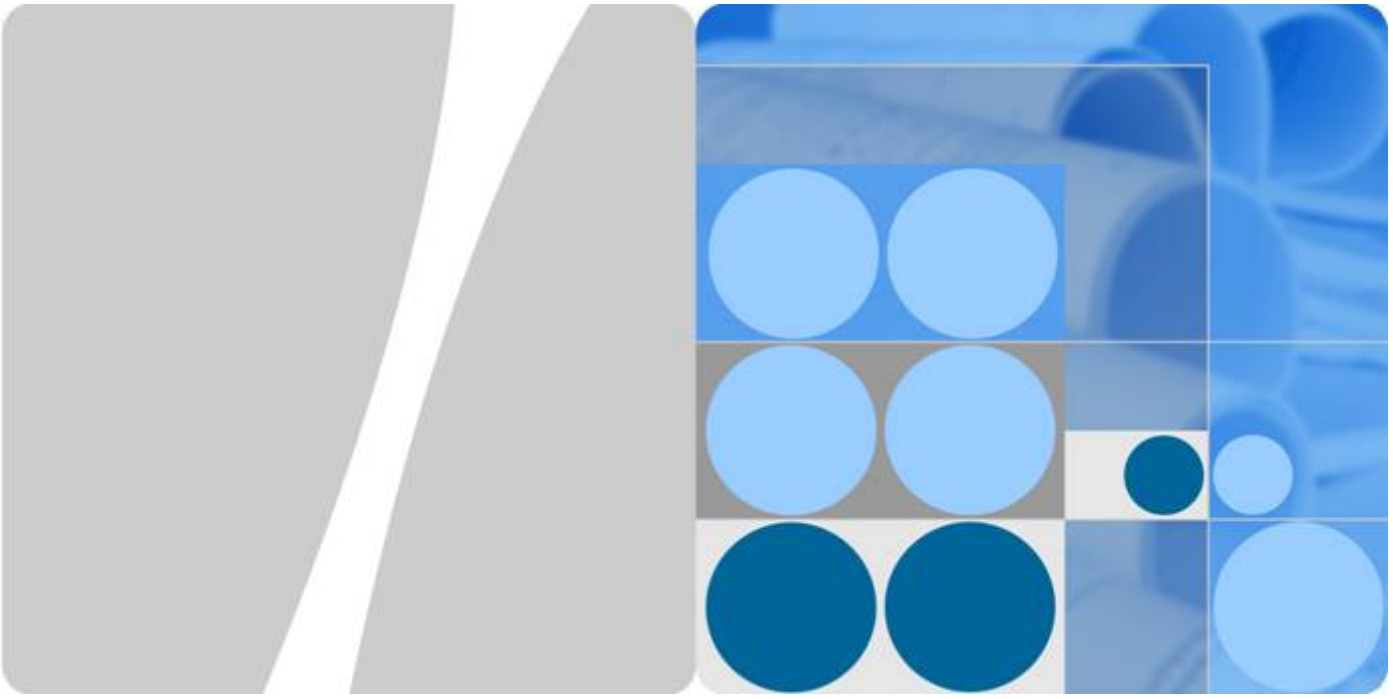


金融行业配置案例

文档版本　03

发布日期　2017-05-08

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://e.huawei.com

目 录

1 前言

声明

由于产品版本升级或其它原因，本手册内容会不定期进行更新。除非另有约定，本手册仅作为使用参考。

由于设备不同版本之间的差异，部分命令和回显之间会有小许差异，请以实际的设备为准。

读者对象

本文档主要供用户在规划组网、配置设备过程中参考。

本文档主要适用于以下工程师：

- 系统维护工程师
- 调测工程师
- 网络监控工程师
- 现场维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。

符号	说明
注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... } *	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...] *	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&的参数可以重复1～n次。
#	由“#”开始的行表示为注释行。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 03 (2017-05-08)

随产品更新。

文档版本 02 (2016-9-10)

该版本的更新如下：

新增：

- M-LAG数据中心部署方案
- 基于“云平台+敏捷控制器+硬件集中式overlay”的数据中心网络部署方案

文档版本 01 (2015-10-10)

第一次正式发布。

2 传统数据中心部署方案

2.1 概述

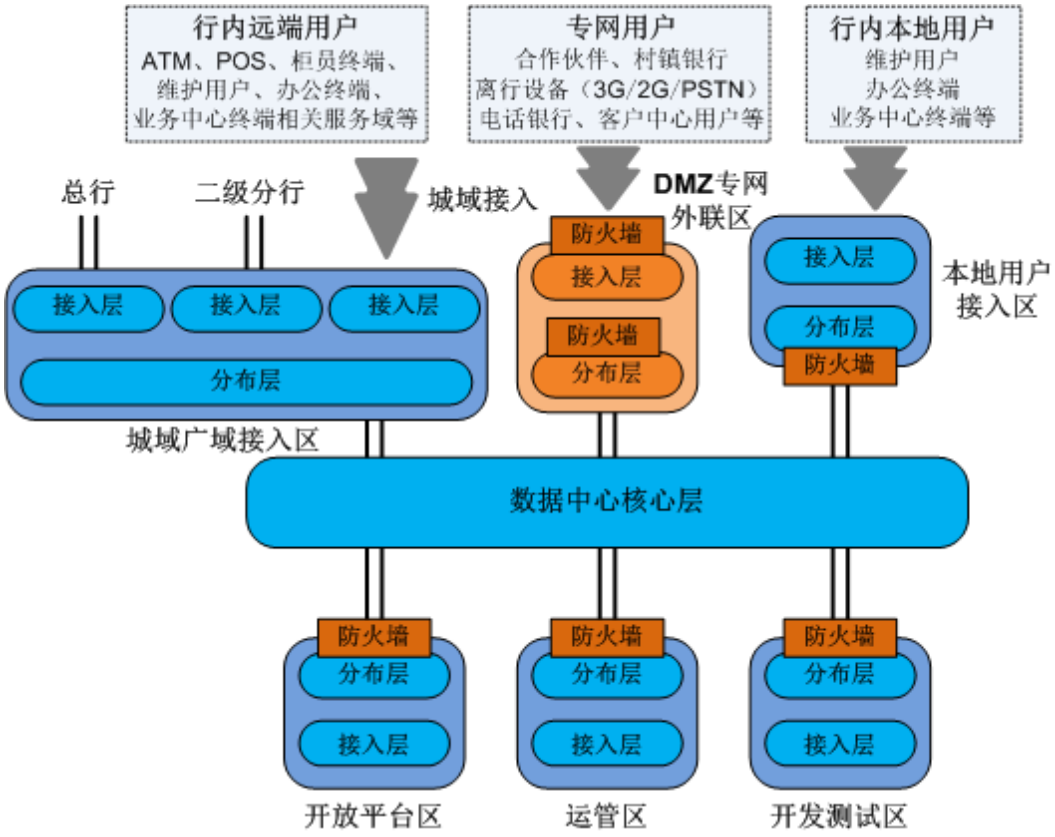
2.1.1 简介

本文档是银行一级分行数据中心的详细设计方案案例，对一级分行数据中心网络架构、IP地址和VLAN规划、路由设计、安全设计、网络可靠性设计、网管部署设计等进行了详细的描述。本文档可用于项目的实施参考。

2.1.2 典型组网

2.1.2.1 逻辑架构

根据功能分区规划，一级分行数据中心网络逻辑拓扑架构如下图：



各功能区介绍如下：

网络分区	分区功能和定位	接受访问
开放平台区：OP	已投产开放系统接入，通常包含直接动账、账目相关和非相关的业务。该区是最主要的业务区，满足生产、办公业务互访。	面向用户端和服务端。

网络分区	分区功能和定位	接受访问
运管区：OM	接入承载运行、监控和维护系统的服务器，用于对网络和系统进行管理及维护。	通常仅面向少数的授权维护用户。
开发测试区：DT	接入承载未投产业务系统的服务器，包括开发测试的主机和开放平台系统接入。	面向用户端和服务端。
城域广域接入区：WN/MN	实现一级分行上联总行与数据中心，下联二级分行与网点，以及与同城机构、分支网点的互联。从全行网络架构上分析，该区完成一级分行辖内区域的接入，包括一级分行局域网和辖内分支机构。	ATM、POS、柜员终端、维护用户、办公终端、业务中心终端等。
本地用户接入区：LU	满足各种类型用户终端接入。	本地维护用户、本地办公终端、本地业务中心终端。
DMZ专网外联区：EP	主要实现业务的外联，包括同行业的往来业务、重点客户的业务、中间代理业务等的平台互连，需要通过电信、联通等运营商提供的线路与合作伙伴互联。	合作伙伴、境外机构、离行设备（3G/2G/PSTN)、电话银行、客服中心用户。

一级分行数据中心网络在逻辑上形成三层结构：核心层、分布层和接入层。

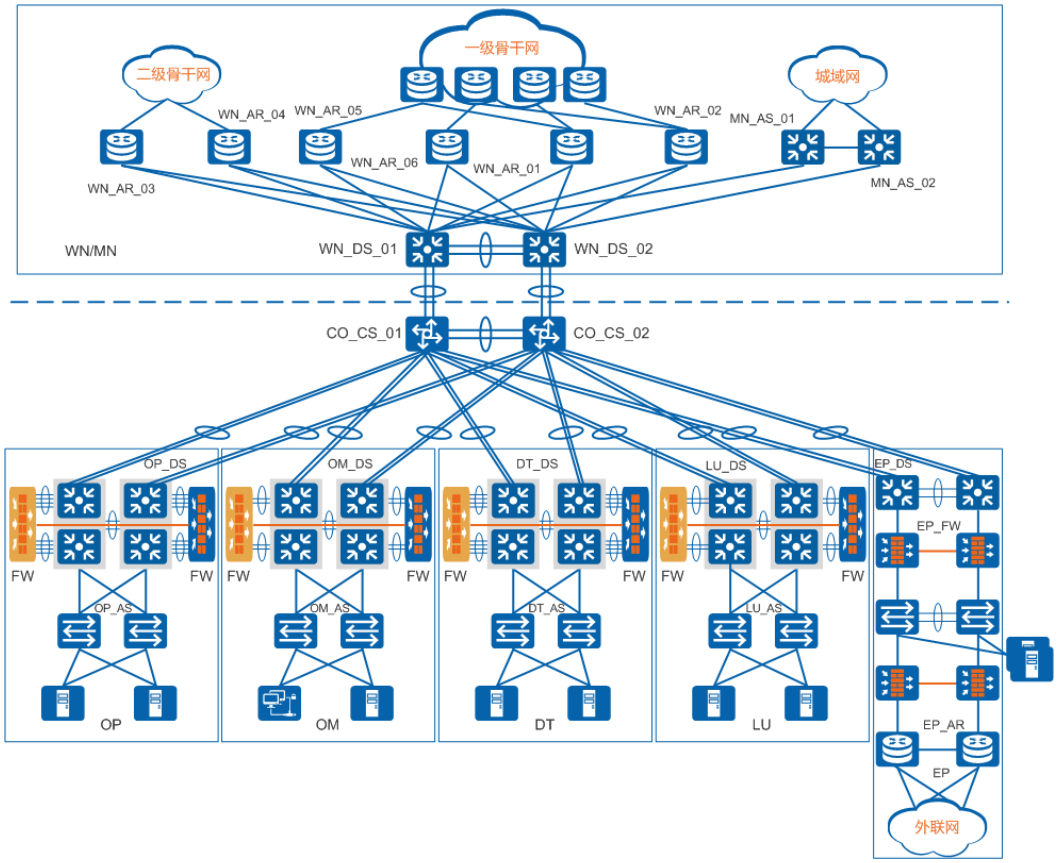
- 核心层：作为高速的三层交换骨干，核心层不直接连接终端和服务器，也不部署影响高速交换性能的ACL等功能。
- 分布层：作为二三层分界，同时作为功能分区边界。分布层与核心层进行三层连接，与接入层进行二层连接，主要完成以下的功能：
  - 作为功能区各类终端和服务器的统一网关；
  - 汇聚功能区内部路由；
  - 实现功能区内VLAN间的路由；
  - 实现功能区到核心层的路由策略；
  - 实施安全访问控制（ACL），实现功能区内部互访控制；
  - 部署防火墙，构建分区间互访安全控制策略。
- 接入层：连接对应功能分区的分布层，主要完成以下功能：
  - 接入层交换机（AS）：

    为服务器及其它终端提供二层网络接入；通过VLAN定义实现接入的隔离。
  - 接入层路由器（AR）：

提供广域、城域网络接入；作为广域网接入ASBR，进行路由控制。

2.1.2.2 物理架构

一级分行数据中心整体物理网络连接如下图：



核心交换区采用两台高性能的数据中心交换机作为整个数据中心网络的核心，核心交换机之间采用万兆以太网接口链路捆绑互联，共同建立起一个高可靠的高速交换核心区。

核心交换区与各分布层交换机的物理连接冗余备份，采用“口”字型连接，保证网络可靠性。核心交换区与各分布层交换机之间采用万兆（或千兆）以太网接口捆绑互联。

各个功能区分布层交换机采用两台高性能交换机作为分区汇聚，两台交换机之间根据实际板卡配置采用万兆或千兆端口进行链路捆绑互联。分区内接入层交换机通过双归的方式交叉上联到两台分布层交换机。

分区内部署防火墙实现各分区安全访问控制。防火墙旁挂在分布层交换机上，采用千兆以太网接口捆绑互联。两台防火墙采用主备冗余架构，当主防火墙出现故障时，系统可在较短的时间内自动切换到备用防火墙上面。如果主备防火墙都出现故障，业务从bypass链路通过，从而保障数据的不间断转发和业务的正常运行。

外联区两对防火墙分别与分布层交换机、接入层交换机、接入路由器通过“口”字型连接。

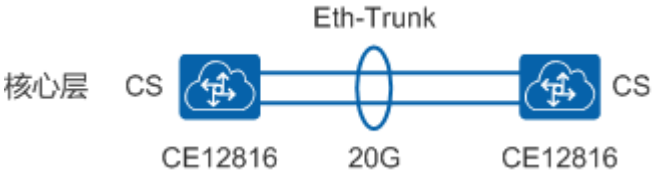
2.1.2.3 产品规划

核心层设备采用CE12816，分布层设备采用CE12808，接入层交换机采用CE6800，接入层路由器采用NE40E-X8，防火墙采用USG5500。

2.1.3 详细架构设计

2.1.3.1 核心交换区

一级分行数据中心核心交换区如下图所示：



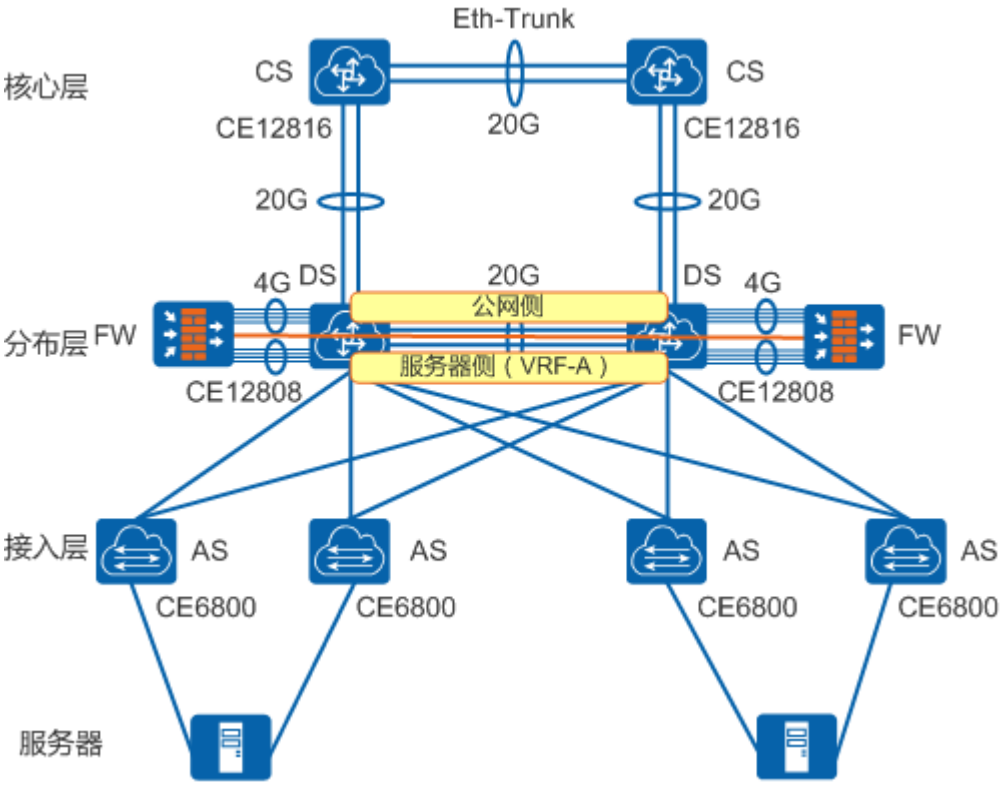
核心层是整个一级分行数据中心网络的核心，连接数据中心内部各个功能分区。核心层由两台高性能数据中心交换机CE12816组成，两台核心交换机之间通过2条10GE链路跨板捆绑，保障连接可靠性。

设备型号如下所示。

CS：华为CE12816

2.1.3.2 开放平台区

一级分行数据中心开放平台区结构如下图所示：



开放平台区分区分布层采用两台高性能数据中心交换机CE12808，上联、互联均采用2×10GE跨板捆绑，接入层交换机CE6800通过GE双归接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用4×GE跨板捆绑。

设备型号如下所示。

CS：华为CE12816

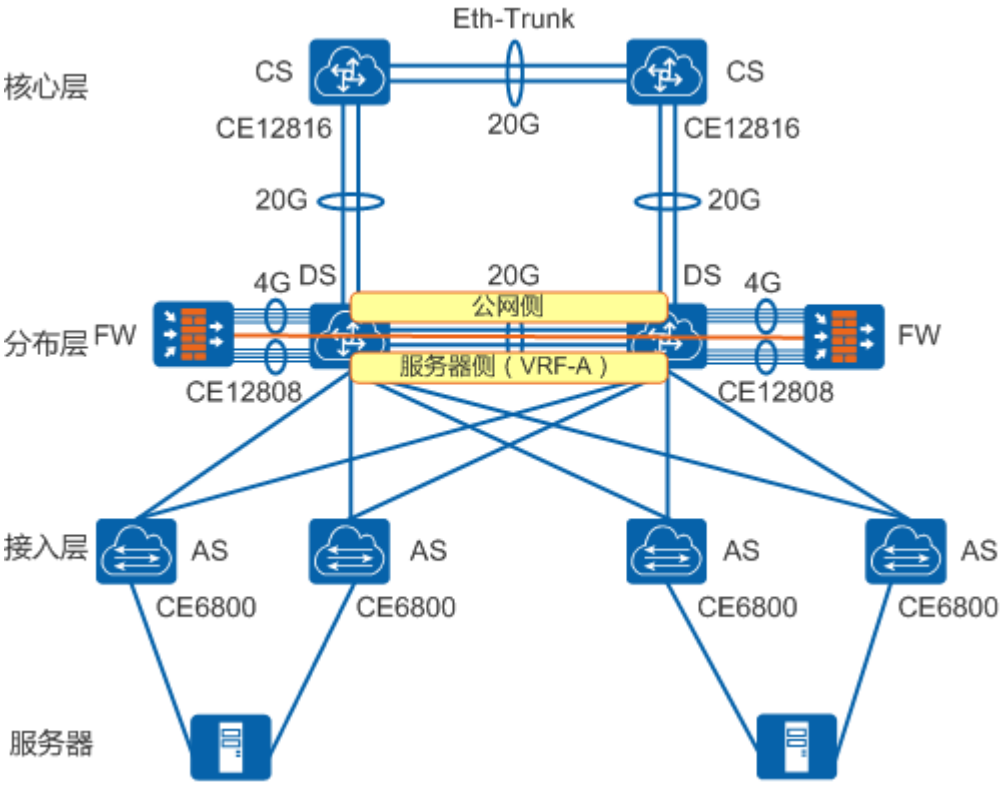
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

2.1.3.3 开发测试区

一级分行数据中心开发测试区结构如下图所示：



开发测试区分区分布层采用两台高性能数据中心交换机CE12808，上联、互联均采用2×10GE跨板捆绑，接入层交换机CE6800通过GE双归接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用4×GE跨板捆绑。

设备型号如下所示。

CS：华为CE12816

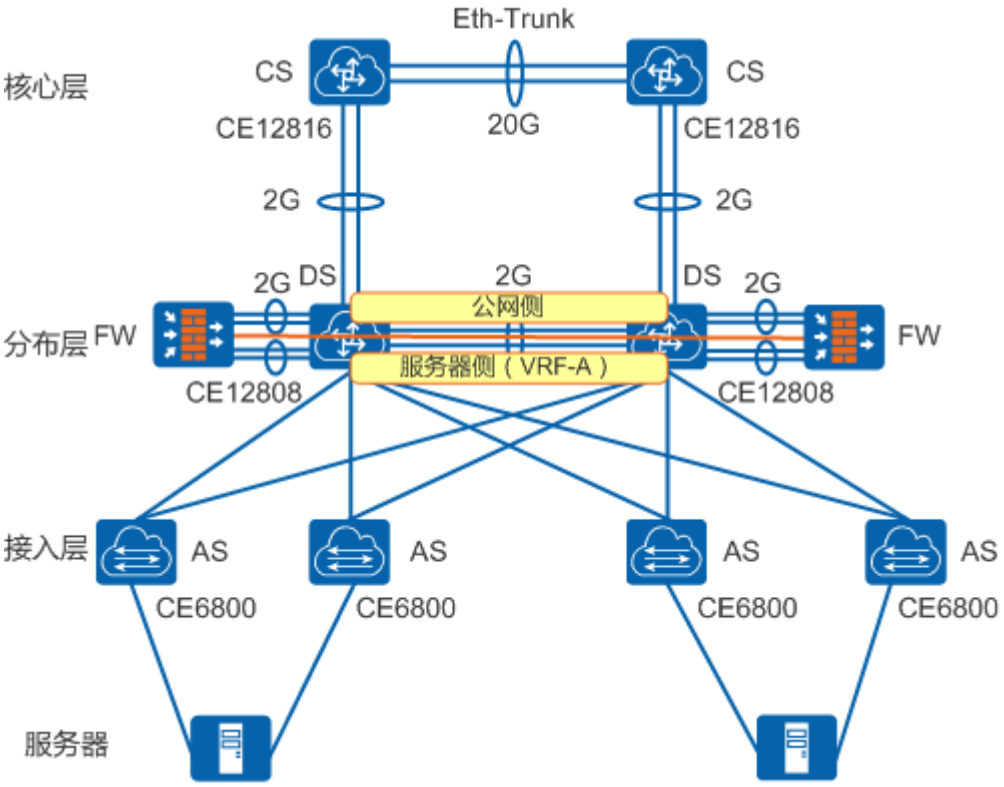
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

2.1.3.4 运管区

一级分行数据中心运管区结构如下图所示：



运管区是一级分行网络的管理及维护中心。该区收集被管理系统、设备的运行状态信息，监控网络、系统状态，下达管理指令，排除系统故障。

分区分布层采用两台高性能数据中心交换机华为CE12808，上联、互联均采用2×GE光口跨板捆绑，接入层交换机通过GE双归接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用2×GE光口跨板捆绑。

运管区部署下面几类设备：

管理服务器：管理服务器基于SNMP协议获取网络、系统运行信息；接收网络、系统发送的网络、系统日志和告警信息。管理服务器将收集的管理信息进行汇总、处理，对数据中心网络/系统运行状况进行监控，生成网络/系统管理报表。

运管平台：一线值班人员通过一级分行数据中心的运行/管理操作台访问管理服务器；对发生故障的设备进行故障诊断和排查。

安全工具：为实现系统安全而提供的配套安全工具。例如Radius服务器，IDS服务器，防病毒系统服务器等。

设备型号如下所示。

CS：华为CE12816

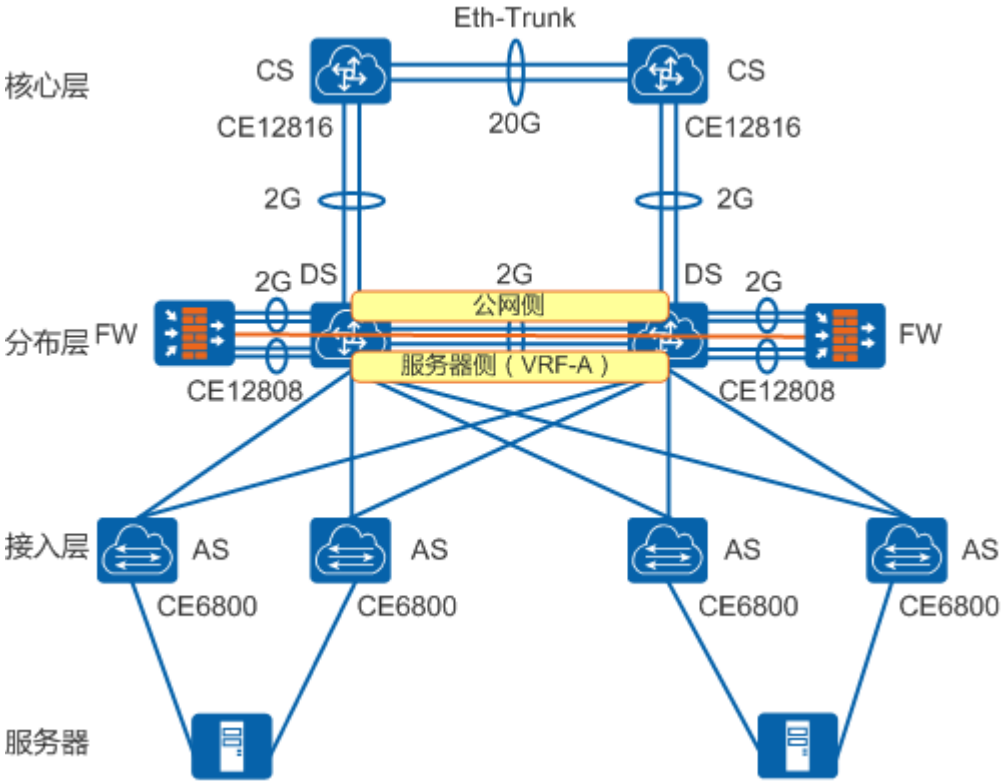
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

2.1.3.5 本地用户接入区

一级分行数据中心本地用户接入区结构如下图所示：



本地用户接入区建设的目标是满足各种类型用户终端互访需求。

分区分布层采用两台高性能数据中心交换机CE12808，上联、互联均采用2×GE光口跨板捆绑，接入层交换机通过GE双归接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用2×GE光口跨板捆绑。

设备型号如下所示。

CS：华为CE12816

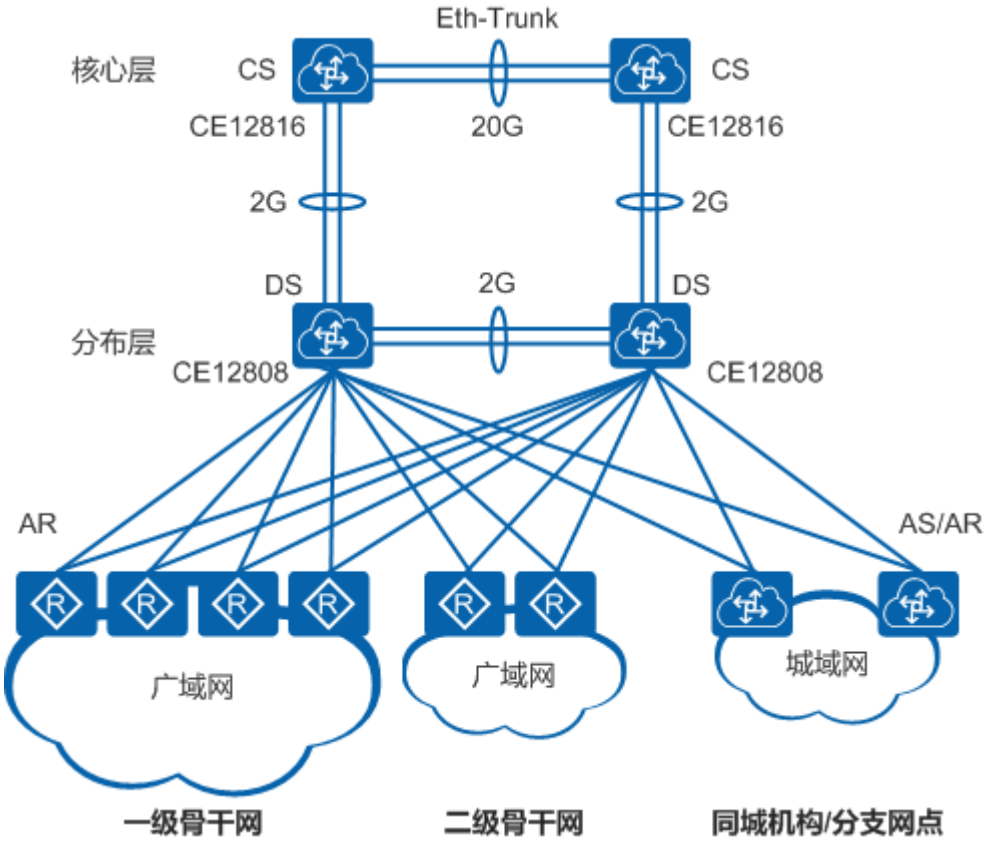
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

2.1.3.6 城域广域接入区

一级分行数据中心广域城域区结构如下图所示：



城域广域接入区实现与上联区、下联区路由器和同城接入设备的互联。

分区分布层采用两台高性能数据中心交换机CE12808，上联、互联均采用2×GE光口跨板捆绑，广域接入层采用双归接入，城域接入层采用“口”字型上联接入。

本区域仅用于广域、城域接入，不存在本地服务器，因此分布层不部署防火墙，接入的同城机构、分支网点或者二级分行部署UTM进行安全防护。

设备型号如下所示。

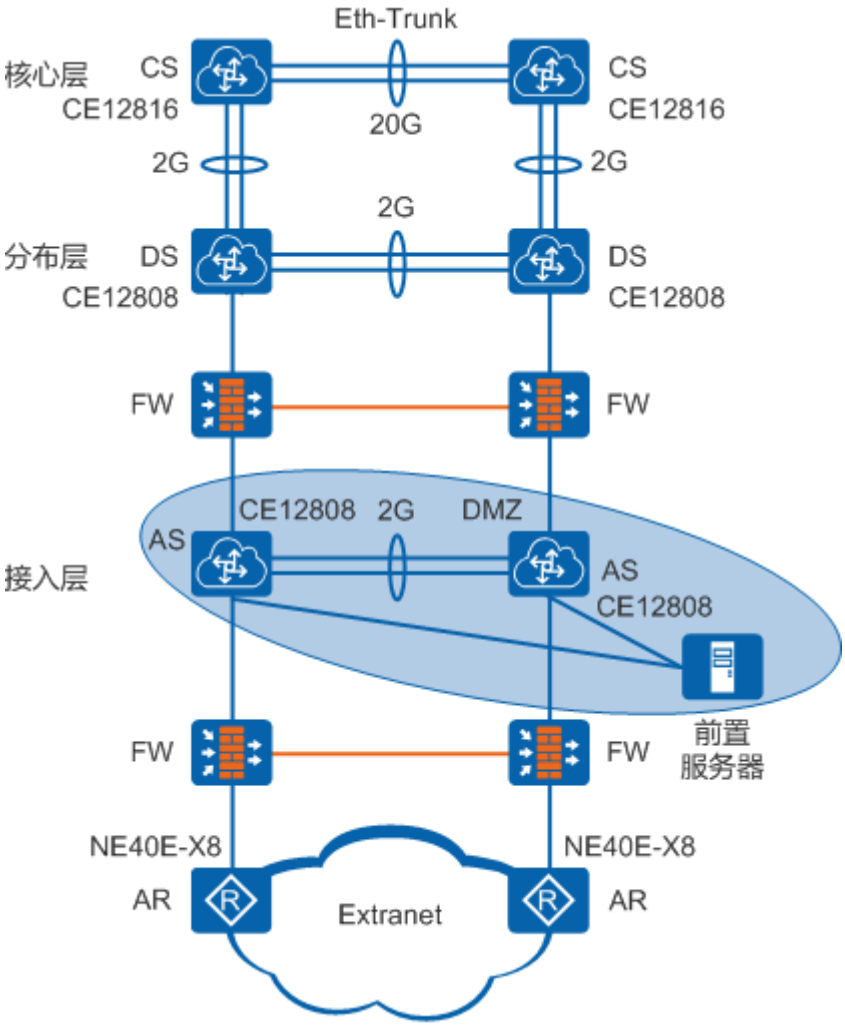
CS：华为CE12816

DS：华为CE12808

AR：华为NE40E-X8

2.1.3.7 外联区

一级分行数据中心外联区结构如下图所示：



外联区主要是实现与合作伙伴的网络连通性。为了提高该区域的安全性，避免外联单位直接访问本行的内网服务器区，采用两层异构防火墙的架构，把整个区域划分成外联区、DMZ区和内网区共3个等级不同的安全子区，3个安全子区的功能作用如下表所示：

网络分区	功能作用
外联区	提供与合作伙伴网络连接的通路，实现合作伙伴的专线接入和合作伙伴私网地址到DMZ私网地址的翻译
DMZ区	部署分行外联区业务前置机
内网区	一级分行数据中心网络系统

外联区的每一个层次在逻辑上提供不同的网络功能，安全级别由外向内逐一提高。下面针对该物理结构，由外到内分别作介绍：

角色	功能作用
外联路由器	用于第三方合作伙伴的接入，两台路由器分别接入不同运营商的线路，主线接入主用路由器，备线接入备用路由器，实现线路的冗余备份接入； 路由器与外层防火墙的互联端口启用虚拟路由器冗余备份协议（VRRP）。一般情况下，数据流始终先到主用路由器上，出现故障时，才切换到备用路由器，防止单机故障，实现设备的可靠性和冗余性； 如果接入的是ATM，MSTP等无法自动检测链路状态的线路类型时，需要手动在接口上配置OAM或BFD等链路故障检测协议，并要求对方也支持并启用该协议。
外层防火墙	用于外联区和DMZ区的逻辑分割和安全控制，防火墙应根据应用的需要配置安全策略。 两台防火墙工作在NAT模式下，采用HA的双机冗余架构，通常情况下一台防火墙工作在主用模式下，而另外一台防火墙工作在备用模式下，当主防火墙出现故障时，系统可在较短的时间内自动切换到备用防火墙上面，从而保障了数据的不间断转发和业务的正常运行。
接入层交换机	用于外联区前置服务器的接入，交换机之间采用双链路捆绑的方式连接，提高了设备的可靠性。 外联区接入层交换机可根据需要灵活增加。
内层防火墙	用于DMZ区和内网的逻辑分割和安全控制，防火墙应根据应用的需要配置安全策略。 两台防火墙工作在NAT模式下，采用HA的双机冗余架构，通常情况下一台防火墙工作在主用模式下，而另外一台防火墙工作在备用模式下，当主防火墙出现故障时，系统可在较短的时间内自动切换到备用防火墙上面，从而保障了数据的不间断转发和业务的正常运行。
分布层交换机	用于一级分行外联区与内部局域网之间的连接。 两台分布层交换机之间采用双链路捆绑的方式连接，提高了设备的可靠性。

设备型号如下所示。

CS：华为CE12816

DS：华为CE12808

AS：华为CE12808

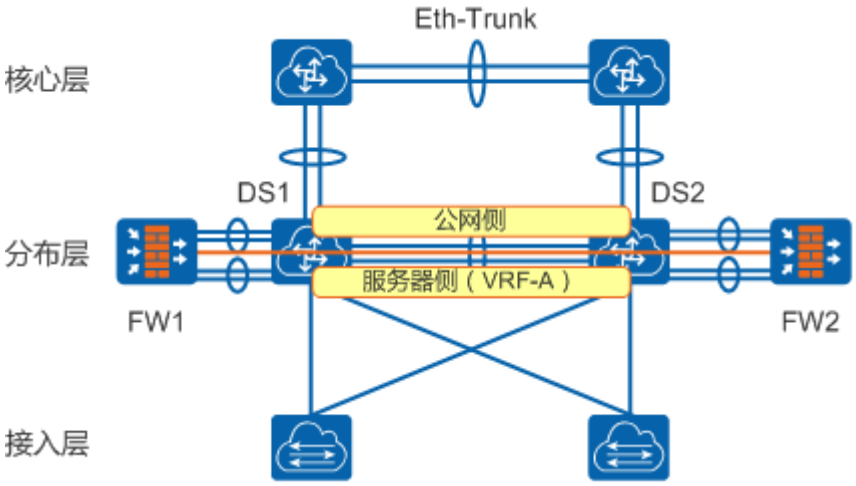
AR：华为NE40E-X8

FW：华为USG5500

2.1.3.8 防火墙部署设计

为了提升网络安全，一级分行数据中心网络中，在开放平台区（OP）、开发测试区（DT）、本地用户接入区（LU）和运管区（OM）部署防火墙，通过配置访问控制策略，实现功能分区之间的隔离和控制，对这些分区内部的服务器资源进行安全防护。

防火墙设备的部署采用旁挂方式。防火墙旁挂结构如下图所示：



- 防火墙采用HA方式部署，配置抢占模式。正常情况， 左侧FW1为主防火墙，右侧FW2为备防火墙。
- 两台防火墙之间心跳线采用两个独立端口直连。
- FW1和FW2防火墙旁挂方式跨接在2台分布层交换机上。
- 防火墙与分布层交换机采用链路聚合方式绑定接口互连。主防火墙FW1上连接口根据不同分区需求将4个或2个接口捆绑成一个Eth-Trunk1连接DS1交换机；下连接口根据不同分区需求将4个或2个接口捆绑成一个Eth-Trunk2连接DS1交换机。备防火墙FW2上连接口将4个或2个接口捆绑成一个Eth-Trunk1连接DS2交换机；下连接口将4个或2个接口捆绑成一个Eth-Trunk2连接DS2交换机。
- 防火墙监控Eth-Trunk1和Eth-Trunk2两个Eth-Trunk接口的物理状态，当两个接口中的任意一个发生故障时，防火墙进行主备切换，FW2变为主防火墙，FW1变为备份防火墙。
- 当主备防火墙都发生故障时，可以手动切换数据流经Bypass链路旁路防火墙。Bypass链路部署在汇聚交换机上下两个VRF之间，使用独立外接链路方式。
- 防火墙与DS交换机间采用静态路由＋VRRP方式进行对接。
- 防火墙配置trust和untrust区进行逻辑分割和安全控制，防火墙根据应用的需要配置安全策略。

  设备型号如下所示。

CS：华为CE12816
DS：华为CE12808
AS：华为CE6800
FW：华为USG5500

2.2 业务设计与配置

2.2.1 系统配置

2.2.1.1 登录设备配置

用户可以通过Console口、Telnet或STelnet方式登录设备，实现对设备的本地或远程维护。首次登录设备需要使用Console口登录。使用Telnet或者STelnet方式可以实现对设备的远程管理和维护。

下面分别介绍通过Console口登录设备和通过STelnet登录设备两种方式。

- 通过Console口登录设备

  在配置用户通过Console口登录设备之前，需完成以下任务：

  a. 准备好Console通信电缆。
  b. PC端准备好终端仿真软件。

  说明

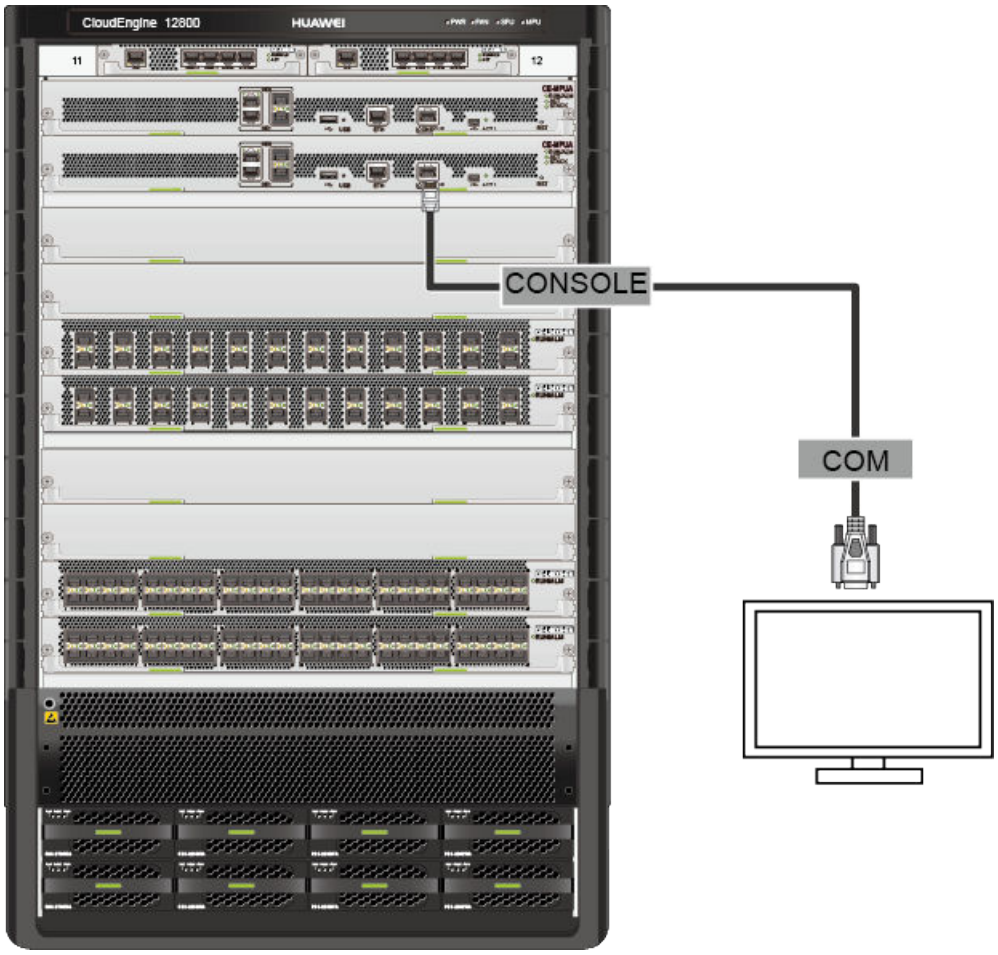
  如果PC使用系统自带的终端仿真软件（如Windows 2000系统的超级终端），则无需另行准备；如果系统不带终端仿真软件，请您准备第三方终端仿真软件，使用方法请参照该软件的使用指导或联机帮助。

  操作步骤：

  使用终端仿真软件通过Console口登录设备。

  a. 请使用产品随机附带的Console通信电缆的DB9（孔）插头插入PC机的9芯（针）串口插座，再将RJ-45插头端插入设备的Console口中，如图1所示。

图 2-1 通过 Console 口连接设备



b. 在PC上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。

说明

因为PC端可能会存在多个连接接口，这里需要选择的是连接Console线缆的那个接口。一般情况下，选择的接口是COM1。

若修改了设备的串口通信参数值，需要在PC端更换通信参数值与设备的串口通信参数值一致后，重新连接。

c. 按Enter键，直到系统出现如下显示，提示用户输入密码。（AAA认证时，提示输入用户名和密码，以下显示信息仅为示意）

```
Login authentication


Password:
```

进入设备后，用户可以键入命令，对设备进行配置，需要帮助可以随时键入“?”。

- 通过STelnet登录设备

  在配置用户通过STelnet登录设备之前，需完成以下任务：

  a. 终端与设备之间路由可达。

  b. 终端上已安装SSH客户端软件。

  操作步骤：

  a. 配置STelnet服务器功能及参数

```
<HUAWEI> system-view
[~HUAWEI] rsa local-key-pair create
```

```
The key name will be: HUAWEI_Host
The range of public key size is (512 ~ 2048).
NOTE: Key pair generation will take a short while.
Input the bits in the modulus [default = 2048] : 2048  //从V200R001C00版本开始，仅支持2048bit，不需要用户输入。
[*HUAWEI] stelnet server enable
[*HUAWEI] commit
```

b. 配置SSH用户登录的用户界面

```
[~HUAWEI] user-interface vty 0 4
[~HUAWEI-ui-vty0-4] authentication-mode aaa
[*HUAWEI-ui-vty0-4] protocol inbound ssh
[*HUAWEI-ui-vty0-4] commit
[~HUAWEI-ui-vty0-4] quit
```

c. 配置SSH用户

配置SSH用户包括配置SSH用户的验证方式，设备支持的认证方式包括RSA、password、password-rsa、DSA、password-dsa、ECC、password-ecc和all。其中：

password-rsa认证需要同时满足password认证和RSA认证。

password-dsa认证需要同时满足password认证和DSA认证。

password-ecc认证需要同时满足password认证和ECC认证。

all认证是指password认证、RSA、DSA或ECC认证方式满足其中一种即可。

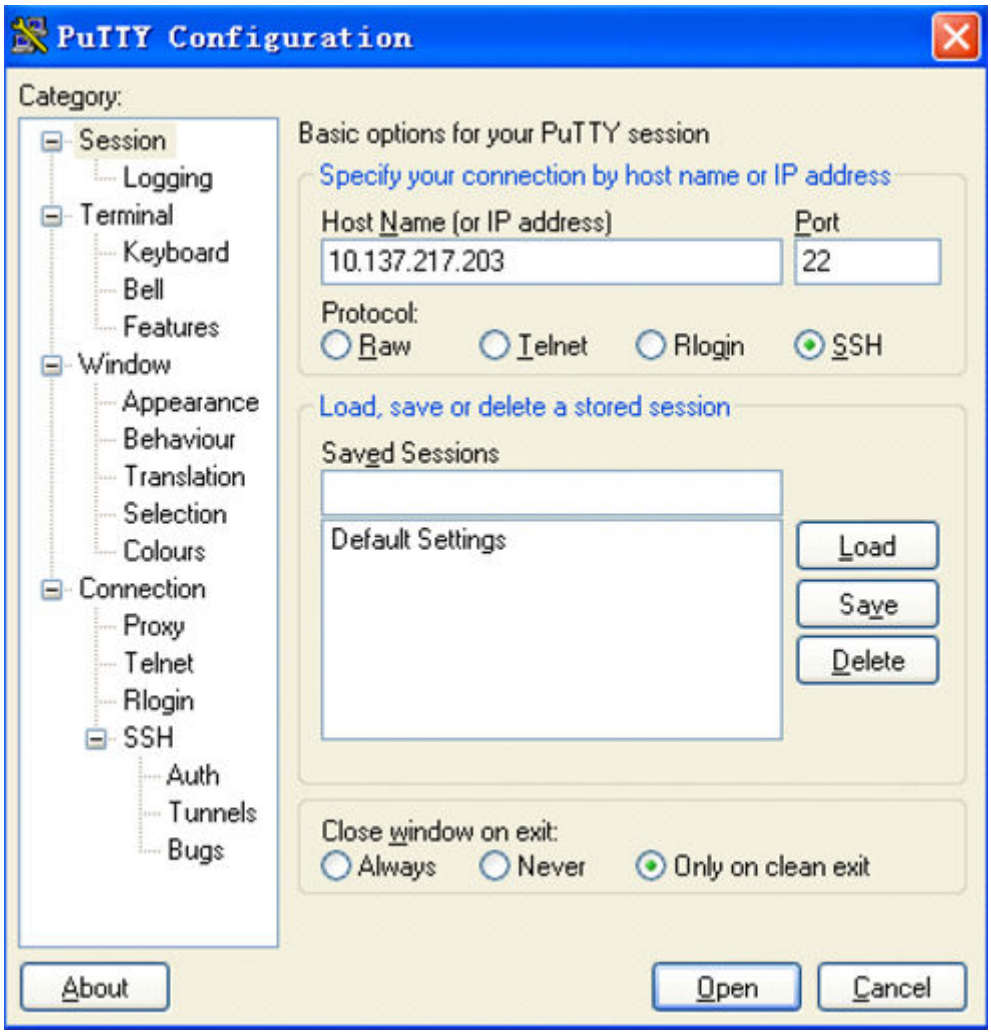
```
[~HUAWEI] ssh user client001
[*HUAWEI] ssh user client001 authentication-type password
[*HUAWEI] ssh user client001 service-type stelnet
[*HUAWEI] aaa
[*HUAWEI-aaa] local-user client001 password irreversible-cipher Huawei@123
[*HUAWEI-aaa] local-user client001 level 3
[*HUAWEI-aaa] local-user client001 service-type ssh
[*HUAWEI-aaa] quit
[*HUAWEI] commit
```

4．用户通过STelnet登录设备

此处使用第三方软件PuTTY为例进行介绍。

通过PuTTY软件登录设备，输入设备的IP地址，选择协议类型为SSH。如图2所示。

图 2-2 通过 PuTTY 软件用 password 认证方式连接 SSH 服务器示意图



单击“Open”，出现如下界面，输入用户名和密码，并按“Enter”键，至此已登录到SSH服务器。（以下显示信息仅为示意）

```
login as: client001
Sent username "client001"
client001@10.137.217.203's password:

Warning: The initial password poses security risks.
The password needs to be changed. Change now? [Y/N]: n

Info: The max number of VTY users is 21, the number of current VTY users online is 2, and
total number of terminal users online is 2.
      The current login time is 2012-08-04 20:09:11+00:00.
      First login successfully.
<HUAWEI>
```

2.2.1.2 设备命名配置

为便于一级分行数据中心网络实施和分行网络运维管理，本次项目遵循网络设备命名统一规范，设备命名规则将采用字母与数字结合的方法，具体规则为：字段1_字段2_字段3_nn。

根据本次一级分行数据中心网络建设项目实施内容及目标，各字段详细命名含义如下：

字段1	字段1用于标识设备安装地点，对一级分行数据中心为： **一级分行地名缩写+当地地名缩写+行级** 其中： 1. 行级 数据中心：0 一级分行：1 二级分行：2 三级支行：3 保 留：4 网 点：5 下挂ATM：6 以“安徽合肥长江路支行”为例，可以标识为AHCJL3
字段2	字段2用于标识功能区，根据一级分行数据中心的整体网络结构，定义为： 1. 核心区(CORE)：CO 2. 开放平台区：OP 3. 开发测试区：DT 4. 运管区：OM 5. 本地用户接入区：LU 6. 外联区（Extranet）：EP 7. 城域广域网接入区：WN
字段3	字段3用于标识设备功能，根据一级分行数据中心的整体逻辑层次，定义为： 1. 核心层交换机：CS 2. 分布（汇聚）层交换机：DS 3. 接入层交换机：AS 4. 广域网接入路由器：AR 5. 防火墙：FW
nn	同一区域同一应用系统网络设备编号（01～99）

