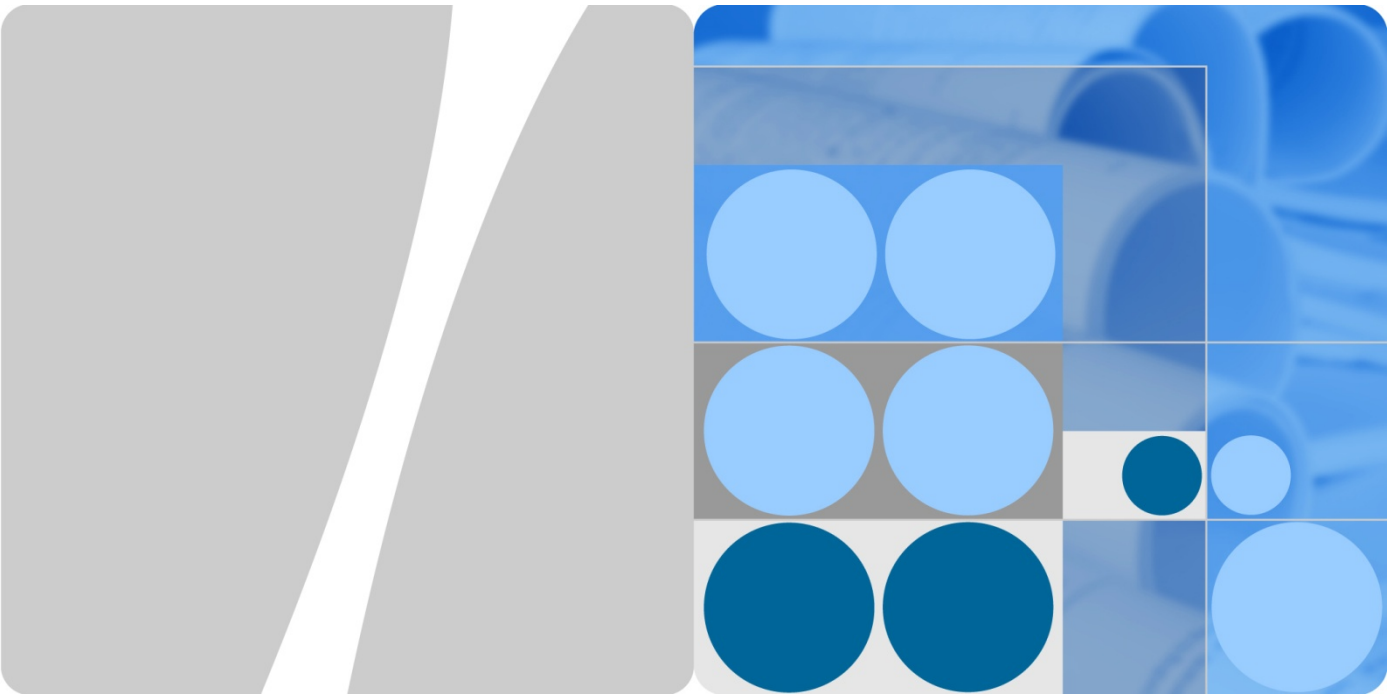


园区网解决方案
V100R001C00
部署指南

文档版本 01

发布日期 2011-09-15

华为技术有限公司

商标声明


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默示的声明或保证。

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办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 园区网概述

1.1 园区网定义

园区网一般是指企业或者机构的内部业务承载网络，通常包括数据中心（DC）网络、办公网络以及和 WAN/Internet 互联的网络。建设园区网的主要目的是使企业主业务运作更有效率。

有时候企事业单位还存在不同地域的办公分支机构，这些分支机构是不包含在园区网内部的。通常所说的园区网都止于公网边缘，可以理解为一个私网。

常见的典型园区网包括：

- 企事业办公网，例如政府、金融、能源、交通等行业的办公网络。
- 企业生产网，例如电力、石油、制造行业的生产控制网络。
- 科技园区网，例如高新科技园、软件园的园区网。
- 校园网，例如大学、科研机构的园区网。

园区网按规模来可以分为大型园区网、中型园区网、小型园区网。

- 大型园区网：终端用户数量大于 1000。
- 中型园区网：终端用户数量小于 1000，大于 200。
- 小型园区网：终端用户数量小于 200。

说明

其中中型园区网和小型园区网有时统称为中小型园区网。另外，有时候少于 10 人的网络有时候也被成为 SOHO 网络。

1.2 园区网架构

1.2.1 园区网设计总体原则

园区网通常是一种用户高密度的非运营网络，在有限的空间内聚集了大量的终端和用户。同时对于园区网而言，注重的是网络的简单可靠、易部署、易维护。因此在园区网中，拓扑结构通常以星型结构为主，较少使用环网结构（环网结构较多的运用在运营商的城域网络和骨干网络中，可以节约光纤资源）。

基于星型结构的园区网设计，通常遵循如下原则：

- 层次化

  将园区网络划分为核心层、汇聚层、接入层。每层功能清晰，架构稳定，易于扩展和易于维护。

- 模块化

  将园区网络中的每个部门或者每个功能区划分为一个模块，模块内部调整涉及范围小，易于进行问题定位。

- 冗余性

  关键设备采用双节点冗余设计；关键链路采用 Trunk 方式冗余备份或者负载分担；关键设备的电源、主控板等关键部件冗余备份。提高整个网络的可靠性。

- 安全隔离

  园区网络应具备有效的安全控制。按业务、按权限进行分区逻辑隔离，对特别重要的业务采取物理隔离。

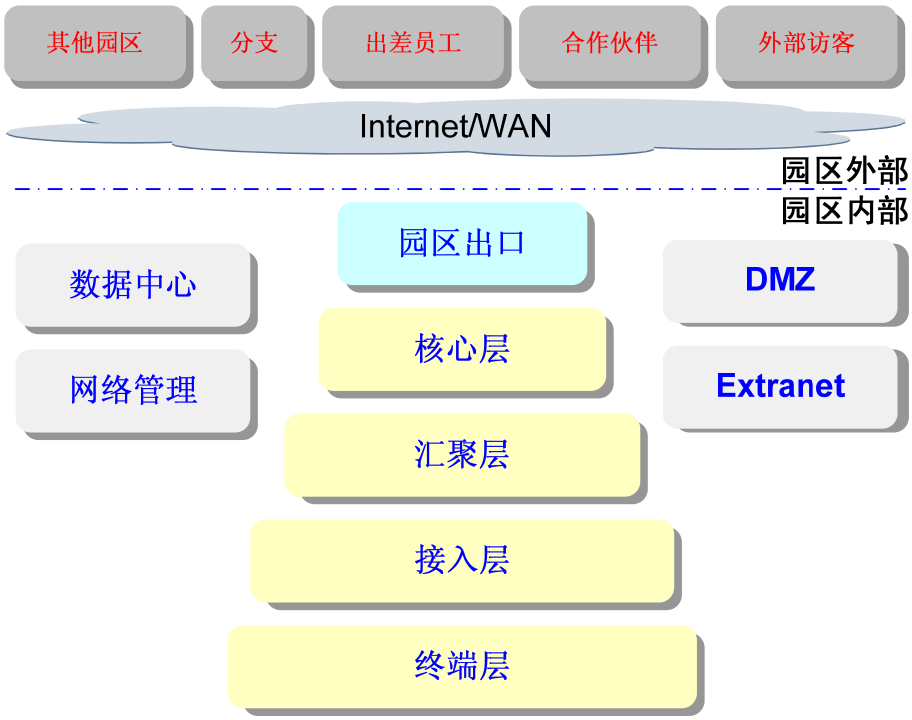
- 可管理性和可维护性

  网络应当具有良好的可管理性。为了便于维护，应尽可能选取集成度高、模块可通用的产品。

1.2.2 园区逻辑组网架构

基于上述设计原则，典型的园区网逻辑架构如图 1-1 所示。

图1-1 园区网典型逻辑结构图



园区网中的各分层和模块的说明如下：

- 终端层

  包含了园区内的各种终端设备，例如 PC、笔记本电脑、打印机、传真、POTS 话机、SIP 话机、手机、摄像头等等。

- 接入层

  负责将各种终端接入到园区网络，通常由以太网交换机组成。对于某些终端，可能还要增加特定的接入设备，例如无线接入的 AP 设备、POTS 话机接入的 IAD 等。

- 汇聚层

  汇聚层将众多的接入设备和大量用户经过一次汇聚后再接入到核心层，扩展核心层接入用户的数量。汇聚层通常还作为用户三层网关的位置，承担 L2/L3 边缘的角色，提供用户管理、安全管理、QoS 调度等各项跟用户和业务相关的处理。

- 核心层

  核心层负责整个园区网的高速互联，一般不部署具体的业务。核心网络需要实现带宽的高利用率和故障的快速收敛。

- 园区出口

  园区出口是园区网络到外部公网的边界，园区网的内部用户通过边缘网络接入到公网，外部用户（包括客户、合作伙伴、分支机构、远程用户等）也通过边缘网络接入到内部网络。

- 数据中心区

  部署服务器和应用系统的区域。为企业内部和外部用户提供数据和应用服务。

- DMZ 区

  通常公用服务器部署与该区域，为外部访客（非企业员工或分支机构的员工）提供相应的访问业务，其安全性受到严格控制。

- Extranet 区

  与 DMZ 区相似，但它主要是面向合作伙伴提供服务。

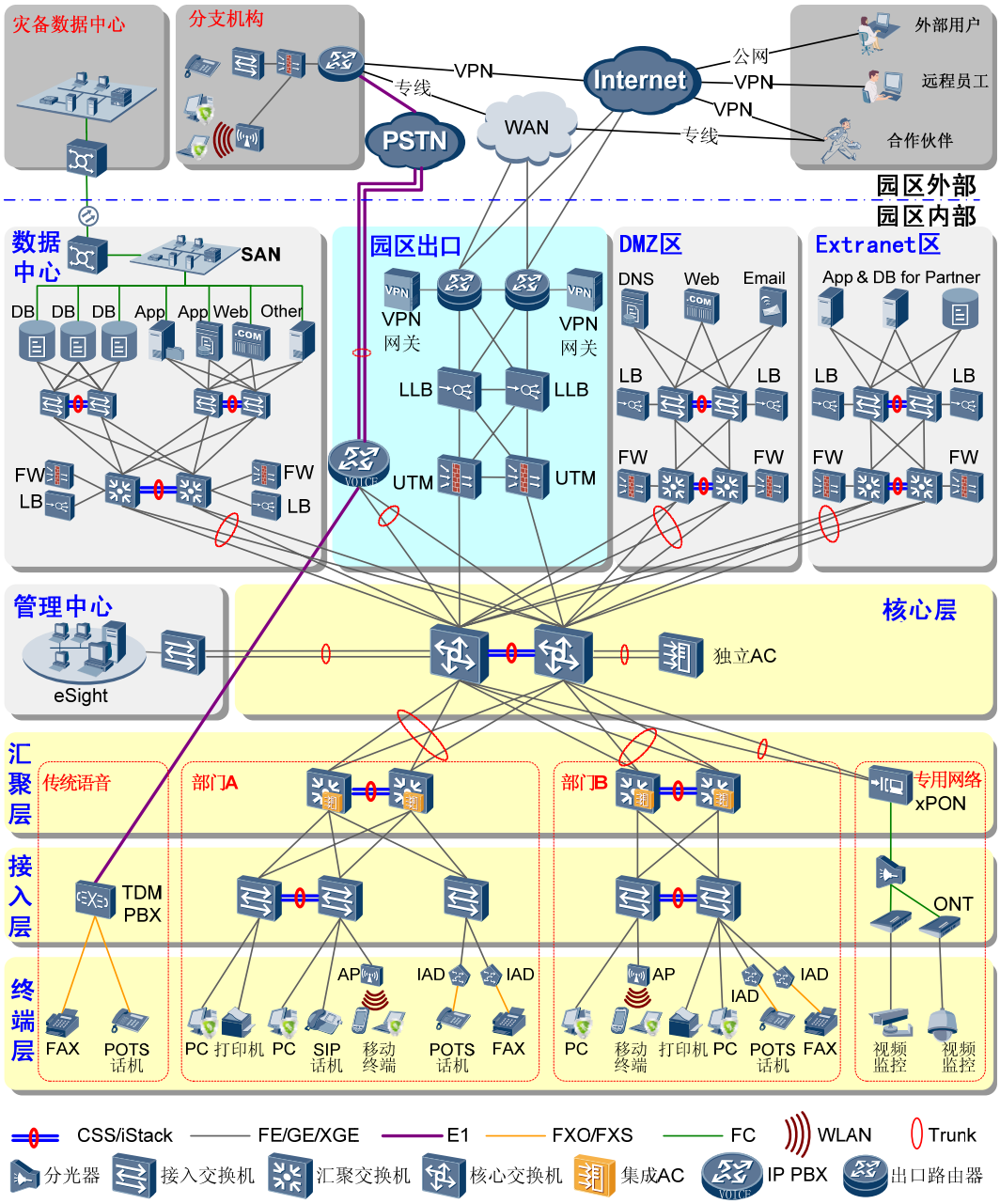
- 网络管理区

  对网络、服务器、应用系统进行管理的区域。包括故障管理，配置管理，性能管理，安全管理等。

1.2.3 园区物理组网架构

典型的园区网物理组网图如图 1-2 所示。

图1-2 园区网典型物理组网图



该组网结构具有如下特点：

- 以核心节点为“根”的星型分层拓扑，架构稳定，易于扩展和易于维护。
- 各部门和功能分区模块清晰，模块块内部调整涉及范围小，易于进行问题定位。
- 双节点冗余设计，关键链路均采用 Trunk 链路，保证网络的可靠性。
- 支持各种业务终端接入，一张 IP 网络承载所有业务。
- 支持分支接入、员工远程接入、合作伙伴接入、用户访问等各种外联场景。

1.3 园区网部署的主要关注点

1.3.1 园区互联

园区互联是指通过对网络设备的接口、VLAN、IP 地址、DHCP、DNS、路由等方面的部署，使园区内的所有模块、所有终端能够实现最基本的互联互通，终端用户可以正常上线，并访问园区内的各种资源。

接口和链路

在接口的部署方面，主要需要考虑如下几个方面：

- 通常情况下，接入交换机的用户侧接口使用 FE 接口，实现百兆到桌面的接入。如果要实现千兆到桌面的接入，则接入交换机需要使用 S5700 以上的交换机。
- 除了接入交换机的用户侧接口之外，其他的节点互联一般都采用 GE/XGE 接口。
- 通常接入交换机和汇聚交换机之间的链路、汇聚交换机和核心交换机之间的链路、核心交换机之间的互联链路建议采用 Eth-Trunk 链路。Eth-Trunk 链路两端的设备上应创建 Eth-Trunk 接口并加入物理成员接口。

除了物理接口的选择之外，对于某个接口来说，还需要设置接口的链路类型。例如除了接入交换机的用户侧接口应配置为 Access 或者 Hybrid 类型之外，其他的接口均应配置为 Trunk 或者 Hybrid 接口类型。

VLAN

VLAN 的部署对于园区网来说至关重要，通过 VLAN 的部署，既可以隔离广播域，减少广播风暴；又可以实现用户之间的隔离，增强信息的安全性。

在企业网中的 VLAN 一般可以分为如下几种。

表1-1 VLAN 分类

分类	描述
用户 VLAN	用户 VLAN 用来对不同的用户端口进行隔离，或者用来分割较大的广播域，减少广播风暴。用户 VLAN 通常根据业务需要进行规划。VLAN 最好不要跨交换机，即使跨交换机，数目也需要限制。
Voice VLAN	Voice VLAN 是为用户的语音数据流划分的专用 VLAN，用户通过创建 Voice VLAN 并将连接语音设备的端口加入 Voice VLAN，可以使语音数据集中在 Voice VLAN 中进行传输，便于对语音流进行有针对性的 QoS 配置，提高语音流量的传输优先级，保证通话质量。
Guest VLAN	如果园区网中部署了基于 802.1x 的 NAC 系统，则用户在通过 802.1x 认证之前，接入交换机会把该用户端口加入到 Guest VLAN，用户只能访问有限的网络资源，用于获取认证客户端软件或者执行其他一些应用升级程序（例如防病毒软件、操作系统补丁程序等）。当用户认证通过后，端口离开 Guest VLAN 并加入用户 VLAN。

分类	描述
Multicast VLAN	Multicast VLAN 用来承载组播业务流。组播 VLAN 主要是用来解决当客户端处于不同 VLAN 中时，组播路由器必须在每个用户 VLAN 复制一份组播流，导致带宽浪费的问题。

园区网中部署 VLAN，一般可遵循如下原则：

- 按照不同业务区域划分不同的 VLAN。
- 同一业务区域按照具体的业务类型（如 Web、APP、DB）划分不同的 VLAN。
- VLAN 需连续分配以保证 VLAN 资源合理利用。
- 预留一定数目 VLAN 方便后续扩展。

例如按照逻辑区域、地理区域和人员结构，可以分层规划 VLAN 如下。

表1-2 VLAN 规划样例

<table>
<tr><th>逻辑区域</th><th colspan="5">VLAN 规划</th></tr>
<tr><td>核心层</td><td colspan="5">100～199</td></tr>
<tr><td rowspan="3">数据中心</td><td rowspan="3">200～999</td><td>Web 区域</td><td colspan="3">200～299</td></tr>
<tr><td>App 区域</td><td colspan="3">300～399</td></tr>
<tr><td>DB 区域</td><td colspan="3">400～499</td></tr>
<tr><td rowspan="3">接入网络</td><td rowspan="3">2000～3499</td><td rowspan="2">A 地域</td><td rowspan="2">2000~2199</td><td>部门 X</td><td>2000~2009</td></tr>
<tr><td>部门 Y</td><td>2010~2019</td></tr>
<tr><td>B 地域</td><td colspan="3">2200~2399</td></tr>
<tr><td>业务网络</td><td colspan="5">3500～3999</td></tr>
</table>

IP 地址

IP 地址的合理规划是网络设计中的重要一环，大型网络必须对 IP 地址进行统一规划并得到实施。IP 地址规划的好坏，影响到网络路由协议算法的效率、网络的性能、网络的可扩展性和网络的管理，也必将直接影响到网络应用的进一步发展。

园区网的 IP 地址主要分为以下几类：

- LoopBack 地址

  为了方便管理，会为每一台网络设备创建一个 LoopBack 接口，并在该接口上单独指定一个 IP 地址作为管理地址。LoopBack 地址务必使用 32 位掩码的地址，最后一位是奇数的表示路由器，是偶数的表示交换机，越是核心的设备，LoopBack 地址越小。
- 互联地址

互联地址是指两台网络设备相互连接的接口所需要的地址，互联地址务必使用 30 位掩码的地址。核心设备使用较小的一个地址，互联地址通常要聚合后发布，在规划时要充分考虑使用连续的可聚合地址。

- 业务地址

  业务地址是连接在以太网上的各种服务器、主机所使用的地址以及网关的地址，业务地址规划时所有的网关地址统一使用相同的末位数字，例如 X.X.X.254 都是表示网关。

园区网的 IP 地址规划，一般可遵循如下原则：

- 唯一性、连续性、扩展性、实意性。
  - 唯一性：一个 IP 网络中不能有两个主机采用相同的 IP 地址。即使使用了支持地址重叠的 MPLS/VPN 技术，也尽量不要规划为相同的地址。
  - 连续性：连续地址在层次结构网络中易于进行路径叠合，大大缩减路由表，提高路由算法的效率。
  - 扩展性：地址分配在每一层次上都要留有余量，在网络规模扩展时能保证地址叠合所需的连续性。
  - 实意性：好的 IP 地址规划使每个地址具有实际含义，看到一个地址就可以大至判断出该地址所属的设备。
- 内部的 IP 地址建议使用私网 IP 地址，在边缘网络通过 NAT 转换成公网地址后接入公网。
- 汇聚交换机下接入的网段可能有很多，在规划的时候需要考虑路由聚合，这样可以减少核心网络的路由数。

DHCP

园区网中建议使用 DHCP 来为用户分配 IP 地址。园区网中的 DHCP 部署比较灵活，通常有如下部署方式：

- 使用外置的独立 DHCP 服务器，此时需要在汇聚交换机上部署 DHCP Relay 功能。适用于规模较大的园区网。
- 使用汇聚交换机内置的 DHCP 服务器（全局地址池），此时需要在汇聚交换机部署全局 DHCP Server 功能。适用于规模中等的园区网。
- 使用汇聚交换机内置的 DHCP 服务器（接口地址池），此时需要在汇聚交换机部署 DHCP Server 功能（接口地址池方式）。适用于规模较小的园区网。

园区网中 DHCP 分配地址时，一般根据 VLAN 来进行分配，如有特殊要求，可以在接入交换机部署 DHCP Option82 功能，根据交换机的接入信息来进行分配。

另外，为了防止园区网中的各种有意或无意的 DHCP 攻击，例如 DHCP DoS 攻击、DHCP Server 仿冒攻击、DHCP 仿冒续租报文攻击等。可以在接入交换机上部署 DHCP Snooping 功能来进行防范。

DNS

在配置 DHCP 服务器时，一般还需要同时部署 DNS 服务器，提供域名解析服务。

DNS 服务器一般采用 1+N 的方式部署。

- 一台 Master 服务器，作为 DNS 的管理服务器，可以增加、删除、修改域名，并把信息同步到 Slave 服务器。
- N 台 Slave 服务器，采用多台服务器形成集群的方式，统一对外提供 DNS 服务，一般采用基于硬件的负载均衡器提供服务器集群的功能。

另外，还可以在 Slave 服务器上部署 Cache 服务器功能，用于缓存用户的 DNS 请求结果，加快后续的访问。

路由

对于一般的园区网而言，通常不需要部署 BGP。除非出现如下场景，才需要部署 BGP：

- 网络中的路由数量过于庞大，IGP 难以胜任。
- 需要大量的使用路由策略或者是业务分流，IGP 等协议无法实现。
- 部署 MPLS L3VPN 技术时，需要实现复杂的隔离策略。

因此在本章中不介绍 BGP 的具体部署，详细的部署方式可参见具体场景中的介绍。

对于 IGP，企业园区网中可以选择 IS-IS 或 OSPF（对于小园区网，也可选择 RIP），IS-IS 和 OSPF 协议在总体上差别不大，均可选择。但是在总体上，企业网中选择 OSPF 的居多（IS-IS 在运营商网络中使用较多）。

以下以 OSPF 为例介绍 IGP 的部署。

在企业网中部署 OSPF，可以按照如下原则进行：

- 如果不需要部署 MPLS L3VPN，只启动一个 OSPF 进程即可。
- 园区出口和核心交换机作为 OSPF 的 Area0。出口路由器作为 ASBR 和 ABR，核心交换机为 ABR。
- 每个业务部门区域作为一个单独的 OSPF Area，编号 1、2…N。
- Area1、2…N 使用 OSPF NSSA 区域，限制 LSA 在区域间的传播。
- 核心交换机和出口路由器，通过区域汇总，限制区域间传播的 LSA 条目。
- 如果部门较少，可以把所有路由节点都配置为 Area0。

1.3.2 园区无线接入

园区无线接入是指在园区内部署 WLAN 网络，实现各种移动终端（例如智能手机、PDA、笔记本电脑等）的接入，并提供与固定终端相同的接入体验。

WLAN 网络主要由 STA、AP、AC 等部件组成。

- STA（Station）：指各种接入终端，例如电脑、手机、PDA 等。
- AP（Access Point）：AP 是 WLAN 网络的主要设备，是实现无线技术的关键部件。AP 对上提供有线连接，对下提供无线接入，起到有线和无线网络的桥接作用。
- AC（Access Controller）：AC 主要完成对 AP 设备的管理。包括 AP 点管理、射频管理、用户认证、完全管理等。AC 通过 CAPWAP（Controlling and Provisioning of Wireless Access Point）协议完成管理功能。

有关园区无线接入的详细描述信息请参见“3 园区无线接入部署”。本节只简单在部署园区无线网络时需要考虑的几个主要方面。

WLAN 的架构

WLAN 网络主要有自治式和集中式两种网络架构。

- 自治式架构

  自治式架构又称为 FAT AP 架构。在该架构下，AP 实现所有无线接入功能（称为“胖 AP”），不需要 AC 设备形态。

  WLAN 早期广泛采用自治式架构，随着企业大量部署 AP 时，对 AP 进行配置、升级软件等管理工作将给用户带来很高的操作成本，管理成本提高，自治式架构应用逐步减少。目前通常在一些 SOHO 或者家庭 WLAN 中使用。

- 集中式架构

  集中式架构又称为 FIT AP 架构。在该架构下，通过 AC 集中管理和控制多个 AP（称为瘦 AP）。在集中式架构下，所有无线接入功能由 AP 和 AC 间共同完成：

  - AC 完成网络具有重要意义的功能，例如移动管理、身份验证、VLAN 划分、射频资源管理、无线 IDS 和数据包转发等。
  - AP 完成无线空口的控制，例如无线信号发射与探测响应、数据加密解密、数据传输确认、空口数据优先级管理等等。
  - AP 和 AC 间采用 CAPWAP 协议进行通讯，AC 与 AP 间可以是直连或者穿越二层或三层网络。

  集中式架构是企业网、运营商等 WLAN 方案的主要架构，便于集中管理、集中认证和集中安全管理。下文中的 WLAN 部署方案均基于集中式架构。

AC 的部署方式

在集中式 WLAN 架构中，根据 AC 的部署方式，又可分为集中式 AC 方案和分布式 AC 方案。

- 集中式 AC 方案，是指整个网络中集中部署 AC 设备（一般是独立的 AC 设备），来控制和管理整网的 AP 设备。
- 分布式 AC 方案，是指网络中分区域采用多个 AC 设备，分别对本区域的 AP 设备进行管理。分布式 AC 方案一般不采用独立的 AC 设备，而是采用在汇聚交换机上集成 AC 功能，来实现对本交换机下挂的所有 AP 进行管理。

集中式 AC 方案对于用户和网络的集中管理能力强，但是对 AC 的性能要求较高，投资成本较高；分布式 AC 方案对性能要求较低，投资成本较低，但是由于管理点分散，因此部署和管理相对复杂。

AC 的部署位置

根据 AC 在网络上所处位置，可分为 AC 旁挂方案和 AC 直路方案。

- AC 旁挂方案

  AC 旁挂方案是指将 AC 部署在用户网关设备（汇聚或核心交换机）一侧，实现对用户网关设备下所有 AP 的管理。

  旁挂方案主要用于原有网络汇聚/核心设备非华为设备的场景。

- AC 直路方案

AC 直路方案是指在将 AC 部署在 AP 与用户网关设备（汇聚或核心交换机）之间，实现对下辖所有 AP 的管理。

直路方案主要用于新建网络或原有网络汇聚/核心设备为华为设备的场景。

AC 的硬件形态

根据 AC 的硬件形态，可分为独立 AC 方案和集成 AC 方案。

- 独立 AC 方案

  独立 AC 方案是指采用单独的 AC 硬件设备（例如 WS6603 产品），通过直路或者旁挂方式实现对于所有 AP 的管理。

  独立 AC 方案一般应用在集中式 AC 的 WLAN 部署方案中。独立 AC 的性能优异，可以实现大容量高性能的 WLAN 网络部署。但是独立 AC 相比交换机集成的 AC 价格昂贵一些。

- 集成 AC 方案

  集成 AC 方案是指不采用单独的 AC 硬件设备，而是采用在交换机中集成的 AC 硬件插卡（例如 S9300 的 SPU 板），来实现对交换机下所有 AP 的管理。

  集成 AC 方案可应用在集中式 AC 部署方案中，也可应用在分布式 AC 部署方案中。集成 AC 方案部署较为简便，价格相对低廉一些，但是性能方面与独立的 AC 设备相比略差。

业务转发模式

业务转发模式是指 AP 针对用户的业务数据的转发处理方式，包括独立转发模式和隧道模式两种。

- 独立转发模式

  独立转发模式又称直接转发模式，是指 AP 上对用户数据由本地直接转发到上层网络，不需要经过 AC 处理，AC 只对 AP 进行管理。而 AP 管理流封装在 CAPWAP 隧道中，到达 AC 终止。

  独立转发模式下，业务部署和设备管理简单，数据流量不经过 AC，AC 负担小；但是无法实施统一的安全监管策略。

- 隧道转发模式

  隧道转发模式是指 AP 将用户数据、自身管理数据统一封装在 CAPWAP 隧道中，发送至 AC，由 AC 统一转发。

  隧道转发模式下，流量全部经过 AC，可以按用户需求规划安全监管策略；但是 AC 数据压力较大，对 AC 设备本身处理能力要求较高。

AP 发现 AC 的方式

当 FIT AP 上线后，需要知道本 AP 所归属 AC 的 IP 地址，才能从 AC 获得相应的参数配置。AP 发现 AC 通常有三种方式：

- 广播方式

  在这种方式下，AP 通过广播的方式向网络中所有的 AC 发起 CAPWAP 隧道连接，当有 AC 响应该 AP 后，CAPWAP 隧道建立。这种方式下，AP 发现 AC 是自主行为，在 AC 上无需进行任何配置。

- 通过 DHCP Option43 发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option43 选项，将 AC 的 IP 地址告知 AP。

- 通过 DHCP Option15 和 DNS 解析发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option15 选项，将 AC 的 DNS 域名告知 AP。

  AP 再向 DNS 服务器发起 AC 域名的解析请求，DNS 服务器返回响应报文，告知 AC 的 IP 地址。

上述几种方式的对比如表 1-3 所示。

表1-3 AP 发现 AC 的不同方式对比

方式	部署要求	优势	劣势	适用网络
广播方式	无	对已有网络没有额外要求	仅能用于AP/AC二层组网中	小型 WLAN 网络，AP/AC 二层组网
Option43 方式	DHCP Server 启动 Option 43 属性	适用于 AP/AC 任何组网中	对网络有部署要求	大中型 WLAN 网络，AP/AC 二层或三层组网
Option15+ DNS 方式	部署 DNS Server； DHCP Server 支持 Option 15 属性	适用于 AP/AC 任何组网中	对网络有部署要求	大中型 WLAN 网络，AP/AC 二层或三层组网

终端认证方式

IEEE 802.11 标准要求 WLAN 终端在准备连接到网络时，必需进行“身份验证”。WLAN 终端身份认证主要有两种方式：

- 开放系统认证（Open-System Authentication）

  开放系统认证是 IEEE 802.11 标准要求必备的一种方法，是最简单的认证算法，即不认证。所有请求认证的客户端都会通过认证。

  开放系统身份验证比较适合有众多用户的电信运营 WLAN 网络。

- 共享密钥认证（Shared-Key Authentication）

  共享密钥式认证必需使用加密方式，要求每个 WLAN 终端都配置和 AP 完全一致的密钥（key）。

  共享密钥认证一般适用于企业网、校园网及家庭网络等。

用户认证方式

相对于简单的 WLAN 终端身份验证机制，用户身份验证的安全性大大提高。通过提供有限的访问权限来验证用户身份，只有确定用户身份后才给予完整的网络访问权限，可有效判别用户的合法性。

WLAN 用户身份验证主要有 Portal、PSK、WAPI、802.1x 等几种认证方式。由于在园区网中还有有线接入用户，而有线用户的认证方式一般是 Portal 认证和 802.1x 认证，因此为了实现有线无线一体化的用户体验，推荐 WLAN 中也使用 Portal 认证和 802.1x 认证。

1.3.3 网络虚拟化

经典的园区网分层、分模块设计，还存在着一定的不足。

- 汇聚层、核心层的双节点冗余设计，虽然提高了网络的可靠性，但是也使得网络结构和互联关系变得复杂，网络的扩展也变得困难。
- 冗余结构使得网络的树形结构中出现环路，并且随着企业的不断发展，环网规模不断扩大。因此一般都需要部署 MSTP 等协议消除环路，同时运行 VRRP 等来支持节点冗余备份，导致网络协议的部署变得复杂。
- 不同部门/群组用户的资源访问权限需要进行控制，不同业务间的访问、传输和应用也需要进行端到端的隔离。但是传统的物理隔离技术已经无法满足这种需求，导致网络重复建设、管理分散、安全策略难以部署。

通过部署网络虚拟化，可以较好的解决上述问题。网络虚拟化包括横向虚拟化和纵向虚拟化两个层面。部署了网络虚拟化的园区网被称为虚拟园区网。

- 横向虚拟化

  横向虚拟化方案是指在园区网的核心层、汇聚层、接入层分别采用集群/堆叠技术，将多台物理设备虚拟化成单台逻辑设备，达到简化网络结构、简化网络协议部署、提高网络可靠性和可管理性的目的。

  关于横向虚拟化方案的详细信息请参见“5.1.1 虚拟园区网简介”。
- 纵向虚拟化

  纵向虚拟化方案是通过各种隔离技术，将一个物理网络划分成几个相互独立的逻辑网络，实现了终端和业务的安全隔离、应用资源的按需分配等。

  要实现逻辑网络的隔离，有 VLAN、隧道、MCE、VPN 等多种方式，但从业务隔离灵活性、配置管理复杂度、扩展性、组网对设备的要求等多方面综合对比，MPLS L3VPN 技术最适合应用在大、中型园区内进行业务隔离。

  关于纵向虚拟化方案的详细信息请参见“5.1.1 虚拟园区网简介”。

1.3.4 NAC 系统

NAC（Network Access Control）系统，主要用来对用户终端的接入进行认证和控制，并将终端安全状况和网络准入控制结合在一起，通过检查、隔离、加固和审计等手段，加强网络用户终端的主动防御能力，保护企业网络的安全性。

华为的 NAC 系可以实现如下功能：

- 通过多种身份认证方式确认终端用户的合法性。
- 绑定检查终端的安全漏洞、终端杀毒软件的安装和病毒库更新情况。

- 通过统一接入策略和安全策略管理，控制终端用户的网络访问权限。
- 通过桌面运维，完成进行桌面资产注册和监控、外设管理和软件分发。

有关 NAC 系统部署的详细信息，请参考“6 NAC 系统部署”。

1.3.5 VoIP 语音&UC

在大型企业中，可以基于 IP 网络自建语音通信系统，可以使企业内部的语音通信不再需要通信费用，从而节省了企业的运营成本。

建设 IP 语音通信系统面临的挑战是如何在 IP 网络基础上，既可以保护原有投资和用户使用习惯，又可以让企业的语音业务和数据业务在同一张 IP 网络上协调运作，同时可以满足 IP 语音通信后续的发展及用户数量的扩容需求。

有关 VoIP 语音部署的详细信息，请参考“7 VoIP 语音部署”。

1.3.6 可靠性

园区网中的可靠性措施包括以下几类：

- 设备可靠性：通过部署 CSS/iStack、部件冗余等方式保证设备自身的可靠性。
- 链路可靠性：通过部署 Eth-Trunk 来实现链路的冗余备份和负载分担。
- 二层网络可靠性：通过部署 MSTP、SmartLink、DLDP、SEP、RRPP 等特性来保证二层网络的可靠性。
- 三层网络可靠性：通过部署 IP FRR、VRRP、BFD 等特性来保证三层网络的可靠性。

我们推荐使用 CSS/iStack + Eth-Trunk 的组合方案（即横向虚拟化方案）来保证网络的可靠性。在这种方案中，由于采用了 CSS/iStack 技术将多台设备虚拟成了一台设备，而传统的双归接入等拓扑结构也被更简单的 Eth-Trunk 所取代。

采用 CSS/iStack + Eth-Trunk 后，通常不再需要部署 MSTP、SmartLink、DLDP、SEP、RRPP 等二层可靠性特性，也不再需要部署 VRRP+BFD。只需要再配合部署 IP FRR 等部分三层可靠性特性，即可保证整个园区网络的可靠性。

1.3.7 服务质量

在园区网中，对于 QoS 的部署主要考虑如下两个因素：

- 园区网中，除了传统的 WWW、E-Mail、FTP 等数据业务，还承载着视频监控、电视会议、语音电话、生产调度等业务。这些业务有一个共同特点，即对带宽、延迟、延迟抖动等传输性能有着特殊的需求。比如视频监控、电视会议需要高带宽、低延迟抖动的保证。语音业务虽然不要求高带宽，但非常注重时延，在拥塞发生时要求优先获得处理。
- 园区网应该是一个无阻塞的网络，园区网部署 QoS 主要是防止 BT 等非正常业务流量对园区网关键业务以及关键客户流量形成冲击。

在园区网中部署 QoS，一般需要关注如下内容：

- 通常采用 Diff-Serv 模型。
- 最重要的是要根据不同业务类型，做好各种业务的优先级和带宽规划。
- 接入层设备在用户侧对各种业务进行识别，并给业务流报文加上优先级标记。

- 其余各层设备按照优先级对报文进行队列调度和转发。
- 如果网络的带宽无法保证所有业务的无阻塞转发，则可以在汇聚层和核心层设备上部署流量监管、流量整形、拥塞避免等 QoS 措施，保障高优先级业务。

关于各类业务的优先级规划，在 RFC4594 中给出了一个参考规划，如表 1-4 所示。

表1-4 业务优先级规划

业务分类	业务说明	PHB	DSCP	802.1P	EXP
网络控制	网络控制平面业务，如 OSPF、BGP、VRRP 协议报文等。	CS6	48	6	6
语音业务	VoIP 业务，包括 G.711、G.729 等语音流。	EF	46	5	5
广播视频	广播电视和视频监控业务，特点是丢包敏感，不具备重新发送和流控能力。	CS5	40	5	5
桌面会议	桌面多媒体协同应用软件，包括语音和视频的应用。如华为 eSpace。	AF41、AF42、AF43	32、36、38	4	4
交互视频	室内部署的交互视频应用，具有语音和视频能力。如视频会议、高清视频等	CS4	32	4	4
视频点播	VoD 视频点播业务。这类业务允许一定的时延，丢包能够重传，比广播和实时媒体业务更具弹性。	AF31、AF32、AF33	26、28、30	3	3
呼叫信令	IP 语音和视频业务信令流。如 SIP、H323、MGCP、VMP 等。	CS3	24	3	3
事务处理	交互式的重要数据业务。如即时消息、ERP、数据库查询。	AF21、AF22、AF23	18、20、22	2	2
网络管理	网络维护和管理业务。例如 SNMP、SSH、SysLog。	CS2	16	2	2
Bulk 数据	指非交互式“背景”业务，其特点是不需要等待业务响应，不会影响工作效率。如 Email、FTP、文件共享等业务。	AF1	10、12、14	1	1
背景流量	与公司业务无关，多是娱乐性的业务。如 BT、eMule、YouTube 等非组织性的内容。	CS1	8	0	0

业务分类	业务说明	PHB	DSCP	802.1P	EXP
尽力服务	采用默认优先级 0，大多数业务不进行优先级标记。	DF(CS0)	0	0	0

说明

按照业界通行做法，广播视频和呼叫信令业务 PHB 通常不遵循 RFC 标准，广播视频定义为 CS5，而呼叫信令定义为 CS3。

1.3.8 分支接入

分支接入是指对于企业的分支机构（例如外研所、办事处等），通过专网或公网方式，接入到企业的总部园区，实现分支与总部的互通。

分支接入主要有专网方式、MPLS VPN 方式、公网方式。

1. 专网方式

   专网方式通过企业自建的广域专网，实现多分支之间的互联。这种方式一般只适用于拥有自建骨干网的大型或特大型企业。

2. MPLS VPN 方式

   MPLS VPN 方式通过租用运营商的 MPLS VPN 业务（L3VPN 或者 L2VPN），实现多分支之间的互联。这种方式经济高效，比较适合有一定数量分支机构，但是没有自建广域网的企业。

3. 公网方式

   公网方式是指不租用运营商的 VPN 业务，而是直接使用公共网络来实现分支和总部之间的互联互通。公网方式比较适合于只有少量小型分支机构或者 SOHO 员工的企业。

   公网方式是通过不安全的公共网络接入的，因此关键是要保证数据的安全性。公网方式是依靠在分支和总部园区网关之间构建点对点 VPN，通过隧道方式来保证数据的安全可靠传输。

   对于分支来说，公网方式所使用的 VPN 技术是 GRE over IPSec。GRE 是常用的隧道封装协议，可以很好的实现对于远程访问的数据承载，但是 GRE 只有简单的密码验证，没有加密功能。而 IPSec 隧道加密功能很强，但是不能承载路由协议，对于 VPN 的扩展性有较大影响。通过 GRE 和 IPSec 的结合，可以很好的实现对于远程访问的数据流的承载和安全保护。

----结束

1.3.9 远程接入

远程接入是指出差员工或者合作伙伴在非固定办公地点，例如酒店、机场等场所，通过公网（例如 Internet）接入园区网，并访问园区网中的内部资源。

由于远程接入是通过不安全的公共网络接入的，因此关键是要保证远程访问的安全性。远程接入是依靠在用户终端和园区网网关之间构建点对点 VPN，通过隧道方式来保证数据的安全可靠传输。

远程接入所使用的 VPN 技术主要有如下几种。

- L2TP over IPSec

  L2TP 也是常用的隧道封装协议，并且具有很好的用户认证功能，但是 L2TP 也没有加密功能。因此，也可以通过 L2TP 和 IPSec 的结合，实现对于远程访问数据流的承载和安全保护。

- SSL VPN

  SSL VPN 是以 HTTPS（Secure HTTP）为基础的 VPN 技术，工作在传输层和应用层之间。SSL VPN 充分利用了 SSL 协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，可以为应用层之间的通信建立安全连接。

  SSL VPN 广泛应用于基于 Web 的远程安全接入，为用户远程访问公司内部网络提供了安全保证。

1.3.10 访问公网

访问公网是指园区网的内部用户访问公共网络（如 Internet）的场景。在园区网中，访问公网都是通过企业的园区出口路由器统一出口的。在部署访问公网时，一般需要考虑如下因素：

- 由于企业内部用户一般是采用私网 IP 地址，因此园区出口处，需要通过旁挂或直路的方式，部署 NAT 设备，实现私网和公网地址的转换。
- 园区出口是内网和外网的边界，因此必须要在园区出口处，需要通过旁挂或直路的方式，部署防火墙设备，对数据流进行过滤保护，防护来自公网的安全威胁。
- 如果园区网中部署了 MPLS L3VPN，那么在园区出口处的 NAT 和 FW，也需要能够支持 VPN 多实例，以便为不同 VPN 的用户提供隔离的出口服务。
- 如果希望对用户访问公网的权限进行控制，则可以部署 Proxy 服务器与 Internet 相连，并在 Proxy 服务器上对用户权限进行控制。用户通过访问 Proxy 服务器来间接访问 Internet，非 Proxy 的公网访问请求直接拒绝。

1.3.11 网络管理

对于中小型企业，在成本不允许的情况下，可以不部署网管系统。而对于大型或特大型企业来说，一般都需要网管系统，实现对于园区网络的统一监控和管理。

在园区网中部署网管系统，一般需要考虑如下因素：

- 多厂商设备共管

  IP 网络是开放的，各厂商混合组网成为企业组网普遍情况。因此在企业中部署具备多厂商设备共管能力的网管系统，可以极大降低网络管理维护的成本，提高效率。

- IP 和 IT 设备共管

  传统的网管系统只对 IP 网络设备进行管理，而对于服务器、打印机等 IT 设备不进行管理。因此如果可以实现对 IP 和 IT 设备的共同管理，则可以很好的实现企业资源的统一管理，提高管理效率，降低管理成本。

- 业务部署和发放

  传统的 IP 网管系统更多的是对于网络的监控和维护，而对于具体的业务部署和发放，则一般需要在设备上通过命令行的方式进行配置。如果网管系统中可以实现业务的部署和发放，则可以实现业务的集中部署，并且业务发放也变得可视化。

- 精细化的流量监控和分析

  对于企业来说，精细化的流量监控和分析，是企业进行网络建设和优化的前提保证，因此企业的网管系统应该支持 NetStream、NetFlow、NQA 等流量监控技术，并能对监控统计结果进行精细分析，给网络质量进行评估，为网络优化提供依据。

eSight 应用平台是华为面向企业网管理推出的新一代面向企业园区和分支网络管理系统，实现对企业资源、业务、用户的统一管理以及智能联动。eSight 应用平台支持对 IT&IP，以及第三方设备的统一管理，同时提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

在华为的企业园区网部署方案中，推荐使用 eSight 应用平台实现对网络的管理。eSight 不仅可以实现对于网络中各类节点和资源的监控，还可以实现对于 WLAN 和 IPSec 等业务的配置。

1.4 产品配套关系

表1-5 园区网解决方案产品配套关系表

部件	产品	版本
接入交换机	S2700/S3700系列	V100R006C01
汇聚交换机	S5700/S7700/S9300系列	V100R006C01
核心交换机	S7700/S9300系列	V100R006C01
AC	S9300 SPU插卡（集成 AC）	V100R006C01
	WS6603（独立 AC）	V100R003C05
AP	WA603SN WA603DN WA633SN WA653SN WA653DN WA653EN	V100R003C01
出口路由器	AR G3 系列路由器	V200R001C01
	NE20/20E 系列路由器	V200R005
	NE40E/80E 系列路由器	V600R003C00
VPN 网关	AR G3 系列路由器	V200R001C01
	SRG 系列业务路由网关	非特定
	Eudemon 系列防火墙	非特定
防火墙	Eudemon 系列防火墙	非特定
NAC 准入服务器	TSM Server	V100R002C06

部件	产品	版本
NAC 终端代理	TSM Agent	V100R002C06
IP PBX	SoftCo 系列	V100R002
	AR G3 系列路由器	V200R001C01
SIP AG	AR G3 系列路由器	V200R001C01
IAD	非特定，根据需要可选择华为生产的IAD101H/102H/104H/208E(M)/132E(T)/1280等型号的IAD产品。	非特定
SIP 话机	非特定，根据需要可选择华为生产的HW ET325/523/525/635/655/685、HW MC820C/830C/850/851等型号的产品。	非特定
网管系统	eSight	V200R001C00

说明

- 如果要在汇聚层或核心层使用 CSS 集群功能，则只能选用 S9300 系列。
- 如果接入层需要部署 MCE 功能，则不能选用 S2700 系列。

2 园区基础网络部署

2.1 概述

2.1.1 园区基础网络部署简介

园区基础网络部署，其目的是通过对网络设备的接口、VLAN、IP 地址、DHCP、路由等方面的配置，使园区内的所有模块、所有终端能够实现最基本的互联互通，终端用户可以正常上线，并访问园区内的各种资源。

2.1.2 配套版本

表2-1 园区基础网络配套产品和版本

部件	产品	版本
接入交换机	S2700/S3700 系列	V100R006C01
汇聚交换机	S5700/S7700/S9300 系列	V100R006C01
核心交换机	S7700/S9300 系列	V100R006C01

说明

如果要在汇聚层或核心层使用 CSS 集群功能，则只能选用 S9300 系列。

2.1.3 部署思路

前置任务

- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- 接入、汇聚、核心层设备已插入堆叠/集群插卡，并通过堆叠/集群线缆连接。
- 完成 VLAN、IP 地址等数据的规划。

配置思路

配置思路	配置注意事项
配置堆叠/集群系统	S2700/S3700/S5700 系列的交换机，堆叠系统可以自动建立。 对于 S9300 系列的交换机，集群系统的建立需要手工使能。
配置管理 IP 地址	• S7700/S9300 系列交换机的管理 IP 地址通过 Eth0/0/0（非堆叠）或者 Eth0/0/0/0（堆叠）接口来配置。 • S5700 系列交换机的管理 IP 地址通过 MEth0/0/0 接口来配置。 • S2700/S3700 系列机的管理 IP 地址需要通过创建 VLANIF 接口来配置。
配置接口和 VLAN	• 通常接入交换机和汇聚交换机之间的链路、汇聚交换机和核心交换机之间的链路、核心交换机之间的互联链路建议采用 Eth-Trunk 链路。 • 接入交换机的用户侧接口应配置为 Access 或 Hybrid 类型，其余情况均应配置为 Trunk 或者 Hybrid 类型。 • 汇聚和核心交换机需要创建 VLANIF 接口并配置 IP 地址。
配置路由	• 除非超大型园区或者有复杂的路由策略需要部署，一般情况下不需要部署 BGP。 • 企业网中 IGP 推荐使用 OSPF。 • 通常只启动一个 OSPF 进程。 • 核心交换机作为 OSPF 的 Area0。 • 每个业务部门区域作为一个单独的 OSPF Area，编号 1、2…N。 • 如果部门较少，可以把所有路由节点都配置为 Area0。
配置 DHCP	在园区网中 DHCP 的部署方式比较灵活，通常可以部署 DHCP Snooping（接入层）、DHCP Relay（汇聚层）或者 DHCP Server 功能（汇聚层）。
配置 QoS	QoS 需要端到端部署，通常接入节点通过 Remark 动作进行业务流量区分，其他节点根据流分类调度。

配置思路	配置注意事项
配置可靠性	推荐使用 CSS/iStack + Eth-Trunk 的组合方案来保证网络的可靠性。此时不再需要部署 MSTP、SmartLink、DLDP、SEP、RRPP 等二层可靠性特性，也不再需要部署 VRRP+BFD。可简化网络部署。

2.2 配置堆叠/集群

关于堆叠/集群的配置请参见“5.2 配置堆叠/集群系统”。

2.3 配置管理 IP 地址

1. 执行命令 **system-view**，进入系统视图。
2. 进入管理网口视图。
   - 对于堆叠的 S9300 系列交换机，执行命令 **interface ethernet 0/0/0/0**。
   - 对于非堆叠的 S9300/S7700 系列交换机，执行命令 **interface ethernet /0/0/0**。
   - 对于 S5700 系列交换机，执行命令 **interface meth 0/0/1**。
   - 对于 S2700/S3700 系列交换机。
     - 执行命令 **vlan** *vlan-id*，创建 VLAN 并进入 VLAN 视图。
     - 执行命令 **quit**，返回系统视图。
     - 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口并进入 VLANIF 接口视图。

   说明

   只有当 VLAN 内存在状态为 UP 的物理接口时，VLANIF 接口才能 UP。
3. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置管理网口的 IP 地址。

----结束

2.4 配置接口和 VLAN

2.4.1 配置 Eth-Trunk 接口

在园区网中，为了保证链路的可靠性，在许多场合需要部署 Eth-Trunk，例如：

- 接入交换机和汇聚交换机之间的链路
- 汇聚交换机和核心交换机之间的链路
- 核心交换机之间的互联链路

Eth-Trunk 链路有手工负载分担和静态 LACP 两种工作模式。除非对于各条物理链路的负载分担情况有特殊规划，否则通常采用静态 LACP 模式即可。

如果需要部署 Eth-Trunk 链路，请在链路两端的交换机上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface eth-trunk** *trunk-id* 命令，创建 Eth-Trunk 接口并进入接口视图。
3. 执行命令 **mode lacp-static**，配置 Eth-Trunk 的工作模式为静态 LACP 模式。
4. 执行命令 **quit**，返回系统视图。
5. 执行命令 **interface** *interface-type interface-number*，进入物理接口视图。
6. 执行命令 **eth-trunk** *trunk-id*，将该物理接口加入到 Eth-Trunk 接口。

----结束

2.4.2 接入交换机下行接口配置

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，批量创建 VLAN。
3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
4. 执行命令 **port link-type access**，配置接口的链路类型为 Access 类型。
5. 执行命令 **port default vlan** *vlan-id*，配置接口的缺省 VLAN。

说明

本处给出的是普通终端的接入配置，如果接入的是语音终端（SIP 话机），则接口的配置与之不同，详细指导请参考“7 VoIP 语音部署”。

----结束

2.4.3 接入交换机上行接口配置

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，批量创建 VLAN。
3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
4. 执行命令 **port link-type trunk**，配置接口的链路类型为 Trunk 类型。
5. 执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，将接口加入 VLAN。

----结束

2.4.4 汇聚/核心交换机接口配置

说明

汇聚交换机的上下行接口、核心交换机的下行接口、核心交换机互连的接口，其配置基本类似，只需要根据网络规划，配置不同的 VLAN 和 IP 地址即可。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，批量创建 VLAN。
3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
4. 执行命令 **port link-type trunk**，配置接口的链路类型为 Trunk 类型。
5. 执行命令 **port trunk allow-pass vlan** { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }，将接口加入 VLAN。
6. 执行命令 **quit**，返回系统视图。
7. 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口并进入 VLANIF 接口视图。
8. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 IP 地址。

----结束

2.5 配置路由

对于一般的园区网而言，通常不需要部署 BGP。除非出现如下场景，才需要部署 BGP：

- 网络中的路由数量过于庞大，IGP 难以胜任。
- 需要大量的使用路由策略或者是业务分流，IGP 等协议无法实现。
- 部署 MPLS L3VPN 技术时，需要实现复杂的隔离策略。

因此在本章中不介绍 BGP 的具体配置，如果有特殊需要，可以参考所使用产品的产品文档来进行部署。

对于 IGP，企业园区网中可以选择 IS-IS 或 OSPF（对于小园区网，也可选择 RIP），IS-IS 和 OSPF 协议在总体上差别不大，均可选择。以下以 OSPF 为例介绍 IGP 的部署。

在企业网中部署 OSPF，可以按照如下原则进行：

- 如果不需要部署 MPLS L3VPN，只启动一个 OSPF 进程即可。
- 核心交换机作为 OSPF 的 Area0。
- 每个业务部门区域作为一个单独的 OSPF Area，编号 1、2…N。Area1、2…N 使用 OSPF NSSA 区域，限制 LSA 在区域间的传播。
- 如果部门较少，可以把所有路由节点都配置为 Area0。

2.5.1 配置 OSPF 基本功能

请在需要运行 OSPF 协议的每台交换机上进行以下配置。

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **ospf** [*process-id*]，启动 OSPF 进程，进入 OSPF 视图。
3. 执行命令 **area** *area-id*，进入 OSPF 区域视图。
4. 执行命令 **network** *ip-address wildcard-mask* [**description** *text*]，配置区域所包含的网段。

----结束

2.5.2（可选）配置 NSSA 区域

如果要把某个区域设定为 NSSA 区域，请在 NSSA 区域中所有路由器上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ospf** [*process-id*]，进入 OSPF 视图。
3. 执行命令 **area** *area-id*，进入 OSPF 区域视图。
4. 执行命令 **nssa** [**default-route-advertise** | **flush-waiting-timer** *interval-value* | **no-import-route** | **no-summary** | **set-n-bit** | **suppress-forwarding-address** | **translator-always** | **translator-interval** *interval-value* | **zero-address-forwarding**] *，配置一个区域为 NSSA 区域。

----结束

2.5.3（可选）配置 IGP FC

为了保证 OSPF 的快速收敛，提高网络可靠性，可以配置 IGP FC 功能。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ospf** [*process-id*]，进入 OSPF 视图。
3. 执行命令 **prefix-priority** { **critical** | **high** | **medium** } **ip-prefix** *ip-prefix-name*，配置 OSPF 路由的收敛优先级。
4. 执行命令 **lsa-originate-interval** { **0** | { **intelligent-timer** *max-interval start-interval hold-interval* | **other-type** *interval* } * }，配置 LSA 的更新时间间隔。
5. 执行命令 **lsa-arrival-interval** { *interval* | **intelligent-timer** *max-interval start-interval hold-interval* }，配置 LSA 被接收的时间间隔。
6. 执行命令 **spf-schedule-interval** { *interval1* | **intelligent-timer** *max-interval start-interval hold-interval* | **millisecond** *interval2* }，设置 SPF 计算间隔。

----结束

2.6 配置 DHCP

在园区网中 DHCP 的部署方式比较灵活，通常有如下部署方式：

- 使用外置 DHCP 服务器，此时需要进行如下配置：
  - 接入交换机配置 DHCP Snooping

  - 汇聚交换机配置 DHCP Relay
- 使用汇聚交换机内置的 DHCP 服务器（全局地址池），此时需要进行如下配置：
  - 接入交换机配置 DHCP Snooping
  - 汇聚交换机配置 DHCP Server（全局地址池）
- 使用汇聚交换机内置的 DHCP 服务器（接口地址池），此时需要进行如下配置：
  - 接入交换机配置 DHCP Snooping
  - 汇聚交换机配置 DHCP Server（接口地址池）

说明

在汇聚交换机上配置 DHCP Relay 和 DHCP Server，均有多种配置方式和可选步骤，本节只介绍基本的配置方式和步骤，其他的配置方式以及可选步骤，请参见具体产品的文档。

2.6.1 接入交换机上配置 DHCP Snooping

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dhcp enable**，使能全局的 DHCP 功能。
3. 执行命令 **dhcp snooping enable**，使能全局的 DHCP Snooping 功能。
4. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
5. 执行命令 **dhcp snooping enable**，使能接口的 DHCP Snooping 功能。
6. （对于上行接口）执行命令 **dhcp snooping trusted**，配置接口为“信任”状态。

----结束

2.6.2 汇聚交换机上配置 DHCP Relay

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dhcp enable**，使能全局的 DHCP 功能。
3. 执行命令 **dhcp server group** *group-name*，创建 DHCP 服务器组。
4. 执行命令 **dhcp server** *ip-address*，配置 DHCP 服务器的 IP 地址。
5. 执行命令 **quit**，返回系统视图。
6. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
7. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 IP 地址。

   说明

   如果之前的配置过程中，VLANIF 接口已经配置了 IP 地址，则省略本步骤。
8. 执行命令 **dhcp select relay**，使能 VLANIF 接口的 DHCP 中继功能。
9. 执行命令 **dhcp relay server-select** *group-name*，配置 VLANIF 接口的 DHCP 服务器组。

----结束

2.6.3 汇聚交换机上配置 DHCP Server（全局地址池）

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dhcp enable**，使能全局的 DHCP 功能。
3. 执行命令 **ip pool** *ip-pool-name*，创建全局地址池并进入地址池视图。
4. 执行命令 **network** *ip-address* [**mask** { *mask* | *mask-length* }]，配置地址池中的 IP 地址。
5. 执行命令 **gateway-list** *ip-address* &<1-8>，配置地址池的出口网关。
6. 执行命令 **quit**，返回系统视图。
7. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
8. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 IP 地址。

   说明

   如果之前的配置过程中，VLANIF 接口已经配置了 IP 地址，则省略本步骤。
9. 执行命令 **dhcp select global**，使能接口的 DHCP 服务功能，并从全局地址池分配地址。

----结束

说明

使用全局地址池时，交换机会根据用户接入的 VLANIF 接口上所以配置的 IP 地址，选择位于同一网段的全局地址池来给用户分配 IP 地址。如果 VLANIF 接口没有配置 IP 地址，或者没有和接口 IP 地址位于同一网段的全局地址池，则用户无法上线。

2.6.4 汇聚交换机上配置 DHCP Server（接口地址池）

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dhcp enable**，使能全局的 DHCP 功能。
3. 执行命令 **interface vlanif** *vlan-id*，进入 VLANIF 接口视图。
4. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置 IP 地址。

   说明

   如果之前的配置过程中，VLANIF 接口已经配置了 IP 地址，则省略本步骤。
5. 执行命令 **dhcp select interface**，使能接口的 DHCP 服务功能，并从接口地址池分配地址。

----结束

说明

接口地址池的地址范围就是接口的 IP 地址所在的网段，且只在此接口下有效。

2.7 配置 QoS

园区网应该是一个无阻塞的网络，园区网部署 QoS 主要是防止 BT 等非正常业务流量对园区网关键业务以及关键客户流量形成冲击。

QoS 的部署需要是端到端的，每一层承担不同的角色，通常接入节点通过 Remark 动作进行业务流量区分，其他节点根据流分类调度即可。

以下以保障 VoIP 或者视频业务的高优先级（非 Voice VLAN 方式）为例，介绍园区网中 QoS 的基本部署方式。

2.7.1 接入交换机上配置重标记

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **traffic classifier** *classifier-name*，创建流分类并进入流分类视图。
3. 执行命令 **if-match vlan-id** *start-vlan-id* [**to** *end-vlan-id*]，定义基于 VLAN 的匹配规则。

   说明

   这里的 VLAN 就是指 VoIP 业务或视频业务所对应的 VLAN。
4. 执行命令 **quit**，返回系统视图。
5. 执行命令 **traffic behavior** *behavior-name*，创建流行为并进入流行为视图。
6. 执行命令 **remark 8021p** *8021p-value*，指定重新标记 802.1p 优先级。
7. 执行命令 **quit**，返回系统视图。
8. 执行命令 **traffic policy** *policy-name*，创建流策略并进入流策略视图。
9. 执行命令 **classifier** *classifier-name* **behavior** *behavior-name*，关联流分类和流行为。
10. 执行命令 **quit**，返回系统视图。
11. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

    说明

    这里的接口是指 VoIP 或视频业务接入的物理接口。
12. 执行命令 **traffic-policy** *policy-name* **inbound**，在接口入方向应用流策略。

----结束

2.7.2 汇聚层交换机上配置 QoS 调度

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

   说明

   这里的接口是指汇聚交换机的上行物理接口（非 Eth-Trunk 接口）。
3. 执行命令 **qos pq**，配置端口队列调度方式为 PQ。

----结束

2.8 配置可靠性

2.8.1 可靠性概述

园区网中的可靠性措施包括以下几类：

- 设备可靠性：通过部署 CSS/iStack、部件冗余等方式保证设备自身的可靠性。
- 链路可靠性：通过部署 Eth-Trunk 来实现链路的冗余备份和负载分担。
- 二层网络可靠性：通过部署 MSTP、SmartLink、DLDP、SEP、RRPP 等特性来保证二层网络的可靠性。
- 三层网络可靠性：通过部署 IP FRR、NSF/GR、VRRP、BFD 等特性来保证三层网络的可靠性。

我们推荐使用 CSS/iStack + Eth-Trunk 的组合方案来保证网络的可靠性。在这种方案中，由于采用了 CSS/iStack 技术将多台设备虚拟成了一台设备，而传统的双归接入等拓扑结构也被更简单的 Eth-Trunk 所取代。

采用 CSS/iStack + Eth-Trunk 后，通常不再需要部署 MSTP、SmartLink、DLDP、SEP、RRPP 等二层可靠性特性，也不再需要部署 VRRP+BFD。只需要再配合部署 IP FRR 等部分三层可靠性特性，即可保证整个园区网络的可靠性。

关于 CSS/iStack 的配置，请参见“5.2 配置堆叠/集群系统”。

关于 Eth-Trunk 的配置，请参见“2.4.1 配置 Eth-Trunk 接口”。

本节中只简单介绍 IP FRR 的配置。如果需要部署其他的可靠性特性，请参考所使用产品的产品文档。

说明

S2700/S3700/S5700 系列交换机不支持 IP FRR，S7700/S9300 系列交换机支持 IP FRR。

2.8.2 配置 IP FRR

请在运行动态路由协议的汇聚/核心交换机上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node*，创建 Route-Policy 的节点，并进入 Route-Policy 视图。
3. 根据需要执行不同的 **if-match** 子句，定义针对备份路由的过滤规则。
4. 执行命令 **apply backup-interface** *interface-type interface-number*，设置备份出接口。
5. 执行命令 **apply backup-nexthop** *ip-address*，设置备份下一跳。

说明

- 如果指定了备份下一跳，必须同时指定备份出接口。
- 如果在 P2P 链路上指定了备份出接口，可以不指定下一跳。
- 如果在非 P2P 链路上指定了备份出接口，必须同时指定下一跳。

6. 执行命令 **quit**，返回系统视图。
7. 执行命令 **ip frr route-policy** *route-policy-name*，使能 IP FRR 功能。

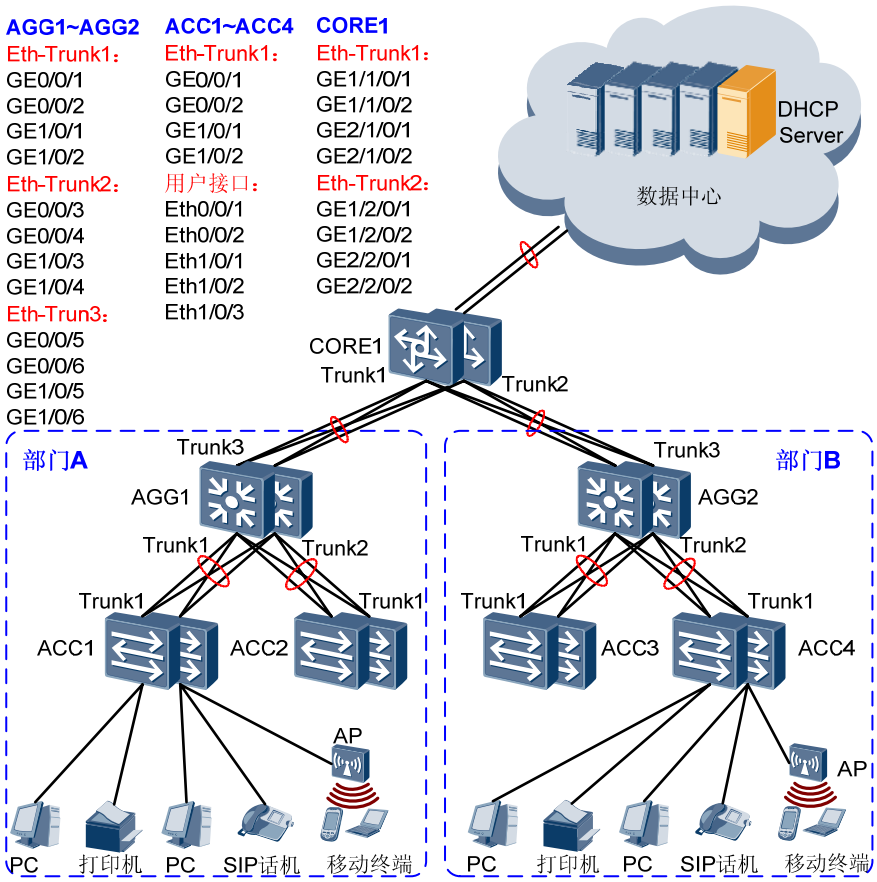
----结束

2.9 配置举例

组网需求

企业信息网络中，接入、汇聚、核心层采用支持堆叠/集群功能的交换机，组成堆叠/集群系统。企业中有 PC、打印机、SIP 话机以及移动设备等终端，需要进行终端的 VLAN 隔离，同时要保证 VoIP 业务的高优先级。如图 2-1 所示。

图2-1 基础网络部署组网图



数据准备

表2-2 数据规划表

配置项	配置子项	数据
VLAN	ACC1	部门 A 的 PC 终端：501 部门 A 的 SIP 终端：701 部门 A 的无线终端：801
	ACC2	部门 A 的 PC 终端：502 部门 A 的 SIP 终端：702 部门 A 的无线终端：802
	ACC3	部门 A 的 PC 终端：503 部门 A 的 SIP 终端：703 部门 A 的无线终端：803

配置项	配置子项	数据
	ACC4	部门 A 的 PC 终端：504 部门 A 的 SIP 终端：704 部门 A 的无线终端：804
	AGG1	1001
	AGG2	1002
设备 IP 地址	AGG1	VLANIF 501：10.20.1.1/24 VLANIF 701：10.21.1.1/24 VLANIF 801：10.22.1.1/24 VLANIF 502：10.20.2.1/24 VLANIF 702：10.21.2.1/24 VLANIF 802：10.22.2.1/24 VLANIF 1001：10.1.0.1/24 LoopBack0：2.2.2.2/32
	AGG2	VLANIF 503：10.20.3.1/24 VLANIF 703：10.21.3.1/24 VLANIF 803：10.22.3.1/24 VLANIF 504：10.20.4.1/24 VLANIF 704：10.21.4.1/24 VLANIF 804：10.22.4.1/24 VLANIF 1002：10.1.1.1/24 LoopBack0：3.3.3.3/32
	CORE1	VLANIF 1001：10.1.0.2/24 VLANIF 1002：10.1.1.2/24 LoopBack0：1.1.1.1/32
服务器 IP 地址	DHCP 服务器	10.10.0.1
用户 IP 地址	部门 A	PC 终端：10.20.1.0/24~10.20.2.0/24 SIP 话机：10.21.1.0/24~10.21.2.0/24 无线终端：10.22.1.0/24~10.22.2.0/24
	部门 B	PC 终端：10.20.3.0/24~10.20.4.0/24 SIP 话机：10.21.3.0/24~10.21.4.0/24 无线终端：10.22.3.0/24~10.22.4.0/24
QoS	SIP 业务优先级	7

