permit source 10.1.2.12 0
[Switch-acl-basic-2001] rule deny time-range rest-time
[Switch-acl-basic-2001] quit
```

4. 配置基于基本 ACL 的流分类

配置流分类 tc1，对匹配 ACL 2001 的报文进行分类。

```
[Switch] traffic classifier tc1
[Switch-classifier-acl] if-match acl 2001
[Switch-classifier-acl] quit
```

5. 配置流行为

配置流行为 tb1，动作为允许报文通过（缺省值，不需配置）。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] quit
```

6. 配置流策略

定义流策略，将流分类与流行为关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

7. 在接口下应用流策略

由于内网主机访问外网的流量均从接口 10GE1/0/4 出口流向 Internet，所以可以在接口 10GE1/0/4 的出方向应用流策略 tp1。

```
[Switch] interface 10GE 1/0/4
```

```
[Switch-10GE1/0/4] traffic-policy tp1 outbound
[Switch-10GE1/0/4] quit
```

8. 验证配置结果

查看 ACL 规则的配置信息

```
[Switch] display acl 2001
Basic ACL 2001, 3 rules
Acl's step is 5
rule 5 permit source 10.1.1.11 0 (0 times matched)
rule 10 permit source 10.1.2.12 0 (0 times matched)
rule 15 deny time-range rest-time (Inactive) (0 times matched)
```

查看流分类的配置信息

```
[Switch] display traffic classifier
User Defined Classifier Information:
Classifier: tc1
Type: OR
Rule(s) :
    if-match acl 2001

Total classifier number is 1
```

查看流策略的配置信息

```
[Switch] display traffic policy tp1
User Defined Traffic Policy Information:
Policy: tp1
Classifier: tc1
Type: OR
Behavior: tb1
    Permit

Total policy number is 1
```

上班时间，所有员工都可以访问外网。周末时间，仅研发部和市场部经理主机（IP 地址为 10.1.1.11 和 10.1.2.12）可以访问外网。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 10 20
#
time-range rest-time 00:00 to 23:59 off-day
```

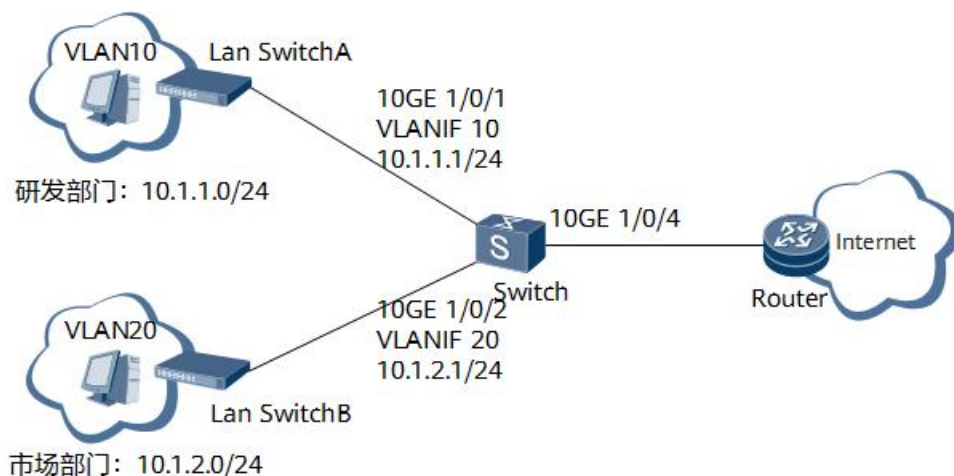
```
#
acl number 2001
 rule 5 permit source 10.1.1.11 0
 rule 10 permit source 10.1.2.12 0
 rule 15 deny time-range rest-time
#
traffic classifier tc1 type or
 if-match acl 2001
#
traffic behavior tb1
 permit
#
traffic policy tp1
 classifier tc1 behavior tb1 precedence 5
#
interface Vlanif10
 ip address 10.1.1.1 24
#
interface Vlanif20
 ip address 10.1.2.1 24
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface 10GE1/0/4
 port link-type trunk
 port trunk allow-pass vlan 10 20
 traffic-policy tp1 outbound
#
return
```

1.1.5.7.4.5 举例：使用高级 ACL 限制不同网段的用户互访

组网需求

如图 1 所示，某公司通过 Switch 实现各部门之间的互连。为方便管理网络，管理员为公司的研发部和市场部规划了两个网段的 IP 地址，两个部门划分在不同 VLAN 之中。要求通过配置限制两个网段之间互访，防止公司机密泄露。

图 1 使用高级 ACL 限制不同网段的用户互访组网图



配置思路

采用如下的思路在 Switch 上进行配置：

1. 配置高级 ACL 和基于 ACL 的流分类，使设备可以对研发部与市场部互访的报文进行过滤。
2. 配置流行为，拒绝匹配上 ACL 的报文通过。
3. 配置并应用流策略，使 ACL 和流行为生效。

操作步骤

1. 配置接口所属的 VLAN 以及接口的 IP 地址

创建 VLAN10 和 VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20
```

配置 Switch 的接口 10GE1/0/1 和 10GE1/0/2 为 trunk 类型接口，并分别加入 VLAN10 和 VLAN20。

```
[Switch] interface 10GE 1/0/1
[Switch-10GE1/0/1] port link-type trunk
[Switch-10GE1/0/1] port trunk allow-pass vlan 10
[Switch-10GE1/0/1] quit
[HUAWEISwitch] interface 10ge 1/0/2
[Switch-10GE1/0/2] port link-type trunk
[Switch-10GE1/0/2] port trunk allow-pass vlan 20
[Switch-10GE1/0/2] quit
```

创建 VLANIF10 和 VLANIF20，并配置各 VLANIF 接口的 IP 地址。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.1.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 10.1.2.1 24
[Switch-Vlanif20] quit
```

2. 配置高级 ACL

创建高级 ACL 3001 并配置 ACL 规则，拒绝任一部门访问另一部门的报文通过，这里以拒绝研发部访问市场部的报文通过为例。

```
[Switch] acl 3001
[Switch-acl-adv-3001] rule deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
[Switch-acl-adv-3001] quit
```

3. 配置基于高级 ACL 的流分类

配置流分类 tc1，对匹配 ACL 3001 的报文进行分类。

```
[Switch] traffic classifier tc1
[Switch-classifier-acl] if-match acl 3001
[Switch-classifier-acl] quit
```

4. 配置流行为

配置流行为 tb1，动作为拒绝报文通过。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] deny
[Switch-behavior-tb1] quit
```

5. 配置流策略

定义流策略，将流分类与流行为关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

6. 在接口下应用流策略

由于研发部访问市场部的流量从接口 10GE1/0/1 进入 Switch，所以在接口 10GE1/0/1 的入方向应用流策略。

```
[Switch] interface 10GE 1/0/1
[Switch-10GE1/0/1] traffic-policy tp1 inbound
[Switch-10GE1/0/1] quit
```

7. 验证配置结果

查看 ACL 规则的配置信息。

```
[Switch] display acl 3001
Advanced ACL 3001, 1 rule
```

Acl's step is 5

rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255 (0 times matched)

查看流分类的配置信息。

[Switch] **display traffic classifier**

User Defined Classifier Information:

Classifier: tc1

Type: OR

Rule(s) :

if-match acl 3001

Total classifier number is 1

查看流策略的配置信息。

[Switch] **display traffic policy tp1**

User Defined Traffic Policy Information:

Policy: tp1

Classifier: tc1

Type: OR

Behavior: tb1

Deny

研发部和市场部所在的两个网段之间不能互访，但是均可以与其他网段互访。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 10 20
#
acl number 3001
rule 5 deny ip source 10.1.1.0 0.0.0.255 destination 10.1.2.0 0.0.0.255
#
traffic classifier tc1 type or
if-match acl 3001
#
traffic behavior tb1
deny
#
traffic policy tp1
classifier tc1 behavior tb1 precedence 5
#
```

```

interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 traffic-policy tp1 inbound
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
return

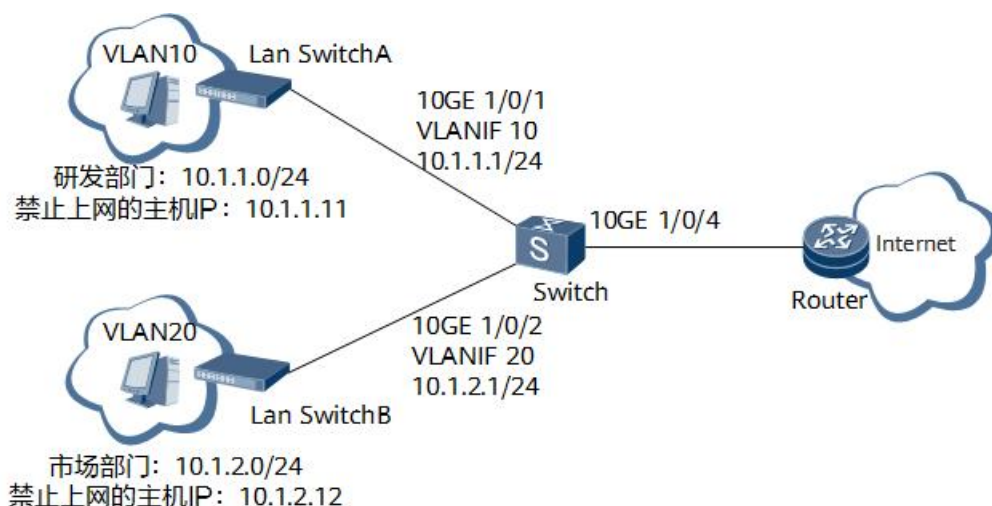
```

1.1.5.7.4.6 举例：使用基本 ACL 限制内网主机访问外网网站

组网需求

如图 1 所示，某公司通过 Switch 实现各部门之间的互连。现要求 Switch 能够禁止研发部和市场部的部分主机访问外网，防止公司机密泄露。

图 1 使用基本 ACL 限制内网主机访问外网网站组网图



配置思路

采用如下的思路在 Switch 上进行配置：

1. 配置基本 ACL 和基于 ACL 的流分类，使设备可以对研发部与市场部的指定主机的报文进行过滤。

2. 配置流行为，拒绝匹配上 ACL 的报文通过。
3. 配置并应用流策略，使 ACL 和流行为生效。

操作步骤

1. 配置接口所属的 VLAN 以及接口的 IP 地址

创建 VLAN10 和 VLAN20。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20
```

配置 Switch 的接口 10GE1/0/1、10GE1/0/2 为 trunk 类型接口，并分别加入 VLAN10 和 VLAN20；配置 Switch 的接口 10GE1/0/4 为 trunk 类型接口，加入 VLAN10 和 VLAN20。

```
[Switch] interface 10GE 1/0/1
[Switch-10GE1/0/1] port link-type trunk
[Switch-10GE1/0/1] port trunk allow-pass vlan 10
[Switch-10GE1/0/1] quit
[Switch] interface 10GE 1/0/2
[Switch-10GE1/0/2] port link-type trunk
[Switch-10GE1/0/2] port trunk allow-pass vlan 20
[Switch-10GE1/0/2] quit
[Switch] interface 10GE 1/0/4
[Switch-10GE1/0/4] port link-type trunk
[Switch-10GE1/0/4] port trunk allow-pass vlan 10 20
[Switch-10GE1/0/4] quit
```

创建 VLANIF10 和 VLANIF20，并配置各 VLANIF 接口的 IP 地址。

```
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.1.1.1 24
[Switch-Vlanif10] quit
[Switch] interface vlanif 20
[Switch-Vlanif20] ip address 10.1.2.1 24
[Switch-Vlanif20] quit
```

2. 配置基本 ACL

创建基本 ACL 2001 并配置 ACL 规则，拒绝源 IP 地址为 10.1.1.11 和 10.1.2.12 的主机的报文通过。

```
[Switch] acl 2001
[Switch-acl-basic-2001] rule deny source 10.1.1.11 0
[Switch-acl-basic-2001] rule deny source 10.1.2.12 0
[Switch-acl-basic-2001] quit
```

3. 配置基于基本 ACL 的流分类

配置流分类 tc1，对匹配 ACL 2001 的报文进行分类。

```
[Switch] traffic classifier tc1
```

```
[Switch-classifier-acl] if-match acl 2001
[Switch-classifier-acl] quit
```

4. 配置流行为

配置流行为 tb1，动作为拒绝报文通过。

```
[Switch] traffic behavior tb1
[Switch-behavior-tb1] deny
[Switch-behavior-tb1] quit
```

5. 配置流策略

定义流策略，将流分类与流行为关联。

```
[Switch] traffic policy tp1
[Switch-trafficpolicy-tp1] classifier tc1 behavior tb1
[Switch-trafficpolicy-tp1] quit
```

6. 在接口下应用流策略

由于内网主机访问外网的流量均从接口 10GE1/0/4 出口流向 Internet，所以可以在接口 10GE1/0/4 的出方向应用流策略。

```
[Switch] interface 10GE 1/0/4
[Switch-10GE1/0/4] traffic-policy tp1 outbound
[Switch-10GE1/0/4] quit
```

7. 验证配置结果

查看 ACL 规则的配置信息

```
[Switch] display acl 2001
Basic ACL 2001, 2 rules
Acl's step is 5
rule 5 permit source 10.1.1.11 0 (match-counter 0)
rule 10 permit source 10.1.2.12 0 (match-counter 0)
```

查看流分类的配置信息

```
[Switch] display traffic classifier
User Defined Classifier Information:
Classifier: tc1
Type: OR
Rule(s) :
    if-match acl 2001

Total classifier number is 1
```

查看流策略的配置信息

```
[Switch] display traffic policy tp1
User Defined Traffic Policy Information:
Policy: tp1
Classifier: tc1
```

```
Type: OR
Behavior: tb1
Deny
```

IP 地址为 10.1.1.11 和 10.1.2.12 的主机无法访问外网，其他主机均可以访问外网。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 10 20
#
acl number 2001
 rule 5 deny source 10.1.1.11 0
 rule 10 deny source 10.1.2.12 0
#
traffic classifier tc1 type or
 if-match acl 2001
#
traffic behavior tb1
 deny
#
traffic policy tp1
 classifier tc1 behavior tb1 precedence 5
#
interface Vlanif10
 ip address 10.1.1.1 24
#
interface Vlanif20
 ip address 10.1.2.1 24
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 20
#
interface 10GE1/0/4
 port link-type trunk
```

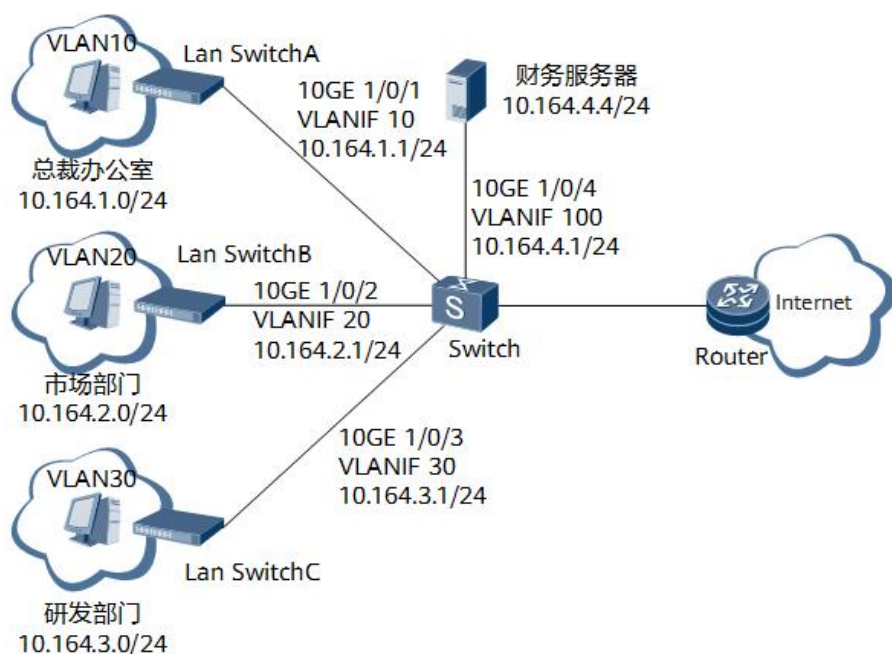
```
port trunk allow-pass vlan 10 20
traffic-policy tp1 outbound
#
return
```

1.1.5.7.4.7 举例：使用高级 ACL 限制外网用户访问内网中服务器的权限

组网需求

如图 1 所示，某公司通过 Switch 实现各部门之间的互连。要求只允许公司内网用户可以访问内网中的财务服务器，外网用户不允许访问。

图 1 使用高级 ACL 限制外网用户访问内网中服务器的权限组网图



配置思路

采用如下的思路在 Switch 上进行配置：

1. 配置高级 ACL 和基于 ACL 的流分类，使设备可以基于 ACL，对用户访问服务器的报文进行过滤，从而禁止外网用户访问该服务器。
2. 配置流行为，允许匹配上 ACL 的 permit 规则的报文通过。
3. 配置并应用流策略，使 ACL 和流行为生效。

操作步骤

1. 配置接口加入 VLAN，并配置 VLANIF 接口的 IP 地址

将 10GE1/0/1~10GE1/0/3 分别加入 VLAN10、20、30，10GE1/0/4 加入 VLAN100，并配置各 VLANIF 接口的 IP 地址。下面配置以 10GE1/0/1 和 VLANIF 10 接口为例，接口 10GE1/0/2、10GE1/0/3 和 10GE1/0/4 的配置与 10GE1/0/1 接口类似，接口 VLANIF 20、VLANIF 30 和 VLANIF 100 的配置与 VLANIF 10 接口类似，不再赘述。

```
<HUAWEI> system-view
[HUAWEI] sysname Switch
[Switch] vlan batch 10 20 30
[Switch] interface 10GE 1/0/1
[Switch-10GE1/0/1] port link-type trunk
[Switch-10GE1/0/1] port trunk allow-pass vlan 10
[Switch-10GE1/0/1] quit
[Switch] interface vlanif 10
[Switch-Vlanif10] ip address 10.164.1.1 255.255.255.0
[Switch-Vlanif10] quit
```

2. 配置高级 ACL

创建高级 ACL 3002 并配置 ACL 规则，允许位于内网的总裁办公室、市场部和研发部访问财务服务器的报文通过，拒绝外网用户访问财务服务器的报文通过。

```
[Switch] acl 3002
[Switch-acl-adv-3002] rule permit ip source 10.164.1.0 0.0.0.255 destination 10.164.4.4 0.0.0.0
[Switch-acl-adv-3002] rule permit ip source 10.164.2.0 0.0.0.255 destination 10.164.4.4 0.0.0.0
[Switch-acl-adv-3002] rule permit ip source 10.164.3.0 0.0.0.255 destination 10.164.4.4 0.0.0.0
[Switch-acl-adv-3002] rule deny ip source 10.164.4.4 0.0.0.0
[Switch-acl-adv-3002] quit
```

3. 配置高级 ACL 的流分类

配置流分类 c_network，对匹配 ACL 3002 的报文进行分类。

```
[Switch] traffic classifier c_network
[Switch-classifier-c_network] if-match acl 3002
[Switch-classifier-c_network] quit
```

4. 配置流行为

配置流行为 b_network，动作为允许报文通过（缺省值，不需配置）。

```
[Switch] traffic behavior b_network
[Switch-behavior-b_network] quit
```

5. 配置流策略

配置流策略 p_network，将流分类 c_network 与流行为 b_network 关联。

```
[Switch] traffic policy p_network
[Switch-trafficpolicy-p_network] classifier c_network behavior b_network
[Switch-trafficpolicy-p_network] quit
```

6. 应用流策略

由于内外网访问服务器的流量均从接口 10GE1/0/4 出口流向服务器，所以可以在 10GE1/0/4 接口的出方向应用流策略 p_network。

```
[Switch] interface 10GE 1/0/4
[Switch-10GE1/0/4] traffic-policy p_network outbound
[Switch-10GE1/0/4] quit
```

7. 验证配置结果

查看 ACL 规则的配置信息。

```
[Switch] display acl 3002
Advanced ACL 3002, 4 rules
Acl's step is 5
rule 5 permit ip source 10.164.1.0 0.0.0.255 destination 10.164.4.4 0 (0 times matched)
rule 10 permit ip source 10.164.2.0 0.0.0.255 destination 10.164.4.4 0 (0 times matched)
rule 15 permit ip source 10.164.3.0 0.0.0.255 destination 10.164.4.4 0 (0 times matched)
rule 20 deny ip destination 10.164.4.4 0 (0 times matched)
```

查看流分类的配置信息。

```
[Switch] display traffic classifier
User Defined Classifier Information:
Classifier: c_network
Type: OR
Rule(s) :
    if-match acl 3002

Total classifier number is 1
```

查看流策略的配置信息。

```
[Switch] display traffic policy p_network
User Defined Traffic Policy Information:
Policy: p_network
Classifier: c_network
Type: OR
Behavior: b_network
Permit
```

查看流策略的应用信息。

```
[Switch] display traffic-policy applied-record
Total record : 1

-----
Policy Type/Name:  Apply Parameter      Slot      State
-----
p_network          10GE1/0/4(OUT)    1          success
-----
```

总裁办公室、市场部和研发部均可以访问财务服务器，但是外网用户无法访问财务服务器。

配置脚本

Switch 的配置脚本

```
#
sysname Switch
#
vlan batch 10 20 30 100
#
acl number 3002
rule 5 permit ip source 10.164.1.0 0.0.0.255 destination 10.164.4.4 0
rule 10 permit ip source 10.164.2.0 0.0.0.255 destination 10.164.4.4 0
rule 15 permit ip source 10.164.3.0 0.0.0.255 destination 10.164.4.4 0
rule 20 deny ip destination 10.164.4.4 0
#
traffic classifier c_network type or
if-match acl 3002
#
traffic behavior b_network
permit
#
traffic policy p_network
classifier c_network behavior b_network precedence 5
#
interface Vlanif10
ip address 10.164.1.1 255.255.255.0
#
interface Vlanif20
ip address 10.164.2.1 255.255.255.0
#
interface Vlanif30
ip address 10.164.3.1 255.255.255.0
#
interface Vlanif100
ip address 10.164.4.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
```

```
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 30
#
interface 10GE1/0/4
 port link-type trunk
 port trunk allow-pass vlan 100
 traffic-policy p_network outbound
#
return
```

1.1.5.8 IP 路由

IPv4 静态路由

1.1.5.8.1 IPv4 静态路由

举例：IPv4 静态路由实现路由负载分担

举例：IPv4 静态路由实现主备备份

1.1.5.8.1.1 举例：IPv4 静态路由实现路由负载分担

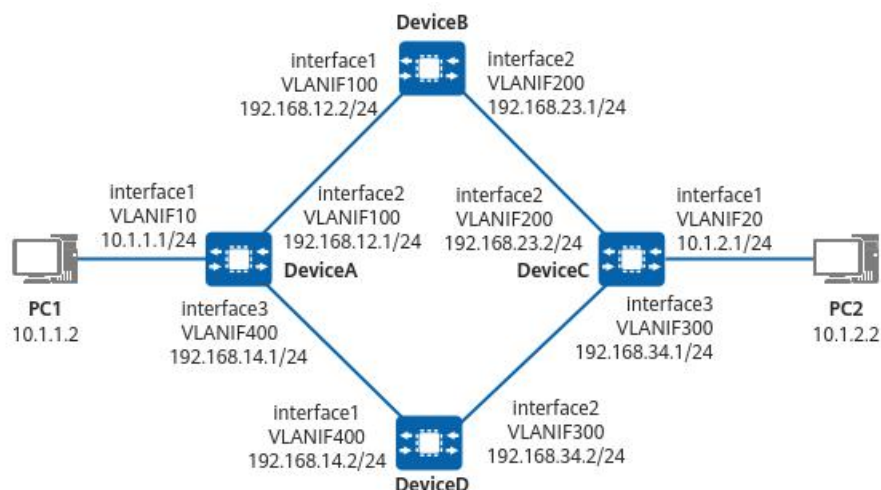
组网需求

如图 1 所示，PC1 和 PC2 通过 4 台 Device 相连，从拓扑图中可以看出，数据从 PC1 到 PC2 有两条路径可以到达，分别是 PC1-DeviceA-DeviceB-DeviceC-PC2 和 PC1-DeviceA-DeviceD-DeviceC-PC2，为了有效利用链路，要求从 PC1 到 PC2 的数据流平均分配到两条链路上，而且当一条链路故障之后数据流自动切换到另一条链路上去。

说明

本例中 interface1，interface2 和 interface3 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3。

图 1 配置静态路由实现路由负载分担组网图



配置注意事项

一般情况下两个设备之间的通信是双向的，因此路由也必须是双向的，在本端配置完静态路由以后，请不要忘记在对端设备上配置回程路由。

在企业网络双出口的场景中，通过配置两条等价的静态路由可以实现负载分担，流量可以均衡的分配到两条不同的链路上；通过配置两条不等价的静态路由可以实现主备份，当主用链路故障的时候流量切换到备用链路上。

配置思路

采用如下的思路配置静态路由实现路由负载分担：

1. 创建 VLAN 并配置各接口所属 VLAN，配置各 VLANIF 接口的 IP 地址。
2. 配置数据流来回两个方向的静态路由。
3. 在各主机上配置 IP 地址和默认网关。

操作步骤

1. 配置各接口所属 VLAN

配置 DeviceA。DeviceB、DeviceC 和 DeviceD 的配置与 DeviceA 类似。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 100 400
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 100
[DeviceA-10GE1/0/2] quit
  
```

```
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 400
[DeviceA-10GE1/0/3] quit
```

2. 配置各 VLANIF 接口的 IP 地址

配置 DeviceA。DeviceB、DeviceC 和 DeviceD 的配置与 DeviceA 类似。

```
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.1 24
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] ip address 192.168.12.1 24
[DeviceA-Vlanif100] quit
[DeviceA] interface vlanif 400
[DeviceA-Vlanif400] ip address 192.168.14.1 24
[DeviceA-Vlanif400] quit
```

3. 配置 PC1 PC2 的去程的静态路由

配置 DeviceA，配置两条等价的静态路由，下一跳分别指向 DeviceB 和 DeviceD，这样就能实现去程的流量的负载分担。

```
[DeviceA] ip route-static 10.1.2.0 24 192.168.12.2
[DeviceA] ip route-static 10.1.2.0 24 192.168.14.2
```

配置 DeviceB。

```
[DeviceB] ip route-static 10.1.2.0 24 192.168.23.2
```

配置 DeviceD。

```
[DeviceD] ip route-static 10.1.2.0 24 192.168.34.1
```

4. 配置 PC1 PC2 的回程的静态路由

配置 DeviceC，配置两条等价的静态路由，下一跳分别指向 DeviceB 和 DeviceD，这样就能实现回程流量的负载分担。

```
[DeviceC] ip route-static 10.1.1.0 24 192.168.23.1
[DeviceC] ip route-static 10.1.1.0 24 192.168.34.2
```

配置 DeviceB。

```
[DeviceB] ip route-static 10.1.1.0 24 192.168.12.1
```

配置 DeviceD。

```
[DeviceD] ip route-static 10.1.1.0 24 192.168.14.1
```

5. 配置主机

配置主机 PC1 的 IP 地址为 10.1.1.2/24，默认网关为 10.1.1.1；配置主机 PC2 的 IP 地址为 10.1.2.2/24，默认网关为 10.1.2.1。

6. 验证配置结果

查看 DeviceA 的 IP 路由表。

[DeviceA] display ip routing-table

Route Flags: R – relay, D – download to fib, T – to vpn-instance

Routing Tables: Public

Destinations : 9 Routes : 10

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.1.1.0/24	Direct	0	0	D	10.1.1.1	Vlanif10
10.1.1.1/32	Direct	0	0	D	127.0.0.1	Vlanif10
10.1.2.0/24	Static	60	0	RD	192.168.12.2	Vlanif100
	Static	60	0	RD	192.168.14.2	Vlanif400
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
192.168.12.0/24	Direct	0	0	D	192.168.12.1	Vlanif100
192.168.12.1/32	Direct	0	0	D	127.0.0.1	Vlanif100
192.168.14.0/24	Direct	0	0	D	192.168.14.1	Vlanif400
192.168.14.1/32	Direct	0	0	D	127.0.0.1	Vlanif400

从 DeviceA 的 IP 路由表中可以看出，到达 10.1.2.0/24 这个网段有两条等价路由，这种情况下数据流将会平均分配到两条不同的链路上，即实现流量的负载分担。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 10 100 400
#
interface Vlanif10
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif100
 ip address 192.168.12.1 255.255.255.0
#
interface Vlanif400
 ip address 192.168.14.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 10
#
```

```
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 400
#
ip route-static 10.1.2.0 255.255.255.0 192.168.12.2
ip route-static 10.1.2.0 255.255.255.0 192.168.14.2
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 100 200
#
interface Vlanif100
ip address 192.168.12.2 255.255.255.0
#
interface Vlanif200
ip address 192.168.23.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
ip route-static 10.1.1.0 255.255.255.0 192.168.12.1
ip route-static 10.1.2.0 255.255.255.0 192.168.23.2
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 20 200 300
```



```
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif200
 ip address 192.168.23.2 255.255.255.0
#
interface Vlanif300
 ip address 192.168.34.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 20
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 300
#
ip route-static 10.1.1.0 255.255.255.0 192.168.23.1
ip route-static 10.1.1.0 255.255.255.0 192.168.34.2
#
return
```

DeviceD

```
#
sysname DeviceD
#
vlan batch 300 400
#
interface Vlanif300
 ip address 192.168.34.2 255.255.255.0
#
interface Vlanif400
 ip address 192.168.14.2 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 400
#
```

```
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 300
#
ip route-static 10.1.1.0 255.255.255.0 192.168.14.1
ip route-static 10.1.2.0 255.255.255.0 192.168.34.1
#
return
```

1.1.5.8.1.2 举例：IPv4 静态路由实现主备备份

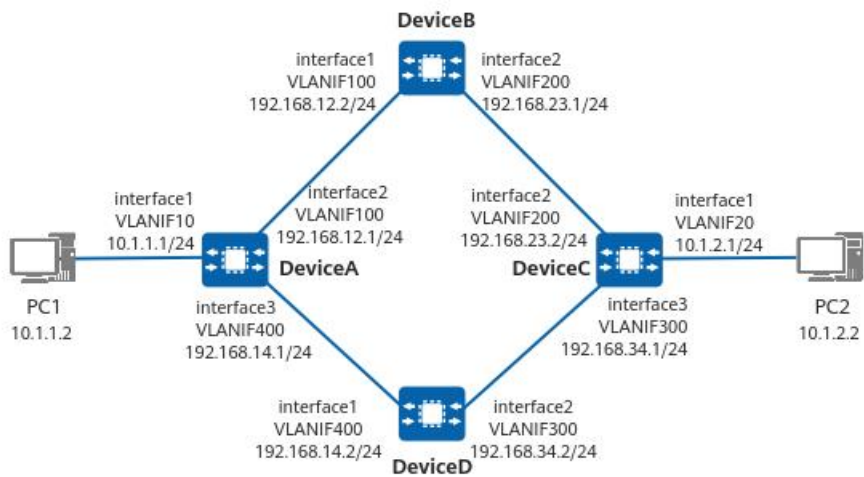
组网需求

如图 1 所示，PC1 和 PC2 通过 4 台 Device 相连，从拓扑图中可以看出，数据从 PC1 到 PC2 有两条路径可以到达，分别是 PC1-DeviceA-DeviceB-DeviceC-PC2 和 PC1-DeviceA-DeviceD-DeviceC-PC2，用户希望要求从 PC1 到 PC2 的数据流实现主备备份，即优先走经过 DeviceB 的这条路径，当这条路径故障的时候流量自动切换到经过 DeviceD 的这条路径。

说明

本例中 interface1，interface2 和 interface3 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3。

图 1 配置静态路由实现主备备份组网图



配置注意事项

一般情况下两个设备之间的通信是双向的，因此路由也必须是双向的，在本端配置完静态路由以后，请不要忘记在对端设备上配置回程路由。

在企业网络双出口的场景中，通过配置两条等价的静态路由可以实现负载分担，流量可以均衡的分配到两条不同的链路上；通过配置两条不等价的静态路由可以实现主备份，当主用链路故障的时候流量切换到备用链路上。

配置思路

采用如下的思路配置静态路由实现主备备份：

1. 创建 VLAN 并配置各接口所属 VLAN，配置各 VLANIF 接口的 IP 地址。
2. 配置数据流来回两个方向的静态路由。
3. 在各主机上配置 IP 地址和默认网关。

操作步骤

1. 配置各接口所属 VLAN

配置 DeviceA。DeviceB、DeviceC 和 DeviceD 的配置与 DeviceA 类似。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 100 400
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 100
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 400
[DeviceA-10GE1/0/3] quit
```

2. 配置各 VLANIF 接口的 IP 地址

配置 DeviceA。DeviceB、DeviceC 和 DeviceD 的配置与 DeviceA 类似。

```
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.1 24
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] ip address 192.168.12.1 24
[DeviceA-Vlanif100] quit
[DeviceA] interface vlanif 400
[DeviceA-Vlanif400] ip address 192.168.14.1 24
[DeviceA-Vlanif400] quit
```

3. 配置 PC1 PC2 的去程的静态路由

配置 DeviceA，配置两条优先级不同的静态路由，下一跳分别指向 DeviceB 和 DeviceD，实现数据流优先发往 DeviceB，当去往 DeviceB 的链路发生故障的时候流量自动切换至 DeviceD。

```
[DeviceA] ip route-static 10.1.2.0 24 192.168.12.2
```

```
[DeviceA] ip route-static 10.1.2.0 24 192.168.14.2 preference 70
```

配置 DeviceB。

```
[DeviceB] ip route-static 10.1.2.0 24 192.168.23.2
```

配置 DeviceD。

```
[DeviceD] ip route-static 10.1.2.0 24 192.168.34.1
```

4. 配置 PC1 PC2 的回程的静态路由，需要注意数据流来回的路径主备是一致的。

配置 DeviceC，配置两条优先级不同的静态路由，下一跳分别指向 DeviceB 和 DeviceD，实现数据流优先发往 DeviceB，当去往 DeviceB 的链路发生故障的时候流量自动切换至 DeviceD。

```
[DeviceC] ip route-static 10.1.1.0 24 192.168.23.1
```

```
[DeviceC] ip route-static 10.1.1.0 24 192.168.34.2 preference 70
```

配置 DeviceB。

```
[DeviceB] ip route-static 10.1.1.0 24 192.168.12.1
```

配置 DeviceD。

```
[DeviceD] ip route-static 10.1.1.0 24 192.168.14.1
```

5. 配置主机

配置主机 PC1 的 IP 地址为 10.1.1.2/24，默认网关为 10.1.1.1；配置主机 PC2 的 IP 地址为 10.1.2.2/24，默认网关为 10.1.2.1。

6. 验证配置结果

查看 DeviceA 的 IP 路由表。

```
[DeviceA] display ip routing-table
```

Route Flags: R – relay, D – download to fib, T – to vpn-instance

Routing Tables: Public

Destinations : 9 Routes : 9

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.1.1.0/24	Direct	0	0	D	10.1.1.1	Vlanif10
10.1.1.1/32	Direct	0	0	D	127.0.0.1	Vlanif10
10.1.2.0/24	Static	60	0	RD	192.168.12.2	Vlanif100
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
192.168.12.0/24	Direct	0	0	D	192.168.12.1	Vlanif100
192.168.12.1/32	Direct	0	0	D	127.0.0.1	Vlanif100
192.168.14.0/24	Direct	0	0	D	192.168.14.1	Vlanif400
192.168.14.1/32	Direct	0	0	D	127.0.0.1	Vlanif400

查看 DeviceA 的 IP 路由表详细信息。

```
[DeviceA] display ip routing-table 10.1.2.0 24 verbose
```

```
Route Flags: R – relay, D – download to fib, T – to vpn-instance
```

```
-----
```

```
Routing Table : Public
```

```
Summary Count : 1
```

```
Destination: 10.1.2.0/24
```

```
Protocol: Static      Process ID: 0
```

```
Preference: 60        Cost: 0
```

```
NextHop: 192.168.12.2 Neighbour: 0.0.0.0
```

```
State: Active Adv Relied Age: 00h13m13s
```

```
Tag: 0                Priority: medium
```

```
Label: NULL           QoSInfo: 0x0
```

```
IndirectID: 0x80000001
```

```
RelayNextHop: 0.0.0.0 Interface: Vlanif100
```

```
TunnelID: 0x0         Flags: RD
```

```
RouteColor: 0
```

对 DeviceA 的 Vlanif100 接口执行 **shutdown** 命令，模拟链路故障。

```
[DeviceA] interface vlanif 100
```

```
[DeviceA-Vlanif100] shutdown
```

```
[DeviceA-Vlanif100] quit
```

再次查看 DeviceA 的 IP 路由表详细信息。可以看出，主链路失效后，备份链路 DeviceA-DeviceD-DeviceC 生效，去往 10.1.2.0/24 路由的下一跳地址为 192.168.14.2。

```
[DeviceA] display ip routing-table 10.1.2.0 24 verbose
```

```
Route Flags: R – relay, D – download to fib, T – to vpn-instance
```

```
-----
```

```
Routing Table : Public
```

```
Summary Count : 1
```

```
Destination: 10.1.2.0/24
```

```
Protocol: Static      Process ID: 0
```

```
Preference: 70        Cost: 0
```

```
NextHop: 192.168.14.2 Neighbour: 0.0.0.0
```

```
State: Active Adv Relied Age: 00h00m45s
```

```
Tag: 0                Priority: medium
```

```
Label: NULL           QoSInfo: 0x0
```

```
IndirectID: 0x80000002
```

```
RelayNextHop: 0.0.0.0 Interface: Vlanif400
```

```
TunnelID: 0x0         Flags: R
```

```
RouteColor: 0
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 10 100 400
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
#
interface Vlanif100
ip address 192.168.12.1 255.255.255.0
#
interface Vlanif400
ip address 192.168.14.1 255.255.255.0
#
interface 10GE1/0/1
port link-type access
port default vlan 10
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 400
#
ip route-static 10.1.2.0 255.255.255.0 192.168.12.2
ip route-static 10.1.2.0 255.255.255.0 192.168.14.2 preference 70
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 100 200
#
interface Vlanif100
ip address 192.168.12.2 255.255.255.0
#
```

```
interface Vlanif200
 ip address 192.168.23.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
ip route-static 10.1.1.0 255.255.255.0 192.168.12.1
ip route-static 10.1.2.0 255.255.255.0 192.168.23.2
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 20 200 300
#
interface Vlanif20
 ip address 10.1.2.1 255.255.255.0
#
interface Vlanif200
 ip address 192.168.23.2 255.255.255.0
#
interface Vlanif300
 ip address 192.168.34.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 20
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 300
#
```

```
ip route-static 10.1.1.0 255.255.255.0 192.168.23.1
ip route-static 10.1.1.0 255.255.255.0 192.168.34.2 preference 70
#
return
```

DeviceD

```
#
sysname DeviceD
#
vlan batch 300 400
#
interface Vlanif300
 ip address 192.168.34.2 255.255.255.0
#
interface Vlanif400
 ip address 192.168.14.2 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 400
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 300
#
ip route-static 10.1.1.0 255.255.255.0 192.168.14.1
ip route-static 10.1.2.0 255.255.255.0 192.168.34.1
#
return
```

1.1.5.9 VPN

[IPv4 L3VPN](#)

[IPv6 L3VPN](#)

1.1.5.9.1 IPv4 L3VPN

[举例：配置本地 IPv4 L3VPN 互访](#)

[举例：配置基本 IPv4 L3VPN over MPLS 场景](#)

[举例：配置 Hub and Spoke 示例（Hub-PE 和 Hub-CE 双链路接入）](#)

举例：配置 L3VPN+VRRP 综合场景

举例：配置企业使用路由策略控制 L3VPN 分支间用户互访场景

1.1.5.9.1.1 举例：配置本地 IPv4 L3VPN 互访

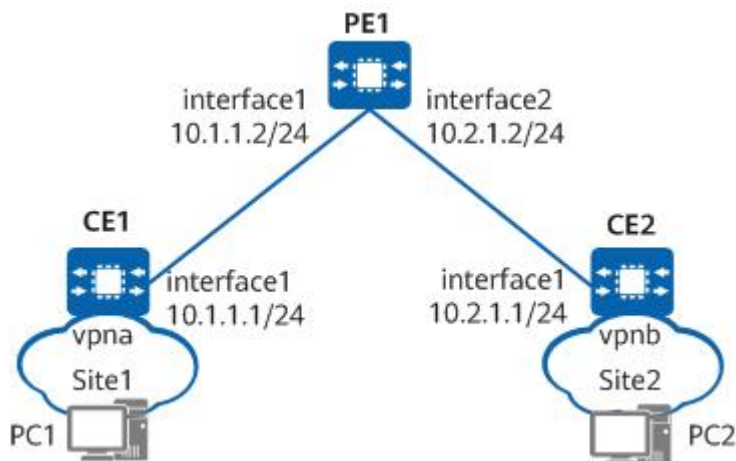
组网需求

如图 1，CE1 和 CE2 均连接到 PE1 上，其中 CE1 属于 vpna，CE2 属于 vpnb。当前由于业务需求，Site1 和 Site2 之间需要互访。可以配置本地 VPN 互访功能，满足上述需求。

图 1 本地 IPv4 VPN 互访组网图

说明

本例中 interface1，interface2 分别代表 Vlanif100，Vlanif200。



配置思路

本例按如下思路配置 VPN 互访：

1. 在 PE1 上配置 VPN 实例，为 VPN 实例配置不同的 VPN-Target 属性，实现不同 VPN 的隔离。
2. 在 PE1 上配置与 CE 相连的接口与 VPN 实例绑定，接入 VPN 用户。
3. 在 PE1 上配置将到本地 CE 的直连路由引入 VPN 路由表，同时在 CE 上配置访问另一 CE 设备的路由，以实现本地互访。

操作步骤

1. 在 PE 设备上配置 VPN 实例，将 CE 接入 PE。

配置 PE1。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
```

```

[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 export-extcommunity
[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 222:2 import-extcommunity
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] route-distinguisher 100:2
[PE1-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 export-extcommunity
[PE1-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 111:1 import-extcommunity
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
[PE1] vlan batch 100 200
[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] port link-type trunk
[PE1-10GE1/0/1] port trunk allow-pass vlan 100
[PE1-10GE1/0/1] quit
[PE1] interface Vlanif 100
[PE1-Vlanif100] ip binding vpn-instance vpna
[PE1-Vlanif100] ip address 10.1.1.2 24
[PE1-Vlanif100] quit
[PE1] interface 10GE1/0/2
[PE1-10GE1/0/2] port link-type trunk
[PE1-10GE1/0/2] port trunk allow-pass vlan 200
[PE1-10GE1/0/2] quit
[PE1] interface Vlanif 200
[PE1-Vlanif200] ip binding vpn-instance vpnb
[PE1-Vlanif200] ip address 10.2.1.2 24
[PE1-Vlanif200] quit

```

配置 CE1 的接口 IP 地址。

```

<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] vlan batch 100
[CE1] interface 10ge 1/0/1
[CE1-10GE1/0/1] port link-type trunk
[CE1-10GE1/0/1] port trunk allow-pass vlan 100
[CE1-10GE1/0/1] quit
[CE1] interface Vlanif 100
[CE1-Vlanif100] ip address 10.1.1.1 24
[CE1-Vlanif100] quit

```

配置 CE2 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] vlan batch 100
[CE2] interface 10ge 1/0/1
[CE2-10GE1/0/1] port link-type trunk
[CE2-10GE1/0/1] port trunk allow-pass vlan 100
[CE2-10GE1/0/1] quit
[CE2] interface Vlanif 100
[CE2-Vlanif100] ip address 10.2.1.1 24
[CE2-Vlanif100] quit
```

PE 能 Ping 通自己接入的 CE。以 PE1 和 CE1 为例：

```
[PE1] ping -vpn-instance vpna 10.1.1.1
PING 10.1.1.1: 56 data bytes, press CTRL_C to break
Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=2 ms
Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=2 ms
Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=2 ms
Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=2 ms
Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=2 ms

--- 10.1.1.1 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 2/2/2 ms
```

2. 配置 BGP，将到本地 CE 的直连路由引入 VPN 路由表。

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
[PE1-bgp] ipv4-family vpn-instance vpnb
[PE1-bgp-vpnb] import-route direct
[PE1-bgp-vpnb] quit
[PE1-bgp] quit
```

3. 配置 CE 上的静态路由。

配置 CE1。

```
[CE1] ip route-static 10.2.1.0 24 10.1.1.2
```

配置 CE2。

```
[CE2] ip route-static 10.1.1.0 24 10.2.1.2
```

检查配置结果

配置完成后，在 PE1 上执行 **display ip routing-table vpn-instance** 可以看到不同 VPN 路由相互引入，以 vpn1 为例：

```
[PE1] display ip routing-table vpn-instance vpn1
```

```
Proto: Protocol    Pre: Preference
```

```
Route Flags: R – relay, D – download to fib, T – to vpn-instance, B – black hole route
```

```
-----
```

```
Routing Table : vpn1
```

```
Destinations : 7    Routes : 7
```

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.1.1.0/24	Direct	0	0	D	10.1.1.2	Vlanif100
10.1.1.2/32	Direct	0	0	D	127.0.0.1	Vlanif100
10.1.1.255/32	Direct	0	0	D	127.0.0.1	Vlanif100
10.2.1.0/24	BGP	255	0	RD	10.2.1.2	Vlanif200
10.2.1.2/32	BGP	255	0	RD	127.0.0.1	Vlanif200
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

CE1 和 CE2 能够相互 Ping 通。

```
[CE1] ping 10.2.1.1
```

```
PING 10.2.1.1: 56 data bytes, press CTRL_C to break
```

```
Reply from 10.2.1.1: bytes=56 Sequence=1 ttl=254 time=8 ms
```

```
Reply from 10.2.1.1: bytes=56 Sequence=2 ttl=254 time=3 ms
```

```
Reply from 10.2.1.1: bytes=56 Sequence=3 ttl=254 time=2 ms
```

```
Reply from 10.2.1.1: bytes=56 Sequence=4 ttl=254 time=3 ms
```

```
Reply from 10.2.1.1: bytes=56 Sequence=5 ttl=254 time=2 ms
```

```
--- 10.2.1.1 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 2/3/8 ms
```

配置脚本

```
PE1
```

```
#
```

```
sysname PE1
```

```
#
```

```
vlan batch 100 200
#
ip vpn-instance vpna
ipv4-family
route-distinguisher 100:1
vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity
vpn-target 222:2 import-extcommunity
#
ip vpn-instance vpnb
ipv4-family
route-distinguisher 100:2
vpn-target 222:2 export-extcommunity
vpn-target 222:2 import-extcommunity
vpn-target 111:1 import-extcommunity
#
interface Vlanif100
ip binding vpn-instance vpna
ip address 10.1.1.2 255.255.255.0
#
interface Vlanif200
ip binding vpn-instance vpnb
ip address 10.2.1.2 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
bgp 100
#
ipv4-family unicast
#
ipv4-family vpn-instance vpna
import-route direct
#
ipv4-family vpn-instance vpnb
import-route direct
#
```

```
return
```

CE1

```
#
sysname CE1
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
ip route-static 10.2.1.0 255.255.255.0 10.1.1.2
#
return
```

CE2

```
#
sysname CE2
#
vlan batch 100
#
interface Vlanif100
 ip address 10.2.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
ip route-static 10.1.1.0 255.255.255.0 10.2.1.2
#
return
```

1.1.5.9.1.2 举例：配置基本 IPv4 L3VPN over MPLS 场景

组网需求

如图 1 所示：

CE1、CE3 属于 vpna。

CE2、CE4 属于 vpnb。

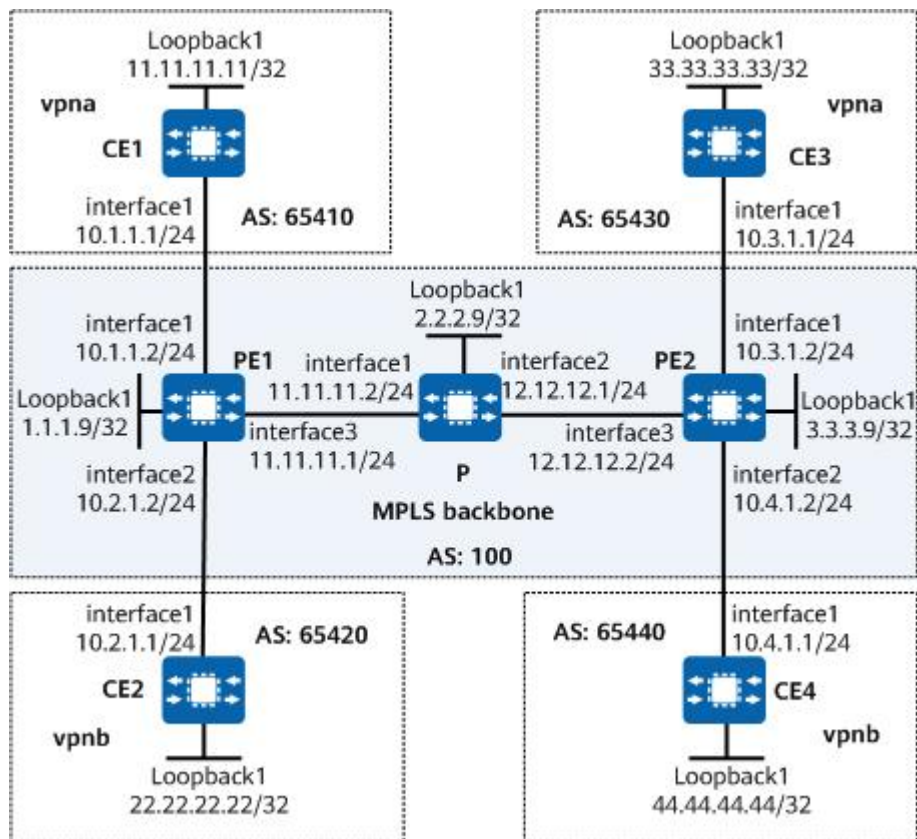
vpna 使用的 VPN-target 属性为 111:1，vpnb 使用的 VPN-target 属性为 222:2。

使相同 VPN 用户之间可以互访，不同 VPN 用户之间不能互相访问。

图 1 IPv4 L3VPN 组网图

说明

本例中 interface1, interface2 和 interface3 分别代表 Vlanif100, Vlanif200, Vlanif300。



配置注意事项

在配置过程中，需注意以下事项：

同一 VPN 的 Export VPN-Target 列表与其它站点的 Import VPN-Target 列表有共同的 VPN-Target，Import VPN-Target 列表与其它站点的 Export VPN-Target 列表有共同的 VPN-Target。
 PE 与 CE 相连的接口绑定了 VPN 实例后，将删除该接口上已经配置的 IP 地址、路由协议等三层特性，如果需要应重新配置。

配置思路

采用如下的思路配置 IPv4 L3VPN：

1. 骨干网上配置 OSPF 实现 PE 之间的互通。
2. 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 MPLS LSP。

3. PE 上配置使能 IPv4 地址族 VPN 实例，并把与 CE 相连的接口和相应的 VPN 实例绑定。
4. PE 之间配置 MP-IBGP 交换 VPN 路由信息。
5. CE 与 PE 之间配置 EBGP 交换 VPN 路由信息。

操作步骤

1. 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 和 P 的互通。本例中以 IGP 为 OSPF 为例进行说明。

配置 PE1。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.9 32
[PE1-LoopBack1] quit
[PE1] vlan batch 100 200 300
[PE1] interface 10GE1/0/3
[PE1-10GE1/0/3] port link-type trunk
[PE1-10GE1/0/3] port trunk allow-pass vlan 300
[PE1-10GE1/0/3] quit
[PE1] interface Vlanif 300
[PE1-Vlanif300] ip address 11.11.11.1 24
[PE1-Vlanif300] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 11.11.11.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 P。

```
<HUAWEI> system-view
[HUAWEI] sysname P
[P] interface loopback 1
[P-LoopBack1] ip address 2.2.2.9 32
[P-LoopBack1] quit
[P] vlan batch 100 200
[P] interface 10ge 1/0/1
[P-10GE1/0/1] port link-type trunk
[P-10GE1/0/1] port trunk allow-pass vlan 100
[P-10GE1/0/1] quit
[P] interface Vlanif 100
[P-Vlanif100] ip address 11.11.11.2 24
```



```

[P-Vlanif100] quit
[P] interface 10GE1/0/2
[P-10GE1/0/2] port link-type trunk
[P-10GE1/0/2] port trunk allow-pass vlan 200
[P-10GE1/0/2] quit
[P] interface Vlanif 200
[P-Vlanif200] ip address 12.12.12.1 24
[P-Vlanif200] quit
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 11.11.11.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[P-ospf-1-area-0.0.0.0] network 2.2.2.9 0.0.0.0
[P-ospf-1-area-0.0.0.0] quit
[P-ospf-1] quit

```

配置 PE2。

```

<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 3.3.3.9 32
[PE2-LoopBack1] quit
[PE2] vlan batch 100 200 300
[PE2] interface 10GE1/0/3
[PE2-10GE1/0/3] port link-type trunk
[PE2-10GE1/0/3] port trunk allow-pass vlan 300
[PE2-10GE1/0/3] quit
[PE2] interface Vlanif 300
[PE2-Vlanif300] ip address 12.12.12.2 24
[PE2-Vlanif300] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 12.12.12.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 3.3.3.9 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit

```

配置完成后，PE1、P、PE2 之间应能建立 OSPF 邻居关系，执行 **display ospf peer** 命令可以看到邻居状态为 Full。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback1 路由。以 PE1 的显示为例：

```

[PE1] display ip routing-table
Proto: Protocol      Pre: Preference
Route Flags: R – relay, D – download to fib, T – to vpn-instance, B – black hole route
-----

```

Routing Table: _public_

Destinations : 11 Routes : 11

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
1.1.1.9/32	Direct	0	0	D	127.0.0.1	LoopBack1
2.2.2.9/32	OSPF	10	2	D	11.11.11.2	Vlanif300
3.3.3.9/32	OSPF	10	3	D	11.11.11.2	Vlanif300
11.11.11.0/24	Direct	0	0	D	11.11.11.1	Vlanif300
11.11.11.1/32	Direct	0	0	D	127.0.0.1	Vlanif300
11.11.11.255/32	Direct	0	0	D	127.0.0.1	Vlanif300
12.12.12.0/24	OSPF	10	2	D	11.11.11.2	Vlanif300
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
127.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

[PE1] **display ospf peer**

(M) Indicates MADJ neighbor

OSPF Process 1 with Router ID 1.1.1.9

Area 0.0.0.0 interface 11.11.11.1(Vlanif300)'s neighbors

Router ID: 2.2.2.9 Address: 11.11.11.2

State: **Full** Mode:Nbr is Slave Priority: 1

DR: 1.1.1.9 BDR: 2.2.2.9 MTU: 1500

Dead timer due (in seconds) : 38

Retrans timer interval : 0

Neighbor up time : 00h00m29s

Neighbor up time stamp : 2018-06-08 01:41:57

Authentication Sequence : 0

2. 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。

配置 PE1。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface Vlanif 300
[PE1-Vlanif300] mpls
[PE1-Vlanif300] mpls ldp
[PE1-Vlanif300] quit
```

配置 P。

```
[P] mpls lsr-id 2.2.2.9
[P] mpls
[P-mpls] quit
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface Vlanif 100
[P-Vlanif100] mpls
[P-Vlanif100] mpls ldp
[P-Vlanif100] quit
[P] interface Vlanif 200
[P-Vlanif200] mpls
[P-Vlanif200] mpls ldp
[P-Vlanif200] quit
```

配置 PE2。

```
[PE2] mpls lsr-id 3.3.3.9
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface Vlanif 300
[PE2-Vlanif300] mpls
[PE2-Vlanif300] mpls ldp
[PE2-Vlanif300] quit
```

上述配置完成后，PE1 与 P、P 与 PE2 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为 “Operational”。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。

以 PE1 的显示为例：

```
[PE1] display mpls ldp session
```

LDP Session(s) in Public Network

Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)

An asterisk (*) before a session means the session is being deleted.

```
-----
Peer-ID      Status    LAM  SsnRole SsnAge   KA-Sent/Rcv
-----
2.2.2.9:0    Operational DU   Passive 0006:20:55 39551/39552
-----
```

TOTAL: 1 session(s) Found.

```
[PE1] display mpls ldp lsp
LDP LSP Information
```

 Flag after Out IF: (I) – RLFA Iterated LSP, (I*) – Normal and RLFA Iterated LSP

DestAddress/Mask	In/OutLabel	UpstreamPeer	NextHop	OutInterface
1.1.1.9/32	3/NULL	2.2.2.9	127.0.0.1	InLoop0
*1.1.1.9/32	Liberal/1024		DS/2.2.2.9	
2.2.2.9/32	NULL/3	–	11.11.11.2	Vlanif300
2.2.2.9/32	1024/3	2.2.2.9	11.11.11.2	Vlanif300
3.3.3.9/32	NULL/1025	–	11.11.11.2	Vlanif300
3.3.3.9/32	1025/1025	2.2.2.9	11.11.11.2	Vlanif300

TOTAL: 5 Normal LSP(s) Found.

TOTAL: 1 Liberal LSP(s) Found.

TOTAL: 0 Frr LSP(s) Found.