例如：XX分行开放平台区DS交换机1设备命名为：XX1_OP_DS_01

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] sysname XX1_OP_DS_01
[*HUAWEI] commit
```

2.2.1.3 设备管理配置

设备管理配置主要包括重启设备、指定设备下次启动时采用的启动文件等功能。

推荐配置指定设备下次启动时采用的启动文件。

- 重启设备。

  为了使指定的系统软件及相关文件生效，需要在配置完系统启动文件后，对设备进行重新启动。设备支持两种重启方式：立即重启和定时重启。

  立即重启配置示例：

  ```
  <HUAWEI> reboot
  ```

  定时重启配置示例：

  ```
  <HUAWEI> schedule reboot at 22:00
  Warning: The current configuration will be saved to the next startup saved-configuration
  file. Continue? [Y/N]:y
  Now saving the current configuration...
  Save the configuration successfully.
  Info: Reboot system at 22:00:00 2015/07/17 UTC (in 15 hours and 49 minutes).
  Confirm? [Y/N]:y
  ```

- 指定系统启动文件。

  指定系统启动文件包括指定系统启动用的系统软件和配置文件，这样可以保证设备在下一次启动时以指定的系统软件启动以及以指定的配置文件初始化配置。如果系统启动时还需要加载新的补丁，则还需指定补丁文件。

  配置下次启动使用的系统软件示例：

  ```
  <HUAWEI> startup system-software basicsoft.cc slave-board
  ```

可选参数**slave-board**只对采用双主控环境的交换机有效。

2.2.1.4 网管配置

网络管理是标准配置推荐的一个重要部分，目前应用比较普遍的是SNMP。SNMP包括SNMPv1，SNMPv2c和SNMPv3版本，其中SNMPv1和SNMPv2c是通过团体名进行认证，具有潜在安全风险，推荐使用SNMPv3版本。

下面以SNMPv3为例，配置设备使用SNMPv3与网管进行通信。

1. 使能SNMP Agent

   ```
   <HUAWEI> system-view
   [~HUAWEI] snmp-agent
   ```

2. 配置SNMP的版本为SNMPv3

   ```
   [*HUAWEI] snmp-agent sys-info version v3
   ```

   说明

   用户可以根据自己的需求配置对应的SNMP版本，但设备侧使用的SNMP协议版本必须和网管侧使用的SNMP版本保持一致，否则设备无法与网管连接。

3. 配置用户访问权限

   # 配置ACL，仅允许IP地址为192.168.1.10的网管访问设备。

   ```
   [*HUAWEI] acl 2001
   [*HUAWEI-acl4-basic-2001] rule permit source 192.168.1.10 0.0.0.0
   [*HUAWEI-acl4-basic-2001] quit
   ```

   # 配置MIB视图为alliso，访问的视图包含iso。

   ```
   [*HUAWEI] snmp-agent mib-view include alliso iso
   ```

   说明

   请根据实际需要配置用户的访问权限。

4. 配置SNMPv3用户组名为huawei_group，用户名为huawei_user，安全级别都为privacy，并应用访问控制

```
[*HUAWEI] snmp-agent group v3 huawei_group privacy write-view alliso acl 2001
[*HUAWEI] snmp-agent usm-user v3 huawei_user group huawei_group
[*HUAWEI] snmp-agent usm-user v3 huawei_user authentication-mode sha
Please configure the authentication password (8-255)
Enter Password:                 //输入认证密码
Confirm Password:               //确认认证密码
[*HUAWEI] snmp-agent usm-user v3 huawei_user privacy-mode aes256
Please configure the privacy password (8-255)
Enter Password:                 //输入加密密码
Confirm Password:               //确认加密密码
```

5. 配置告警主机

```
[*HUAWEI] snmp-agent target-host trap address udp-domain 192.168.1.10 params securityname
huawei_user v3 privacy
[*HUAWEI] commit
```

2.2.1.5 信息中心配置

运管区是网络的管理及维护中心，该区收集设备的运行状态信息。可通过配置信息中心将设备的日志信息发送至运管区的管理服务器，方便监控设备运行状态和定位故障。

步骤1 使能信息中心功能

```
<HUAWEI> system-view
[~HUAWEI] info-center enable
[*HUAWEI] commit
```

步骤2 配置向日志主机发送日志信息。

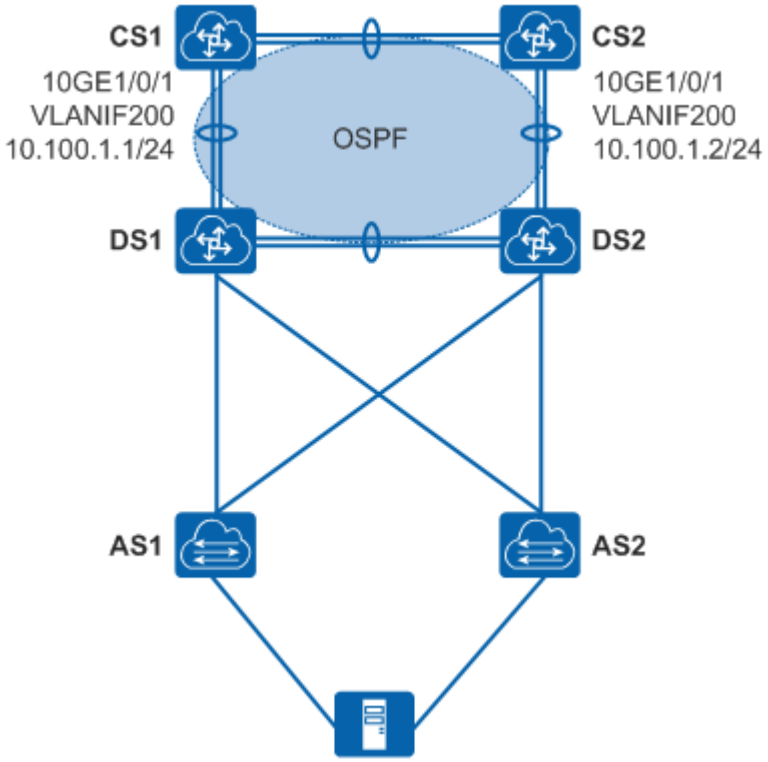
```
[~HUAWEI] info-center loghost 10.1.1.1
[*HUAWEI] commit
```

----结束

2.2.1.6 NTP 配置

在数据中心网络中设置NTP时钟源，为全网提供NTP时钟源服务。数据中心所有网络设备的时钟与此NTP时钟源同步。

将全网的NTP工作模式设置为单播服务器/客户端模式，配置CS1为主时间服务器，且CS1的时间已经同步到权威时钟（卫星定位系统）。配置CS2、DS和AS为客户端。为了保证安全性，建议使能NTP认证功能。



在CS1上配置NTP主时钟并启动NTP认证功能，使能CS1的NTP服务器功能。

```
<CS1> system-view
[~CS1] ntp refclock-master 1
[*CS1] ntp authentication enable
[*CS1] ntp authentication-keyid 42 authentication-mode hmac-sha256 Hello@123456
[*CS1] ntp trusted authentication-keyid 42
[*CS1] undo ntp server disable
[*CS1] commit
```

在DS1上指定CS1为NTP服务器。（其他的配置类似）

```
<DS1> system-view
[~DS1] ntp authentication enable
[*DS1] ntp authentication-keyid 42 authentication-mode hmac-sha256 Hello@123456
[*DS1] ntp trusted authentication-keyid 42
[*DS1] ntp unicast-server 10.100.1.1 authentication-keyid 42
[*DS1] commit
```

2.2.2 业务配置

2.2.2.1 接口配置

为保障网络的可靠性，物理接口配置遵守如下规则：

- 接口缺省使用自协商模式。

  例如10GE电接口，常见配置如下：

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface 10ge 1/0/1
  [~HUAWEI-10GE1/0/1] undo negotiation disable
  [*HUAWEI-10GE1/0/1] speed auto 100 1000 10000
  [*HUAWEI-10GE1/0/1] commit
  ```

- 没有启用的物理接口，必须处于shutdown状态。

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] shutdown
[*HUAWEI-10GE1/0/1] commit
```

- 接口启用链路故障检测功能。

  常见配置如下：

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface 10ge 1/0/1
  [~HUAWEI-10GE1/0/1] port crc-statistics trigger error-down
  [*HUAWEI-10GE1/0/1] commit
  ```

- 用于设备互联的接口按照接口编号从大到小的顺序启用，用于连接用户终端的接口按照接口编号从小到大的顺序启用。

2.2.2.2 VLAN 配置

根据业务的不同划分几个相应的网络分区，每个网络分区又有若干种类的应用业务系统，每一类业务都包含了多种子业务系统，且每种子业务系统的业务特点、协议类型、服务质量要求（如延时、抖动等）、安全等级要求是不尽相同的。

为了实现上述的网络系统架构设计，需要进行VLAN划分。通过VLAN技术将不同种类的业务区分开来，可以更好地实现服务质量（QoS）。通过VLAN技术将不同安全级别的业务在逻辑上隔离开来，基于不同的VLAN和应用实现相应的安全策略控制，提高网络的安全性。

这里，选用基于端口划分VLAN的方式进行统一的VLAN分配。具体的VLAN划分依据和部署规范如下：

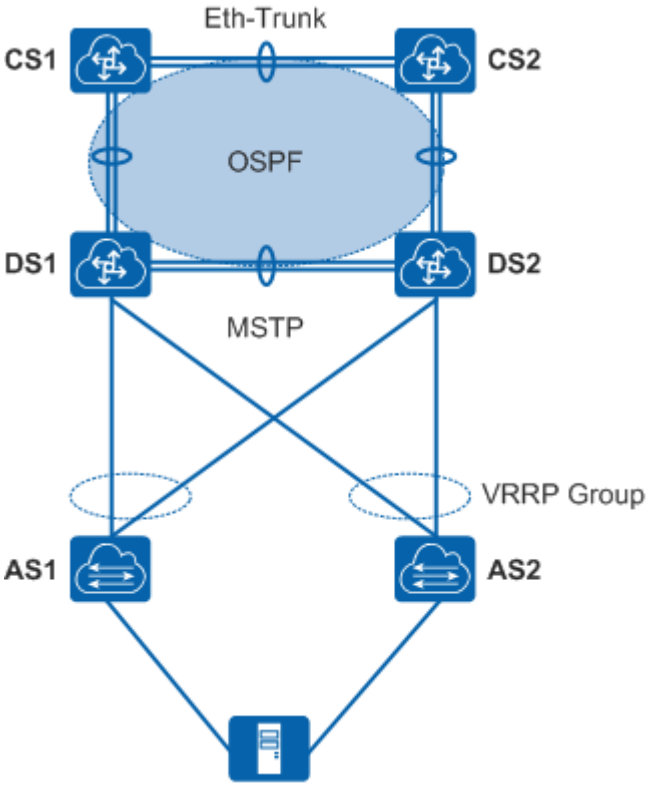
1. VLAN划分依据
   - 不同区域互联规划互连VLAN ，各个区域内的VLAN ID只是本区有效，禁止在区域之间存在跨区VLAN现象。
   - 每个功能分区都被分配了一定范围的VLAN，然后在网络分区里面根据不同级别的应用再进行分配，同时每个网络分区都预留了部分的VLAN，以满足将来不同应用系统的扩展使用。
   - 不同分区VLAN段不同，不同业务系统使用不同VLAN，同一业务系统服务器在同一VLAN中，按照从小到大的方式使用，城域和辖内广域用户接入VLAN复用本地用户接入VLAN。
2. VLAN部署规范
   - 同一个功能区，AS和DS上配置该区域的所有用户VLAN。该区内部的业务VLAN在AS-DS、DS-DS之间的Trunk链路上都允许通过。
   - Trunk链路不能采用允许所有VLAN通过的方式。
   - 所有Trunk链路不允许VLAN 1通过。

VLAN分配总体规划如下表所示：

表 2-1 VLAN 分配总体规划表

序号	功能	VLAN ID	备注
1	开放平台区	200-399	—
2	开发测试区	400-499	—

序号	功能	VLAN ID	备注
3	运营区	500-599	—
4	本地用户接入区	850-949	城域和辖内广域用户复用
5	extranet外联区	650-699	—
6	网络设备互联VLAN	800-849	—
7	网络设备管理VLAN	600-649	—
8	备用预留	10-199、700-799、950-1049	—



将AS和服务器相连的链路配置为Access链路，将AS-DS、DS-DS之间的链路配置为Trunk链路。

VLAN配置要点如下（以AS1为例，其他类似）：

```
<AS1> system-view
[~AS1] vlan batch 200
[*AS1] interface ge 1/0/1
[*AS1-GE1/0/1] port default vlan 200
[*AS1-GE1/0/1] quit
[*AS1] interface 10ge 1/0/11
[*AS1-10GE1/0/11] port link-type trunk
[*AS1-10GE1/0/11] port trunk allow-pass vlan 200
[*AS1-10GE1/0/11] undo port trunk allow-pass vlan 1
[*AS1-10GE1/0/11] quit
```

```
[*AS1] interface 10ge 1/0/12
[*AS1-10GE1/0/12] port link-type trunk
[*AS1-10GE1/0/12] port trunk allow-pass vlan 200
[*AS1-10GE1/0/12] undo port trunk allow-pass vlan 1
[*AS1-10GE1/0/12] quit
[*AS1] commit
```

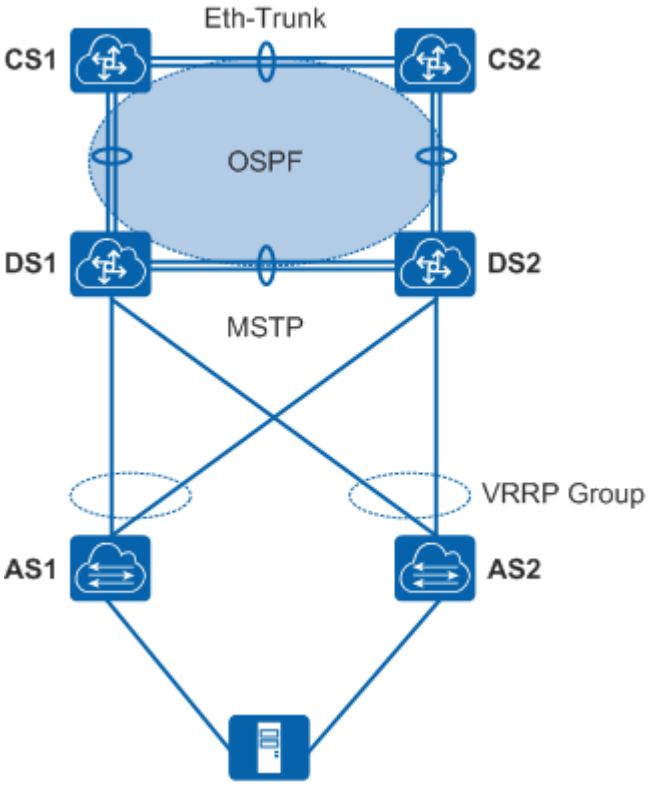
2.2.2.3 链路聚合配置

对于有高带宽、高可靠性需求的链路，需要使用链路聚合。

在CS-CS、CS-DS、DS-DS、DS-防火墙、防火墙心跳、AS-DS、AS-服务器均可采用链路聚合技术，保证高带宽高可靠性。

链路聚合部署技术要求：

- 链路聚合成员端口要求部署在不同的单板，以提升单板故障情况下的链路可靠性。
- 链路聚合使用手工负载分担模式，聚合端口速率一致。
- 链路聚合成员端口工作模式采用自协商模式。（如果自协商无法成功，则采用强制模式，同时启用DLDP）



链路聚合配置要点如下（以DS-DS为例，其他类似）：

```
<DS1> system-view
[~DS1] vlan batch 200
[*DS1] interface eth-trunk 1
[*DS1-Eth-Trunk1] trunkport 10ge 1/0/3
[*DS1-Eth-Trunk1] trunkport 10ge 2/0/3
[*DS1-Eth-Trunk1] port link-type trunk
[*DS1-Eth-Trunk1] port trunk allow-pass vlan 200
[*DS1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[*DS1-Eth-Trunk1] quit
[*DS1] commit
```

```
<DS2> system-view
[~DS2] vlan batch 200
[*DS2] interface eth-trunk 1
[*DS2-Eth-Trunk1] trunkport 10ge 1/0/3
[*DS2-Eth-Trunk1] trunkport 10ge 2/0/3
[*DS2-Eth-Trunk1] port link-type trunk
[*DS2-Eth-Trunk1] port trunk allow-pass vlan 200
[*DS2-Eth-Trunk1] undo port trunk allow-pass vlan 1
[*DS2-Eth-Trunk1] quit
[*DS2] commit
```

缺省情况下，Eth-Trunk的工作模式为手工负载分担模式。

2.2.2.4 IP 地址配置

分行数据中心新建局域网IP地址规划应遵循如下原则：

- 采用TCP/IP协议的IPv4版本；
- 局域网范围内的网间网互连地址，使用29位（255.255.255.248）的子网掩码，便于网络结构的灵活扩展部署，以及临时测试设备的插入，一个C类地址空间可以划分出32个局域网的互联网段；
- 规划方案要便于在总行和分行间实现路由汇总；
- 局域网网关地址使用该网段内的最大IP地址，当使用VRRP或类似技术时，虚拟地址和实际地址从该网段中的最大的IP地址（也就是从最后的可用地址）依次向前分配；
- 网络设备的管理地址（Loopback0）采用32位（255.255.255.255）的子网掩码，作为相关路由协议（OSPF）的ID标识；所有网络设备的管理地址按设备网络层次从同一网段依次连续分配；
- 根据各功能区和网络分区进行IP地址分配，各功能区汇聚设备下行口开始（包括分布层设备互连）为同一分区IP地址规划，核心交换机互连各区接口为核心交换区IP地址规划，广域DS交换机各广域设备接入为城域/广域IP地址规划。

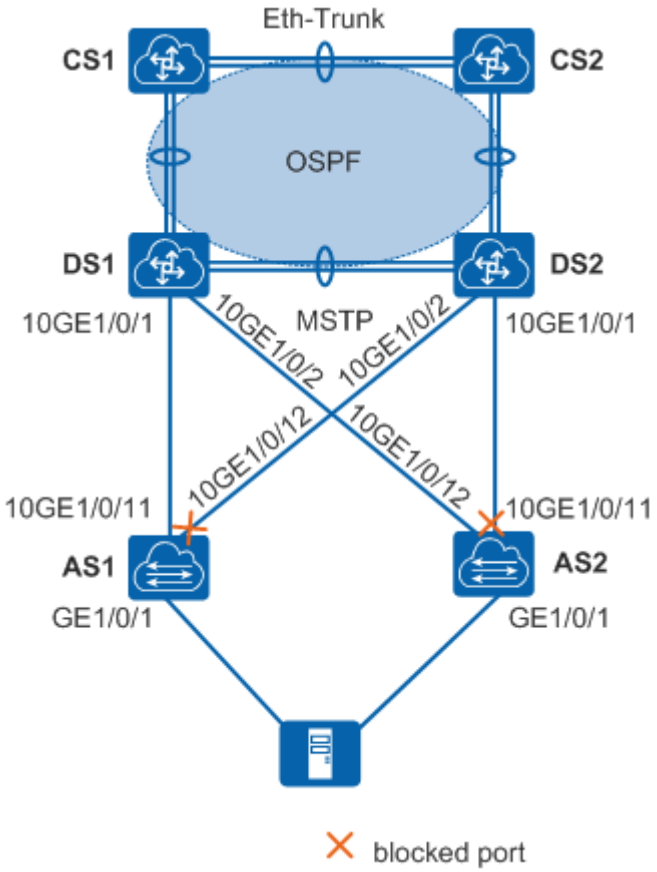
常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] interface vlanif 201
[*HUAWEI-Vlanif201] ip address 10.1.0.1 255.255.255.0
```

2.2.2.5 STP 配置

破环协议在二层网络中尤为重要，关于STP设计推荐采用STP和MSTP协议进行破环。

这里采用MSTP的配置为例，在满足组网业务需求、可靠性需求的前提下，尽可能简化配置，达到简化部署和维护简单的目的。



以数据中心某功能分区为例：

设备角色	MSTP全局配置	MSTP端口配置建议
DS1	1.根桥（和默认VRRP主保持一致） 2.配置TC保护 3.配置根保护（在连接AS的端口上配置） 4.配置BPDU保护（只在配置了边缘端口的情况下才启用该功能）	1.DS-CS端口关闭MSTP功能。 2.如DS侧挂IP模式防火墙，DS和防火墙互联端口关闭MSTP功能。 3.如果有直连服务器的端口，设置为边缘端口。
DS2	1.备用根桥 2.配置TC保护 3.配置BPDU保护（只在配置了边缘端口的情况下才启用该功能）	1.DS-CS端口关闭MSTP功能。 2.如DS侧挂IP模式防火墙，DS和防火墙互联端口关闭MSTP功能。 3.如果有直连服务器的端口，设置为边缘端口。
AS	1.配置TC保护 2.配置BPDU保护	1.直连服务器等终端的端口，设置为边缘端口。

MSTP配置要点：

1. 配置DS和AS到域名为RG1的域内，创建实例MSTI1

   以DS1为例，其他相同。

```
<DS1> system-view
[~DS1] stp region-configuration
[~DS1-mst-region] region-name RG1
[*DS1-mst-region] instance 1 vlan 200
[*DS1-mst-region] quit
[*DS1] commit
```

2. 配置MSTI1的根桥为DS1，备份根桥为DS2

```
[~DS1] stp instance 1 root primary
[*DS1] commit
[~DS2] stp instance 1 root secondary
[*DS2] commit
```

3. 配置端口路径开销计算方法为华为计算方法，将实例MSTI1中要被阻塞端口的路径开销值配置大于缺省值

```
[~DS1] stp pathcost-standard legacy
[*DS1] commit
[~DS2] stp pathcost-standard legacy
[*DS2] commit
[~AS1] stp pathcost-standard legacy
[*AS1] interface 10ge 1/0/12
[*AS1-10GE1/0/12] stp instance 1 cost 20000
[*AS1-10GE1/0/12] quit
[*AS1] commit
[~AS2] stp pathcost-standard legacy
[*AS2] interface 10ge 1/0/11
[*AS2-10GE1/0/11] stp instance 1 cost 20000
[*AS2-10GE1/0/11] quit
[*AS2] commit
```

4. 使能MSTP，实现破除环路

   以DS1为例，其他相同。

```
[~DS1] stp enable
[*DS1] commit
```

5. 配置保护功能，将与服务器相连的端口设置为边缘端口

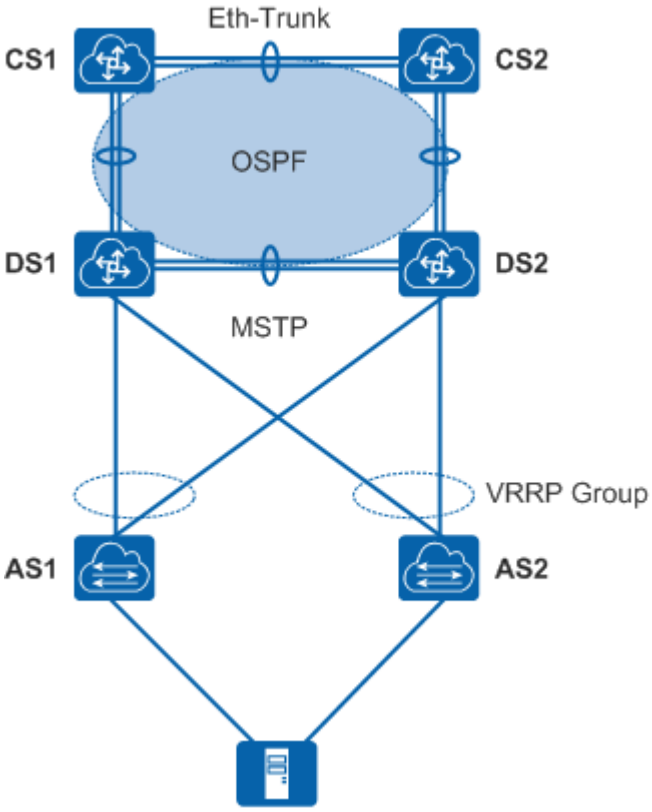
```
[~DS1] stp tc-protection
[*DS1] interface 10ge 1/0/1
[*DS1-10GE1/0/1] stp root-protection
[*DS1-10GE1/0/1] quit
[*DS1] interface 10ge 1/0/2
[*DS1-10GE1/0/2] stp root-protection
[*DS1-10GE1/0/2] quit
[*DS1] commit
[~DS2] stp tc-protection
[*DS2] commit
[~AS1] stp tc-protection
[*AS1] interface ge 1/0/1
[*AS1-GE1/0/1] stp edged-port enable
[*AS1-GE1/0/1] quit
[*AS1] stp bpdu-protection
[*AS1] commit
[~AS2] stp tc-protection
[*AS2] interface ge 1/0/1
[*AS2-GE1/0/1] stp edged-port enable
[*AS2-GE1/0/1] quit
[*AS2] stp bpdu-protection
[*AS2] commit
```

2.2.3 可靠性配置

2.2.3.1 VRRP 配置

通常情况下，网络内部的所有主机都设置一条相同的缺省路由，指向出口网关，实现主机与外部网络的通信。当出口网关发生故障时，主机与外部网络的通信就会中断。

VRRP将几台路由设备联合组成一台虚拟路由设备，将虚拟路由设备的IP地址作为用户的默认网关实现与外部网络通信。当网关设备发生故障时，VRRP机制能够选举新的网关设备承担数据流量，从而保障网络的可靠通信。



DS1和DS2交换机上分别创建不同的VLAN，对不同的VLANIF接口配置IP地址并部署VRRP协议，不同的VRRP虚拟地址分别作为AS交换机下不同服务器组的网关，DS1和DS2之间Eth-Trunk链路允许这些VLAN通过。在AS和DS设备之间配置MSTP破除环路，MSTP阻塞点配置在备份设备和下行交换机之间的链路上。同时，在DS和CS设备上配置OSPF实现三层互通。

VRRP配置要点：

1. 在DS1上配置VRRP备份组1
```
<DS1> system-view
[~DS1] interface vlanif 100
[~DS1-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
```
2. 在DS1上配置VRRP备份组1的优先级
```
[*DS1-Vlanif100] vrrp vrid 1 priority 120
```
3. 在DS1上配置VRRP备份组1的抢占时间为20s
```
[*DS1-Vlanif100] vrrp vrid 1 preempt timer delay 20
```
4. 在DS1上配置VRRP备份组1的VRRP通告报文发送间隔为2s
```
[*DS1-Vlanif100] vrrp vrid 1 timer advertise 2
[*DS1-Vlanif100] commit
[~DS1-Vlanif100] quit
```
5. 在DS2上配置VRRP备份组1

```
<DS2> system-view
[~DS2] interface vlanif 100
[~DS2-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
```

6. 在DS2上配置VRRP备份组1的VRRP通告报文发送间隔为2s

```
[*DS2-Vlanif100] vrrp vrid 1 timer advertise 2
[*DS2-Vlanif100] commit
[~DS2-Vlanif100] quit
```

7. 如需要配置VRRP负载分担，则在接口上配置两个或多个VRRP备份组，各备份组之间以VRID区分
   - 在DS1上配置VRRP备份组2及相应参数

```
[~DS1] interface vlanif 100
[~DS1-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[*DS1-Vlanif100] vrrp vrid 2 timer advertise 2
[*DS1-Vlanif100] commit
[~DS1-Vlanif100] quit
```

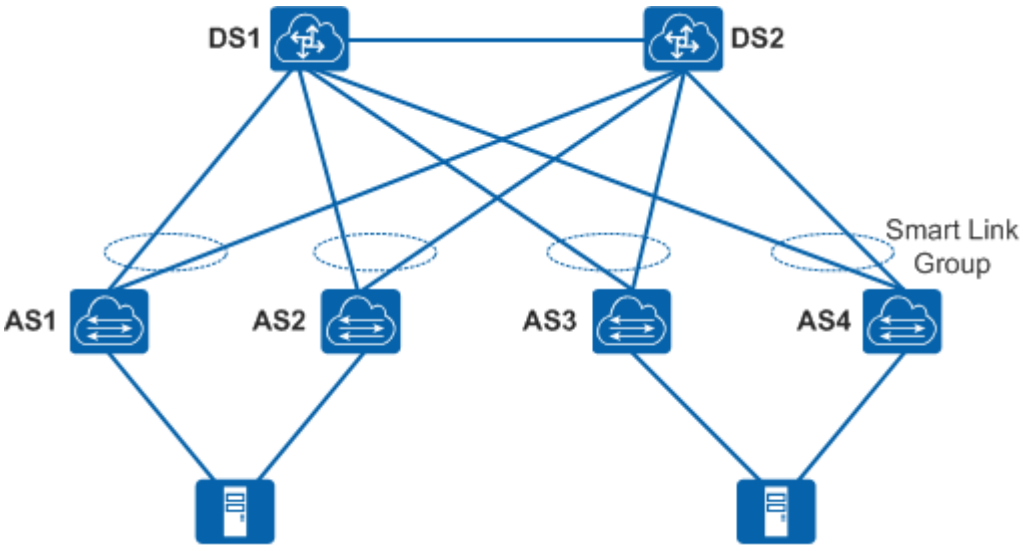
   - 在DS2上配置VRRP备份组2及相应参数

```
[~DS2] interface vlanif 100
[~DS2-Vlanif100] vrrp vrid 2 virtual-ip 10.1.1.112
[*DS2-Vlanif100] vrrp vrid 2 priority 120
[*DS2-Vlanif100] vrrp vrid 2 preempt timer delay 20
[*DS2-Vlanif100] vrrp vrid 2 timer advertise 2
[*DS2-Vlanif100] commit
[~DS2-Vlanif100] quit
```

2.2.3.2 Smart Link 配置

Smart Link针对双上行组网，实现主备链路冗余备份。

双上行的两个链路组成一个备份链路组。Smart Link组只有一个端口处于转发（Active）状态，另一个端口被阻塞，处于阻塞（Inactive）状态。当转发状态的端口链路故障时，Smart Link组将该端口阻塞，并将原阻塞的端口切换到转发状态。



针对一级分行数据中心功能分区，具体组网如上图所示，每台AS双上联到两台DS，两个上行链路（上行链路可以为链路聚合）加入到一个Smart Link备份组，整网组成一个无环的拓扑。

在计算拓扑方面，Smart Link并不需要对端设备在协议上的配合，AS能独立完成破环。但是，为了在拓扑变换后能快速刷新MAC表，需要对端设备处理AS发出的Flush报文，因该协议为私有协议，因此当DS和AS为不同厂家设备的情况下，DS会因为无法识别私有协议报文而不能及时刷新MAC。考虑到接入的服务器通常会不断发出各种数

据报文，该问题在实际应用中影响应该不大。（注：各厂家类似Smart Link技术的实现在MAC地址刷新机制方面存在差异，请以实际情况为准）

Smart Link配置要点：

1. 两个上行端口加入到一个Smart Link保护组
```
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] stp disable
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
[~HUAWEI] interface 10ge 1/0/2
[~HUAWEI-10GE1/0/2] stp disable
[*HUAWEI-10GE1/0/2] commit
[~HUAWEI-10GE1/0/2] quit
[~HUAWEI] smart-link group 1
[*HUAWEI-smlk-group1] port 10ge 1/0/1 master
[*HUAWEI-smlk-group1] port 10ge 1/0/2 slave
[*HUAWEI-smlk-group1] commit
```
2. 指定Smart Link需要保护的VLAN实例
```
[~HUAWEI] smart-link group 1
[*HUAWEI-smlk-group1] protected-vlan reference-instance 10
```
3. 配置Flush报文发送功能
```
[*HUAWEI-smlk-group1] flush send control-vlan 200 password sha 123
[*HUAWEI-smlk-group1] quit
[*HUAWEI] commit
```
4. 配置Flush报文接收功能

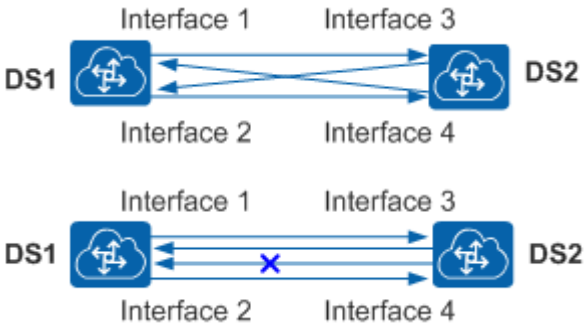
   如在AS1上配置Flush报文发送功能，则需要在DS1和DS2上配置Flush报文接收功能。
```
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] stp disable
[*HUAWEI-10GE1/0/1] smart-link flush receive control-vlan 200 password sha 123
[*HUAWEI-10GE1/0/1] commit
[~HUAWEI-10GE1/0/1] quit
[~HUAWEI] interface 10ge 1/0/2
[~HUAWEI-10GE1/0/2] smart-link flush receive control-vlan 200 password sha 123
[*HUAWEI-10GE1/0/2] commit
[~HUAWEI-10GE1/0/2] quit
```
5. 如需两台链路负载分担，则需要创建多个VLAN实例，并指定负载分担实例
```
[~HUAWEI] stp region-configuration
[~HUAWEI-mst-region] instance 10 vlan 201
[*HUAWEI-mst-region] commit
[~HUAWEI-mst-region] quit
[~HUAWEI] smart-link group 1
[~HUAWEI-smlk-group1] load-balance instance 10 slave
[*HUAWEI-smlk-group1] commit
```
6. 配置故障恢复后的回切时间，建议为60秒以上。
```
[~HUAWEI-smlk-group1] restore enable
[*HUAWEI-smlk-group1] timer wtr 120
[*HUAWEI-smlk-group1] commit
```

2.2.3.3 DLDP

DLDP用于检测单向链路，并在出现故障时关闭端口或者通知网络管理员。

实际网络中有时会出现光纤交叉连接、一条光纤未连接、一条光纤或双绞线中的一条线路断路的情况，此时链路两端的端口之一可以收到对端发送的链路层报文，但对端不能收到本端发送的报文，这种链路即为单向链路。在单向链路中，由于物理层处于连通状态，能正常工作，因而物理层的检测机制（如自动协商机制）无法发现设备间通信存在问题，从而导致流量的错误转发。

如下面两图所示，以光纤为例，单向链路分为两种类型：一种是光纤交叉连接，另一种是光纤未连接或一条光纤断路。



DLDP有两种工作模式：

- **普通模式**：系统只能识别一种类型的单向链路：光纤交叉连接。
- **加强模式**：系统能识别两种类型的单向链路：一种是光纤交叉连接，另一种是一条光纤未连接或一条光纤断路。该模式为默认模式。

DLDP的主要默认参数如下：

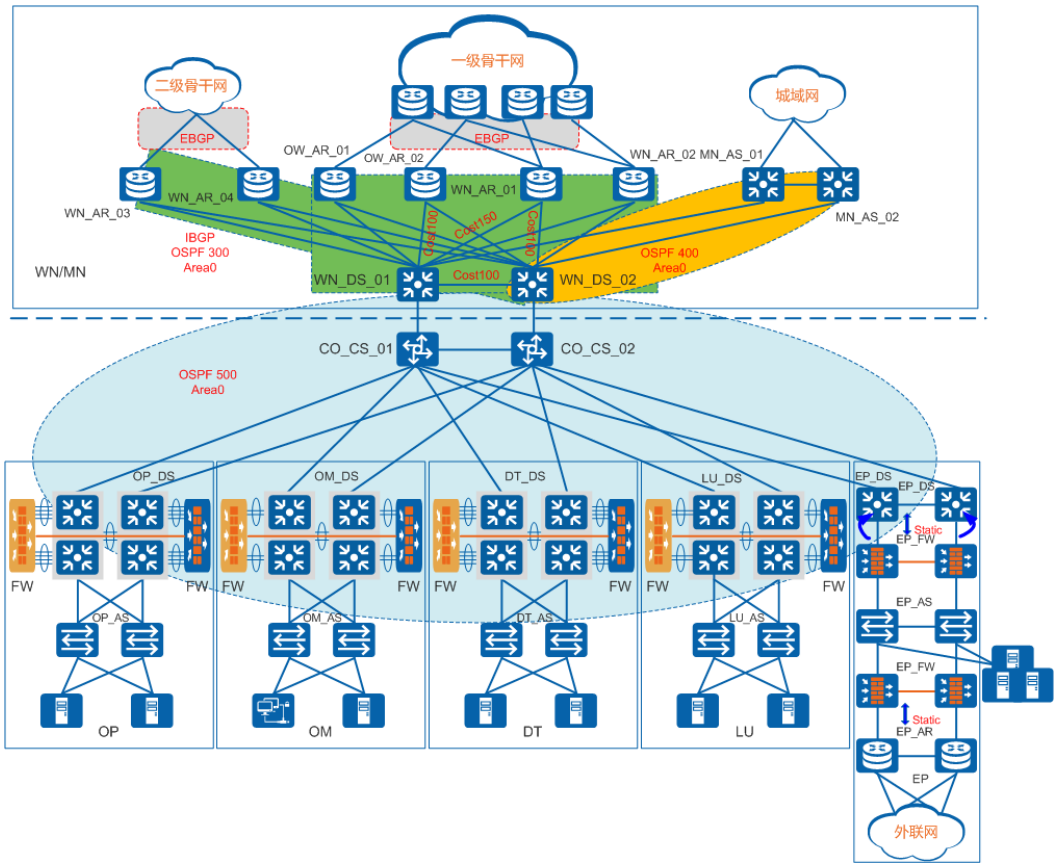
参数	缺省值
DLDP功能	关闭
DLDP工作模式	加强模式
发现单向链路后端口的堵塞模式	自动模式

在设备之间的互联端口使能DLDP，DLDP的建议配置：

1. 全局使能DLDP
```
<HUAWEI> system-view
[~HUAWEI] dldp enable
[*HUAWEI] commit
```
2. 端口使能DLDP
```
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] dldp enable
[*HUAWEI-10GE1/0/1] commit
```

2.2.4 路由配置

一级分行数据中心整体路由设计示意图如下：



整个数据中心规划可以分为局域网部分和广域城域区两部分。

整体路由设计：

广域城域区使用BGP与总行、二级分行对接交互业务路由，区域内部使用OSPF作为IGP。

局域网部分，除外联区DS－AR间使用静态路由外，核心区及其它分区整体使用OSPF进行业务路由承载。

EBGP：

一级分行规划为独立的自治域，使用私有的AS号。

IBGP：

一级分行的广域网区运行IBGP，OSPF300为广域网区WN_DS和WN_AR之间的IBGP提供联通性。

网络整体规划使用三个OSPF域，分别为OSPF300、OSPF400、OSPF500。

OSPF300：

OSPF300进程用于提供广域网区WN_DS和WN_AR之间的IBGP连通性，广域网区设备之间互联链路归属area0。

OSPF400：

OSPF400进程用于城域广域区和一级分行同城机构的路由互通，互联链路归属area0。

OSPF500：

OSPF500进程用于分行局域网区和WN_DS的路由互通，互联链路归属area0，承载一级分行业务。

Static:

外联区EP_AR和外部FW之间，外部FW和内部FW之间，内部FW和EP_DS之间通过静态路由互指互通。

路由协议优先级（preference/distance）设计：

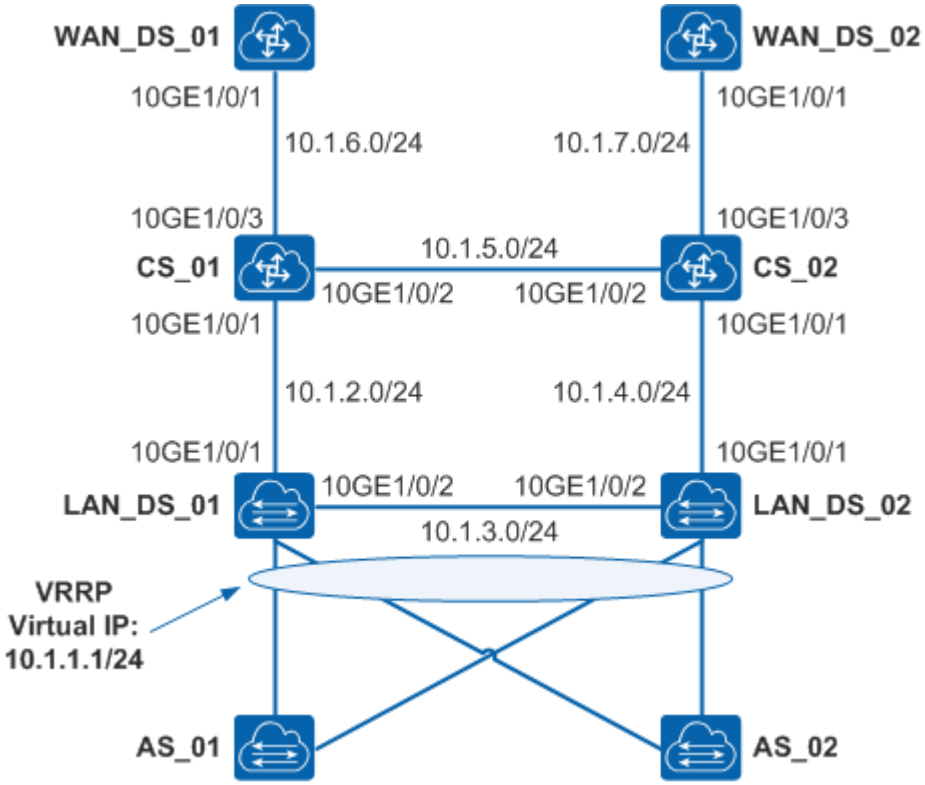
为保证不同厂家设备、不同路由协议间路由优选的一致性，对全网设备可能使用的路由协议的优先级统一规划如下：

协议类型	优先级
静态路由	5
OSPF	10
IBGP	170
EBGP	170
OSPF ASE	190
浮动静态路由	200

2.2.4.1 局域网路由配置

一、路由设计概述及基本功能配置

图 2-3 局域网路由规划示意图



如图所示，为某数据中心局域网部分，AS为接入设备，LAN_DS为局域网内汇聚设备，网关配置在汇聚设备上，LAN_DS下行配置VRRP，保证可靠性。CS设备为核心转发设备，WAN_DS设备是广域城域区域的汇聚设备，用于连接局域网核心设备和网络出口路由器。

本例整网采用OSPF协议保证域内连通性。

OSPF区域划分

整网采用OSPF路由协议，路由协议进程号为500。由于局域网内需运行OSPF的设备数量较少，所以OSPF500进程中仅使用Area0骨干区。需要使能OSPF的接口如下：

- LAN_DS下行VRRP的虚IP
- LAN_DS、WAN_DS、CS设备互联接口
- 用于Router ID的Loopback接口，注意该接口不需要参与OSPF计算，所以配置为Silent Interface。

OSPF Router ID规划

在每个OSPF进程中，路由器需要有唯一的Router ID来标识自己。在缺省情况下，路由器指定最大的Loopback IP地址作为自己的Router ID。为保证OSPF Router ID相对稳定，在OSPF进程的配置中，指定Loopback0接口的IP地址为Router ID。

OSPF基本功能配置

LAN_DS设备以LAN_DS_01为例：

```
<LAN_DS_01> system-view
[~LAN_DS_01] interface loopback 0
[*LAN_DS_01-LoopBack0] ip address 172.16.1.1 32
[*LAN_DS_01-LoopBack0] quit
[*LAN_DS_01] ospf 500 router-id 172.16.1.1
[*LAN_DS_01-ospf-500] silent-interface loopback 0
[*LAN_DS_01-ospf-500] area 0
[*LAN_DS_01-ospf-500-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[*LAN_DS_01-ospf-500-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[*LAN_DS_01-ospf-500-area-0.0.0.0] network 10.1.3.0 0.0.0.255
[*LAN_DS_01-ospf-500-area-0.0.0.0] commit
```

CS设备以CS_01为例：

```
<CS_01> system-view
[~CS_01] interface loopback 0
[*CS_01-LoopBack0] ip address 172.16.1.2 32
[*CS_01-LoopBack0] quit
[*CS_01] ospf 500 router-id 172.16.1.2
[*CS_01-ospf-500] silent-interface loopback 0
[*CS_01-ospf-500] area 0
[*CS_01-ospf-500-area-0.0.0.0] network 10.1.2.0 0.0.0.255
[*CS_01-ospf-500-area-0.0.0.0] network 10.1.5.0 0.0.0.255
[*CS_01-ospf-500-area-0.0.0.0] network 10.1.6.0 0.0.0.255
[*CS_01-ospf-500-area-0.0.0.0] commit
```

二、路由协议性能、可靠性和安全性设计及配置

以下配置均以CS_01为例，其他设备配置类似。

OSPF接口网络类型规划

缺省情况下，以太网中OSPF接口的网络类型是broadcast，但是本例中所有OSPF邻居均为两台互联，所以为了加快邻居建立和路由收敛，非Silent接口OSPF的网络类型统一配置为Point-to-Point。

```
<CS_01> system-view
[~CS_01] interface 10ge 1/0/1
[~CS_01-10GE1/0/1] undo portswitch
[*CS_01-10GE1/0/1] ospf network-type p2p
```

OSPF定时器规划

如果没有特殊需求，OSPF的定时器建议全部使用缺省值，本例即全部使用缺省值。如果需要修改定时器参数，需要保证相邻设备OSPF定时器参数一致。

例：修改OSPF发送Hello报文的时间间隔为20秒。

```
<CS_01> system-view
[~CS_01] interface 10ge 1/0/1
[~CS_01-10GE1/0/1] undo portswitch
[*CS_01-10GE1/0/1] ospf timer hello 20
```

OSPF Metric值

缺省情况下，OSPF接口Metric值是通过自动计算得出的，计算公式为：参考带宽/接口带宽。参考带宽可修改，缺省值为100Mbps。

本例中，考虑到方便后续维护管理，不使用自动计算模式，手动配置各链路的OSPF Metric值，规划如下：

表 2-2 OSPF Metric 值规划

序号	链路	Metric
1	CS-CS、DS-DS之间东西向链路	100
2	CS-DS之间南北向链路	100
3	DS业务接口	1000
4	CS/DS Loopback接口	0（无需配置）

例：配置CS-CS规划值为100：

```
<CS_01> system-view
[~CS_01] interface 10ge 1/0/1
[~CS_01-10GE1/0/1] undo portswitch
[*CS_01-10GE1/0/1] ospf cost 100
```

BFD for OSPF

BFD for OSPF就是将BFD和OSPF协议关联起来，BFD对链路故障的快速感应会通知OSPF协议，从而加快OSPF协议对于网络拓扑变化的响应。

通过在所有OSPF非silent接口与邻居建立动态BFD会话，可以实现OSPF邻居间链路故障（包括物理链路故障和上层转发故障）的毫秒级检测，并联动OSPF邻居状态快速切换，触发路由收敛计算。

所有BFD会话统一使用如下参数：

表 2-3 BFD for OSPF 参数规划

参数	参数说明	建议取值
min-rx-interval	期望从对端接收BFD报文的最小接收间隔。	1000ms
min-tx-interval	向对端发送BFD报文的最小发送间隔。	1000ms
detect-multiplier	本地检测倍数。	3

```
<CS_01> system-view
[~CS_01] bfd
[*CS_01-bfd] quit
[*CS_01] ospf 500
[*CS_01-ospf-500] bfd all-interfaces enable
[*CS_01-ospf-500] bfd all-interfaces min-tx-interval 1000 min-rx-interval 1000 detect-multiplier 3
```

OSPF智能定时器

网络不稳定时，可能会频繁进行路由计算，造成系统CPU消耗过大。尤其是在不稳定网络中，经常会产生和传播描述不稳定拓扑的LSA，频繁处理这样的LSA，不利于整个网络的快速稳定。OSPF智能定时器分别对路由计算、LSA的产生、LSA的接收进行控制，加速网络收敛。

OSPF智能定时器可以通过以下两种方式来加速网络收敛：

- 在频繁进行路由计算的网络中，OSPF智能定时器根据用户的配置和指数衰减技术动态调整两次路由计算的时间间隔，减少路由计算的次数，从而减少CPU的消耗，待网络拓扑稳定后再进行路由计算。
- 在不稳定网络中，当路由器由于拓扑的频繁变化需要产生或接收LSA时，OSPF智能定时器可以动态调整时间间隔，在时间间隔之内不产生LSA或对接收到的LSA不进行处理，从而减少整个网络无效LSA的产生和传播。

OSPF智能定时器统一使用如下参数：

表 2-4 OSPF 智能定时器规划

智能定时器	说明	建议取值
spf-schedule-interval	控制OSPF路由计算的时间间隔。	建议使用缺省值。即：SPF计算的最长间隔时间为10000毫秒、初始间隔时间为500毫秒、基数间隔时间为1000毫秒。
lsa-arrival-interval	控制OSPF LSA接收的时间间隔。	建议使用缺省值。即：接收LSA的最长间隔时间为1000毫秒、初始间隔时间为500毫秒、基数间隔时间为500毫秒。
lsa-originate-interval	控制OSPF LSA的更新时间间隔。	建议使用缺省值。即：更新LSA的最长间隔时间为5000毫秒、初始间隔时间为500毫秒、基数间隔时间为1000毫秒。