操作步骤

1. 配置 CORE 的 CSS 集群。

   # 在 CORE1 的主交换机上配置 CSS 集群。

```
<CORE1> system-view
[CORE1] set css priority 255
[CORE1] css enable
```

   # 在 CORE1 的从交换机上配置 CSS 集群。

```
<CORE1_S> system-view
[CORE1_S] set css id 2
[CORE1_S] css enable
```

   配置之后，CORE1 集群建立，后续的配置都在主交换机上进行。

   说明

   对于其余交换机设备，只要各交换机都插入堆叠卡，并且使用堆叠线缆正确连接，则各交换机上电之后，会自动建立 iStack 堆叠系统，无需进行配置。

2. 配置接口和 VLAN。

   # 配置接入交换机 ACC1 的接口和 VLAN。

```
<ACC1> system-view
[ACC1] vlan batch 501 701 801
[ACC1] interface Ethernet 0/0/1
[ACC1-Ethernet0/0/1] port link-type access
[ACC1-Ethernet0/0/1] port default vlan 501
[ACC1-Ethernet0/0/1] quit
[ACC1] interface Ethernet 0/0/2
[ACC1-Ethernet0/0/2] port link-type access
[ACC1-Ethernet0/0/2] port default vlan 501
[ACC1-Ethernet0/0/2] quit
[ACC1] interface Ethernet 1/0/1
[ACC1-Ethernet1/0/1] port link-type access
[ACC1-Ethernet1/0/1] port default vlan 501
[ACC1-Ethernet1/0/1] quit
[ACC1] interface Ethernet 1/0/2
[ACC1-Ethernet1/0/2] port link-type access
[ACC1-Ethernet1/0/2] port default vlan 701
[ACC1-Ethernet1/0/2] quit
[ACC1] interface Ethernet 1/0/3
[ACC1-Ethernet1/0/3] port link-type access
[ACC1-Ethernet1/0/3] port default vlan 801
[ACC1-Ethernet1/0/3] quit
[ACC1] interface Eth-Trunk 1
[ACC1-Eth-Trunk1] port link-type trunk
[ACC1-Eth-Trunk1] port trunk allow-pass vlan 501 701 801
[ACC1-Eth-Trunk1] mode lacp-static
[ACC1-Eth-Trunk1] load-balance src-mac
[ACC1-Eth-Trunk1] quit
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet0/0/1] Eth-Trunk 1
[ACC1-GigabitEthernet0/0/1] quit
```

```
[ACC1] interface GigabitEthernet 0/0/2
[ACC1-GigabitEthernet0/0/2] Eth-Trunk 1
[ACC1-GigabitEthernet0/0/2] quit
[ACC1] interface GigabitEthernet 1/0/1
[ACC1-GigabitEthernet1/0/1] Eth-Trunk 1
[ACC1-GigabitEthernet1/0/1] quit
[ACC1] interface GigabitEthernet 1/0/2
[ACC1-GigabitEthernet1/0/2] Eth-Trunk 1
[ACC1-GigabitEthernet1/0/2] quit
```

配置接入交换机 ACC2 的接口和 VLAN。

```
<ACC2> system-view
[ACC2] vlan batch 502 702 802
[ACC2] interface Ethernet 0/0/1
[ACC2-Ethernet0/0/1] port link-type access
[ACC2-Ethernet0/0/1] port default vlan 502
[ACC2-Ethernet0/0/1] quit
[ACC2] interface Ethernet 0/0/2
[ACC2-Ethernet0/0/2] port link-type access
[ACC2-Ethernet0/0/2] port default vlan 502
[ACC2-Ethernet0/0/2] quit
[ACC2] interface Ethernet 1/0/1
[ACC2-Ethernet1/0/1] port link-type access
[ACC2-Ethernet1/0/1] port default vlan 502
[ACC2-Ethernet1/0/1] quit
[ACC2] interface Ethernet 1/0/2
[ACC2-Ethernet1/0/2] port link-type access
[ACC2-Ethernet1/0/2] port default vlan 702
[ACC2-Ethernet1/0/2] quit
[ACC2] interface Ethernet 1/0/3
[ACC2-Ethernet1/0/3] port link-type access
[ACC2-Ethernet1/0/3] port default vlan 802
[ACC2-Ethernet1/0/3] quit
[ACC2] interface Eth-Trunk 1
[ACC2-Eth-Trunk1] port link-type trunk
[ACC2-Eth-Trunk1] port trunk allow-pass vlan 502 702 802
[ACC2-Eth-Trunk1] mode lacp-static
[ACC2-Eth-Trunk1] load-balance src-mac
[ACC2-Eth-Trunk1] quit
[ACC2] interface GigabitEthernet 0/0/1
[ACC2-GigabitEthernet0/0/1] Eth-Trunk 1
[ACC2-GigabitEthernet0/0/1] quit
[ACC2] interface GigabitEthernet 0/0/2
[ACC2-GigabitEthernet0/0/2] Eth-Trunk 1
[ACC2-GigabitEthernet0/0/2] quit
[ACC2] interface GigabitEthernet 1/0/1
[ACC2-GigabitEthernet1/0/1] Eth-Trunk 1
[ACC2-GigabitEthernet1/0/1] quit
[ACC2] interface GigabitEthernet 1/0/2
[ACC2-GigabitEthernet1/0/2] Eth-Trunk 1
[ACC2-GigabitEthernet1/0/2] quit
```

配置接入交换机 ACC3 的接口和 VLAN。

```
<ACC3> system-view
[ACC3] vlan batch 503 703 803
```

```
[ACC3] interface Ethernet 0/0/1
[ACC3-Ethernet0/0/1] port link-type access
[ACC3-Ethernet0/0/1] port default vlan 503
[ACC3-Ethernet0/0/1] quit
[ACC3] interface Ethernet 0/0/2
[ACC3-Ethernet0/0/2] port link-type access
[ACC3-Ethernet0/0/2] port default vlan 503
[ACC3-Ethernet0/0/2] quit
[ACC3] interface Ethernet 1/0/1
[ACC3-Ethernet1/0/1] port link-type access
[ACC3-Ethernet1/0/1] port default vlan 503
[ACC3-Ethernet1/0/1] quit
[ACC3] interface Ethernet 1/0/2
[ACC3-Ethernet1/0/2] port link-type access
[ACC3-Ethernet1/0/2] port default vlan 703
[ACC3-Ethernet1/0/2] quit
[ACC3] interface Ethernet 1/0/3
[ACC3-Ethernet1/0/3] port link-type access
[ACC3-Ethernet1/0/3] port default vlan 803
[ACC3-Ethernet1/0/3] quit
[ACC3] interface Eth-Trunk 1
[ACC3-Eth-Trunk1] port link-type trunk
[ACC3-Eth-Trunk1] port trunk allow-pass vlan 503 703 803
[ACC3-Eth-Trunk1] mode lacp-static
[ACC3-Eth-Trunk1] load-balance src-mac
[ACC3-Eth-Trunk1] quit
[ACC3] interface GigabitEthernet 0/0/1
[ACC3-GigabitEthernet0/0/1] Eth-Trunk 1
[ACC3-GigabitEthernet0/0/1] quit
[ACC3] interface GigabitEthernet 0/0/2
[ACC3-GigabitEthernet0/0/2] Eth-Trunk 1
[ACC3-GigabitEthernet0/0/2] quit
[ACC3] interface GigabitEthernet 1/0/1
[ACC3-GigabitEthernet1/0/1] Eth-Trunk 1
[ACC3-GigabitEthernet1/0/1] quit
[ACC3] interface GigabitEthernet 1/0/2
[ACC3-GigabitEthernet1/0/2] Eth-Trunk 1
[ACC3-GigabitEthernet1/0/2] quit
```

配置接入交换机 ACC4 的接口和 VLAN。

```
<ACC4> system-view
[ACC4] vlan batch 504 704 804
[ACC4] interface Ethernet 0/0/1
[ACC4-Ethernet0/0/1] port link-type access
[ACC4-Ethernet0/0/1] port default vlan 504
[ACC4-Ethernet0/0/1] quit
[ACC4] interface Ethernet 0/0/2
[ACC4-Ethernet0/0/2] port link-type access
[ACC4-Ethernet0/0/2] port default vlan 504
[ACC4-Ethernet0/0/2] quit
[ACC4] interface Ethernet 1/0/1
[ACC4-Ethernet1/0/1] port link-type access
[ACC4-Ethernet1/0/1] port default vlan 504
[ACC4-Ethernet1/0/1] quit
[ACC4] interface Ethernet 1/0/2
```



```
[ACC4-Ethernet1/0/2] port link-type access
[ACC4-Ethernet1/0/2] port default vlan 704
[ACC4-Ethernet1/0/2] quit
[ACC4] interface Ethernet 1/0/3
[ACC4-Ethernet1/0/3] port link-type access
[ACC4-Ethernet1/0/3] port default vlan 804
[ACC4-Ethernet1/0/3] quit
[ACC4] interface Eth-Trunk 1
[ACC4-Eth-Trunk1] port link-type trunk
[ACC4-Eth-Trunk1] port trunk allow-pass vlan 504 704 804
[ACC4-Eth-Trunk1] mode lacp-static
[ACC4-Eth-Trunk1] load-balance src-mac
[ACC4-Eth-Trunk1] quit
[ACC4] interface GigabitEthernet 0/0/1
[ACC4-GigabitEthernet0/0/1] Eth-Trunk 1
[ACC4-GigabitEthernet0/0/1] quit
[ACC4] interface GigabitEthernet 0/0/2
[ACC4-GigabitEthernet0/0/2] Eth-Trunk 1
[ACC4-GigabitEthernet0/0/2] quit
[ACC4] interface GigabitEthernet 1/0/1
[ACC4-GigabitEthernet1/0/1] Eth-Trunk 1
[ACC4-GigabitEthernet1/0/1] quit
[ACC4] interface GigabitEthernet 1/0/2
[ACC4-GigabitEthernet1/0/2] Eth-Trunk 1
[ACC4-GigabitEthernet1/0/2] quit
```

配置汇聚交换机 AGG1 的接口和 VLAN。

```
<AGG1> system-view
[AGG1] vlan batch 501 502 701 702 801 802 1001
[AGG1] interface Eth-Trunk 1
[AGG1-Eth-Trunk1] port link-type trunk
[AGG1-Eth-Trunk1] port trunk allow-pass vlan 501 701 801
[AGG1-Eth-Trunk1] mode lacp-static
[AGG1-Eth-Trunk1] load-balance src-mac
[AGG1-Eth-Trunk1] quit
[AGG1] interface GigabitEthernet 0/0/1
[AGG1-GigabitEthernet0/0/1] Eth-Trunk 1
[AGG1-GigabitEthernet0/0/1] quit
[AGG1] interface GigabitEthernet 0/0/2
[AGG1-GigabitEthernet0/0/2] Eth-Trunk 1
[AGG1-GigabitEthernet0/0/2] quit
[AGG1] interface GigabitEthernet 1/0/1
[AGG1-GigabitEthernet1/0/1] Eth-Trunk 1
[AGG1-GigabitEthernet1/0/1] quit
[AGG1] interface GigabitEthernet 1/0/2
[AGG1-GigabitEthernet1/0/2] Eth-Trunk 1
[AGG1-GigabitEthernet1/0/2] quit
[AGG1] interface Eth-Trunk 2
[AGG1-Eth-Trunk2] port link-type trunk
[AGG1-Eth-Trunk2] port trunk allow-pass vlan 502 702 802
[AGG1-Eth-Trunk2] mode lacp-static
[AGG1-Eth-Trunk2] load-balance src-mac
[AGG1-Eth-Trunk2] quit
[AGG1] interface GigabitEthernet 0/0/3
[AGG1-GigabitEthernet0/0/3] Eth-Trunk 2
```

```
[AGG1-GigabitEthernet0/0/3] quit
[AGG1] interface GigabitEthernet 0/0/4
[AGG1-GigabitEthernet0/0/4] Eth-Trunk 2
[AGG1-GigabitEthernet0/0/4] quit
[AGG1] interface GigabitEthernet 1/0/3
[AGG1-GigabitEthernet1/0/3] Eth-Trunk 2
[AGG1-GigabitEthernet1/0/3] quit
[AGG1] interface GigabitEthernet 1/0/4
[AGG1-GigabitEthernet1/0/4] Eth-Trunk 2
[AGG1-GigabitEthernet1/0/4] quit
[AGG1] interface Eth-Trunk 3
[AGG1-Eth-Trunk3] port link-type trunk
[AGG1-Eth-Trunk3] port trunk allow-pass vlan 1001
[AGG1-Eth-Trunk3] mode lacp-static
[AGG1-Eth-Trunk3] load-balance src-mac
[AGG1-Eth-Trunk3] quit
[AGG1] interface GigabitEthernet 0/0/5
[AGG1-GigabitEthernet0/0/5] Eth-Trunk 3
[AGG1-GigabitEthernet0/0/5] quit
[AGG1] interface GigabitEthernet 0/0/6
[AGG1-GigabitEthernet0/0/6] Eth-Trunk 3
[AGG1-GigabitEthernet0/0/6] quit
[AGG1] interface GigabitEthernet 1/0/5
[AGG1-GigabitEthernet1/0/5] Eth-Trunk 3
[AGG1-GigabitEthernet1/0/5] quit
[AGG1] interface GigabitEthernet 1/0/6
[AGG1-GigabitEthernet1/0/6] Eth-Trunk 3
[AGG1-GigabitEthernet1/0/6] quit
[AGG1] interface vlanif 501
[AGG1-Vlanif501] ip address 10.20.1.1 255.255.255.0
[AGG1-Vlanif501] quit
[AGG1] interface vlanif 701
[AGG1-Vlanif701] ip address 10.21.1.1 255.255.255.0
[AGG1-Vlanif701] quit
[AGG1] interface vlanif 801
[AGG1-Vlanif801] ip address 10.22.1.1 255.255.255.0
[AGG1-Vlanif801] quit
[AGG1] interface vlanif 502
[AGG1-Vlanif502] ip address 10.20.2.1 255.255.255.0
[AGG1-Vlanif502] quit
[AGG1] interface vlanif 702
[AGG1-Vlanif702] ip address 10.21.2.1 255.255.255.0
[AGG1-Vlanif702] quit
[AGG1] interface vlanif 802
[AGG1-Vlanif802] ip address 10.22.2.1 255.255.255.0
[AGG1-Vlanif802] quit
[AGG1] interface vlanif 1001
[AGG1-Vlanif1001] ip address 10.1.0.1 255.255.255.0
[AGG1-Vlanif1001] quit
```

配置汇聚交换机 AGG2 的接口和 VLAN。

```
<AGG2> system-view
[AGG2] vlan batch 503 504 703 704 803 804 1002
[AGG2] interface Eth-Trunk 1
[AGG2-Eth-Trunk1] port link-type trunk
```

```
[AGG2-Eth-Trunk1] port trunk allow-pass vlan 503 703 803
[AGG2-Eth-Trunk1] mode lacp-static
[AGG2-Eth-Trunk1] load-balance src-mac
[AGG2-Eth-Trunk1] quit
[AGG2] interface GigabitEthernet 0/0/1
[AGG2-GigabitEthernet0/0/1] Eth-Trunk 1
[AGG2-GigabitEthernet0/0/1] quit
[AGG2] interface GigabitEthernet 0/0/2
[AGG2-GigabitEthernet0/0/2] Eth-Trunk 1
[AGG2-GigabitEthernet0/0/2] quit
[AGG2] interface GigabitEthernet 1/0/1
[AGG2-GigabitEthernet1/0/1] Eth-Trunk 1
[AGG2-GigabitEthernet1/0/1] quit
[AGG2] interface GigabitEthernet 1/0/2
[AGG2-GigabitEthernet1/0/2] Eth-Trunk 1
[AGG2-GigabitEthernet1/0/2] quit
[AGG2] interface Eth-Trunk 2
[AGG2-Eth-Trunk2] port link-type trunk
[AGG2-Eth-Trunk2] port trunk allow-pass vlan 504 704 804
[AGG2-Eth-Trunk2] mode lacp-static
[AGG2-Eth-Trunk2] load-balance src-mac
[AGG2-Eth-Trunk2] quit
[AGG2] interface GigabitEthernet 0/0/3
[AGG2-GigabitEthernet0/0/3] Eth-Trunk 2
[AGG2-GigabitEthernet0/0/3] quit
[AGG2] interface GigabitEthernet 0/0/4
[AGG2-GigabitEthernet0/0/4] Eth-Trunk 2
[AGG2-GigabitEthernet0/0/4] quit
[AGG2] interface GigabitEthernet 1/0/3
[AGG2-GigabitEthernet1/0/3] Eth-Trunk 2
[AGG2-GigabitEthernet1/0/3] quit
[AGG2] interface GigabitEthernet 1/0/4
[AGG2-GigabitEthernet1/0/4] Eth-Trunk 2
[AGG2-GigabitEthernet1/0/4] quit
[AGG2] interface Eth-Trunk 3
[AGG2-Eth-Trunk3] port link-type trunk
[AGG2-Eth-Trunk3] port trunk allow-pass vlan 1002
[AGG2-Eth-Trunk3] mode lacp-static
[AGG2-Eth-Trunk3] load-balance src-mac
[AGG2-Eth-Trunk3] quit
[AGG2] interface GigabitEthernet 0/0/5
[AGG2-GigabitEthernet0/0/5] Eth-Trunk 3
[AGG2-GigabitEthernet0/0/5] quit
[AGG2] interface GigabitEthernet 0/0/6
[AGG2-GigabitEthernet0/0/6] Eth-Trunk 3
[AGG2-GigabitEthernet0/0/6] quit
[AGG2] interface GigabitEthernet 1/0/5
[AGG2-GigabitEthernet1/0/5] Eth-Trunk 3
[AGG2-GigabitEthernet1/0/5] quit
[AGG2] interface GigabitEthernet 1/0/6
[AGG2-GigabitEthernet1/0/6] Eth-Trunk 3
[AGG2-GigabitEthernet1/0/6] quit
[AGG2] interface vlanif 503
[AGG2-Vlanif503] ip address 10.20.3.1 255.255.255.0
[AGG2-Vlanif503] quit
```

```
[AGG2] interface vlanif 703
[AGG2-Vlanif703] ip address 10.21.3.1 255.255.255.0
[AGG2-Vlanif703] quit
[AGG2] interface vlanif 803
[AGG2-Vlanif803] ip address 10.22.3.1 255.255.255.0
[AGG2-Vlanif803] quit
[AGG2] interface vlanif 504
[AGG2-Vlanif504] ip address 10.20.4.1 255.255.255.0
[AGG2-Vlanif504] quit
[AGG2] interface vlanif 704
[AGG2-Vlanif704] ip address 10.21.4.1 255.255.255.0
[AGG2-Vlanif704] quit
[AGG2] interface vlanif 804
[AGG2-Vlanif804] ip address 10.22.4.1 255.255.255.0
[AGG2-Vlanif804] quit
[AGG2] interface vlanif 1002
[AGG2-Vlanif1002] ip address 10.1.1.1 255.255.255.0
[AGG2-Vlanif1002] quit
```

配置核心交换机 CORE1 的接口和 VLAN。

```
<CORE1> system-view
[CORE1] vlan batch 1001 1002
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] port link-type trunk
[CORE1-Eth-Trunk1] port trunk allow-pass vlan 1001
[CORE1-Eth-Trunk1] mode lacp-static
[CORE1-Eth-Trunk1] load-balance src-mac
[CORE1-Eth-Trunk1] lacp preempt enable
[CORE1-Eth-Trunk1] quit
[CORE1] interface GigabitEthernet 1/1/0/1
[CORE1-GigabitEthernet1/1/0/1] Eth-Trunk 1
[CORE1-GigabitEthernet1/1/0/1] quit
[CORE1] interface GigabitEthernet 1/1/0/2
[CORE1-GigabitEthernet1/1/0/2] Eth-Trunk 1
[CORE1-GigabitEthernet1/1/0/2] quit
[CORE1] interface GigabitEthernet 2/1/0/1
[CORE1-GigabitEthernet2/1/0/1] Eth-Trunk 1
[CORE1-GigabitEthernet2/1/0/1] quit
[CORE1] interface GigabitEthernet 2/1/0/2
[CORE1-GigabitEthernet2/1/0/2] Eth-Trunk 1
[CORE1-GigabitEthernet2/1/0/2] quit
[CORE1] interface Eth-Trunk 2
[CORE1-Eth-Trunk2] port link-type trunk
[CORE1-Eth-Trunk2] port trunk allow-pass vlan 1002
[CORE1-Eth-Trunk2] mode lacp-static
[CORE1-Eth-Trunk2] load-balance src-mac
[CORE1-Eth-Trunk2] lacp preempt enable
[CORE1-Eth-Trunk2] quit
[CORE1] interface GigabitEthernet 1/2/0/1
[CORE1-GigabitEthernet1/2/0/1] Eth-Trunk 2
[CORE1-GigabitEthernet1/2/0/1] quit
[CORE1] interface GigabitEthernet 1/2/0/2
[CORE1-GigabitEthernet1/2/0/2] Eth-Trunk 2
[CORE1-GigabitEthernet1/2/0/2] quit
[CORE1] interface GigabitEthernet 2/2/0/1
```

```
[CORE1-GigabitEthernet2/2/0/1] Eth-Trunk 2
[CORE1-GigabitEthernet2/2/0/1] quit
[CORE1] interface GigabitEthernet 2/2/0/2
[CORE1-GigabitEthernet2/2/0/2] Eth-Trunk 2
[CORE1-GigabitEthernet2/2/0/2] quit
[CORE1] interface vlanif 1001
[CORE1-Vlanif1001] ip address 10.1.0.2 255.255.255.0
[CORE1-Vlanif1001] quit
[CORE1] interface vlanif 1002
[CORE1-Vlanif1002] ip address 10.1.1.2 255.255.255.0
[CORE1-Vlanif1002] quit
```

3. 配置路由协议。

   # 配置 AGG1 上的路由协议。

```
[AGG1] interface LoopBack 0
[AGG1-LoopBack0] ip address 2.2.2.2 32
[AGG1-LoopBack0] quit
[AGG1] ospf 1
[AGG1-ospf-1] area 0
[AGG1-ospf-1-area-0.0.0.0] network 10.20.1.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 10.20.2.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 10.21.1.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 10.21.2.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 10.22.1.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 10.22.2.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 10.1.0.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[AGG1-ospf-1-area-0.0.0.0] quit
```

   # 配置 AGG2 上的路由协议。

```
[AGG2] interface LoopBack 0
[AGG2-LoopBack0] ip address 3.3.3.3 32
[AGG2-LoopBack0] quit
[AGG2] ospf 1
[AGG2-ospf-1] area 0
[AGG2-ospf-1-area-0.0.0.0] network 10.20.3.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 10.20.4.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 10.21.3.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 10.21.4.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 10.22.3.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 10.22.4.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[AGG2-ospf-1-area-0.0.0.0] quit
```

   # 配置 CORE1 上的路由协议。

```
[CORE1] interface LoopBack 0
[CORE1-LoopBack0] ip address 1.1.1.1 32
[CORE1-LoopBack0] quit
[CORE1] ospf 1
[CORE1-ospf-1] area 0
[CORE1-ospf-1-area-0.0.0.0] network 10.1.0.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 10.1.1.2 0.0.0.255
```

```
[CORE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[CORE1-ospf-1-area-0.0.0.0] quit
```

4. 配置 DHCP。

   # 配置 ACC1 上的 DHCP Snooping 功能。

```
[ACC1] dhcp enable
[ACC1] dhcp snooping enable
[ACC1] interface Ethernet 0/0/1
[ACC1-Ethernet0/0/1] dhcp snooping enable
[ACC1-Ethernet0/0/1] quit
[ACC1] interface Ethernet 0/0/2
[ACC1-Ethernet0/0/2] dhcp snooping enable
[ACC1-Ethernet0/0/2] quit
[ACC1] interface Ethernet 1/0/1
[ACC1-Ethernet1/0/1] dhcp snooping enable
[ACC1-Ethernet1/0/1] quit
[ACC1] interface Ethernet 1/0/2
[ACC1-Ethernet1/0/2] dhcp snooping enable
[ACC1-Ethernet1/0/2] quit
[ACC1] interface Ethernet 1/0/3
[ACC1-Ethernet1/0/3] dhcp snooping enable
[ACC1-Ethernet1/0/3] quit
[ACC1] interface Eth-Trunk 1
[ACC1-Eth-Trunk1] dhcp snooping enable
[ACC1-Eth-Trunk1] dhcp snooping trusted
[ACC1-Eth-Trunk1] quit
```

   ACC2、ACC3、ACC4 的配置与 ACC1 相同。

   # 配置 AGG1 上的 DHCP Relay 功能。

```
[AGG1] dhcp enable
[AGG1] dhcp server group group1
[AGG1-dhcp-server-group-group1] dhcp-server 10.10.0.1
[AGG1-dhcp-server-group-group1] quit
[AGG1] interface vlanif 501
[AGG1-Vlanif501] dhcp select relay
[AGG1-Vlanif501] dhcp relay server-select group1
[AGG1-Vlanif501] quit
[AGG1] interface vlanif 701
[AGG1-Vlanif701] dhcp select relay
[AGG1-Vlanif701] dhcp relay server-select group1
[AGG1-Vlanif701] quit
[AGG1] interface vlanif 801
[AGG1-Vlanif801] dhcp select relay
[AGG1-Vlanif801] dhcp relay server-select group1
[AGG1-Vlanif801] quit
[AGG1] interface vlanif 502
[AGG1-Vlanif502] dhcp select relay
[AGG1-Vlanif502] dhcp relay server-select group1
[AGG1-Vlanif502] quit
[AGG1] interface vlanif 702
[AGG1-Vlanif702] dhcp select relay
[AGG1-Vlanif702] dhcp relay server-select group1
[AGG1-Vlanif702] quit
```

```
[AGG1] interface vlanif 802
[AGG1-Vlanif802] dhcp select relay
[AGG1-Vlanif802] dhcp relay server-select group1
[AGG1-Vlanif802] quit
```

配置 AGG2 上的 DHCP Relay 功能。

```
[AGG2] dhcp enable
[AGG2] dhcp server group group1
[AGG2-dhcp-server-group-group1] dhcp-server 10.10.0.1
[AGG2-dhcp-server-group-group1] quit
[AGG2] interface vlanif 503
[AGG2-Vlanif503] dhcp select relay
[AGG2-Vlanif503] dhcp relay server-select group1
[AGG2-Vlanif503] quit
[AGG2] interface vlanif 703
[AGG2-Vlanif703] dhcp select relay
[AGG2-Vlanif703] dhcp relay server-select group1
[AGG2-Vlanif703] quit
[AGG2] interface vlanif 803
[AGG2-Vlanif803] dhcp select relay
[AGG2-Vlanif803] dhcp relay server-select group1
[AGG2-Vlanif803] quit
[AGG2] interface vlanif 504
[AGG2-Vlanif504] dhcp select relay
[AGG2-Vlanif504] dhcp relay server-select group1
[AGG2-Vlanif504] quit
[AGG2] interface vlanif 704
[AGG2-Vlanif704] dhcp select relay
[AGG2-Vlanif704] dhcp relay server-select group1
[AGG2-Vlanif704] quit
[AGG2] interface vlanif 804
[AGG2-Vlanif804] dhcp select relay
[AGG2-Vlanif804] dhcp relay server-select group1
[AGG2-Vlanif804] quit
```

5. 配置 QoS。

配置 ACC1。

```
[ACC1] traffic classifier voip
[ACC1-classifier-voip] if-match vlan 701
[ACC1-classifier-voip] quit
[ACC1] traffic behavior voip
[ACC1-behavior-voip] remark 8021p 7
[ACC1-behavior-voip] quit
[ACC1] traffic policy voip
[ACC1-trafficpolicy-voip] classifier voip behavior voip
[ACC1-trafficpolicy-voip] quit
[ACC1] interface Ethernet 1/0/2
[ACC1-Ethernet1/0/2] traffic-policy voip inbound
```

ACC2、ACC3、ACC4 的配置与 ACC1 类似，只需要把 if-match 子句中的 VLAN 分别改为 702、703 和 704。

配置 AGG1。

```
[AGG1] interface GigabitEthernet 0/0/5
[AGG1-GigabitEthernet0/0/5] qos pq
[AGG1-GigabitEthernet0/0/5] quit
[AGG1] interface GigabitEthernet 0/0/6
[AGG1-GigabitEthernet0/0/6] qos pq
[AGG1-GigabitEthernet0/0/6] quit
[AGG1] interface GigabitEthernet 1/0/5
[AGG1-GigabitEthernet1/0/5] qos pq
[AGG1-GigabitEthernet1/0/5] quit
[AGG1] interface GigabitEthernet 1/0/6
[AGG1-GigabitEthernet1/0/6] qos pq
[AGG1-GigabitEthernet1/0/6] quit
```

AGG2 的配置与 AGG1 相同。

----结束

配置文件

- ACC1 配置文件

```
#
 sysname ACC1
#
 vlan batch 501 701 801
#
 dhcp enable
 dhcp snooping enable
#
traffic classifier voip operator and
 if-match vlan-id 701
#
traffic behavior voip
 remark 8021p 7
#
traffic policy voip
 classifier voip behavior voip
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 501 701 801
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
 dhcp snooping enable
 dhcp snooping trusted
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 501
 dhcp snooping enable
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 501
 dhcp snooping enable
```



```
#
interface Ethernet1/0/1
 port link-type access
 port default vlan 501
 dhcp snooping enable
#
interface Ethernet1/0/2
 port link-type access
 port default vlan 701
 traffic-policy voip inbound
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
interface GigabitEthernet1/0/1
 eth-trunk 1
#
interface GigabitEthernet1/0/2
 eth-trunk 1
#
return
```

ACC2~ACC4 的配置与之类似，只是配置的 VLAN 不同。

- AGG1 配置文件

```
#
 sysname AGG1
#
  vlan batch 501 to 502 701 to 702 801 to 802 1001
#
 dhcp enable
#
dhcp server group group1
 dhcp-server 10.10.0.1 0
#
interface Vlanif501
 ip address 10.20.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif502
 ip address 10.20.2.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif701
 ip address 10.21.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif702
 ip address 10.21.2.1 255.255.255.0
```



```
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif801
 ip address 10.22.1.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif802
 ip address 10.22.2.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif1001
 ip address 10.1.0.1 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 501 701 801
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 502 702 802
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface Eth-Trunk3
 port link-type trunk
 port trunk allow-pass vlan 1001
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
interface GigabitEthernet0/0/3
 eth-trunk 2
#
interface GigabitEthernet0/0/4
 eth-trunk 2
#
interface GigabitEthernet0/0/5
 eth-trunk 3
 qos pq
#
interface GigabitEthernet0/0/6
 eth-trunk 3
```

```
 qos pq
#
interface GigabitEthernet1/0/1
 eth-trunk 1
#
interface GigabitEthernet1/0/2
 eth-trunk 1
#
interface GigabitEthernet1/0/3
 eth-trunk 2
#
interface GigabitEthernet1/0/4
 eth-trunk 2
#
interface GigabitEthernet1/0/5
 eth-trunk 3
 qos pq
#
interface GigabitEthernet1/0/6
 eth-trunk 3
 qos pq
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.20.1.0 0.0.0.255
  network 10.20.2.0 0.0.0.255
  network 10.21.1.0 0.0.0.255
  network 10.21.2.0 0.0.0.255
  network 10.22.1.0 0.0.0.255
  network 10.22.2.0 0.0.0.255
  network 10.1.0.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
return
```

- AGG2 配置文件

```
#
 sysname AGG2
#
  vlan batch 503 to 504 703 to 704 801 to 804 1002
#
 dhcp enable
#
dhcp server group group1
 dhcp-server 10.10.0.1 0
#
interface Vlanif503
 ip address 10.20.3.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif504
 ip address 10.20.4.1 255.255.255.0
```



```
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif703
 ip address 10.21.3.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif704
 ip address 10.21.4.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif803
 ip address 10.22.3.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif804
 ip address 10.22.4.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif1002
 ip address 10.1.1.1 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 503 703 803
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 504 704 804
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface Eth-Trunk3
 port link-type trunk
 port trunk allow-pass vlan 1002
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface GigabitEthernet0/0/1
 eth-trunk 1
#
interface GigabitEthernet0/0/2
 eth-trunk 1
#
interface GigabitEthernet0/0/3
 eth-trunk 2
```



```
#
interface GigabitEthernet0/0/4
 eth-trunk 2
#
interface GigabitEthernet0/0/5
 eth-trunk 3
 qos pq
#
interface GigabitEthernet0/0/6
 eth-trunk 3
 qos pq
#
interface GigabitEthernet1/0/1
 eth-trunk 1
#
interface GigabitEthernet1/0/2
 eth-trunk 1
#
interface GigabitEthernet1/0/3
 eth-trunk 2
#
interface GigabitEthernet1/0/4
 eth-trunk 2
#
interface GigabitEthernet1/0/5
 eth-trunk 3
 qos pq
#
interface GigabitEthernet1/0/6
 eth-trunk 3
 qos pq
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.20.3.0 0.0.0.255
  network 10.20.4.0 0.0.0.255
  network 10.21.3.0 0.0.0.255
  network 10.21.4.0 0.0.0.255
  network 10.22.3.0 0.0.0.255
  network 10.22.4.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
return
```

- CORE1 的配置文件

```
#
 sysname CORE1
#
  vlan batch 1001 to 1002
#
interface Vlanif1001
 ip address 10.1.0.2 255.255.255.0
```



```
#
interface Vlanif1002
 ip address 10.1.1.2 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 1001
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 1002
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface GigabitEthernet1/1/0/1
 eth-trunk 1
#
interface GigabitEthernet1/1/0/2
 eth-trunk 1
#
interface GigabitEthernet1/2/0/1
 eth-trunk 2
#
interface GigabitEthernet1/2/0/2
 eth-trunk 2
#
interface GigabitEthernet2/1/0/1
 eth-trunk 1
#
interface GigabitEthernet2/1/0/2
 eth-trunk 1
#
interface GigabitEthernet2/2/0/1
 eth-trunk 2
#
interface GigabitEthernet2/2/0/2
 eth-trunk 2
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 10.1.0.0 0.0.0.255
  network 10.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
return
```

3 园区无线接入部署

3.1 概述

3.1.1 WLAN 简介

WLAN 基本概念

WLAN（Wireless Local Area Network）广义上是指是指以无线电波、激光、红外线等无线信道来代替有线局域网中的部分或全部传输媒介所构成的无线局域网。而狭义的WLAN 是指利用高频射频信号（例如 2.5GHz 或 5GHz）作为传输信道的无线局域网。

广义的 WLAN 实际上包含了多种技术标准，例如蓝牙、802.11 系列、HiperLAN2 等。随着技术的发展和演进，802.11 系列由于技术相对简单，通信可靠，具有灵活、移动、高吞吐量和快速安装等特点，成为 WLAN 的主流标准。在下文中的 WLAN 均指基于 802.11 系列标准的技术。

802.11 是 IEEE 在 1997 年为 WLAN 定义的一个无线网络通信的工业标准。此后这一标准又不断得到补充和完善，形成 802.11 的标准系列。例如比较重要的 802.11、802.11a、802.11b、802.11e、802.11g、802.11i、802.11n 等。其中基于 802.11b 标准的有时也被成为 Wi-Fi 标准。

WLAN 的优势

WLAN 的优势是显而易见的：

- 网络使用自由。凡是自由空间均可连接网络，不受限于线缆和端口位置。在办公大楼、机场候机厅、度假村、商务酒店等场所尤为适用。
- 网络建设更经济、通信更便利。终端与交换设备之间省去布线，有效降低布线成本。也适用于特殊地理环境下的网络建设，如隧道、港口码头、高速公路等。
- 工作更高效。不受限于时间和地点的接入网络，满足各行各业对于网络应用的需求。例如体育场馆、商业展馆、制造车间、物流运输等。

3.1.2 WLAN 基本架构

基于 802.11 系列标准的 WLAN 网络主要由 STA、AP、AC 等部件组成。

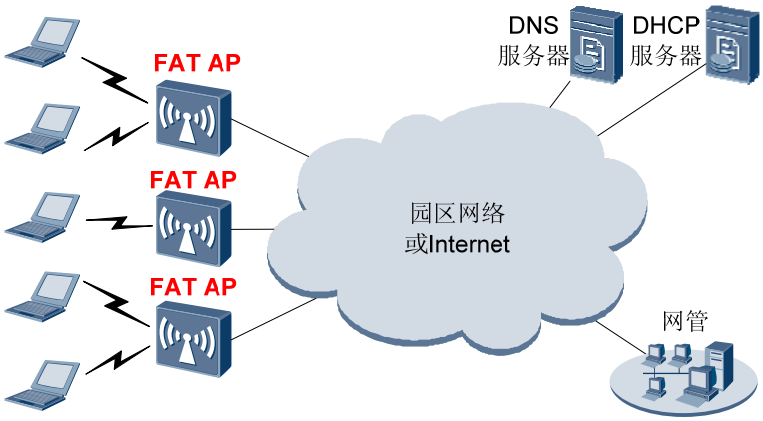
- STA（Station）：指各种接入终端，例如电脑、手机、PDA 等。
- AP（Access Point）：AP 是 WLAN 网络的主要设备，是实现无线技术的关键部件。AP 对上提供有线连接，对下提供无线接入，起到有线和无线网络的桥接作用。
- AC（Access Controller）：AC 主要完成对 AP 设备的管理。包括 AP 点管理、射频管理、用户认证、完全管理等。AC 通过 CAPWAP（Controlling and Provisioning of Wireless Access Point）协议完成管理功能。

WLAN 网络主要有自治式和集中式两种网络架构。

自治式架构

自治式架构又称为 FAT AP 架构。在该架构下，AP 实现所有无线接入功能（称为“胖 AP”），不需要 AC 设备形态。如图 3-1 所示。

图3-1 自治式架构

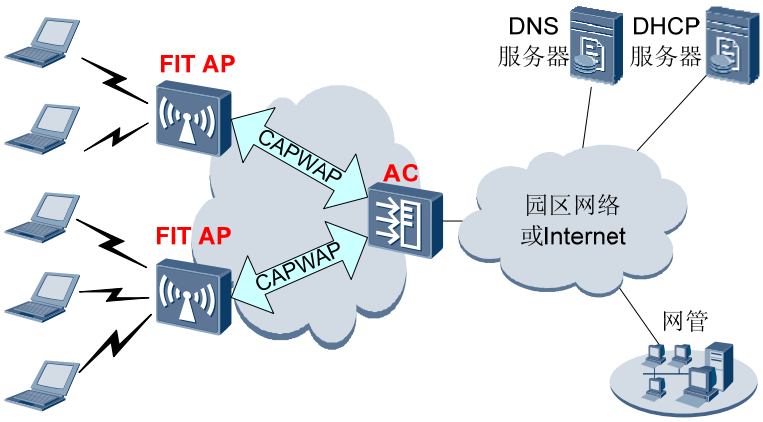


WLAN 早期广泛采用自治式架构，随着企业大量部署 AP 时，对 AP 进行配置、升级软件等管理工作将给用户带来很高的操作成本，管理成本提高，自治式架构应用逐步减少。

集中式架构

自治式架构又称为 FIT AP 架构。在该架构下，通过 AC 集中管理和控制多个 AP（称为瘦 AP），如图 3-2 所示。

图3-2 集中式架构



在集中式架构下，所有无线接入功能由 AP 和 AC 间共同完成：

- AC 完成网络具有重要意义的功能，例如移动管理、身份验证、VLAN 划分、射频资源管理、无线 IDS 和数据包转发等。
- AP 完成无线空口的控制，例如无线信号发射与探测响应、数据加密解密、数据传输确认、空口数据优先级管理等等。
- AP 和 AC 间采用 CAPWAP 协议进行通讯，AC 与 AP 间可以是直连或者穿越二层或三层网络。

集中式架构是企业网、运营商等 WLAN 方案的主要架构，便于集中管理、集中认证和集中安全管理。下文中的 WLAN 部署方案均基于集中式架构。

3.1.3 企业 WLAN 组网方案

对于企业的 WLAN 网络部署来说，可以按照企业和机构的规模大小、机构类型等因素来考虑采用不同的 WLAN 组网方案。

大中型园区网 WLAN 方案

大中型园区网定位为大中型企业总部、大型分支机构、高校、机场等场所。大型园区 WLAN 部署的 AP 数量较多，有内部需求可能也有访客上网需求。

从网络运维以及安全考虑，大中型园区网主要采用集中式架构（FIT AP 架构）来部署 WLAN。根据 AC 的部署方式，又可分为集中式 AC 方案和分布式 AC 方案。

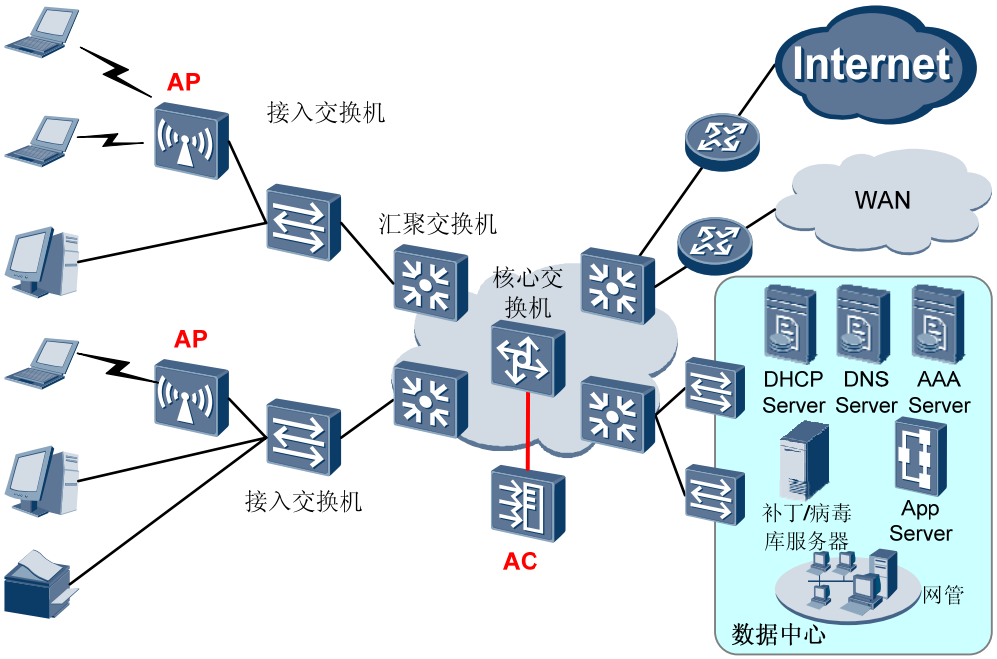
1. 集中式 AC 方案

集中式 AC 方案，是指整个网络中集中部署 AC 设备（一般是独立的 AC 设备），来控制和管理整网的 AP 设备。AC 的部署可以采用直路（直接部署在 AP 和汇聚/核心交换机之间）或旁挂方式（旁挂在汇聚/核心交换机旁侧）。

- 直路方式主要用于新建网络或原有网络汇聚/核心设备为华为设备的场景。
- 旁挂方式主要用于原有网络汇聚/核心设备非华为设备的场景。

大中型园区网的集成 AC 组网方案如图 3-3 所示。（以旁挂方式为例）

图3-3 大中型园区网集中式 AC 方案

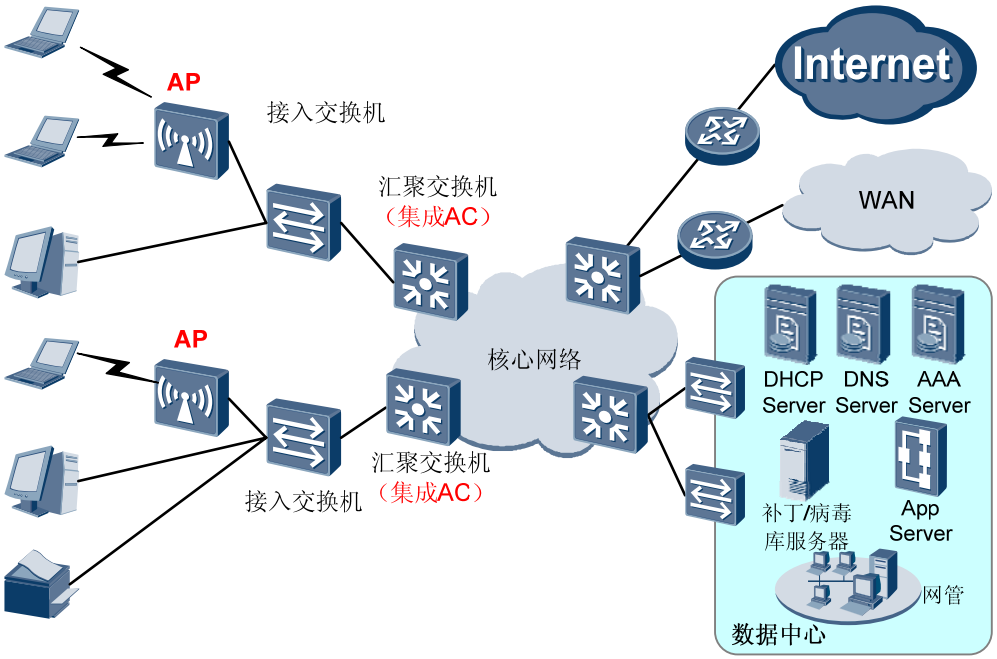


2. 分布式 AC 方案

分布式 AC 方案，是指网络中分区域采用多个 AC 设备，分别对本区域的 AP 设备进行管理。分布式 AC 方案一般不采用独立的 AC 设备，而是采用在汇聚交换机上集成 AC 功能，来实现对本交换机下挂的所有 AP 进行管理。

大中型园区网的集成 AC 组网方案如图 3-4 所示。

图3-4 大中型园区网集成 AC 方案



----结束

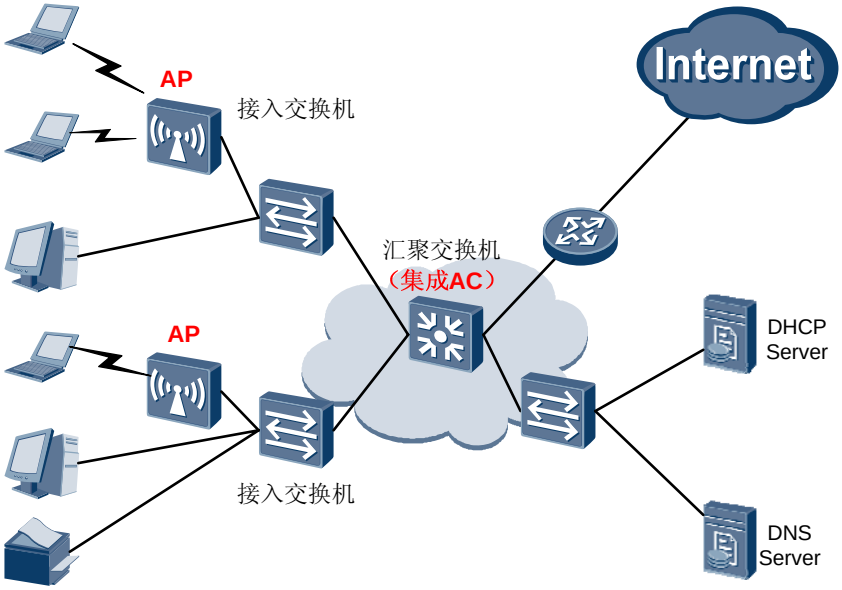
小型园区网 WLAN 方案

小型园区网定位为中小型企业包括独立的小型园区网，也包括只在分支机构部署 WLAN 的场景。小型园区网 WLAN 部署规模小于大型园区但高于 SOHO。

相对于大型 WLAN 网络而言，小型园区网 WLAN 可能较少考虑网络可靠性，可能因为成本因素而不需要专门的网管设备以及认证服务器。

小型园区网由于规模较小，一般采用集中式 AC 方案。可采用独立 AC 设备或者交换机集成 AC 的部署方式。如图 3-5 所示。（以交换机集成 AC 为例）

图3-5 小型园区网 WLAN 方案

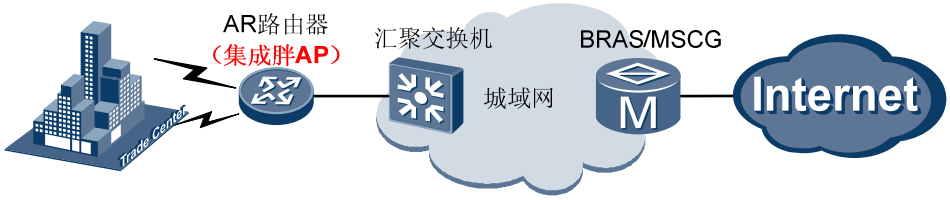


SOHO WLAN 方案

SOHO WLAN 方案主要适用于用户规模较小的独立的小型场点，如小型企业、商店、咖啡吧、SOHO 办公等，或者独立部署 WLAN 业务的企业分支机构。SOHO WLAN 网络中一般不会单独部署认证服务器以及网管设备。

SOHO 的 WLAN 方案一般可采用自治式架构（胖 AP 架构），不需要 AC 设备。此时可采用华为公司的 AR 路由器作为胖 AP（也可采用第三方的胖 AP 产品）来进行组网。如图 3-6 所示。

图3-6 SOHO WLAN 方案



注意

使用 AR 路由器作为胖 AP 实现 SOHO WLAN 的部署指导，请直接参考 AR 路由器产品的产品文档。

分支 WLAN 方案

分支 WLAN 方案定位为总部与分支均部署了 WLAN 且总部需要管理分支 WLAN 的场景（完全不需要总部管理的场景，可根据分支的大小归入前面三种场景）。

企业分支根据可能 AC 部署方式分为大小型，与分支的规模大小没有严格的对应关系。企业分支的 WLAN 方案如图 3-7 和图 3-8 所示。

图3-7 大型分支 WLAN 方案

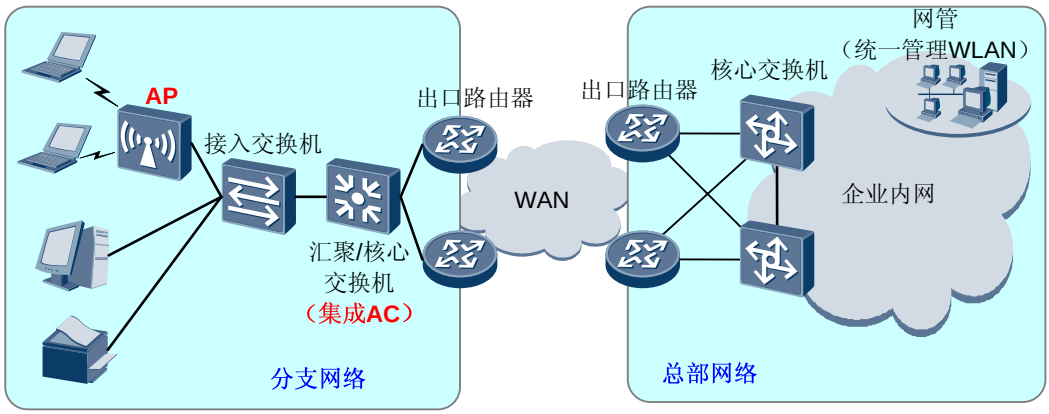
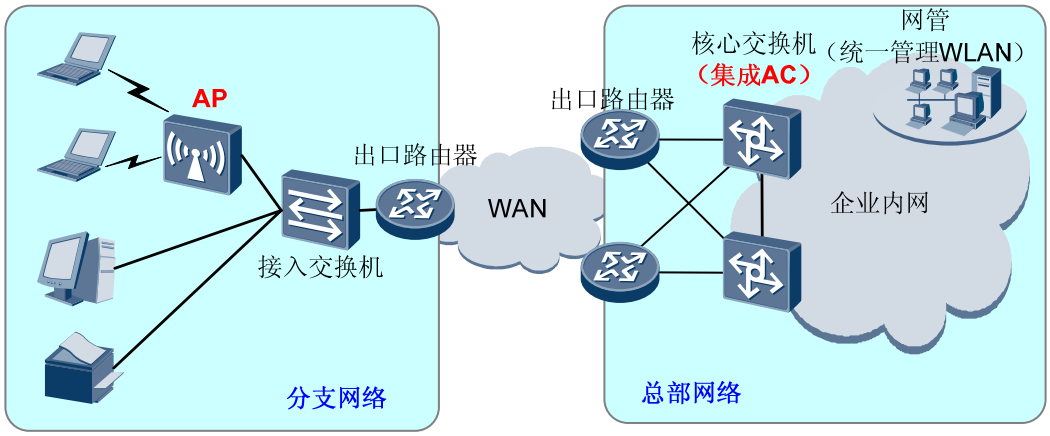


图3-8 小型分支 WLAN 方案



注意

在后续的部署指导中，以完整的大中型园区网 WLAN 方案为基础，按照 AC 的设备形态（独立 AC 和集成 AC）为维度进行描述。部署的相关指导对于各种不同类型的企业网络均可参考使用。

3.1.4 典型组网

在 WLAN 部署中，最关键的部件包括 AP 和 AC。按照 AC 的设备形态不同，有以下两种典型组网。

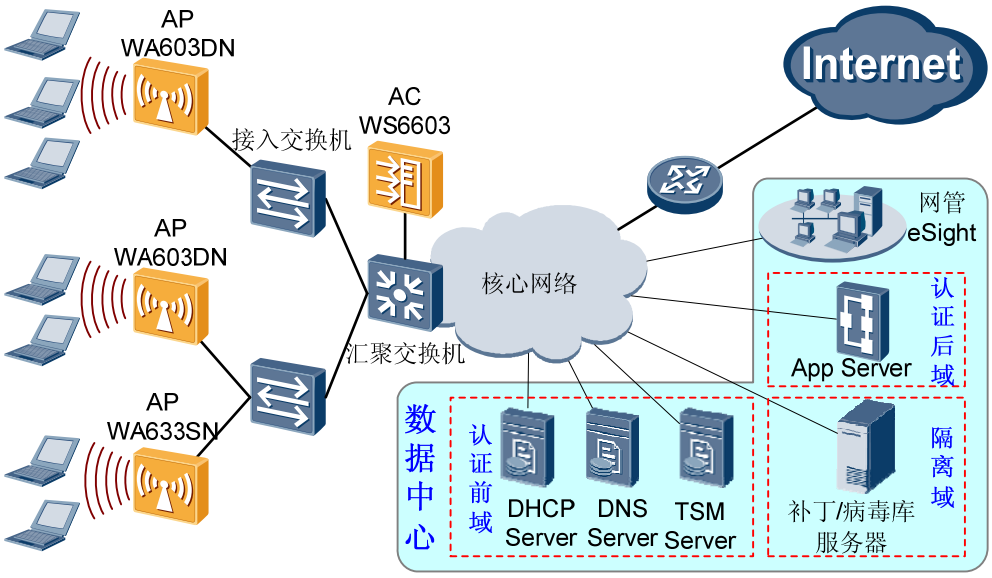
独立 AC 方案

独立 AC 方案是指采用单独的 AC 硬件设备（例如 WS6603 产品），通过直路或者旁挂方式实现对于所有 AP 的管理。

独立 AC 方案一般应用在集中式 AC 的 WLAN 部署方案中。独立 AC 的性能优异，可以实现大容量高性能的 WLAN 网络部署。但是独立 AC 相比交换机集成的 AC 价格昂贵一些。企业可以根据自身的实际情况进行选择。

企业 WLAN 独立 AC 方案的典型组网如图 3-9 所示。

图3-9 独立 AC 方案典型组网图



在独立 AC 方案中，采用集中式架构（FIT AP 架构），使用 FIT AP（例如 WA603DN）来负责无线终端的接入。使用独立的 AC 设备（WS6603）并旁挂在用户业务网关（汇聚或者核心交换机）一侧，负责完成对 AP 设备的管理。

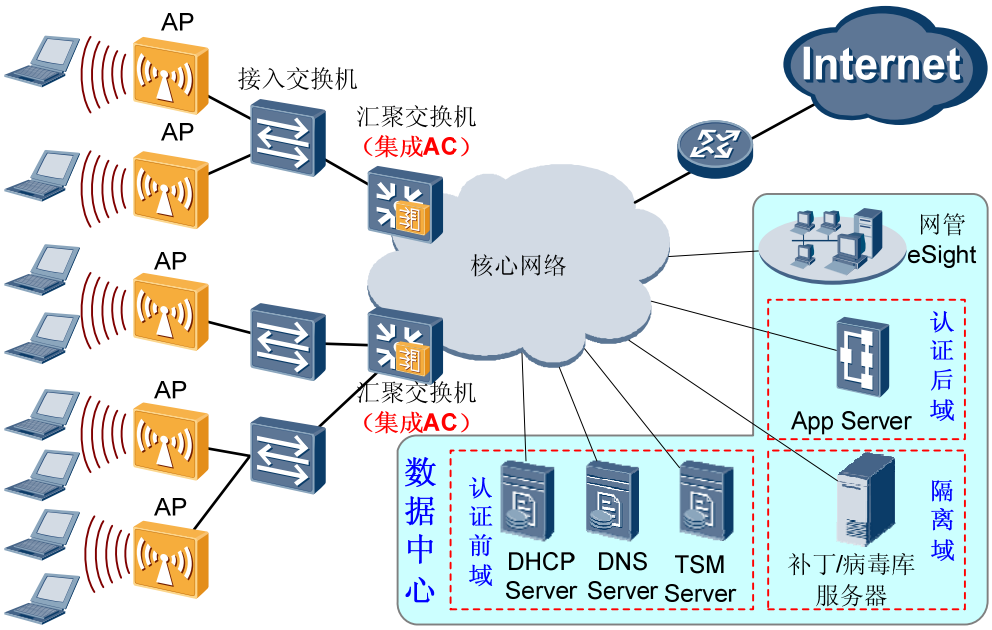
集成 AC 方案

集成 AC 方案是指不采用单独的 AC 硬件设备，而是采用在交换机中集成的 AC 硬件插卡（例如 S9300 的 SPU 板），来实现对交换机下所有 AP 的管理。

集成 AC 方案可应用在集中式 AC 部署方案中，也可应用在分布式 AC 部署方案中。集成 AC 方案部署较为简便，价格相对低廉一些，但是性能方面与独立的 AC 设备相比略差。企业可以根据自身的实际情况进行选择。

企业 WLAN 集成 AC 方案的典型组网如图 3-10 所示。

图3-10 集成 AC 方案典型组网图



在集成 AC 方案中，采用集中式架构（FIT AP 架构），使用 FIT AP（例如 WA603DN）来负责无线终端的接入。使用 S9300 集成的 SPU 板卡作为 AC，负责完成对 AP 设备的管理。

3.1.5 配套版本

表3-1 配套产品和版本

部件		产品	版本
AP		WA603SN WA603DN WA633SN WA653SN WA653DN WA653EN	V100R003C01
接入交换机		非特定，推荐 S2700/S3700 系列	非特定
汇聚交换机		S9300	V100R006C01
AC	集成 AC	S9300 SPU 插卡	V100R006C01
	独立 AC	WS6603	V100R003C05
DHCP 服务器		非特定，可以是外置服务器，或者交换机内置的 DHCP 服务器，也可以使用 AC 内置的 DHCP 服务器	非特定

部件	产品	版本
DNS 服务器	非特定	非特定

3.1.6 部署思路

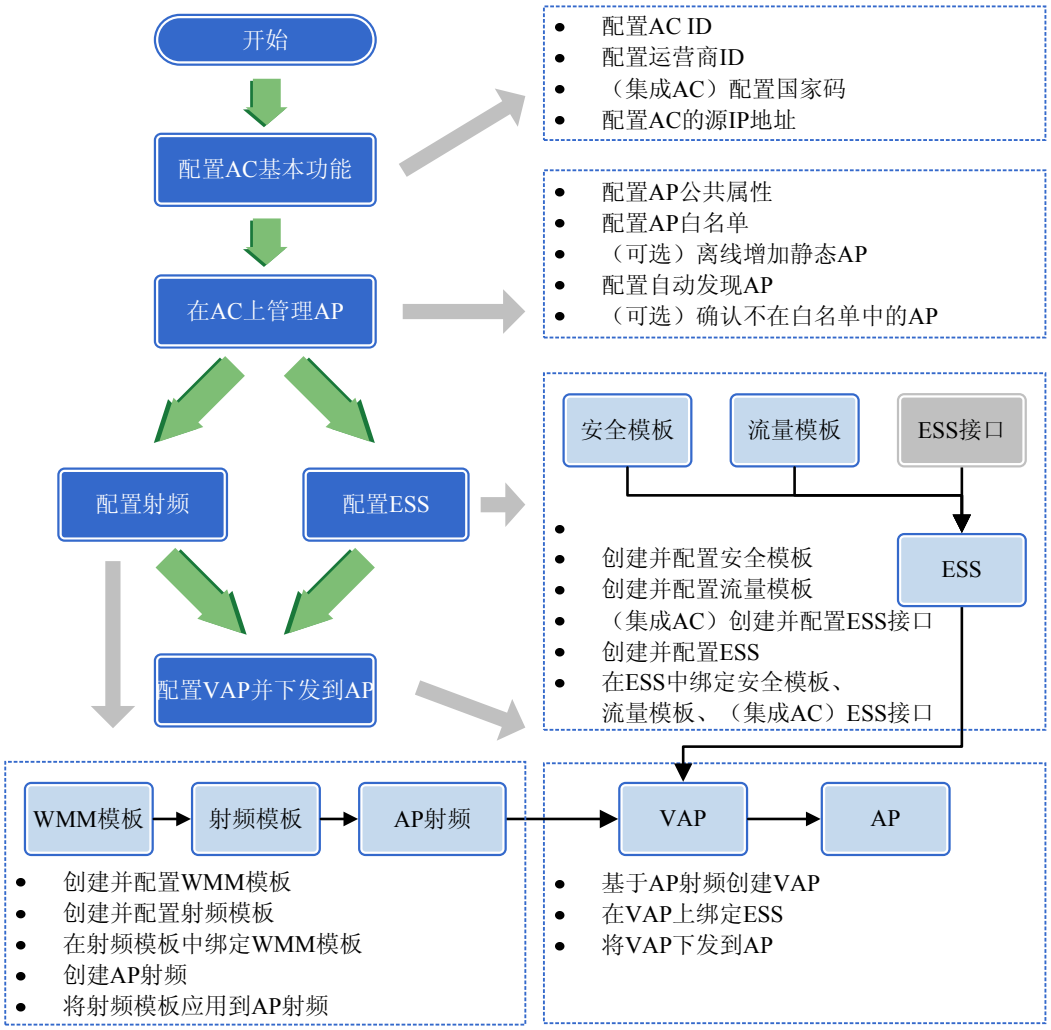
前置任务

- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- 完成 VLAN/SSID、IP 地址等数据的规划。

配置思路

配置思路	配置注意事项
在各网元部件上配置接口、VLAN、IP 地址和路由，实现网络的基础互通。	NA
配置 AP 发现 AC 的方式，包括以下两种： • AP 通过 DHCP 服务器返回的报文中的 Option 43 字段来得知 AC 的 IP 地址。 • AP 通过 DHCP 服务器返回的报文中的 Option 15 字段得知 AC 的 DNS 域名，然后向 DNS 服务器发送 DNS 解析请求来得知 AC 的 IP 地址。	• 第一种方式要求 DHCP 服务器上配置 Option 43 选项，内容为 AC 的 IP 地址。 • 第二种方式要求 DHCP 服务器上配置 Option 15 选项，内容为 AC 的 DNS 域名。同时配置 DNS 服务器，增加 AC 域名对应的 IP 地址。
配置 AC 对 AP 的管理，配置步骤如下： • 配置 AC 基本功能。 • 在 AC 上管理 AP。 • 配置 WLAN 射频。 • 配置 ESS（Extended Service-Set）。 • 配置 VAP（Virtual AP）并下发到 AP。	详细的 AC 配置流程顺序、步骤详解和相互关系可以参见图 3-11。
配置移动终端，连接到无线网络。	不同的移动终端有不同的配置方式，请根据终端实际情况进行配置。 一般推荐使用自动发现无线网络的方式接入 WLAN。

图3-11 AC 配置流程图



3.2 配置网络互通

配置网络互通主要是在网络设备上配置接口、VLAN、IP 地址、路由等，以及在服务器上配置 IP 地址等，实现终端、网络设备、服务器之间的网络层互相连通。

详细的配置过程略，请参考相应产品的产品文档。

3.3 配置 AP 发现 AC

3.3.1 概述

当 FIT AP 上线后，需要知道本 AP 所归属 AC 的 IP 地址，才能从 AC 获得相应的参数配置。AP 发现 AC 通常有三种方式：

- 广播方式

  在这种方式下，AP 通过广播的方式向网络中所有的 AC 发起 CAPWAP 隧道连接，当有 AC 响应该 AP 后，CAPWAP 隧道建立。这种方式下，AP 发现 AC 是自主行为，在 AC 上无需进行任何配置。

- 通过 DHCP Option43 发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option43 选项，将 AC 的 IP 地址告知 AP。

- 通过 DHCP Option15 和 DNS 解析发现 AC

  在这种方式下，FIT AP 上电后发起 DHCP 请求，以获取 IP 地址。DHCP 服务器返回 DHCP 响应报文，除了分配 IP 地址之外，还通过响应报文中所携带的 Option15 选项，将 AC 的 DNS 域名告知 AP。

  AP 再向 DNS 服务器发起 AC 域名的解析请求，DNS 服务器返回响应报文，告知 AC 的 IP 地址。

上述几种方式的对比如表 3-2 所示。

表3-2 AP 发现 AC 的不同方式对比

方式	部署要求	优势	劣势	适用网络
广播方式	无	对已有网络没有额外要求	仅能用于AP/AC二层组网中	小型 WLAN 网络，AP/AC 二层组网
Option43 方式	DHCP Server 启动 Option 43 属性	适用于 AP/AC 任何组网中	对网络有部署要求	大中型 WLAN 网络，AP/AC 二层或三层组网
Option15+ DNS 方式	部署 DNS Server； DHCP Server 支持 Option 15 属性	适用于 AP/AC 任何组网中	对网络有部署要求	大中型 WLAN 网络，AP/AC 二层或三层组网

3.3.2 配置 AP 通过 DHCP Option43 发现 AC

背景信息

在本方式下，DHCP 服务器在配置地址段和地址池时，同时需要配置 Option43 选项。

DHCP 服务器的部署比较灵活，可以采用外置 DHCP 服务器、交换机内置的 DHCP 服务器或者 AC 内置的 DHCP 服务器。

本节以 AC（WS6603）内置的 DHCP 服务器来举例说明配置过程，其他情况请参考相应产品的产品文档。

配置步骤

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口。
4. 执行命令 **ip address** *ip-address mask*，设置 VLANIF 的 IP 地址作为数据转发的三层接口。
5. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
6. 执行命令 **wlan ac source interface vlanif** *vlan-id*，设置 AC 的源 IP 地址。
7. 执行命令 **ip pool** *pool-name*，创建 IP 地址池。
8. 执行命令 **gateway** *ip-address mask*，配置 IP 地址池的网关。
9. 执行命令 **section** *section-id start-ip-address end-ip-address*，配置 IP 地址池中的地址段。
10. 执行命令 **option 43 string** *text*，配置 DHCP 服务的 Option 功能，通过 DHCP option43 通告 AC 的 IP 地址。

注意

- 配置 Option 43 时，请注意 option 选项参数的格式必须为“HuaweiAC-x.x.x.x”，其中“x.x.x.x”为 IP 地址。
- 如果涉及多个 IP 地址，则格式必须为“HuaweiAC-x.x.x.x,x.x.x.x”，即 IP 地址之间用逗号隔开。

----结束

3.3.3 配置 AP 通过 DHCP Option15 和 DNS 解析发现 AC

背景信息

在本方式下，DHCP 服务器在配置地址段和地址池时，同时需要配置 Option15 选项。同时需要指定 DNS 服务器，用于对 AC 的域名进行解析。

DHCP 服务器的部署比较灵活，可以采用外置 DHCP 服务器、交换机内置的 DHCP 服务器或者 AC 内置的 DHCP 服务器。

本节以 AC（WS6603）内置的 DHCP 服务器来举例说明配置过程，其他情况请参考相应产品的产品文档。

有关 DNS 服务器的部署和配置请参考相应产品的产品文档。

配置步骤

1. 执行命令 **enable**，进入特权模式。

2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **interface vlanif** *vlan-id*，创建 VLANIF 接口。
4. 执行命令 **ip address** *ip-address mask*，设置 VLANIF 的 IP 地址作为数据转发的三层接口。
5. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
6. 执行命令 **wlan ac source interface vlanif** *vlan-id*，设置 AC 的源 IP 地址。
7. 执行命令 **ip pool** *pool-name*，创建 IP 地址池。
8. 执行命令 **gateway** *ip-address mask*，配置 IP 地址池的网关。
9. 执行命令 **section** *section-id start-ip-address end-ip-address*，配置 IP 地址池中的地址段。
10. 执行命令 **dns-suffix** *suffix-content*，配置 IP 地址池的 DNS 后缀。
11. 执行命令 **dns-server** *ip-address* [**secondary** | **third**]，配置 IP 地址池的 DNS 服务器地址。

----结束

3.4 配置 AC（独立 AC 方式）

3.4.1 配置 AC 基本功能

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac-global** { **carrier id** { **cmcc** | **ctc** | **cuc** | **other** } | **ac id** *ac-id* } *，配置 AC ID，同时可以配置 AC 的运营商标识。
4. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
5. 执行命令 **wlan ac source interface** { **loopback** *loopback-num* | **vlanif** *vlanif-num* }，配置 loopback 接口或 VLANIF 接口地址为 AC 源的 IP 地址。

   每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下接入 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

----结束

3.4.2 在 AC 上管理 AP

配置 AP 公共属性

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。

5. 执行命令 **max-sta-num** *max-sta-num*，配置某 AP 类型允许接入 AC 的 AP 个数。
6. 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式。
7. 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id*，配置 AP 升级对应的升级文件。
   - 当升级模式为 ac-mode 时，需要将 AP 升级文件上载到 AC 中。
   - 当升级模式为 ftp-mode 时，执行命令 **ap-update ftp-server** *server-ip-address* [**ftp-username** *ftp-username* | **ftp-password** *ftp-password*] *，配置 FTP 服务器 IP、客户端用户名、密码。

----结束

配置 AP 黑白名单

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **ap-whitelist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }，增加合法 AP 的 MAC 或者 SN 到白名单里，可以批量增加。
5. 执行命令 **ap-blacklist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }，增加非法 AP 的 MAC 或者 SN 到黑名单里，可以批量增加。