An asterisk (*) before an LSP means the LSP is not established

An asterisk (*) before a Label means the USCB or DSCB is stale

An asterisk (*) before an UpstreamPeer means the session is stale

An asterisk (*) before a DS means the session is stale

An asterisk (*) before a NextHop means the LSP is FRR LSP

3. 在 PE 设备上配置使能 IPv4 地址族的 VPN 实例，将 CE 接入 PE。

配置 PE1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] ipv4-family
[PE1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv4-family
[PE1-vpn-instance-vpnb-af-ipv4] route-distinguisher 100:2
[PE1-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 both
[PE1-vpn-instance-vpnb-af-ipv4] quit
[PE1-vpn-instance-vpnb] quit
[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] port link-type trunk
[PE1-10GE1/0/1] port trunk allow-pass vlan 100
[PE1-10GE1/0/1] quit
[PE1] interface vlanif 100
[PE1-Vlanif100] ip binding vpn-instance vpna
[PE1-Vlanif100] ip address 10.1.1.2 24
[PE1-Vlanif100] quit
```

```
[PE1] interface 10GE1/0/2
[PE1-10GE1/0/2] port link-type trunk
[PE1-10GE1/0/2] port trunk allow-pass vlan 200
[PE1-10GE1/0/2] quit
[PE1] interface vlanif 200
[PE1-Vlanif200] ip binding vpn-instance vpnb
[PE1-Vlanif200] ip address 10.2.1.2 24
[PE1-Vlanif200] quit
```

配置 PE2。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] ipv4-family
[PE2-vpn-instance-vpna-af-ipv4] route-distinguisher 200:1
[PE2-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE2-vpn-instance-vpna-af-ipv4] quit
[PE2-vpn-instance-vpna] quit
[PE2] ip vpn-instance vpnb
[PE2-vpn-instance-vpnb] ipv4-family
[PE2-vpn-instance-vpnb-af-ipv4] route-distinguisher 200:2
[PE2-vpn-instance-vpnb-af-ipv4] vpn-target 222:2 both
[PE2-vpn-instance-vpnb-af-ipv4] quit
[PE2-vpn-instance-vpnb] quit
[PE2] interface 10ge 1/0/1
[PE2-10GE1/0/1] port link-type trunk
[PE2-10GE1/0/1] port trunk allow-pass vlan 100
[PE2-10GE1/0/1] quit
[PE2] interface vlanif 100
[PE2-Vlanif100] ip binding vpn-instance vpna
[PE2-Vlanif100] ip address 10.3.1.2 24
[PE2-Vlanif100] quit
[PE2] interface 10GE1/0/2
[PE2-10GE1/0/2] port link-type trunk
[PE2-10GE1/0/2] port trunk allow-pass vlan 200
[PE2-10GE1/0/2] quit
[PE2] interface vlanif 200
[PE2-Vlanif200] ip binding vpn-instance vpnb
[PE2-Vlanif200] ip address 10.4.1.2 24
[PE2-Vlanif200] quit
```

按图 1 配置各 CE 的接口 IP 地址，配置过程请参见后面的配置文件。

配置完成后，在 PE 设备上执行 **display ip vpn-instance verbose** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。



说明

当 PE 上有多个绑定了同一个 VPN 的接口，则使用 **ping -vpn-instance** 命令 ping 对端 PE 接入的 CE 时，要指定源 IP 地址，即要指定 **ping -vpn-instance vpn-instance-name -a source-ip-address dest-ip-address** 命令中的参数 **-a source-ip-address**，否则可能 ping 不通。

以 PE1 为例：

```
[PE1] display ip vpn-instance verbose
```

```
Total VPN-Instances configured : 2
```

```
Total IPv4 VPN-Instances configured : 2
```

```
Total IPv6 VPN-Instances configured : 0
```

```
VPN-Instance Name and ID : vpna, 1
```

```
Interfaces : Vlanif100
```

```
Address family ipv4
```

```
Create date : 2009/01/21 11:30:35
```

```
Up time : 0 days, 00 hours, 05 minutes and 19 seconds
```

```
Vrf Status : UP
```

```
Route Distinguisher : 100:1
```

```
Export VPN Targets : 111:1
```

```
Import VPN Targets : 111:1
```

```
Label policy: label per route
```

```
The diffserv-mode Information is : uniform
```

```
The ttl-mode Information is : pipe
```

```
VPN-Instance Name and ID : vpnb, 2
```

```
Interfaces : Vlanif200
```

```
Address family ipv4
```

```
Create date : 2009/01/21 11:31:18
```

```
Up time : 0 days, 00 hours, 04 minutes and 36 seconds
```

```
Vrf Status : UP
```

```
Route Distinguisher : 100:2
```

```
Export VPN Targets : 222:2
```

```
Import VPN Targets : 222:2
```

```
Label policy: label per route
```

```
The diffserv-mode Information is : uniform
```

```
The ttl-mode Information is : pipe
```

```
[PE1] ping -vpn-instance vpna 10.1.1.1
```

```
PING 10.1.1.1: 56 data bytes, press CTRL_C to break
```

```
Reply from 10.1.1.1: bytes=56 Sequence=1 ttl=255 time=56 ms
```

```
Reply from 10.1.1.1: bytes=56 Sequence=2 ttl=255 time=4 ms
```

```
Reply from 10.1.1.1: bytes=56 Sequence=3 ttl=255 time=4 ms
```

```
Reply from 10.1.1.1: bytes=56 Sequence=4 ttl=255 time=52 ms
```

```
Reply from 10.1.1.1: bytes=56 Sequence=5 ttl=255 time=3 ms
```

```
--- 10.1.1.1 ping statistics ---
```

```
5 packet(s) transmitted
```

```
5 packet(s) received
```

```
0.00% packet loss
```

```
round-trip min/avg/max = 3/23/56 ms
```

4. 在 PE 与 CE 之间建立 EBGP 对等体关系。

配置 CE1。

```
[CE1] interface loopback 1
[CE1-LoopBack1] ip address 11.11.11.11 32
[CE1-LoopBack1] quit
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.2 as-number 100
[CE1-bgp] network 11.11.11.11 32
[CE1-bgp] quit
```

说明

CE2 ~ CE4 配置与 CE1 设备配置类似，配置过程请参见后面的配置文件。

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] peer 10.1.1.1 as-number 65410
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
[PE1-bgp] ipv4-family vpn-instance vpnb
[PE1-bgp-vpnb] peer 10.2.1.1 as-number 65420
[PE1-bgp-vpnb] import-route direct
[PE1-bgp-vpnb] quit
[PE1-bgp] quit
```

说明

PE2 的配置与 PE1 类似，配置过程请参见后面的配置文件。

配置完成后，在 PE 设备上执行 **display bgp vpnv4 vpn-instance peer** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE1 与 CE1 的对等体关系为例：

```
[PE1] display bgp vpnv4 vpn-instance vpna peer
Status codes: * - Dynamic
BGP local router ID : 1.1.1.9
Local AS number : 100
```

VPN-Instance vpna, Router ID 1.1.1.9:

Total number of peers : 1

Peers in established state : 1

Total number of dynamic peers : 0

Peer	V	AS	MsgRcvd	MsgSent	OutQ	Up/Down	State	PrefRcv
10.1.1.1	4	65410	11	9	0	00:06:37	Established	1

5. 在 PE 之间建立 MP-IBGP 对等体关系

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 3.3.3.9 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 1
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 1.1.1.9 enable
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer** 或 **display bgp vpnv4 all peer** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

```
[PE1] display bgp peer
Status codes: * - Dynamic
BGP local router ID : 1.1.1.9
Local AS number : 100
Total number of peers : 1
Peers in established state : 1
Total number of dynamic peers : 0

Peer      V  AS  MsgRcvd  MsgSent  OutQ  Up/Down    State    PrefRcv
3.3.3.9   4  100    2      6    0 00:00:12  Established    0

[PE1] display bgp vpnv4 all peer
Status codes: * - Dynamic
BGP local router ID : 1.1.1.9
Local AS number : 100
Total number of peers : 3
```


Peers in established state : 3

Total number of dynamic peers : 0

Peer	V	AS	MsgRcvd	MsgSent	OutQ	Up/Down	State	PrefRcv
3.3.3.9	4	100	12	18	0	00:09:38	Established	0

Peer of vpn instance:

VPN-Instance vpna, router ID 1.1.1.9:

10.1.1.1	4	65410	25	25	0	00:17:57	Established	1

VPN-Instance vpnb, router ID 1.1.1.9:

10.2.1.1	4	65420	21	22	0	00:17:10	Established	1

检查配置结果

在 PE 设备上执行 **display ip routing-table vpn-instance** 命令，可以看到去往 CE 上的 Loopback 口路由。

以 PE1 的显示为例：

[PE1] **display ip routing-table vpn-instance vpna**

Proto: Protocol Pre: Preference

Route Flags: R – relay, D – download to fib, T – to vpn-instance, B – black hole route

Routing Table: vpna

Destinations : 6 Routes : 6

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.1.1.0/24	Direct	0	0	D	10.1.1.2	Vlanif100
10.1.1.2/32	Direct	0	0	D	127.0.0.1	Vlanif100
10.1.1.255/32	Direct	0	0	D	127.0.0.1	Vlanif100
11.11.11.11/32	EBGP	255	0	RD	10.1.1.1	Vlanif100
33.33.33.33/32	IBGP	255	0	RD	3.3.3.9	Vlanif300
255.255.255.255/32	Direct	0	0	D	127.0.0.1	InLoopBack0

[PE1] **display ip routing-table vpn-instance vpnb**

Proto: Protocol Pre: Preference

Route Flags: R – relay, D – download to fib, T – to vpn-instance, B – black hole route

Routing Table: vpnb

Destinations : 6 Routes : 6

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.2.1.0/24	Direct	0	0	D	10.2.1.2	Vlanif200
10.2.1.2/32	Direct	0	0	D	127.0.0.1	Vlanif200
10.2.1.255/32	Direct	0	0	D	127.0.0.1	Vlanif200

```

22.22.22.22/32 EBGP 255 0 RD 10.2.1.1 Vlanif200
44.44.44.44/32 IBGP 255 0 RD 3.3.3.9 Vlanif300
255.255.255.255/32 Direct 0 0 D 127.0.0.1 InLoopBack0

```

同一 VPN 的 CE 能够相互 Ping 通，不同 VPN 的 CE 不能相互 Ping 通。

例如：CE1 能够 Ping 通 CE3（10.3.1.1），但不能 Ping 通 CE4（10.4.1.1）。

[CE1] ping -a 11.11.11.11 33.33.33.33

PING 33.33.33.33: 56 data bytes, press CTRL_C to break

Reply from 33.33.33.33: bytes=56 Sequence=1 ttl=251 time=72 ms

Reply from 33.33.33.33: bytes=56 Sequence=2 ttl=251 time=34 ms

Reply from 33.33.33.33: bytes=56 Sequence=3 ttl=251 time=50 ms

Reply from 33.33.33.33: bytes=56 Sequence=4 ttl=251 time=50 ms

Reply from 33.33.33.33: bytes=56 Sequence=5 ttl=251 time=34 ms

--- 33.33.33.33 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 34/48/72 ms

[CE1] ping -a 11.11.11.11 44.44.44.44

PING 44.44.44.44: 56 data bytes, press CTRL_C to break

Request time out

Request time out

Request time out

Request time out

Request time out

--- 44.44.44.44 ping statistics ---

5 packet(s) transmitted

0 packet(s) received

100.00% packet loss

配置脚本

PE1

```

#
sysname PE1
#
vlan batch 100 200 300
#
ip vpn-instance vpna
ipv4-family
route-distinguisher 100:1
vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity

```

```
#
ip vpn-instance vpnb
  ipv4-family
    route-distinguisher 100:2
    vpn-target 222:2 export-extcommunity
    vpn-target 222:2 import-extcommunity
#
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
#
interface Vlanif100
  ip binding vpn-instance vpna
  ip address 10.1.1.2 255.255.255.0
#
interface Vlanif200
  ip binding vpn-instance vpnb
  ip address 10.2.1.2 255.255.255.0
#
interface Vlanif300
  ip address 11.11.11.1 255.255.255.0
  mpls
  mpls ldp
#
interface 10GE1/0/1
  port link-type trunk
  port trunk allow-pass vlan 100
#
interface 10GE1/0/2
  port link-type trunk
  port trunk allow-pass vlan 200
#
interface 10GE1/0/3
  port link-type trunk
  port trunk allow-pass vlan 300
#
interface LoopBack1
  ip address 1.1.1.9 255.255.255.255
#
bgp 100
  peer 3.3.3.9 as-number 100
```

```
peer 3.3.3.9 connect-interface LoopBack1
#
ipv4-family unicast
peer 3.3.3.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 3.3.3.9 enable
#
ipv4-family vpn-instance vpna
import-route direct
peer 10.1.1.1 as-number 65410
#
ipv4-family vpn-instance vpnb
import-route direct
peer 10.2.1.1 as-number 65420
#
ospf 1
area 0.0.0.0
network 11.11.11.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
return
```

P

```
#
sysname P
#
vlan batch 100 200
#
mpls lsr-id 2.2.2.9
#
mpls
#
mpls ldp
#
interface Vlanif100
ip address 11.11.11.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif200
ip address 12.12.12.1 255.255.255.0
```

```
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
ospf 1
area 0.0.0.0
network 11.11.11.0 0.0.0.255
network 12.12.12.0 0.0.0.255
network 2.2.2.9 0.0.0.0
#
return
```

PE2

```
#
sysname PE2
#
vlan batch 100 200 300
#
ip vpn-instance vpna
ipv4-family
route-distinguisher 200:1
vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity
#
ip vpn-instance vpnb
ipv4-family
route-distinguisher 200:2
vpn-target 222:2 export-extcommunity
vpn-target 222:2 import-extcommunity
#
mpls lsr-id 3.3.3.9
#
mpls
```

```
#
mpls ldp
#
interface Vlanif100
 ip binding vpn-instance vpna
 ip address 10.3.1.2 255.255.255.0
#
interface Vlanif200
 ip binding vpn-instance vpnb
 ip address 10.4.1.2 255.255.255.0
#
interface Vlanif300
 ip address 12.12.12.2 255.255.255.0
 mpls
 mpls ldp
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 300
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
#
ipv4-family unicast
 peer 1.1.1.9 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 1.1.1.9 enable
#
ipv4-family vpn-instance vpna
```

```
import-route direct
peer 10.3.1.1 as-number 65430
#
ipv4-family vpn-instance vpnb
import-route direct
peer 10.4.1.1 as-number 65440
#
ospf 1
area 0.0.0.0
network 12.12.12.0 0.0.0.255
network 3.3.3.9 0.0.0.0
#
return
```

CE1

```
#
sysname CE1
#
vlan batch 100
#
interface Vlanif100
ip address 10.1.1.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface LoopBack1
ip address 11.11.11.11 255.255.255.255
#
bgp 65410
peer 10.1.1.2 as-number 100
#
ipv4-family unicast
network 11.11.11.11 255.255.255.255
peer 10.1.1.2 enable
#
return
```

CE2

```
#
sysname CE2
#
```

```
vlan batch 100
#
interface Vlanif100
 ip address 10.2.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface LoopBack1
 ip address 22.22.22.22 255.255.255.255
#
bgp 65420
 peer 10.2.1.2 as-number 100
#
ipv4-family unicast
 network 22.22.22.22 255.255.255.255
 peer 10.2.1.2 enable
#
return
```

CE3

```
#
sysname CE3
#
vlan batch 100
#
interface Vlanif100
 ip address 10.3.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface LoopBack1
 ip address 33.33.33.33 255.255.255.255
#
bgp 65430
 peer 10.3.1.2 as-number 100
#
ipv4-family unicast
 network 33.33.33.33 255.255.255.255
 peer 10.3.1.2 enable
```



```
#  
return
```

CE4

```
#  
sysname CE4  
#  
vlan batch 100  
#  
interface Vlanif100  
ip address 10.4.1.1 255.255.255.0  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 100  
#  
interface LoopBack1  
ip address 44.44.44.44 255.255.255.255  
#  
bgp 65440  
peer 10.4.1.2 as-number 100  
#  
ipv4-family unicast  
network 44.44.44.44 255.255.255.255  
peer 10.4.1.2 enable  
#  
return
```

1.1.5.9.1.3 举例：配置 Hub and Spoke 示例（Hub-PE 和 Hub-CE 双链路接入）

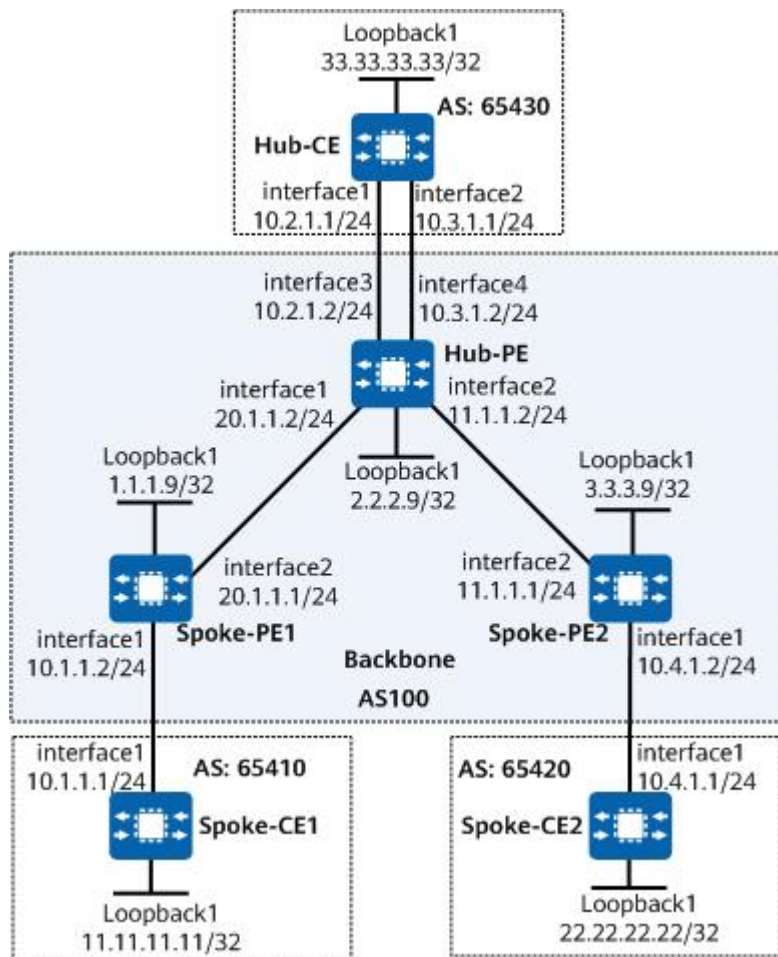
组网需求

如图 1 所示，Spoke-CE 之间的通信通过中心站点 Hub-CE 控制，即 Spoke-CE 之间的流量经过 Hub-CE 转发，而不是只经过 Hub-PE 转发。同时，Hub-PE 和 Hub-CE 双链路接入。

图 1 Hub and Spoke 组网图

说明

本例中 interface1，interface2、interface3、interface4 分别代表 Vlanif100，Vlanif200，Vlanif300，Vlanif400。



配置注意事项

在配置过程中，需注意以下事项：

Spoke-PE 上配置的 Import Target 和 Export Target 应不同。

Hub-PE 上创建两个 VPN 实例（vpn_in，vpn_out）。其中，vpn_in 接收的 VPN-target 团体属性为两个 Spoke-PE 发布的 VPN-target 团体属性值；vpn_out 发布的 VPN-target 团体属性值与接收的 VPN-target 团体属性不同，且为两个 Spoke-PE 接收的 VPN-target 团体属性值。

Hub-PE 上配置允许接收 AS_Path 中 AS 号重复 1 次的路由。

配置思路

采用如下的思路配置 IPv4 L3VPN：

1. 骨干网上配置 OSPF 实现 PE 之间的互通。
2. 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 MPLS LSP。
3. PE 上配置使能 IPv4 地址族 VPN 实例，并把与 CE 相连的接口和相应的 VPN 实例绑定。
4. PE 之间配置 MP-IBGP 交换 VPN 路由信息。
5. CE 与 PE 之间配置 EBGP 交换 VPN 路由信息。

操作步骤

1. 在骨干网上配置 IGP 协议，实现骨干网 Hub-PE 和 Spoke-PE 的互通。

本例中采用 OSPF，具体配置过程请参见后面的配置文件。

配置完成后，Hub-PE 和 Spoke-PE 之间应能建立 OSPF 邻居关系，执行 **display ospf peer** 命令可以看到邻居状态为 Full。执行 **display ip routing-table** 命令可以看到 Hub-PE 和 Spoke-PE 之间学习到对方的 Loopback 路由。

2. 在骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。

具体配置过程请参见后面的配置文件。

配置完成后，Hub-PE 和 Spoke-PE 之间应该建立起 LDP 对等体关系，在各设备上执行 **display mpls ldp session** 命令可以看到显示结果中 Session State 项为 “Operational”。

3. 在各 PE 设备上配置使能 IPv4 地址族的 VPN 实例，将 CE 接入 PE。

说明

Hub-PE 上其中一个 VPN 的 Import-Target 列表必须包含所有 Spoke-PE 的 Export-Target 属性。

Hub-PE 上另一个 VPN 的 Export-Target 列表必须包含所有 Spoke-PE 的 Import-Target 属性。

配置 Spoke-PE1。

```
<Spoke-PE1> system-view
[Spoke-PE1] ip vpn-instance vpna
[Spoke-PE1-vpn-instance-vpna] ipv4-family
[Spoke-PE1-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[Spoke-PE1-vpn-instance-vpna-af-ipv4] vpn-target 100:1 export-extcommunity
[Spoke-PE1-vpn-instance-vpna-af-ipv4] vpn-target 200:1 import-extcommunity
[Spoke-PE1-vpn-instance-vpna-af-ipv4] quit
[Spoke-PE1-vpn-instance-vpna] quit
[Spoke-PE1] interface Vlanif 100
[Spoke-PE1-Vlanif100] ip binding vpn-instance vpna
[Spoke-PE1-Vlanif100] ip address 10.1.1.2 24
[Spoke-PE1-Vlanif100] quit
```

配置 Spoke-PE2。

```
<Spoke-PE2> system-view
[Spoke-PE2] ip vpn-instance vpna
[Spoke-PE2-vpn-instance-vpna] ipv4-family
[Spoke-PE2-vpn-instance-vpna-af-ipv4] route-distinguisher 100:3
[Spoke-PE2-vpn-instance-vpna-af-ipv4] vpn-target 100:1 export-extcommunity
[Spoke-PE2-vpn-instance-vpna-af-ipv4] vpn-target 200:1 import-extcommunity
[Spoke-PE2-vpn-instance-vpna-af-ipv4] quit
[Spoke-PE2-vpn-instance-vpna] quit
[Spoke-PE2] interface Vlanif 100
[Spoke-PE2-Vlanif100] ip binding vpn-instance vpna
[Spoke-PE2-Vlanif100] ip address 10.4.1.2 24
```

```
[Spoke-PE2-Vlanif100] quit
```

配置 Hub-PE。

```
<Hub-PE> system-view
[Hub-PE] ip vpn-instance vpn_in
[Hub-PE-vpn-instance-vpn_in] ipv4-family
[Hub-PE-vpn-instance-vpn_in-af-ipv4] route-distinguisher 100:21
[Hub-PE-vpn-instance-vpn_in-af-ipv4] vpn-target 100:1 import-extcommunity
[Hub-PE-vpn-instance-vpn_in-af-ipv4] quit
[Hub-PE-vpn-instance-vpn_in] quit
[Hub-PE] ip vpn-instance vpn_out
[Hub-PE-vpn-instance-vpn_out] ipv4-family
[Hub-PE-vpn-instance-vpn_out-af-ipv4] route-distinguisher 100:22
[Hub-PE-vpn-instance-vpn_out-af-ipv4] vpn-target 200:1 export-extcommunity
[Hub-PE-vpn-instance-vpn_out-af-ipv4] quit
[Hub-PE-vpn-instance-vpn_out] quit
[Hub-PE] interface Vlanif 300
[Hub-PE-Vlanif300] ip binding vpn-instance vpn_in
[Hub-PE-Vlanif300] ip address 10.2.1.2 24
[Hub-PE-Vlanif300] quit
[Hub-PE] interface Vlanif 400
[Hub-PE-Vlanif400] ip binding vpn-instance vpn_out
[Hub-PE-Vlanif400] ip address 10.3.1.2 24
[Hub-PE-Vlanif400] quit
```

按图 1 配置各 CE 的接口 IP 地址，配置过程请参见后面的配置文件。

配置完成后，在 PE 设备上执行 **display ip vpn-instance verbose** 命令可以看到 VPN 实例的配置情况。各 PE 能用 **ping -vpn-instance vpn-name ip-address** 命令 ping 通自己接入的 CE。

说明

当 PE 上有多个绑定了同一个 VPN 的接口，则使用 **ping -vpn-instance** 命令 ping 对端 PE 接入的 CE 时，要指定源 IP 地址，即要指定 **ping -vpn-instance vpn-instance-name -a source-ip-address dest-ip-address** 命令中的参数 **-a source-ip-address**，否则可能 ping 不通。

4. 在 PE 与 CE 之间建立 EBGP 对等体关系，引入 VPN 路由。

说明

Hub-PE 上需要配置允许 AS 号重复一次，以接收 Hub-CE 发布的路由。

Spoke-PE 上不需要配置允许 AS 号重复一次，因为设备接收 IBGP 对等体发布的路由时并不检查其中的 AS-PATH 属性。

配置 Spoke-CE1。

```
[Spoke-CE1] interface loopback 1
[Spoke-CE1-Loopback1] ip address 11.11.11.11 32
[Spoke-CE1-Loopback1] quit
```

```
[Spoke-CE1] bgp 65410  
[Spoke-CE1-bgp] peer 10.1.1.2 as-number 100  
[Spoke-CE1-bgp] network 11.11.11.11 32  
[Spoke-CE1-bgp] quit
```

配置 Spoke-PE1。

```
[Spoke-PE1] bgp 100  
[Spoke-PE1-bgp] ipv4-family vpn-instance vpna  
[Spoke-PE1-bgp-vpna] peer 10.1.1.1 as-number 65410  
[Spoke-PE1-bgp-vpna] quit  
[Spoke-PE1-bgp] quit
```

配置 Spoke-CE2。

```
[Spoke-CE2] interface loopback 1  
[Spoke-CE2-Loopback1] ip address 22.22.22.22 32  
[Spoke-CE2-Loopback1] quit  
[Spoke-CE2] bgp 65420  
[Spoke-CE2-bgp] peer 10.4.1.2 as-number 100  
[Spoke-CE2-bgp] network 22.22.22.22 32  
[Spoke-CE2-bgp] quit
```

配置 Spoke-PE2。

```
[Spoke-PE2] bgp 100  
[Spoke-PE2-bgp] ipv4-family vpn-instance vpna  
[Spoke-PE2-bgp-vpna] peer 10.4.1.1 as-number 65420  
[Spoke-PE2-bgp-vpna] quit  
[Spoke-PE2-bgp] quit
```

配置 Hub-CE。

```
[Hub-CE] interface loopback 1  
[Hub-CE-Loopback1] ip address 33.33.33.33 32  
[Hub-CE-Loopback1] quit  
[Hub-CE] bgp 65430  
[Hub-CE-bgp] peer 10.2.1.2 as-number 100  
[Hub-CE-bgp] peer 10.3.1.2 as-number 100  
[Hub-CE-bgp] network 33.33.33.33 32  
[Hub-CE-bgp] quit
```

配置 Hub-PE。

```
[Hub-PE] bgp 100  
[Hub-PE-bgp] ipv4-family vpn-instance vpn_in  
[Hub-PE-bgp-vpn_in] peer 10.2.1.1 as-number 65430  
[Hub-PE-bgp-vpn_in] quit  
[Hub-PE-bgp] ipv4-family vpn-instance vpn_out  
[Hub-PE-bgp-vpn_out] peer 10.3.1.1 as-number 65430
```

```
[Hub-PE-bgp-vpn_out] peer 10.3.1.1 allow-as-loop 1
[Hub-PE-bgp-vpn_out] quit
[Hub-PE-bgp] quit
```

配置完成后，在各 PE 设备上执行 **display bgp vpnv4 all peer** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

5. 在 PE 之间建立 MP-IBGP 对等体关系。

配置 Spoke-PE1。

```
[Spoke-PE1] bgp 100
[Spoke-PE1-bgp] peer 2.2.2.9 as-number 100
[Spoke-PE1-bgp] peer 2.2.2.9 connect-interface loopback 1
[Spoke-PE1-bgp] ipv4-family vpnv4
[Spoke-PE1-bgp-af-vpnv4] peer 2.2.2.9 enable
[Spoke-PE1-bgp-af-vpnv4] quit
```

配置 Spoke-PE2。

```
[Spoke-PE2] bgp 100
[Spoke-PE2-bgp] peer 2.2.2.9 as-number 100
[Spoke-PE2-bgp] peer 2.2.2.9 connect-interface loopback 1
[Spoke-PE2-bgp] ipv4-family vpnv4
[Spoke-PE2-bgp-af-vpnv4] peer 2.2.2.9 enable
[Spoke-PE2-bgp-af-vpnv4] quit
```

配置 Hub-PE。

```
[Hub-PE] bgp 100
[Hub-PE-bgp] peer 1.1.1.9 as-number 100
[Hub-PE-bgp] peer 1.1.1.9 connect-interface loopback 1
[Hub-PE-bgp] peer 3.3.3.9 as-number 100
[Hub-PE-bgp] peer 3.3.3.9 connect-interface loopback 1
[Hub-PE-bgp] ipv4-family vpnv4
[Hub-PE-bgp-af-vpnv4] peer 1.1.1.9 enable
[Hub-PE-bgp-af-vpnv4] peer 3.3.3.9 enable
[Hub-PE-bgp-af-vpnv4] quit
```

配置完成后，在各 PE 设备上执行 **display bgp peer** 或 **display bgp vpnv4 all peer** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

检查配置结果

完成上述配置后，Spoke-CE 之间可以相互 Ping 通，使用 Tracert 可以看到 Spoke-CE 之间的流量经过 Hub-CE 转发，也可以通过 Ping 结果中的 TTL 值推算 Spoke-CE 之间经过的转发设备数目。

以 Spoke-CE1 的显示为例：

```
<Spoke-CE1> ping -a 11.11.11.11 22.22.22.22
PING 22.22.22.22: 56 data bytes, press CTRL_C to break
```

```

Reply from 22.22.22.22: bytes=56 Sequence=1 ttl=250ime=80 ms
Reply from 22.22.22.22: bytes=56 Sequence=2 ttl=250ime=129 ms
Reply from 22.22.22.22: bytes=56 Sequence=3 ttl=250 time=132 ms
Reply from 22.22.22.22: bytes=56 Sequence=4 ttl=250 time=92 ms
Reply from 22.22.22.22: bytes=56 Sequence=5 ttl=250 time=126 ms
--- 22.22.22.22 ping statistics ---
 5 packet(s) transmitted
 5 packet(s) received
 0.00% packet loss
 round-trip min/avg/max = 80/111/132 ms
<Spoke-CE1> tracert -a 11.11.11.11 22.22.22.22
traceroute to 22.22.22.22(22.22.22.22), max hops: 64, packet length: 40, press CTRL_C to break
 1 10.1.1.2 31 ms 12 ms 6 ms
 2 10.3.1.2 9 ms 11 ms 24 ms
 3 10.3.1.1 46 ms 27 ms 9 ms
 4 10.2.1.2 23 ms 22 ms 28 ms
 5 10.4.1.2 12 ms 34 ms 23 ms
 6 22.22.22.22 46 ms 1 ms 9 ms

```

在 Spoke-CE 上执行 **display bgp routing-table** 命令，可以看到去往对端 Spoke-CE 的 BGP 路由的 AS 路径中存在重复的 AS 号。

以 Spoke-CE1 的显示为例：

```

<Spoke-CE1> display bgp routing-table

BGP Local router ID is 11.11.11.11
Status codes: * - valid, > - best, d - damped, x - best external, a - add path,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 3

   Network      NextHop      MED      LocPrf  PrefVal Path/Ogn
*>  11.11.11.11/32  0.0.0.0          0          0    i
*>  22.22.22.22/32  10.1.1.2          0   100 65430 100 65420i
*>  33.33.33.33/32  10.1.1.2          0   100 65430i

```

配置脚本

Spoke-CE1

```

#
sysname Spoke-CE1
#
vlan batch 100

```

```
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface Loopback 1
 ip address 11.11.11.11 255.255.255.255
#
bgp 65410
 peer 10.1.1.2 as-number 100
#
ipv4-family unicast
 network 11.11.11.11 255.255.255.255
 peer 10.1.1.2 enable
#
return
```

Spoke-PE1

```
#
sysname Spoke-PE1
#
vlan batch 100 200
#
ip vpn-instance vpna
 ipv4-family
  route-distinguisher 100:1
  vpn-target 100:1 export-extcommunity
  vpn-target 200:1 import-extcommunity
#
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
#
interface Vlanif100
 ip binding vpn-instance vpna
 ip address 10.1.1.2 255.255.255.0
#
interface Vlanif200
```



```
ip address 20.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
bgp 100
peer 2.2.2.9 as-number 100
peer 2.2.2.9 connect-interface LoopBack1
#
ipv4-family unicast
peer 2.2.2.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 2.2.2.9 enable
#
ipv4-family vpn-instance vpna
peer 10.1.1.1 as-number 65410
#
ospf 1
area 0.0.0.0
network 20.1.1.0 0.0.0.255
network 1.1.1.9 0.0.0.0
#
return
```

Spoke-PE2

```
#
sysname Spoke-PE2
#
vlan batch 100 200
#
ip vpn-instance vpna
```

```
ipv4-family
route-distinguisher 100:3
vpn-target 100:1 export-extcommunity
vpn-target 200:1 import-extcommunity
#
mpls lsr-id 3.3.3.9
#
mpls
#
mpls ldp
#
interface Vlanif100
ip binding vpn-instance vpna
ip address 10.4.1.2 255.255.255.0
#
interface Vlanif200
ip address 11.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
interface LoopBack1
ip address 3.3.3.9 255.255.255.255
#
bgp 100
peer 2.2.2.9 as-number 100
peer 2.2.2.9 connect-interface LoopBack1
#
ipv4-family unicast
peer 2.2.2.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 2.2.2.9 enable
#
ipv4-family vpn-instance vpna
```

```
peer 10.4.1.1 as-number 65420
#
ospf 1
area 0.0.0.0
network 3.3.3.9 0.0.0.0
network 11.1.1.0 0.0.0.255
#
return
```

Spoke-CE2

```
#
sysname Spoke-CE2
#
vlan batch 100
#
interface Vlanif100
ip address 10.4.1.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface Loopback 1
ip address 22.22.22.22 255.255.255.255
#
bgp 65420
peer 10.4.1.2 as-number 100
#
ipv4-family unicast
network 22.22.22.22 255.255.255.255
peer 10.4.1.2 enable
#
return
```

Hub-CE

```
#
sysname Hub-CE
#
vlan batch 100 200
#
interface Vlanif100
ip address 10.2.1.1 255.255.255.0
#
```

```
interface Vlanif200
 ip address 10.3.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface Loopback 1
 ip address 33.33.33.33 255.255.255.255
#
bgp 65430
 peer 10.2.1.2 as-number 100
 peer 10.3.1.2 as-number 100
#
ipv4-family unicast
 peer 10.3.1.2 enable
 network 33.33.33.33 255.255.255.255
 peer 10.2.1.2 enable
#
return
```

Hub-PE

```
#
sysname Hub-PE
#
vlan batch 100 200 300 400
#
ip vpn-instance vpn_in
 ipv4-family
  route-distinguisher 100:21
  vpn-target 100:1 import-extcommunity
#
ip vpn-instance vpn_out
 ipv4-family
  route-distinguisher 100:22
  vpn-target 200:1 export-extcommunity
#
mpls lsr-id 2.2.2.9
#
```

```
mpls
#
mpls ldp
#
interface Vlanif100
ip address 20.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif200
ip address 11.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif300
ip binding vpn-instance vpn_in
ip address 10.2.1.2 255.255.255.0
#
interface Vlanif400
ip binding vpn-instance vpn_out
ip address 10.3.1.2 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 300
#
interface 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 400
#
interface LoopBack1
ip address 2.2.2.9 255.255.255.255
#
bgp 100
peer 1.1.1.9 as-number 100
```

```
peer 1.1.1.9 connect-interface LoopBack1
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack1
#
ipv4-family unicast
peer 1.1.1.9 enable
peer 3.3.3.9 enable
#
ipv4-family vpnv4
policy vpn-target
peer 1.1.1.9 enable
peer 3.3.3.9 enable
#
ipv4-family vpn-instance vpn_in
peer 10.2.1.1 as-number 65430
#
ipv4-family vpn-instance vpn_out
peer 10.3.1.1 as-number 65430
peer 10.3.1.1 allow-as-loop
#
ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 20.1.1.0 0.0.0.255
network 11.1.1.0 0.0.0.255
#
return
```

1.1.5.9.1.4 举例：配置 L3VPN+VRRP 综合场景

组网需求

如图 1 所示，CE1 和 CE2 属于 vpna，CE1 通过 PE4 双归属到 PE1 和 PE2。用户希望实现：

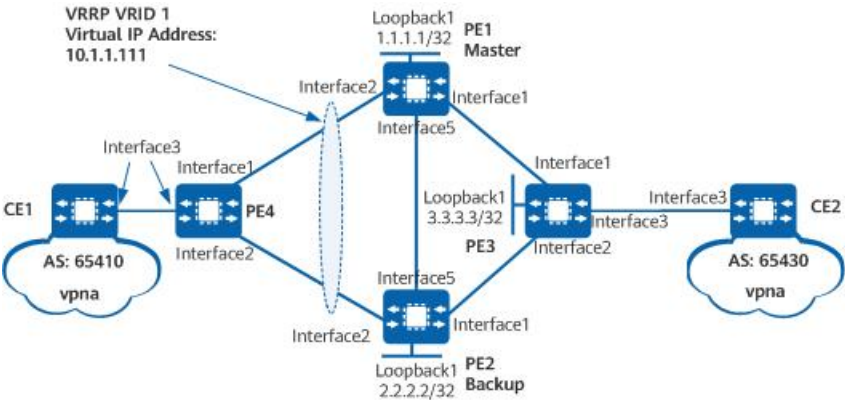
正常情况下，CE1 以 PE1 为默认网关与 CE2 互通。当 PE1 故障时，PE2 接替作为网关继续进行工作，实现网关的冗余备份。

PE1 故障恢复后，其延时 20 秒通过抢占的方式重新成为 Master，承担数据传输。

图 1 配置 L3VPN+VRRP 综合示例组网图

说明

本例中 interface1、interface2、interface3、interface5 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/5。



设备	接口	对应的 Vlanif	IP 地址
PE1	10GE1/0/1	VLANIF300	192.168.1.1/24
	10GE1/0/2	VLANIF100	10.1.1.1/24
	10GE1/0/5	VLANIF100	10.1.1.1/24
PE2	10GE1/0/1	VLANIF200	192.168.2.1/24
	10GE1/0/2	VLANIF100	10.1.1.2/24
	10GE1/0/5	VLANIF100	10.1.1.2/24
PE3	10GE1/0/1	VLANIF300	192.168.1.2/24
	10GE1/0/2	VLANIF200	192.168.2.2/24
	10GE1/0/3	VLANIF400	172.16.1.100/24
CE1	10GE1/0/3	VLANIF100	10.1.1.100/24
CE2	10GE1/0/3	VLANIF400	172.16.1.200/24

配置注意事项

在配置过程中，需注意以下事项：

同一 VPN 的 Export VPN-Target 列表与其它站点的 Import VPN-Target 列表有共同的 VPN-Target，Import VPN-Target 列表与其它站点的 Export VPN-Target 列表有共同的 VPN-Target。

PE 与 CE 相连的接口绑定了 VPN 实例后，将删除该接口上已经配置的 IP 地址、路由协议等三层特性，如果需要应重新配置。

配置思路

采用如下的思路配置 IPv4 L3VPN：

1. 骨干网上配置 OSPF 实现 PE 之间的互通。

2. 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 MPLS LSP。
3. PE 上配置使能 IPv4 地址族 VPN 实例，并把与 CE 相连的接口和相应的 VPN 实例绑定。
4. PE 之间配置 MP-IBGP 交换 VPN 路由信息。
5. CE 与 PE 之间配置 EBGP 交换 VPN 路由信息。

操作步骤

1. 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 的互通
配置 PE1。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] vlan batch 100 300
[PE1] interface 10GE1/0/1
[PE1-10GE1/0/1] port link-type hybrid
[PE1-10GE1/0/1] port hybrid pvid vlan 300
[PE1-10GE1/0/1] port hybrid untagged vlan 300
[PE1-10GE1/0/1] quit
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] quit
[PE1] interface vlanif 300
[PE1-Vlanif300] ip address 192.168.1.1 24
[PE1-Vlanif300] quit
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 PE2。

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] vlan batch 100 200
[PE2] interface 10GE1/0/1
[PE2-10GE1/0/1] port link-type hybrid
[PE2-10GE1/0/1] port hybrid pvid vlan 200
[PE2-10GE1/0/1] port hybrid untagged vlan 200
[PE2-10GE1/0/1] quit
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 2.2.2.2 32
[PE2-LoopBack1] quit
```



```
[PE2] interface vlanif 200
[PE2-Vlanif200] ip address 192.168.2.1 24
[PE2-Vlanif200] quit
[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置 PE3。

```
<HUAWEI> system-view
[HUAWEI] sysname PE3
[PE3] vlan batch 200 300 400
[PE3] interface 10GE1/0/1
[PE3-10GE1/0/1] port link-type hybrid
[PE3-10GE1/0/1] port hybrid pvid vlan 300
[PE3-10GE1/0/1] port hybrid untagged vlan 300
[PE3-10GE1/0/1] quit
[PE3] interface 10GE1/0/2
[PE3-10GE1/0/2] port link-type hybrid
[PE3-10GE1/0/2] port hybrid pvid vlan 200
[PE3-10GE1/0/2] port hybrid untagged vlan 200
[PE3-10GE1/0/2] quit
[PE3] interface loopback 1
[PE3-LoopBack1] ip address 3.3.3.3 32
[PE3-LoopBack1] quit
[PE3] interface vlanif 200
[PE3-Vlanif200] ip address 192.168.2.2 24
[PE3-Vlanif200] quit
[PE3] interface vlanif 300
[PE3-Vlanif300] ip address 192.168.1.2 24
[PE3-Vlanif300] quit
[PE3] ospf 1
[PE3-ospf-1] area 0
[PE3-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[PE3-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[PE3-ospf-1-area-0.0.0.0] quit
[PE3-ospf-1] quit
```

2. 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE1。

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlanif 300
[PE1-Vlanif300] mpls
[PE1-Vlanif300] mpls ldp
[PE1-Vlanif300] quit
```

配置 PE2。

```
[PE2] mpls lsr-id 2.2.2.2
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlanif 200
[PE2-Vlanif200] mpls
[PE2-Vlanif200] mpls ldp
[PE2-Vlanif200] quit
```

配置 PE3。

```
[PE3] mpls lsr-id 3.3.3.3
[PE3] mpls
[PE3-mpls] quit
[PE3] mpls ldp
[PE3-mpls-ldp] quit
[PE3] interface vlanif 200
[PE3-Vlanif200] mpls
[PE3-Vlanif200] mpls ldp
[PE3-Vlanif200] quit
[PE3] interface vlanif 300
[PE3-Vlanif300] mpls
[PE3-Vlanif300] mpls ldp
[PE3-Vlanif300] quit
```

3. 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

配置 PE4。

```
<HUAWEI> system-view
[HUAWEI] sysname PE4
[PE4] vlan batch 100
[PE4] interface 10GE1/0/1
[PE4-10GE1/0/1] port link-type hybrid
[PE4-10GE1/0/1] port hybrid pvid vlan 100
```

```
[PE4-10GE1/0/1] port hybrid untagged vlan 100
[PE4-10GE1/0/1] quit
[PE4] interface 10GE1/0/2
[PE4-10GE1/0/2] port link-type hybrid
[PE4-10GE1/0/2] port hybrid pvid vlan 100
[PE4-10GE1/0/2] port hybrid untagged vlan 100
[PE4-10GE1/0/2] quit
[PE4] interface 10GE1/0/3
[PE4-10GE1/0/3] port link-type hybrid
[PE4-10GE1/0/3] port hybrid pvid vlan 100
[PE4-10GE1/0/3] port hybrid untagged vlan 100
[PE4-10GE1/0/3] quit
```

配置 PE1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] interface 10GE1/0/2
[PE1-10GE1/0/2] port link-type hybrid
[PE1-10GE1/0/2] port hybrid pvid vlan 100
[PE1-10GE1/0/2] port hybrid untagged vlan 100
[PE1-10GE1/0/2] quit
[PE1] interface 10GE1/0/5
[PE1-10GE1/0/5] port link-type hybrid
[PE1-10GE1/0/5] port hybrid pvid vlan 100
[PE1-10GE1/0/5] port hybrid untagged vlan 100
[PE1-10GE1/0/5] quit
[PE1] interface vlanif 100
[PE1-Vlanif100] ip binding vpn-instance vpna
[PE1-Vlanif100] ip address 10.1.1.1 24
[PE1-Vlanif100] quit
```

配置 PE2。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 100:1
[PE2-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE2-vpn-instance-vpna-af-ipv4] quit
[PE2-vpn-instance-vpna] quit
[PE2] interface 10GE1/0/2
[PE2-10GE1/0/2] port link-type hybrid
[PE2-10GE1/0/2] port hybrid pvid vlan 100
[PE2-10GE1/0/2] port hybrid untagged vlan 100
```

```
[PE2-10GE1/0/2] quit
[PE2] interface 10GE1/0/5
[PE2-10GE1/0/5] port link-type hybrid
[PE2-10GE1/0/5] port hybrid pvid vlan 100
[PE2-10GE1/0/5] port hybrid untagged vlan 100
[PE2-10GE1/0/5] quit
[PE2] interface vlanif 100
[PE2-Vlanif100] ip binding vpn-instance vpna
[PE2-Vlanif100] ip address 10.1.1.2 24
[PE2-Vlanif100] quit
```

配置 PE3。

```
[PE3] ip vpn-instance vpna
[PE3-vpn-instance-vpna] route-distinguisher 100:1
[PE3-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE3-vpn-instance-vpna-af-ipv4] quit
[PE3-vpn-instance-vpna] quit
[PE3] interface 10GE1/0/3
[PE3-10GE1/0/3] port link-type hybrid
[PE3-10GE1/0/3] port hybrid pvid vlan 400
[PE3-10GE1/0/3] port hybrid untagged vlan 400
[PE3-10GE1/0/3] quit
[PE3] interface vlanif 400
[PE3-Vlanif400] ip binding vpn-instance vpna
[PE3-Vlanif400] ip address 172.16.1.100 24
[PE3-Vlanif400] quit
```

配置 CE1。

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] vlan 100
[CE1-vlan100] quit
[CE1] interface 10GE1/0/3
[CE1-10GE1/0/3] port link-type hybrid
[CE1-10GE1/0/3] port hybrid pvid vlan 100
[CE1-10GE1/0/3] port hybrid untagged vlan 100
[CE1-10GE1/0/3] quit
[CE1] interface vlanif 100
[CE1-Vlanif100] ip address 10.1.1.100 24
[CE1-Vlanif100] quit
```

配置 CE2。

```
<HUAWEI> system-view
[HUAWEI] sysname CE2
```

```
[CE2] vlan 400
[CE2-vlan400] quit
[CE2] interface 10GE1/0/3
[CE2-10GE1/0/3] port link-type hybrid
[CE2-10GE1/0/3] port hybrid pvid vlan 400
[CE2-10GE1/0/3] port hybrid untagged vlan 400
[CE2-10GE1/0/3] quit
[CE2] interface vlanif 400
[CE2-Vlanif400] ip address 172.16.1.200 24
[CE2-Vlanif400] quit
```

4. 在 PE 与 CE 之间建立 EBGP 对等体关系，引入 VPN 路由

配置 CE1。

```
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.111 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] quit
```

配置 CE2。

```
[CE2] bgp 65430
[CE2-bgp] peer 172.16.1.100 as-number 100
[CE2-bgp] import-route direct
[CE2-bgp] quit
```

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] peer 10.1.1.100 as-number 65410
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-vpna] peer 10.1.1.100 as-number 65410
[PE2-bgp-vpna] import-route direct
[PE2-bgp-vpna] quit
[PE2-bgp] quit
```

配置 PE3。

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpna
[PE3-bgp-vpna] peer 172.16.1.200 as-number 65430
[PE3-bgp-vpna] import-route direct
```

```
[PE3-bgp-vpna] quit
[PE3-bgp] quit
```

5. 在 PE 之间建立 MP-IBGP 对等体关系

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 3.3.3.3 as-number 100
[PE1-bgp] peer 3.3.3.3 connect-interface loopback 1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 3.3.3.3 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 3.3.3.3 as-number 100
[PE2-bgp] peer 3.3.3.3 connect-interface loopback 1
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 3.3.3.3 enable
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

配置 PE3。

```
[PE3] bgp 100
[PE3-bgp] peer 1.1.1.1 as-number 100
[PE3-bgp] peer 2.2.2.2 as-number 100
[PE3-bgp] peer 1.1.1.1 connect-interface loopback 1
[PE3-bgp] peer 2.2.2.2 connect-interface loopback 1
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpnv4] peer 1.1.1.1 enable
[PE3-bgp-af-vpnv4] peer 2.2.2.2 enable
[PE3-bgp-af-vpnv4] quit
[PE3-bgp] quit
```

6. 配置 MSTP 协议，对 PE2 与 PE4 之间的链路进行阻塞，防止环路的产生

配置 PE1 设备的 MSTP 工作模式，此模式默认使能。

```
[PE1] stp mode mstp
```

配置 PE2 设备的 MSTP 工作模式，此模式默认使能。

```
[PE2] stp mode mstp
```

配置 PE4 设备的 MSTP 工作模式，此模式默认使能。

```
[PE4] stp mode mstp
```

配置 PE1 为根桥。

```
[PE1] stp root primary
```

配置 PE2 为备份根桥。

```
[PE2] stp root secondary
```

配置 PE2 与 PE4 的互连接口的端口路径开销值为 400000，以实现将 PE2 与 PE4 之间的链路进行阻塞。

```
[PE2] interface 10GE1/0/2
[PE2-10GE1/0/2] stp cost 400000
[PE2-10GE1/0/2] quit
[PE4] interface 10GE1/0/2
[PE4-10GE1/0/2] stp cost 400000
[PE4-10GE1/0/2] quit
```

配置 PE4 与 CE1 相连接口 STP 去使能。

```
[PE4] interface 10GE1/0/3
[PE4-10GE1/0/3] stp disable
[PE4-10GE1/0/3] quit
```

配置设备 PE1 全局使能 STP，此功能默认使能。

```
[PE1] stp enable
```

配置设备 PE2 全局使能 STP，此功能默认使能。

```
[PE2] stp enable
```

配置设备 PE4 全局使能 STP，此功能默认使能。

```
[PE4] stp enable
```

配置完成后，在 PE4 上执行 **display stp brief** 命令，查看接口状态，接口 10GE1/0/2 在生成树选举中成为 Alternate 端口，处于 DISCARDING 状态。

```
[PE4] display stp brief
```

MSTID	Port	Role	STP State	Protection	Cost	Edged
0	10GE1/0/1	ROOT	FORWARDING	NONE	2000	enable
0	10GE1/0/2	ALTE	DISCARDING	NONE	400000	enable

7. 配置 VRRP 备份组

在 PE1 上创建 VRRP 备份组 1，配置 PE1 在该备份组中的优先级为 120，并配置抢占时间为 20 秒。

```
[PE1] interface vlanif 100
[PE1-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[PE1-Vlanif100] vrrp vrid 1 priority 120
[PE1-Vlanif100] vrrp vrid 1 preempt timer delay 20
[PE1-Vlanif100] quit
```

在 PE2 上创建 VRRP 备份组 1，其在该备份组中的优先级为缺省值 100。

```
[PE2] interface vlanif 100
[PE2-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[PE2-Vlanif100] quit
```

检查配置结果

完成上述配置以后，在 PE1 和 PE2 上分别执行 **display vrrp verbose** 命令，可以看到 PE1 在备份组中的状态为 Master，PE2 在备份组中的状态为 Backup。

[PE1] **display vrrp verbose**

Vlanif100 | Virtual Router 1

State : Master

Virtual IP : 10.1.1.111

Master IP : 10.1.1.1

PriorityRun : 120

PriorityConfig : 120

MasterPriority : 120

Preempt : YES Delay Time : 20 s Remain : --

Hold Multiplier: 3

TimerRun : 1 s

TimerConfig : 1 s

Auth type : NONE

Virtual MAC : 0000-5e00-0101

Check TTL : YES

Config type : normal-vrrp

Backup-forward : disabled

Create time : 2012-01-12 20:15:46

Last change time : 2012-01-12 20:15:46

[PE2] **display vrrp verbose**

Vlanif100 | Virtual Router 1

State : Backup

Virtual IP : 10.1.1.111

Master IP : 10.1.1.1

PriorityRun : 100

PriorityConfig : 100

MasterPriority : 120

Preempt : YES Delay Time : 0 s Remain : --

Hold Multiplier: 3

TimerRun : 1 s

TimerConfig : 1 s

Auth type : NONE

Virtual MAC : 0000-5e00-0101

Check TTL : YES

Config type : normal-vrrp

Backup-forward : disabled

Create time : 2012-01-12 20:15:46

Last change time : 2012-01-12 20:15:46

在 PE1 的接口 10GE1/0/2 和接口 10GE1/0/5 上执行 **shutdown** 命令，模拟 PE1 出现故障。

```
[PE1] interface 10GE1/0/2
[PE1-10GE1/0/2] shutdown
[PE1-10GE1/0/2] quit
[PE1] interface 10GE1/0/5
[PE1-10GE1/0/5] shutdown
[PE1-10GE1/0/5] quit
```

在 PE2 上执行 **display vrrp verbose** 命令查看 VRRP 状态信息，可以看到 PE2 的状态是 Master。

```
[PE2] display vrrp verbose
Vlanif100 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.1.111
  Master IP : 10.1.1.2
  PriorityRun : 100
  PriorityConfig : 100
  MasterPriority : 100
  Preempt : YES   Delay Time : 0 s   Remain : --
  Hold Multiplier: 3
  TimerRun : 1 s
  TimerConfig : 1 s
  Auth type : NONE
  Virtual MAC : 0000-5e00-0101
  Check TTL : YES
  Config type : normal-vrrp
  Backup-forward : disabled
  Create time : 2012-01-12 20:15:46
  Last change time : 2012-01-12 20:18:40
```

在 PE1 的接口 10GE1/0/2 和接口 10GE1/0/5 上执行 **undo shutdown** 命令，等待 20 秒后，在 PE1 上执行 **display vrrp verbose** 命令查看 VRRP 状态信息，可以看到 PE1 的状态恢复成 Master。

```
[PE1] interface 10GE1/0/2
[PE1-10GE1/0/2] undo shutdown
[PE1-10GE1/0/2] quit
[PE1] interface 10GE1/0/5
[PE1-10GE1/0/5] undo shutdown
[PE1-10GE1/0/5] quit
[PE1] display vrrp verbose
Vlanif100 | Virtual Router 1
  State : Master
  Virtual IP : 10.1.1.111
  Master IP : 10.1.1.1
  PriorityRun : 120
```

```
PriorityConfig : 120
MasterPriority : 120
Preempt : YES   Delay Time : 20 s   Remain : --
Hold Multiplier: 3
TimerRun : 1 s
TimerConfig : 1 s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : normal-vrrp
Backup-forward : disabled
Create time : 2012-01-12 20:15:46
Last change time : 2012-01-12 20:20:56
```

配置脚本

PE1

```
#
sysname PE1
#
vlan batch 100 300
#
stp instance 0 root primary
stp enable
#
ip vpn-instance vpna
  ipv4-family
    route-distinguisher 100:1
    vpn-target 111:1 export-extcommunity
    vpn-target 111:1 import-extcommunity
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#
interface Vlanif100
  ip binding vpn-instance vpna
  ip address 10.1.1.1 255.255.255.0
  vrrp vrid 1 virtual-ip 10.1.1.111
  vrrp vrid 1 priority 120
  vrrp vrid 1 preempt timer delay 20
```

```
#
interface Vlanif300
 ip address 192.168.1.1 255.255.255.0
 mpls
 mpls ldp
#
interface 10GE1/0/1
 port link-type hybrid
 port hybrid pvid vlan 300
 port hybrid untagged vlan 300
#
interface 10GE1/0/2
 port link-type hybrid
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface 10GE1/0/5
 port link-type hybrid
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 3.3.3.3 as-number 100
 peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
 undo synchronization
 peer 3.3.3.3 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 3.3.3.3 enable
#
ipv4-family vpn-instance vpna
 import-route direct
 peer 10.1.1.100 as-number 65410
#
ospf 1
 area 0.0.0.0
 network 1.1.1.1 0.0.0.0
```

```
network 192.168.1.0 0.0.0.255
#
return
```

PE2

```
#
sysname PE2
#
vlan batch 100 200
#
stp instance 0 root secondary
stp enable
#
ip vpn-instance vpna
ipv4-family
route-distinguisher 100:1
vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity
#
mpls lsr-id 2.2.2.2
#
mpls
#
mpls ldp
#
interface Vlanif100
ip binding vpn-instance vpna
ip address 10.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.111
#
interface Vlanif200
ip address 192.168.2.1 255.255.255.0
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type hybrid
port hybrid pvid vlan 200
port hybrid untagged vlan 200
#
interface 10GE1/0/2
port link-type hybrid
port hybrid pvid vlan 100
```

```
port hybrid untagged vlan 100
stp instance 0 cost 400000
#
interface 10GE1/0/5
port link-type hybrid
port hybrid pvid vlan 100
port hybrid untagged vlan 100
#
interface LoopBack1
ip address 2.2.2.2 255.255.255.255
#
bgp 100
peer 3.3.3.3 as-number 100
peer 3.3.3.3 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 3.3.3.3 enable
#
ipv4-family vpnv4
policy vpn-target
peer 3.3.3.3 enable
#
ipv4-family vpn-instance vpna
import-route direct
peer 10.1.1.100 as-number 65410
#
ospf 1
area 0.0.0.0
network 2.2.2.2 0.0.0.0
network 192.168.2.0 0.0.0.255
#
return
```

PE3

```
#
sysname PE3
#
vlan batch 200 300 400
#
ip vpn-instance vpna
ipv4-family
route-distinguisher 100:1
```

```
vpn-target 111:1 export-extcommunity
vpn-target 111:1 import-extcommunity
#
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
#
interface Vlanif200
ip address 192.168.2.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif300
ip address 192.168.1.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif400
ip binding vpn-instance vpna
ip address 172.16.1.100 255.255.255.0
#
interface 10GE1/0/1
port link-type hybrid
port hybrid pvid vlan 300
port hybrid untagged vlan 300
#
interface 10GE1/0/2
port link-type hybrid
port hybrid pvid vlan 200
port hybrid untagged vlan 200
#
interface 10GE1/0/3
port link-type hybrid
port hybrid pvid vlan 400
port hybrid untagged vlan 400
#
interface LoopBack1
ip address 3.3.3.3 255.255.255.255
#
bgp 100
peer 1.1.1.1 as-number 100
peer 1.1.1.1 connect-interface LoopBack1
```

```
peer 2.2.2.2 as-number 100
peer 2.2.2.2 connect-interface LoopBack1
#
ipv4-family unicast
undo synchronization
peer 1.1.1.1 enable
peer 2.2.2.2 enable
#
ipv4-family vpnv4
policy vpn-target
peer 1.1.1.1 enable
peer 2.2.2.2 enable
#
ipv4-family vpn-instance vpna
import-route direct
peer 172.16.1.200 as-number 65430
#
ospf 1
area 0.0.0.0
network 3.3.3.3 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
return
```

PE4

```
#
sysname PE4
#
vlan batch 100
#
stp enable
#
interface 10GE1/0/1
port link-type hybrid
port hybrid pvid vlan 100
port hybrid untagged vlan 100
#
interface 10GE1/0/2
port link-type hybrid
port hybrid pvid vlan 100
port hybrid untagged vlan 100
stp instance 0 cost 400000
```

```
#
interface 10GE1/0/3
 port link-type hybrid
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
 stp disable
#
return
```

CE1

```
#
sysname CE1
#
vlan batch 100
#
interface Vlanif100
 ip address 10.1.1.100 255.255.255.0
#
interface 10GE1/0/3
 port link-type hybrid
 port hybrid pvid vlan 100
 port hybrid untagged vlan 100
#
bgp 65410
 peer 10.1.1.111 as-number 100
#
ipv4-family unicast
 undo synchronization
 import-route direct
 peer 10.1.1.111 enable
#
return
```

CE2

```
#
sysname CE2
#
vlan batch 400
#
interface Vlanif400
 ip address 172.16.1.200 255.255.255.0
#
interface 10GE1/0/3
```