```
<CS_01> system-view
[~CS_01] ospf 500
[*CS_01-ospf-500] lsa-arrival-interval intelligent-timer 1000 500 500
[*CS_01-ospf-500] lsa-originate-interval intelligent-timer 5000 500 1000
[*CS_01-ospf-500] spf-schedule-interval intelligent-timer 10000 500 1000
```

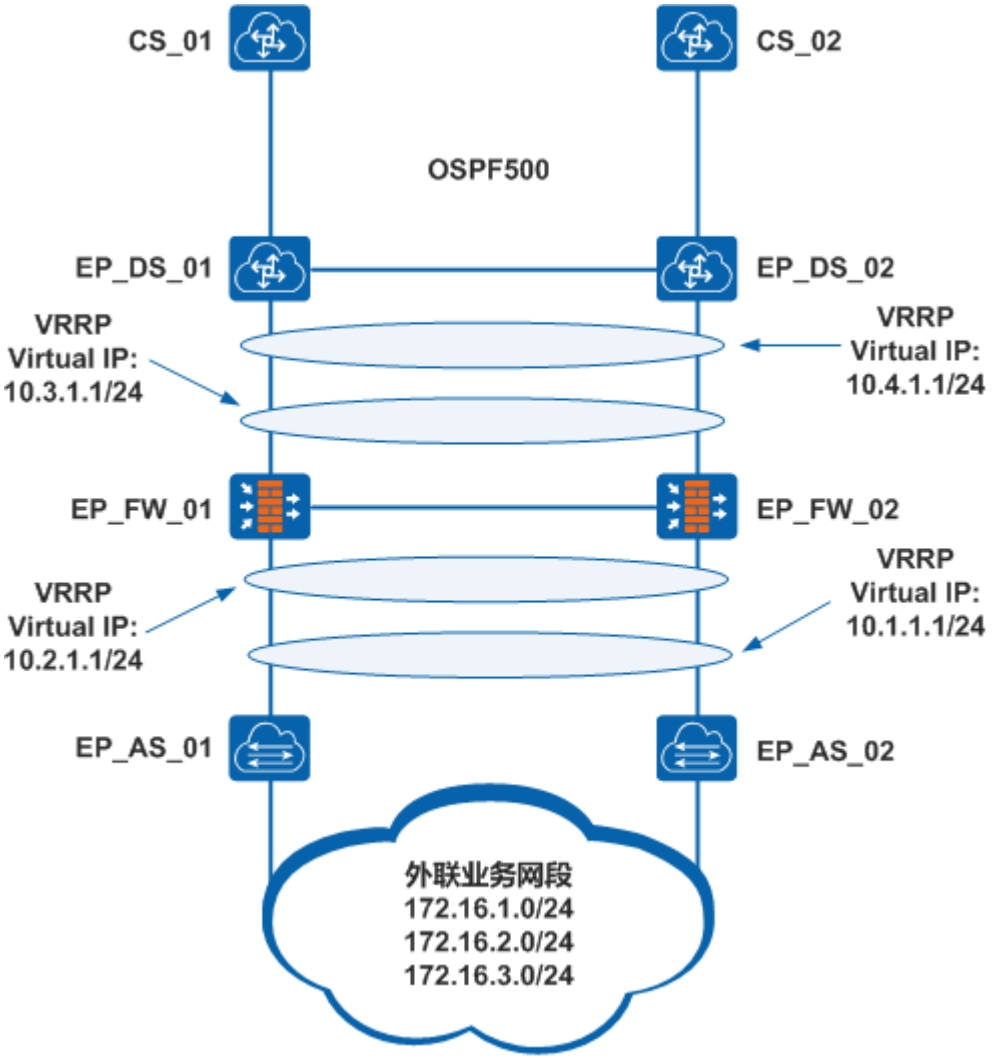
OSPF路由认证

为防止非法设备接入OSPF网络获取网络路由信息，可以部署OSPF路由认证的功能。本例中，统一部署OSPF区域认证，验证模式为MD5，具体密码不做说明，由客户自行指定。

```
<CS_01> system-view
[~CS_01] ospf 500
[*CS_01-ospf-500] area 0
[*CS_01-ospf-500-area-0.0.0.0] authentication-mode md5 1 cipher xxxxxxxx
```

2.2.4.2 外联区域路由配置

图 2-4 外联区域路由规划示意图



外联区域用于数据中心和其他业务区域的互联，由于需要对访问权限做比较精细的控制，外联区域采用防火墙串连的方式进行组网。

路由设计上，外联区域路由均采用静态明细路由+静态缺省路由的方式，和局域网区域进行路由隔离。下面给出各设备关键配置：

外联区域的汇聚设备（EP_DS）

外联区域的汇聚设备（EP_DS）设备上行和局域网的CS设备依旧采用OSPF进行互通，但是下行需要配置到所有外联业务网段的静态明细路由，下一跳均指向防火墙设备（EP_FW）的上行VRRP地址。OSPF500和VRRP相关配置见“局域网路由配置”。下面仅给出EP_DS_01静态明细路由配置，EP_DS_02配置和EP_DS_01相同。

```
<EP_DS_01> system-view
[~EP_DS_01] ip route-static 172.16.1.0 24 10.3.1.1
[*EP_DS_01] ip route-static 172.16.2.0 24 10.3.1.1
[*EP_DS_01] ip route-static 172.16.3.0 24 10.3.1.1
```

防火墙设备（EP_FW）

EP_FW上行采用静态缺省路由，下一跳指向EP_DS设备下行VRRP地址。下行配置到所有外联业务网段的静态明细路由，下一跳均指向外联区域接入设备（EP_AS）的上行VRRP地址。下面仅给出EP_FW_01静态路由配置，EP_FW_02配置和EP_FW_01相同。

```
<EP_FW_01> system-view
[~EP_FW_01] ip route-static 172.16.1.0 24 10.1.1.1
[*EP_FW_01] ip route-static 172.16.2.0 24 10.1.1.1
[*EP_FW_01] ip route-static 172.16.3.0 24 10.1.1.1
[*EP_FW_01] ip route-static 0.0.0.0 0 10.4.1.1
```

外联区域的接入设备（EP_AS）

EP_AS上行采用静态缺省路由，下一跳指向EP_FW的下行VRRP地址。下行配置到所有外联业务网段的静态明细路由，下一跳指向对端直连设备的接口地址。下面给出EP_AS_01的静态路由配置，对端直连设备的接口地址用“x.x.x.x”代替。

```
<EP_AS_01> system-view
[~EP_AS_01] ip route-static 172.16.1.0 24 x.x.x.x
[*EP_AS_01] ip route-static 172.16.2.0 24 x.x.x.x
[*EP_AS_01] ip route-static 172.16.3.0 24 x.x.x.x
[*EP_AS_01] ip route-static 0.0.0.0 0 10.2.1.1
```

2.2.4.3 广域城域部分路由配置

广域城域区使用BGP与总行、二级分行对接交互业务路由。

2.2.5 安全配置

2.2.5.1 ACL 防病毒配置

对于已知具有3、4层特征的病毒破坏，华为推荐在网络设备上采用定义ACL对这些数据流进行过滤，增加网络的安全性。推荐的常见防病毒配置如下：

```
[*HUAWEI]acl number 3000
[*HUAWEI-acl4-advence-3000]rule 0 deny tcp destination-port eq 445
[*HUAWEI-acl4-advence-3000]rule 1 deny udp destination-port eq 445
[*HUAWEI-acl4-advence-3000]rule 2 deny tcp destination-port eq 135
[*HUAWEI-acl4-advence-3000]rule 3 deny tcp destination-port eq 136
[*HUAWEI-acl4-advence-3000]rule 4 deny tcp destination-port eq 137
[*HUAWEI-acl4-advence-3000]rule 5 deny tcp destination-port eq 138
[*HUAWEI-acl4-advence-3000]rule 6 deny tcp destination-port eq 139
[*HUAWEI-acl4-advence-3000]rule 7 deny udp destination-port eq 135
[*HUAWEI-acl4-advence-3000]rule 8 deny udp destination-port eq 136
[*HUAWEI-acl4-advence-3000]rule 9 deny udp destination-port eq netbios-ns
[*HUAWEI-acl4-advence-3000]rule 10 deny udp destination-port eq netbios-dgm
[*HUAWEI-acl4-advence-3000]rule 11 deny udp destination-port eq netbios-ssn
[*HUAWEI-acl4-advence-3000]rule 12 deny udp destination-port eq 1434
[*HUAWEI-acl4-advence-3000]rule 13 deny udp destination-port eq 6667
[*HUAWEI-acl4-advence-3000]rule 14 deny udp destination-port eq 7626
[*HUAWEI-acl4-advence-3000]rule 15 deny udp destination-port eq 6789
[*HUAWEI-acl4-advence-3000]rule 16 deny udp destination-port eq 5800
[*HUAWEI-acl4-advence-3000]rule 17 deny udp destination-port eq 5900
[*HUAWEI-acl4-advence-3000]rule 18 deny tcp destination-port eq 5900
[*HUAWEI-acl4-advence-3000]rule 19 deny tcp destination-port eq 5800
[*HUAWEI-acl4-advence-3000]rule 20 deny tcp destination-port eq 1999
[*HUAWEI-acl4-advence-3000]rule 21 deny tcp destination-port eq 5554
[*HUAWEI-acl4-advence-3000]rule 22 deny tcp destination-port eq 9995
[*HUAWEI-acl4-advence-3000]rule 23 deny tcp destination-port eq 9996
[*HUAWEI-acl4-advence-3000]rule 24 deny udp destination-port eq 12345
[*HUAWEI-acl4-advence-3000]rule 25 deny udp destination-port eq 1057
[*HUAWEI-acl4-advence-3000]rule 26 deny udp destination-port eq 2616
```

2.2.5.2 广播风暴抑制配置

当网络中出现广播风暴时，会严重影响到网络使用。通过部署广播风暴抑制，可以降低广播风暴对网络的影响。

该功能在接近用户的设备上配置效果最好，因此在汇聚交换机下联端口和接入交换机的所有端口配置广播风暴抑制功能。

当报文的平均速率大于5000kbit/s时，进行风暴抑制，将超过的报文丢弃。

在汇聚交换机下行端口、汇聚交换机互联端口和接入交换机上联端口进行如下配置：

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] storm suppression broadcast cir 5000
```

2.2.5.3 MAC 地址漂移检测

MAC地址漂移即设备上一个接口学习到的MAC地址在同一VLAN中另一个接口上也被学习到，后学习到的MAC地址表项覆盖原来的表项。

配置MAC地址漂移检测功能可以检测到设备上所有的MAC地址是否发生了漂移。若发生漂移，设备会上报告警到网管系统，维护人员可根据告警信息定位故障。

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] mac-address flapping detection
```

2.2.5.4 MAC 刷新 ARP 功能

网络设备进行三层转发时，通过查找ARP表，命中表项后直接转发。某些时候，终端的逻辑位置发生了变化（比如服务器主备网卡发生切换），这个时候该IP对应的端口发生了变化。

MAC地址表项的出接口是通过报文触发刷新的，ARP表项的出接口是在老化时间到后通过老化探测进行刷新的。这样就可能会出现MAC表项和ARP表项出接口不一致的情况，即MAC地址表项的出接口已刷新，而ARP表项的出接口没有及时刷新的情况。

这个时候，就要开启MAC地址联动ARP功能，一旦MAC地址检测到端口发生变化，同时触发ARP表的刷新。

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] mac-address update arp enable
```

2.2.5.5 单端口防环路检测

当网络中某个端口下出现环路时，STP一般无法检测成功，需要开启单端口防环路检测功能。

在接入交换机下行端口上进行如下配置：

```
<HUAWEI> system-view
[~HUAWEI] interface ge 1/0/1
[~HUAWEI-GE1/0/1] loopback-detect enable
```

2.2.5.6 ARP 防攻击配置

- **配置ARP报文速率抑制**

如果网络中有主机通过向设备发送大量目标IP地址不能解析的IP报文来攻击设备，则会对网络设备造成很大的危害。

系统视图下配置ARP报文速率抑制功能：

```
<HUAWEI> system-view
[~HUAWEI] arp anti-attack rate-limit 200
```

VLAN视图下配置ARP报文速率抑制功能：

```
<HUAWEI> system-view
[~HUAWEI] vlan 201
[*HUAWEI-vlan201] arp anti-attack rate-limit 200
```

- **配置ARP报文源IP地址抑制**

  考虑到某些特定的用户有特别的需求，在对ARP报文进行源IP地址抑制时，可以针对该用户的IP地址配置不同于其他IP地址的ARP报文抑制速率。

说明

默认情况下，根据源IP地址配置的ARP报文限速值为30pps。当同一个源IP地址的ARP报文速率超过30pps时，如果是在网关请求同网段内很多个用户MAC地址的场景下，则需要增大设备的ARP报文源IP地址抑制速率值，否则超过30pps的ARP报文将被丢弃，会造成网关学习ARP很慢；如果是在ARP扫描攻击的场景下，则需要减小设备的ARP报文源IP地址抑制速率值。

配置根据任意源IP地址进行ARP报文限速的限速值：

```
<HUAWEI> system-view
[~HUAWEI] arp anti-attack rate-limit source-ip maximum 100
```

配置对指定IP地址10.1.1.1的ARP报文限速的限速值：

```
<HUAWEI> system-view
[~HUAWEI] arp anti-attack rate-limit source-ip 10.1.1.1 maximum 100
```

两种配置同时存在的情况下，当ARP报文源IP地址匹配限速指定的IP地址时，对该源IP地址的ARP报文限速值为后一步骤中配置的maximum值；否则为前一步骤中配置的maximum值。

- **配置ARP Miss消息源IP抑制**

  考虑到某些特定的用户有特别的需求，对于该用户的IP地址可以配置不同于其他IP地址的ARP Miss抑制速率。

  说明

  默认情况下，根据源IP地址配置的ARP Miss限速值为30pps。如果同一个源IP地址频繁触发ARP Miss消息且触发的ARP Miss消息速率超过30pps属于正常的情况，则需要增大ARP Miss消息的源IP地址抑制速率值。否则超过30pps的ARP Miss消息会触发ARP Miss消息源抑制，设备默认在5秒钟内丢弃匹配该源IP地址的所有ARP Miss报文，造成该源IP地址无法触发ARP学习。

  配置根据任意源IP地址进行ARP Miss消息限速的限速值：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp miss anti-attack rate-limit source-ip maximum 60
  ```

  配置对指定IP地址用户的ARP Miss消息进行限速的限速值：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp miss anti-attack rate-limit source-ip 10.0.0.1 maximum 60
  ```

  两种配置同时存在的情况下，当触发ARP Miss消息的IP报文的源IP地址匹配限速指定的IP地址时，对该源IP地址的IP报文触发的ARP Miss消息限速值为后一步骤中配置的maximum值；否则为前一步骤中配置的maximum值。

- **配置严格学习ARP表项**

  严格学习ARP表项指的是设备只学习自己发送的ARP请求报文的应答报文。

  配置全局ARP表项严格学习功能：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp learning strict
  ```

  配置接口的ARP表项严格学习功能：

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface vlanif 201
  [~HUAWEI-Vlanif201] arp learning strict force-enable
  ```

- **配置防止ARP地址欺骗**

  为了防止ARP地址欺骗攻击，可以使能ARP表项固化功能。

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp anti-attack entry-check fixed-mac enable
  ```

- **配置防止ARP中间人攻击（CE12800E和CE6880EI不支持该配置）**

  防止ARP中间人攻击，可以配置ARP报文检查功能，对接口或VLAN下收到的ARP报文和绑定表进行匹配检查，当报文的检查项和绑定表中的特征项一致时，转发该报文，否则丢弃报文。

  同时可以配置告警功能，当丢弃的报文数超过限制的阈值时，发出告警信息。

  说明

  本功能仅适用于DHCP用户场景，对于DHCP用户，设备使能DHCP Snooping功能后会自动生成绑定表。

  使能动态ARP检测功能（即对ARP报文进行绑定表匹配检查功能）：

  ```
  <HUAWEI> system-view
  [~HUAWEI] vlan 201
  [*HUAWEI-vlan201] arp anti-attack check user-bind enable
  ```

  配置对ARP报文进行绑定表匹配检查的检查项：

  ```
  [*HUAWEI-vlan201] arp anti-attack check user-bind check-item ip-address
  ```

  如果希望仅匹配绑定表某一项或某两项内容的特殊ARP报文也能够通过，则可以配置对ARP报文进行绑定表匹配检查时只检查某一项或某两项内容。

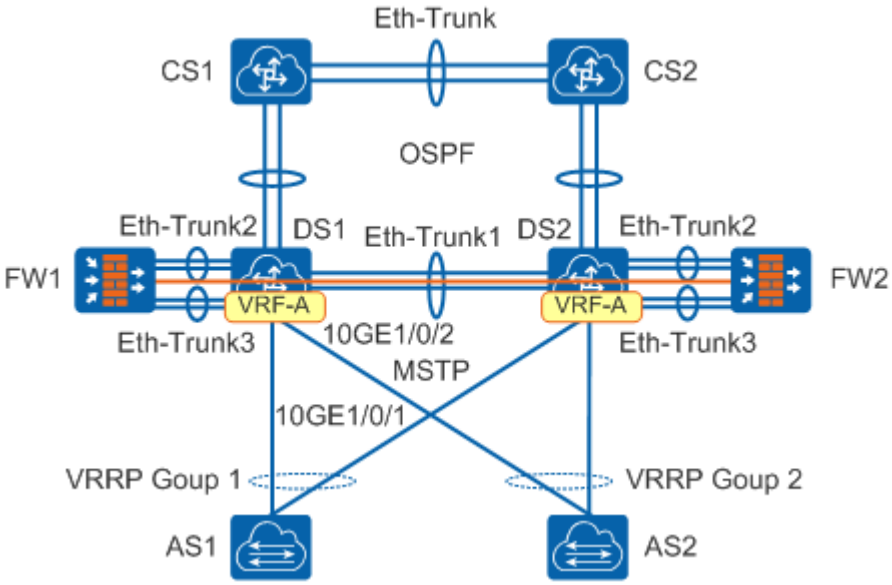
  说明

  指定ARP报文绑定表匹配检查项对配置了静态绑定表的用户不起作用，即设备仍然按照静态绑定表的内容对ARP报文进行绑定表匹配检查。

2.2.6 防火墙配置

开放平台区、开发测试区、运管区和分区出口采用旁挂方式部署防火墙，保证本分区和其它功能区的互访有安全控制。

分布层通过创建VRF隔离业务网段路由与公网路由，采用旁挂方式部署防火墙，保证不同区域互访的安全控制，两台防火墙进行双机热备份，保证高可靠性。



DS1和DS2交换机上分别创建不同的VLAN，对不同的VLANIF接口配置IP地址并部署VRRP协议，不同的VRRP虚拟地址分别作为AS交换机下不同服务器组的网关，DS1和DS2之间Eth-Trunk链路允许这些VLAN通过。在AS和DS设备之间配置MSTP破除环路，同时在DS和CS设备上配置OSPF实现三层互通。

DS设备上创建VPN实例VRF-A，将业务接口和连接防火墙下行的接口绑定到VRF-A，VRF-A的缺省路由指向防火墙的下行VRRP虚拟IP。DS设备配置至业务网段的静态路由，下一跳指向防火墙上行VRRP的虚拟IP。

防火墙与DS设备之间采用静态路由。防火墙配置双机热备，并根据应用的需要配置安全策略。

1. DS1上创建VLAN200、VLAN300和VLAN400。创建逻辑接口VLANIF200、VLANIF300和VLAN400。配置10GE1/0/1和Eth-Trunk1接口允许VLAN200通过，Eth-Trunk3接口允许VLAN300通过，Eth-Trunk2接口允许VLAN400通过。
2. DS1和DS2上进行MSTP和VRRP配置，DS1作为VRRP主设备。
3. DS1上创建VPN实例VRF-A，将VLANIF200和连接防火墙下行的VLANIF300绑定到VRF-A，VRF-A的缺省路由指向防火墙的下行VRRP虚拟IP。

   说明

   将接口绑定到VRF-A时，接口上的IP地址会被删除，需要重新配置IP地址。

```
[~HUAWEI] ip vpn-instance VRF-A
[*HUAWEI-vpn-instance-VRF-A] ipv4-family
[*HUAWEI-vpn-instance-VRF-A-af-ipv4] route-distinguisher 100:1
[*HUAWEI-vpn-instance-VRF-A-af-ipv4] vpn-target 111:1 both
[*HUAWEI-vpn-instance-VRF-A-af-ipv4] quit
[*HUAWEI-vpn-instance-VRF-A] quit
[*HUAWEI] interface vlanif 200
[*HUAWEI-Vlanif200] ip binding vpn-instance VRF-A
[*HUAWEI-Vlanif200] ip address 10.10.1.1 24
[*HUAWEI-Vlanif200] quit
[*HUAWEI] interface vlanif 300
[*HUAWEI-Vlanif300] ip binding vpn-instance VRF-A
[*HUAWEI-Vlanif300] ip address 10.10.2.1 24
[*HUAWEI-Vlanif300] quit
[*HUAWEI] ip route-static vpn-instance VRF-A 0.0.0.0 0.0.0.0 10.10.2.5
[*HUAWEI] commit
```

4. 配置DS1至业务网段的静态路由，下一跳指向防火墙上行VRRP的虚拟IP。DS1与CS设备间运行OSPF，并在OSPF中引入静态路由。

```
[~HUAWEI] ip route-static 10.10.1.0 255.255.255.0 10.10.3.5
[*HUAWEI] ospf 100
[*HUAWEI-ospf-100] area 0
[*HUAWEI-ospf-100-area-0.0.0.0] network 10.10.4.0 0.0.0.255
[*HUAWEI-ospf-100-area-0.0.0.0] network 10.10.5.0 0.0.0.255
[*HUAWEI-ospf-100-area-0.0.0.0] quit
[*HUAWEI-ospf-100] import-route static
[*HUAWEI-ospf-100] quit
[*HUAWEI] commit
```

5. FW设备上完成基础配置，包括配置设备名，接口，IP地址等。此处略。
6. 在FW1上配置安全区域。

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface eth-trunk 3
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface eth-trunk 2
[FW1-zone-untrust] quit
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface eth-trunk 1
[FW1-zone-dmz] quit
```

7. 在FW2上配置安全区域。

```
[FW2] firewall zone trust
[FW2-zone-trust] add interface eth-trunk 3
[FW2-zone-trust] quit
[FW2] firewall zone untrust
[FW2-zone-untrust] add interface eth-trunk 2
[FW2-zone-untrust] quit
[FW2] firewall zone dmz
[FW2-zone-dmz] add interface eth-trunk 1
[FW2-zone-dmz] quit
```

8. 在FW1上配置静态路由。内网访问外网的路由，缺省路由下一跳为交换机上连接防火墙上行接口的VLAN300的IP地址。外网访问内网的路由，目的地址为内网服务器网段，下一跳为交换机上连接防火墙下行接口的VLAN200的IP地址。

```
[FW1] ip route-static 0.0.0.0 0.0.0.0 10.10.3.1
[FW1] ip route-static 10.10.1.0 255.255.255.0 10.10.2.1
```

9. 在FW2上配置静态路由。

```
[FW2] ip route-static 0.0.0.0 0.0.0.0 10.10.3.1
[FW2] ip route-static 10.10.1.0 255.255.255.0 10.10.2.1
```

10. 在FW1上配置双机热备。

```
[FW1] interface eth-trunk 3
[FW1-Eth-Trunk3] vrrp vrid 1 virtual-ip 10.10.2.5 24 master
[FW1-Eth-Trunk3] quit
[FW1] interface eth-trunk 2
[FW1-Eth-Trunk2] vrrp vrid 2 virtual-ip 10.10.3.5 24 master
[FW1-Eth-Trunk2] quit
[FW1] hrp interface eth-trunk 1 remote 10.1.1.2
[FW1] firewall packet-filter default permit interzone local dmz
[FW1] hrp enable
```

11. 在FW2上配置双机热备。

```
[FW2] interface eth-trunk 3
[FW2-Eth-Trunk3] vrrp vrid 1 virtual-ip 10.10.2.5 24 slave
[FW2-Eth-Trunk3] quit
[FW2] interface eth-trunk 2
[FW2-Eth-Trunk2] vrrp vrid 2 virtual-ip 10.10.3.5 24 slave
[FW2-Eth-Trunk2] quit
[FW2] hrp interface eth-trunk 1 remote 10.1.1.1
[FW2] firewall packet-filter default permit interzone local dmz
[FW2] hrp enable
```

说明

双机热备功能配置完成后，主用设备的配置和会话会自动备份到备用设备上，因此以下功能只需在主用防火墙FW1上配置即可。

12. 配置安全策略和入侵防御。

说明

配置入侵防御功能前，需要保证入侵防御特征库已升级至最新的版本。

配置入侵防御功能时，通常使用默认存在的入侵防御配置文件default。

```
HRP_M[FW1] policy interzone trust untrust outbound
HRP_M[FW1-policy-interzone-trust-untrust-outbound] policy 1
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] policy source 10.10.1.0 mask 24
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] action permit
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] profile ips default
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] quit
HRP_M[FW1-policy-interzone-trust-untrust-outbound] quit
HRP_M[FW1] policy interzone trust untrust inbound
HRP_M[FW1-policy-interzone-trust-untrust-inbound] policy 1
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] policy destination 10.10.1.0 mask 24
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] policy service service-set ftp http
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] action permit
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] profile ips default
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] quit
HRP_M[FW1-policy-interzone-trust-untrust-inbound] quit
HRP_M[FW1] ips enable
```

13. 配置攻击防范。

说明

本举例中的攻击防范阈值仅供参考，实际配置时，请根据网络实际流量进行配置。

```
HRP_M[FW1] firewall defend syn-flood enable
HRP_M[FW1] firewall defend syn-flood zone untrust max-rate 20000
HRP_M[FW1] firewall defend udp-flood enable
HRP_M[FW1] firewall defend udp-flood zone untrust max-rate 1500
HRP_M[FW1] firewall defend icmp-flood enable
HRP_M[FW1] firewall defend icmp-flood zone untrust max-rate 20000
HRP_M[FW1] firewall blacklist enable
HRP_M[FW1] firewall defend ip-sweep enable
HRP_M[FW1] firewall defend ip-sweep max-rate 4000
HRP_M[FW1] firewall defend port-scan enable
HRP_M[FW1] firewall defend port-scan max-rate 4000
HRP_M[FW1] firewall defend ip-fragment enable
HRP_M[FW1] firewall defend ip-spoofing enable
```

14. 配置ASPF。此处以FTP协议为例，如果内网中还存在其他应用，就需要开启相应协议的ASPF功能。

```
HRP_M[FW1] firewall interzone trust untrust
HRP_M[FW1-interzone-trust-untrust] detect ftp
HRP_M[FW1-interzone-trust-untrust] quit
```

3 M-LAG 数据中心部署方案

3.1 概述

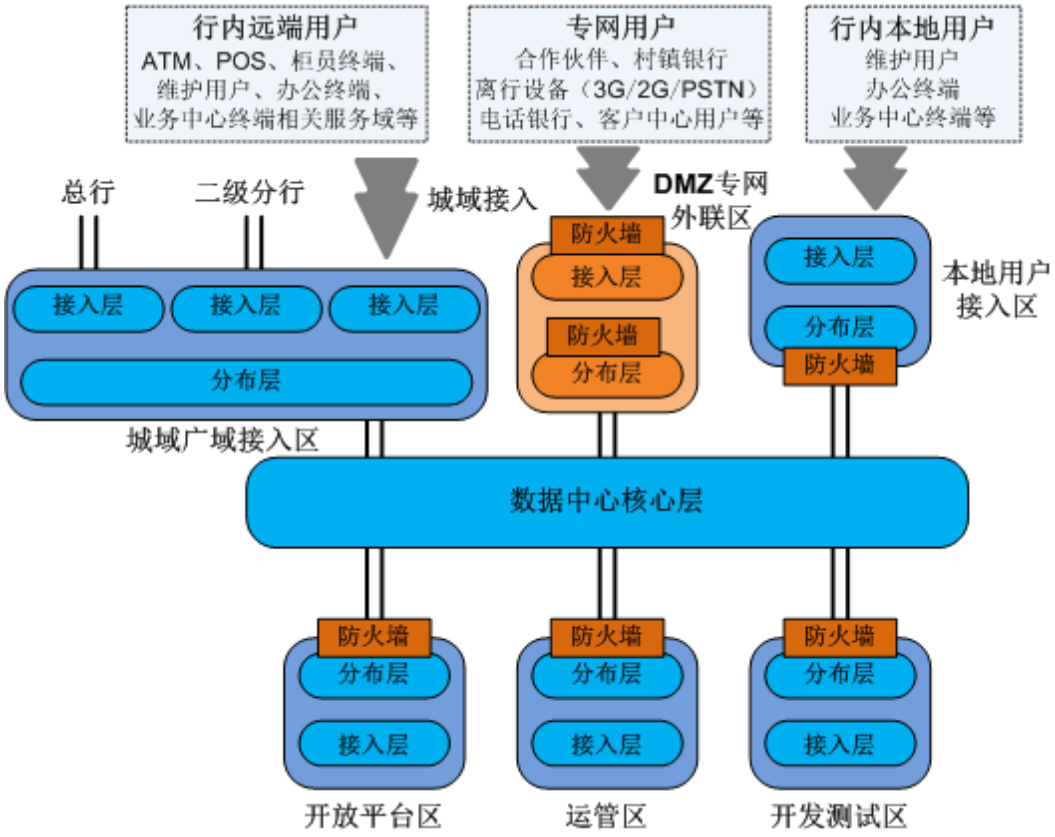
3.1.1 简介

本文档是银行一级分行数据中心的详细设计方案案例，对一级分行数据中心网络架构、IP地址和VLAN规划、路由设计、安全设计、网络可靠性设计、网管部署设计等进行了详细的描述。本文档可用于项目的实施参考。

3.1.2 典型组网

3.1.2.1 逻辑架构

根据功能分区规划，一级分行数据中心网络逻辑拓扑架构如下图：



各功能区介绍如下：

网络分区	分区功能和定位	接受访问
开放平台区：OP	已投产开放系统接入，通常包含直接动账、账目相关和非相关的业务。该区是最主要的业务区，满足生产、办公业务互访。	面向用户端和服务端。

网络分区	分区功能和定位	接受访问
运管区：OM	接入承载运行、监控和维护系统的服务器，用于对网络和系统进行管理及维护。	通常仅面向少数的授权维护用户。
开发测试区：DT	接入承载未投产业务系统的服务器，包括开发测试的主机和开放平台系统接入。	面向用户端和服务端。
城域广域接入区：WN/MN	实现一级分行上联总行与数据中心，下联二级分行与网点，以及与同城机构、分支网点的互联。从全行网络架构上分析，该区完成一级分行辖内区域的接入，包括一级分行局域网和辖内分支机构。	ATM、POS、柜员终端、维护用户、办公终端、业务中心终端等。
本地用户接入区：LU	满足各种类型用户终端接入。	本地维护用户、本地办公终端、本地业务中心终端。
DMZ专网外联区：EP	主要实现业务的外联，包括同行业的往来业务、重点客户的业务、中间代理业务等的平台互连，需要通过电信、联通等运营商提供的线路与合作伙伴互联。	合作伙伴、境外机构、离行设备（3G/2G/PSTN)、电话银行、客服中心用户。

一级分行数据中心网络在逻辑上形成三层结构：核心层、分布层和接入层。

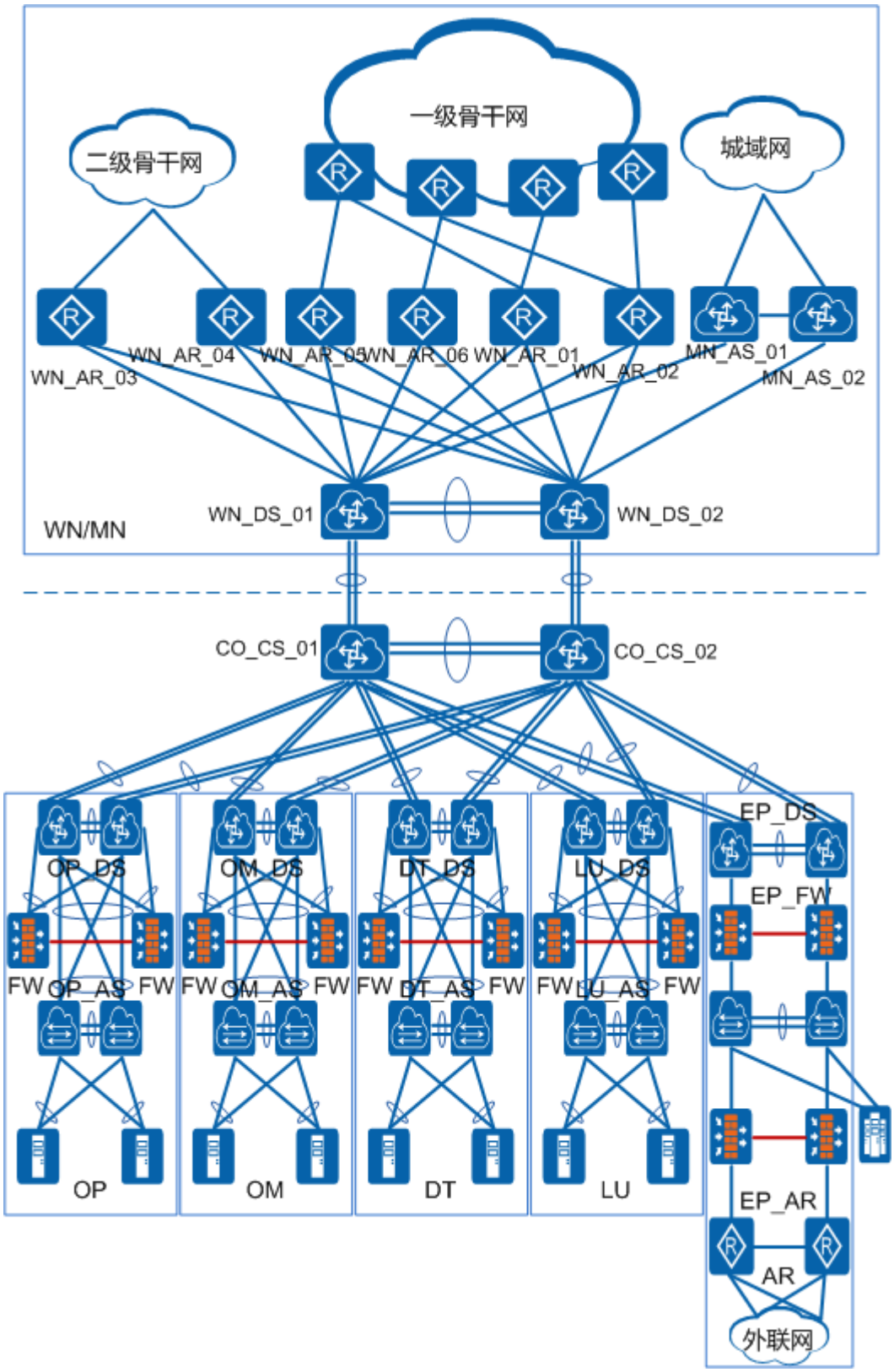
- 核心层：作为高速的三层交换骨干，核心层不直接连接终端和服务器，也不部署影响高速交换性能的ACL等功能。
- 分布层：作为二三层分界，同时作为功能分区边界。分布层与核心层进行三层连接，与接入层进行二层连接，主要完成以下的功能：
  - 作为功能区各类终端和服务器的统一网关；
  - 汇聚功能区内部路由；
  - 实现功能区内VLAN间的路由；
  - 实现功能区到核心层的路由策略；
  - 实施安全访问控制（ACL），实现功能区内部互访控制；
  - 部署防火墙，构建分区间互访安全控制策略。
- 接入层：连接对应功能分区的分布层，主要完成以下功能：
  - 接入层交换机（AS）：

    为服务器及其它终端提供二层网络接入；通过VLAN定义实现接入的隔离。
  - 接入层路由器（AR）：

提供广域、城域网络接入；作为广域网接入ASBR，进行路由控制。

3.1.2.2 物理架构

一级分行数据中心整体物理网络连接如下图：



核心交换区采用两台高性能的数据中心交换机作为整个数据中心网络的核心，核心交换机之间采用万兆以太网接口链路捆绑互联，共同建立起一个高可靠的高速交换核心区。

核心交换区与各分布层交换机的物理连接冗余备份，采用“口”字型连接，保证网络可靠性。核心交换区与各分布层交换机之间采用万兆（或千兆）以太网接口捆绑互联。

各个功能区分布层交换机采用两台高性能交换机作为分区汇聚，部署多级M-LAG代替传统的汇聚+接入的二层传统网络，在保证可靠性、提供链路利用率的同时扩展双归接入的网络规模。网关部署在汇聚层，支持应用服务器集群虚拟化，便于将来部署大二层、业务快速部署和迁移。

分区内部署防火墙实现各分区安全访问控制。防火墙旁挂在分布层交换机上，采用千兆以太网接口捆绑互联。两台防火墙采用主备冗余架构，当主防火墙出现故障时，系统可在较短的时间内自动切换到备用防火墙上面。如果主备防火墙都出现故障，业务从bypass链路通过，从而保障数据的不间断转发和业务的正常运行。

外联区两对防火墙分别与分布层交换机、接入层交换机、接入路由器通过“口”字型连接。

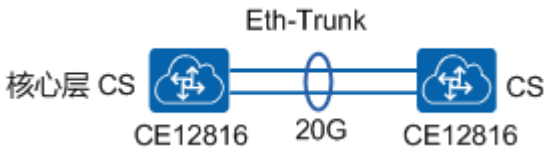
3.1.2.3 产品规划

核心层设备采用CE12816，分布层设备采用CE12808，接入层交换机采用CE6800，接入层路由器采用NE40E-X8，防火墙采用USG5500。

3.1.3 详细架构设计

3.1.3.1 核心交换区

一级分行数据中心核心交换区如下图所示：



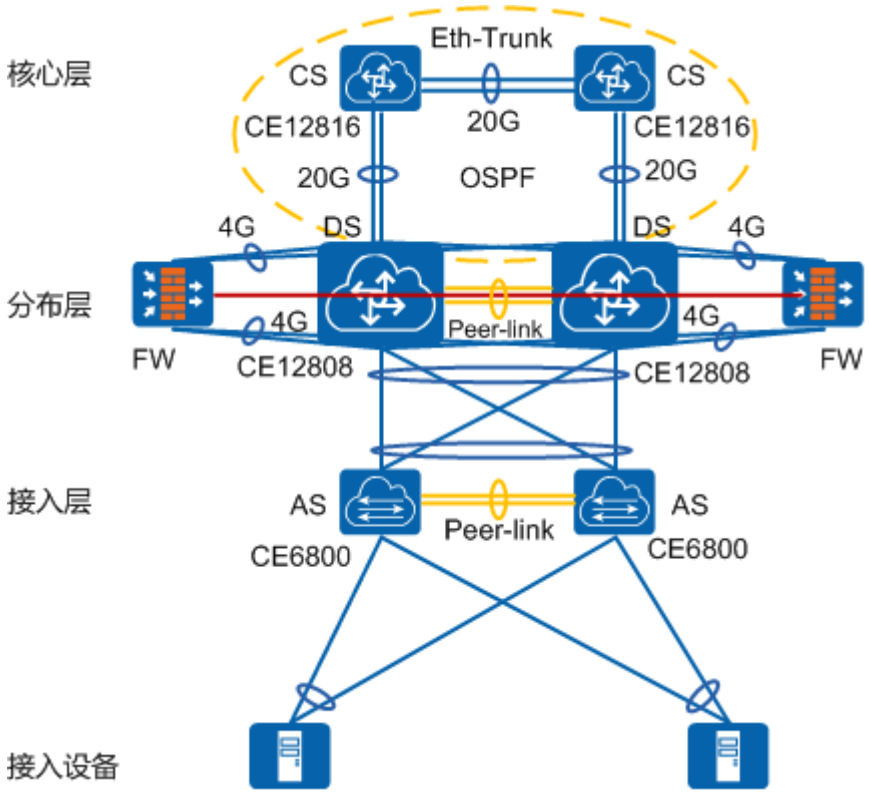
核心层是整个一级分行数据中心网络的核心，连接数据中心内部各个功能分区。核心层由两台高性能数据中心交换机CE12816组成，两台核心交换机之间通过2条10GE链路跨板捆绑，保障连接可靠性。

设备型号如下所示。

CS：华为CE12816

3.1.3.2 开放平台区

一级分行数据中心开放平台区结构如下图所示：



开放平台区分区分布层采用两级M-LAG互联，两台高性能数据中心交换机CE12808，上联采用2×10GE跨板捆绑，同时作为双活网关。核心层和分布层交换机使能OSPF，实现三层互通。接入层交换机CE6800通过M-LAG双活接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用4×GE跨板捆绑。

设备型号如下所示。

CS：华为CE12816

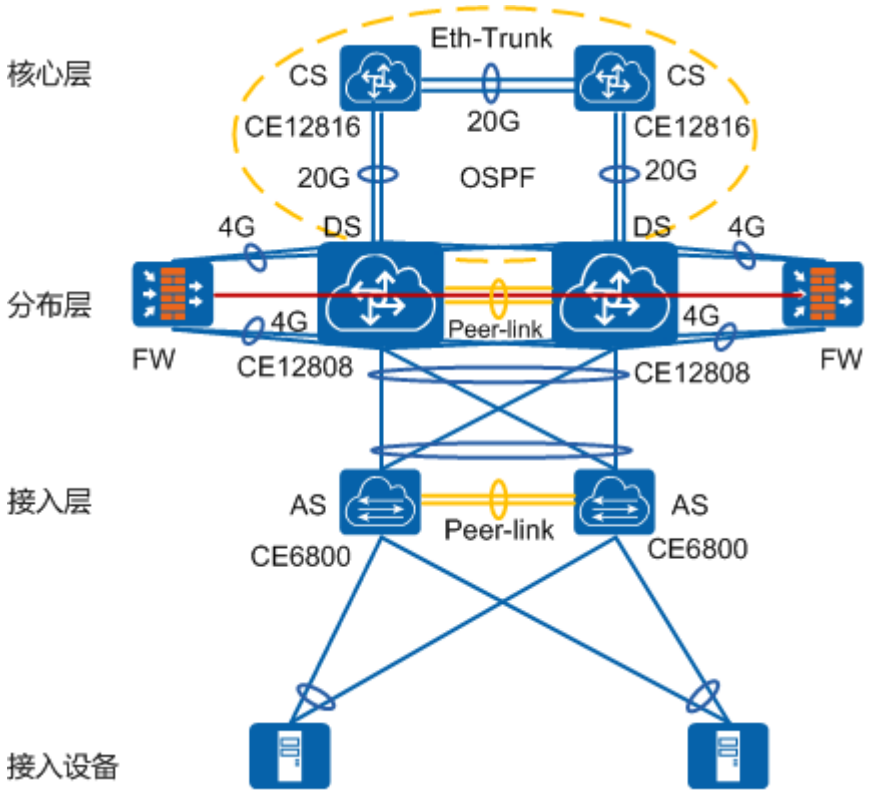
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

3.1.3.3 开发测试区

一级分行数据中心开发测试区结构如下图所示：



开发测试区分区分布层采用两级M-LAG互联，两台高性能数据中心交换机CE12808，上联采用2×10GE跨板捆绑，同时作为双活网关。核心层和分布层交换机使能OSPF，实现三层互通。接入层交换机CE6800通过M-LAG双活接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用4×GE跨板捆绑。

设备型号如下所示。

CS：华为CE12816

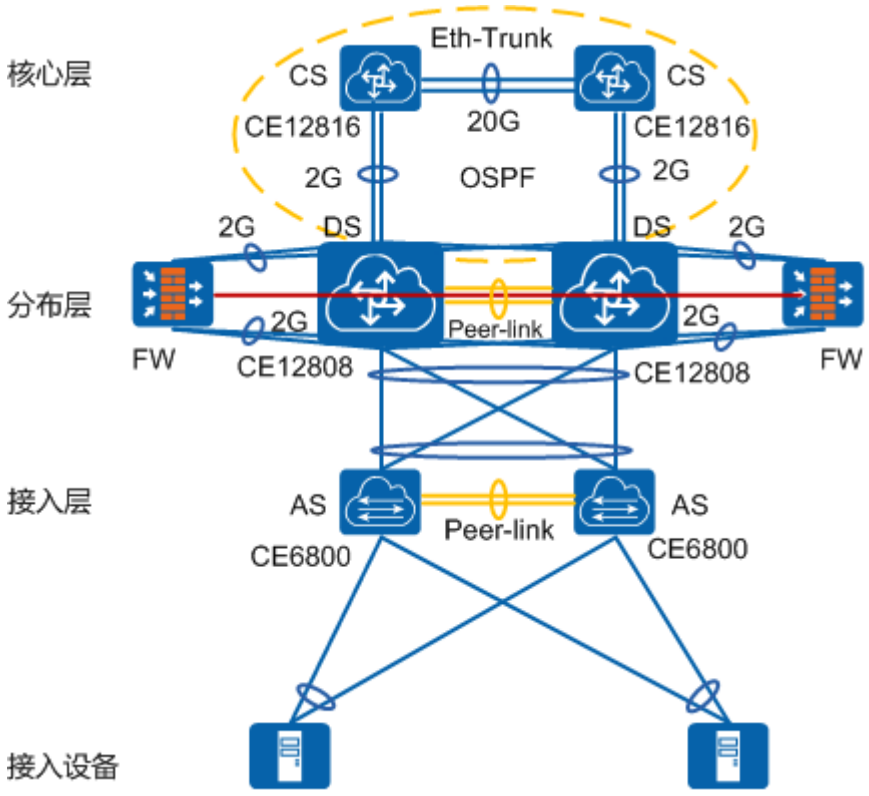
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

3.1.3.4 运管区

一级分行数据中心运管区结构如下图所示：



运管区是一级分行网络的管理及维护中心。该区收集被管理系统、设备的运行状态信息，监控网络、系统状态，下达管理指令，排除系统故障。

分布层采用两级M-LAG互联，两台高性能数据中心交换机CE12808，上联、互联均采用2×GE光口跨板捆绑，同时作为双活网关。核心层和分布层交换机使能OSPF，实现三层互通。接入层交换机CE6800通过GE口M-LAG双活接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用2×GE光口跨板捆绑。

运管区部署下面几类设备：

管理服务器：管理服务器基于SNMP协议获取网络、系统运行信息；接收网络、系统发送的网络、系统日志和告警信息。管理服务器将收集的管理信息进行汇总、处理，对数据中心网络/系统运行状况进行监控，生成网络/系统管理报表。

运管平台：一线值班人员通过一级分行数据中心的运行/管理操作台访问管理服务器；对发生故障的设备进行故障诊断和排查。

安全工具：为实现系统安全而提供的配套安全工具。例如Radius服务器，IDS服务器，防病毒系统服务器等。

设备型号如下所示。

CS：华为CE12816

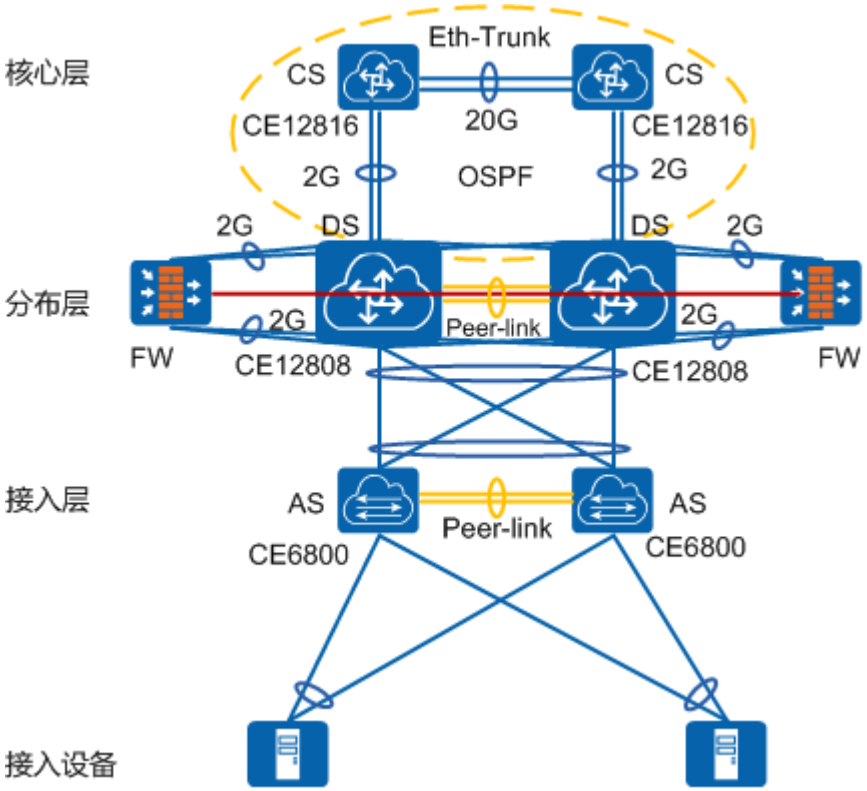
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

3.1.3.5 本地用户接入区

一级分行数据中心本地用户接入区结构如下图所示：



本地用户接入区建设的目标是满足各种类型用户终端互访需求。

分布层采用两级M-LAG互联，两台高性能数据中心交换机CE12808，上联、互联均采用2×GE光口跨板捆绑，同时作为双活网关。核心层和分布层交换机使能OSPF，实现三层互通。接入层交换机CE6800通过GE口M-LAG双活接入。