----结束

（可选）离线配置 AP

通常情况下，当配置了 AP 的公共属性和 AP 黑白名单后，AP 上线时，AC 是自动发现 AP 的。但是也可以通过手工的方式，离线增加一个 AP。

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行 **ap-auth-mode** *auth-mode* 命令，修改 AP 的认证模式，MAC 认证或 SN 认证。
5. 执行命令 **ap id** *ap-id* [{ **type-id** *type-id* | **ap-type** *ap-type* } { **mac** *ap-mac* | **sn***ap-sn* } *]，离线增加一个 AP。
6. （可选）执行命令 **region-id** *region-id*，将增加的 AP 加入指定域。
7. （可选）执行命令 **profile-id** *profile-id*，将增加的 AP 绑定指定 AP 模板。
8. （可选）执行命令 **cpu warn-threshold** *threshold-num* 命令设置 AP 的 CPU 告警阈值。
9. （可选）执行命令 **mem warn-threshold** *threshold-num* 命令设置 AP 的内存告警阈值。

----结束

配置自动发现 AP

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. （可选）执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。
5. 执行命令 **ap-auth-mode** *auth-mode*，配置 AP 的认证方式（MAC、SN 或不检测）。

----结束

（可选）确认不在白名单中的 AP

如果 AP 未在白名单中配置，那么 AP 上线后，会处于未授权状态，此时，需要在 AC 上手工对 AP 进行确认，确认之后，AP 进入授权状态。

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **ap-confirm** { **all** | { **mac** *ap-mac* | **sn** *ap-sn* } [**id** *ap-id*] }，对 AP 进行确认。

AP 确认成功后，其 MAC 或 SN 将自动加入白名单，此 AP 自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，AP 正常工作。

----结束

3.4.3 配置 WLAN 射频

配置 WMM 模板

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }*，配置 WMM 模板。
5. 执行命令 **wmm enable**，使能 WMM 功能。
6. 执行命令 **wmm mandatory enable**，打开 WMM 控制许可开关。
7. （可选）执行命令 **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* }*，配置终端上四个 WMM 队列的 EDCA 参数。
8. （可选）执行命令 **wmm edca ap** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } }*，配置 AP 上四个 WMM 队列的 EDCA 参数。

----结束

配置射频模板并绑定 WMM 模板

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。
5. （可选）执行命令 **radio-type** { **80211a** | **80211an** | **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** }，配置射频模板的射频类型。
6. （可选）执行命令 **power-mode** { **auto** | **fixed** }，配置射频模板的功率模式。
7. （可选）执行命令 **channel-mode** { **auto** | **fixed** }，配置射频模板的信道模式。
8. 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }，为射频模板绑定 WMM 模板。只有绑定了 WMM 模板的射频模板才可以被射频绑定。

----结束

将射频模板应用到指定射频

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。
5. 执行命令 **bind radio-profile** { **id** *profile-id* | **name** *profile-name* }，为射频绑定射频模板。

----结束

（可选）配置 AP 射频资源管理

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。
5. 执行命令 **channel-mode auto**，配置指定射频模板中的信道模式为自动模式，AP 能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。
6. 执行命令 **power-mode auto**，配置指定射频模板中的功率模式为自动模式，AP 能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。
7. 执行命令 **calibrate-interval** *calibrate-interval*，配置指定射频模板中的射频参数调优周期，启动 AP 域内局部调优。

8. 手工启动全局调优：

   a. 执行命令 **quit**，返回 WLAN 视图。

   b. 执行命令 **calibrate startup region** *region-id* [**listen-uncontrol-neighbor**]，启动指定域的全局调优。

   c. 执行命令 **calibrate auto-startup region** *region-id* **time** *time* [**listen-uncontrol -neighbor**]，定时启动调优。

   ----结束

（可选）配置 AP 负载均衡

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **load-balance-group** { **name** *group-name* | **id** *group-id* }*，配置负载均衡组。
5. 执行命令 **member ap-id** *ap-id* **radio-id** *radio-id*，向负载均衡组内添加射频。
6. 配置负载均衡组的负载均衡模式：
   - 执行命令 **traffic gap** *gap-threshold*，配置负载均衡组的负载均衡模式为流量模式。
   - 执行命令 **session gap***gap-threshold*，配置负载均衡组的负载均衡模式为会话模式。缺省情况下，负载均衡组的负载均衡模式为会话模式。
7. 执行命令 **associate-threshold** *associate-threshold*，配置负载均衡组的最大关联次数。

   ----结束

3.4.4 配置 ESS

配置安全模板

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* }*，配置安全模板。
5. 配置安全策略，选择下述认证方式中的一种：
   - WEP 开放系统认证
     - 执行命令 **security-policy wep**，配置安全策略为 WEP 方式。
     - 执行命令 **wep authentication-methodopen-system** [**data-encrypt**]，配置使用 WEP 开放系统认证。
   - WEP 共享密钥认证

- 执行命令 **security-policy wep**，配置安全策略为 WEP 方式。
- 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。
- 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。
- 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。

- WPA/WPA2 认证
  - 执行命令 **security-policy wpa**，配置安全策略为 WPA 方式。
  - 执行命令{ **wpa** | **wpa2** } **authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 802.1x 认证方式和相应的加密方式。
  - 执行命令{ **wpa** | **wpa2** } **authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。
- WAPI 认证
  - 执行命令 **security-policyapi**，配置安全策略为 WAPI 方式。
  - 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。
  - 执行命令 **wapi import certificate** { **ac** | **asu** | **issuer** } **file-name** *file-name*，导入 AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件。
  - 执行命令 **wapi import private-key file-name** *file-name*，导入 AC 的私钥文件。
  - 执行命令 **wapi asuip** *ip-address*，配置 ASU 服务器的 IP 地址。

----结束

配置流量模板

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* }*，配置流量模板。
5. （可选）执行命令 **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* }，配置 AP 的上行 802.3 报文的 802.1p 优先级值。
6. （可选）执行命令 **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7*，配置下行时 802.1p 优先级值到用户优先级值的映射关系。
7. （可选）执行命令 **rate-limit** { **client** | **vap** } { **up** | **down** } *ratelimit-value*，限制单个终端或整个 VAP 内所有终端的无线侧上下行报文速率。
8. （可选）执行命令 **tunnel-priority up designate** { **tos** | **8021p** } *priority-value*，指定上行隧道优先级值。或者执行命令 **tunnel-priority up map** { **tos-tos** | **tos-8021p** | **8021p-tos** | **8021p-8021p** } *value0 value1 value2 value3 value4 value5 value6 value7*，配置上行隧道优先级的映射关系。

----结束

配置 ESS 并绑定安全模板和流量模板

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **ess name** *ess-name* [**id** *ess-id*] **ssid** *ssid* **traffic-profile** *traffic-profile-name* **security-profile** *security-profile-name* [**ssid-hide** { **enable** | **disable** } | **user-isolate** { **enable** | **disable** } | **type** { **service** | **ap-management** | **ac-management** } | **max-user-number** *user-number* | **association-timeout** *time* | **igmp-mode** { **proxy** | **snooping** | **off** }] *，配置 ESS 并绑定安全模板和流量模板。

----结束

3.4.5 配置 VAP 并下发到 AP

配置 VAP 并绑定 ESS

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **vap ap** *ap-id* **radio** *radio-id* **ess** { **id** *ess-id* | **name** *ess-name* } [**wlan** *wlan-id*]创建单个 VAP 或执行命令 **vap batch ap** { *ap-id* [**to** ap-id] } &<1-10> **radio** { *radio-id* [**to** *radio-id*] } &<1-10> **ess** { *ess-id* [**to** *ess-id*] } &<1-10>创建多个 VAP。

   说明

   也可以执行 **service-batch ap-type** { i**d** *ap-type-id* | **name** *ap-type-value* } **radio** *radio-id* **radio-profile** { **id** *profile-id* | **name** *radio-profile-name* } **ess id** { *ess-id* [**to** *ess-id*] } &<1-10>命令批量配置 VAP。

----结束

将 VAP 下发到 AP

1. 执行命令 **enable**，进入特权模式。
2. 执行命令 **config**，进入全局配置模式。
3. 执行命令 **wlan ac**，进入 WLAN-AC 模式。
4. 执行命令 **commit** { **all** | **ap** *ap-id* }，下发 VAP 到 AP。

----结束

3.5 配置 AC（集成 AC 方式）

3.5.1 配置 AC 基本功能

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan ac-global ac id** *ac-id* [**carrier id** { **cmcc** | **ctc** | **cuc** |**other** }]，配置 AC ID，同时可以配置 AC 的运营商标识。

   在实际应用中，为了便于管理，用户需要为每个 AC 配置 AC ID 和运营商标识。

   缺省情况下，AC ID 为 0，运营商标识为 **other**。
3. 执行命令 **wlan ac-global country-code** *country-code*，配置 AC 的国家码标识。
4. 执行命令 **wlan**，进入 WLAN 视图。
5. 执行命令 **wlan ac source interface** { **LoopBack** *loopback-num* | **Vlanif** *vlan-id* }，配置 AC 的源地址。

   每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下接入 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

   ----结束

3.5.2 在 AC 上管理 AP

配置 AP 公共属性

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap-license** *ap-license number*，配置允许接入 AC 的 AP 个数。
4. 执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。
5. 执行命令 **ap-update mode** { **ftp-mode** | **ac-mode** }，配置 AP 升级模式。
6. 执行命令 **ap-update update-filename** *filename* **ap-type** *type-id*，配置 AP 升级对应的升级文件。
   - 当升级模式为 ac-mode 时，需要将 AP 升级文件上载到 AC 中。
   - 当升级模式为 ftp-mode 时，执行命令 **ap-update ftp-server** *server-ip-address* [**ftp-username** *ftp-username* | **ftp-password** *ftp-password*] *，配置 FTP 服务器 IP、客户端用户名、密码。

   ----结束

配置 AP 白名单

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap-whitelist** { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }，增加合法 AP 的 MAC 或者 SN 到白名单里，可以批量增加。

----结束

（可选）离线配置 AP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap id** *ap-id* [{ **type-id** *type-id* | **ap-type** *ap-type* } { **mac** *ap-mac* | **sn***ap-sn* } *]，离线增加一个 AP。
4. （可选）执行命令 **region-id** *region-id*，将增加的 AP 加入指定域。
5. （可选）执行命令 **profile-id** *profile-id*，将增加的 AP 绑定指定 AP 模板。
6. （可选）执行命令 **ap-threshold** { **cpu-usage** | **memory-usage** } *threshold-value*，配置 AP 的 CPU 和内存的告警阈值。
7. （可选）执行命令 **ap-threshold temperature** *high-value* [*low-value*]，配置 AP 的温度告警阈值。

----结束

配置自动发现 AP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. （可选）执行命令 **ap-type** { **id** *type-id* | **type** *ap-type* }*，配置新的 AP 类型。
4. 执行命令 **ap-auth-mode** *auth-mode*，配置 AP 的认证方式（MAC、SN 或不检测）。

----结束

（可选）确认不在白名单中的 AP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap-confirm** { **all** | { **mac** *ap-mac* | **sn** *ap-sn* } [**id** *ap-id*] }，对 AP 进行确认。

   AP 确认成功后，其 MAC 或 SN 将自动加入白名单，此 AP 自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，AP 正常工作。

----结束

3.5.3 配置 WLAN 射频

配置 WMM 模板

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }*，配置 WMM 模板。
4. 执行命令 **wmm enable**，使能 WMM 功能。
5. （可选）执行命令 **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* }*，配置终端上四个 WMM 队列的 EDCA 参数。
6. （可选）执行命令 **wmm edca ap** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } }*，配置 AP 上四个 WMM 队列的 EDCA 参数。

----结束

配置射频模板并绑定 WMM 模板

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。
4. （可选）执行命令 **radio-type** { **80211a** | **80211an** | **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** }，配置射频模板的射频类型。
5. （可选）执行命令 **power-mode** { **auto** | **fixed** }，配置射频模板的功率模式。
6. （可选）执行命令 **channel-mode** { **auto** | **fixed** }，配置射频模板的信道模式。
7. 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }，为射频模板绑定 WMM 模板。只有绑定了 WMM 模板的射频模板才可以被射频绑定。

----结束

将射频模板应用到指定射频

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。
4. 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }，为指定射频绑定射频模板。

----结束

（可选）配置 AP 射频资源管理

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }*，配置射频模板。
4. 执行命令 **channel-mode auto**，配置指定射频模板中的信道模式为自动模式，AP 能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。
5. 执行命令 **power-mode auto**，配置指定射频模板中的功率模式为自动模式，AP 能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。
6. 执行命令 **calibrate-interval** *calibrate-interval*，配置指定射频模板中的射频参数调优周期，启动 AP 域内局部调优。
7. 手工启动全局调优：
   a. 执行命令 **quit**，返回 WLAN 视图。
   b. 执行命令 **calibrate startup region** *region-id* [**listen-uncontrol-neighbor**]，启动指定域的全局调优。
   c. 执行命令 **calibrate auto-startup region** *region-id* **time** *time* [**listen-uncontrol -neighbor**]，定时启动调优。

----结束

（可选）配置 AP 负载均衡

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **load-balance-group** { **name** *group-name* | **id** *group-id* }*，配置负载均衡组。
4. 执行命令 **member ap-id** *ap-id* **radio-id** *radio-id*，向负载均衡组内添加射频。
5. 配置负载均衡组的负载均衡模式：
   - 执行命令 **traffic gap** *gap-threshold*，配置负载均衡组的负载均衡模式为流量模式。
   - 执行命令 **session gap***gap-threshold*，配置负载均衡组的负载均衡模式为会话模式。缺省情况下，负载均衡组的负载均衡模式为会话模式。
6. 执行命令 **associate-threshold** *associate-threshold*，配置负载均衡组的最大关联次数。

----结束

3.5.4 配置 ESS

配置 WLAN-ESS 接口

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **interface wlan-ess** *wlan-ess-number*，创建 WLAN-ESS 接口。
3. 配置 WLAN-ESS 接口下接入用户的认证方式：
   - 执行命令 **dot1x-authentication enable**，配置认证方式为 802.1x 认证。
   - 执行命令 **mac-authentication enable**，配置认证方式为 MAC 认证。
   - 执行命令 **web-authentication enable**，配置认证方式为 Portal 认证（Web 认证）。
4. 如果采用 802.1x 认证，执行如下步骤：
   a. 执行命令 **dot1x authentication-method** { **chap** | **pap** | **eap** }，配置 802.1x 认证方法。
   b. （可选）执行命令 **dot1x guest-vlan** *vlan-id*，配置端口所在的 guest-vlan。
   c. （可选）执行命令 **dot1x restrict-vlan** *vlan-id*，配置端口所在的 restrict-vlan。
   d. （可选）执行命令 **dot1x authentication domain** *domain-name*，在接口上绑定域。
5. （可选）执行命令 **port-isolate enable**，用于使能 AC 设备上的端口隔离功能。

----结束

配置安全模板

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* }*，配置安全模板。
4. 配置安全策略：
   - WEP 开放系统认证
     - 执行命令 **security-policy wep**，配置安全策略为 WEP 方式。
     - 执行命令 **wep authentication-methodopen-system** [**data-encrypt**]，配置使用 WEP 开放系统认证。
   - WEP 共享密钥认证
     - 执行命令 **security-policy wep**，配置安全策略为 WEP 方式。
     - 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。
     - 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。
     - 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。
   - WPA/WPA2 认证
     - 执行命令 **security-policy wpa**，配置安全策略为 WPA 方式。
     - 执行命令{ **wpa** | **wpa2** } **authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 802.1x 认证方式和相应的加密方式。
     - 执行命令{ **wpa** | **wpa2** } **authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。
   - WAPI 认证

- 执行命令 **security-policyapi**，配置安全策略为 WAPI 方式。
- 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。
- 执行命令 **wapi import certificate** { **ac** | **asu** | **issuer** } **file-name** *file-name*，导入 AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件。
- 执行命令 **wapi import private-key file-name** *file-name*，导入 AC 的私钥文件。
- 执行命令 **wapi asuip** *ip-address*，配置 ASU 服务器的 IP 地址。

----结束

配置流量模板

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* }*，配置流量模板。
4. （可选）执行命令 **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* }，配置 AP 的上行 802.3 报文的 802.1p 优先级值。
5. （可选）执行命令 **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7*，配置下行时 802.1p 优先级值到用户优先级值的映射关系。
6. （可选）执行命令 **rate-limit** { **client** | **vap** } { **up** | **down** } *ratelimit-value*，限制单个终端或整个 VAP 内所有终端的无线侧上下行报文速率。
7. （可选）执行命令 **tunnel-priority up designate** { **tos** | **8021p** } *priority-value*，指定上行隧道优先级值。或者执行命令 **tunnel-priority up map** { **tos-tos** | **tos-8021p** | **8021p-tos** | **8021p-8021p** } *value0 value1 value2 value3 value4 value5 value6 value7*，配置上行隧道优先级的映射关系。

----结束

配置 ESS 并绑定 WLAN-ESS 接口、安全模板和流量模板

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* }*，创建 ESS。
4. 执行命令 **forward-mode** { **direct-forward** | **tunnel** }，配置 ESS 的数据转发模式。
5. （可选）执行命令 **type** { **ac-management** | **ap-management** | **service** }，配置 ESS 类型。
6. （可选）执行命令 **ssid** *ssid*，配置 ESS 的 SSID。
7. （可选）执行命令 **service-vlan**，配置 ESS 的 VLAN ID。
8. 执行命令 **wlan-ess** *wlan-ess-number*，在 ESS 中绑定 WLAN-ESS 接口。
9. 执行命令 **security-profile** { **name** *profile-name* | **id** *profile-id* }，在 ESS 中绑定安全模板。

10. 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* }，在 ESS 中绑定流量模板。

----结束

3.5.5 配置 VAP 并下发到 AP

配置 VAP 并绑定 ESS

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **ap** *ap-id* **radio** *radio-id*，进入射频视图。
4. 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } [**wlan** *wlan-id*]，在射频上绑定 ESS。

说明

也可以在 WLAN 视图下使用 **batch ap** { *ap-id* [**to** *ap-id*] } &<1-10> **radio** { *radio-id* [**to** *radio-id*] } &<1-10> **service-set** { *service-set-id* [**to** *service-set-id*] } &<1-10>命令批量配置 VAP。

----结束

将 VAP 下发到 AP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **wlan**，进入 WLAN 视图。
3. 执行命令 **commit** { **all** | **ap** *ap-id* }，下发 VAP 到 AP。

----结束

3.6 配置终端

对于 WLAN 接入的终端（STA），需要具备支持 802.11 系列标准的无线网络硬件模块（例如无线网卡），才能实现和 AP 的无线对接。

在 STA 上，首先要对无线网络进行配置，例如设置 WLAN 网络的 SSID、密码和加密方式等，这样 STA 才能正常接入 AP。

配置无线网络可以使用自动发现的方式进行，也可以采用手工添加的方式进行。

- 对于自动发现的方式，只要在 STA 发现 WLAN 网络后，按照相应的提示进行连接（有可能需要输入连接的密码）即可。
- 对于手工配置无线网络，首先需要联系网络管理员，获得当前 WLAN 网络中 AP 的 SSID、安全类型和加密方式等参数，然后通过手工添加的方式来进行配置。

注意

- 推荐 STA 使用自动发现的方式来连接到 WLAN 网络。
- 对于手工配置无线网络的方式，请参考 STA 的文档进行配置。

3.7 配置举例

3.7.1 独立 AC 配置举例

组网需求

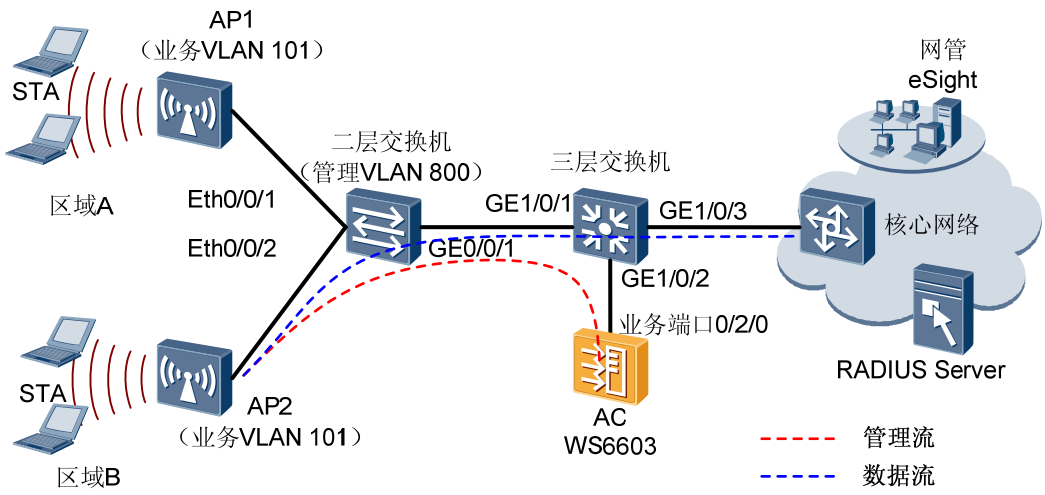
企业网络中为某两个相隔较远的区域（区域 A、区域 B）提供 WLAN 接入服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 使用 WS6603，采用“旁挂式”组网，如图 3-12 所示，由 AC 下发业务 VLAN，二层交换机透传所有的业务 VLAN，并给 AP 管理报文打管理 VLAN tag。

AC 同时作为 DHCP Server 给 AP 分配 IP 地址，且 AC 通过 DHCP Option43 向 AP 通告 AC 的 IP 地址。

AP1 和 AP2 的业务数据都是由本地直接转发，AC 只对 AP 进行管理。即 AP 管理流封装在 CAPWAP 隧道中，到达 AC 终止；AP 业务流不加 CAPWAP 封装，而直接由 AP 发送到三层交换机，再由三层交换机透传至上层设备中。

图3-12 独立 AC 旁挂组网图



数据准备

表3-3 数据规划表

配置项	数据
WLAN 服务	AP 认证类型：WEP 认证策略，Open-system 认证模式
	认证报文的加密类型：不加密
AP 管理 VLAN	VLAN 800（由二层交换机打 VLAN tag）
AP Region	AP1：101
	AP2：102
ESS	• 名称：huawei-1 • SSID：huawei-F4 • 映射模式：AP 域映射 • 映射 VLAN：101 • 数据转发模式：直接转发
	• 名称：huawei-2 • SSID：huawei-F5 • 映射模式：AP 域映射 • 映射 VLAN：102 • 数据转发模式：直接转发
上网业务 VLAN	STA1/STA2：VLAN 101（由 AC 下发）
	STA3/STA4：VLAN 102（由 AC 下发）
二层交换机上 VLAN	• 接 AP1 端口（Eth0/0/1）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 101/800 通过 • 接 AP2 端口（Eth0/0/2）：Trunk 类型，缺省 VLAN ID 为 800，允许 VLAN 102/800 通过 • 接三层交换机端口（GE0/0/1)：Trunk 类型，允许 VLAN 101/102/800 通过
三层交换机上 VLAN	• 接二层交换机端口（GE1/1/1）：Trunk 类型，允许 VLAN 101/102/800 通过 • 接 AC 端口（GE1/1/2）：Trunk 类型，允许 VLAN800 通过 • 接上行网络端口（GE1/1/3）：Trunk 类型，允许 VLAN 101/102 通过
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址(Loopback 接口)	3.3.3.3/32

配置项	数据
AP 管理 IP 地址池	192.168.1.2～192.168.1.254/24
AP 管理网关	192.168.1.1/24（三层交换机上）
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址

操作步骤

1. 配置交换机，使 AP 与 AC 互通。

   a. 配置二层交换机连接 AP 的以太网端口（Eth0/0/1 和 Eth0/0/2）类型为 Trunk 类型，缺省 VLAN 为 800，分别允许 VLAN101/800 和 VLAN102/800 通过。

   说明

   此处配置以华为 S3300 系列交换机为例，其他类型交换机请参考相应的产品文档。

   注意

   需要将所有二层交换机在 AP 管理 VLAN 和业务 VLAN 内的下行口上配置端口隔离，如果不配置端口隔离，可能会在 VLAN 内存在不必要的广播报文，或者导致不同 AP 间的 WLAN 用户二层互通的问题。

```
[huawei] vlan 101
[huawei-vlan101] quit
[huawei] vlan 102
[huawei-vlan102] quit
[huawei] vlan 800
[huawei-vlan800] quit
[huawei] interface Ethernet 0/0/1
[huawei-Ethernet0/0/1] port link-type trunk
[huawei-Ethernet0/0/1] port trunk pvid 800
[huawei-Ethernet0/0/1] port trunk allow-pass vlan 101
[huawei-Ethernet0/0/1] port trunk allow-pass vlan 800
[huawei-Ethernet0/0/1] port-isolate enable
[huawei-Ethernet0/0/1] quit
[huawei] interface Ethernet 0/0/2
[huawei-Ethernet0/0/2] port link-type trunk
[huawei-Ethernet0/0/2] port trunk pvid 800
[huawei-Ethernet0/0/2] port trunk allow-pass vlan 102
[huawei-Ethernet0/0/2] port trunk allow-pass vlan 800
[huawei-Ethernet0/0/2] port-isolate enable
[huawei-Ethernet0/0/2] quit
```

   b. 配置二层交换机连接三层交换机的 GE 端口（GE0/0/1）透传所有管理 VLAN 与业务 VLAN。

```
[huawei] interface GigabitEthernet 0/0/1
[huawei-GigabitEthernet0/0/1] port link-type trunk
[huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 101
```

```
[huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 102
[huawei-GigabitEthernet0/0/1] port trunk allow-pass vlan 800
[huawei-GigabitEthernet0/0/1] quit
```

c. 配置三层交换机连接二层交换机的 GE 端口(GE0/1/1)透传所有管理 VLAN 与业务 VLAN。

说明

此处配置以华为 S9300 系列交换机为例，其他类型交换机请参考相应的产品文档。

```
[huawei] interface GigabitEthernet 1/0/1
[huawei-GigabitEthernet1/0/1] port link-type trunk
[huawei-GigabitEthernet1/0/1] port trunk allow-pass vlan 101
[huawei-GigabitEthernet1/0/1] port trunk allow-pass vlan 102
[huawei-GigabitEthernet1/0/1] port trunk allow-pass vlan 800
[huawei-GigabitEthernet1/0/1] quit
```

d. 配置三层交换机连接 AC 的 GE 端口(GE0/1/2)透传管理 VLAN。

```
[huawei] interface GigabitEthernet 1/0/2
[huawei-GigabitEthernet1/0/2] port link-type trunk
[huawei-GigabitEthernet1/0/2] port trunk allow-pass vlan 800
[huawei-GigabitEthernet1/0/2] quit
```

e. 配置三层交换机连接上行网络的 GE 端口(GE0/1/3)透传业务 VLAN。

```
[huawei] interface GigabitEthernet 1/0/3
[huawei-GigabitEthernet1/0/3] port link-type trunk
[huawei-GigabitEthernet1/0/3] port trunk allow-pass vlan 101
[huawei-GigabitEthernet1/0/3] port trunk allow-pass vlan 102
[huawei-GigabitEthernet1/0/3] quit
```

f. 配置三层交换机的 DHCP Relay 功能。

```
[huawei] dhcp enable
[huawei] interface vlanif 800
[huawei-Vlanif800] ip address 192.168.1.1 255.255.255.0
[huawei-Vlanif800] dhcp select relay
[huawei-Vlanif800] dhcp relay server-ip 192.168.2.2
[huawei-Vlanif800] quit
```

g. VLANIF1 的 IP 地址为 192.168.2.1，作为连接 AC 的三层接口。

```
[huawei] interface vlanif 1
[huawei-Vlanif1] ip address 192.168.2.1 255.255.255.0
[huawei-Vlanif1] quit
```

h. 配置三层交换机中继 DHCP 服务到 AC 上，AC 作为 DHCP 服务器。

```
[huawei] dhcp server group AC-srv1
[huawei-dhcp-server-group-AC-srv1] dhcp-server 0 3.3.3.3
[huawei-dhcp-server-group-AC-srv1] quit
```

i. 配置三层交换机到 AC 的路由。

说明

IP 地址 3.3.3.3 为 AC 的 Loopback 接口 IP 地址。

```
[huawei] ip route 3.3.3.3 255.255.255.255 192.168.2.2
```

2. AC 基础配置。

a. 配置全局 AC 参数（运营商标识、全局 ID）方便识别和管理。

#配置 AC 运营商标识为 CTC，全局 AC ID 为 1。

```
huawei(config)# wlan ac-global carrier id ctc ac id 1
```

b. 配置 AC 连接二层交换机端口 VLAN。

#创建 VLAN 101、102 和 800。

```
huawei(config)# vlan 101
huawei(config)# vlan 102
huawei(config)# vlan 800
```

#将 VLAN 800 加入业务端口 0/2/0。

```
huawei(config)# port vlan 800 0/2 0
```

c. 在 AC 上创建 VLANIF。

#VLANIF 1 的 IP 地址为 192.168.2.2，作为连接三层交换机的三层接口。

```
huawei(config)# interface vlanif 1
huawei(config-if-vlanif1)# ip address 192.168.2.2 255.255.255.0
{ <cr>|description<K>|sub<K> }:
Command:
ip address 192.168.2.2 255.255.255.0
```

使能 VLANIF 接口的 DHCP 功能，使 AC 兼作 DHCP server，为 AP 分配 IP 地址。

```
huawei(config-if-vlanif1)# dhcps enable
huawei(config-if-vlanif1)# quit
```

说明

- AP 需要获取一个 AC 的 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。
- 此处配置 AP 从 AC 上获取 IP 地址。

d. 配置 Loopback 接口，作为 AC 的源 IP，用于 AP 和 AC 之间建立隧道通信。

说明

设置 Loopback 接口地址，必须使用 32 位掩码。

```
huawei(config)# interface loopback 0
huawei(config-if-loopback0)# ip address 3.3.3.3 255.255.255.255
huawei(config-if-loopback0)# quit
```

e. 设置 AC 的源 IP 地址。

#配置 Loopback 接口作为 AC 的源 IP 地址。

说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下挂接所有 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

```
huawei(config)# wlan ac
huawei(config-wlan-ac-view)# wlan ac source interface loopback 0
huawei(config-wlan-ac-view)# quit
```

f. 在 AC 上配置 AP 的 IP 地址池。

#IP 地址池 ctc-ap-server 对应 loopback0。

```
huawei(config)# ip pool ap-server
It's successful to create an IP address pool
huawei(config-ip-pool-ap-server)# gateway 192.168.1.1 255.255.255.0
```

```
huawei(config-ip-pool-ap-server)# section 0 192.168.1.2 192.168.1.254
huawei(config-ip-pool-ap-server)# quit
```

#配置 DHCP 服务的 Option60 和 Option43 功能，通过 DHCP option43 通告 AC 的 IP 地址。

```
huawei(config-ip-pool-ap-server)# option 60 string Huawei AP
huawei(config-ip-pool-ap-server)# option 43 string HuaweiAC-3.3.3.3
huawei(config-ip-pool-ap-server)# quit
```

说明

- 配置 option60 功能时，文字参数信息必须为“Huawei AP”。
- 配置 option43 功能时，文字参数信息格式必须为“HuaweiAC-X.X.X.X”，其中 X.X.X.X 是指 AC 的 IP 地址。

g. 配置 AC 到 192.168.1.0 网段的路由。

```
huawei(config)# ip route 192.168.1.0 255.255.255.0 192.168.2.1
```

3. 配置 AC 与 AP 的互通。

a. 配置 AP 的认证模式为“sn-auth”。

```
huawei(config)# wlan ac
huawei(config-wlan-ac-view)# ap-auth-mode sn-auth
huawei(config-wlan-ac-view)# quit
```

b. 离线添加 AP。

#查询 AP 的设备类型。

```
huawei(config-wlan-ac-view)# display ap-type all
All AP types information:
------------------------------------------------------------------------------
ID Type
------------------------------------------------------------------------------
0 WA601
1 WA631
2 WA651
3 WA602
4 WA632
5 WA652
6 WA603SN
7 WA603DN
8 WA633SN
11 WA603DE
12 WA653DE
14 WA653SN
15 SRG1201GW
------------------------------------------------------------------------------
Total number: 13
```

#根据查询到的 AP 设备类型 ID，离线添加设备类型为 WA601 的 AP1 和 AP2（typeid 为 0）。AP1 的 AP ID 为 1，SN 为 SN000001，AP2 的 AP ID 为 2，SN 为 SN000002。

```
huawei(config-wlan-ac-view)# ap id 1 type-id 0 sn SN000001
huawei(config-wlan-ac-view)# ap id 2 type-id 0 sn SN000002
```

#将 AP 上线，AP 将直接进入“normal”状态。

```
huawei(config-wlan-ac-view)# display ap all
All AP information:
------------------------------------------------------------------------------
AP AP Profile Region AP
ID Type ID ID State
------------------------------------------------------------------------------
1 WA601 0 0 normal
2 WA601 0 0 normal
------------------------------------------------------------------------------
Total number: 2
```

c. 配置 AP 域。

#AP 域 ID 分别为 101 和 102。

```
huawei(config-wlan-ac-view)# ap-region id 101
huawei(config-wlan-ap-region-101)# quit
huawei(config-wlan-ac-view)# ap-region id 102
huawei(config-wlan-ap-region-102)# quit
```

d. 配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
huawei(config-wlan-ac-view)# ap id 1
{ <cr>|ap-type<K>|type-id<K> }:
Command:
ap id 1
huawei(config-wlan-ap-1)# region-id 101
huawei(config-wlan-ap-1)# quit
huawei(config-wlan-ac-view)# ap id 2
{ <cr>|ap-type<K>|type-id<K> }:
Command:
ap id 2
huawei(config-wlan-ap-2)# region-id 102
huawei(config-wlan-ap-2)# quit
```

4. 配置 AP 对应的射频。

a. 创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
huawei(config-wlan-ac-view)# wmm-profile name wmm-1 id 1
huawei(config-wlan-wmm-prof-wmm-profile-1)# quit
```

b. 创建名为“radio-1”的 Radio 模板，绑定 WMM 模板“wmm-1”。

```
huawei(config-wlan-ac-view)# radio-profile name radio-1 id 1
huawei(config-wlan-radio-prof-radio-1)# bind wmm-profile name wmm-1
huawei(config-wlan-radio-prof-radio-1)# quit
```

c. 将 AP1 和 AP2 对应的射频绑定 Radio 模板“radio-1”。

```
huawei(config-wlan-ac-view)# radio ap-id 1 radio-id 0
huawei(config-wlan-radio-1/0)# bind radio-profile name radio-1
huawei(config-wlan-radio-1/0)# quit
huawei(config-wlan-ac-view)# radio ap-id 2 radio-id 0
huawei(config-wlan-radio-2/0)# bind radio-profile name radio-1
huawei(config-wlan-radio-2/0)# quit
```

说明

可以为一个 AP 指定不同的射频，也可以为多个 AP 指定同一个射频。

5. 配置 AP 对应的 ESS。

a. 创建 Security 模板。

#Security 模板名为“security-1”，认证模式为 WEP 认证，开放认证，不加密。

```
huawei(config-wlan-ac-view)# security-profile name security-1 id 1
huawei(config-wlan-security-prof-security-1)# authentication policy wep
huawei(config-wlan-security-prof-security-1)# policy wep open-system
huawei(config-wlan-security-prof-security-1)# quit
```

b. 创建 Traffic 模板（即 QoS 模板）。

#Traffic 模板名为“traffic-1”，参数采用默认配置。

```
huawei(config-wlan-ac-view)# traffic-profile name traffic-1 id 1
huawei(config-wlan-traffic-prof-traffic-1)# quit
```

c. 分别创建与 AP1 及 AP2 对应的 ESS，并绑定 Traffic 模板及 Security 模板。

#ESS 名为“huawei-1”，SSID 为“huawei-F4”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)# ess name huawei-1 ssid huawei-F4 traffic-profile traffic-1
security-profile security-1
```

#ESS 名为“huawei-2”，SSID 为“huawei-F5”，绑定 Traffic 模板“traffic-1”，Security 模板“security-1”。

```
huawei(config-wlan-ac-view)# ess name huawei-2 ssid huawei-F5 traffic-profile traffic-1
security-profile security-1
```

说明

ESS 是一个业务参数集合，是 VAP 的属性集合。当 ESS 被绑定到指定 AP 设备的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP 对象上，AP 设备将会以这些业务参数向用户提供差异化的无线功能。

d. 分别配置 AP1 及 AP2 与 ESS 的 VLAN 映射方式。

#ESS 的 VLAN 映射关系为根据 Ap-Region 映射。配置 Ap-Region 101 映射 VLAN 101。

```
huawei(config-wlan-ac-view)# vlan-mapping ess name huawei-1 mode region
huawei(config-wlan-ac-view)# vlan-mapping ess name huawei-1 type tag region 101 vlan101
Success: 1
Failure: 0
huawei(config-wlan-ac-view)# vlan-mapping ess name huawei-2 mode region
huawei(config-wlan-ac-view)# vlan-mapping ess name huawei-2 type tag region 102 vlan102
Success: 1
Failure: 0
```

6. 配置数据转发模式。

#配置数据转发模式为根据 ESS 转发。

```
huawei(config-wlan-ac-view)# forward-mode type ess
```

#配置名为“huawei-1”和“huawei-2”的 ESS 采用数据直接转发模式。

```
huawei(config-wlan-ac-view)# forward-mode ess 0 mode direct-forward
huawei(config-wlan-ac-view)# forward-mode ess 1 mode direct-forward
```

7. 配置 AP 对应的 VAP，下发 WLAN 服务。

a. 分别创建 AP1 及 AP2 对应的 VAP（即 WLAN 服务），并指定射频和 ESS。

```
huawei(config-wlan-ac-view)# vap ap 1 radio 0 ess name huawei-1 wlan 1
huawei(config-wlan-ac-view)# vap ap 2 radio 0 ess name huawei-2 wlan 1
```

说明

- VAP 可以理解为 AP 设备、射频和服务集（ESS）模板三者的绑定关系。当用户将服务集模板绑定到 AP 设备的射频上时，系统即生成一个 VAP。
- VAP 相当于服务集模板在 AP 设备的射频上的实例化，它具备服务集模板的所有属性，同时使用 AP 设备的射频硬件。

b. 下发 AP 的 WLAN 服务。

```
huawei(config-wlan-ac-view)# commit ap 1
huawei(config-wlan-ac-view)# commit ap 2
huawei(config-wlan-ac-view)# quit
```

----结束

配置文件

AC 上的配置文件：

```
#
wlan ac-global carrier id ctc ac id 1
vlan 101
vlan 102
vlan 800
port vlan 800 0/2 0
interface vlanif 1
ip address 192.168.2.2 255.255.255.0
dhcps enable
quit
nterface loopback 0
ip address 3.3.3.3 255.255.255.255
quit
wlan ac
wlan ac source interface loopback 0
quit
ip pool ap-server
gateway 192.168.1.1 255.255.255.0
section 0 192.168.1.2 192.168.1.254
quit
option 60 string Huawei AP
option 43 string HuaweiAC-3.3.3.3
quit
ip route 192.168.1.0 255.255.255.0 192.168.2.1
wlan ac
ap-auth-mode sn-auth
quit
ap id 1 type-id 0 sn SN000001
ap id 2 type-id 0 sn SN000002
ap-region id 101
quit
ap-region id 102
quit
ap id 1
```

```
region-id 101
quit
ap id 2
region-id 102
quit
wmm-profile name wmm-1 id 1
quit
radio-profile name radio-1 id 1
bind wmm-profile name wmm-1
quit
radio ap-id 1 radio-id 0
bind radio-profile name radio-1
quit
radio ap-id 2 radio-id 0
bind radio-profile name radio-1
quit
security-profile name security-1 id 1
authentication policy wep
policy wep open-system
quit
traffic-profile name traffic-1 id 1
quit
ess name huawei-1 ssid huawei-F4 traffic-profile traffic-1 security-profile security-1
ess name huawei-2 ssid huawei-F5 traffic-profile traffic-1 security-profile security-1
vlan-mapping ess name huawei-1 mode region
vlan-mapping ess name huawei-1 type tag region 101 vlan 101
vlan-mapping ess name huawei-2 mode region
vlan-mapping ess name huawei-2 type tag region 102 vlan 102
forward-mode type ess
forward-mode ess 0 mode direct-forward
forward-mode ess 1 mode direct-forward
vap ap 1 radio 0 ess name huawei-1 wlan 1
vap ap 2 radio 0 ess name huawei-2 wlan 1
commit ap 1
commit ap 2
quit
```

3.7.2 集成 AC 配置举例

组网需求

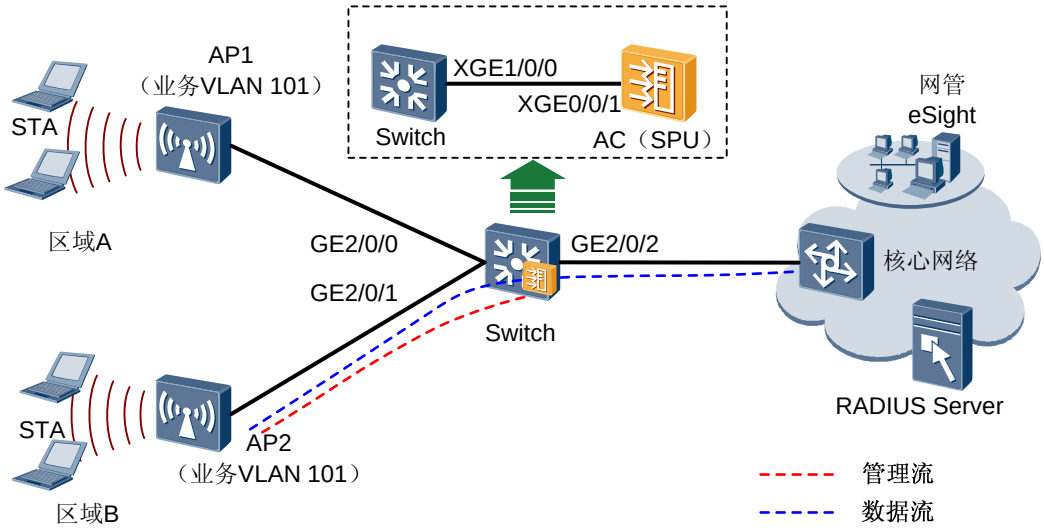
企业网络中为某两个相隔较远的区域（区域 A、区域 B）提供 WLAN 接入服务，AP1 为区域 A 提供 WLAN 业务，AP2 为区域 B 提供 WLAN 业务。

AC 使用 S9300 集成的 SPU 板，插在 S9300 的 1 槽位，如图 3-13 所示，由 AC 分配下发业务 VLAN，S9300 透传所有的业务 VLAN，并给 AP 管理报文打管理 VLAN tag。

AC 同时作为 DHCP Server 给 AP 分配 IP 地址，且 AC 通过 DHCP Option43 向 AP 通告 AC 的 IP 地址。

AP1 和 AP2 的业务数据都是由本地直接转发，AC 只对 AP 进行管理。即 AP 管理流封装在 CAPWAP 隧道中，到达 AC 终止；AP 业务流不加 CAPWAP 封装，而直接由 AP 发送到三层交换机，再由三层交换机透传至上层设备中。

图3-13 集成 AC 组网图



数据准备

表3-4 数据规划表

配置项	数据
WLAN 服务	WEP，Open-system 认证模式，不加密
AP 管理 VLAN	VLAN 100（Switch 分配）
AP Region	AP1：101
	AP2：102
ESS	• 名称：huawei-1 • SSID：huawei-1 • WLAN 虚接口：WLAN-ESS 0 • 数据转发模式：隧道转发
	• 名称：huawei-2 • SSID：huawei-2 • WLAN 虚接口：WLAN-ESS 1 • 数据转发模式：隧道转发
WLAN 用户 VLAN	AP1：VLAN 101 AP2：VLAN 102
交换机 VLAN	VLAN 100/101/102
AC Carrier ID/AC ID	CTC/1
AC 管理 IP 地址	Vlanif 接口：192.168.0.1/24

配置项	数据
AP 管理 IP 地址池	192.168.0.2～192.168.0.254/24
AP 网关	192.168.1.1/24（AC）
DHCP 服务器	AC 作为 DHCP 服务器，给 AP 分配 IP 地址

配置思路

1. 配置 Switch 和 AC，实现 AP 和 AC 互通。
2. 配置 AC 的基本功能，包括配置 AC 运营商标识和 ID、AC 与 AP 之间通信的源接口，实现 AC 作为 DHCP Server 功能。
3. 配置 AP 上线的认证方式，并把 AP 加入 AP 域中，实现 AP 正常工作。
4. 配置 VAP，下发 WLAN 业务，实现 STA 访问 WLAN 网络功能。

   其中配置 VAP，需要：

   a. 配置 WLAN-ESS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AC 后能够送至 WLAN 业务处理模块功能。
   b. 配置 AP 对应的射频模板，并在射频下绑定该模板，实现 STA 与 AP 之间的无线通信参数配置。
   c. 配置 AP 对应的服务集，并在服务集下配置数据直接转发模式，绑定安全模板、流量模板，实现 STA 接入网络安全策略及 QoS 控制。
   d. 配置 VAP 并下发，实现 STA 访问 WLAN 网络功能。

   ----结束

操作步骤

1. 配置 Switch 和 AC，使 AP 和 AC 互通。

   #配置 Switch 连接 AP 的以太网端口（GE2/0/0 和 GE2/0/1）类型为 trunk 类型，PVID 为 100。

```
<Quidway> system-view
[Quidway] vlan batch 100 to 102
[Quidway] interface GigabitEthernet 2/0/0
[Quidway-GigabitEthernet2/0/0] port link-type trunk
[Quidway-GigabitEthernet2/0/0] port trunk pvid vlan 100
[Quidway-GigabitEthernet2/0/0] port trunk allow-pass vlan 100 101
[Quidway-GigabitEthernet2/0/0] quit
[Quidway] interface GigabitEthernet 2/0/1
[Quidway-GigabitEthernet2/0/1] port link-type trunk
[Quidway-GigabitEthernet2/0/1] port trunk pvid vlan 100
[Quidway-GigabitEthernet2/0/1] port trunk allow-pass vlan 100 102
[Quidway-GigabitEthernet2/0/1] quit
```

   #配置 Switch 上连接 AC 的 XGE 接口透传所有业务和管理 VLAN。

```
[Quidway] interface XGigabitEthernet 1/0/0
[Quidway-XGigabitEthernet1/0/0] port link-type trunk
[Quidway-XGigabitEthernet1/0/0] port trunk allow-pass vlan 100 to 102
```

#配置 AC 上连接 Switch 的 XGE 接口透传所有业务和管理 VLAN。

```
<Quidway> system-view
[Quidway] sysname AC
[AC] vlan batch 100 to 102
[AC] interface XGigabitEthernet 0/0/1
[AC-XGigabitEthernet0/0/1] port link-type trunk
[AC-XGigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
[AC-XGigabitEthernet0/0/1] quit
```

2. 配置 AC 的基本功能。

#配置 AC 全局参数（运营商标识、ID、国家码）方便识别和管理。

```
[AC] wlan ac-global ac id 1 carrier id  ctc
[AC] wlan ac-global country-code cn
```

#创建 VLANIF 接口，配置其 IP 地址作为数据转发的三层接口，使能 DHCP 服务功能。

Vlanif 100 为 AP 分配 IP 地址，Vlanif 101 为区域 A 的 STA 分配 IP 地址，Vlanif 102 为区域 B 的 STA 分配 IP 地址。

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 192.168.0.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
[AC] interface vlanif 101
[AC-Vlanif101] ip address 192.168.1.1 24
[AC-Vlanif101] dhcp select interface
[AC-Vlanif101] quit
[AC] interface vlanif 102
[AC-Vlanif102] ip address 192.168.2.1 24
[AC-Vlanif102] dhcp select interface
[AC-Vlanif102] quit
```

说明

AP 需要获取一个 IP 地址才能与 AC 建立连接，可以从 AC、BRAS 或 DHCP 服务器获取 IP 地址。此处配置 AC 为 DHCP 服务器，AP 从 AC 上获取 IP 地址。

#配置 AC 的源接口，用于 AP 和 AC 之间建立隧道通信。

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
[AC-wlan-view] quit
```

说明

每台 AC 设备都需要指定 AC 的源 IP 地址，使得该 AC 设备下接入 AP 学到的 AC 地址都是指定的 AC 源 IP 地址。

3. 配置 AP 并上线。

#配置 AP 的认证方式为“no-auth”。

```
[AC-wlan-view] ap-auth-mode no-auth
```


说明

如果 AP 认证模式为“no-auth”，上线 AP 将自动按照类型匹配自动上线，并自动加入到默认域中，绑定默认的 AP 模板，各项属性置为默认配置，进入“normal”状态。

#配置 AP 域 ID 分别为 101 和 102。

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
```

#配置 AP1 加入 AP 域 101，AP2 加入 AP 域 102。

```
[AC-wlan-view] ap id 0
[AC-wlan-ap-0] region-id 101
[AC-wlan-ap-0] quit
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 102
[AC-wlan-ap-1] quit
```

4. 配置 WLAN-ESS 虚接口。

```
[AC] interface wlan-ess 0
[AC-WLAN-ESS0] port link-type hybrid
[AC-WLAN-ESS0] port hybrid untagged vlan 101
[AC-WLAN-ESS0] quit
[AC] interface wlan-ess 1
[AC-WLAN-ESS1] port link-type hybrid
[AC-WLAN-ESS1] port hybrid untagged vlan 102
[AC-WLAN-ESS1] quit
```

5. 配置 AP 对应的射频。

#创建名为“wmm-1”的 WMM 模板，参数采用默认配置。

```
[AC] wlan
[AC-wlan-view] wmm-profile name wmm-1 id 1
[AC-wlan-wmm-prof-wmm-1] quit
```

#创建名为“radio-1”的射频模板，绑定 WMM 模板“wmm-1”。

```
[AC-wlan-view] radio-profile name radio-1
[AC-wlan-radio-prof-radio-1] wmm-profile name wmm-1
[AC-wlan-radio-prof-radio-1] quit
```

#将 AP1 和 AP2 对应的射频绑定射频模板“radio-1”。

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] radio-profile name radio-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] radio-profile name radio-1
[AC-wlan-radio-1/0] quit
```

6. 配置 AP 对应的服务集。

#创建安全模板。

安全模板名为“security-1”，认证模式为 WEP 认证，开放认证，不加密。

```
[AC-wlan-view] security-profile name security-1 id 1
[AC-wlan-sec-prof-security-1] wep authentication-method open-system
[AC-wlan-sec-prof-security-1] security-policy wep
[AC-wlan-sec-prof-security-1] quit
```

#配置 QoS 策略，创建流量模板。

流量模板名为“traffic-1”，参数采用缺省配置。

```
[AC-wlan-view] traffic-profile name traffic-1
[AC-wlan-traffic-prof-traffic-1] quit
```

#分别创建与 AP1 及 AP2 对应的服务集，并绑定流量模板及安全模板、WLAN-ESS 接口。

```
[AC-wlan-view] service-set name huawei-1
[AC-wlan-service-set-huawei-1] ssid huawei-1
[AC-wlan-service-set-huawei-1] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-1] wlan-ess 0
[AC-wlan-service-set-huawei-1] service-vlan 101
[AC-wlan-service-set-huawei-1] forward-mode tunnel
[AC-wlan-service-set-huawei-1] quit
[AC-wlan-view] service-set name huawei-2
[AC-wlan-service-set-huawei-2] ssid huawei-2
[AC-wlan-service-set-huawei-2] traffic-profile name traffic-1
[AC-wlan-service-set-huawei-2] wlan-ess 1
[AC-wlan-service-set-huawei-2] service-vlan 102
[AC-wlan-service-set-huawei-2] forward-mode tunnel
[AC-wlan-service-set-huawei-2] quit
```

配置 AP 对应的 VAP，下发 WLAN 服务。

#将 AP1 和 AP2 对应的射频绑定服务集“Huawei-1”和“Huawei-2”。

```
[AC-wlan-view] ap 0 radio 0
[AC-wlan-radio-0/0] service-set name huawei-1
[AC-wlan-radio-0/0] quit
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] service-set name huawei-2
[AC-wlan-radio-1/0] quit
```

#下发 AP 的 WLAN 服务。

```
[AC-wlan-view] commit ap 0
[AC-wlan-view] commit ap 1
```

7. 验证配置结果。

   AP1 和 AP2 下的无线接入用户可以搜索到 SSID 标识为 huawei-1 和 huawei-2 的 WLAN 网络，无需验证即可以正常使用 WLAN 上网服务。

----结束

配置文件

- AC 上的配置文件

```
#
```



```
 sysname AC
#
 vlan batch 100 to 102
#
 dhcp enable
#
 wlan ac-global carrier id ctc ac id 1
#
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select interface
#
interface WLAN-ESS0
 port hybrid untagged vlan 101
#
interface WLAN-ESS1
 port hybrid untagged vlan 102
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 undo port trunk allow-pass vlan 1
 port trunk allow-pass vlan 100 to 102
#
wlan
 wlan ac source interface Vlanif100
 ap-region id 101
 ap-region id 102
 ap-auth-mode no-auth
 ap id 0
 ap id 1
 wmm-profile name wmm-1 id 1
 traffic-profile name traffic-1 id 1
 security-profile name security-1 id 2
 service-set name huawei-1 id 3
  wlan-ess 0
  ssid huawei-1
  traffic-profile id 1
  service-vlan 101
  forward-mode tunnel
 service-set name huawei-2 id 4
  wlan-ess 1
  ssid huawei-2
  traffic-profile id 2
  service-vlan 102
  forward-mode tunnel
 radio-profile name radio-1 id 1
  wmm-profile id 1
```

```
 ap 0 radio 0
  radio-profile name radio-1
  service-set name huawei-1 wlan 1
 ap 1 radio 0
  radio-profile name radio-1
  service-set name huawei-2 wlan 2
#
return
```

- Switch 的配置文件