```

port link-type hybrid
port hybrid pvid vlan 400
port hybrid untagged vlan 400
#
bgp 65430
peer 172.16.1.100 as-number 100
#
ipv4-family unicast
undo synchronization
import-route direct
peer 172.16.1.100 enable
#
return

```

1.1.5.9.1.5 举例：配置企业使用路由策略控制 L3VPN 分支间用户互访场景

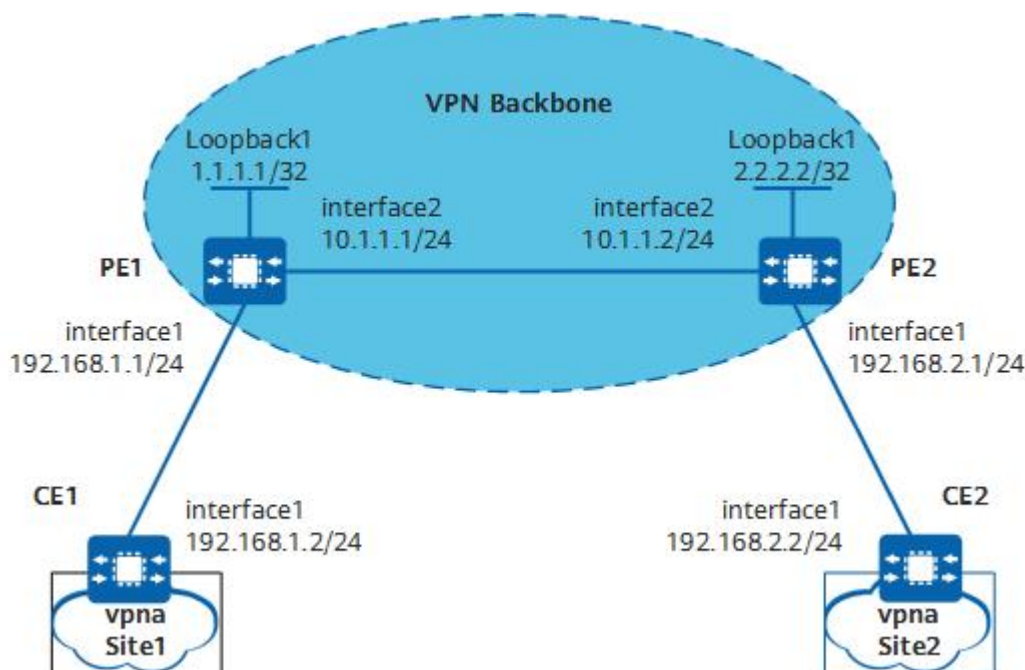
组网需求

如图 1 所示，CE1 连接分支 Site1、CE2 连接分支 Site2，Site1 和 Site2 之间穿越运营商骨干网。因业务需求，公司希望 Site1 和 Site2 间部分网段的用户能够安全互访。

图 1 配置企业使用路由策略控制 L3VPN 分支间用户互访组网图

说明

本例中 interface1 和 interface2 分别代表 Vlanif10，Vlanif100。



配置注意事项

在配置过程中，需注意以下事项：

同一 VPN 的 Export VPN-Target 列表与其它站点的 Import VPN-Target 列表有共同的 VPN-Target，Import VPN-Target 列表与其它站点的 Export VPN-Target 列表有共同的 VPN-Target。

PE 与 CE 相连的接口绑定了 VPN 实例后，将删除该接口上已经配置的 IP 地址、路由协议等三层特性，如果需要应重新配置。

配置思路

采用如下的思路配置企业使用路由策略控制 L3VPN 分支间用户互访：

1. PE 之间配置 OSPF，实现骨干网的 IP 连通性。
2. PE 之间配置 MPLS 基本能力和 MPLS LDP，建立 MPLS LSP 公网隧道，传输 VPN 数据。
3. PE 上配置 VPN 实例，接入 VPN 用户，并指定不同的 VPN Target，实现分支间的用户隔离。
4. PE 上配置路由策略，改变通过路由策略过滤的路由的 VPN Target，实现分支间特定网段的用户互通。
5. CE 与 PE 之间配置 EBGP，交换 VPN 路由信息。
6. PE 之间配置 MP-IBGP，交换 VPN 路由信息。

操作步骤

1. 在 MPLS 骨干网上配置 IGP 协议，实现骨干网 PE 间的互通
配置 PE1。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] interface loopback 1
[PE1-LoopBack1] ip address 1.1.1.1 32
[PE1-LoopBack1] quit
[PE1] vlan batch 10 100
[PE1] interface 10GE 1/0/1
[PE1-10GE1/0/1] port link-type trunk
[PE1-10GE1/0/1] port trunk allow-pass vlan 10
[PE1-10GE1/0/1] quit
[PE1] interface 10GE 1/0/7
[PE1-10GE1/0/7] port link-type trunk
[PE1-10GE1/0/7] port trunk allow-pass vlan 100
[PE1-10GE1/0/7] quit
[PE1] interface vlanif 100
[PE1-Vlanif100] ip address 10.1.1.1 24
[PE1-Vlanif100] quit
```

```
[PE1] ospf 1
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

配置 PE2。

```
<HUAWEI> system-view
[HUAWEI] sysname PE2
[PE2] interface loopback 1
[PE2-LoopBack1] ip address 2.2.2.2 32
[PE2-LoopBack1] quit
[PE2] vlan batch 10 100
[PE2] interface 10GE 1/0/1
[PE2-10GE1/0/1] port link-type trunk
[PE2-10GE1/0/1] port trunk allow-pass vlan 10
[PE2-10GE1/0/1] quit
[PE2] interface 10GE 1/0/7
[PE2-10GE1/0/7] port link-type trunk
[PE2-10GE1/0/7] port trunk allow-pass vlan 100
[PE2-10GE1/0/7] quit
[PE2] interface vlanif 100
[PE2-Vlanif100] ip address 10.1.1.2 24
[PE2-Vlanif100] quit
[PE2] ospf 1
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[PE2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

配置完成后，PE1、PE2 之间应能建立 OSPF 邻居关系，执行 **display ospf peer** 命令可以看到邻居状态为 Full。执行 **display ip routing-table** 命令可以看到 PE 之间学习到对方的 Loopback1 路由。

2. 在 MPLS 骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP

配置 PE1。

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface vlanif 100
[PE1-Vlanif100] mpls
```

```
[PE1-Vlanif100] mpls ldp
[PE1-Vlanif100] quit
```

配置 PE2。

```
[PE2] mpls lsr-id 2.2.2.2
[PE2] mpls
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface vlanif 100
[PE2-Vlanif100] mpls
[PE2-Vlanif100] mpls ldp
[PE2-Vlanif100] quit
```

上述配置完成后，PE1 与 PE2 之间应能建立 LDP 会话，执行 **display mpls ldp session** 命令可以看到显示结果中 Status 项为 “Operational”。

3. 在 PE 设备上配置 VPN 实例，将 CE 接入 PE

配置 PE1。

```
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] route-distinguisher 100:1
[PE1-vpn-instance-vpna-af-ipv4] vpn-target 111:1 both
[PE1-vpn-instance-vpna-af-ipv4] quit
[PE1-vpn-instance-vpna] quit
[PE1] interface vlanif 10
[PE1-Vlanif10] ip binding vpn-instance vpna
[PE1-Vlanif10] ip address 192.168.1.1 24
[PE1-Vlanif10] quit
```

配置 PE2。

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] route-distinguisher 200:1
[PE2-vpn-instance-vpna-af-ipv4] vpn-target 222:1 both
[PE2-vpn-instance-vpna-af-ipv4] quit
[PE2-vpn-instance-vpna] quit
[PE2] interface vlanif 10
[PE2-Vlanif10] ip binding vpn-instance vpna
[PE2-Vlanif10] ip address 192.168.2.1 24
[PE2-Vlanif10] quit
```

按图 1 配置各 CE1 和 CE2 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] vlan batch 10
[CE1] interface 10GE 1/0/1
```

```

[CE1-10GE1/0/1] port link-type trunk
[CE1-10GE1/0/1] port trunk allow-pass vlan 10
[CE1-10GE1/0/1] quit
[CE1] interface vlanif 10
[CE1-Vlanif10] ip address 192.168.1.2 24
[CE1-Vlanif10] quit
<HUAWEI> system-view
[HUAWEI] sysname CE2
[CE2] vlan batch 10
[CE2] interface 10GE 1/0/1
[CE2-10GE1/0/1] port link-type trunk
[CE2-10GE1/0/1] port trunk allow-pass vlan 10
[CE2-10GE1/0/1] quit
[CE2] interface vlanif 10
[CE2-Vlanif10] ip address 192.168.2.2 24
[CE2-Vlanif10] quit

```

配置完成后，在 PE 设备上执行 **display ip vpn-instance verbose** 命令可以看到 VPN 实例的配置情况。各 PE 能 ping 通自己接入的 CE。

说明

当 PE 上有多个接口绑定了同一个 VPN 时，则使用 **ping -vpn-instance** 命令 ping 对端 PE 接入的 CE 时，要指定源 IP 地址，即要指定 **ping -vpn-instance vpn-instance-name -a source-ip-address dest-ip-address** 命令中的参数 **-a source-ip-address**，否则可能 ping 不通。

4. 配置路由策略

配置 PE1。

```

[PE1] ip ip-prefix ipPrefix1 index 10 permit 192.168.1.0 24 greater-equal 24 less-equal 32
[PE1] route-policy vpnroute permit node 1
[PE1-route-policy] if-match ip-prefix ipPrefix1
[PE1-route-policy] apply extcommunity rt 222:1
[PE1-route-policy] quit
[PE1] ip vpn-instance vpna
[PE1-vpn-instance-vpna] export route-policy vpnroute
[PE1-vpn-instance-vpna] quit

```

配置 PE2。

```

[PE2] ip ip-prefix ipPrefix1 index 10 permit 192.168.2.0 24 greater-equal 24 less-equal 32
[PE2] route-policy vpnroute permit node 1
[PE2-route-policy] if-match ip-prefix ipPrefix1
[PE2-route-policy] apply extcommunity rt 111:1
[PE2-route-policy] quit
[PE2] ip vpn-instance vpna
[PE2-vpn-instance-vpna] export route-policy vpnroute

```

```
[PE2-vpn-instance-vpna] quit
```

5. 在 PE 与 CE 之间建立 EBGP 对等体关系，引入 VPN 路由

配置 CE1。CE2 的配置与 CE1 类似，此处不作赘述。

```
[CE1] bgp 65410
[CE1-bgp] peer 192.168.1.1 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] quit
```

配置 PE1。PE2 的配置与 PE1 类似，此处不作赘述。

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] peer 192.168.1.2 as-number 65410
[PE1-bgp-vpna] import-route direct
[PE1-bgp-vpna] quit
[PE1-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp vpnv4 vpn-instance vpna peer** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，显示结果中 State 项为 “Established”。

6. 在 PE 之间建立 MP-IBGP 对等体关系

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 2.2.2.2 as-number 100
[PE1-bgp] peer 2.2.2.2 connect-interface loopback 1
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] peer 2.2.2.2 enable
[PE1-bgp-af-vpnv4] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.1 as-number 100
[PE2-bgp] peer 1.1.1.1 connect-interface loopback 1
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpnv4] peer 1.1.1.1 enable
[PE2-bgp-af-vpnv4] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp peer** 或 **display bgp vpnv4 all peer** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

检查配置结果

在 PE 上执行 **ping -vpn-instance** 命令，可以 Ping 通对端 PE 接入的 Site。

以 PE1 的显示为例：

[PE1] ping -vpn-instance vpna 192.168.2.2

PING 192.168.2.2: 56 data bytes, press CTRL_C to break

Reply from 192.168.2.2: bytes=56 Sequence=1 ttl=254 time=6 ms

Reply from 192.168.2.2: bytes=56 Sequence=2 ttl=254 time=5 ms

Reply from 192.168.2.2: bytes=56 Sequence=3 ttl=254 time=7 ms

Reply from 192.168.2.2: bytes=56 Sequence=4 ttl=254 time=6 ms

Reply from 192.168.2.2: bytes=56 Sequence=5 ttl=254 time=5 ms

--- 192.168.2.2 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 5/5/7 ms

配置脚本

PE1

```
#
sysname PE1
#
vlan batch 10 100
#
ip vpn-instance vpna
  ipv4-family
    route-distinguisher 100:1
    export route-policy vpnroute
    vpn-target 111:1 export-extcommunity
    vpn-target 111:1 import-extcommunity
#
mpls lsr-id 1.1.1.1
mpls
#
mpls ldp
#
interface Vlanif10
  ip binding vpn-instance vpna
  ip address 192.168.1.1 255.255.255.0
#
interface Vlanif100
  ip address 10.1.1.1 255.255.255.0
  mpls
  mpls ldp
```

```
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface 10GE1/0/7
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface LoopBack1
 ip address 1.1.1.1 255.255.255.255
#
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack1
#
ipv4-family unicast
 undo synchronization
 peer 2.2.2.2 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 2.2.2.2 enable
#
ipv4-family vpn-instance vpna
 import-route direct
 peer 192.168.1.2 as-number 65410
#
ospf 1
 area 0.0.0.0
 network 1.1.1.1 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
route-policy vpnroute permit node 1
 if-match ip-prefix ipPrefix1
 apply extcommunity rt 222:1
#
ip ip-prefix ipPrefix1 index 10 permit 192.168.1.0 24 greater-equal 24 less-equal 32
#
return
```

PE2 的配置文件

```
#
```



```
sysname PE2
#
vlan batch 10 100
#
ip vpn-instance vpna
  ipv4-family
    route-distinguisher 200:1
    export route-policy vpnroute
    vpn-target 222:1 export-extcommunity
    vpn-target 222:1 import-extcommunity
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface Vlanif10
  ip binding vpn-instance vpna
  ip address 192.168.2.1 255.255.255.0
#
interface Vlanif100
  ip address 10.1.1.2 255.255.255.0
  mpls
  mpls ldp
#
interface 10GE1/0/1
  port link-type trunk
  port trunk allow-pass vlan 10
#
interface 10GE1/0/7
  port link-type trunk
  port trunk allow-pass vlan 100
#
interface LoopBack1
  ip address 2.2.2.2 255.255.255.255
#
bgp 100
  peer 1.1.1.1 as-number 100
  peer 1.1.1.1 connect-interface LoopBack1
#
  ipv4-family unicast
    undo synchronization
    peer 1.1.1.1 enable
```

```
#
ipv4-family vpnv4
 policy vpn-target
 peer 1.1.1.1 enable
#
ipv4-family vpn-instance vpna
 import-route direct
 peer 192.168.2.2 as-number 65420
#
ospf 1
 area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
route-policy vpnroute permit node 1
 if-match ip-prefix ipPrefix1
 apply extcommunity rt 111:1
#
ip ip-prefix ipPrefix1 index 10 permit 192.168.2.0 24 greater-equal 24 less-equal 32
#
return
```

PE2

```
#
sysname PE2
#
vlan batch 10 100
#
ip vpn-instance vpna
 ipv4-family
 route-distinguisher 200:1
 export route-policy vpnroute
 vpn-target 222:1 export-extcommunity
 vpn-target 222:1 import-extcommunity
#
mpls lsr-id 2.2.2.2
mpls
#
mpls ldp
#
interface Vlanif10
 ip binding vpn-instance vpna
 ip address 192.168.2.1 255.255.255.0
```

```
#
interface Vlanif100
 ip address 10.1.1.2 255.255.255.0
 mpls
 mpls ldp
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
#
interface 10GE1/0/7
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface LoopBack1
 ip address 2.2.2.2 255.255.255.255
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack1
#
ipv4-family unicast
 undo synchronization
 peer 1.1.1.1 enable
#
ipv4-family vpnv4
 policy vpn-target
 peer 1.1.1.1 enable
#
ipv4-family vpn-instance vpna
 import-route direct
 peer 192.168.2.2 as-number 65420
#
ospf 1
 area 0.0.0.0
 network 2.2.2.2 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
route-policy vpnroute permit node 1
 if-match ip-prefix ipPrefix1
 apply extcommunity rt 111:1
#
ip ip-prefix ipPrefix1 index 10 permit 192.168.2.0 24 greater-equal 24 less-equal 32
```

```
#  
return
```

CE1

```
#  
sysname CE1  
#  
vlan batch 10  
#  
interface Vlanif10  
 ip address 192.168.1.2 255.255.255.0  
#  
interface 10GE1/0/1  
 port link-type trunk  
 port trunk allow-pass vlan 10  
#  
bgp 65410  
 peer 192.168.1.1 as-number 100  
#  
ipv4-family unicast  
 undo synchronization  
 import-route direct  
 peer 192.168.1.1 enable  
#  
return
```

CE2

```
#  
sysname CE2  
#  
vlan batch 10  
#  
interface Vlanif10  
 ip address 192.168.2.2 255.255.255.0  
#  
interface 10GE1/0/1  
 port link-type trunk  
 port trunk allow-pass vlan 10  
#  
bgp 65420  
 peer 192.168.2.1 as-number 100  
#  
ipv4-family unicast
```

```
undo synchronization
import-route direct
peer 192.168.2.1 enable
#
return
```

1.1.5.9.2 IPv6 L3VPN

举例：配置基本 IPv6 L3VPN over MPLS 场景

举例：配置 IPv6 L3VPN over MPLS Hub and Spoke (IPv6) 场景

1.1.5.9.2.1 举例：配置基本 IPv6 L3VPN over MPLS 场景

组网需求

不同用户站点希望通过公网进行 IPv6 的数据通信，而又不希望公网感知到站点内部的路由信息，此时可以配置 IPv6 L3VPN。此外，IPv6 L3VPN 还可以隔离不同 VPN 之间的通信，使得属于同一 VPN 的站点可以互访，不同 VPN 的站点不能互访。

如图 1 所示，CE1 和 CE3 属于 vpna，CE2 和 CE4 属于 vpnb。希望通过配置 IPv6 L3VPN，使得 vpna、vpnb 的内部站点可以通过 MPLS 骨干网互相访问，而 vpna 的站点与 vpnb 的站点之间不能互访。同时希望 PE 与 CE 之间采用不同的方法来交换路由，具体为：

PE1 和 CE1、PE2 和 CE4 采用 BGP4+

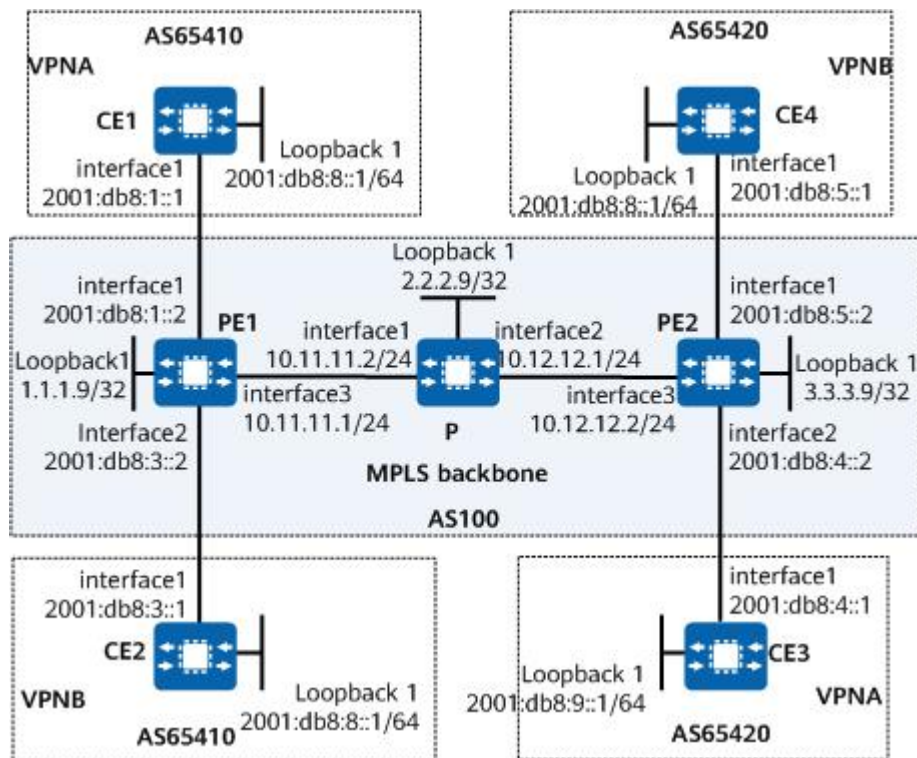
PE1 和 CE2 采用 IPv6 静态路由

PE2 和 CE3 采用 OSPFv3

图 1 配置基本 IPv6 L3VPN 组网图

说明

本例中 interface1，interface2 和 interface3 分别代表 Vlanif100，Vlanif200，Vlanif300。



配置思路

采用如下的思路配置基本 IPv6 L3VPN:

1. 在 IPv4 骨干网上配置 IGP 协议，实现 PE 之间互通。
2. 在各 PE 和 P 设备上配置 MPLS 和 MPLS LDP，建立 PE 之间的 LDP LSP。
3. 在 PE1 和 PE2 上配置 MP-IBGP，即 PE 间用 BGP 来交换 IPv6 VPN 路由。
4. 在 PE1 和 PE2 上创建支持 IPv6 地址族的 VPN 实例，并将 PE 连接 CE 的接口与 VPN 实例绑定。
5. 在 PE 与 CE 之间配置 IPv6 路由协议，使 PE 和 CE 能交换 IPv6 路由。

数据准备

为完成此配置例，需准备如下的数据:

各 PE、CE 所在的 AS 号

VPN 实例名称

VPN 实例 IPv6 地址族的属性信息，如 RD、VPN Target

操作步骤

1. 配置各设备上接口的 IP 地址或 IPv6 地址。

在 CE1 上配置接口的 IPv6 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
```

```
[CE1] vlan batch 100
[CE1] interface 10GE 1/0/1
[CE1-10GE1/0/1] port link-type trunk
[CE1-10GE1/0/1] port trunk allow-pass vlan 100
[CE1-10GE1/0/1] quit
[CE1] interface Vlanif 100
[CE1-Vlanif100] ipv6 enable
[CE1-Vlanif100] ipv6 address 2001:db8:1::1 64
[CE1-Vlanif100] quit
```

CE2 ~ CE4、P、PE1 和 PE2 的配置与 CE1 类似，具体配置请参见后面的配置文件。

2. 配置 IPv4 骨干网的 IGP 协议，实现 PE 之间互通，本例 IGP 以 IS-IS 为例。

配置 PE1。

```
[PE1] isis 1
[PE1-isis-1] network-entity 10.1111.1111.1111.00
[PE1-isis-1] quit
[PE1] interface Vlanif 300
[PE1-Vlanif300] isis enable 1
[PE1-Vlanif300] quit
[PE1] interface loopback 1
[PE1-LoopBack1] isis enable 1
[PE1-LoopBack1] quit
```

P、PE2 的配置与 PE1 类似，具体配置请参见后面的配置文件。

配置完成后，PE1、P 和 PE2 之间应能学习到相互的路由，包括接口 Loopback 的路由，可通过 **display ip routing-table** 命令查看。以 PE1 的显示为例：

```
[PE1] display ip routing-table
Route Flags: R – relay, D – download to fib, T – to vpn-instance, B – black hole route
-----
Routing Table: _public_
    Destinations : 11    Routes : 11

Destination/Mask  Proto  Pre  Cost   Flags NextHop     Interface
-----
1.1.1.9/32        Direct 0   0       D 127.0.0.1   InLoopBack0
2.2.2.9/32        ISIS-L2 15  10       D 10.11.11.2  Vlanif300
3.3.3.9/32        ISIS-L2 15  20       D 10.11.11.2  Vlanif300
127.0.0.0/8       Direct 0   0       D 127.0.0.1   InLoopBack0
127.0.0.1/32      Direct 0   0       D 127.0.0.1   InLoopBack0
127.255.255.255/32 Direct 0   0       D 127.0.0.1   InLoopBack0
10.11.11.0/24     Direct 0   0       D 10.11.11.1  Vlanif300
10.11.11.1/32     Direct 0   0       D 127.0.0.1   Vlanif300
10.11.11.255/32   Direct 0   0       D 127.0.0.1   Vlanif300
```

```
10.12.12.0/24    ISIS-L2 15 20    D 10.11.11.2    Vlanif300
255.255.255.255/32 Direct 0 0      D 127.0.0.1    InLoopBack0
```

3. IPv4 骨干网各设备及其接口使能 MPLS、MPLS LDP，创建 PE1 和 PE2 之间的 LDP LSP
使能 PE1 的 MPLS 和 MPLS LDP。

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface Vlanif 300
[PE1-Vlanif300] mpls
[PE1-Vlanif300] mpls ldp
[PE1-Vlanif300] quit
```

P、PE2 的配置与 PE1 类似，具体配置请参见后面的配置文件。
上述配置完成后，PE1 与 PE2 之间应能建立 LDP LSP。执行 **display mpls ldp lsp** 命令，可以看到 LDP LSP 的建立情况。以 PE1 的显示为例：

```
[PE1] display mpls ldp lsp
LDP LSP Information
-----
Flag after Out IF: (I) – RLFA Iterated LSP, (I*) – Normal and RLFA Iterated LSP
-----
DestAddress/Mask  In/OutLabel  UpstreamPeer  NextHop      OutInterface
-----
1.1.1.9/32        3/NULL       2.2.2.9       127.0.0.1    InLoop0
*1.1.1.9/32       Liberal/1024          DS/2.2.2.9
2.2.2.9/32        NULL/3       -             10.11.11.2   Vlanif300
2.2.2.9/32        1024/3       2.2.2.9       10.11.11.2   Vlanif300
3.3.3.9/32        NULL/1025    -             10.11.11.2   Vlanif300
3.3.3.9/32        1025/1025    2.2.2.9       10.11.11.2   Vlanif300
-----
TOTAL: 5 Normal LSP(s) Found.
TOTAL: 1 Liberal LSP(s) Found.
TOTAL: 0 Frr LSP(s) Found.
An asterisk (*) before an LSP means the LSP is not established
An asterisk (*) before a Label means the USCB or DSCB is stale
An asterisk (*) before an UpstreamPeer means the session is stale
An asterisk (*) before a DS means the session is stale
An asterisk (*) before a NextHop means the LSP is FRR LSP
```

4. PE 上创建支持 IPv6 地址族的 VPN 实例，并将 PE 连接 CE 的接口与 VPN 实例绑定。
PE1 上配置支持 IPv6 地址族的 VPN 实例 vpna。

```
[PE1] ip vpn-instance vpna
```



```
[PE1-vpn-instance-vpna] ipv6-family
[PE1-vpn-instance-vpna-af-ipv6] route-distinguisher 100:1
[PE1-vpn-instance-vpna-af-ipv6] vpn-target 22:22 export-extcommunity
[PE1-vpn-instance-vpna-af-ipv6] vpn-target 33:33 import-extcommunity
[PE1-vpn-instance-vpna-af-ipv6] quit
[PE1-vpn-instance-vpna] quit
```

将 PE1 上直连 CE1 的接口与 vpna 相绑定。

```
[PE1] interface Vlanif 100
[PE1-Vlanif100] ip binding vpn-instance vpna
[PE1-Vlanif100] ipv6 enable
[PE1-Vlanif100] ipv6 address 2001:db8:1::2 64
[PE1-Vlanif100] quit
```

PE1 上配置支持 IPv6 地址族的 VPN 实例 vpnb。

```
[PE1] ip vpn-instance vpnb
[PE1-vpn-instance-vpnb] ipv6-family
[PE1-vpn-instance-vpnb-af-ipv6] route-distinguisher 100:3
[PE1-vpn-instance-vpnb-af-ipv6] vpn-target 44:44 export-extcommunity
[PE1-vpn-instance-vpnb-af-ipv6] vpn-target 55:55 import-extcommunity
[PE1-vpn-instance-vpnb-af-ipv6] quit
[PE1-vpn-instance-vpnb] quit
```

将 PE1 上直连 CE2 的接口与 vpnb 相绑定。

```
[PE1] interface Vlanif 200
[PE1-Vlanif200] ip binding vpn-instance vpnb
[PE1-Vlanif200] ipv6 enable
[PE1-Vlanif200] ipv6 address 2001:db8:3::2 64
[PE1-Vlanif200] quit
```

PE2 的配置与 PE1 类似，具体配置请参见后面的配置文件。

上述配置完成后，在各 PE 上可通过 **display ip vpn-instance verbose** 命令查看 VPN 实例的配置信息；各 PE 能 ping 通自己接入的 CE。以 PE1 的显示为例：

```
[PE1] display ip vpn-instance verbose
Total VPN-Instances configured : 2
Total IPv4 VPN-Instances configured : 0
Total IPv6 VPN-Instances configured : 2

VPN-Instance Name and ID : vpna, 1
Interfaces : Vlanif100
Address family ipv6
Create date : 2010/07/20 12:31:47
Up time : 0 days, 04 hours, 37 minutes and 05 seconds
Vrf Status : UP
Route Distinguisher : 100:1
```

```

Export VPN Targets : 22:22
Import VPN Targets : 33:33
Label Policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe

VPN-Instance Name and ID : vpnb, 2
Interfaces : Vlanif200
Address family ipv6
Create date : 2010/07/20 14:41:46
Up time : 0 days, 02 hours, 27 minutes and 06 seconds
Vrf Status : UP
Route Distinguisher : 100:3
Export VPN Targets : 44:44
Import VPN Targets : 55:55
Label Policy : label per route
The diffserv-mode Information is : uniform
The ttl-mode Information is : pipe

```

[PE1] **ping ipv6 vpn-instance vpna 2001:db8:1::1**

```

PING 2001:db8:1::1 : 56 data bytes, press CTRL_C to break

```

```

  Reply from 2001:db8:1::1

```

```

    bytes=56 Sequence=1 hop limit=64 time = 20 ms

```

```

  Reply from 2001:db8:1::1

```

```

    bytes=56 Sequence=2 hop limit=64 time = 30 ms

```

```

  Reply from 2001:db8:1::1

```

```

    bytes=56 Sequence=3 hop limit=64 time = 30 ms

```

```

  Reply from 2001:db8:1::1

```

```

    bytes=56 Sequence=4 hop limit=64 time = 1 ms

```

```

  Reply from 2001:db8:1::1

```

```

    bytes=56 Sequence=5 hop limit=64 time = 1 ms

```

```

--- 2001:db8:1::1 ping statistics ---

```

```

  5 packet(s) transmitted

```

```

  5 packet(s) received

```

```

  0.00% packet loss

```

```

 round-trip min/avg/max = 1/16/30 ms

```

5. PE 之间建立 VPNv6 对等体关系。

配置 PE1。

```

[PE1] bgp 100
[PE1-bgp] peer 3.3.3.9 as-number 100
[PE1-bgp] peer 3.3.3.9 connect-interface loopback 1
[PE1-bgp] ipv6-family vpnv6

```

```
[PE1-bgp-af-vpnv6] peer 3.3.3.9 enable
[PE1-bgp-af-vpnv6] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 1.1.1.9 as-number 100
[PE2-bgp] peer 1.1.1.9 connect-interface loopback 1
[PE2-bgp] ipv6-family vpnv6
[PE2-bgp-af-vpnv6] peer 1.1.1.9 enable
[PE2-bgp-af-vpnv6] quit
[PE2-bgp] quit
```

以上配置完成后，在 PE 上可通过 **display bgp vpnv6 all peer** 查看 VPNv6 对等体的建立情况。以 PE1 的显示为例：

```
[PE1] display bgp vpnv6 all peer
BGP local router ID : 1.1.1.9
Local AS number : 100
Total number of peers : 1          Peers in established state : 1

Peer      V      AS  MsgRcvd  MsgSent  OutQ  Up/Down   State   PrefRcv
-----
3.3.3.9   4      100    4        3    0 00:01:50 Established  0
```

由上可以看到 VPNv6 对等体的状态为 **Established**，说明 PE1 和 PE2 的 VPNv6 对等体关系已建立。

6. 在 PE1 和 CE1 上配置 BGP4+

在 PE1 上配置 EBGP。

```
[PE1] bgp 100
[PE1-bgp] ipv6-family vpn-instance vpna
[PE1-bgp6-vpna] peer 2001:db8:1::1 as-number 65410
[PE1-bgp6-vpna] quit
[PE1-bgp] quit
```

在 CE1 上配置 EBGP。

```
[CE1] bgp 65410
[CE1-bgp] router-id 10.10.10.10
[CE1-bgp] peer 2001:db8:1::2 as-number 100
[CE1-bgp] ipv6-family unicast
[CE1-bgp-af-ipv6] network 2001:db8:8:: 64
[CE1-bgp-af-ipv6] peer 2001:db8:1::2 enable
[CE1-bgp-af-ipv6] import-route direct
[CE1-bgp-af-ipv6] quit
[CE1-bgp] quit
```

PE2-CE4 之间的配置与 PE1-CE1 之间类似，具体配置信息请参见后面的配置文件。

以上配置完成后，可在 PE 上执行命令 **display bgp vpnv6 vpn-instance *vpn-instance-name* peer** 查看对等体的建立情况。以 PE1 的显示信息为例：

```
[PE1] display bgp vpnv6 vpn-instance vpna peer
BGP local router ID : 1.1.1.9
Local AS number : 100
Total number of peers : 1          Peers in established state : 1

Peer      V      AS  MsgRcvd  MsgSent  OutQ  Up/Down    State PrefRcv
-----
2001:DB8:1::1  4    65410    3      3    0 00:00:37 Established    1
```

7. 在 PE1 和 CE2 上配置静态路由。

在 PE1 上为 VPN 实例 vpnb 配置 IPv6 静态路由，并将该路由引入到 BGP-VPN 实例 IPv6 地址族路由表中。

```
[PE1] ipv6 route-static vpn-instance vpnb 2001:db8:8:: 64 2001:db8:3::1
[PE1] bgp 100
[PE1-bgp] ipv6-family vpn-instance vpnb
[PE1-bgp6-vpnb] import-route static
[PE1-bgp6-vpnb] quit
[PE1-bgp] quit
```

在 CE2 配置 IPv6 缺省路由。

```
[CE2] ipv6 route-static :: 0 2001:db8:3::2
```

8. 在 PE2-CE3 之间配置 OSPFv3。

在 PE2 上配置 OSPFv3。

```
[PE2] ospfv3 1 vpn-instance vpna
[PE2-ospfv3-1] router-id 10.10.11.11
[PE2-ospfv3-1] area 0.0.0.0
[PE2-ospfv3-1-area 0.0.0.0] quit
[PE2-ospfv3-1] import-route bgp
[PE2-ospfv3-1] quit
[PE2] interface Vlanif 200
[PE2-Vlanif200] ospfv3 1 area 0
[PE2-Vlanif200] quit
```

在 PE2 上把 OSPFv3 引入 BGP。

```
[PE2] bgp 100
[PE2-bgp] ipv6-family vpn-instance vpna
[PE2-bgp6-vpna] import-route ospfv3 1
[PE2-bgp6-vpna] quit
[PE2-bgp] quit
```

在 CE3 上配置 OSPFv3。

```
[CE3] ospfv3 1
[CE3-ospfv3-1] router-id 22.22.22.22
[CE3-ospfv3-1] area 0.0.0.0
[CE3-ospfv3-1-area 0.0.0.0] quit
[CE3-ospfv3-1] quit
[CE3] interface Vlanif100
[CE3-Vlanif100] ospfv3 1 area 0
[CE3-Vlanif100] quit
[CE3] interface LoopBack 1
[CE3-LoopBack1] ospfv3 1 area 0
[CE3-LoopBack1] quit
```

检查配置结果

以上配置完成后，CE1 与 CE3 之间，CE2 与 CE4 之间能够带源 Ping 通。以 CE1 的显示为例：

```
[CE1] ping ipv6 -a 2001:db8:8::1 2001:db8:9::1
PING 2001:db8:9::1 : 56 data bytes, press CTRL_C to break
  Reply from 2001:db8:9::1:
    bytes=56 Sequence=1 hop limit=62 time = 170 ms
  Reply from 2001:db8:9::1:
    bytes=56 Sequence=2 hop limit=62 time = 140 ms
  Reply from 2001:db8:9::1:
    bytes=56 Sequence=3 hop limit=62 time = 150 ms
  Reply from 2001:db8:9::1:
    bytes=56 Sequence=4 hop limit=62 time = 140 ms
  Reply from 2001:db8:9::1:
    bytes=56 Sequence=5 hop limit=62 time = 170 ms

--- 2001:db8:9::1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
 round-trip min/avg/max = 140/154/170 ms
```

由于 CE4 上也同样存在 2001:db8:9::1/64 地址，判断数据的转发路径和预期一致，只需在 PE2 上用 **display ipv6 statistics interface** 检查接口下接收/发送 ICMPv6 报文的数量变化。

CE1 上运行命令 **ping ipv6 -a 2001:db8:8::1 -c 100 2001:db8:9::1**，发送 100 个带有源地址的 IPv6 数据包，同时 PE2 上不断轮换执行命令 **display ipv6 statistics interface Vlanif100** 或者 **display ipv6 statistics interface Vlanif200**，查看各接口下接收/发送 ICMPv6 报文的数量变化。由于 Vlanif200 接口下数据一直在变化，可以知道 IPv6 数据转发给了属于同一 VPN 的 CE3，这也说明了不同的 VPN 之间是隔离的。

配置脚本

PE1

```
#
sysname PE1
#
vlan batch 100 200 300
#
ip vpn-instance vpna
ipv6-family
 route-distinguisher 100:1
 vpn-target 22:22 export-extcommunity
 vpn-target 33:33 import-extcommunity
#
ip vpn-instance vpnb
ipv6-family
 route-distinguisher 100:3
 vpn-target 44:44 export-extcommunity
 vpn-target 55:55 import-extcommunity
#
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
#
isis 1
 network-entity 10.1111.1111.1111.00
#
interface Vlanif100
 ip binding vpn-instance vpna
 ipv6 enable
 ipv6 address 2001:db8:1::2/64
#
interface Vlanif200
 ip binding vpn-instance vpnb
 ipv6 enable
 ipv6 address 2001:db8:3::2/64
#
interface Vlanif300
 ip address 10.11.11.1 255.255.255.0
 isis enable 1
```

```
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 300
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
isis enable 1
#
bgp 100
peer 3.3.3.9 as-number 100
peer 3.3.3.9 connect-interface LoopBack1
#
ipv4-family unicast
peer 3.3.3.9 enable
#
ipv6-family vpnv6
policy vpn-target
peer 3.3.3.9 enable
#
ipv6-family vpn-instance vpna
peer 2001:db8:1::1 as-number 65410
#
ipv6-family vpn-instance vpnb
import-route static
#
ipv6 route-static vpn-instance vpnb 2001:db8:8:: 64 2001:db8:3::1
#
return
```

P

```
#
sysname P
```

```
#
vlan batch 100 200

#
mpls lsr-id 2.2.2.9
#
mpls
#
mpls ldp
#
isis 1
 network-entity 20.2222.2222.2222.00
#
interface Vlanif100
 ip address 10.11.11.2 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface Vlanif200
 ip address 10.12.12.1 255.255.255.0
 isis enable 1
 mpls
 mpls ldp
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
 isis enable 1
#
return
```

PE2

```
#
sysname PE2
#
vlan batch 100 200 300
```



```
#
ip vpn-instance vpna
ipv6-family
route-distinguisher 100:2
vpn-target 33:33 export-extcommunity
vpn-target 22:22 import-extcommunity
#
ip vpn-instance vpnb
ipv6-family
route-distinguisher 100:4
vpn-target 55:55 export-extcommunity
vpn-target 44:44 import-extcommunity
#
mpls lsr-id 3.3.3.9
#
mpls
#
mpls ldp
#
isis 1
network-entity 30.3333.3333.3333.00
#
ospfv3 1 vpn-instance vpna
router-id 10.10.11.11
import-route bgp
area 0.0.0.0
#
interface Vlanif100
ip binding vpn-instance vpnb
ipv6 enable
ipv6 address 2001:db8:5::2/64
#
interface Vlanif200
ip binding vpn-instance vpna
ipv6 enable
ipv6 address 2001:db8:4::2/64
ospfv3 1 area 0.0.0.0
#
interface Vlanif300
ip address 10.12.12.2 255.255.255.0
isis enable 1
mpls
mpls ldp
```

```
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 300
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
 isis enable 1
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
#
ipv4-family unicast
 peer 1.1.1.9 enable
#
ipv6-family vpnv6
 policy vpn-target
 peer 1.1.1.9 enable
#
ipv6-family vpn-instance vpna
 import-route ospfv3 1
#
ipv6-family vpn-instance vpnb
 peer 2001:db8:5::1 as-number 65420
#
return
```

CE1

```
#
sysname CE1
#
vlan batch 100
#
interface Vlanif100
```

```
ipv6 enable
ipv6 address 2001:db8:1::1/64
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface LoopBack1
ipv6 enable
ipv6 address 2001:db8:8::1/64
#
bgp 65410
router-id 10.10.10.10
peer 2001:db8:1::2 as-number 100
#
ipv4-family unicast
#
ipv6-family unicast
network 2001:db8:8:: 64
import-route direct
peer 2001:db8:1::2 enable
#
return
```

CE2

```
#
sysname CE2
#
vlan batch 100
#
interface Vlanif100
ipv6 enable
ipv6 address 2001:db8:3::1/64
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface LoopBack1
ipv6 enable
ipv6 address 2001:db8:8::1/64
#
ipv6 route-static :: 0 2001:db8:3::2
```

```
#  
return
```

CE3

```
#  
sysname CE3  
  
#  
vlan batch 100  
  
#  
ospfv3 1  
router-id 22.22.22.22  
area 0.0.0.0  
  
#  
interface Vlanif100  
ipv6 enable  
ipv6 address 2001:db8:4::1/64  
ospfv3 1 area 0.0.0.0  
  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 100  
  
#  
interface LoopBack1  
ipv6 enable  
ipv6 address 2001:db8:9::1/64  
ospfv3 1 area 0.0.0.0  
  
#  
return
```

CE4

```
#  
sysname CE4  
  
#  
vlan batch 100  
  
#  
interface Vlanif100  
ipv6 enable  
ipv6 address 2001:db8:5::1/64  
  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 100  
  
#
```

```
interface LoopBack1
  ipv6 enable
  ipv6 address 2001:db8:9::1/64
#
bgp 65420
  router-id 33.33.33.33
  peer 2001:db8:5::2 as-number 100
#
  ipv4-family unicast
#
  ipv6-family unicast
  import-route direct
  peer 2001:db8:5::2 enable
#
return
```

1.1.5.9.2.2 举例：配置 IPv6 L3VPN over MPLS Hub and Spoke（IPv6）场景

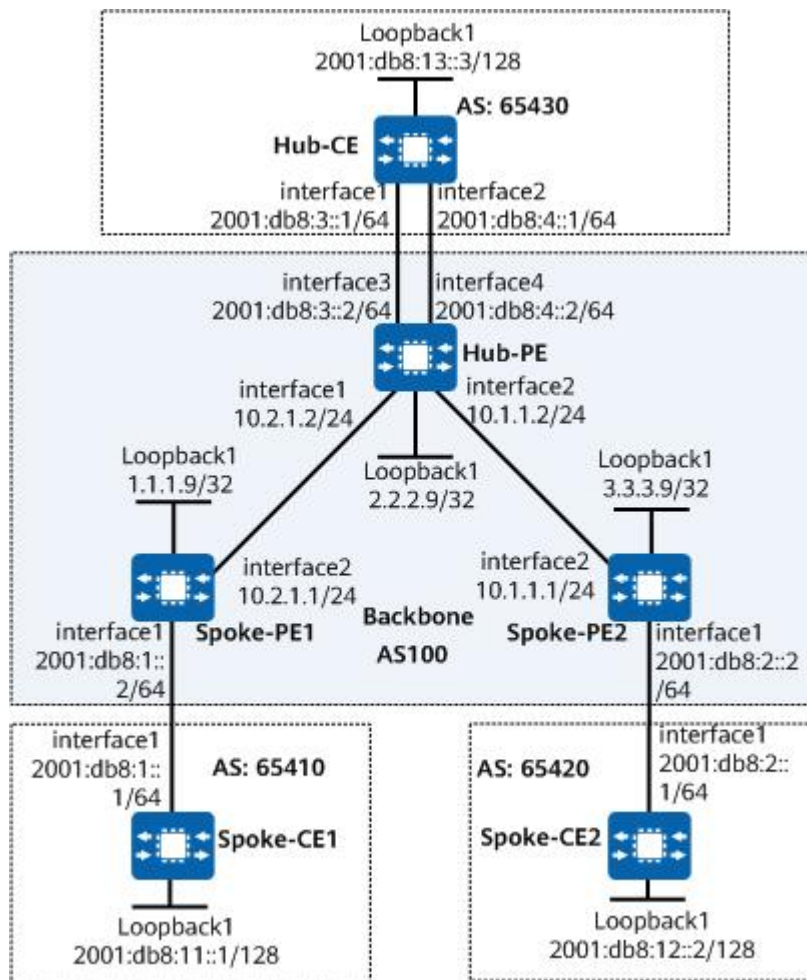
组网需求

如[图 1](#)所示，Spoke-CE 之间的通信通过中心站点 Hub-CE 控制，即 Spoke-CE 之间的流量经过 Hub-CE 转发，而不是只经过 Hub-PE 转发。

图 1 Hub and Spoke 组网图

说明

本例中 interface1，interface2、interface3、interface4 分别代表 Vlanif100，Vlanif200，Vlanif300，Vlanif400。



配置注意事项

在配置过程中，需注意以下事项：

Spoke-PE 上配置的 Import Target 和 Export Target 应不同。

Hub-PE 上创建两个 VPN 实例（vpn_in，vpn_out）。其中，vpn_in 接收的 VPN-target 团体属性为两个 Spoke-PE 发布的 VPN-target 团体属性值；vpn_out 发布的 VPN-target 团体属性值与接收的 VPN-target 团体属性不同，且为两个 Spoke-PE 接收的 VPN-target 团体属性值。

Hub-PE 上配置允许接收 AS_Path 中 AS 号重复 1 次的路由。

配置思路

采用如下思路配置 Hub and Spoke：

1. Hub-PE 与 Spoke-PE 建立 MP-IBGP 对等体关系。（Spoke-PE 之间不建立 MP-IBGP 对等体关系，不交换 VPN 路由信息）
2. PE 上创建 VPN 实例，并配置 VPN-Target。
3. CE 和 PE 之间配置 EBGP 连接。

操作步骤

1. 在骨干网上配置 IGP 协议，实现骨干网 Hub-PE 和 Spoke-PE 的互通。
本例中采用 OSPF，具体配置过程请参见后面的配置文件。
配置完成后，Hub-PE 和 Spoke-PE 之间应能建立 OSPF 邻居关系，执行 **display ospf peer** 命令可以看到邻居状态为 Full。执行 **display ip routing-table** 命令可以看到 Hub-PE 和 Spoke-PE 之间学习到对方的 Loopback 路由。
2. 在骨干网上配置 MPLS 基本能力和 MPLS LDP，建立 LDP LSP。
具体配置过程请参见后面的配置文件。
配置完成后，Hub-PE 和 Spoke-PE 之间应该建立起 LDP 对等体关系，在各设备上执行 **display mpls ldp session** 命令可以看到显示结果中 Session State 项为“Operational”。
3. 在各 PE 设备上配置使能 IPv6 地址族的 VPN 实例，将 CE 接入 PE。

说明

Hub-PE 上其中一个 VPN 的 Import-Target 列表必须包含所有 Spoke-PE 的 Export-Target 属性。

Hub-PE 上另一个 VPN 的 Export-Target 列表必须包含所有 Spoke-PE 的 Import-Target 属性。

配置 Spoke-PE1。

```
<Spoke-PE1> system-view
[Spoke-PE1] ip vpn-instance vpna
[Spoke-PE1-vpn-instance-vpna] ipv6-family
[Spoke-PE1-vpn-instance-vpna-af-ipv6] route-distinguisher 100:1
[Spoke-PE1-vpn-instance-vpna-af-ipv6] vpn-target 100:1 export-extcommunity
[Spoke-PE1-vpn-instance-vpna-af-ipv6] vpn-target 200:1 import-extcommunity
[Spoke-PE1-vpn-instance-vpna-af-ipv6] quit
[Spoke-PE1] interface Vlanif100
[Spoke-PE1-Vlanif100] ip binding vpn-instance vpna
[Spoke-PE1-Vlanif100] ipv6 enable
[Spoke-PE1-Vlanif100] ipv6 address 2001:db8:1::2 64
[Spoke-PE1-Vlanif100] quit
```

配置 Spoke-PE2。

```
<Spoke-PE2> system-view
[Spoke-PE2] ip vpn-instance vpna
[Spoke-PE2-vpn-instance-vpna] ipv6-family
[Spoke-PE2-vpn-instance-vpna-af-ipv6] route-distinguisher 100:3
[Spoke-PE2-vpn-instance-vpna-af-ipv6] vpn-target 100:1 export-extcommunity
[Spoke-PE2-vpn-instance-vpna-af-ipv6] vpn-target 200:1 import-extcommunity
[Spoke-PE2-vpn-instance-vpna-af-ipv6] quit
[Spoke-PE2] interface Vlanif100
[Spoke-PE2-Vlanif100] ip binding vpn-instance vpna
[Spoke-PE2-Vlanif100] ipv6 enable
[Spoke-PE2-Vlanif100] ipv6 address 2001:db8:2::2 64
[Spoke-PE2-Vlanif100] quit
```

配置 Hub-PE。

```

<Hub-PE> system-view
[Hub-PE] ip vpn-instance vpn_in
[Hub-PE-vpn-instance-vpn_in] ipv6-family
[Hub-PE-vpn-instance-vpn_in-af-ipv6] route-distinguisher 100:21
[Hub-PE-vpn-instance-vpn_in-af-ipv6] vpn-target 100:1 import-extcommunity
[Hub-PE-vpn-instance-vpn_in-af-ipv6] quit
[Hub-PE-vpn-instance-vpn_in] quit
[Hub-PE] ip vpn-instance vpn_out
[Hub-PE-vpn-instance-vpn_out] ipv6-family
[Hub-PE-vpn-instance-vpn_out-af-ipv6] route-distinguisher 100:22
[Hub-PE-vpn-instance-vpn_out-af-ipv6] vpn-target 200:1 export-extcommunity
[Hub-PE-vpn-instance-vpn_out-af-ipv6] quit
[Hub-PE-vpn-instance-vpn_out] quit
[Hub-PE] interface Vlanif300
[Hub-PE-Vlanif300] ip binding vpn-instance vpn_in
[Hub-PE-Vlanif300] ipv6 enable
[Hub-PE-Vlanif300] ipv6 address 2001:db8:3::2 64
[Hub-PE-Vlanif300] quit
[Hub-PE] interface Vlanif400
[Hub-PE-Vlanif400] ip binding vpn-instance vpn_out
[Hub-PE-Vlanif400] ipv6 enable
[Hub-PE-Vlanif400] ipv6 address 2001:db8:4::2 64
[Hub-PE-Vlanif400] quit

```

按图 1 配置各 CE 的接口 IP 地址，配置过程请参见后面的配置文件。

配置完成后，在 PE 设备上执行 **display ip vpn-instance verbose** 命令可以看到 VPN 实例的配置情况。各 PE 能用 **ping ipv6 vpn-instance *vpn-name* *ipv6-address*** 命令 ping 通自己接入的 CE。

4. 在 PE 与 CE 之间建立 EBGP 对等体关系，引入 VPN 路由。

说明

Hub-PE 上需要配置允许 AS 号重复一次，以接收 Hub-CE 发布的路由。

Spoke-PE 上不需要配置允许 AS 号重复一次，因为设备接收 IBGP 对等体发布的路由时并不检查其中的 AS-PATH 属性。

配置 Spoke-CE1。

```

[Spoke-CE1] interface loopback 1
[Spoke-CE1-Loopback1] ipv6 enable
[Spoke-CE1-Loopback1] ipv6 address 2001:db8:11::1 128
[Spoke-CE1-Loopback1] quit
[Spoke-CE1] bgp 65410
[Spoke-CE1-bgp] ipv6-family unicast
[Spoke-CE1-bgp-af-ipv6] peer 2001:db8:1::2 as-number 100
[Spoke-CE1-bgp-af-ipv6] network 2001:db8:11::1 128

```



```
[Spoke-CE1-bgp-af-ipv6] quit
[Spoke-CE1-bgp] quit
```

配置 Spoke-PE1。

```
[Spoke-PE1] bgp 100
[Spoke-PE1-bgp] ipv6-family vpn-instance vpna
[Spoke-PE1-bgp-6-vpna] peer 2001:db8:1::1 as-number 65410
[Spoke-PE1-bgp-6-vpna] quit
[Spoke-PE1-bgp] quit
```

配置 Spoke-CE2。

```
[Spoke-CE2] interface loopback 1
[Spoke-CE2-Loopback1] ipv6 enable
[Spoke-CE2-Loopback1] ipv6 address 2001:db8:12::2 128
[Spoke-CE2-Loopback1] quit
[Spoke-CE2] bgp 65420
[Spoke-CE2-bgp] ipv6-family unicast
[Spoke-CE2-bgp-af-ipv6] peer 2001:db8:2::2 as-number 100
[Spoke-CE2-bgp-af-ipv6] network 2001:db8:12::2 128
[Spoke-CE2-bgp-af-ipv6] quit
[Spoke-CE2-bgp] quit
```

配置 Spoke-PE2。

```
[Spoke-PE2] bgp 100
[Spoke-PE2-bgp] ipv6-family vpn-instance vpna
[Spoke-PE2-bgp-6-vpna] peer 2001:db8:2::1 as-number 65420
[Spoke-PE2-bgp-6-vpna] quit
[Spoke-PE2-bgp] quit
```

配置 Hub-CE。

```
[Hub-CE] interface loopback 1
[Hub-CE-Loopback1] ipv6 enable
[Hub-CE-Loopback1] ipv6 address 2001:db8:13::3 128
[Hub-CE-Loopback1] quit
[Hub-CE] bgp 65430
[Hub-CE-bgp] ipv6-family unicast
[Hub-CE-bgp-af-ipv6] peer 2001:db8:3::2 as-number 100
[Hub-CE-bgp-af-ipv6] peer 2001:db8:4::2 as-number 100
[Hub-CE-bgp-af-ipv6] network 2001:db8:13::3 128
[Hub-CE-bgp-af-ipv6] quit
[Hub-CE-bgp] quit
```

配置 Hub-PE。

```
[Hub-PE] bgp 100
[Hub-PE-bgp] ipv6-family vpn-instance vpn_in
```

```
[Hub-PE-bgp-6-vpn_in] peer 2001:db8:3::1 as-number 65430
[Hub-PE-bgp-6-vpn_in] quit
[Hub-PE-bgp] ipv6-family vpn-instance vpn_out
[Hub-PE-bgp-6-vpn_out] peer 2001:db8:4::1 as-number 65430
[Hub-PE-bgp-6-vpn_out] peer 2001:db8:4::1 allow-as-loop 1
[Hub-PE-bgp-6-vpn_out] quit
[Hub-PE-bgp] quit
```

配置完成后，在各 PE 设备上执行 **display bgp vpnv6 all peer** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

5. 在 PE 之间建立 MP-IBGP 对等体关系。

配置 Spoke-PE1。

```
[Spoke-PE1] bgp 100
[Spoke-PE1-bgp] peer 2.2.2.9 as-number 100
[Spoke-PE1-bgp] peer 2.2.2.9 connect-interface loopback 1
[Spoke-PE1-bgp] ipv6-family vpnv6
[Spoke-PE1-bgp-af-vpnv6] peer 2.2.2.9 enable
[Spoke-PE1-bgp-af-vpnv6] quit
```

配置 Spoke-PE2。

```
[Spoke-PE2] bgp 100
[Spoke-PE2-bgp] peer 2.2.2.9 as-number 100
[Spoke-PE2-bgp] peer 2.2.2.9 connect-interface loopback 1
[Spoke-PE2-bgp] ipv6-family vpnv6
[Spoke-PE2-bgp-af-vpnv6] peer 2.2.2.9 enable
[Spoke-PE2-bgp-af-vpnv6] quit
```

配置 Hub-PE。

```
[Hub-PE] bgp 100
[Hub-PE-bgp] peer 1.1.1.9 as-number 100
[Hub-PE-bgp] peer 1.1.1.9 connect-interface loopback 1
[Hub-PE-bgp] peer 3.3.3.9 as-number 100
[Hub-PE-bgp] peer 3.3.3.9 connect-interface loopback 1
[Hub-PE-bgp] ipv6-family vpnv6
[Hub-PE-bgp-af-vpnv6] peer 1.1.1.9 enable
[Hub-PE-bgp-af-vpnv6] peer 3.3.3.9 enable
[Hub-PE-bgp-af-vpnv6] quit
```

配置完成后，在各 PE 设备上执行 **display bgp peer** 或 **display bgp vpnv6 all peer** 命令，可以看到 PE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

检查配置结果

完成上述配置后，Spoke-CE 之间可以相互 Ping 通。

以 Spoke-CE1 的显示为例：

```
<Spoke-CE1> ping ipv6 -a 2001:db8:11::1 2001:db8:12::2
PING 2001:db8:12::2 : 56 data bytes, press CTRL_C to break
  Reply from 2001:db8:12::2:
    bytes=56 Sequence=1 hop limit=59 time=7 ms
  Reply from 2001:db8:12::2:
    bytes=56 Sequence=2 hop limit=59 time=3 ms
  Reply from 2001:db8:12::2:
    bytes=56 Sequence=3 hop limit=59 time=3 ms
  Reply from 2001:db8:12::2:
    bytes=56 Sequence=4 hop limit=59 time=3 ms
  Reply from 2001:db8:12::2:
    bytes=56 Sequence=5 hop limit=59 time=3 ms

---2001:db8:12::2 ping statistics---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max=3/3/7 ms
```

在 Spoke-CE 上执行 **display bgp ipv6 routing-table** 命令，可以看到去往对端 Spoke-CE 的 BGP 路由的 AS 路径中存在重复的 AS 号。

以 Spoke-CE1 的显示为例：

```
<Spoke-CE1> display bgp ipv6 routing-table
BGP Local router ID is 1.1.1.1
Status codes: * - valid, > - best, d - damped, x - best external,
              h - history, i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 3
*> Network : 2001:db8:11::1          PrefixLen : 128
    NextHop ::                      LocPrf  :
    MED   : 0                      PrefVal : 0
    Label :
    Path/Ogn : i
*> Network : 2001:db8:12::2          PrefixLen : 128
    NextHop : 2001:db8:1::2          LocPrf  :
    MED   :                          PrefVal : 0
    Label :
    Path/Ogn : 100 65430 100 65420i
*> Network : 2001:db8:13::3          PrefixLen : 128
    NextHop : 2001:db8:1::2          LocPrf  :
```

MED : PrefVal : 0
Label :
Path/Ogn : 100 65430i

配置脚本

Spoke-CE1

```
#
sysname Spoke-CE1
#
vlan batch 100
#
interface Vlanif100
ipv6 enable
ipv6 address 2001:db8:1::1/64
#
interface LoopBack1
ipv6 enable
ipv6 address 2001:db8:11::1/128
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
bgp 65410
router-id 1.1.1.1
peer 2001:db8:1::2 as-number 100
#
ipv6-family unicast
network 2001:db8:11::1 128
peer 2001:db8:1::2 enable
#
return
```

Spoke-PE1

```
#
sysname Spoke-PE1
#
vlan batch 100 200
#
ip vpn-instance vpna
ipv6-family
```

```
route-distinguisher 100:1
vpn-target 100:1 export-extcommunity
vpn-target 200:1 import-extcommunity
#
mpls lsr-id 1.1.1.9
#
mpls
#
mpls ldp
#
interface Vlanif100
ip binding vpn-instance vpna
ipv6 enable
ipv6 address 2001:db8:1::2/64
#
interface Vlanif200
ip address 10.2.1.1 255.255.255.0
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
interface LoopBack1
ip address 1.1.1.9 255.255.255.255
#
bgp 100
peer 2.2.2.9 as-number 100
peer 2.2.2.9 connect-interface LoopBack1
#
ipv4-family unicast
peer 2.2.2.9 enable
#
ipv6-family vpnv6
policy vpn-target
peer 2.2.2.9 enable
#
ipv6-family vpn-instance vpna
```

```
peer 2001:db8:1::1 as-number 65410
#
ospf 1
area 0.0.0.0
network 1.1.1.9 0.0.0.0
network 10.2.1.0 0.0.0.255
#
return
```

Spoke-PE2

```
#
sysname Spoke-PE2
#
vlan batch 100 200
#
ip vpn-instance vpna
ipv6-family
route-distinguisher 100:3
vpn-target 100:1 export-extcommunity
vpn-target 200:1 import-extcommunity
#
mpls lsr-id 3.3.3.9
#
mpls
#
mpls ldp
#
interface Vlanif100
ip binding vpn-instance vpna
ipv6 enable
ipv6 address 2001:db8:2::2/64
#
interface Vlanif200
ip address 10.1.1.1 255.255.255.0
mpls
mpls ldp
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
```

```
port trunk allow-pass vlan 200
#
interface LoopBack1
 ip address 3.3.3.9 255.255.255.255
#
bgp 100
 peer 2.2.2.9 as-number 100
 peer 2.2.2.9 connect-interface LoopBack1
#
ipv4-family unicast
 peer 2.2.2.9 enable
#
ipv6-family vpnv6
 policy vpn-target
 peer 2.2.2.9 enable
#
ipv6-family vpn-instance vpna
 peer 2001:db8:2::1 as-number 65420
#
ospf 1
 area 0.0.0.0
 network 3.3.3.9 0.0.0.0
 network 10.1.1.0 0.0.0.255
#
return
```

Spoke-CE2

```
#
sysname Spoke-CE2
#
vlan batch 100
#
interface Vlanif100
 ipv6 enable
 ipv6 address 2001:db8:2::1/64
#
interface LoopBack1
 ipv6 enable
 ipv6 address 2001:db8:12::2/128
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
```

```
#
bgp 65420
router-id 3.3.3.3
peer 2001:db8:2::2 as-number 100
#
ipv6-family unicast
network 2001:db8:12::2 128
peer 2001:db8:2::2 enable
#
return
```

Hub-CE