分区出口部署防火墙，保证本分区和其它功能区的互访有安全控制，采用旁挂方式，上下联均采用2×GE光口跨板捆绑。

设备型号如下所示。

CS：华为CE12816

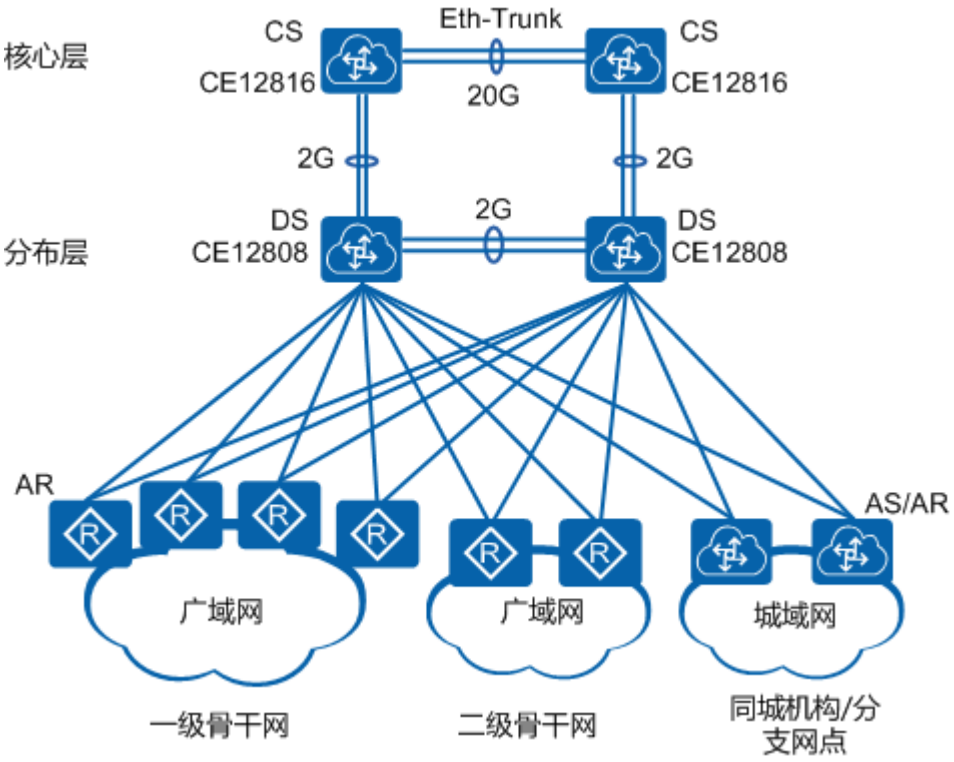
DS：华为CE12808

AS：华为CE6800

FW：华为USG5500

3.1.3.6 城域广域接入区

一级分行数据中心广域城域区结构如下图所示：



城域广域接入区实现与上联区、下联区路由器和同城接入设备的互联。

分区分布层采用两台高性能数据中心交换机CE12808，上联、互联均采用2×GE光口跨板捆绑，广域接入层采用双归接入，城域接入层采用“口”字型上联接入。

本区域仅用于广域、城域接入，不存在本地服务器，因此分布层不部署防火墙，接入的同城机构、分支网点或者二级分行部署UTM进行安全防护。

设备型号如下所示。

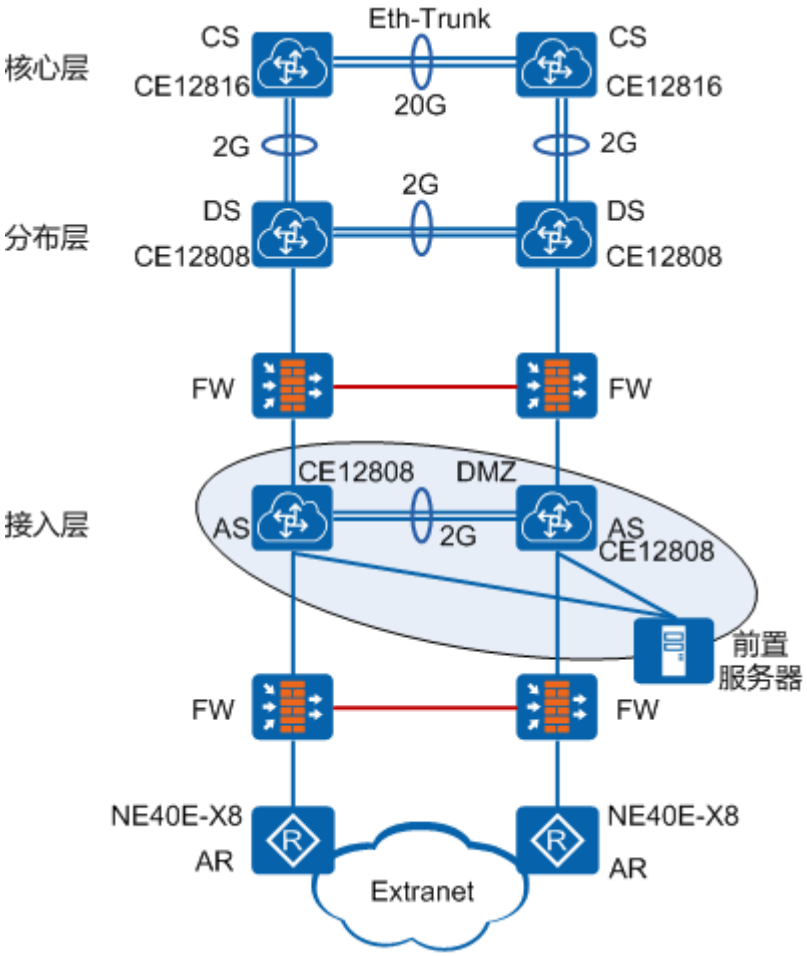
CS：华为CE12816

DS：华为CE12808

AR：华为NE40E-X8

3.1.3.7 外联区

一级分行数据中心外联区结构如下图所示：



外联区主要是实现与合作伙伴的网络连通性。为了提高该区域的安全性，避免外联单位直接访问本行的内网服务器区，采用两层异构防火墙的架构，把整个区域划分成外联区、DMZ区和内网区共3个等级不同的安全子区，3个安全子区的功能作用如下表所示：

网络分区	功能作用
外联区	提供与合作伙伴网络连接的通路，实现合作伙伴的专线接入和合作伙伴私网地址到DMZ私网地址的翻译
DMZ区	部署分行外联区业务前置机
内网区	一级分行数据中心网络系统

外联区的每一个层次在逻辑上提供不同的网络功能，安全级别由外向内逐一提高。下面针对该物理结构，由外到内分别作介绍：

角色	功能作用
外联路由器	用于第三方合作伙伴的接入，两台路由器分别接入不同运营商的线路，主线接入主用路由器，备线接入备用路由器，实现线路的冗余备份接入； 路由器与外层防火墙的互联端口启用虚拟路由器冗余备份协议（VRRP）。一般情况下，数据流始终先到主用路由器上，出现故障时，才切换到备用路由器，防止单机故障，实现设备的可靠性和冗余性； 如果接入的是ATM，MSTP等无法自动检测链路状态的线路类型时，需要手动在接口上配置OAM或BFD等链路故障检测协议，并要求对方也支持并启用该协议。
外层防火墙	用于外联区和DMZ区的逻辑分割和安全控制，防火墙应根据应用的需要配置安全策略。 两台防火墙工作在NAT模式下，采用HA的双机冗余架构，通常情况下一台防火墙工作在主用模式下，而另外一台防火墙工作在备用模式下，当主防火墙出现故障时，系统可在较短的时间内自动切换到备用防火墙上面，从而保障了数据的不间断转发和业务的正常运行。
接入层交换机	用于外联区前置服务器的接入，交换机之间采用双链路捆绑的方式连接，提高了设备的可靠性。 外联区接入层交换机可根据需要灵活增加。
内层防火墙	用于DMZ区和内网的逻辑分割和安全控制，防火墙应根据应用的需要配置安全策略。 两台防火墙工作在NAT模式下，采用HA的双机冗余架构，通常情况下一台防火墙工作在主用模式下，而另外一台防火墙工作在备用模式下，当主防火墙出现故障时，系统可在较短的时间内自动切换到备用防火墙上面，从而保障了数据的不间断转发和业务的正常运行。
分布层交换机	用于一级分行外联区与内部局域网之间的连接。 两台分布层交换机之间采用双链路捆绑的方式连接，提高了设备的可靠性。

设备型号如下所示。

CS：华为CE12816

DS：华为CE12808

AS：华为CE12808

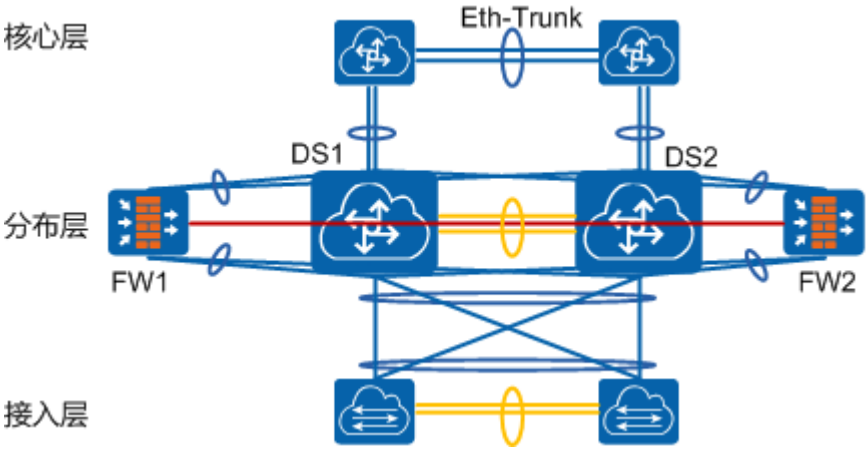
AR：华为NE40E-X8

FW：华为USG5500

3.1.3.8 防火墙部署设计

为了提升网络安全，一级分行数据中心网络中，在开放平台区（OP）、开发测试区（DT）、本地用户接入区（LU）和运管区（OM）部署防火墙，通过配置访问控制策略，实现功能分区之间的隔离和控制，对这些分区内部的服务器资源进行安全防护。

防火墙设备的部署采用旁挂方式。防火墙旁挂结构如下图所示：



- 防火墙采用HA方式部署，配置抢占模式。正常情况， 左侧FW1为主防火墙，右侧FW2为备防火墙。
- 两台防火墙之间心跳线采用两个独立端口直连。
- FW1和FW2防火墙旁挂方式跨接在2台分布层交换机上。
- 防火墙与分布层交换机采用链路聚合方式绑定接口互连。主防火墙FW1上连接口根据不同分区需求将4个或2个接口捆绑成一个Eth-Trunk1连接DS1交换机；下连接口根据不同分区需求将4个或2个接口捆绑成一个Eth-Trunk2连接DS1交换机。备防火墙FW2上连接口将4个或2个接口捆绑成一个Eth-Trunk1连接DS2交换机；下连接口将4个或2个接口捆绑成一个Eth-Trunk2连接DS2交换机。
- 防火墙监控Eth-Trunk1和Eth-Trunk2两个Eth-Trunk接口的物理状态，当两个接口中的任意一个发生故障时，防火墙进行主备切换，FW2变为主防火墙，FW1变为备份防火墙。
- 当主备防火墙都发生故障时，可以手动切换数据流经Bypass链路旁路防火墙。Bypass链路部署在汇聚交换机上下两个VRF之间，使用独立外接链路方式。
- 防火墙与DS交换机间采用静态路由＋VRRP方式进行对接。
- 防火墙配置trust和untrust区进行逻辑分割和安全控制，防火墙根据应用的需要配置安全策略。

  设备型号如下所示。

CS：华为CE12816
DS：华为CE12808
AS：华为CE6800
FW：华为USG5500

3.2 业务设计与配置

3.2.1 系统配置

3.2.1.1 登录设备配置

用户可以通过Console口、Telnet或STelnet方式登录设备，实现对设备的本地或远程维护。首次登录设备需要使用Console口登录。使用Telnet或者STelnet方式可以实现对设备的远程管理和维护。

下面分别介绍通过Console口登录设备和通过STelnet登录设备两种方式。

- 通过Console口登录设备

  在配置用户通过Console口登录设备之前，需完成以下任务：

  a. 准备好Console通信电缆。
  b. PC端准备好终端仿真软件。

  说明

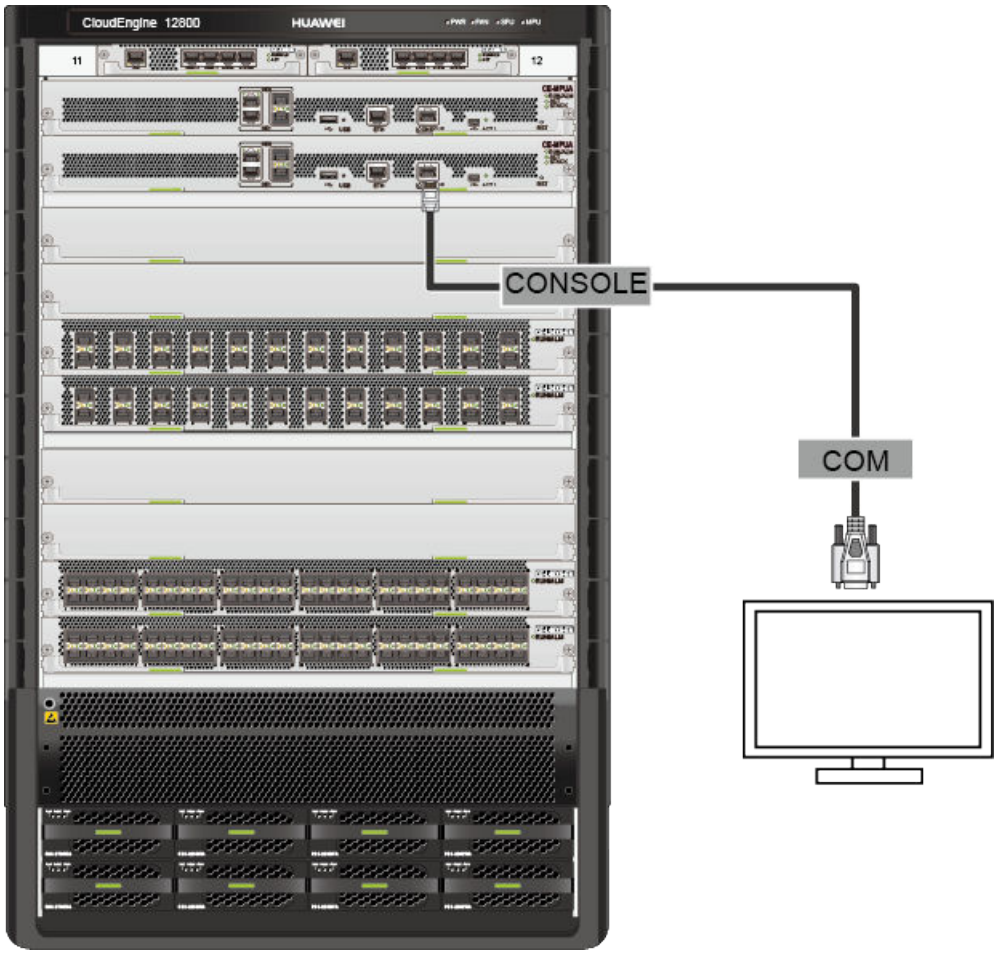
  如果PC使用系统自带的终端仿真软件（如Windows 2000系统的超级终端），则无需另行准备；如果系统不带终端仿真软件，请您准备第三方终端仿真软件，使用方法请参照该软件的使用指导或联机帮助。

  操作步骤：

  使用终端仿真软件通过Console口登录设备。

  a. 请使用产品随机附带的Console通信电缆的DB9（孔）插头插入PC机的9芯（针）串口插座，再将RJ-45插头端插入设备的Console口中，如图1所示。

图 3-1 通过 Console 口连接设备



b. 在PC上打开终端仿真软件，新建连接，设置连接的接口以及通信参数。

说明

因为PC端可能会存在多个连接接口，这里需要选择的是连接Console线缆的那个接口。一般情况下，选择的接口是COM1。

若修改了设备的串口通信参数值，需要在PC端更换通信参数值与设备的串口通信参数值一致后，重新连接。

c. 按Enter键，直到系统出现如下显示，提示用户输入密码。（AAA认证时，提示输入用户名和密码，以下显示信息仅为示意）

```
Login authentication


Password:
```

进入设备后，用户可以键入命令，对设备进行配置，需要帮助可以随时键入“?”。

- 通过STelnet登录设备

  在配置用户通过STelnet登录设备之前，需完成以下任务：

  a. 终端与设备之间路由可达。

  b. 终端上已安装SSH客户端软件。

  操作步骤：

  a. 配置STelnet服务器功能及参数

```
<HUAWEI> system-view
[~HUAWEI] rsa local-key-pair create
```

```
The key name will be: HUAWEI_Host
The range of public key size is (512 ~ 2048).
NOTE: Key pair generation will take a short while.
Input the bits in the modulus [default = 2048] : 2048  //从V200R001C00版本开始，仅支持2048bit，不需要用户输入。
[*HUAWEI] stelnet server enable
[*HUAWEI] commit
```

b. 配置SSH用户登录的用户界面

```
[~HUAWEI] user-interface vty 0 4
[~HUAWEI-ui-vty0-4] authentication-mode aaa
[*HUAWEI-ui-vty0-4] protocol inbound ssh
[*HUAWEI-ui-vty0-4] commit
[~HUAWEI-ui-vty0-4] quit
```

c. 配置SSH用户

配置SSH用户包括配置SSH用户的验证方式，设备支持的认证方式包括RSA、password、password-rsa、DSA、password-dsa、ECC、password-ecc和all。其中：

password-rsa认证需要同时满足password认证和RSA认证。

password-dsa认证需要同时满足password认证和DSA认证。

password-ecc认证需要同时满足password认证和ECC认证。

all认证是指password认证、RSA、DSA或ECC认证方式满足其中一种即可。

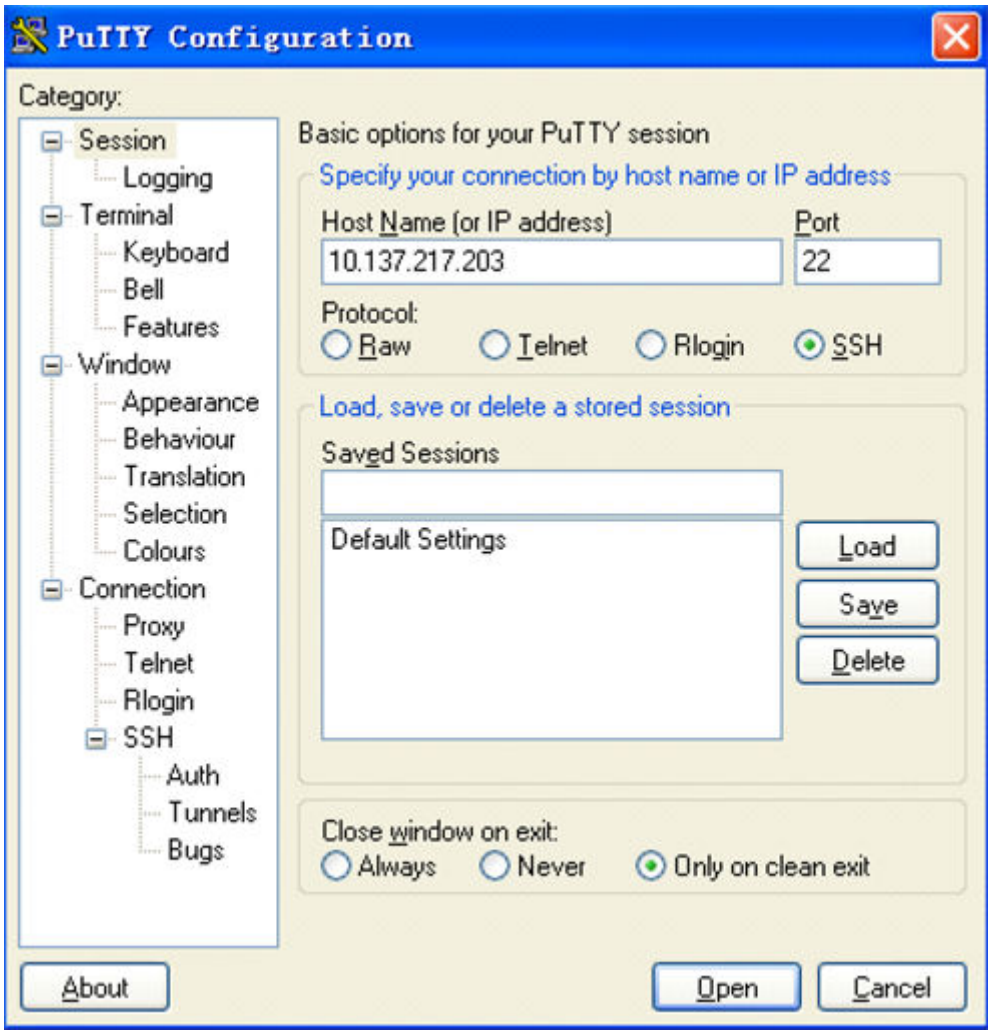
```
[~HUAWEI] ssh user client001
[*HUAWEI] ssh user client001 authentication-type password
[*HUAWEI] ssh user client001 service-type stelnet
[*HUAWEI] aaa
[*HUAWEI-aaa] local-user client001 password irreversible-cipher Huawei@123
[*HUAWEI-aaa] local-user client001 level 3
[*HUAWEI-aaa] local-user client001 service-type ssh
[*HUAWEI-aaa] quit
[*HUAWEI] commit
```

4．用户通过STelnet登录设备

此处使用第三方软件PuTTY为例进行介绍。

通过PuTTY软件登录设备，输入设备的IP地址，选择协议类型为SSH。如图2所示。

图 3-2 通过 PuTTY 软件用 password 认证方式连接 SSH 服务器示意图



单击“Open”，出现如下界面，输入用户名和密码，并按“Enter”键，至此已登录到SSH服务器。（以下显示信息仅为示意）

```
login as: client001
Sent username "client001"
client001@10.137.217.203's password:

Warning: The initial password poses security risks.
The password needs to be changed. Change now? [Y/N]: n

Info: The max number of VTY users is 21, the number of current VTY users online is 2, and
total number of terminal users online is 2.
      The current login time is 2012-08-04 20:09:11+00:00.
      First login successfully.
<HUAWEI>
```

3.2.1.2 设备命名配置

为便于一级分行数据中心网络实施和分行网络运维管理，本次项目遵循网络设备命名统一规范，设备命名规则将采用字母与数字结合的方法，具体规则为：字段1_字段2_字段3_nn。

根据本次一级分行数据中心网络建设项目实施内容及目标，各字段详细命名含义如下：

字段1	字段1用于标识设备安装地点，对一级分行数据中心为： **一级分行地名缩写+当地地名缩写+行级** 其中： 1. 行级 数据中心：0 一级分行：1 二级分行：2 三级支行：3 保 留：4 网 点：5 下挂ATM：6 以“安徽合肥长江路支行”为例，可以标识为AHCJL3
字段2	字段2用于标识功能区，根据一级分行数据中心的整体网络结构，定义为： 1. 核心区(CORE)：CO 2. 开放平台区：OP 3. 开发测试区：DT 4. 运管区：OM 5. 本地用户接入区：LU 6. 外联区（Extranet）：EP 7. 城域广域网接入区：WN
字段3	字段3用于标识设备功能，根据一级分行数据中心的整体逻辑层次，定义为： 1. 核心层交换机：CS 2. 分布（汇聚）层交换机：DS 3. 接入层交换机：AS 4. 广域网接入路由器：AR 5. 防火墙：FW
nn	同一区域同一应用系统网络设备编号（01～99）

例如：XX分行开放平台区DS交换机1设备命名为：XX1_OP_DS_01

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] sysname XX1_OP_DS_01
[*HUAWEI] commit
```

3.2.1.3 设备管理配置

设备管理配置主要包括重启设备、指定设备下次启动时采用的启动文件等功能。

推荐配置指定设备下次启动时采用的启动文件。

- 重启设备。

  为了使指定的系统软件及相关文件生效，需要在配置完系统启动文件后，对设备进行重新启动。设备支持两种重启方式：立即重启和定时重启。

  立即重启配置示例：

  ```
  <HUAWEI> reboot
  ```

  定时重启配置示例：

  ```
  <HUAWEI> schedule reboot at 22:00
  Warning: The current configuration will be saved to the next startup saved-configuration
  file. Continue? [Y/N]:y
  Now saving the current configuration...
  Save the configuration successfully.
  Info: Reboot system at 22:00:00 2015/07/17 UTC (in 15 hours and 49 minutes).
  Confirm? [Y/N]:y
  ```

- 指定系统启动文件。

  指定系统启动文件包括指定系统启动用的系统软件和配置文件，这样可以保证设备在下一次启动时以指定的系统软件启动以及以指定的配置文件初始化配置。如果系统启动时还需要加载新的补丁，则还需指定补丁文件。

  配置下次启动使用的系统软件示例：

  ```
  <HUAWEI> startup system-software basicsoft.cc slave-board
  ```

可选参数**slave-board**只对采用双主控环境的交换机有效。

3.2.1.4 网管配置

网络管理是标准配置推荐的一个重要部分，目前应用比较普遍的是SNMP。SNMP包括SNMPv1，SNMPv2c和SNMPv3版本，其中SNMPv1和SNMPv2c是通过团体名进行认证，具有潜在安全风险，推荐使用SNMPv3版本。

下面以SNMPv3为例，配置设备使用SNMPv3与网管进行通信。

1. 使能SNMP Agent

   ```
   <HUAWEI> system-view
   [~HUAWEI] snmp-agent
   ```

2. 配置SNMP的版本为SNMPv3

   ```
   [*HUAWEI] snmp-agent sys-info version v3
   ```

   说明

   用户可以根据自己的需求配置对应的SNMP版本，但设备侧使用的SNMP协议版本必须和网管侧使用的SNMP版本保持一致，否则设备无法与网管连接。

3. 配置用户访问权限

   # 配置ACL，仅允许IP地址为192.168.1.10的网管访问设备。

   ```
   [*HUAWEI] acl 2001
   [*HUAWEI-acl4-basic-2001] rule permit source 192.168.1.10 0.0.0.0
   [*HUAWEI-acl4-basic-2001] quit
   ```

   # 配置MIB视图为alliso，访问的视图包含iso。

   ```
   [*HUAWEI] snmp-agent mib-view include alliso iso
   ```

   说明

   请根据实际需要配置用户的访问权限。

4. 配置SNMPv3用户组名为huawei_group，用户名为huawei_user，安全级别都为privacy，并应用访问控制

```
[*HUAWEI] snmp-agent group v3 huawei_group privacy write-view alliso acl 2001
[*HUAWEI] snmp-agent usm-user v3 huawei_user group huawei_group
[*HUAWEI] snmp-agent usm-user v3 huawei_user authentication-mode sha
Please configure the authentication password (8-255)
Enter Password:                 //输入认证密码
Confirm Password:               //确认认证密码
[*HUAWEI] snmp-agent usm-user v3 huawei_user privacy-mode aes256
Please configure the privacy password (8-255)
Enter Password:                 //输入加密密码
Confirm Password:               //确认加密密码
```

5. 配置告警主机

```
[*HUAWEI] snmp-agent target-host trap address udp-domain 192.168.1.10 params securityname
huawei_user v3 privacy
[*HUAWEI] commit
```

3.2.1.5 信息中心配置

运管区是网络的管理及维护中心，该区收集设备的运行状态信息。可通过配置信息中心将设备的日志信息发送至运管区的管理服务器，方便监控设备运行状态和定位故障。

步骤1 使能信息中心功能

```
<HUAWEI> system-view
[~HUAWEI] info-center enable
[*HUAWEI] commit
```

步骤2 配置向日志主机发送日志信息。

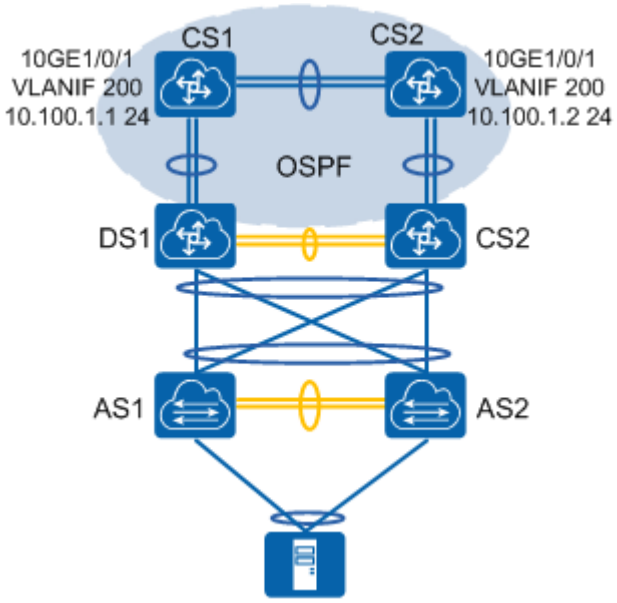
```
[~HUAWEI] info-center loghost 10.1.1.1
[*HUAWEI] commit
```

----结束

3.2.1.6 NTP 配置

在数据中心网络中设置NTP时钟源，为全网提供NTP时钟源服务。数据中心所有网络设备的时钟与此NTP时钟源同步。

将全网的NTP工作模式设置为单播服务器/客户端模式，配置CS1为主时间服务器，且CS1的时间已经同步到权威时钟（卫星定位系统）。配置CS2、DS和AS为客户端。为了保证安全性，建议使能NTP认证功能。



在CS1上配置NTP主时钟并启动NTP认证功能，使能CS1的NTP服务器功能。

```
<CS1> system-view
[~CS1] ntp refclock-master 1
[*CS1] ntp authentication enable
[*CS1] ntp authentication-keyid 42 authentication-mode hmac-sha256 Hello@123456
[*CS1] ntp trusted authentication-keyid 42
[*CS1] undo ntp server disable
[*CS1] commit
```

在DS1上指定CS1为NTP服务器。（其他的配置类似）

```
<DS1> system-view
[~DS1] ntp authentication enable
[*DS1] ntp authentication-keyid 42 authentication-mode hmac-sha256 Hello@123456
[*DS1] ntp trusted authentication-keyid 42
[*DS1] ntp unicast-server 10.100.1.1 authentication-keyid 42
[*DS1] commit
```

3.2.2 业务配置

3.2.2.1 接口配置

为保障网络的可靠性，物理接口配置遵守如下规则：

- 接口缺省使用自协商模式。

  例如10GE电接口，常见配置如下：

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface 10ge 1/0/1
  [~HUAWEI-10GE1/0/1] undo negotiation disable
  [*HUAWEI-10GE1/0/1] speed auto 100 1000 10000
  [*HUAWEI-10GE1/0/1] commit
  ```

- 没有启用的物理接口，必须处于shutdown状态。

  常见配置如下：

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface 10ge 1/0/1
  [~HUAWEI-10GE1/0/1] shutdown
  [*HUAWEI-10GE1/0/1] commit
  ```

- 接口启用链路故障检测功能。

  常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] port crc-statistics trigger error-down
[*HUAWEI-10GE1/0/1] commit
```

- 用于设备互联的接口按照接口编号从大到小的顺序启用，用于连接用户终端的接口按照接口编号从小到大的顺序启用。

3.2.2.2 VLAN 配置

根据业务的不同划分几个相应的网络分区，每个网络分区又有若干种类的应用业务系统，每一类业务都包含了多种子业务系统，且每种子业务系统的业务特点、协议类型、服务质量要求（如延时、抖动等）、安全等级要求是不尽相同的。

为了实现上述的网络系统架构设计，需要进行VLAN划分。通过VLAN技术将不同种类的业务区分开来，可以更好地实现服务质量（QoS）。通过VLAN技术将不同安全级别的业务在逻辑上隔离开来，基于不同的VLAN和应用实现相应的安全策略控制，提高网络的安全性。

这里，选用基于端口划分VLAN的方式进行统一的VLAN分配。具体的VLAN划分依据和部署规范如下：

1. VLAN划分依据
   - 不同区域互联规划互连VLAN ，各个区域内的VLAN ID只是本区有效，禁止在区域之间存在跨区VLAN现象。
   - 每个功能分区都被分配了一定范围的VLAN，然后在网络分区里面根据不同级别的应用再进行分配，同时每个网络分区都预留了部分的VLAN，以满足将来不同应用系统的扩展使用。
   - 不同分区VLAN段不同，不同业务系统使用不同VLAN，同一业务系统服务器在同一VLAN中，按照从小到大的方式使用，城域和辖内广域用户接入VLAN复用本地用户接入VLAN。
2. VLAN部署规范
   - 同一个功能区，AS和DS上配置该区域的所有用户VLAN。该区内部的业务VLAN在AS-DS、DS-DS之间的Trunk链路上都允许通过。
   - Trunk链路不能采用允许所有VLAN通过的方式。
   - 所有Trunk链路不允许VLAN 1通过。

VLAN分配总体规划如下表所示：

表 3-1 VLAN 分配总体规划表

序号	功能	VLAN ID	备注
1	开放平台区	200-399	—
2	开发测试区	400-499	—
3	运营区	500-599	—
4	本地用户接入区	850-949	城域和辖内广域用户复用

序号	功能	VLAN ID	备注
5	extranet外联区	650-699	—
6	网络设备互联VLAN	800-849	—
7	网络设备管理VLAN	600-649	—
8	备用预留	10-199、700-799、950-1049	—

3.2.2.3 链路聚合配置

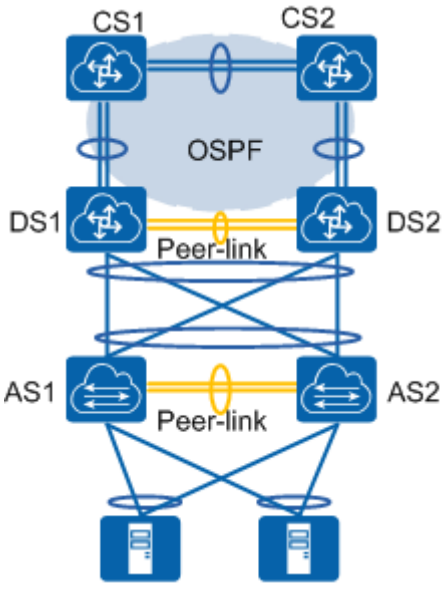
对于有高带宽、高可靠性需求的链路，需要使用链路聚合。

在CS-CS、CS-DS、DS-DS、DS-防火墙、防火墙心跳、AS-DS、AS-服务器均可采用链路聚合技术，保证高带宽高可靠性。

链路聚合部署技术要求：

- 链路聚合成员端口要求部署在不同的单板，以提升单板故障情况下的链路可靠性。
- 链路聚合使用手工负载分担模式，聚合端口速率一致。
- 链路聚合成员端口工作模式采用自协商模式。（如果自协商无法成功，则采用强制模式，同时启用DLDP）

图 3-3 链路聚合配置示意图



链路聚合配置要点如下（以AS为例，其他类似）：

```
<DS1> system-view
[~DS1] vlan batch 200
[*DS1] interface eth-trunk 1
[*DS1-Eth-Trunk1] trunkport 10ge 1/0/1
[*DS1-Eth-Trunk1] trunkport 10ge 1/0/2
[*DS1-Eth-Trunk1] port link-type trunk
[*DS1-Eth-Trunk1] port trunk allow-pass vlan 200
```

```
[*DS1-Eth-Trunk1] undo port trunk allow-pass vlan 1
[*DS1-Eth-Trunk1] quit
[*DS1] commit
[~DS1] interface eth-trunk 2
[*DS1-Eth-Trunk2] trunkport 10ge 1/0/3
[*DS1-Eth-Trunk2] trunkport 10ge 1/0/4
[*DS1-Eth-Trunk2] port link-type access
[*DS1-Eth-Trunk2] port default vlan 200
[*DS1-Eth-Trunk2] undo port trunk allow-pass vlan 1
[*DS1-Eth-Trunk2] quit
[*DS1] commit
```

缺省情况下，Eth-Trunk的工作模式为手工负载分担模式。

3.2.2.4 IP 地址配置

分行数据中心新建局域网IP地址规划应遵循如下原则：

- 采用TCP/IP协议的IPv4版本；
- 局域网范围内的网间网互连地址，使用29位（255.255.255.248）的子网掩码，便于网络结构的灵活扩展部署，以及临时测试设备的插入，一个C类地址空间可以划分出32个局域网的互联网段；
- 规划方案要便于在总行和分行间实现路由汇总；
- 局域网网关地址使用该网段内的最大IP地址，当使用VRRP或类似技术时，虚拟地址和实际地址从该网段中的最大的IP地址（也就是从最后的可用地址）依次向前分配；
- 网络设备的管理地址（Loopback0）采用32位（255.255.255.255）的子网掩码，作为相关路由协议（OSPF）的ID标识；所有网络设备的管理地址按设备网络层次从同一网段依次连续分配；
- 根据各功能区和网络分区进行IP地址分配，各功能区汇聚设备下行口开始（包括分布层设备互连）为同一分区IP地址规划，核心交换机互连各区接口为核心交换区IP地址规划，广域DS交换机各广域设备接入为城域/广域IP地址规划。

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] interface vlanif 201
[*HUAWEI-Vlanif201] ip address 10.1.0.1 255.255.255.0
```

3.2.2.5 STP 配置

破环协议在二层网络中尤为重要，在多级M-LAG场景下二层网络可以采用V-STP协议进行破环。V-STP技术支持STP/RSTP破坏协议，可以感知M-LAG主备协商状态，在M-LAG主备协商成功后，两台设备被虚拟化成一台设备进行端口角色计算和快速收敛计算。

在满足组网业务需求、可靠性需求的前提下，尽可能简化配置，达到简化部署和维护简单的目的。

V-STP配置要点：

配置DS和AS使能V-STP。

以DS1和DS2为例，假设DS1为M-LAG主设备，DS2为M-LAG备设备，AS1和AS2配置相同。

```
<DS1> system-view
[~DS1] stp mode rstp
```

```
[*DS1] stp v-stp enable
[*DS1] commit
```

```
<DS2> system-view
[~DS2] stp mode rstp
[*DS2] stp v-stp enable
[*DS2] stp priority 36864
[*DS2] commit
```

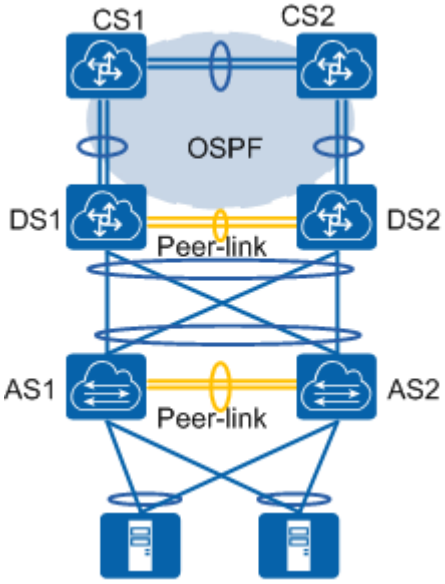
3.2.3 可靠性配置

3.2.3.1 M-LAG 配置

基于M-LAG组成的双活系统提供了设备级的可靠性，将双归接入的两台设备在逻辑上虚拟成一台设备。M-LAG提供了一个没有环路的二层拓扑同时实现冗余备份。

多级M-LAG互联可以在保证可靠性、提供链路利用率的同时扩展双归接入的网络规模，满足客户的需求。

图 3-4 M-LAG 配置示意图



DS1和DS2、AS1和AS2交换机组建了多级M-LAG，DS1和DS2之间Eth-Trunk链路配置Peer-Link，交互M-LAG同步报文。在M-LAG设备之间配置V-STP破除环路。同时，在DS和CS设备上配置OSPF实现三层互通。

M-LAG配置要点：

以AS1和AS2组建M-LAG为例，DS设备配置类似。

1. 在AS1和AS2上配置主接口的IP地址，且保证能够三层互通，专门用于M-LAG主备设备间心跳报文的传输。

```
<AS1> system-view
[~AS1] interface meth 0/0/0
[~AS1-MEth0/0/0] ip address 10.1.1.1 24
[*AS1-MEth0/0/0] quit
<AS2> system-view
[~AS2] interface meth 0/0/0
[~AS2-MEth0/0/0] ip address 10.1.1.2 24
[*AS2-MEth0/0/0] quit
```

2. 在AS1和AS2上配置M-LAG的DFS Group。

```
[*AS1] dfs-group 1
[*AS1-dfs-group-1] source ip 10.1.1.1
[*AS1-dfs-group-1] priority 150
[*AS1-dfs-group-1] quit
[*AS2] dfs-group 1
[*AS2-dfs-group-1] source ip 10.1.1.2
[*AS2-dfs-group-1] priority 120
[*AS2-dfs-group-1] quit
```

3. 在AS1和AS2上配置M-LAG的Peer-Link

```
[*AS1] interface eth-trunk 0
[*AS1-Eth-Trunk0] trunkport 10ge 1/0/3
[*AS1-Eth-Trunk0] trunkport 10ge 1/0/4
[*AS1-Eth-Trunk0] mode lacp-static
[*AS1-Eth-Trunk0] peer-link 1
[*AS1-Eth-Trunk0] quit
[*AS2] interface eth-trunk 0
[*AS2-Eth-Trunk0] trunkport 10ge 1/0/3
[*AS2-Eth-Trunk0] trunkport 10ge 1/0/4
[*AS2-Eth-Trunk0] mode lacp-static
[*AS2-Eth-Trunk0] peer-link 1
[*AS2-Eth-Trunk0] quit
```

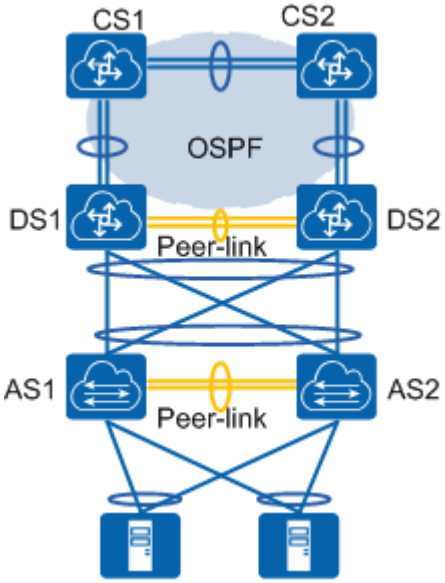
4. 在AS1和AS2上配置M-LAG的成员口

```
[*AS1] vlan batch 11
[*AS1] interface eth-trunk 20
[*AS1-Eth-Trunk20] mode lacp-static
[*AS1-Eth-Trunk20] port link-type trunk
[*AS1-Eth-Trunk20] port trunk allow-pass vlan 11
[*AS1-Eth-Trunk20] trunkport 10ge 1/0/1 to 1/0/2
[*AS1-Eth-Trunk20] dfs-group 1 m-lag 1
[*AS1-Eth-Trunk20] quit
[*AS1] interface eth-trunk 30
[*AS1-Eth-Trunk30] mode lacp-static
[*AS1-Eth-Trunk30] port link-type trunk
[*AS1-Eth-Trunk30] port trunk allow-pass vlan 11
[*AS1-Eth-Trunk30] trunkport 10ge 1/0/5 to 1/0/6
[*AS1-Eth-Trunk30] dfs-group 1 m-lag 2
[*AS1-Eth-Trunk30] quit
[*AS1] commit
[*AS2] vlan batch 11
[*AS2] interface eth-trunk 20
[*AS2-Eth-Trunk20] mode lacp-static
[*AS2-Eth-Trunk20] port link-type trunk
[*AS2-Eth-Trunk20] port trunk allow-pass vlan 11
[*AS2-Eth-Trunk20] trunkport 10ge 1/0/1 to 1/0/2
[*AS2-Eth-Trunk20] dfs-group 1 m-lag 1
[*AS2-Eth-Trunk20] quit
[*AS2] interface eth-trunk 30
[*AS2-Eth-Trunk30] mode lacp-static
[*AS2-Eth-Trunk30] port link-type trunk
[*AS2-Eth-Trunk30] port trunk allow-pass vlan 11
[*AS2-Eth-Trunk30] trunkport 10ge 1/0/5 to 1/0/6
[*AS2-Eth-Trunk30] dfs-group 1 m-lag 2
[*AS2-Eth-Trunk30] quit
[*AS2] commit
```

3.2.3.2 Monitor Link 配置

为了避免因上行链路故障导致用户侧流量无法转发而丢弃，需要配置Monitor Link关联上行接口和下行接口。

当DS1的上行链路故障时，用户侧的流量如果从DS1转发会被丢弃，需要在DS1上配置Monitor Link关联上行接口和下行接口，这样DS1的下行接口也将处于Down状态使用户侧流量不从DS1转发，保证流量正常的转发。



Monitor Link配置要点：

以DS1为例，DS2设备配置相同。

1. 配置DS1的单接口为Monitor link组的上行接口或下行接口，进行关联。

```
[~DS1] monitor-link group 1
[*DS1-mtlk-group1] port eth-trunk 10 uplink
[*DS1-mtlk-group1] port eth-trunk 20 downlink 1
```

配置Monitor Link组后，上行接口将被实时监控，一旦所有上行接口出现故障，其所在组的所有下行接口都会被强制设为ERROR DOWN状态。

Error-Down是指设备检测到故障后将接口状态设置为ERROR DOWN状态，此时接口不能收发报文，接口指示灯为常灭。

2. 配置DS1的Monitor Link组自动回切时间。

```
[*DS1-mtlk-group1] timer recover-time 5
[*DS1-mtlk-group1] quit
[*DS1] commit
```

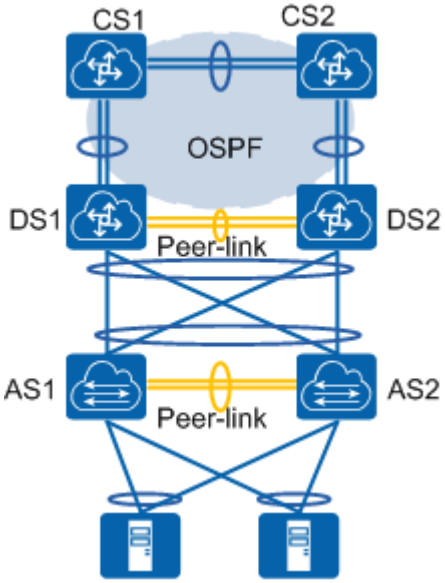
下行接口处于Error-Down状态时，如果需要恢复下行接口为UP状态，则需要先排除上行接口故障，上行接口状态UP后，经过自动回切时间，下行接口将会恢复UP状态。

3.2.3.3 双活网关配置

通常情况下，网络内部的所有主机都设置一条相同的缺省路由，指向出口网关，实现主机与外部网络的通信。当出口网关发生故障时，主机与外部网络的通信就会中断。

M-LAG将主备设备联合组成一台虚拟路由设备，将虚拟路由设备的IP地址作为用户的默认网关实现与外部网络通信。当其中一台网关设备发生故障时，M-LAG机制能够保证另一台网关设备承担数据流量，从而保障网络的可靠通信。

图 3-5 双活网关配置示意图



M-LAG双活网关有两种配置方式：

- **通过配置VRRP实现双活网关功能：**在VLANIF接口上创建VRRP备份组并使VLANIF接口具有相同的虚拟IP和虚拟MAC，在M-LAG基础上配置VRRP实现双活网关功能。
- **通过配置VLANIF接口IP地址和MAC地址实现双活网关功能 ：**在VLANIF接口上配置相同的IP地址并使用mac-address命令配置相同的虚拟MAC地址。

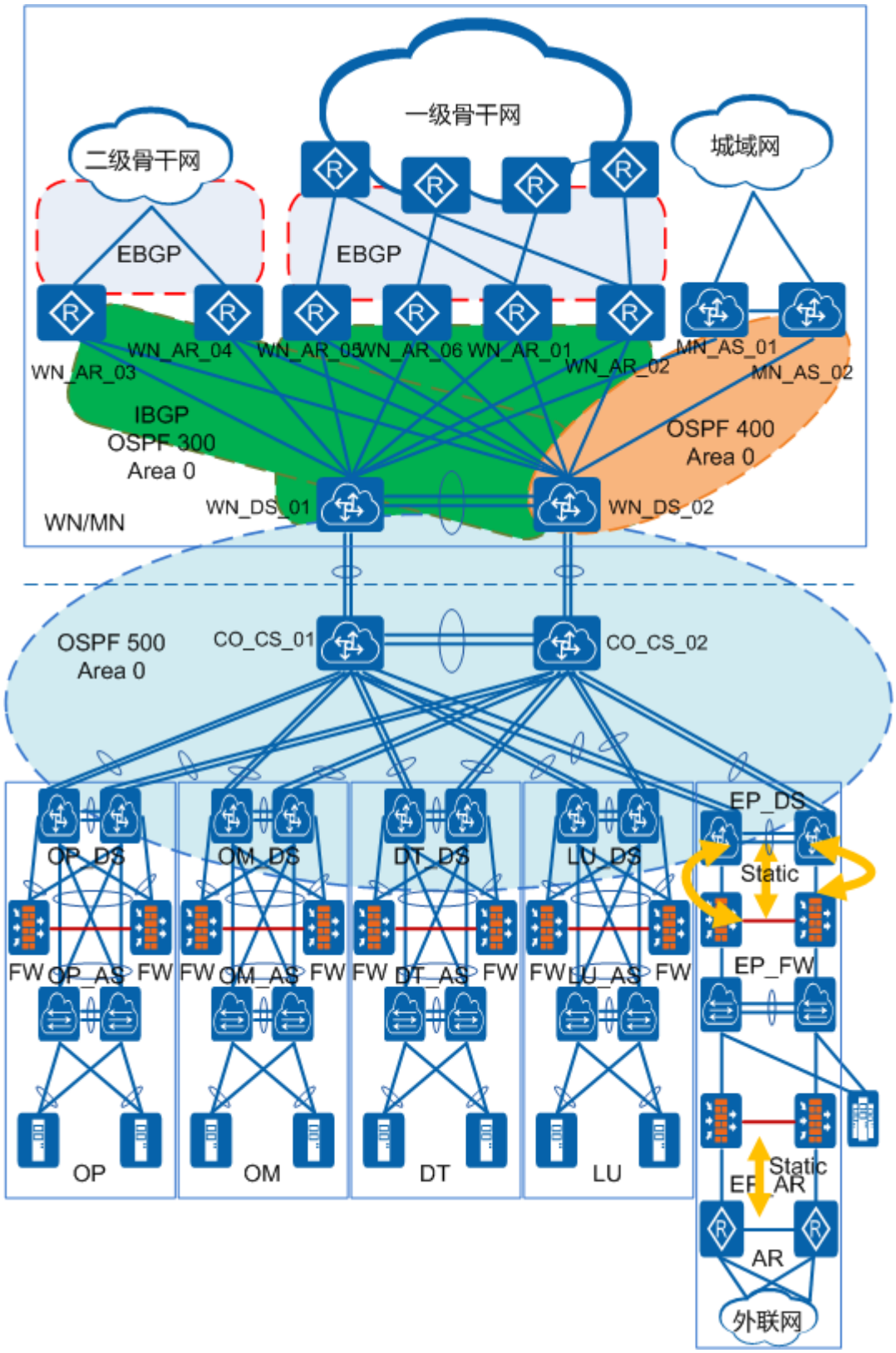
在DS设备之间配置M-LAG双活网关功能，作为接入设备的双活网关：

以DS1为例，DS2配置类似。

1. 在DS设备上的VLANIF接口配置VRRP备份组，作为M-LAG主备设备的双活网关
```
[~DS1] interface vlanif 11
[*DS1-Vlanif11] ip address 10.2.1.1 24
[*DS1-Vlanif11] vrrp vrid 1 virtual-ip 10.2.1.111
[*DS1-Vlanif11] vrrp vrid 1 priority 120
[*DS1-Vlanif11] quit
[*DS1] commit
```
2. 在DS设备上的VLANIF接口配置相同IP地址和MAC地址，作为M-LAG主备设备的双活网关
```
[~DS1] interface vlanif 11
[*DS1-Vlanif11] ip address 10.2.1.1 24
[*DS1-Vlanif11] mac-address 0000-5e00-0101
[*DS1-Vlanif11] quit
[*DS1] commit
```
采用配置VLANIF接口IP地址和MAC地址方式时，由于两端配置相同的IP地址，会产生IP地址冲突告警。如果要屏蔽该告警，可以执行命令undo snmp-agent trap enable feature-name arp trap-name hwethernetarpipconflictevent来关闭IP地址冲突告警开关。

3.2.4 路由配置

一级分行数据中心整体路由设计示意图如下：



整个数据中心规划可以分为局域网部分和广域城域区两部分。

整体路由设计：

广域城域区使用BGP与总行、二级分行对接交互业务路由，区域内部使用OSPF作为IGP。

局域网部分，除外联区DS－AR间使用静态路由外，核心区及其它分区整体使用OSPF进行业务路由承载。

EBGP：

一级分行规划为独立的自治域，使用私有的AS号。

IBGP：

一级分行的广域网区运行IBGP，OSPF300为广域网区WN_DS和WN_AR之间的IBGP提供联通性。

网络整体规划使用三个OSPF域，分别为OSPF300、OSPF400、OSPF500。

OSPF300：

OSPF300进程用于提供广域网区WN_DS和WN_AR之间的IBGP连通性，广域网区设备之间互联链路归属area0。

OSPF400：

OSPF400进程用于城域广域区和一级分行同城机构的路由互通，互联链路归属area0。

OSPF500：

OSPF500进程用于分行局域网区和WN_DS的路由互通，互联链路归属area0，承载一级分行业务。

Static:

外联区EP_AR和外部FW之间，外部FW和内部FW之间，内部FW和EP_DS之间通过静态路由互指互通。

路由协议优先级（preference/distance）设计：

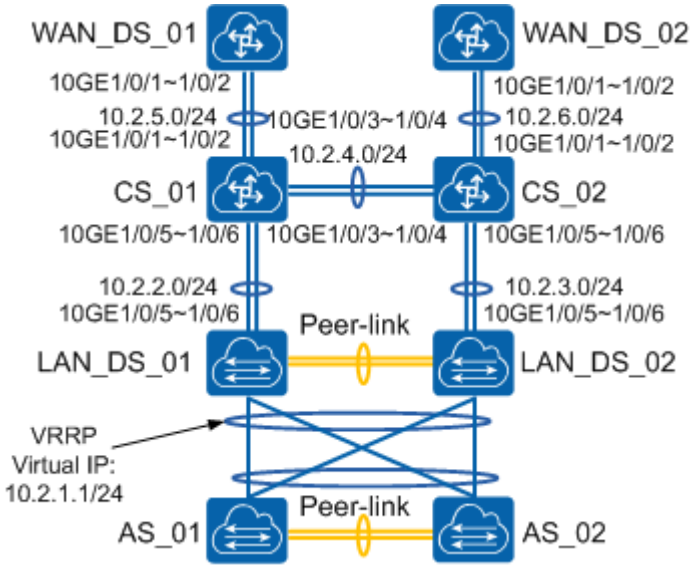
为保证不同厂家设备、不同路由协议间路由优选的一致性，对全网设备可能使用的路由协议的优先级统一规划如下：

协议类型	优先级
静态路由	5
OSPF	10
IBGP	170
EBGP	170
OSPF ASE	190
浮动静态路由	200

3.2.4.1 局域网路由配置

一、路由设计概述及基本功能配置

图 3-6 局域网路由规划示意图



如图所示，为某数据中心局域网部分，AS为接入设备，LAN_DS为局域网内汇聚设备，网关配置在汇聚设备上，LAN_DS下行配置VRRP，保证可靠性。CS设备为核心转发设备，WAN_DS设备是广域城域区域的汇聚设备，用于连接局域网核心设备和网络出口路由器。

本例整网采用OSPF协议保证域内连通性。

OSPF区域划分

整网采用OSPF路由协议，路由协议进程号为500。由于局域网内需运行OSPF的设备数量较少，所以OSPF500进程中仅使用Area0骨干区。需要使能OSPF的接口如下：

- LAN_DS下行VRRP的虚IP
- LAN_DS、WAN_DS、CS设备互联接口
- 用于Router ID的Loopback接口，注意该接口不需要参与OSPF计算，所以配置为Silent Interface。

OSPF Router ID规划

在每个OSPF进程中，路由器需要有唯一的Router ID来标识自己。在缺省情况下，路由器指定最大的Loopback IP地址作为自己的Router ID。为保证OSPF Router ID相对稳定，在OSPF进程的配置中，指定Loopback0接口的IP地址为Router ID。

OSPF基本功能配置

LAN_DS设备以LAN_DS_01为例：