```
#
interface GigabitEthernet2/0/0
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 to 101
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk pvid vlan 100
 port trunk allow-pass vlan 100 102
#
interface GigabitEthernet1/0/0
 port link-type trunk
 port trunk allow-pass vlan 100 to 102
#
```

4 分支和远程接入部署

4.1 概述

4.1.1 分支和远程接入简介

分支和远程接入主要是考虑来自园区外部的各种角色的访问，主要包括：

- 企业分支机构接入
- 合作伙伴企业接入
- 出差员工远程接入
- 外部 Internet 客户访问

分支接入

分支接入是指对于企业的分支机构（例如外研所、办事处等），通过专网或公网方式，接入到企业的总部园区，实现分支与总部的互通。

分支接入主要有专网方式、MPLS VPN 方式、公网方式。

- 专网方式

  专网方式是指通过企业自建的广域专网，实现多分支之间的互联。这种方式一般只适用于拥有自建骨干网的大型或特大型企业。

  专网方式广义上也包括租用运营商的专线（例如 FR 专线）来实现分支和总部之间的互联的方式，这种方式下，在企业范围内的部署与自建专网是相同的。

- MPLS VPN 方式

  MPLS VPN 方式通过租用运营商的 MPLS VPN 业务（L3VPN 或者 L2VPN），实现多分支之间的互联。这种方式经济高效，比较适合有一定数量分支机构，但是没有自建广域网的企业。

- 公网方式

  公网方式是指不租用运营商的 VPN 业务，而是直接使用公共网络来实现分支和总部之间的互联互通。公网方式比较适合于只有少量小型分支机构或者 SOHO 员工的企业。

公网方式是通过不安全的公共网络接入的，因此关键是要保证数据的安全性。公网方式是依靠在分支和总部园区网关之间构建点对点 VPN，通过隧道方式来保证数据的安全可靠传输。

对于分支来说，公网方式所使用的 VPN 技术是 GRE over IPSec。GRE 是常用的隧道封装协议，可以很好的实现对于远程访问的数据承载，但是 GRE 只有简单的密码验证，没有加密功能。而 IPSec 隧道加密功能很强，但是不能承载路由协议，对于 VPN 的扩展性有较大影响。通过 GRE 和 IPSec 的结合，可以很好的实现对于远程访问的数据流的承载和安全保护。

合作伙伴接入

在某些企业中，可能需要开放部分的资源，供合作伙伴进行访问，以便完成和合作伙伴之间的协同开发。这部分资源所处的区域，一般称为 Extranet 区。

合作伙伴接入企业总部，与分支接入企业总部的方式较为类似（使用最多的是通过公网的 GRE over IPSec 隧道来进行接入），但是要控制其接入总部园区后的访问权限，一般可通过 ACL 来实现。

出差员工远程接入

远程接入是指出差员工或者合作伙伴在非固定办公地点，例如酒店、机场等场所，通过公网（例如 Internet）接入园区网，并访问园区网中的内部资源。

由于远程接入是通过不安全的公共网络接入的，因此关键是要保证远程访问的安全性。远程接入是依靠在用户终端和园区网网关之间构建点对点 VPN，通过隧道方式来保证数据的安全可靠传输。

远程接入所使用的 VPN 技术主要有如下几种。

- L2TP over IPSec

  L2TP 也是常用的隧道封装协议，并且具有很好的用户认证功能，但是 L2TP 也没有加密功能。因此，也可以通过 L2TP 和 IPSec 的结合，实现对于远程访问数据流的承载和安全保护。

- SSL VPN

  SSL VPN 是以 HTTPS（Secure HTTP）为基础的 VPN 技术，工作在传输层和应用层之间。SSL VPN 充分利用了 SSL 协议提供的基于证书的身份认证、数据加密和消息完整性验证机制，可以为应用层之间的通信建立安全连接。

  SSL VPN 广泛应用于基于 Web 的远程安全接入，为用户远程访问公司内部网络提供了安全保证。

外部 Internet 客户访问

某些企业会对外部用户提供一系列的服务，例如 Web、Email、FTP 等等。为外部客户提供服务时，企业通常都会把对外的服务器放置在一个特定区域，这个区域也被称为 DMZ 区。外部用户只能访问 DMZ 区中的资源。

外部用户访问 DMZ 区，不需要特殊的配置，通过普通的公网访问即可。而在企业的出口网关处，需要部署防火墙，对外部用户的访问进行限制，限制其只能访问 DMZ 区的资源，并对外部可能的攻击和入侵进行防范。

4.1.2 部署思路

前置任务

- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- 完成园区基础互联的配置和部署，参见“2 园区基础网络部署”。

配置思路

请参见以下各具体场景中的详细描述。

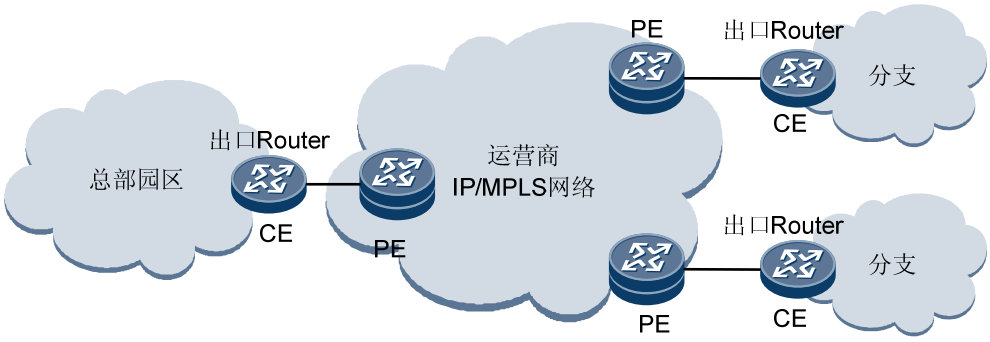
4.2 部署分支通过 WAN 专网接入

分支如果通过企业自建的 WAN 专网接入，则此时在总部和分支的出口路由器上配置各自相关的广域网接口（例如 POS 接口等），并配置 IGP 和 BGP 协议，通过广域网实现互通，即可实现分支到总部园区的接入。相关配置本节不作详细描述。

4.3 部署分支通过运营商 L3VPN 接入

分支如果通过运营商提供的 MPLS L3VPN 服务来接入总部园区，此时总部和各分支都相当于 L3VPN 中的一个 Site，总部和各分支的出口路由器作为 L3VPN 的 CE 设备，连接到运营商的 PE 设备，通过运营商的 MPLS 网络实现互通。

图4-1 分支通过运营商 L3VPN 接入



分支通过运营商 L3VPN 接入时，运营商网络中的 P 和 PE 等设备由运营商负责进行部署，本处不作介绍。

在企业的出口路由器（CE）上需要进行如下部署：

- 配置 CE 与 PE 相连的接口和 IP 地址
- 配置 CE 的 IGP，引入本站点的所有路由
- 配置 CE 和 PE 间的路由交互

4.3.1 配置 CE 与 PE 相连的接口和 IP 地址

具体配置过程略，CE 与 PE 相连的接口的 IP 地址，需要和 PE 上对应接口的 IP 地址处于同一网段。该地址由运营商进行分配。

4.3.2 配置 CE 的 IGP

CE 上配置 IGP，主要是要引入本站点的所有路由信息，具体配置过程本处不作详细介绍，请参考相关产品的 IGP 配置指导即可。

4.3.3 配置 CE 和 PE 间的路由交互

PE 和 CE/MCE 间的路由交互可以采用 EBGP、IBGP、静态路由、RIP、OSPF、ISIS，任选一种即可。以下过程以 EBGP 为例进行描述，其余方式请参考相应产品的文档中关于 VPN 的配置指导。

在 CE 上进行如下配置：

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
3. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将 PE 配置为对等体。
4. 执行命令 **import-route** { **direct** | **static** | **rip** *process-id* | **ospf** *process-id* | **isis** *process-id* } [**med** *med* | **route-policy** *route-policy-name*]*，引入本站点的路由。

----结束

4.4 部署分支通过公网 GRE over IPSec 隧道接入

分支通过公网 GRE over IPSec 隧道接入园区总部时，需要在分支和总部的出口路由器上分别进行 GRE 和 IPSec 的配置，同时配置分支和总部之间互通的静态路由。

本节只以出口路由器支持 GRE 和 IPSec 的情形来说明配置过程。如果分支或总部不支持 GRE 或 IPSec，则需要另外部署专用的 VPN 网关设备，相关的 GRE 和 IPSec 配置在 VPN 网关上进行，配置过程相似，本节不再重复。

4.4.1 配置出口路由器接口的 IP 地址

根据运营商分配的公网 IP 地址，配置总部和分支的出口路由器的公网侧接口的 IP 地址，具体配置过程略。

根据内部 IP 地址规划，配置总部和分支的出口路由器的内网侧接口的 IP 地址，具体配置过程略。

4.4.2 配置 GRE 隧道

在总部和分支的出口路由器分别进行如下配置：

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **interface tunnel** *tunnel-id*，创建隧道接口并进入接口视图。
3. 执行命令 **tunnel-protocol gre**，配置隧道协议为 GRE。
4. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置隧道接口 IP 地址。

   该地址与出口路由器的内网侧接口 IP 地址相同。
5. 执行命令 **source** *source-ip-address*，设置隧道的源 IP 地址。

   该地址与出口路由器的公网侧接口 IP 地址相同。
6. 执行命令 **destination** *dest-ip-address*，设置隧道的目的 IP 地址。

   该地址与对端出口路由器的公网侧接口 IP 地址相同。

----结束

4.4.3 配置静态路由

在总部和分支的出口路由器分别进行如下配置：

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ip route-static** *ip-address* { *mask* | *mask-length* } **tunnel** *tunnel-id*，配置到对端的静态路由。

   目的地址是对端的私网网段，*tunnel-id* 是已配置的 GRE 隧道的 ID。
3. 执行命令 **ip route-static** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*]，配置到对端的静态路由。

   目的地址是对端的公网地址，*interface-type interface-number* 是出口路由器的公网侧接口，*nexthop-address* 是公网上的下一跳地址。

----结束

4.4.4 配置 IPSec

配置 IPSec 隧道有手工建立和 IKE 协商两种方式，以下过程只介绍 IKE 协商方式，手工建立方式请另外参考相关产品的文档。

定义要保护的数据流

在总部和分支的出口路由器分别进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **acl** [*number*] *acl-number* [**match-order** { **auto** | **config** }]，创建高级 ACL。
3. 执行命令 **rule permit ip source** *source-ip-address source-wildcard* **destination** *dest-ip-address dest-wildcard*，定义要保护的数据流。

   source-ip-address 是出口路由器的公网侧接口 IP 地址，*dest-ip-address* 是对端出口路由器的公网侧接口 IP 地址。*source-wildcard* 和 *dest-wildcard* 设为 0。

4. 执行命令 **quit**，返回系统视图。

配置安全提议

在总部和分支的出口路由器分别进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ipsec proposal** *proposal-name*，创建安全提议并进入安全提议视图。
3. （可选）执行命令 **transform** { **ah** | **esp** | **ah-esp** }，配置安全协议。
4. （可选）执行命令 **ah authentication-algorithm** { **md5** | **sha1** }，设置 AH 采用的认证算法。
5. （可选）执行命令 **esp authentication-algorithm** [**md5** | **sha1**]，设置 ESP 采用的认证算法。
6. （可选）执行命令 **esp encryption-algorithm** { **3des** | **des** | **aes-128** | **aes-192** | **aes-256** }，设置 ESP 协议采用的加密算法。
7. （可选）执行命令 **encapsulation-mode** { **transport** | **tunnel** }，选择报文封装形式。

----结束

注意

在 IPSec 隧道两端，安全协议、认证算法、加密算法和封装形式应保持一致。

配置 IKE 安全提议

在总部和分支的出口路由器分别进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ike proposal** *proposal-number*，创建 IKE 安全提议并进入 IKE 安全提议视图。
3. （可选）执行命令 **encryption-algorithm** { **des-cbc** | **3des-cbc** | **aes-cbc-128** | **aes-cbc-192** | **aes-cbc-256** }，配置加密算法。
4. （可选）执行命令 **authentication-method pre-share**，设置预共享密钥认证方法。
5. （可选）执行命令 **authentication-algorithm** { **md5** | **sha1** }，选择认证算法。
6. （可选）执行命令 **dh** { **group1** | **group2** }，选择 Diffie-Hellman 组标识。
7. （可选）执行命令 **prf** { **hmac-md5** | **hmac-sha1** }，配置伪随机数产生函数的算法。
8. （可选）执行命令 **sa duration** *interval*，设置安全联盟生存周期。

----结束

注意

IKE SA 两端的认证算法、加密算法、认证方法和 DH 组标识应保持一致。

配置 IKE Peer

在总部和分支的出口路由器分别进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ike peer** *peer-name* { **v1** | **v2** }，创建 IKE Peer 并进入 IKE Peer 视图。
3. 执行命令 **exchange-mode** { **main** | **aggressive** }，配置协商模式。

   在野蛮模式下本地 ID 类型可配置为本端 IP 地址或本机名称，主模式下只能配置为本端 IP 地址。
4. 执行命令 **ike-proposal** *proposal-number*，配置 IKE 安全提议。
5. （可选）执行命令 **local-id-type** { **ip** | **name** }，配置 IKE Peer 的 ID 类型。

   缺省情况下，本地 ID 类型为 IP 地址形式。
6. （可选）执行命令 **local-address** *address*，配置 IKE 本端 IP 地址。

   缺省情况下，本端 IP 地址是绑定此 IPSec 策略的接口地址。
7. （可选）执行命令 **ike local-name** *local-name*，设置 IKE 协商时的本机名称。

   执行命令 **local-id-type** 配置本地 ID 类型为 name 时，需要配置本机名称。本机名称配置区分大小写，远端设备配置 IKE Peer 的 **remote-name** 时需要区分大小写，即和本机名称配置完全匹配。
8. （可选）执行命令 **peer-id-type** { **ip** | **name** }，配置远端 IKE Peer 的 ID 类型。

   缺省情况下，ID 类型为 IP 地址形式。本命令只在 IKE V2 版本时配置才有效。
9. （可选）执行命令 **nat traversal**，配置是否需要进行 NAT 穿越。

   配置 NAT 穿越时，需要配置 **local-id-type name**。
10. 执行命令 **pre-shared-key** *key-string*，配置与对端共享的 pre-shared key。

    如果选择了 pre-shared key 验证方法，需要为每个对端配置预共享密钥。建立安全连接的两个对端的预共享密钥必须一致。

    使用 pre-shared key 的验证方法时必须配置验证字。
11. （可选）执行命令 **remote-address** *ip-address*，配置对端的 IP 地址。
12. 执行命令 **remote-name** *name*，配置对端名称（只在野蛮模式下且使用名字认证时使用）。

    如果是 IKEv2 版本，**local-id-type** 为 ip，**peer-id-type** 为 name，那么也要指定 remote-name。

----结束

配置安全策略

在总部和分支的出口路由器分别进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ipsec policy** *policy-name seq-number* **isakmp**，创建安全策略。
3. 执行命令 **proposal** *proposal-name*&<1-6>，引用安全提议。
4. 执行命令 **security acl** *acl-number*，引用 ACL。
5. 执行命令 **ike-peer** *peer-name*，引用 IKE Peer。

----结束

应用安全策略

在总部和分支的出口路由器分别进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

   interface-type interface-number 是指出口路由器的公网侧接口。
3. 执行命令 **ipsec policy** *policy-name*，在接口上应用 IPSec 安全策略组。

----结束

4.5 部署合作伙伴通过公网 GRE over IPSec 隧道接入

合作伙伴通过 GRE over IPSec 隧道接入的配置，与分支通过 GRE over IPSec 隧道接入的配置基本相同。但是需要添加对于合作伙伴的访问权限控制，限制其只能访问处于 Extranet 区的服务器。相关的配置不做详细描述。

4.6 部署出差员工通过 L2TP over IPSec 隧道接入

出差员工通过公网 L2TP over IPSec 隧道接入园区总部时，员工的 PC 作为 L2TP 的 LAC，园区的出口路由器作为 LNS（如果网关路由器不支持 L2TP 功能，则需要另外部署 LNS 设备），并且在员工 PC 和出口路由器之间配置 IPSec，对 LAC 和 LNS 之间的数据流进行保护。

不同的产品对于 L2TP over IPSec 隧道的配置，根据产品的不同而有所不同，以下以 SRG 路由器为例来进行说明。

4.6.1 配置出口路由器接口的 IP 地址

根据运营商分配的公网 IP 地址，配置总部和分支的出口路由器的公网侧接口的 IP 地址，具体配置过程略。

根据内部 IP 地址规划，配置总部和分支的出口路由器的内网侧接口的 IP 地址，具体配置过程略。

4.6.2 配置出口路由器的 LNS 功能

配置 AAA 功能

配置 AAA 功能的步骤，可参考“6.2.1 配置 AAA 功能”。

配置地址池

配置地址池是为 L2TP 接入的用户分配 IP 地址。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **aaa**，进入 AAA 视图。
3. 执行命令 **domain** *domain-name*，进入域视图。
4. 执行命令 **ip pool** *pool-number first-address* [*last-address*]，配置域地址池。

----结束

配置虚拟模板接口

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface virtual-template** *virtual-template-number*，创建虚拟接口模板，并进入虚拟接口模板视图。
3. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]，配置本端 IP 地址。
4. 执行命令 **remote address pool** *pool-number*，配置为对端分配的地址。

   pool-number 为上面已配置的域地址池。
5. 执行命令 **ppp authentication-mode** { **chap** [**pap**] | **pap** } [**call-in**]，配置用户验证方式。

----结束

配置 LNS 侧的 L2TP 连接

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **l2tp enable**，使能 L2TP 功能。
3. 执行命令 **l2tp-group** *group-number*，创建 L2TP 组，并进入 L2TP 组视图。
4. 执行命令 **allow l2tp virtual-template** *virtual-template-number* [**remote** *remote-name*]，配置用来接受 LAC 的连接请求的的虚拟模板接口，以及隧道对端的名称。

说明

除 L2TP 组 1 之外，其余的 L2TP 组均需要指定 **remote** *remote-name*。LAC 拨号时，根据 LAC 侧的主机名（或 PC 的计算机名）来确定该 LAC 所归属的 L2TP 组，如果某个 LAC 的主机名在 LNS 侧未配置对应的 *remote-name*，则使用缺省的 L2TP 组 1 来处理该 LAC 的拨号请求。

5. （可选）执行命令 **tunnel name** *tunnel-name*，配置隧道本端名称。
6. （可选）执行命令 **tunnel authentication**，使能隧道验证功能。并执行命令 **tunnel password** { **cipher** | **simple** } **password**，配置隧道进行验证时的密码。

说明

配置隧道验证功能是为了保证安全性，如果使用 Windows 操作系统自带的 L2TP 拨号软件，由于其不支持隧道验证，则需要在 LNS 上取消隧道验证功能。

----结束

4.6.3 配置到 L2TP 用户网段的静态路由

由于 L2TP 用户没有 IGP，无法发布路由，因此需要在总部的三层路由设备（比如核心交换机）上配置一条到 L2TP 用户所在网段的静态路由。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ip route-static** *ip-address* { *mask* | *mask-length* } *nexthop-address*，配置到对端的静态路由。

   目的地址是 L2TP 用户所在网段，*nexthop-address* 是出口路由器上的内网侧接口 IP 地址。

----结束

4.6.4 配置出口路由器的 IPSec 功能

配置 IPSec 来保护 L2TP 隧道的方式与保护 GRE 隧道的方式基本相同，可请参见“4.4.4 配置 IPSec”。

不同的是用来定义被保护的数据流的 ACL 配置方式不同，因为无法直接用源和目的 IP 地址来定义匹配规则，但是可以使用 L2TP 报文本身的源端口号（1701）来定义匹配规则。另外由于出差员的 IP 地址不固定，路由器上 IPSec 的配置需要采用策略模版方式，被动接受隧道建立。

具体配置方式如下：

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **acl** [*number*] *acl-number* [**match-order** { **auto** | **config** }]，创建高级 ACL。
3. 执行命令 **rule permit udp source-port eq 1701**，定义要对 L2TP 数据流进行保护。

----结束

4.6.5 员工终端配置

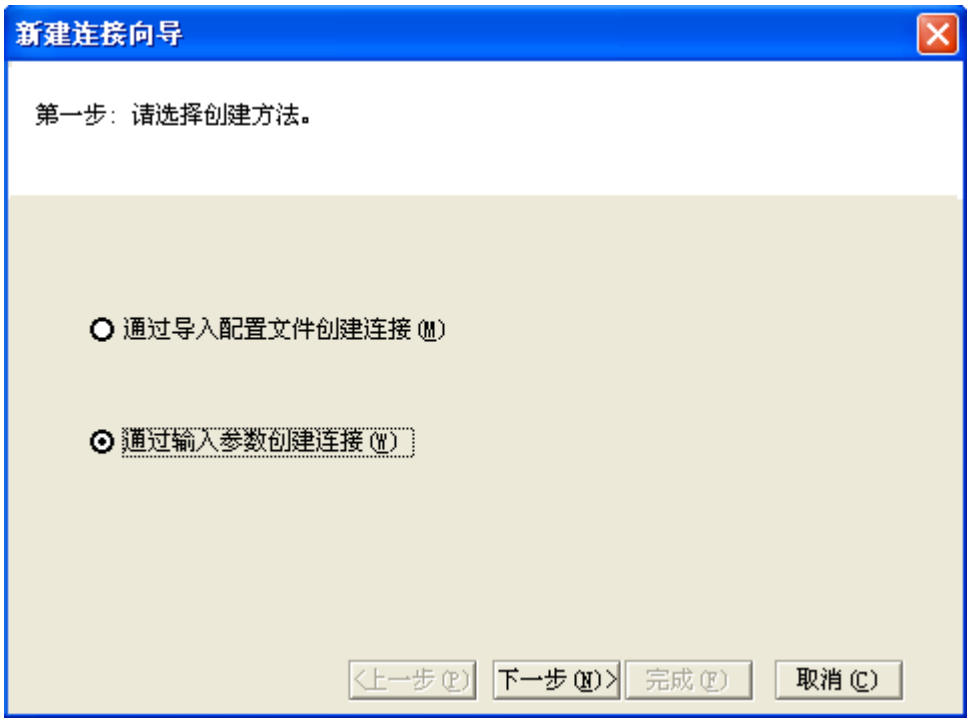
在员工的终端 PC 上，可以使用 Windows 操作系统自带的 L2TP 拨号软件来实现 L2TP over IPSec 隧道的接入，也可以使用专用的 VPN Client 软件进行拨号。

以下以华为公司开发的 Secoway VPN Client 软件为例，来说明员工终端上的配置。

1. 在菜单栏中选择“文件 > 新建”或在单击工具栏中单击“新建”按钮。

   弹出“第一步：请选择创建方法”对话框。

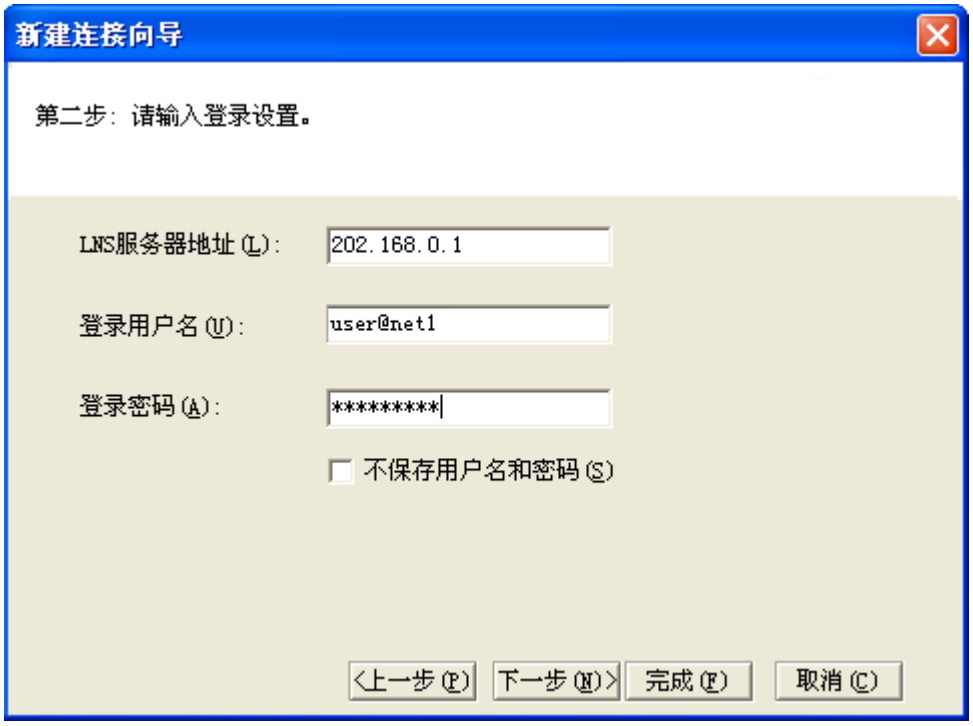
图4-2 选择创建方法



2. 选中“通过输入参数创建连接”，单击“下一步”。

   弹出“第二步：请输入登录设置”对话框。

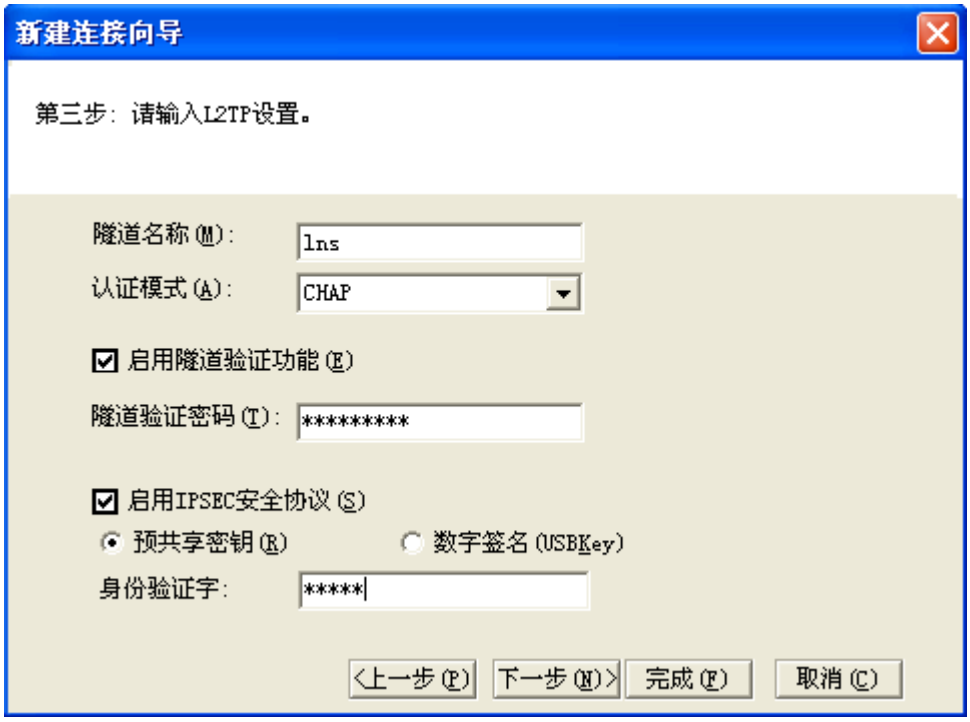
图4-3 登录设置



3. 输入 LNS 服务器地址、登录用户名和登录密码，单击“下一步”。

   弹出“第三步：请输入 L2TP 设置”对话框。

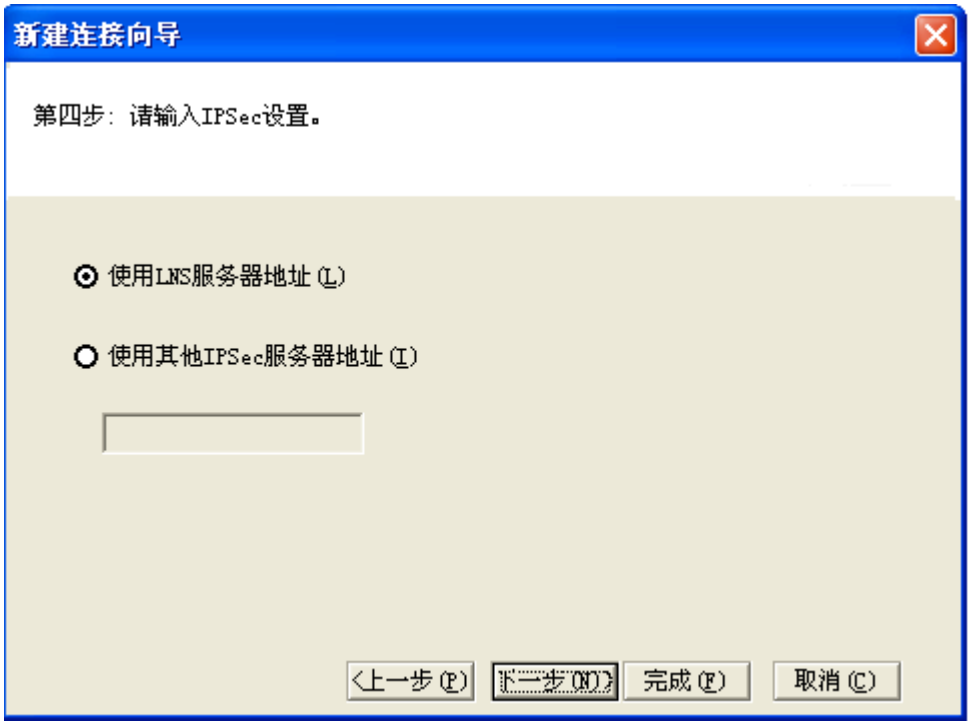
图4-4 输入 L2TP 设置



4. 参考图 4-4，输入或选择相关参数后，单击“下一步”。

   弹出“第四步：请输入 IPSec 设置”对话框。

图4-5 输入 IPSec 设置



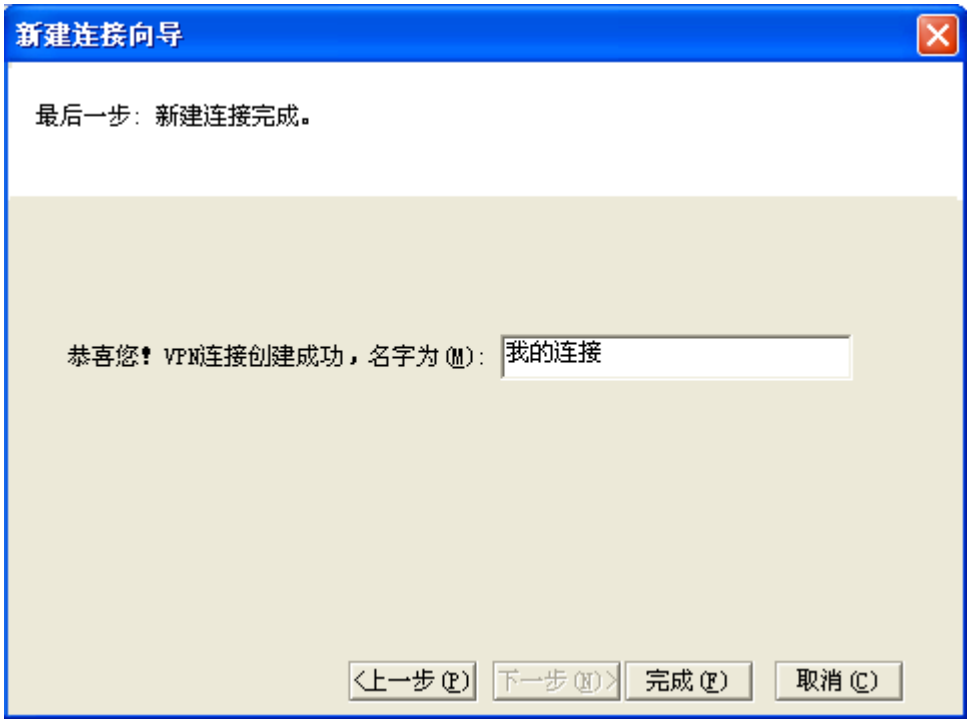
5. 选择使用 LNS 服务器地址，单击“下一步”。

   弹出“第五步：请输入 IPSec 高级设置”对话框。

图4-6 输入 IPSec 高级设置

6. 采用和出口路由器上的 IPSec/IKE 相同的参数设置界面上的所有参数，单击“下一步”。弹出“最后一步：新建连接完成”对话框。

图4-7 新建连接完成



7. 输入连接的名字，单击“完成”。

----结束

4.7 部署出差员工通过 SSL VPN 接入

SSL VPN 是以 SSL/TLS 协议为基础，利用标准浏览器都内置支持 SSL/TLS 的优势，对其应用功能进行扩展的新型 VPN。

除了 Web 访问、TCP/UDP 应用之外，SSL VPN 还能够对 IP 通信进行保护。SSL VPN 通信基于标准 TCP/UDP，不受 NAT 限制，能够穿越 NAT，使用户在任何地方都能够通过 SSL VPN 虚拟网关代理访问内网资源，使得远程安全接入更加灵活简单，大大降低了企业部署维护 VPN 的费用。

部署出差员工通过 SSL VPN 接入，主要是要在企业出口处部署 SSL VPN 网关来完成用户的接入，SSL VPN 网关可以使用独立设备（例如 SVN3000），也可以使用防火墙或者出口路由器上集成的 SSL VPN 功能。

而在用户终端上不需要特殊的配置，只要使用浏览器，以 HTTPS 方式访问 SSL VPN 网关的域名或者 IP 地址（例如 https://www.company.com），然后输入用户名和密码进行登录之后，在页面上可以选择相应的内网资源进行访问。

以下以 SRG 路由器为例说明 SSL VPN 网关的相关配置。

4.7.1 配置虚拟网关

SSL VPN 以虚拟网关的形式对外提供服务，所以在使用 SSL VPN 业务之前，必须先配置虚拟网关。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **v-gateway** *v-gateway-name ip-address* { **private** [*domain-name*] | **public** *domain-name* }，创建虚拟网关并进入虚拟网关视图。
3. 执行命令 **quit**，退回到系统视图。
4. （可选）执行命令 **v-gateway** *v-gateway-name* **max-user** *max-user*，配置虚拟网关的最大用户数。
5. （可选）执行命令 **v-gateway** *v-gateway-name* **cur-max-user** *cur-max-user*，配置虚拟网关的最大并发用户数。
6. （可选）执行命令 **v-gateway** *v-gateway-name* **max-resource** *max-resource*，配置虚拟网关的最大资源数。

----结束

4.7.2 配置用户认证

配置 SSL VPN 用户的认证和授权有多种方式，例如：

- 在网关路由器上直接配置用户名和密码，在本地进行认证。
- 在 RADIUS 服务器上配置用户名和密码，在网关路由器上配置 RADIUS 认证。
- 在 LDAP 服务器上配置用户名和密码，在网关路由器上配置 LDAP 认证。
- 通过 CA 证书，对用户身份进行认证。

以下只以在 SRG 路由器上配置本地用户名和密码为例，说明用户认证的配置方式，其他方式请参考相应产品的说明文档。

配置认证方案

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **aaa**，进入 AAA 视图。
3. 执行命令 **authentication-scheme** *scheme-name*，创建认证方案，并进入认证方案视图。

   说明

   在虚拟网关已经创建的情况下，请配置名为“虚拟网关名.scm”的认证方案。
4. 执行命令 **authentication-mode vpndb**，配置认证方法为 VPNDB 认证。

----结束

配置授权方案

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **aaa**，进入 AAA 视图。
3. 执行命 **authorization-scheme** *scheme-name*，创建授权方案，并进入授权方案视图。

   说明

   在虚拟网关已经创建的情况下，请配置名为“虚拟网关名.scm”的授权方案。

4. 执行命令 **authorization-mode vpndb**，配置授权方法为 VPNDB 授权。

----结束

配置域

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **aaa**，进入 AAA 视图。
3. 执行命令令 **domain** *domain-name*，创建域，并进入域视图。

   说明

   在虚拟网关已经创建的情况下，请配置名为“虚拟网关名.dom”的域。

4. 执行命令 **authentication-scheme** *scheme-name*，设置域的认证方案。
5. 执行命令 **authorization-scheme** *scheme-name*，配置域的授权方案。

----结束

配置 VPNDB 用户组

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **v-gateway** *v-gateway-name*，进入虚拟网关视图。
3. 执行命令 **vpndb**，进入虚拟网关 VPNDB 视图。
4. 执行命令 **group** *group-name* [*gid*] [**description** *group-info*]，添加 VPNDB 组。
5. 执行命令 **group** *group-name* {{ **files-share** | **network-extension** | **port-forwarding** | **web-proxy** } * | **all** } **enable**，启用 VPNDB 组的 SSL VPN 业务。

----结束

配置 VPNDB 用户

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **v-gateway** *v-gateway-name*，进入虚拟网关视图。
3. 执行命令 **vpndb**，进入虚拟网关 VPNDB 视图。
4. 执行命令 **user** *user-name user-password user-repassword* [**user-id** *user-gid* | *virtual-ip*] *，添加 VPNDB 用户并指定 UID、GID 或绑定虚拟 IP 地址。
5. 执行命令 **user** *user-name* **group** *group-name*，为 VPNDB 用户指定所属组。

----结束

4.7.3 配置端口转发

端口转发在应用级对用户访问进行控制，可控制是否提供各种应用服务（如：Telnet、远程桌面、FTP、E-mail 等基于 TCP 连接的服务）。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **v-gateway** *v-gateway-name*，进入虚拟网关视图。
3. 执行命令 **service**，进入虚拟网关服务视图。
4. 执行命令 **port-forwarding enable**，启用端口转发功能。
5. 执行命令 **port-forwarding resource** *resource-alias* { **any** | **host-ip** *ip-address* | **host-name** *hostname* } *port* [*resource-description*]，添加端口转发资源。
6. （可选）执行命令 **port-forwarding auto-start enable**，启用端口转发自动启动功能。

   启用端口转发的自动启动功能后，用户在虚拟网关页面上根据提示安装控件后，端口转发的功能便会自动启动。
7. （可选）执行命令 **port-forwarding keep-alive enable**，启用端口转发保持连接功能。

   启用端口转发的保持连接功能后，客户端会定时向网关发送报文，这样客户端和 SRG 的端口转发连接不会因为 SSL 会话超时而断开。

----结束

4.7.4 配置策略

策略主要用来过滤 SSL VPN 用户可以访问的资源和进行流控制。管理员可以配置一系列的匹配规则，以识别需要过滤或放行的资源和报文。

虚拟网关的策略包括如下四种类型：

- 虚拟网关源 IP 型：通过限制客户端源 IP 地址定义对当前虚拟网关的访问控制。
- 用户源 IP 型：通过限制源 IP 地址定义用户对虚拟网关的访问控制。
- 用户目的 IP 型：通过限制目的 IP 和端口定义用户对虚拟网关内网资源的访问控制。
- 用户 URL 型：通过限制目的 URL 定义用户对虚拟网关内网资源的访问控制。

对于出差员工通过 SSL VPN 接入总部来说，一般需要配置用户目的 IP 型的策略。

策略的配置可以分为三个层次：

- 配置针对整个虚拟网关的默认策略。对虚拟网关中未配置策略的用户组或用户有效。
- 配置针对某个用户组的策略。用户组策略对组内所有用户有效。
- 配置针对单个用户的策略。对于有特殊需求的用户，可另外单独配置其策略。

如果针对用户的策略和针对用户组的策略冲突，则需要和针对整个虚拟网关的默认策略进行比较，与默认策略相反的策略优先。

配置针对虚拟网关的目的 IP 型默认策略

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **v-gateway** *v-gateway-name*，进入虚拟网关视图。
3. 执行命令 **security**，进入虚拟网关安全视图。
4. 执行命令 **policy-default-action** { **deny** | **permit** } **user-dst-ip**，配置针对虚拟网关的目的 IP 型默认策略。

----结束

配置针对用户组的目的 IP 型策略

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **v-gateway** *v-gateway-name*，进入虚拟网关视图。
3. 执行命令 **vpndb**，进入虚拟网关 VPNDB 视图。

执行命令 **group** *group-name* **policy** { **deny** | **permit** } **dst-ip**{ *ip-address mask* | **any** } **port** { *port* | **any** }，为用户组添加目的 IP 型策略。

----结束

配置针对用户的目的 IP 型策略

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **v-gateway** *v-gateway-name*，进入虚拟网关视图。
3. 执行命令 **vpndb**，进入虚拟网关 VPNDB 视图。

执行命令 **user** *user-name* **policy** { **deny** | **permit** } **dst-ip**{ *ip-address mask* | **any** } **port** { *port* | **any** }，为用户添加目的 IP 型策略。

----结束

4.8 部署外部 Internet 客户访问 DMZ 区

外部访客访问 DMZ 区无特殊配置，主要是通过在出口路由器或者防火墙上配置 ACL，限制外部访客只能访问 DMZ 区中的服务器。

如果 DMZ 区中的服务器使用的是私网 IP 地址，则需要部署 NAT（使用 NAT 设备或者使用出口路由器/防火墙集成的 NAT 功能），实现私网地址和公网地址的转换。

具体的配置步骤略。

4.9 配置举例

> **注意**
>
> 部分场景由于配置较为简单，或者无特殊需要说明的配置，因此不提供配置举例。

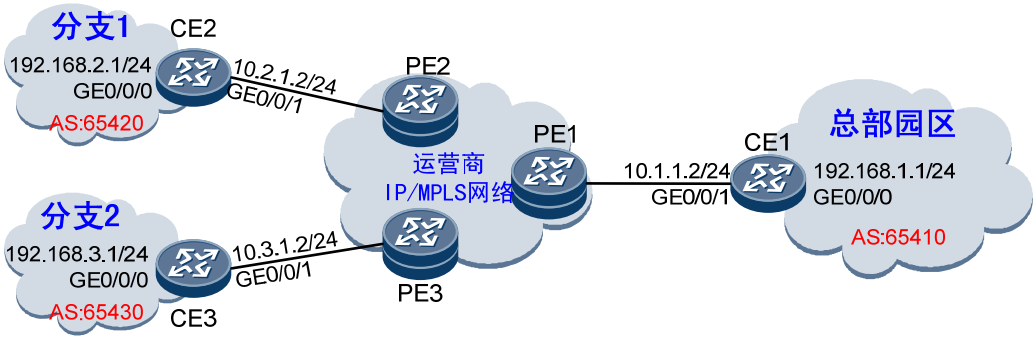
4.9.1 部署分支通过运营商 L3VPN 接入

组网需求

某企业有较多的、具有一定规模的分支机构，需要实现分支和总部、分支和分支之间的互联。但是企业没有自建的广域网，另外传统的 VPN 技术（例如 GRE 隧道等）都只能实现点对点的互联，多点之间的互联部署会非常复杂。因此最佳的方式是租用运营商提供的 MPLS L3VPN 服务来实现多点之间的互联。

分支通过运营商提供的 MPLS L3VPN 服务来接入总部园区，此时总部和各分支都相当于 L3VPN 中的一个 Site，总部和各分支的出口路由器作为 L3VPN 的 CE 设备，连接到运营商的 PE 设备，通过运营商的 IP/MPLS 网络实现互通。

图4-8 分支通过运营商 L3VPN 接入组网图



数据准备

表4-1 数据规划表

配置项	配置子项	数据
IP 地址	接口 IP 地址	参见组网图中的标注

操作步骤

注意

下面的操作步骤中省略了总部内部和分支内部的相同配置，以及运营商网络中 PE 和 P 的相关配置，重点关注作为 CE 设备的总部/分支出口路由器的配置。

1. 配置接口 IP 地址

   # 配置 CE1 的 IP 地址。

```
<Qudiway> system-view
[Qudiway] sysname CE1
[CE1] interface GigabitEthernet 0/0/1
[CE1-GigabitEthernet0/0/1] ip address 10.1.1.2 255.255.255.0
[CE1-GigabitEthernet0/0/1] quit
[CE1] interface GigabitEthernet 0/0/0
[CE1-GigabitEthernet0/0/0] ip address 192.168.1.1 255.255.255.0
[CE1-GigabitEthernet0/0/0] quit
```

   # 配置 CE2 的 IP 地址。

```
<Qudiway> system-view
[Qudiway] sysname CE2
[CE2] interface GigabitEthernet 0/0/1
[CE2-GigabitEthernet0/0/1] ip address 10.2.1.2 255.255.255.0
[CE2-GigabitEthernet0/0/1] quit
[CE2] interface GigabitEthernet 0/0/0
[CE2-GigabitEthernet0/0/0] ip address 192.168.2.1 255.255.255.0
[CE2-GigabitEthernet0/0/0] quit
```

   # 配置 CE3 的 IP 地址。

```
<Qudiway> system-view
[Qudiway] sysname CE3
[CE3] interface GigabitEthernet 0/0/1
[CE3-GigabitEthernet0/0/1] ip address 10.3.1.2 255.255.255.0
[CE3-GigabitEthernet0/0/1] quit
[CE3] interface GigabitEthernet 0/0/0
[CE3-GigabitEthernet0/0/0] ip address 192.168.3.1 255.255.255.0
[CE3-GigabitEthernet0/0/0] quit
```

2. 配置 IGP

   # 配置 CE1 的 OSPF。

```
[CE1] ospf 1
[CE1-ospf-1] import-route direct
[CE1-ospf-1] import-route static
[CE1-ospf-1] area 0
[CE1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[CE1-ospf-1-area-0.0.0.0] quit
[CE1-ospf-1] quit
```

   # 配置 CE2 的 OSPF。

```
[CE2] ospf 1
[CE2-ospf-1] import-route direct
```

```
[CE2-ospf-1] import-route static
[CE2-ospf-1] area 0
[CE2-ospf-1-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[CE2-ospf-1-area-0.0.0.0] quit
[CE2-ospf-1] quit
```

配置 CE3 的 OSPF。

```
[CE3] ospf 1
[CE3-ospf-1] import-route direct
[CE3-ospf-1] import-route static
[CE3-ospf-1] area 0
[CE3-ospf-1-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[CE3-ospf-1-area-0.0.0.0] quit
[CE3-ospf-1] quit
```

3. 配置 CE 和 PE 间的路由交互

配置 CE1 与 PE1 的路由交互（假设运营商的 IP/MPLS 网络的 AS 号为 100，PE1 连接 CE1 的接口地址为 10.1.1.1）。

```
[CE1] bgp 65410
[CE1-bgp] peer 10.1.1.1 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] import-route static
[CE1-bgp] import-route ospf 1
[CE1-bgp] quit
```

配置 CE2 与 PE2 的路由交互（假设运营商的 IP/MPLS 网络的 AS 号为 100，PE2 连接 CE2 的接口地址为 10.2.1.1）。

```
[CE2] bgp 65420
[CE2-bgp] peer 10.2.1.1 as-number 100
[CE2-bgp] import-route direct
[CE2-bgp] import-route static
[CE2-bgp] import-route ospf 1
[CE2-bgp] quit
```

配置 CE3 与 PE3 的路由交互（假设运营商的 IP/MPLS 网络的 AS 号为 100，PE3 连接 CE3 的接口地址为 10.3.1.1）。

```
[CE3] bgp 65430
[CE3-bgp] peer 10.3.1.1 as-number 100
[CE3-bgp] import-route direct
[CE3-bgp] import-route static
[CE3-bgp] import-route ospf 1
[CE3-bgp] quit
```

----结束

配置文件

- CE1 的配置文件

```
#
 sysname CE1
#
interface GigabitEthernet0/0/0
```

```
 undo shutdown
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
bgp 65410
 peer 10.1.1.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  import-route static
  import-route ospf 1
  peer 10.1.1.1 enable
#
ospf 1
 import-route direct
 import-route static
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
#
return
```

- CE2 的配置文件

```
#
 sysname CE2
#
interface GigabitEthernet0/0/0
 undo shutdown
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 undo shutdown
 ip address 10.2.1.2 255.255.255.0
#
bgp 65420
 peer 10.2.1.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  import-route static
  import-route ospf 1
  peer 10.2.1.1 enable
#
ospf 1
 import-route direct
 import-route static
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
#
return
```

- CE3 的配置文件

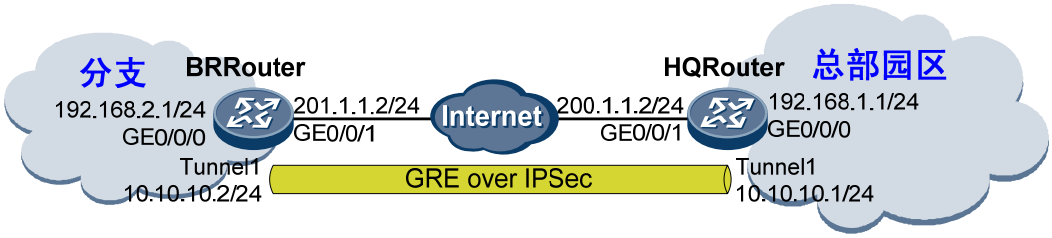

```
#
 sysname CE3
#
interface GigabitEthernet0/0/0
 undo shutdown
 ip address 192.168.3.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 undo shutdown
 ip address 10.3.1.2 255.255.255.0
#
bgp 65430
 peer 10.3.1.1 as-number 100
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  import-route static
  import-route ospf 1
  peer 10.3.1.1 enable
#
ospf 1
 import-route direct
 import-route static
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
#
return
```

4.9.2 部署分支通过公网 GRE over IPSec 隧道接入

组网需求

企业在外地建立分支机构，由于暂无条件在总部和企业之间构建专线互联，只能通过Internet 网络实现分支的接入，由于 Internet 网络本身并不安全，因此要求通过 GRE over IPSec 隧道来实现总部和分支之间数据的可靠传输。

图4-9 部署分支通过公网 GRE over IPSec 隧道接入组网图



数据准备

表4-2 数据规划表

配置项	配置子项	数据
IP 地址	接口 IP 地址	参见组网图中的标注
IPSec	安全协议	ESP
	封装模式	隧道模式
	ESP 认证算法	SHA1
	加密算法	DES
IKE	认证算法	MD5
	协商模式	野蛮模式
	预认证共享密钥	abcde

操作步骤

注意

下面的操作步骤中省略了总部内部和分支内部的配置。

1. 配置总部出口路由器

   # 配置公网侧 IP 地址。

```
<Qudiway> system-view
[Qudiway] sysname HQRouter
[HQRouter] interface GigabitEthernet 0/0/1
[HQRouter-GigabitEthernet0/0/1] ip address 200.1.1.2 255.255.255.0
[HQRouter-GigabitEthernet0/0/1] quit
```

   # 配置内网侧 IP 地址。

```
[HQRouter] interface GigabitEthernet 0/0/0
[HQRouter-GigabitEthernet0/0/0] ip address 192.168.1.1 255.255.255.0
[HQRouter-GigabitEthernet0/0/0] quit
```

   # 配置 GRE 隧道。

```
[HQRouter] interface tunnel 1
[HQRouter-Tunnel1] tunnel-protocol gre
[HQRouter-Tunnel1] ip address 10.10.10.1 255.255.255 0
[HQRouter-Tunnel1] source 200.1.1.2
[HQRouter-Tunnel1] destination 201.1.1.2
```

```
[HQRouter-Tunnel1] quit
```

配置到分支的静态路由。（假设总部出口路由器的公网下一跳地址是 200.1.1.1）

```
[HQRouter] ip route-static 192.168.2.0 255.255.255.0 tunnel 1
[HQRouter] ip route-static 201.1.1.0 255.255.255.0 GigabitEthernet 0/0/1 200.1.1.1
```

配置 ACL，定义要保护的数据流。

```
[HQRouter] acl 3000
[HQRouter-acl-adv-3000] rule permit ip source 200.1.1.2 0 destination 201.1.1.2 0
[HQRouter-acl-adv-3000] quit
```

配置安全提议。

```
[HQRouter] ipsec proposal tran1
[HQRouter-ipsec-proposal-tran1] encapsulation-mode tunnel
[HQRouter-ipsec-proposal-tran1] transform esp
[HQRouter-ipsec-proposal-tran1] esp authentication-algorithm sha1
[HQRouter-ipsec-proposal-tran1] esp encryption-algorithm des
[HQRouter-ipsec-proposal-tran1] quit
```

配置 IKE 提议。

```
[HQRouter] ike proposal 10
[HQRouter-ike-proposal-10] authentication-method pre-share
[HQRouter-ike-proposal-10] authentication-algorithm md5
[HQRouter-ike-proposal-10] quit
```

配置 IKE 对等体。

```
[HQRouter] ike local-name HQRouter
[HQRouter] ike peer br
[HQRouter-ike-peer-br] undo version 2
[HQRouter-ike-peer-br] exchange-mode aggressive
[HQRouter-ike-peer-br] local-id-type name
[HQRouter-ike-peer-br] remote-name BRRouter
[HQRouter-ike-peer-br] ike-proposal 10
[HQRouter-ike-peer-br] remote-address 201.1.1.2
[HQRouter-ike-peer-br] pre-shared-key abcde
[HQRouter-ike-peer-br] quit
```

配置安全策略。

```
[HQRouter] ipsec policy map1 10 isakmp
[HQRouter-ipsec-policy-isakmp-map1-10] security acl 3000
[HQRouter-ipsec-policy-isakmp-map1-10] proposal tran1
[HQRouter-ipsec-policy-isakmp-map1-10] ike-peer br
[HQRouter-ipsec-policy-manual-map1-10] quit
```

应用安全策略。

```
[HQRouter] interface GigabitEthernet 0/0/1
[HQRouter-GigabitEthernet0/0/1] ipsec policy map1
[HQRouter-GigabitEthernet0/0/1] quit
```

2. 配置分支出口路由器

配置公网侧 IP 地址。


```
<Qudiway> system-view
[Qudiway] sysname BRRouter
[BRRouter] interface GigabitEthernet 0/0/1
[BRRouter-GigabitEthernet0/0/1] ip address 201.1.1.2 255.255.255.0
[BRRouter-GigabitEthernet0/0/1] quit
```

配置内网侧 IP 地址。

```
[BRRouter] interface GigabitEthernet 0/0/0
[BRRouter-GigabitEthernet0/0/0] ip address 192.168.2.1 255.255.255.0
[BRRouter-GigabitEthernet0/0/0] quit
```

配置 GRE 隧道。

```
[BRRouter] interface tunnel 1
[BRRouter-Tunnel1] tunnel-protocol gre
[BRRouter-Tunnel1] ip address 10.10.10.2 255.255.255 0
[BRRouter-Tunnel1] source 201.1.1.2
[BRRouter-Tunnel1] destination 200.1.1.2
[BRRouter-Tunnel1] quit
```

配置到总部的静态路由。（假设分支出口路由器的公网下一跳地址是 201.1.1.1）

```
[BRRouter] ip route-static 192.168.1.0 255.255.255.0 tunnel 1
[BRRouter] ip route-static 200.1.1.0 255.255.255.0 GigabitEthernet 0/0/1 201.1.1.1
```

配置 ACL，定义要保护的数据流。

```
[BRRouter] acl 3000
[BRRouter-acl-adv-3000] rule permit ip source 201.1.1.2 0 destination 200.1.1.2 0
[BRRouter-acl-adv-3000] quit
```

配置安全提议。

```
[BRRouter] ipsec proposal tran1
[BRRouter-ipsec-proposal-tran1] encapsulation-mode tunnel
[BRRouter-ipsec-proposal-tran1] transform esp
[BRRouter-ipsec-proposal-tran1] esp authentication-algorithm sha1
[BRRouter-ipsec-proposal-tran1] esp encryption-algorithm des
[BRRouter-ipsec-proposal-tran1] quit
```

配置 IKE 提议。

```
[BRRouter] ike proposal 10
[BRRouter-ike-proposal-10] authentication-method pre-share
[BRRouter-ike-proposal-10] authentication-algorithm md5
[BRRouter-ike-proposal-10] quit
```

配置 IKE 对等体。

```
[BRRouter] ike local-name BRRouter
[BRRouter] ike peer hq
[BRRouter-ike-peer-hq] undo version 2
[BRRouter-ike-peer-hq] exchange-mode aggressive
[BRRouter-ike-peer-hq] local-id-type name
[BRRouter-ike-peer-hq] remote-name HQRouter
[BRRouter-ike-peer-hq] ike-proposal 10
[BRRouter-ike-peer-hq] remote-address 200.1.1.2
[BRRouter-ike-peer-hq] pre-shared-key abcde
```

```
[BRRouter-ike-peer-hq] quit
```

配置安全策略。

```
[BRRouter] ipsec policy map1 10 isakmp
[BRRouter-ipsec-policy-isakmp-map1-10] security acl 3000
[BRRouter-ipsec-policy-isakmp-map1-10] proposal tran1
[BRRouter-ipsec-policy-isakmp-map1-10] ike-peer hq
[BRRouter-ipsec-policy-manual-map1-10] quit
```

应用安全策略。

```
[BRRouter] interface GigabitEthernet 0/0/1
[BRRouter-GigabitEthernet0/0/1] ipsec policy map1
[BRRouter-GigabitEthernet0/0/1] quit
```

----结束

配置文件

- 总部出口路由器的配置文件

```
#
 sysname HQRouter
#
acl number 3000
 rule permit ip source 200.1.1.0 0.0.0.255 destination 201.1.1.0 0.0.0.255
#
 ike local-name HQRouter
#
ike proposal 10
 authentication-algorithm md5
#
ike peer br
 exchange-mode aggressive
 pre-shared-key abcde
 ike-proposal 10
 undo version 2
 local-id-type name
 remote-name BRRouter
 remote-address 201.1.1.2
#
ipsec proposal tran1
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer br
 proposal tran1
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 200.1.1.2 255.255.255.0
 ipsec policy map1
#
```

```
interface Tunnel1
 tunnel-protocol gre
 ip address 10.10.10.1 255.255.255.0
 source 200.1.1.2
 destination 201.1.1.2
#
 ip route-static 192.168.2.1 255.255.255.0 tunnel 1
 ip route-static 201.1.1.0 255.255.255.0 GigabitEthernet 0/0/1 200.1.1.1
#
Return
```

- 分支出口路由器的配置文件

```
#
 sysname BRRouter
#
acl number 3000
 rule permit ip source 201.1.1.0 0.0.0.255 destination 200.1.1.0 0.0.0.255
#
 ike local-name BRRouter
#
ike proposal 10
 authentication-algorithm md5
#
ike peer hq
 exchange-mode aggressive
 pre-shared-key abcde
 ike-proposal 10
 undo version 2
 local-id-type name
 remote-name HQRouter
 remote-address 201.1.1.2
#
ipsec proposal tran1
 esp authentication-algorithm sha1
#
ipsec policy map1 10 isakmp
 security acl 3000
 ike-peer hq
 proposal tran1
#
interface GigabitEthernet0/0/0
 ip address 192.168.2.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 201.1.1.2 255.255.255.0
 ipsec policy map1
#
interface Tunnel1
 tunnel-protocol gre
 ip address 10.10.10.2 255.255.255.0
 source 201.1.1.2
 destination 200.1.1.2
#
 ip route-static 192.168.1.1 255.255.255.0 tunnel 1
 ip route-static 200.1.1.0 255.255.255.0 GigabitEthernet 0/0/1 201.1.1.1
#
```

```
Return
```

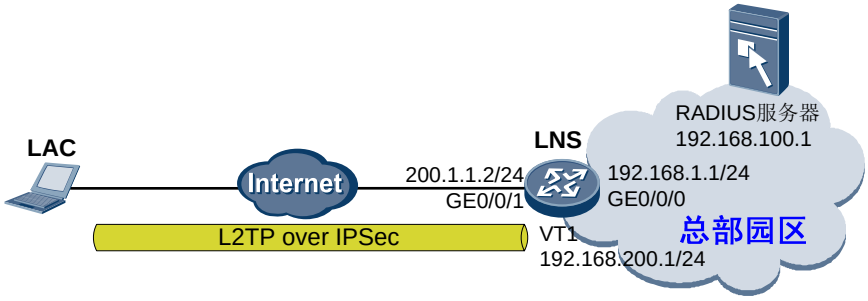
4.9.3 部署出差员工通过 L2TP over IPSec 隧道接入

组网需求

企业中的出差员工在非固定办公地点，例如酒店等场所，希望通过随身携带的笔记本电脑，通过公网接入到企业总部园区进行办公。并且获得和在园区内固定办公一样的权限，同时还要保证数据在公网上传输的可靠性。

此时可以通过在出差员工的 PC 和企业总部园区的出口路由器之间构建 L2TP over IPSec 隧道来实现上述需求。出差员工能过 VPN Client 软件（Secoway VPN Client）进行 L2TP 拨号接入总部园区。

图4-10 部署出差员工通过公网 L2TP over IPSec 隧道接入组网图



数据准备

表4-3 数据规划表

配置项	配置子项	数据
IP 地址	接口 IP 地址	参见组网图中的标注
	L2TP 用户地址池	192.168.200.0/24
IPSec	安全协议	ESP
	封装模式	隧道模式
	ESP 认证算法	MD5
	加密算法	DES
IKE	认证算法	MD5
	加密算法	DES-CBC
	DH 组	DH 组 1
	协商模式	野蛮模式

配置项	配置子项	数据
	预认证共享密钥	abcde

操作步骤

注意

下面的操作步骤中省略了总部内部的配置。

1. 配置 LNS 的 IP 地址和路由

   # 配置公网侧 IP 地址。

```
<Qudiway> system-view
[Qudiway] sysname LNS
[LNS] interface GigabitEthernet 0/0/1
[LNS-GigabitEthernet0/0/1] ip address 200.1.1.2 255.255.255.0
[LNS-GigabitEthernet0/0/1] quit
```

   # 配置内网侧 IP 地址。

```
[LNS] interface GigabitEthernet 0/0/0
[LNS-GigabitEthernet0/0/0] ip address 192.168.1.1 255.255.255.0
[LNS-GigabitEthernet0/0/0] quit
```

   # 配置到公网的静态路由。（假设总部出口路由器的公网下一跳地址是 200.1.1.1）

```
[LNS] ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet 0/0/1 200.1.1.1
```

2. 配置 LNS 功能

   # 启用 L2TP 功能。

```
[LNS] l2tp enable
```

   # 配置 IP 地址池。

```
[LNS] aaa
[LNS-aaa] domain l2tp
[LNS-aaa-domain-l2tp] ip pool 1 192.168.200.2 192.168.200.254
[LNS-aaa-domain-l2tp] quit
[LNS-aaa] quit
```

   # 配置虚拟模板接口。

```
[LNS] interface Virtual-Template 1
[LNS-Virtual-Template1] ppp authentication-mode chap
[LNS-Virtual-Template1] ip address 192.168.200.1 255.255.255.0
[LNS-Virtual-Template1] remote address pool 1
[LNS-Virtual-Template1] quit
```

配置域名分隔符。

```
[LNS] l2tp domain suffix-separator @
```

配置 L2TP 组。

```
[LNS] l2tp-group 1
[LNS-l2tp1] tunnel name lns
[LNS-l2tp1] allow l2tp virtual-template 1
[LNS-l2tp1] tunnel authentication
[LNS-l2tp1] tunnel password simple Admin@124
[LNS-l2tp1] quit
```

说明

由于 PC 操作系统自带的 VPN 客户端无法配置隧道验证功能，如果出差用户使用 PC 操作系统自带的 VPN 客户端接入，则必须取消 LNS 的隧道验证功能。

创建认证方案。

```
[LNS] aaa
[LNS-aaa] authentication-scheme auth1
[LNS-aaa-authen-auth1] authentication-mode radius
[LNS-aaa-authen-auth1] quit
[LNS-aaa] quit
```

配置 RADIUS 模板。

```
[LNS] radius-server template rd1
[LNS-radius-rd1] radius-server authentication 192.168.200.1 1645
[LNS-radius-rd1] radius-server shared-key key1
[LNS-radius-rd1] radius-server user-name domain-included
[LNS-radius-rd1] quit
# 配置域，应用 RADIUS 模板及认证方案。
[LNS] aaa
[LNS-aaa] domain l2tp
[LNS-aaa-domain-l2tp] authentication-scheme auth1
[LNS-aaa-domain-l2tp] radius-server rd1
[LNS-aaa-domain-l2tp] quit
[LNS-aaa] quit
```

3. 配置 IPSec 功能

配置 ACL，定义要保护的数据流。

```
[LNS] acl 3000
[LNS-acl-adv-3000] rule permit ip source 200.1.1.2 0 destination 201.1.1.2 0
[LNS-acl-adv-3000] quit
```

配置安全提议。

```
[LNS] ipsec proposal tran1
[LNS-ipsec-proposal-tran1] encapsulation-mode tunnel
[LNS-ipsec-proposal-tran1] transform esp
[LNS-ipsec-proposal-tran1] esp authentication-algorithm md5
[LNS-ipsec-proposal-tran1] esp encryption-algorithm des
[LNS-ipsec-proposal-tran1] quit
```

配置 IKE 提议。

```
[LNS] ike proposal 10
[LNS-ike-proposal-10] authentication-method pre-share
[LNS-ike-proposal-10] authentication-algorithm md5
[LNS-ike-proposal-10] encryption-algorithm des-cbc
[LNS-ike-proposal-10] quit
```

配置 IKE 对等体。

```
[LNS] ike peer lac
[LNS-ike-peer-lac] exchange-mode aggressive
[LNS-ike-peer-lac] ike-proposal 10
[LNS-ike-peer-lac] pre-shared-key abcde
[LNS-ike-peer-lac] quit
```

配置安全策略模板和安全策略。

```
[LNS] ipsec policy-template map_temp 1
[LNS-ipsec-policy-templet-map_temp-1] security acl 3000
[LNS-ipsec-policy-templet-map_temp-1] proposal tran1
[LNS-ipsec-policy-templet-map_temp-1] ike-peer lac
[LNS-ipsec-policy-templet-map_temp-1] quit
[LNS] ipsec policy map1 10 isakmp template map_temp
```

应用安全策略。

```
[LNS] interface GigabitEthernet 0/0/1
[LNS-GigabitEthernet0/0/1] ipsec policy map1
[LNS-GigabitEthernet0/0/1] quit
```

4. 配置终端

请参考“4.6.5 员工终端配置”对终端进行配置。

LNS 相关参数如下：

- LNS 服务器地址：200.1.1.2
- 登录用户名：xxx@l2tp，xxx 为用户名
- 登录密码：设定的用户密码
- 隧道名称：lns
- 认证模式：CHAP
- 启用隧道验证功能
- 隧道验证密码：Admin@124
- 启用 IPSEC 安全协议并选择“预共享密钥”
- 身份验证字：abcde

IPSec 相关参数如下：

- 封装模式：隧道模式
- 安全协议：ESP
- ESP 协议验证算法：MD5
- ESP 协议加密算法：DES
- NAT 穿越：不启用

IKE 协商参数如下：

- 协商模式：野蛮模式
- ID 类型：IP 地址
- 验证算法：MD5
- 加密算法：DES-CBC
- DH 组标志：Group 1

----结束

配置文件

LNS 配置文件：

```
#
 sysname LNS
#
acl number 3000
 rule 5 permit udp source-port eq 1701
#
 l2tp enable
#
 l2tp domain suffix-separator @
#
radius-server template rd1
 radius-server shared-key key1
 radius-server authentication 192.168.100.1 1645
 radius-server user-name domain-included
#
ike proposal 10
 authentication-algorithm md5
#
ike peer lac
 exchange-mode aggressive
 pre-shared-key abcde
 ike-proposal 10
#
ipsec proposal tran1
 esp authentication-algorithm md5
#
ipsec policy-template map_temp 1
 security acl 3000
 proposal tran1
 ike-peer lac
ipsec policy map1 10 isakmp template map_temp
#
interface Virtual-Template1
 ppp authentication-mode chap
 ip address 192.168.200.1 255.255.255.0
 remote address pool 1
#
 interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
```



```
#
interface GigabitEthernet0/0/1
 ip address 200.1.1.2 255.255.255.0
 ipsec policy map1
#
l2tp-group 1
 tunnel password simple Admin@124
 allow l2tp virtual-template 1
#
aaa
#
 authentication-scheme default
 authentication-scheme auth1
 #
 authorization-scheme default
 authorization-scheme auth1
  authorization-mode  radius
 #
 accounting-scheme default
 #
 domain default
#
 domain l2tp
  ip pool 192.168.200.2 192.168.200.254
  authentication-scheme auth1
  radius-server rd1
#
 ip route-static 0.0.0.0 0.0.0.0 200.1.1.1
#
 return
```

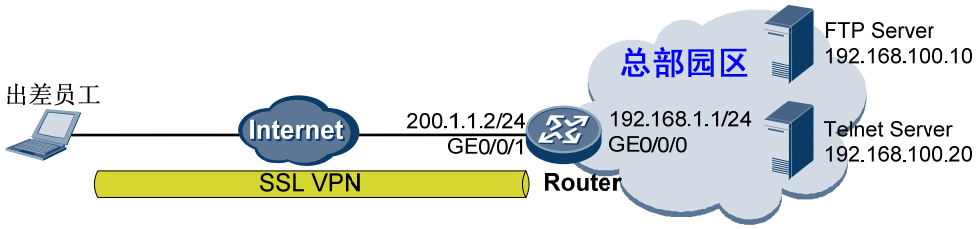
4.9.4 部署出差员工通过 SSL VPN 接入

组网需求

企业中的出差员工在非固定办公地点，例如酒店等场所，希望通过随身携带的笔记本电脑，通过公网接入到企业总部园区进行办公，能访问园区内的特定资源（FTP 服务器）并且能使用 Notes 应用。另外部分员工还能够访问 Telnet 服务器。

为使出差员工更方便的接入总部园区，而不需要进行特殊配置或者安装的客户端软件，可以部署 SSL VPN，这样员工只需要使用 Web 浏览器即可通过 SSL VPN 接入。

图4-11 部署出差员工通过 SSL VPN 接入组网图



数据准备

表4-4 数据规划表

配置项	配置子项	数据
IP 地址	接口 IP 地址	参见组网图中的标注
	应用服务器 IP 地址	参见组网图中的标注
SSL VPN 虚拟网关	类型	独占型
	域名	www.employee.com
	最大用户数	200
	同时在线最大用户数	50
	最大资源数	1024
用户和权限	用户 1	用户名：tom 密码：123456 权限：FTP、Telnet、Notes
	用户 2	用户名：tony 密码：654321 权限：FTP、Notes

操作步骤

注意

下面的操作步骤中省略了总部内部的配置。

1. 配置地址和路由

   # 配置公网侧 IP 地址。

```
<Qudiway> system-view
[Qudiway] sysname Router
[Router] interface GigabitEthernet 0/0/1
[Router-GigabitEthernet0/0/1] ip address 200.1.1.2 255.255.255.0
[Router-GigabitEthernet0/0/1] quit
```

   # 配置内网侧 IP 地址。

```
[Router] interface GigabitEthernet 0/0/0
[Router-GigabitEthernet0/0/0] ip address 192.168.1.1 255.255.255.0
[Router-GigabitEthernet0/0/0] quit
```

配置到公网的静态路由。（假设总部出口路由器的公网下一跳地址是 200.1.1.1）

```
[Router] ip route-static 0.0.0.0 0.0.0.0 GigabitEthernet 0/0/1 200.1.1.1
```

2. 配置虚拟网关

```
[Router] v-gateway employee 200.1.1.2 private www.employee.com
[Router-employee] quit
[Router] v-gateway employee max-user 200
[Router] v-gateway employee cur-max-user 50
[Router] v-gateway employee max-resource 1024
```

3. 配置用户认证

配置认证方案。

```
[Router] aaa
[Router-aaa] authentication-scheme employee.scm
[Router-aaa-authen-employee.scm] authentication-mode vpndb
[Router-aaa-authen-employee.scm] quit
```

配置授权方案。

```
[Router-aaa] authorization-scheme employee.scm
[Router-aaa-author-employee.scm] authorization-mode vpndb
[Router-aaa-author-employee.scm] quit
```

配置域。

```
[Router-aaa] domain employee.dom
[Router-aaa-domain-employee.dom] authentication-scheme employee.scm
[Router-aaa-domain-employee.dom] authorization-scheme employee.scm
[Router-aaa-domain-employee.dom] quit
[Router-aaa] quit
```

配置用户组。

```
[Router] v-gateway employee
[Router-employee] vpndb
[Router-employee-vpndb] group rd description ForResearchAndDevelopment
[Router-employee-vpndb] group rd port-forwarding web-proxy enable
```

配置用户。

```
[Router-employee-vpndb] user tom 123456 123456
[Router-employee-vpndb] user tom group rd
[Router-employee-vpndb] user tony 654321 654321
[Router-employee-vpndb] user tony group rd
[Router-employee-vpndb] quit
```

4. 配置端口转发

```
[Router-employee] service
[Router-employee-service] port-forwarding enable
[Router-employee-service] port-forwarding resource ftp host-ip 192.168.100.10 21 ftp
[Router-employee-service] port-forwarding resource telnet host-ip 192.168.100.20 23
telnet
[Router-employee-service] port-forwarding resource notes any 1600 notes
[Router-employee-service] port-forwarding auto-start enable
[Router-employee-service] port-forwarding keep-alive enable
```

```
[Router-employee-service] quit
```

5. 配置策略

#配置针对虚拟网关的目的 IP 型默认策略。

```
[Router-employee] security
[Router-employee-security] policy-default-action deny user-dst-ip
[Router-employee-security] quit
```

配置针对用户组的目的 IP 型策略。

```
[Router-employee] vpndb
[Router-employee-vpndb] group rd policy permit dst-ip 192.168.100.10 255.255.255.255
port 21
[Router-employee-vpndb] group rd policy deny dst-ip 192.168.100.20 255.255.255.255 port
23
[Router-employee-vpndb] group rd policy permit dst-ip any port 1600
```

配置针对用户的目的 IP 型策略。

```
[Router-employee-vpndb] user tom policy permit dst-ip 192.168.100.20 255.255.255.255
port 23
```

6. 用户终端接入

出差员工在浏览器中输入地址 https://www.company.com，进入虚拟网关登录界面。输入用户名 tom 和密码 123456，单击“登录”，登录虚拟网关。然后在“端口转发”区域框中，选择相应的资源进行访问。

----结束

配置文件

Router 配置文件：

```
#
 sysname Router
#
 undo firewall session link-state check
#
#
v-gateway employee 200.1.1.2 private www.employee.com
#
#
radius-server template employee.tpl
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 200.1.1.2 255.255.255.0
#
aaa
 authentication-scheme default
 authentication-scheme employee.scm
  authentication-mode  vpndb
```