```
#
sysname Hub-CE
#
vlan batch 100 200
#
interface Vlanif100
ipv6 enable
ipv6 address 2001:db8:3::1/64
#
interface Vlanif200
ipv6 enable
ipv6 address 2001:db8:4::1/64
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 200
#
interface LoopBack1
ipv6 enable
ipv6 address 2001:db8:13::3/128
#
bgp 65430
router-id 2.2.2.2
peer 2001:db8:3::2 as-number 100
peer 2001:db8:4::2 as-number 100
#
ipv6-family unicast
```



```
network 2001:db8:13::3 128
peer 2001:db8:3::2 enable
peer 2001:db8:4::2 enable
#
return
```

Hub-PE

```
#
sysname Hub-PE
#
vlan batch 100 200 300 400
#
ip vpn-instance vpn_in
ipv6-family
route-distinguisher 100:21
vpn-target 100:1 import-extcommunity
#
ip vpn-instance vpn_out
ipv6-family
route-distinguisher 100:22
vpn-target 200:1 export-extcommunity
#
mpls lsr-id 2.2.2.9
#
mpls
#
mpls ldp
#
interface Vlanif100
ip address 10.2.1.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif200
ip address 10.1.1.2 255.255.255.0
mpls
mpls ldp
#
interface Vlanif300
ip binding vpn-instance vpn_in
ipv6 enable
ipv6 address 2001:db8:3::2/64
#
```

```
interface Vlanif400
 ip binding vpn-instance vpn_out
 ipv6 enable
 ipv6 address 2001:db8:4::2/64
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 100
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 200
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 300
#
interface 10GE1/0/4
 port link-type trunk
 port trunk allow-pass vlan 400
#
interface LoopBack1
 ip address 2.2.2.9 255.255.255.255
#
bgp 100
 peer 1.1.1.9 as-number 100
 peer 1.1.1.9 connect-interface LoopBack1
 peer 3.3.3.9 as-number 100
 peer 3.3.3.9 connect-interface LoopBack1
#
ipv4-family unicast
 peer 1.1.1.9 enable
 peer 3.3.3.9 enable
#
ipv6-family vpnv6
 policy vpn-target
 peer 1.1.1.9 enable
 peer 3.3.3.9 enable
#
ipv6-family vpn-instance vpn_in
 peer 2001:db8:3::1 as-number 65430
#
ipv6-family vpn-instance vpn_out
```

```
peer 2001:db8:4::1 as-number 65430
peer 2001:db8:4::1 allow-as-loop
#
ospf 1
area 0.0.0.0
network 2.2.2.9 0.0.0.0
network 10.2.1.0 0.0.0.255
network 10.1.1.0 0.0.0.255
#
return
```

1.1.5.10 网络切片

[举例：配置 EVPN L3VPNv4 over SRv6 BE 网络切片示例（静态配置）](#)

介绍通过 EVPN L3VPNv4 over SRv6 BE 网络切片的配置过程。

[举例：配置 VLAN 切片示例](#)

介绍 VLAN 切片的配置过程。

1.1.5.10.1 举例：配置 EVPN L3VPNv4 over SRv6 BE 网络切片示例（静态配置）

介绍通过 EVPN L3VPNv4 over SRv6 BE 网络切片的配置过程。

组网需求

说明

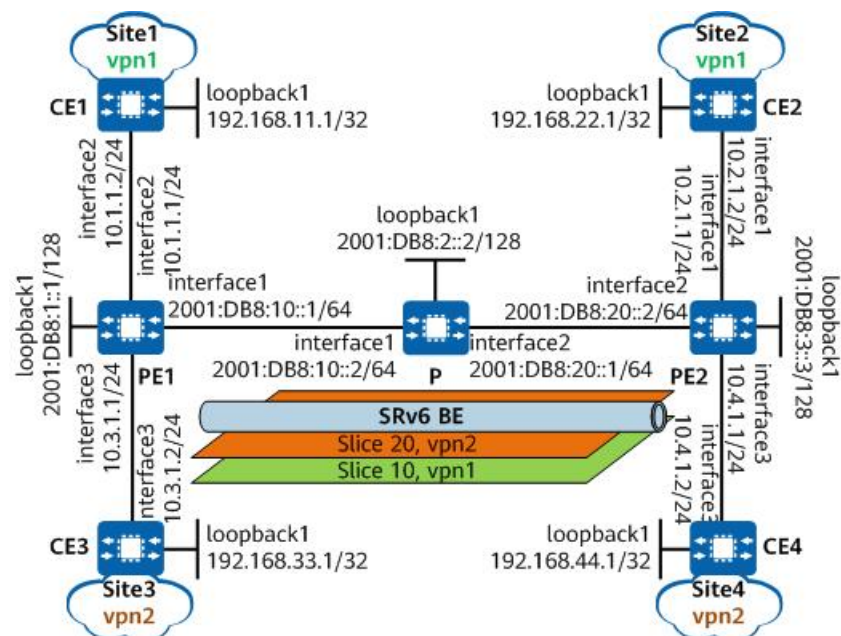
该配置仅 S6730-H-V2、S5755-H、S5732-H-V2 系列支持。

如[图 1](#)所示：PE1、P 和 PE2 属于同一自治系统。在 PE1 和 PE2 之间通过建立双向 SRv6 BE 承载 EVPN L3VPNv4 业务。此外，为了满足保障 CE1 和 CE2 之间 VPN 实例 vpn1 的业务 SLA，可以在公网上创建网络切片 10，专门承载 vpn1 的业务；为了满足保障 CE3 和 CE4 之间 VPN 实例 vpn2 的业务 SLA，可以在公网上创建网络切片 20，专门承载 vpn2 的业务。

图 1 配置 EVPN L3VPNv4 over SRv6 BE 网络切片组网图

说明

本例中 interface1，interface2 和 interface3 分别代表 Vlanif100，Vlanif200 和 Vlanif300。



配置注意事项

1. SRv6 BE 基于路由的 Color 引流到网络切片时，首先需要为路由配置扩展团体属性 Color，可以使用入口策略也可以使用出口策略。

配置思路

采用如下的思路配置 EVPN L3VPNv4 over SRv6 BE 网络切片：

1. 使能 PE1、P 和 PE2 各接口的 IPv6 转发能力，配置各接口的 IPv6 地址。
2. 在 PE1、P 和 PE2 上使能 OSPFv3。
3. 在 PE 设备上配置 EVPN L3VPN 实例并将 EVPN L3VPN 实例绑定到接入侧接口。
4. 在 PE 和 CE 之间建立 EBGp 对等体关系。
5. 在 PE 设备之间建立 BGP EVPN 对等体关系。
6. 在 PE 设备上配置 SRv6 BE，配置 OSPFv3 的 SRv6 能力。
7. 在 PE1、P 和 PE2 上创建网络切片实例，并配置基础接口。
8. 在 PE1 和 PE2 上配置流策略，引流到切片。

操作步骤

1. 使能各接口的 IPv6 转发能力，配置 IPv6 地址，以 PE1 为例，其他设备的配置过程相同，不再赘述。

```
[PE1] vlan batch 100 200 300
[PE1] interface vlanif 100
[PE1-Vlanif100] ipv6 enable
[PE1-Vlanif100] ipv6 address 2001:DB8:10::1 64
[PE1-Vlanif100] quit
```

```
[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] port link-type access
[PE1-10GE1/0/1] port default vlan 100
[PE1-10GE1/0/1] quit
[PE1] interface LoopBack 1
[PE1-LoopBack1] ipv6 enable
[PE1-LoopBack1] ipv6 address 2001:DB8:1::1 128
[PE1-LoopBack1] quit
```

2. 配置 OSPFv3。

配置 PE1。

```
[PE1] ospfv3 1
[PE1-ospfv3-1] router-id 1.1.1.1
[PE1-ospfv3-1] area 0
[PE1-ospfv3-1-area-0.0.0.0] quit
[PE1-ospfv3-1] quit
[PE1] interface vlanif 100
[PE1-Vlanif100] ospfv3 1 area 0.0.0.0
[PE1-Vlanif100] quit
[PE1] interface loopback1
[PE1-LoopBack1] ospfv3 1 area 0.0.0.0
[PE1-LoopBack1] quit
```

配置 P。

```
[P] ospfv3 1
[P-ospfv3-1] router-id 2.2.2.2
[P-ospfv3-1] area 0
[P-ospfv3-1-area-0.0.0.0] quit
[P-ospfv3-1] quit
[P] interface vlanif 100
[P-Vlanif100] ospfv3 1 area 0.0.0.0
[P-Vlanif100] quit
[P] interface vlanif 200
[P-Vlanif200] ospfv3 1 area 0.0.0.0
[P-Vlanif200] quit
[P] interface loopback1
[P-LoopBack1] ospfv3 1 area 0.0.0.0
[P-LoopBack1] quit
```

配置 PE2。

```
[PE2] ospfv3 1
[PE2-ospfv3-1] router-id 3.3.3.3
[PE2-ospfv3-1] area 0
[PE2-ospfv3-1-area-0.0.0.0] quit
```

```
[PE2-ospfv3-1] quit
[PE2] interface vlanif 200
[PE2-Vlanif200] ospfv3 1 area 0.0.0.0
[PE2-Vlanif200] quit
[PE2] interface loopback1
[PE2-LoopBack1] ospfv3 1 area 0.0.0.0
[PE2-LoopBack1] quit
```

配置完成后，可按如下指导检查 OSPFv3 是否配置成功。

显示 OSPFv3 邻居信息。以 PE1 为例。

```
[PE1] display ospfv3 peer

OSPFv3 Process (1)
Total number of peer(s): 1
Peer(s) in full state: 1
OSPFv3 Area (0.0.0.0)
Neighbor ID    Pri State      Dead Time Interface    Instance ID
2.2.2.2        1 Full/Backup 00:00:37 Vlanif100     0
```

3. 在 PE 设备上配置 EVPN L3VPN 实例并将 EVPN L3VPN 实例绑定到接入侧接口。

配置 PE1。

```
[PE1] evpn-overlay enable
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] ipv4-family
[PE1-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[PE1-vpn-instance-vpn1-af-ipv4] vpn-target 1:1 evpn
[PE1-vpn-instance-vpn1-af-ipv4] quit
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] ipv4-family
[PE1-vpn-instance-vpn2-af-ipv4] route-distinguisher 100:2
[PE1-vpn-instance-vpn2-af-ipv4] vpn-target 2:2 evpn
[PE1-vpn-instance-vpn2-af-ipv4] quit
[PE1-vpn-instance-vpn2] quit
[PE1] vlan batch 200 300
[PE1] interface Vlanif 200
[PE1-Vlanif200] ip binding vpn-instance vpn1
[PE1-Vlanif200] ip address 10.1.1.1 24
[PE1-Vlanif200] quit
[PE1] interface Vlanif 300
[PE1-Vlanif300] ip binding vpn-instance vpn2
[PE1-Vlanif300] ip address 10.3.1.1 24
[PE1-Vlanif300] quit
```

```
[PE1] interface 10ge 1/0/2
[PE1-10GE1/0/2] port link-type access
[PE1-10GE1/0/2] port default vlan 200
[PE1-10GE1/0/2] quit
[PE1] interface 10ge 1/0/3
[PE1-10GE1/0/3] port link-type access
[PE1-10GE1/0/3] port default vlan 300
[PE1-10GE1/0/3] quit
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] import-route direct
[PE1-bgp-vpn1] advertise l2vpn evpn
[PE1-bgp-vpn1] quit
[PE1-bgp] ipv4-family vpn-instance vpn2
[PE1-bgp-vpn1] import-route direct
[PE1-bgp-vpn1] advertise l2vpn evpn
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] evpn-overlay enable
[PE2] ip vpn-instance vpn1
[PE2-vpn-instance-vpn1] ipv4-family
[PE2-vpn-instance-vpn1-af-ipv4] route-distinguisher 200:1
[PE2-vpn-instance-vpn1-af-ipv4] vpn-target 1:1 evpn both
[PE2-vpn-instance-vpn1-af-ipv4] quit
[PE2-vpn-instance-vpn1] quit
[PE2] ip vpn-instance vpn2
[PE2-vpn-instance-vpn2] ipv4-family
[PE2-vpn-instance-vpn2-af-ipv4] route-distinguisher 200:2
[PE2-vpn-instance-vpn2-af-ipv4] vpn-target 2:2 evpn both
[PE2-vpn-instance-vpn2-af-ipv4] quit
[PE2-vpn-instance-vpn2] quit
[PE2] interface Vlanif 100
[PE2-Vlanif100] ip binding vpn-instance vpn1
[PE2-Vlanif100] ip address 10.2.1.1 24
[PE2-Vlanif100] quit
[PE2] interface Vlanif 300
[PE2-Vlanif300] ip binding vpn-instance vpn1
[PE2-Vlanif300] ip address 10.4.1.1 24
[PE2-Vlanif300] quit
[PE2] interface 10ge 1/0/1
[PE2-10GE1/0/1] port link-type access
```

```
[PE2-10GE1/0/1] port default vlan 100
[PE2-10GE1/0/1] quit
[PE2] interface 10ge 1/0/3
[PE2-10GE1/0/3] port link-type access
[PE2-10GE1/0/3] port default vlan 300
[PE2-10GE1/0/3] quit
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-vpn1] import-route direct
[PE2-bgp-vpn1] advertise l2vpn evpn
[PE2-bgp-vpn1] quit
[PE2-bgp] ipv4-family vpn-instance vpn2
[PE2-bgp-vpn2] import-route direct
[PE2-bgp-vpn2] advertise l2vpn evpn
[PE2-bgp-vpn2] quit
[PE2-bgp] quit
```

4. 在 PE 与 CE 之间建立 EBGp 对等体关系。

配置 CE1。

```
[CE1] interface loopback 1
[CE1-LoopBack1] ip address 192.168.11.1 32
[CE1-LoopBack1] quit
[CE1] bgp 65410
[CE1-bgp] router-id 192.168.11.1
[CE1-bgp] peer 10.1.1.1 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] quit
```

配置 CE3。

```
[CE3] interface loopback 1
[CE3-LoopBack1] ip address 192.168.33.1 32
[CE3-LoopBack1] quit
[CE3] bgp 65430
[CE3-bgp] router-id 192.168.33.1
[CE3-bgp] peer 10.3.1.1 as-number 100
[CE3-bgp] import-route direct
[CE3-bgp] quit
```

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] router-id 1.1.1.1
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-vpn1] peer 10.1.1.2 as-number 65410
```



```
[PE1-bgp-vpn1] import-route direct
[PE1-bgp-vpn1] quit
[PE1-bgp] ipv4-family vpn-instance vpn2
[PE1-bgp-vpn2] peer 10.3.1.2 as-number 65430
[PE1-bgp-vpn2] import-route direct
[PE1-bgp-vpn2] quit
[PE1-bgp] quit
```

配置 CE2。

```
[CE2] interface loopback 1
[CE2-LoopBack1] ip address 192.168.22.1 32
[CE2-LoopBack1] quit
[CE2] bgp 65420
[CE2-bgp] peer 10.2.1.1 as-number 100
[CE2-bgp] import-route direct
[CE2-bgp] quit
```

配置 CE4。

```
[CE4] interface loopback 1
[CE4-LoopBack1] ip address 192.168.44.1 32
[CE4-LoopBack1] quit
[CE4] bgp 65440
[CE4-bgp] peer 10.4.1.1 as-number 100
[CE4-bgp] import-route direct
[CE4-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] router-id 3.3.3.3
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-vpn1] peer 10.2.1.2 as-number 65420
[PE2-bgp-vpn1] import-route direct
[PE2-bgp] ipv4-family vpn-instance vpn2
[PE2-bgp-vpn2] peer 10.4.1.2 as-number 65440
[PE2-bgp-vpn2] import-route direct
[PE2-bgp-vpn2] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp vpnv4 vpn-instance peer** 命令，可以看到 PE 与 CE 之间的 BGP 对等体关系已建立，并达到 Established 状态。

以 PE1 与 CE1 的对等体关系为例：

```
[PE1] display bgp vpnv4 vpn-instance vpn1 peer

BGP local router ID : 1.1.1.1
Local AS number : 100
```

VPN-Instance vpn1, Router ID 1.1.1.1:

Total number of peers : 1 Peers in established state : 1

Peer	V	AS	MsgRcvd	MsgSent	OutQ	Up/Down	State	PrefRcv
10.1.1.2	4	65410	43	47	0	00:35:32	Established	1

5. 在 PE 设备之间建立 BGP EVPN 对等体关系。

配置 PE1。

```
[PE1] bgp 100
[PE1-bgp] peer 2001:DB8:3::3 as-number 100
[PE1-bgp] peer 2001:DB8:3::3 connect-interface loopback 1
[PE1-bgp] l2vpn-family evpn
[PE1-bgp-af-evpn] peer 2001:DB8:3::3 enable
[PE1-bgp-af-evpn] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] bgp 100
[PE2-bgp] peer 2001:DB8:1::1 as-number 100
[PE2-bgp] peer 2001:DB8:1::1 connect-interface loopback 1
[PE2-bgp] l2vpn-family evpn
[PE2-bgp-af-evpn] peer 2001:DB8:1::1 enable
[PE2-bgp-af-evpn] quit
[PE2-bgp] quit
```

配置完成后，在 PE 设备上执行 **display bgp evpn peer** 命令，可以看到 PE 之间的 BGP EVPN 对等体关系已建立，并达到 Established 状态。

6. 在 PE 设备之间建立 SRv6 BE。

配置 PE1。

```
[PE1] segment-routing ipv6
[PE1-segment-routing-ipv6] encapsulation source-address 2001:DB8:1::1
[PE1-segment-routing-ipv6] locator PE1 ipv6-prefix 2001:DB8:100:: 64 static 32
[PE1-segment-routing-ipv6-locator] opcode ::100 end-dt4 vpn-instance vpn1 evpn
[PE1-segment-routing-ipv6-locator] quit
[PE1-segment-routing-ipv6] quit
[PE1] ospfv3 1
[PE1-ospfv3-1] segment-routing ipv6 locator PE1 auto-sid-disable
[PE1-ospfv3-1] quit
[PE1] bgp 100
[PE1-bgp] l2vpn-family evpn
[PE1-bgp-af-evpn] peer 2001:DB8:3::3 advertise encap-type srv6
[PE1-bgp-af-evpn] quit
[PE1-bgp] ipv4-family vpn-instance vpn1
```

```
[PE1-bgp-vpn1] segment-routing ipv6 locator PE1 evpn
[PE1-bgp-vpn1] segment-routing ipv6 best-effort evpn
[PE1-bgp-vpn1] quit
[PE1-bgp] quit
```

配置 PE2。

```
[PE2] segment-routing ipv6
[PE2-segment-routing-ipv6] encapsulation source-address 2001:DB8:3::3
[PE2-segment-routing-ipv6] locator PE2 ipv6-prefix 2001:DB8:130:: 64 static 32
[PE2-segment-routing-ipv6-locator] opcode ::200 end-dt4 vpn-instance vpn1 evpn
[PE2-segment-routing-ipv6-locator] quit
[PE2-segment-routing-ipv6] quit
[PE2] ospfv3 1
[PE2-ospfv3-1] segment-routing ipv6 locator PE2 auto-sid-disable
[PE2-ospfv3-1] quit
[PE2] bgp 100
[PE2-bgp] l2vpn-family evpn
[PE2-bgp-af-evpn] peer 2001:DB8:1::1 advertise encap-type srv6
[PE2-bgp-af-evpn] quit
[PE2-bgp] ipv4-family vpn-instance vpn1
[PE2-bgp-vpn1] segment-routing ipv6 locator PE2 evpn
[PE2-bgp-vpn1] segment-routing ipv6 best-effort evpn
[PE2-bgp-vpn1] quit
[PE2-bgp] quit
```

7. 创建网络切片实例，并配置切片接口。

以 PE1 为例，PE2 配置类似。

```
[PE1] network-slice enable
[PE1] network-slice protocol-number 160
[PE1] network-slice instance 10
[PE1] network-slice instance 20
[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] network-slice 10 flex-channel 1000
[PE1-10GE1/0/1] network-slice 20 flex-channel 1000
[PE1-10GE1/0/1] quit
```

配置 P 设备网络切片

```
[P] network-slice enable
[P] network-slice protocol-number 160
[P] network-slice instance 10
[P] network-slice instance 20
[P] interface 10ge 1/0/1
[P-10GE1/0/1] network-slice 10 flex-channel 1000
[P-10GE1/0/1] network-slice 20 flex-channel 1000
```

```
[P-10GE1/0/1] quit
[P] interface 10ge 1/0/2
[P-10GE1/0/2] network-slice 10 flex-channel 1000
[P-10GE1/0/2] network-slice 20 flex-channel 1000
[P-10GE1/0/2] quit
```

8. 配置流策略，引流到切片

配置 PE1，PE2 设备配置和 PE1 配置类似。

```
[PE1] traffic classifier c1
[PE1-classifier-c1] if-match any
[PE1-classifier-c1] quit
[PE1] traffic behavior b1
[PE1-behavior-b1] network-slice-instance 10
[PE1-behavior-b1] quit
[PE1] traffic policy p1
[PE1-trafficpolicy-p1] classifier c1 behavior b1 precedence 5
[PE1-trafficpolicy-p1] quit
[PE1] traffic classifier c2
[PE1-classifier-c2] if-match any
[PE1-classifier-c2] quit
[PE1] traffic behavior b2
[PE1-behavior-b2] network-slice-instance 20
[PE1-behavior-b2] quit
[PE1] traffic policy p2
[PE1-trafficpolicy-p2] classifier c2 behavior b2 precedence 5
[PE1-trafficpolicy-p2] quit
```

9. 应用流策略

以 PE1 为例，PE2 设备配置逻辑相同。

```
[PE1] ip vpn-instance vpn1
[PE1-vpn-instance-vpn1] traffic-policy p1 inbound
[PE1-vpn-instance-vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn-instance-vpn2] traffic-policy p2 inbound
[PE1-vpn-instance-vpn2] quit
```

配置脚本

PE1

```
#
sysname PE1
#
evpn-overlay enable
```

```
#
vlan batch 100 200 300
#
ip vpn-instance vpn1
 traffic-policy p1 inbound
 ipv4-family
  route-distinguisher 100:1
  vpn-target 1:1 export-extcommunity evpn
  vpn-target 1:1 import-extcommunity evpn
#
ip vpn-instance vpn2
 traffic-policy p2 inbound
 ipv4-family
  route-distinguisher 100:2
  vpn-target 2:2 export-extcommunity evpn
  vpn-target 2:2 import-extcommunity evpn
#
traffic classifier c1 type or
 if-match any
#
traffic classifier c2 type or
 if-match any
#
traffic behavior b1
 network-slice-instance 10
#
traffic behavior b2
 network-slice-instance 20
#
traffic policy p1
 classifier c1 behavior b1 precedence 5
#
traffic policy p2
 classifier c2 behavior b2 precedence 5
#
network-slice instance 10
network-slice instance 20
#
segment-routing ipv6
 encapsulation source-address 2001:DB8:1::1
 locator PE1 ipv6-prefix 2001:DB8:100:: 64 static 32
 opcode ::100 end-dt4 vpn-instance vpn1 evpn
#
```

```
ospfv3 1
router-id 1.1.1.1
segment-routing ipv6 locator PE1 auto-sid-disable
area 0.0.0.0
#
interface Vlanif100
ipv6 enable
ipv6 address 2001:DB8:10::1/64
ospfv3 1 area 0.0.0.0
#
interface Vlanif200
ip binding vpn-instance vpn1
ip address 10.1.1.1 255.255.255.0
#
interface Vlanif300
ip binding vpn-instance vpn2
ip address 10.3.1.1 255.255.255.0
#
interface 10GE1/0/1
port link-type access
port default vlan 100
network-slice 10 flex-channel 1000
network-slice 20 flex-channel 1000
#
interface 10GE1/0/2
port link-type access
port default vlan 200
#
interface 10GE1/0/3
port link-type access
port default vlan 300
#
interface LoopBack1
ipv6 enable
ipv6 address 2001:DB8:1::1/128
ospfv3 1 area 0.0.0.0
#
bgp 100
router-id 1.1.1.1
peer 2001:DB8:3::3 as-number 100
peer 2001:DB8:3::3 connect-interface LoopBack1
#
ipv4-family unicast
```

```
undo synchronization
#
ipv4-family vpn-instance vpn1
import-route direct
advertise l2vpn evpn
segment-routing ipv6 locator PE1 evpn
segment-routing ipv6 best-effort evpn
peer 10.1.1.2 as-number 65410
#
ipv4-family vpn-instance vpn2
import-route direct
advertise l2vpn evpn
segment-routing ipv6 locator PE1 evpn
segment-routing ipv6 best-effort evpn
peer 10.3.1.2 as-number 65430
#
l2vpn-family evpn
undo policy vpn-target
peer 2001:DB8:3::3 enable
peer 2001:DB8:3::3 advertise encap-type srv6
#
network-slice protocol-number 160
#
return
```

P

```
#
sysname P
#
vlan batch 100 200
#
ospfv3 1
router-id 2.2.2.2
area 0.0.0.0
#
interface Vlanif100
ipv6 enable
ipv6 address 2001:DB8:10::2/64
ospfv3 1 area 0.0.0.0
#
interface Vlanif200
ipv6 enable
ipv6 address 2001:DB8:20::1/64
```

```
ospfv3 1 area 0.0.0.0
#
interface 10GE1/0/1
port link-type access
port default vlan 100
network-slice 10 flex-channel 1000
network-slice 20 flex-channel 1000
#
interface 10GE1/0/2
port link-type access
port default vlan 200
network-slice 10 flex-channel 1000
network-slice 20 flex-channel 1000
#
interface LoopBack1
ipv6 enable
ipv6 address 2001:DB8:2::2/128
ospfv3 1 area 0.0.0.0
#
return
```

PE2

```
#
sysname PE2
#
evpn-overlay enable
#
vlan batch 100 200 300
#
network-slice instance 10
network-slice instance 20
#
ip vpn-instance vpn1
traffic-policy p1 inbound
ipv4-family
route-distinguisher 200:1
vpn-target 1:1 export-extcommunity evpn
vpn-target 1:1 import-extcommunity evpn
#
ip vpn-instance vpn2
traffic-policy p2 inbound
ipv4-family
route-distinguisher 200:2
```



```
vpn-target 2:2 export-extcommunity evpn
vpn-target 2:2 import-extcommunity evpn
#
traffic classifier c1 type or
if-match any
#
traffic classifier c2 type or
if-match any
#
traffic behavior b1
network-slice-instance 10
#
traffic behavior b2
network-slice-instance 20
#
traffic policy p1
classifier c1 behavior b1 precedence 5
#
traffic policy p2
classifier c2 behavior b2 precedence 5
#
network-slice instance 10
network-slice instance 20
#
segment-routing ipv6
encapsulation source-address 2001:DB8:3::3
locator PE2 ipv6-prefix 2001:DB8:130:: 64 static 32
opcode ::200 end-dt4 vpn-instance vpn1 evpn
#
ospfv3 1
router-id 3.3.3.3
segment-routing ipv6 locator PE1 auto-sid-disable
area 0.0.0.0
#
interface Vlanif 100
ip binding vpn-instance vpn1
ip address 10.2.1.1 255.255.255.0
#
interface Vlanif 200
ipv6 enable
ipv6 address 2001:DB8:20::2/64
ospfv3 1 area 0.0.0.0
#
```

```
interface Vlanif 300
 ip binding vpn-instance vpn2
 ip address 10.4.1.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 100
#
interface 10GE1/0/2
 port link-type access
 port default vlan 200
 network-slice 10 flex-channel 1000
 network-slice 20 flex-channel 1000
#
interface 10GE1/0/3
 port link-type access
 port default vlan 300
#
interface LoopBack1
 ipv6 enable
 ipv6 address 2001:DB8:3::3/128
 ospfv3 1 area 0.0.0.0
#
bgp 100
 router-id 3.3.3.3
 peer 2001:DB8:1::1 as-number 100
 peer 2001:DB8:1::1 connect-interface LoopBack1
#
ipv4-family unicast
 undo synchronization
#
ipv4-family vpn-instance vpn1
 import-route direct
 advertise l2vpn evpn
 segment-routing ipv6 locator PE2 evpn
 segment-routing ipv6 best-effort evpn
 peer 10.2.1.2 as-number 65420
#
ipv4-family vpn-instance vpn2
 import-route direct
 advertise l2vpn evpn
 segment-routing ipv6 locator PE2 evpn
 segment-routing ipv6 best-effort evpn
```

```
peer 10.4.1.2 as-number 65440
#
l2vpn-family evpn
undo policy vpn-target
peer 2001:DB8:1::1 enable
peer 2001:DB8:1::1 advertise encap-type srv6
#
network-slice protocol-number 160
#
return
```

CE1

```
#
sysname CE1
#
vlan batch 200
#
interface Vlanif200
ip address 10.1.1.2 255.255.255.0
#
interface 10GE1/0/1
port link-type access
port default vlan 200
#
interface LoopBack1
ip address 192.168.11.1 255.255.255.255
#
bgp 65410
peer 10.1.1.1 as-number 100
#
ipv4-family unicast
undo synchronization
import-route direct
peer 10.1.1.1 enable
#
return
```

CE2

```
#
sysname CE2
#
vlan batch 100
#
```

```
interface Vlanif100
 ip address 10.2.1.2 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 100
#
interface LoopBack1
 ip address 192.168.22.1 255.255.255.255
#
bgp 65420
 peer 10.2.1.1 as-number 100
#
ipv4-family unicast
 undo synchronization
 import-route direct
 peer 10.2.1.1 enable
#
return
```

CE3

```
#
sysname CE3
#
vlan batch 300
#
interface Vlanif300
 ip address 10.3.1.2 255.255.255.0
#
interface 10GE1/0/1
 port link-type access
 port default vlan 300
#
interface LoopBack1
 ip address 192.168.33.1 255.255.255.255
#
bgp 65430
 peer 10.3.1.1 as-number 100
#
ipv4-family unicast
 undo synchronization
 import-route direct
 peer 10.3.1.1 enable
```

```
#  
return
```

CE4

```
#  
sysname CE4  
#  
vlan batch 300  
#  
interface Vlanif300  
ip address 10.4.1.2 255.255.255.0  
#  
interface 10GE1/0/1  
port link-type access  
port default vlan 300  
#  
interface LoopBack1  
ip address 192.168.44.1 255.255.255.255  
#  
bgp 65440  
peer 10.4.1.1 as-number 100  
#  
ipv4-family unicast  
undo synchronization  
import-route direct  
peer 10.4.1.1 enable  
#  
return
```

1.1.5.10.2 举例：配置 VLAN 切片示例

介绍 VLAN 切片的配置过程。

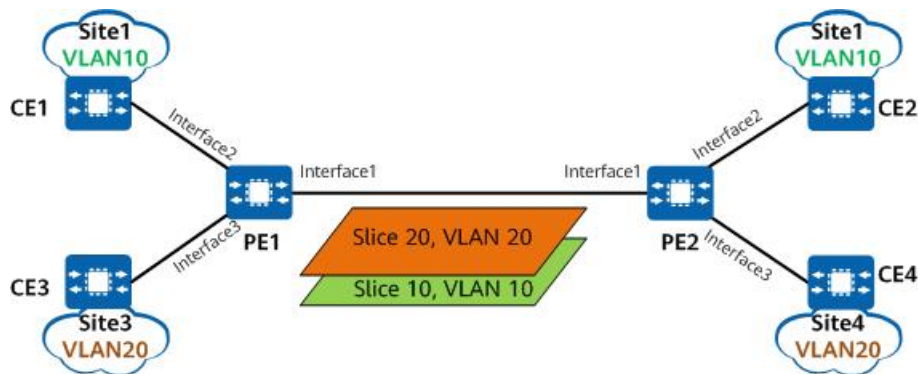
组网需求

如图 1 所示：在 PE1 和 PE2 之间通过 VLAN 互通。为了满足保障 CE1 和 CE2 之间 VLAN 10 的业务 SLA，可以在公网上创建网络切片 10，专门承载 VLAN 10 的业务；为了满足保障 CE3 和 CE4 之间 VLAN 20 业务 SLA，可以在公网上创建网络切片 20，专门承载 VLAN 20 的业务。

图 1 配置 VLAN 切片组网图

说明

本例中 interface1，interface2 和 interface3 分别代表 10GE1/0/1，10GE1/0/2 和 10GE1/0/3。



注意事项

为了避免 VLAN 的切片信息流入其他网络中，影响流量转发，在切片网络的出口，配置 VLAN 切片的终结模式，如 PE 设备的 interface2、interface3。

配置思路

采用如下的思路配置 VLAN 切片：

1. 设备创建 VLAN。
2. 将 PE 的 interface1 同时加入 VLAN 10、VLAN 20，interface2 加入 VLAN 10，interface 3 加入 VLAN 20。
3. CE1、CE2 与 PE 连接的接口加入 VLAN 10，CE3、CE4 与 PE 连接的接口加入 VLAN 20。
4. 在 PE1、PE2 上创建网络切片实例，并配置基础接口。
5. 在 PE1 和 PE2 上配置流策略，引流到切片。

说明

本用例以接口下配置流策略为例，也可以选择通过 **traffic-policy policy-name global inbound** 命令在全局应用流策略。

仅 S6730-H-V2、S5755-H、S5732-H-V2 系列支持全局流策略配置。

操作步骤

1. 在设备上创建 VLAN。
配置 PE1，PE2 与 PE1 配置相同。

```
<HUAWEI> system-view
[HUAWEI] sysname PE1
[PE1] vlan batch 10 20
```

配置 CE1，CE2 与 CE1 配置相同。

```
<HUAWEI> system-view
[HUAWEI] sysname CE1
[CE1] vlan batch 10
```

配置 CE3，CE4 与 CE3 配置相同。

```
<HUAWEI> system-view
[HUAWEI] sysname CE3
[CE3] vlan batch 20
```

2. 配置 PE 设备端口加入 VLAN。

配置 PE1，PE2 与 PE1 配置相同。

```
[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] port link-type trunk
[PE1-10GE1/0/1] port trunk allow-pass vlan 10 20
[PE1-10GE1/0/1] quit
[PE1] interface 10ge 1/0/2
[PE1-10GE1/0/2] port link-type trunk
[PE1-10GE1/0/2] port trunk allow-pass vlan 10
[PE1-10GE1/0/2] quit
[PE1] interface 10ge 1/0/3
[PE1-10GE1/0/3] port link-type trunk
[PE1-10GE1/0/3] port trunk allow-pass vlan 20
[PE1-10GE1/0/3] quit
```

配置完成后，可以查看 VLAN 下的端口信息。

```
[PE1] display vlan 10
```

```
-----
-
U: Up;      D: Down;    TG: Tagged;    UT: Untagged;
MP: Vlan-mapping;      ST: Vlan-stacking;
#: ProtocolTransparent-vlan; *: Management-vlan;
MAC-LRN: MAC-address learning; STAT: Statistic;
BC: Broadcast; MC: Multicast; UC: Unknown-unicast;
FWD: Forward; DSD: Discard;
-----
-
VID      Ports
-----
-
10      TG:10GE1/0/1(U) 10GE1/0/2(U)
VID Type  Status Property MAC-LRN STAT  BC MC UC Description
-----
-
10 common enable default enable disable FWD FWD FWD VLAN 0010
```

3. 在 CE 设备端口加入 VLAN。

配置 CE1。

```
[CE1] interface 10ge 1/0/1
[CE1-10GE1/0/1] port link-type trunk
[CE1-10GE1/0/1] port trunk allow-pass vlan 10
[CE1-10GE1/0/1] quit
```

配置 CE2。

```
[CE2] interface 10ge 1/0/1
[CE2-10GE1/0/1] port link-type trunk
[CE2-10GE1/0/1] port trunk allow-pass vlan 10
[CE2-10GE1/0/1] quit
```

配置 CE3。

```
[CE3] interface 10ge 1/0/1
[CE3-10GE1/0/1] port link-type trunk
[CE3-10GE1/0/1] port trunk allow-pass vlan 20
[CE3-10GE1/0/1] quit
```

配置 CE4。

```
[CE4] interface 10ge 1/0/1
[CE4-10GE1/0/1] port link-type trunk
[CE4-10GE1/0/1] port trunk allow-pass vlan 20
[CE4-10GE1/0/1] quit
```

4. 创建网络切片实例，并配置切片接口。

以 PE1 为例，PE2 配置类似。

```
[PE1] network-slice enable
[PE1] network-slice vlan-encapsulate enable
[PE1] network-slice instance 10
[PE1-network-slice-instance-10] quit
[PE1] network-slice instance 20
[PE1-network-slice-instance-20] quit
[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] network-slice 10 flex-channel 1000
[PE1-10GE1/0/1] network-slice 20 flex-channel 1000
[PE1-10GE1/0/1] quit
[PE1] interface 10ge 1/0/2
[PE1-10GE1/0/2] network-slice 10 flex-channel 100 end-mode
[PE1-10GE1/0/2] quit
[PE1] interface 10ge 1/0/3
[PE1-10GE1/0/3] network-slice 20 flex-channel 100 end-mode
[PE1-10GE1/0/3] quit
```

5. 配置流策略，引流到切片

配置 PE1，PE2 设备配置和 PE1 配置类似。

```
[PE1] traffic classifier c1
```



```

[PE1-classifier-c1] if-match vlan 10
[PE1-classifier-c1] quit
[PE1] traffic behavior b1
[PE1-behavior-b1] network-slice-instance 10
[PE1-behavior-b1] quit
[PE1] traffic classifier c2
[PE1-classifier-c2] if-match vlan 20
[PE1-classifier-c2] quit
[PE1] traffic behavior b2
[PE1-behavior-b2] network-slice-instance 20
[PE1-behavior-b2] quit
[PE1] traffic policy p1
[PE1-trafficpolicy-p1] classifier c1 behavior b1 precedence 5
[PE1-trafficpolicy-p1] classifier c2 behavior b2 precedence 5
[PE1-trafficpolicy-p1] quit

```

查看 traffic policy 的配置信息。

```

[PE1] display traffic policy p1
Traffic Policy Information:
Policy: p1
Classifier: c1
Type: OR
Behavior: b1
network-slice-instance 10
Classifier: c2
Type: OR
Behavior: b2
network-slice-instance 20

```

6. 应用流策略

配置 PE1。

```

[PE1] interface 10ge 1/0/1
[PE1-10GE1/0/1] traffic-policy p1 inbound
[PE1-10GE1/0/1] quit
[PE1] interface 10ge 1/0/2
[PE1-10GE1/0/2] traffic-policy p1 inbound
[PE1-10GE1/0/2] quit
[PE1] interface 10ge 1/0/3
[PE1-10GE1/0/3] traffic-policy p1 inbound
[PE1-10GE1/0/3] quit

```

配置 PE2。

```

[PE2] interface 10ge 1/0/1
[PE2-10GE1/0/1] traffic-policy p1 inbound

```

```
[PE2-10GE1/0/1] quit
[PE2] interface 10ge 1/0/2
[PE2-10GE1/0/2] traffic-policy p1 inbound
[PE2-10GE1/0/2] quit
[PE2] interface 10ge 1/0/3
[PE2-10GE1/0/3] traffic-policy p1 inbound
[PE2-10GE1/0/3] quit
```

查看 traffic policy 的配置结果，以 PE1 为例。

```
[PE1] display traffic-policy applied-record
```

Total records : 1

-			
Policy Type/Name	Apply Parameter	Slot	State

-			
p1	10GE1/0/1(IN)	1	success
	10GE1/0/2(IN)	1	success
	10GE1/0/3(IN)	1	success

-			

配置脚本

PE1

```
#
sysname PE1
#
vlan batch 10 20
#
traffic classifier c1 type or
if-match vlan 10
#
traffic classifier c2 type or
if-match vlan 20
#
traffic behavior b1
network-slice-instance 10
#
traffic behavior b2
network-slice-instance 20
#
traffic policy p1
```

```
classifier c1 behavior b1 precedence 5
classifier c2 behavior b2 precedence 5
#
network-slice instance 10
network-slice instance 20
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10 20
traffic-policy p1 inbound
network-slice 10 flex-channel 1000
network-slice 20 flex-channel 1000
#
interface 10GE1/0/2
port link-type trunk
traffic-policy p1 inbound
port trunk allow-pass vlan 10
network-slice 10 flex-channel 100 end-mode
#
interface 10GE1/0/3
port link-type trunk
traffic-policy p1 inbound
port trunk allow-pass vlan 20
network-slice 20 flex-channel 100 end-mode
#
network-slice enable
#
network-slice vlan-encapsulate enable
#
return
```

PE2

```
#
sysname PE2
#
vlan batch 10 20
#
traffic-policy p1 global inbound
#
traffic classifier c1 type or
if-match vlan 10
#
traffic classifier c2 type or
```

```
if-match vlan 20
#
traffic behavior b1
  network-slice-instance 10
#
traffic behavior b2
  network-slice-instance 20
#
traffic policy p1
  classifier c1 behavior b1 precedence 5
  classifier c2 behavior b2 precedence 5
#
network-slice instance 10
network-slice instance 20
#
interface 10GE1/0/1
  port link-type trunk
  port trunk allow-pass vlan 10 20
  traffic-policy p1 inbound
  network-slice 10 flex-channel 1000
  network-slice 20 flex-channel 1000
#
interface 10GE1/0/2
  port link-type trunk
  port trunk allow-pass vlan 10
  traffic-policy p1 inbound
  network-slice 10 flex-channel 100 end-mode
#
interface 10GE1/0/3
  port link-type trunk
  port trunk allow-pass vlan 20
  traffic-policy p1 inbound
  network-slice 20 flex-channel 100 end-mode
#
network-slice enable
#
network-slice vlan-encapsulate enable
#
return
```

CE1

```
#
sysname CE1
```

```
#  
vlan batch 10  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 10  
#  
return
```

CE2

```
#  
sysname CE2  
#  
vlan batch 10  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 10  
#  
return
```

CE3

```
#  
sysname CE3  
#  
vlan batch 20  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 20  
#  
return
```

CE4

```
#  
sysname CE4  
#  
vlan batch 20  
#  
interface 10GE1/0/1  
port link-type trunk  
port trunk allow-pass vlan 20  
#
```

```
return
```

1.1.5.11 可靠性

VRRP

M-LAG

1.1.5.11.1 VRRP

举例：配置 VRRP 网络传输组播数据

1.1.5.11.1.1 举例：配置 VRRP 网络传输组播数据

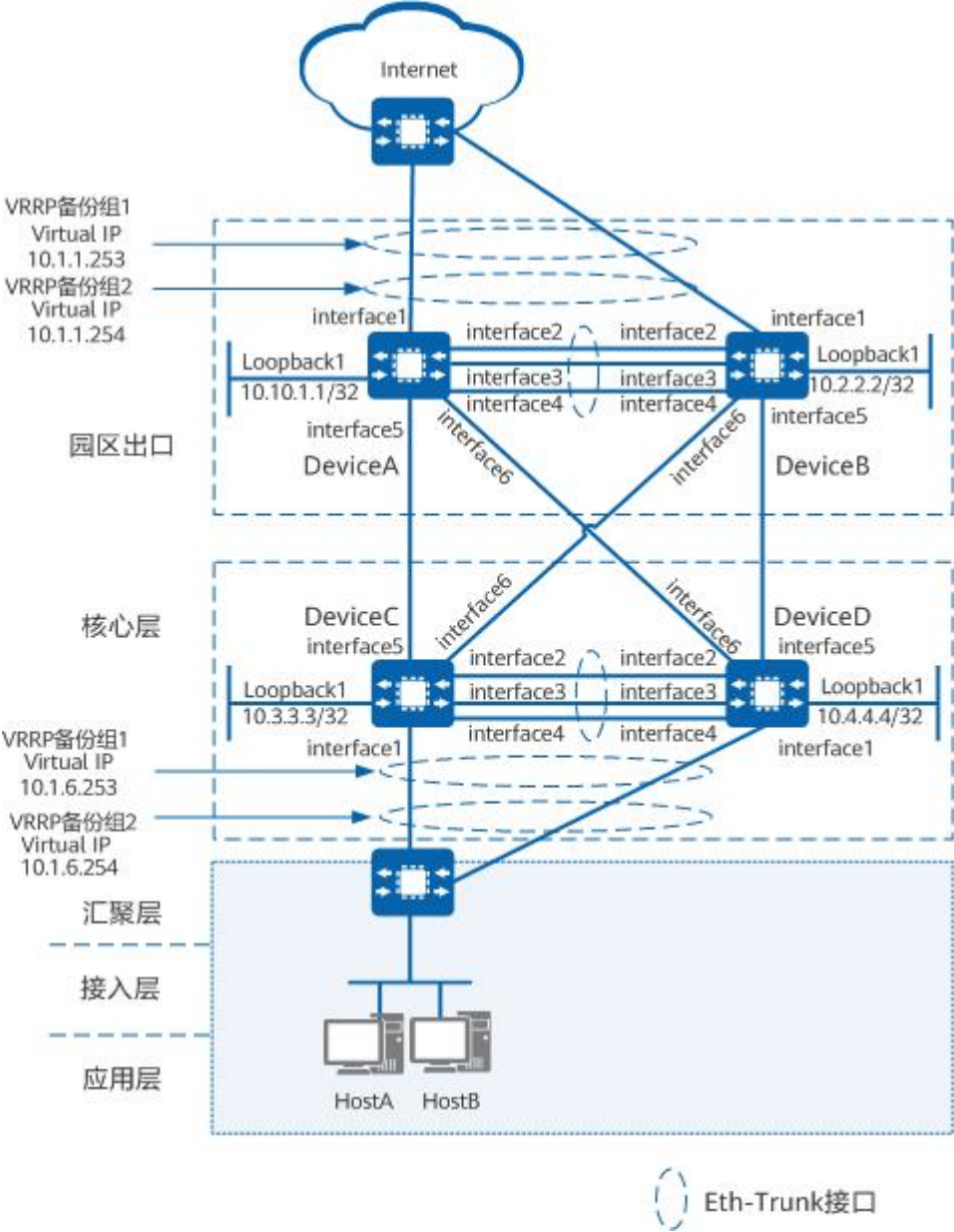
组网需求

如[图 1 配置 VRRP 网络传输组播数据组网图](#)所示，DeviceA、DeviceB 为园区网络的出口网关，DeviceC、DeviceD 为园区网络的核心设备，组播源通过路由器接入园区网。从横向看，网络关键节点实现了可靠冗余；从纵向看，出口网关与核心设备进行全连接，实现了链路间的冗余备份。通过配置 VRRP 网络传输组播数据，可确保组播数据能够安全、可靠地传输到下游网络。

图 1 配置 VRRP 网络传输组播数据组网图

说明

本例中 interface1, interface2, interface3, interface4, interface5, interface6 分别代表 10GE1/0/1, 10GE1/0/2, 10GE1/0/3, 10GE1/0/4, 10GE1/0/5, 10GE1/0/6。



设备	接口	加入的 VLAN	VLANIF 接口的 IP 地址	设备	接口	加入的 VLAN	VLANIF 接口的 IP 地址
DeviceA	10GE1/0/1	VLAN100	10.1.1.1/24	DeviceC	10GE1/0/1	VLAN400	10.1.6.1/24
	Eth-trunk 1 (成员接口为 10GE1/0/2、10GE1/0/3、10GE1/0/4)	VLAN100、VLAN200	未创建 VLANIF200 接口		Eth-trunk 1 (成员接口为 10GE1/0/2、10GE1/0/3、10GE1/0/4)	VLAN400、VLAN500	未创建 VLANIF500 接口
	10GE1/0/5	VLAN301	10.1.2.1/24		10GE1/0/5	VLAN301	10.1.2.2/24

设备	接口	加入的 VLAN	VLANIF 接口的 IP 地址	设备	接口	加入的 VLAN	VLANIF 接口的 IP 地址
	10GE1/0/6	VLAN302	10.1.3.1/24		10GE1/0/6	VLAN304	10.1.5.2/24
DeviceB	10GE1/0/1	VLAN100	10.1.1.2/24	DeviceD	10GE1/0/1	VLAN400	10.1.6.2/24
	Eth-trunk 1 (成员接口为 10GE1/0/2、10GE1/0/3、10GE1/0/4)	VLAN100、VLAN200	未创建 VLANIF200 接口		Eth-trunk 1 (成员接口为 10GE1/0/2、10GE1/0/3、10GE1/0/4)	VLAN400、VLAN500	未创建 VLANIF500 接口
	10GE1/0/5	VLAN303	10.1.4.1/24		10GE1/0/5	VLAN303	10.1.4.2/24
	10GE1/0/6	VLAN304	10.1.5.1/24		10GE1/0/6	VLAN302	10.1.3.2/24

配置注意事项

- 1. 各备份组之间的虚拟 IP 地址不能重复，并且必须和接口的 IP 地址在同一网段。
- 2. 同一备份组的设备上配置相同的备份组 ID。

配置思路

采用如下的思路配置 VRRP 网络传输组播数据：

- 1. 配置链路聚合。DeviceA 与 DeviceB 之间，DeviceC 与 DeviceD 之间配置链路聚合，保证 VRRP 协议报文能够交互，VRRP 能够正常运行。
- 2. 配置 VLAN。各设备上创建 VLAN，接口加入 VLAN，对应 VLANIF 接口配 IP 地址，使本地网络可达。

说明

交换机的二层接口默认使能 STP。如果当前二层网络为环形组网，STP 会将其中的一个端口阻塞以防止环路。在本配置示例中，DeviceC、DeviceD 和下游二层交换机已经构成了二层环网。为了不影响后面 OSPF 路由负载分担功能，建议 DeviceC、DeviceD 去使能与下游二层交换机相连的二层接口上的 STP 功能。同时可在下游的二层交换机上配置 Smart Link 负载分担功能，确保二层环网不会广播风暴的同时，还能实现链路的负载分担。

- 3. 配置 OSPF 路由协议。各设备上配置 OSPF 路由协议，使网络层互通。

4. 配置 VRRP 备份组。DeviceA 与 DeviceB 之间，DeviceC 与 DeviceD 之间配置 VRRP 备份组，实现设备间冗余备份，确保组播数据可靠转发。不同备份组间实现单播转发的负载均衡，减轻单设备同时转发单播数据和组播数据的压力。
5. 配置组播协议。各设备上配置组播协议，实现组播数据正常转发。
6. 配置 BFD for OSPF、BFD for PIM，确保设备能快速感知链路故障，使得路由快速收敛。

操作步骤

1. 配置链路聚合。在 DeviceA 上创建 Eth-Trunk 接口并加入成员接口。DeviceB、DeviceC、DeviceD 的配置与 DeviceA 类似，详见配置脚本。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] trunkport 10ge 1/0/2 to 1/0/4
[DeviceA-Eth-Trunk1] quit
```

2. 配置 VLAN。

- a. 在 DeviceA 上创建 VLAN，配置接口加入 VLAN。DeviceB、DeviceC、DeviceD 的配置与 DeviceA 类似，详见配置脚本。

```
[DeviceA] vlan batch 100 200 301 302
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 100
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/5
[DeviceA-10GE1/0/5] port link-type trunk
[DeviceA-10GE1/0/5] port trunk allow-pass vlan 301
[DeviceA-10GE1/0/5] quit
[DeviceA] interface 10ge 1/0/6
[DeviceA-10GE1/0/6] port link-type trunk
[DeviceA-10GE1/0/6] port trunk allow-pass vlan 302
[DeviceA-10GE1/0/6] quit
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] port link-type trunk
[DeviceA-Eth-Trunk1] port trunk allow-pass vlan 100 200
[DeviceA-Eth-Trunk1] quit
```

- b. 在 DeviceA 上的三层接口上配置 IP 地址。DeviceB、DeviceC、DeviceD 的配置与 DeviceA 类似，详见配置脚本。

```
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] ip address 10.1.1.1 24
[DeviceA-Vlanif100] quit
```

```
[DeviceA] interface vlanif 301
[DeviceA-Vlanif301] ip address 10.1.2.1 24
[DeviceA-Vlanif301] quit
[DeviceA] interface vlanif 302
[DeviceA-Vlanif302] ip address 10.1.3.1 24
[DeviceA-Vlanif302] quit
[DeviceA] interface loopback 1
[DeviceA-LoopBack1] ip address 10.10.1.1 32
[DeviceA-LoopBack1] quit
```

3. 配置 OSPF 路由协议。在 DeviceA 上使能 OSPF，设备加入 Area 0，配置 Area 0 内需要发布的网段。DeviceB、DeviceC、DeviceD 的配置与 DeviceA 类似，详见配置脚本。

```
[DeviceA] ospf
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] network 10.10.1.1 0.0.0.0
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

4. 配置 VRRP 备份组。

- a. 在 DeviceA 和 DeviceB 上创建 VRRP 备份组 1，配置 DeviceA 为 Master 设备，DeviceB 为 Backup 设备。

配置 DeviceA。

```
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.253
[DeviceA-Vlanif100] vrrp vrid 1 priority 120
[DeviceA-Vlanif100] vrrp vrid 1 preempt timer delay 20
[DeviceA-Vlanif100] quit
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface vlanif 100
[DeviceB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.253
[DeviceB-Vlanif100] quit
```

- b. 在 DeviceA 和 DeviceB 上创建 VRRP 备份组 2，配置 DeviceB 为 Master 设备，DeviceA 为 Backup 设备。

配置 DeviceA。

```
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.254
```

```
[DeviceA-Vlanif100] quit
```

配置 DeviceB。

```
[DeviceB] interface vlanif 100
[DeviceB-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.254
[DeviceB-Vlanif100] vrrp vrid 2 priority 120
[DeviceB-Vlanif100] vrrp vrid 2 preempt timer delay 20
[DeviceB-Vlanif100] quit
```

DeviceC 和 DeviceD 的配置步骤与 DeviceA 和 DeviceB 的配置步骤类似，详见配置脚本。

5. 配置组播协议。

在 DeviceA 上使能组播路由功能。DeviceB 的配置与 DeviceA 类似，详见配置脚本。

```
[DeviceA] multicast routing-enable
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] pim sm
[DeviceA-Vlanif100] quit
[DeviceA] interface vlanif 301
[DeviceA-Vlanif301] pim sm
[DeviceA-Vlanif301] quit
[DeviceA] interface vlanif 302
[DeviceA-Vlanif302] pim sm
[DeviceA-Vlanif302] quit
[DeviceA] interface loopback 1
[DeviceA-LoopBack1] pim sm
[DeviceA-LoopBack1] quit
```

在 DeviceC 上使能组播路由功能、IGMP 功能并配置动态 RP。DeviceD 的配置与 DeviceC 类似，详见配置脚本。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] multicast routing-enable
[DeviceC] interface vlanif 400
[DeviceC-Vlanif400] pim sm
[DeviceC-Vlanif400] igmp enable
[DeviceC-Vlanif400] quit
[DeviceC] interface vlanif 301
[DeviceC-Vlanif301] pim sm
[DeviceC-Vlanif301] quit
[DeviceC] interface vlanif 304
[DeviceC-Vlanif304] pim sm
[DeviceC-Vlanif304] quit
[DeviceC] interface loopback 1
[DeviceC-LoopBack1] pim sm
```

```
[DeviceC-LoopBack1] quit
[DeviceC] pim
[DeviceC-pim] c-bsr loopback 1
[DeviceC-pim] c-rp loopback 1
[DeviceC-pim] quit
```

6. 配置 BFD 功能。

- a. 在 DeviceA 上使能全局 BFD 功能。DeviceB、DeviceC、DeviceD 上的配置与 DeviceA 上类似，详见配置脚本。

```
[DeviceA] bfd
[DeviceA-bfd] quit
```

- b. 在 DeviceA 上配置 BFD for OSPF 功能。DeviceB、DeviceC、DeviceD 上的配置与 DeviceA 上类似，详见配置脚本。

```
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] ospf bfd enable
[DeviceA-Vlanif100] quit
[DeviceA] interface vlanif 301
[DeviceA-Vlanif301] ospf bfd enable
[DeviceA-Vlanif301] quit
[DeviceA] interface vlanif 302
[DeviceA-Vlanif302] ospf bfd enable
[DeviceA-Vlanif302] quit
```

- c. 在 DeviceA 上配置 BFD for PIM 功能。DeviceB、DeviceC、DeviceD 上的配置与 DeviceA 上类似，详见配置脚本。

```
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] pim bfd enable
[DeviceA-Vlanif100] quit
[DeviceA] interface vlanif 301
[DeviceA-Vlanif301] pim bfd enable
[DeviceA-Vlanif301] quit
[DeviceA] interface vlanif 302
[DeviceA-Vlanif302] pim bfd enable
[DeviceA-Vlanif302] quit
```

检查配置结果

1. 检查链路聚合功能是否配置正确。

在 DeviceA 上执行 **display eth-trunk 1** 命令，可以看出 Eth-Trunk 1 中包含 3 个成员接口 10GE1/0/2、10GE1/0/3 和 10GE1/0/4，成员接口的状态都为 Up。DeviceB、DeviceC、DeviceD 上的检查过程与 DeviceA 类似。

```
[DeviceA] display eth-trunk 1
```

Eth-Trunk1's state information is:

WorkingMode: **NORMAL** Hash arithmetic: According to SIP-XOR-DIP

Least Active-linknumber: 1 Max Bandwidth-affected-linknumber: 8

Operate status: up Number Of Up Ports In Trunk: 3

-

PortName	Status	Weight
10GE1/0/2	Up	1
10GE1/0/3	Up	1
10GE1/0/4	Up	1

2. 检查 VRRP 协议是否配置正确。

在 DeviceA 上执行 **display vrrp verbose** 命令，可以看到 DeviceA 在备份组 1 中作为 Master 设备，在备份组 2 中作为 Backup 设备。

```
[DeviceA] display vrrp verbose
```

Vlanif100 | Virtual Router 1

State : Master

Virtual IP : 10.1.1.253

Master IP : 10.1.1.1

PriorityRun : 120

PriorityConfig : 120

MasterPriority : 120

Preempt : YES Delay Time : 20 s

TimerRun : 1 s

TimerConfig : 1 s

Auth type : NONE

Virtual MAC : 0000-5e00-0101

Check TTL : YES

Config type : normal-vrrp

Create time : 2012-12-31 10:34:23 UTC+08:00

Last change time : 2012-12-31 10:34:26 UTC+08:00

Vlanif100 | Virtual Router 2

State : Backup

Virtual IP : 10.1.1.254

Master IP : 10.1.1.2

PriorityRun : 100

PriorityConfig : 100

MasterPriority : 120

Preempt : YES Delay Time : 0 s

TimerRun : 1 s

TimerConfig : 1 s

Auth type : NONE
Virtual MAC : 0000-5e00-0102
Check TTL : YES
Config type : normal-vrrp
Create time : 2012-12-31 10:35:39 UTC-08:00
Last change time : 2012-12-31 10:35:43 UTC-08:00

在 DeviceB 上执行 **display vrrp verbose** 命令，可以看到 DeviceB 在备份组 1 中作为 Backup 设备，在备份组 2 中作为 Master 设备。

[DeviceB] **display vrrp verbose**

Vlanif100 | Virtual Router 1

State : Backup

Virtual IP : 10.1.1.253
Master IP : 10.1.1.1
PriorityRun : 100
PriorityConfig : 100
MasterPriority : 120
Preempt : YES Delay Time : 0 s
TimerRun : 1 s
TimerConfig : 1 s
Auth type : NONE
Virtual MAC : 0000-5e00-0101
Check TTL : YES
Config type : normal-vrrp
Create time : 2012-12-31 10:34:23 UTC-08:00
Last change time : 2012-12-31 10:34:26 UTC-08:00

Vlanif100 | Virtual Router 2

State : Master

Virtual IP : 10.1.1.254
Master IP : 10.1.1.2
PriorityRun : 120
PriorityConfig : 120
MasterPriority : 120
Preempt : YES Delay Time : 20 s
TimerRun : 1 s
TimerConfig : 1 s
Auth type : NONE
Virtual MAC : 0000-5e00-0102
Check TTL : YES
Config type : normal-vrrp
Create time : 2012-12-31 10:35:39 UTC-08:00
Last change time : 2012-12-31 10:35:43 UTC-08:00