```
<LAN_DS_01> system-view
[~LAN_DS_01] interface loopback 0
[*LAN_DS_01-LoopBack0] ip address 172.16.1.1 32
[*LAN_DS_01-LoopBack0] quit
[*LAN_DS_01] ospf 500 router-id 172.16.1.1
[*LAN_DS_01-ospf-500] silent-interface loopback 0
```

```
[*LAN_DS_01-ospf-500] area 0
[*LAN_DS_01-ospf-500-area-0.0.0.0] network 10.2.1.0 0.0.0.255
[*LAN_DS_01-ospf-500-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[*LAN_DS_01-ospf-500-area-0.0.0.0] commit
```

CS设备以CS_01为例：

```
<CS_01> system-view
[~CS_01] interface loopback 0
[*CS_01-LoopBack0] ip address 172.16.1.2 32
[*CS_01-LoopBack0] quit
[*CS_01] ospf 500 router-id 172.16.1.2
[*CS_01-ospf-500] silent-interface loopback 0
[*CS_01-ospf-500] area 0
[*CS_01-ospf-500-area-0.0.0.0] network 10.2.2.0 0.0.0.255
[*CS_01-ospf-500-area-0.0.0.0] network 10.2.4.0 0.0.0.255
[*CS_01-ospf-500-area-0.0.0.0] network 10.2.5.0 0.0.0.255
[*CS_01-ospf-500-area-0.0.0.0] commit
```

二、路由协议性能、可靠性和安全性设计及配置

以下配置均以CS_01为例，其他设备配置类似。

OSPF接口网络类型规划

缺省情况下，以太网中OSPF接口的网络类型是broadcast，但是本例中所有OSPF邻居均为两台互联，所以为了加快邻居建立和路由收敛，非Silent接口OSPF的网络类型统一配置为Point-to-Point。

```
<CS_01> system-view
[~CS_01] interface 10ge 1/0/1
[~CS_01-10GE1/0/1] undo portswitch
[*CS_01-10GE1/0/1] ospf network-type p2p
```

OSPF定时器规划

如果没有特殊需求，OSPF的定时器建议全部使用缺省值，本例即全部使用缺省值。如果需要修改定时器参数，需要保证相邻设备OSPF定时器参数一致。

例：修改OSPF发送Hello报文的时间间隔为20秒。

```
<CS_01> system-view
[~CS_01] interface 10ge 1/0/1
[~CS_01-10GE1/0/1] undo portswitch
[*CS_01-10GE1/0/1] ospf timer hello 20
```

OSPF Metric值

缺省情况下，OSPF接口Metric值是通过自动计算得出的，计算公式为：参考带宽/接口带宽。参考带宽可修改，缺省值为100Mbps。

本例中，考虑到方便后续维护管理，不使用自动计算模式，手动配置各链路的OSPF Metric值，规划如下：

表 3-2 OSPF Metric 值规划

序号	链路	Metric
1	CS-CS、DS-DS之间东西向链路	100
2	CS-DS之间南北向链路	100
3	DS业务接口	1000

序号	链路	Metric
4	CS/DS Loopback接口	0（无需配置）

例：配置CS-CS规划值为100：

```
<CS_01> system-view
[~CS_01] interface 10ge 1/0/1
[~CS_01-10GE1/0/1] undo portswitch
[*CS_01-10GE1/0/1] ospf cost 100
```

BFD for OSPF

BFD for OSPF就是将BFD和OSPF协议关联起来，BFD对链路故障的快速感应会通知OSPF协议，从而加快OSPF协议对于网络拓扑变化的响应。

通过在所有OSPF非silent接口与邻居建立动态BFD会话，可以实现OSPF邻居间链路故障（包括物理链路故障和上层转发故障）的毫秒级检测，并联动OSPF邻居状态快速切换，触发路由收敛计算。

所有BFD会话统一使用如下参数：

表 3-3 BFD for OSPF 参数规划

参数	参数说明	建议取值
min-rx-interval	期望从对端接收BFD报文的最小接收间隔。	1000ms
min-tx-interval	向对端发送BFD报文的最小发送间隔。	1000ms
detect-multiplier	本地检测倍数。	3

```
<CS_01> system-view
[~CS_01] bfd
[*CS_01-bfd] quit
[*CS_01] ospf 500
[*CS_01-ospf-500] bfd all-interfaces enable
[*CS_01-ospf-500] bfd all-interfaces min-tx-interval 1000 min-rx-interval 1000 detect-multiplier 3
```

OSPF智能定时器

网络不稳定时，可能会频繁进行路由计算，造成系统CPU消耗过大。尤其是在不稳定网络中，经常会产生和传播描述不稳定拓扑的LSA，频繁处理这样的LSA，不利于整个网络的快速稳定。OSPF智能定时器分别对路由计算、LSA的产生、LSA的接收进行控制，加速网络收敛。

OSPF智能定时器可以通过以下两种方式来加速网络收敛：

- 在频繁进行路由计算的网络中，OSPF智能定时器根据用户的配置和指数衰减技术动态调整两次路由计算的时间间隔，减少路由计算的次数，从而减少CPU的消耗，待网络拓扑稳定后再进行路由计算。

- 在不稳定网络中，当路由器由于拓扑的频繁变化需要产生或接收LSA时，OSPF智能定时器可以动态调整时间间隔，在时间间隔之内不产生LSA或对接收到的LSA不进行处理，从而减少整个网络无效LSA的产生和传播。

OSPF智能定时器统一使用如下参数：

表 3-4 OSPF 智能定时器规划

智能定时器	说明	建议取值
spf-schedule-interval	控制OSPF路由计算的时间间隔。	建议使用缺省值。即：SPF计算的最长间隔时间为10000毫秒、初始间隔时间为500毫秒、基数间隔时间为1000毫秒。
lsa-arrival-interval	控制OSPF LSA接收的时间间隔。	建议使用缺省值。即：接收LSA的最长间隔时间为1000毫秒、初始间隔时间为500毫秒、基数间隔时间为500毫秒。
lsa-originate-interval	控制OSPF LSA的更新时间间隔。	建议使用缺省值。即：更新LSA的最长间隔时间为5000毫秒、初始间隔时间为500毫秒、基数间隔时间为1000毫秒。

```
<CS_01> system-view
[~CS_01] ospf 500
[*CS_01-ospf-500] lsa-arrival-interval intelligent-timer 1000 500 500
[*CS_01-ospf-500] lsa-originate-interval intelligent-timer 5000 500 1000
[*CS_01-ospf-500] spf-schedule-interval intelligent-timer 10000 500 1000
```

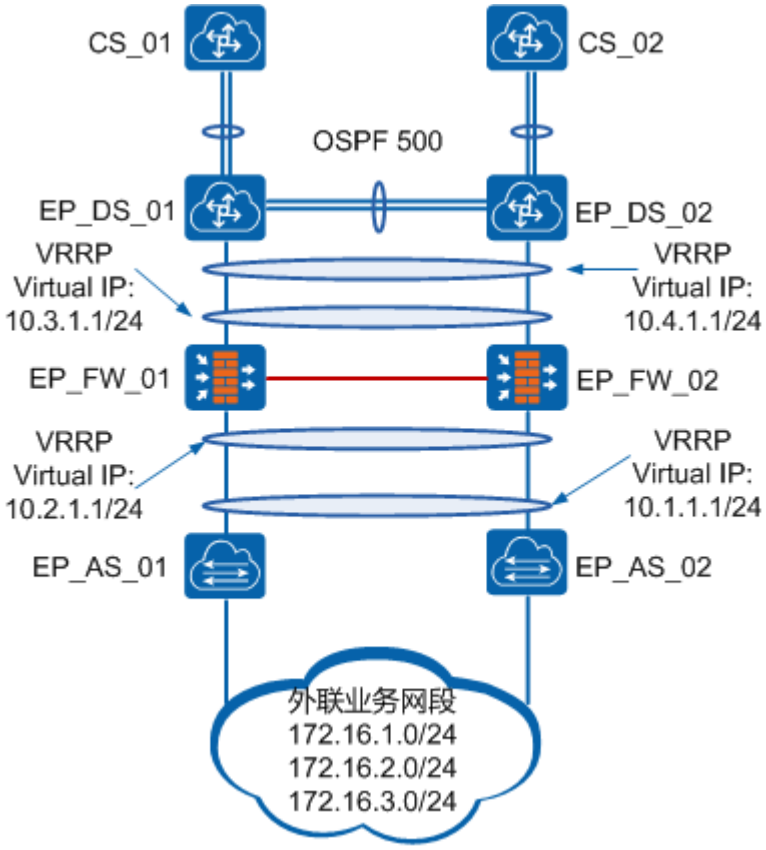
OSPF路由认证

为防止非法设备接入OSPF网络获取网络路由信息，可以部署OSPF路由认证的功能。本例中，统一部署OSPF区域认证，验证模式为MD5，具体密码不做说明，由客户自行指定。

```
<CS_01> system-view
[~CS_01] ospf 500
[*CS_01-ospf-500] area 0
[*CS_01-ospf-500-area-0.0.0.0] authentication-mode md5 1 cipher xxxxxxxx
```

3.2.4.2 外联区域路由配置

图 3-7 外联区域路由规划示意图



外联区域用于数据中心和其他业务区域的互联，由于需要对访问权限做比较精细的控制，外联区域采用防火墙串连的方式进行组网。

路由设计上，外联区域路由均采用静态明细路由+静态缺省路由的方式，和局域网区域进行路由隔离。下面给出各设备关键配置：

外联区域的汇聚设备（EP_DS）

外联区域的汇聚设备（EP_DS）设备上行和局域网的CS设备依旧采用OSPF进行互通，但是下行需要配置到所有外联业务网段的静态明细路由，下一跳均指向防火墙设备（EP_FW）的上行VRRP地址。OSPF500和VRRP相关配置见“局域网路由配置”。下面仅给出EP_DS_01静态明细路由配置，EP_DS_02配置和EP_DS_01相同。

```
<EP_DS_01> system-view
[~EP_DS_01] ip route-static 172.16.1.0 24 10.3.1.1
[*EP_DS_01] ip route-static 172.16.2.0 24 10.3.1.1
[*EP_DS_01] ip route-static 172.16.3.0 24 10.3.1.1
```

防火墙设备（EP_FW）

EP_FW上行采用静态缺省路由，下一跳指向EP_DS设备下行VRRP地址。下行配置到所有外联业务网段的静态明细路由，下一跳均指向外联区域接入设备（EP_AS）的上行VRRP地址。下面仅给出EP_FW_01静态路由配置，EP_FW_02配置和EP_FW_01相同。

```
<EP_FW_01> system-view
[~EP_FW_01] ip route-static 172.16.1.0 24 10.1.1.1
[*EP_FW_01] ip route-static 172.16.2.0 24 10.1.1.1
```

```
[*EP_FW_01] ip route-static 172.16.3.0 24 10.1.1.1
[*EP_FW_01] ip route-static 0.0.0.0 0 10.4.1.1
```

外联区域的接入设备（EP_AS）

EP_AS上行采用静态缺省路由，下一跳指向EP_FW的下行VRRP地址。下行配置到所有外联业务网段的静态明细路由，下一跳指向对端直连设备的接口地址。下面给出EP_AS_01的静态路由配置，对端直连设备的接口地址用“x.x.x.x”代替。

```
<EP_AS_01> system-view
[~EP_AS_01] ip route-static 172.16.1.0 24 x.x.x.x
[*EP_AS_01] ip route-static 172.16.2.0 24 x.x.x.x
[*EP_AS_01] ip route-static 172.16.3.0 24 x.x.x.x
[*EP_AS_01] ip route-static 0.0.0.0 0 10.2.1.1
```

3.2.4.3 广域城域部分路由配置

广域城域区使用BGP与总行、二级分行对接交互业务路由。

3.2.5 安全配置

3.2.5.1 ACL 防病毒配置

对于已知具有3、4层特征的病毒破坏，华为推荐在网络设备上采用定义ACL对这些数据流进行过滤，增加网络的安全性。推荐的常见防病毒配置如下：

```
[*HUAWEI]acl number 3000
[*HUAWEI-acl4-advence-3000]rule 0 deny tcp destination-port eq 445
[*HUAWEI-acl4-advence-3000]rule 1 deny udp destination-port eq 445
[*HUAWEI-acl4-advence-3000]rule 2 deny tcp destination-port eq 135
[*HUAWEI-acl4-advence-3000]rule 3 deny tcp destination-port eq 136
[*HUAWEI-acl4-advence-3000]rule 4 deny tcp destination-port eq 137
[*HUAWEI-acl4-advence-3000]rule 5 deny tcp destination-port eq 138
[*HUAWEI-acl4-advence-3000]rule 6 deny tcp destination-port eq 139
[*HUAWEI-acl4-advence-3000]rule 7 deny udp destination-port eq 135
[*HUAWEI-acl4-advence-3000]rule 8 deny udp destination-port eq 136
[*HUAWEI-acl4-advence-3000]rule 9 deny udp destination-port eq netbios-ns
[*HUAWEI-acl4-advence-3000]rule 10 deny udp destination-port eq netbios-dgm
[*HUAWEI-acl4-advence-3000]rule 11 deny udp destination-port eq netbios-ssn
[*HUAWEI-acl4-advence-3000]rule 12 deny udp destination-port eq 1434
[*HUAWEI-acl4-advence-3000]rule 13 deny udp destination-port eq 6667
[*HUAWEI-acl4-advence-3000]rule 14 deny udp destination-port eq 7626
[*HUAWEI-acl4-advence-3000]rule 15 deny udp destination-port eq 6789
[*HUAWEI-acl4-advence-3000]rule 16 deny udp destination-port eq 5800
[*HUAWEI-acl4-advence-3000]rule 17 deny udp destination-port eq 5900
[*HUAWEI-acl4-advence-3000]rule 18 deny tcp destination-port eq 5900
[*HUAWEI-acl4-advence-3000]rule 19 deny tcp destination-port eq 5800
[*HUAWEI-acl4-advence-3000]rule 20 deny tcp destination-port eq 1999
[*HUAWEI-acl4-advence-3000]rule 21 deny tcp destination-port eq 5554
[*HUAWEI-acl4-advence-3000]rule 22 deny tcp destination-port eq 9995
[*HUAWEI-acl4-advence-3000]rule 23 deny tcp destination-port eq 9996
[*HUAWEI-acl4-advence-3000]rule 24 deny udp destination-port eq 12345
[*HUAWEI-acl4-advence-3000]rule 25 deny udp destination-port eq 1057
[*HUAWEI-acl4-advence-3000]rule 26 deny udp destination-port eq 2616
```

3.2.5.2 广播风暴抑制配置

当网络中出现广播风暴时，会严重影响到网络使用。通过部署广播风暴抑制，可以降低广播风暴对网络的影响。

该功能在接近用户的设备上配置效果最好，因此在汇聚交换机下联端口和接入交换机的所有端口配置广播风暴抑制功能。

当报文的平均速率大于5000kbit/s时，进行风暴抑制，将超过的报文丢弃。

在汇聚交换机下行端口、汇聚交换机互联端口和接入交换机上联端口进行如下配置：

```
<HUAWEI> system-view
[~HUAWEI] interface 10ge 1/0/1
[~HUAWEI-10GE1/0/1] storm suppression broadcast cir 5000
```

3.2.5.3 MAC 地址漂移检测

MAC地址漂移即设备上一个接口学习到的MAC地址在同一VLAN中另一个接口上也被学习到，后学习到的MAC地址表项覆盖原来的表项。

配置MAC地址漂移检测功能可以检测到设备上所有的MAC地址是否发生了漂移。若发生漂移，设备会上报告警到网管系统，维护人员可根据告警信息定位故障。

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] mac-address flapping detection
```

3.2.5.4 MAC 刷新 ARP 功能

网络设备进行三层转发时，通过查找ARP表，命中表项后直接转发。某些时候，终端的逻辑位置发生了变化（比如服务器主备网卡发生切换），这个时候该IP对应的端口发生了变化。

MAC地址表项的出接口是通过报文触发刷新的，ARP表项的出接口是在老化时间到后通过老化探测进行刷新的。这样就可能会出现MAC表项和ARP表项出接口不一致的情况，即MAC地址表项的出接口已刷新，而ARP表项的出接口没有及时刷新的情况。

这个时候，就要开启MAC地址联动ARP功能，一旦MAC地址检测到端口发生变化，同时触发ARP表的刷新。

常见配置如下：

```
<HUAWEI> system-view
[~HUAWEI] mac-address update arp enable
```

3.2.5.5 单端口防环路检测

当网络中某个端口下出现环路时，STP一般无法检测成功，需要开启单端口防环路检测功能。

在接入交换机下行端口上进行如下配置：

```
<HUAWEI> system-view
[~HUAWEI] interface ge 1/0/1
[~HUAWEI-GE1/0/1] loopback-detect enable
```

3.2.5.6 ARP 防攻击配置

- **配置ARP报文速率抑制**

如果网络中有主机通过向设备发送大量目标IP地址不能解析的IP报文来攻击设备，则会对网络设备造成很大的危害。

系统视图下配置ARP报文速率抑制功能：

```
<HUAWEI> system-view
[~HUAWEI] arp anti-attack rate-limit 200
```

VLAN视图下配置ARP报文速率抑制功能：

```
<HUAWEI> system-view
[~HUAWEI] vlan 201
[*HUAWEI-vlan201] arp anti-attack rate-limit 200
```

- **配置ARP报文源IP地址抑制**

  考虑到某些特定的用户有特别的需求，在对ARP报文进行源IP地址抑制时，可以针对该用户的IP地址配置不同于其他IP地址的ARP报文抑制速率。

  说明

  默认情况下，根据源IP地址配置的ARP报文限速值为30pps。当同一个源IP地址的ARP报文速率超过30pps时，如果是在网关请求同网段内很多个用户MAC地址的场景下，则需要增大设备的ARP报文源IP地址抑制速率值，否则超过30pps的ARP报文将被丢弃，会造成网关学习ARP很慢；如果是在ARP扫描攻击的场景下，则需要减小设备的ARP报文源IP地址抑制速率值。

  配置根据任意源IP地址进行ARP报文限速的限速值：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp anti-attack rate-limit source-ip maximum 100
  ```

  配置对指定IP地址10.1.1.1的ARP报文限速的限速值：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp anti-attack rate-limit source-ip 10.1.1.1 maximum 100
  ```

  两种配置同时存在的情况下，当ARP报文源IP地址匹配限速指定的IP地址时，对该源IP地址的ARP报文限速值为后一步骤中配置的maximum值；否则为前一步骤中配置的maximum值。

- **配置ARP Miss消息源IP抑制**

  考虑到某些特定的用户有特别的需求，对于该用户的IP地址可以配置不同于其他IP地址的ARP Miss抑制速率。

  说明

  默认情况下，根据源IP地址配置的ARP Miss限速值为30pps。如果同一个源IP地址频繁触发ARP Miss消息且触发的ARP Miss消息速率超过30pps属于正常的情况，则需要增大ARP Miss消息的源IP地址抑制速率值。否则超过30pps的ARP Miss消息会触发ARP Miss消息源抑制，设备默认在5秒钟内丢弃匹配该源IP地址的所有ARP Miss报文，造成该源IP地址无法触发ARP学习。

  配置根据任意源IP地址进行ARP Miss消息限速的限速值：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp miss anti-attack rate-limit source-ip maximum 60
  ```

  配置对指定IP地址用户的ARP Miss消息进行限速的限速值：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp miss anti-attack rate-limit source-ip 10.0.0.1 maximum 60
  ```

  两种配置同时存在的情况下，当触发ARP Miss消息的IP报文的源IP地址匹配限速指定的IP地址时，对该源IP地址的IP报文触发的ARP Miss消息限速值为后一步骤中配置的maximum值；否则为前一步骤中配置的maximum值。

- **配置严格学习ARP表项**

  严格学习ARP表项指的是设备只学习自己发送的ARP请求报文的应答报文。

  配置全局ARP表项严格学习功能：

  ```
  <HUAWEI> system-view
  [~HUAWEI] arp learning strict
  ```

  配置接口的ARP表项严格学习功能：

  ```
  <HUAWEI> system-view
  [~HUAWEI] interface vlanif 201
  [~HUAWEI-Vlanif201] arp learning strict force-enable
  ```

- **配置防止ARP地址欺骗**

  为了防止ARP地址欺骗攻击，可以使能ARP表项固化功能。

```
<HUAWEI> system-view
[~HUAWEI] arp anti-attack entry-check fixed-mac enable
```

- **配置防止ARP中间人攻击**

  防止ARP中间人攻击，可以配置ARP报文检查功能，对接口或VLAN下收到的ARP报文和绑定表进行匹配检查，当报文的检查项和绑定表中的特征项一致时，转发该报文，否则丢弃报文。

  同时可以配置告警功能，当丢弃的报文数超过限制的阈值时，发出告警信息。

  说明

  - 本功能仅适用于DHCP用户场景，对于DHCP用户，设备使能DHCP Snooping功能后会自动生成绑定表。
  - CE6880EI和CE12800E不支持此功能。

  使能动态ARP检测功能（即对ARP报文进行绑定表匹配检查功能）：

```
<HUAWEI> system-view
[~HUAWEI] vlan 201
[*HUAWEI-vlan201] arp anti-attack check user-bind enable
```

  配置对ARP报文进行绑定表匹配检查的检查项：

```
[*HUAWEI-vlan201] arp anti-attack check user-bind check-item ip-address
```

  如果希望仅匹配绑定表某一项或某两项内容的特殊ARP报文也能够通过，则可以配置对ARP报文进行绑定表匹配检查时只检查某一项或某两项内容。

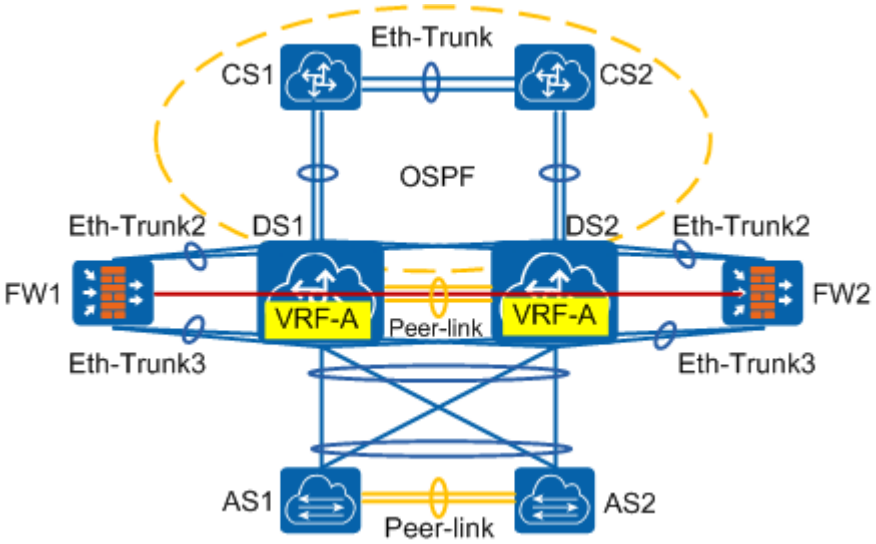
  说明

  指定ARP报文绑定表匹配检查项对配置了静态绑定表的用户不起作用，即设备仍然按照静态绑定表的内容对ARP报文进行绑定表匹配检查。

3.2.6 防火墙配置

开放平台区、开发测试区、运管区和分区出口采用旁挂方式部署防火墙，保证本分区和其它功能区的互访有安全控制。

分布层通过创建VRF隔离业务网段路由与公网路由，采用旁挂方式部署防火墙，保证不同区域互访的安全控制，两台防火墙进行双机热备份，保证高可靠性。



DS设备上创建VPN实例VRF-A，将业务接口和连接防火墙下行的接口绑定到VRF-A，VRF-A的缺省路由指向防火墙的下行VRRP虚拟IP。DS设备配置至业务网段的静态路由，下一跳指向防火墙上行VRRP的虚拟IP。

防火墙与DS设备之间采用静态路由。防火墙配置双机热备，并根据应用的需要配置安全策略。

1. 在DS1和DS2之间之间配置M-LAG，并配置VRPP备份组分别作为用户侧网关和防火墙的下一跳。在接口VLANIF200上创建VRRP备份组作为防火墙上行的下一跳，在接口VLANIF300上创建VRRP备份组作为防火墙下行的下一跳。
2. DS1上创建VPN实例VRF-A，将VLANIF200和连接防火墙下行的VLANIF300绑定到VRF-A，VRF-A的缺省路由指向防火墙的下行VRRP虚拟IP。

   说明

   将接口绑定到VRF-A时，接口上的IP地址会被删除，需要重新配置IP地址。

```
[~DS1] ip vpn-instance VRF-A
[*DS1-vpn-instance-VRF-A] ipv4-family
[*DS1-vpn-instance-VRF-A-af-ipv4] route-distinguisher 100:1
[*DS1-vpn-instance-VRF-A-af-ipv4] vpn-target 111:1 both
[*DS1-vpn-instance-VRF-A-af-ipv4] quit
[*DS1-vpn-instance-VRF-A] quit
[*DS1] interface vlanif 200
[*DS1-Vlanif200] ip binding vpn-instance VRF-A
[*DS1-Vlanif200] ip address 10.10.1.1 24
[*DS1-Vlanif200] quit
[*DS1] interface vlanif 300
[*DS1-Vlanif300] ip binding vpn-instance VRF-A
[*DS1-Vlanif300] ip address 10.10.2.1 24
[*DS1-Vlanif300] quit
[*DS1] ip route-static vpn-instance VRF-A 0.0.0.0 0.0.0.0 10.10.2.5
[*DS1] commit
```

3. 配置DS1至业务网段的静态路由，下一跳指向防火墙上行VRRP的虚拟IP。DS1与CS设备间运行OSPF，并在OSPF中引入静态路由。

```
[~HUAWEI] ip route-static 10.10.1.0 255.255.255.0 10.10.3.5
[*HUAWEI] ospf 100
[*HUAWEI-ospf-100] area 0
[*HUAWEI-ospf-100-area-0.0.0.0] network 10.10.4.0 0.0.0.255
[*HUAWEI-ospf-100-area-0.0.0.0] network 10.10.5.0 0.0.0.255
[*HUAWEI-ospf-100-area-0.0.0.0] quit
[*HUAWEI-ospf-100] import-route static
[*HUAWEI-ospf-100] quit
[*HUAWEI] commit
```

4. FW设备上完成基础配置，包括配置设备名，接口，IP地址等。此处略。
5. 在FW1上配置安全区域。

```
[FW1] firewall zone trust
[FW1-zone-trust] add interface eth-trunk 3
[FW1-zone-trust] quit
[FW1] firewall zone untrust
[FW1-zone-untrust] add interface eth-trunk 2
[FW1-zone-untrust] quit
[FW1] firewall zone dmz
[FW1-zone-dmz] add interface eth-trunk 1
[FW1-zone-dmz] quit
```

6. 在FW2上配置安全区域。

```
[FW2] firewall zone trust
[FW2-zone-trust] add interface eth-trunk 3
[FW2-zone-trust] quit
[FW2] firewall zone untrust
[FW2-zone-untrust] add interface eth-trunk 2
[FW2-zone-untrust] quit
[FW2] firewall zone dmz
[FW2-zone-dmz] add interface eth-trunk 1
[FW2-zone-dmz] quit
```

7. 在FW1上配置静态路由。内网访问外网的路由，缺省路由下一跳为交换机上连接防火墙上行接口的VLAN300的IP地址。外网访问内网的路由，目的地址为内网服务器网段，下一跳为交换机上连接防火墙下行接口的VLAN200的IP地址。

```
[FW1] ip route-static 0.0.0.0 0.0.0.0 10.10.3.1
[FW1] ip route-static 10.10.1.0 255.255.255.0 10.10.2.1
```

8. 在FW2上配置静态路由。

```
[FW2] ip route-static 0.0.0.0 0.0.0.0 10.10.3.1
[FW2] ip route-static 10.10.1.0 255.255.255.0 10.10.2.1
```

9. 在FW1上配置双机热备。

```
[FW1] interface eth-trunk 3
[FW1-Eth-Trunk3] vrrp vrid 1 virtual-ip 10.10.2.5 24 master
[FW1-Eth-Trunk3] quit
[FW1] interface eth-trunk 2
[FW1-Eth-Trunk2] vrrp vrid 2 virtual-ip 10.10.3.5 24 master
[FW1-Eth-Trunk2] quit
[FW1] hrp interface eth-trunk 1 remote 10.1.1.2
[FW1] firewall packet-filter default permit interzone local dmz
[FW1] hrp enable
```

10. 在FW2上配置双机热备。

```
[FW2] interface eth-trunk 3
[FW2-Eth-Trunk3] vrrp vrid 1 virtual-ip 10.10.2.5 24 slave
[FW2-Eth-Trunk3] quit
[FW2] interface eth-trunk 2
[FW2-Eth-Trunk2] vrrp vrid 2 virtual-ip 10.10.3.5 24 slave
[FW2-Eth-Trunk2] quit
[FW2] hrp interface eth-trunk 1 remote 10.1.1.1
[FW2] firewall packet-filter default permit interzone local dmz
[FW2] hrp enable
```

说明

双机热备功能配置完成后，主用设备的配置和会话会自动备份到备用设备上，因此以下功能只需在主用防火墙FW1上配置即可。

11. 配置安全策略和入侵防御。

说明

配置入侵防御功能前，需要保证入侵防御特征库已升级至最新的版本。

配置入侵防御功能时，通常使用默认存在的入侵防御配置文件default。

```
HRP_M[FW1] policy interzone trust untrust outbound
HRP_M[FW1-policy-interzone-trust-untrust-outbound] policy 1
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] policy source 10.10.1.0 mask 24
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] action permit
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] profile ips default
HRP_M[FW1-policy-interzone-trust-untrust-outbound-1] quit
HRP_M[FW1-policy-interzone-trust-untrust-outbound] quit
HRP_M[FW1] policy interzone trust untrust inbound
HRP_M[FW1-policy-interzone-trust-untrust-inbound] policy 1
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] policy destination 10.10.1.0 mask 24
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] policy service service-set ftp http
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] action permit
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] profile ips default
HRP_M[FW1-policy-interzone-trust-untrust-inbound-1] quit
HRP_M[FW1-policy-interzone-trust-untrust-inbound] quit
HRP_M[FW1] ips enable
```

12. 配置攻击防范。

说明

本举例中的攻击防范阈值仅供参考，实际配置时，请根据网络实际流量进行配置。

```
HRP_M[FW1] firewall defend syn-flood enable
HRP_M[FW1] firewall defend syn-flood zone untrust max-rate 20000
HRP_M[FW1] firewall defend udp-flood enable
HRP_M[FW1] firewall defend udp-flood zone untrust max-rate 1500
HRP_M[FW1] firewall defend icmp-flood enable
```

```
HRP_M[FW1] firewall defend icmp-flood zone untrust max-rate 20000
HRP_M[FW1] firewall blacklist enable
HRP_M[FW1] firewall defend ip-sweep enable
HRP_M[FW1] firewall defend ip-sweep max-rate 4000
HRP_M[FW1] firewall defend port-scan enable
HRP_M[FW1] firewall defend port-scan max-rate 4000
HRP_M[FW1] firewall defend ip-fragment enable
HRP_M[FW1] firewall defend ip-spoofing enable
```

13. 配置ASPF。此处以FTP协议为例，如果内网中还存在其他应用，就需要开启相应协议的ASPF功能。

```
HRP_M[FW1] firewall interzone trust untrust
HRP_M[FW1-interzone-trust-untrust] detect ftp
HRP_M[FW1-interzone-trust-untrust] quit
```

4 基于“云平台+敏捷控制器+硬件集中式 overlay”的数据中心网络部署方案

4.1 概述

4.1.1 简介

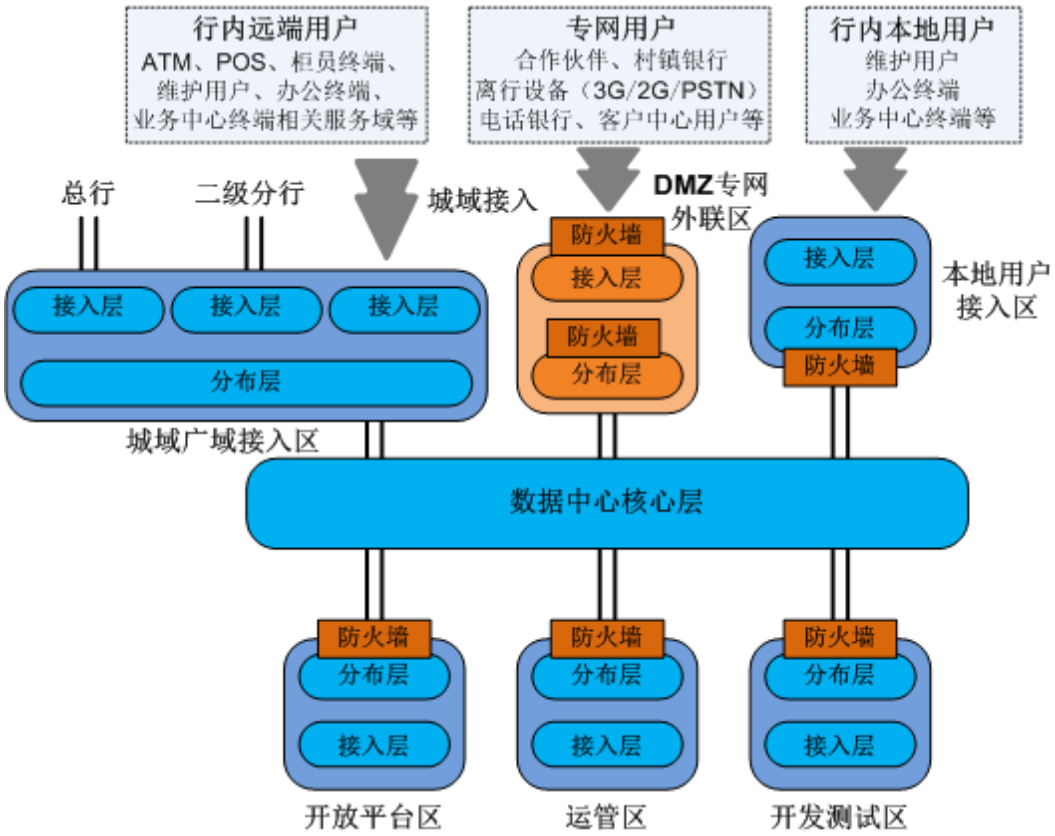
本文档是银行一级分行数据中心的详细设计方案，该方案全称为华为敏捷数据中心硬件Overlay组网（集中式网关）云网一体化方案，采用云平台和敏捷控制器对银行的网络进行集中控制。

本文档可用于项目的实施参考。

4.1.2 典型组网

4.1.2.1 逻辑架构

根据功能分区规划，一级分行数据中心网络逻辑拓扑架构如下图：



各功能区介绍如下：

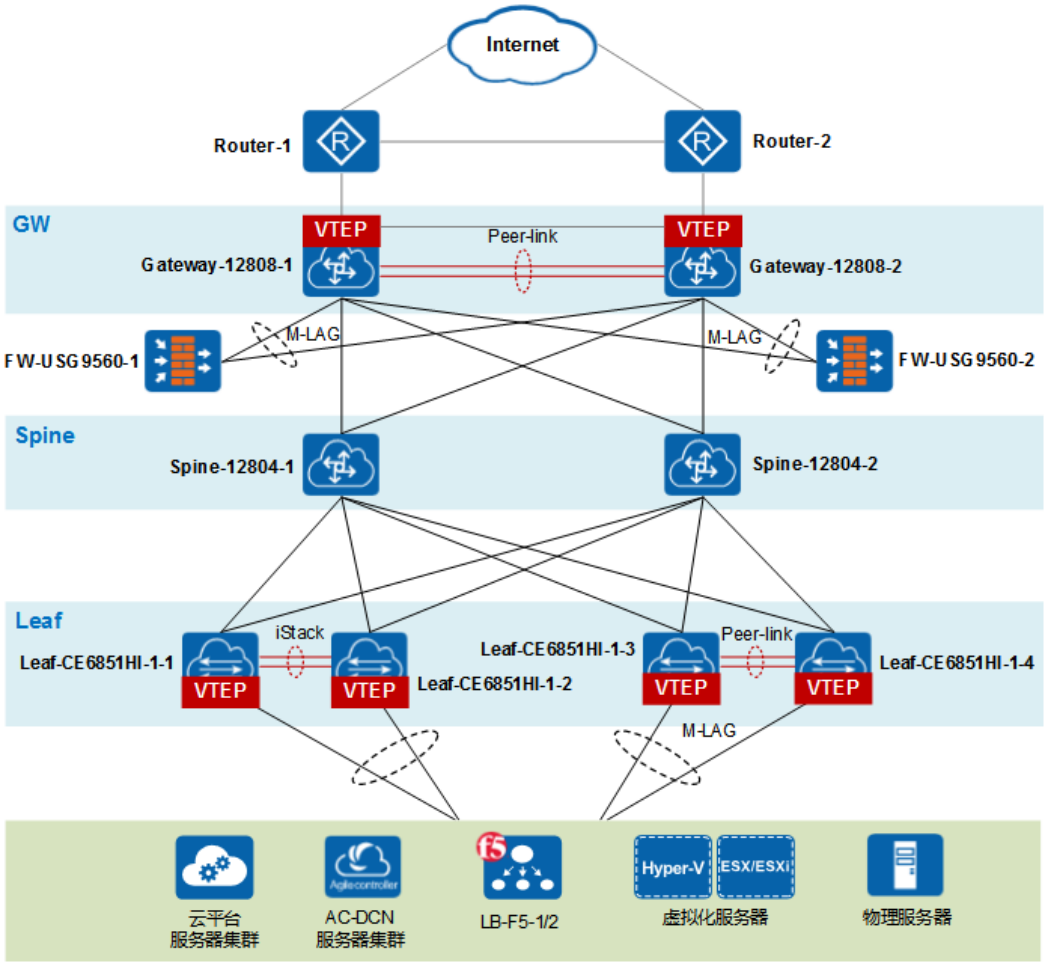
网络分区	分区功能和定位	接受访问
开放平台区：OP	已投产开放系统接入，通常包含直接动账、账目相关和非相关的业务。该区是最主要的业务区，满足生产、办公业务互访。	面向用户端和服务端。
运管区：OM	接入承载运行、监控和维护系统的服务器，用于对网络和系统进行管理及维护。	通常仅面向少数的授权维护用户。
开发测试区：DT	接入承载未投产业务系统的服务器，包括开发测试的主机和开放平台系统接入。	面向用户端和服务端。
城域广域接入区：WN/MN	实现一级分行上联总行与数据中心，下联二级分行与网点，以及与同城机构、分支网点的互联。从全行网络架构上分析，该区完成一级分行辖内区域的接入，包括一级分行局域网和辖内分支机构。	ATM、POS、柜员终端、维护用户、办公终端、业务中心终端等。
本地用户接入区：LU	满足各种类型用户终端接入。	本地维护用户、本地办公终端、本地业务中心终端。
DMZ专网外联区：EP	主要实现业务的外联，包括同行业的往来业务、重点客户的业务、中间代理业务等的平台互连，需要通过电信、联通等运营商提供的线路与合作伙伴互联。	合作伙伴、境外机构、离行设备（3G/2G/PSTN)、电话银行、客服中心用户。

“云平台+敏捷控制器+硬件集中式overlay”的数据中心网络部署方案与传统数据中心网络部署方案不同，该方案采用SDN技术实现计算、存储、网络的大规模资源池化，通过云平台对一级分行的网络进行统一管理，按照需要调用资源池中的资源实现各个分区的功能，能够更加灵活地部署网络并提高资源共享的利用率。

4.1.2.2 物理架构

本方案为三层架构有防火墙纳管方案，该方案的物理组网拓扑如图4-1所示。

图 4-1 三层架构有防火墙纳管方案物理组网图



- 服务器层：虚拟化服务器、物理服务器、云平台服务器、AC-DCN服务器通过Leaf节点交换机接入网络。
- Leaf：采用堆叠方式连接服务器，或采用M-LAG方式连接服务器。Leaf节点和Spine节点通过三层互联。Leaf的堆叠组或M-LAG组作为VTEP实现服务器流量接入VXLAN网络。
- Spine：分别与Leaf节点和GW互联，运行路由协议保证Underlay三层可达。Spine节点不作为VTEP。
- GW：两台GW之间组成M-LAG，即双活网关。GW与Spine之间三层互联。GW对外连接外部路由器Router-1和Router-2。
- FW：两台FW分别旁挂在GW，FW之间配置为主备镜像模式工作。
- LB：云平台纳管LB设备，LB设备由厂商部署。在SDN场景中LB是以二层方式接入到网络中，与实际处理业务的成员服务器共用VBDIF网关，所以推荐LB的部署方式与成员服务器的接入方式保持一致，便于运维。即两台LB以Eth-trunk方式接入到Leaf设备，LB的浮动IP与实际处理业务的成员服务器在相同子网，与成员服务器共用VBDIF网关。如果接入到GW且GW是CE12800系列，则需要配置FD/FDA系列单板和F/G类型交换网板。

4.1.3 版本配套关系

组网中涉及的产品及其配套关系，参见表4-1。

表 4-1 产品配套关系

类别		产品	Version
云平台		Fusionsphere OpenStack	V100R006C00 + V100R006C00SPC001
		OpenStack	Kilo
控制器		Agile Controller-DCN	V200R001C00SPC705
负载均衡设备		硬件F5 BIG-IP	软件版本：11.6.1 插件版本： ● 1.0.12.hw.fs.001（对接FusionSphere） ● 1.0.12.hw.os.001（对接OpenStack）
防火墙		Eudemon E8000E-X（运营商）	V500R002C00SPC300
		Eudemon E1000E-N（运营商）	V500R002C00SPC300
		USG6600	V500R001C30SPC300
		USG9500	V500R001C30SPC300
L3	集中式VXLAN网关	CE12800	V200R001C00SPC700 + V200R001SPH001
		CE7850/CE8860	V200R001C00SPC700
L2	TOR	CE7850/ CE6855HI / CE6851HI/CE6850HI	V200R001C00SPC700
	vSwitch	VDS	vSphere 6.0
		Hyper-V vSwitch	2012-R2
VMM		VMware vCenter	vSphere 6.0
		Microsoft System Center（与FusionSphere OpenStack云平台对接时不支持）	2012-R2
虚拟化		VMware ESX	vSphere 6.0
		Microsoft Hyper-V（与FusionSphere OpenStack云平台对接时不支持）	2012-R2

说明

AC-DCN控制器不纳管LB；FW当前只支持纳管华为产品，第三方厂家FW不支持纳管。

AC-DCN与FusionSphere OpenStack云平台对接时不支持Microsoft System Center。

4.1.4 方案约束限制

在本方案组网中有一些约束限制，请在设计网络时考虑这些因素。

解决方案相关

- 对接开源OpenStack时，不支持VPC间互通（VPC间只能通过EIP来互通）。
- 同一个POD中不支持CE交换机的V100R006版本和V200R001版本混用。
- OpenStack云平台和FusionSphere OpenStack云平台对接F5设备时：
  - 均不支持SSL offload模式的HTTPS服务的负载均衡服务。可采用默认的bypass模式的HTTPS负载分担服务。
  - 均不支持WRR权重调度，只支持RR轮询调度策略。
- AC-DCN不支持通过NETCONF给防火墙下发SNMP的用户名和密码配置，需手工在防火墙上配置SNMP的用户名和密码。

AC-DCN 相关

- 只支持纳管Admin-VS。
- 不支持双活以上的多活网关，支持多组双活网关。
- 不支持外部网络绑定到多个网关组。
- 不建议同时采用控制器方式和手工命令行方式进行组网部署，避免手工配置的命令与控制器下发的命令冲突，导致业务无法自动发放。
- 全互联场景（业务网关不配置VPN隔离）不支持租户子网的IP地址重叠，不支持配置防火墙和VPN业务。
- AC-DCN集群上的节点不能手工修改AC-DCN节点服务器的系统时间，如果修改系统时间，会导致不同AC-DCN节点的时间不同步（AC-DCN采用NTP同步系统时间），引发系统异常，需要在安装AC-DCN之前就部署NTP，完成时钟同步
- 不支持AC-DCN集群在线运行时进行扩容或减容操作，需要在网络建设期间规划好集群规模并完成部署。
- 在AC-DCN界面上添加F5设备时，每台F5设备的名称默认为“F5LBAAS”。如果F5设备名称不设置成“F5LBAAS”，会造成LB业务下发失败。
- 防火墙主备镜像模式下，AC-DCN纳管防火墙时不支持通过防火墙loopback口或管理口（Meth）纳管，AC-DCN需通过业务口（三层物理主接口或Eth-Trunk口）来纳管防火墙。
- 当虚拟机在网卡中配置多个IP时，AC-DCN页面只会显示其中一个，即AC-DCN只支持VM其中一个IP的单路径探测。
- 路径探测时只支持路径上是华为CE交换机，且这些CE交换机要支持VXLAN。
- AC-DCN的升级回退功能存在如下限制：版本升级后不能进行功能检查（如设备审计）或新业务下发，会导致版本回退后该功能不可用。建议按照升级手册重装升级前AC-DCN版本，通过恢复数据库实现回退。

防火墙相关

- 防火墙需要加载vsys功能的License。

- 支持防火墙以物理直挂集中式VXLAN L3网关方式进行组网，也支持物理旁挂方式组网。
- 防火墙支持无防火墙模式、支持1+1镜像模式（两台防火墙接口配置一样，备设备不提供服务），不支持防火墙通过VRRP切换的1+1主备模式，不支持1+1双活部署方式。
- 不支持部署软件分布式防火墙。
- 云网一体化场景不支持防火墙旁挂Service Leaf，只支持防火墙旁挂网关。

负载均衡相关

负载均衡设备（F5）在云网一体化场景中，安装插件后可以被Fusionsphere OpenStack和开源OpenStack云平台纳管。

负载均衡设备只支持二层方式接入。当CE12800设备仅配置了FD/FDA类型接口板，且仅配置了F/G类型交换网板时，负载均衡设备可以旁挂接入到VXLAN L3网关上，否则只支持接入到Service Leaf或Spine设备。