```
 #
 authorization-scheme default
 authorization-scheme employee.scm
  authorization-mode  vpndb
 #
 accounting-scheme default
 #
 domain default
 domain employee.dom
  authentication-scheme  employee.scm
  authorization-scheme employee.scm
  radius-server employee.tpl
  ldap-server employee.tpl
 #
#
 ip route-static 0.0.0.0 0.0.0.0 200.1.1.1
#
v-gateway employee ip address 200.1.1.2
#****BEGIN***employee**1****#
v-gateway employee
 basic
  ssl version allversion
  ssl timeout 5
  ssl lifecycle 1440
  ssl ciphersuit custom aes256-sha des-cbc3-sha rc4-sha rc4-md5 aes128-sha des-c
bc-sha
  logoname &logo&.gif
  welcome &welcome&.txt
  title &title&.txt
 service
  port-forwarding enable
  port-forwarding keep-alive enable
  port-forwarding auto-start enable
  port-forwarding resource ftp host-ip 192.168.100.10 21 ftp
  port-forwarding resource telnet host-ip 192.168.100.20 23 telnet
  port-forwarding resource notes any 1600 notes
  network-extension mode split
 security
  policy-default-action permit user-src-ip
  policy-default-action deny user-dst-ip
  policy-default-action permit user-url
  policy-default-action permit vg-src-ip
  password-setting password-intension low 1 high 31 digits 0 letters 0 unmix
  password-setting safepolicy 1
  password-setting lifetime 0 alarm 0
  certification cert-anonymous cert-field user-filter subject cn group-filter su
bject cn
  certification cert-anonymous filter-policy permit-all
  certification cert-challenge cert-field user-filter subject cn
#****END****#
#

return
```

5 虚拟园区网部署

5.1 概述

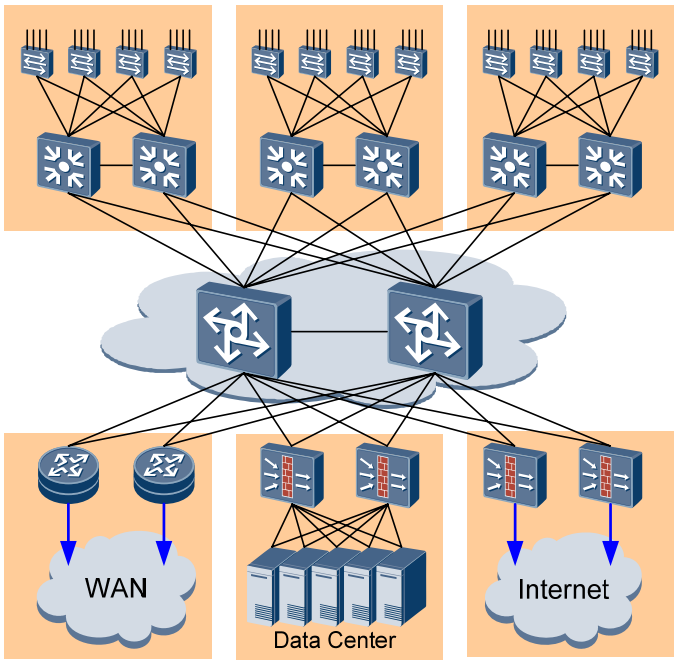
5.1.1 虚拟园区网简介

概述

当前的园区网建设，采取的组网形式主要是分层、分模块的部署模式，如图 5-1 所示。

- 分层部署就是将网络按接入、汇聚、核心规划为多层结构，各层网络部署不同的功能特性，使网络结构清晰，便于扩展。
- 接入层网络一般采用二层设计将用户的三层网关设置在汇聚层设备上，为了保证节点的可靠性性，汇聚层和核心层采用双节点组网。
- 园区网的模块化设计是指以企业的物理结构或逻辑结构，采用统一的设计方式，形成模块化的网络结构，这样设计使园区网的管理及扩展更加的容易。

图5-1 传统的园区网组网结构



但是，随着业务的发展，这种经典的园区网设计也逐渐体现出一些不足，主要表现为：

- 汇聚层、核心层的双节点冗余设计，虽然提高了网络的可靠性，但是也使得网络结构和互联关系变得复杂，网络的扩展也变得困难。
- 冗余结构使得网络的树形结构中出现环路，并且随着企业的不断发展，环网规模不断扩大。因此一般都需要部署 MSTP 等协议消除环路，同时运行 VRRP 等来支持节点冗余备份，导致网络协议的部署变得复杂。
- 不同部门/群组用户的资源访问权限需要进行控制，不同业务间的访问、传输和应用也需要进行端到端的隔离。但是传统的物理隔离技术已经无法满足这种需求，导致网络重复建设、管理分散、安全策略难以部署。

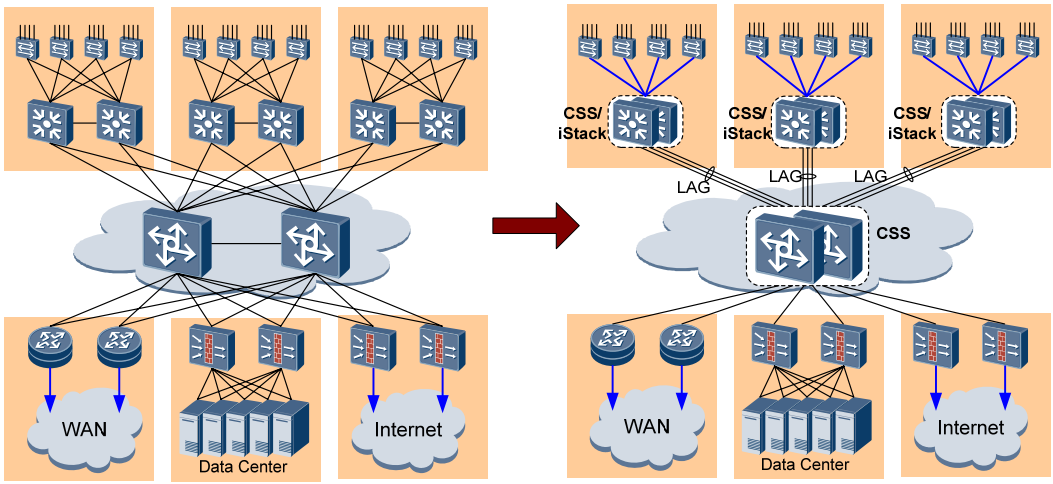
为了解决上述问题，华为公司提出了虚拟园区网解决方案，来解决上述问题。虚拟园区网是指把共用的一套物理网络、客户端、服务器资源虚拟出多套逻辑资源，供不同的群组/部门、业务使用，虽然在物理上这些资源是统一、集中的，但对不同的用户/业务来说，能够使用到的资源、配置的安全/管理策略可能各不相同。

虚拟园区网解决方案包括横向虚拟化方案和纵向虚拟化方案两部分。

横向虚拟化方案

横向虚拟化方案是指在园区网的核心层、汇聚层、接入层分别采用集群/堆叠技术，将多台物理设备虚拟化成单台逻辑设备，达到简化网络结构、简化网络协议部署、提高网络可靠性和可管理性的目的。横向虚拟化方案如图 5-2 所示。

图5-2 横向虚拟化方案



在横向虚拟化方案中：

- 在核心层采用 CSS（Cluster Switch System）技术，将多台核心交换机（S9300）组合成一台逻辑设备。
- 在汇聚层和接入层，采用 CSS 或者 iStack 堆叠技术，将多台汇聚/接入交换机组合成一台虚拟的逻辑交换机。
- 互联方面，可采用 LAG（Link Aggregation Group）技术，将多个物理接口捆绑在一起作为一个逻辑接口来增加带宽。

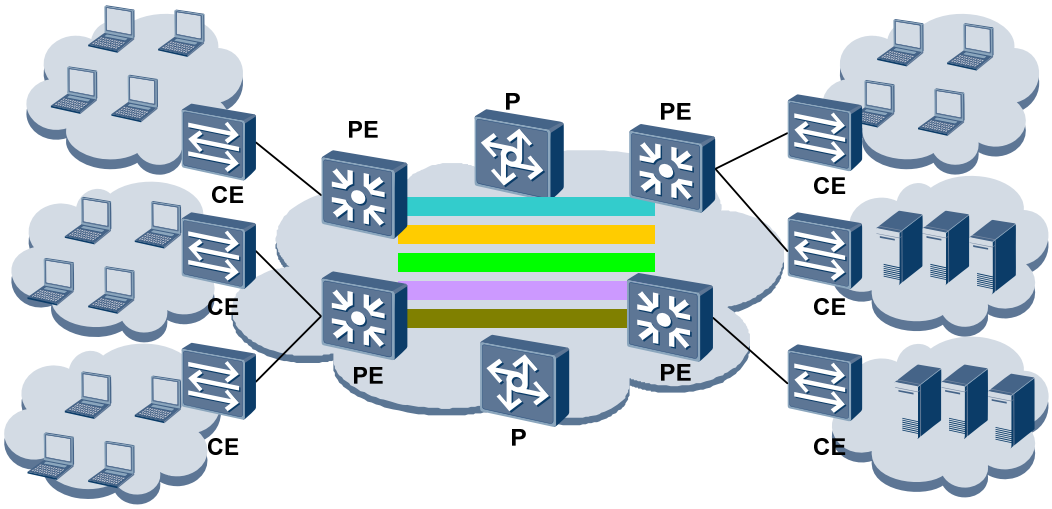
纵向虚拟化方案

纵向虚拟化方案是通过各种隔离技术，将一个物理网络划分成几个相互独立的逻辑网络，实现了终端和业务的安全隔离、应用资源的按需分配等。

对园区内共用一个物理网络传输各种应用数据的横向逻辑隔离，有 VLAN、隧道、MCE、VPN 等多种方式，但从业务隔离灵活性、配置管理复杂度、扩展性、组网对设备的要求等多方面综合对比，MPLS L3VPN 技术最适合应用在大、中型园区内进行业务隔离。

在园区网中，通过三层交换机可以构建 MPLS VPN 网络，承载所有业务的传输数据，并进行安全隔离。如图 5-3 所示。

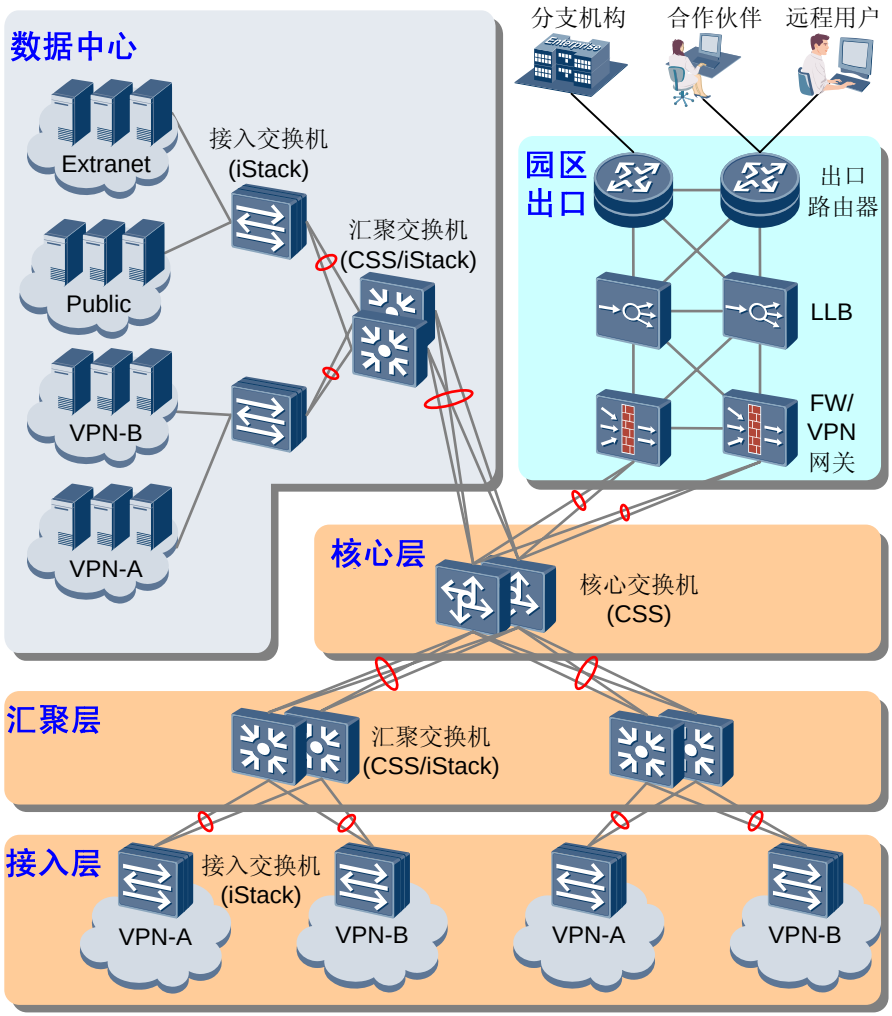
图5-3 MPLS L3VPN 网络



5.1.2 典型组网

虚拟园区网的典型组网如图 5-4 所示。

图5-4 虚拟园区网典型组网



在虚拟园区网的典型组网中，接入、汇聚、核心层采用支持堆叠/集群功能的交换机，组成堆叠/集群系统，将多台设备虚拟化为单台逻辑设备，简化网络结构，消除环路，实现横向虚拟化。

在纵向虚拟化（MPLS VPN 隔离）方面，根据接入和汇聚层设备的不同情况，有三种不同的 MPLS L3VPN 部署方案：

- 汇聚层设备支持 MPLS，并且每个接入交换机下只接入一个 VPN，则汇聚层设备作为 PE 来部署 MPLS VPN，核心层设备只作为 P 设备。
- 汇聚层设备支持 MPLS，并且每个接入交换机下可接入多个 VPN，则汇聚层设备作为 PE 来部署 MPLS VPN，核心层设备只作为 P 设备，同时接入交换机上部署 MCE 功能（需要接入交换机支持 MCE 功能），实现不同 VPN 的接入。
- 汇聚层设备不支持 MPLS，则核心层设备作为 PE 来部署 MPLS VPN，汇聚层设备上部署 MCE 功能（需要汇聚层设备支持 MCE 功能），实现不同 VPN 的接入。

5.1.3 配套版本

表5-1 虚拟园区网配套产品和版本

部件	产品	版本
接入交换机	S2700/S3700 系列（如果接入层需要部署MCE，则不能选用 S2700 系列）	V100R006C01
汇聚交换机	S5700（不包括 S5700SI）系列 S9300 系列	V100R006C01
核心交换机	S9300 系列	V100R006C01

5.1.4 部署思路

前置任务

- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- 接入、汇聚、核心层设备已插入堆叠/集群插卡，并通过堆叠/集群线缆连接。
- 完成 VLAN/SSID、IP 地址、VPN 的 RD 和 vpn-target 等数据的规划。

配置思路

配置思路	配置注意事项
配置堆叠/集群系统	S2700/S3700/S5700 系列的交换机，堆叠系统可以自动建立。 对于 S9300 系列的交换机，集群系统的建立需要手工使能。
配置 MPLS L3VPN	• 如果汇聚层不支持 MPLS，则把核心层设备作为 PE 来配置 MPLS L3VPN。 • 如果汇聚层支持 MPLS，则把汇聚层设备作为 PE 配置 MPLS L3VPN，而核心层仅作为 P 设备。 • 如果需要实现数据传输的高可靠性，可以配置 MPLS TE 隧道（CR-LSP）来取代普通的 LDP LSP 来承载 VPN 业务。 • 如果要实现 VPN 之间的单向访问/双向互访等需求，可以通过灵活配置 VPN 实例的 vpn-target 属性来实现。
配置 MCE 功能	• 如果汇聚层设备不支持 MPLS，则需要部署 MCE 功能，实现不同 VPN 的接入。 • 如果汇聚层设备支持 MPLS，但是每个接入交换机下接入多个 VPN，则需要在接入交换机上部署 MCE 功能，实现不同 VPN 的接入。

5.2 配置堆叠/集群系统

5.2.1 配置 iStack 系统

对于接入层和汇聚层的 S2700/S3700/S5700 系列的交换机，只要各交换机都插入堆叠卡，并且使用堆叠线缆正确连接，则各交换机上电之后，会自动建立 iStack 堆叠系统，而无需进行手工使能或配置。

以下介绍的是一些 iStack 功能的一些可选配置内容：

- 缺省情况下，交换机的堆叠功能是使能的。
  如果堆叠功能被去使能，则可以在系统视图下使用 **stack enable** 命令，使能交换机的堆叠功能。
- 缺省情况下，如果交换机的堆叠 ID 未配置，则交换机的堆叠 ID 是在堆叠系统建立时，由堆叠系统自动分配。
  如果想手工交换机的堆叠 ID，则可以在系统视图下执行 **stack slot** *slot-id* **renumber** *new-slot-id* 命令，配置设备的堆叠 ID。
- 缺省情况下，堆叠系统的主交换机选举是自动进行的。
  如果想人工调整堆叠系统的交换机选举结果，则可以在系统视图下执行 **stack slot** *slot-id* **priority** *priority*，配置指定堆叠设备的优先级。

说明

以上命令在未建立堆叠时，可以在各交换机上配置。如果堆叠已建立，则只能在主交换机上配置。

5.2.2 配置 CSS 系统

背景信息

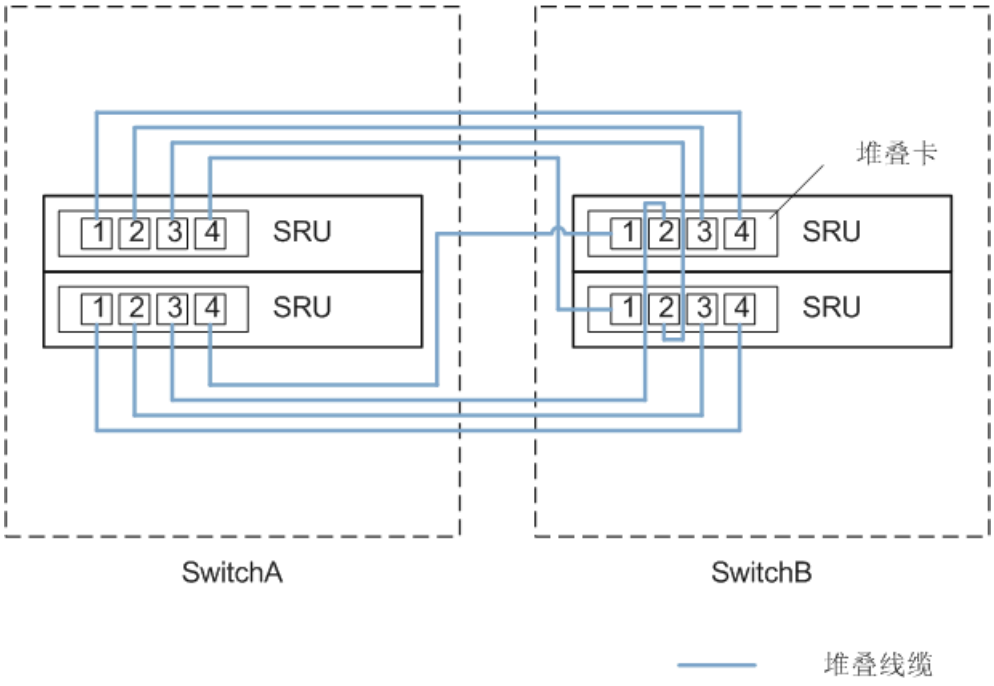
对于汇聚层和核心层的 S9300 系列交换机来说，需要通过手工配置使能 CSS 功能，然后两台交换机才会自动建立 CSS 系统。

说明

要建立 CSS 系统，必须满足如下条件：

- 设备型号为 S9306 或者 S9312，不能是 S9303。
- 每台设备上配置两块相同的主控板（SRUA 或 SRUB），两台设备之间可以不同。
- 在每块主控板上都插入堆叠卡。（四个插口）
- 两台设备之间采用专用的 QSFP（Quad Small Form-Factor Pluggable）高速线缆，按照图 5-5 所示线序，将两台设备进行连接。

图5-5 堆叠线缆连接规则



操作步骤

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **set css** { **id** *new-id* | **priority** *priority* } [**frame** *frame-id*]，设置堆叠机框的 ID 或堆叠机框竞争的优先级。
3. （可选）执行命令 **css master force** [**frame** *frame-id*]，强制指定交换机在堆叠系统中作为堆叠主交换机。
4. 执行命令 **css enable**，使能设备的堆叠功能。

----结束

5.3 配置 MPLS L3VPN

5.3.1 配置 IP 地址和 IGP

按照规划配置各设备的物理接口和 Loopback 接口的 IP 地址，具体的配置过程略。

按照规划在 PE 设备和 P 设备上配置 IGP（如果是在核心层部署 MPLS L3VPN，则可能没有 P 设备）。IGP 可以选择 OSPF 或者 IS-IS，具体的配置过程略。

5.3.2 使能 MPLS 基本能力

请在 PE 和 P 节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls lsr-id** *lsr-id*，配置本节点的 LSR ID。
3. 执行命令 **mpls**，使能本节点的 MPLS 功能，并进入 MPLS 视图。
4. 执行命令 **quit**，返回系统视图。
5. 执行命令 **mpls ldp**，使能全局的 LDP 功能，并进入 MPLS-LDP 视图。
6. 执行命令 **quit**，返回系统视图。
7. 执行命令 **interface vlanif** *interface-number*，进入 VLANIF 接口视图。
8. 执行命令 **mpls**，使能接口的 MPLS 功能。
9. 执行命令 **mpls ldp**，使能接口的 LDP 功能。

说明

如果所有的 VPN 业务都是用 MPLS TE 隧道来承载，则可以不使能 LDP，而是使用 RSVP-TE 作为隧道建立的信令协议。

----结束

5.3.3（可选）配置 MPLS TE 隧道

如果需要使用可靠性较高的基于 RSVP-TE 的 MPLS TE 隧道，而不是普通的 LDP LSP 来承载 VPN 业务，则需要执行本任务。

使能 MPLS TE 和 RSVP-TE

请在所有 PE 和 P 节点上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **mpls**，进入 MPLS 视图。
3. 执行命令 **mpls te**，使能本节点的 MPLS TE 功能。
4. 执行命令 **mpls rsvp-te**，使能本节点的 RSVP-TE 功能。
5. 执行命令 **mpls te cspf**，使能本节点的 CSPF 功能。
6. 执行命令 **quit**，返回系统视图。
7. 执行命令 **interface vlanif** *interface-number*，进入 VLANIF 接口视图。

说明

这里的 VLANIF 接口是指 MPLS TE 隧道两端的物理接口所属的 VLANIF 接口。

8. 执行命令 **mpls te**，使能接口的 MPLS TE 功能。
9. 执行命令 **mpls rsvp-te**，在接口上使能 RSVP-TE 功能。

----结束

（可选）使能 IGP TE

如果不配置 IGP TE（OSPF TE 或 IS-IS TE），则网络中不能形成 TEDB。此时生成的 CR-LSP 是由 IGP（OSPF 或 IS-IS）路由计算得到的，而非 CSPF 计算得到。为了使 CR-LSP 由 CSPF 计算生成，需要使能 IGP-TE。

对于 OSPF，请在所有 PE 和 P 节点上进行如下配置。

a. 执行命令 **system-view**，进入系统视图。

b. 执行命令 **ospf** [*process-id*]，进入 OSPF 视图。

c. 执行命令 **opaque-capability enable**，使能 OSPF 的 Opaque 能力。

d. 执行命令 **area** *area-id*，进入 OSPF 的区域视图。

e. 执行命令 **mpls-te enable** [**standard-complying**]，在当前 OSPF 区域使能 TE。

对于 IS-IS，请在所有 PE 和 P 节点上进行如下配置。

a. 执行命令 **system-view**，进入系统视图。

b. 执行命令 **isis** [*process-id*]，进入 IS-IS 协议视图。

c. 执行命令 **cost-style** { **compatible** [**relax-spf-limit**] | **wide** | **wide-compatible** }，配置 IS-IS 的 Wide Metric 属性。

d. 执行命令 **traffic-eng** [**level-1** | **level-2** | **level-1-2**]，使能 IS-IS TE。

创建并配置 MPLS TE 隧道

说明

对于堆叠/集群系统，Tunnel 接口请在堆叠/集群系统中进行配置，不要配置在单台成员交换机上，避免因物理故障导致 Tunnel 接口故障。

请在隧道的入节点（例如 PE 节点）上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface tunnel** *tunnel-number*，创建 Tunnel 接口，并进入 Tunnel 接口视图。
3. 执行命令 **ip address unnumbered interface loopback** *interface-number*，配置隧道接口借用环回接口的 IP 地址。
4. 执行命令 **tunnel-protocol mpls te**，配置隧道协议为 MPLS TE。
5. 执行命令 **destination** *ip-address*，配置隧道的目的地址（出节点的 LSR ID）。
6. 执行命令 **mpls te tunnel-id** *tunnel-id*，配置隧道 ID。
7. 执行命令 **mpls te signal-protocol rsvp-te**，配置隧道使用 RSVP-TE 作为信令协议。
8. 执行命令 **mpls te reserved-for-binding**，使能隧道的 VPN 绑定。
9. 执行命令 **mpls te commit**，提交隧道当前配置。

----结束

创建隧道策略

请在隧道的入节点（例如 PE 节点）上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **tunnel-policy** *policy-name*，创建隧道策略，并进入隧道策略视图。
3. 执行命令 **tunnel binding destination** *dest-ip-address* **te tunnel** *interface-number*，将对端地址与隧道策略绑定，使从本端到目的地址的 VPN 数据从绑定的隧道上传输。

----结束

5.3.4 配置 VPN 实例

在接入 CE 的 PE 设备上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ip vpn-instance** *vpn-instance-name*，创建 VPN 实例，并进入 VPN 实例视图。
3. 执行命令 **ipv4-family**，使能 VPN 实例 IPv4 地址族，并进入 VPN 实例 IPv4 地址族视图。
4. 执行命令 **route-distinguisher** *route-distinguisher*，配置 VPN 实例 IPv4 地址族的 RD。
5. 执行命令 **vpn-target** *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]，为 VPN 实例 IPv4 地址族配置 VPN-target 扩展团体属性。
6. （可选）执行命令 **tnl-policy** *policy-name*，对 VPN 实例 IPv4 地址族应用隧道策略。

----结束

5.3.5 在接口上绑定 VPN 实例

在接入 CE 的 PE 设备上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface vlanif** *interface-number*，进入要绑定 VPN 实例的接口视图。
3. 执行命令 **ip binding vpn-instance** *vpn-instance-name*，将当前接口与 VPN 实例绑定。
4. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IP 地址。

----结束

5.3.6 在 PE 之间建立 MP-IBGP 对等体

在接入 CE 的 PE 设备上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
3. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将对端 PE 配置为对等体。

4. 执行命令 **peer** *ipv4-address* **connect-interface loopback** *interface-number*，指定建立 TCP 连接的接口。
5. 执行 **ipv4-family vpnv4**，进入 BGP-VPNv4 子地址族视图。
6. 执行 **peer** *ipv4-address* **enable**，使能对等体交换 VPNv4 路由信息的能力。

----结束

5.3.7 配置 PE 和 CE/MCE 之间的路由交互

PE 和 CE/MCE 间的路由交互可以采用 EBGP、IBGP、静态路由、RIP、OSPF、ISIS，任选一种即可。以下过程以 EBGP 为例进行描述，其余方式请参考相应产品的文档中关于 VPN 的配置指导。

在 PE 上配置 EBGP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
3. 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP-VPN 实例 IPv4 地址族视图。
4. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将 CE 配置为 VPN 私网对等体。
5. （可选）执行命令 **import-route direct** [**med** *med* | **route-policy** *route-policy-name*]*，引入到本地 CE 的直连路由。

----结束

在 CE/MCE 上配置 EBGP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
3. （可选）如果是 MCE 设备，执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP-VPN 实例视图。
4. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将 PE 配置为对等体。
5. 执行命令 **import-route** { **direct** | **static** | **rip** *process-id* | **ospf** *process-id* | **isis** *process-id* } [**med** *med* | **route-policy** *route-policy-name*]*，引入本站点的路由。

----结束

5.4 配置 MCE

如前所述，如果汇聚层设备不支持 MPLS，则核心层设备作为 PE 来部署 MPLS VPN，汇聚层设备上可以部署 MCE 功能（需要汇聚层设备支持 MCE 功能），实现不同 VPN 的接入。

或者汇聚层设备支持 MPLS，但是每个接入交换机下可接入多个 VPN，则汇聚层设备作为 PE 来部署 MPLS VPN，核心层设备只作为 P 设备，同时接入交换机上部署 MCE 功能（需要接入交换机支持 MCE 功能），实现不同 VPN 的接入。

本节介绍作为 MCE 的汇聚交换机或接入交换机上如何配置 MCE 功能。

5.4.1 配置 VPN 实例

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **ip vpn-instance** *vpn-instance-name*，创建 VPN 实例，并进入 VPN 实例视图。
3. 执行命令 **route-distinguisher** *route-distinguisher*，配置 VPN 实例 IPv4 地址族的 RD。

----结束

说明

由于 MCE 下接入多个 VPN，所以请根据需要创建多个 VPN 实例。

5.4.2 在接口上绑定 VPN 实例

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface vlanif** *interface-number*，进入要绑定 VPN 实例的 VLAN 接口视图。
3. 执行命令 **ip binding vpn-instance** *vpn-instance-name*，将当前接口与 VPN 实例绑定。
4. 执行命令 **ip address** *ip-address* { *mask* | *mask-length* }，配置接口的 IP 地址。

----结束

5.4.3 配置 PE 和 MCE 之间的路由交互

请参见“5.3.7 配置 PE 和 CE/MCE 之间的路由交互”。

5.4.4 配置 MCE 和 CE 之间的路由交互

MCE 与 CE 之间的路由交互可以采用 EBGP、IBGP、静态路由、RIP、OSPF、ISIS，任选一种即可。以下过程以 EBGP 为例进行描述，其余方式请参考相应产品的文档中关于 VPN 的配置指导。

在 MCE 上配置 EBGP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
3. 执行命令 **ipv4-family vpn-instance** *vpn-instance-name*，进入 BGP-VPN 实例 IPv4 地址族视图。
4. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将 CE 配置为 VPN 私网对等体。

5. （可选）执行命令 **import-route direct** [**med** *med* | **route-policy** *route-policy-name*]*，引入到本地 CE 的直连路由。

----结束

在 CE 上配置 EBGP

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **bgp** *as-number*，进入 BGP 视图。
3. 执行命令 **peer** *ipv4-address* **as-number** *as-number*，将 PE 配置为对等体。
4. 执行命令 **import-route** { **direct** | **static** | **rip** *process-id* | **ospf** *process-id* | **isis** *process-id* } [**med** *med* | **route-policy** *route-policy-name*]*，引入本站点的路由。

----结束

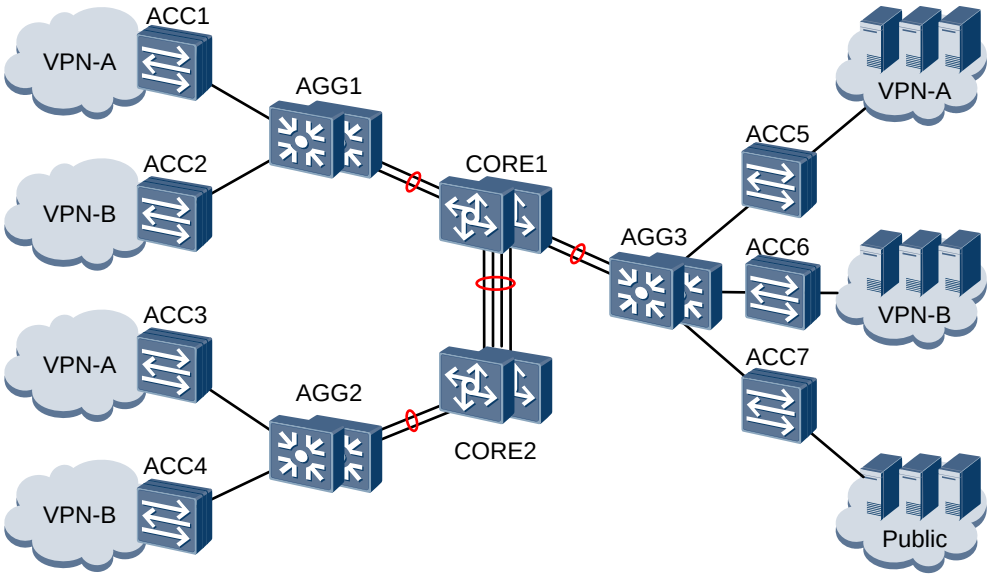
5.5 配置举例

组网需求

企业信息网络中，接入、汇聚、核心层采用支持堆叠/集群功能的交换机，组成堆叠/集群系统。同时，企业中的接入汇聚层，根据部门设置，将用户划分为 VPN-A 和 VPN-B，对于数据中心，同样划分为 VPN-A 的服务器群和 VPN-B 的服务器群，另有公共的服务器群，可供所有的用户同时访问。如图 5-6 所示。

在该组网中，由于汇聚层设备不支持 MPLS，因此只在核心层设备上配置 MPLS L3VPN，而在汇聚层部署 MCE 功能，负责汇聚接入多个 VPN。

图5-6 虚拟园区网配置组网图



数据准备

表5-2 数据规划表

配置项	配置子项	数据
接口和 VLAN	ACC1	To AGG1：GE0/0/1，VLAN 11
	ACC2	To AGG1：GE0/0/1，VLAN 22
	ACC3	To AGG2：GE0/0/1，VLAN 11
	ACC4	To AGG2：GE0/0/1，VLAN 22
	ACC5	To AGG3：GE0/0/1，VLAN 11
	ACC6	To AGG3：GE0/0/1，VLAN 22
	ACC7	To AGG3：GE0/0/1，VLAN 33
	AGG1	To ACC1：GE1/0/1，VLAN 11 To ACC2：GE2/0/1，VLAN 22 To CORE1：Eth-Trunk1（GE1/0/24、GE2/0/24），VLAN 101 202
	AGG2	To ACC3：GE1/0/1，VLAN 11 To ACC4：GE2/0/1，VLAN 22 To CORE2：Eth-Trunk1（GE1/0/24、GE2/0/24），VLAN 101 202
	AGG3	To ACC5：GE1/0/1，VLAN 11 To ACC6：GE2/0/1，VLAN 22 To ACC7：GE3/0/1，VLAN 33 To CORE1：Eth-Trunk3（GE1/0/24、GE2/0/24），VLAN 111 222 333
	CORE1	To AGG1：Eth-Trunk1（GE1/1/0/24、GE2/1/0/24），VLAN 101 202 To AGG3：Eth-Trunk3（GE1/2/0/24、GE2/2/0/24），VLAN 111 222 333 To CORE2：Eth-Trunk2（GE1/3/0/23、GE1/3/0/24、GE2/3/0/23、GE2/3/0/24），VLAN 100
	CORE2	To AGG2：Eth-Trunk1（GE1/1/0/24、GE2/1/0/24），VLAN 101 202 To CORE1：Eth-Trunk2（GE1/3/0/23、GE1/3/0/24、GE2/3/0/23、GE2/3/0/24），VLAN 100

配置项	配置子项	数据
IP 地址	AGG1	VLANIF 11：192.168.1.11/24 VLANIF 22：192.168.2.11/24 VLANIF 101：192.168.11.11/24 VLANIF 202：192.168.22.11/24
	AGG2	VLANIF 11：192.168.3.11/24 VLANIF 22：192.168.4.11/24 VLANIF 101：192.168.33.11/24 VLANIF 202：192.168.44.11/24
	AGG3	VLANIF 11：192.168.5.11/24 VLANIF 22：192.168.6.11/24 VLANIF 33：192.168.7.11/24 VLANIF 111：192.168.55.11/24 VLANIF 222：192.168.66.11/24 VLANIF 333：192.168.77.11/24
	CORE1	VLANIF 101：192.168.11.12/24 VLANIF 202：192.168.22.12/24 VLANIF 111：192.168.55.12/24 VLANIF 222：192.168.66.12/24 VLANIF 333：192.168.77.12/24 VLANIF 100：100.1.1.1/24 Loopback0：1.1.1.1/32
	CORE2	VLANIF 101：192.168.33.12/24 VLANIF 202：192.168.44.12/24 VLANIF 100：100.1.1.2/24 Loopback0：2.2.2.2/32
VPN	VPN-A	VLAN：11、101、111 OSPF 进程号：11 RD：11:1 VPN-Target（Export）：11:1 VPN-Target（Import）：11:1

配置项	配置子项	数据
	VPN-B	VLAN：22、202、222 OSPF 进程号：22 RD：22:1 VPN-Target（Export）：22:1 VPN-Target（Import）：22:1
	VPN-Public	VLAN：33、333 OSPF 进程号：33 RD：33:1 VPN-Target（Export）：11:1 22:1 VPN-Target（Import）：11:1 22:1

操作步骤

1. 配置 CORE1 和 CORE2 的 CSS 集群。

   # 在 CORE1 的主交换机上配置 CSS 集群。

   ```
   <CORE1> system-view
   [CORE1] set css priority 255
   [CORE1] css enable
   ```

   # 在 CORE1 的从交换机上配置 CSS 集群。

   ```
   <CORE1_S> system-view
   [CORE1_S] set css id 2
   [CORE1_S] css enable
   ```

   配置之后，CORE1 集群建立，后续的配置都在主交换机上进行。

   CORE2 的配置与之相同。

   说明

   对于其余交换机设备，只要各交换机都插入堆叠卡，并且使用堆叠线缆正确连接，则各交换机上电之后，会自动建立 iStack 堆叠系统，无需进行配置。

2. 配置接口和 VLAN。

   # 配置接入交换机 ACC1 的接口和 VLAN。

   ```
   <ACC1> system-view
   [ACC1] vlan batch 11
   [ACC1] interface GigabitEthernet 0/0/1
   [ACC1-GigabitEthernet0/0/1] port link-type trunk
   [ACC1-GigabitEthernet0/0/1] port trunk allow-pass vlan 11
   [ACC1-GigabitEthernet0/0/1] quit
   ```

   其余接入交换机的配置与之类似，其中 ACC3、ACC5 的 VLAN 也是 11，ACC2、ACC4、ACC6 的 VLAN 是 22，ACC7 的 VLAN 是 33。

配置汇聚交换机 AGG1 的接口和 VLAN。

```
<AGG1> system-view
[AGG1] vlan batch 11 22 101 202
[AGG1] interface GigabitEthernet 1/0/1
[AGG1-GigabitEthernet1/0/1] port link-type trunk
[AGG1-GigabitEthernet1/0/1] port trunk allow-pass vlan 11
[AGG1-GigabitEthernet1/0/1] quit
[AGG1] interface GigabitEthernet 2/0/1
[AGG1-GigabitEthernet2/0/1] port link-type trunk
[AGG1-GigabitEthernet2/0/1] port trunk allow-pass vlan 22
[AGG1-GigabitEthernet2/0/1] quit
[AGG1] interface Eth-Trunk 1
[AGG1-Eth-Trunk1] port link-type trunk
[AGG1-Eth-Trunk1] port trunk allow-pass vlan 101 202
[AGG1-Eth-Trunk1] mode lacp-static
[AGG1-Eth-Trunk1] load-balance src-mac
[AGG1-Eth-Trunk1] quit
[AGG1] interface GigabitEthernet 1/0/24
[AGG1-GigabitEthernet1/0/24] Eth-Trunk 1
[AGG1-GigabitEthernet1/0/24] quit
[AGG1] interface GigabitEthernet 2/0/24
[AGG1-GigabitEthernet2/0/24] Eth-Trunk 1
[AGG1-GigabitEthernet2/0/24] quit
[AGG1] interface vlanif 11
[AGG1-Vlanif11] quit
[AGG1] interface vlanif 22
[AGG1-Vlanif22] quit
[AGG1] interface vlanif 101
[AGG1-Vlanif101] quit
[AGG1] interface vlanif 202
[AGG1-Vlanif202] quit
```

配置汇聚交换机 AGG2 的接口和 VLAN。

```
<AGG2> system-view
[AGG2] vlan batch 11 22 101 202
[AGG2] interface GigabitEthernet 1/0/1
[AGG2-GigabitEthernet1/0/1] port link-type trunk
[AGG2-GigabitEthernet1/0/1] port trunk allow-pass vlan 11
[AGG2-GigabitEthernet1/0/1] quit
[AGG2] interface GigabitEthernet 2/0/1
[AGG2-GigabitEthernet2/0/1] port link-type trunk
[AGG2-GigabitEthernet2/0/1] port trunk allow-pass vlan 22
[AGG2-GigabitEthernet2/0/1] quit
[AGG2] interface Eth-Trunk 1
[AGG2-Eth-Trunk1] port link-type trunk
[AGG2-Eth-Trunk1] port trunk allow-pass vlan 101 202
[AGG2-Eth-Trunk1] mode lacp-static
[AGG2-Eth-Trunk1] load-balance src-mac
[AGG2-Eth-Trunk1] quit
[AGG2] interface GigabitEthernet 1/0/24
[AGG2-GigabitEthernet1/0/24] Eth-Trunk 1
[AGG2-GigabitEthernet1/0/24] quit
[AGG2] interface GigabitEthernet 2/0/24
[AGG2-GigabitEthernet2/0/24] Eth-Trunk 1
```

```
[AGG2-GigabitEthernet2/0/24] quit
[AGG2] interface vlanif 11
[AGG2-Vlanif11] quit
[AGG2] interface vlanif 22
[AGG2-Vlanif22] quit
[AGG2] interface vlanif 101
[AGG2-Vlanif101] quit
[AGG2] interface vlanif 202
[AGG2-Vlanif202] quit
```

配置汇聚交换机 AGG3 的接口和 VLAN。

```
<AGG3> system-view
[AGG3] vlan batch 11 22 111 222 333
[AGG3] interface GigabitEthernet 1/0/1
[AGG3-GigabitEthernet1/0/1] port link-type trunk
[AGG3-GigabitEthernet1/0/1] port trunk allow-pass vlan 11
[AGG3-GigabitEthernet1/0/1] quit
[AGG3] interface GigabitEthernet 2/0/1
[AGG3-GigabitEthernet2/0/1] port link-type trunk
[AGG3-GigabitEthernet2/0/1] port trunk allow-pass vlan 22
[AGG3-GigabitEthernet2/0/1] quit
[AGG3] interface GigabitEthernet 3/0/1
[AGG3-GigabitEthernet3/0/1] port link-type trunk
[AGG3-GigabitEthernet3/0/1] port trunk allow-pass vlan 33
[AGG3-GigabitEthernet3/0/1] quit
[AGG3] interface Eth-Trunk 1
[AGG3-Eth-Trunk1] port link-type trunk
[AGG3-Eth-Trunk1] port trunk allow-pass vlan 111 222 333
[AGG3-Eth-Trunk1] mode lacp-static
[AGG3-Eth-Trunk1] load-balance src-mac
[AGG3-Eth-Trunk1] quit
[AGG3] interface GigabitEthernet 1/0/24
[AGG3-GigabitEthernet1/0/24] Eth-Trunk 1
[AGG3-GigabitEthernet1/0/24] quit
[AGG3] interface GigabitEthernet 2/0/24
[AGG3-GigabitEthernet2/0/24] Eth-Trunk 1
[AGG3-GigabitEthernet2/0/24] quit
[AGG3] interface vlanif 11
[AGG3-Vlanif11] quit
[AGG3] interface vlanif 22
[AGG3-Vlanif22] quit
[AGG3] interface vlanif 111
[AGG3-Vlanif111] quit
[AGG3] interface vlanif 222
[AGG3-Vlanif222] quit
[AGG3] interface vlanif 333
[AGG3-Vlanif333] quit
```

配置核心交换机 CORE1 的接口和 VLAN。

```
<CORE1> system-view
[CORE1] vlan batch 100 101 202 111 222 333
[CORE1] interface Eth-Trunk 1
[CORE1-Eth-Trunk1] port link-type trunk
[CORE1-Eth-Trunk1] port trunk allow-pass vlan 101 202
[CORE1-Eth-Trunk1] mode lacp-static
```

```
[CORE1-Eth-Trunk1] load-balance src-mac
[CORE1-Eth-Trunk1] lacp preempt enable
[CORE1-Eth-Trunk1] quit
[CORE1] interface GigabitEthernet 1/1/0/24
[CORE1-GigabitEthernet1/1/0/24] Eth-Trunk 1
[CORE1-GigabitEthernet1/1/0/24] quit
[CORE1] interface GigabitEthernet 2/1/0/24
[CORE1-GigabitEthernet2/1/0/24] Eth-Trunk 1
[CORE1-GigabitEthernet2/1/0/24] quit
[CORE1] interface Eth-Trunk 2
[CORE1-Eth-Trunk2] port link-type trunk
[CORE1-Eth-Trunk2] port trunk allow-pass vlan 100
[CORE1-Eth-Trunk2] quit
[CORE1] interface GigabitEthernet 1/3/0/23
[CORE1-GigabitEthernet1/3/0/23] Eth-Trunk 2
[CORE1-GigabitEthernet1/3/0/23] quit
[CORE1] interface GigabitEthernet 1/3/0/24
[CORE1-GigabitEthernet1/3/0/24] Eth-Trunk 2
[CORE1-GigabitEthernet1/3/0/24] quit
[CORE1] interface GigabitEthernet 2/3/0/23
[CORE1-GigabitEthernet2/3/0/23] Eth-Trunk 2
[CORE1-GigabitEthernet2/3/0/23] quit
[CORE1] interface GigabitEthernet 2/3/0/24
[CORE1-GigabitEthernet2/3/0/24] Eth-Trunk 2
[CORE1-GigabitEthernet2/3/0/24] quit
[CORE1] interface Eth-Trunk 3
[CORE1-Eth-Trunk3] port link-type trunk
[CORE1-Eth-Trunk3] port trunk allow-pass vlan 111 222 333
[CORE1-Eth-Trunk3] mode lacp-static
[CORE1-Eth-Trunk3] load-balance src-mac
[CORE1-Eth-Trunk3] lacp preempt enable
[CORE1-Eth-Trunk3] quit
[CORE1] interface GigabitEthernet 1/2/0/24
[CORE1-GigabitEthernet1/2/0/24] Eth-Trunk 3
[CORE1-GigabitEthernet1/2/0/24] quit
[CORE1] interface GigabitEthernet 2/2/0/24
[CORE1-GigabitEthernet2/2/0/24] Eth-Trunk 3
[CORE1-GigabitEthernet2/2/0/24] quit
[CORE1] interface vlanif 100
[CORE1-Vlanif100] quit
[CORE1] interface vlanif 101
[CORE1-Vlanif101] quit
[CORE1] interface vlanif 111
[CORE1-Vlanif111] quit
[CORE1] interface vlanif 202
[CORE1-Vlanif202] quit
[CORE1] interface vlanif 222
[CORE1-Vlanif222] quit
[CORE1] interface vlanif 333
[CORE1-Vlanif333] quit
```

配置核心交换机 CORE2 的接口和 VLAN。

```
<CORE2> system-view
[CORE2] vlan batch 100 101 202
[CORE2] interface Eth-Trunk 1
```

```
[CORE2-Eth-Trunk1] port link-type trunk
[CORE2-Eth-Trunk1] port trunk allow-pass vlan 101 202
[CORE2-Eth-Trunk1] mode lacp-static
[CORE2-Eth-Trunk1] load-balance src-mac
[CORE2-Eth-Trunk1] lacp preempt enable
[CORE2-Eth-Trunk1] quit
[CORE2] interface GigabitEthernet 1/1/0/24
[CORE2-GigabitEthernet1/1/0/24] Eth-Trunk 1
[CORE2-GigabitEthernet1/1/0/24] quit
[CORE2] interface GigabitEthernet 2/1/0/24
[CORE2-GigabitEthernet2/1/0/24] Eth-Trunk 1
[CORE2-GigabitEthernet2/1/0/24] quit
[CORE2] interface Eth-Trunk 2
[CORE2-Eth-Trunk2] port link-type trunk
[CORE2-Eth-Trunk2] port trunk allow-pass vlan 100
[CORE2-Eth-Trunk2] quit
[CORE2] interface GigabitEthernet 1/3/0/23
[CORE2-GigabitEthernet1/3/0/23] Eth-Trunk 2
[CORE2-GigabitEthernet1/3/0/23] quit
[CORE2] interface GigabitEthernet 1/3/0/24
[CORE2-GigabitEthernet1/3/0/24] Eth-Trunk 2
[CORE2-GigabitEthernet1/3/0/24] quit
[CORE2] interface GigabitEthernet 2/3/0/23
[CORE2-GigabitEthernet2/3/0/23] Eth-Trunk 2
[CORE2-GigabitEthernet2/3/0/23] quit
[CORE2] interface GigabitEthernet 2/3/0/24
[CORE2-GigabitEthernet2/3/0/24] Eth-Trunk 2
[CORE2-GigabitEthernet2/3/0/24] quit
[CORE2] interface vlanif 100
[CORE2-Vlanif100] quit
[CORE2] interface vlanif 101
[CORE2-Vlanif101] quit
[CORE2] interface vlanif 202
[CORE2-Vlanif202] quit
```

3. 配置 MCE。

   # 配置汇聚交换机 AGG1 上的 MCE 功能。

```
[AGG1] ip vpn-instance vpna
[AGG1-vpn-instance-vpna] route-distinguisher 11:1
[AGG1-vpn-instance-vpna] vpn-target 11:1 export-extcommunity
[AGG1-vpn-instance-vpna] vpn-target 11:1 import-extcommunity
[AGG1-vpn-instance-vpna] quit
[AGG1] ip vpn-instance vpnb
[AGG1-vpn-instance-vpnb] route-distinguisher 22:1
[AGG1-vpn-instance-vpnb] vpn-target 22:1 export-extcommunity
[AGG1-vpn-instance-vpnb] vpn-target 22:1 import-extcommunity
[AGG1-vpn-instance-vpnb] quit
[AGG1] interface vlanif 11
[AGG1-Vlanif11] ip binding vpn-instance vpna
[AGG1-Vlanif11] ip address 192.168.1.11 255.255.255.0
[AGG1-Vlanif11] quit
[AGG1] interface vlanif 22
[AGG1-Vlanif22] ip binding vpn-instance vpnb
[AGG1-Vlanif22] ip address 192.168.2.11 255.255.255.0
```

```
[AGG1-Vlanif22] quit
[AGG1] interface vlanif 101
[AGG1-Vlanif101] ip binding vpn-instance vpna
[AGG1-Vlanif101] ip address 192.168.11.11 255.255.255.0
[AGG1-Vlanif101] quit
[AGG1] interface vlanif 202
[AGG1-Vlanif202] ip binding vpn-instance vpnb
[AGG1-Vlanif202] ip address 192.168.22.11 255.255.255.0
[AGG1-Vlanif202] quit
```

配置汇聚交换机 AGG2 上的 MCE 功能。

```
[AGG2] ip vpn-instance vpna
[AGG2-vpn-instance-vpna] route-distinguisher 11:1
[AGG2-vpn-instance-vpna] vpn-target 11:1 export-extcommunity
[AGG2-vpn-instance-vpna] vpn-target 11:1 import-extcommunity
[AGG2-vpn-instance-vpna] quit
[AGG2] ip vpn-instance vpnb
[AGG2-vpn-instance-vpnb] route-distinguisher 22:1
[AGG2-vpn-instance-vpnb] vpn-target 22:1 export-extcommunity
[AGG2-vpn-instance-vpnb] vpn-target 22:1 import-extcommunity
[AGG2-vpn-instance-vpnb] quit
[AGG2] interface vlanif 11
[AGG2-Vlanif11] ip binding vpn-instance vpna
[AGG2-Vlanif11] ip address 192.168.3.11 255.255.255.0
[AGG2-Vlanif11] quit
[AGG2] interface vlanif 22
[AGG2-Vlanif22] ip binding vpn-instance vpnb
[AGG2-Vlanif22] ip address 192.168.4.11 255.255.255.0
[AGG2-Vlanif22] quit
[AGG2] interface vlanif 101
[AGG2-Vlanif101] ip binding vpn-instance vpna
[AGG2-Vlanif101] ip address 192.168.33.11 255.255.255.0
[AGG2-Vlanif101] quit
[AGG2] interface vlanif 202
[AGG2-Vlanif202] ip binding vpn-instance vpnb
[AGG2-Vlanif202] ip address 192.168.44.11 255.255.255.0
[AGG2-Vlanif202] quit
```

配置汇聚交换机 AGG3 上的 MCE 功能。

```
[AGG3] ip vpn-instance vpna
[AGG3-vpn-instance-vpna] route-distinguisher 11:1
[AGG3-vpn-instance-vpna] vpn-target 11:1 export-extcommunity
[AGG3-vpn-instance-vpna] vpn-target 11:1 import-extcommunity
[AGG3-vpn-instance-vpna] quit
[AGG3] ip vpn-instance vpnb
[AGG3-vpn-instance-vpnb] route-distinguisher 22:1
[AGG3-vpn-instance-vpnb] vpn-target 22:1 export-extcommunity
[AGG3-vpn-instance-vpnb] vpn-target 22:1 import-extcommunity
[AGG3-vpn-instance-vpnb] quit
[AGG3] ip vpn-instance public
[AGG3-vpn-instance-public] route-distinguisher 33:1
[AGG3-vpn-instance-public] vpn-target 11:1 22:1 export-extcommunity
[AGG3-vpn-instance-public] vpn-target 11:1 22:1 import-extcommunity
[AGG3-vpn-instance-public] quit
[AGG3] interface vlanif 11
```

```
[AGG3-Vlanif11] ip binding vpn-instance vpna
[AGG3-Vlanif11] ip address 192.168.5.11 255.255.255.0
[AGG3-Vlanif11] quit
[AGG3] interface vlanif 22
[AGG3-Vlanif22] ip binding vpn-instance vpnb
[AGG3-Vlanif22] ip address 192.168.6.11 255.255.255.0
[AGG3-Vlanif22] quit
[AGG3] interface vlanif 33
[AGG3-Vlanif33] ip binding vpn-instance public
[AGG3-Vlanif33] ip address 192.168.7.11 255.255.255.0
[AGG3-Vlanif33] quit
[AGG3] interface vlanif 111
[AGG3-Vlanif111] ip binding vpn-instance vpna
[AGG3-Vlanif111] ip address 192.168.55.11 255.255.255.0
[AGG3-Vlanif111] quit
[AGG3] interface vlanif 202
[AGG3-Vlanif222] ip binding vpn-instance vpnb
[AGG3-Vlanif222] ip address 192.168.66.11 255.255.255.0
[AGG3-Vlanif222] quit
[AGG3] interface vlanif 303
[AGG3-Vlanif333] ip binding vpn-instance public
[AGG3-Vlanif333] ip address 192.168.77.11 255.255.255.0
[AGG3-Vlanif333] quit
```

4. 配置公网路由协议，实现互通。

   # 配置 CORE1 上的路由协议。

```
[CORE1] interface LoopBack 0
[CORE1-LoopBack0] ip address 1.1.1.1 32
[CORE1-LoopBack0] quit
[CORE1] interface Vlanif 100
[CORE1-Vlanif100] ip address 100.1.1.1 24
[CORE1-Vlanif100] quit
[CORE1] ospf 1
[CORE1-ospf-1] area 0
[CORE1-ospf-1-area-0.0.0.0] network 100.1.1.1 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[CORE1-ospf-1-area-0.0.0.0] quit
```

   # 配置 CORE2 上的路由协议。

```
[CORE2] interface LoopBack 0
[CORE2-LoopBack0] ip address 2.2.2.2 32
[CORE2-LoopBack0] quit
[CORE2] interface Vlanif 100
[CORE2-Vlanif100] ip address 100.1.1.2 24
[CORE2-Vlanif100] quit
[CORE2] ospf 1
[CORE2-ospf-1] area 0
[CORE2-ospf-1-area-0.0.0.0] network 100.1.1.2 0.0.0.255
[CORE2-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[CORE2-ospf-1-area-0.0.0.0] quit
```

5. 使能 MPLS。

   # 配置 CORE1 的 MPLS 和 LDP 功能。

```
[CORE1] mpls lsr-id 1.1.1.1
[CORE1] mpls
[CORE1-mpls] label advertise non-null
[CORE1-mpls] quit
[CORE1] interface Vlanif 100
[CORE1-Vlanif100] mpls
```

配置 CORE2 的 MPLS 和 LDP 功能。

```
[CORE2] mpls lsr-id 2.2.2.2
[CORE2] mpls
[CORE2-mpls] label advertise non-null
[CORE2-mpls] quit
[CORE2] interface Vlanif 100
[CORE2-Vlanif100] mpls
```

6. 配置 MPLS TE 隧道承载 VPN 业务。

配置 CORE1 的 MPLS TE 隧道。

```
[CORE1] mpls
[CORE1-mpls] mpls te
[CORE1-mpls] mpls rsvp-te
[CORE1-mpls] mpls te cspf
[CORE1-mpls] quit
[CORE1] ospf
[CORE1-ospf-1] opaque-capability enable
[CORE1-ospf-1] area 0
[CORE1-ospf-1-area-0.0.0.0] mpls-te enable
[CORE1-ospf-1-area-0.0.0.0] quit
[CORE1] interface Vlanif 100
[CORE1-Vlanif100] mpls te
[CORE1-Vlanif100] mpls rsvp-te
[CORE1-Vlanif100] quit
[CORE1] interface Tunnel0/0/0/1
[CORE1-Tunnel0/0/0/1] ip address unnumbered interface LoopBack0
[CORE1-Tunnel0/0/0/1] tunnel-protocol mpls te
[CORE1-Tunnel0/0/0/1] destination 2.2.2.2
[CORE1-Tunnel0/0/0/1] mpls te tunnel-id 22
[CORE1-Tunnel0/0/0/1] mpls te reserved-for-binding
[CORE1-Tunnel0/0/0/1] mpls te commit
[CORE1-Tunnel0/0/0/1] quit
[CORE1] tunnel-policy p1
[CORE1-tunnel-policy-p1] tunnel binding destination 2.2.2.2 te tunnel0/0/0/1
[CORE1-tunnel-policy-p1] quit
```

配置 CORE2 的 MPLS TE 隧道。

```
[CORE2] mpls
[CORE2-mpls] mpls te
[CORE2-mpls] mpls rsvp-te
[CORE2-mpls] mpls te cspf
[CORE2-mpls] quit
[CORE2] ospf
[CORE2-ospf-1] opaque-capability enable
[CORE2-ospf-1] area 0
[CORE2-ospf-1-area-0.0.0.0] mpls-te enable
```

```
[CORE2-ospf-1-area-0.0.0.0] quit
[CORE2] interface Vlanif 100
[CORE2-Vlanif100] mpls te
[CORE2-Vlanif100] mpls rsvp-te
[CORE2-Vlanif100] quit
[CORE2] interface Tunnel0/0/0/1
[CORE2-Tunnel0/0/0/1] ip address unnumbered interface LoopBack0
[CORE2-Tunnel0/0/0/1] tunnel-protocol mpls te
[CORE2-Tunnel0/0/0/1] destination 1.1.1.1
[CORE2-Tunnel0/0/0/1] mpls te tunnel-id 22
[CORE2-Tunnel0/0/0/1] mpls te reserved-for-binding
[CORE2-Tunnel0/0/0/1] mpls te commit
[CORE2-Tunnel0/0/0/1] quit
 [CORE2] tunnel-policy p1
[CORE2-tunnel-policy-p1] tunnel binding destination 1.1.1.1 te tunnel0/0/0/1
[CORE2-tunnel-policy-p1] quit
```

7. 配置 MPLS L3VPN。

   # 配置 CORE1 的 VPN 业务。

```
[CORE1] ip vpn-instance vpna
[CORE1-vpn-instance-vpna] route-distinguisher 11:1
[CORE1-vpn-instance-vpna] vpn-target 11:1 export-extcommunity
[CORE1-vpn-instance-vpna] vpn-target 11:1 import-extcommunity
[CORE1-vpn-instance-vpna] tnl-policy p1
[CORE1-vpn-instance-vpna] quit
[CORE1] ip vpn-instance vpnb
[CORE1-vpn-instance-vpnb] route-distinguisher 22:1
[CORE1-vpn-instance-vpnb] vpn-target 22:1 export-extcommunity
[CORE1-vpn-instance-vpnb] vpn-target 22:1 import-extcommunity
[CORE1-vpn-instance-vpnb] tnl-policy p1
[CORE1-vpn-instance-vpnb] quit
[CORE1] ip vpn-instance public
[CORE1-vpn-instance-public] route-distinguisher 33:1
[CORE1-vpn-instance-public] vpn-target 11:1 22:1 export-extcommunity
[CORE1-vpn-instance-public] vpn-target 11:1 22:1 import-extcommunity
[CORE1-vpn-instance-public] tnl-policy p1
[CORE1-vpn-instance-public] quit
[CORE1] interface vlanif 101
[CORE1-Vlanif101] ip binding vpn-instance vpna
[CORE1-Vlanif101] ip address 192.168.11.12 255.255.255.0
[CORE1-Vlanif101] quit
[CORE1] interface vlanif 202
[CORE1-Vlanif202] ip binding vpn-instance vpnb
[CORE1-Vlanif202] ip address 192.168.22.12 255.255.255.0
[CORE1-Vlanif202] quit
[CORE1] interface vlanif 111
[CORE1-Vlanif111] ip binding vpn-instance vpna
[CORE1-Vlanif111] ip address 192.168.55.12 255.255.255.0
[CORE1-Vlanif111] quit
[CORE1] interface vlanif 222
[CORE1-Vlanif222] ip binding vpn-instance vpnb
[CORE1-Vlanif222] ip address 192.168.66.12 255.255.255.0
[CORE1-Vlanif222] quit
[CORE1] interface vlanif 333
```

```
[CORE1-Vlanif333] ip binding vpn-instance public
[CORE1-Vlanif333] ip address 192.168.77.12 255.255.255.0
[CORE1-Vlanif333] quit
```

配置 CORE2 的 VPN 业务。

```
[CORE2] ip vpn-instance vpna
[CORE2-vpn-instance-vpna] route-distinguisher 11:1
[CORE2-vpn-instance-vpna] vpn-target 11:1 export-extcommunity
[CORE2-vpn-instance-vpna] vpn-target 11:1 import-extcommunity
[CORE2-vpn-instance-vpna] tnl-policy p1
[CORE2-vpn-instance-vpna] quit
[CORE2] ip vpn-instance vpnb
[CORE2-vpn-instance-vpnb] route-distinguisher 22:1
[CORE2-vpn-instance-vpnb] vpn-target 22:1 export-extcommunity
[CORE2-vpn-instance-vpnb] vpn-target 22:1 import-extcommunity
[CORE2-vpn-instance-vpnb] tnl-policy p1
[CORE2-vpn-instance-vpnb] quit
[CORE2] interface vlanif 101
[CORE2-Vlanif101] ip binding vpn-instance vpna
[CORE2-Vlanif101] ip address 192.168.33.12 255.255.255.0
[CORE2-Vlanif101] quit
[CORE2] interface vlanif 202
[CORE2-Vlanif202] ip binding vpn-instance vpnb
[CORE2-Vlanif202] ip address 192.168.44.12 255.255.255.0
[CORE2-Vlanif202] quit
```

8. 在 PE 间建立 MP-IBGP 对等体。

   # 配置 CORE1。

```
[CORE1] bgp 100
[CORE1-bgp] peer 2.2.2.2 as-number 100
[CORE1-bgp] peer 2.2.2.2 connect-interface LoopBack 0
[CORE1-bgp] ipv4-family vpnv4
[CORE1-bgp-af-vpnv4] peer 2.2.2.2 enable
[CORE1-bgp-af-vpnv4] quit
```

   # 配置 CORE2。

```
[CORE2] bgp 100
[CORE2-bgp] peer 1.1.1.1 as-number 100
[CORE2-bgp] peer 1.1.1.1 connect-interface LoopBack 0
[CORE2-bgp] ipv4-family vpnv4
[CORE2-bgp-af-vpnv4] peer 1.1.1.1 enable
[CORE2-bgp-af-vpnv4] quit
```

9. 配置 PE 和 MCE 之间的路由交互。

   # 配置 AGG1。

```
[AGG1] ospf 11 vpn-instance vpna
[AGG1-ospf-11] vpn-instance-capability simple
[AGG1-ospf-11] area 0
[AGG1-ospf-11-area-0.0.0.0] network 192.168.1.0 0.0.0.255
[AGG1-ospf-11-area-0.0.0.0] network 192.168.11.0 0.0.0.255
[AGG1-ospf-11-area-0.0.0.0] quit
[AGG1-ospf-11] quit
```

```
[AGG1] ospf 22 vpn-instance vpnb
[AGG1-ospf-22] import-route bgp
[AGG1-ospf-22] vpn-instance-capability simple
[AGG1-ospf-22] area 0
[AGG1-ospf-22-area-0.0.0.0] network 192.168.2.0 0.0.0.255
[AGG1-ospf-22-area-0.0.0.0] network 192.168.22.0 0.0.0.255
[AGG1-ospf-22-area-0.0.0.0] quit
[AGG1-ospf-22] quit
```

配置 AGG2。

```
[AGG2] ospf 11 vpn-instance vpna
[AGG2-ospf-11] vpn-instance-capability simple
[AGG2-ospf-11] area 0
[AGG2-ospf-11-area-0.0.0.0] network 192.168.3.0 0.0.0.255
[AGG2-ospf-11-area-0.0.0.0] network 192.168.33.0 0.0.0.255
[AGG2-ospf-11-area-0.0.0.0] quit
[AGG2-ospf-11] quit
[AGG2] ospf 22 vpn-instance vpnb
[AGG2-ospf-22] import-route bgp
[AGG2-ospf-22] vpn-instance-capability simple
[AGG2-ospf-22] area 0
[AGG2-ospf-22-area-0.0.0.0] network 192.168.4.0 0.0.0.255
[AGG2-ospf-22-area-0.0.0.0] network 192.168.44.0 0.0.0.255
[AGG2-ospf-22-area-0.0.0.0] quit
[AGG2-ospf-22] quit
```

配置 AGG3。

```
[AGG3] ospf 11 vpn-instance vpna
[AGG3-ospf-11] import-route bgp
[AGG3-ospf-11] vpn-instance-capability simple
[AGG3-ospf-11] area 0
[AGG3-ospf-11-area-0.0.0.0] network 192.168.5.0 0.0.0.255
[AGG3-ospf-11-area-0.0.0.0] network 192.168.55.0 0.0.0.255
[AGG3-ospf-11-area-0.0.0.0] quit
[AGG3-ospf-11] quit
[AGG3] ospf 22 vpn-instance vpnb
[AGG3-ospf-22] import-route bgp
[AGG3-ospf-22] vpn-instance-capability simple
[AGG3-ospf-22] area 0
[AGG3-ospf-22-area-0.0.0.0] network 192.168.6.0 0.0.0.255
[AGG3-ospf-22-area-0.0.0.0] network 192.168.66.0 0.0.0.255
[AGG3-ospf-22-area-0.0.0.0] quit
[AGG3-ospf-22] quit
[AGG3] ospf 33 vpn-instance public
[AGG3-ospf-33] import-route bgp
[AGG3-ospf-33] vpn-instance-capability simple
[AGG3-ospf-33] area 0
[AGG3-ospf-33-area-0.0.0.0] network 192.168.7.0 0.0.0.255
[AGG3-ospf-33-area-0.0.0.0] network 192.168.77.0 0.0.0.255
[AGG3-ospf-33-area-0.0.0.0] quit
[AGG3-ospf-33] quit
```

配置 CORE1。

```
[CORE1] ospf 11 vpn-instance vpna
```

```
[CORE1-ospf-11] import-route bgp
[CORE1-ospf-11] vpn-instance-capability simple
[CORE1-ospf-11] area 0
[CORE1-ospf-11-area-0.0.0.0] network 192.168.11.0 0.0.0.255
[CORE1-ospf-11-area-0.0.0.0] network 192.168.55.0 0.0.0.255
[CORE1-ospf-11-area-0.0.0.0] quit
[CORE1-ospf-11] quit
[CORE1] ospf 22 vpn-instance vpnb
[CORE1-ospf-22] import-route bgp
[CORE1-ospf-22] vpn-instance-capability simple
[CORE1-ospf-22] area 0
[CORE1-ospf-22-area-0.0.0.0] network 192.168.22.0 0.0.0.255
[CORE1-ospf-22-area-0.0.0.0] network 192.168.66.0 0.0.0.255
[CORE1-ospf-22-area-0.0.0.0] quit
[CORE1-ospf-22] quit
```

配置 CORE2。

```
[CORE2] ospf 11 vpn-instance vpna
[CORE2-ospf-11] import-route bgp
[CORE2-ospf-11] vpn-instance-capability simple
[CORE2-ospf-11] area 0
[CORE2-ospf-11-area-0.0.0.0] network 192.168.33.0 0.0.0.255
[CORE2-ospf-11-area-0.0.0.0] quit
[CORE2-ospf-11] quit
[CORE2] ospf 22 vpn-instance vpnb
[CORE2-ospf-22] import-route bgp
[CORE2-ospf-22] vpn-instance-capability simple
[CORE2-ospf-22] area 0
[CORE2-ospf-22-area-0.0.0.0] network 192.168.44.0 0.0.0.255
[CORE2-ospf-22-area-0.0.0.0] quit
[CORE2-ospf-22] quit
```

10. VPN 路由配置。

配置 AGG3。

```
[AGG3] bgp 1
[AGG3-bgp] ipv4-family unicast
[AGG3-bgp-af-ipv4] undo synchronization
[AGG3-bgp-af-ipv4] quit
[AGG3-bgp] ipv4-family vpn-instance vpna
[AGG3-bgp-vpna] import-route ospf 11
[AGG3-bgp-vpna] quit
[AGG3-bgp] ipv4-family vpn-instance vpnb
[AGG3-bgp-vpnb] import-route ospf 22
[AGG3-bgp-vpnb] quit
[AGG3-bgp] ipv4-family vpn-instance public
[AGG3-bgp-public] import-route ospf 33
[AGG3-bgp-public] quit
```

配置 CORE1。

```
[CORE1] bgp 100
[CORE1-bgp] ipv4-family unicast
[CORE1-bgp-af-ipv4] undo synchronization
[CORE1-bgp-af-ipv4] quit
```

```
[CORE1-bgp] ipv4-family vpn-instance vpna
[CORE1-bgp-vpna] import-route direct
[CORE1-bgp-vpna] import-route ospf 11
[CORE1-bgp-vpna] quit
[CORE1-bgp] ipv4-family vpn-instance vpnb
[CORE1-bgp-vpnb] import-route direct
[CORE1-bgp-vpnb] import-route ospf 22
[CORE1-bgp-vpnb] quit
```

配置 CORE2。

```
[CORE2] bgp 100
[CORE2-bgp] ipv4-family unicast
[CORE2-bgp-af-ipv4] undo synchronization
[CORE2-bgp-af-ipv4] quit
[CORE2-bgp] ipv4-family vpn-instance vpna
[CORE2-bgp-vpna] import-route direct
[CORE2-bgp-vpna] import-route ospf 11
[CORE2-bgp-vpna] quit
[CORE2-bgp] ipv4-family vpn-instance vpnb
[CORE2-bgp-vpnb] import-route direct
[CORE2-bgp-vpnb] import-route ospf 22
[CORE2-bgp-vpnb] quit
```

----结束

配置文件

- ACC1 配置文件

```
#
 sysname ACC1
#
 vlan batch 11
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 11
#
return
```

ACC2~ACC7 的配置与之类似，其中 ACC3、ACC5 的 VLAN 也是 11，ACC2、ACC4、ACC6 的 VLAN 是 22，ACC7 的 VLAN 是 33。

- AGG1 配置文件

```
#
 sysname AGG1
#
 vlan batch 11 22 101 202
#
ip vpn-instance vpna
 route-distinguisher 11:1
 vpn-target 11:1 export-extcommunity
 vpn-target 11:1 import-extcommunity
ip vpn-instance vpnb
 route-distinguisher 22:1
```

```
 vpn-target 22:1 export-extcommunity
 vpn-target 22:1 import-extcommunity
#
interface Vlanif11
 ip binding vpn-instance vpna
 ip address 192.168.1.11 255.255.255.0
#
interface Vlanif22
 ip binding vpn-instance vpnb
 ip address 192.168.2.11 255.255.255.0
#
interface Vlanif101
 ip binding vpn-instance vpna
 ip address 192.168.11.11 255.255.255.0
#
interface Vlanif202
 ip binding vpn-instance vpnb
 ip address 192.168.22.11 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 101 202
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 11
#
interface GigabitEthernet1/0/24
 eth-trunk 1
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 22
#
interface GigabitEthernet2/0/24
 eth-trunk 1
#
ospf 11 vpn-instance vpna
 vpn-instance-capability simple
 area 0.0.0.0
  network 192.168.1.0 0.0.0.255
  network 192.168.11.0 0.0.0.255
#
ospf 22 vpn-instance vpnb
 vpn-instance-capability simple
 area 0.0.0.0
  network 192.168.2.0 0.0.0.255
  network 192.168.22.0 0.0.0.255
#
return
```

- AGG2 配置文件

```
#
```

```
 sysname AGG2
#
 vlan batch 11 22 101 202
#
ip vpn-instance vpna
 route-distinguisher 11:1
 vpn-target 11:1 export-extcommunity
 vpn-target 11:1 import-extcommunity
ip vpn-instance vpnb
 route-distinguisher 22:1
 vpn-target 22:1 export-extcommunity
 vpn-target 22:1 import-extcommunity
#
interface Vlanif11
 ip binding vpn-instance vpna
 ip address 192.168.3.11 255.255.255.0
#
interface Vlanif22
 ip binding vpn-instance vpnb
 ip address 192.168.4.11 255.255.255.0
#
interface Vlanif101
 ip binding vpn-instance vpna
 ip address 192.168.33.11 255.255.255.0
#
interface Vlanif202
 ip binding vpn-instance vpnb
 ip address 192.168.44.11 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 101 202
 mode lacp-static
 load-balance src-mac
 lacp preempt enable
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 11
#
interface GigabitEthernet1/0/24
 eth-trunk 1
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 22
#
interface GigabitEthernet2/0/24
 eth-trunk 1
#
ospf 11 vpn-instance vpna
 vpn-instance-capability simple
 area 0.0.0.0
  network 192.168.3.0 0.0.0.255
  network 192.168.33.0 0.0.0.255
```



```
#
ospf 22 vpn-instance vpnb
 vpn-instance-capability simple
 area 0.0.0.0
  network 192.168.4.0 0.0.0.255
  network 192.168.44.0 0.0.0.255
#
return
```

- AGG3 配置文件

```
#
 sysname AGG3
#
 vlan batch 11 22 33 111 222 333
#
ip vpn-instance vpna
 route-distinguisher 11:1
 vpn-target 11:1 export-extcommunity
 vpn-target 11:1 import-extcommunity
ip vpn-instance vpnb
 route-distinguisher 22:1
 vpn-target 22:1 export-extcommunity
 vpn-target 22:1 import-extcommunity
ip vpn-instance public
 route-distinguisher 33:1
 vpn-target 11:1 22:1 export-extcommunity
 vpn-target 11:1 22:1 import-extcommunity
#
interface Vlanif11
 ip binding vpn-instance vpna
 ip address 192.168.5.11 255.255.255.0
#
interface Vlanif22
 ip binding vpn-instance vpnb
 ip address 192.168.6.11 255.255.255.0
#
interface Vlanif33
 ip binding vpn-instance public
 ip address 192.168.7.11 255.255.255.0
#
interface Vlanif111
 ip binding vpn-instance vpna
 ip address 192.168.55.11 255.255.255.0
#
interface Vlanif222
 ip binding vpn-instance vpnb
 ip address 192.168.66.11 255.255.255.0
#
interface Vlanif333
 ip binding vpn-instance public
 ip address 192.168.77.11 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 111 222 333
 mode lacp-static
```



```
 load-balance src-mac
 lacp preempt enable
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 11
#
interface GigabitEthernet1/0/24
 eth-trunk 1
#
interface GigabitEthernet2/0/1
 port link-type trunk
 port trunk allow-pass vlan 22
#
interface GigabitEthernet2/0/24
 eth-trunk 1
#
interface GigabitEthernet3/0/1
 port link-type trunk
 port trunk allow-pass vlan 33
#
bgp 1
 #
 ipv4-family unicast
  undo synchronization
 #
 ipv4-family vpn-instance public
  import-route ospf 33
 #
 ipv4-family vpn-instance vpna
  import-route ospf 11
 #
 ipv4-family vpn-instance vpnb
  import-route ospf 22
#
ospf 11 vpn-instance vpna
 import-route bgp
 vpn-instance-capability simple
 area 0.0.0.0
  network 192.168.55.0 0.0.0.255
  network 192.168.5.0 0.0.0.255
#
ospf 22 vpn-instance vpnb
 import-route bgp
 vpn-instance-capability simple
 area 0.0.0.0
  network 192.168.6.0 0.0.0.255
  network 192.168.66.0 0.0.0.255
#
ospf 33 vpn-instance public
 area 0.0.0.0
  network 192.168.7.0 0.0.0.255
  network 192.168.77.0 0.0.0.255
#
return
```

- CORE1 的配置文件

```
#
 sysname CORE1
#
 vlan batch 100 to 101 111 202 222 333
#
ip vpn-instance vpna
 route-distinguisher 11:1
 tnl-policy p1
 vpn-target 11:1 export-extcommunity
 vpn-target 11:1 import-extcommunity
ip vpn-instance vpnb
 route-distinguisher 22:1
 tnl-policy p1
 vpn-target 22:1 export-extcommunity
 vpn-target 22:1 import-extcommunity
ip vpn-instance public
 route-distinguisher 33:1
 tnl-policy p1
 vpn-target 11:1 22:1 export-extcommunity
 vpn-target 11:1 22:1 import-extcommunity
#
 mpls lsr-id 1.1.1.1
 mpls
  mpls te
  label advertise non-null
  mpls rsvp-te
  mpls te cspf
#
#
interface Vlanif100
 ip address 100.1.1.1 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif101
 ip binding vpn-instance vpna
 ip address 192.168.11.12 255.255.255.0
#
interface Vlanif111
 ip binding vpn-instance vpna
 ip address 192.168.55.12 255.255.255.0
#
interface Vlanif202
 ip binding vpn-instance vpnb
 ip address 192.168.22.12 255.255.255.0
#
interface Vlanif222
 ip binding vpn-instance vpnb
 ip address 192.168.66.12 255.255.255.0
#
interface Vlanif333
 ip binding vpn-instance public
 ip address 192.168.77.12 255.255.255.0
```

```
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 101 202
 mode lacp-static
 load-balance dst-mac
 lacp preempt enable
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 100
 mode lacp-static
#
interface Eth-Trunk3
 port link-type trunk
 port trunk allow-pass vlan 111 222 333
 mode lacp-static
 load-balance dst-mac
 lacp preempt enable
#
interface GigabitEthernet1/1/0/24
 eth-trunk 1
#
interface GigabitEthernet1/2/0/24
 eth-trunk 3
#
interface GigabitEthernet1/3/0/23
 eth-trunk 2
#
interface GigabitEthernet1/3/0/24
 eth-trunk 2
#
interface GigabitEthernet2/1/0/24
 eth-trunk 1
#
interface GigabitEthernet2/2/0/24
 eth-trunk 3
#
interface GigabitEthernet2/3/0/23
 eth-trunk 2
#
interface GigabitEthernet2/3/0/24
 eth-trunk 2
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
interface Tunnel0/0/0/1
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 2.2.2.2
 mpls te tunnel-id 22
 mpls te reserved-for-binding
 mpls te commit
#
```