DeviceC、DeviceD 上的检查过程与 DeviceA、DeviceB 上类似。

3. 检查 OSPF 协议是否配置成功。

在 DeviceA 上执行 **display ip routing-table** 命令，可以看出到达 10.1.6.0/24 网段的 IP 路由有两条，实现了单播的负载分担。

[DeviceA] display ip routing-table

Route Flags: R – relay, D – download to fib, T – to vpn-instance

Routing Tables: Public

Destinations : 15 Routes : 18

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.1.1.0/24	Direct	0	0	D	10.1.1.1	Vlanif100
10.1.1.1/32	Direct	0	0	D	127.0.0.1	Vlanif100
10.1.1.253/32	Direct	0	0	D	127.0.0.1	Vlanif100
10.1.1.254/32	Direct	0	0	D	127.0.0.1	Vlanif100
10.1.2.0/24	Direct	0	0	D	10.1.2.1	Vlanif301
10.1.2.1/32	Direct	0	0	D	127.0.0.1	Vlanif301
10.1.3.0/24	Direct	0	0	D	10.1.3.1	Vlanif302
10.1.3.1/32	Direct	0	0	D	127.0.0.1	Vlanif302
10.1.4.0/24	OSPF	10	2	D	10.1.3.2	Vlanif302
10.1.5.0/24	OSPF	10	2	D	10.1.2.2	Vlanif301
10.1.6.0/24	OSPF	10	2	D	10.1.2.2	Vlanif301
	OSPF	10	2	D	10.1.3.2	Vlanif302
10.1.6.253/32	OSPF	10	2	D	10.1.2.2	Vlanif301
	OSPF	10	2	D	10.1.3.2	Vlanif302
10.1.6.254/32	OSPF	10	2	D	10.1.3.2	Vlanif302
	OSPF	10	2	D	10.1.2.2	Vlanif301
127.0.0.0/8	Direct	0	0	D	127.0.0.1	InLoopBack0
127.0.0.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0

DeviceB、DeviceC、DeviceD 上的检查过程与 DeviceA 上类似。

4. 检查组播协议是否配置成功。

在 DeviceB、DeviceD 上执行 **display pim routing-table** 命令，可以看到组播组 225.0.0.10 的 PIM 路由表项建立成功。

说明

根据动态 RP 竞选规则，如果 C-RP 接口地址掩码、优先级、Hash 计算结果都相同，则选 IP 地址较大的作为 RP。所以选择 DeviceD 的 Loopback1 为 RP 接口。

根据 RPF 检查规则，如果在 IP 路由表里有两条等价的最优路由表项，设备在建立 PIM 路由表项时会选择下一跳地址最大的最优路由表项作为 RPF 路由。所以 DeviceD 选择了下一跳地址是 10.1.4.1、目的网段是 10.1.1.0/24 的路由为到达 10.1.1.0/24 网段的 RPF 路由。

[DeviceB] **display pim routing-table**

VPN-Instance: public net

Total 0 (*, G) entry; 1 (S, G) entry

(10.100.1.1, 225.0.0.10)

RP: 10.4.4.4

Protocol: pim-sm, Flag: SPT ACT

UpTime: 00:00:42

Upstream interface: **Vlanif100**

Upstream neighbor: 10.1.1.3

RPF prime neighbor: 10.1.1.3

Downstream interface(s) information:

Total number of downstreams: 1

1: **Vlanif303**

Protocol: pim-sm, UpTime: 00:00:42, Expires:-

[DeviceD] **display pim routing-table**

VPN-Instance: public net

Total 0 (*, G) entry; 1 (S, G) entry

(10.100.1.1, 225.0.0.10)

RP: 10.4.4.4

Protocol: pim-sm, Flag: SPT ACT

UpTime: 00:00:42

Upstream interface: **Vlanif303**

Upstream neighbor: 10.1.4.1

RPF prime neighbor: 10.1.4.1

Downstream interface(s) information:

Total number of downstreams: 1

1: **Vlanif400**

Protocol: pim-sm, UpTime: 00:00:42, Expires:-

5. 检查 BFD 功能是否配置成功。

- a. 在 DeviceA 上执行 **display ospf bfd session all** 命令，可以看到 OSPF BFD 会话建立成功。

[DeviceA] **display ospf bfd session all**

OSPF Process 1 with Router ID 10.10.1.1

Area 0.0.0.0 interface 10.1.1.1(Vlanif100)'s BFD Sessions

NeighborId:10.2.2.2 AreaId:0.0.0.0 Interface: Vlanif100

BFDState:up rx :1000 tx :1000

Multiplier:3 BFD Local Dis:8196 LocalIpAdd:10.1.1.1

RemoteIpAdd:10.1.1.2 Diagnostic Info:No diagnostic information

Area 0.0.0.0 interface 10.1.1.1(Vlanif100)'s BFD Sessions

NeighborId:5.5.5.5 AreaId:0.0.0.0 Interface: Vlanif100
BFDState:up rx :1000 tx :1000
Multiplier:4 BFD Local Dis:8195 LocalIpAdd:10.1.1.1
RemoteIpAdd:10.1.1.3 Diagnostic Info:No diagnostic information

Area 0.0.0.0 interface 10.1.2.1(Vlanif301)'s BFD Sessions

NeighborId:10.3.3.3 AreaId:0.0.0.0 Interface: Vlanif301
BFDState:up rx :1000 tx :1000
Multiplier:3 BFD Local Dis:8194 LocalIpAdd:10.1.1.1
RemoteIpAdd:10.1.2.2 Diagnostic Info:No diagnostic information

Area 0.0.0.0 interface 10.1.3.1(Vlanif302)'s BFD Sessions

NeighborId:10.4.4.4 AreaId:0.0.0.0 Interface: Vlanif302
BFDState:up rx :1000 tx :1000
Multiplier:3 BFD Local Dis:8193 LocalIpAdd:10.1.1.1
RemoteIpAdd:10.1.3.2 Diagnostic Info:No diagnostic information

DeviceB、DeviceC、DeviceD 上的检查过程与 DeviceA 上类似。

- b. 在 DeviceA 上执行 **display pim bfd session** 命令，可以看到 PIM BFD 会话建立成功。

```
[DeviceA] display pim bfd session
VPN-Instance: public net
Total 4 BFD session Created

Vlanif100 (10.1.1.1): Total 2 BFD session Created

Neighbor  ActTx(ms)  ActRx(ms)  ActMulti  Local/Remote  State
10.1.1.2  1000        1000       3         8192/8192     Up
10.1.1.3  1000        1000       3         8191/8191     Up

Vlanif301 (10.1.2.1): Total 1 BFD session Created

Neighbor  ActTx(ms)  ActRx(ms)  ActMulti  Local/Remote  State
10.1.2.2  1000        1000       3         8193/8193     Up

Vlanif302 (10.1.3.1): Total 1 BFD session Created

Neighbor  ActTx(ms)  ActRx(ms)  ActMulti  Local/Remote  State
10.1.3.2  1000        1000       3         8194/8194     Up
```

DeviceB、DeviceC、DeviceD 上的检查过程与 DeviceA 上类似。

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 100 200 301 302
#
multicast routing-enable
#
bfd
#
interface Vlanif100
 ip address 10.1.1.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.1.253
 vrrp vrid 1 priority 120
 vrrp vrid 1 preempt timer delay 20
 vrrp vrid 2 virtual-ip 10.1.1.254
 pim sm
 pim bfd enable
 ospf bfd enable
#
interface Vlanif301
 ip address 10.1.2.1 255.255.255.0
 pim sm
 pim bfd enable
 ospf bfd enable
#
interface Vlanif302
 ip address 10.1.3.1 255.255.255.0
 pim sm
 pim bfd enable
 ospf bfd enable
#
interface Eth-Trunk1
 trunkport 10GE1/0/2 to 10GE1/0/4
 port link-type trunk
 port trunk allow-pass vlan 100 200
#
interface 10GE1/0/1
```

```
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
eth-trunk 1
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
port link-type trunk
port trunk allow-pass vlan 301
#
interface 10GE1/0/6
port link-type trunk
port trunk allow-pass vlan 302
#
interface LoopBack1
ip address 10.10.1.1 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 10.1.1.0 0.0.0.255
network 10.1.2.0 0.0.0.255
network 10.1.3.0 0.0.0.255
network 10.10.1.1 0.0.0.0
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 100 200 303 304
#
multicast routing-enable
#
bfd
#
```

```
interface Vlanif100
ip address 10.1.1.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.1.253
vrrp vrid 2 virtual-ip 10.1.1.254
vrrp vrid 2 priority 120
vrrp vrid 2 preempt timer delay 20
pim sm
pim bfd enable
ospf bfd enable
#
interface Vlanif303
ip address 10.1.4.1 255.255.255.0
pim sm
pim bfd enable
ospf bfd enable
#
interface Vlanif304
ip address 10.1.5.1 255.255.255.0
pim sm
pim bfd enable
ospf bfd enable
#
interface Eth-Trunk1
trunkport 10GE1/0/2 to 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 100 200
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 100
#
interface 10GE1/0/2
eth-trunk 1
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
port link-type trunk
port trunk allow-pass vlan 303
```

```
#
interface 10GE1/0/6
 port link-type trunk
 port trunk allow-pass vlan 304
#
interface LoopBack1
 ip address 10.2.2.2 255.255.255.255
 pim sm
#
ospf 1
 area 0.0.0.0
 network 10.1.1.0 0.0.0.255
 network 10.1.4.0 0.0.0.255
 network 10.1.5.0 0.0.0.255
 network 10.2.2.2 0.0.0.0
#
return
```

DeviceC

```
#
sysname DeviceC
#
vlan batch 301 304 400 500
#
multicast routing-enable
#
bfd
#
interface Vlanif301
 ip address 10.1.2.2 255.255.255.0
 pim sm
 pim bfd enable
 ospf bfd enable
#
interface Vlanif304
 ip address 10.1.5.2 255.255.255.0
 pim sm
 pim bfd enable
 ospf bfd enable
#
interface Vlanif400
 ip address 10.1.6.1 255.255.255.0
 vrrp vrid 1 virtual-ip 10.1.6.253
```

```
vrp vrid 1 priority 120
vrp vrid 1 preempt timer delay 20
vrp vrid 2 virtual-ip 10.1.6.254
pim sm
pim bfd enable
igmp enable
ospf bfd enable
#
interface Eth-Trunk1
trunkport 10GE1/0/2 to 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 400 500
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 400
stp disable
#
interface 10GE1/0/2
eth-trunk 1
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
port link-type trunk
port trunk allow-pass vlan 301
#
interface 10GE1/0/6
port link-type trunk
port trunk allow-pass vlan 304
#
interface LoopBack1
ip address 10.3.3.3 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 10.1.2.0 0.0.0.255
network 10.1.5.0 0.0.0.255
```

```
network 10.1.6.0 0.0.0.255
network 10.3.3.3 0.0.0.0
#
pim
c-bsr LoopBack1
c-rp LoopBack1
#
return
```

DeviceD

```
#
sysname DeviceD
#
vlan batch 302 303 400 500
#
multicast routing-enable
#
bfd
#
interface Vlanif302
ip address 10.1.3.2 255.255.255.0
pim sm
pim bfd enable
ospf bfd enable
#
interface Vlanif303
ip address 10.1.4.2 255.255.255.0
pim sm
pim bfd enable
ospf bfd enable
#
interface Vlanif400
ip address 10.1.6.2 255.255.255.0
vrrp vrid 1 virtual-ip 10.1.6.253
vrrp vrid 2 virtual-ip 10.1.6.254
vrrp vrid 2 priority 120
vrrp vrid 2 preempt timer delay 20
pim sm
pim bfd enable
igmp enable
ospf bfd enable
#
interface Eth-Trunk1
```

```
trunkport 10GE1/0/2 to 10GE1/0/4
port link-type trunk
port trunk allow-pass vlan 400 500
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 400
stp disable
#
interface 10GE1/0/2
eth-trunk 1
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
port link-type trunk
port trunk allow-pass vlan 303
#
interface 10GE1/0/6
port link-type trunk
port trunk allow-pass vlan 302
#
interface LoopBack1
ip address 10.4.4.4 255.255.255.255
pim sm
#
ospf 1
area 0.0.0.0
network 10.1.3.0 0.0.0.255
network 10.1.4.0 0.0.0.255
network 10.1.6.0 0.0.0.255
network 10.4.4.4 0.0.0.0
#
pim
c-bsr LoopBack1
c-rp LoopBack1
#
return
```


1.1.5.11.2 M-LAG

举例：配置 M-LAG 双归接入二层网络（根桥方式）

举例：配置 M-LAG 双归接入三层网络（V-STP 方式）

举例：配置动态路由接入 M-LAG（V-STP 方式）

举例：配置多级 M-LAG 互联（V-STP 方式）

举例：配置 M-LAG 设备作为 DHCPv4 中继（插入 Option82 选项的子选项）

举例：配置 M-LAG 设备作为 DHCPv4 中继（Option82 选项携带回程地址信息）

1.1.5.11.2.1 举例：配置 M-LAG 双归接入二层网络（根桥方式）

组网需求

如图 1 所示，采用 M-LAG 方式将主机双归接入二层网络。由于用户对于业务的可靠性要求很高，如果主机和接入设备之间做链路聚合只能保证链路级的可靠性，接入设备发生故障时则会导致业务中断。这时用户可以采用跨设备链路聚合技术，正常工作时链路进行负载分担且任何一台设备故障对业务均没有影响，保证业务的高可靠性。由于普通以太网络中存在阻塞端口无法传输 M-LAG 主备设备的心跳报文，这里采用配置 DFS Group 绑定管理网口 IP 地址，保证 M-LAG 主备设备的心跳报文能够正常传输。

图 1 配置 M-LAG 双归接入二层网络组网图

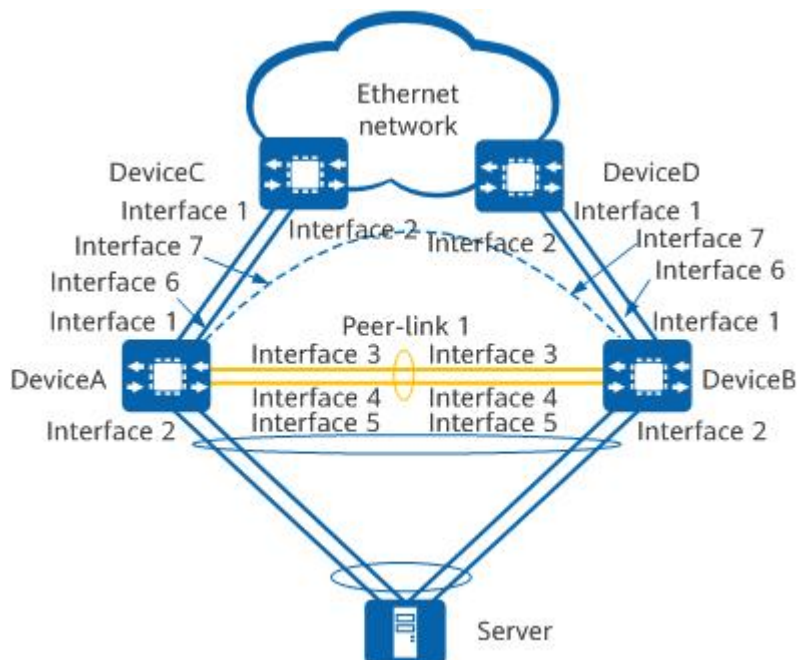
说明

本例中 DeviceA 的 interface1、interface2、interface3、interface4、interface5、interface6 和 interface7 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4，10GE1/0/5，10GE1/0/7 和 mesh 0/0/0。

本例中 DeviceB 的 interface1、interface2、interface3、interface4、interface5、interface6 和 interface7 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4，10GE1/0/5，10GE1/0/7 和 mesh 0/0/0。

本例中 DeviceC 的 interface1 和 interface2 代表 10GE1/0/1 和 10GE1/0/2。

本例中 DeviceD 的 interface1 和 interface2 代表 10GE1/0/1 和 10GE1/0/2。



配置思路

1. 将 DeviceA 和 DeviceB 配置为根桥，配置相同的桥 MAC，保证 M-LAG 主备设备在二层网络中处于根桥地位。
2. 分别在 DeviceA 和 DeviceB 上配置管理网口的 IP 地址，且保证能够三层互通，用于 M-LAG 主备设备间心跳报文的传输。
3. 分别在 DeviceA 和 DeviceB 上配置 M-LAG 特性，实现服务器的双归接入。

操作步骤

1. 将 DeviceA 和 DeviceB 配置为根桥，配置相同的桥 MAC。

说明

如果组成 M-LAG 的设备下行接入的是设备，必须配置根保护功能。

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stp root primary
[DeviceA] stp bridge-address 00e0-fc12-3458 //配置根桥的桥 MAC（M-LAG 主设备的 MAC 地址）
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] trunkport 10ge 1/0/2
[DeviceA-Eth-Trunk1] trunkport 10ge 1/0/5
[DeviceA-Eth-Trunk1] stp edged-port enable
[DeviceA-Eth-Trunk1] quit
```

配置 DeviceB。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname DeviceB
[DeviceB] stp root primary
[DeviceB] stp bridge-address 00e0-fc12-3458 //配置根桥的桥 MAC
[DeviceB] interface eth-trunk 1
[DeviceB-Eth-Trunk1] trunkport 10ge 1/0/2
[DeviceB-Eth-Trunk1] trunkport 10ge 1/0/5
[DeviceB-Eth-Trunk1] stp edged-port enable
[DeviceB-Eth-Trunk1] quit
```

2. 分别配置 DeviceA 和 DeviceB 管理网口的 IP 地址。

DeviceA 和 DeviceB 管理网口需要保证能够三层互通。

配置 DeviceA。

```
[DeviceA] interface meth 0/0/0
[DeviceA-MEth0/0/0] ip address 10.1.1.1 24
[DeviceA-MEth0/0/0] quit
```

配置 DeviceB。

```
[DeviceB] interface meth 0/0/0
[DeviceB-MEth0/0/0] ip address 10.1.1.2 24
[DeviceB-MEth0/0/0] quit
```

3. 在 DeviceA 和 DeviceB 上分别创建 DFS 并绑定管理网口的 IP 地址。

配置 DeviceA。

```
[DeviceA] dfs-group 1
[DeviceA-dfs-group-1] dual-active detection source ip 10.1.1.1 peer 10.1.1.2
[DeviceA-dfs-group-1] priority 150
[DeviceA-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceA-dfs-group-1] quit
```

配置 DeviceB。

```
[DeviceB] dfs-group 1
[DeviceB-dfs-group-1] dual-active detection source ip 10.1.1.2 peer 10.1.1.1
[DeviceB-dfs-group-1] priority 120
[DeviceB-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceB-dfs-group-1] quit
```

4. 配置 DeviceA 和 DeviceB 之间的 peer-link。

配置 DeviceA。

```
[DeviceA] interface eth-trunk 0
[DeviceA-Eth-Trunk0] mode lacp-static
[DeviceA-Eth-Trunk0] trunkport 10ge 1/0/3
[DeviceA-Eth-Trunk0] trunkport 10ge 1/0/4
[DeviceA-Eth-Trunk0] undo stp enable
[DeviceA-Eth-Trunk0] peer-link 1
```

```
[DeviceA-Eth-Trunk0] quit
```

配置 DeviceB。

```
[DeviceB] interface eth-trunk 0
[DeviceB-Eth-Trunk0] mode lacp-static
[DeviceB-Eth-Trunk0] trunkport 10ge 1/0/3
[DeviceB-Eth-Trunk0] trunkport 10ge 1/0/4
[DeviceB-Eth-Trunk0] undo stp enable
[DeviceB-Eth-Trunk0] peer-link 1
[DeviceB-Eth-Trunk0] quit
```

5. 配置 DeviceA 和 DeviceB 连接服务器的 Eth-Trunk 接口加入 VLAN 11 并绑定 DFS Group。
服务器上连接交换机的端口需要绑定在一个聚合链路中且链路聚合模式需要和交换机侧的聚合模式匹配，以交换机侧配置为静态 LACP 模式为例。

配置 DeviceA。

```
[DeviceA] vlan batch 11
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] mode lacp-static
[DeviceA-Eth-Trunk1] port link-type access
[DeviceA-Eth-Trunk1] port default vlan 11
[DeviceA-Eth-Trunk1] dfs-group 1 m-lag 1
[DeviceA-Eth-Trunk1] quit
```

配置 DeviceB。

```
[DeviceB] vlan batch 11
[DeviceB] interface eth-trunk 1
[DeviceB-Eth-Trunk1] mode lacp-static
[DeviceB-Eth-Trunk1] port link-type access
[DeviceB-Eth-Trunk1] port default vlan 11
[DeviceB-Eth-Trunk1] dfs-group 1 m-lag 1
[DeviceB-Eth-Trunk1] quit
```

6. 配置 DeviceA 和 DeviceC 之间链路以及 DeviceB 和 DeviceD 之间链路，并配置接口类型和通过的 VLAN。

配置 DeviceA。

```
[DeviceA] interface eth-trunk 2
[DeviceA-Eth-Trunk2] mode lacp-static
[DeviceA-Eth-Trunk2] port link-type trunk
[DeviceA-Eth-Trunk2] port trunk allow-pass vlan 11
[DeviceA-Eth-Trunk2] trunkport 10ge 1/0/1
[DeviceA-Eth-Trunk2] trunkport 10ge 1/0/7
[DeviceA-Eth-Trunk2] quit
```

配置 DeviceB。

```
[DeviceB] interface eth-trunk 2
```

```
[DeviceB-Eth-Trunk2] mode lacp-static
[DeviceB-Eth-Trunk2] port link-type trunk
[DeviceB-Eth-Trunk2] port trunk allow-pass vlan 11
[DeviceB-Eth-Trunk2] trunkport 10ge 1/0/1
[DeviceB-Eth-Trunk2] trunkport 10ge 1/0/7
[DeviceB-Eth-Trunk2] quit
```

配置 DeviceC。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] vlan batch 11
[DeviceC] interface eth-trunk 2
[DeviceC-Eth-Trunk2] mode lacp-static
[DeviceC-Eth-Trunk2] port link-type trunk
[DeviceC-Eth-Trunk2] port trunk allow-pass vlan 11
[DeviceC-Eth-Trunk2] trunkport 10ge 1/0/1
[DeviceC-Eth-Trunk2] trunkport 10ge 1/0/2
[DeviceC-Eth-Trunk2] quit
```

配置 DeviceD。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] vlan batch 11
[DeviceD] interface eth-trunk 2
[DeviceD-Eth-Trunk2] mode lacp-static
[DeviceD-Eth-Trunk2] port link-type trunk
[DeviceD-Eth-Trunk2] port trunk allow-pass vlan 11
[DeviceD-Eth-Trunk2] trunkport 10ge 1/0/1
[DeviceD-Eth-Trunk2] trunkport 10ge 1/0/2
[DeviceD-Eth-Trunk2] quit
```

检查配置结果

查看 DFS Group 编号为 1 的 M-LAG 信息。

```
[DeviceA] display dfs-group 1 m-lag
*           : Local node
Heart beat state   : OK
Node 1 *
Dfs-Group ID      : 1
Priority           : 150
Dual-active Address : 10.1.1.1
VPN-Instance      : public net
State             : Master
```

```
Causation      : -
System ID      : 00e0-fc12-3456
SysName       : DeviceA
Version       : V600R023C00
Device Type    : S6700
```

Node 2

```
Dfs-Group ID   : 1
Priority       : 120
Dual-active Address : 10.1.1.2
VPN-Instance   : public net
State         : Backup
Causation      : -
System ID      : 00e0-fc12-3457
SysName       : DeviceB
Version       : V600R023C00
Device Type    : S6700
```

查看 DeviceA 上的 M-LAG 信息。

```
[DeviceA] display dfs-group 1 node 1 m-lag brief
```

```
* - Local node
```

M-Lag ID	Interface	Port State	Status	Consistency-check
1	Eth-Trunk 1	Up	active(*)-active	--

Failed reason:

- 1 -- Relationship between vlan and port is inconsistent
- 2 -- STP configuration under the port is inconsistent
- 3 -- STP port priority configuration is inconsistent
- 4 -- LACP mode of M-LAG is inconsistent
- 5 -- M-LAG configuration is inconsistent
- 6 -- The number of M-LAG members is inconsistent
- 7 -- LACP system-id of M-LAG is inconsistent
- 8 -- LACP priority of M-LAG is inconsistent
- 9 -- STP port edged configuration is inconsistent
- 10 -- M-LAG mode configuration is inconsistent

查看 DeviceB 上的 M-LAG 信息。

```
[DeviceB] display dfs-group 1 node 2 m-lag brief
```

```
* - Local node
```

M-Lag ID	Interface	Port State	Status	Consistency-check
1	Eth-Trunk 1	Up	active-active(*)	--

Failed reason:

- 1 -- Relationship between vlan and port is inconsistent
- 2 -- STP configuration under the port is inconsistent
- 3 -- STP port priority configuration is inconsistent
- 4 -- LACP mode of M-LAG is inconsistent
- 5 -- M-LAG configuration is inconsistent
- 6 -- The number of M-LAG members is inconsistent
- 7 -- LACP system-id of M-LAG is inconsistent
- 8 -- LACP priority of M-LAG is inconsistent
- 9 -- STP port edged configuration is inconsistent
- 10 -- M-LAG mode configuration is inconsistent

通过以上显示信息可以看到，“Heart beat state”的状态是“OK”，表明心跳状态正常；DeviceA 作为 Node 1，优先级为 150，“State”的状态是“Master”；DeviceB 作为 Node 2，优先级为 120，“State”的状态是“Backup”。同时“Causation”的状态是“-”，Node 1 的“Port State”状态为“Up”，Node 2 的“Port State”状态为“Up”，且 Node 1 和 Node 2 的 M-LAG 状态均为“active”，表明 M-LAG 的配置正确。

配置文件

DeviceA 的配置脚本

```
#
sysname DeviceA
#
dfs-group 1
priority 150
dual-active detection source ip 10.1.1.1 peer 10.1.1.2
authentication-mode hmac-sha256 password %+%##!!!!!!!!!!!!"!!!!"!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!!!!!9!!!!>fwJ)l0E{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!!!%+%#
#
vlan batch 11
#
stp bridge-address 00e0-fc12-3458
stp root primary
#
interface MEth0/0/0
ip address 10.1.1.1 255.255.255.0
#
interface Eth-Trunk0
mode lacp-static
stp disable
```

```

peer-link 1
#
interface Eth-Trunk1
port default vlan 11
stp edged-port enable
mode lacp-static
dfs-group 1 m-lag 1
#
interface Eth-Trunk2
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 2
#
interface 10GE1/0/7
eth-trunk 2
#
interface 10GE1/0/3
eth-trunk 0
#
interface 10GE1/0/4
eth-trunk 0
#
interface 10GE1/0/5
eth-trunk 1
#
interface 10GE1/0/2
eth-trunk 1
#
return

```

DeviceB 的配置脚本

```

#
sysname DeviceB
#
dfs-group 1
priority 120
dual-active detection source ip 10.1.1.2 peer 10.1.1.1
authentication-mode hmac-sha256 password %+%##!!!!!!!"!!!!*!!!!=I9f8>C{!P_bhB31@7r-
=jrS8c|_"(Bn~#=!!!!!!!!!!!!!!9!!!!kx-6@.tGA(wAt/IQXI6>[g{6YIOi9$!!!!!!!!!!%+%#
#

```



```
vlan batch 11
#
stp bridge-address 00e0-fc12-3458
stp root primary
#
interface MEth0/0/0
 ip address 10.1.1.2 255.255.255.0
#
interface Eth-Trunk0
 mode lacp-static
 stp disable
 peer-link 1
#
interface Eth-Trunk1
 port default vlan 11
 stp edged-port enable
 mode lacp-static
 dfs-group 1 m-lag 1
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 11
 mode lacp-static
#
interface 10GE1/0/1
 eth-trunk 2
#
interface 10GE1/0/7
 eth-trunk 2
#
interface 10GE1/0/3
 eth-trunk 0
#
interface 10GE1/0/4
 eth-trunk 0
#
interface 10GE1/0/5
 eth-trunk 1
#
interface 10GE1/0/2
 eth-trunk 1
#
```

```
return
```

DeviceC 的配置脚本

```
#
sysname DeviceC
#
vlan batch 11
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 11
 mode lacp-static
#
interface 10GE1/0/1
 eth-trunk 2
#
interface 10GE1/0/2
 eth-trunk 2
#
return
```

DeviceD 的配置脚本

```
#
sysname DeviceD
#
vlan batch 11
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 11
 mode lacp-static
#
interface 10GE1/0/1
 eth-trunk 2
#
interface 10GE1/0/2
 eth-trunk 2
#
return
```

1.1.5.11.2.2 举例：配置 M-LAG 双归接入三层网络（V-STP 方式）

组网需求

如图 1 所示，通过配置 M-LAG 双归接入三层网络可以满足以下要求：

当一条接入链路发生故障时，流量可以快速切换到另一条链路，保证可靠性。

为了高效利用带宽，两条链路同时处于 active 状态，可实现使用负载分担的方式转发流量。

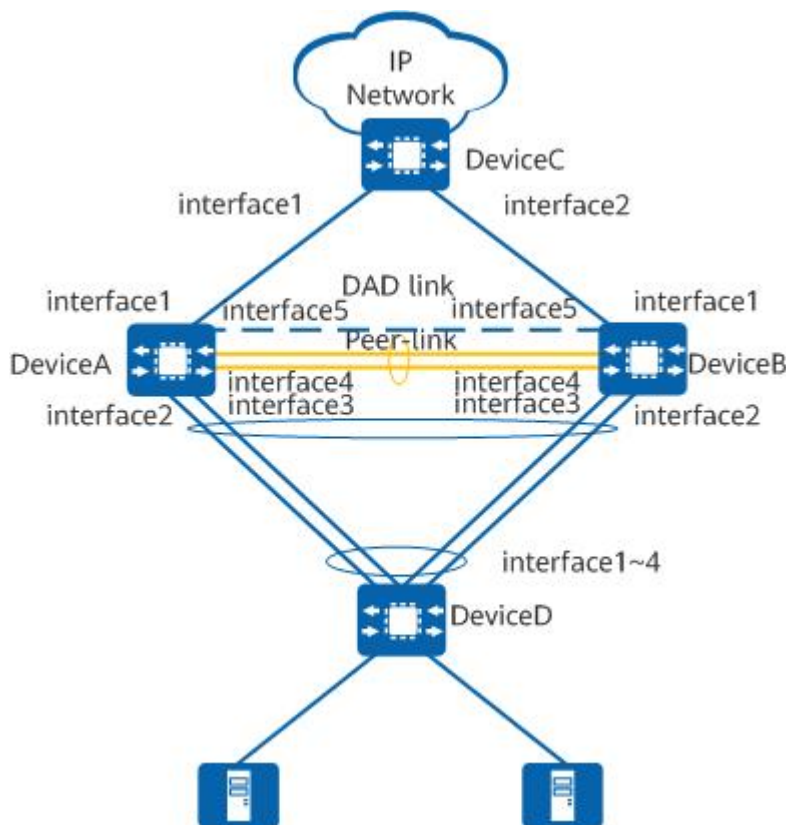
图 1 配置 M-LAG 双归接入三层网图

说明

本例中 DeviceA 的 interface1、interface2、interface3、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceB 的 interface1、interface2、interface3、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceC 的 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

采用如下的思路配置 M-LAG 双归接入 IP 网络：

1. 在 DeviceD 上配置上行接口绑定在一个 Eth-Trunk 中。
2. 分别在 DeviceA 和 DeviceB 上配置 V-STP、创建 DFS Group 并绑定管理网口的 IP 地址、配置 peer-link 和 M-LAG 接口。
3. 分别在 DeviceA 和 DeviceB 上配置 VLANIF 接口 IP 地址和 MAC 地址，作为接入设备的双活网关。
4. 分别在 DeviceA、DeviceB 和 DeviceC 上配置 OSPF 功能，保证三层互通。

说明

在 V-STP 场景下，为防止接口因生成树协议计算结果被阻塞，可以通过配置主接口实现三层互通或者去使能 IP 网络侧的生成树协议。

5. 分别在 DeviceA 和 DeviceB 上配置 Monitor Link 关联上行接口和下行接口，避免因上行链路故障导致用户侧流量无法转发而丢弃。

操作步骤

1. 在 DeviceD 上配置上行接口绑定在一个 Eth-Trunk 中。

配置 DeviceD。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] vlan batch 11
[DeviceD] interface eth-trunk 20
[DeviceD-Eth-Trunk20] mode lacp-static
[DeviceD-Eth-Trunk20] port link-type trunk
[DeviceD-Eth-Trunk20] port trunk allow-pass vlan 11
[DeviceD-Eth-Trunk20] trunkport 10ge 1/0/1 to 1/0/4
[DeviceD-Eth-Trunk20] quit
```

2. 分别在 DeviceA 和 DeviceB 上配置 V-STP、创建 DFS Group 并绑定管理网口的 IP 地址、配置 peer-link 和 M-LAG 接口。

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stp mode rstp
[DeviceA] stp v-stp enable
[DeviceA] interface meth 0/0/0
[DeviceA-MEth0/0/0] ip address 10.200.1.1 24
[DeviceA-MEth0/0/0] quit
[DeviceA] dfs-group 1
[DeviceA-dfs-group-1] dual-active detection source ip 10.200.1.1 peer 10.200.1.2
[DeviceA-dfs-group-1] priority 150
[DeviceA-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceA-dfs-group-1] quit
[DeviceA] interface eth-trunk 1
[DeviceA-Eth-Trunk1] trunkport 10ge 1/0/4
[DeviceA-Eth-Trunk1] trunkport 10ge 1/0/5
[DeviceA-Eth-Trunk1] mode lacp-static
[DeviceA-Eth-Trunk1] peer-link 1
[DeviceA-Eth-Trunk1] port vlan exclude 1
```

```
[DeviceA-Eth-Trunk1] quit
[DeviceA] vlan batch 11
[DeviceA] interface eth-trunk 10
[DeviceA-Eth-Trunk10] mode lacp-static
[DeviceA-Eth-Trunk10] port link-type trunk
[DeviceA-Eth-Trunk10] port trunk allow-pass vlan 11
[DeviceA-Eth-Trunk10] trunkport 10ge 1/0/2
[DeviceA-Eth-Trunk10] trunkport 10ge 1/0/3
[DeviceA-Eth-Trunk10] dfs-group 1 m-lag 1
[DeviceA-Eth-Trunk10] quit
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] stp mode rstp
[DeviceB] stp v-stp enable
[DeviceB] interface meth 0/0/0
[DeviceB-MEth0/0/0] ip address 10.200.1.2 24
[DeviceB-MEth0/0/0] quit
[DeviceB] dfs-group 1
[DeviceB-dfs-group-1] dual-active detection source ip 10.200.1.2 peer 10.200.1.1
[DeviceB-dfs-group-1] priority 120
[DeviceB-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceB-dfs-group-1] quit
[DeviceB] interface eth-trunk 1
[DeviceB-Eth-Trunk1] trunkport 10ge 1/0/4
[DeviceB-Eth-Trunk1] trunkport 10ge 1/0/5
[DeviceB-Eth-Trunk1] mode lacp-static
[DeviceB-Eth-Trunk1] peer-link 1
[DeviceB-Eth-Trunk1] port vlan exclude 1
[DeviceB-Eth-Trunk1] quit
[DeviceB] vlan batch 11
[DeviceB] interface eth-trunk 10
[DeviceB-Eth-Trunk10] mode lacp-static
[DeviceB-Eth-Trunk10] port link-type trunk
[DeviceB-Eth-Trunk10] port trunk allow-pass vlan 11
[DeviceB-Eth-Trunk10] trunkport 10ge 1/0/2
[DeviceB-Eth-Trunk10] trunkport 10ge 1/0/3
[DeviceB-Eth-Trunk10] dfs-group 1 m-lag 1
[DeviceB-Eth-Trunk10] quit
```

3. 分别在 DeviceA 和 DeviceB 上配置 VLANIF 接口 IP 地址和 MAC 地址，作为接入设备的双活网关。
DeviceA 和 DeviceB 的虚拟 IP 和虚拟 MAC 配置要求完全一致。

配置 DeviceA。

```
[DeviceA] interface vlanif 11
[DeviceA-Vlanif11] ip address 10.2.1.1 24
[DeviceA-Vlanif11] mac-address 0000-5e00-0101
[DeviceA-Vlanif11] quit
```

配置 DeviceB。

```
[DeviceB] interface vlanif 11
[DeviceB-Vlanif11] ip address 10.2.1.1 24
[DeviceB-Vlanif11] mac-address 0000-5e00-0101
[DeviceB-Vlanif11] quit
```

4. 分别在 DeviceA、DeviceB 和 DeviceC 上配置 OSPF 功能，保证三层互通。DeviceA、DeviceB 和 DeviceC 的 OSPF 区域号需与 DeviceA、DeviceB 和 DeviceD 的 OSPF 区域号不同。

配置 DeviceA。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] undo portswitch
[DeviceA-10GE1/0/1] ip address 10.3.1.1 24
[DeviceA-10GE1/0/1] quit
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] area 1
[DeviceA-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.1] quit
[DeviceA-ospf-1] quit
```

配置 DeviceB。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] undo portswitch
[DeviceB-10GE1/0/1] ip address 10.4.1.1 24
[DeviceB-10GE1/0/1] quit
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] area 1
[DeviceB-ospf-1-area-0.0.0.1] network 10.2.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.1] quit
[DeviceB-ospf-1] quit
```

配置 DeviceC。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] interface 10ge 1/0/1
[DeviceC-10GE1/0/1] undo portswitch
[DeviceC-10GE1/0/1] ip address 10.3.1.2 24
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10ge 1/0/2
[DeviceC-10GE1/0/2] undo portswitch
[DeviceC-10GE1/0/2] ip address 10.4.1.2 24
[DeviceC-10GE1/0/2] quit
[DeviceC] ospf 1
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] quit

```

5. 分别在 DeviceA 和 DeviceB 上配置 Monitor Link 关联上行接口和下行接口。

配置 DeviceA。

```

[DeviceA] monitor-link group 1
[DeviceA-mtlk-group1] port 10ge 1/0/1 uplink
[DeviceA-mtlk-group1] port eth-trunk 10 downlink 1
[DeviceA-mtlk-group1] quit

```

配置 DeviceB。

```

[DeviceB] monitor-link group 1
[DeviceB-mtlk-group1] port 10ge 1/0/1 uplink
[DeviceB-mtlk-group1] port eth-trunk 10 downlink 1
[DeviceB-mtlk-group1] quit

```

检查配置结果

查看 DFS Group 编号为 1 的 M-LAG 信息。

```

[DeviceA] display dfs-group 1 m-lag
*           : Local node
Heart beat state   : OK
Node 1 *
Dfs-Group ID      : 1
Priority           : 150
Dual-active Address : 10.200.1.1
VPN-Instance      : public net
State              : Master
Causation          : -

```

System ID : 00e0-fc12-3457

SysName : DeviceA

Version : V600R023C00

Device Type : S6700

Node 2

Dfs-Group ID : 1

Priority : 120

Dual-active Address : 10.200.1.2

VPN-Instance : public net

State : **Backup**

Causation : -

System ID : 00e0-fc12-3458

SysName : DeviceB

Version : V600R023C00

Device Type : S6700

查看 DeviceA 上的 M-LAG 信息。

[DeviceA] display dfs-group 1 node 1 m-lag brief

* - Local node

M-Lag ID	Interface	Port State	Status	Consistency-check
1	Eth-Trunk 10	Up	active(*)-active	--

Failed reason:

1 -- Relationship between vlan and port is inconsistent

2 -- STP configuration under the port is inconsistent

3 -- STP port priority configuration is inconsistent

4 -- LACP mode of M-LAG is inconsistent

5 -- M-LAG configuration is inconsistent

6 -- The number of M-LAG members is inconsistent

7 -- LACP system-id of M-LAG is inconsistent

8 -- LACP priority of M-LAG is inconsistent

9 -- STP port edged configuration is inconsistent

10 -- M-LAG mode configuration is inconsistent

查看 DeviceB 上的 M-LAG 信息。

[DeviceB] display dfs-group 1 node 2 m-lag brief

* - Local node

M-Lag ID	Interface	Port State	Status	Consistency-check
1	Eth-Trunk 10	Up	active-active(*)	--

Failed reason:

- 1 -- Relationship between vlan and port is inconsistent
- 2 -- STP configuration under the port is inconsistent
- 3 -- STP port priority configuration is inconsistent
- 4 -- LACP mode of M-LAG is inconsistent
- 5 -- M-LAG configuration is inconsistent
- 6 -- The number of M-LAG members is inconsistent
- 7 -- LACP system-id of M-LAG is inconsistent
- 8 -- LACP priority of M-LAG is inconsistent
- 9 -- STP port edged configuration is inconsistent
- 10 -- M-LAG mode configuration is inconsistent

通过以上显示信息可以看到，“Heart beat state”的状态是“OK”，表明心跳状态正常；DeviceA 作为 Node 1，优先级为 150，“State”的状态是“Master”；DeviceB 作为 Node 2，优先级为 120，“State”的状态是“Backup”。同时“Causation”的状态是“-”，Node 1 的“Port State”状态为“Up”，Node 2 的“Port State”状态为“Up”，且 Node 1 和 Node 2 的 M-LAG 状态均为“active”，表明 M-LAG 的配置正确。

配置文件

DeviceA 的配置脚本

```
#
sysname DeviceA
#
dfs-group 1
priority 150
dual-active detection source ip 10.200.1.1 peer 10.200.1.2
authentication-mode hmac-sha256 password %+%##!!!!!!!!!!!!"!!!!"!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!!!!!9!!!!>fwJ)l0E{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!!!%+%#
#
vlan batch 11
#
stp mode rstp
stp v-stp enable
#
interface Vlanif11
ip address 10.2.1.1 255.255.255.0
mac-address 0000-5e00-0101
#
interface Eth-Trunk1
mode lacp-static
peer-link 1
port vlan exclude 1
```

```
#
interface Eth-Trunk10
 port link-type trunk
 port trunk allow-pass vlan 11
 mode lacp-static
 dfs-group 1 m-lag 1
#
interface MEth0/0/0
 ip address 10.200.1.1 255.255.255.0
#
interface 10GE1/0/1
 undo portswitch
 ip address 10.3.1.1 255.255.255.0
#
interface 10GE1/0/2
 eth-trunk 10
#
interface 10GE1/0/3
 eth-trunk 10
#
interface 10GE1/0/4
 eth-trunk 1
#
interface 10GE1/0/5
 eth-trunk 1
#
monitor-link group 1
 port 10GE1/0/1 uplink
 port Eth-Trunk10 downlink 1
#
ospf 1
 area 0.0.0.0
 network 10.3.1.0 0.0.0.255
 area 0.0.0.1
 network 10.2.1.0 0.0.0.255
#
return
```

DeviceB 的配置脚本

```
#
sysname DeviceB
#
dfs-group 1
```

```
priority 120
dual-active detection source ip 10.200.1.2 peer 10.200.1.1
authentication-mode hmac-sha256 password %+%##!!!!!!"!!!!*!!!!=I9f8>C{!P_bhB31@7r-
=jrS8c|_"(Bn~#=!!!!!!9!!!!kx-6@.tGA(wAt/IQXI6>[g{6YIOi9$!!!!!!%+%#
#
vlan batch 11
#
stp mode rstp
stp v-stp enable
#
interface Vlanif11
ip address 10.2.1.1 255.255.255.0
mac-address 0000-5e00-0101
#
interface Eth-Trunk1
mode lacp-static
peer-link 1
port vlan exclude 1
#
interface Eth-Trunk10
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
dfs-group 1 m-lag 1
#
interface MEth0/0/0
ip address 10.200.1.2 255.255.255.0
#
interface 10GE1/0/1
undo portswitch
ip address 10.4.1.1 255.255.255.0
#
interface 10GE1/0/2
eth-trunk 10
#
interface 10GE1/0/3
eth-trunk 10
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
```

```
eth-trunk 1
#
monitor-link group 1
port 10GE1/0/1 uplink
port Eth-Trunk10 downlink 1
#
ospf 1
area 0.0.0.0
network 10.4.1.0 0.0.0.255
area 0.0.0.1
network 10.2.1.0 0.0.0.255
#
return
```

DeviceC 的配置脚本

```
#
sysname DeviceC
#
interface 10GE1/0/1
undo portswitch
ip address 10.3.1.2 255.255.255.0
#
interface 10GE1/0/2
undo portswitch
ip address 10.4.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.3.1.0 0.0.0.255
network 10.4.1.0 0.0.0.255
#
return
```

DeviceD 的配置脚本

```
#
sysname DeviceD
#
vlan batch 11
#
interface Eth-Trunk20
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
#
```

```
interface 10GE1/0/1
 eth-trunk 20
#
interface 10GE1/0/2
 eth-trunk 20
#
interface 10GE1/0/3
 eth-trunk 20
#
interface 10GE1/0/4
 eth-trunk 20
#
return
```

1.1.5.11.2.3 举例：配置动态路由接入 M-LAG（V-STP 方式）

组网需求

如[图 1](#)所示，DeviceA、DeviceB 和 DeviceC 组成 M-LAG 系统，DeviceB 和 DeviceC 的 M-LAG 端口支持动态路由协议，用户在服务器上配置动态路由通过三层路由方式接入到 M-LAG 系统。

图 1 配置动态路由接入 M-LAG 组网图

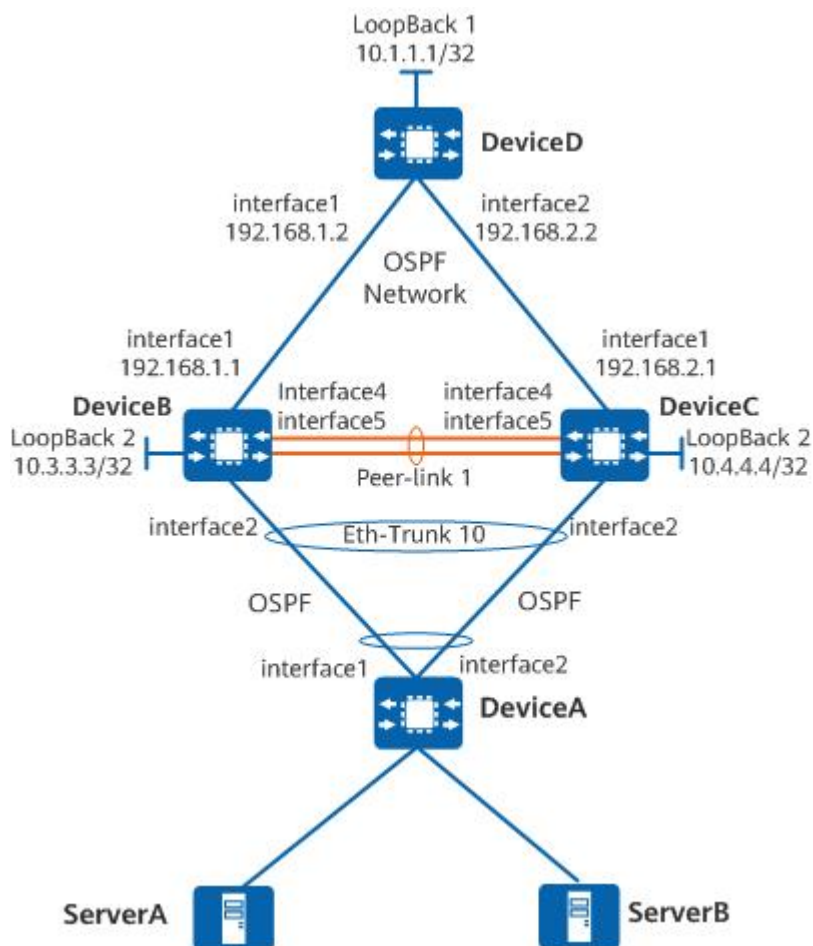
说明

本例中 DeviceA 的 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。

本例中 DeviceB 的 interface1、interface2、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceC 的 interface1、interface2、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceD 的 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

采用如下思路配置动态路由接入 M-LAG：

1. 分别在 DeviceB、DeviceC、DeviceD 上配置路由协议，实现网络三层互通。
2. 创建 Eth-Trunk 接口。
3. 配置 V-STP。
4. 配置 M-LAG：

分别在 DeviceB 和 DeviceC 上配置 DFS Group 并绑定管理网口的 IP 地址。

将 DeviceB 和 DeviceC 之间的链路配置为 peer-link。

分别在 DeviceB 和 DeviceC 上配置绑定 DFS Group 和用户侧 Eth-Trunk 接口。

5. 配置 OSPF over M-LAG 的 IP 地址。
6. OSPF 通过指定 IP 地址与 DeviceA 之间建立 OSPF 邻居。

操作步骤

1. 配置路由协议。

配置 DeviceB。DeviceC 和 DeviceD 的配置与 DeviceB 类似，这里不再赘述。配置 OSPF 时，注意需要发布 32 位 Loopback 接口地址。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface loopback 2
[DeviceB-LoopBack2] ip address 10.3.3.3 32
[DeviceB-LoopBack2] quit
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] undo portswitch
[DeviceB-10GE1/0/1] ip address 192.168.1.1 24
[DeviceB-10GE1/0/1] quit
[DeviceB] ospf 1 router-id 10.11.1.1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 10.3.3.3 0.0.0.0
[DeviceB-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit

```

OSPF 成功配置后，DeviceB、DeviceC、DeviceD 之间可通过 OSPF 协议发现对方的 Loopback 接口的 IP 地址，并能互相 ping 通。

2. 创建 Eth-Trunk 接口，并将以太物理接口加入 Eth-Trunk 接口。

服务器上行连接交换机的端口需要绑定在一个聚合链路中且链路聚合模式需要和交换机侧的聚合模式匹配。

在 DeviceB 上创建 Eth-Trunk，配置为 LACP 模式并加入成员口。DeviceC 的配置与 DeviceB 类似，此处不再赘述。

```

[DeviceB] interface eth-trunk 1
[DeviceB-Eth-Trunk1] mode lacp-static
[DeviceB-Eth-Trunk1] trunkport 10ge 1/0/4
[DeviceB-Eth-Trunk1] trunkport 10ge 1/0/5
[DeviceB-Eth-Trunk1] quit
[DeviceB] interface eth-trunk 10
[DeviceB-Eth-Trunk10] mode lacp-static
[DeviceB-Eth-Trunk10] lacp mixed-rate link enable
[DeviceB-Eth-Trunk10] trunkport 10ge 1/0/2
[DeviceB-Eth-Trunk10] quit

```

3. 配置 V-STP。

配置 DeviceB。

```

[DeviceB] stp mode rstp
[DeviceB] stp v-stp enable

```

配置 DeviceC。

```

[DeviceC] stp mode rstp
[DeviceC] stp v-stp enable

```

4. 分别在 DeviceB 和 DeviceC 上配置 DFS Group 并绑定管理网口的 IP 地址。

DeviceB 和 DeviceC 管理网口需要保证能够三层互通。

配置 DeviceB。DeviceC 的配置与 DeviceB 类似，此处不再赘述。

```
[DeviceB] interface meth 0/0/0
[DeviceB-MEth0/0/0] ip address 10.200.1.1 24
[DeviceB-MEth0/0/0] quit
[DeviceB] dfs-group 1
[DeviceB-dfs-group-1] dual-active detection source ip 10.200.1.1 peer 10.200.2.1
[DeviceB-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceB-dfs-group-1] quit
```

5. 将 DeviceB 和 DeviceC 之间的链路配置为 peer-link。

配置 DeviceB。DeviceC 的配置与 DeviceB 类似，此处不再赘述。

```
[DeviceB] interface eth-trunk 1
[DeviceB-Eth-Trunk1] peer-link 1
[DeviceB-Eth-Trunk1] quit
```

6. 分别在 DeviceB 和 DeviceC 上配置绑定 DFS 和用户侧 Eth-Trunk 接口。

配置 DeviceB。DeviceC 的配置与 DeviceB 类似，此处不再赘述。

```
[DeviceB] interface eth-trunk 10
[DeviceB-Eth-Trunk10] dfs-group 1 m-lag 1
[DeviceB-Eth-Trunk10] quit
```

7. 分别在 DeviceB 和 DeviceC 上配置 OSPF over M-LAG 的 IP 地址。

配置 DeviceB。DeviceC 的配置与 DeviceB 类似，此处不再赘述。

```
[DeviceB] vlan 100
[DeviceB-vlan100] quit
[DeviceB] interface vlanif 100
[DeviceB-Vlanif100] ip address 10.100.0.1 255.255.255.0
[DeviceB-Vlanif100] ospf source sub-address 10.100.0.3
[DeviceB-Vlanif100] m-lag ip address 10.100.0.3 255.255.255.0
[DeviceB-Vlanif100] mac-address 0000-5e00-0101
[DeviceB-Vlanif100] arp proxy enable
[DeviceB-Vlanif100] quit
```

8. OSPF 通过指定 IP 地址与 DeviceA 之间建立 OSPF 邻居。DeviceA、DeviceB 和 DeviceC 的 OSPF 区域号需与 DeviceB、DeviceC 和 DeviceD 的 OSPF 区域号不同。

配置 DeviceB。DeviceC 的配置与 DeviceB 类似，此处不再赘述。

```
[DeviceB] ospf
[DeviceB-ospf-1] area 1
[DeviceB-ospf-1-area-0.0.0.1] network 10.100.0.0 0.0.0.255
[DeviceB-ospf-1-area-0.0.0.1] quit
[DeviceB-ospf-1] quit
```

#配置 DeviceA。


```
[DeviceA] vlan 100
[DeviceA-vlan100] quit
[DeviceA] interface vlanif 100
[DeviceA-Vlanif100] ip address 10.100.0.2 255.255.255.0
[DeviceA-Vlanif100] quit
[DeviceA] ospf 1 router-id 10.11.4.4
[DeviceA-ospf-1] area 1
[DeviceA-ospf-1-area-0.0.0.1] network 10.100.0.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.1] quit
[DeviceA-ospf-1] quit
```

检查配置结果

执行命令 **display dfs-group 1 m-lag**，查看 M-LAG 的相关信息。

```
[DeviceB] display dfs-group 1 m-lag
*           : Local node
Heart beat state   : OK
Node 1 *
  Dfs-Group ID     : 1
  Priority          : 100
  Dual-active Address : 10.200.1.1
  VPN-Instance     : public net
  State            : Master
  Causation        : -
  System ID        : 00e0-fc12-3457
  SysName          : DeviceB
  Version          : V600R023C00
  Device Type      : S6700
Node 2
  Dfs-Group ID     : 1
  Priority          : 100
  Dual-active Address : 10.200.2.1
  VPN-Instance     : public net
  State            : Backup
  Causation        : -
  System ID        : 00e0-fc12-3458
  SysName          : DeviceC
  Version          : V600R023C00
  Device Type      : S6700
```

查看 DeviceB 上的 M-LAG 信息。

```
[DeviceB] display dfs-group 1 node 1 m-lag brief
```

* – Local node

M-Lag ID	Interface	Port State	Status	Consistency-check
1	Eth-Trunk 10	Up	active(*)-active	--

Failed reason:

- 1 -- Relationship between vlan and port is inconsistent
- 2 -- STP configuration under the port is inconsistent
- 3 -- STP port priority configuration is inconsistent
- 4 -- LACP mode of M-LAG is inconsistent
- 5 -- M-LAG configuration is inconsistent
- 6 -- The number of M-LAG members is inconsistent
- 7 -- LACP system-id of M-LAG is inconsistent
- 8 -- LACP priority of M-LAG is inconsistent
- 9 -- STP port edged configuration is inconsistent
- 10 -- M-LAG mode configuration is inconsistent

查看 DeviceC 上的 M-LAG 信息。

[DeviceC] **display dfs-group 1 node 2 m-lag brief**

* – Local node

M-Lag ID	Interface	Port State	Status	Consistency-check
1	Eth-Trunk 10	Up	active(*)-active	--

Failed reason:

- 1 -- Relationship between vlan and port is inconsistent
- 2 -- STP configuration under the port is inconsistent
- 3 -- STP port priority configuration is inconsistent
- 4 -- LACP mode of M-LAG is inconsistent
- 5 -- M-LAG configuration is inconsistent
- 6 -- The number of M-LAG members is inconsistent
- 7 -- LACP system-id of M-LAG is inconsistent
- 8 -- LACP priority of M-LAG is inconsistent
- 9 -- STP port edged configuration is inconsistent
- 10 -- M-LAG mode configuration is inconsistent

在 DeviceB、DeviceC、DeviceA 上执行 **display ospf peer brief** 命令，可查看到 OSPF 中各邻居的信息。

查看 DeviceB 上的 OSPF 邻居信息。

[DeviceB] **display ospf peer brief**

(M) Indicates MADJ interface

OSPF Process 1 with Router ID 10.11.1.1

Peer Statistic Information

Total number of peer(s): 3

Peer(s) in full state: 3

```

-----
Area Id      Interface      Neighbor id    State
0.0.0.0      10GE1/0/1      10.11.3.3     Full
0.0.0.0      Vlanif100      10.11.2.2     Full
0.0.0.1      Vlanif100      10.11.4.4     Full

```

查看 DeviceC 上的 OSPF 邻居信息。

[DeviceC] **display ospf peer brief**

(M) Indicates MADJ interface

OSPF Process 1 with Router ID 10.11.2.2

Peer Statistic Information

Total number of peer(s): 3

Peer(s) in full state: 3

```

-----
Area Id      Interface      Neighbor id    State
0.0.0.0      10GE1/0/1      10.11.3.3     Full
0.0.0.0      Vlanif100      10.11.1.1     Full
0.0.0.1      Vlanif100      10.11.4.4     Full

```

查看 DeviceA 上的 OSPF 邻居信息。

[DeviceA] **display ospf peer brief**

(M) Indicates MADJ interface

OSPF Process 1 with Router ID 10.11.4.4

Peer Statistic Information

Total number of peer(s): 2

Peer(s) in full state: 2

```

-----
Area Id      Interface      Neighbor id    State
0.0.0.1      Vlanif100      10.11.1.1     Full
0.0.0.1      Vlanif100      10.11.2.2     Full

```

配置文件

DeviceB 的配置脚本

```

#
sysname DeviceB
#
dfs-group 1
dual-active detection source ip 10.200.1.1 peer 10.200.2.1
authentication-mode hmac-sha256 password %+%##!!!!!!"!!!!"!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!9!!!!>fwJ)I0E{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!%+%#
#

```

```
vlan batch 100
#
stp mode rstp
stp v-stp enable
#
interface Vlanif100
ip address 10.100.0.1 255.255.255.0
ospf source sub-address 10.100.0.3
mac-address 0000-5e00-0101
m-lag ip address 10.100.0.3 255.255.255.0
arp proxy enable
#
interface Eth-Trunk1
mode lacp-static
peer-link 1
#
interface Eth-Trunk10
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
mode lacp-static
lacp mixed-rate link enable
dfs-group 1 m-lag 1
#
interface MEth0/0/0
ip address 10.200.1.1 255.255.255.0
#
interface 10GE1/0/1
undo portswitch
ip address 192.168.1.1 255.255.255.0
#
interface 10GE1/0/2
eth-trunk 10
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
eth-trunk 1
#
interface LoopBack2
ip address 10.3.3.3 255.255.255.255
#
```

```

ospf 1 router-id 10.11.1.1
area 0.0.0.0
network 10.3.3.3 0.0.0.0
network 192.168.1.0 0.0.0.255
area 0.0.0.1
network 10.100.0.0 0.0.0.255
#
return

```

DeviceC 的配置脚本

```

#
sysname DeviceC
#
dfs-group 1
dual-active detection source ip 10.200.2.1 peer 10.200.1.1
authentication-mode hmac-sha256 password %+%##!!!!!!!"!!!!!!!"*!!!!=I9f8>C{!P_bhB31@7r-
=jrS8c|_"(Bn~#=!!!!!!!!!!!!!!9!!!!kx-6@.tGA(wAt/IQXI6>[g{6YIOi9$!!!!!!!!!!%+%#
#
vlan batch 100
#
stp mode rstp
stp v-stp enable
#
interface Vlanif100
ip address 10.100.0.1 255.255.255.0
ospf source sub-address 10.100.0.4
mac-address 0000-5e00-0101
m-lag ip address 10.100.0.4 255.255.255.0
arp proxy enable
#
interface Eth-Trunk1
mode lacp-static
peer-link 1
#
interface Eth-Trunk10
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
mode lacp-static
lacp mixed-rate link enable
dfs-group 1 m-lag 1
#
interface MEth0/0/0

```