CE 交换机相关

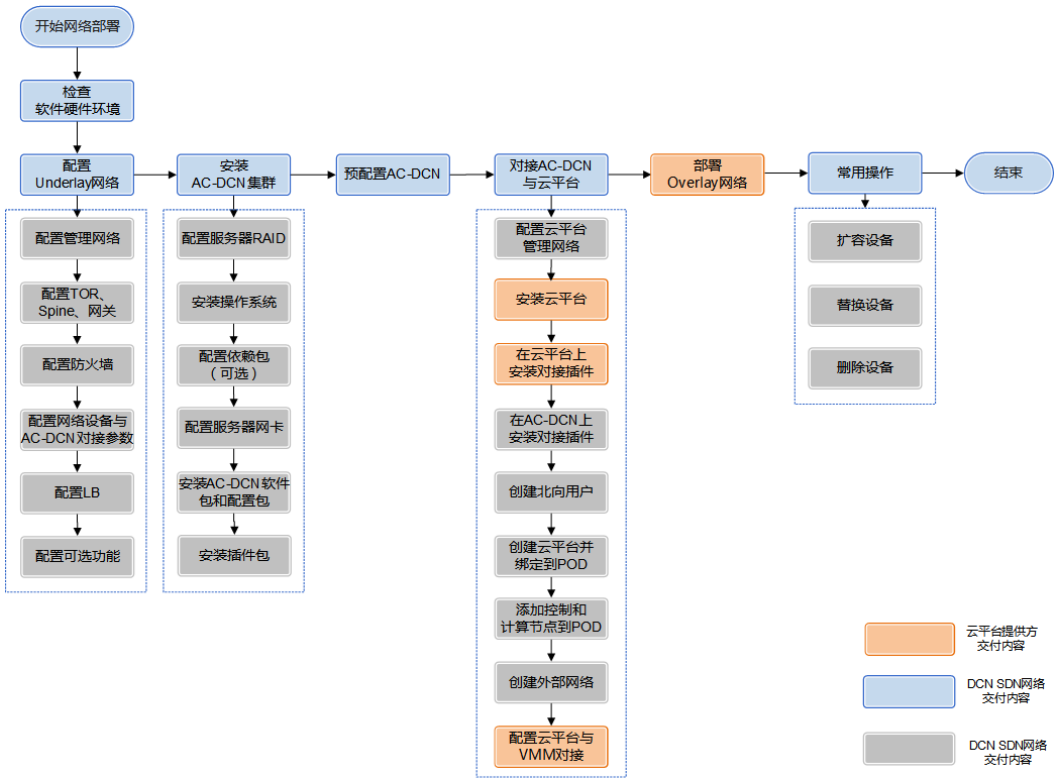
- CE12800系列交换机部署VXLAN不需要License。CE8800\CE7800\CE6800系列交换机部署VXLAN需要加载License。
- CE设备不支持对VXLAN报文进行分片或重组。当VXLAN网络中同时存在CE和非CE系列设备共同组网时，为了避免VXLAN报文在非CE设备上进行了分片，而CE设备无法将其重组造成的转发失败问题，建议在服务器上配置报文的最大帧长不超过1400字节或者VXLAN报文经过的非CE设备将MTU值调大。
- CE设备不支持同一台设备上对报文进行VXLAN封装后再进行MPLS封装，也不支持对报文进行MPLS解封装后再进行VXLAN解封装，组网方案上可以规避，即在设备A上VXLAN封装后转发到设备B后行MPLS封装。
- EA和GE单板不推荐与EC\ED\EF\EG\FD\FDA单板混插且部署VXLAN业务（会导致该设备上所有EA\EC\ED\EF\EG\GE单板转发VXLAN报文的性能下降50%左右），部署传统VLAN业务没有影响。
- TOR盒式交换机做VxLAN三层网关时推荐使用CE7855EI和CE6870EI，CE8860EI\CE7850EI\CE6850HI\CE6851HI\CE6850UHI做VxLAN三层网关时需要规划部分业务端口配置为外部环回口，这部分业务端口不能用于其他业务，不需要插光模块和连线，环回接口的带宽至少是VxLAN三层网关流量所占带宽2倍，CE7855和CE6855不需要外部环回口。
- AC-DCN纳管防火墙场景中，不支持CE6855单机、堆叠或者SVF（父交换机）作为VXLAN L3网关（原因：CE6855做L3网关时，产品约束限制上行口与FW、路由器等设备对接不能用VLANIF或主接口，需要使用VBDIF接口，而AC-DCN纳管防火墙时，会自动在接口下配置VLAN和创建VLANIF对接），推荐使用CE7855或者CE6870。
- EC\ED\EF\EG单板不支持VxLAN二三层混跑(在GW上同时存在VXLAN二层子接口接入和VXLAN隧道接入，其中隧道侧的BD在GW上有网关vBDIF），可以通过命令行调整为环回模式来支持此场景，但会导致EC\ED\EF\EG单板转发VXLAN报文的性能下降50%左右。
- 盒盒SVF作为Leaf时只支持VTEP到VTEP路径的探测，不支持VM到VM的路径探测，不建议CE5810EI作为盒盒SVF的叶子，推荐CE5855EI作为叶子给服务器以千兆口接入。
- 三层网络架构，中间Spine也必须为华为设备，否则会导致AC路径探测等运维功能不可用。

4.2 网络部署

4.2.1 网络部署全景图

完成硬件设备的安装、连线后，网络工程师开始网络层面的部署。在网络部署阶段，主要的流程如图4-2所示。

图 4-2 网络部署主要流程图



各阶段任务简介参见表4-2。

表 4-2 网络部署阶段任务一览

任务	说明
检查软硬件环境	检查硬件和软件的版本、License是否与规划的配套，如果不匹配需要升级或更换。
Underlay网络部署	配置管理网络以及Fabric基础组网，使AC-DCN能纳管Fabric网络。
安装AC-DCN	在物理服务器集群上安装AC-DCN软件。
预配置AC-DCN	激活AC-DCN的license，发现资源并创建POD，对资源进行预配置，为Overlay网络部署做准备。

任务	说明
对接AC-DCN与云平台	在AC-DCN和云平台两侧分别进行对接配置，使两者对接成功，为Overlay网络部署做准备。
部署Overlay网络	根据具体业务需求，在云平台提供的Portal上进行业务的创建和下发。
常用操作	根据业务实际需求，在AC-DCN的协助下完成设备的扩容、替换和删除的操作。

4.2.2 检查软硬件环境

在进行部署前，需要根据4.1.3 版本配套关系检查现场的硬件设备和软件的版本号及补丁是否符合要求。如不符合要求，请在部署前更换或升级设备。

检查 CE 交换机版本、License 和运行状态

步骤1 执行命令**display version**，查看CE交换机版本号。

```
<HUAWEI> display version   //查看设备配套版本是否是V200R001C00SPC700
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.13 (CE12800 V200R001C00SPC700)
Copyright (C) 2012-2016 Huawei Technologies Co., Ltd.
HUAWEI CE12804 uptime is 0 day, 1 hour, 55 minutes

<HUAWEI> display patch-information   //查看设备是否加载最新补丁
Patch Package Name    :flash:/CE12800-V200R001SPH003.PAT
Patch Package Version : V200R001SPH003
Patch Package State   :Running    //查看补丁是否是Running状态
Patch Package Run Time:2016-11-09 17:57:27
```

步骤2 执行命令**display license**，查看CE交换机License信息。

```
<HUAWEI> display license //CE12800不需要VXLAN的license，TOR需要
MainBoard:
 Active License    : flash:/CloudEngine7800.dat
 License state     : Demo
 Revoke ticket     : No ticket
 RD of Huawei Technologies Co., Ltd.
 Product name      : CloudEngine 7800
 Product version   : V200R001
 License Serial No : LIC201411261KSH50
 Creator           : Huawei Technologies Co., Ltd.
 Created Time      : 2016-11-09 17:57:27
 Feature name      : CELIC
 Authorize type    : demo
 Expired date      : 2017-02-20
 Trial days        : -

 Item name          Item type      Value      Description
 ------------------------------------------------------------
 CE-LIC-VXLAN       Function       YES          CE-LIC-VXLAN
```

步骤3 执行命令**display device**（查看单板注册状态是否正常）和**display alarm active**（查看设备当前active的告警信息），查看CE交换机运行状态。

```
<HUAWEI> display device    //查看设备状态，当“Register”列为“Registered”、“Alarm”列为“Normal”时，状态正常。

CE12804's Device status:
--------------------------------------------------------------------------
Slot  Card   Type                Online   Power Register     Alarm     Primary
```

```
------------------------------------------------------------------
3     -      CE-L24LQ-EA          Present  On    Registered   Normal    NA
4     -      CE-L24XS-EA          Present  On    Registered   Normal    NA
5     -      CE-MPUA              Present  On    Registered   Normal    Master
7     -      CE-CMUA              Present  On    Registered   Normal    Master
13    -      CE-SFU04C            Present  On    Registered   Normal    NA
PWR2  -      -                    Present  On    Registered   Normal    NA
FAN3  -      -                    Present  On    Registered   Normal    NA
FAN4  -      -                    Present  On    Registered   Normal    NA
FAN5  -      -                    Present  On    Registered   Normal    NA
FAN7  -      -                    Present  On    Registered   Normal    NA
FAN8  -      -                    Present  On    Registered   Normal    NA
FAN9  -      -                    Present  On    Registered   Normal    NA
------------------------------------------------------------------
<HUAWEI> display alarm active
------------------------------------------------------------------
Sequence   AlarmId    Severity Date Time  Description
------------------------------------------------------------------
20         0x8520003  Major    2013-12-26 The interface status changes. (ifName=
                               09:10:31  Eth-Trunk19, AdminStatus=UP, OperStatu
                                         s=DOWN, Reason=The conditions for the
                                         activation of the interface are not me
                                         t, mainName=Eth-Trunk19)
------------------------------------------------------------------
```

----结束

检查防火墙版本、License 和运行状态

步骤1 执行命令**display version**，查看防火墙版本号：

```
<USG9000> display version   //查看设备配套版本是否正确
Huawei Technologies Versatile Security Platform Software
Software Version: USG9520&9560&9580 V500R001C30 (VRP (R) Software, Version
5.70)
Copyright (C) 2007-2013 Huawei Technologies Co., Ltd. All rights reserved.
Secospace USG9580 uptime is 0 day, 23 hours, 35 minutes
USG9580 version information:

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

步骤2 执行命令**display license**，查看防火墙License信息：

```
<USG9000> display license     //查看是否开启vsys功能
MainBoard:
Device ESN is: 030KKR10B1003130
The file activated is: cfcard:/license.dat
The time when activated is: 2014/04/08  10:11:47
Firewall default Performance per cpu: 40Gbps
Number of VPN Tunnels-R: 1000000
Number of Virtual Systems: 4095
GTP: Enable
6RD Session Scale: 1280M
NAT64 Session Scale: 1280M
DS-Lite Session Scale: 1280M
Firewall Upgrade Additional Performance: 1280Gbps
Expiration Date of The IPS Update Service: 2014-05-18
SlaveBoard:
Device ESN is: 030KKR10B1000131
The file activated is: cfcard:/license.dat
The time when activated is: 2014/04/08  10:11:47
Firewall default Performance per cpu: 40Gbps
Number of VPN Tunnels-R: 1000000
Number of Virtual Systems: 4095
GTP: Enable
6RD Session Scale: 1280M
NAT64 Session Scale: 1280M
DS-Lite Session Scale: 1280M
Firewall Upgrade Additional Performance: 1280Gbps
Expiration Date of The IPS Update Service: 2014-05-18
```

步骤3 执行命令**display device**（查看单板注册状态是否正常） 和**display alarm all**（查看设备当前active的告警信息），查看防火墙运行状态。

```
<USG9000> display device  //查看设备状态，当“Register”列为“Registered”、“Alarm”列为“Normal”时，状态正常。
USG9580's Device status:
Slot #    Type       Online    Register      Status      Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1         LPU        Present   Registered    Normal      NA
5         LPU        Present   Registered    Normal      NA
6         SPU        Present   Registered    Normal      NA
9         MPU        Present   Registered    Normal      Master
10        MPU        Present   Registered    Normal      Slave
13        SFU        Present   Registered    Normal      NA
14        SFU        Present   Registered    Normal      NA
15        CLK        Present   Registered    Normal      Master
16        CLK        Present   Registered    Normal      Slave
17        PWR        Present   Registered    Normal      NA
19        FAN        Present   Registered    Normal      NA
<USG9000> display alarm all
------------------------------------------------------------------------------
Index  Level      Date      Time                        Info

1      Emergency  11-07-05  11:25:40    The 48 V power supply for the board was abnormal.[LPU 5]
```

----结束

检查 AC-DCN 软件包

通常情况下，AC-DCN的软件包包含以下文件：

- 操作系统镜像文件（.iso）
- AC-DCN安装包（Install_Pkg）
- AC-DCN配置包（Config_Pkg）
- AC-DCN对接云平台插件（eSDK）
- 云平台对接插件（OPS&FSP_Plugin）
- Breeze_iDeploy安装工具
- 上述每个文件的签名验证文件（.asc）

步骤1 检查下载的软件版本号是否准确。

步骤2 推荐使用华为发布的PGPVerify工具验证文件的完整性，本步骤请参考**《使用华为PGPVerify工具验证文件签名》**。

----结束

4.2.3 部署 Underlay 网络

4.2.3.1 配置管理网络

管理网络分为带外管理和带内管理两种：

- 带外管理：采用设备专用的管理口进行设备管理，此方式管控分离，推荐使用带外管理的方式。

  以带外管理为例，客户管理VLAN ID为20，需要配置带外管理的网络设备主要有交换机、防火墙、LB。将网络设备的管理口接入客户的管理交换机，根据规划好

的管理地址分别配置交换机的管理网口，方便后续远程登录。管理口配置及各网元的登录设置请参考各产品的产品文档。

AC-DCN服务器带外管理是将AC-DCN服务器的BMC口接入客户的管理交换机，并分别设置BMC口的IP地址、掩码和管理网段网关，后续可以远程登录。其他服务器管理网段的设置与AC-DCN服务器类似。

- 带内管理：使用设备的业务口进行设备管理，此方式的弊端是如果业务网络出现问题，可能会影响设备登录。

  网络设备的带内管理方式不需要增加额外成本。在本场景示例中，每台设备规划的路由Router-ID的Loopback地址就可以作为带内管理IP地址使用，本文就不再单独举例说明。

4.2.3.2 配置 TOR 堆叠工作组

Leaf-CE6851HI-1和Leaf-CE6851HI-2组成堆叠组，相关配置思路如下：

1. 组建堆叠组：配置堆叠和双主检测，并重启设备、连接线缆，使堆叠生效。
2. 配置IP地址：配置Leaf与Spine的三层互联接口地址、Loopback0地址（作为Router-ID和VTEP IP）、管理口（Meth0/0/0）IP地址、VTEP IP地址。
3. 配置服务器接入：介绍业务服务器和AC-DCN服务器接入堆叠组时，堆叠组交换机上的配置。
4. 配置路由：在堆叠组上配置BGP动态路由，邻居为两个Spine设备，使堆叠组上的网段与Spine上的网段三层可达。

组建堆叠组

步骤1 配置Leaf-CE6851HI-1的堆叠成员ID为1，优先级为150，Domain ID为10。

```
<HUAWEI> system-view
[~HUAWEI] sysname Leaf-CE6851HI-1
[*HUAWEI] commit
[~Leaf-CE6851HI-1] stack
[~Leaf-CE6851HI-1-stack] stack member 1 priority 150
[*Leaf-CE6851HI-1-stack] stack member 1 domain 10
[*Leaf-CE6851HI-1-stack] quit
[*Leaf-CE6851HI-1] commit
```

步骤2 配置Leaf-CE6851HI-2的Domain ID为10。

```
<HUAWEI> system-view
[~HUAWEI] sysname Leaf-CE6851HI-2
[*HUAWEI] commit
[~Leaf-CE6851HI-2] stack
[~Leaf-CE6851HI-2-stack] stack member 1 renumber 2 inherit-config
[*Leaf-CE6851HI-2-stack] stack member 1 domain 10
[*Leaf-CE6851HI-2-stack] quit
[*Leaf-CE6851HI-2] commit
```

步骤3 配置堆叠端口。

将Leaf-CE6851HI-1的业务口40GE1/0/1～40GE1/0/2加入堆叠端口1/1。

```
[~Leaf-CE6851HI-1] interface stack-port 1/1
[*Leaf-CE6851HI-1-Stack-Port1/1] port member-group interface 40ge 1/0/1 to 1/0/2
Warning: The interface(s) (40GE1/0/1-1/0/2) will be converted to stack mode and be configured with
the port crc-statistics trigger error-down command if the configuration does not exist. After the
configuration is complete, these interfaces may go Error-Down (crc-statistics) because there is no
shutdown configuration on the interfaces. [Y/N]: y
[*Leaf-CE6851HI-1-Stack-Port1/1] quit
[*Leaf-CE6851HI-1] commit
[~Leaf-CE6851HI-1] quit
```

将Leaf-CE6851HI-2的业务口40GE1/0/1～40GE1/0/2加入堆叠端口1/1。

```
[~Leaf-CE6851HI-2] interface stack-port 1/1
[*Leaf-CE6851HI-2-Stack-Port1/1] port member-group interface 40ge 1/0/1 to 1/0/2
Warning: The interface(s) (40GE1/0/1-1/0/2) will be converted to stack mode and be configured with
the port crc-statistics trigger error-down command if the configuration does not exist. After the
configuration is complete, these interfaces may go Error-Down (crc-statistics) because there is no
shutdown configuration on the interfaces. [Y/N]: y
[*Leaf-CE6851HI-2-Stack-Port1/1] quit
[*Leaf-CE6851HI-2] commit
[~Leaf-CE6851HI-2] quit
```

步骤4 保存配置后重启设备。

保存Leaf-CE6851HI-1的配置，然后重启设备。其他TOR的操作与之类似，不再赘述。

```
<Leaf-CE6851HI-1> save
Warning: The current configuration will be written to the device. Continue? [Y/N]: y
<Leaf-CE6851HI-1> reboot
Warning: The system will reboot. Continue? [Y/N]:y
```

步骤5 连接堆叠线缆，建立堆叠。

步骤6 堆叠组建后执行命令**save**保存配置。

步骤7 堆叠建立后，配置堆叠组的双主检测，防止堆叠组分裂后网络中存在两个配置冲突的网络设备。

带外管理时，可配置基于管理口的双主检测。

```
[~Leaf-CE6851HI-1] sysname Leaf-CE6851HI-1&CE6851HI-2
[*Leaf-CE6851HI-1] commit
[~Leaf-CE6851HI-1&CE6851HI-2] interface Meth0/0/0
[~Leaf-CE6851HI-1&CE6851HI-2-MEth0/0/0] dual-active detect enable
[*Leaf-CE6851HI-1&CE6851HI-2-MEth0/0/0] commit
```

带内管理时，可采用业务口直连的方式配置双主检测，建议规划的直连链路至少2条，保证可靠性，配置示例如下。

```
[~Leaf-CE6851HI-1] sysname Leaf-CE6851HI-1&CE6851HI-2
[*Leaf-CE6851HI-1] commit
[~Leaf-CE6851HI-1&CE6851HI-2] interface 10GE1/0/30
[~Leaf-CE6851HI-1&CE6851HI-2-10GE1/0/30] description "for DAD"
[*Leaf-CE6851HI-1&CE6851HI-2-10GE1/0/30] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue? [Y/N]: y
[*Leaf-CE6851HI-1&CE6851HI-2-10GE1/0/30] quit
[*Leaf-CE6851HI-1&CE6851HI-2] interface 10GE1/0/31
[*Leaf-CE6851HI-1&CE6851HI-2-10GE1/0/31] description "for DAD"
[*Leaf-CE6851HI-1&CE6851HI-2-10GE1/0/31] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue? [Y/N]: y
[*Leaf-CE6851HI-1&CE6851HI-2-10GE1/0/31] quit
[*Leaf-CE6851HI-1&CE6851HI-2] interface 10GE2/0/30
[*Leaf-CE6851HI-1&CE6851HI-2-10GE2/0/30] description "for DAD"
[*Leaf-CE6851HI-1&CE6851HI-2-10GE2/0/30] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue? [Y/N]: y
[*Leaf-CE6851HI-1&CE6851HI-2-10GE2/0/30] quit
[*Leaf-CE6851HI-1&CE6851HI-2] interface 10GE2/0/31
[*Leaf-CE6851HI-1&CE6851HI-2-10GE2/0/31] description "for DAD"
[*Leaf-CE6851HI-1&CE6851HI-2-10GE2/0/31] dual-active detect mode direct
Warning: The interface will block common data packets, except BPDU packets. Continue? [Y/N]: y
[*Leaf-CE6851HI-1&CE6851HI-2-10GE2/0/31] commit
[~Leaf-CE6851HI-1&CE6851HI-2-10GE2/0/31] quit
```

----结束

配置 IP 地址

步骤1 配置互连接口地址。

说明

对于CE6855HI和CE7855EI，在切换三层接口之前，要先配置**vlan reserved for main-interface startvlanid to endvlanid**，配置三层主接口专用的保留VLAN。

```
[~Leaf-CE6851HI-1] sysname Leaf-CE6851HI-1&CE6851HI-2
[*Leaf-CE6851HI-1] commit
[~Leaf-CE6851HI-1&CE6851HI-2] interface 40GE1/0/3
[~Leaf-CE6851HI-1&CE6851HI-2] description "to_Spine-CE12804-1-40GE1/0/0"
[~Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/3]undo portswitch
[*Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/3]ip address 11.254.40.157 30
[*Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/3]commit
[~Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/3]quit
[~Leaf-CE6851HI-1&CE6851HI-2] interface 40GE1/0/4
[~Leaf-CE6851HI-1&CE6851HI-2] description "to_Spine-CE12804-2-40GE1/0/1"
[~Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/4] undo portswitch
[*Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/4]ip address 11.254.40.165 30
[*Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/4]commit
[~Leaf-CE6851HI-1&CE6851HI-2-40GE1/0/4]quit
[~Leaf-CE6851HI-1&CE6851HI-2] interface 40GE2/0/3
[~Leaf-CE6851HI-1&CE6851HI-2] description "to_Spine-CE12804-2-40GE1/0/0"

[~Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/3]undo portswitch
[*Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/3]ip address 11.254.40.161 30
[*Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/3]commit
[~Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/3]quit
[~Leaf-CE6851HI-1&CE6851HI-2] interface 40GE2/0/4
[~Leaf-CE6851HI-1&CE6851HI-2] description "to_Spine-CE12804-1-40GE1/0/1"
[~Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/4] undo portswitch
[*Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/4]ip address 11.254.40.169 30
[*Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/4]commit
[~Leaf-CE6851HI-1&CE6851HI-2-40GE2/0/4]quit
```

步骤2 配置Loopback口地址。

```
[~Leaf-CE6851HI-1&CE6851HI-2] interface loopback0
[~Leaf-CE6851HI-1&CE6851HI-2] description "VTEP&Router-ID"
[*Leaf-CE6851HI-1&CE6851HI-2-LoopBack0] ip address 11.11.11.1132
[*Leaf-CE6851HI-1&CE6851HI-2-LoopBack0] commit
[~Leaf-CE6851HI-1&CE6851HI-2-LoopBack0] quit
```

步骤3 配置管理口地址。

```
[~Leaf-CE6851HI-1&CE6851HI-2] interface Meth0/0/0
[*Leaf-CE6851HI-1&CE6851HI-2-Meth0/0/0] ip address 100.125.94.2 24
[*Leaf-CE6851HI-1&CE6851HI-2-Meth0/0/0] dual-active backup ip address 100.125.94.20 member 2  //配置备交换机的Meth0/0/0口的备份地址，当堆叠分裂时，备交换机的Meth/0/0/0口使用此地址，不会和主交换机的Meth0/0/0地址冲突
[*Leaf-CE6851HI-1&CE6851HI-2-Meth0/0/0] commit
[~Leaf-CE6851HI-1&CE6851HI-2-Meth0/0/0] quit
```

步骤4 配置VTEP地址。

```
[~Leaf-CE6851HI-1&CE6851HI-2] interface NVE1
[*Leaf-CE6851HI-1&CE6851HI-2-Nve1] source11.11.11.11
[*Leaf-CE6851HI-1&CE6851HI-2-Nve1] commit
[~Leaf-CE6851HI-1&CE6851HI-2-Nve1] quit
```

----结束

配置服务器接入

介绍业务服务器和AC-DCN服务器接入堆叠组时，堆叠组交换机上的配置。

步骤1 在Leaf-CE6851HI-1与Leaf-CE6851HI-2上配置普通业务服务器接入示例。

普通业务服务器以负载均衡模式接入堆叠组。

```
[*Leaf-CE6851HI-1&CE6851HI-2] interface eth-trunk 1
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk1] mode lacp-static
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk1] port link-type trunk
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk1] undo port trunk allow-pass vlan 1
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk1] trunkport 10ge 1/0/1
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk1] trunkport 10ge 2/0/1
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk1] quit
[*Leaf-CE6851HI-1&CE6851HI-2] commit
```

普通业务服务器以主备模式接入堆叠组时，只需要连接好物理网线即可，接口下的配置全部由AC-DCN下发。

步骤2 如果AC-DCN服务器通过堆叠组TOR接入配置如下。如果AC-DCN服务器通过M-LAG接入，则参见2.4.3.3 配置TOR M-LAG工作组。

1. 配置AC-DCN的业务网关地址。

```
[~Leaf-CE6851HI-1&CE6851HI-2] VLAN 10
[*Leaf-CE6851HI-1&CE6851HI-2-vlan10] interface vlanif 10
[*Leaf-CE6851HI-1&CE6851HI-2-Vlanif10] ip address 100.125.100.2 24
[*Leaf-CE6851HI-1&CE6851HI-2-Vlanif10] commit
```

2. 在Leaf-CE6851HI-1与Leaf-CE6851HI-2上配置AC-DCN服务器接入（以负载均衡模式为例）。

```
[*Leaf-CE6851HI-1&CE6851HI-2] interface eth-trunk 100
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk100] mode lacp-static
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk100] port default vlan 10
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk100] trunkport 10ge 1/0/46
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk100] trunkport 10ge 2/0/46
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk100] quit
[*Leaf-CE6851HI-1&CE6851HI-2] commit

[*Leaf-CE6851HI-1&CE6851HI-2] interface eth-trunk 101
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk101] mode lacp-static
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk101] port default vlan 10
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk101] trunkport 10ge 1/0/47
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk101] trunkport 10ge 2/0/47
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk2] quit
[*Leaf-CE6851HI-1&CE6851HI-2] commit

[*Leaf-CE6851HI-1&CE6851HI-2] interface eth-trunk 102
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk102] mode lacp-static
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk102] port default vlan 10
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk102] trunkport 10ge 1/0/48
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk102] trunkport 10ge 2/0/48
[*Leaf-CE6851HI-1&CE6851HI-2-Eth-Trunk102] quit
[*Leaf-CE6851HI-1&CE6851HI-2] commit
```

----结束

配置路由

在堆叠组上配置BGP路由，对接Spine。

```
[~Leaf-CE6851HI-1&CE6851HI-2] BGP 65021
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] router-id 11.11.11.11
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] timer keepalive 10 hold 30
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] group Spine-CE12804-1 external
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer Spine-CE12804-1 as-number 65009
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.158 as-number 65009
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.158 group_Spine-CE12804-1
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.170 as-number 65009
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.170 group Spine-CE12804-1
```

```
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] group Spine-CE12804-2 external
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer Spine-CE12804-2 as-number 65010
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.166 as-number 65010
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.166 group Spine-CE12804-2
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.162 as-number 65010
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] peer 11.254.40.162 group Spine-CE12804-2
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] ipv4-family unicast
[*Leaf-CE6851HI-1&CE6851HI-2-bgp-af-ipv4] preference 20 200 10
[*Leaf-CE6851HI-1&CE6851HI-2-bgp-af-ipv4] network 11.11.11.11 255.255.255.255
[*Leaf-CE6851HI-1&CE6851HI-2-bgp-af-ipv4] network 100.125.100.0 255.255.255.0   //如果AC-DCN通过此堆叠组接入，且在堆叠组上配置了业务网段，则需在BGP中发布AC-DCN的网段
[*Leaf-CE6851HI-1&CE6851HI-2-bgp-af-ipv4] maximum load-balancing 32
[*Leaf-CE6851HI-1&CE6851HI-2-bgp-af-ipv4] quit
[*Leaf-CE6851HI-1&CE6851HI-2-bgp] quit
[*Leaf-CE6851HI-1&CE6851HI-2] commit
```

说明

如果需要从外部网络访问到AC-DCN服务器，则需要在TOR上配置静态路由或动态路由，将AC-DCN服务器的业务地址发布出去，保证外部网络有访问AC-DCN服务器的路由，同时需要保证TOR上有到外部网络的路由。

4.2.3.3 配置 TOR M-LAG 工作组

在Leaf-CE6851HI-3和CE6851HI-4上配置M-LAG，相关配置思路如下：

1. 配置IP地址：配置Leaf交换机与Spine的三层互联接口地址、Loopback0地址（作为VTEP IP）、Loopback1地址（作为Router-ID）、管理口（Meth0/0/0）IP地址、VTEP IP地址（两台设备设置相同）、AC-DCN的网关地址（如果AC-DCN通过此M-LAG接入）。
2. 配置M-LAG：在交换机上配置M-LAG全局模式、DFS组、Peer-Link，并分别配置普通业务服务器和AC-DCN服务器接入M-LAG，配置Monitor Link关联上行接口和下行接口。
3. 配置路由：在M-LAG组上配置BGP动态路由，邻居为两个Spine设备，使堆叠组上的网段与Spine上的网段三层可达。

配置 IP 地址

步骤1 配Leaf-CE6851HI-3与Leaf-CE6851HI-4直连接口地址。

说明

对于CE6855HI和CE7855EI，在切换三层接口之前，要先配置命令**vlan reserved for main-interface** *startvlanid* **to** *endvlanid*，配置三层主接口专用的保留VLAN。

```
[~HUAWEI] sysname Leaf-CE6851HI-3
[*Leaf-CE6851HI-3] commit
[~Leaf-CE6851HI-3] interface 40GE1/0/3
[~Leaf-CE6851HI-3-40GE1/0/3] description "to_Spine-CE12804-1-40GE1/0/2"
[~Leaf-CE6851HI-3-40GE1/0/3] undo portswitch
[*Leaf-CE6851HI-3-40GE1/0/3] ip address 11.254.41.157 30
[*Leaf-CE6851HI-3-40GE1/0/3] commit
[~Leaf-CE6851HI-3-40GE1/0/3] quit
[~Leaf-CE6851HI-3] interface 40GE1/0/4
[~Leaf-CE6851HI-3-40GE1/0/3] description "to_Spine-CE12804-2-40GE1/0/3"
[~Leaf-CE6851HI-3-40GE1/0/4] undo portswitch
[*Leaf-CE6851HI-3-40GE1/0/4] ip address 11.254.41.165 30
[*Leaf-CE6851HI-3-40GE1/0/4] commit
[~Leaf-CE6851HI-3-40GE1/0/4] quit

[~HUAWEI] sysname Leaf-CE6851HI-4
[*Leaf-CE6851HI-4] commit
[~Leaf-CE6851HI-4] interface 40GE1/0/3
[~Leaf-CE6851HI-4-40GE1/0/3] description "to_Spine-CE12804-1-40GE1/0/2"
```

```
[~Leaf-CE6851HI-4-40GE1/0/3] undo portswitch
[*Leaf-CE6851HI-4-40GE1/0/3] ip address 11.254.41.169 30
[*Leaf-CE6851HI-4-40GE1/0/3] commit
[~Leaf-CE6851HI-4-40GE1/0/3] quit
[~Leaf-CE6851HI-4] interface 40GE1/0/4
[~Leaf-CE6851HI-4-40GE1/0/3] description "to_Spine-CE12804-2-40GE1/0/3"
[~Leaf-CE6851HI-4-40GE1/0/4] undo portswitch
[*Leaf-CE6851HI-4-40GE1/0/4] ip address 11.254.41.161 30
[*Leaf-CE6851HI-4-40GE1/0/4] commit
[~Leaf-CE6851HI-4-40GE1/0/4] quit
```

步骤2 配Loopback口地址，规划用Loopback0地址作为VTEP，用Loopback1地址作为Router-ID。

```
[~Leaf-CE6851HI-3] interface loopback0    //作为VTEP地址
[*Leaf-CE6851HI-3-LoopBack0] ip address 11.11.11.12 32
[*Leaf-CE6851HI-3-LoopBack0] commit
[~Leaf-CE6851HI-3-LoopBack0] quit
[~Leaf-CE6851HI-3] interface loopback1
[*Leaf-CE6851HI-3-LoopBack1] ip address 13.13.13.13 32
[*Leaf-CE6851HI-3-LoopBack1] commit
[~Leaf-CE6851HI-3-LoopBack1] quit

[~Leaf-CE6851HI-4] interface loopback0     //作为VTEP地址
[*Leaf-CE6851HI-4-LoopBack0] ip address 11.11.11.12 32
[*Leaf-CE6851HI-4-LoopBack0] commit
[~Leaf-CE6851HI-4-LoopBack0] quit
[~Leaf-CE6851HI-4] interface loopback1
[*Leaf-CE6851HI-4-LoopBack1] ip address 14.14.14.14 32
[*Leaf-CE6851HI-4-LoopBack1] commit
[~Leaf-CE6851HI-4-LoopBack1] quit
```

步骤3 配置管理口地址。

```
[~Leaf-CE6851HI-3] interface Meth0/0/0
[*Leaf-CE6851HI-3- Meth0/0/0] ip address 100.125.94.3 24
[*Leaf-CE6851HI-3- Meth0/0/0] commit
[~Leaf-CE6851HI-3- Meth0/0/0] quit

[~Leaf-CE6851HI-4] interface Meth0/0/0
[*Leaf-CE6851HI-4- Meth0/0/0] ip address 100.125.94.4 24
[*Leaf-CE6851HI-4- Meth0/0/0] commit
[~Leaf-CE6851HI-4- Meth0/0/0] quit
```

步骤4 配置VTEP地址，两台设备设置一致。

```
[~Leaf-CE6851HI-3] interface NVE1
[*Leaf-CE6851HI-3-Nve1] source 11.11.11.12
[*Leaf-CE6851HI-3-Nve1] commit
[~Leaf-CE6851HI-3-Nve1] quit

[~Leaf-CE6851HI-4] interface NVE1
[*Leaf-CE6851HI-4-Nve1] source 11.11.11.12
[*Leaf-CE6851HI-4-Nve1] commit
[*Leaf-CE6851HI-4-Nve1] quit
```

步骤5 配置AC-DCN业务网关地址。

```
[~Leaf-CE6851HI-3] VLAN10
[*Leaf-CE6851HI-3-vlan10] interface vlanif 10
[*Leaf-CE6851HI-3-Vlanif10] ip address 100.125.100.2 24
[*Leaf-CE6851HI-3-Vlanif10] vrrp vrid 1 virtual-ip 100.125.100.1
[~Leaf-CE6851HI-3-Vlanif10] commit

[~Leaf-CE6851HI-4] VLAN10
[*Leaf-CE6851HI-4-vlan10] interface vlanif 10
[*Leaf-CE6851HI-4-Vlanif10] ip address 100.125.100.3 24
[*Leaf-CE6851HI-4-Vlanif10] vrrp vrid 1 virtual-ip 100.125.100.1
[*Leaf-CE6851HI-4-Vlanif10] commit
```

----结束

配置 M-LAG

步骤1 配置M-LAG模式。

```
<Leaf-CE6851HI-3> system-view
[~Leaf-CE6851HI-3] stp mode rstp
[*Leaf-CE6851HI-3] stp v-stp enable
[*Leaf-CE6851HI-3] commit
[~Leaf-CE6851HI-3] lacp m-lag system-id 00e0-fc00-0001
[*Leaf-CE6851HI-3] commit

<Leaf-CE6851HI-4> system-view
[~Leaf-CE6851HI-4] stp mode rstp
[*Leaf-CE6851HI-4] stp v-stp enable
[*Leaf-CE6851HI-4] commit
[~Leaf-CE6851HI-4] lacpm-lag system-id 00e0-fc00-0001
```

步骤2 在Leaf-CE6851HI-3与Leaf-CE6851HI-4上配置M-LAG的DFS Group。

```
[~Leaf-CE6851HI-3] dfs-group 1
[*Leaf-CE6851HI-3-dfs-group-1] source ip 13.13.13.13
[*Leaf-CE6851HI-3-dfs-group-1] priority 150
[*Leaf-CE6851HI-3-dfs-group-1] quit
[*Leaf-CE6851HI-3] commit

[*Leaf-CE6851HI-4] dfs-group 1
[*Leaf-CE6851HI-4-dfs-group-1] source ip 14.14.14.14
[*Leaf-CE6851HI-4-dfs-group-1] priority 120
[*Leaf-CE6851HI-4-dfs-group-1] quit
[*Leaf-CE6851HI-4] commit
```

步骤3 在Leaf-CE6851HI-3与Leaf-CE6851HI-4上配置M-LAG的Peer-Link。

```
[~Leaf-CE6851HI-3] interface eth-trunk 0
[*Leaf-CE6851HI-3-Eth-Trunk0] trunkport 40ge 1/0/1
[*Leaf-CE6851HI-3-Eth-Trunk0] trunkport 40ge 1/0/2
[*Leaf-CE6851HI-3-Eth-Trunk0] mode lacp-static
[*Leaf-CE6851HI-3-Eth-Trunk0] peer-link 1
[*Leaf-CE6851HI-3-Eth-Trunk0] quit
[*Leaf-CE6851HI-3] commit

[*Leaf-CE6851HI-4] interface eth-trunk 0
[*Leaf-CE6851HI-4-Eth-Trunk0] trunkport 40ge 1/0/1
[*Leaf-CE6851HI-4-Eth-Trunk0] trunkport 40ge 1/0/2
[*Leaf-CE6851HI-4-Eth-Trunk0] mode lacp-static
[*Leaf-CE6851HI-4-Eth-Trunk0] peer-link 1
[*Leaf-CE6851HI-4-Eth-Trunk0] quit
[*Leaf-CE6851HI-4] commit
```

步骤4 在Leaf-CE6851HI-3与Leaf-CE6851HI-4上配置M-LAG的成员口（服务器以负载均衡模式接入M-LAG）。

```
[*Leaf-CE6851HI-3] interface eth-trunk 1
[*Leaf-CE6851HI-3-Eth-Trunk1] mode lacp-static
[*Leaf-CE6851HI-3-Eth-Trunk1] port link-type trunk
[*Leaf-CE6851HI-3-Eth-Trunk1] undo port trunk allow-pass vlan 1
[*Leaf-CE6851HI-3-Eth-Trunk1] trunkport 10ge 1/0/1
[*Leaf-CE6851HI-3-Eth-Trunk1] dfs-group1 m-lag 1
[*Leaf-CE6851HI-3-Eth-Trunk1] quit
[*Leaf-CE6851HI-3] commit

[*Leaf-CE6851HI-4] interface eth-trunk 1
[*Leaf-CE6851HI-4-Eth-Trunk1] mode lacp-static
[*Leaf-CE6851HI-4-Eth-Trunk1] port link-type trunk
[*Leaf-CE6851HI-4-Eth-Trunk1] trunkport 10ge 1/0/1
[*Leaf-CE6851HI-4-Eth-Trunk1] undo port trunk allow-pass vlan 1
[*Leaf-CE6851HI-4-Eth-Trunk1] dfs-group1 m-lag 1
[*Leaf-CE6851HI-4-Eth-Trunk1] quit
[*Leaf-CE6851HI-4] commit
```

说明

若普通业务服务器以主备方式接入M-LAG，此时接入交换机连接服务器的端口不要作为M-LAG的成员接口，即物理接口不需要做任何配置，物理接口下的接入配置全部由AC-DCN下发。

步骤5 在Leaf-CE6851HI-3与Leaf-CE6851HI-4上配置M-LAG的成员口（AC-DCN服务器负载均衡模式接入示例）。

```
[~Leaf-CE6851HI-3] interface eth-trunk 100
[*Leaf-CE6851HI-3-Eth-Trunk100] mode lacp-static
[*Leaf-CE6851HI-3-Eth-Trunk100] port default vlan 10
[*Leaf-CE6851HI-3-Eth-Trunk100] trunkport 10ge 1/0/44
[*Leaf-CE6851HI-3-Eth-Trunk100] dfs-group1 m-lag 40
[*Leaf-CE6851HI-3-Eth-Trunk100] quit
[*Leaf-CE6851HI-4] interface eth-trunk 100
[*Leaf-CE6851HI-4-Eth-Trunk100] mode lacp-static
[*Leaf-CE6851HI-4-Eth-Trunk100] port defaultvlan 10
[*Leaf-CE6851HI-4-Eth-Trunk100] trunkport 10ge 1/0/44
[*Leaf-CE6851HI-4-Eth-Trunk100] dfs-group1 m-lag 40
[*Leaf-CE6851HI-4-Eth-Trunk100] quit
[*Leaf-CE6851HI-4] commit

[~Leaf-CE6851HI-3] interface eth-trunk 101
[*Leaf-CE6851HI-3-Eth-Trunk101] mode lacp-static
[*Leaf-CE6851HI-3-Eth-Trunk101] port defaultvlan 10
[*Leaf-CE6851HI-3-Eth-Trunk101] trunkport 10ge 1/0/45
[*Leaf-CE6851HI-3-Eth-Trunk101] dfs-group1 m-lag 41
[*Leaf-CE6851HI-3-Eth-Trunk101] quit
[*Leaf-CE6851HI-4] interface eth-trunk 101
[*Leaf-CE6851HI-4-Eth-Trunk101] mode lacp-static
[*Leaf-CE6851HI-4-Eth-Trunk101] port default vlan 10
[*Leaf-CE6851HI-4-Eth-Trunk101] trunkport 10ge 1/0/45
[*Leaf-CE6851HI-4-Eth-Trunk101] dfs-group1 m-lag 41
[*Leaf-CE6851HI-4-Eth-Trunk101] quit
[*Leaf-CE6851HI-4] commit

[~Leaf-CE6851HI-3] interface eth-trunk 102
[*Leaf-CE6851HI-3-Eth-Trunk102] mode lacp-static
[*Leaf-CE6851HI-3-Eth-Trunk102] port default vlan 10
[*Leaf-CE6851HI-3-Eth-Trunk102] trunkport 10ge 1/0/46
[*Leaf-CE6851HI-3-Eth-Trunk102] dfs-group1 m-lag 42
[*Leaf-CE6851HI-3-Eth-Trunk102] quit
[*Leaf-CE6851HI-4] interface eth-trunk 102
[*Leaf-CE6851HI-4-Eth-Trunk102] mode lacp-static
[*Leaf-CE6851HI-4-Eth-Trunk102]port default vlan 10
[*Leaf-CE6851HI-4-Eth-Trunk102] trunkport 10ge 1/0/46
[*Leaf-CE6851HI-4-Eth-Trunk102] dfs-group1 m-lag 42
[*Leaf-CE6851HI-4-Eth-Trunk102] quit
[*Leaf-CE6851HI-4] commit
```

说明

若AC-DCN服务器以主备方式接入M-LAG，此时接入交换机连接服务器的端口不要作为M-LAG的成员接口，仅需要在物理接口下配置VLAN即可。

步骤6 分别在Leaf-CE6851HI-3与Leaf-CE6851HI-4上配置Monitor Link关联上行接口和下行接口，避免因上行链路故障导致用户侧流量无法转发而丢弃。

```
[~Leaf-CE6851HI-3] monitor-link group 1
[*Leaf-CE6851HI-3-mtlk-group1] port 40GE1/0/3 uplink
[*Leaf-CE6851HI-3-mtlk-group1] port 40GE1/0/4 uplink
[*Leaf-CE6851HI-3-mtlk-group1] port 10GE1/0/1 downlink 1

[~Leaf-CE6851HI-4] monitor-link group 1
[*Leaf-CE6851HI-4-mtlk-group1] port 40GE1/0/3 uplink
[*Leaf-CE6851HI-4-mtlk-group1] port 40GE1/0/4 uplink
[*Leaf-CE6851HI-4-mtlk-group1] port 10GE1/0/1 downlink 1
```

----结束

配置路由

步骤1 在Leaf-CE6851HI-3上配置BGP路由，对接Spine。

```
[~Leaf-CE6851HI-3] BGP 65022
[*Leaf-CE6851HI-3-bgp] router-id 13.13.13.13
[*Leaf-CE6851HI-3-bgp] timer keepalive 10 hold 30
[*Leaf-CE6851HI-3-bgp] group Spine-CE12804-1 external
[*Leaf-CE6851HI-3-bgp] peer Spine-CE12804-1 as-number 65009
[*Leaf-CE6851HI-3-bgp] peer 11.254.41.158 as-number 65009
[*Leaf-CE6851HI-3-bgp] peer 11.254.41.158 group Spine-CE12804-1
[*Leaf-CE6851HI-3-bgp] group Spine-CE12804-2 external
[*Leaf-CE6851HI-3-bgp] peer Spine-CE12804-2 as-number 65010
[*Leaf-CE6851HI-3-bgp] peer 11.254.41.166 as-number 65010
[*Leaf-CE6851HI-3-bgp] peer 11.254.41.166 group Spine-CE12804-2
[*Leaf-CE6851HI-3-bgp] ipv4-family unicast
[*Leaf-CE6851HI-3-bgp-af-ipv4] preference 20 200 10
[*Leaf-CE6851HI-3-bgp-af-ipv4] network 11.11.11.12 255.255.255.255
[*Leaf-CE6851HI-3-bgp-af-ipv4] network 100.125.100.0 255.255.255.0
[*Leaf-CE6851HI-3-bgp-af-ipv4] network 13.13.13.13 255.255.255.255
[*Leaf-CE6851HI-3-bgp-af-ipv4] maximum load-balancing 32
[*Leaf-CE6851HI-3-bgp-af-ipv4] quit
[*Leaf-CE6851HI-3-bgp] quit
[*Leaf-CE6851HI-3] commit
```

步骤2 在Leaf-CE6851HI-4上配置BGP路由，对接Spine。

```
[~Leaf-CE6851HI-4] BGP 65023
[*Leaf-CE6851HI-4-bgp] router-id 14.14.14.14
[*Leaf-CE6851HI-4-bgp] timer keepalive 10 hold 30
[*Leaf-CE6851HI-4-bgp] group Spine-CE12804-1 external
[*Leaf-CE6851HI-4-bgp] peer Spine-CE12804-1 as-number 65009
[*Leaf-CE6851HI-4-bgp] peer 11.254.41.170 as-number 65009
[*Leaf-CE6851HI-4-bgp] peer 11.254.41.170 group Spine-CE12804-1
[*Leaf-CE6851HI-4-bgp] group Spine-CE12804-2 external
[*Leaf-CE6851HI-4-bgp] peer Spine-CE12804-2 as-number 65010
[*Leaf-CE6851HI-4-bgp] peer 11.254.41.162 as-number 65010
[*Leaf-CE6851HI-4-bgp] peer 11.254.41.162 group Spine-CE12804-2
[*Leaf-CE6851HI-4-bgp] ipv4-family unicast
[*Leaf-CE6851HI-4-bgp-af-ipv4] preference 20 200 10
[*Leaf-CE6851HI-4-bgp-af-ipv4] network 11.11.11.12 255.255.255.255
[*Leaf-CE6851HI-4-bgp-af-ipv4] network 100.125.100.0 255.255.255.0
[*Leaf-CE6851HI-4-bgp-af-ipv4] network 14.14.14.14 255.255.255.255
[*Leaf-CE6851HI-4-bgp-af-ipv4] maximum load-balancing 32
[*Leaf-CE6851HI-4-bgp-af-ipv4] quit
[*Leaf-CE6851HI-4-bgp] quit
[*Leaf-CE6851HI-4] commit
```

说明

如果需要从外部网络访问到AC-DCN服务器，则需要在TOR上配置静态路由或动态路由，将AC-DCN服务器的业务地址发布出去，保证外部网络有访问AC-DCN服务器的路由，同时需要保证TOR上有到外部网络的路由。

----结束

4.2.3.4 配置 Spine 节点

在两台Spine节点上配置上下联的互联接口地址和路由，使Underlay网络三层互通，配置思路如下：

1. 配置IP地址：分别配置Spine节点与Leaf和GW设备的三层互联地址、管理口（Meth0/0/0）IP地址、Loopback地址（作为Router-ID）。
2. 配置路由：在两台Spine节点上分别配置BGP动态路由，邻居为Leaf堆叠组、Leaf M-LAG组两台设备、GW M-LAG两台设备，使Spine上的网段与Leaf和GW上的网段三层可达。

配置 IP 地址

步骤1 配置互连接口IP地址

在Spine-CE12804-1上配置接口IP地址。

```
[~HUAWEI] sysname Spine-CE12804-1
[*Spine-CE12804-1] commit
[~Spine-CE12804-1] interface 40GE1/0/0
[~Spine-CE12804-1-40GE1/0/0] undo portswitch
[*Spine-CE12804-1-40GE1/0/0] ip address 11.254.40.158 30
[*Spine-CE12804-1-40GE1/0/0] commit
[~Spine-CE12804-1-40GE1/0/0]quit
[~Spine-CE12804-1] interface 40GE1/0/1
[~Spine-CE12804-1-40GE1/0/1] undo portswitch
[*Spine-CE12804-1-40GE1/0/1] ip address 11.254.40.170 30
[*Spine-CE12804-1-40GE1/0/1] commit
[~Spine-CE12804-1-40GE1/0/1] quit
[~Spine-CE12804-1] interface 40GE1/0/2
[~Spine-CE12804-1] description "to-Leaf-CE6851-3-40GE1/0/3"
[~Spine-CE12804-1-40GE1/0/2] undo portswitch
[*Spine-CE12804-1-40GE1/0/2] ip address 11.254.41.158 30
[*Spine-CE12804-1-40GE1/0/2] commit
[~Spine-CE12804-1-40GE1/0/2]quit
[~Spine-CE12804-1] interface 40GE1/0/3
[*Spine-CE12804-1] description "to-Leaf-CE6851-4-40GE1/0/4"
[~Spine-CE12804-1-40GE1/0/3] undo portswitch
[*Spine-CE12804-1-40GE1/0/3] ip address 11.254.41.170 30
[*Spine-CE12804-1-40GE1/0/3] commit
[~Spine-CE12804-1-40GE1/0/3] quit
[~Spine-CE12804-1] interface 40GE1/0/4
[~Spine-CE12804-1-40GE1/0/4] undo portswitch
[*Spine-CE12804-1-40GE1/0/4] ip address 11.254.42.157 30
[*Spine-CE12804-1-40GE1/0/4] commit
[~Spine-CE12804-1-40GE1/0/4]quit
[~Spine-CE12804-1] interface 40GE1/0/5
[~Spine-CE12804-1-40GE1/0/5] undo portswitch
[*Spine-CE12804-1-40GE1/0/5] ip address 11.254.42.161 30
[*Spine-CE12804-1-40GE1/0/5] commit
[~Spine-CE12804-1-40GE1/0/5] quit
```

在Spine-CE12804-2节点上配置接口IP地址。