```
bgp 100
 peer 2.2.2.2 as-number 100
 peer 2.2.2.2 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  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
  import-route ospf 11
 #
 ipv4-family vpn-instance vpnb
  import-route direct
  import-route ospf 22
 #
ipv4-family vpn-instance public
  import-route direct
  import-route ospf 33
 #
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 100.1.1.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
  mpls-te enable
#
ospf 11 vpn-instance vpna
 import-route bgp
 area 0.0.0.0
  network 192.168.11.0 0.0.0.255
  network 192.168.55.0 0.0.0.255
#
ospf 22 vpn-instance vpnb
 import-route bgp
 area 0.0.0.0
  network 192.168.22.0 0.0.0.255
  network 192.168.66.0 0.0.0.255
#
ospf 33 vpn-instance public
 import-route bgp
 area 0.0.0.0
  network 192.168.77.0 0.0.0.255
#
tunnel-policy p1
 tunnel binding destination 2.2.2.2 te Tunnel0/0/0/1
#
return
```

- CORE2 的配置文件

```
#
 sysname CORE2
#
 vlan batch 100 to 101 202
#
ip vpn-instance vpna
 route-distinguisher 11:1
 tnl-policy p1
 vpn-target 11:1 export-extcommunity
 vpn-target 11:1 import-extcommunity
ip vpn-instance vpnb
 route-distinguisher 22:1
 tnl-policy p1
 vpn-target 22:1 export-extcommunity
 vpn-target 22:1 import-extcommunity
#
 mpls lsr-id 2.2.2.2
 mpls
  mpls te
  label advertise non-null
  mpls rsvp-te
  mpls te cspf
#
#
interface Vlanif100
 ip address 100.1.1.2 255.255.255.0
 mpls
 mpls te
 mpls rsvp-te
#
interface Vlanif101
 ip binding vpn-instance vpna
 ip address 192.168.33.12 255.255.255.0
#
interface Vlanif202
 ip binding vpn-instance vpnb
 ip address 192.168.44.12 255.255.255.0
#
interface Eth-Trunk1
 port link-type trunk
 port trunk allow-pass vlan 101 202
 mode lacp-static
 load-balance dst-mac
 lacp preempt enable
#
interface Eth-Trunk2
 port link-type trunk
 port trunk allow-pass vlan 100
 mode lacp-static
#
interface GigabitEthernet1/1/0/24
 eth-trunk 1
#
interface GigabitEthernet1/3/0/23
 eth-trunk 2
```

```
#
interface GigabitEthernet1/3/0/24
 eth-trunk 2
#
interface GigabitEthernet2/1/0/24
 eth-trunk 1
#
interface GigabitEthernet2/3/0/23
 eth-trunk 2
#
interface GigabitEthernet2/3/0/24
 eth-trunk 2
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
interface Tunnel0/0/0/1
 ip address unnumbered interface LoopBack0
 tunnel-protocol mpls te
 destination 1.1.1.1
 mpls te tunnel-id 22
 mpls te reserved-for-binding
 mpls te commit
#
bgp 100
 peer 1.1.1.1 as-number 100
 peer 1.1.1.1 connect-interface LoopBack0
 #
 ipv4-family unicast
  undo synchronization
  import-route direct
  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
  import-route ospf 11
 #
 ipv4-family vpn-instance vpnb
  import-route direct
  import-route ospf 22
 #
#
ospf 1
 opaque-capability enable
 area 0.0.0.0
  network 100.1.1.0 0.0.0.255
  network 2.2.2.2 0.0.0.0
  mpls-te enable
#
ospf 11 vpn-instance vpna
 import-route bgp
```

```
 area 0.0.0.0
  network 192.168.33.0 0.0.0.255
#
ospf 22 vpn-instance vpnb
 import-route bgp
 area 0.0.0.0
  network 192.168.44.0 0.0.0.255
#
tunnel-policy p1
 tunnel binding destination 1.1.1.1 te Tunnel0/0/0/1
#
return
```

6 NAC 系统部署

6.1 概述

6.1.1 NAC 系统简介

NAC 系统的作用和组成

如何在企业中构建安全的网络，在办公便捷、网络资源合理共享的同时发现并隔离不合法和不安全的终端主机，确保只有被授权的和通过安全检查的终端主机才能访问网络资源，从而保护重要的网络资源，是高层管理人员和 IT 部门较为关注的问题。

按照通用的企业网络架构，对于用户的认证和授权是通过部署 NAC 系统来完成。NAC 系统一般由如下部件组成：

- 终端代理

  终端代理是安装在用户终端系统上的专用客户端软件，与准入服务器联动进行用户身份认证、终端安全检查、系统修复升级，终端行为监控审计等工作。

- 网络准入设备

  网络准入设备是终端访问网络的网络控制点，是企业安全策略的实施者，负责按照准入服务器制定的安全策略，实施相应的准入控制（允许、拒绝、隔离或限制）。

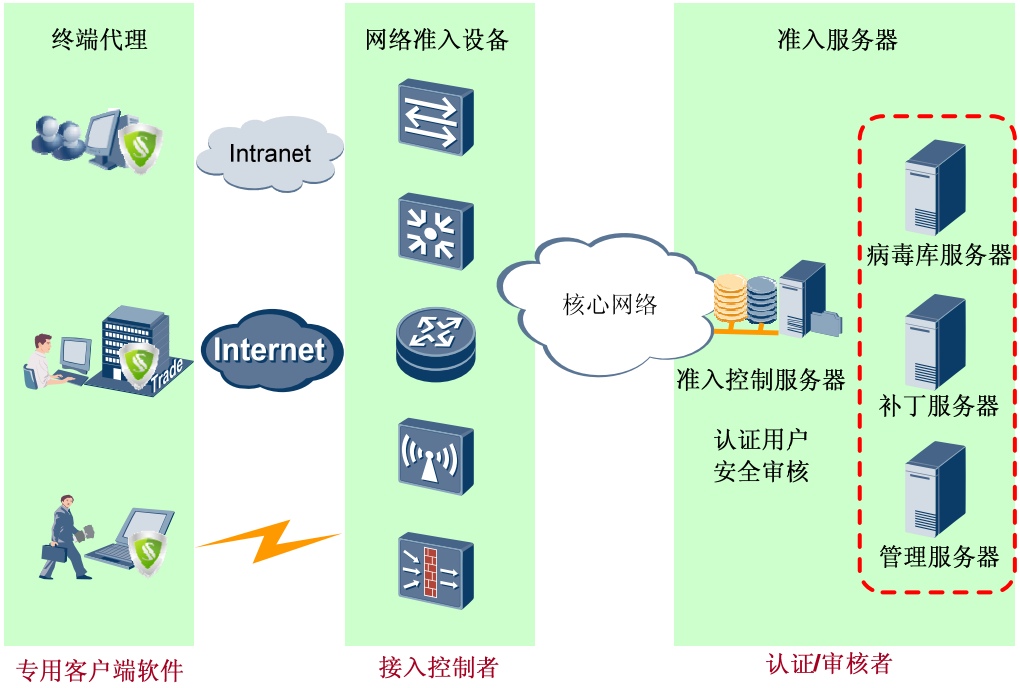
  网络准入设备通常又可称为用户业务网关，并不是一个物理实体，而是一个角色概念，通常由网络中的汇聚交换机（或者接入交换机）来担任。

- 准入服务器

  准入服务器是后台的安全管理和控制服务器。它可以进行用户管理，增加、删除、修改用户权限及用户部门配置，及安全策略的定制和管理等。还需要进行用户认证和安全审核，实施安全策略，并且与网络准入设备联动，下发用户权限。另外，准入服务器也包括病毒库服务器和补丁服务器等用于终端安全修复的服务器。

  准入服务器经常也被称为 AAA 服务器，它与用户业务网关之间可采用 RADIUS 等协议进行通信，共同完成对于用户的认证、计费和授权等功能。

图6-1 NAC 系统组成示意图



接入认证技术简介

华为公司 NAC 方案，支持 802.1x、MAC 认证、Portal 认证多种网络访问控制方式，并可灵活部署在用户网络的接入交换机、汇聚交换机、无线控制器、AR 等多种网络设备上，配合 NAC 的代理客户端和服务器共同完成 NAC 控制，为企业网、园区网、城域网提供安全可靠的访问控制。

在园区网中，用户的接入认证技术主要如下几种：

1. Portal 认证

Portal 认证是一种三层认证方式。用户可以通过访问 Portal 服务器（Web 服务器）上的 Web 认证页面，输入用户帐号信息，实现对终端用户身份的认证。采用 Portal 认证，有如下几种认证方式：

- 用户使用 Web 浏览器直接访问 Portal 服务器的认证页面，并在认证页面上输入用户名和密码进行认证。
- 用户使用 Web 浏览器访问任意其他站点，由业务网关将其访问重定向到 Portal 服务器的认证页面，用户在认证页面上输入用户名和密码进行认证。
- 用户使用 TSM Agent 软件（需配置好 Portal 认证服务器的地址），在软件界面上输入用户名和密码进行认证。

如果需要实现对终端状态的安全检查，则有两种方式：

- 使用 TSM Agent 软件进行认证，TSM Agent 软件具备终端安全检查和修复的功能。

- 如果使用 Web 浏览器进行访问和认证，则需要在对 Portal 服务器的认证页面加上 ActiveX 插件下载的功能，用户通过认证之后，Web 浏览器可自动下载一个 ActiveX 插件，该插件可以对终端安全进行检查并报告 Portal 服务器。

2. 802.1x 认证

   802.1x 协议是一种基于端口的网络接入控制协议，用于在局域网接入设备的端口一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

   802.1x 认证使用 EAP（Extensible Authentication Protocol）认证协议，实现客户端、设备端和认证服务器之间认证信息的交换。在客户端与设备端之间，EAP 协议报文使用 EAPoL（EAP over LAN）封装格式，直接承载于 LAN 环境中。

3. MAC 认证

   对某些特殊情况，终端用户不想或不能通过输入用户帐号信息的方式完成认证。例如某些特权终端希望能“免认证”直接访问网络；对于某些特殊的 PC 终端，如打印机、IP 电话等设备，无法安装客户端软件，也无法通过输入用户帐号信息的方式进行认证授权。此时可以采用 MAC 认证的方式实现对终端的网络访问控制。

   MAC 认证就是以终端的 MAC 地址作为身份凭据到系统进行认证。启用 MAC 认证后，当终端接入网络时，网络准入设备提取终端 MAC 地址，并将该 MAC 地址作为用户名和密码进行认证。如果认证失败使用户下线，并保持一段时间内不再发起认证和探测，超时后重新开始探测过程。如果认证成功，交换机将增加该 MAC 地址进入 MAC 表，用户将可以正常访问网络。

表6-1 接入认证技术比较

技术比较	MAC	Portal	802.1x
标准化程度	标准	Web 软件厂商私有	标准
IP 地址	无认证	认证前分配	认证后分配
客户端软件	不需要	不需要	需要
对设备要求	无	私有设备	大多数交换机
安全性	低	高	高
使用场景	适用于 SIP 终端，打印机，传真机等终端接入认证的场景	认证方式灵活，适用于用户分散、无线、外客访问等场景	新建网络，用户集中，信息安全要求严格的场景

----结束

TSM 简介

为了解决企业内部网络管理失控的问题，保障企业内部网络的畅通、终端主机的安全和公司信息数据的安全，实现企业网络安全建设的目标，华为公司推出 TSM 产品，该产

品为企业提供整合的内部网络安全解决方案，实现从终端到业务系统的控制和管理功能。

TSM 基于 TSM 代理为企业提供安全接入控制、终端安全管理、补丁管理、终端用户的行为管理、软件分发和资产管理六大功能。其核心思想是建立网络准入控制机制，基本要素是安全检查、访问控制和安全修复。有效控制网络日渐增多的接入点，包括企业员工、外部访客、合作伙伴和临时雇员等对网络的访问，发现并隔离带有威胁的终端主机，提升网络防御安全威胁的能力。

TSM 系统基于 Client/Server 模式，由 TSM Server 和 TSM Agent 两部分组成。其中 TSM Agent 是 TSM 的一个组件，作为 TSM 的客户端软件，安装在终端主机。

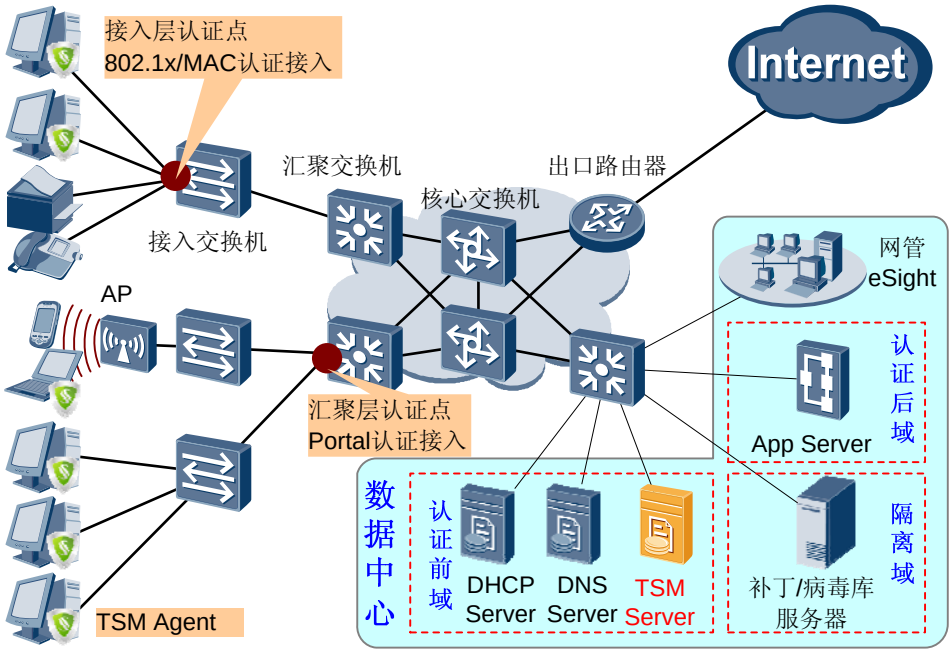
- TSM Server 是 TSM 系统的后台服务器部分，它可以作为企业 NAC 系统的准入服务器来进行部署，可提供接入认证、权限控制、终端管理、攻击防御、资产管理等功能，并具有高可靠性、执行灵活、融合开放等特点。
- TSM Agent 并不仅仅是一个认证客户端软件，而是一个终端安全综合管理软件，它提供了强大的终端安全管理功能，包括身份认证、终端安全状态检查和修复、终端用户行为管理、注册资产、接收公告等多种功能。

对于 TSM Agent 来说，支持 Portal 认证、802.1x 认证、MAC 认证等多种认证方式，并且其认证方式是集成融合的，一个客户端即可实现多种认证方式。用户不需要再使用 Web 浏览器或者单独的 802.1x 客户端软件。

6.1.2 典型组网

NAC 系统部署的典型组网如图 6-2 所示。

图6-2 NAC 系统典型组网图



在 NAC 系统中，准入服务器可以使用 TSM Server，终端代理可使用 TSM Agent。如果是 802.1x 认证或 MAC 认证，可以使用接入交换机作为网络准入设备，如果是 Portal 认证，可以使用汇聚交换机作为网络准入设备。

6.1.3 配套版本

表6-2 虚拟园区网配套产品和版本

部件	产品	版本
接入交换机	S2700/S3700 系列	V100R006C01
汇聚交换机	S5700 /S7700 系列	V100R006C01
核心交换机	S7700/S9300 系列	V100R006C01
终端代理	TSM Agent	V100R002C06
准入服务器	TSM Server	V100R002C06

6.1.4 部署思路

前置任务

- 完成各网元/部件的安装调试和线缆连接，各网元上电正常工作。
- TSM 服务器的操作系统和 TSM 软件已经安装完毕。
- 完成 VLAN/SSID、IP 地址等数据的规划。

配置思路

配置思路	配置注意事项
在各网元部件上配置接口、VLAN、IP 地址和路由，实现网络的基础互通。	本章不再描述配置步骤。 当需要把用户侧接口配置为 802.1x 认证时，不要配置接口类型，使用默认的Hybrid类型即可。也不要配置默认 VLAN。 如果在接入层部署 802.1x 认证，则接入交换机需要配置上行的 VLANIF 接口并配置 IP 地址，以便和认证服务器进行通信。
在业务网关上配置 NAC 功能，实现对接入用户的认证和授权。 业务网关的角色根据接入认证方式的选择而定。如果是 802.1x 认证，则选择接入交换机；如果是 Portal 认证，则选择汇聚交换机。	主要包括： • 配置 AAA 功能，设置用户的归属域、认证/授权的模式以及相应的 AAA 服务器等。 • 在接入交换机上配置 802.1x 认证或者在汇聚交换机上配置 Portal 认证。

配置思路	配置注意事项
配置 TSM 服务器。主要配置包括： • 配置认证服务器（Portal 认证服务器或者 802.1x 认证服务器），用于对终端进行安全认证。 • 配置隔离域和认证后域的信息。 • 配置策略模板，并将策略下发到用户。 • 配置用户账号（包括普通账号、MAC 账号、AD 账号及 LDAP 账号等），为账号配置接入隔离域及后域，实现对用户的网络权限控制。	• DHCP 服务器、DNS 服务器、TSM 服务器属于认证前域。 • 用于安全修复的补丁服务器或者病毒库服务器则划分到隔离域。 • 其他的应用服务器属于认证后域。 • 如果是普通账号，则需要在 TSM 服务器上配置用户名和密码。 • 如果是 AD 域账号，则需要另外部署域控制服务器，并配置用户名和密码。然后将账号同步至 TSM 服务器。
配置终端代理 TSM Agent。	配置认证方式、认证服务器等，并进行认证接入。

6.2 配置业务网关

在业务网关上（例如 S9300 交换机），NAC 的部署主要包括如下几方面：

- 配置 AAA 功能，设置用户的归属域、认证/授权的模式以及相应的 AAA 服务器等。
- 在用户接入的接口下配置 802.1x 或者 Portal 认证。

下面以 S9300 作为业务网关为例，列出了最基本的常用 NAC 配置步骤。更详细完整的配置步骤和内容请参见所使用产品的产品文档。

6.2.1 配置 AAA 功能

配置认证方案

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **aaa**，进入 AAA 视图。
3. 执行命令 **authentication-scheme** *authentication-scheme-name*，创建认证方案，并进入认证方案视图。
4. 执行命令 **authentication-mode** { **hwtacacs** | **radius** | **local** }* [**none**]，配置认证模式。

----结束

配置授权方案

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **aaa**，进入 AAA 视图。

3. 执行命令 **authorization-scheme** *authorization-scheme-name*，创建授权方案，并进入授权方案视图。
4. 执行命令 **authorization-mode** [**hwtacacs**] { **if-authenticated** | **local** | **none** }，配置授权模式。

----结束

配置 RADIUS 服务器模板

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **radius-server template** *template-name*，创建 RADIUS 服务器模板，并进入 RADIUS 服务器模板视图。
3. 执行命令 **radius-server authentication** *ip-address port* [**source loopback** *interface-number*]，配置 RADIUS 认证服务器。
4. 执行命令 **radius-server accounting** *ip-address port* [**source loopback** *interface-number*]，配置 RADIUS 计费服务器。
5. 执行命令 **quit**，返回系统视图。
6. 执行命令 **radius-server authorization** *ip-address* { **server-group** *group-name* | **shared-key** { **cipher** | **simple** } *key-string* } * [**ack-reserved-interval** *interval*]，配置 RADIUS 授权服务器。

----结束

配置域

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **aaa**，进入 AAA 视图。
3. 执行命令 **domain** *domain-name*，创建域，并进入域视图。
4. 执行命令 **authentication-scheme** *authentication-scheme-name*，配置域使用的认证方案。
5. （可选）执行命令 **authorization-scheme** *authorization-scheme-name*，配置域使用的授权方案。

   如果使用 RADIUS 认证，则省略本步骤。
6. 执行命令 **accounting-scheme** *accounting-scheme-name*，配置域使用的计费方案。
7. 执行命令 **radius-server** t*emplate-name*，配置域使用的 RADIUS 服务器模板。

----结束

6.2.2 配置 Portal 认证

配置 Web 认证服务器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **web-auth-server** *server-name*，配置 Web 认证服务器，并进入 Web 认证服务器视图。
3. 执行命令 **server-ip** *ip-address*，配置 Web 认证服务器的 IP 地址。
4. 执行命令 **port** *port-number* [**all**]，配置 Web 认证服务器接收 S9300 发送的通知报文的端口号。
5. （可选）如果要部署 Web 强推认证，执行命令 **url** *url-string*，配置 Web 认证服务器的认证页面所对应的 URL。

注意

- Web 强推认证是指当需要 Portal 认证的用户，在未认证前试图访问其无权访问的地址时，业务网关将其访问请求强制重定向到强制 Web 认证服务器，让用户进行认证。如果不部署 Web 强推认证，则用户在未认证之前进行未授权访问时，业务网关直接阻断其访问请求，而不会进行重定向操作。
- 如果希望对于使用 Web 浏览器进行访问和认证的用户进行终端安全检查，则 URL 应指向具有 ActiveX 下载功能的认证页面。

----结束

接口下绑定 Web 认证服务器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。

   说明

   只能是 VLANIF 接口，S9300/S7700 只能通过 VLANIF 接口完成对接入用户的 Web 认证。
3. 执行命令 **web-auth-server** *server-name*，在 VLANIF 接口下绑定 Web 认证服务器。

----结束

（可选）配置 Portal 认证的 Free Rule

当某些特殊用户在未通过认证的情况下需要访问特定资源，可以配置 Free Rule。

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **portal free-rule** *rule-id* { **destination** { **any** | **ip** { *ip-address mask* { *mask-length* | *ip-mask* } | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address mask* { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* }* } }*，配置免认证规则。

----结束

6.2.3 配置 802.1x 认证

使能 802.1x 认证

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dot1x enable**，使能全局 802.1x 认证功能。
3. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
4. 执行命令 **dot1x enable**，在接口下使能 802.1x 认证功能。

----结束

配置 802.1x 用户的认证方法

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **dot1x authentication-method** { **chap** | **eap** | **pap** }，配置 802.1x 用户的认证方法。

----结束

配置 802.1x 认证的 Guest VLAN

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **dot1x guest-vlan** *vlan-id*，配置接口的 Guest VLAN。

----结束

（可选）使能 MAC 旁路认证功能

MAC 旁路认证，指当终端进行 802.1x 认证失败后，把它的 MAC 地址作为用户名和密码上送 RADIUS 服务器进行认证。对于某些特殊终端，例如打印机等，无法使用和安装 802.1x 终端软件，可以通过基于 MAC 的旁路认证方式进行认证。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **interface** *interface-type interface-number*，进入接口视图。
3. 执行命令 **dot1x mac-bypass**，在接口下使能 MAC 旁路认证功能。

----结束

6.3 配置 TSM 服务器

注意

在本节中，重点描述 TSM 的接入认证和权限控制功能的配置，其余功能（例如终端管理、攻击防御、资产管理等）的配置请参考 TSM 产品的相关文档。

TSM 在接入认证和权限控制方面，主要发挥如下作用：

- 对本地用户进行管理，增加、删除、修改用户权限及用户部门配置，以及安全策略的定制和管理等。或者对外部认证源服务器的用户账号进行同步。
- 与网络准入设备联动，基于用户账号（本地账号或者同步的外部账号）完成用户认证和安全审核，实施安全策略，下发用户权限。

下面的 TSM 服务器部署也主要围绕着两大方面来进行介绍。包括如下内容：

- 配置普通账号
- 同步 AD 域账号
- 配置 Portal 认证控制
- 配置 802.1x 认证控制

注意

TSM 不支持同时启用 802.1x 交换机接入控制方式和 Portal 网关接入控制方式。

6.3.1 配置普通账号

在 TSM 中，用户管理涉及三个依次隶属的概念：部门、终端用户、账号。一个部门可以包含多个终端用户，一个终端用户可包含多个账号。

账号可以分为本地账号和外部认证源账号（例如 AD 域账号）两种。

- 本地账号是指用户名和密码等信息都配置在 TSM 服务器上的普通账号。
- 外部认证源账号是指企业中另外部署了其他认证服务器，为了确保终端用户使用现有的账号而不是新建账号进行认证，TSM 服务器上只同步外部认证源账号信息（不包括密码），用户直接使用外部认证源账号进行网络登录。

配置部门信息

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“部门用户 > 部门用户管理”，进入“部门用户管理”页面。
3. 在右侧操作区域选择“部门”页签。

4. 在部门导航树选择待创建部门的上级部门。
5. 在“部门”页签下方单击“增加”，出现“增加部门”对话框。

图6-3 增加部门

6. 输入部门的参数后，单击“确定”，出现“增加成功”的对话框。
7. 单击“确定”，完成部门信息的创建。

----结束

配置终端用户信息

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“部门用户 > 部门用户管理”，进入“部门用户管理”页面。
3. 在右侧操作区域选择“用户”页签。
4. 在部门导航树选择需要创建终端用户的目标部门。
5. 在“用户”页签下方单击“增加”，出现“增加用户”对话框。

图6-4 增加用户

6. 输入终端用户的参数后，单击“确定”，出现“增加成功”的对话框。
7. 单击“确定”，完成终端用户信息的创建。

----结束

配置本地账号信息

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“部门用户 > 部门用户管理”，进入“部门用户管理”页面。
3. 在右侧操作区域选择“用户”页签。
4. 在“部门用户管理”界面左侧的部门导航树选择需要创建普通账号的目标部门。

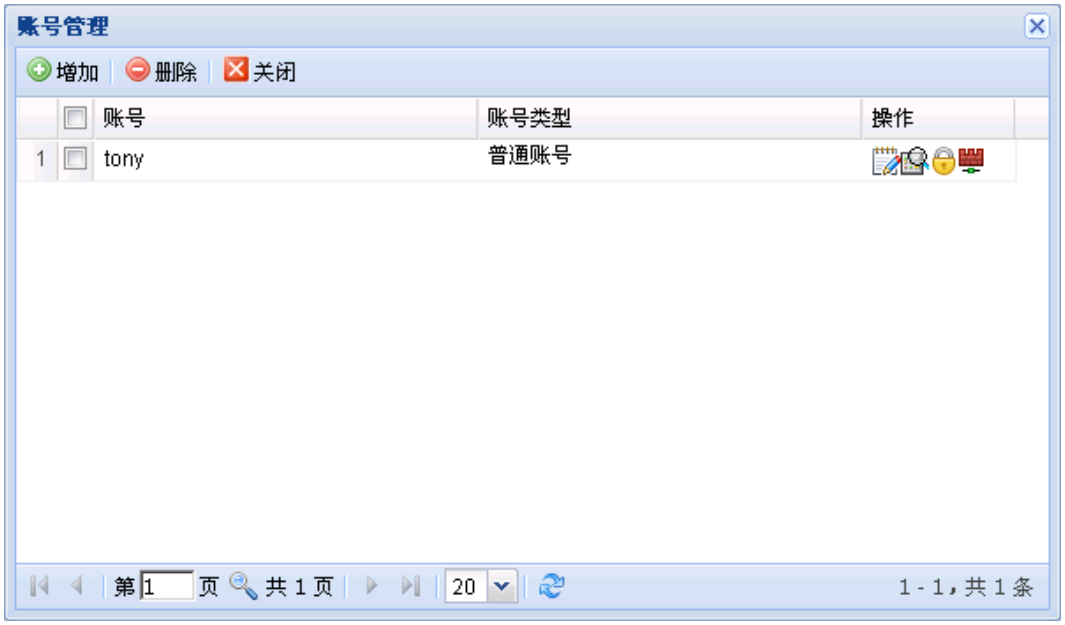
   “部门用户管理”界面右侧显示该部门下的所有终端用户。

图6-5 查看指定部门的所有终端用户

		用户名	所属部门	用户ID	职务	办公电话	描述	操作
1		张三	TSM财务部	00000001	会计	0755-368...	负责公司的各类...	
2		李四	TSM财务部	00000002	会计	0755-368...	负责公司的各类...	
3		王五	TSM财务部	00000003	会计	0755-368...	负责公司的各类...	

5. 在需要创建普通账号的终端用户右侧单击。显示终端用户的账户列表。

图6-6 查看终端用户的账户列表



6. 单击“增加”，出现“增加账号”对话框。

图6-7 增加账号

7. 输入普通账号的参数后，单击“确定”，出现“增加成功”的对话框。

注意

普通账号的登录类型有 Web、Agent、ActiveX 三种，其含义如下：

- Web：表示允许终端用户使用该账号通过 Web 浏览器进行身份认证。
- Agent：表示允许终端用户使用该账号通过 TSM Agent 软件进行身份认证。
- ActiveX：表示允许终端用户使用该账号通过 Web 浏览器的 Agent 插件进行身份认证。

8. 单击“确定”，完成普通账号信息的创建。

----结束

6.3.2 配置按 OU 方式同步 AD 域账号信息

注意

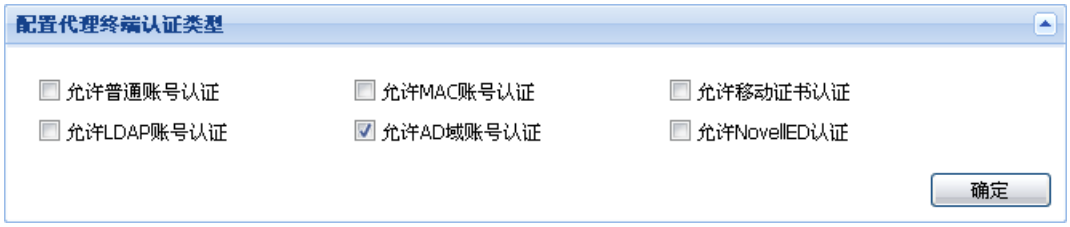
关于 AD 域控制服务器的设置，以及用户账号信息的创建的步骤，请参考相关产品的帮助或文档，或者参考 TSM Server 软件的联机帮助文档。

本节只描述如何将 AD 域服务器上的 AD 账号信息同步到 TSM 服务器的过程和步骤。

启用 Microsoft AD 域认证方式

1. 在 TSM 管理器的导航栏单击“系统配置”。
2. 在左侧菜单栏选择“终端配置 > 全局参数”。出现“配置代理终端认证类型”对话框。

图6-8 配置代理终端认证类型



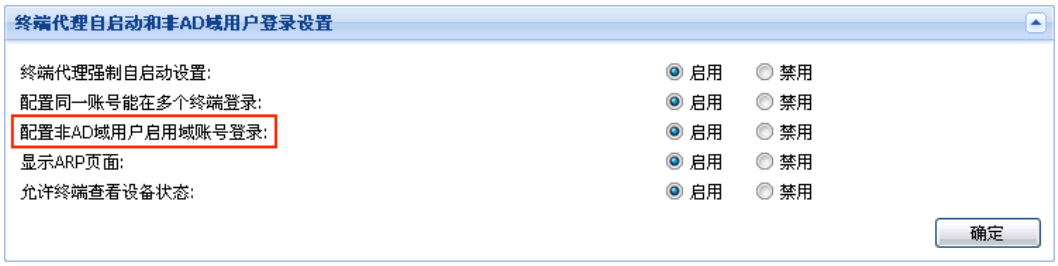
3. 选中“允许 AD 域账号认证”。
4. 单击“确定”，出现“修改成功”的对话框。
5. 单击“确定”，完成配置。

----结束

（可选）配置非 Microsoft AD 域用户启用域账号登录

1. 在 TSM 管理器的导航栏单击“系统配置”。
2. 在左侧菜单栏选择“终端配置 > 全局参数”。出现“终端代理自启动和非 AD 域用户登录”对话框。

图6-9 终端代理自启动和非 AD 域用户登录



3. 根据实际情况选择是否允许未使用 Microsoft AD 域账号登录的终端用户通过 Microsoft AD 域账号进行认证。
   - 要允许未使用 Microsoft AD 域账号登录的终端用户通过 Microsoft AD 域账号进行认证，选中“配置非 AD 域用户启用域账号登录”右侧的“启用”。
   - 要禁止未使用 Microsoft AD 域账号登录的终端用户通过 Microsoft AD 域账号进行认证，选中“配置非 AD 域用户启用域账号登录”右侧的“禁用”。
4. 单击“确定”，出现“修改成功”的对话框。
5. 单击“确定”，完成配置。

----结束

配置 Microsoft AD 域控制器的连接参数

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“外部数据源 > AD 服务器”。
3. 单击“增加”，出现“增加 AD”对话框。

图6-10 增加 AD 服务器

详细参数解释如表 6-3 所示。

表6-3 设置同步 Microsoft AD 域账号时 Microsoft AD 域控制器连接的参数说明

参数	类型	说明
同步类型	必填项	设置是否从 Microsoft AD 域控制器同步节点与账号。 按 OU 同步 Microsoft AD 域账号时，选择“按 OU 同步”。
认证源	必填项	设置 Microsoft AD 域控制器的名称，方便管理员区分 TSM 与哪一台 Microsoft AD 域控制器联动。 该名称不能与已配置的认证源名称重复，最大长度为 100byte。
类型	无	显示外部认证源的类型。
主服务器地址	必填项	输入 Microsoft AD 域控制器的 IP 地址。
备用服务器地址	选填项	如果 Microsoft AD 域控制器采用主备方式部署，请输入 Microsoft AD 备份域控制器的 IP 地址。
端口	必填项	输入 Microsoft AD 域控制器提供目录服务的端口号。 在安装 Microsoft AD 域控制器时，如果不配置 SSL，Microsoft AD 域控制器默认使用 389 作为服务端口。如果配置了 SSL，Microsoft AD 域控制器默认使用 636 作为服务端口。 除非在安装规划时改变了服务端口，否则请保持默认值。
服务器域名	必填项	输入 Microsoft AD 域控制器的域名。
基准 DN	必填项	输入根节点的 DN。
同步账号	必填项	输入在 Microsoft AD 域控制器中创建的同步账号。
同步密码	必填项	输入“同步账号”对应的密码。
认证账号	选填项	输入在 Microsoft AD 域控制器中创建的认证账号。
认证密码	选填项	输入“认证账号”对应的密码。
AD 故障时，允许 AD 认证直接通过(Kerberos 除外)	选填项	设置当 Microsoft AD 域控制器出现故障时，是否取消向 Microsoft AD 域控制器验证终端用户身份的过程。该参数仅适用于非 Kerberos 认证流程。 选中该项，当 Microsoft AD 域账号认证不采用 Kerberos 认证流程时，只要终端用户使用的 Microsoft AD 域账号已经同步到 TSM 管理器，则终端用户能够认证通过。
启用 SSL	选填项	设置是否启用 SSL。启用 SSL 后，TSM 与 Microsoft AD 域控制器联动时，将采用 SSL 协议加密，能够提高联动过程的安全性。 在 TSM 配置启用 SSL 的前提条件是：已经在 Microsoft AD 域控制器完成了 SSL 的相关配置。有关在 Microsoft AD 域控制器配置 SSL 的操作请参见 Microsoft AD 域控制器的相关文档。

4. 输入 Microsoft AD 域控制器的连接参数后，单击“确定”，出现“增加成功”的对话框。
5. 单击“确定”，完成 Microsoft AD 域控制器的连接参数的配置。

----结束

配置部门信息

请参见“6.3.1 配置普通账号”中的“配置部门信息”。

设置 Microsoft AD 域账号支持的接入方式

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“外部数据源 > AD 服务器”，出现外部认证源列表。

图6-11 查看外部认证源列表

3. 单击认证源右侧的。出现“外部认证源配置”对话框。

图6-12 配置外部认证源

4. 在“登录类型”中选中需要支持的接入受控网络的方式。
5. 单击“确定”，出现“设置成功”的对话框。
6. 单击“确定”，完成配置。

----结束

（可选）自定义 TSM 管理器与 Microsoft AD 域控制器字段的关联关系

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“外部数据源 > AD 服务器”，出现外部认证源列表。
3. 单击认证源右侧的。出现“外部认证源配置”对话框。

图6-13 配置外部认证源

4. 选择“部门”页签。输入部门参数。
5. 选择“用户”页签。输入终端用户参数。

图6-14 配置外部认证源的终端用户信息

6. 选择“其它”页签。输入其它参数。

图6-15 配置外部认证源的其它信息

7. 单击“确定”，出现“设置成功”的对话框。
8. 单击“确定”，完成配置。

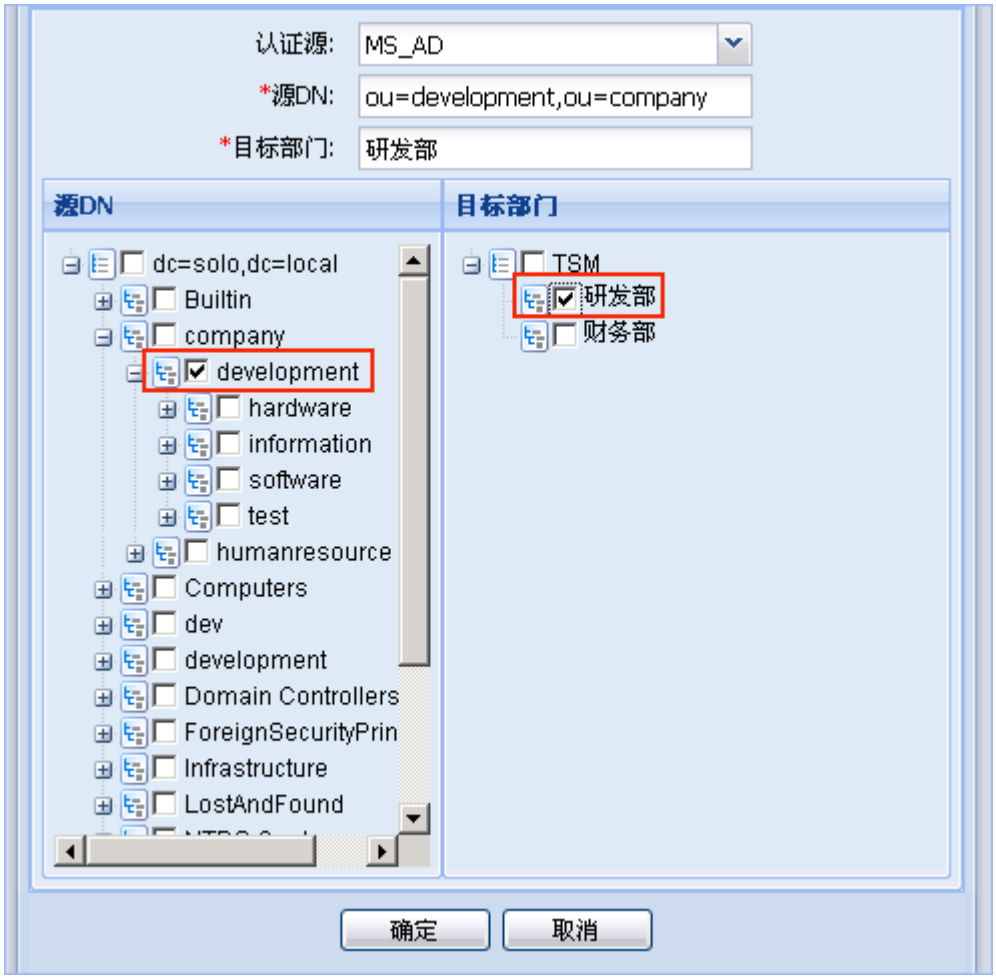
----结束

关联源 DN 与目标部门

指定源节点与目标部门的关联关系，以便源节点的子节点及其账号能够同步复制到 TSM 管理器的目标部门。

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“外部数据源 > 同步范围”。
3. 单击“增加 OU 同步”。出现设置源 DN 和目标部门的关联对话框。

图6-16 设置源 DN 和目标部门的关联



4. 设置源 DN 与目标部门的关联参数，单击“确定”，出现“增加成功”对话框。
5. 单击“确定”，完成源 DN 和目标部门的关联。

----结束

配置同步任务的执行周期

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“外部数据源 > AD 服务器”，出现外部认证源列表。

图6-17 查看外部认证源列表

3. 单击认证源右侧的。出现“自动同步设置”对话框。

图6-18 自动同步设置

4. 设置自动同步参数，单击“确定”，出现“设置成功”的对话框。
5. 单击“确定”，完成配置。

----结束

立即同步子节点和账号

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“外部数据源 > AD 服务器”，出现外部认证源列表。

图6-19 查看外部认证源列表

3. 单击认证源右侧的。出现“同步任务开始执行”对话框。
4. 单击“确定”，等待同步任务完成。

----结束

6.3.3 配置 Portal 认证控制

配置 Portal 网关

1. 在 TSM 管理器顶部单击“接入控制”。
2. 在左侧的菜单栏中选择“接入控制配置 > PORTAL 网关”。
3. 选择“PORTAL 网关”页签。
4. 单击“增加”。出现 Portal 网关配置对话框。

图6-20 Portal 网关配置

5. 输入 Portal 网关的连接参数。
6. 单击“增加”，出现“增加 IP 地址段”对话框。

图6-21 增加 IP 地址段

7. 输入起始 IP 地址和结束 IP 地址。

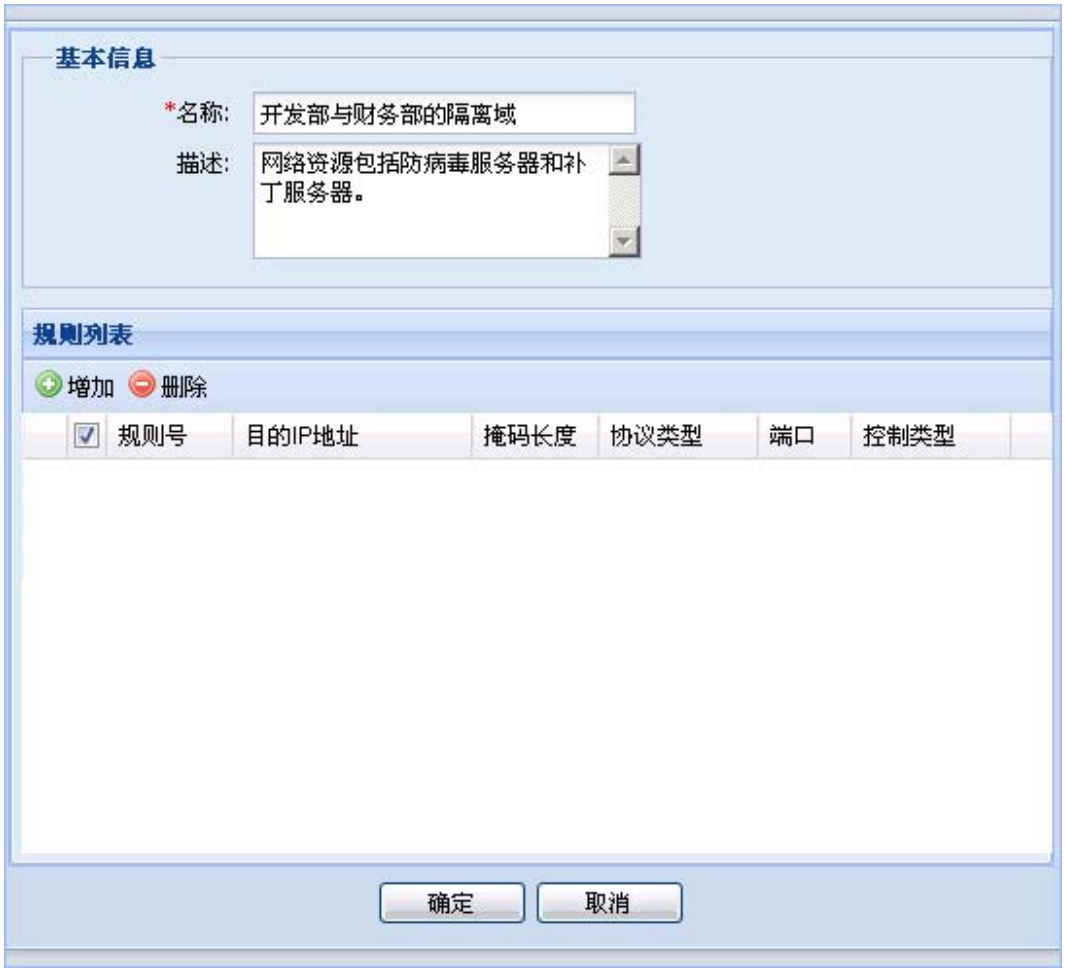
8. 单击“确定”，关闭“增加 IP 地址段”对话框。完成 IP 地址段的配置，将终端主机所在网段加入 IP 地址列表，表示对这些 IP 地址段启用 Portal 认证网关。
9. 单击“确定”，出现“增加成功”对话框。
10. 单击“确定”，完成配置。

----结束

配置隔离域

1. 在 TSM 管理器顶部单击“接入控制”。
2. 在左侧的菜单栏中选择“接入控制配置 > PORTAL 网关”。
3. 选择“隔离域”页签。
4. 单击“增加”，出现隔离域配置对话框。

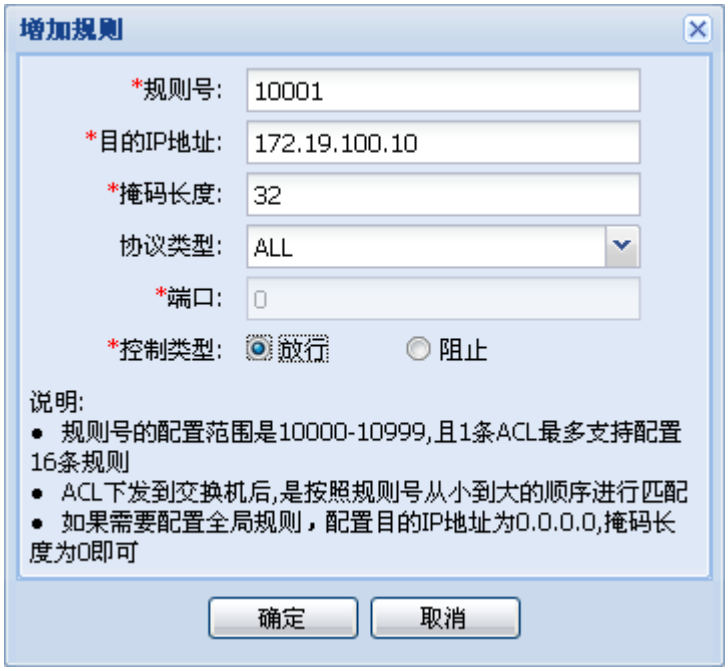
图6-22 隔离域配置



5. 输入隔离域的相关参数。

6. 单击“增加”。出现“增加规则”对话框。

图6-23 增加规则



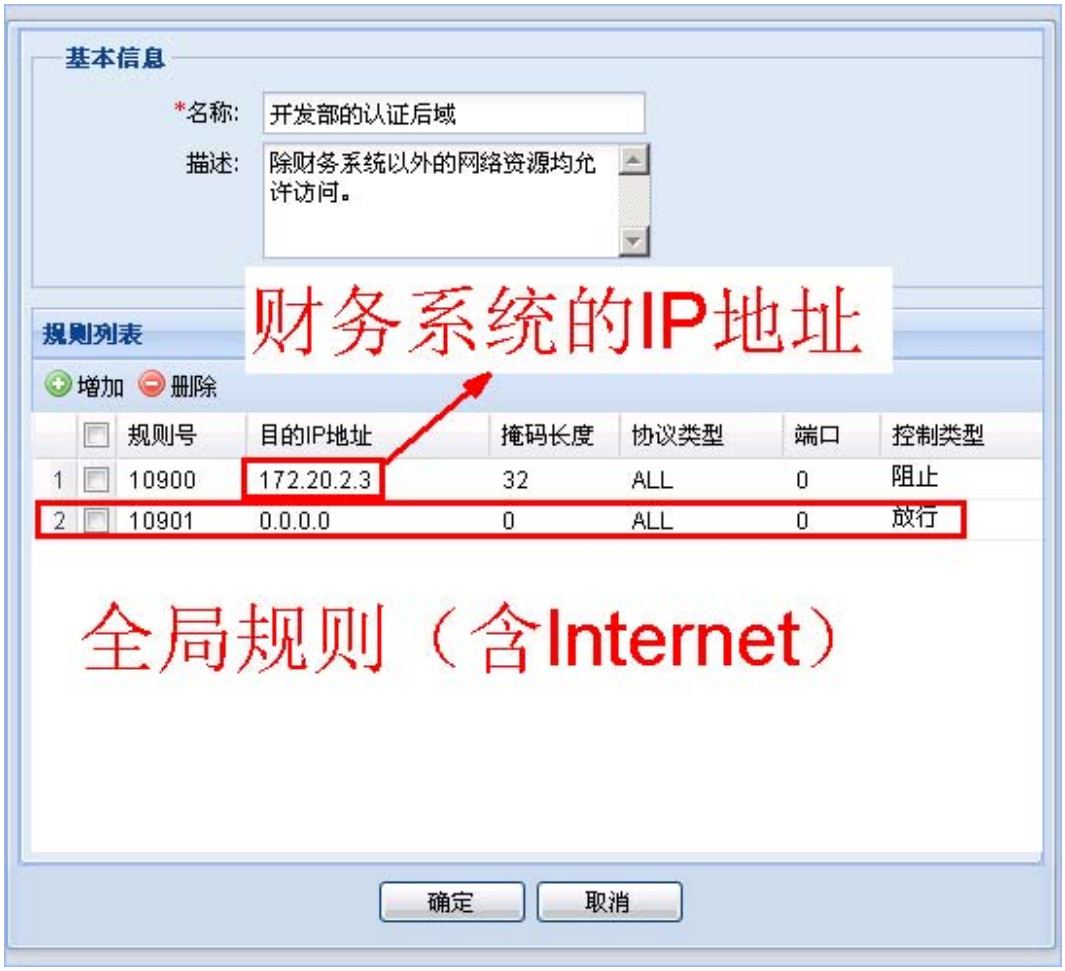
7. 输入规则的相关参数。单击“确定”，完成规则的配置并返回隔离域配置对话框。
8. 单击“确定”，出现“增加成功”对话框。
9. 单击“确定”，完成隔离域的配置。

----结束

配置认证后域

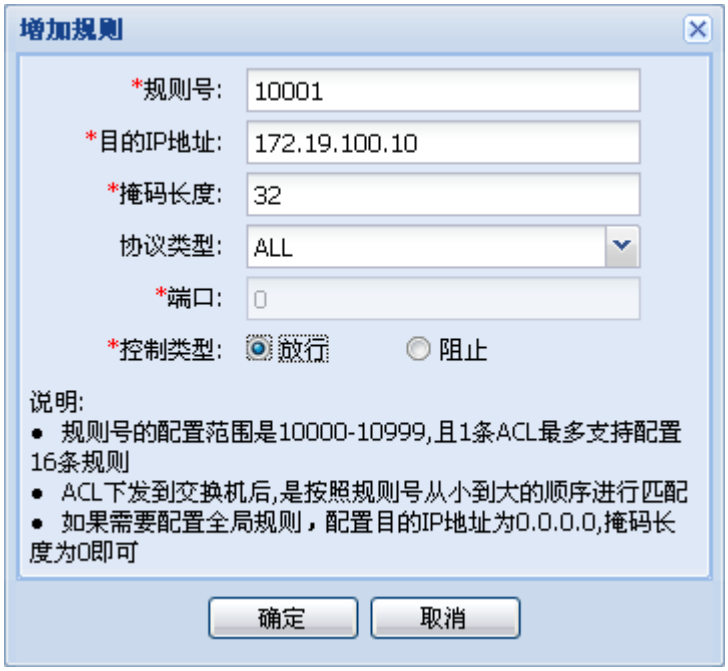
1. 在 TSM 管理器顶部单击“接入控制”。
2. 在左侧的菜单栏中选择“接入控制配置 > PORTAL 网关”。
3. 选择“后域”页签。
4. 单击“增加”，出现认证后域配置对话框。

图6-24 认证后域配置



5. 输入认证后域的相关参数。
6. 单击“增加”。出现“增加规则”对话框。

图6-25 增加规则



7. 输入规则的相关参数。单击“确定”，完成规则的配置并返回认证后域配置对话框。
8. 单击“确定”，出现“增加成功”对话框。
9. 单击“确定”，完成认证后域的配置。

----结束

将隔离域和认证后域应用到部门

1. 在 TSM 管理器的导航栏单击“部门管理”。
2. 在左侧菜单栏选择“部门用户 > 部门用户管理”。
3. 选择“部门”页签。
4. 在部门导航树中选中待应用隔离域和认证后域的部门，然后在工具栏单击“部门接入控制管理”。
5. 选择“自定义设置”。
6. 选择“PORTAL 网关”页签。
7. 设置开发部的隔离域和认证后域。

图6-26 设置部门的隔离域和认证后域

8. 单击“确定”，出现“设置成功”对话框。
9. 单击“确定”，完成隔离域和认证后域到部门的应用。

----结束

6.3.4 配置 802.1x 认证控制

注意

本节所描述的配置步骤和过程是基于 802.1x 标准协议(交换机组中的交换机类型选择除“华为 NAC 系列”之外的类型)，该种方式下无法基于部门和角色对用户权限进行控制。

如果选择的是华为 NAC 系列，则还可以配置隔离域、认证后域，并应用到部门或者具体账号。主要注意的是，802.1x 认证中的隔离域和认证后域的配置方式与 Portal 认证的配置方式有所不同，相关详细配置请参考 TSM Server 的帮助文档。

配置交换机组

1. 在 TSM 管理器的导航栏单击“接入控制”。
2. 在左侧菜单栏选择“接入控制配置 > 802.1x 交换机”。
3. 选择“交换机组”页签。
4. 单击“增加”，输入交换机组的相关参数。

图6-27 输入交换机组的相关参数

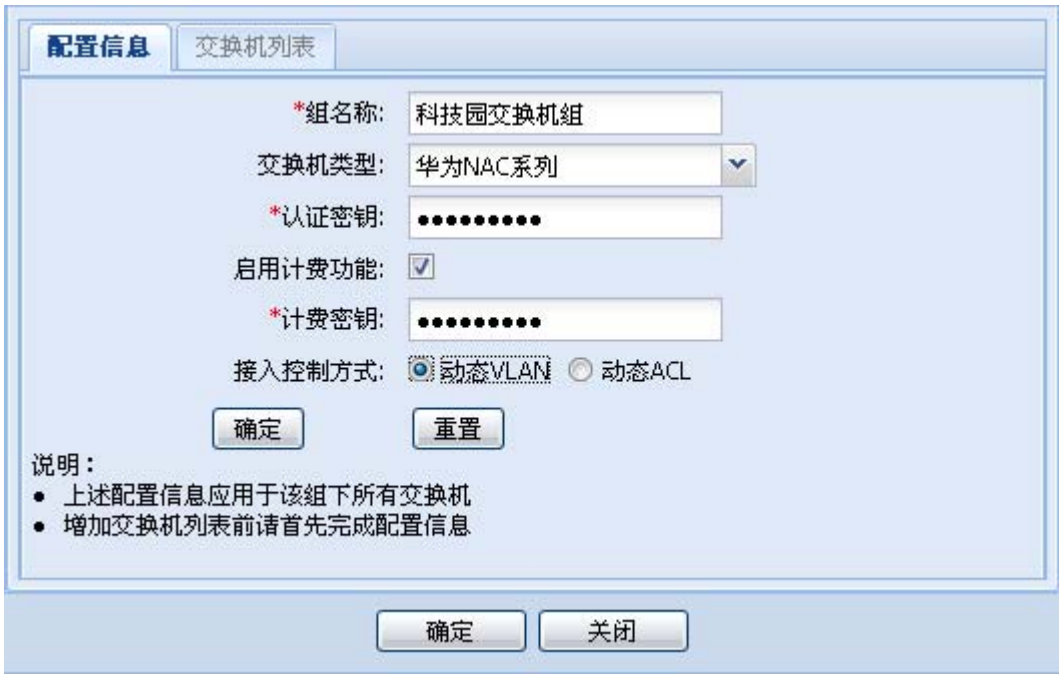


表6-4 增加交换机组的参数说明

参数	说明
组名称	输入交换机组的唯一名称。
交换机类型	选择该交换机组中交换机的厂家类型，未在下拉列表中单独列出的交换机类型，请选择其他类型。
认证密钥	交换机上配置的与 TSM 控制器通信的认证加密密钥。
启用计费功能	少数交换机需要启用计费功能，才能使认证通过的终端主机长时间保持端口开放，服务器上配置启用该功能用于配合交换机完成计费。
计费密钥	如果配置启用计费功能，此处填写交换机上配置的计费加密密钥。

参数	说明
接入控制方式	当“交换机类型”设置为“华为 NAC 系列”时，设置是通过“动态 VLAN”还是“动态 ACL”来实现接入控制。在使用标准 802.1x 协议的交换机实施接入控制时不能选择接入控制方式。

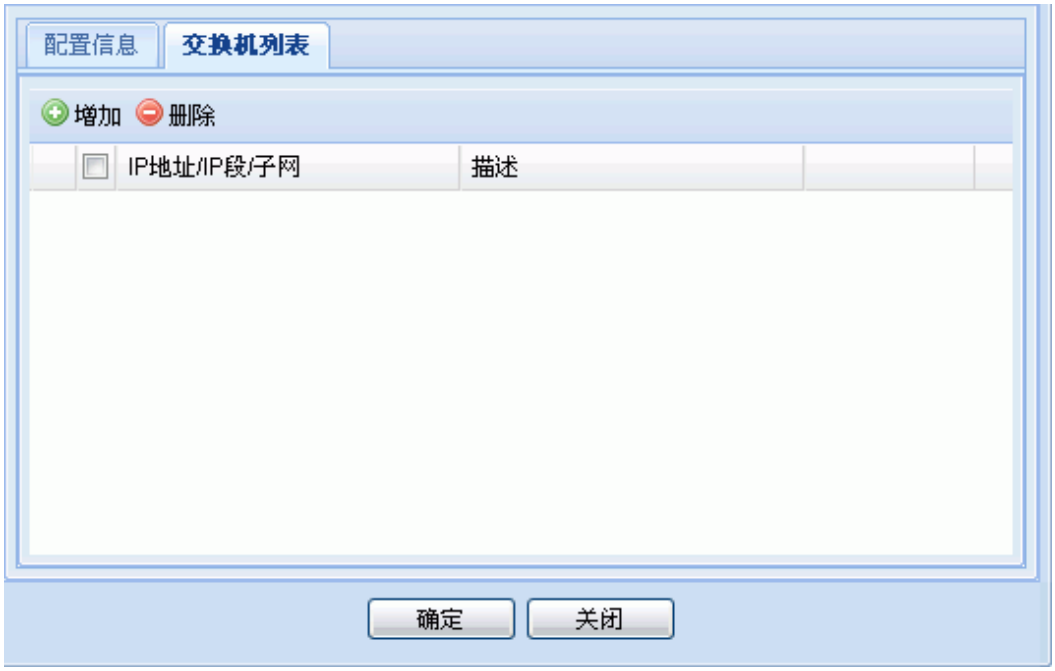
5. 单击“确定”，出现“保存配置信息成功”对话框。
6. 单击“确定”，完成交换机组的配置。

----结束

配置交换机列表

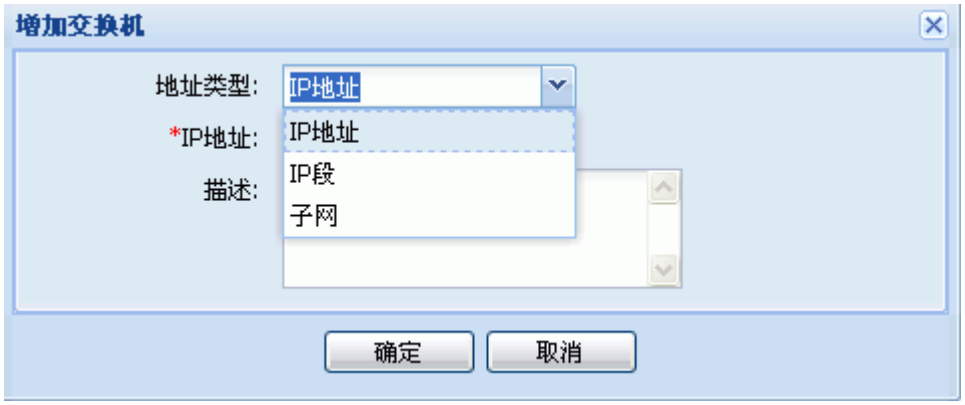
配置交换机组成功后，会自动跳转到交换机列表界面。

图6-28 交换机列表



1. 单击“增加”，出现“增加交换机”对话框。

图6-29 增加交换机



2. 输入交换机的参数。

表6-5 增加交换机的参数说明

参数	说明
地址类型	• IP 地址：通过增加 IP 地址增加一台交换机。 • IP 段：指定一个地址段，该 IP 地址段中的所有地址均是交换机的 IP 地址。 • 子网：通过地址 + 掩码的方式指定一个子网，该子网中所有的 IP 地址均为交换机的 IP 地址。 交换机可能配置了多个 IP 地址，NAS-IP 是交换机专门供 RADIUS 通信用的地址，添加的交换机 IP 地址必须是交换机的 NAS-IP，否则会产生“radius no response”错误。 如果交换机没有提供配置 NAS-IP 的命令，则应在交换机路由表中查找到达 TSM 控制器的出接口，出接口对应的 IP 地址作为添加交换机时输入的 IP 地址。
描述	输入交换机的描述信息，方便管理员维护该交换机列表。

3. 单击“确定”，出现“增加交换机成功”对话框。
4. 单击“确定”，完成交换机的配置。

----结束

6.4 配置 TSM Agent

注意

很多情况下，TSM Agent 的安装程序已经根据企业的部署需求，由网络管理员或华为技术支持工程师完成定制，此时终端用户只需要完成软件的安装后，即可进行认证并接入网络，无需进行额外的配置。

1. 在终端上安装 TSM Agent 软件，具体过程略。

   安装完成后，Windows 桌面的系统托盘中会出现 TSM Agent 的图标。表示终端用户未进行认证。

2. 双击图标，打开 TSM Agent 认证界面。

   图6-30 TSM Agent 认证界面

3. 在账号和密码框中分别输入用户名和密码。然后根据需要选择是否“保存密码”和“自动认证”。

   说明

   用户名和密码必须已在 TSM 服务器上注册，详细过程请参见“6.3.1 配置普通账号”或者“6.3.2 配置按 OU 方式同步 AD 域账号信息”。

4. 如果是首次使用 TSM Agent，则单击“高级设置”按钮，展开高级设置选项。

   a. 在“服务器”中输入 TSM 认证服务器的 IP 地址。

   b. 如果要使用 802.1x 认证，则选中“启用 802.1x 协议”复选框，并且根据需要选择是否启用安全认证（推荐启用）以及 802.1x 的接入协议（推荐使用标准协议即可）。如果使用 Portal 认证，则不选中“启用 802.1x 协议”复选框。

   c. 单击“保存”按钮，保存所有的高级设置。

图6-31 TSM Agent 认证高级选项

5. 单击“认证”按钮，客户端发起认证。

图6-32 TSM Agent 发起认证

如果认证通过，则系统托盘中的图标变成，表示终端用户成功通过身份认证和安全认证。用户可以正常访问网络。

说明

如果系统托盘中的图标为，表示终端用户已经通过安全认证，但是终端主机存在违规信息。如果系统托盘中的图标为，表示终端用户未通过安全认证，终端主机的网络访问受限。

----结束

注意

上述配置过程是以普通账号来进行举例的。在企业网络中，用户也可以通过 AD 域账号进行认证。如图 6-33 所示。

如果用户使用 AD 域账号登录，则需要注意以下几点：

- 需要另外部署域控制服务器，在域服务器上配置用户名和密码。有关于控制服务器的配置请按照相关产品的文档指导进行。
- TSM 服务器上只需要同步配置 AD 域用户账号。请参考“6.3.2 配置按 OU 方式同步 AD 域账号信息”。
- 用户终端需要加入域，详细配置请参考终端操作系统（例如 Windows）的帮助文档。

图6-33 使用 AD 域账号进行认证

6.5 配置举例

6.5.1 部署基于 802.1x 认证的 NAC 系统

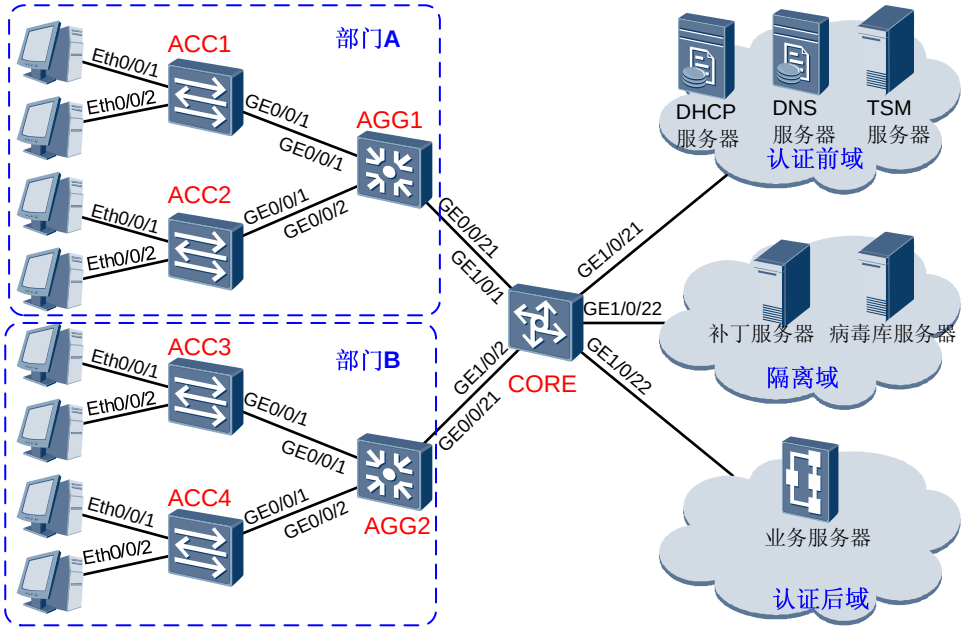
组网需求

企业的园区网中，将网络分为接入、汇聚和核心三层。在接入层交换机上，使用 802.1x 认证对部门 A 和部门 B 的接入用户进行认证，认证服务器使用 TSM Server。如图 6-34 所示。

园区中的数据中心分为认证前域（包括 DHCP 服务器、DNS 服务器和 TSM 服务器）、隔离域（包括补丁服务器和病毒库服务器）和认证后域（企业的业务服务器）。用户未

认证前只能访问认证前域。用户通过认证后，如果终端不安全，则只能访问隔离域中的服务器进行补丁修复和病毒库升级。当用户通过认证并且终端安全时，可正常访问业务服务器。

图6-34 基于 802.1x 认证的 NAC 系统组网图



数据准备

表6-6 数据规划表

配置项	配置子项	数据
接口和 VLAN	ACC1~ACC2	用户认证前 VLAN：11 用户隔离 VLAN：12 用户认证后 VLAN：13 交换机上行 VLAN：14
	AGG3~ACC4	用户认证前 VLAN：21 用户隔离 VLAN：22 用户认证后 VLAN：23 交换机上行 VLAN：24
	AGG1	上行 VLAN：101
	AGG2	上行 VLAN：102
	CORE	认证前域 VLAN：201 隔离域 VLAN：202 认证后域 VLAN：203

配置项	配置子项	数据
设备 IP 地址	ACC1	VLANIF 14：192.168.14.2/24
	ACC2	VLANIF 14：192.168.14.3/24
	ACC3	VLANIF 24：192.168.24.2/24
	ACC4	VLANIF 24：192.168.24.3/24
	AGG1	VLANIF 11：192.168.11.1/24 VLANIF 12：192.168.12.1/24 VLANIF 13：192.168.13.1/24 VLANIF 14：192.168.14.1/24 VLANIF 101：192.168.101.1/24 Loopback0：2.2.2.2/32
	AGG2	VLANIF 21：192.168.21.1/24 VLANIF 22：192.168.22.1/24 VLANIF 23：192.168.23.1/24 VLANIF 24：192.168.24.1/24 VLANIF 102：192.168.102.1/24 Loopback0：3.3.3.3/32
	CORE	VLANIF 101：192.168.101.2/24 VLANIF 102：192.168.102.2/24 VLANIF 201：192.168.201.1/24 VLANIF 202：192.168.202.1/24 VLANIF 203：192.168.203.1/24 Loopback0：1.1.1.1/32
服务器 IP 地址	TSM 服务器	192.168.201.2
	DHCP 服务器	192.168.201.3
	DNS 服务器	192.168.201.4
	补丁服务器	192.168.202.2
	病毒库服务器	192.168.202.3
	业务服务器	192.168.203.2

操作步骤

1. 配置接口和 VLAN。

配置接入交换机 ACC1 的接口和 VLAN。

```
<ACC1> system-view
[ACC1] vlan batch 11 to 14
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet0/0/1] port link-type trunk
[ACC1-GigabitEthernet0/0/1] port trunk allow-pass vlan 11 to 14
[ACC1-GigabitEthernet0/0/1] quit
[ACC1] interface vlanif 14
[ACC1-Vlanif14] ip address 192.168.14.2 255.255.255.0
[ACC1-Vlanif14] quit
```

说明

当需要把用户侧接口配置为 802.1x 认证时，不要配置接口类型，使用默认的 Hybrid 类型即可。也不要配置默认 VLAN。

ACC2 的配置与 ACC1 相似，但 VLANIF 14 的 IP 地址为 192.168.14.3。

配置接入交换机 ACC3 的接口和 VLAN。