```
ip address 10.200.2.1 255.255.255.0
#
interface 10GE1/0/1
undo portswitch
ip address 192.168.2.1 255.255.255.0
#
interface 10GE1/0/2
eth-trunk 10
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
eth-trunk 1
#
interface LoopBack2
ip address 10.4.4.4 255.255.255.255
#
ospf 1 router-id 10.11.2.2
area 0.0.0.0
network 10.4.4.4 0.0.0.0
network 192.168.2.0 0.0.0.255
area 0.0.0.1
network 10.100.0.0 0.0.0.255
#
return
```

DeviceD 的配置脚本

```
#
sysname DeviceD
#
interface 10GE1/0/1
undo portswitch
ip address 192.168.1.2 255.255.255.0
#
interface 10GE1/0/2
undo portswitch
ip address 192.168.2.2 255.255.255.0
#
interface LoopBack1
ip address 10.1.1.1 255.255.255.255
#
ospf 1 router-id 10.11.3.3
```

```
area 0.0.0.0
network 10.1.1.1 0.0.0.0
network 192.168.1.0 0.0.0.255
network 192.168.2.0 0.0.0.255
#
return
```

DeviceA 的配置脚本

```
#
sysname DeviceA
#
vlan batch 100
#
interface Vlanif100
ip address 10.100.0.2 255.255.255.0
#
interface Eth-Trunk10
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 100
mode lacp-static
lacp mixed-rate link enable
#
interface 10GE1/0/1
eth-trunk 10
#
interface 10GE1/0/2
eth-trunk 10
#
ospf 1 router-id 10.11.4.4
area 0.0.0.1
network 10.100.0.0 0.0.0.255
#
return
```

1.1.5.11.2.4 举例：配置多级 M-LAG 互联（V-STP 方式）

组网需求

如图 1 所示，多级 M-LAG 互联可以在保证可靠性、提供链路利用率的同时扩展双归接入的网络规模，满足客户的需求。同时汇聚层设备作为双活网关，核心层设备和汇聚层设备之间采用交叉连线方式，保证设备级可靠性。服务器以负载分担或主备方式接入，服务器负载分担接入时，推荐 M-LAG 使用双活模式，服务器主备接

入时，推荐 M-LAG 使用主备模式。本例中采用服务器以负载分担方式接入来进行说明。接入层和汇聚层 M-LAG 设备之间通过单独链路作为双主检测链路，提升可靠性。

图 1 配置多级 M-LAG 互联组网图

说明

本例中的 interface1、interface2、interface3、interface4、interface5、interface6 和 interface7 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4，10GE1/0/5，10GE1/0/6 和 10GE1/0/7。

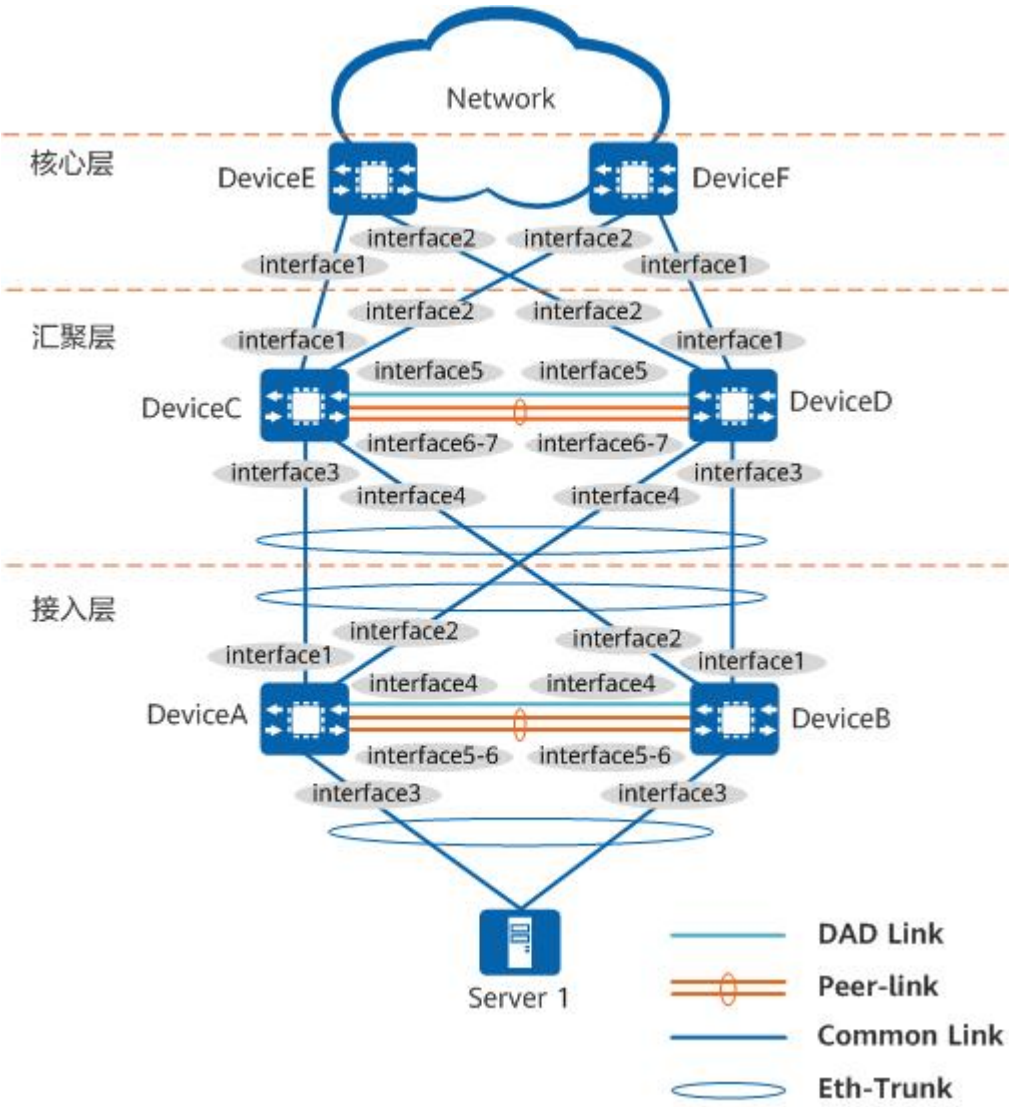


表 1 数据规划表

设备名称	接口	IP 地址	虚拟 MAC 地址
DeviceA	10GE1/0/4	10.1.1.1/24	–
DeviceB	10GE1/0/4	10.1.1.2/24	–
DeviceC	10GE1/0/1	10.4.1.1/24	–
	10GE1/0/2	10.5.1.1/24	–
	VLANIF11	10.3.1.1/24	0000-5e00-0110

表 1 数据规划表

设备名称	接口	IP 地址	虚拟 MAC 地址
	VLANIF100	10.10.10.1/30	–
	10GE1/0/5	10.2.1.1/24	–
DeviceD	10GE1/0/1	10.6.1.1/24	–
	10GE1/0/2	10.7.1.1/24	–
	VLANIF11	10.3.1.1/24	0000–5e00–0110
	VLANIF100	10.10.10.2/30	–
	10GE1/0/5	10.2.1.2/24	–
DeviceE	10GE1/0/1	10.4.1.2/24	–
	10GE1/0/2	10.7.1.2/24	–
DeviceF	10GE1/0/1	10.6.1.2/24	–
	10GE1/0/2	10.5.1.2/24	–

配置思路

采用如下的思路配置多级 M-LAG 互联：

- 1. 在接入层 DeviceA 和 DeviceB 上配置 M-LAG、配置接入层与汇聚层级联链路、配置服务器接入。
- 2. 在汇聚层 DeviceC 和 DeviceD 上配置 M-LAG、配置汇聚层与接入层级联链路、配置三层网关、配置出口网络。
- 3. 在核心层 DeviceE 和 DeviceF 上配置接口 IP 地址、使能 OSPF 功能，实现与汇聚层的三层互通。

操作步骤

1. 配置接入层设备 DeviceA 和 DeviceB。

- a. 配置 M-LAG。
配置 V-STP 方式 M-LAG。
配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] stp mode rstp
[DeviceA] stp v-stp enable
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] stp mode rstp
[DeviceB] stp v-stp enable
```

部署独立直连物理链路，用于 M-LAG 心跳检测。

配置 DeviceA。

```
[DeviceA] interface 10GE1/0/4
[DeviceA-10GE1/0/4] undo portswitch
[DeviceA-10GE1/0/4] ip address 10.1.1.1 24
[DeviceA-10GE1/0/4] m-lag unpaired-port reserved
[DeviceA-10GE1/0/4] quit
```

配置 DeviceB。

```
[DeviceB] interface 10GE1/0/4
[DeviceB-10GE1/0/4] undo portswitch
[DeviceB-10GE1/0/4] ip address 10.1.1.2 24
[DeviceB-10GE1/0/4] m-lag unpaired-port reserved
[DeviceB-10GE1/0/4] quit
```

配置 DFS Group 并绑定 IP 地址。

配置 DeviceA。

```
[DeviceA] dfs-group 1
[DeviceA-dfs-group-1] priority 150
[DeviceA-dfs-group-1] dual-active detection source ip 10.1.1.1 peer 10.1.1.2
[DeviceA-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceA-dfs-group-1] quit
```

配置 DeviceB。

```
[DeviceA] dfs-group 1
[DeviceA-dfs-group-1] priority 120
[DeviceA-dfs-group-1] dual-active detection source ip 10.1.1.2 peer 10.1.1.1
[DeviceA-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceA-dfs-group-1] quit
```

配置 M-LAG 的 peer-link 口。

配置 DeviceA。

```
[DeviceA] interface Eth-Trunk0
[DeviceA-Eth-Trunk0] trunkport 10GE1/0/5
[DeviceA-Eth-Trunk0] trunkport 10GE1/0/6
[DeviceA-Eth-Trunk0] mode lacp-static
[DeviceA-Eth-Trunk0] peer-link 1
[DeviceA-Eth-Trunk0] port vlan exclude 1
[DeviceA-Eth-Trunk0] quit
```

配置 DeviceB。

```
[DeviceB] interface Eth-Trunk0
[DeviceB-Eth-Trunk0] trunkport 10GE1/0/5
[DeviceB-Eth-Trunk0] trunkport 10GE1/0/6
[DeviceB-Eth-Trunk0] mode lacp-static
[DeviceB-Eth-Trunk0] peer-link 1
[DeviceB-Eth-Trunk0] port vlan exclude 1
[DeviceB-Eth-Trunk0] quit
```

b. 配置接入层与汇聚层级联链路。

配置 DeviceA。

```
[DeviceA] vlan batch 11
[DeviceA] interface Eth-Trunk10
[DeviceA-Eth-Trunk10] trunkport 10GE1/0/1
[DeviceA-Eth-Trunk10] trunkport 10GE1/0/2
[DeviceA-Eth-Trunk10] mode lacp-static
[DeviceA-Eth-Trunk10] port link-type trunk
[DeviceA-Eth-Trunk10] undo port trunk allow-pass vlan 1
[DeviceA-Eth-Trunk10] port trunk allow-pass vlan 11
[DeviceA-Eth-Trunk10] dfs-group 1 m-lag 10
[DeviceA-Eth-Trunk10] quit
```

配置 DeviceB。

```
[DeviceB] vlan batch 11
[DeviceB] interface Eth-Trunk10
[DeviceB-Eth-Trunk10] trunkport 10GE1/0/1
[DeviceB-Eth-Trunk10] trunkport 10GE1/0/2
[DeviceB-Eth-Trunk10] mode lacp-static
[DeviceB-Eth-Trunk10] port link-type trunk
[DeviceB-Eth-Trunk10] undo port trunk allow-pass vlan 1
[DeviceB-Eth-Trunk10] port trunk allow-pass vlan 11
[DeviceB-Eth-Trunk10] dfs-group 1 m-lag 10
[DeviceB-Eth-Trunk10] quit
```

c. 配置服务器接入。

配置 DeviceA。

```
[DeviceA] interface Eth-Trunk1
[DeviceA-Eth-Trunk1] trunkport 10GE1/0/3
[DeviceA-Eth-Trunk1] mode lacp-static
[DeviceA-Eth-Trunk1] port link-type trunk
[DeviceA-Eth-Trunk1] undo port trunk allow-pass vlan 1
[DeviceA-Eth-Trunk1] port trunk allow-pass vlan 11
[DeviceA-Eth-Trunk1] dfs-group 1 m-lag 1
[DeviceA-Eth-Trunk1] quit
```

配置 DeviceB。

```
[DeviceB] interface Eth-Trunk1
[DeviceB-Eth-Trunk1] trunkport 10GE1/0/3
[DeviceB-Eth-Trunk1] mode lacp-static
[DeviceB-Eth-Trunk1] port link-type trunk
[DeviceB-Eth-Trunk1] undo port trunk allow-pass vlan 1
[DeviceB-Eth-Trunk1] port trunk allow-pass vlan 11
[DeviceB-Eth-Trunk1] dfs-group 1 m-lag 1
[DeviceB-Eth-Trunk1] quit
```

2. 配置汇聚层设备 DeviceC 和 DeviceD。

a. 配置 M-LAG。

配置 V-STP 方式 M-LAG。

配置 DeviceC。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceC
[DeviceC] stp mode rstp
[DeviceC] stp v-stp enable
```

配置 DeviceD。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceD
[DeviceD] stp mode rstp
[DeviceD] stp v-stp enable
```

部署独立直连物理链路，用于 M-LAG 心跳检测。

配置 DeviceC。

```
[DeviceC] interface 10GE1/0/5
[DeviceC-10GE1/0/5] undo portswitch
[DeviceC-10GE1/0/5] ip address 10.2.1.1 24
[DeviceC-10GE1/0/5] m-lag unpaired-port reserved
[DeviceC-10GE1/0/5] quit
```

配置 DeviceD。

```
[DeviceD] interface 10GE1/0/5
[DeviceD-10GE1/0/5] undo portswitch
[DeviceD-10GE1/0/5] ip address 10.2.1.2 24
[DeviceD-10GE1/0/5] m-lag unpaired-port reserved
[DeviceD-10GE1/0/5] quit
```

配置 DFS Group 并绑定 IP 地址。

配置 DeviceC。

```
[DeviceC] dfs-group 1
[DeviceC-dfs-group-1] priority 150
```

```
[DeviceC-dfs-group-1] dual-active detection source ip 10.2.1.1 peer 10.2.1.2
[DeviceC-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceC-dfs-group-1] quit
```

配置 DeviceD。

```
[DeviceD] dfs-group 1
[DeviceD-dfs-group-1] priority 120
[DeviceD-dfs-group-1] dual-active detection source ip 10.2.1.2 peer 10.2.1.1
[DeviceD-dfs-group-1] authentication-mode hmac-sha256 password YsHsjx_202206
[DeviceD-dfs-group-1] quit
```

配置 M-LAG 的 peer-link 口。

配置 DeviceC。

```
[DeviceC] interface Eth-Trunk0
[DeviceC-Eth-Trunk0] trunkport 10GE1/0/6
[DeviceC-Eth-Trunk0] trunkport 10GE1/0/7
[DeviceC-Eth-Trunk0] mode lacp-static
[DeviceC-Eth-Trunk0] peer-link 1
[DeviceC-Eth-Trunk0] port vlan exclude 1
[DeviceC-Eth-Trunk0] quit
```

配置 DeviceD。

```
[DeviceD] interface Eth-Trunk0
[DeviceD-Eth-Trunk0] trunkport 10GE1/0/6
[DeviceD-Eth-Trunk0] trunkport 10GE1/0/7
[DeviceD-Eth-Trunk0] mode lacp-static
[DeviceD-Eth-Trunk0] peer-link 1
[DeviceD-Eth-Trunk0] port vlan exclude 1
[DeviceD-Eth-Trunk0] quit
```

b. 配置汇聚层与接入层级联链路。

配置 DeviceC。

```
[DeviceC] vlan batch 11
[DeviceC] interface Eth-Trunk10
[DeviceC-Eth-Trunk10] trunkport 10GE1/0/3
[DeviceC-Eth-Trunk10] trunkport 10GE1/0/4
[DeviceC-Eth-Trunk10] mode lacp-static
[DeviceC-Eth-Trunk10] port link-type trunk
[DeviceC-Eth-Trunk10] undo port trunk allow-pass vlan 1
[DeviceC-Eth-Trunk10] port trunk allow-pass vlan 11
[DeviceC-Eth-Trunk10] dfs-group 1 m-lag 10
[DeviceC-Eth-Trunk10] quit
```

配置 DeviceD。

```
[DeviceD] vlan batch 11
```

```
[DeviceD] interface Eth-Trunk10
[DeviceD-Eth-Trunk10] trunkport 10GE1/0/3
[DeviceD-Eth-Trunk10] trunkport 10GE1/0/4
[DeviceD-Eth-Trunk10] mode lacp-static
[DeviceD-Eth-Trunk10] port link-type trunk
[DeviceD-Eth-Trunk10] undo port trunk allow-pass vlan 1
[DeviceD-Eth-Trunk10] port trunk allow-pass vlan 11
[DeviceD-Eth-Trunk10] dfs-group 1 m-lag 10
[DeviceD-Eth-Trunk10] quit
```

- c. 配置三层网关。DeviceC 和 DeviceD 上配置 VLANIF 接口 IP 地址和 MAC 地址要求完全一致，作为接入层的双活网关。

配置 DeviceC。

```
[DeviceC] interface vlanif 11
[DeviceC-Vlanif11] ip address 10.3.1.1 24
[DeviceC-Vlanif11] mac-address 0000-5e00-0110
[DeviceC-Vlanif11] quit
```

配置 DeviceD。

```
[DeviceD] interface vlanif 11
[DeviceD-Vlanif11] ip address 10.3.1.1 24
[DeviceD-Vlanif11] mac-address 0000-5e00-0110
[DeviceD-Vlanif11] quit
```

- d. 配置出口网络。复用 peer-link 物理链路作为 DeviceC 与 DeviceD 之间出口逃生路径，通过 peer-link 上配置专用的 VLANIF 接口进行三层互联。

配置 DeviceC。

```
[DeviceC] interface 10GE1/0/1
[DeviceC-10GE1/0/1] undo portswitch
[DeviceC-10GE1/0/1] ip address 10.4.1.1 24
[DeviceC-10GE1/0/1] quit
[DeviceC] interface 10GE1/0/2
[DeviceC-10GE1/0/2] undo portswitch
[DeviceC-10GE1/0/2] ip address 10.5.1.1 24
[DeviceC-10GE1/0/2] quit
[DeviceC] vlan batch 100
[DeviceC] interface vlanif 100
[DeviceC-Vlanif100] ip address 10.10.10.1 30
[DeviceC-Vlanif100] ospf cost 10000
[DeviceC-Vlanif100] quit
[DeviceC] ospf 1
[DeviceC-ospf-1] area 0
[DeviceC-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
```

```
[DeviceC-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[DeviceC-ospf-1-area-0.0.0.0] network 10.10.10.0 0.0.0.3
[DeviceC-ospf-1-area-0.0.0.0] quit
[DeviceC-ospf-1] quit
```

配置 DeviceD。

```
[DeviceD] interface 10GE1/0/1
[DeviceD-10GE1/0/1] undo portswitch
[DeviceD-10GE1/0/1] ip address 10.6.1.1 24
[DeviceD-10GE1/0/1] quit
[DeviceD] interface 10GE1/0/2
[DeviceD-10GE1/0/2] undo portswitch
[DeviceD-10GE1/0/2] ip address 10.7.1.1 24
[DeviceD-10GE1/0/2] quit
[DeviceD] interface vlanif 100
[DeviceD-Vlanif100] ip address 10.10.10.2 30
[DeviceD-Vlanif100] ospf cost 10000
[DeviceD-Vlanif100] quit
[DeviceD] ospf 1
[DeviceD-ospf-1] area 0
[DeviceD-ospf-1-area-0.0.0.0] network 10.3.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 10.7.1.0 0.0.0.255
[DeviceD-ospf-1-area-0.0.0.0] network 10.10.10.0 0.0.0.3
[DeviceD-ospf-1-area-0.0.0.0] quit
[DeviceD-ospf-1] quit
```

3. 配置核心层设备 DeviceE 和 DeviceF。

配置 DeviceE。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceE
[DeviceE] interface 10GE1/0/1
[DeviceE-10GE1/0/1] undo portswitch
[DeviceE-10GE1/0/1] ip address 10.4.1.2 24
[DeviceE-10GE1/0/1] quit
[DeviceE] interface 10GE1/0/2
[DeviceE-10GE1/0/2] undo portswitch
[DeviceE-10GE1/0/2] ip address 10.7.1.2 24
[DeviceE-10GE1/0/2] quit
[DeviceE] ospf 1
[DeviceE-ospf-1] area 0
[DeviceE-ospf-1-area-0.0.0.0] network 10.4.1.0 0.0.0.255
[DeviceE-ospf-1-area-0.0.0.0] network 10.7.1.0 0.0.0.255
```

```
[DeviceE-ospf-1-area-0.0.0.0] quit
[DeviceE-ospf-1] quit
```

配置 DeviceF。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceF
[DeviceF] interface 10GE1/0/1
[DeviceF-10GE1/0/1] undo portswitch
[DeviceF-10GE1/0/1] ip address 10.6.1.2 24
[DeviceF-10GE1/0/1] quit
[DeviceF] interface 10GE1/0/2
[DeviceF-10GE1/0/2] undo portswitch
[DeviceF-10GE1/0/2] ip address 10.5.1.2 24
[DeviceF-10GE1/0/2] quit
[DeviceF] ospf 1
[DeviceF-ospf-1] area 0
[DeviceF-ospf-1-area-0.0.0.0] network 10.5.1.0 0.0.0.255
[DeviceF-ospf-1-area-0.0.0.0] network 10.6.1.0 0.0.0.255
[DeviceF-ospf-1-area-0.0.0.0] quit
[DeviceF-ospf-1] quit
```

检查配置结果

执行命令 **display dfs-group 1 m-lag** 查看 M-LAG 状态。正常情况下，会显示两台成员设备的状态，一台为“Master”，另一台为“Backup”。

查看接入层 M-LAG 状态。

```
[DeviceA] display dfs-group 1 m-lag
*                : Local node
Heart beat state  : OK
Node 1 *
Dfs-Group ID     : 1
Priority          : 150
Dual-active Address : 10.1.1.1
VPN-Instance     : public net
State            : Master
Causation        : -
System ID        : 00e0-fc12-3457
SysName          : DeviceA
Version          : V600R023C00
Device Type      : S6700
Node 2
Dfs-Group ID     : 1
Priority          : 120
```



```
Dual-active Address : 10.1.1.2
VPN-Instance      : public net
State             : Backup
Causation         : -
System ID         : 00e0-fc12-3458
SysName           : DeviceB
Version           : V600R023C00
Device Type       : S6700
```

查看汇聚层 M-LAG 状态。

```
[DeviceC] display dfs-group 1 m-lag
```

```
*           : Local node
```

```
Heart beat state : OK
```

Node 1 *

```
Dfs-Group ID    : 1
Priority         : 150
Dual-active Address : 10.2.1.1
VPN-Instance     : public net
State           : Master
Causation       : -
System ID       : 00e0-fc12-3459
SysName         : DeviceC
Version         : V600R023C00
Device Type     : S6700
```

Node 2

```
Dfs-Group ID    : 1
Priority         : 120
Dual-active Address : 10.2.1.2
VPN-Instance     : public net
State           : Backup
Causation       : -
System ID       : 00e0-fc12-3460
SysName         : DeviceD
Version         : V600R023C00
Device Type     : S6700
```

执行命令 **display dfs-group 1 node 1 m-lag [brief]** 查看 M-LAG 链路聚合组的状态。

查看 DeviceA 的 M-LAG 链路聚合组的状态。

```
[DeviceA] display dfs-group 1 node 1 m-lag brief
```

```
* - Local node
```

M-Lag ID	Interface	Port State	Status	Consistency-check
1	Eth-Trunk 1	Up	active(*)-active	success

```
10 Eth-Trunk 10 Up active(*)-active success
.....
```

查看 DeviceC 的 M-LAG 链路聚合组的状态。

```
[DeviceC] display dfs-group 1 node 1 m-lag brief
```

```
* - Local node
```

```
M-Lag ID   Interface   Port State   Status           Consistency-check
10 Eth-Trunk 10 Up active(*)-active success
.....
```

配置脚本

DeviceA 的配置脚本

```
#
sysname DeviceA
#
dfs-group 1
priority 150
dual-active detection source ip 10.1.1.1 peer 10.1.1.2
authentication-mode hmac-sha256 password %+%##!!!!!!!!!!!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!!!9!!!!>fwJ)I0E{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!!!!!%+%#
#
vlan batch 11
#
stp mode rstp
stp v-stp enable
#
interface Eth-Trunk0
mode lacp-static
peer-link 1
port vlan exclude 1
#
interface Eth-Trunk1
mode lacp-static
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 11
dfs-group 1 m-lag 1
#
interface Eth-Trunk10
mode lacp-static
port link-type trunk
```

```
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 11
dfs-group 1 m-lag 10
#
interface 10GE1/0/1
eth-trunk 10
#
interface 10GE1/0/2
eth-trunk 10
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
undo portswitch
ip address 10.1.1.1 255.255.255.0
m-lag unpaired-port reserved
#
interface 10GE1/0/5
eth-trunk 0
#
interface 10GE1/0/6
eth-trunk 0
#
return
```

DeviceB 的配置脚本

```
#
sysname DeviceB
#
dfs-group 1
priority 120
dual-active detection source ip 10.1.1.2 peer 10.1.1.1
authentication-mode hmac-sha256 password %+%##!!!!!!!!!!!!!!"!!!!"!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!!!!!9!!!!>fwJ)l0E{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!!!!!%+%#
#
vlan batch 11
#
stp mode rstp
stp v-stp enable
#
interface Eth-Trunk0
mode lacp-static
```

```
peer-link 1
port vlan exclude 1
#
interface Eth-Trunk1
mode lacp-static
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 11
dfs-group 1 m-lag 1
#
interface Eth-Trunk10
mode lacp-static
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 11
dfs-group 1 m-lag 10
#
interface 10GE1/0/1
eth-trunk 10
#
interface 10GE1/0/2
eth-trunk 10
#
interface 10GE1/0/3
eth-trunk 1
#
interface 10GE1/0/4
undo portswitch
ip address 10.1.1.2 255.255.255.0
m-lag unpaired-port reserved
#
interface 10GE1/0/5
eth-trunk 0
#
interface 10GE1/0/6
eth-trunk 0
#
return
```

DeviceC 的配置脚本

```
#
sysname DeviceC
#
```

```
dfs-group 1
priority 150
dual-active detection source ip 10.2.1.1 peer 10.2.1.2
authentication-mode hmac-sha256 password %+%##!!!!!!!"!!!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!!!9!!!!>fwJ)l0E{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!%+%#
#
vlan batch 11 100
#
stp mode rstp
stp v-stp enable
#
interface Vlanif11
ip address 10.3.1.1 255.255.255.0
mac-address 0000-5e00-0110
#
interface Vlanif100
ip address 10.10.10.1 255.255.255.252
ospf cost 10000
#
interface Eth-Trunk0
mode lacp-static
peer-link 1
port vlan exclude 1
#
interface Eth-Trunk10
mode lacp-static
port link-type trunk
undo port trunk allow-pass vlan 1
port trunk allow-pass vlan 11
dfs-group 1 m-lag 10
#
interface 10GE1/0/1
undo portswitch
ip address 10.4.1.1 255.255.255.0
#
interface 10GE1/0/2
undo portswitch
ip address 10.5.1.1 255.255.255.0
#
interface 10GE1/0/3
eth-trunk 10
#
interface 10GE1/0/4
```

```
eth-trunk 10
#
interface 10GE1/0/5
undo portswitch
ip address 10.2.1.1 255.255.255.0
m-lag unpaired-port reserved
#
interface 10GE1/0/6
eth-trunk 0
#
interface 10GE1/0/7
eth-trunk 0
#
ospf 1
area 0.0.0.0
network 10.3.1.0 0.0.0.255
network 10.4.1.0 0.0.0.255
network 10.5.1.0 0.0.0.255
network 10.10.10.0 0.0.0.3
#
return
```

DeviceD 的配置脚本

```
#
sysname DeviceD
#
dfs-group 1
priority 120
dual-active detection source ip 10.2.1.2 peer 10.2.1.1
authentication-mode hmac-sha256 password %+%##!!!!!!!!!!!!"!!!!"!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!!!!!9!!!!>fwJ)l0E{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!!!%+%#
#
vlan batch 11 100
#
stp mode rstp
stp v-stp enable
#
interface Vlanif11
ip address 10.3.1.1 255.255.255.0
mac-address 0000-5e00-0110
#
interface Vlanif100
ip address 10.10.10.2 255.255.255.252
```

```
ospf cost 10000
#
interface Eth-Trunk0
 mode lacp-static
 peer-link 1
 port vlan exclude 1
#
interface Eth-Trunk10
 mode lacp-static
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 11
 dfs-group 1 m-lag 10
#
interface 10GE1/0/1
 undo portswitch
 ip address 10.6.1.1 255.255.255.0
#
interface 10GE1/0/2
 undo portswitch
 ip address 10.7.1.1 255.255.255.0
#
interface 10GE1/0/3
 eth-trunk 10
#
interface 10GE1/0/4
 eth-trunk 10
#
interface 10GE1/0/5
 undo portswitch
 ip address 10.2.1.2 255.255.255.0
 m-lag unpaired-port reserved
#
interface 10GE1/0/6
 eth-trunk 0
#
interface 10GE1/0/7
 eth-trunk 0
#
ospf 1
 area 0.0.0.0
  network 10.3.1.0 0.0.0.255
  network 10.6.1.0 0.0.0.255
```

```
network 10.7.1.0 0.0.0.255
network 10.10.10.0 0.0.0.3
#
return
```

DeviceE 的配置脚本

```
#
sysname DeviceE
#
interface 10GE1/0/1
undo portswitch
ip address 10.4.1.2 255.255.255.0
#
interface 10GE1/0/2
undo portswitch
ip address 10.7.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.4.1.0 0.0.0.255
network 10.7.1.0 0.0.0.255
#
return
```

DeviceF 的配置脚本

```
#
sysname DeviceF
#
interface 10GE1/0/1
undo portswitch
ip address 10.5.1.2 255.255.255.0
#
interface 10GE1/0/2
undo portswitch
ip address 10.6.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.5.1.0 0.0.0.255
network 10.6.1.0 0.0.0.255
#
return
```


1.1.5.11.2.5 举例：配置 M-LAG 设备作为 DHCPv4 中继（插入 Option82 选项的子选项）

组网需求

如图 1 所示，DeviceA 和 DeviceB 组建 M-LAG 系统，下挂设备 DeviceD 通过配置 M-LAG 双归接入三层网络。现需要在 DeviceA 和 DeviceB 上部署 DHCPv4 中继，以实现通过 DHCPv4 服务器为 DeviceD 分配 IP 地址的目的。

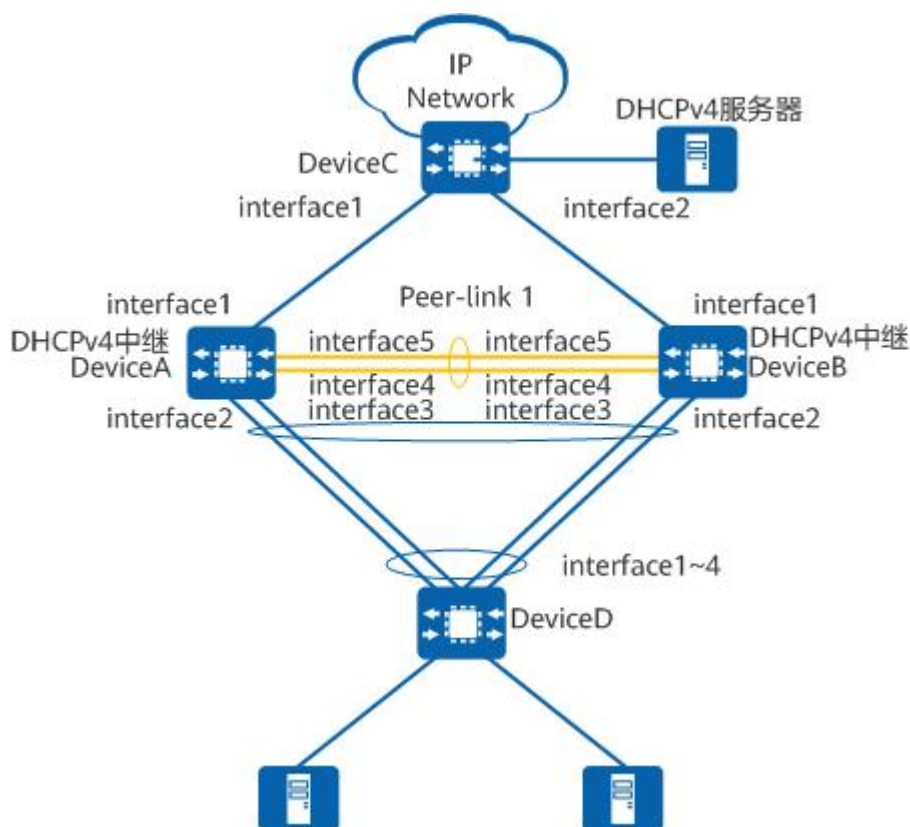
图 1 配置 M-LAG 设备作为 DHCPv4 中继

说明

本例中 DeviceA 的 interface1、interface2、interface3、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceB 的 interface1、interface2、interface3、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceC 的 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

1. 配置 M-LAG 双活网关，具体的配置步骤请参见 [举例：配置 M-LAG 双归接入三层网络（V-STP 方式）](#)。
2. 在 M-LAG 双活网关 DeviceA 和 DeviceB 上配置 DHCPv4 中继功能，包括：

- a. 开启 DHCPv4 中继功能。
 - b. 配置 Option82 选项的子选项 suboption5，实现精准选路。
 - c. 发布本地环回地址的路由。
3. 在 DeviceC 上配置到 DHCPv4 服务器的路由。

操作步骤

1. 在 DeviceA 和 DeviceB 上配置 DHCPv4 中继功能。

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface loopback 0
[DeviceA-LoopBack0] ip address 5.5.5.5 32
[DeviceA-LoopBack0] quit
[DeviceA] interface vlanif 11
[DeviceA-Vlanif11] dhcp select relay
[DeviceA-Vlanif11] dhcp relay server-ip 192.168.1.1
[DeviceA-Vlanif11] dhcp relay information enable
[DeviceA-Vlanif11] dhcp relay giaddr source-interface loopback0
[DeviceA-Vlanif11] dhcp option82 link-selection insert enable
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface loopback 0
[DeviceB-LoopBack0] ip address 6.6.6.6 32
[DeviceB-LoopBack0] quit
[DeviceB] interface vlanif 11
[DeviceB-Vlanif11] dhcp select relay
[DeviceB-Vlanif11] dhcp relay server-ip 192.168.1.1
[DeviceB-Vlanif11] dhcp relay information enable
[DeviceB-Vlanif11] dhcp relay giaddr source-interface loopback0
[DeviceB-Vlanif11] dhcp option82 link-selection insert enable
```

2. 在 DeviceA 和 DeviceB 上发布到本地环回地址的路由。

配置 DeviceA。

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

配置 DeviceB。

```
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 6.6.6.6 0.0.0.0
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

3. 在 DeviceC 上配置到 DHCPv4 服务器（DHCPv4 服务器的 IP 地址为 192.168.1.1）的路由。

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

检查配置结果

在 DeviceA 上查看 DHCPv4 中继的配置信息。DeviceB 上的信息与其一致。

```
[DeviceA] display dhcp relay configuration
DHCP relay global running information :
DHCP relay address cycle      : Disable (default)
DHCP relay trust option82     : Enable (default)
DHCP relay request server-match : Enable (default)
DHCP relay reply forward all   : Disable (default)
DHCP relay agent running information of interface Vlanif11 :
Relay select                  : Enable
Server IP address [00] : 192.168.1.1
GIADDR source interface : LoopBack0
Link-selection insert : Enable
Server-id-override insert : Disable
Vss-control insert : Disable
Giaddr outgoing-interface-address : Disable
```

配置文件

DeviceA 的配置脚本

```
#
sysname DeviceA
#
dfs-group 1
priority 150
dual-active detection source ip 10.200.1.1 peer 10.200.1.2
authentication-mode hmac-sha256 password %+%#!!!!!!"!!!!"!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!9!!!!>fwJ)IOE{=:%,*,XRhbH&t0MCy_8=7!!!!!!!!!!%+%#
```

```
#
vlan batch 11
#
stp mode rstp stp v-stp enable
#
interface Vlanif11
 ip address 10.2.1.1 255.255.255.0
 mac-address 0000-5e00-0101
 dhcp select relay
 dhcp relay information enable
 dhcp relay server-ip 192.168.1.1
 dhcp relay giaddr source-interface loopback 0
 dhcp option82 link-selection insert enable
#
interface Eth-Trunk1
 mode lacp-static
 peer-link 1
#
interface Eth-Trunk10
 port link-type trunk
 port trunk allow-pass vlan 11
 mode lacp-static
 dfs-group 1 m-lag 1
#
interface 10GE1/0/1
 undo portswitch
 ip address 10.3.1.1 255.255.255.0
#
interface 10GE1/0/2
 eth-trunk 10
#
interface 10GE1/0/3
 eth-trunk 10
#
interface 10GE1/0/4
 eth-trunk 1
#
interface 10GE1/0/5
 eth-trunk 1
#
interface LoopBack0
 ip address 5.5.5.5 255.255.255.255
#
```

```
monitor-link group 1
port 10GE1/0/1 uplink
port Eth-Trunk10 downlink 1
#
ospf 1
area 0.0.0.0
network 5.5.5.5 0.0.0.0
network 10.2.1.0 0.0.0.255
network 10.3.1.0 0.0.0.255
#
return
```

DeviceB 的配置脚本

```
#
sysname DeviceB
#
dfs-group 1
priority 120
dual-active detection source ip 10.200.1.2 peer 10.200.1.1
authentication-mode hmac-sha256 password %+%##!!!!!!!"!!!!!!!"*!!!!=I9f8>C{!P_bhB31@7r-
=jrS8c|_"(Bn~#=!!!!!!!"9!!!!kx-6@.tGA(wAt/IQXI6>[g{6YIOi9$!!!!!!!"%+%#
#
vlan batch 11
#
stp mode rstp stp v-stp enable
#
interface Vlanif11
ip address 10.2.1.1 255.255.255.0
mac-address 0000-5e00-0101
dhcp select relay
dhcp relay information enable
dhcp relay server-ip 192.168.1.1
dhcp relay giaddr source-interface loopback 0
dhcp option82 link-selection insert enable
#
interface Eth-Trunk1
mode lacp-static
peer-link 1
#
interface Eth-Trunk10
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
```

```
dfs-group 1 m-lag 1
#
interface 10GE1/0/1
undo portswitch
ip address 10.4.1.1 255.255.255.0
#
interface 10GE1/0/2
eth-trunk 10
#
interface 10GE1/0/3
eth-trunk 10
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
eth-trunk 1
#
interface LoopBack0
ip address 6.6.6.6 255.255.255.255
#
monitor-link group 1
port 10GE1/0/1 uplink
port Eth-Trunk10 downlink 1
#
ospf 1
area 0.0.0.0
network 6.6.6.6 0.0.0.0
network 10.2.1.0 0.0.0.255
network 10.4.1.0 0.0.0.255
#
return
```

DeviceC 的配置脚本

```
#
sysname DeviceC
#
interface 10GE1/0/1
undo portswitch
ip address 10.3.1.2 255.255.255.0
#
interface 10GE1/0/2
undo portswitch
```

```
ip address 10.4.1.2 255.255.255.0
#
ospf 1
area 0.0.0.0
network 10.3.1.0 0.0.0.255
network 10.4.1.0 0.0.0.255
network 192.168.1.0 0.0.0.255
#
return
```

DeviceD 的配置脚本

```
#
sysname DeviceD
#
vlan batch 11
#
interface Eth-Trunk20
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 20
#
interface 10GE1/0/2
eth-trunk 20
#
interface 10GE1/0/3
eth-trunk 20
#
interface 10GE1/0/4
eth-trunk 20
#
return
```

1.1.5.11.2.6 举例：配置 M-LAG 设备作为 DHCPv4 中继（Option82 选项携带回程地址信息）

组网需求

如图 1 所示，DeviceA 和 DeviceB 组建 M-LAG 系统，下挂设备 DeviceD 通过配置 M-LAG 双归接入三层网络。现需要在 DeviceA 和 DeviceB 上部署 DHCPv4 中继，以实现通过 DHCPv4 服务器为 DeviceD 分配 IP 地址的目的。

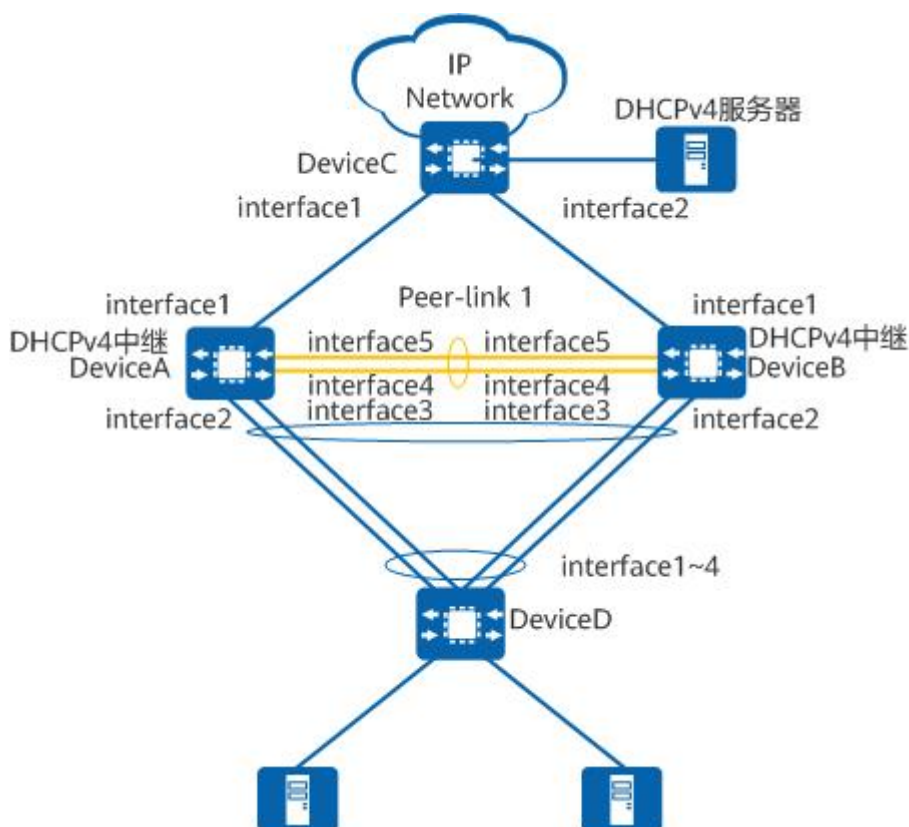
图 1 配置 M-LAG 设备作为 DHCPv4 中继

说明

本例中 DeviceA 的 interface1、interface2、interface3、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceB 的 interface1、interface2、interface3、interface4 和 interface5 分别代表 10GE1/0/1，10GE1/0/2，10GE1/0/3，10GE1/0/4 和 10GE1/0/5。

本例中 DeviceC 的 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

1. 配置 M-LAG 双活网关，具体的配置步骤请参见 [举例：配置 M-LAG 双归接入三层网络（V-STP 方式）](#)。
2. 在 M-LAG 双活网关 DeviceA 和 DeviceB 上配置 DHCPv4 中继功能，包括：
 - a. 开启 DHCPv4 中继功能。
 - b. 配置 Option82 选项携带回程地址信息。
 - c. 发布本地环回地址的路由。
3. 在 DeviceC 上配置到 DHCPv4 服务器的路由。

操作步骤

1. 在 DeviceA 和 DeviceB 上配置 DHCPv4 中继功能。

配置 DeviceA。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] interface loopback 0
[DeviceA-LoopBack0] ip address 5.5.5.5 32
[DeviceA-LoopBack0] quit
[DeviceA] interface vlanif 11
[DeviceA-Vlanif11] dhcp select relay
[DeviceA-Vlanif11] dhcp relay server-ip 192.168.1.1
[DeviceA-Vlanif11] dhcp relay information enable
[DeviceA-Vlanif11] dhcp option82 vendor-specific format vendor-sub-option 2 source-ip-address
5.5.5.5
```

配置 DeviceB。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] interface loopback 0
[DeviceB-LoopBack0] ip address 6.6.6.6 32
[DeviceB-LoopBack0] quit
[DeviceB] interface vlanif 11
[DeviceB-Vlanif11] dhcp select relay
[DeviceB-Vlanif11] dhcp relay server-ip 192.168.1.1
[DeviceB-Vlanif11] dhcp relay information enable
[DeviceB-Vlanif11] dhcp option82 vendor-specific format vendor-sub-option 2 source-ip-address
6.6.6.6
```

2. 在 DeviceA 和 DeviceB 上发布到本地环回地址的路由。

配置 DeviceA。

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 5.5.5.5 0.0.0.0
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

配置 DeviceB。

```
[DeviceB] ospf 1
[DeviceB-ospf-1] area 0
[DeviceB-ospf-1-area-0.0.0.0] network 6.6.6.6 0.0.0.0
[DeviceB-ospf-1-area-0.0.0.0] quit
[DeviceB-ospf-1] quit
```

3. 在 DeviceC 上配置到 DHCPv4 服务器（DHCPv4 服务器的 IP 地址为 192.168.1.1）的路由。

```
[DeviceA] ospf 1
[DeviceA-ospf-1] area 0
[DeviceA-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[DeviceA-ospf-1-area-0.0.0.0] quit
[DeviceA-ospf-1] quit
```

检查配置结果

在 DeviceA 上查看 DHCPv4 中继的配置信息。DeviceB 上的信息与其一致。

```
[DeviceA] display dhcp relay configuration
DHCP relay global running information :
DHCP relay address cycle      : Disable (default)
DHCP relay trust option82     : Enable (default)
DHCP relay request server-match : Enable (default)
DHCP relay reply forward all   : Disable (default)
DHCP relay agent running information of interface Vlanif11 :
Relay select                  : Enable
Server IP address [00] : 192.168.1.1
Link-selection insert         : Disable
Server-id-override insert     : Disable
Vss-control insert            : Disable
Giaddr outgoing-interface-address : Disable
```

配置文件

DeviceA 的配置脚本

```
#
sysname DeviceA
#
dfs-group 1
priority 150
dual-active detection source ip 10.200.1.1 peer 10.200.1.2
authentication-mode hmac-sha256 password %+%##!!!!!!"!!!!"!!!!*!!!!C+tR0CW9x*eB&pWp`t),Azgw-
h\o8#4LZPD!!!!!!!!!!!!9!!!!>fwJ)l0E{=:%,*XRhbH&t0MCy_8=7!!!!!!!!!!%+%#
#
vlan batch 11
#
stp mode rstp stp v-stp enable
#
interface Vlanif11
```

```
ip address 10.2.1.1 255.255.255.0
mac-address 0000-5e00-0101
dhcp select relay
dhcp relay information enable
dhcp relay server-ip 192.168.1.1
dhcp option82 vendor-specific format vendor-sub-option 2 source-ip-address 5.5.5.5
#
interface Eth-Trunk1
mode lacp-static
peer-link 1
#
interface Eth-Trunk10
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
dfs-group 1 m-lag 1
#
interface 10GE1/0/1
undo portswitch
ip address 10.3.1.1 255.255.255.0
#
interface 10GE1/0/2
eth-trunk 10
#
interface 10GE1/0/3
eth-trunk 10
#
interface 10GE1/0/4
eth-trunk 1
#
interface 10GE1/0/5
eth-trunk 1
#
interface LoopBack0
ip address 5.5.5.5 255.255.255.255
#
monitor-link group 1
port 10GE1/0/1 uplink
port Eth-Trunk10 downlink 1
#
ospf 1
area 0.0.0.0
network 5.5.5.5 0.0.0.0
```

```

network 10.2.1.0 0.0.0.255
network 10.3.1.0 0.0.0.255
#
return

```

DeviceB 的配置脚本

```

#
sysname DeviceB
#
dfs-group 1
priority 120
dual-active detection source ip 10.200.1.2 peer 10.200.1.1
authentication-mode hmac-sha256 password %+%##!!!!!!!"!!!!!!*!!!!=I9f8>C{!P_bhB31@7r-
=jrS8c|_"(Bn~#=!!!!!!!"!!!!!!9!!!!kx-6@.tGA(wAt/IQXI6>[g{6YIOi9$!!!!!!!"%+%#
#
vlan batch 11
#
stp mode rstp stp v-stp enable
#
interface Vlanif11
ip address 10.2.1.1 255.255.255.0
mac-address 0000-5e00-0101
dhcp select relay
dhcp relay information enable
dhcp relay server-ip 192.168.1.1
dhcp option82 vendor-specific format vendor-sub-option 2 source-ip-address 6.6.6.6
#
interface Eth-Trunk1
mode lacp-static
peer-link 1
#
interface Eth-Trunk10
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
dfs-group 1 m-lag 1
#
interface 10GE1/0/1
undo portswitch
ip address 10.4.1.1 255.255.255.0
#
interface 10GE1/0/2
eth-trunk 10

```

```
#
interface 10GE1/0/3
 eth-trunk 10
#
interface 10GE1/0/4
 eth-trunk 1
#
interface 10GE1/0/5
 eth-trunk 1
#
interface LoopBack0
 ip address 6.6.6.6 255.255.255.255
#
monitor-link group 1
 port 10GE1/0/1 uplink
 port Eth-Trunk10 downlink 1
#
ospf 1
 area 0.0.0.0
 network 6.6.6.6 0.0.0.0
 network 10.2.1.0 0.0.0.255
 network 10.4.1.0 0.0.0.255
#
return
```

DeviceC 的配置脚本

```
#
sysname DeviceC
#
interface 10GE1/0/1
 undo portswitch
 ip address 10.3.1.2 255.255.255.0
#
interface 10GE1/0/2
 undo portswitch
 ip address 10.4.1.2 255.255.255.0
#
ospf 1
 area 0.0.0.0
 network 10.3.1.0 0.0.0.255
 network 10.4.1.0 0.0.0.255
 network 192.168.1.0 0.0.0.255
#
```

```
return
```

DeviceD 的配置脚本

```
#
sysname DeviceD
#
vlan batch 11
#
interface Eth-Trunk20
port link-type trunk
port trunk allow-pass vlan 11
mode lacp-static
#
interface 10GE1/0/1
eth-trunk 20
#
interface 10GE1/0/2
eth-trunk 20
#
interface 10GE1/0/3
eth-trunk 20
#
interface 10GE1/0/4
eth-trunk 20
#
return
```

1.1.5.12 用户接入与认证

[AAA](#)

[NAC](#)

1.1.5.12.1 AAA

[举例：配置 AAA 本地认证和授权](#)

[举例：配置 HWTACACS 认证、授权和计费](#)

[举例：配置 RADIUS 认证、授权和计费](#)

1.1.5.12.1.1 举例：配置 AAA 本地认证和授权

组网需求

如图 1 所示，企业希望管理员使用 AAA 本地认证，通过 STelnet 登录设备：

1. 管理员输入正确的用户名和密码才能通过 STelnet 登录设备。
2. 管理员通过 STelnet 登录设备后，授权管理员级别为 3 级。

图 1 配置 AAA 本地认证和授权示例

说明

本例中 interface1 代表 10GE1/0/1。



配置思路

1. 配置 STelnet 登录：配置 VTY 界面的认证方式为 AAA、使能 STelnet 服务、配置 SSH 用户的认证方式和服务方式。
2. 配置 AAA 本地认证：创建用户名和密码、配置用户的接入类型、配置用户级别。

配置注意事项

配置前请确保各设备之间路由可达。

操作步骤

1. 配置接口的 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 192.168.10.1 24
[DeviceA-Vlanif10] quit
```

2. 配置 STelnet 登录。

在服务器端生成本地密钥对。

```
[DeviceA] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 3072).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

配置 VTY 用户界面 0~4 的认证方式为 AAA 认证、支持的协议为 SSH。

```
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] authentication-mode aaa
[DeviceA-ui-vty0-4] protocol inbound ssh
[DeviceA-ui-vty0-4] quit
```

开启设备的 SSH 服务器功能。

```
[DeviceA] stelnet server enable
[DeviceA] ssh server-source -i vlanif 10
```

配置所有 SSH 用户的认证方式为 Password 认证、服务方式为 STelnet。

```
[DeviceA] ssh authentication-type default password
```

3. 配置 AAA 本地认证。

```
[DeviceA] aaa
[DeviceA-aaa] local-user user1-huawei password irreversible-cipher
YsHsjx_202206
[DeviceA-aaa] local-user user1-huawei service-type ssh
[DeviceA-aaa] local-user user1-huawei privilege level 3
[DeviceA-aaa] quit
```

检查配置结果

管理员通过 STelnet 客户端，输入正确的用户名和密码后，能够登录 DeviceA。

配置脚本

```
#
sysname DeviceA
#
aaa
local-user user1-huawei password irreversible-cipher
$1d$OwseVRh@LH}ZeTBm$1nH4$ab>d(N{-%0!ab48y=lc*xEUR4pVhR2"9-~, $
local-user user1-huawei privilege level 3
local-user user1-huawei service-type ssh
#
vlan batch 10
#
```



```
interface Vlanif10
ip address 192.168.10.1 24
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
stelnet server enable
ssh server-source -i Vlanif 10
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return
```

1.1.5.12.1.2 举例：配置 HWTACACS 认证、授权和计费

组网需求

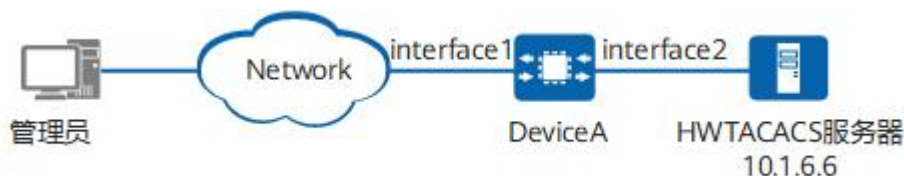
如图 1 所示，网络中部署了 HWTACACS 服务器，企业希望管理员使用 HWTACACS 认证，通过 STelnet 登录设备：

1. 管理员输入正确的用户名和密码才能通过 STelnet 登录设备。
2. 管理员通过 STelnet 登录设备后，授权管理员级别为 3 级，并且能够控制管理员不可执行部分命令并记录管理员执行过的命令。

图 1 配置 HWTACACS 认证、授权和计费示例

说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

1. 在 DeviceA 上配置 STelnet 登录：配置 VTY 界面的认证方式为 AAA、使能 STelnet 服务、配置 SSH 用户的认证方式和服务方式。
2. 在 DeviceA 上配置 HWTACACS 认证：创建 HWTACACS 服务器模板，配置 AAA 方案、记录方案，并使能命令行授权功能。

3. 配置 HWTACACS 服务器。

配置注意事项

配置前请确保各设备之间路由可达。

操作步骤

1. 配置接口的 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.2 255.255.255.0
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.6.2 255.255.255.0
[DeviceA-Vlanif20] quit
```

2. 配置 STelnet 登录。

在服务器端生成本地密钥对。

```
[DeviceA] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 3072).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

配置 VTY 用户界面 0~4 的认证方式为 AAA 认证、支持的协议为 SSH。

```
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] authentication-mode aaa
[DeviceA-ui-vty0-4] protocol inbound ssh
[DeviceA-ui-vty0-4] quit
```

开启设备的 SSH 服务器功能。

```
[DeviceA] stelnet server enable
[DeviceA] ssh server-source -i vlanif 10
```

配置所有 SSH 用户的认证方式为 Password 认证、服务方式为 STelnet。

```
[DeviceA] ssh authentication-type default password
```

3. 配置 HWTACACS 认证、授权和计费。

配置 HWTACACS 服务器模板 template1，实现设备与 HWTACACS 服务器的通信。

```
[DeviceA] hwtacacs-server template template1
[DeviceA-hwtacacs-template1] hwtacacs-server authentication 10.1.6.6 49
[DeviceA-hwtacacs-template1] hwtacacs-server authorization 10.1.6.6 49
[DeviceA-hwtacacs-template1] hwtacacs-server accounting 10.1.6.6 49
[DeviceA-hwtacacs-template1] hwtacacs-server shared-key cipher YsHsjx_202206139
[DeviceA-hwtacacs-template1] quit
```

配置认证方案 sch1，指定认证方式为 HWTACACS 认证。

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme sch1
[DeviceA-aaa-authen-sch1] authentication-mode hwtacacs
[DeviceA-aaa-authen-sch1] quit
```

配置授权方案 sch2，指定授权方式为 HWTACACS 授权，并使能 3 级用户的命令行授权功能。

```
[DeviceA-aaa] authorization-scheme sch2
[DeviceA-aaa-author-sch2] authorization-mode hwtacacs
[DeviceA-aaa-author-sch2] authorization-cmd 3 hwtacacs
[DeviceA-aaa-author-sch2] quit
```

配置记录方案 sch0，记录用户执行的命令行。

```
[DeviceA-aaa] recording-scheme sch0
[DeviceA-aaa-recording-sch0] recording-mode hwtacacs template1
[DeviceA-aaa-recording-sch0] quit
[DeviceA-aaa] cmd recording-scheme sch0
```

配置计费方案 sch3，指定计费方式为 HWTACACS 计费。

```
[DeviceA-aaa] accounting-scheme sch3
[DeviceA-aaa-accounting-sch3] accounting-mode hwtacacs
[DeviceA-aaa-accounting-sch3] quit
```

在域 huawei.com 下引用 HWTACACS 服务器模板和 AAA 方案。

```
[DeviceA-aaa] domain huawei.com
[DeviceA-aaa-domain-huawei.com] hwtacacs-server template1
[DeviceA-aaa-domain-huawei.com] authentication-scheme sch1
[DeviceA-aaa-domain-huawei.com] authorization-scheme sch2
[DeviceA-aaa-domain-huawei.com] accounting-scheme sch3
[DeviceA-aaa-domain-huawei.com] quit
[DeviceA-aaa] quit
```

配置域 huawei.com 为全局默认管理域。

```
[DeviceA] domain huawei.com admin
```

4. 配置 HWTACACS 服务器，以配置 Secure ACS 为例

配置步骤包括：添加设备、添加用户、配置用户级别为 3 级、配置命令行授权（不允许执行命令 **reset hwtacacs-server statistics all**）。

在 **Reports and Activity -> TACACS+ Administration** 中可以查看所有用户（包括非 HWTACACS 认证用户）命令执行成功或失败的日志记录。

检查配置结果

管理员通过 STelnet 客户端，输入正确的用户名和密码后，能够登录 DeviceA。

用户登录后，执行命令 **reset hwtacacs-server statistics all**，提示 **Error: Failed to pass the authorization.** 表示命令行授权成功。

```
[DeviceA] quit
<DeviceA> reset hwtacacs-server statistics all
Error: Failed to pass the authorization.
```

配置脚本

DeviceA 的配置脚本

```
#
sysname DeviceA
#
hwtacacs-server template template1
hwtacacs-server authentication 10.1.6.6
hwtacacs-server authorization 10.1.6.6
hwtacacs-server accounting 10.1.6.6
hwtacacs-server shared-key cipher %+%##!!!!!!"!!!!*!!!!SKvr$[[Fs."u,S-6a-
X1'[X=L"cpF!5Oz`1!!!!2jp5!!!!A!!!!x>cM8i{y6!);(8Dr9:dK`&BHfE(H2=.:SH{@pT%+%#
#
aaa
authentication-scheme sch1
authentication-mode hwtacacs
authorization-scheme sch2
authorization-mode hwtacacs
authorization-cmd 3 hwtacacs
accounting-scheme sch3
accounting-mode hwtacacs
recording-scheme sch0
recording-mode hwtacacs template1
cmd recording-scheme sch0
```