```
[~HUAWEI] sysname Spine-CE12804-2
[*Spine-CE12804-2] commit
[~Spine-CE12804-2] interface 40GE1/0/0
[~Spine-CE12804-2-40GE1/0/0] undo portswitch
[*Spine-CE12804-2-40GE1/0/0] ip address 11.254.40.162 30
[*Spine-CE12804-2-40GE1/0/0] commit
[~Spine-CE12804-2-40GE1/0/0]quit
[~Spine-CE12804-2] interface 40GE1/0/1
[~Spine-CE12804-2-40GE1/0/1] undo portswitch
[*Spine-CE12804-2-40GE1/0/1] ip address 11.254.40.166 30
[*Spine-CE12804-2-40GE1/0/1] commit
[~Spine-CE12804-2-40GE1/0/1] quit
[~Spine-CE12804-2] interface 40GE1/0/2
[*Spine-CE12804-2] description "to-Leaf-CE6851-4-40GE1/0/3"
[~Spine-CE12804-2-40GE1/0/2] undo portswitch
[*Spine-CE12804-2-40GE1/0/2] ip address 11.254.41.162 30
[*Spine-CE12804-2-40GE1/0/2] commit
[~Spine-CE12804-2-40GE1/0/2]quit
[~Spine-CE12804-2] interface 40GE1/0/3
[*Spine-CE12804-2] description "to-Leaf-CE6851-3-40GE1/0/4"
[~Spine-CE12804-2-40GE1/0/3] undo portswitch
[*Spine-CE12804-2-40GE1/0/3] ip address 11.254.41.166 30
[*Spine-CE12804-2-40GE1/0/3] commit
[~Spine-CE12804-2-40GE1/0/3] quit
```

```
[~Spine-CE12804-2] interface 40GE1/0/4
[~Spine-CE12804-2-40GE1/0/4] undo portswitch
[*Spine-CE12804-2-40GE1/0/4] ip address 11.254.43.157 30
[*Spine-CE12804-2-40GE1/0/4] commit
[~Spine-CE12804-2-40GE1/0/4]quit
[~Spine-CE12804-2] interface 40GE1/0/5
[~Spine-CE12804-2-40GE1/0/5] undo portswitch
[*Spine-CE12804-2-40GE1/0/5] ip address 11.254.43.161 30
[*Spine-CE12804-2-40GE1/0/5] commit
[~Spine-CE12804-2-40GE1/0/5] quit
```

步骤2 配置管理口地址。

```
[~Spine-CE12804-1] interface Meth0/0/0
[*Spine-CE12804-1- Meth0/0/0] ip address 100.125.94.5 24
[*Spine-CE12804-1- Meth0/0/0] commit
[~Spine-CE12804-1- Meth0/0/0] quit

[~Spine-CE12804-2] interface Meth0/0/0
[*Spine-CE12804-2- Meth0/0/0] ip address 100.125.94.6 24
[*Spine-CE12804-2- Meth0/0/0] commit
[~Spine-CE12804-2- Meth0/0/0] quit
```

步骤3 配置Loopback地址。

```
[~Spine-CE12804-1] interface loopback0
[*Spine-CE12804-1-LoopBack0] ip address 11.11.11.14 32
[*Spine-CE12804-1-LoopBack0] commit
[~Spine-CE12804-1-LoopBack0] quit

[~Spine-CE12804-2] interface loopback0
[*Spine-CE12804-2-LoopBack0] ip address 11.11.11.15 32
[*Spine-CE12804-2-LoopBack0] commit
[~Spine-CE12804-2-LoopBack0] quit
```

----结束

配置路由

步骤1 在Spine-CE12804-1上配置BGP路由。

```
[~Spine-CE12804-1]BGP 65009
[*Spine-CE12804-1-bgp] router-id 11.11.11.14
[*Spine-CE12804-1-bgp] timer keepalive 10 hold 30
[*Spine-CE12804-1-bgp] group Leaf-CE6851HI-1&CE6851HI-2 external
[*Spine-CE12804-1-bgp] peer Leaf-CE6851HI-1&CE6851HI-2 as-number 65021
[*Spine-CE12804-1-bgp] peer 11.254.40.157 as-number 65021
[*Spine-CE12804-1-bgp] peer 11.254.40.157 group Leaf-CE6851HI-1&CE6851HI-2
[*Spine-CE12804-1-bgp] peer 11.254.40.169 as-number 65021
[*Spine-CE12804-1-bgp] peer 11.254.40.169 group Leaf-CE6851HI-1&CE6851HI-2
[*Spine-CE12804-1-bgp] group Leaf-CE6851HI-3 external
[*Spine-CE12804-1-bgp] peer Leaf-CE6851HI-3 as-number 65022
[*Spine-CE12804-1-bgp] peer 11.254.41.157 as-number 65022
[*Spine-CE12804-1-bgp] peer 11.254.41.157 group Leaf-CE6851HI-3
[*Spine-CE12804-1-bgp] group Leaf-CE6851HI-4 external
[*Spine-CE12804-1-bgp] peer Leaf-CE6851HI-4 as-number 65023
[*Spine-CE12804-1-bgp] peer 11.254.41.169 as-number 65023
[*Spine-CE12804-1-bgp] peer 11.254.41.169 group Leaf-CE6851HI-4
[*Spine-CE12804-1-bgp] group Gateway-CE12808-1 external
[*Spine-CE12804-1-bgp] peer Gateway-CE12808-1 as-number 65000
[*Spine-CE12804-1-bgp] peer 11.254.42.158 as-number 65000
[*Spine-CE12804-1-bgp] peer 11.254.42.158 group Gateway-CE12808-1
[*Spine-CE12804-1-bgp] group Gateway-CE12808-2 external
[*Spine-CE12804-1-bgp] peer Gateway-CE12808-2 as-number 65001
[*Spine-CE12804-1-bgp] peer 11.254.42.162 as-number 65001
[*Spine-CE12804-1-bgp] peer 11.254.42.162 group Gateway-CE12808-2
[*Spine-CE12804-1-bgp] ipv4-family unicast
[*Spine-CE12804-1-bgp-af-ipv4] preference 20 200 10
[*Spine-CE12804-1-bgp-af-ipv4] network 11.11.11.14 255.255.255.255
```

```
[*Spine-CE12804-1-bgp-af-ipv4] maximum load-balancing 32
[*Spine-CE12804-1-bgp-af-ipv4] quit
[*Spine-CE12804-1-bgp] quit
[*Spine-CE12804-1] commit
```

步骤2 在Spine-CE12804-2上配置BGP路由。

```
[~Spine-CE12804-2]BGP 65010
[*Spine-CE12804-2-bgp] router-id 11.11.11.15
[*Spine-CE12804-2-bgp] timer keepalive 10 hold 30
[*Spine-CE12804-2-bgp] group Leaf-CE6851HI-1&CE6851HI-2 external
[*Spine-CE12804-2-bgp] peer Leaf-CE6851HI-1&CE6851HI-2 as-number 65021
[*Spine-CE12804-2-bgp] peer 11.254.40.165 as-number 65021
[*Spine-CE12804-2-bgp] peer 11.254.40.165 group Leaf-CE6851HI-1&CE6851HI-2
[*Spine-CE12804-2-bgp] peer 11.254.40.161 as-number 65021
[*Spine-CE12804-2-bgp] peer 11.254.40.161 group Leaf-CE6851HI-1&CE6851HI-2
[*Spine-CE12804-2-bgp] group Leaf-CE6851HI-3 external
[*Spine-CE12804-2-bgp] peer Leaf-CE6851HI-3 as-number 65022
[*Spine-CE12804-2-bgp] peer 11.254.41.165 as-number 65022
[*Spine-CE12804-2-bgp] peer 11.254.41.165 group Leaf-CE6851HI-3
[*Spine-CE12804-2-bgp] group Leaf-CE6851HI-4 external
[*Spine-CE12804-2-bgp] peer Leaf-CE6851HI-4 as-number 65023
[*Spine-CE12804-2-bgp] peer 11.254.41.161 as-number 65023
[*Spine-CE12804-2-bgp] peer 11.254.41.161 group Leaf-CE6851HI-4
[*Spine-CE12804-2-bgp] group Gateway-CE12808-1 external
[*Spine-CE12804-2-bgp] peer Gateway-CE12808-1 as-number 65000
[*Spine-CE12804-2-bgp] peer 11.254.43.162 as-number 65000
[*Spine-CE12804-2-bgp] peer 11.254.43.162 group Gateway-CE12808-1
[*Spine-CE12804-2-bgp] group Gateway-CE12808-2 external
[*Spine-CE12804-2-bgp] peer Gateway-CE12808-2 as-number 65001
[*Spine-CE12804-2-bgp] peer 11.254.43.158 as-number 65001
[*Spine-CE12804-2-bgp] peer 11.254.43.158 group Gateway-CE12808-2
[*Spine-CE12804-2-bgp] ipv4-family unicast
[*Spine-CE12804-2-bgp-af-ipv4] preference 20 200 10
[*Spine-CE12804-2-bgp-af-ipv4] network 11.11.11.15 255.255.255.255
[*Spine-CE12804-2-bgp-af-ipv4] maximum load-balancing 32
[*Spine-CE12804-2-bgp-af-ipv4] quit
[*Spine-CE12804-2-bgp] quit
[*Spine-CE12804-2] commit
```

----结束

4.2.3.5 配置网关工作组

网关的两台CE交换机Gateway-CE12808-1和Gateway-CE12808-2组成M-LAG，相关配置思路如下：

1. 配置IP地址：分别配置与Spine节点，并配置防火墙的管理VLAN地址；配置Loopback0地址（作为VTEP地址）、Loopback1地址（作为Router-ID）；配置管理口地址（Meth0/0/0）；配置VTEP IP地址（两台设备设置相同）。
2. 配置M-LAG：在GW交换机上配置M-LAG全局模式、DFS组、Peer-Link，并分别配置与两台防火墙的互联管理VLAN和业务链路。
3. 配置路由：在GW上分别配置BGP动态路由，邻居为两个Spine设备，使GW上的网段与Spine上的网段三层可达；配置与外部路由器的路由。
4. 配置MAC漂移白名单：在GW设备上将Spine设备与GW互联的三层口MAC地址配置为白名单，不再检测MAC漂移。
5. 配置网关设备与外部路由器的互联，使网关与外部路由器形成“口”字型出口网络：分别配置网关与外部路由器之间的互联接口地址、配置网关设备之间的互联接口地址、配置网关设备上的出口路由协议（外部路由器上的配置与之类似，本文不涉及）。

配置 IP 地址

步骤1 配置接口IP地址。

配置Gateway-CE12808-1的接口IP地址。

```
[~Gateway-CE12808-1] interface 40GE1/0/0//连接Spine节点
[~Gateway-CE12808-1-40GE1/0/0] undo portswitch
[*Gateway-CE12808-1-40GE1/0/0] ip address 11.254.42.158 30
[*Gateway-CE12808-1-40GE1/0/0] commit
[~Gateway-CE12808-1-40GE1/0/0]quit
[~Gateway-CE12808-1] interface 40GE1/0/1 //连接Spine节点
[~Gateway-CE12808-1-40GE1/0/1] undo portswitch
[*Gateway-CE12808-1-40GE1/0/1] ip address 11.254.43.162 30
[*Gateway-CE12808-1-40GE1/0/1] commit
[~Gateway-CE12808-1-40GE1/0/1] quit
[*Gateway-CE12808-1] vlan batch 11
[~Gateway-CE12808-1] interface vlanif 11//网关设备与防火墙管理互联VLAN
[*Gateway-CE12808-1-vlanif11] description "to firewall-1~2"
[*Gateway-CE12808-1-vlanif11] ip address 11.254.45.154 29
[*Gateway-CE12808-1-vlanif11] vrrp vrid 1 virtual-ip 11.254.45.153
[*Gateway-CE12808-1-vlanif11] commit
[~Gateway-CE12808-1-vlanif11] quit
```

配置Gateway-CE12808-2的接口IP地址。

```
[~Gateway-CE12808-2] interface 40GE1/0/0//连接Spine节点
[~Gateway-CE12808-2-40GE1/0/0] undo portswitch
[*Gateway-CE12808-2-40GE1/0/0] ip address 11.254.42.162 30
[*Gateway-CE12808-2-40GE1/0/0] commit
[~Gateway-CE12808-2-40GE1/0/0]quit
[~Gateway-CE12808-2] interface 40GE1/0/1 //连接Spine节点
[~Gateway-CE12808-2-40GE1/0/1] undo portswitch
[*Gateway-CE12808-2-40GE1/0/1] ip address 11.254.43.158 30
[*Gateway-CE12808-2-40GE1/0/1] commit
[~Gateway-CE12808-2-40GE1/0/1] quit
[~Gateway-CE12808-2] vlan batch 11
[*Gateway-CE12808-2] interface vlanif 11//网关设备与防火墙管理互联VLAN
[*Gateway-CE12808-2-vlanif11] description "to firewall-1-2"
[*Gateway-CE12808-2-vlanif11] ip address 11.254.45.155 29
[*Gateway-CE12808-2-vlanif11] vrrp vrid 1 virtual-ip 11.254.45.153
[*Gateway-CE12808-2-vlanif11] commit
[*Gateway-CE12808-2-vlanif11] quit
```

步骤2 配置Loopback口地址。

```
[~Gateway-CE12808-1] interface loopback0//作为VTEP地址
[*Gateway-CE12808-1-LoopBack0] ip address 11.11.11.16 32
[*Gateway-CE12808-1-LoopBack0] commit
[~Gateway-CE12808-1-LoopBack0] quit
[~Gateway-CE12808-1] interface loopback1
[*Gateway-CE12808-1-LoopBack1] ip address 18.18.18.18 32
[*Gateway-CE12808-1-LoopBack1] commit
[~Gateway-CE12808-1-LoopBack1] quit
[~Gateway-CE12808-1] interface loopback2
[*Gateway-CE12808-1-LoopBack2] ip address 21.21.21.21 32
[*Gateway-CE12808-1-LoopBack2] commit
[~Gateway-CE12808-1-LoopBack2] quit

[~Gateway-CE12808-2] interface loopback0//作为VTEP地址
[*Gateway-CE12808-2-LoopBack0] ip address 11.11.11.16 32
[*Gateway-CE12808-2-LoopBack0] commit
[~Gateway-CE12808-2-LoopBack0] quit
[~Gateway-CE12808-2] interface loopback1
[*Gateway-CE12808-2-LoopBack1] ip address 19.19.19.19 32
[*Gateway-CE12808-2-LoopBack1] commit
[~Gateway-CE12808-2-LoopBack1] quit
[~Gateway-CE12808-2] interface loopback2
```

```
[*Gateway-CE12808-2-LoopBack2] ip address 22.22.22.22 32
[*Gateway-CE12808-2-LoopBack2] commit
[~Gateway-CE12808-2-LoopBack2] quit
```

步骤3 配置管理口地址。

```
[~Gateway-CE12808-1] interface Meth0/0/0
[*Gateway-CE12808-1-Meth0/0/0] ip address 100.125.94.7 24
[*Gateway-CE12808-1-Meth0/0/0] commit
[~Gateway-CE12808-1-Meth0/0/0] quit

[~Gateway-CE12808-2] interface Meth0/0/0
[*Gateway-CE12808-2-Meth0/0/0] ip address 100.125.94.8 24
[*Gateway-CE12808-2-Meth0/0/0] commit
[~Gateway-CE12808-2-Meth0/0/0] quit
```

步骤4 配置VTEP地址。

```
[~Gateway-CE12808-1] interface NVE1
[*Gateway-CE12808-1-Nve1] source 11.11.11.16
[*Gateway-CE12808-1-Nve1] commit
[~Gateway-CE12808-1-Nve1] quit

[~Gateway-CE12808-2] interface NVE1
[*Gateway-CE12808-2-Nve1] source 11.11.11.16
[*Gateway-CE12808-2-Nve1] commit
[~Gateway-CE12808-2-Nve1] quit
```

----结束

组建 M-LAG 组

步骤1 配置M-LAG模式。

```
< Gateway-CE12808-1> system-view
[~Gateway-CE12808-1] stp mode rstp
[*Gateway-CE12808-1] stp v-stp enable
[*Gateway-CE12808-1] lacp m-lag priority 10

[~Gateway-CE12808-1] lacp m-lag system-id 00e0-fc00-0101
//建议使用M-LAG中Master的系统MAC作为system-id，在对端设备上system-id的配置要保持一致。可以使用命令display system mac-address来查看系统MAC。
[*Gateway-CE12808-1] commit

<Gateway-CE12808-2> system-view
[~Gateway-CE12808-2] stp mode rstp
[*Gateway-CE12808-2] stp v-stp enable
[*Gateway-CE12808-2] commit
[*Gateway-CE12808-1] lacp m-lag priority 10
[~Gateway-CE12808-2] lacp m-lag system-id 00e0-fc00-0101
[*Gateway-CE12808-2] commit
```

步骤2 在Gateway-CE12808-1和Gateway-CE12808-2上配置M-LAG的DFS Group及网关双活。

```
[~Gateway-CE12808-1] dfs-group 1
[*Gateway-CE12808-1-dfs-group-1] source ip 18.18.18.18
[*Gateway-CE12808-1-dfs-group-1] priority 150
[*Gateway-CE12808-1-dfs-group-1] active-active-gateway
[*Gateway-CE12808-1-dfs-group-1-active-active-gateway] peer 19.19.19.19
[*Gateway-CE12808-1-dfs-group-1-active-active-gateway] quit
[*Gateway-CE12808-1-dfs-group-1] quit
[*Gateway-CE12808-1] commit

[*Gateway-CE12808-2] dfs-group 1
[*Gateway-CE12808-2-dfs-group-1] source ip 19.19.19.19
[*Gateway-CE12808-2-dfs-group-1] priority 120
[*Gateway-CE12808-2-dfs-group-1] active-active-gateway
[*Gateway-CE12808-1-dfs-group-1-active-active-gateway] peer 18.18.18.18
[*Gateway-CE12808-2-dfs-group-1-active-active-gateway] quit
```

```
[*Gateway-CE12808-2-dfs-group-1] quit
[*Gateway-CE12808-2] commit
```

步骤3 在Gateway-CE12808-1和Gateway-CE12808-2上配置M-LAG的Peer-Link。

```
[*Gateway-CE12808-1] interface eth-trunk 0
[*Gateway-CE12808-1-Eth-Trunk0] trunkport 40ge 1/0/23
[*Gateway-CE12808-1-Eth-Trunk0] trunkport 40ge 2/0/23
[*Gateway-CE12808-1-Eth-Trunk0] mode lacp-static
[*Gateway-CE12808-1-Eth-Trunk0] peer-link 1
[*Gateway-CE12808-1-Eth-Trunk0] quit
[*Gateway-CE12808-1] commit

[*Gateway-CE12808-2] interface eth-trunk 0
[*Gateway-CE12808-2-Eth-Trunk0] trunkport 40ge 1/0/23
[*Gateway-CE12808-2-Eth-Trunk0] trunkport 40ge 2/0/23
[*Gateway-CE12808-2-Eth-Trunk0] mode lacp-static
[*Gateway-CE12808-2-Eth-Trunk0] peer-link 1
[*Gateway-CE12808-2-Eth-Trunk0] quit
[*Gateway-CE12808-2] commit
```

步骤4 在Gateway-CE12808-1和Gateway-CE12808-2上配置M-LAG成员口（对接防火墙示例）。

配置Gateway-CE12808-1与防火墙的互联。

```
[*Gateway-CE12808-1] interface eth-trunk 20
[*Gateway-CE12808-1] description "to-FW-USG9560-1-GE1/0/1"
[*Gateway-CE12808-1-Eth-Trunk20] port default vlan 11
[*Gateway-CE12808-1-Eth-Trunk20] trunkport 10ge 3/0/0
[*Gateway-CE12808-1-Eth-Trunk20] dfs-group 1 m-lag 1
[*Gateway-CE12808-1-Eth-Trunk20] quit
[*Gateway-CE12808-1] interface eth-trunk 30
[*Gateway-CE12808-1] description "to-FW-USG9560-2-GE1/0/1"
[*Gateway-CE12808-1-Eth-Trunk30] port default vlan 11
[*Gateway-CE12808-1-Eth-Trunk30] trunkport 10ge 3/0/1
[*Gateway-CE12808-1-Eth-Trunk30] dfs-group 1 m-lag 2
[*Gateway-CE12808-1-Eth-Trunk30] quit
[*Gateway-CE12808-1] commit

[*Gateway-CE12808-1] interface eth-trunk 21 //配置防火墙与网关互联的业务链路，业务链路的互联地址、互联VLAN、来回路由由AC-DCN下发，此处只需要连接好网线，配置完Eth-Trunk、M-LAG即可。
[*Gateway-CE12808-1] description "to-FW-USG9560-1-GE1/0/3"
[*Gateway-CE12808-1-Eth-Trunk21] port link-type trunk
[*Gateway-CE12808-1-Eth-Trunk21] undo port trunk allow-pass vlan 1
[*Gateway-CE12808-1-Eth-Trunk21] trunkport 10ge 3/0/2
[*Gateway-CE12808-1-Eth-Trunk21] dfs-group 1 m-lag 3
[*Gateway-CE12808-1-Eth-Trunk21] quit
[*Gateway-CE12808-1] interface eth-trunk 31
[*Gateway-CE12808-1] description "to-FW-USG9560-2-GE1/0/3"
[*Gateway-CE12808-1-Eth-Trunk31] port link-type trunk
[*Gateway-CE12808-1-Eth-Trunk31] undo port trunk allow-pass vlan 1
[*Gateway-CE12808-1-Eth-Trunk31] trunkport 10ge 3/0/3
[*Gateway-CE12808-1-Eth-Trunk31] dfs-group 1 m-lag 4
[*Gateway-CE12808-1-Eth-Trunk31] quit
[*Gateway-CE12808-1] commit
```

配置Gateway-CE12808-2与防火墙的互联。

```
[*Gateway-CE12808-2] interface eth-trunk 20
[*Gateway-CE12808-2] description "to-FW-USG9560-1-GE1/0/2"
[*Gateway-CE12808-2-Eth-Trunk20] port default vlan 11
[*Gateway-CE12808-2-Eth-Trunk20] trunkport 10ge 3/0/0
[*Gateway-CE12808-2-Eth-Trunk20] dfs-group 1 m-lag 1
[*Gateway-CE12808-2-Eth-Trunk20] quit
[*Gateway-CE12808-2] interface eth-trunk 30
[*Gateway-CE12808-2] description "to-FW-USG9560-2-GE1/0/2"
[*Gateway-CE12808-2-Eth-Trunk30] port default vlan 11
[*Gateway-CE12808-2-Eth-Trunk30] trunkport 10ge 3/0/1
[*Gateway-CE12808-2-Eth-Trunk30] dfs-group 1 m-lag 2
```

```
[*Gateway-CE12808-2-Eth-Trunk30] quit
[*Gateway-CE12808-2] commit

[*Gateway-CE12808-2] interface eth-trunk 21 //配置防火墙与网关互联的业务链路，业务链路的互联地址、互联VLAN、来回路由由AC-DCN下发，此处只需要连接好网线，配置完Eth-Trunk、M-LAG即可。
[*Gateway-CE12808-2] description "to-FW-USG9560-1-GE1/0/4"
[*Gateway-CE12808-2-Eth-Trunk21] port link-type trunk
[*Gateway-CE12808-2-Eth-Trunk21] trunkport 10ge 3/0/2
[*Gateway-CE12808-2-Eth-Trunk21] dfs-group 1 m-lag 3
[*Gateway-CE12808-2-Eth-Trunk21] quit
[*Gateway-CE12808-2] interface eth-trunk 31
[*Gateway-CE12808-2] description "to-FW-USG9560-2-GE1/0/4"
[*Gateway-CE12808-2-Eth-Trunk31] port link-type trunk
[*Gateway-CE12808-2-Eth-Trunk31] trunkport 10ge 3/0/3
[*Gateway-CE12808-2-Eth-Trunk31] dfs-group 1 m-lag 4
[*Gateway-CE12808-2-Eth-Trunk31] quit
[*Gateway-CE12808-2] commit
```

说明

SDN场景防火墙对接网关采用M-LAG时，两端的LAG模式仅能为手工负载分担模式。

----结束

配置路由

步骤1 在Gateway-CE12808-1上配置BGP路由用于打通Underlay层面的路由。

```
[~Gateway-CE12808-1] BGP 65000
[*Gateway-CE12808-1-bgp] router-id 18.18.18.18
[*Gateway-CE12808-1-bgp] timer keepalive 10 hold 30
[*Gateway-CE12808-1-bgp] group Spine-CE12804-1 external   //对接Spine
[*Gateway-CE12808-1-bgp] peer Spine-CE12804-1 as-number 65009
[*Gateway-CE12808-1-bgp] peer 11.254.42.157 as-number 65009
[*Gateway-CE12808-1-bgp] peer 11.254.42.157 group Spine-CE12804-1
[*Gateway-CE12808-1-bgp] group Spine-CE12804-2 external
[*Gateway-CE12808-1-bgp] peer Spine-CE12804-2 as-number 65010
[*Gateway-CE12808-1-bgp] peer 11.254.43.161 as-number 65010
[*Gateway-CE12808-1-bgp] peer 11.254.43.161 group Spine-CE12804-2
[*Gateway-CE12808-1-bgp] ipv4-family unicast
[*Gateway-CE12808-1-bgp-af-ipv4] preference 20 200 10
[*Gateway-CE12808-1-bgp-af-ipv4] network 11.11.11.16 255.255.255.255
[*Gateway-CE12808-1-bgp-af-ipv4] network 18.18.18.18 255.255.255.255
[*Gateway-CE12808-1-bgp-af-ipv4] network 11.254.45.152 255.255.255.248
[*Gateway-CE12808-1-bgp-af-ipv4] maximum load-balancing 32
[*Gateway-CE12808-1-bgp-af-ipv4] quit
[*Gateway-CE12808-1-bgp] quit
[*Gateway-CE12808-1] commit
```

步骤2 在Gateway-CE12808-2上配置BGP路由用于打通Underlay层面的路由。

```
[~Gateway-CE12808-2] BGP 65001
[*Gateway-CE12808-2-bgp] router-id 19.19.19.19
[*Gateway-CE12808-2-bgp] timer keepalive 10 hold 30
[*Gateway-CE12808-2-bgp] group Spine-CE12804-1 external    //对接Spine
[*Gateway-CE12808-2-bgp] peer Spine-CE12804-1 as-number 65009
[*Gateway-CE12808-2-bgp] peer 11.254.42.161 as-number 65009
[*Gateway-CE12808-2-bgp] peer 11.254.42.161 group Spine-CE12804-1
[*Gateway-CE12808-2-bgp] group Spine-CE12804-2 external
[*Gateway-CE12808-2-bgp] peer Spine-CE12804-2 as-number 65010
[*Gateway-CE12808-2-bgp] peer 11.254.43.157 as-number 65010
[*Gateway-CE12808-2-bgp] peer 11.254.43.157 group Spine-CE12804-2
[*Gateway-CE12808-2-bgp] ipv4-family unicast
[*Gateway-CE12808-2-bgp-af-ipv4] preference 20 200 10
[*Gateway-CE12808-2-bgp-af-ipv4] network 11.11.11.16 255.255.255.255
[*Gateway-CE12808-2-bgp-af-ipv4] network 19.19.19.19 255.255.255.255
[*Gateway-CE12808-2-bgp-af-ipv4] network 11.254.45.152 255.255.255.248
[*Gateway-CE12808-2-bgp-af-ipv4] maximum load-balancing 32
[*Gateway-CE12808-2-bgp-af-ipv4] quit
```

```
[*Gateway-CE12808-2-bgp] quit
[*Gateway-CE12808-2] commit
```

----结束

配置 MAC 漂移白名单

三层架构时，VXLAN流量经过Spine设备到达GW时，可能会由于产品约束限制在GW上学习了错误的MAC地址导致MAC漂移告警，需要在GW设备上基于MAC地址配置MAC漂移白名单，将Spine设备与GW互联的三层口MAC地址配置为白名单不再检测MAC漂移，正常情况下此MAC是作为隧道报文的外层源MAC，不应该被学习，所以调整后对业务功能不会有任何影响。

步骤1 查看两台Spine设备与GW互连的三层口MAC地址。

```
[~Spine-CE12804-1] interface 40GE1/0/4//获取Spine-1设备与GW互连的三层口MAC地址
[*Spine-CE12804-1-40GE1/0/4] undo portswitch
[~Spine-CE12804-1-40GE1/0/4] commit
[~Spine-CE12804-1-40GE1/0/4] display this interface | includeHardware address
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 200b-c732-d202
[~Spine-CE12804-1-40GE1/0/4] quit
[~Spine-CE12804-1] interface 40GE1/0/5
[*Spine-CE12804-1-40GE1/0/5] undo portswitch
[~Spine-CE12804-1-40GE1/0/5] commit
[~Spine-CE12804-1-40GE1/0/5] display this interface | includeHardware address
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 200b-c732-d202
[~Spine-CE12804-1-40GE1/0/5] quit

[~Spine-CE12804-2] interface 40GE1/0/4 //获取Spine-2设备与GW互连的三层口MAC地址
[*Spine-CE12804-2-40GE1/0/4] undo portswitch
[~Spine-CE12804-2-40GE1/0/4] commit
[~Spine-CE12804-2-40GE1/0/4] display this interface | includeHardware address
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 346a-c246-be01
[~Spine-CE12804-2-40GE1/0/4] quit
[~Spine-CE12804-2] interface 40GE1/0/5
[*Spine-CE12804-2-40GE1/0/5] undo portswitch
[~Spine-CE12804-2-40GE1/0/5] commit
[~Spine-CE12804-2-40GE1/0/5] display this interface | includeHardware address
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 346a-c246-be01
[~Spine-CE12804-2-40GE1/0/5] quit
```

步骤2 根据步骤一中获取到的MAC地址配置白名单。

```
[~Gateway-CE12808-1] mac-address flapping detection exclude 200b-c732-d202 48
[~Gateway-CE12808-1] mac-address flapping detection exclude 346a-c246-be01 48

[~Gateway-CE12808-2] mac-address flapping detection exclude 200b-c732-d202 48
[~Gateway-CE12808-2] mac-address flapping detection exclude 346a-c246-be01 48
```

----结束

配置网关与外部路由器互联

步骤1 配置网关与外部路由器的互联端口。

在Gateway-CE12808-1配置与Router-1的互联端口。

```
[~Gateway-CE12808-1] interface Eth-Trunk1    //连接外部PE设备（Router-1）
[*Gateway-CE12808-1-Eth-Trunk1] trunkport 10GE 3/0/4
[*Gateway-CE12808-1-Eth-Trunk1] trunkport 10GE 3/0/5
[*Gateway-CE12808-1-Eth-Trunk1] undo portswitch
[*Gateway-CE12808-1-Eth-Trunk1] ip address 11.254.44.157 30
[*Gateway-CE12808-1-Eth-Trunk1] commit
[~Gateway-CE12808-1-Eth-Trunk1] quit
```

在Gateway-CE12808-2配置与Router-2的互联端口。

```
[~Gateway-CE12808-2] interface Eth-Trunk1    //连接外部PE设备（Router-2）
[*Gateway-CE12808-2-Eth-Trunk1] trunkport 10GE 3/0/4
[*Gateway-CE12808-2-Eth-Trunk1] trunkport 10GE 3/0/5
[*Gateway-CE12808-2-Eth-Trunk1] undo portswitch
[*Gateway-CE12808-2-Eth-Trunk1] ip address 11.254.44.161 30
[*Gateway-CE12808-2-Eth-Trunk1] commit
[~Gateway-CE12808-2-Eth-Trunk1] quit
```

步骤2 配置网关之间的三层互联端口，以组成“口”字型。

在Gateway-CE12808-1配置与Gateway-CE12808-2的互联端口。

```
[~Gateway-CE12808-1] interface 10GE3/0/6    //连接Gateway-CE12808-2
[*Gateway-CE12808-1-10GE3/0/6] undo portswitch
[*Gateway-CE12808-1-10GE3/0/6] ip address 11.254.44.165 30
[*Gateway-CE12808-1-10GE3/0/61] commit
[~Gateway-CE12808-1-10GE3/0/61] quit
```

在Gateway-CE12808-2配置与Gateway-CE12808-1的互联端口。

```
[~Gateway-CE12808-2] interface 10GE 3/0/6    //连接Gateway-CE12808-1
[*Gateway-CE12808-2-10GE3/0/6] undo portswitch
[*Gateway-CE12808-2-10GE3/0/6] ip address 11.254.44.166 30
[*Gateway-CE12808-2-10GE3/0/6] commit
[~Gateway-CE12808-2-10GE3/0/6] quit
```

步骤3 网关设备上与外部路由器Loopback地址互通的路由，本例以OSPF路由为例。

在Gateway-CE12808-1配置OSPF路由。

```
[~Gateway-CE12808-1] ospf 1 router-id 18.18.18.18
[~Gateway-CE12808-1-ospf-1] area 0
[~Gateway-CE12808-1-ospf-1-area-0.0.0.0] network 11.254.44.156 0.0.0.3
[~Gateway-CE12808-1-ospf-1-area-0.0.0.0] network 22.22.22.21 0.0.0.0
[~Gateway-CE12808-1-ospf-1-area-0.0.0.0] commit
[~Gateway-CE12808-1-ospf-1-area-0.0.0.0] quit
```

在Gateway-CE12808-2配置OSPF路由。

```
[~Gateway-CE12808-2] ospf 1 router-id 19.19.19.19
[~Gateway-CE12808-2-ospf-1] area 0
[~Gateway-CE12808-2-ospf-1-area-0.0.0.0] network 11.254.44.160 0.0.0.3
[~Gateway-CE12808-2-ospf-1-area-0.0.0.0] network 22.22.22.22 0.0.0.0
[~Gateway-CE12808-2-ospf-1-area-0.0.0.0] commit
[~Gateway-CE12808-2-ospf-1-area-0.0.0.0] quit
```

步骤4 在网关上配置与外部路由器和对端网关设备的EBGP邻居。

在Gateway-CE12808-1上分别配置与Router-1和Gateway-CE12808-2的EBGP路由。

```
[~Gateway-CE12808-1] BGP 65000
[*Gateway-CE12808-1-bgp] router-id18.18.18.18
[*Gateway-CE12808-1-bgp] timer keepalive10 hold 30
[*Gateway-CE12808-1-bgp] group Router-1external      //对接出口路由器
[*Gateway-CE12808-1-bgp] peer Router-1as-number 65047
[*Gateway-CE12808-1-bgp] peer Router-1ebgp-max-hop 10
[*Gateway-CE12808-1-bgp] peer Router-1connect-interface LoopBack2   //本端使用Loopback2作为建立BGP
邻居的端口
[*Gateway-CE12808-1-bgp] peer21.21.21.22 as-number 65047
[*Gateway-CE12808-1-bgp] peer21.21.21.22 group Router-1
[*Gateway-CE12808-1-bgp] group GW-2 external      //与GW-2建立EBGP邻居
[*Gateway-CE12808-1-bgp] peer GW-2 as-number65001
[*Gateway-CE12808-1-bgp] peer 11.254.44.166as-number 65001
[*Gateway-CE12808-2-bgp] peer 11.254.42.166 group GW-2
[*Gateway-CE12808-2-bgp] commit
[*Gateway-CE12808-2-bgp] quit
```

在Gateway-CE12808-2上配置与Router-2和Gateway-CE12808-1的EBGP路由。

```
[~Gateway-CE12808-2] BGP 65001
[*Gateway-CE12808-2-bgp] router-id19.19.19.19
[*Gateway-CE12808-2-bgp] timer keepalive10 hold 30
[*Gateway-CE12808-2-bgp] group Router-2external    //对接出口路由器
[*Gateway-CE12808-2-bgp] peer Router-2as-number 65048
[*Gateway-CE12808-2-bgp] peer Router-2ebgp-max-hop 10
[*Gateway-CE12808-2-bgp] peer Router-2connect-interface LoopBack2   //本端使用Loopback2作为建立BGP
邻居的端口
[*Gateway-CE12808-2-bgp] peer22.22.22.23 as-number 65048
[*Gateway-CE12808-2-bgp] peer22.22.22.23 group Router-2
[*Gateway-CE12808-1-bgp] group GW-1 external      //与GW-1建立EBGP邻居
[*Gateway-CE12808-1-bgp] peer GW-1as-number 65000
[*Gateway-CE12808-1-bgp] peer11.254.44.165 as-number 65000
[*Gateway-CE12808-2-bgp] peer 11.254.42.165 group GW-2
[*Gateway-CE12808-2-bgp] commit
[*Gateway-CE12808-2-bgp] quit
```

步骤5 在外部路由器Router-1和Router-2上配置互联网络，包括：

1. 外部路由器与网关的互联接口；
2. 外部路由器之间的互联接口；
3. 外部路由器上的OSPF路由，用于外部路由器和网关之间的Loopback地址互通；
4. 外部路由器上的EBGP路由，用于和网关设备建立EBGP邻居。

----结束

4.2.3.6 配置防火墙

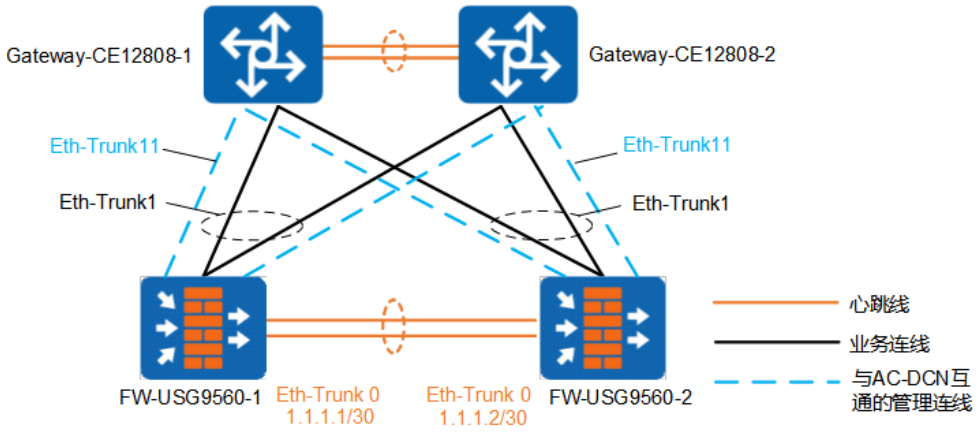
两台物理防火墙USG9560通过业务端口连接GW，配置管理网段与AC-DCN互通。两台防火墙使用另外的业务端口与GW互联，作为业务链路。两台防火墙工作在主备镜像模式。

内、外部链路可以合一共用物理链路，也可以单独规划物理连线，本节使用内、外部链路合一场景举例。

防火墙的配置思路如下：

1. 配置两台防火墙之间的心跳接口。
2. 配置两台防火墙工作在双机热备模式。
3. 配置镜像模式和双机热备管理接口。
4. 配置**hrp base config enable**，并重启防火墙。
5. 配置防火墙与网关的管理互联接口。
6. 配置防火墙与网关的业务互联接口。
7. 将端口加入安全域并配置缺省安全策略。

图 4-3 防火墙与网关互联配置



说明

两台主备镜像模式防火墙必须使用同样的接口连接到同一个GW设备。例如FW-1使用GE 1/0/1接口连接GW-1，那么FW-2也需要使用GE 1/0/1接口连接GW-1。

防火墙不支持AC-DCN使用NETCONF协议通过Meth管理口来对接。

下配置由AC-DCN自动下发，无需手动配置：业务链路与网关的互联地址VLAN和互联地址；根墙和虚墙中的路由和引流；虚墙中的安全域、EIP、SNAT和安全策略等。

不能在防火墙根墙上配置缺省路由，否则会和AC-DCN自动下发的默认路由冲突。

步骤1 配置与网关交换机CE12808互联的管理端口。

```
<FW-USG9560-1> system-view
[FW-USG9560-1] interface Eth-Trunk11
[FW-USG9560-1-Eth-Trunk11] description To-GW-CE12808
[FW-USG9560-1-Eth-Trunk11] ip address 11.254.45.156 29
[FW-USG9560-1-Eth-Trunk11] trunkport GigabitEthernet 1/0/1 to 1/0/2
[FW-USG9560-1-Eth-Trunk11] undo service-manage enable
[FW-USG9560-1-Eth-Trunk11] quit

<FW-USG9560-2> system-view
[FW-USG9560-2] interface Eth-Trunk11
[FW-USG9560-2-Eth-Trunk11] description To-GW-CE12808
[FW-USG9560-2-Eth-Trunk11] ip address 11.254.45.157 29
[FW-USG9560-2-Eth-Trunk11] trunkport GigabitEthernet 1/0/1 to 1/0/2
[FW-USG9560-2-Eth-Trunk11] undo service-manage enable
[FW-USG9560-2-Eth-Trunk11] quit
```

步骤2 配置与网关交换机CE12808互联的业务端口。

```
<FW-USG9560-1> system-view
[FW-USG9560-1] interface Eth-Trunk1
[FW-USG9560-1-Eth-Trunk1] description To-CE12808
[FW-USG9560-1-Eth-Trunk1] portswitch
[FW-USG9560-1-Eth-Trunk1] trunkport GigabitEthernet 1/0/3 to 1/0/4
[FW-USG9560-1-Eth-Trunk1] undo service-manage enable
[FW-USG9560-1-Eth-Trunk1] quit

<FW-USG9560-2> system-view
[FW-USG9560-2] interface Eth-Trunk1
[FW-USG9560-2-Eth-Trunk1] description To-CE12808
[FW-USG9560-2-Eth-Trunk1] portswitch
[FW-USG9560-2-Eth-Trunk1] trunkport GigabitEthernet 1/0/3 to 1/0/4
[FW-USG9560-2-Eth-Trunk1] undo service-manage enable
[FW-USG9560-2-Eth-Trunk1] quit
```

步骤3 配置防火墙之间组成双机热备的心跳接口。

配置FW-USG9560-1的心跳接口。

```
<FW-USG9560-1> system-view
[FW-USG9560-1] interface Eth-Trunk0
[FW-USG9560-1-Eth-Trunk0] ip address 1.1.1.1 255.255.255.252
[FW-USG9560-1-Eth-Trunk0] quit
[FW-USG9560-1] interface GigabitEthernet7/1/0
[FW-USG9560-1-GigabitEthernet7/1/0] description FW-HRP
[FW-USG9560-1-GigabitEthernet7/1/0] undo shutdown
[FW-USG9560-1-GigabitEthernet7/1/0] eth-trunk 0
[FW-USG9560-1-GigabitEthernet7/1/0] quit
[FW-USG9560-1] interface GigabitEthernet7/1/1
[FW-USG9560-1-GigabitEthernet7/1/1] description FW-HRP
[FW-USG9560-1-GigabitEthernet7/1/1] undo shutdown
[FW-USG9560-1-GigabitEthernet7/1/1] eth-trunk 0
[FW-USG9560-1-GigabitEthernet7/1/1] quit
```

配置FW-USG9560-2的心跳接口。

```
<FW-USG9560-2> system-view
[FW-USG9560-2] interface Eth-Trunk0
[FW-USG9560-2-Eth-Trunk0] ip address 1.1.1.2 255.255.255.252
[FW-USG9560-2-Eth-Trunk0] quit
[FW-USG9560-2] interface GigabitEthernet7/1/0
[FW-USG9560-2-GigabitEthernet7/1/0] description FW-HRP
[FW-USG9560-2-GigabitEthernet7/1/0] undo shutdown
[FW-USG9560-2-GigabitEthernet7/1/0] eth-trunk 0
[FW-USG9560-2-GigabitEthernet7/1/0] quit
[FW-USG9560-2] interface GigabitEthernet7/1/1
[FW-USG9560-2-GigabitEthernet7/1/1] description FW-HRP
[FW-USG9560-2-GigabitEthernet7/1/1] undo shutdown
[FW-USG9560-2-GigabitEthernet7/1/1] eth-trunk 0
[FW-USG9560-2-GigabitEthernet7/1/1] quit
```

步骤4 配置防火墙双机热备功能。

在FW-USG9560-1上配置双机热备。

```
<FW-USG9560-1> system-view
[FW-USG9560-1] hrp interface Eth-Trunk0 remote 1.1.1.2
[FW-USG9560-1] hrp mirror config enable
[FW-USG9560-1] hrp enable
```

在FW-USG9560-2上配置双机热备。

```
<FW-USG9560-2> system-view
[FW-USG9560-2] hrp interface Eth-Trunk0 remote 1.1.1.1
[FW-USG9560-2] hrp mirror config enable
[FW-USG9560-2] hrp enable
```

步骤5 配置双机热备的功能项。

在FW-USG9560-1上配置以下双机热备功能。

```
HRP_M[FW-USG9560-1] hrp track interface Eth-Trunk1  //设置配置VGMP组监控接口为业务口，此配置会同步到HRP备防火墙
HRP_M[FW-USG9560-1] hrp mgt-interface Eth-Trunk11  //设置双机热备的管理接口，此配置会同步到HRP备防火墙
HRP_M[FW-USG9560-1] hrp mirror session enable  //启用会话快速备份功能，此配置会同步到HRP备防火墙
HRP_M[FW-USG9560-1] hrp standby config enable  //开启备用设备的部分配置功能
```

步骤6 配置防火墙重启时以双机热备基础配置启动，并从另一台正常的防火墙上同步正常的业务配置。

配置命令**hrp base config enable**。

```
HRP_M[FW-USG9560-1] hrp base config enable
```

重启防火墙，使配置生效。

```
HRP_M<FW-USG9560-1> reboot
  System will reboot! Do you want to save the running configuration? [Y/N]: y
```

```
  System will reboot! Continue? [Y/N]: y

HRP_S<FW-USG9560-2> reboot
  System will reboot! Do you want to save the running configuration? [Y/N]: y
  System will reboot! Continue? [Y/N]: y
```

步骤7 将端口加入安全域并配置缺省安全策略。

将Virtual-if0增加到安全域中，用于根墙与虚墙之间的引流。

```
HRP_M[FW-USG9560-1] firewall zone untrust
HRP_M[FW-USG9560-1-zone-untrust] add interface Virtual-if0
HRP_M[FW-USG9560-1-zone-untrust] quit
```

#将管理网络口和心跳口加入到DMZ域。

```
HRP_M[FW-USG9560-1] firewall zone dmz
HRP_M[FW-USG9560-1-zone-dmz] add interface eth-trunk11      //将管理网络口加入到DMZ域
HRP_M[FW-USG9560-1-zone-dmz] add interface eth-trunk0     //将心跳口加入到DMZ域
HRP_M[FW-USG9560-1-zone-dmz] quit
```

配置缺省的安全策略为permit。

```
HRP_M[FW-USG9560-1] security-policy
HRP_M[FW-USG9560-1-security-policy] default action permit
```

----结束

4.2.3.7 配置 SNMP

为了使AC-DCN可以通过SNMP协议发现、添加设备，需要提前在设备侧配置SNMP协议参数。配置好的SNMP参数与在AC-DCN界面的对接操作中填写的参数要保持一致。

SNMP协议参数在CE交换机和防火墙上的配置有所不同。

说明

端口的配置与其他SNMP协议参数的配置不同。设备侧需要配置与AC-DCN连接使用的端口，默认为161；AC-DCN需要配置与设备侧连接使用的端口，默认为1666。

AC-DCN只支持通过安全性更高的SNMPv3协议与设备建立SNMP连接。

AC-DCN支持的iso层级的MIB树，包括“nt iso”、“rd iso”、“wt iso”和“iso-view iso”。

在配置SNMP参数之前，首先要保证设备info-center处于开启状态，否则设备无法向AC-DCN上报Trap。

执行命令**display info-center**检查设备info-center是否开启：

- 如果回显信息为**Information Center : enabled**，表示info-center已经开启，可以进行SNMP参数配置。
- 如果回显信息为**Information Center : disabled**，表示info-center未开启，执行命令**info-center enable**开启info-center。

配置 CE 交换机

在CE交换机上配置与AC-DCN互联的SNMPv3参数，主要需规划以下数据。

参数项	参数值（示例）	说明
snmp-agent udp-port	**161**	SNMP Agent（CE交换机）与AC连接所使用的UDP端口号，默认就是161

参数项	参数值（示例）	说明
snmp-agent group	**dc-admin**	SNMPv3用户组的组名
snmp-agent usm-user	**admin**	SNMPv3用户
snmp-agent usm-user authentication-mode	**SHA**	用户的认证方式
authentication password	**Huawei@123**	用户的认证密码
privacy-mode	**AES128**	认证加密方式
privacy password	**Huawei@123**	加密密码

下面以Gateway-CE12808-1为例进行配置，其他CE交换机的配置命令类似，此处不再赘述。

步骤1 执行system-view命令，进入系统视图。

步骤2 修改SNMP Agent与AC-DCN连接所使用的端口号。缺省情况下，SNMP Agent与AC-DCN连接所使用的端口号为161。

```
[~Gateway-CE12808-1] snmp-agent udp-port 161
```

步骤3 配置SNMPv3用户组和用户，并配置认证和加密方式。以下示例中用户组为dc-admin，用户名为admin，认证方式为SHA，加密方式为AES128。

```
[*Gateway-CE12808-1] snmp-agent usm-user v3 admin group dc-admin
[*Gateway-CE12808-1] snmp-agent usm-user v3 admin authentication-mode sha
Please configure the authentication password (8-255)
Enter Password:                //输入认证密码，本例的认证密码为：Huawei@123。
Confirm Password:              //确认认证密码，本例的认证密码为：Huawei@123。
[*Gateway-CE12808-1] snmp-agent usm-user v3 admin privacy-mode aes128
Please configure the privacy password (8-255)
Enter Password:                //输入加密密码，本例的加密密码为：Huawei@123。
Confirm Password:              //确认加密密码，本例的加密密码为：Huawei@123。
```

步骤4 配置设备SNMPv3向AC-DCN上报告警Trap。