```
<ACC3> system-view
[ACC3] vlan batch 21 to 24
[ACC3] interface GigabitEthernet 0/0/1
[ACC3-GigabitEthernet0/0/1] port link-type trunk
[ACC3-GigabitEthernet0/0/1] port trunk allow-pass vlan 21 to 24
[ACC3-GigabitEthernet0/0/1] quit
[ACC3] interface vlanif 24
[ACC3-Vlanif24] ip address 192.168.24.2 255.255.255.0
[ACC3-Vlanif24] quit
```

ACC4 的配置与 ACC3 相似，但是 VLANIF 14 的 IP 地址为 192.168.24.3。

配置汇聚交换机 AGG1 的接口和 VLAN。

```
<AGG1> system-view
[AGG1] vlan batch 11 to 14 101
[AGG1] interface GigabitEthernet 0/0/1
[AGG1-GigabitEthernet0/0/1] port link-type trunk
[AGG1-GigabitEthernet0/0/1] port trunk allow-pass vlan 11 to 14
[AGG1-GigabitEthernet0/0/1] quit
[AGG1] interface GigabitEthernet 0/0/2
[AGG1-GigabitEthernet0/0/2] port link-type trunk
[AGG1-GigabitEthernet0/0/2] port trunk allow-pass vlan 11 to 14
[AGG1-GigabitEthernet0/0/2] quit
[AGG1] interface GigabitEthernet 0/0/21
[AGG1-GigabitEthernet0/0/21] port link-type trunk
[AGG1-GigabitEthernet0/0/21] port trunk allow-pass vlan 101
[AGG1-GigabitEthernet0/0/21] quit
[AGG1] interface vlanif 11
[AGG1-Vlanif11] ip address 192.168.11.1 255.255.255.0
[AGG1-Vlanif11] quit
[AGG1] interface vlanif 12
[AGG1-Vlanif12] ip address 192.168.12.1 255.255.255.0
[AGG1-Vlanif12] quit
[AGG1] interface vlanif 13
[AGG1-Vlanif13] ip address 192.168.13.1 255.255.255.0
[AGG1-Vlanif13] quit
```

```
[AGG1] interface vlanif 14
[AGG1-Vlanif14] ip address 192.168.14.1 255.255.255.0
[AGG1-Vlanif14] quit
[AGG1] interface vlanif 101
[AGG1-Vlanif101] ip address 192.168.101.1 255.255.255.0
[AGG1-Vlanif101] quit
```

配置汇聚交换机 AGG2 的接口和 VLAN。

```
<AGG2> system-view
[AGG2] vlan batch 21 to 24 102
[AGG2] interface GigabitEthernet 0/0/1
[AGG2-GigabitEthernet0/0/1] port link-type trunk
[AGG2-GigabitEthernet0/0/1] port trunk allow-pass vlan 21 to 24
[AGG2-GigabitEthernet0/0/1] quit
[AGG2] interface GigabitEthernet 0/0/2
[AGG2-GigabitEthernet0/0/2] port link-type trunk
[AGG2-GigabitEthernet0/0/2] port trunk allow-pass vlan 21 to 24
[AGG2-GigabitEthernet0/0/2] quit
[AGG2] interface GigabitEthernet 0/0/21
[AGG2-GigabitEthernet0/0/21] port link-type trunk
[AGG2-GigabitEthernet0/0/21] port trunk allow-pass vlan 102
[AGG2-GigabitEthernet0/0/21] quit
[AGG2] interface vlanif 21
[AGG2-Vlanif21] ip address 192.168.21.1 255.255.255.0
[AGG2-Vlanif21] quit
[AGG2] interface vlanif 22
[AGG2-Vlanif22] ip address 192.168.22.1 255.255.255.0
[AGG2-Vlanif22] quit
[AGG2] interface vlanif 23
[AGG2-Vlanif23] ip address 192.168.23.1 255.255.255.0
[AGG2-Vlanif23] quit
[AGG2] interface vlanif 24
[AGG2-Vlanif24] ip address 192.168.24.1 255.255.255.0
[AGG2-Vlanif24] quit
[AGG2] interface vlanif 102
[AGG2-Vlanif102] ip address 192.168.102.1 255.255.255.0
[AGG2-Vlanif102] quit
```

配置核心交换机 CORE 的接口和 VLAN。

```
<CORE> system-view
[CORE] vlan batch 101 to 102 201 to 203
[CORE] interface GigabitEthernet 1/0/1
[CORE-GigabitEthernet1/0/1] port link-type trunk
[CORE-GigabitEthernet1/0/1] port trunk allow-pass vlan 101
[CORE-GigabitEthernet1/0/1] quit
[CORE] interface GigabitEthernet 1/0/2
[CORE-GigabitEthernet1/0/1] port link-type trunk
[CORE-GigabitEthernet1/0/1] port trunk allow-pass vlan 102
[CORE-GigabitEthernet1/0/1] quit
[CORE] interface GigabitEthernet 1/0/21
[CORE-GigabitEthernet1/0/21] port link-type trunk
[CORE-GigabitEthernet1/0/21] port trunk allow-pass vlan 201
[CORE-GigabitEthernet1/0/21] quit
[CORE] interface GigabitEthernet 1/0/22
[CORE-GigabitEthernet1/0/22] port link-type trunk
```

```
[CORE-GigabitEthernet1/0/22] port trunk allow-pass vlan 202
[CORE-GigabitEthernet1/0/22] quit
[CORE] interface GigabitEthernet 1/0/23
[CORE-GigabitEthernet1/0/23] port link-type trunk
[CORE-GigabitEthernet1/0/23] port trunk allow-pass vlan 203
[CORE-GigabitEthernet1/0/23] quit
[CORE] interface vlanif 101
[CORE-Vlanif101] ip address 192.168.101.2 255.255.255.0
[CORE-Vlanif101] quit
[CORE] interface vlanif 102
[CORE-Vlanif102] ip address 192.168.102.2 255.255.255.0
[CORE-Vlanif102] quit
[CORE] interface vlanif 201
[CORE-Vlanif201] ip address 192.168.201.1 255.255.255.0
[CORE-Vlanif201] quit
[CORE] interface vlanif 202
[CORE-Vlanif202] ip address 192.168.202.1 255.255.255.0
[CORE-Vlanif202] quit
[CORE] interface vlanif 203
[CORE-Vlanif203] ip address 192.168.203.1 255.255.255.0
[CORE-Vlanif203] quit
```

2. 配置路由协议。

   # 配置 AGG1 上的路由协议。

```
[AGG1] interface LoopBack 0
[AGG1-LoopBack0] ip address 2.2.2.2 32
[AGG1-LoopBack0] quit
[AGG1] ospf 1
[AGG1-ospf-1] area 0
[AGG1-ospf-1-area-0.0.0.0] network 192.168.11.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 192.168.12.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 192.168.13.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 192.168.14.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 192.168.101.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[AGG1-ospf-1-area-0.0.0.0] quit
```

   # 配置 AGG2 上的路由协议。

```
[AGG2] interface LoopBack 0
[AGG2-LoopBack0] ip address 3.3.3.3 32
[AGG2-LoopBack0] quit
[AGG2] ospf 1
[AGG2-ospf-1] area 0
[AGG2-ospf-1-area-0.0.0.0] network 192.168.21.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 192.168.22.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 192.168.23.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 192.168.24.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 192.168.102.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[AGG2-ospf-1-area-0.0.0.0] quit
```

   # 配置 CORE1 上的路由协议。

```
[CORE1] interface LoopBack 0
```

```
[CORE1-LoopBack0] ip address 1.1.1.1 32
[CORE1-LoopBack0] quit
[CORE1] ospf 1
[CORE1-ospf-1] area 0
[CORE1-ospf-1-area-0.0.0.0] network 192.168.101.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.102.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.201.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.202.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.203.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[CORE1-ospf-1-area-0.0.0.0] quit
```

3. 配置 DHCP。

   # 在 DHCP 服务器上分别配置如下 6 个地址池：

   - 地址池 1：192.168.11.0/24，网关地址：192.168.11.1，DNS 地址：192.168.201.4
   - 地址池 2：192.168.12.0/24，网关地址：192.168.12.1，DNS 地址：192.168.201.4
   - 地址池 3：192.168.13.0/24，网关地址：192.168.13.1，DNS 地址：192.168.201.4
   - 地址池 4：192.168.21.0/24，网关地址：192.168.21.1，DNS 地址：192.168.201.4
   - 地址池 5：192.168.22.0/24，网关地址：192.168.22.1，DNS 地址：192.168.201.4
   - 地址池 6：192.168.23.0/24，网关地址：192.168.23.1，DNS 地址：192.168.201.4

   具体配置过程略。

   # 配置 ACC1 上的 DHCP Snooping 功能。

```
[ACC1] dhcp enable
[ACC1] dhcp snooping enable
[ACC1] interface Ethernet 0/0/1
[ACC1-Ethernet0/0/1] dhcp snooping enable
[ACC1-Ethernet0/0/1] quit
[ACC1] interface Ethernet 0/0/2
[ACC1-Ethernet0/0/2] dhcp snooping enable
[ACC1-Ethernet0/0/2] quit
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet0/0/1] dhcp snooping enable
[ACC1-GigabitEthernet0/0/1] dhcp snooping trusted
[ACC1-GigabitEthernet0/0/1] quit
```

   ACC2、ACC3、ACC4 的配置与 ACC1 相同。

   # 配置 AGG1 上的 DHCP Relay 功能。

```
[AGG1] dhcp enable
[AGG1] dhcp server group group1
[AGG1-dhcp-server-group-group1] dhcp-server 192.168.201.3
[AGG1-dhcp-server-group-group1] quit
[AGG1] interface vlanif 11
[AGG1-Vlanif11] dhcp select relay
[AGG1-Vlanif11] dhcp relay server-select group1
[AGG1-Vlanif11] quit
[AGG1] interface vlanif 12
[AGG1-Vlanif12] dhcp select relay
[AGG1-Vlanif12] dhcp relay server-select group1
```

```
[AGG1-Vlanif12] quit
[AGG1] interface vlanif 13
[AGG1-Vlanif13] dhcp select relay
[AGG1-Vlanif13] dhcp relay server-select group1
[AGG1-Vlanif13] quit
```

配置 AGG2 上的 DHCP Relay 功能。

```
[AGG2] dhcp enable
[AGG2] dhcp server group group1
[AGG2-dhcp-server-group-group1] dhcp-server 192.168.201.3
[AGG2-dhcp-server-group-group1] quit
[AGG2] interface vlanif 21
[AGG2-Vlanif21] dhcp select relay
[AGG2-Vlanif21] dhcp relay server-select group1
[AGG2-Vlanif21] quit
[AGG2] interface vlanif 22
[AGG2-Vlanif22] dhcp select relay
[AGG2-Vlanif22] dhcp relay server-select group1
[AGG2-Vlanif22] quit
[AGG2] interface vlanif 23
[AGG2-Vlanif23] dhcp select relay
[AGG2-Vlanif23] dhcp relay server-select group1
[AGG2-Vlanif23] quit
```

4. 配置 AAA 功能。

配置 ACC1 上的 AAA 功能。

```
[ACC1] radius-server template tsm
[ACC1-radius-tsm] radius-server authentication 192.168.201.2 1812
[ACC1-radius-tsm] undo radius-server user-name domain-included
[ACC1-radius-tsm] quit
[ACC1] radius-server authorization 192.168.201.2 shared-key simple hello
[ACC1] aaa
[ACC1-aaa] authentication-scheme tsm
[ACC1-aaa-authen-tsm] authentication-mode radius
[ACC1-aaa-authen-tsm] quit
[ACC1-aaa] authorization-scheme tsm
[ACC1-aaa-author-tsm] authorization-mode if-authenticated
[ACC1-aaa-author-tsm] quit
[ACC1-aaa] domain default
[ACC1-aaa-domain-default] authentication-scheme tsm
[ACC1-aaa-domain-default] authorization-scheme tsm
[ACC1-aaa-domain-default] radius-server tsm
[ACC1-aaa-domain-default] quit
```

ACC2~ACC4 上的配置与 ACC1 相同。

5. 配置 802.1x 认证。

在 ACC1 上配置 802.1x 认证。

```
[ACC1] dot1x enable
[ACC1] dot1x authentication-method eap
[ACC1] interface Ethernet 0/0/1
[ACC1-Ethernet0/0/1] dot1x enable
[ACC1-Ethernet0/0/1] dot1x guest-vlan 11
```

```
[ACC1-Ethernet0/0/1] dot1x port-method port
[ACC1-Ethernet0/0/1] quit
[ACC1] interface Ethernet 0/0/2
[ACC1-Ethernet0/0/2] dot1x enable
[ACC1-Ethernet0/0/2] dot1x guest-vlan 11
[ACC1-Ethernet0/0/2] dot1x port-method port
[ACC1-Ethernet0/0/2] quit
```

ACC2 的配置与 ACC1 相同。

在 ACC3 上配置 802.1x 认证。

```
[ACC3] dot1x enable
[ACC3] dot1x authentication-method eap
[ACC3] interface Ethernet 0/0/1
[ACC3-Ethernet0/0/1] dot1x enable
[ACC3-Ethernet0/0/1] dot1x guest-vlan 21
[ACC3-Ethernet0/0/1] dot1x port-method port
[ACC3-Ethernet0/0/1] quit
[ACC3] interface Ethernet 0/0/2
[ACC3-Ethernet0/0/2] dot1x enable
[ACC3-Ethernet0/0/2] dot1x guest-vlan 21
[ACC3-Ethernet0/0/2] dot1x port-method port
[ACC3-Ethernet0/0/2] quit
```

ACC4 的配置与 ACC3 相同。

6. 配置 TSM 服务器。

   TSM 服务器上的配置请参考“6.3 配置 TSM 服务器”。

注意

在 TSM 服务器上需要配置隔离域和认证后域，并且为每个交换机指定隔离域和认证后域的动态 VLAN。ACC1 和 ACC2 的隔离域动态 VLAN 为 12，认证后域的动态 VLAN 为 13。ACC3 和 ACC4 的隔离域动态 VLAN 为 22，认证后域的动态 VLAN 为 23。

----结束

配置文件

- ACC1 配置文件

```
#
 sysname ACC1
#
 vlan batch 11 to 14
#
 dot1x enable
 dot1x authentication-method eap
#
 dhcp enable
 dhcp snooping enable
```

```
#
aaa
 authentication-scheme default
 authentication-scheme tsm
  authentication-mode radius
 authorization-scheme default
 authorization-scheme tsm
  authorization-mode if-authenticated
 accounting-scheme default
 domain default
  authentication-scheme tsm
  authorization-scheme tsm
  radius-server  tsm
 domain default_admin
#
interface Vlanif14
 ip address 192.168.14.2 255.255.255.0
#
interface Ethernet0/0/1
 dot1x enable
 dot1x max-user 1
 dot1x guest-vlan 11
 dot1x port-method port
 dhcp snooping enable
#
interface Ethernet0/0/2
 dot1x enable
 dot1x max-user 1
 dot1x guest-vlan 11
 dot1x port-method port
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 11 to 14
 dhcp snooping enable
 dhcp snooping trusted
#
return
```

ACC2 配置与 ACC1 相似，唯一不同的是 VLANIF14 的 IP 地址为 192.168.14.3。

- ACC3 配置文件

```
#
 sysname ACC3
#
 vlan batch 21 to 24
#
 dot1x enable
 dot1x authentication-method eap
#
 dhcp enable
 dhcp snooping enable
#
aaa
 authentication-scheme default
```



```
 authentication-scheme tsm
  authentication-mode radius
 authorization-scheme default
 authorization-scheme tsm
  authorization-mode if-authenticated
 accounting-scheme default
 domain default
  authentication-scheme tsm
  authorization-scheme tsm
  radius-server  tsm
 domain default_admin
#
interface Vlanif24
 ip address 192.168.24.2 255.255.255.0
#
interface Ethernet0/0/1
 dot1x enable
 dot1x max-user 1
 dot1x guest-vlan 21
 dot1x port-method port
 dhcp snooping enable
#
interface Ethernet0/0/2
 dot1x enable
 dot1x max-user 1
 dot1x guest-vlan 21
 dot1x port-method port
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 21 to 24
 dhcp snooping enable
 dhcp snooping trusted
#
return
```

ACC4 配置与 ACC3 相似，唯一不同的是 VLANIF24 的 IP 地址为 192.168.24.3。

- AGG1 配置文件

```
#
 sysname AGG1
#
  vlan batch 11 to 14 101
#
 dhcp enable
#
dhcp server group group1
 dhcp-server 192.168.201.3 0
#
interface Vlanif11
 ip address 192.168.11.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif12
```



```
 ip address 192.168.12.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif13
 ip address 192.168.13.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif14
 ip address 192.168.14.1 255.255.255.0
#
interface Vlanif101
 ip address 192.168.101.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 11 to 14
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 11 to 14
#
interface GigabitEthernet0/0/21
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 192.168.11.0 0.0.0.255
  network 192.168.12.0 0.0.0.255
  network 192.168.13.0 0.0.0.255
  network 192.168.14.0 0.0.0.255
  network 192.168.101.0 0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
return
```

- AGG2 配置文件

```
#
 sysname AGG2
#
  vlan batch 21 to 24 102
#
 dhcp enable
#
dhcp server group group1
 dhcp-server 192.168.201.3 0
#
interface Vlanif21
 ip address 192.168.21.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
```



```
#
interface Vlanif22
 ip address 192.168.22.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif23
 ip address 192.168.23.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif24
 ip address 192.168.24.1 255.255.255.0
#
interface Vlanif102
 ip address 192.168.102.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 21 to 24
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 21 to 24
#
interface GigabitEthernet0/0/21
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 192.168.21.0 0.0.0.255
  network 192.168.22.0 0.0.0.255
  network 192.168.23.0 0.0.0.255
  network 192.168.24.0 0.0.0.255
  network 192.168.102.0 0 0.0.0.255
  network 3.3.3.3 0.0.0.0
#
return
```

- CORE 的配置文件

```
#
 sysname CORE1
#
  vlan batch 101 to 102 201 to 203
#
interface Vlanif101
 ip address 192.168.101.2 255.255.255.0
#
interface Vlanif102
 ip address 192.168.102.2 255.255.255.0
#
interface Vlanif201
```



```
 ip address 192.168.201.1 255.255.255.0
#
interface Vlanif202
 ip address 192.168.202.1 255.255.255.0
#
interface Vlanif203
 ip address 192.168.203.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet1/0/21
 port link-type trunk
 port trunk allow-pass vlan 201
#
interface GigabitEthernet1/0/22
 port link-type trunk
 port trunk allow-pass vlan 202
#
interface GigabitEthernet1/0/23
 port link-type trunk
 port trunk allow-pass vlan 203
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 192.168.101.0 0.0.0.255
  network 192.168.102.0 0.0.0.255
  network 192.168.201.0 0.0.0.255
  network 192.168.202.0 0.0.0.255
  network 192.168.203.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
return
```

6.5.2 部署基于 Portal 认证的 NAC 系统

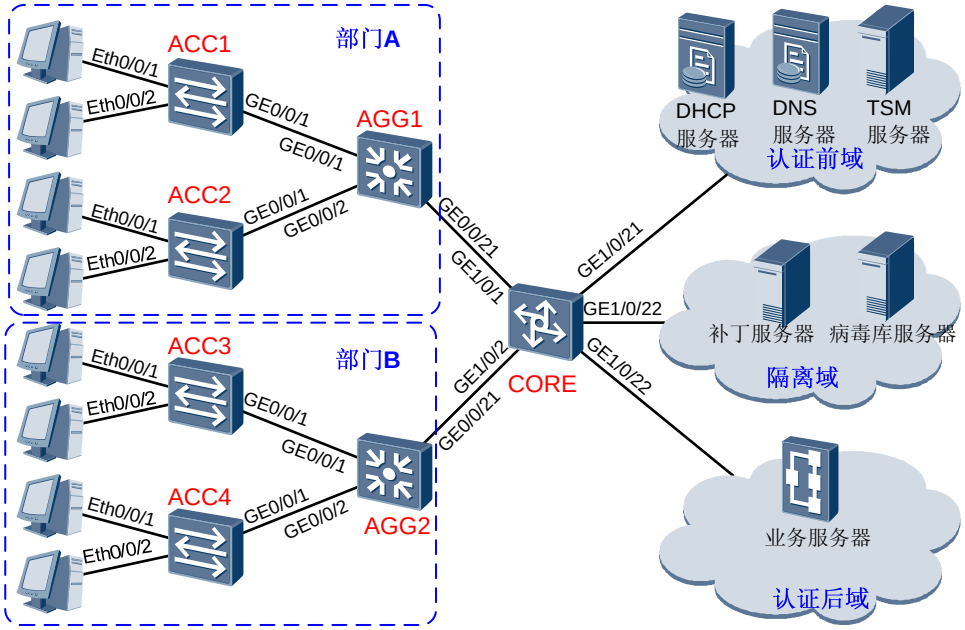
组网需求

企业的园区网中，将网络分为接入、汇聚和核心三层。在汇聚层交换机上，使用 Portal 认证对部门 A 和部门 B 的接入用户进行认证，认证服务器使用 TSM Server。如图 6-35 所示。

园区中的数据中心分为认证前域（包括 DHCP 服务器、DNS 服务器和 TSM 服务器）、隔离域（包括补丁服务器和病毒库服务器）和认证后域（企业的业务服务器）。用户未认证前只能访问认证前域。用户通过认证后，如果终端不安全，则只能访问隔离域中的

服务器进行补丁修复和病毒库升级。当用户通过认证并且终端安全时，可正常访问业务服务器。

图6-35 基于 Portal 认证的 NAC 系统组网图



数据准备

表6-7 数据规划表

配置项	配置子项	数据
接口和 VLAN	ACC1~ACC2	部门 A 用户接入 VLAN：11
	AGG3~ACC4	部门 B 用户接入 VLAN：12
	AGG1	上行 VLAN：101
	AGG2	上行 VLAN：102
	CORE	认证前域 VLAN：201 隔离域 VLAN：202 认证后域 VLAN：203
设备 IP 地址	AGG1	VLANIF 1：192.168.11.1/24 VLANIF 101：192.168.101.1/24 Loopback0：2.2.2.2/32
	AGG2	VLANIF 2：192.168.12.1/24 VLANIF 102：192.168.102.1/24 Loopback0：3.3.3.3/32

配置项	配置子项	数据
	CORE	VLANIF 101：192.168.101.2/24 VLANIF 102：192.168.102.2/24 VLANIF 201：192.168.201.1/24 VLANIF 202：192.168.202.1/24 VLANIF 203：192.168.203.1/24 Loopback0：1.1.1.1/32
服务器 IP 地址	TSM 服务器	192.168.201.2
	DHCP 服务器	192.168.201.3
	DNS 服务器	192.168.201.4
	补丁服务器	192.168.202.2
	病毒库服务器	192.168.202.3
	业务服务器	192.168.203.2

操作步骤

1. 配置接口和 VLAN。

   # 配置接入交换机 ACC1 的接口和 VLAN。

```
<ACC1> system-view
[ACC1] vlan batch 11
[ACC1] interface Ethernet 0/0/1
[ACC1-Ethernet0/0/1] port link-type access
[ACC1-Ethernet0/0/1] port default vlan 11
[ACC1-Ethernet0/0/1] quit
[ACC1] interface Ethernet 0/0/2
[ACC1-Ethernet0/0/2] port link-type access
[ACC1-Ethernet0/0/2] port default vlan 11
[ACC1-Ethernet0/0/2] quit
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet0/0/1] port link-type trunk
[ACC1-GigabitEthernet0/0/1] port trunk allow-pass vlan 11
[ACC1-GigabitEthernet0/0/1] quit
```

   ACC2 的配置与 ACC1 相同。

   # 配置接入交换机 ACC3 的接口和 VLAN。

```
<ACC3> system-view
[ACC3] vlan batch 12
[ACC3] interface Ethernet 0/0/1
[ACC3-Ethernet0/0/1] port link-type access
[ACC3-Ethernet0/0/1] port default vlan 12
[ACC3-Ethernet0/0/1] quit
```

```
[ACC3] interface Ethernet 0/0/2
[ACC3-Ethernet0/0/2] port link-type access
[ACC3-Ethernet0/0/2] port default vlan 12
[ACC3-Ethernet0/0/2] quit
[ACC3] interface GigabitEthernet 0/0/1
[ACC3-GigabitEthernet0/0/1] port link-type trunk
[ACC3-GigabitEthernet0/0/1] port trunk allow-pass vlan 12
[ACC3-GigabitEthernet0/0/1] quit
```

ACC4 的配置与 ACC3 相同。

配置汇聚交换机 AGG1 的接口和 VLAN。

```
<AGG1> system-view
[AGG1] vlan batch 11 101
[AGG1] interface GigabitEthernet 0/0/1
[AGG1-GigabitEthernet0/0/1] port link-type trunk
[AGG1-GigabitEthernet0/0/1] port trunk allow-pass vlan 11
[AGG1-GigabitEthernet0/0/1] quit
[AGG1] interface GigabitEthernet 0/0/2
[AGG1-GigabitEthernet0/0/2] port link-type trunk
[AGG1-GigabitEthernet0/0/2] port trunk allow-pass vlan 11
[AGG1-GigabitEthernet0/0/2] quit
[AGG1] interface GigabitEthernet 0/0/21
[AGG1-GigabitEthernet0/0/21] port link-type trunk
[AGG1-GigabitEthernet0/0/21] port trunk allow-pass vlan 101
[AGG1-GigabitEthernet0/0/21] quit
[AGG1] interface vlanif 11
[AGG1-Vlanif11] ip address 192.168.11.1 255.255.255.0
[AGG1-Vlanif11] quit
[AGG1] interface vlanif 101
[AGG1-Vlanif101] ip address 192.168.101.1 255.255.255.0
[AGG1-Vlanif101] quit
```

配置汇聚交换机 AGG2 的接口和 VLAN。

```
<AGG2> system-view
[AGG2] vlan batch 12 102
[AGG2] interface GigabitEthernet 0/0/1
[AGG2-GigabitEthernet0/0/1] port link-type trunk
[AGG2-GigabitEthernet0/0/1] port trunk allow-pass vlan 12
[AGG2-GigabitEthernet0/0/1] quit
[AGG2] interface GigabitEthernet 0/0/2
[AGG2-GigabitEthernet0/0/2] port link-type trunk
[AGG2-GigabitEthernet0/0/2] port trunk allow-pass vlan 12
[AGG2-GigabitEthernet0/0/2] quit
[AGG2] interface GigabitEthernet 0/0/21
[AGG2-GigabitEthernet0/0/21] port link-type trunk
[AGG2-GigabitEthernet0/0/21] port trunk allow-pass vlan 102
[AGG2-GigabitEthernet0/0/21] quit
[AGG2] interface vlanif 12
[AGG2-Vlanif12] ip address 192.168.12.1 255.255.255.0
[AGG2-Vlanif12] quit
[AGG2] interface vlanif 102
[AGG2-Vlanif102] ip address 192.168.102.1 255.255.255.0
[AGG2-Vlanif102] quit
```

配置核心交换机 CORE 的接口和 VLAN。

```
<CORE> system-view
[CORE] vlan batch 101 to 102 201 to 203
[CORE] interface GigabitEthernet 1/0/1
[CORE-GigabitEthernet1/0/1] port link-type trunk
[CORE-GigabitEthernet1/0/1] port trunk allow-pass vlan 101
[CORE-GigabitEthernet1/0/1] quit
[CORE] interface GigabitEthernet 1/0/2
[CORE-GigabitEthernet1/0/1] port link-type trunk
[CORE-GigabitEthernet1/0/1] port trunk allow-pass vlan 102
[CORE-GigabitEthernet1/0/1] quit
[CORE] interface GigabitEthernet 1/0/21
[CORE-GigabitEthernet1/0/21] port link-type trunk
[CORE-GigabitEthernet1/0/21] port trunk allow-pass vlan 201
[CORE-GigabitEthernet1/0/21] quit
[CORE] interface GigabitEthernet 1/0/22
[CORE-GigabitEthernet1/0/22] port link-type trunk
[CORE-GigabitEthernet1/0/22] port trunk allow-pass vlan 202
[CORE-GigabitEthernet1/0/22] quit
[CORE] interface GigabitEthernet 1/0/23
[CORE-GigabitEthernet1/0/23] port link-type trunk
[CORE-GigabitEthernet1/0/23] port trunk allow-pass vlan 203
[CORE-GigabitEthernet1/0/23] quit
[CORE] interface vlanif 101
[CORE-Vlanif101] ip address 192.168.101.2 255.255.255.0
[CORE-Vlanif101] quit
[CORE] interface vlanif 102
[CORE-Vlanif102] ip address 192.168.102.2 255.255.255.0
[CORE-Vlanif102] quit
[CORE] interface vlanif 201
[CORE-Vlanif201] ip address 192.168.201.1 255.255.255.0
[CORE-Vlanif201] quit
[CORE] interface vlanif 202
[CORE-Vlanif202] ip address 192.168.202.1 255.255.255.0
[CORE-Vlanif202] quit
[CORE] interface vlanif 203
[CORE-Vlanif203] ip address 192.168.203.1 255.255.255.0
[CORE-Vlanif203] quit
```

2. 配置路由协议。

配置 AGG1 上的路由协议。

```
[AGG1] interface LoopBack 0
[AGG1-LoopBack0] ip address 2.2.2.2 32
[AGG1-LoopBack0] quit
[AGG1] ospf 1
[AGG1-ospf-1] area 0
[AGG1-ospf-1-area-0.0.0.0] network 192.168.11.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 192.168.101.1 0.0.0.255
[AGG1-ospf-1-area-0.0.0.0] network 2.2.2.2 0.0.0.0
[AGG1-ospf-1-area-0.0.0.0] quit
```

配置 AGG2 上的路由协议。

```
[AGG2] interface LoopBack 0
```

```
[AGG2-LoopBack0] ip address 3.3.3.3 32
[AGG2-LoopBack0] quit
[AGG2] ospf 1
[AGG2-ospf-1] area 0
[AGG2-ospf-1-area-0.0.0.0] network 192.168.12.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 192.168.102.1 0.0.0.255
[AGG2-ospf-1-area-0.0.0.0] network 3.3.3.3 0.0.0.0
[AGG2-ospf-1-area-0.0.0.0] quit
```

配置 CORE1 上的路由协议。

```
[CORE1] interface LoopBack 0
[CORE1-LoopBack0] ip address 1.1.1.1 32
[CORE1-LoopBack0] quit
[CORE1] ospf 1
[CORE1-ospf-1] area 0
[CORE1-ospf-1-area-0.0.0.0] network 192.168.101.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.102.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.201.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.202.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 192.168.203.2 0.0.0.255
[CORE1-ospf-1-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[CORE1-ospf-1-area-0.0.0.0] quit
```

3. 配置 DHCP。

在 DHCP 服务器上分别配置如下两个地址池：

- 地址池 1：192.168.11.0/24，网关地址：192.168.11.1，DNS 地址：192.168.201.4
- 地址池 2：192.168.12.0/24，网关地址：192.168.12.1，DNS 地址：192.168.201.4

具体配置过程略。

配置 ACC1 上的 DHCP Snooping 功能。

```
[ACC1] dhcp enable
[ACC1] dhcp snooping enable
[ACC1] interface Ethernet 0/0/1
[ACC1-Ethernet0/0/1] dhcp snooping enable
[ACC1-Ethernet0/0/1] quit
[ACC1] interface Ethernet 0/0/2
[ACC1-Ethernet0/0/2] dhcp snooping enable
[ACC1-Ethernet0/0/2] quit
[ACC1] interface GigabitEthernet 0/0/1
[ACC1-GigabitEthernet0/0/1] dhcp snooping enable
[ACC1-GigabitEthernet0/0/1] dhcp snooping trusted
[ACC1-GigabitEthernet0/0/1] quit
```

ACC2、ACC3、ACC4 的配置与 ACC1 相同。

配置 AGG1 上的 DHCP Relay 功能。

```
[AGG1] dhcp enable
[AGG1] dhcp server group group1
[AGG1-dhcp-server-group-group1] dhcp-server 192.168.201.3
[AGG1-dhcp-server-group-group1] quit
[AGG1] interface vlanif 11
[AGG1-Vlanif11] dhcp select relay
```

```
[AGG1-Vlanif11] dhcp relay server-select group1
[AGG1-Vlanif11] quit
```

配置 AGG2 上的 DHCP Relay 功能。

```
[AGG2] dhcp enable
[AGG2] dhcp server group group1
[AGG2-dhcp-server-group-group1] dhcp-server 192.168.201.3
[AGG2-dhcp-server-group-group1] quit
[AGG2] interface vlanif 12
[AGG2-Vlanif12] dhcp select relay
[AGG2-Vlanif12] dhcp relay server-select group1
[AGG2-Vlanif12] quit
```

4. 配置 AAA 功能。

配置 AGG1 上的 AAA 功能。

```
[AGG1] radius-server template tsm
[AGG1-radius-tsm] radius-server authentication 192.168.201.2 1812
[AGG1-radius-tsm] undo radius-server user-name domain-included
[AGG1-radius-tsm] quit
[AGG1] radius-server authorization 192.168.201.2 shared-key simple hello
[AGG1] aaa
[AGG1-aaa] authentication-scheme tsm
[AGG1-aaa-authen-tsm] authentication-mode radius
[AGG1-aaa-authen-tsm] quit
[AGG1-aaa] authorization-scheme tsm
[AGG1-aaa-author-tsm] authorization-mode if-authenticated
[AGG1-aaa-author-tsm] quit
[AGG1-aaa] domain default
[AGG1-aaa-domain-default] authentication-scheme tsm
[AGG1-aaa-domain-default] authorization-scheme tsm
[AGG1-aaa-domain-default] radius-server tsm
[AGG1-aaa-domain-default] quit
```

AGG2 上的配置与 AGG1 相同。

5. 配置 Portal 认证。

在 AGG1 上配置 Portal 认证。

```
[AGG1] web-auth-server tsm
[AGG1-web-auth-server-tsm] server-ip 192.168.201.2
[AGG1-web-auth-server-tsm] port 50200
[AGG1-web-auth-server-tsm] shared-key simple hello
[AGG1-web-auth-server-tsm] url https://192.168.201.2:8443/SCServer/webauth.jsp
[AGG1-web-auth-server-tsm] quit
[AGG1] interface vlanif 11
[AGG1-Vlanif11] web-auth-server tsm
[AGG1-Vlanif11] quit
```

在 AGG2 上配置 Portal 认证。

```
[AGG2] web-auth-server tsm
[AGG2-web-auth-server-tsm] server-ip 192.168.201.2
[AGG2-web-auth-server-tsm] port 50200
[AGG2-web-auth-server-tsm] shared-key simple hello
```

```
[AGG2-web-auth-server-tsm] url https://192.168.201.2:8443/SCServer/webauth.jsp
[AGG2-web-auth-server-tsm] quit
[AGG2] interface vlanif 12
[AGG2-Vlanif12] web-auth-server tsm
[AGG2-Vlanif12] quit
```

6. 配置 TSM 服务器。

   TSM 服务器上的配置请参考“6.3 配置 TSM 服务器”。

----结束

配置文件

- ACC1 配置文件

```
#
 sysname ACC1
#
 vlan batch 11
#
 dhcp enable
 dhcp snooping enable
#
interface Ethernet0/0/1
 port link-type access
 port default vlan 11
 dhcp snooping enable
#
interface Ethernet0/0/2
 port link-type access
 port default vlan 11
 dhcp snooping enable
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 11
 dhcp snooping enable
 dhcp snooping trusted
#
return
```

ACC2~ACC4 配置类似。ACC2 配置 VLAN 是 11，ACC3~ACC4 配置 VLAN 是 12。

- AGG1 配置文件

```
#
 sysname AGG1
#
  vlan batch 11 101
#
 dhcp enable
#
web-auth-server tsm
 server-ip 192.168.201.2
 port 50200
 shared-key simple hello
```

```
 url https://192.168.201.2:8443/SCServer/webauth.jsp
#
dhcp server group group1
 dhcp-server 192.168.201.3 0
#
aaa
 authentication-scheme default
 authentication-scheme tsm
  authentication-mode radius
 authorization-scheme default
 authorization-scheme tsm
  authorization-mode if-authenticated
 accounting-scheme default
 domain default
  authentication-scheme tsm
  authorization-scheme tsm
  radius-server  tsm
 domain default_admin
#
interface Vlanif11
 web-auth-server tsm
 ip address 192.168.11.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif101
 ip address 192.168.101.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 11
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 11
#
interface GigabitEthernet0/0/21
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface LoopBack0
 ip address 2.2.2.2 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 192.168.11.0 0.0.0.255
  network 192.168.101.0 0 0.0.0.255
  network 2.2.2.2 0.0.0.0
#
return
```

- AGG2 配置文件

```
#
 sysname AGG2
#
  vlan batch 12 102
```



```
#
 dhcp enable
#
web-auth-server tsm
 server-ip 192.168.201.2
 port 50200
 shared-key simple hello
 url https://192.168.201.2:8443/SCServer/webauth.jsp
#
dhcp server group group1
 dhcp-server 192.168.201.3 0
#
aaa
 authentication-scheme default
 authentication-scheme tsm
  authentication-mode radius
 authorization-scheme default
 authorization-scheme tsm
  authorization-mode  if-authenticated
 accounting-scheme default
 domain default
  authentication-scheme tsm
  authorization-scheme tsm
  radius-server  tsm
 domain default_admin
#
interface Vlanif12
 web-auth-server tsm
 ip address 192.168.12.1 255.255.255.0
 dhcp select relay
 dhcp relay server-select group1
#
interface Vlanif102
 ip address 192.168.102.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 12
#
interface GigabitEthernet0/0/2
 port link-type trunk
 port trunk allow-pass vlan 12
#
interface GigabitEthernet0/0/21
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface LoopBack0
 ip address 3.3.3.3 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 192.168.12.0 0.0.0.255
  network 192.168.102.0 0 0.0.0.255
  network 3.3.3.3 0.0.0.0
```



```
#
return
```

- CORE 的配置文件

```
#
 sysname CORE1
#
  vlan batch 101 to 102 201 to 203
#
interface Vlanif101
 ip address 192.168.101.2 255.255.255.0
#
interface Vlanif102
 ip address 192.168.102.2 255.255.255.0
#
interface Vlanif201
 ip address 192.168.201.1 255.255.255.0
#
interface Vlanif202
 ip address 192.168.202.1 255.255.255.0
#
interface Vlanif203
 ip address 192.168.203.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 port link-type trunk
 port trunk allow-pass vlan 101
#
interface GigabitEthernet1/0/2
 port link-type trunk
 port trunk allow-pass vlan 102
#
interface GigabitEthernet1/0/21
 port link-type trunk
 port trunk allow-pass vlan 201
#
interface GigabitEthernet1/0/22
 port link-type trunk
 port trunk allow-pass vlan 202
#
interface GigabitEthernet1/0/23
 port link-type trunk
 port trunk allow-pass vlan 203
#
interface LoopBack0
 ip address 1.1.1.1 255.255.255.255
#
ospf 1
 area 0.0.0.0
  network 192.168.101.0 0.0.0.255
  network 192.168.102.0 0.0.0.255
  network 192.168.201.0 0.0.0.255
  network 192.168.202.0 0.0.0.255
  network 192.168.203.0 0.0.0.255
  network 1.1.1.1 0.0.0.0
#
```



```
return
```

7 VoIP 语音部署

7.1 概述

7.1.1 企业语音业务简介

在大型企业中，可以基于 IP 网络自建语音通信系统，可以使企业内部的语音通信不再需要通信费用，从而节省了企业的运营成本。

建设 IP 语音通信系统面临的挑战是如何在 IP 网络基础上，既可以保护原有投资和用户使用习惯，又可以让企业的语音业务和数据业务在同一张 IP 网络上协调运作，同时可以满足 IP 语音通信后续的发展及用户数量的扩容需求。

在企业中部署 IP 语音业务，需要重点考虑如下内容。

呼叫控制方案

呼叫控制方案分为集中式、分布式和混合型三种。

- 集中式呼叫控制

  企业总部集中部署 IP PBX（AR/SoftCo），分支机构的语音网关（VG）部署为 AG 形态，分支与企业总部之间通过 WAN/MAN 连接。

  总部与分支的语音用户全部注册到企业总部的 IP PBX。总部 IP PBX 为企业内所有用户提供呼叫控制服务，并且提供与本地运营商互通。

  集中式呼叫控制比较适合企业在同一个区域的情况。

- 分布式呼叫控制

  企业总部和各分支机构分别部署 IP PBX，分支与总部之间通过企业 IP 专网连接。总部与分支的 IP PBX 分别完成本地用户的注册和呼叫控制，总部 IP PBX 为各个分支互通提供呼叫路由，形成总部为一级呼叫路由，分支为二级呼叫路由的结构。

  总部和分支的 IP PBX 分别完成与当地运营商的 PTSN 网络的互通。

  分布式呼叫控制比较适合企业在不同区域的情况。

- 混合型呼叫控制

  混合型呼叫控制是上述两种方式的结合，该方案针对企业分布复杂，既有同区域分支，也有不同区域的分支的情况，分别采用不同的呼叫控制方式。如果某个区域有

多个分支，则可以选择其中较大的一个分支部署 IP PBX，而其余分支部署 AG，由大分支的 IP PBX 完成该区域所有分支的呼叫控制。

终端接入方式

在企业的 IP 语音通信系统中，主要的终端类型有模拟电话（POTS 话机）、IP 电话（SIP 话机）、PC 软终端和传真机等。

- POTS 话机接入

  POTS 话机的接入方式主要有如下几种：

  - POTS 话机通过 FXS 线路接到 AG，再接到 IP PBX。
  - POTS 话机通过 FXS 线路接到 IAD 设备，IAD 设备通过以太网接到 IP PBX。
  - POTS 话机通过 FXS 线路接到 TDM PBX 设备，TDM PBX 设备通过 E1 线路接到 IP PBX。
- SIP 话机接入

  SIP 话机通过 LAN 网络接入并注册到 IP PBX 设备。
- PC 软终端

  PC 软终端通过 LAN 网络接入并注册到 IP PBX 设备。
- 传真机接入

  传真机的接入方式与 POTS 话机接入方式相同。

原有电话系统接入

原有语音通信系统中有大量已有的投资，如 TDM PBX、POTS 话机，新建 IP 语音通信系统应充分考虑对原有投资的利用。对于企业语音通信系统的更新，原有设备的处理方案有二种方案：

- 原有连接 PSTN 网络的 TDM PBX 设备，将原来连接 PSTN 网络的 E1/FXO 接口切换接入到企业出口多业务路由器 AR 设备上，从而保证原有设备的充分利用。
- 对于 TDM PBX 设备下的语音用户比较多，同时还有一定扩容能力的 TDM PBX 设备，可以通过 E1 接口将 AR 的语音用户转到 TDM PBX 设备，再通过 TDM PBX 设备连接到 PSTN 网络。

号码规划

企业的号码规划一般有 DDI 方式和非 DDI 两种方式。

表7-1 号码规划方式

规划方式	说明
DDI 方式	• 企业内部的每部电话都有一个长号，同时企业内部将长号的后四位或后五位作为每部电话的短号，企业内部的拔号直接通过短号互拔。 • 企业拔打公网语音用户，则通过拔打出局字冠+被叫号码进行出局形成出局呼叫。 • 公网语音用户拔打企业语音用户时，可以直接使用企业语音用户的长号进行拔号通信。
非 DDI 方式	• 非 DDI 方式下的企业号码规划，企业内部的每部电话分配一个短号，企业内部的拔号直接通过短号互拔。 • 企业内部语音用户拔打公网语音用户时，通过 IP PBX 智能选择一个空闲出局号码，形成出局呼叫。 • 公网语音用户拔打企业语音用户时，外线先拔总机号码，再按照语音提示转发分机号码进行拔号通信。

对于不同类型的企业进行号码规划方式的选择建议如下：

- 外贸型企业，企业的语音通信主要是对外，建议采用 DDI 的方式进行企业语音用户的号码规划。
- 生产型企业，企业的语音通信主要是内部通信，建议采用非 DDI 方式进行企业语音用户的号码规划，同时根据对外的业务分析来确定企业内部语音用户拔打外线的收敛比例。

PSTN/PLMN 出局

PSTN/PLMN 出局主要有三个作用：

- 提供企业内部语音用户与 PSTN/PLMN 公网语音用户进行语音互通。
- 提供语音用户拔打有企业分支的地区时，通过企业 IP 网络出局到被叫语音用户所在地，再通过企业分支出局到 PSTN/PLMN 网络，从而使企业的长途通话，只花费被叫用户的本地市话费。
- 提供企业语音用户的故障保护，在总部与分支之间的 IP 网络出现问题后，企业的语音用户可以通过 PSTN/PLMN 网络进行语音用户保护。

对于集中式呼叫控制的企业，由企业总部的 IP PBX 统一出局，与 PSTN/PLMN 互通。各分支机构的 AG 设备不单独出局，但可通过 FXO 接口与本地 PSTN 连接，仅在发生故障时，通过 SRST 功能提供逃生保护。

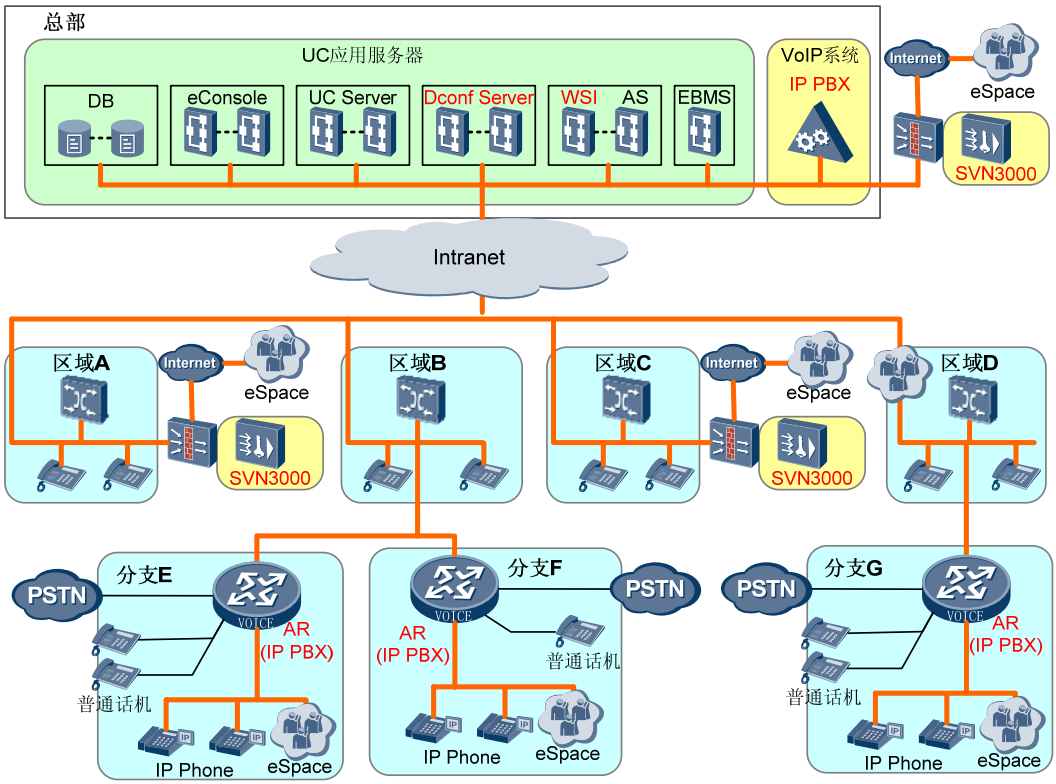
对于分布式呼叫控制的企业，各机构的 IP PBX 分别单独与当地 PSTN/PLMN 互通。

UC 系统部署

统一通信又称为 UC（Unified Communications），是指把计算机技术与传统通信技术融为一体的新通信模式，其核心内容是让人们无论任何时间、任何地点，都可以通过任何设备、任何网络，获得数据、图像和声音的自由通信。

在 VoIP 网络中增加 UC 服务器，可以平滑演进到 UC 统一通信系统。如图 7-1 所示。

图7-1 UC 系统示意图



- 总部部署

  在总部增加部署 AS、eServer、EBMS、eConsole 的服务器，实现 UC 控制。

  - AS 作为呼叫业务控制中心，所有软终端集中注册到 AS 上，软终端的业务由 AS 提供，座机保持原有部署不动，分散注册到各个代表处的 AR（IP PBX）上，并实现本地出局到 PSTN。
  - eServer 服务器作为数据业务控制中心，实现软终端之间的即时消息、状态呈现等数据业务。
  - EBMS 提供开销户受理接口。
  - eConsole 提供面向系统管理员等角色的管理功能，例如查询员工信息等。
  - 总部 IP PBX 作为语音网关，提供使用会议资源（即时会议）及 PSTN 出局功能。
  - 外网用户通过 SVN 实现语音、数据外网接入，SVN 服务器可集中部署在公司总部也可分布式部署在大区域的 DC。

- 大区域 DC 部署

  - SVN 负责各区域 Internet 用户的接入。
  - 部署 IP PBX 为区域中心用户提供 VoIP 业务，并通过 E1 实现本地 PSTN 落地。也可以通过 SIP Trunk 与运营商 IMS/NGN 网络互通。
  - 本区域中心的 IP PBX 为该区域下各个代表处间语音互通提供二级呼叫路由。

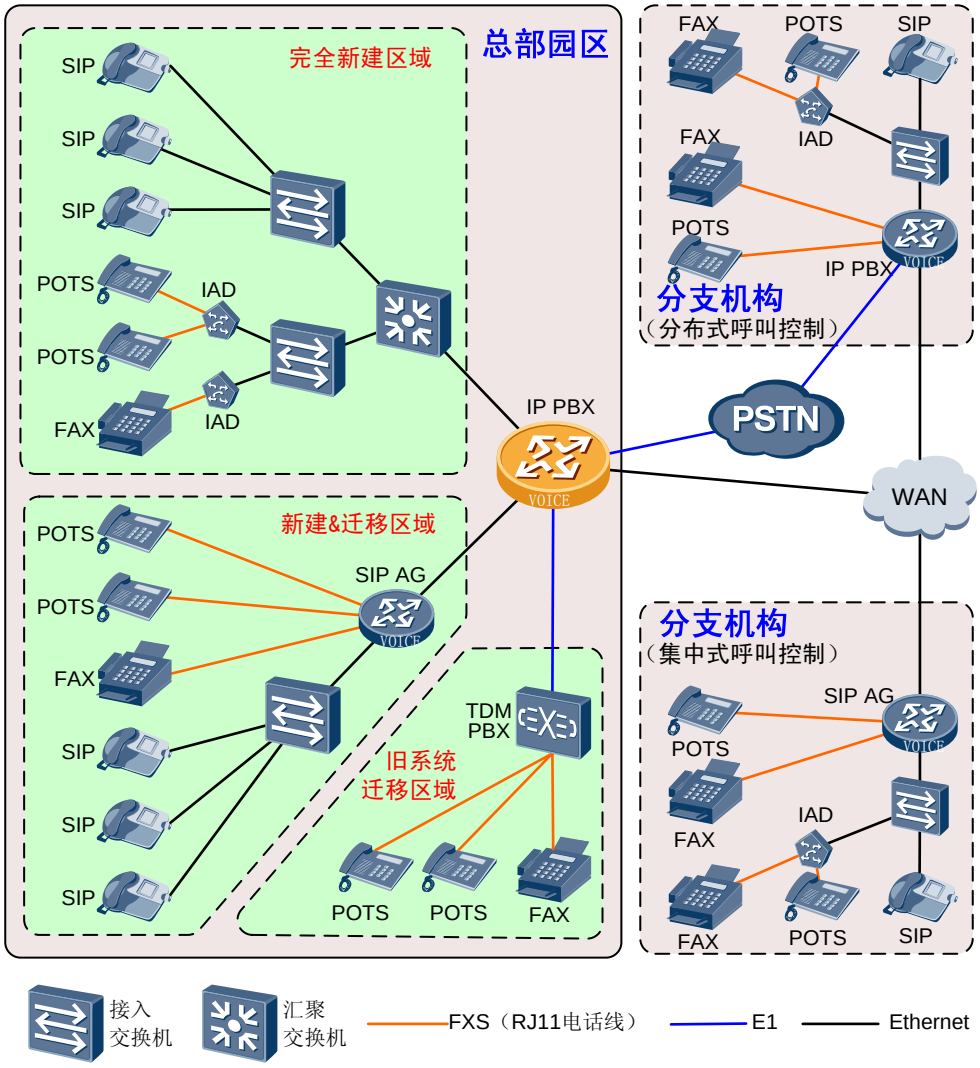
- 小分支（办事处）部署

部署 IP PBX，负责办事处语音接入，并通过 FXO/E1 实现本地 PSTN 落地。

7.1.2 典型组网

企业语音业务的典型组网如图 7-2 所示。

图7-2 企业语音业务典型组网



注意

关于 UC 系统部署的详细信息，请参考 UC 产品的相关文档，本章中不作详细介绍。

7.1.3 配套版本

表7-2 配套产品和版本

部件	产品	版本
IP PBX	SoftCo 系列产品	V100R002
	AR G3 系列产品	V200R001C01
SIP AG	AR G3 系列产品	V200R001C01
IAD	非特定，根据需要可选择华为生产的IAD101H/102H/104H/208E(M)/132E(T)/1280 等型号的 IAD 产品。	非特定
SIP 话机	非特定，根据需要可选择华为生产的HW ET325/523/525/635/655/685、HW MC820C/830C/850/851 等型号的产品。	非特定
接入交换机	非特定，推荐 S2700/S3700 系列	非特定
汇聚交换机	非特定，推荐 S5700/S7700 系列	非特定
POTS 话机	非特定	非特定
FAX	非特定	非特定
TDM PBX	非特定	非特定

7.2 配置网络互通

配置网络互通主要是在网络设备上配置接口、VLAN、IP 地址、路由等，以及在服务器上配置 IP 地址等，实现终端、网络设备、服务器之间的网络层互相连通。

详细的配置过程略，请参考相应产品的产品文档。

7.3 配置总部/分布式分支的 IP PBX

7.3.1 配置信令 IP 地址和媒体 IP 地址

1. 执行命令 **system-view**，进入系统视图
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **voip-address media** *interface interface-type interface-number* { *ip-address* | **dynamic** }，配置媒体 IP 地址池。

4. 执行命令 **voip-address signalling interface** *interface-type interface-number* { *ip-address* | **dynamic** }，配置信令 IP 地址池。

----结束

7.3.2 配置号码归属的企业、群、号首集

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **pbx**，进入 PBX 视图。
4. 执行命令 **enterprise** *enterprise-name*，创建企业并进入企业视图。
5. 执行命令 **centrex** *centrex-name* [**description** *description*]，创建 Centrex 群。
6. 执行命令 **dn-set** *dn-set-name* [**description** *description*]，配置企业的号首集。

----结束

7.3.3 配置 SIP 服务器

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **pbx**，进入 PBX 视图。
4. 执行命令 **sipserver**，进入 SIP 服务器视图。
5. 执行命令 **signalling-ip**{ *ip-address* | **signaling-addr-name** *signaling-addr-name-value* }，配置 SIP 服务器的信令 IP 地址或动态信令 IP 地址名称。
6. （可选）IP 服务器采用动态信令 IP 地址时，执行命令 **signalling-domain** *signaling-domain-value*，配置 SIP 服务器在采用动态信令 IP 地址时的信令域名。
7. （可选）执行命令 **ddns-client** *ddns-client-name*，配置 SIP 服务器在采用动态信令 IP 地址时的动态 DNS（DDNS）客户端名称。

   说明

   如果 SIP 服务器采用静态配置的信令 IP 地址，则不需要配置本步骤。

8. 执行命令 **signalling-port** *port-number*，配置 SIP 服务器的信令端口。
9. 执行命令 **media-ip** *ip-address*，配置 SIP 服务器的媒体 IP 地址。
10. 执行命令 **register-uri** *uri*，配置 SIP 服务器的 URI。
11. 执行命令 **home-domain** *domain*，配置 SIP 服务器的归属域。

----结束

7.3.4 配置字冠

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **pbx**，进入 PBX 视图。
4. 执行命令 **callprefix** *callprefix-name*，进入呼叫字冠模板视图。
5. 执行命令 **prefix** *prefix*，配置呼叫字冠。
6. 执行命令 **enterprise** *enterprise-name*，配置绑定企业和呼叫字冠。
7. 执行命令 **dn-set** *dn-set-name*，配置绑定号首集和呼叫字冠。
8. 执行命令 **call-type category** *callcategory* **attribute** *attribute*，配置呼叫字冠的呼叫类型和呼叫属性。
9. 执行命令 **maximum-length** *maximum-length*，配置最大号码分析长度。
10. 执行命令 **minimum-length** *minimum-length*，配置最小号码分析长度。

----结束

7.3.5 配置 PBX 用户

配置设备标识

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **pbxuser** *name*，增加一个 PBX 用户并进入 PBX 用户视图。
4. 执行命令 **type** { **port** *port-number* | **sipue** *eid-value* }，配置 PBX 用户类型。
5. 执行命令 **enterprise** *enterprise-name*，配置 PBX 用户所属的企业。

----结束

配置用户标识

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **dialno** *name*，增加 PBX 用户标识并进入 PBX 用户标识。
4. 执行命令 **pbxuser** *username*，绑定用户标识和 PBX 用户。
5. 执行命令 **telno** *countrycode areacode telno*，配置用户的国家码、地区码和电话号码。
6. 执行命令 **dn-set** *dn-set-name*，配置用户的国家码、地区码和电话号码。
7. （可选）执行命令 **centrex** *centrex-name centrex-telno-value*，配置用户所属的 Centrex 群。
8. （可选）执行命令 **callin-right** *inrightt-value*，配置呼入权限。
9. （可选）执行命令 **callout-right** *outright-value*，配置呼出权限。

----结束

7.4 配置 SIP 话机接入 IP PBX

背景信息

SIP 话机通过企业的以太网接入总部或分支的 IP PBX 设备，需要考虑如下方面：

- 设置 SIP 话机

  在 SIP 话机上需要设置 SIP 服务器地址，本机的 IP 地址以及本机的电话号码。相关设置在 SIP 话机上通过按键操作完成，详细指导请参考具体 SIP 话机的产品说明书。

- IP PBX 上配置用户

  在 IP PBX 上需要保证已配置该 SIP 话机用户，具体配置可参见“7.3.5 配置 PBX 用户”。

- 保证 SIP 话机和 IP PBX 的网络连通性

  SIP 话机和 IP PBX 之间是基于以太网的 IP 承载网络，需要通过配置网络设备的接口、VLAN、IP 地址和路由等，保证 SIP 话机和 IP PBX 之间的 IP 网络互通。请根据具体组网拓扑和网络规划，对各网络节点进行配置，本节不作详细介绍。

  如果 SIP 话机接入 SIP AG 后再接入 IP PBX，则此时 SIP AG 只作为 IP 路由设备对 SIP 话机的 IP 报文进行路由转发，不进行任何语音业务的识别和处理。因此对于 SIP AG 不需要进行特别的配置。

- （可选）保证 VoIP 业务 QoS 优先级

  通常企业的 VoIP 是和其他非语音业务是通过同一张 IP 网络来承载的，而 VoIP 业务对于业务的实时性要求较高，因此需要配置 VoIP 业务的 QoS 优先级来保证 VoIP 业务保证在网络中得到优先调度。

  配置 VoIP 业务 QoS 优先级有两种方式：

  - 传统的流分类配置方式。通常接入节点通过 Remark 动作进行业务流量区分，其他节点根据流分类调度即可。请参见“2.7 配置 QoS”。
  - 配置 Voice VLAN。Voice VLAN 通过识别收到的报文中的源 MAC 地址，判断是否是语音数据，并自动将收到语音数据的端口加入 Voice VLAN 中，同时自动部署优先级规则，保证语音数据的优先级和通话质量，从而简化了用户配置，且便于用户管理语音数据。

操作步骤

在 SIP 话机接入的交换机上进行如下配置：

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>，批量创建 VLAN。
3. 执行命令 **voice-vlan mac-address** *mac-address* **mask** *oui-mask* [**description** *text*]，配置 Voice VLAN 的 OUI 地址。

OUI 是二进制 MAC 地址的前 24 位，是 IEEE 为不同设备供应商分配的全球唯一标识符。OUI 地址表示一个 MAC 地址段，将 48 位的 MAC 地址和掩码的对应位作与运算可以确定 OUI 地址。只要终端的 MAC 地址前 24 位和 OUI 匹配，那么使能 Voice VLAN 功能的接口将认为此数据流是语音数据流。

4. 执行命令 **interface** *interface-type interface-number*，进入 SIP 话机接入的接口视图。
5. 执行命令 **voice-vlan** *vlan-id* **enable**，指定 VLAN 是 Voice VLAN，同时使能接口的 Voice VLAN 功能。

----结束

7.5 配置 POTS 话机/FAX 通过 IAD 接入 IP PBX

背景信息

POTS 话机/FAX 通过 IAD 接入 IP PBX 时，IAD 负责将 POTS 话机/FAX 的模拟语音信号转换成基于 SIP 协议的 IP 报文，对于 IP PBX 来说，POTS 话机/FAX 是不可见的，而 IAD 就相当于一台（或多台）SIP 话机终端。

因此配置 POTS 话机/FAX 通过 IAD 接入 IPPBX 时，需要考虑如下方面：

- 设置 IAD

  在 IAD 上需要设置 SIP 服务器地址、本机 IP 地址以及下连 POTS 话机/FAX 的号码。
- IP PBX 上配置用户
- 保证 IAD 和 IP PBX 的网络连通性
- （可选）保证 VoIP 业务 QoS 优先级

本节只介绍 IAD 上的相关配置，其余内容和 SIP 话机的接入相同，可参考“7.4 配置 SIP 话机接入 IP PBX”。

操作步骤

1. 执行命令 **enable**，从普通模式进入特权模式。
2. 执行命令 **configure terminal**，进入全局配置模式。
3. 配置 IAD 的 IP 地址。IAD 支持 3 种 IP 获取方式，分别为静态 IP、DHCP 和 PPPoE。缺省情况下，IAD 通过 DHCP 自动获取 IP 地址，如果需要修改：
   - 执行 **ipaddress static** *ip-address subnet-mask default-gateway* 配置静态 IP 地址。
   - 执行 **ipaddress dhcp** 启动 DHCP 方式获取 IP 地址。
   - 执行 **pppoe username** *username* **password** *password* 配置 PPPoE 用户名和密码，然后执行 **ipaddress pppoe** 启用 PPPoE 方式获取 IP 地址。
4. 执行命令 **sip server** *index* **address** *ip-address*，配置 SIP 服务器。
5. 执行命令 **sip user** *port-number* **id** *id*，配置 SIP 用户。
6. 执行命令 **write**，保存当前配置。

----结束

7.6 配置 POTS 话机/FAX 通过 SIP AG 接入 IP PBX

配置 POTS 话机/FAX 通过 SIP AG 接入 IP PBX，主要需要考虑如下方面：

- SIP AG 本身的配置，例如媒体 IP 地址、信令 IP 地址、信令端口号等等。
- 在 SIP AG 上配置 POTS 话机/FAX 用户，包括接入的端口号、电话号码等。
- 实现 SIP AG 到 IP PBX 的接入

7.6.1 配置 SIP AG 接口

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **voip-address media interface** *interface-typeinterface-number* { *ip-address* | **dynamic** }，配置媒体 IP 地址池。
4. 执行命令 **voip-address signalling interface***interface-typeinterface-number* { *ip-address* | **dynamic** }，配置信令 IP 地址池。
5. 执行命令 **sipag** *mgid*，创建 SIPAG，并进入 SIPAG 视图。
6. 执行命令 **media-ip** { *media-ip* | **media-addr-name** *media-addr-name* }，配置 SIPAG 接口的媒体 IP 地址，媒体 IP 地址必须从媒体 IP 地址池获取。
7. 执行命令 **signalling-ip** { *signal-ip* | **signalling-addr-name** *signal-addr-name* }，配置 SIPAG 接口的信令 IP 地址，信令 IP 地址必须从信令 IP 地址池中选取。
8. 执行命令 **signalling-port** *signalling-port-value*，配置 SIPAG 接口的信令端口号。

----结束

7.6.2 配置 SIP AG 用户

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **sipaguser** *sipaguser-name*，创建 SIPAG 用户，并进入 SIPAG 用户视图。
4. 执行命令 **port** *interface-number*，配置 SIPAG 用户的接口编号。
5. 执行命令 **mgid** *mgid*，配置 SIPAG 用户关联的 SIPAG。
6. 执行命令 **base-telno** *telno-value*，配置 SIPAG 用户的电话号码。

----结束

7.6.3 配置 SIP AG 接入 IP PBX

SIP AG 接入 IP PBX 有两种场景。一种是总部 SIP AG，它只需要接入在同一个园区的总部 IP PBX；另一种是分支 SIP AG，它需要通过广域网来接入总部的 IP PBX。

这两种场景在保证 SIP AG 和 IP PBX 之间的 IP 连通性的情况下，其余的配置是完全相同的。SIP AG 和 IP PBX 的 IP 连通性的配置本节不作详细描述，请根据具体组网拓扑和网络规划进行配置。

SIP AG 接入 IP PBX 时，在 SIP AG 上需要指定代理服务器（即 IP PBX）的相关信息，而在 IP PBX 上只需要配置 PBX 用户即可。具体配置可参见“7.3.5 配置 PBX 用户”。

请在 SIP AG 上进行如下配置。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **sipag** *mgid*，进入 SIPAG 视图。
4. 执行命令 **proxy-address-mode** { **static** | **dns-a** | **dns-srv** | **dns-naptr** }，配置代理服务器的 IP 地址获取方式。

   代理服务器的 IP 地址获取方式：

   - 配置为 static 时，必须配置主用代理服务器的 IP 地址和端口号。
   - 配置为 DNS-A、DNS-SRV 或 DNS-NAPTR 时，必须配置主用代理服务器的域名。
5. 执行命令 **primary-proxy-ip** *primary-proxy-ip-value1* [*primary-proxy-ip-value2*]，配置主用代理服务器 IP 地址。
6. 执行命令 **primary-proxy-domain** *primary-proxy-domain-name*，配置主用代理服务器域名。
7. 执行命令 **primary-proxy-port** *primary-proxy-port-value*，配置主用代理服务器端口号。
8. 执行命令 **transfer** { **tcp** | **udp** | **sctp** }，配置 SIPAG 的传输协议。
9. 执行命令 **home-domain** *home-domain-value*，配置 SIG AG 的归属域名。

----结束

7.6.4 复位 SIPAG

当需要使修改后的 SIPAG 属性生效、启动新建的 SIPAG 时，需要重新复位 SIPAG，复位前配置的属性信息才能生效。

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **sipag** *mgid*，进入 SIPAG 视图。
4. 执行命令 **reset**，复位 SIPAG。

----结束

7.7 配置总部/分支 IP PBX 互联

总部和分支的 IP PBX 互通是通过配置 SIPIP 中继群以及呼叫路由来实现的。需要在总部和分支的 IP PBX 上分别进行配置。

7.7.1 配置 SIPIP 中继群

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **trunkgroup** *name*，配置并进入中继群视图。
4. 执行命令 **signalling sip**，配置中继群的信令类型为 SIP。
5. 执行命令 **dn-set** *name*，配置中继群绑定的号首集。
6. 执行命令 **sip reg-mode** *value*，配置 SIP 中继注册方式。
7. 执行命令 **callin-right** *name*，配置中继呼入的权限。
8. 执行命令 **callout-righ** *name*，配置中继呼出的权限。
9. 执行命令 **default-caller-telno** *country-code-value area-code-value value*，配置中继群国家码、区域码和默认显示号码。
10. 执行命令 **sip signalling-ip** { *ip-address* | **signaling-addr-name** *signaling-addr-name-value* }，配置本端信令 IP 地址或动态信令 IP 地址名称。
11. 执行命令 **sip media-ip** {*ip-address* | **media-addr-name** *media-addr-name-value*}，配置本端媒体 IP 地址或动态媒体 IP 地址名称。
12. 执行命令 **sip signaling-port** *signalport-value*，配置本端信令端口。
13. 执行命令 **sip peer static** *primary-ip-value primary-ip-value*，配置对端 IP 地址和端口。
14. 执行命令 **sip register-uri** *register-uri-value*，配置注册服务器 URI。
15. 执行命令 **sip home-domain** *value*，配置对端 IP 中继归属域名。

----结束

7.7.2 配置呼叫路由

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **callroute** *name*，创建呼叫路由。
4. 执行命令 **enterprise** *enterprise-name*，配置呼叫路由应用的主叫号码绑定的企业。
5. 执行命令 **centrex** *centrex-name*，配置呼叫路由应用的主叫号码绑定的群。
6. 执行命令 **dn-set** *dn-set-name*，配置呼叫路由应用的主叫号码的绑定的号首集。
7. 执行命令 **callprefix** *callprefix-name*，配置呼叫路由应用的被叫号码的字冠。

说明

该字冠即为对端 IP PBX 下用户号码的字冠，例如对于总部 IP PBX 来说，这里需指定分支 IP PBX 下用户的字冠。

8. 执行命令 **condition caller-telno** { *country-code-value area-code-value caller-telno-value* | **disable** }，配置呼叫路由的主叫条件。
9. 执行命令 **condition time-period** { **period** { **from** *begin-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **disable** }，配置呼叫路由的时间条件。
10. 执行命令 **trunkgroup** *trunkgroup-name1* [*trunkgroup-name2* [*trunkgroup-name3*] [*trunkgroup-name4*]]，配置呼叫路由关联的中继群。

说明

这里关联的中继群即为上面所配置 SIPIP 中继群。

----结束

7.8 配置总部 IP PBX 与原有 TDM PBX 互联

对于原有 TDM PBX 系统的接入 IP PBX 来说，原有的用户数据等都注册在 TDM PBX 上，在 IP PBX 上只需要配置拨打 TDM PBX 下用户的字冠数据，以及到 TDM PBX 的中继/中继群和呼叫路由信息即可。

对于 TDM PBX，由于是原有系统迁移，只需要在 TDM PBX 上配置到 IP PBX 的中继信息和相关字冠信息即可。由于是旧有系统，因此本节不介绍其配置，可参考相应产品的文档进行配置。

对于在 IP PBX 上配置 TDM PBX 下用户的字冠数据，请参考“7.3.4 配置字冠”。

7.8.1 配置 PRA 中继群

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **trunkgroup** *name*，配置并进入中继群视图。
4. 执行命令 **signalling** *sigtype*，配置中继群的信令类型。
5. 执行命令 **dn-set** name，配置中继群绑定的号首集。
6. 执行命令 **enterprise** *name*，配置中继群绑定的企业。
7. 执行命令 **callin-right** *name*，配置中继呼入的权限。
8. 执行命令 **pra standard**，配置 PRA 中继协议标准类型。

----结束

7.8.2 配置 PRA 中继

1. 执行命令 **system-view**，进入系统视图。

2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **trunk-pra** *name*，配置并进入 PRA 中继视图。
4. 执行命令 **trunk-pra** *lotid/subcardid/portid*，配置 PRA 中继的端口物理信息。

   说明

   这里的端口是 IP PBX 连接 TDM PBX 的物理端口。

5. 执行命令 **trunkgroup** *name*，配置 PRA 中继所属的中继群。

   说明

   这里的中继群即为上面配置 PRA 中继群。

----结束

7.8.3 配置呼叫路由

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。
3. 执行命令 **callroute** *name*，创建呼叫路由。
4. 执行命令 **enterprise** *enterprise-name*，配置呼叫路由应用的主叫号码绑定的企业。
5. 执行命令 **centrex** *centrex-name*，配置呼叫路由应用的主叫号码绑定的群。
6. 执行命令 **dn-set** *dn-set-name*，配置呼叫路由应用的主叫号码的绑定的号首集。
7. 执行命令 **callprefix** *callprefix-name*，配置呼叫路由应用的被叫号码的字冠。

   说明

   该字冠即为呼叫 TDM PBX 下用户的字冠。

8. 执行命令 **condition caller-telno** { *country-code-value area-code-value caller-telno-value* | **disable** }，配置呼叫路由的主叫条件。
9. 执行命令 **condition time-period** { **period** { **from** *begin-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **disable** }，配置呼叫路由的时间条件。
10. 执行命令 **trunkgroup** *trunkgroup-name1* [*trunkgroup-name2* [*trunkgroup-name3*] [*trunkgroup-name4*]]，配置呼叫路由关联的中继群。

    说明

    这里关联的中继群即为上面所配置 PRA 中继群。

----结束

7.8.4 配置路由后号码变换

1. 执行命令 **system-view**，进入系统视图。
2. 执行命令 **voice**，进入语音视图。

3. 执行命令 **afterroute-change** *name*，创建路由后号码变换方案，并进路由后号码变换视图。 缺省情况下，没有配置路由后号码变换方案。
4. 执行命令 **enterprise** *name*，配置路由后号码变换业务绑定的企业。
5. 执行命令 **dn-set** *dn-set-name*，配置路由后号码变换业务绑定的号首集。
6. 执行命令 **centrex** *centrex-name*，配置路由后号码变换业务绑定的 Centrex 群。
7. 执行命令 **callprefix** *callprefix-name*，配置路由后号码变换业务绑定的字冠。

   说明

   该字冠即为呼叫 TDM PBX 下用户的字冠。
8. 执行命令 **condition caller-telno** { **telno** { telno *country-code-value area-code-value long-telno-value* | **centrex** *short-telno-value* } | **disable** }，配置需要做路由后变换的主叫用户。
9. 执行命令 **trunkgroup** *trunkgroup-name* ，路由后号码变换关联的中继群。

   说明

   这里关联的中继群即为上面所配置 PRA 中继群。
10. 执行命令 **caller** { **del-then-insert** *del-offset del-len insert-telnum* | **del** *del-offsetval del-lenval* | **insert** *insert-offset insert-telnum-val* | **no-change** }，配置主叫号码变化规则。
11. 执行命令 **called** { **del-then-insert** *del-offset del-len insert-telnum* | **del** *del-offsetval del-lenval* | **insert** *insert-offset insert-telnum-val* | **no-change** }，配置被叫号码变化规则。
12. （可选）执行命令 **caller property**，配置路由后号码变换中主叫用户号码变换的号码类型。

----结束

7.9 配置总部/分支 IP PBX 与 PSTN/PLMN 互联

总部/分支的 IP PBX 与 PSTN/PLMN 互联，其性质与 IP PBX 和 TDM PBX 互联的性质是完全相同的，只是需要考虑呼叫外部用户时的字冠数据规划。相关配置请参考“7.8 配置总部 IP PBX 与原有 TDM PBX 互联”。

7.10 配置举例

组网需求

某企业通过自建 VoIP 语音网络，实现总部内部、分支内部以及总部和分支之间的语音通信，以节省通讯费用。

由于企业的原有网络状况以及分支机构的不同特点，企业的语音网络有五种不同的情况：

- 总部完全新建区域

完全新建区域全部采用以太网来承载 VoIP 语音业务，终端也以 SIP 话机为主，少量的 POTS 话机和传真机采用 IAD 设备进行转换，实现全 VoIP 语音。

- 总部新建&迁移区域

  该其余既有部分是新部署的 SIP 话机终端，又有不少传统 POTS 话机和传真机，此时单独部署一台 SIP AG 设备，既可以接入 SIP 话机（此时 SIP AG 只作为路由设备），又可以接入适量的 POTS 话机和传真机。

- 总部旧系统迁移区域

  该部分区域基本上都是传统的 POTS 话机和传真机，采用 TDM PBX 设备进行交换，这种情况下，不对原有网络进行改造，而是保留原有系统，直接将 TDM PBX 设备挂接到新的 IP PBX 下，TDM PBX 和 IP PBX 之间配置 PRA 中继实现通信。

- 分布式分支

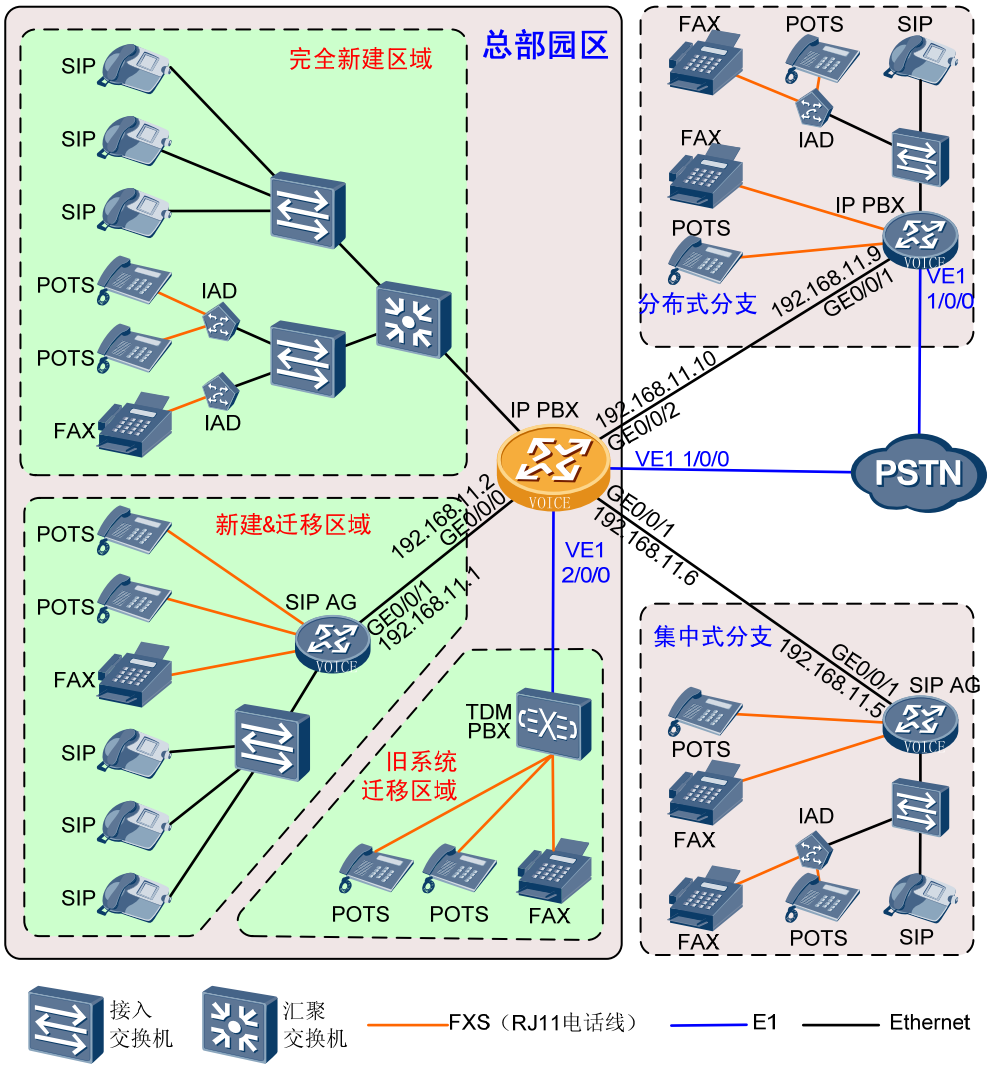
  某些分支规模较大，因此在分支中独立部署 IP PBX 设备，用户直接注册在分支的 IP PBX 上，分支 IP PBX 和总部 IP PBX 之间配置 SIPIP 中继实现通信。另外，分布式分支也和当地的 PSTN/PLMN 互联，实现独立出局功能。

- 集中式分支

  集中式分支规模较小，因此不单独部署 IP PBX 设备，而是部署 SIP AG 设备，所有用户均注册在总部的 IP PBX 上，并通过总部的 IP PBX 设备进行呼叫控制。集中式分支的 SIP AG 不单独出局，只通过广域网与总部 IP PBX 互联。

具体的组网结构如图 7-3 所示。

图7-3 VoIP 语音配置举例组网图



数据准备

表7-3 数据规划表

配置项	配置子项	数据
接口 IP 地址	NA	参见组网图中各网元节点的标注
总部 IP PBX	信令/媒体网关地址	192.168.11.2
	信令端口号	5060
	SIP 中继信令端口	5070
分布式分支 IP PBX	信令/媒体网关地址	192.168.11.9
	信令端口号	5060

配置项	配置子项	数据
	SIP 中继信令端口	5070
总部 SIP AG	信令/媒体网关地址	192.168.11.1
	信令端口号	5060
集中式分支 SIP AG	信令/媒体网关地址	192.168.11.5
	信令端口号	5060
号码规划	总部本地用户字冠	5662
	分布式分支用户字段	2222
	集中式分支用户字冠	3333
	TDM PBX 用户字冠	8
	拨打外部用户字冠	20000

操作步骤

注意

本操作步骤中只介绍了和语音业务相关的配置，省略了网络互通的配置。

1. 配置总部 IP PBX

   # 配置信令和媒体网关地址。