```
domain huawei.com
authentication-scheme sch1
accounting-scheme sch3
authorization-scheme sch2
hwtacacs-server template1
#
domain huawei.com admin
#
vlan batch 10 20
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
#
interface Vlanif20
ip address 10.1.6.2 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
#
stelnet server enable
ssh server-source -i Vlanif10
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return
```

1.1.5.12.1.3 举例：配置 RADIUS 认证、授权和计费

组网需求

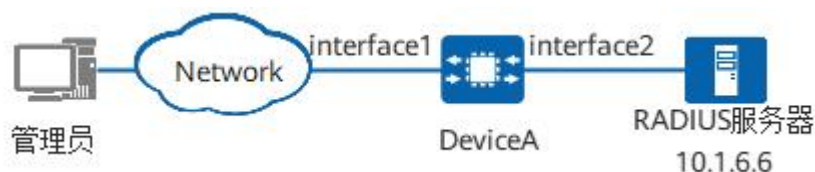
如[图 1](#)所示，网络中部署了 RADIUS 服务器，企业希望管理员使用 RADIUS 认证方式，通过 STelnet 登录设备：

1. 管理员输入正确的用户名和密码才能通过 STelnet 登录设备。
2. 管理员通过 STelnet 登录设备后，授权管理员级别为 3 级。

图 1 配置 RADIUS 认证、授权和计费示例

说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



配置思路

1. 在 DeviceA 上配置 STelnet 登录：配置 VTY 界面的认证方式为 AAA、使能 STelnet 服务、配置 SSH 用户的认证方式和服务方式。
2. 在 DeviceA 上配置 RADIUS 认证：创建 RADIUS 服务器模板和 AAA 认证方案并在域下引用。
3. 配置 RADIUS 服务器。

配置注意事项

配置前请确保各设备之间路由可达。

请确保 RADIUS 服务器模板内的共享密钥和 RADIUS 服务器上的配置保持一致。

域被配置成全局默认管理域之后，管理用户的用户名中携带该域名或者不携带域名时，会使用全局默认管理域下的 AAA 配置信息。

如果 RADIUS 服务器不支持包含域名的用户名，可以在 RADIUS 服务器模板视图下，配置命令 **undo radius-server user-name domain-included** 使设备向 RADIUS 服务器发送的报文中的用户名不包含域名。

配置命令 **undo radius-server user-name domain-included** 后，设备仅会修改发送报文中的用户名格式，不会影响用户所属的域。例如，配置该命令后，用户名为“username@huawei.com”的用户仍使用 huawei.com 域下的 AAA 配置信息。

使用 RADIUS 扩展属性 HW-Exec-Privilege（26-29）来授权管理员用户的优先级时，有效值范围是 0~3。取值大于等于 4 为无效值。

操作步骤

1. 配置接口的 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
```

```
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type trunk
[DeviceA-10GE1/0/2] port trunk allow-pass vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 10.1.1.2 255.255.255.0
[DeviceA-Vlanif10] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 10.1.6.2 255.255.255.0
[DeviceA-Vlanif20] quit
```

2. 配置 STelnet 登录。

在服务器端生成本地密钥对。

```
[DeviceA] rsa local-key-pair create
The key name will be:Host
The range of public key size is (2048, 3072).
NOTE: Key pair generation will take a short while.
Please input the modulus [default = 3072]:3072
```

配置 VTY 用户界面 0~4 的认证方式为 AAA 认证、支持的协议为 SSH。

```
[DeviceA] user-interface vty 0 4
[DeviceA-ui-vty0-4] authentication-mode aaa
[DeviceA-ui-vty0-4] protocol inbound ssh
[DeviceA-ui-vty0-4] quit
```

开启设备的 SSH 服务器功能。

```
[DeviceA] stelnet server enable
[DeviceA] ssh server-source -i vlanif 10
```

配置所有 SSH 用户的认证方式为 Password 认证、服务方式为 STelnet。

```
[DeviceA] ssh authentication-type default password
```

3. 配置 RADIUS 认证、授权和计费。

配置 RADIUS 服务器模板，实现与 RADIUS 服务器的通信。

```
[DeviceA] radius-server template 1
[DeviceA-radius-1] radius-server authentication 10.1.6.6 1812
[DeviceA-radius-1] radius-server accounting 10.1.6.6 1813
[DeviceA-radius-1] radius-server shared-key cipher YsHsjx_202206139
[DeviceA-radius-1] quit
```

配置 AAA 认证方案，指定认证方式为 RADIUS。

```
[DeviceA] aaa
```

```
[DeviceA-aaa] authentication-scheme auth1
[DeviceA-aaa-authen-auth1] authentication-mode radius
[DeviceA-aaa-authen-auth1] quit
```

配置计费方案 acc1，指定计费方式为 RADIUS 计费。

```
[DeviceA-aaa] accounting-scheme acc1
[DeviceA-aaa-accounting-acc1] accounting-mode radius
[DeviceA-aaa-accounting-acc1] quit
```

在域下引用 AAA 方案、RADIUS 服务器模板。

```
[DeviceA-aaa] domain huawei.com
[DeviceA-aaa-domain-huawei.com] authentication-scheme auth1
[DeviceA-aaa-domain-huawei.com] accounting-scheme acc1
[DeviceA-aaa-domain-huawei.com] radius-server 1
[DeviceA-aaa-domain-huawei.com] quit
[DeviceA-aaa] quit
```

4. 配置管理员所属域为全局默认管理域，这样管理员通过 STelnet 登录设备时就不需要输入域名。

```
[DeviceA] domain huawei.com admin
```

5. 配置 RADIUS 服务器。

配置步骤包括：添加设备、添加用户、配置授权用户级别为 3。

检查配置结果

管理员通过 STelnet 客户端，输入正确的用户名和密码后，能够登录 DeviceA。

配置脚本

DeviceA 的配置脚本

```
#
sysname DeviceA
#
radius-server template 1
radius-server shared-key
cipher %+%##!!!!!!!"!!!!!!*!!!!SKvr$[Fs.3t@/5k|BENhEu>W(3~-XG!!D;!!!!2jp5!!!!!!A!!!!3"pK8qv!}9M#(4$jGWvQ
F/R[CNe/+:W^jk8HUe&W%+%#
radius-server authentication 10.1.6.6 1812 weight 80
radius-server accounting 10.1.6.6 1813 weight 80
#
aaa
authentication-scheme auth1
authentication-mode radius
accounting-scheme acc1
```



```
accounting-mode radius
domain huawei.com
authentication-scheme auth1
accounting-scheme acc1
radius-server 1
#
domain huawei.com admin
#
vlan batch 10 20
#
interface Vlanif10
ip address 10.1.1.2 255.255.255.0
#
interface Vlanif20
ip address 10.1.6.2 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 20
#
stelnet server enable
ssh server-source -i Vlanif10
#
user-interface vty 0 4
authentication-mode aaa
protocol inbound ssh
#
return
```

1.1.5.12.2 NAC

举例：配置 802.1X 认证（AAA 采用 RADIUS 方式）

举例：配置 802.1X 认证（AAA 采用本地认证）

1.1.5.12.2.1 举例：配置 802.1X 认证（AAA 采用 RADIUS 方式）

组网需求

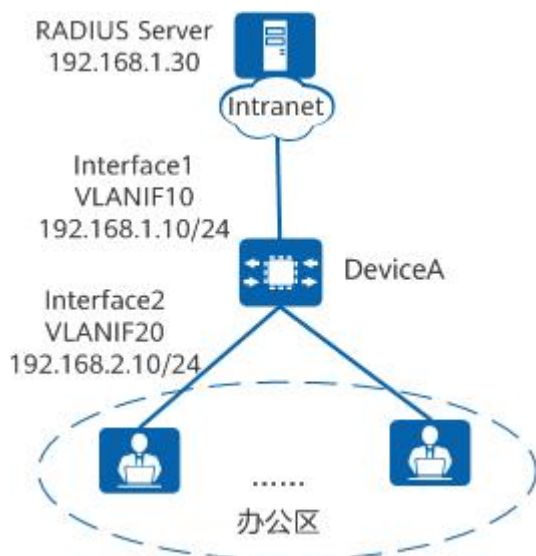
如图 1 所示，某公司办公区内终端通过 DeviceA 接入公司内部网络。DeviceA 的下行接口（例如 10GE1/0/2）与办公区内终端直接相连，DeviceA 的上行接口 10GE1/0/1 通过内部网络与 RADIUS 服务器相连。

为了满足企业的高安全性需求，使用 802.1X 认证并通过 RADIUS 服务器对办公区内终端进行认证，并且认证点部署在 DeviceA 与办公区内终端直连的接口（例如 10GE1/0/2）上。

图 1 配置 802.1X 认证组网图

说明

本例中 Interface1、Interface2 分别代表 10GE1/0/1、10GE1/0/2。



操作步骤

1. 配置网络互连互通。

创建 VLAN 并配置接口允许通过的 VLAN、IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 192.168.1.10 24
[DeviceA-Vlanif10] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
```

```
[DeviceA-10GE1/0/2] port default vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 192.168.2.10 24
[DeviceA-Vlanif20] quit
```

2. 配置 AAA。

创建并配置 RADIUS 服务器模板 “rd1”。

```
[DeviceA] radius-server template rd1
[DeviceA-radius-rd1] radius-server authentication 192.168.1.30 1812
[DeviceA-radius-rd1] radius-server shared-key cipher Huawei@123456789
[DeviceA-radius-rd1] quit
```

创建 AAA 认证方案 “abc” 并配置认证方式为 RADIUS。

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme abc
[DeviceA-aaa-authen-abc] authentication-mode radius
[DeviceA-aaa-authen-abc] quit
```

创建认证域 “example.com”，并在其上绑定 AAA 认证方案 “abc” 与 RADIUS 服务器模板 “rd1”。

```
[DeviceA-aaa] domain example.com
[DeviceA-aaa-domain-example.com] authentication-scheme abc
[DeviceA-aaa-domain-example.com] radius-server rd1
[DeviceA-aaa-domain-example.com] quit
[DeviceA-aaa] quit
```

测试用户是否能够通过 RADIUS 模板的认证。（已在 RADIUS 服务器上配置了测试用户 test，用户密码 Example2012）

```
[DeviceA] test-aaa test Example2012 radius-template rd1
Info: Account test succeeded.
```

3. 配置 802.1X 认证。

配置 802.1X 接入模板 “d1”。

```
[DeviceA] dot1x-access-profile name d1
[DeviceA-dot1x-access-profile-d1] dot1x authentication-method eap
[DeviceA-dot1x-access-profile-d1] dot1x timer client-timeout 30
[DeviceA-dot1x-access-profile-d1] quit
```

说明

802.1X 接入模板默认采用 EAP 认证方式。请确保 RADIUS 服务器支持 EAP 协议，否则无法处理 802.1X 认证请求。

配置认证模板 “p1”，并在其上绑定 802.1X 接入模板 “d1”、指定认证模板下用户的强制认证域为 “example.com”。

```
[DeviceA] authentication-profile name p1
[DeviceA-authen-profile-p1] dot1x-access-profile d1
[DeviceA-authen-profile-p1] access-domain example.com force
[DeviceA-authen-profile-p1] quit
```

在下行接口上绑定认证模板“p1”，开启 802.1X 认证。以接口 10GE1/0/2 为例，其他接口配置与其类似。

```
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] authentication-profile p1
[DeviceA-10GE1/0/2] quit
```

检查配置结果

1. 用户在终端上启动 802.1X 客户端，输入用户名和密码，开始认证。
2. 如果用户输入的用户名和密码验证正确，客户端页面会显示认证成功信息。用户即可访问网络。
3. 用户上线后，管理员可在设备上执行命令 **display access-user access-type dot1x** 查看在线 802.1X 用户信息。

配置脚本

DeviceA 的配置脚本

```
#
sysname DeviceA
#
authentication-profile name p1
dot1x-access-profile d1
access-domain example.com force
#
vlan batch 10 to 20
#
aaa
authentication-scheme abc
authentication-mode radius
domain example.com
authentication-scheme abc
radius-server rd1
#
radius-server template rd1
radius-server shared-key
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"SKvr$[Fs.3t@/5k|BENhEu>W(3~XG!!D;!!!!2jp5!!!!!!A!!!!3"pK8qv!]9M#{4$jGWvQ
F/R[CNe/+:W^jk8HUe&W%+%#
radius-server authentication 192.168.1.30 1812 weight 80
```

```
#
dot1x-access-profile name d1
dot1x timer client-timeout 30
#
interface Vlanif10
ip address 192.168.1.10 255.255.255.0
#
interface Vlanif20
ip address 192.168.2.10 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
interface 10GE1/0/2
port default vlan 20
authentication-profile p1
#
return
```

1.1.5.12.2.2 举例：配置 802.1X 认证（AAA 采用本地认证）

组网需求

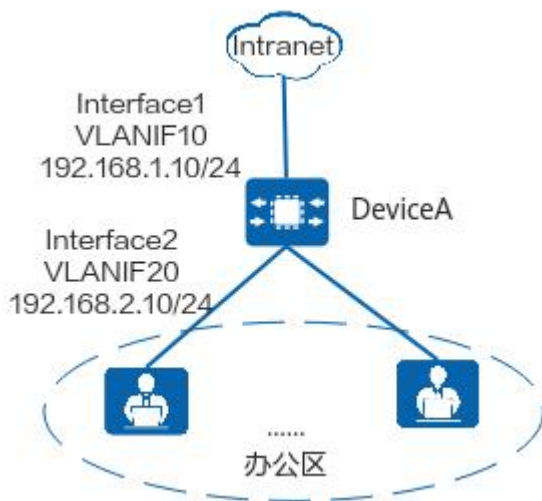
如[图 1](#)所示，某公司办公区内终端通过 DeviceA 接入公司内部网络。DeviceA 的下行接口（例如 10GE1/0/2）与办公区内终端直接相连。

为了满足企业的高安全性需求，使用 802.1X 认证+本地认证方式对办公区内终端进行认证，并且认证点部署在 DeviceA 与办公区内终端直连的接口（例如 10GE1/0/2）上。

图 1 配置 802.1X 认证组网图

说明

本例中 Interface1、Interface2 分别代表 10GE1/0/1、10GE1/0/2。



操作步骤

1. 配置网络互连互通。

创建 VLAN 并配置接口允许通过的 VLAN、IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10 20
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type trunk
[DeviceA-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface vlanif 10
[DeviceA-Vlanif10] ip address 192.168.1.10 24
[DeviceA-Vlanif10] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface vlanif 20
[DeviceA-Vlanif20] ip address 192.168.2.10 24
[DeviceA-Vlanif20] quit
```

2. 配置 AAA 本地认证。

配置认证方案“a1”为本地认证。

```
[DeviceA] aaa
[DeviceA-aaa] authentication-scheme a1
[DeviceA-aaa-authen-a1] authentication-mode local
[DeviceA-aaa-authen-a1] quit
```

配置授权方案“b1”为本地授权。

```
[DeviceA-aaa] authorization-scheme b1
[DeviceA-aaa-author-b1] authorization-mode local
[DeviceA-aaa-author-b1] quit
```

配置本地用户的用户名、密码和用户接入类型。

说明

将终端的 MAC 地址配置为本地用户名，密码配置为 Example@123，接入类型为 MAC 认证（8021x）。以下以打印机 1 为例（MAC 地址为 00e0-fcd4-8828）。

```
[DeviceA-aaa] local-access-user 00e0-fcd4-8828
[DeviceA-aaa-access-user-00e0-fcd4-8828] password cipher Example@123
[DeviceA-aaa-access-user-00e0-fcd4-8828] service-type dot1x
[DeviceA-aaa-access-user-00e0-fcd4-8828] quit
```

配置业务方案“s1”。通过业务方案“s1”同一个用户名最多可以接入 15 个用户。

```
[DeviceA-aaa] service-scheme s1
[DeviceA-aaa-service-s1] access-limit user-name max-num 15
[DeviceA-aaa-service-s1] quit
```

配置域“example.com”，并在域下应用认证方案“a1”、授权方案“b1”和业务方案“s1”。

```
[DeviceA-aaa] domain example.com
[DeviceA-aaa-domain-example.com] authentication-scheme a1
[DeviceA-aaa-domain-example.com] authorization-scheme b1
[DeviceA-aaa-domain-example.com] service-scheme s1
[DeviceA-aaa-domain-example.com] quit
[DeviceA-aaa] quit
```

3. 配置 802.1X 认证。

配置 802.1X 接入模板“d1”。

```
[DeviceA] dot1x-access-profile name d1
[DeviceA-dot1x-access-profile-d1] dot1x authentication-method eap
[DeviceA-dot1x-access-profile-d1] dot1x timer client-timeout 30
[DeviceA-dot1x-access-profile-d1] quit
```

配置认证模板“p1”，并在其上绑定 802.1X 接入模板“d1”、指定认证模板下用户的强制认证域为“example.com”。

```
[DeviceA] authentication-profile name p1
[DeviceA-authen-profile-p1] dot1x-access-profile d1
[DeviceA-authen-profile-p1] access-domain example.com force
[DeviceA-authen-profile-p1] quit
```

在下行接口上绑定认证模板“p1”，开启 802.1X 认证。以接口 10GE1/0/2 为例，其他接口配置与其类似。

```
[DeviceA] interface 10ge 1/0/2
```

```
[DeviceA-10GE1/0/2] authentication-profile p1
```

```
[DeviceA-10GE1/0/2] quit
```

检查配置结果

1. 用户启动终端后，设备会自动获取用户终端的 MAC 地址作为用户名和密码进行认证。
2. 用户认证成功后即可访问网络。
3. 用户上线后，管理员可在设备上执行命令 **display access-user access-type dot1x** 查看在线 802.1X 用户信息。

配置脚本

DeviceA 的配置脚本

```
#
sysname DeviceA
#
authentication-profile name p1
dot1x-access-profile d1
access-domain example.com force
#
vlan batch 10 to 20
#
aaa
authentication-scheme a1
authentication-mode local
authorization-scheme b1
authorization-mode local
service-scheme s1
access-limit user-name max-num 15
domain example.com
authentication-scheme a1
authorization-scheme b1
service-scheme s1
local-access-user 00e0-fcd4-8828
password
cipher %+%##!!!!!!!"!!!!!!!"!!!!!!!"SKvr$[Fs.<FvBB,.w;M75IN5Z>'!L8G:n-!!!!2jp5!!!!!!<!!!!k9&fPO<BSRW}jPT(,ew
KyfIL"zVtM1~=>e.!!!!!!%+%#
service-type dot1x
#
dot1x-access-profile name d1
dot1x timer client-timeout 30
```



```
#
interface Vlanif10
 ip address 192.168.1.10 255.255.255.0
#
interface Vlanif20
 ip address 192.168.2.10 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 authentication-profile p1
#
interface 10GE1/0/2
 port default vlan 20
#
return
```

1.1.5.13 安全

[IPSG](#)

[端口安全](#)

1.1.5.13.1 IPSG

[举例：基于接口配置静态绑定表的 IPSG](#)

[举例：基于 VLAN 配置静态绑定表的 IPSG](#)

[举例：配置 IPSG 防止 DHCP 动态主机私自更改 IP 地址](#)

[举例：基于 VLAN 配置动态绑定表的 IPSG](#)

1.1.5.13.1.1 举例：基于接口配置静态绑定表的 IPSG

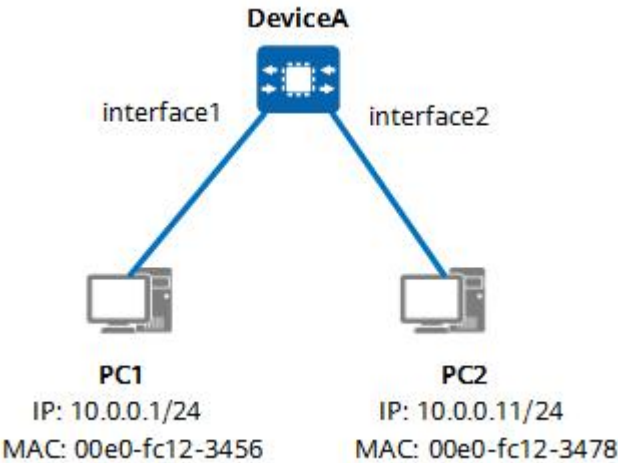
组网需求

如[图 基于接口配置静态绑定表的 IPSG 组网图](#)所示，PC1 和 PC2 通过 DeviceA 接入网络，PC1 和 PC2 均使用静态配置的 IP 地址。管理员希望用户使用固定 IP 地址上网，不允许私自更改 IP 地址非法获取网络访问权限。

图 1 基于接口配置静态绑定表的 IPSG 组网图

 说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



操作步骤

1. 在 DeviceA 上创建静态绑定表项。
在 DeviceA 上创建静态绑定表项。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] user-bind static ip-address 10.0.0.1 mac-address 00e0-fc12-3456
[DeviceA] user-bind static ip-address 10.0.0.11 mac-address 00e0-fc12-3478
```

2. 开启 IPSG 功能。
在 DeviceA 的 10GE1/0/1、10GE1/0/2 接口使能 IPSG。

```
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] ipv4 source check user-bind enable
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] ipv4 source check user-bind enable
[DeviceA-10GE1/0/2] quit
```

检查配置结果

查看静态绑定表信息。

```
[DeviceA] display ip source check user-bind status
```

DHCP Bind-table on slot 1:

IP Address	Prefix	MAC Address	Vlan(O/I)	Interface	Type	Status

10.0.0.1	-	00e0-fc12-3456	-	/-	-	Static IPv4/-
10.0.0.11	-	00e0-fc12-3478	-	/-	-	Static IPv4/-

Total count:		2				

配置文件

DeviceA

```
#
sysname DeviceA
#
user-bind static ip-address 10.0.0.1 mac-address 00e0-fc12-3456
user-bind static ip-address 10.0.0.11 mac-address 00e0-fc12-3478
#
interface 10GE1/0/1
  ipv4 source check user-bind enable
#
interface 10GE1/0/2
  ipv4 source check user-bind enable
#
return
```

1.1.5.13.1.2 举例：基于 VLAN 配置静态绑定表的 IPSG

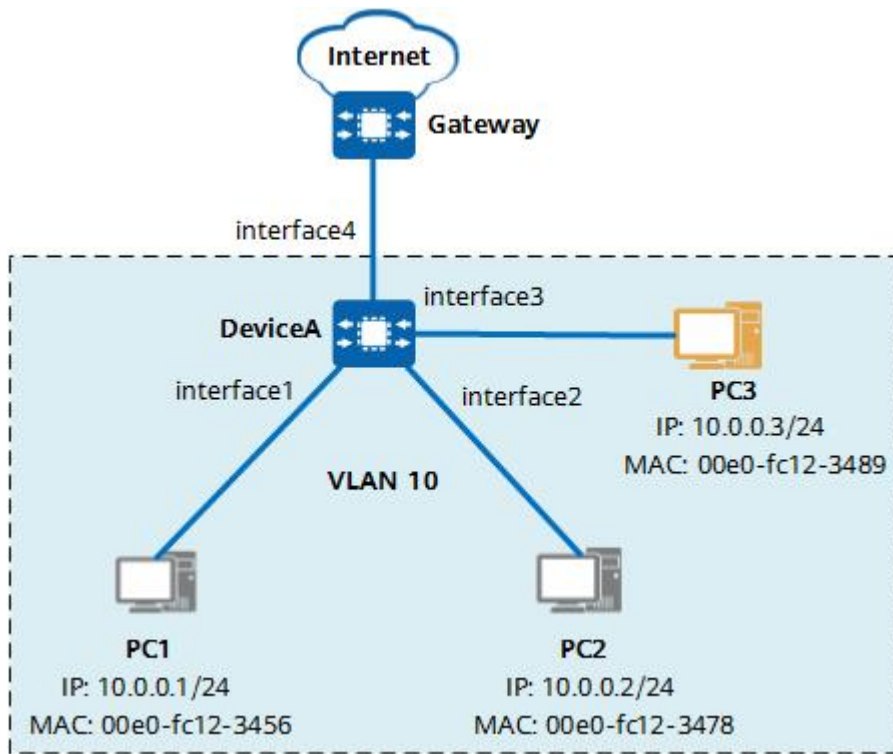
组网需求

如[图 基于 VLAN 配置静态绑定表的 IPSG 组网图](#)所示，PC1 和 PC2 通过 DeviceA 接入网络，Gateway 为企业出口网关，PC1 和 PC2 均使用静态配置的 IP 地址。管理员在 DeviceA 上做了接口限制，希望 PC 使用管理员分配的固定 IP 地址、从固定的接口上线。同时为了安全考虑，不允许外来人员的电脑随意接入内网。

图 1 基于 VLAN 配置静态绑定表的 IPSG 组网图

 说明

本例中 interface1、interface2、interface3 和 interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3 和 10GE1/0/4。



操作步骤

1. 配置各接口所属 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 10
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10GE 1/0/3
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 10
[DeviceA-10GE1/0/3] quit
[DeviceA] interface 10GE 1/0/4
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/4] quit
```

2. 在 DeviceA 的 10GE1/0/1 和 10GE1/0/2 接口上创建静态绑定表项。

```
[DeviceA] user-bind static ip-address 10.0.0.1 mac-address 00e0-fc12-3456 interface 10GE 1/0/1
[DeviceA] user-bind static ip-address 10.0.0.2 mac-address 00e0-fc12-3478 interface 10GE 1/0/2
```

3. 配置上行口 10GE1/0/4 为信任接口。

```
[DeviceA] dhcp enable
[DeviceA] dhcp snooping enable
[DeviceA] interface 10GE 1/0/4
[DeviceA-10GE1/0/4] dhcp snooping trusted
[DeviceA-10GE1/0/4] quit
```

4. 在连接 PC 的 VLAN10 上使能 IPSP 功能。

```
[DeviceA] vlan 10
[DeviceA-vlan10] ipv4 source check user-bind enable
[DeviceA-vlan10] quit
```

检查配置结果

查看静态绑定表信息。

```
[DeviceA] display ip source check user-bind status
```

DHCP Bind-table on slot 1:

IP Address	Prefix	MAC Address	Vlan(O/I)	Interface	Type	Status
10.0.0.1	-	00e0-fc12-3456	- /-	10GE1/0/1	Static	IPv4/-
10.0.0.2	-	00e0-fc12-3478	- /-	10GE1/0/2	Static	IPv4/-

Total count: 2

配置脚本

DeviceA

```
#
sysname DeviceA
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.0.0.1 mac-address 00e0-fc12-3456 interface 10GE1/0/1
user-bind static ip-address 10.0.0.2 mac-address 00e0-fc12-3478 interface 10GE1/0/2
#
vlan batch 10
#
vlan 10
ipv4 source check user-bind enable
#
```

```
interface 10GE1/0/1
 port default vlan 10
#
interface 10GE1/0/2
 port default vlan 10
#
interface 10GE1/0/3
 port default vlan 10
#
interface 10GE1/0/4
 port link-type trunk
 port trunk allow-pass vlan 10
 dhcp snooping trusted
#
return
```

1.1.5.13.1.3 举例：配置 IPSPG 防止 DHCP 动态主机私自更改 IP 地址

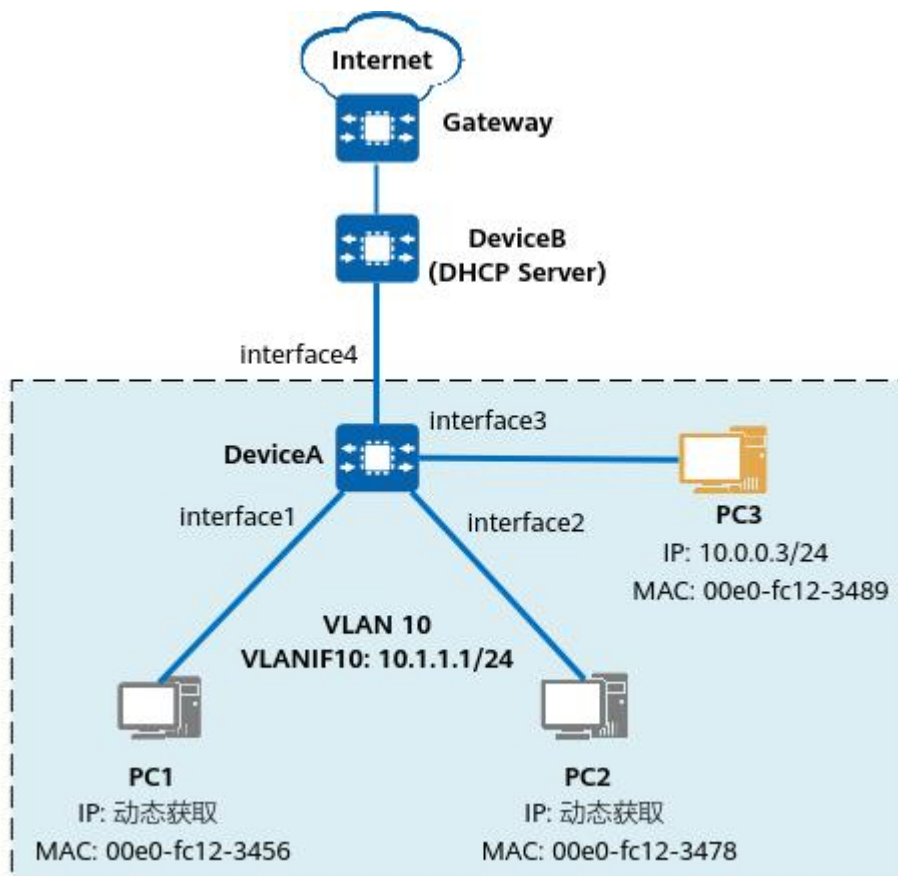
组网需求

如[图 1](#)所示，PC1、PC2 和 PC3 通过 DeviceA 接入网络，DeviceB 作为 DHCP Server 为 PC1 和 PC2 动态分配 IP 地址，PC3 使用静态 IP 地址，Gateway 为企业出口网关。管理员希望 PC 不能私自配置静态 IP 地址，私自配置 IP 地址后将无法访问网络。

说明

本例中 interface1、interface2、interface3 和 interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3 和 10GE1/0/4。

图 1 配置 IPSPG 防止 DHCP 动态主机私自更改 IP 地址组网图



操作步骤

1. 在 DeviceB 上配置 DHCP Server 功能。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10
[DeviceB] interface 10GE 1/0/1
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceB-10GE1/0/1] quit
[DeviceB] dhcp enable
[DeviceB] ip pool 10
[DeviceB-ip-pool-10] network 10.1.1.0 mask 24
[DeviceB-ip-pool-10] gateway-list 10.1.1.1
[DeviceB-ip-pool-10] quit
[DeviceB] interface vlanif 10
[DeviceB-Vlanif10] dhcp enable
[DeviceB] interface vlanif 10
[DeviceB-Vlanif10] ip address 10.1.1.1 255.255.255.0
[DeviceB-Vlanif10] dhcp select global
[DeviceB-Vlanif10] quit
```

2. 在 DeviceA 上配置 DHCP Snooping 功能。

配置各接口所属 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 10
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10GE 1/0/3
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 10
[DeviceA-10GE1/0/3] quit
[DeviceA] interface 10GE 1/0/4
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/4] quit
```

使能 DHCP Snooping 功能，并将连接 DHCP Server 的 10GE1/0/4 接口配置为信任接口。

```
[DeviceA] dhcp enable
[DeviceA] dhcp snooping enable
[DeviceA] vlan 10
[DeviceA-vlan10] dhcp snooping enable
[DeviceA-vlan10] dhcp snooping trusted interface 10GE 1/0/4
```

3. 创建 PC3 的静态绑定表项。

```
[DeviceA] user-bind static ip-address 10.1.1.2 mac-address 00e0-fc12-3489 interface 10GE 1/0/3 vlan 10
```

4. 在连接 PC 的 VLAN10 上使能 IPSG 功能。

```
[DeviceA] vlan 10
[DeviceA-vlan10] ipv4 source check user-bind enable
[DeviceA-vlan10] quit
```

检查配置结果

查看 PC1 和 PC2 的动态绑定表信息。

```
[DeviceA] display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
```


IP Address	MAC Address	VSI/VLAN(O/I/P)	Interface	Lease
10.1.1.254	00e0-fc12-3456	10 /-- /--	GE10GE1/0/1	2014.08.17-07:31
10.1.1.253	00e0-fc12-3478	10 /-- /--	GE10GE1/0/2	2014.08.17-07:34

Print count:	2	Total count:	2	

查看 PC3 的静态绑定表信息。

```
[DeviceA] display user-bind static all
```

DHCP static Bind-table:

Flags:O – outer vlan ,I – inner vlan

IP Address	MAC Address	VLAN(O/I)	Interface
10.1.1.2	00e0-fc12-3489	10/--	10GE1/0/3

Print count: 1 Total count: 1

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
user-bind static ip-address 10.1.1.2 mac-address 00e0-fc12-3489 interface 10GE 1/0/3 vlan 10
#
vlan 10
dhcp snooping enable
dhcp snooping trusted interface 10GE 1/0/4
ipv4 source check user-bind enable
#
interface 10GE 1/0/1
port link-type access
port default vlan 10
#
interface 10GE 1/0/2
port link-type access
port default vlan 10
#
```

```
interface 10GE 1/0/3
port link-type access
port default vlan 10
#
interface 10GE 1/0/4
port link-type trunk
port trunk allow-pass vlan 10
#
return
```

DeviceB

```
#
sysname DeviceB
#
vlan batch 10
#
dhcp enable
#
ip pool 10
gateway-list 10.1.1.1
network 10.1.1.0 mask 255.255.255.0
#
interface Vlanif10
ip address 10.1.1.1 255.255.255.0
dhcp select global
#
interface 10GE 1/0/1
port link-type trunk
port trunk allow-pass vlan 10
#
return
```

1.1.5.13.1.4 举例：基于 VLAN 配置动态绑定表的 IPSG

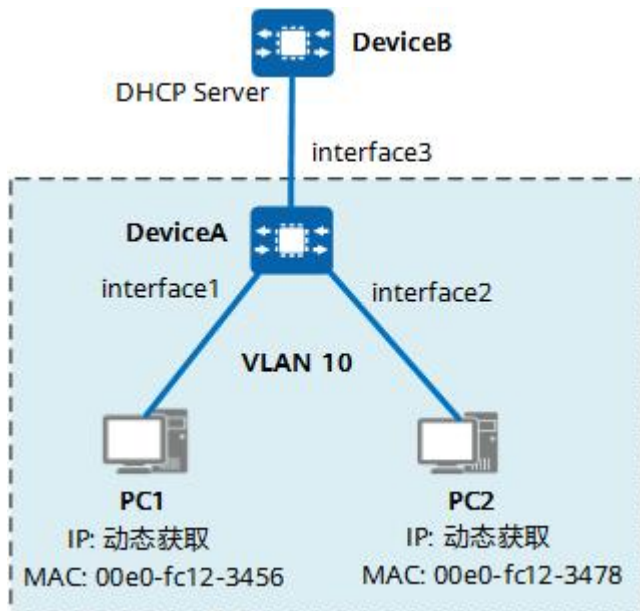
组网需求

如图 [基于 VLAN 配置动态绑定表的 IPSP 组网图](#) 所示，PC1 和 PC2 通过 DeviceA 接入网络。管理员希望 PC 使用动态分配的地址，不允许私自配置静态 IP 地址，如果私自指定 IP 地址将无法访问网络。

图 1 基于 VLAN 配置动态绑定表的 IPSP 组网图

说明

本例中 interface1、interface2 和 interface3 分别代表 10GE1/0/1、10GE1/0/2 和 10GE1/0/3。



操作步骤

1. 配置各接口所属 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10GE 1/0/1
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10GE 1/0/2
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 10
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10GE 1/0/3
[DeviceA-10GE1/0/3] port link-type trunk
[DeviceA-10GE1/0/3] port trunk allow-pass vlan 10
[DeviceA-10GE1/0/3] quit
```

2. 使能 DHCP Snooping 功能，并将连接 DHCP Server 的 10GE1/0/3 接口配置为信任接口。

```
[DeviceA] dhcp enable
[DeviceA] dhcp snooping enable
[DeviceA] vlan 10
[DeviceA-vlan10] dhcp snooping enable
[DeviceA-vlan10] dhcp snooping trusted interface 10GE 1/0/3
```

3. 在 DeviceA 的 VLAN10 上使能 IPSG 功能。

```
[DeviceA-vlan10] ipv4 source check user-bind enable
[DeviceA-vlan10] quit
```

检查配置结果

查看动态绑定表信息。

[DeviceA] display ip source check user-bind status

DHCP Bind-table on slot 1:

IP Address	MAC Address	Vlan(O/I)	Interface	Type	Status
10.1.1.254	00e0-fc12-3456	10 /-	10GE1/0/1	Dynamic	IPv4/-
10.1.1.253	00e0-fc12-3478	10 /-	10GE1/0/2	Dynamic	IPv4/-
Total count:		2			

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 10
#
dhcp enable
#
dhcp snooping enable
#
vlan 10
  dhcp snooping enable
  dhcp snooping trusted interface 10GE1/0/3
  ipv4 source check user-bind enable
#
interface 10GE1/0/1
  port default vlan 10
#
interface 10GE1/0/2
  port default vlan 10
#
interface 10GE1/0/3
  port link-type trunk
  port trunk allow-pass vlan 10
#
return
```

1.1.5.13.2 端口安全

举例：配置端口安全

1.1.5.13.2.1 举例：配置端口安全

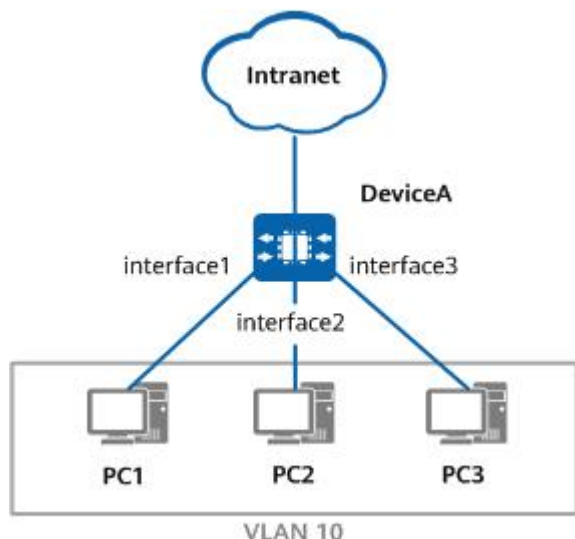
组网需求

如图 1 所示，本公司员工的 PC1、PC2、PC3，在同一个 VLAN10 中可以互通，并且通过接入设备 DeviceA 连接到公司网络。为了保证公司网络的安全性，希望仅允许本公司员工的 PC1、PC2、PC3 可以访问公司网络，其他外来人员使用自己携带的 PC 禁止访问公司网络。

图 1 端口安全组网图

说明

本例中 interface1, interface2, interface3 分别代表 10GE1/0/1, 10GE1/0/2, 10GE1/0/3。



配置思路

1. 配置 VLAN，实现本公司员工 PC 间互通。
2. 配置端口安全功能，限制接口 MAC 学习数量，阻止外来人员 PC 访问公司网络。

操作步骤

1. 配置 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
```

```
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 10
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port link-type access
[DeviceA-10GE1/0/3] port default vlan 10
[DeviceA-10GE1/0/3] quit
```

2. 配置端口安全功能。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port-security enable maximum 1
[DeviceA-10GE1/0/1] port-security mac-address sticky
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] port-security enable maximum 1
[DeviceA-10GE1/0/2] port-security mac-address sticky
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] port-security enable maximum 1
[DeviceA-10GE1/0/3] port-security mac-address sticky
[DeviceA-10GE1/0/3] quit
```

检查配置结果

DeviceA 的这 3 个接口，插入 PC1、PC2、PC3 以外的其他 PC，无法访问公司网络。

配置脚本

```
#
sysname DeviceA
#
vlan batch 10
#
interface 10GE1/0/1
port default vlan 10
port-security enable maximum 1
```

```
port-security mac-address sticky
#
interface 10GE1/0/2
port default vlan 10
port-security enable maximum 1
port-security mac-address sticky
#
interface 10GE1/0/3
port default vlan 10
port-security enable maximum 1
port-security mac-address sticky
#
return
```

1.1.5.14 QoS

[流量统计](#)

[流量监管、流量整形和接口限速](#)

[拥塞管理](#)

1.1.5.14.1 流量统计

[举例：配置基于 MQC 的流量统计](#)

1.1.5.14.1.1 举例：配置基于 MQC 的流量统计

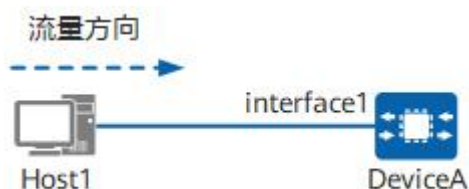
组网需求

如[图 1](#)所示，Host1 发往 DeviceA 的报文中，业务报文的 802.1p 优先级为 6。现在对业务报文进行流量统计，以确定带宽资源的分配。

图 1 配置流量统计组网图

说明

本例中 interface1 代表 10GE1/0/1。



操作步骤

1. 配置 ACL 规则

在 DeviceA 上创建编码为 4000 的二层 ACL，匹配 802.1p 值为 6 的报文。

```
[DeviceA] acl 4000
[DeviceA-acl-L2-4000] rule permit 8021p 6
[DeviceA-acl-L2-4000] quit
```

2. 配置流分类

在 DeviceA 上创建流分类 c1，匹配规则为 ACL4000。

```
[DeviceA] traffic classifier c1
[DeviceA-classifier-c1] if-match acl 4000
[DeviceA-classifier-c1] quit
```

3. 配置流行为

在 DeviceA 上创建流行为 b1，并配置流量统计动作。

```
[DeviceA] traffic behavior b1
[DeviceA-behavior-b1] statistics enable
[DeviceA-behavior-b1] quit
```

4. 配置流策略并应用到接口上

在 DeviceA 上创建流策略 p1，将流分类和对应的流行为进行绑定。

```
[DeviceA] traffic policy p1
[DeviceA-trafficpolicy-p1] classifier c1 behavior b1
[DeviceA-trafficpolicy-p1] quit
```

将流策略 p1 应用到接口 10GE1/0/1 的入方向上。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] traffic-policy p1 inbound
[DeviceA-10GE1/0/1] quit
[DeviceA] quit
```

检查配置结果

查看 ACL 规则的配置信息。

```
<DeviceA> display acl 4000
L2 ACL 4000, 1 rule
ACL's step is 5
rule 5 permit 8021p 6 (0 times matched)
```

查看流分类的配置信息。

```
<DeviceA> display traffic classifier c1
Traffic Classifier Information:
Classifier: c1
```



```
Type: OR
Rule(s):
  if-match acl 4000
```

查看流策略的配置信息。

```
<DeviceA> display traffic policy p1
Traffic Policy Information:
  Policy: p1
  Classifier: c1
  Type: OR
  Behavior: b1
  Statistics: enable
```

查看流量统计信息。

```
<DeviceA> display traffic-policy statistics interface 10ge 1/0/1 inbound
Traffic policy: p1, inbound

-----
Slot: 1
Item          Packets      Bytes      pps      bps
-----
Matched       212185      22067448   1600     1379215
Passed        212185      22067448   1600     1379215
Dropped         0           0          0         0
Filter         0           0          0         0
CAR            0           0          0         0
-----
```

可以看到接口 10GE1/0/1 下业务报文的流量统计信息。

配置脚本

DeviceA 的配置脚本

```
#
sysname DeviceA
#
vlan batch 100
#
acl number 4000
  rule 5 permit 8021p 6
#
traffic classifier c1 type or
  if-match acl 4000
#
traffic behavior b1
```

```
statistics enable
#
traffic policy p1
 classifier c1 behavior b1 precedence 5
#
interface 10GE1/0/1
 traffic-policy p1 inbound
#
return
```

1.1.5.14.2 流量监管、流量整形和接口限速

举例：配置基于 DiffServ 域优先级映射的流量整形

举例：配置基于信任 802.1p 优先级的流量整形

举例：配置流量监管实现接口限速

举例：配置一级 CAR 的流量监管（MQC 方式）

1.1.5.14.2.1 举例：配置基于 DiffServ 域优先级映射的流量整形

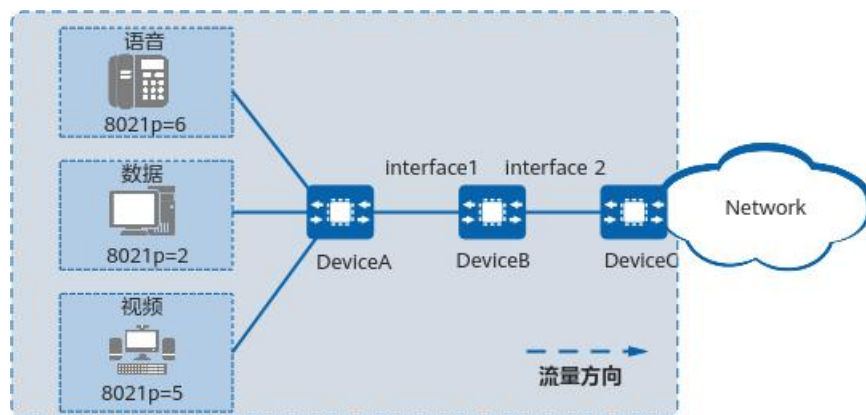
组网需求

如[图 1](#)所示，来自用户侧的业务有语音、视频、数据，通过 DeviceA 和 DeviceB 上送报文，经 DeviceC 与外部网络互通。

图 1 流量整形配置组网图

说明

本例中 interface1、interface2 分别代表 10GE1/0/1、10GE1/0/2。



语音、视频、数据业务的报文使用 802.1p 优先级进行标识，分别为 6、5、2。接口带宽限制为 10000kbit/s。当报文从 DeviceB 的 interface2 到达 DeviceC 时，可能会发生抖动。为了减少带宽抖动，同时保证各类业务带宽要求，现要求如下：

表 1 DeviceB 上为各业务提供的带宽

接口/业务类型	保证带宽（kbit/s）	峰值带宽（kbit/s）
语音	3000	5000
视频	5000	8000
数据	2000	3000

操作步骤

1. 在 DeviceB 上创建 VLAN 并配置各接口，使用户能够通过 DeviceB 访问网络。

创建 VLAN 10。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10
```

将接口 10GE1/0/1、10GE1/0/2 分别以 Trunk 方式加入 VLAN 10。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 10
[DeviceB-10GE1/0/2] quit
```

2. 配置优先级映射

创建 DiffServ 域 ds1，将 802.1p 优先级 6、5、2 分别映射为 PHB 行为 CS7、EF、AF2。

```
[DeviceB] diffserv domain ds1
[DeviceB-dsdomain-ds1] 8021p-inbound 6 phb cs7 //将不同业务携带的 802.1p 优先级映射为不同的 PHB 行为，保证其分别进入不同的队列
[DeviceB-dsdomain-ds1] 8021p-inbound 5 phb ef
[DeviceB-dsdomain-ds1] 8021p-inbound 2 phb af2
[DeviceB-dsdomain-ds1] quit
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] trust upstream ds1
[DeviceB-10GE1/0/1] quit
```

3. 配置接口整形

在 DeviceB 上配置接口整形，将接口速率限制在 10000kbit/s。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] qos lr cir 10000 outbound //在接口的流量出方向配置基于接口的限速，限制总带宽
```

4. 配置端口队列整形

在 DeviceB 上配置端口队列整形，使语音、视频、数据业务的带宽分别限制为 3000kbit/s、5000kbit/s、2000kbit/s，最多分别不超过 5000kbit/s、8000kbit/s、3000kbit/s。

```
[DeviceB-10GE1/0/2] qos queue 7 shaping cir 3000 pir 5000 //根据 PHB 与本地优先级缺省的映射关系，配置进入队列 7 的语音报文带宽为 3000kbit/s
[DeviceB-10GE1/0/2] qos queue 5 shaping cir 5000 pir 8000
[DeviceB-10GE1/0/2] qos queue 2 shaping cir 2000 pir 3000
[DeviceB-10GE1/0/2] quit
```

检查配置结果

查看 10GE1/0/2 出方向队列统计计数。

```
[DeviceB] display qos queue statistics interface 10ge 1/0/2
```

Queue	CIR/PIR	Passed	Pass Rate	Dropped	Drop Rate	Drop Time
	(% or kbps)	(Packets/Bytes)	(pps/bps)	(Packets/Bytes)	(pps/bps)	

0	0	0	0	0	0	-
	10000000	0	0	0	0	

1	0	0	0	0	0	-
	10000000	0	0	0	0	

2	2000	54584	0	0	0	-
	3000	5676736	0	0	0	

3	0	0	0	0	0	-
	10000000	0	0	0	0	

4	0	0	0	0	0	-
	10000000	0	0	0	0	

5	5000	49648	0	0	0	-
	8000	5163392	0	0	0	

6	0	0	0	0	0	-
	10000000	0	0	0	0	

7	3000	49998	0	0	0	-
	5000	5199792	0	0	0	

配置脚本

DeviceB 的配置脚本

```
#
sysname DeviceB
#
vlan batch 10
#
diffserv domain ds1
 8021p-inbound 6 phb cs7 green
#
interface 10GE1/0/1
 port link-type trunk
 port trunk allow-pass vlan 10
 trust upstream ds1
#
interface 10GE1/0/2
 port link-type trunk
 port trunk allow-pass vlan 10
 qos lr cir 10000 cbs 1250000 outbound
 qos queue 2 shaping cir 2000 pir 3000
 qos queue 5 shaping cir 5000 pir 8000
 qos queue 7 shaping cir 3000 pir 5000
#
return
```

1.1.5.14.2.2 举例：配置基于信任 802.1p 优先级的流量整形

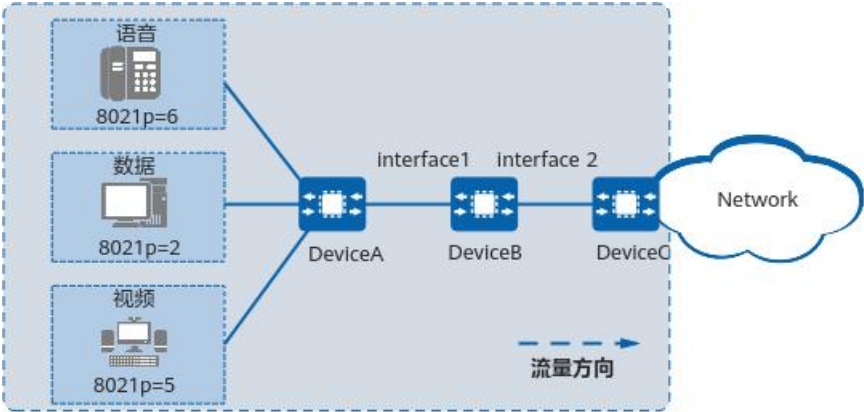
组网需求

如 图 1 所示，来自用户侧的业务有语音、视频、数据，通过 DeviceA 和 DeviceB 上送报文，经 DeviceC 与外部网络互通。

图 1 流量整形配置组网图

说明

本例中 interface1、interface2 分别代表 10GE1/0/1、10GE1/0/2。



语音、视频、数据业务的报文使用 802.1p 优先级进行标识，分别为 6、5、2。接口带宽限制为 10000kbit/s。当报文从 DeviceB 的 interface2 到达 DeviceC 时，可能会发生抖动。为了减少带宽抖动，同时保证各类业务带宽要求，现要求如下：

表 1 DeviceB 上为各业务提供的带宽

接口/业务类型	保证带宽（kbit/s）	峰值带宽（kbit/s）
语音	3000	5000
视频	5000	8000
数据	2000	3000

操作步骤

1. 在 DeviceB 上创建 VLAN 并配置各接口，使用户能够通过 DeviceB 访问网络。

创建 VLAN 10。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10
```

将接口 10GE1/0/1、10GE1/0/2 分别以 Trunk 方式加入 VLAN 10。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10
```

```
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 10
[DeviceB-10GE1/0/2] quit
```

2. 配置接口信任报文的类型

配置接口信任报文的 802.1p 优先级。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] trust 8021p outer //配置接口信任 802.1p 优先级，即报文根据 802.1p 优先级与本地优先级和
队列之间的缺省关系进入不同的队列
[DeviceB-10GE1/0/1] quit
```

3. 配置接口整形

在 DeviceB 上配置接口整形，将接口速率限制在 10000kbit/s。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] qos lr cir 10000 outbound //在接口的流量出方向配置基于接口的限速，限制总带宽
```

4. 配置端口队列整形

在 DeviceB 上配置端口队列整形，使语音、视频、数据业务的带宽分别限制为 3000kbit/s、5000kbit/s、2000kbit/s，最多分别不超过 5000kbit/s、8000kbit/s、3000kbit/s。

```
[DeviceB-10GE1/0/2] qos queue 6 shaping cir 3000 pir 5000 //根据 PHB 与本地优先级缺省的映射关系，配置
进入队列 7 的语音报文带宽为 3000kbit/s
[DeviceB-10GE1/0/2] qos queue 5 shaping cir 5000 pir 8000
[DeviceB-10GE1/0/2] qos queue 2 shaping cir 2000 pir 3000
[DeviceB-10GE1/0/2] quit
```

检查配置结果

查看 10GE1/0/2 出方向队列统计计数。

```
[DeviceB] display qos queue statistics interface 10ge 1/0/2
```

Queue	CIR/PIR	Passed	Pass Rate	Dropped	Drop Rate	Drop Time
(% or kbps)	(Packets/Bytes)	(pps/bps)	(Packets/Bytes)	(pps/bps)		
0	0	0	0	0	0	-
100000000		0	0	0	0	
1	0	0	0	0	0	-
100000000		0	0	0	0	

2	2000	54584	0	0	0	-
	3000	5676736	0	0	0	
3	0	0	0	0	0	-
	10000000	0	0	0	0	
4	0	0	0	0	0	-
	10000000	0	0	0	0	
5	5000	49648	0	0	0	-
	8000	5163392	0	0	0	
6	3000	49998	0	0	0	-
	5000	5199792	0	0	0	
7	0	0	0	0	0	-
	10000000	0	0	0	0	

配置脚本

DeviceB 的配置脚本

```
#
sysname DeviceB
#
vlan batch 10
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 10
trust 8021p outer
#
interface 10GE1/0/1
port link-type trunk
```



```
port trunk allow-pass vlan 10
trust upstream ds1
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 10
qos lr cir 10000 cbs 1250000 outbound
qos queue 2 shaping cir 2000 pir 3000
qos queue 5 shaping cir 5000 pir 8000
qos queue 6 shaping cir 3000 pir 5000
#
return
```

1.1.5.14.2.3 举例：配置流量监管实现接口限速

组网需求

如图 1 所示，Host 通过 DeviceA 上送报文，要求 Host 上送报文的带宽不超过 100Mbit/s。

图 1 接口限速配置组网图

说明

本例中 interface1 代表 10GE1/0/1。



操作步骤

1. 配置 CAR 模板。

在 DeviceA 上创建 CAR 模板 car1，对 Host 的流量进行监管。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] qos car car1 cir 100000
```

2. 应用 CAR 模板。

在 DeviceA 的接口 10GE1/0/1 的入方向应用模板 car1，对 Host 的流量进行监管。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] qos car inbound car1
[DeviceA-10GE1/0/1] quit
```

检查配置结果

查看 CAR 模板的配置信息。

```
[DeviceA] display qos car car1

-----

CAR Name : car1
CAR Index : 0
car cir 100000 kbps cbs 800000 bytes
Applied number on behavior : 0
Applied number on interface inbound : 1
10GE1/0/1
Applied number on Eth-Trunk inbound : 0
Applied number on interface outbound : 0
Applied number on Eth-Trunk outbound : 0
```

分别使用 60000kbit/s 和 110000kbit/s 的速率向接口 10GE1/0/1 输入报文流，然后使用命令 **display qos car statistics** 查看流量统计信息。如果配置成功：使用 60000kbit/s 向接口 10GE1/0/1 输入报文流时，报文全部转发，无丢弃报文；使用 110000kbit/s 向接口 10GE1/0/1 输入报文流时，报文有部分丢弃。

配置脚本

DeviceA 的配置脚本

```
#
sysname DeviceA
#
qos car car1 cir 100000 kbps
#
interface 10GE1/0/1
qos car inbound car1
#
return
```

1.1.5.14.2.4 举例：配置一级 CAR 的流量监管（MQC 方式）

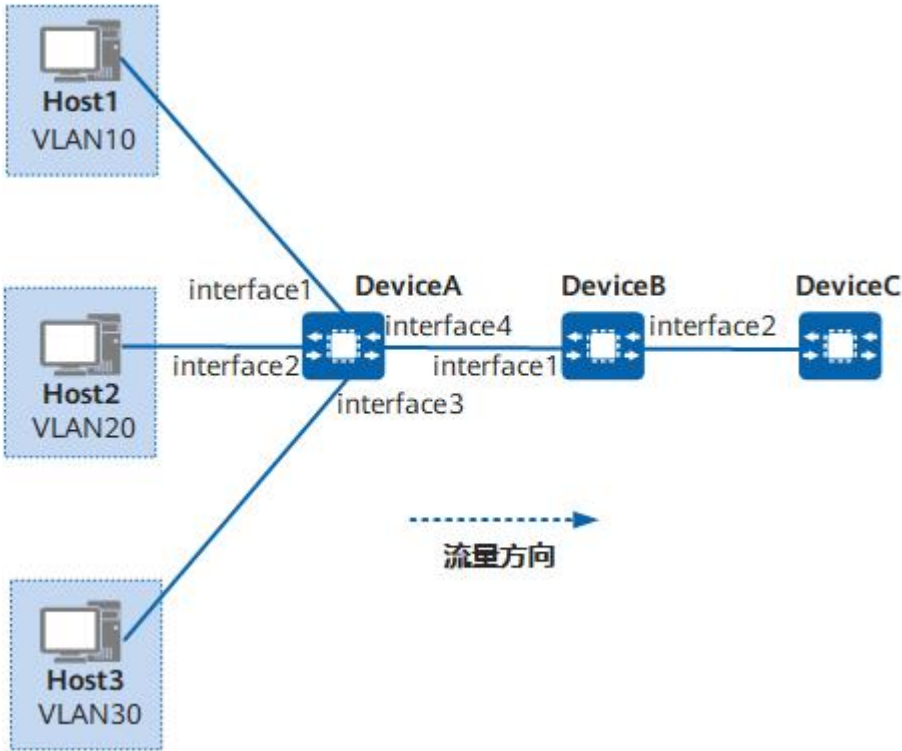
组网需求

如图 1 所示，Host1、Host2 和 Host3 通过 DeviceA 和 DeviceB 上送报文，经 DeviceC 与外部网络互通。把连接 Host1 的接口划分到 VLAN 10，把连接 Host2 的接口划分到 VLAN 20，把连接 Host3 的接口划分到 VLAN 30。

图 1 MQC 实现流量监管配置组网图

说明

本例中 interface1、interface2、interface3、interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4。



根据每个租户的业务量，在 DeviceB 上需要对不同 Host 的报文分别进行流量监管，以将流量限制在一个合理的范围之内，具体带宽需求如表 1 所示。

表 1 DeviceB 为上行流量提供的 QoS 限制

Host	CIR(kbit/s)
Host1	2000
Host2	4000
Host3	8000

操作步骤

1. 创建 VLAN 并配置各接口，使 Host 能够通过 DeviceB 访问网络。
在 DeviceA 上创建 VLAN 10、20、30，并将接口加入相应 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
```

```
[DeviceA] vlan batch 10 20 30
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port default vlan 20
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] portswitch
[DeviceA-10GE1/0/3] port default vlan 30
[DeviceA-10GE1/0/3] quit
[DeviceA] interface 10ge 1/0/4
[DeviceA-10GE1/0/4] portswitch
[DeviceA-10GE1/0/4] port link-type trunk
[DeviceA-10GE1/0/4] port trunk allow-pass vlan 10 20 30
[DeviceA-10GE1/0/4] quit
```

在 DeviceB 上创建 VLAN 10、20、30，并将接口 10GE1/0/1 加入 VLAN。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 10 20 30
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 10 20 30
[DeviceB-10GE1/0/1] quit
```