```
<Qudiway> system-view
[Qudiway] sysname hqpbx
[hqpbx] voice
[hqpbx-voice] voip-address signalling interface gigabitethernet 0/0/0 192.168.11.2
[hqpbx-voice] voip-address media interface gigabitethernet 0/0/0 192.168.11.2
```

   # 配置号码归属的企业、群、号首集。

```
[hqpbx-voice] pbx
[hqpbx-voice-pbx] enterprise huawei
[hqpbx-voice-pbx-enterprise-huawei] dn-set local
[hqpbx-voice-pbx-enterprise-huawei] centrex company
[hqpbx-voice-pbx-enterprise-huawei] quit
```

   #配置 SIP 服务器。

```
[hqpbx-voice] pbx
[hqpbx-voice-pbx] sipserver
[hqpbx-voice-pbx-sipserver] signalling-ip 192.168.11.2
[hqpbx-voice-pbx-sipserver] signalling-port 5060
```

```
[hqpbx-voice-pbx-sipserver] media-ip 192.168.11.2
[hqpbx-voice-pbx-sipserver] register-uri company.com
[hqpbx-voice-pbx-sipserver] home-domain company.com
[hqpbx-voice-pbx-sipserver] reset
[hqpbx-voice-pbx-sipserver] quit
```

配置本地用户的字冠。

```
[hqpbx-voice-pbx] callprefix 5662
[hqpbx-voice-pbx-callprefix-5662] enterprise company
[hqpbx-voice-pbx-callprefix-5662] dn-set local
[hqpbx-voice-pbx-callprefix-5662] prefix 5662
[hqpbx-voice-pbx-callprefix-5662] centrex company
[hqpbx-voice-pbx-callprefix-5662] call-type category 0 attribute 3
[hqpbx-voice-pbx-callprefix-5662] maximum-length 8
[hqpbx-voice-pbx-callprefix-5662] minimum-length 4
[hqpbx-voice-pbx-callprefix-5662] quit
```

配置集中式分支用户的字冠。

```
[hqpbx-voice-pbx] callprefix 3333
[hqpbx-voice-pbx-callprefix-3333] enterprise company
[hqpbx-voice-pbx-callprefix-3333] dn-set local
[hqpbx-voice-pbx-callprefix-3333] prefix 3333
[hqpbx-voice-pbx-callprefix-3333] centrex company
[hqpbx-voice-pbx-callprefix-3333] call-type category 0 attribute 3
[hqpbx-voice-pbx-callprefix-3333] maximum-length 8
[hqpbx-voice-pbx-callprefix-3333] minimum-length 4
[hqpbx-voice-pbx-callprefix-3333] quit
```

配置分布式分支用户的字冠。

```
[hqpbx-voice-pbx] callprefix 2222
[hqpbx-voice-pbx-callprefix-2222] enterprise company
[hqpbx-voice-pbx-callprefix-2222] dn-set local
[hqpbx-voice-pbx-callprefix-2222] prefix 2222
[hqpbx-voice-pbx-callprefix-2222] centrex company
[hqpbx-voice-pbx-callprefix-2222] call-type category 0 attribute 3
[hqpbx-voice-pbx-callprefix-2222] maximum-length 15
[hqpbx-voice-pbx-callprefix-2222] minimum-length 1
[hqpbx-voice-pbx-callprefix-2222] destination-location inter-office
[hqpbx-voice-pbx-callprefix-2222] quit
```

配置原有 TDM PBX 下用户的字冠。

```
[hqpbx-voice-pbx] callprefix 8
[hqpbx-voice-pbx-callprefix-8] enterprise company
[hqpbx-voice-pbx-callprefix-8] dn-set local
[hqpbx-voice-pbx-callprefix-8] prefix 8
[hqpbx-voice-pbx-callprefix-8] centrex company
[hqpbx-voice-pbx-callprefix-8] call-type category 0 attribute 3
[hqpbx-voice-pbx-callprefix-8] maximum-length 20
[hqpbx-voice-pbx-callprefix-8] minimum-length 1
[hqpbx-voice-pbx-callprefix-8] destination-location inter-office
[hqpbx-voice-pbx-callprefix-8] quit
```

配置外部用户（PSTN/PLMN）的字冠。

```
[hqpbx-voice-pbx] callprefix 20000
[hqpbx-voice-pbx-callprefix-20000] enterprise company
[hqpbx-voice-pbx-callprefix-20000] dn-set local
[hqpbx-voice-pbx-callprefix-20000] prefix 20000
[hqpbx-voice-pbx-callprefix-20000] centrex company
[hqpbx-voice-pbx-callprefix-20000] call-type category 0 attribute 3
[hqpbx-voice-pbx-callprefix-20000] maximum-length 20
[hqpbx-voice-pbx-callprefix-20000] minimum-length 5
[hqpbx-voice-pbx-callprefix-20000] destination-location inter-office
[hqpbx-voice-pbx-callprefix-20000] quit
```

配置 PBX 用户（此处只列举了部分用户，包括总部和集中式分支的用户）。

```
[hqpbx-voice] pbxuser 56620001
[hqpbx-voice-pbxuser-56620001] type sipue 56620001
[hqpbx-voice-pbxuser-56620001] enterprise company
[hqpbx-voice-pbxuser-56620001] quit
[hqpbx-voice] dialno 56620001
[hqpbx-voice-dialno-56620001] pbxuser 56620001
[hqpbx-voice-dialno-56620001] telno 86 25 56620001
[hqpbx-voice-dialno-56620001] dn-set local
[hqpbx-voice-dialno-56620001] callout-right 2
[hqpbx-voice-dialno-56620001] callin-right 2
[hqpbx-voice-dialno-56620001] quit
[hqpbx-voice] pbxuser 56620002
[hqpbx-voice-pbxuser-56620002] type sipue 56620002
[hqpbx-voice-pbxuser-56620002] enterprise company
[hqpbx-voice-pbxuser-56620002] quit
[hqpbx-voice] dialno 56620002
[hqpbx-voice-dialno-56620002] pbxuser 56620002
[hqpbx-voice-dialno-56620002] telno 86 25 56620002
[hqpbx-voice-dialno-56620002] dn-set local
[hqpbx-voice-dialno-56620002] callout-right 2
[hqpbx-voice-dialno-56620002] callin-right 2
[hqpbx-voice-dialno-56620002] quit
[hqpbx-voice] pbxuser 56620003
[hqpbx-voice-pbxuser-56620003] type sipue 56620003
[hqpbx-voice-pbxuser-56620003] enterprise company
[hqpbx-voice-pbxuser-56620003] quit
[hqpbx-voice] dialno 56620003
[hqpbx-voice-dialno-56620003] pbxuser 56620003
[hqpbx-voice-dialno-56620003] telno 86 25 56620003
[hqpbx-voice-dialno-56620003] dn-set local
[hqpbx-voice-dialno-56620003] callout-right 2
[hqpbx-voice-dialno-56620003] callin-right 2
[hqpbx-voice-dialno-56620003] quit
[hqpbx-voice] pbxuser 56620004
[hqpbx-voice-pbxuser-56620004] type sipue 56620004
[hqpbx-voice-pbxuser-56620004] enterprise company
[hqpbx-voice-pbxuser-56620004] quit
[hqpbx-voice] dialno 56620004
[hqpbx-voice-dialno-56620004] pbxuser 56620004
[hqpbx-voice-dialno-56620004] telno 86 25 56620004
[hqpbx-voice-dialno-56620004] dn-set local
[hqpbx-voice-dialno-56620004] callout-right 2
[hqpbx-voice-dialno-56620004] callin-right 2
```

```
[hqpbx-voice-dialno-56620004] quit
[hqpbx-voice] pbxuser 33330001
[hqpbx-voice-pbxuser-33330001] type sipue 33330001
[hqpbx-voice-pbxuser-33330001] enterprise company
[hqpbx-voice-pbxuser-33330001] quit
[hqpbx-voice] dialno 33330001
[hqpbx-voice-dialno-33330001] pbxuser 33330001
[hqpbx-voice-dialno-33330001] telno 86 25 33330001
[hqpbx-voice-dialno-33330001] dn-set local
[hqpbx-voice-dialno-33330001] callout-right 2
[hqpbx-voice-dialno-33330001] callin-right 2
[hqpbx-voice-dialno-33330001] quit
[hqpbx-voice] pbxuser 33330002
[hqpbx-voice-pbxuser-33330002] type sipue 33330002
[hqpbx-voice-pbxuser-33330002] enterprise company
[hqpbx-voice-pbxuser-33330002] quit
[hqpbx-voice] dialno 33330002
[hqpbx-voice-dialno-33330002] pbxuser 33330002
[hqpbx-voice-dialno-33330002] telno 86 25 33330002
[hqpbx-voice-dialno-33330002] dn-set local
[hqpbx-voice-dialno-33330002] callout-right 2
[hqpbx-voice-dialno-33330002] callin-right 2
[hqpbx-voice-dialno-33330002] quit
```

配置到分布式分支 IP PBX 的 SIP 中继群。

```
[hqpbx-voice] trunkgroup sipip
[hqpbx-voice-trunkgroup-sipip] signalling sip
[hqpbx-voice-trunkgroup-sipip] enterprise company
[hqpbx-voice-trunkgroup-sipip] dn-set local
[hqpbx-voice-trunkgroup-sipip] callin-right 3
[hqpbx-voice-trunkgroup-sipip] callout-right 3
[hqpbx-voice-trunkgroup-sipip] sip reg-mode 0
[hqpbx-voice-trunkgroup-sipip] sip mgc-type 0
[hqpbx-voice-trunkgroup-sipip] sip signalling-ip 192.168.11.2
[hqpbx-voice-trunkgroup-sipip] sip signalling-port 5070
[hqpbx-voice-trunkgroup-sipip] sip media-ip 192.168.11.2
[hqpbx-voice-trunkgroup-sipip] sip peer static 192.168.11.9 5070
[hqpbx-voice-trunkgroup-sipip] sip register-uri company.com
[hqpbx-voice-trunkgroup-sipip] sip home-domain company.com
[hqpbx-voice-trunkgroup-sipip] quit
```

配置到分布式分支 IP PBX 的呼叫路由。

```
 [hqpbx-voice] callroute 2222
[hqpbx-voice-callroute-2222] enterprise company
[hqpbx-voice-callroute-2222] dn-set local
[hqpbx-voice-callroute-2222] centrex -
[hqpbx-voice-callroute-2222] callprefix 2222
[hqpbx-voice-callroute-2222] condition time-period disable
[hqpbx-voice-callroute-2222] condition time-repeat disable
[hqpbx-voice-callroute-2222] condition caller-telno disable
[hqpbx-voice-callroute-2222] trunkgroup sipip
[hqpbx-voice-callroute-2222] quit
```

配置到 PSTN/PLMN 的中继群。

```
[hqpbx-voice] trunkgroup pra1
[hqpbx-voice-trunkgroup-pra1] signalling dss1-user
[hqpbx-voice-trunkgroup-pra1] enterprise company
[hqpbx-voice-trunkgroup-pra1] dn-set local
[hqpbx-voice-trunkgroup-pra1] pra standard Q931
[hqpbx-voice-trunkgroup-pra1] quit
```

配置到 PSTN/PLMN 的中继。

```
[hqpbx-voice] trunk-pra pra1
[hqpbx-voice-trunk-pra-pra1] port ve1 1/0/0
[hqpbx-voice-trunk-pra-pra1] trunkgroup pra1
[hqpbx-voice-trunk-pra-pra1] quit
```

配置到 PSTN/PLMN 的呼叫路由。

```
[hqpbx-voice] callroute 20000
[hqpbx-voice-callroute-20000] enterprise company
[hqpbx-voice-callroute-20000] dn-set local
[hqpbx-voice-callroute-20000] centrex -
[hqpbx-voice-callroute-20000] callprefix 20000
[hqpbx-voice-callroute-20000] condition time-period disable
[hqpbx-voice-callroute-20000] condition time-repeat disable
[hqpbx-voice-callroute-20000] condition caller-telno disable
[hqpbx-voice-callroute-20000] trunkgroup pra1
[hqpbx-voice-callroute-20000] quit
```

配置到 PSTN/PLMN 的路由后号码变换。

```
[hqpbx-voice] afterroute-change pra1
[hqpbx-voice-afterroute-change-pra1] enterprise company
[hqpbx-voice-afterroute-change-pra1] dn-set local
[hqpbx-voice-afterroute-change-pra1] centrex -
[hqpbx-voice-afterroute-change-pra1] callprefix 20000
[hqpbx-voice-afterroute-change-pra1] condition caller-telno disable
[hqpbx-voice-afterroute-change-pra1] trunkgroup pra1
[hqpbx-voice-afterroute-change-pra1] caller no-change
[hqpbx-voice-afterroute-change-pra1] caller property 1
[hqpbx-voice-afterroute-change-pra1] called del 8 5
[hqpbx-voice-afterroute-change-pra1] quit
```

配置到 TDM PBX 的中继群。

```
[hqpbx-voice] trunkgroup pra2
[hqpbx-voice-trunkgroup-pra2] signalling dss1-user
[hqpbx-voice-trunkgroup-pra2] enterprise company
[hqpbx-voice-trunkgroup-pra2] dn-set local
[hqpbx-voice-trunkgroup-pra2] pra standard Q931
[hqpbx-voice-trunkgroup-pra2] quit
```

配置到 TDM PBX 的中继。

```
[hqpbx-voice] trunk-pra pra2
[hqpbx-voice-trunk-pra-pra2] port ve1 2/0/0
[hqpbx-voice-trunk-pra-pra2] trunkgroup pra2
[hqpbx-voice-trunk-pra-pra2] quit
```

配置到 TDM PBX 的呼叫路由。

```
[hqpbx-voice] callroute 8
[hqpbx-voice-callroute-8] enterprise company
[hqpbx-voice-callroute-8] dn-set local
[hqpbx-voice-callroute-8] centrex -
[hqpbx-voice-callroute-8] callprefix 8
[hqpbx-voice-callroute-8] condition time-period disable
[hqpbx-voice-callroute-8] condition time-repeat disable
[hqpbx-voice-callroute-8] condition caller-telno disable
[hqpbx-voice-callroute-8] trunkgroup pra2
[hqpbx-voice-callroute-8] quit
```

配置到 TDM PBX 的路由后号码变换。

```
[hqpbx-voice] afterroute-change pra2
[hqpbx-voice-afterroute-change-pra2] enterprise company
[hqpbx-voice-afterroute-change-pra2] dn-set local
[hqpbx-voice-afterroute-change-pra2] centrex -
[hqpbx-voice-afterroute-change-pra2] callprefix 8
[hqpbx-voice-afterroute-change-pra2] condition caller-telno disable
[hqpbx-voice-afterroute-change-pra2] trunkgroup pra2
[hqpbx-voice-afterroute-change-pra2] caller no-change
[hqpbx-voice-afterroute-change-pra2] caller property 1
[hqpbx-voice-afterroute-change-pra2] called del 8 1
[hqpbx-voice-afterroute-change-pra2] quit
```

2. 配置总部的 SIP AG

配置 IP 地址池。

```
<Quidway> system-view
[Quidway] sysname hgag
[hqag] interface gigabitethernet 0/0/1
[hqag-GigabitEthernet0/0/1] ip address 192.168.11.1
[hqag-GigabitEthernet0/0/1] quit
```

配置用于媒体和信令交互的 IP 地址池。

```
[hqag] voice
[hqag-voice] voip-address signalling interface gigabitethernet 0/0/1 192.168.11.1
[hqag-voice] voip-address media interface gigabitethernet 0/0/1 192.168.11.1
```

配置 SIPAG 接口参数。

```
[hqag-voice] sipag 1
[hqag-voice-sipag-1] signalling-ip 192.168.11.1
[hqag-voice-sipag-1] media-ip 192.168.11.1
[hqag-voice-sipag-1] signalling-port 5060
[hqag-voice-sipag-1] transfer udp
[hqag-voice-sipag-1] primary-proxy-ip 192.168.11.2
[hqag-voice-sipag-1] primary-proxy-port 5060
[hqag-voice-sipag-1] home-domain company.com
[hqag-voice-sipag-1] quit
```

配置 SIPAG 用户。

```
[hqag-voice] sipaguser 56620003
[hqag-voice-sipaguser-56620003] port 3/0/1
[hqag-voice-sipaguser-56620003] mgid 1
```

```
[hqag-voice-sipaguser-56620003] base-telno 56620003
[hqag-voice-sipaguser-56620003] quit
[hqag-voice] sipaguser 56620004
[hqag-voice-sipaguser-56620004] port 3/0/2
[hqag-voice-sipaguser-56620004] mgid 1
[hqag-voice-sipaguser-56620004] base-telno 56620004
[hqag-voice-sipaguser-56620004] quit
```

复位 SIPAG。

```
[hqag-voice] sipag 1
[hqag-voice-sipag-1] reset
Are you sure to reset MG interface?(y/n)[n]: y
[hqag-voice-sipag-1]
 Reset MG interface succeeds!
```

3. 配置总部的终端

配置总部中的 IAD。

```
TERMINAL> enable
TERMINAL# configure terminal
TERMINAL# ipaddress static 192.168.12.2 255.255.254.0
TERMINAL# sip server 0 address 192.168.11.2
TERMINAL# sip user 1 id 56620001
TERMINAL# write
```

配置总部的 SIP 话机。

通过 SIP 话机上的按键配置 SIP 话机的号码、本地 IP 地址、SIP 服务器地址（192.168.11.2），具体配置参见 SIP 话机的产品文档。

4. 配置分布式分支的 IP PBX

配置信令 IP 地址和媒体 IP 地址。

```
<Qudiway> system-view
[Qudiway] sysname brpbx
[brpbx] voice
[brpbx-voice] voip-address signalling interface gigabitethernet 0/0/1 192.168.11.9
[brpbx-voice] voip-address media interface gigabitethernet 0/0/1 192.168.11.9
```

配置号码归属的企业、群、号首集。

```
[brpbx-voice] pbx
[brpbx-voice-pbx] enterprise company
[brpbx-voice-pbx-enterprise-company] dn-set local
[brpbx-voice-pbx-enterprise-company] centrex company
[brpbx-voice-pbx-enterprise-company] quit
```

配置 SIP 服务器。

```
[brpbx-voice] pbx
[brpbx-voice-pbx] sipserver
[brpbx-voice-pbx-sipserver] signalling-ip 192.168.11.9
[brpbx-voice-pbx-sipserver] signalling-port 5060
[brpbx-voice-pbx-sipserver] media-ip 192.168.11.9
[brpbx-voice-pbx-sipserver] register-uri company.com
[brpbx-voice-pbx-sipserver] home-domain company.com
```

```
[brpbx-voice-pbx-sipserver] reset
[brpbx-voice-pbx-sipserver] quit
```

配置本地用户的字冠。

```
[brpbx-voice-pbx] callprefix 2222
[brpbx-voice-pbx-callprefix-2222] enterprise company
[brpbx-voice-pbx-callprefix-2222] dn-set local
[brpbx-voice-pbx-callprefix-2222] prefix 2222
[brpbx-voice-pbx-callprefix-2222] centrex -
[brpbx-voice-pbx-callprefix-2222] call-type category 0 attribute 3
[brpbx-voice-pbx-callprefix-2222] maximum-length 8
[brpbx-voice-pbx-callprefix-2222] minimum-length 4
[brpbx-voice-pbx-callprefix-2222] quit
```

配置总部用户的字冠。

```
[brpbx-voice-pbx] callprefix 5662
[brpbx-voice-pbx-callprefix-5662] enterprise company
[brpbx-voice-pbx-callprefix-5662] dn-set local
[brpbx-voice-pbx-callprefix-5662] prefix 5662
[brpbx-voice-pbx-callprefix-5662] centrex -
[brpbx-voice-pbx-callprefix-5662] call-type category 0 attribute 3
[brpbx-voice-pbx-callprefix-5662] maximum-length 15
[brpbx-voice-pbx-callprefix-5662] minimum-length 1
[brpbx-voice-pbx-callprefix-5662] destination-location inter-office
[brpbx-voice-pbx-callprefix-5662] quit
```

配置集中式分支用户的字冠。

```
[brpbx-voice-pbx] callprefix 3333
[brpbx-voice-pbx-callprefix-3333] enterprise company
[brpbx-voice-pbx-callprefix-3333] dn-set local
[brpbx-voice-pbx-callprefix-3333] prefix 5662
[brpbx-voice-pbx-callprefix-3333] centrex -
[brpbx-voice-pbx-callprefix-3333] call-type category 0 attribute 3
[brpbx-voice-pbx-callprefix-3333] maximum-length 15
[brpbx-voice-pbx-callprefix-3333] minimum-length 1
[brpbx-voice-pbx-callprefix-3333] destination-location inter-office
[brpbx-voice-pbx-callprefix-3333] quit
```

配置到总部 TDM PBX 下用户的字冠。

```
[brpbx-voice-pbx] callprefix 8
[brpbx-voice-pbx-callprefix-8] enterprise company
[brpbx-voice-pbx-callprefix-8] dn-set local
[brpbx-voice-pbx-callprefix-8] prefix 8
[brpbx-voice-pbx-callprefix-8] centrex company
[brpbx-voice-pbx-callprefix-8] call-type category 0 attribute 3
[brpbx-voice-pbx-callprefix-8] maximum-length 20
[brpbx-voice-pbx-callprefix-8] minimum-length 1
[brpbx-voice-pbx-callprefix-8] destination-location inter-office
[brpbx-voice-pbx-callprefix-8] quit
```

配置到外部用户的字冠。

```
[brpbx-voice-pbx] callprefix 20000
[brpbx-voice-pbx-callprefix-20000] enterprise company
```

```
[brpbx-voice-pbx-callprefix-20000] dn-set local
[brpbx-voice-pbx-callprefix-20000] prefix 20000
[brpbx-voice-pbx-callprefix-20000] centrex -
[brpbx-voice-pbx-callprefix-20000] call-type category 0 attribute 3
[brpbx-voice-pbx-callprefix-20000] maximum-length 20
[brpbx-voice-pbx-callprefix-20000] minimum-length 5
[brpbx-voice-pbx-callprefix-20000] destination-location inter-office
[brpbx-voice-pbx-callprefix-20000] quit
```

配置 PBX 用户（此处只已用户 A、用户 B 举例）。

```
[brpbx-voice] pbxuser 22220001
[brpbx-voice-pbxuser-22220001] type port 2/0/2
[brpbx-voice-pbxuser-22220001] enterprise company
[brpbx-voice-pbxuser-22220001] quit
[brpbx-voice] dialno 22220001
[brpbx-voice-dialno-22220001] pbxuser 22220001
[brpbx-voice-dialno-22220001] telno 86 755 22220001
[brpbx-voice-dialno-22220001] dn-set local
[brpbx-voice-dialno-22220001] callout-right 2
[brpbx-voice-dialno-22220001] callin-right 2
[brpbx-voice-dialno-22220001] quit
[brpbx-voice] pbxuser 22220002
[brpbx-voice-pbxuser-22220002] type port 2/0/3
[brpbx-voice-pbxuser-22220002] enterprise company
[brpbx-voice-pbxuser-22220002] quit
[brpbx-voice] dialno 22220002
[brpbx-voice-dialno-22220002] pbxuser 22220002
[brpbx-voice-dialno-22220002] telno 86 755 22220002
[brpbx-voice-dialno-22220002] dn-set local
[brpbx-voice-dialno-22220002] callout-right 2
[brpbx-voice-dialno-22220002] callin-right 2
[brpbx-voice-dialno-22220002] quit
```

配置到总部 IP PBX 的 SIPIP 中继群。

```
[brpbx-voice] trunkgroup sipip
[brpbx-voice-trunkgroup-sipip] signalling sip
[brpbx-voice-trunkgroup-sipip] enterprise company
[brpbx-voice-trunkgroup-sipip] dn-set local
[brpbx-voice-trunkgroup-sipip] callin-right 3
[brpbx-voice-trunkgroup-sipip] callout-right 3
[brpbx-voice-trunkgroup-sipip] sip reg-mode 0
[brpbx-voice-trunkgroup-sipip] sip mgc-type 0
[brpbx-voice-trunkgroup-sipip] sip signalling-ip 192.168.11.9
[brpbx-voice-trunkgroup-sipip] sip signalling-port 5070
[brpbx-voice-trunkgroup-sipip] sip media-ip 192.168.11.9
[brpbx-voice-trunkgroup-sipip] sip peer static 192.168.11.2 5070
[brpbx-voice-trunkgroup-sipip] sip register-uri company.com
[brpbx-voice-trunkgroup-sipip] sip home-domain company.com
```

配置到总部 IP PBX 的呼叫路由。

```
[brpbx-voice] callroute 5662
[brpbx-voice-callroute-5662] enterprise company
[brpbx-voice-callroute-5662] dn-set local
[brpbx-voice-callroute-5662] centrex -
```

```
[brpbx-voice-callroute-5662] callprefix 5662
[brpbx-voice-callroute-5662] condition time-period disable
[brpbx-voice-callroute-5662] condition time-repeat disable
[brpbx-voice-callroute-5662] condition caller-telno disable
[brpbx-voice-callroute-5662] trunkgroup sipip
[brpbx-voice-callroute-5662] quit
[brpbx-voice] callroute 3333
[brpbx-voice-callroute-3333] enterprise company
[brpbx-voice-callroute-3333] dn-set local
[brpbx-voice-callroute-3333] centrex -
[brpbx-voice-callroute-3333] callprefix 3333
[brpbx-voice-callroute-3333] condition time-period disable
[brpbx-voice-callroute-3333] condition time-repeat disable
[brpbx-voice-callroute-3333] condition caller-telno disable
[brpbx-voice-callroute-3333] trunkgroup sipip
[brpbx-voice-callroute-3333] quit
 [brpbx-voice] callroute 8
[brpbx-voice-callroute-8] enterprise company
[brpbx-voice-callroute-8] dn-set local
[brpbx-voice-callroute-8] centrex company
[brpbx-voice-callroute-8] callprefix 8
[brpbx-voice-callroute-8] condition time-period disable
[brpbx-voice-callroute-8] condition time-repeat disable
[brpbx-voice-callroute-8] condition caller-telno disable
[brpbx-voice-callroute-8] trunkgroup sipip
[brpbx-voice-callroute-8] quit
```

配置到总部 IP PBX 的路由后号码变换。

```
[brpbx-voice] afterroute-change sipip
[brpbx-voice-afterroute-change-sipip] enterprise company
[brpbx-voice-afterroute-change-sipip] dn-set local
[brpbx-voice-afterroute-change-sipip] centrex -
[brpbx-voice-afterroute-change-sipip] callprefix 8
[brpbx-voice-afterroute-change-sipip] condition caller-telno disable
[brpbx-voice-afterroute-change-sipip] trunkgroup sipip
[brpbx-voice-afterroute-change-sipip] caller no-change
[brpbx-voice-afterroute-change-sipip] caller property 1
[brpbx-voice-afterroute-change-sipip] called del 8 1
[brpbx-voice-afterroute-change-sipip] quit
```

配置到 PSTN/PLMN 的中继群。

```
[brpbx-voice] trunkgroup pra
[brpbx-voice-trunkgroup-pra] signalling dss1-user
[brpbx-voice-trunkgroup-pra] enterprise company
[brpbx-voice-trunkgroup-pra] dn-set local
[brpbx-voice-trunkgroup-pra] pra standard Q931
[brpbx-voice-trunkgroup-pra] quit
```

配置到 PSTN/PLMN 的中继。

```
[brpbx-voice] trunk-pra pra
[brpbx-voice-trunk-pra-pra] port ve1 1/0/0
[brpbx-voice-trunk-pra-pra] trunkgroup pra
[brpbx-voice-trunk-pra-pra] quit
```

配置到 PSTN/PLMN 的呼叫路由。

```
[brpbx-voice] callroute 20000
[brpbx-voice-callroute-20000] enterprise company
[brpbx-voice-callroute-20000] dn-set local
[brpbx-voice-callroute-20000] centrex company
[brpbx-voice-callroute-20000] callprefix 20000
[brpbx-voice-callroute-20000] condition time-period disable
[brpbx-voice-callroute-20000] condition time-repeat disable
[brpbx-voice-callroute-20000] condition caller-telno disable
[brpbx-voice-callroute-20000] trunkgroup pra
[brpbx-voice-callroute-20000] quit
```

配置到 PSTN/PLMN 的路由后号码变换。

```
[brpbx-voice] afterroute-change pra1
[brpbx-voice-afterroute-change-pra1] enterprise company
[brpbx-voice-afterroute-change-pra1] dn-set local
[brpbx-voice-afterroute-change-pra1] centrex -
[brpbx-voice-afterroute-change-pra1] callprefix 20000
[brpbx-voice-afterroute-change-pra1] condition caller-telno disable
[brpbx-voice-afterroute-change-pra1] trunkgroup pra1
[brpbx-voice-afterroute-change-pra1] caller no-change
[brpbx-voice-afterroute-change-pra1] caller property 1
[brpbx-voice-afterroute-change-pra1] called del 8 5
[brpbx-voice-afterroute-change-pra1] quit
```

5. 配置分布式分支的终端

配置分布式分支中的 IAD。

```
TERMINAL> enable
TERMINAL# configure terminal
TERMINAL# ipaddress static 192.168.13.2 255.255.254.0
TERMINAL# sip server 0 address 192.168.11.9
TERMINAL# sip user 1 id 22220003
TERMINAL# write
```

配置分布式分支的 SIP 话机。

通过 SIP 话机上的按键配置 SIP 话机的号码、本地 IP 地址、SIP 服务器地址（192.168.11.9），具体配置参见 SIP 话机的产品文档。

6. 配置集中式分支的 SIP AG

配置 IP 地址池。

```
<Qudiway> system-view
[Qudiway] sysname brag
[brag] interface gigabitethernet 0/0/1
[brag-GigabitEthernet0/0/1] ip address 192.168.11.5
[brag-GigabitEthernet0/0/1] quit
```

配置用于媒体和信令交互的 IP 地址。

```
[brag] voice
[brag-voice] voip-address signalling interface gigabitethernet 0/0/1 192.168.11.5
[brag-voice] voip-address media interface gigabitethernet 0/0/1 192.168.11.5
```

配置 SIPAG 接口参数。

```
[brag-voice] sipag 1
[brag-voice-sipag-1] signalling-ip 192.168.11.5
[brag-voice-sipag-1] media-ip 192.168.11.5
[brag-voice-sipag-1] signalling-port 5060
[brag-voice-sipag-1] transfer udp
[brag-voice-sipag-1] primary-proxy-ip 192.168.11.2
[brag-voice-sipag-1] primary-proxy-port 5060
[brag-voice-sipag-1] home-domain huawei.com
[brag-voice-sipag-1] quit
```

配置 SIPAG 用户。

```
[brag-voice] sipaguser 33330005
[brag-voice-sipaguser-33330005] port 3/0/1
[brag-voice-sipaguser-33330005] mgid 1
[brag-voice-sipaguser-33330005] base-telno 33330001
[brag-voice-sipaguser-33330005] quit
[brag-voice] sipaguser 33330006
[brag-voice-sipaguser-33330006] port 3/0/2
[brag-voice-sipaguser-33330006] mgid 1
[brag-voice-sipaguser-33330006] base-telno 33330002
[brag-voice-sipaguser-33330006] quit
```

复位 SIPAG。

```
[brag-voice] sipag 1
[brag-voice-sipag-1] reset
Are you sure to reset MG interface?(y/n)[n]: y
[brag-voice-sipag-1]
 Reset MG interface succeeds!
```

7. 配置集中式分支的终端

配置分布式分支中的 IAD。

```
TERMINAL> enable
TERMINAL# configure terminal
TERMINAL# ipaddress static 192.168.14.2 255.255.254.0
TERMINAL# sip server 0 address 192.168.11.2
TERMINAL# sip user 1 id 33330001
TERMINAL# write
```

配置分布式分支的 SIP 话机。

通过 SIP 话机上的按键配置 SIP 话机的号码、本地 IP 地址、SIP 服务器地址（192.168.11.2），具体配置参见 SIP 话机的产品文档。

----结束

配置文件

- 总部 IP PBX 配置文件

```
#
 sysname hqpbx
#
```

```
voice
 voip-address signalling interface GigabitEthernet 0/0/0 192.168.11.2
 voip-address media interface GigabitEthernet 0/0/0 192.168.11.2
#
pbx
#
enterprise company
 dn-set local
 centrex company
#
callprefix 8
 enterprise company
 dn-set local
 centrex company
 prefix 8
 call-type category 0 attribute 3
 maximum-length 20
 minimum-length 1
 destination-location inter-office
#
callprefix 2222
 enterprise company
 dn-set local
 centrex company
 prefix 2222
 call-type category 0 attribute 3
 maximum-length 15
 minimum-length 1
 destination-location inter-office
#
callprefix 3333
 enterprise company
 dn-set local
 centrex company
 prefix 3333
 call-type category 0 attribute 3
 maximum-length 8
 minimum-length 4
#
callprefix 5662
 enterprise company
 dn-set local
 centrex company
 prefix 5662
 call-type category 0 attribute 3
 maximum-length 8
 minimum-length 4
#
callprefix 20000
 enterprise company
 dn-set local
 centrex company
 prefix 20000
 call-type category 0 attribute 3
 maximum-length 20
```

```
 minimum-length 5
 destination-location inter-office
#
sipserver
 signalling-ip 192.168.11.2
 signalling-port 5060
 media-ip 192.168.11.2
 register-uri company.com
 home-domain company.com
#
pbxuser 56620001
 type sipue 56620001
 enterprise company
#
pbxuser 56620002
 type sipue 56620002
 enterprise company
#
pbxuser 56620003
 type sipue 56620003
 enterprise company
#
pbxuser 56620004
 type sipue 56620004
 enterprise company
#
dialno 56620001
 pbxuser 56620001
 telno 86 25 56620001
 dn-set local
 callout-right 2
 callin-right 2
#
dialno 56620002
 pbxuser 56620002
 telno 86 25 56620002
 dn-set local
 callout-right 2
 callin-right 2
#
dialno 56620003
 pbxuser 56620003
 telno 86 25 56620003
 dn-set local
 callout-right 2
 callin-right 2
#
dialno 56620004
 pbxuser 56620004
 telno 86 25 56620004
 dn-set local
 callout-right 2
 callin-right 2
#
pbxuser 33330001
```

```
 type sipue 33330001
 enterprise company
#
dialno 33330001
 pbxuser 33330001
 telno 86 25 33330001
 dn-set local
 callout-right 2
 callin-right 2
#
pbxuser 33330002
 type sipue 33330002
 enterprise company
#
dialno 33330002
 pbxuser 33330002
 telno 86 25 33330002
 dn-set local
 callout-right 2
 callin-right 2
#
trunkgroup pra1
 signalling dss1-user
 enterprise company
 dn-set local
 pra standard Q931
#
trunkgroup pra2
 signalling dss1-user
 enterprise company
 dn-set local
 pra standard Q931
#
trunkgroup sipip
 signalling sip
 enterprise company
 dn-set local
 callin-right 3
 callout-right 3
 sip reg-mode 0
 sip mgc-type 0
 sip signalling-ip 192.168.11.2
 sip signalling-port 5070
 sip media-ip 192.168.11.2
 sip peer static 192.168.11.9 5070
 sip register-uri company.com
 sip home-domain company.com
#
trunk-pra pra1
 port ve1 1/0/0
 trunkgroup pra1

#
trunk-pra pra2
 port ve1 2/0/0
```

```
 trunkgroup pra2
#
callroute 8
 enterprise company
 dn-set local
 centrex -
 condition time-period disable
 condition time-repeat disable
 condition caller-telno disable
 trunkgroup pra2
#
callroute 20000
 enterprise company
 dn-set local
 centrex -
 condition time-period disable
 condition time-repeat disable
 condition caller-telno disable
 trunkgroup pra1
#
afterroute-change pra1
 enterprise company
 dn-set local
 centrex -
 callprefix 20000
 condition caller-telno disable
 trunkgroup pra1
 caller no-change
 caller property 1
 called del 8 5
#
afterroute-change pra2
 enterprise company
 dn-set local
 centrex -
 callprefix 8
 condition caller-telno disable
 trunkgroup pra1
 caller no-change
 caller property 1
 called del 8 1
 #
interface Vlanif2
 description To_NewRegion
 ip address 192.168.12.1 255.255.255.0
#
interface GigabitEthernet0/0/0
 description To_New&TransRegion
 ip address 192.168.11.2 255.255.255.252
#
interface GigabitEthernet0/0/1
 description To_BranchAG
 ip address 192.168.11.6 255.255.255.252
#
interface GigabitEthernet0/0/2
```

```
 description To_BranchPBX
 ip address 192.168.11.10 255.255.255.252
#
interface ethernet 2/0/1
port link-type access
port default vlan 2
#
ip route-static 192.168.10.0 255.255.255.0 192.168.11.1
ip route-static 192.168.13.0 255.255.255.0 192.168.11.9
ip route-static 192.168.14.0 255.255.255.0 192.168.11.5
Return
```

- 分布式分支 IP PBX 配置文件

```
#
 sysname brpbx
#
voice
 voip-address signalling interface GigabitEthernet 0/0/1 192.168.11.9
 voip-address media interface GigabitEthernet 0/0/1 192.168.11.9
#
pbx
#
enterprise company
 dn-set local
centrex company
#
callprefix 8
 enterprise company
 dn-set local
 centrex company
 prefix 8
 call-type category 0 attribute 3
 maximum-length 20
 minimum-length 1
 destination-location inter-office
#
callprefix 2222
 enterprise company
 dn-set local
 centrex company
 prefix 2222
 call-type category 0 attribute 3
 maximum-length 15
 minimum-length 1
 destination-location inter-office
#
callprefix 3333
 enterprise company
 dn-set local
 centrex company
 prefix 3333
 call-type category 0 attribute 3
 maximum-length 8
 minimum-length 4
#
callprefix 5662
```

```
 enterprise company
 dn-set local
 centrex company
 prefix 5662
 call-type category 0 attribute 3
 maximum-length 8
 minimum-length 4
#
callprefix 20000
 enterprise company
 dn-set local
 centrex company
 prefix 20000
 call-type category 0 attribute 3
 maximum-length 20
 minimum-length 5
 destination-location inter-office
#
sipserver
 signalling-ip 192.168.11.9
 signalling-port 5060
 media-ip 192.168.11.9
 register-uri company.com
 home-domain company.com
#
pbxuser 22220001
 type port 2/0/2
 enterprise company
#
pbxuser 22220002
 type port 2/0/3
 enterprise company
#
pbxuser 22220003
 type sipue 22220003
 enterprise company
#
dialno 22220001
 pbxuser 22220001
 telno 86 755 22220001
 dn-set local
 callout-right 2
 callin-right 2
#
dialno 22220002
 pbxuser 22220002
 telno 86 755 22220002
 dn-set local
 callout-right 2
 callin-right 2
#
dialno 22220003
 pbxuser 22220003
 telno 86 755 22220003
 dn-set local
```



```
 callout-right 2
 callin-right 2
#
trunkgroup pra
 signalling dss1-user
 enterprise company
 dn-set local
 pra standard Q931
#
trunkgroup sipip
 signalling sip
 enterprise company
 dn-set local
 callin-right 3
 callout-right 3
 sip reg-mode 0
 sip mgc-type 0
 signalling-ip 192.168.11.9
 sip signalling-port 5070
 sip media-ip 192.168.11.9
 sip peer static 192.168.11.2 5070
 sip register-uri company.com
 sip home-domain company.com
#
trunk-pra pra
 port ve1 1/0/0
 trunkgroup pra
#
callroute 8
 enterprise company
 dn-set local
 centrex -
 condition time-period disable
 condition time-repeat disable
 condition caller-telno disable
 trunkgroup sipip
#
callroute 3333
 enterprise company
 dn-set local
 centrex -
 condition time-period disable
 condition time-repeat disable
 condition caller-telno disable
trunkgroup sipip
#
callroute 5662
 enterprise company
 dn-set local
 centrex -
 condition time-period disable
 condition time-repeat disable
 condition caller-telno disable
trunkgroup sipip
#
```

```
callroute 20000
 enterprise company
 dn-set local
 centrex -
 condition time-period disable
 condition time-repeat disable
 condition caller-telno disable
 trunkgroup pra1
#
afterroute-change pra1
 enterprise company
 dn-set local
 centrex -
 callprefix 20000
 condition caller-telno disable
 trunkgroup pra1
 caller no-change
 caller property 1
 called del 8 5
#
afterroute-change sipip
 enterprise company
 dn-set local
 centrex -
 callprefix 8
 condition caller-telno disable
 trunkgroup sipip
 caller no-change
 caller property 1
 called del 8 1
#
interface Vlanif2
 description To_BranchLAN
 ip address 192.168.13.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 description To_Headquarter
 ip address 192.168.11.9 255.255.255.252
#
interface ethernet 2/0/1
port link-type access
port default vlan 2
#
ip route-static 192.168.11.2 255.255.255.252 192.168.11.10
ip route-static 192.168.12.0 255.255.255.0 192.168.11.10
ip route-static 192.168.14.0 255.255.255.0 192.168.11.10
#
Return
```

- 总部 SIP AG 配置文件

```
#
 sysname hqag
#
voice
 voip-address signalling interface GigabitEthernet 0/0/1 192.168.11.1
 voip-address media interface GigabitEthernet 0/0/1 192.168.11.1
```

```
#
sipag 1
 signalling-ip 192.168.11.1
 signalling-port 5060
 media-ip 1.1.1.1
 primary-proxy-ip 192.168.11.2
 primary-proxy-port 5060
 home-domain company.com
#
sipaguser 56620003
 port 3/0/1
 base-telno 56620003
 mgid 1
#
sipaguser 56620004
 port 3/0/2
 base-telno 56620004
 mgid 1
#
interface GigabitEthernet0/0/1
 ip address 192.168.11.1 255.255.255.0
#
Return
```

- 集中式分支 SIP AG 配置文件

```
#
 sysname brag
#
voice
 voip-address signalling interface GigabitEthernet 0/0/1 192.168.1.5
 voip-address media interface GigabitEthernet 0/0/1 192.168.1.5
#
sipag 1
 signalling-ip 192.168.1.5
 signalling-port 5060
 media-ip 1.1.1.1
 primary-proxy-ip 192.168.1.2
 primary-proxy-port 5060
 home-domain company.com
#
sipaguser 33330001
 port 3/0/1
 base-telno 33330001
 mgid 1
#
sipaguser 33330002
 port 3/0/2
 base-telno 33330002
 mgid 1
#
interface GigabitEthernet0/0/1
 ip address 192.168.1.5 255.255.255.0
#
ip route-static 192.168.11.2 255.255.255.252 192.168.11.6
#
Return
```

8 网络管理

8.1 概述

8.1.1 eSight 简介

eSight 应用平台是华为面向企业网管理推出的新一代面向企业园区和分支网络管理系统，实现对企业资源、业务、用户的统一管理以及智能联动。eSight 应用平台支持对 IT&IP，以及第三方设备的统一管理，同时提供灵活的开放平台，为企业量身打造自己的智能管理系统提供基础。

在华为的企业园区网部署方案中，推荐使用 eSight 应用平台实现对网络的管理。eSight 不仅可以实现对于网络中各类节点和资源的监控，还可以实现对于 WLAN 和 IPSec 等业务的配置。

8.1.2 配套版本

表8-1 eSight 配套产品和版本

部件	产品	版本
网管服务器	eSight	V200R001C00

注意

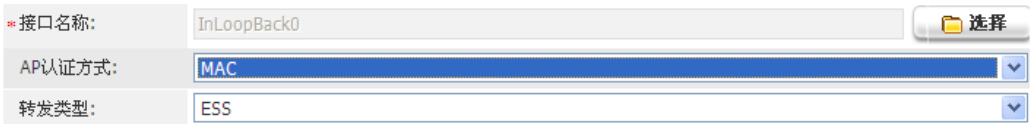
关于 eSight 的安装和配置指导，以及资源管理、性能管理、报表管理、故障管理等基本功能的操作指导，请参考 eSight 产品的配套发布文档和联机帮助。本章中只简要描述 eSight 在业务管理功能方面的操作指导。

8.2 WLAN 业务管理

8.2.1 创建并配置 AC

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”。
3. 在右侧的窗口中，单击“创建”，在“新建 AC”窗口中单击“选择”，在弹出窗口中选择 AC 设备，单击“确定”，新建 AC 设备。
4. 在“新建 AC”窗口中，单击“确定”，AC 创建成功。
5. 单击设置 AC 的基本参数。
6. 在“接口名称”后单击“选择”，选择相应接口，单击“确定”。
7. 配置“AP 认证方式”和“转发类型”参数。

图8-1 配置 AC 基本参数



说明

当 AP 认证方式设置为“不认证”，AP 将自动上线。

当 AP 认证方式设置为“MAC”或“SN”时，用户需要手工导入 AP 设备、离线创建 AP、在白名单中增加 AP 的 MAC 或 SN、在未授权 AP 中对 AP 进行上线确认。

转发类型为 ESS 时，AP 以其绑定的 ESS 模板设置的用户数据转发模式转发用户数据。

转发类型为 AP 时，AP 以自己设置的用户数据转发模式转发用户数据。

----结束

8.2.2 配置 AP 域

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。
3. 在左侧的导航树中选择“WLAN 管理 > AP 域”。
4. 单击“创建”，在弹出的窗口中设置 AP 域的相关参数。

图8-2 配置 AP 域

布放类型取值原则如下。

- 离散布放：域内 AP 的布放非常独立，AP 间信号无任何干扰，此时相当于一个 AP 就是一个域，如果为每个这样的 AP 都创建一个域，用户配置将非常繁琐，因此可以创建一个特殊的域来包含所有的这类 AP，这个域内的 AP 都不需要调优，每个射频都以最大发送功率工作即可。
- 普通布放：域内各 AP 之间分布比较稀疏，为满足基本的业务需求，每个射频的发送功率要求至少达到其最大发送功率的 50%。
- 密集布放：域内各 AP 之间分布比较密集，为满足基本的业务需求，每个射频的发送功率最小可以只达到其最大发送功率的 25%。

5. 单击“确定”，新增 AP 域在列表中显示。

说明

可单击，修改 AP 域的相关参数。

可单击，将对应的 AP 域设置为默认 AP 域。

----结束

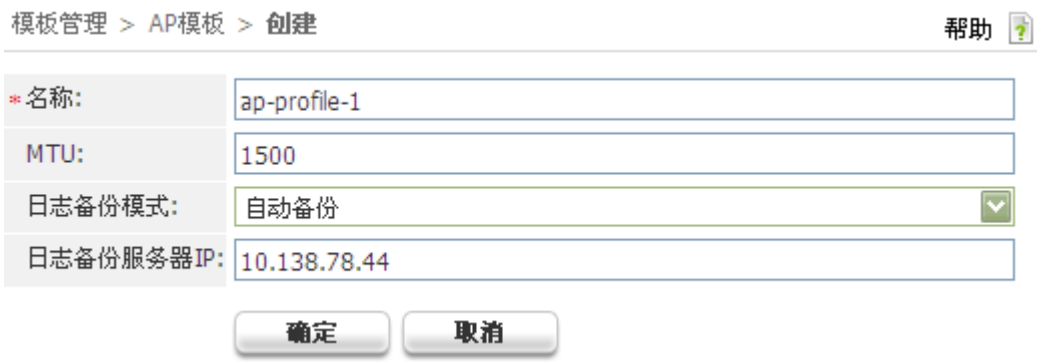
8.2.3 配置模板

通过配置 AP 模板、射频模板、和 ESS 模板并将这些模板与 AP 进行绑定，完成对 AP 的业务配置。

配置 AP 模板

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。
3. 在左侧的导航树中选择“模板管理 > AP 模板”。
4. 单击“创建”，在弹出的窗口中设置 AP 模板的相关参数。

图8-3 配置 AP 模板



5. 单击“确定”，新增 AP 模板在列表中显示。

说明

可单击，修改 AP 模板的相关参数。

----结束

配置射频模板

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。
3. 在左侧的导航树中选择“模板管理 > 射频模板”。
4. 单击“创建”，在弹出的窗口中设置射频模板的相关参数。

图8-4 配置射频模板

5. 单击“确定”，新增射频模板在列表中显示。

说明

可单击，修改射频模板的相关参数。

----结束

配置 ESS 模板

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。
3. 在左侧的导航树中选择“模板管理 > ESS 模板”。
4. 单击“创建”，在弹出的窗口中设置 ESS 模板的相关参数。

图8-5 配置 ESS 模板

5. 单击“确定”，新增 ESS 模板在列表中显示。

说明

可单击，修改 ESS 模板的相关参数。

----结束

8.2.4 配置 AP 上线

AP 上线的一般流程如下：

- 如果某 AP 已经离线添加，则该 AP 可以直接上线。
- 如果没有离线添加 AP，但 AP 的认证模式为“不认证”，或者 AP 的 MAC 或 SN 在已设置的“白名单”中，则该 AP 可以自动添加并上线。
- 如果 AP 设备不存在于白名单或 AP 列表中，且其认证模式非“不认证”情况下，则该 AP 设备存在于未认证 AP 列表之中。可通过确认未认证 AP 列表中的 AP 设备方式添加 AP 设备。

配置 AP 白名单

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。
3. 在左侧的导航树中选择“WLAN 管理 > AP 白名单”。
4. 单击“创建”，在弹出的窗口中设置 AP 白名单的相关参数。。

图8-6 配置 AP 白名单

5. 单击“确定”，新增 AP 白名单在列表中显示。

----结束

离线增加 AP

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。
3. 在左侧的导航树中选择“WLAN 管理 > AP”。
4. 单击“创建”，在弹出的窗口中设置 AP 的相关参数。

图8-7 离线增加 AP

5. 单击“AP 域”的“选择”按钮，选择 AP 所属的域。
6. 单击“AP 模板”的“选择”按钮，为 AP 绑定 AP 模板。
7. 单击“射频模板”的“绑定”按钮，为 AP 绑定射频模板。
8. 单击“ESS 模板”的“绑定”按钮，为 AP 绑定 ESS 模板。
9. 单击“确定”，完成离线 AP 的创建。

----结束

确认未授权 AP

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中单击对应 AC 的“名称”。
3. 在左侧的导航树中选择“WLAN 管理 > 未授权 AP”。
4. 单击“同步”，同步所有 AP 的数据。
5. 如果有未授权的 AP，单击“上线确认”。

图8-8 确认未授权 AP

----结束

8.2.5 监控 WLAN 业务

查看 WLAN 概要信息

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“概览信息 > 概览信息”，在右侧的窗口中可以看到 WLAN 的概要信息。包括：
   - 用户在线趋势图（最近 24 小时）
   - 资源统计（AC 数量、Fit AP 总数、Fit AP 在线数、Rogue AP 数、SSID 总数、在线 STA 总数）
   - Top 5 用户接入 Fit AP
   - Top 5 用户接入 SSID
   - Top 5 告警设备

----结束

图8-9 查看 WLAN 概要信息

查看 AC 信息

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > AC”，在右侧的窗口中可以看到所有 AC 概要信息。

图8-10 查看 AC 概要信息

3. 单击某个 AC 的名称，可以查看指定 AC 的详细信息。

图8-11 查看 AC 详细信息

----结束

查看 AP 信息

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > Fit AP”，在右侧的窗口中可以看到所有 AP 概要信息。

图8-12 查看 AP 概要信息

3. 单击某个 AP 的名称，可以查看指定 AP 的详细信息。

图8-13 查看 AP 详细信息

----结束

查看 STA 信息

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > STA”，在右侧的窗口中可以看到所有 STA 信息。

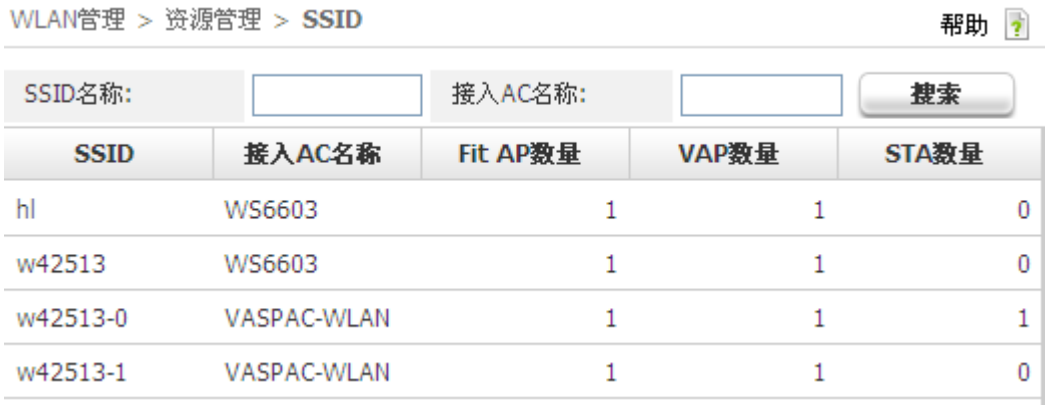
图8-14 查看 STA 信息

----结束

查看 SSID 信息

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > SSID”，在右侧的窗口中可以看到所有 SSID 信息。

图8-15 查看 SSID 信息



----结束

查看 Rogue AP 信息

Rogue AP 即非法 AP，是未授权加入无线网络的接入点，或不具有正确安全配置的接入点。非法 AP 可以允许非授权的网络访问，造成无线终端在不知情的情况下错误地接入到非法 AP，从而造成网络资源的浪费。

1. 在主菜单中选择“网络应用 > WLAN 管理”。
2. 在左侧的导航树中选择“资源管理 > Rogue AP”，在右侧的窗口中可以看到所有 Rogue AP 信息。部分信息解释如下：
   - BSSID：非法 AP 的 MAC 地址。

- 信道：接入点之间通过无线频道通信。当在同一区域中有多个接入点时，相邻接入点设置的信道输至少要间隔 5 个信道，以避免互相干扰。
- RSSI：（Received Signal Strength Indicator）接收信号强度指示。

图8-16 查看 Rogue AP 信息

ID	BSSID	信道	RSSI(dbm)	邻居AP名称	接入AC名称
0	28-6E-D4-31-95-00	6	-0.01	ap-1	VASPAC-WLAN
1	28-6E-D4-27-0D-E1	6	-0.01	ap-1	VASPAC-WLAN
2	28-6E-D4-27-0D-E2	6	-0.01	ap-1	VASPAC-WLAN
3	28-6E-D4-2B-23-60	6	-0.01	ap-1	VASPAC-WLAN
4	28-6E-D4-27-0D-60	6	-0.01	ap-1	VASPAC-WLAN
5	28-6E-D4-27-0D-E0	6	-0.01	ap-1	VASPAC-WLAN
6	02-04-18-03-00-80	6	-0.01	ap-1	VASPAC-WLAN
7	28-6E-D4-31-95-0F	6	-0.01	ap-1	VASPAC-WLAN
8	5C-4C-A9-00-67-E0	6	-0.01	ap-1	VASPAC-WLAN
9	5C-4C-A9-00-67-EF	6	-0.01	ap-1	VASPAC-WLAN
10	02-04-18-03-01-00	6	-0.01	ap-1	VASPAC-WLAN
11	28-6E-D4-31-93-F0	6	-0.01	ap-1	VASPAC-WLAN
12	28-6E-D4-31-93-FF	6	-0.01	ap-1	VASPAC-WLAN
13	28-6E-D4-2B-23-6F	6	-0.01	ap-1	VASPAC-WLAN
14	28-6E-D4-31-A2-41	11	-0.01	ap-1	VASPAC-WLAN

----结束

8.3 IPSec 业务管理

eSight 支持对 IPSec VPN 的监控管理，包括同步网络域隧道、查看网络域详细信息（隧道列表、网络域拓扑）。

8.3.1 新建网络域

用户可以对某一区域的 IPSec VPN 业务进行集中管理。管理 IPSec VPN 业务时，需要新建一个网络域，然后根据管理的需求，在网络域中新增设备。

1. 在主菜单中选择“网络应用 > IPSec VPN 业务管理”。
2. 在基本信息窗格，单击“新建”。
3. 在弹出的窗口中，设置“网络域名称”和“网络域描述”。
4. 在网元列表中单击“创建”，选择网元，单击“确定”。

----结束

8.3.2 发现网络域 IPSec VPN 业务

用户创建网络域之后，需要将设备上的隧道信息同步到 eSight，便于 eSight 对隧道的联通性进行监控。

1. 在主菜单中选择“网络应用 > IPSec VPN 业务管理”。
2. 在左侧导航树中选择“IPSec Vpn 资源管理 > 网络域管理”，在右侧窗口中单击“网络域名称”，进入 IPSec VPN 业务的网络域。
3. 单击“同步”，将设备上的 IPSec VPN 隧道同步到 eSight。

----结束

8.3.3 查看 IPSec VPN 业务拓扑结构

用户在 eSight 执行查看网络域的拓扑结构操作，可以在拓扑图展示了当前网络域的节点之间的隧道以及隧道的状态信息。

1. 在主菜单中选择“网络应用 > IPSec VPN 业务管理”。
2. 在左侧导航树中选择“IPSec Vpn 资源管理 > 网络域管理”，在右侧窗口中单击“网络域名称”，进入 IPSec VPN 业务的网络域。
3. 在“隧道拓扑”窗格中查看 IPSec VPN 业务的拓扑信息。

   拓扑上用颜色区分隧道的连通性状态。

   - 绿色表示连通。
   - 红色表示未连通。

----结束

8.3.4 查看 IPSec VPN 业务运行状态

对 IPSec VPN 业务进行维护时，需要定时查看其运行状态。

1. 在主菜单中选择“网络应用 > IPSec VPN 业务管理”。

2. 在左侧导航树中选择“IPSec Vpn 资源管理 > 网络域管理”，在右侧窗口中单击“网络域名称”，进入 IPSec VPN 业务的网络域。
3. （可选）单击“同步”，将设备上的 IPSec VPN 隧道同步到 eSight。
4. 在“隧道列表”中查看“隧道状态”的值。

----结束