在 DeviceB 上配置 VLANIF 接口，并配置 IP 地址。

```
[DeviceB] interface vlanif 10
[DeviceB-Vlanif10] ip address 192.168.1.1 24
[DeviceB-Vlanif10] quit
[DeviceB] interface vlanif 20
[DeviceB-Vlanif20] ip address 192.168.2.1 24
[DeviceB-Vlanif20] quit
[DeviceB] interface vlanif 30
[DeviceB-Vlanif30] ip address 192.168.3.1 24
[DeviceB-Vlanif30] quit
```

2. 配置流分类。

在 DeviceB 上创建流分类 c1~c3，对来自不同 Host 的业务流按照其 VLAN ID 进行分类。

```
[DeviceB] traffic classifier c1
[DeviceB-classifier-c1] if-match vlan 10
```

```
[DeviceB-classifier-c1] quit
[DeviceB] traffic classifier c2
[DeviceB-classifier-c2] if-match vlan 20
[DeviceB-classifier-c2] quit
[DeviceB] traffic classifier c3
[DeviceB-classifier-c3] if-match vlan 30
[DeviceB-classifier-c3] quit
```

3. 配置流量监管行为。

在 DeviceB 上创建流行为 b1~b3，对来自不同 Host 的报文进行流量监管。

```
[DeviceB] traffic behavior b1
[DeviceB-behavior-b1] car cir 2000
[DeviceB-behavior-b1] statistics enable
[DeviceB-behavior-b1] quit
[DeviceB] traffic behavior b2
[DeviceB-behavior-b2] car cir 4000
[DeviceB-behavior-b2] statistics enable
[DeviceB-behavior-b2] quit
[DeviceB] traffic behavior b3
[DeviceB-behavior-b3] car cir 8000
[DeviceB-behavior-b3] statistics enable
[DeviceB-behavior-b3] quit
```

4. 配置流策略并应用到入接口上。

在 DeviceB 上创建流策略 p1，将流分类和对应的流行为进行绑定并将流策略应用到接口 10GE1/0/1 入方向上，对来自 Host 的报文进行流量监管。

```
[DeviceB] traffic policy p1
[DeviceB-trafficpolicy-p1] classifier c1 behavior b1
[DeviceB-trafficpolicy-p1] classifier c2 behavior b2
[DeviceB-trafficpolicy-p1] classifier c3 behavior b3
[DeviceB-trafficpolicy-p1] quit
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] traffic-policy p1 inbound
[DeviceB-10GE1/0/1] quit
```

检查配置结果

上述配置完成后，在 DeviceB 上可以查看流量监管的配置信息。

查看流分类的配置信息。

```
[DeviceB] display traffic classifier
Traffic Classifier Information:
Classifier: c1
Type: OR
```

Rule(s):

if-match vlan 10

Classifier: c2

Type: OR

Rule(s):

if-match vlan 20

Classifier: c3

Type: OR

Rule(s):

if-match vlan 30

Total classifier number is 3

查看流策略的配置信息。

[DeviceB] **display traffic policy p1**

Traffic Policy Information:

Policy: p1

Classifier: c1

Type: OR

Behavior: b1

Committed Access Rate:

CIR 2000 (Kbps), PIR 2000 (Kbps), CBS 16000 (Bytes), PBS16000 (Bytes)

Color Mode: color blind

Conform Action: pass

Yellow Action: pass

Exceed Action: discard

Statistics: enable

Classifier: c2

Type: OR

Behavior: b2

Committed Access Rate:

CIR 4000 (Kbps), PIR 4000 (Kbps), CBS 32000 (Bytes), PBS 32000 (Bytes)

Color Mode: color blind

Conform Action: pass

Yellow Action: pass

Exceed Action: discard

Statistics: enable

Classifier: c3

Type: OR

Behavior: b3

Committed Access Rate:

CIR 8000 (Kbps), PIR 8000 (Kbps), CBS 64000 (Bytes), PBS 64000 (Bytes)

Color Mode: color blind

Conform Action: pass

Yellow Action: pass

Exceed Action: discard

Statistics: enable

查看 10GE1/0/1 接口上应用的流策略统计信息。

[DeviceB] display traffic-policy statistics interface 10ge 1/0/1 inbound

Traffic policy: p1, inbound

Slot: 1

Item	Packets	Bytes	pps	bps
Matched	363949175	46585494400	8460795	8663854896
Passed	363949175	46585494400	8460795	8663854896
Dropped	0	0	0	0
Filter	0	0	0	0
CAR	0	0	0	0

可以看出，10GE1/0/1 接口上应用的流策略为 p1。

配置脚本

DeviceB 的配置脚本

```
#
sysname DeviceB
#
vlan batch 10 20 30
#
traffic classifier c1 type or
if-match vlan 10
#
traffic classifier c2 type or
if-match vlan 20
#
traffic classifier c3 type or
if-match vlan 30
#
traffic behavior b1
```

```
statistics enable
car cir 2000 kbps
#
traffic behavior b2
statistics enable
car cir 4000 kbps
#
traffic behavior b3
statistics enable
car cir 8000 kbps
#
traffic policy p1
classifier c1 behavior b1 precedence 5
classifier c2 behavior b2 precedence 10
classifier c3 behavior b3 precedence 15
#
interface Vlanif10
ip address 192.168.1.1 255.255.255.0
#
interface Vlanif20
ip address 192.168.2.1 255.255.255.0
#
interface Vlanif30
ip address 192.168.3.1 255.255.255.0
#
interface 10GE1/0/1
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20 30
traffic-policy p1 inbound
#
return
```

DeviceA 的配置脚本

```
#
sysname DeviceA
#
vlan batch 10 20 30
#
interface 10GE1/0/1
portswitch
port default vlan 10
#
```



```
interface 10GE1/0/2
portswitch
port default vlan 20
#
interface 10GE1/0/3
portswitch
port default vlan 30
#
interface 10GE1/0/4
portswitch
port link-type trunk
port trunk allow-pass vlan 10 20 30
#
return
```

1.1.5.14.3 拥塞管理

举例：配置拥塞管理

举例：配置拥塞避免和拥塞管理综合示例（PQ+WDRR 调度和 WRED 模板）

1.1.5.14.3.1 举例：配置拥塞管理

组网需求

来自 Host1 和 Host2 的业务有语音、视频、数据，这些业务可经由 DeviceB 和 DeviceA 到达用户，为了减轻网络拥塞造成的影响，保证用户对于高优先级、低延迟业务的服务要求，配置需求如表 1 所述。

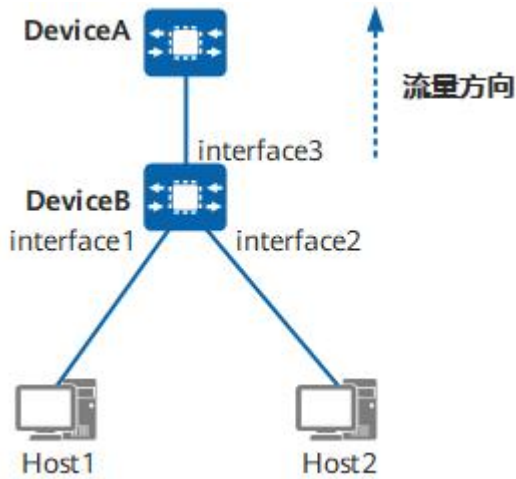
表 1 拥塞管理配置参数

业务类型	设备丢弃优先级	设备内部优先级	调度方式	调度权重
语音	绿	EF	PQ	—
视频	黄	AF3	WDRR	100
数据	红	AF1	WDRR	50

图 1 拥塞管理配置组网图

说明

本例中 interface1，interface2，interface3 分别代表 10GE1/0/1，10GE1/0/2 和 10GE1/0/3。



操作步骤

1. 配置各接口所属的 VLAN，使各设备间链路互通

配置 DeviceB 接口 10GE1/0/3 的接口类型为 trunk，并将接口 10GE1/0/1 加入 VLAN100，接口 10GE1/0/2 加入 VLAN200，接口 10GE1/0/3 加入 VLAN100 和 VLAN200。仅 S6730-H-V2 系列、S5732-H-V2 系列、S5755-H 系列支持命令 **portswitch**。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 100 200
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port default vlan 100
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port default vlan 200
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type trunk
[DeviceB-10GE1/0/3] port trunk allow-pass vlan 100 200
[DeviceB-10GE1/0/3] quit
```

2. 配置优先级映射，根据 802.1p 优先级将语音、数据、视频映射为不同的内部优先级，实现对报文的分类。

创建 DiffServ 域 ds1，将 802.1p 优先级 6、5、2 分别映射为设备内部优先级 EF、AF3、AF1，并分别将丢弃优先级标记为绿色、黄色、红色。

```
[DeviceB] diffserv domain ds1
[DeviceB-dsdomain-ds1] 8021p-inbound 6 phb ef green
[DeviceB-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow
[DeviceB-dsdomain-ds1] 8021p-inbound 2 phb af1 red
```

```
[DeviceB-dsdomain-ds1] quit
```

在 DeviceB 入接口 10GE1/0/1 和 10GE1/0/2 上绑定 DiffServ 域。

```
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] trust 8021p outer
[DeviceB-10GE1/0/1] trust upstream ds1
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] trust 8021p outer
[DeviceB-10GE1/0/2] trust upstream ds1
[DeviceB-10GE1/0/2] quit
```

3. 配置拥塞管理，通过配置各队列的调度参数，如调度方式和权重等，实现对不同优先级队列的差分调度。

在 DeviceB 的报文出接口 10GE1/0/3 上配置各内部优先级对应队列的调度参数。

```
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] qos pq 5 to 7 drr 0 to 4
[DeviceB-10GE1/0/3] qos queue 3 drr weight 100
[DeviceB-10GE1/0/3] qos queue 1 drr weight 50
[DeviceB-10GE1/0/3] quit
[DeviceB] quit
```

检查配置结果

查看 DiffServ 域 ds1 的配置信息。

```
<DeviceB> display diffserv domain ds1
Diffserv domain name:ds1
8021p-inbound 0 phb be green
8021p-inbound 1 phb af1 green
8021p-inbound 2 phb af1 red
8021p-inbound 3 phb af3 green
8021p-inbound 4 phb af4 green
8021p-inbound 5 phb af3 yellow
8021p-inbound 6 phb ef green
8021p-inbound 7 phb cs7 green
8021p-outbound be green map 0
8021p-outbound be yellow map 0
8021p-outbound be red map 0
...
```

可以看到 DiffServ 域中将 802.1p 优先级 6、5、2 分别映射为设备内部优先级 EF、AF3、AF1，并分别将丢弃优先级标记为绿色、黄色、红色。

查看接口 10GE1/0/3 的配置信息，可以看到各内部优先级对应队列的调度参数。

```
<DeviceB> display qos configuration interface 10ge 1/0/3
```

```
interface 10GE1/0/3
-----

trust flag      : outer 8021p
diffserv domain : default
dei enable      : disable
port priority   : 0
phb marking 8021p : disable
phb marking dscp : disable
phb marking exp  : -
port wred       : -
port lr         : cir = -, cbs = -
port car inbound : -
port car outbound : -
schedule profile : -
-----

queue      shaping  schedule  wred
   cir    pir
   cbs    pbs
-----

0      -    -  drr      -
      -    -  weight = 1

1      -    -  drr      -
      -    -  weight = 50

2      -    -  drr      -
      -    -  weight = 1

3      -    -  drr      -
      -    -  weight = 100

4      -    -  drr      -
      -    -  weight = 1

5      -    -  pq       -
      -    -

6      -    -  pq       -
      -    -

7      -    -  pq       -
      -    -
```

配置脚本

DeviceB 的配置脚本

```
#
sysname DeviceB
#
vlan batch 100 200
#
diffserv domain ds1
 8021p-inbound 2 phb af1 red
 8021p-inbound 5 phb af3 yellow
 8021p-inbound 6 phb ef green
#
interface 10GE1/0/1
 port default vlan 100
 trust upstream ds1
#
interface 10GE1/0/2
 port default vlan 200
 trust upstream ds1
#
interface 10GE1/0/3
 port link-type trunk
 port trunk allow-pass vlan 100 200
 qos pq 5 to 7
 qos queue 1 drr weight 50
 qos queue 3 drr weight 100
#
return
```

1.1.5.14.3.2 举例：配置拥塞避免和拥塞管理综合示例（PQ+WDRR 调度和 WRED 模板）

组网需求

DeviceB 通过接口 interface1 与 DeviceA 互连，来自 Internet 的业务有语音、视频、数据，携带的 802.1p 优先级分别为 6、5、2，这些业务可经由 DeviceA 和 DeviceB 到达用户，如[图 1](#)所示。由于 DeviceB 入接口 interface1 的速率大于出接口 interface2、interface3 的速率，在这两个出接口处可能会发生拥塞。

为了减轻网络拥塞造成的影响，保证用户对于高优先级、低延迟业务的服务要求，配置需求如表 1 和表 2 所述。

表 1 拥塞避免配置参数

业务类型	颜色	阈值下限（%）	阈值上限（%）	丢弃概率
语音	绿	80	100	10
视频	黄	60	80	20
数据	红	40	60	40

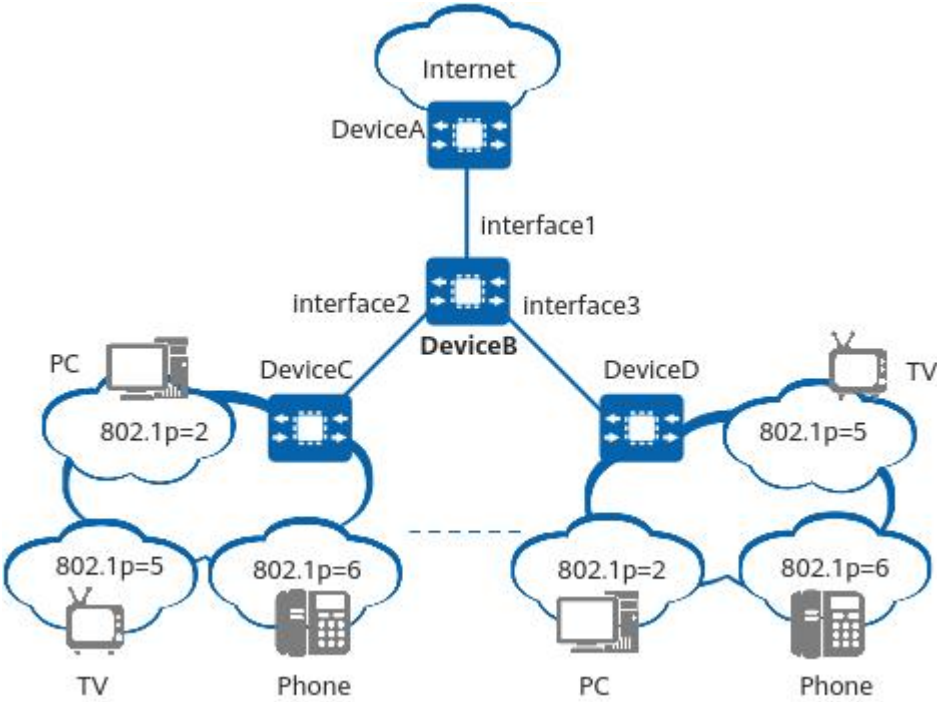
表 2 拥塞管理配置参数

业务类型	服务等级	WDRR
语音	EF	0
视频	AF3	100
数据	AF1	50

图 1 拥塞避免和拥塞管理配置组网图

说明

本例中 interface1，interface2，interface3 分别代表 10GE1/0/1，10GE1/0/2 和 10GE1/0/3。



操作步骤

1. 配置各接口所属的 VLAN，使各设备间链路互通
仅 S6730-H-V2 系列、S5732-H-V2 系列、S5755-H 系列支持命令 `portswitch`。

```

<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan batch 2 5 6
[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] portswitch
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 2 5 6
[DeviceB-10GE1/0/1] quit
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] portswitch
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 2 5 6
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] portswitch
[DeviceB-10GE1/0/3] port link-type trunk
[DeviceB-10GE1/0/3] port trunk allow-pass vlan 2 5 6
[DeviceB-10GE1/0/3] quit

```

2. 配置优先级映射，根据 802.1p 优先级将语音、数据、视频映射为不同的内部优先级，实现对报文的分类。

创建 DiffServ 域 ds1，将 802.1p 优先级 6、5、2 分别映射为设备内部优先级 EF、AF3、AF1，并分别将丢弃优先级标记为绿色、黄色、红色。

```

[DeviceB] diffserv domain ds1
[DeviceB-dsdomain-ds1] 8021p-inbound 6 phb ef green
[DeviceB-dsdomain-ds1] 8021p-inbound 5 phb af3 yellow
[DeviceB-dsdomain-ds1] 8021p-inbound 2 phb af1 red
[DeviceB-dsdomain-ds1] quit

```

在 DeviceB 入接口 10GE1/0/1 上绑定 DiffServ 域。

```

[DeviceB] interface 10ge 1/0/1
[DeviceB-10GE1/0/1] trust 8021p inner
[DeviceB-10GE1/0/1] trust upstream ds1
[DeviceB-10GE1/0/1] quit

```

3. 配置拥塞避免

在 DeviceB 上创建 WRED 模板 wred1，并配置 wred1 的三色报文参数。

```

[DeviceB] drop-profile wred1
[DeviceB-drop-wred1] color green low-limit 80 high-limit 100 discard-percentage 10 //配置 WRED 丢弃模板，设置绿色报文丢弃上下限阈值和最大丢弃概率
[DeviceB-drop-wred1] color yellow low-limit 60 high-limit 80 discard-percentage 20 //配置黄色报文占队列长度百分比为 60%时开始丢弃报文，丢弃概率为 20%，黄色报文占队列长度百分比达到 80%时开始丢弃所有新到达报文
[DeviceB-drop-wred1] color red low-limit 40 high-limit 60 discard-percentage 40

```

```
[DeviceB-drop-wred1] quit
```

在 DeviceB 出接口 10GE1/0/2、10GE1/0/3 上应用 WRED 模板 wred1。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] qos queue 5 wred wred1
[DeviceB-10GE1/0/2] qos queue 3 wred wred1
[DeviceB-10GE1/0/2] qos queue 1 wred wred1
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] qos queue 5 wred wred1
[DeviceB-10GE1/0/3] qos queue 3 wred wred1
[DeviceB-10GE1/0/3] qos queue 1 wred wred1
[DeviceB-10GE1/0/3] quit
```

4. 配置拥塞管理，通过配置各队列的调度参数，如调度方式和权重等，实现对不同优先级队列的差分调度。

在 DeviceB 的报文出接口 10GE1/0/2、10GE1/0/3 上配置各服务等级队列的调度参数。

```
[DeviceB] interface 10ge 1/0/2
[DeviceB-10GE1/0/2] qos pq 5 to 7 drr 0 to 4 //配置 5 到 7 号队列为 PQ 调度，配置 0 到 4 号队列为 WDRR 调度
[DeviceB-10GE1/0/2] qos queue 3 drr weight 100 //配置 3 号队列的 WDRR 调度权值为 100
[DeviceB-10GE1/0/2] qos queue 1 drr weight 50 //配置 1 号队列的 WDRR 调度权值为 50，综上 1 号队列和 3 号
队列中的报文按照 1:2 进行调度
[DeviceB-10GE1/0/2] quit
[DeviceB] interface 10ge 1/0/3
[DeviceB-10GE1/0/3] qos pq 5 to 7 drr 0 to 4 //配置 5 到 7 号队列为 PQ 调度，配置 0 到 4 号队列为 WDRR 调度
[DeviceB-10GE1/0/3] qos queue 3 drr weight 100
[DeviceB-10GE1/0/3] qos queue 1 drr weight 50
[DeviceB-10GE1/0/3] quit
[DeviceB] quit
```

检查配置结果

查看 DiffServ 域 ds1 的配置信息。

```
<DeviceB> display diffserv domain ds1
Diffserv domain name:ds1
8021p-inbound 0 phb be green
8021p-inbound 1 phb af1 green
8021p-inbound 2 phb af1 red
8021p-inbound 3 phb af3 green
8021p-inbound 4 phb af4 green
8021p-inbound 5 phb af3 yellow
8021p-inbound 6 phb ef green
8021p-inbound 7 phb cs7 green
8021p-outbound be green map 0
```



```
8021p-outbound be yellow map 0
8021p-outbound be red map 0
...
```

可以看到 DiffServ 域中将 802.1p 优先级 6、5、2 分别映射为设备内部优先级 EF、AF3、AF1，并分别将丢弃优先级标记为绿色、黄色、红色。

查看 WRED 模板配置信息。

```
[DeviceB] display drop-profile wred1
```

```
Drop-profile[7]: wred1
```

```
Color   Mode   Low-limit  High-limit  Unit  Discard(%)
```

```
-----
```

```
Green   Percentage  80    100    %    10
```

```
Yellow   Percentage  60    80     %    20
```

```
Red      Percentage  40    60     %    40
```

```
-----
```

配置脚本

DeviceB 的配置脚本

```
#
sysname DeviceB
#
vlan batch 2 5 to 6
#
diffserv domain ds1
8021p-inbound 2 phb af1 red
8021p-inbound 5 phb af3 yellow
8021p-inbound 6 phb ef green
#
drop-profile wred1
color green low-limit 80 high-limit 100 discard-percentage 10
color yellow low-limit 60 high-limit 80 discard-percentage 20
color red low-limit 40 high-limit 60 discard-percentage 40
#
interface 10GE1/0/2
port link-type trunk
port trunk allow-pass vlan 2 5 to 6
qos pq 5 to 7 drr 0 to 4
qos queue 1 drr weight 50
qos queue 3 drr weight 100
qos queue 1 wred wred1
qos queue 3 wred wred1
qos queue 5 wred wred1
```

```
#
interface 10GE1/0/3
port link-type trunk
port trunk allow-pass vlan 2 5 to 6
qos pq 5 to 7 drr 0 to 4
qos queue 1 drr weight 50
qos queue 3 drr weight 100
qos queue 1 wred wred1
qos queue 3 wred wred1
qos queue 5 wred wred1
#
interface 10GE1/0/1
port link-type trunk
port trunk allow-pass vlan 2 5 to 6
trust upstream ds1
trust 8021p inner
#
return
```

1.1.5.15 系统监控

镜像

NetStream

1.1.5.15.1 镜像

举例：配置本地端口镜像（N:1）

举例：配置本地端口镜像（1:1）

举例：配置本地端口镜像（1:N，通过单个观察端口方式配置）

举例：配置本地端口镜像（1:N，通过观察端口组方式配置）

举例：配置本地端口镜像（M:N）

举例：配置本地基于 MQC 的流镜像

举例：配置本地 VLAN 镜像

1.1.5.15.1.1 举例：配置本地端口镜像（N:1）

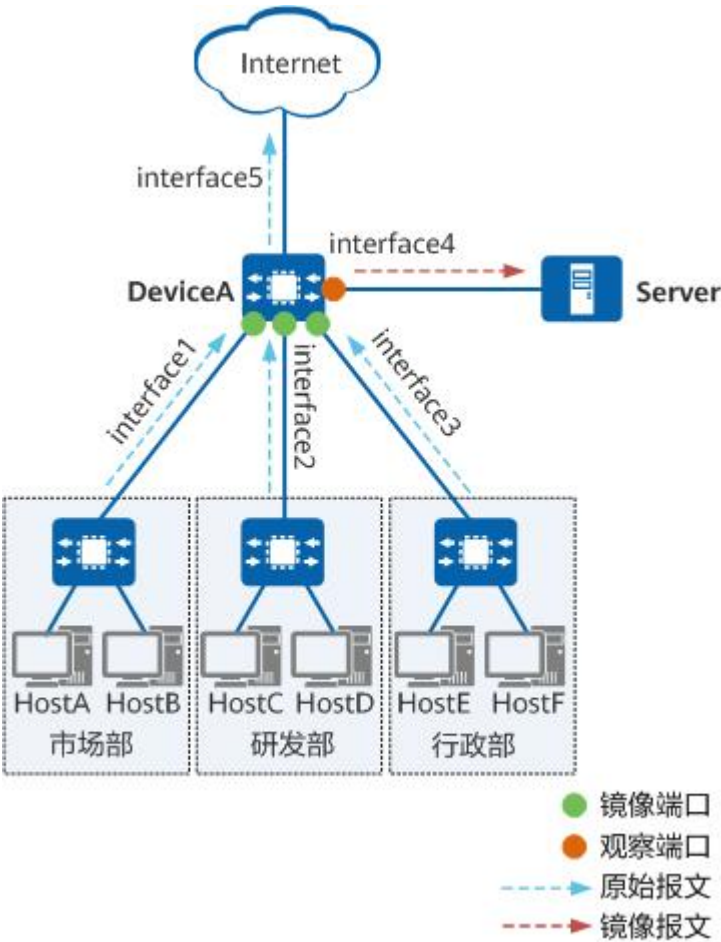
组网需求

如图 1 所示，某公司市场部、研发部、行政部通过 DeviceA 与外部 Internet 通信，监控设备 Server 与 DeviceA 直连。用户希望通过 Server 对这三个部门访问 Internet 的流量进行监控。

图 1 配置本地端口镜像组网图

说明

本例中 interface1、interface2、interface3、interface4、interface5 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4、10GE1/0/5。



操作步骤

1. 在 DeviceA 上配置 10GE1/0/4 为本地观察端口。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] observe-port 1 interface 10ge 1/0/4
```

2. 在 DeviceA 上配置接口 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 为镜像端口，将其入方向绑定到本地观察端口，即将镜像端口接收到的报文复制一份到本地观察端口。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port-mirroring observe-port 1 inbound
[DeviceA-10GE1/0/1] quit
```

```
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] port-mirroring observe-port 1 inbound
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] port-mirroring observe-port 1 inbound
[DeviceA-10GE1/0/3] quit
```

检查配置结果

查看镜像的配置信息。

```
[DeviceA] display port-mirroring
Observe port mirroring:
-----
MirroringPort      Direction      ObservePort : Interface
-----
10GE1/0/1          Inbound        1 : 10GE1/0/4
10GE1/0/2          Inbound        1 : 10GE1/0/4
10GE1/0/3          Inbound        1 : 10GE1/0/4
-----
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
observe-port 1 interface 10GE1/0/4
#
interface 10GE1/0/1
port-mirroring observe-port 1 inbound
#
interface 10GE1/0/2
port-mirroring observe-port 1 inbound
#
interface 10GE1/0/3
port-mirroring observe-port 1 inbound
#
return
```

1.1.5.15.1.2 举例：配置本地端口镜像（1:1）

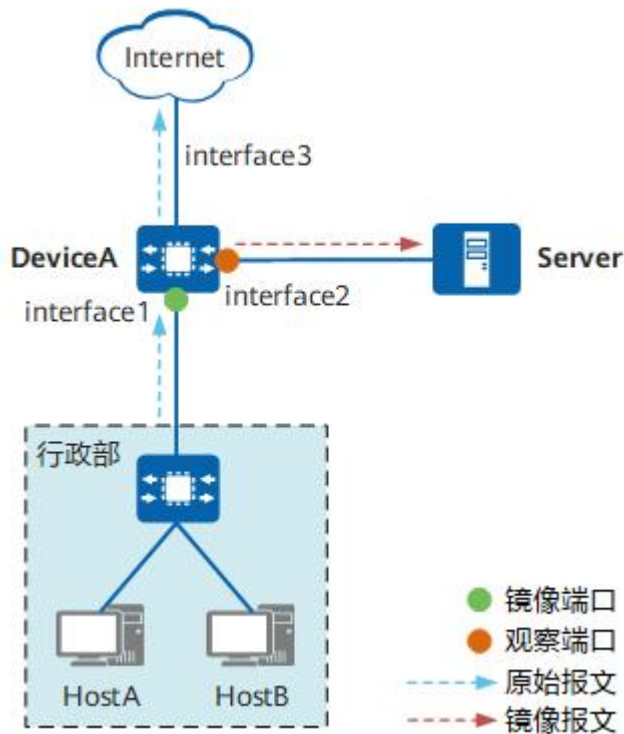
组网需求

如图 1 所示，某公司行政部通过 DeviceA 与外部 Internet 通信，监控设备 Server 与 DeviceA 直连。用户希望通过监控设备 Server 对行政部访问 Internet 的流量进行监控。

图 1 配置本地端口镜像组网图

说明

本例中 interface1、interface2 和 interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 在 DeviceA 上配置 10GE1/0/2 为本地观察端口。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] observe-port 1 interface 10ge 1/0/2
```

2. 在 DeviceA 上配置 10GE1/0/1 为镜像端口，以监控行政部主机发送的报文。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port-mirroring observe-port 1 inbound
[DeviceA-10GE1/0/1] quit
```

检查配置结果

查看镜像的配置信息。

```
[DeviceA] display port-mirroring
Observe port mirroring:
```

MirroringPort	Direction	ObservePort : Interface
10GE1/0/1	Inbound	1 : 10GE1/0/2

配置脚本

DeviceA

```
#
sysname DeviceA
#
observe-port 1 interface 10GE1/0/2
#
interface 10GE1/0/1
port-mirroring observe-port 1 inbound
#
return
```

1.1.5.15.1.3 举例：配置本地端口镜像（1:N，通过单个观察端口方式配置）

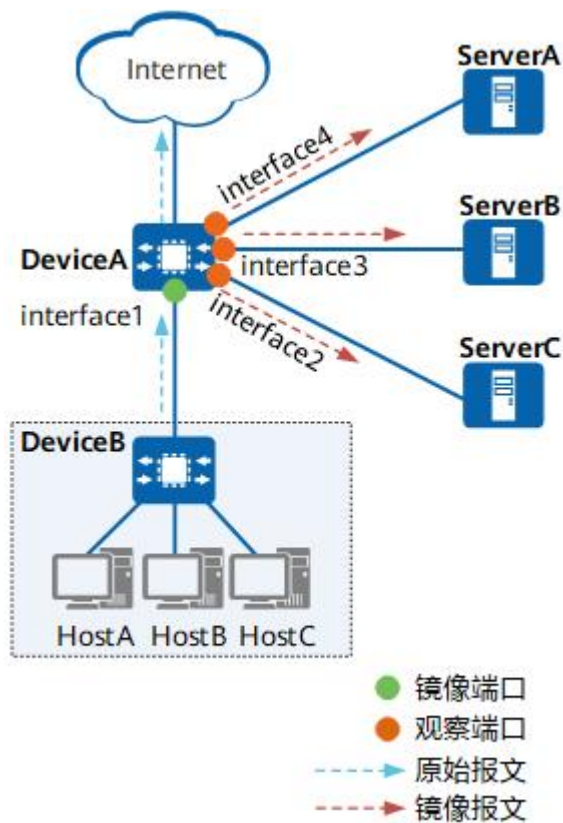
组网需求

如图 1 所示，网络内主机通过 DeviceA 与 Internet 互通，监控设备 ServerA、ServerB 和 ServerC 与 DeviceA 直连。现在希望将网络内主机访问 Internet 的流量镜像到不同 Server 上，对流量进行不同的监控分析。

图 1 配置本地端口镜像组网图

 说明

本例中 interface1、interface2、interface3、interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4。



操作步骤

1. 在 DeviceA 上分别配置接口 10GE1/0/2、10GE1/0/3 和 10GE1/0/4 为观察端口。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] observe-port 1 interface 10ge 1/0/2
[DeviceA] observe-port 2 interface 10ge 1/0/3
[DeviceA] observe-port 3 interface 10ge 1/0/4
```

2. 在 DeviceA 上配置 10GE1/0/1 为镜像端口，将镜像端口入方向流量分别镜像到观察端口 1、2 和 3。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port-mirroring observe-port 1 inbound
[DeviceA-10GE1/0/1] port-mirroring observe-port 2 inbound
[DeviceA-10GE1/0/1] port-mirroring observe-port 3 inbound
[DeviceA-10GE1/0/1] quit
```

检查配置结果

查看观察端口的配置情况。

```
[DeviceA] display observe-port
```

```
-----
Index   : 1
```

```
Interface: 10GE1/0/2
```

```
-----
Index   : 2
Interface: 10GE1/0/3
-----
```

```
-----
Index   : 3
Interface: 10GE1/0/4
-----
```

查看镜像的配置信息。

```
[DeviceA] display port-mirroring
```

```
Observe port mirroring:
```

```
-----
MirroringPort    Direction    ObservePort : Interface
-----
10GE1/0/1        Inbound      1 : 10GE1/0/2
                  Inbound      2 : 10GE1/0/3
                  Inbound      3 : 10GE1/0/4
-----
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
observe-port 1 interface 10GE1/0/2
observe-port 2 interface 10GE1/0/3
observe-port 3 interface 10GE1/0/4
#
interface 10GE1/0/1
port-mirroring observe-port 1 inbound
port-mirroring observe-port 2 inbound
port-mirroring observe-port 3 inbound
#
return
```

1.1.5.15.1.4 举例：配置本地端口镜像（1:N，通过观察端口组方式配置）

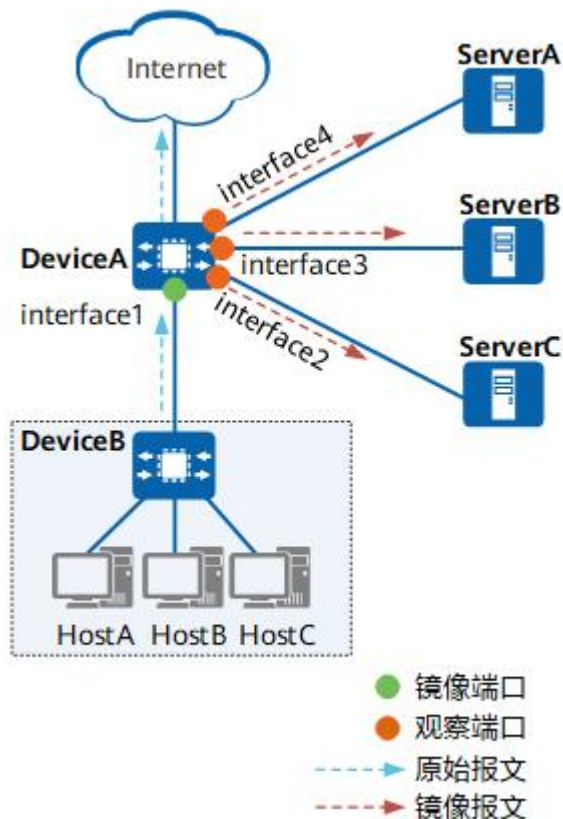
组网需求

如图 1 所示，网络内主机通过 DeviceA 与 Internet 互通，监控设备 ServerA、ServerB 和 ServerC 与 DeviceA 直连。现在希望将网络内主机访问 Internet 的流量镜像到不同 Server 上，对流量进行不同的监控分析。

图 1 配置本地端口镜像组网图

说明

本例中 interface1、interface2、interface3、interface4 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4。



操作步骤

1. 在 DeviceA 上配置观察端口组，将接口 10GE1/0/2、10GE1/0/3 和 10GE1/0/4 加入观察端口组。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] observe-port group 1
[DeviceA-observe-port-group-1] group-member 10ge 1/0/2 to 10ge 1/0/4
[DeviceA-observe-port-group-1] quit
```

2. 在 DeviceA 上配置 10GE1/0/1 为镜像端口，将镜像端口入方向流量镜像到观察端口组 1。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port-mirroring observe-port group 1 inbound
[DeviceA-10GE1/0/1] quit
```

检查配置结果

查看观察端口组的配置情况。

```
[DeviceA] display observe-port
GroupId  MemberPorts
-----
1  10GE1/0/2      10GE1/0/3      10GE1/0/4
-----
```

查看镜像的配置信息。

```
[DeviceA] display port-mirroring
Observe port group mirroring:
-----
MirroringPort  Direction  ObserveGroup
-----
10GE1/0/1      Inbound    1
-----
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
observe-port group 1
group-member 10GE1/0/2
group-member 10GE1/0/3
group-member 10GE1/0/4
#
interface 10GE1/0/1
port-mirroring observe-port group 1 inbound
#
return
```

1.1.5.15.1.5 举例：配置本地端口镜像（M:N）

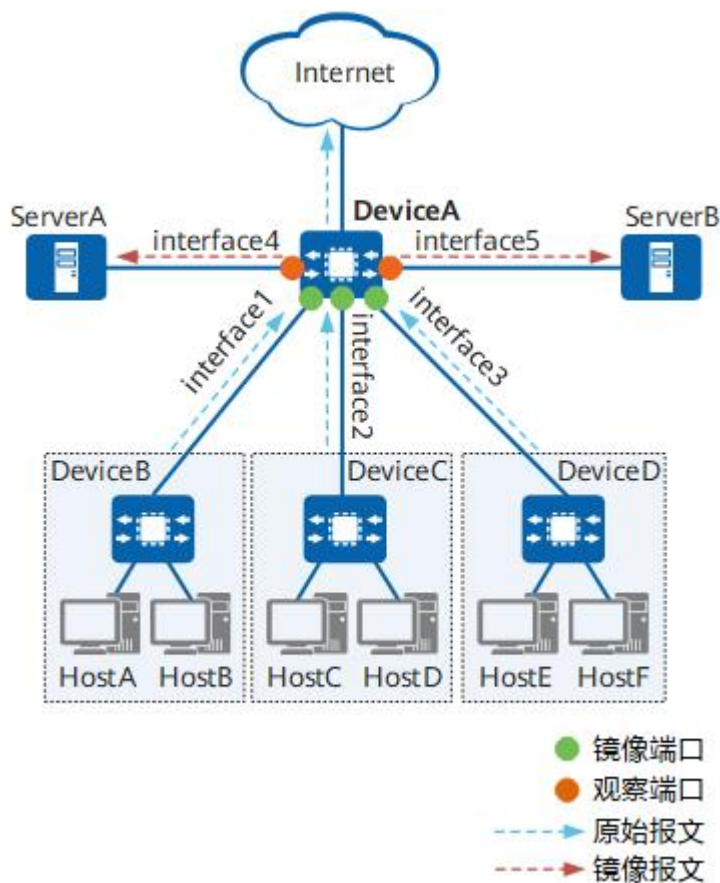
组网需求

如图 1 所示，网络内主机通过 DeviceA 与 Internet 互通，监控设备 ServerA 和 ServerB 与 DeviceA 直连。现在希望将网络内主机访问 Internet 的流量镜像到服务器 ServerA 和 ServerB 上，对流量进行监控分析。

图 1 配置本地端口镜像组网图

说明

本例中 interface1、interface2、interface3、interface4、interface5 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3、10GE1/0/4、10GE1/0/5。



操作步骤

1. 在 DeviceA 上配置观察端口组，将接口 10GE1/0/4 和 10GE1/0/5 加入观察端口组。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] observe-port group 1
[DeviceA-observe-port-group-1] group-member 10ge 1/0/4 to 10ge 1/0/5
[DeviceA-observe-port-group-1] quit
```

2. 在 DeviceA 上分别配置 10GE1/0/1、10GE1/0/2 和 10GE1/0/3 为镜像端口，将镜像端口入方向流量镜像到观察端口组 1。

```
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] port-mirroring observe-port group 1 inbound
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] port-mirroring observe-port group 1 inbound
[DeviceA-10GE1/0/2] quit
[DeviceA] interface 10ge 1/0/3
[DeviceA-10GE1/0/3] port-mirroring observe-port group 1 inbound
```

[DeviceA-10GE1/0/3] quit

检查配置结果

查看观察端口组的配置情况。

```
[DeviceA] display observe-port

-----
Index   : 1
Interface: 10GE1/0/1
-----
Index   : 2
Interface: 10GE1/0/2
-----
GroupId  MemberPorts
-----
   1   10GE1/0/4      10GE1/0/5
-----
```

查看镜像的配置信息。

```
[DeviceA] display port-mirroring
Observe port group mirroring:
-----
MirroringPort    Direction    ObserveGroup
-----
10GE1/0/1        Inbound      1
10GE1/0/2        Inbound      1
10GE1/0/3        Inbound      1
-----
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
observe-port group 1
group-member 10GE1/0/4
group-member 10GE1/0/5
#
interface 10GE1/0/1
port-mirroring observe-port group 1 inbound
#
```

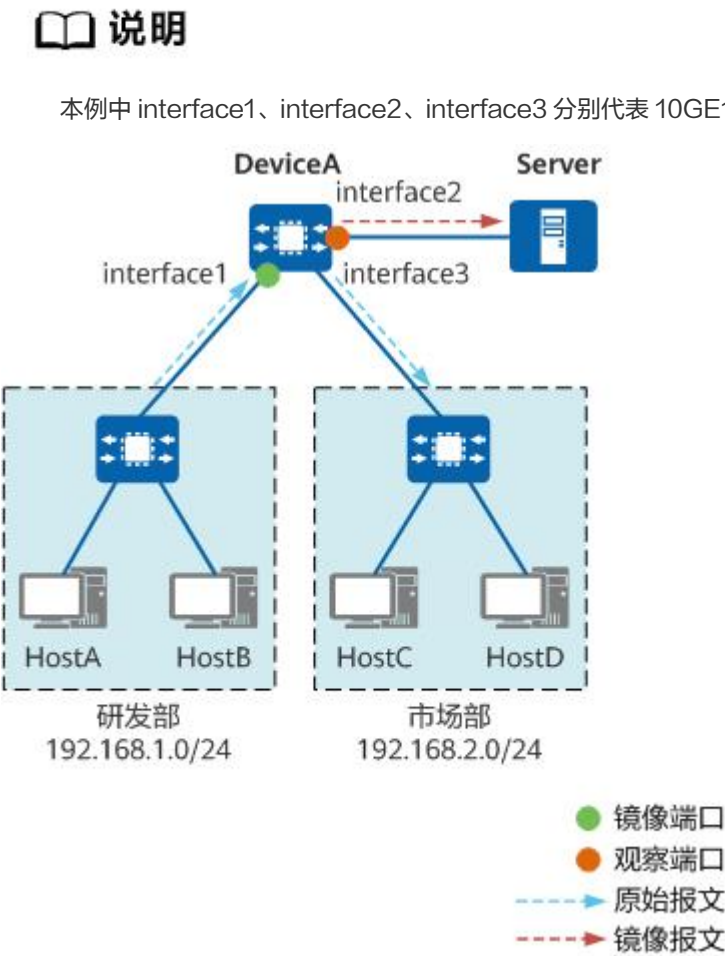
```
interface 10GE1/0/2
port-mirroring observe-port group 1 inbound
#
interface 10GE1/0/3
port-mirroring observe-port group 1 inbound
#
return
```

1.1.5.15.1.6 举例：配置本地基于 MQC 的流镜像

组网需求

如图 1 所示，某公司研发部和市场部分别使用 192.168.1.0/24 和 192.168.2.0/24 两个网段地址，通过 DeviceA 进行通信，监控设备 Server 与 DeviceA 直连。用户希望通过监控设备 Server 对研发部发往市场部的报文进行监控。

图 1 配置本地基于 MQC 的流镜像组网图



操作步骤

1. 在 DeviceA 上配置 10GE1/0/2 为观察端口。

```
<HUAWEI> system-view
```

```
[HUAWEI] sysname DeviceA
[DeviceA] observe-port 1 interface 10ge 1/0/2
```

2. 在 DeviceA 上创建流分类 c1，并配置流分类规则为匹配源地址为 192.168.1.0/24，目的地址为 192.168.2.0/24 的报文。

```
[DeviceA] acl number 3000
[DeviceA-acl4-advance-3000] rule permit ip source 192.168.1.0 24 destination 192.168.2.0 24
[DeviceA-acl4-advance-3000] quit
[DeviceA] traffic classifier c1
[DeviceA-classifier-c1] if-match acl 3000
[DeviceA-classifier-c1] quit
```

3. 在 DeviceA 上创建流行为 b1，并配置流镜像动作。

```
[DeviceA] traffic behavior b1
[DeviceA-behavior-b1] mirroring observe-port 1
[DeviceA-behavior-b1] quit
```

4. 在 DeviceA 上创建流策略 p1，将流分类和对应的流行为进行绑定；并将流策略应用到接口 10GE1/0/1 的入方向上，对研发部访问市场部的报文进行监控。

```
[DeviceA] traffic policy p1
[DeviceA-trafficpolicy-p1] classifier c1 behavior b1
[DeviceA-trafficpolicy-p1] quit
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] traffic-policy p1 inbound
[DeviceA-10GE1/0/1] quit
```

检查配置结果

- # 查看流分类的配置信息。

```
[DeviceA] display traffic classifier c1
Traffic Classifier Information:
Classifier: c1
Type: OR
Rule(s):
if-match acl 3000
```

- # 查看流策略的配置信息。

```
[DeviceA] display traffic policy p1
Traffic Policy Information:
Policy: p1
Classifier: c1
Type: OR
Behavior: b1
```

Mirroring observe-port 1

查看镜像的配置信息。

```
[DeviceA] display port-mirroring
```

```
Traffic mirroring:
```

```
-----
```

TrafficBehavior	ObservePort : Interface
b1	1 : 10GE1/0/2

```
-----
```

配置脚本

DeviceA

```
#
sysname DeviceA
#
observe-port 1 interface 10GE1/0/2
#
acl number 3000
rule 5 permit ip source 192.168.1.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
#
traffic classifier c1 type or
if-match acl 3000
#
traffic behavior b1
mirroring observe-port 1
#
traffic policy p1
classifier c1 behavior b1 precedence 5
#
interface 10GE1/0/1
traffic-policy p1 inbound
#
return
```

1.1.5.15.1.7 举例：配置本地 VLAN 镜像

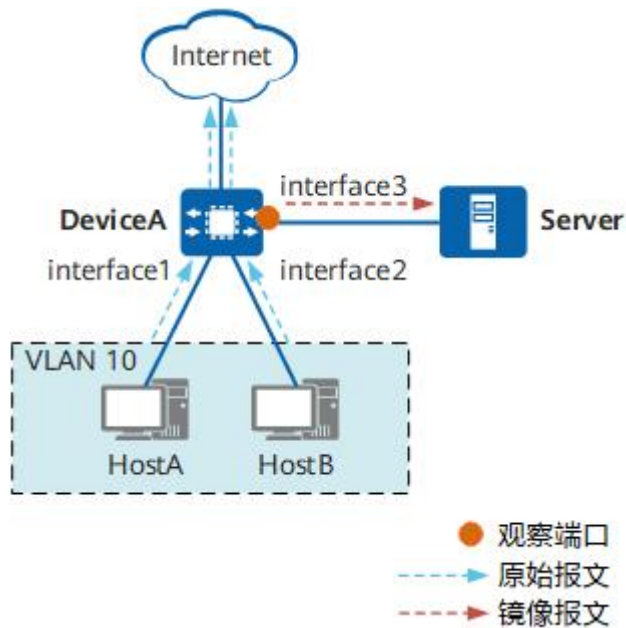
组网需求

如[图 1](#)所示，HostA 和 HostB 同属于 VLAN 10，通过 DeviceA 与外部 Internet 互通。监控设备 Server 与 DeviceA 直连。现在希望通过 Server 对 VLAN 10 内的主机访问 Internet 的流量进行监控。

图 1 配置本地 VLAN 镜像组网图

说明

本例中 interface1、interface2 和 interface3 分别代表 10GE1/0/1、10GE1/0/2、10GE1/0/3。



操作步骤

1. 在 DeviceA 上创建 VLAN 10 并将接口 10GE1/0/1 和 10GE1/0/2 加入 VLAN 10。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] vlan batch 10
[DeviceA] interface 10ge 1/0/1
[DeviceA-10GE1/0/1] portswitch
[DeviceA-10GE1/0/1] port link-type access
[DeviceA-10GE1/0/1] port default vlan 10
[DeviceA-10GE1/0/1] quit
[DeviceA] interface 10ge 1/0/2
[DeviceA-10GE1/0/2] portswitch
[DeviceA-10GE1/0/2] port link-type access
[DeviceA-10GE1/0/2] port default vlan 10
[DeviceA-10GE1/0/2] quit
```

2. 在 DeviceA 上配置 10GE1/0/3 为观察端口。

```
[DeviceA] observe-port 1 interface 10ge 1/0/3
```

3. 在 DeviceA 上配置 VLAN 镜像，将 VLAN 10 内接口接收的报文镜像到观察端口。

```
[DeviceA] vlan 10
[DeviceA-vlan10] mirroring observe-port 1 inbound
[DeviceA-vlan10] quit
```


检查配置结果

查看镜像的配置信息。

[DeviceA] display port-mirroring		
VLAN mirroring:		

VLAN	Direction	ObservePort : Interface

VLAN 10	Inbound	1 : 10GE1/0/3

配置脚本

DeviceA

```
#
sysname DeviceA
#
vlan batch 10
#
observe-port 1 interface 10GE1/0/3
#
vlan 10
  mirroring observe-port 1 inbound
#
interface 10GE1/0/1
  port default vlan 10
#
interface 10GE1/0/2
  port default vlan 10
#
return
```

1.1.5.15.2 NetStream

[举例：配置原始流统计信息的输出功能](#)

[举例：配置灵活流统计信息的输出功能](#)

1.1.5.15.2.1 举例：配置原始流统计信息的输出功能

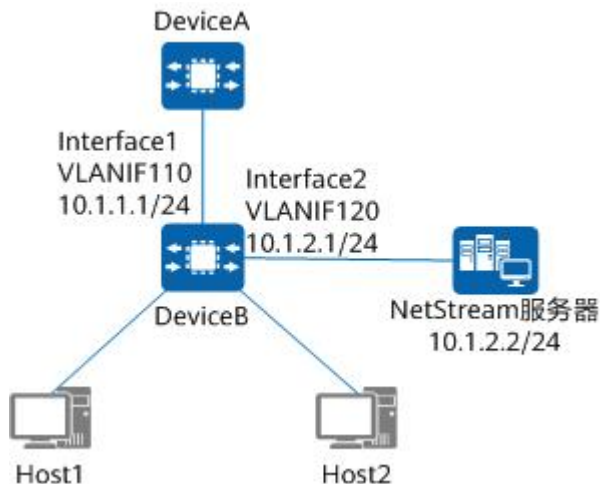
组网需求

如图 [Netstream 组网图](#) 所示，Host1 与 Host2 通过 DeviceB 与 DeviceA 通信，网管人员希望掌握 2 个部门与 DeviceA 通信的流量统计信息，以便进行网络规划。

图 1 Netstream 组网图

说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



操作步骤

1. 如图 [Netstream 组网图](#) 标注所示，配置 DeviceB 的接口 IP 地址。

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceB
[DeviceB] vlan 110
[DeviceB-vlan110] quit
[DeviceB] interface vlanif 110
[DeviceB-Vlanif110] ip address 10.1.1.1 24
[DeviceB-Vlanif110] quit
[DeviceB] interface 10ge1/0/1
[DeviceB-10GE1/0/1] port link-type trunk
[DeviceB-10GE1/0/1] port trunk pvid vlan 110
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 110
[DeviceB-10GE1/0/1] quit
[DeviceB] vlan 120
[DeviceB-vlan120] quit
[DeviceB] interface vlanif 120
[DeviceB-Vlanif120] ip address 10.1.2.1 24
[DeviceB-Vlanif120] quit
[DeviceB] interface 10ge1/0/2
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk pvid vlan 120
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 120
```

```
[DeviceB-10GE1/0/2] quit
```

2. 配置 NetStream 采样功能。

配置 10GE1/0/1 接口出、入流量的 NetStream 采样功能，采样间隔为 8192。

```
[DeviceB] interface 10ge1/0/1
[DeviceB-10GE1/0/1] netstream sampler ip random-packets 8192 inbound
[DeviceB-10GE1/0/1] netstream sampler ip random-packets 8192 outbound
[DeviceB-10GE1/0/1] quit
```

3. 配置 NetStream 的流老化。

配置非活跃流的过期时间为 100 秒，以及开启由 TCP 连接的 FIN 和 RST 报文触发老化。

```
[DeviceB] netstream timeout ip inactive 100
[DeviceB] netstream timeout ip tcp-session
```

4. 配置 NetStream 原始流统计信息输出。

配置 NetStream 原始流统计信息输出报文源地址为 10.1.2.1，目的地址为 10.1.2.2，目的端口号为 6000，DSCP 为 0。

```
[DeviceB] netstream export ip source 10.1.2.1
[DeviceB] netstream export ip host 10.1.2.2 6000 dscp 0
```

5. 配置输出报文版本格式。

缺省情况下，输出报文版本格式为 V9。

6. 使能接口的原始流 NetStream 统计功能。

使能 10GE1/0/1 接口出、入流量的 NetStream 统计功能。

```
[DeviceB] assign forward enp netstream enable
[DeviceB] interface 10ge1/0/1
[DeviceB-10GE1/0/1] netstream outbound ip
[DeviceB-10GE1/0/1] netstream inbound ip
[DeviceB-10GE1/0/1] quit
```

7. 验证配置结果。

配置成功后，查看流量统计信息显示如下。

```
[DeviceB] display netstream statistics ip slot 1
Last time when statistics were cleared: -
-----
Packet Length  : Number
-----
1   ~ 64 : 0
65  ~ 128 : 14
129 ~ 256 : 1
257 ~ 512 : 0
513 ~ 1024 : 0
1025 ~ 1500 : 0
longer than 1500 : 0
```

StreamType				
Current	Aged	Created	Exported	Exported
(streams)	(streams)	(streams)	(streams)	(Packets)
origin				
0	0	0	0	0

配置脚本

DeviceB

```
#
sysname DeviceB
#
vlan batch 110 120
#
netstream timeout ip inactive 100
netstream timeout ip tcp-session
netstream export ip source 10.1.2.1
netstream export ip host 10.1.2.2 6000 dscp 0
assign forward enp netstream enable
#
interface Vlanif110
ip address 10.1.1.1 255.255.255.0
#
interface Vlanif120
ip address 10.1.2.1 255.255.255.0
#
interface 10GE1/0/1
port link-type trunk
port trunk pvid vlan 110
port trunk allow-pass vlan 110
netstream inbound ip
netstream outbound ip
netstream sampler ip random-packets 8192 inbound
netstream sampler ip random-packets 8192 outbound
#
interface 10GE1/0/2
port link-type trunk
port trunk pvid vlan 120
port trunk allow-pass vlan 120
```

```
#  
return
```

1.1.5.15.2.2 举例：配置灵活流统计信息的输出功能

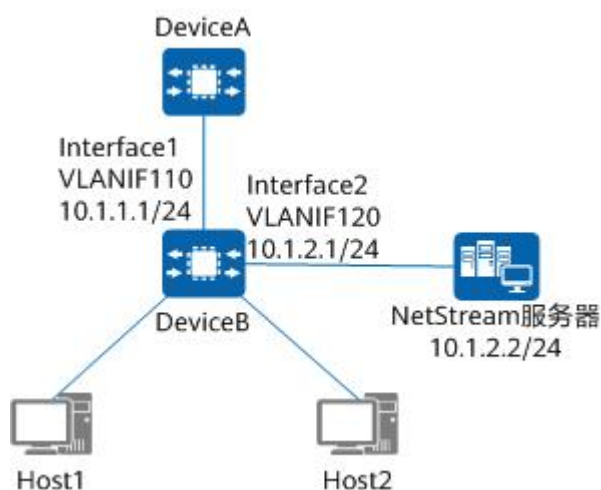
组网需求

如图 [Netstream 组网图](#) 所示，Host1 与 Host2 通过 DeviceB 与 DeviceA 通信，网管人员希望掌握 2 个部门与 DeviceA 通信的流量统计信息，以便进行网络规划。

图 1 Netstream 组网图

说明

本例中 interface1 和 interface2 分别代表 10GE1/0/1 和 10GE1/0/2。



操作步骤

1. 如图 [Netstream 组网图](#) 标注所示，配置 DeviceB 的接口 IP 地址。

```
<HUAWEI> system-view  
[HUAWEI] sysname DeviceB  
[DeviceB] vlan 110  
[DeviceB-vlan110] quit  
[DeviceB] interface vlanif 110  
[DeviceB-Vlanif110] ip address 10.1.1.1 24  
[DeviceB-Vlanif110] quit  
[DeviceB] interface 10ge1/0/1  
[DeviceB-10GE1/0/1] port link-type trunk  
[DeviceB-10GE1/0/1] port trunk pvid vlan 110  
[DeviceB-10GE1/0/1] port trunk allow-pass vlan 110  
[DeviceB-10GE1/0/1] quit  
[DeviceB] vlan 120  
[DeviceB-vlan120] quit
```

```
[DeviceB] interface vlanif 120
[DeviceB-Vlanif120] ip address 10.1.2.1 24
[DeviceB-Vlanif120] quit
[DeviceB] interface 10ge1/0/2
[DeviceB-10GE1/0/2] port link-type trunk
[DeviceB-10GE1/0/2] port trunk pvid vlan 120
[DeviceB-10GE1/0/2] port trunk allow-pass vlan 120
[DeviceB-10GE1/0/2] quit
```

2. 配置灵活流统计模板。

创建名称为“record1”的灵活流统计模板，根据目的地址和源地址进行流量聚合，并配置输出的统计信息中包含字节数和报文数。

```
[DeviceB] netstream record record1 ip
[DeviceB-netstream-record-ipv4-record1] match ip destination-address
[DeviceB-netstream-record-ipv4-record1] match ip source-address
[DeviceB-netstream-record-ipv4-record1] collect counter bytes
[DeviceB-netstream-record-ipv4-record1] collect counter packets
[DeviceB-netstream-record-ipv4-record1] quit
```

3. 配置 NetStream 采样功能。

配置 10GE1/0/1 接口出、入流量的 NetStream 采样功能，采样间隔为 1024。

```
[DeviceB] interface 10ge1/0/1
[DeviceB-10GE1/0/1] netstream sampler ip random-packets 1024 inbound
[DeviceB-10GE1/0/1] netstream sampler ip random-packets 1024 outbound
[DeviceB-10GE1/0/1] quit
```

4. 配置 NetStream 灵活流统计信息输出。

配置 NetStream 灵活流统计信息输出报文的源地址为 10.1.2.1，目的地址为 10.1.2.2，目的端口号为 6000，DSCP 为 0。

```
[DeviceB] netstream export ip source 10.1.2.1
[DeviceB] netstream export ip host 10.1.2.2 6000 dscp 0
```

5. 使能接口的灵活流 NetStream 统计功能。

使能 10GE1/0/1 接口出、入流量的 NetStream 统计功能，并将灵活流统计模板应用到接口上。

```
[DeviceB] assign forward enp netstream enable
[DeviceB] interface 10ge1/0/1
[DeviceB-10GE1/0/1] netstream record record1 ip inbound
[DeviceB-10GE1/0/1] netstream record record1 ip outbound
[DeviceB-10GE1/0/1] netstream inbound ip
[DeviceB-10GE1/0/1] netstream outbound ip
[DeviceB-10GE1/0/1] quit
```

6. 验证配置结果。

配置成功后，查看流量统计信息显示如下。

[DeviceB] display netstream statistics ip slot 1

Last time when statistics were cleared: -

Packet Length : Number

1 ~ 64 : 15
65 ~ 128 : 14
129 ~ 256 : 1
257 ~ 512 : 0
513 ~ 1024 : 0
1025 ~ 1500 : 0
longer than 1500 : 0

StreamType
Current Aged Created Exported Exported
(streams) (streams) (streams) (streams) (Packets)

origin
0 0 0 0 0

record1
2 2 4 2 2

配置脚本

DeviceB

```
#
sysname DeviceB
#
vlan batch 110 120
#
netstream export ip source 10.1.2.1
netstream export ip host 10.1.2.2 6000 dscp 0
assign forward enp netstream enable
#
netstream record record1 ip
collect counter bytes
collect counter packets
match ip destination-address
match ip source-address
#
```

```
interface Vlanif110
 ip address 10.1.1.1 255.255.255.0
#
interface Vlanif120
 ip address 10.1.2.1 255.255.255.0
#
interface 10GE1/0/1
 port link-type trunk
 port trunk pvid vlan 110
 port trunk allow-pass vlan 110
 netstream inbound ip
 netstream outbound ip
 netstream sampler ip random-packets 1024 inbound
 netstream sampler ip random-packets 1024 outbound
 netstream record record1 ip inbound
 netstream record record1 ip outbound
#
interface 10GE1/0/2
 port link-type trunk
 port trunk pvid vlan 120
 port trunk allow-pass vlan 120
#
return
```