```
[*Gateway-CE12808-1] snmp-agent trap enable feature-name trunk
[*Gateway-CE12808-1] snmp-agent trap enable              //使能交换机发送Trap报文。
[*Gateway-CE12808-1] snmp-agent trap source loopback0   //这里的端口是与AC-DCN对接的设备IP地址所在的接口名称。此接口必须是已经配置了IP地址。
[*Gateway-CE12808-1] commit
```

步骤5 设置MIB视图，并将该MIB视图添加到用户组的属性中，使用户组具备读、写、告警上报功能。

说明

AC-DCN需要通过SNMP协议中指定的MIB视图，获取设备的LLDP链路信息。其中，SNMP指定的MIB视图要为iso-view，指定的MIB对象的OID MIB子树要为iso。

```
[*Gateway-CE12808-1] snmp-agent mib-view included iso-view iso
[*Gateway-CE12808-1] snmp-agent mib-view included nt iso
[*Gateway-CE12808-1] snmp-agent mib-view included rd iso
[*Gateway-CE12808-1] snmp-agent mib-view included wt iso
[*Gateway-CE12808-1] snmp-agent group v3 dc-admin privacy read-view rd write-view wt notify-view nt
[*Gateway-CE12808-1] commit
```

----结束

配置防火墙

在防火墙上配置与AC-DCN互联的SNMPv3参数，与CE交换机相比，多出了Trap方面的参数配置，主要需规划以下数据。

参数项	参数值（示例）	说明
snmp-agent udp-port	**161**	SNMP Agent（CE交换机）与AC连接所使用的UDP端口号，默认就是161
snmp-agent group	**dc-admin**	SNMPv3用户组的组名
snmp-agent usm-user	**admin**	SNMPv3用户
snmp-agent usm-user authentication-mode	**SHA**	用户的认证方式
authentication password	**Huawei@123**	用户的认证密码
privacy-mode	**AES128**	认证加密方式
privacy password	**Huawei@123**	加密密码
snmp-agent group	**ACTRAP**	Trap用户组的组名
snmp-agent usm-user	**ACTrapUser**	Trap用户
snmp-agent usm-user authentication-mode	**SHA**	用户的认证方式
authentication password	**Public@1234**	用户的认证密码
privacy-mode	**AES128**	认证加密方式
privacy password	**Admin@5678**	加密密码
snmp-agent trap source	**Eth-Trunk6**	跟AC-DCN对接的设备IP地址所在的接口名称
snmp-agent target-host trap addr	**100.125.100.10/24** **100.125.100.11/24** **100.125.100.12/24**	AC-DCN节点地址示例

下面以FW-USG9650-1为例进行配置，其他FW-USG9650-2的配置命令类似，此处不再赘述。

步骤1 修改SNMP Agent与AC-DCN连接所使用的端口号。缺省情况下，SNMP Agent与AC-DCN连接所使用的端口号为161。

```
HRP_M[FW-USG9650-1] snmp-agent udp-port 161
```

步骤2 配置一个SNMP用户组。

```
HRP_M[FW-USG9650-1] snmp-agent group v3 ACTRAP privacy read-view rd write-view wt notify-view
nt    //rd、wt、nt是mib视图，它需要与设备发现与配置的视图名称保持一致。
```

步骤3 配置SNMPv3用户组和用户，并配置认证和加密方式。以下示例中用户组为dc-admin，用户名为admin，认证方式为SHA，加密方式为AES128。

```
HRP_M[FW-USG9650-1] snmp-agent usm-user v3 admin group dc-admin
HRP_M[FW-USG9650-1] snmp-agent usm-user v3 admin authentication-mode sha
Please configure the authentication password (8-255)
Enter Password:              //输入认证密码，本例的认证密码为：Huawei@123。
Confirm Password:            //确认认证密码，本例的认证密码为：Huawei@123。
HRP_M[FW1] snmp-agent usm-user v3 admin privacy-mode aes128
Please configure the privacy password (8-255)
Enter Password:              //输入加密密码，本例的加密密码为：Priva@1234。
Confirm Password:            //确认加密密码，本例的加密密码为：Priva@1234。
```

步骤4 配置一套用户名为ACTrapUser、认证方式和认证密码为SHA/Public@1234、加密方式和加密密码为AES128/Admin@5678的SNMP参数，使AC-DCN可以通过SNMP获取防火墙系统启动时间。

```
HRP_M[FW-USG9650-1] snmp-agent usm-user v3 ACTrapUser
HRP_M[FW-USG9650-1] snmp-agent usm-user v3 ACTrapUser group ACTRAP
HRP_M[FW-USG9650-1] snmp-agent usm-user v3 ACTrapUser authentication-mode sha
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
//输入两次认证密码，本例为：Public@1234
HRP_M[FW-USG9650-1] snmp-agent usm-user v3 ACTrapUser privacy-mode aes128
Please configure the authentication password (8-64)
Enter Password:
Confirm Password:
//输入两次认证密码，本例为：Admin@5678
```

步骤5 配置设备SNMPv3向AC-DCN上报告警Trap。

```
HRP_M[FW-USG9650-1] snmp-agent trap enable feature-name trunk
HRP_M[FW-USG9650-1] snmp-agent trap enable//使能交换机发送Trap报文
HRP_M[FW-USG9650-1] snmp-agent trap source Eth-trunk 11  //指定跟AC-DCN对接的设备IP地址所在的接口名称
HRP_M[FW-USG9650-1]snmp-agent target-host trap address udp-domain 100.125.100.10 udp-port 1666 params securityname ACTrapUser v3 privacy
//IP地址为AC-DCN节点地址
HRP_M[FW-USG9650-1]snmp-agent target-host trap address udp-domain 100.125.100.11 udp-port 1666 params securityname ACTrapUser v3 privacy
HRP_M[FW-USG9650-1] snmp-agent target-host trap address udp-domain 100.125.100.12 udp-port 1666 params securityname ACTrapUser v3 privacy
```

步骤6 设置MIB视图，并将该MIB视图添加到用户组的属性中，使用户组具备读、写、告警上报功能。

```
HRP_M[FW-USG9650-1] snmp-agent mib-view included iso-view iso
HRP_M[FW-USG9650-1] snmp-agent group v3 dc-admin privacy read-view rd write-view wt notify-view nt
HRP_M[FW-USG9650-1] snmp-agent mib-view included nt iso
HRP_M[FW-USG9650-1] snmp-agent mib-view included rd iso
HRP_M[FW-USG9650-1] snmp-agent mib-view included wt iso
```

----结束

4.2.3.8 配置 NETCONF

为了使AC-DCN可以通过NETCONF为网络设备下发业务配置或获取设备的配置信息，需要提前在设备侧配置NETCONF协议参数。配置好的NETCONF参数与在AC-DCN界面的对接操作中填写的参数要保持一致。

NETCONF参数在CE交换机和防火墙上的配置有所不同。

配置 CE 交换机

在CE交换机上配置与AC-DCN互联的NETCONF参数，主要需规划以下数据。

参数项	参数值（示例）	说明
local-user	**client@huawei.com**	SSH用户名
local-user password irreversible-cipher	**Huawei@123**	SSH用户认证密码

下面以Gateway-CE12808-1为例进行配置，其他CE交换机的配置命令类似，此处不再赘述。

步骤1 配置设备端VTY用户界面支持SSH协议。

```
<Gateway-CE12808-1> system-view
[~Gateway-CE12808-1] user-interface vty 0 4
[~Gateway-CE12808-1-ui-vty0-4] authentication-mode aaa
[~Gateway-CE12808-1-ui-vty0-4] protocol inbound ssh
[~Gateway-CE12808-1-ui-vty0-4] commit
[~Gateway-CE12808-1-ui-vty0-4] quit
```

说明

配置登录协议为SSH后，设备将自动禁止Telnet功能。Telnet协议存在安全风险，不建议您使用**protocol inbound all**命令同时开启SSH和Telnet功能。

步骤2 在设备端部署SSH。

1. 创建SSH用户。

   # 新建本地用户，用户名为**client**，域名为**huawei.com**的SSH用户，并配置密码为**Huawei@123**。

   ```
   [~Gateway-CE12808-1] aaa
   [~Gateway-CE12808-1-aaa] local-user client@huawei.com password irreversible-cipher Huawei@123
   [~Gateway-CE12808-1-aaa] local-user client@huawei.com service-type ssh
   [~Gateway-CE12808-1-aaa] local-user client@huawei.com level 3
   [~Gateway-CE12808-1-aaa] commit
   [~Gateway-CE12808-1-aaa] quit
   ```

2. 产生本地RSA密钥对。

   ```
   [~Gateway-CE12808-1] rsa local-key-pair create
   The key name will be: netconf-agent_Host
   The range of public key size is (512 ~ 2048).
   NOTE: If the key modulus is greater than 512,
           It will take a few minutes.
   Input the bits in the modulus [default = 512] :
   [~Gateway-CE12808-1] commit
   ```

   密钥对生成后，可以执行命令**display rsa local-key-pair public**查看本地密钥对中的公钥部分信息。

   说明

   执行此命令后，生成的密钥对将保存在设备中，设备重启后不会丢失。

   该命令不在配置文件中保存。

3. 配置SSH用户认证方式为Password。

   ```
   [~Gateway-CE12808-1] ssh user client@huawei.com authentication-type password
   [~Gateway-CE12808-1] commit
   ```

4. 配置SSH用户服务方式。

   ```
   [~Gateway-CE12808-1] ssh user client@huawei.com service-type snetconf
   [~Gateway-CE12808-1] commit
   ```

步骤3 使能NETCONF功能，开启SNETCONF服务后，设备会在端口号上使能SSH服务器端的NETCONF服务。

```
[~Gateway-CE12808-1] snetconf server enable
[~Gateway-CE12808-1] commit
```

----结束

配置防火墙

在防火墙上配置与AC-DCN互联的NETCONF参数，主要需规划以下数据。

参数项	参数值（示例）	说明
manager-user	**netconf-admin**	SSH用户名
password	**Huawei@123**	SSH用户认证密码

下面以FW-USG9650-1为例进行配置，其他FW-USG9650-2的配置命令类似，此处不再赘述。

步骤1 配置管理口访问管理，允许NETCONF类型的协议通过。

```
HRP_M<FW-USG9650-1> system-view
HRP_M[FW-USG9650-1] interface eth-trunk11  //用于接入管理网络的接口，可以是Eth-Trunk，也可以是一个物理接口
HRP_M[FW-USG9650-1-Eth-Trunk11] service-manage enable
HRP_M[FW-USG9650-1-Eth-Trunk11] service-mange all permit
HRP_M[FW-USG9650-1-Eth-Trunk11] quit
```

步骤2 配置管理员以及对应的服务类型、级别和认证类型。

```
HRP_M[FW-USG9650-1] aaa
HRP_M[FW-USG9650-1-aaa] manager-user netconf-admin
HRP_M[FW-USG9650-1-aaa-manager-user-netconf-admin] password
Enter Password:
Confirm Password:
HRP_M[FW-USG9650-1-aaa-manager-user-netconf-admin] service-type api
HRP_M[FW-USG9650-1-aaa-manager-user-netconf-admin] level 15
HRP_M[FW-USG9650-1-aaa-manager-user-netconf-admin] authentication-scheme admin_local
HRP_M[FW-USG9650-1-aaa-manager-user-netconf-admin] quit
```

步骤3 配置NETCONF端口号，开启NETCONF接口服务。

```
HRP_M[FW-USG9650-1] api
HRP_M[FW-USG9650-1-api] api netconf enable
HRP_M[FW-USG9650-1-api] quit
```

----结束

4.2.3.9 配置 LLDP

在CE设备全局开启LLDP功能，便于AC-DCN通过LLDP协议发现链路。

下面以Gateway-CE12808-1为例进行配置，其他CE交换机的配置命令类似，此处不再赘述。

步骤1 使能LLDP和LLDP MDN功能。

```
[~Gateway-CE12808-1] lldp enable
[*Gateway-CE12808-1] lldp mdn enable
[*Gateway-CE12808-1] commit
```

步骤2 在接入TOR交换机的服务器上，也需要将服务器的LLDP链路发现协议打开。

说明

部分服务器不支持链路发现功能，所以这些服务器与邻居节点的链路需要在AC-DCN手动添加。

----结束

4.2.3.10 配置 VXLAN

步骤1 配置网关设备的NVO3的扩展功能。

当CE12800设备作为网关时，默认情况下，NVO3的扩展功能未使能。此时在设备上部署NVO3业务后，若再叠加其他需要使用ACL的业务（如MQC、简化ACL、流量监管、BD流量统计、DHCP等），会较大概率出现叠加失败的情况。

在部署NVO3的设备上可以使用以下方法以降低其他业务叠加失败的风险。

```
[~Gateway-CE12808-1] assign forward nvo3 service extend enable
[~Gateway-CE12808-1] assign forward nvo3 acl extend enable
[~Gateway-CE12808-1] reboot

[~Gateway-CE12808-2] assign forward nvo3 service extend enable
[~Gateway-CE12808-2] assign forward nvo3 acl extend enable
[~Gateway-CE12808-2] reboot
```

上述两条命令的使用说明如下。

- 在GW设备系统视图下，使用**assign forward nvo3 service extend enable**命令，使能NVO3业务扩展功能。使能此命令后，在非CE-L48GT-EA、CE-L48GT-EC、CE-L48GS-EA、CE-L48GS-EC、CE-L24XS-BA、CE-L24XS-EA、CE-L48XS-BA、CE-L48XS-EA和CE-L24LQ-EA单板上，能减少这种业务叠加失败的问题。

说明

此命令对CE-L48GT-EA、CE-L48GT-EC、CE-L48GS-EA、CE-L48GS-EC、CE-L24XS-BA、CE-L24XS-EA、CE-L48XS-BA、CE-L48XS-EA和CE-L24LQ-EA单板不生效。

使能此命令后，非上述单板上通过NVO3隧道传输的、长度在230～294字节的报文不能发送至上述单板。

配置此命令后，才能在非CE-L48GT-EA、CE-L48GT-EC、CE-L48GS-EA、CE-L48GS-EC、CE-L24XS-BA、CE-L24XS-EA、CE-L48XS-BA、CE-L48XS-EA和CE-L24LQ-EA单板上使用路径探测功能。

- 在GW设备系统视图下，使用**assign forward nvo3 acl extend enable**命令，使能NVO3的ACL扩展功能。

说明

此命令仅支持在Admin-VS中配置，配置后对所有VS生效。

执行此命令使能NVO3的ACL扩展功能后，需重启设备使配置生效。

步骤2 配置NVO3网关的增强模式。

CE12800缺省情况下，未配置NVO3网关的增强模式，设备采用的是环回模式，即经过NVO3封装后的报文需要在设备内部先环回后才能继续转发。此时，GW设备上的VXLAN三层转发封装/解封装的流量，超过线卡总转发性能的50%时，有较大可能出现丢包。目前，可以根据实际需要配置NVO3的网关增强模式，解决此问题。

在GW设备的系统视图下，使用**assign forward nvo3-gateway enhanced l3**命令行配置NVO3网关的增强模式。

```
[~Gateway-CE12808-1] assign forward nvo3-gateway enhanced l3

[~Gateway-CE12808-2] assign forward nvo3-gateway enhanced l3
```

说明

需要先执行**assign forward nvo3 service extend enable**命令，使能NVO3业务扩展功能。此时请确保设备上不存在CE-L48GT-EA、CE-L48GT-EC、CE-L48GS-EA、CE-L48GS-EC、CE-L24XS-BA、CE-L24XS-EA、CE-L48XS-BA、CE-L48XS-EA和CE-L24LQ-EA单板，或者这些单板上没有承载VXLAN相关业务。

若承载VXLAN业务的单板为CE-L24XS-EC、CE-L48XS-EC、CE-L24LQ-EC、CE-L48XT-EC、CE-L24LQ-EC1、CE-L08CC-EC、CE-L02LQ-EC、CE-L06LQ-EC时，仅支持通过查询ARP主机表进行VXLAN隧道封装，不支持通过查询最长匹配路由表进行VXLAN隧道封装。

服务器网卡主备方式接入的两台接入交换机需要组建为堆叠系统，或者M-LAG方式将服务器双归连接到接入交换机，此时接入交换机连接服务器的端口不要作为M-LAG的成员接口。

- CE8800/CE7800/CE6800系列交换机设备不需要配置步骤1和步骤2中的上述三条命令。
- FD/FDA类型单板不需要配置步骤1和步骤2中的上述三条命令行。

步骤3 配置VXLAN其他功能。

VXLAN的其他功能由AC-DCN下发，不需要人工配置。

注意

VM在线的情况下，请用户不要通过命令行在设备上修改AC-DCN控制器下发的配置，例如删除广播域BD、解除VNI与BD的绑定关系、修改VTEP的IPVBDIF接口、修改VBDIF接口的IP地址等，否则可能会导致VXLAN业务不能正常运行。

----结束

4.2.3.11 配置 LB

LB以Eth-trunk方式与Leaf设备的堆叠或者M-LAG对接。LB设备界面上的配置由LB设备厂商完成。LB配置完成后，根据规划生成一个浮动IP地址作为对外呈现的业务地址。LB的浮动IP与实际处理业务的成员服务器需要在相同子网，与成员服务器共用vbdif网关。

说明

CE12800的EC/ED/EF/EG类型单板承载VXLAN GW业务时，不支持以VXLAN二层子接口方式二层接入到GW（即LB不支持通过二层子接口方式接入到GW设备）。

本文以LB下挂LEAF-CE6851HI-3与LEAF-CE6851HI-4对接M-LAG为例，配置思路如下：

1. 在LEAF-CE6851HI-3与LEAF-CE6851HI-4上分别配置与LB-1和LB-2的M-LAG。
2. 在LEAF-CE6851HI-3与LEAF-CE6851HI-4上连接LB的二层子接口上，配置接入方式的untag，并绑定BD值。

步骤1 M-LAG的DFS和Peer-link为全局共用配置，LEAF-CE6851HI-3和LEAF-CE6851HI-4设备在前文已经配置完成，此时只配置M-LAG接口。

```
[~LEAF-CE6851HI-3] interface eth-trunk 20    //对接LB-1
[*LEAF-CE6851HI-3-Eth-Trunk20] mode lacp-static
[*LEAF-CE6851HI-3-Eth-Trunk20] trunkport 10ge 1/0/47
[*LEAF-CE6851HI-3-Eth-Trunk20] dfs-group 1 m-lag 50
[*LEAF-CE6851HI-3-Eth-Trunk20] quit
[*LEAF-CE6851HI-3] interface eth-trunk 30   //对接LB-2
[*LEAF-CE6851HI-3-Eth-Trunk30] mode lacp-static
```

```
[*LEAF-CE6851HI-3-Eth-Trunk30] trunkport 10ge 1/0/48
[*LEAF-CE6851HI-3-Eth-Trunk30] dfs-group 1 m-lag 51
[*LEAF-CE6851HI-3-Eth-Trunk30] quit
[*LEAF-CE6851HI-3] commit

[~LEAF-CE6851HI-4] interface eth-trunk 20   //对接LB-1
[*LEAF-CE6851HI-4-Eth-Trunk20] mode lacp-static
[*LEAF-CE6851HI-4-Eth-Trunk20] port link-type trunk
[*LEAF-CE6851HI-4-Eth-Trunk20] trunkport 10ge 1/0/47
[*LEAF-CE6851HI-4-Eth-Trunk20] dfs-group 1 m-lag 50
[*LEAF-CE6851HI-4-Eth-Trunk20] quit
[*LEAF-CE6851HI-4] interface eth-trunk 30   //对接LB-2
[*LEAF-CE6851HI-4-Eth-Trunk30] mode lacp-static
[*LEAF-CE6851HI-4-Eth-Trunk30] port link-type trunk
[*LEAF-CE6851HI-4-Eth-Trunk30] trunkport 10ge 1/0/48
[*LEAF-CE6851HI-4-Eth-Trunk30] dfs-group 1 m-lag 51
[*LEAF-CE6851HI-4-Eth-Trunk30] quit
[*LEAF-CE6851HI-4] commit
```

步骤2 配置接入端口配置（需要等AC-DCN业务下发完成后，确认AC-DCN给实际处理业务的成员服务器规划的BD才能配置，此处以BD 2000为例）。

```
[~LEAF-CE6851HI-3] interface Eth-Trunk20.1 mode l2
[~LEAF-CE6851HI-3-Eth-Trunk20.1] encapsulation untag
[~LEAF-CE6851HI-3-Eth-Trunk20.1] bridge-domain 2000
[~LEAF-CE6851HI-3-Eth-Trunk20.1] commit
[~LEAF-CE6851HI-3] interface Eth-Trunk30.1 mode l2
[~LEAF-CE6851HI-3-Eth-Trunk30.1] encapsulation untag
[~LEAF-CE6851HI-3-Eth-Trunk30.1] bridge-domain 2000
[~LEAF-CE6851HI-3-Eth-Trunk30.1] commit

[~LEAF-CE6851HI-4] interface Eth-Trunk20.1 mode l2
[~LEAF-CE6851HI-4-Eth-Trunk20.1] encapsulation untag
[~LEAF-CE6851HI-4-Eth-Trunk20.1] bridge-domain 2000
[~LEAF-CE6851HI-4-Eth-Trunk20.1] commit
[~LEAF-CE6851HI-4] interface Eth-Trunk30.1 mode l2
[~LEAF-CE6851HI-4-Eth-Trunk30.1] encapsulation untag
[~LEAF-CE6851HI-4-Eth-Trunk30.1] bridge-domain 2000
[~LEAF-CE6851HI-4-Eth-Trunk30.1] commit
```

说明

LB与实际处理业务的成员服务器共用VBDIF网关，此部分由AC-DCN自动下发。

----结束

4.2.4 安装 AC-DCN

为了完成AC-DCN的安装，请依次执行以下操作。

步骤1 配置服务器RAID。

RAID配置必须在安装操作系统之前完成。通过配置RAID来保证硬盘的可靠性。

配置RAID的详细操作过程，请参考**Agile Controller-DCN产品手册**中的“安装与Underlay网络配置 > 软件安装 > 配置RAID”。

步骤2 安装服务器的操作系统：推荐使用随AC-DCN软件发布的系统镜像。

安装操作系统的详细操作过程，请参考**Agile Controller-DCN产品手册**中的“安装与Underlay网络配置 > 软件安装 > 安装操作系统（AC-DCN定制的ISO镜像）”。

步骤3 配置服务器网卡：根据规划的网卡工作模式，配置Bond和IP地址、掩码、网关、物理网卡将的工作模式，AC-DCN服务器才能接入网络。

配置服务器网卡的详细操作过程，请参考**Agile Controller-DCN产品手册**中的“FAQ > AC-DCN安装 > 服务器> 如何配置网卡绑定和网络（操作系统类型为：SUSE11 SP3，界面方式）？”。

步骤4 安装AC-DCN：使用iDepoly工具安装AC-DCN的安装包和配置包。

安装AC-DCN的详细操作过程，请参考**Agile Controller-DCN产品手册**中的“安装与Underlay网络配置> 软件安装>安装AC-DCN ”。

----结束

4.2.5 预配置 AC-DCN

4.2.5.1 登录 AC-DCN

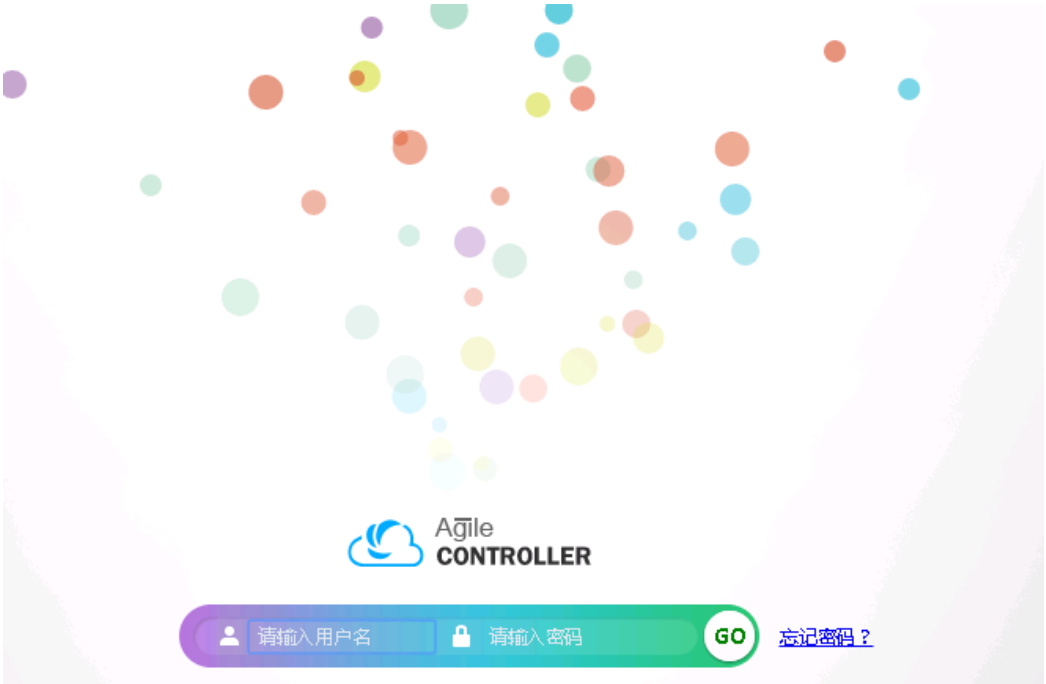
在客户端上通过浏览器方式登录AC-DCN界面进行配置。客户端已安装至少以下一种浏览器：

- Internet Explorer 11。
- Google Chrome 29。
- Mozilla Firefox 22

步骤1 打开浏览器，在地址栏输入**https://x.x.x.x:18002**，按“Enter”键。如果出现安全警示则选择信任和继续。

其中，x.x.x.x表示AC-DCN服务器的北向代理（nginx）的IP地址，如果是集群组网则为北向代理的浮动IP地址。

步骤2 在登录界面输入默认管理员名称**admin**和默认密码**Changeme123**，单击“GO”。



步骤3 登录成功后，根据页面提示修改密码。

步骤4 密码修改完毕后，系统会在5秒后自动跳转到登录页面。请使用新密码重新登录AC-DCN。

----结束

4.2.5.2 申请和导入 License

步骤1 选择“系统 > License管理 > License信息”，单击“获取ESN”，复制弹出框的ESN码。

步骤2 单击“确认”。

步骤3 根据ESN码申请和下载文件。

申请途径是华为的发放系统ESDP（Electronic Software Delivery Platform），网址**http://app.huawei.com/isdp**，具体申请方式请参考该网站的“帮助中心”（需准备好项目合同号）。

步骤4 选择“系统 > License管理 > License信息”，单击“上传”按钮。

步骤5 单击“浏览”，将文件上传到设备上。

步骤6 单击“确认”，加载成功后，显示License状态和资源控制信息。

----结束

4.2.5.3 发现网络设备

在AC-DCN上发现网络设备是AC-DCN纳管设备的基础，执行此步骤的前提是：

- 保证AC-DCN与网络设备可正常通信。
- 网络设备上已经配置SNMP对接参数，可参见“配置SNMP”。

步骤1 选择“网络 > 物理资源 > 网络设备”。

步骤2 单击“自动发现”，填写设备的管理IP地址范围和SNMPv3相关参数，其中SNMPv3参数要与设备侧预配置的参数保持一致。

步骤3 单击“开始”，成功发现设备后，界面会出现发现成功的提示，在设备列表中出现已发现设备。

步骤4 单击“结束”。

步骤5 按照同样方法，发现其他网段的设备。

----结束

4.2.5.4 创建并配置资源池

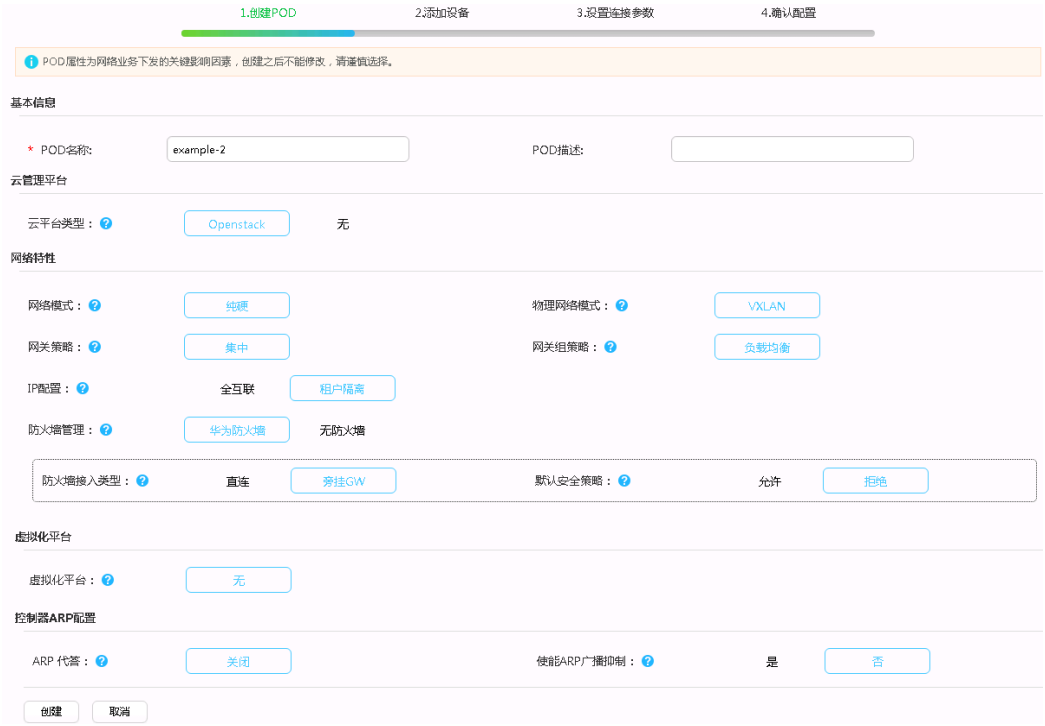
资源池（POD，Point of Delivery）是数据中心基础物理网络划分的基本单元。一个物理设备不能被划到不同的POD中。一个数据中心可以由多个POD组成。每一个POD中的计算资源、存储资源可以分配给租户/项目使用。

执行本操作的前提是：

- 网络设备上完成NETCONF相关预配置，可参见本文“配置NETCONF”。
- AC-DCN已经发现相关网络设备

步骤1 选择“网络 > POD管理 > POD”，进入POD管理页面。

步骤2 在左侧导航树中单击+，即“创建”，在创建页面中配置POD的名称和各类属性。



说明

创建POD页面中已经对配置参数进行了介绍，鼠标放置在配置项右侧的问号处或者悬浮在参数按钮处，可显示解释内容。

ARP广播抑制建议不开启。

步骤3 单击“创建”进入添加网络设备界面。

步骤4 单击“添加设备”，输入网络设备的“起始IP地址”与“结束IP地址”，点击查询后，选中需要添加到POD中的网络设备，单击“添加到POD”。

步骤5 单击“下一步”，将设备添加到POD。

说明

- 一个设备只能添加到一个POD，不能添加到多个POD中。
- 设备添加到POD后，如果想将设备移到另一个POD中，首先要在当前POD中删除该设备。

步骤6 配置AC-DCN与设备的连接参数，使AC-DCN可以通过NETCONF将网络业务配置发放到设备中。

1. 单击“连接参数”页签，选择“NETCONF”界面，输入AC-DCN与设备NETCONF连接的参数，参数值与设备侧NETCONF的配置保持一致。

2. 单击“检查连接”，检查AC-DCN与设备NETCONF连接情况。
3. 单击“下一步”，然后单击“确定”。

说明

由于CE交换机设备NETCONF的默认端口为22，防火墙NETCONF的默认端口为830，因此一次不能将交换机和防火墙共同发现上来，需再执行以下操作建立与防火墙的NETCONF链接。

4. 进入创建的POD资源池，点击“设备”标签，点击“防火墙”，单击需要配置NETCONF参数的防火墙“操作”列的“Netconf”。

5. 在“Netconf配置”对话框中，填写预配置时设置的认证模式、用户名和密码，并设置端口为830，单击“检查连接”。

6. 点击“确认修改”，完成防火墙NETCONF链接参数设置。

----结束

4.2.5.5 发现并添加链路

发现并添加链路后，可以在AC-DCN上查看设备之间的拓扑结构，并查看链路状态和链路的详细信息。链路添加分为自动发现和手动创建两种：

- 自动发现：CE交换机之间的链路可以由AC-DCN自动发现上来。
- 手动创建：防火墙与网关交换机之间的链路不支持通过LLDP自动发现，需要管理员手工创建。

步骤1 自动发现链路。

1. 选择“网络 > 链路管理 > 链路”。
2. 单击“链路发现”，勾选设备，将“LLDP使能”设置为ON，然后单击“发现”。

AC-DCN会对设备做链路自动发现，发现的每条链路会在页面中展示出来。

步骤2 手动创建链路

1. 选择“网络 > 链路管理 > 链路”。
2. 单击“创建”，选择防火墙和网关设备之间的二层链路信息。

说明

添加链路时直接添加物理链路即可。AC-DCN在进行设备发现时已经将相关的Eth-trunk和物理链路之间的关系同时发现上来，添加物理链路之后，AC-DCN会自动将物理链路的端口与Eth-trunk关联，下发配置时直接在Eth-trunk上下发。

----结束

4.2.5.6 指定网络设备的角色

在AC-DCN上指定各个设备在网络中扮演的角色，如接入交换机、汇聚交换机、网关，方便AC-DCN做识别。

可以在以下两种方式中，选择其中一种，配置POD中各个设备的角色。

- （推荐）在POD的“拓扑”页面中，右键对应的设备图标，设置设备的角色。

  以Spine-CE12804-1为例，右键后单击“设置为汇聚交换机”。
- 在POD“设备”页面中，选择“物理网络设备”，在物理网络设备列表中，配置POD设备的角色。

  以Spine-CE12804-1为例，勾选该设备，单击“设置为汇聚”，再单击“保存配置”。

4.2.5.7 配置接入组、网关组和防火墙组

在Underlay组网中，如果网关交换机、接入交换机采用双活配置，如M-LAG，则需要将这些设备设置为网关组、接入组；如果采用堆叠配置则不需要设置。

防火墙工作在主备模式下，需设置防火墙组。

步骤1 设置接入交换机组。

1. 选择“网络 > POD管理 > POD”，单击“设备”页签。
2. 单击“交换机”图标，再单击下方的“接入交换机”页签。
3. 勾选需要设置为多活接入组的交换机，单击“增加到组”，并填写多活组的信息。

   其中，配置的IP为设备组的NVE IP，设置后两台设备具有相同的NVE IP。

步骤2 设置网关组。

1. 选择“网络 > POD管理 > POD”，单击“设备”页签。
2. 在“设备”页签中，单击“网关”。
3. 勾选需要设置为多活网关组的交换机，单击“增加到组”，输入组名、VTEP IP地址和虚MAC地址。

说明

网关与防火墙的虚MAC地址不能重复，本文档中防火墙配置的VRRP VRID值为1，则对应的虚MAC为0000-5e00-0101，集中式多活的网关MAC地址可以设置为0000-5e00-0100（CE设备上的取值范围为0000-5e00-0100 ~ 0000-5e00-01ff）。

步骤3 设置防火墙组。

1. 选择“网络 > POD管理 > POD”，单击“设备”页签。
2. 在“设备”页签中，单击“防火墙”。
3. 勾选2个防火墙设备，单击“增加到组”，并输入组名。

4. 单击“确认”。

----结束

4.2.5.8 添加负载均衡设备和链路

在AC-DCN上添加负载均衡设备和链路，这样可以在POD的拓扑中查看负载均衡设备的状态和链路信息。但是AC-DCN不纳管负载均衡设备，不给负载均衡设备下发配置。

步骤1 添加负载均衡设备。

1. 选择“网络 > POD管理 > POD”，单击“设备”页签。
2. 单击“负载均衡器”图标，再单击“增加”。
3. 在“添加”窗口中，配置负载均衡设备的名称和IP。
   - 设备名称：为F5 Agent中的self.agent_host取值，不是实际设备名称，此处默认填写“F5LBAAS”。

- 设备IP：为F5对接云平台的IP。

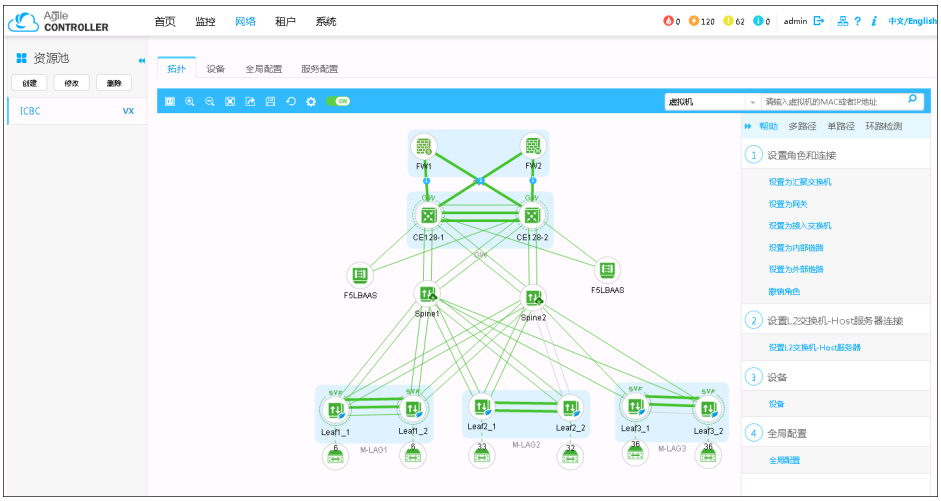
4. 成功添加后，在“负载均衡器”图标旁出现数字2。

步骤2 添加负载均衡设备的链路。

1. 选则“网络 > 链路管理 > 链路”，单击“创建”。
2. 手动创建负载均衡设备与网关交换机之间的链路。

   创建完成的链路如下所示。

链路添加完成后，进入“网络 > POD管理 > POD”，可以看到拓扑中会呈现负载均衡设备及其链路。



----结束

4.2.5.9 设置网络虚拟节点

检查虚拟网络节点信息

如果在Underlay基础配置命令中已经在VTEP设备上配置了NVE信息，则不需要在AC-DCN界面重新设置，只需要在AC-DCN界面检查AC-DCN获取的VTEP IP与手工配置的是否相同。

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在“设备”页面中，选择“虚拟网络节点”。

步骤3 选中设备，点击“读设备VTEP IP”，检查获取的VTEP IP与AC-DCN中的数据是否一致。

- 如果一致，则正常。
- 如果不一致，单击“设置”按钮，配置与设备读取信息一致的VTEP IP地址，单击“确认”。

----结束

设置虚拟网络节点信息

如果设备上没有配置NVE信息，则按照此任务完成NVE节点的配置。如果设备上已经预配置了NVE信息，则不需要重复设置NVE，可忽略此节操作。

步骤1 选择“网络 > POD管理 > POD”

步骤2 在“设备”页面中，选择“虚拟网络节点”。

步骤3 增加或导入虚拟网络节点，可以选择以下任意一种方法。

- 手工增加：

1. 勾选需要增加虚拟网络节点的设备，单击“增加虚拟网络节点”。
   以leaf1为例，管理IP为“11.1.1.100”，VTEP IP为“11.1.1.1”。

2. 单击“确认”。
3. 单击“写设备VTEP IP”。
4. 按照同样方法，给POD中其他NVE设备配置NVE信息。

5. 配置完成后，单击“读设备VTEP IP”，检查当前配置是否与规划的数值一致。

- 批量导入：

1. 单击“导出”，下载虚拟网络节点模板表格。
2. 填写表格中的虚拟网络节点参数，形式参见下表（表中数据仅作示例）。

设备名称	节点类型（请输入接入交换机、网关或者虚拟交换机）	IP（X.X.X.X）	VTEP IP（AC）（X.X.X.X）	VTEP IP(设备)	网关IP【仅节点类型为虚拟交换机时必选】（X.X.X.X）	掩码【仅节点类型为虚拟交换机时必选】（1-31）
Leaf-CE6851HI-1&CE6851HI-2	接入交换机	100.125.94.2	11.11.11.11	11.11.11.11	-	-

3. 单击“导入”，将虚拟网络节点模板表格导入到AC-DCN中。

----结束

4.2.5.10 设置防火墙内外部链路

防火墙旁挂网关时，需要分别指定防火墙与网关之间的内部链路和外部链路。

- 内部链路：承载从租户VRF（网关）到租户VSYS（防火墙虚墙）的流量。
- 外部链路：承载从根VSYS（防火墙根墙）到根VRF（网关）之间的流量。

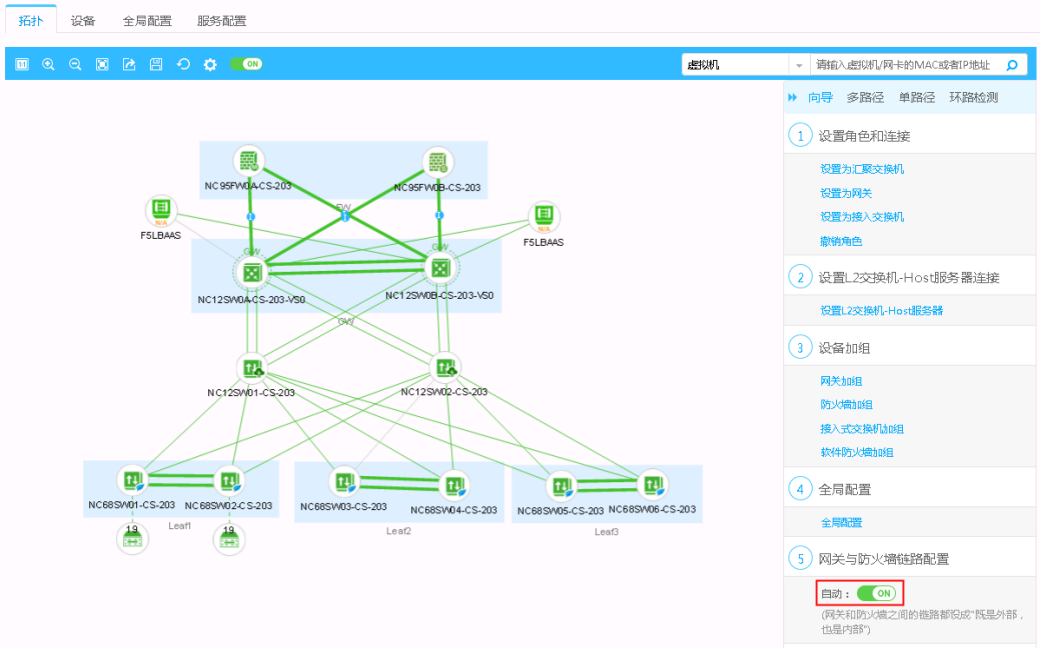
内外部链路共用

在防火墙与网关之间的内外部链路共用时，需配置AC-DCN采用自动的方式下发内外部链路上的配置。

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD拓扑页面。

步骤3 在界面右下角“网关与防火墙链路设置”中，将自动开关设置为“ON”。



----结束

内外部链路独立

在防火墙与网关之间的内外部链路相互独立时，需在AC-DCN上分别指明外部链路和外部链路。

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD拓扑页面。

步骤3 在界面的右下角“网关与防火墙链路配置”中将自动设置为“OFF”。

步骤4 在拓扑中，右键选择防火墙与网关之间的链路，根据需要将链路设置为“内部链路”或“外部链路”。

说明

防火墙直连场景需要将防火墙与网关互联的所有链路（不包括管理链路）设为内部链路。

----结束

4.2.5.11 配置接口互联资源

网关与防火墙的互联接口和路由配置、负载均衡设备与网关的互联接口和路由配置由AC-DCN下发。本步骤用来指定上述配置中使用的互联VLAN号的范围和互联IP地址段的范围。

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 选择“全局配置 > 接口互联资源”，为网关与防火墙、负载均衡的接口预留VLAN和IP资源。

1. 在“VLAN”栏填写互联VLAN使用的范围，单击。

2. 在“IP地址段”栏填写用于互联IP地址范围，单击。
3. 单击“应用”。

----结束

4.2.5.12 配置 VNI/VLAN/BD 的可用范围

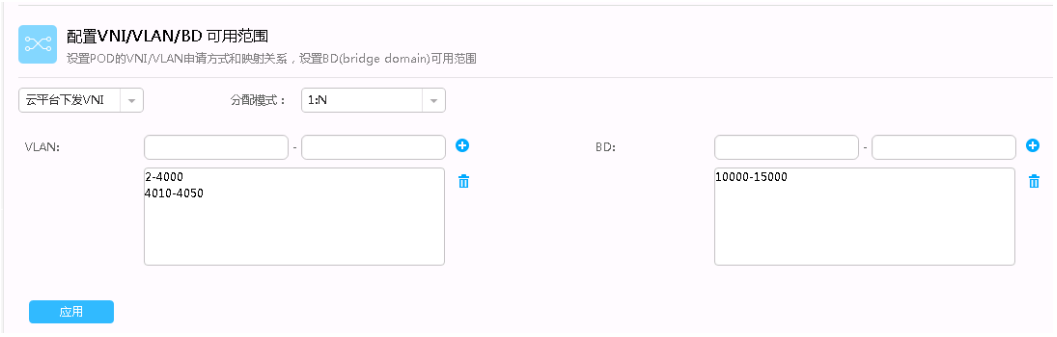
VM或物理服务器要通过VTEP接入到VXLAN网络，当服务器报文到达VTEP端口时，需要将服务器的VLAN Tag/Untag报文通过BD映射到VNI，从而使VTEP能封装正确的VXLAN帧。VTEP端口的这种映射配置，由AC-DCN下发，本节中即是指定AC-DCN下发这种配置时使用的**VLAN/VNI/BD**范围。

步骤1 选择“网络 > POD管理 > POD”。

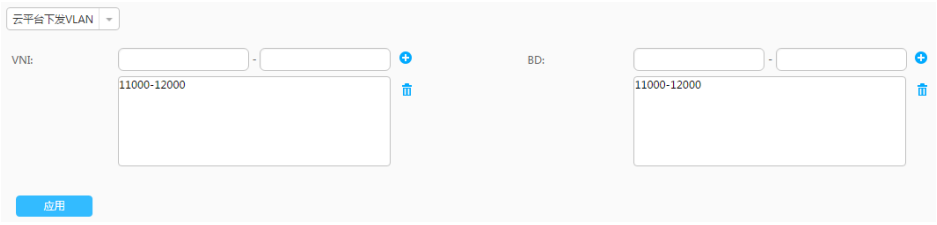
步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 选择“全局配置 > 配置VNI/VLAN/BD可用范围”，配置可用范围。

- AC-DCN与Fusionsphere OpenStack对接时，只需配置VLAN和BD的范围，并选择“云平台下发VNI”。



- AC-DCN与开源OpenStack对接时，只需配置VNI和BD的范围，并选择“云平台下发VLAN”。



----结束

4.2.5.13 配置 PXE 网络

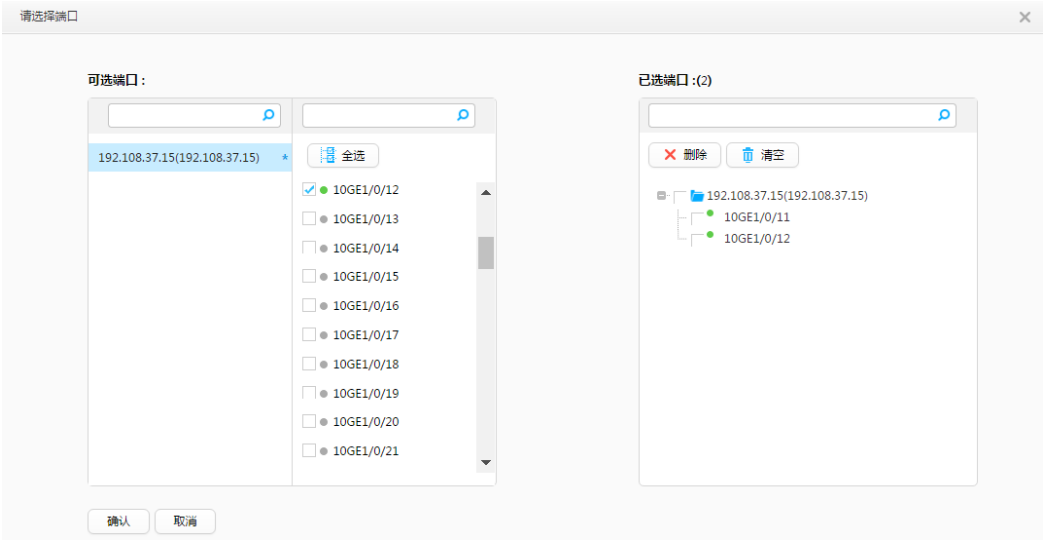
当网络中规划了裸金属服务器时，需要配置PXE网络，使裸金属服务器接入数据中心网络。

步骤1 选择“网络 > POD管理 > POD”，在POD列表中，选择指定的POD，进入到POD管理页面。

步骤2 在“全局配置”页面中，选择“PXE网络”，配置PXE网络的VLAN和VNI。

VNI的配置需要和PXE服务器上PXE网络的保持一致。

步骤3 填写VNI，单击“创建”。勾选接入交换机上连接裸金属服务器的接口，单击“确认”。



----结束

4.2.6 配置 AC-DCN 对接 Fusionsphere OpenStack

在AC-DCN与云平台FusionSphere OpenStack对接时，需通过AC-DCN的L2BR下发VXLAN管理网络，并在AC-DCN和FusionSphere OpenStack双方安装对接插件，最后创建北向接口用户用于两个平台之间的对接。

4.2.6.1 创建 FusionSphere 管理网络

AC-DCN与FusionSphere OpenStack云平台对接一般采用带内管理模式，即FusionSphere OpenStack的管理网络由AC-DCN下发L2BR来配置。

AC-DCN通过VLAN方式接入，在TOR或网关上创建三层VLANIF接口，将AC-DCN控制器和FusionSphere OpenStack的管理网段引入路由域，打通AC-DCN与FusionSphere OpenStack管理平面之间的路由。

通过AC-DCN下发L2BR打通FusionSphere OpenStack各个节点的管理网络。
FusionSphere OpenStack网络平面规划的一个示例（以IT侧规划为准）如下所示。

L2BR名称	类别/名称	接入类型	VNI	VLAN	网关类型	网关地址
Fsp	External_OM	dot1q	29901	1998	单机	10.100.2.254/24
	External_API	dot1q	29900	1999	单机	10.100.1.254/24
	Internal_base	Untag	29902	NA	NA	NA

步骤1 选择“网络 > POD管理 > POD”。在资源池列表中，选择指定的资源池，进入到资源池管理页面。

步骤2 在“服务配置”页面中，选择“L2BR端口组”，单击“创建”，创建L2BR。

步骤3 在“基本信息”页面，填写L2BR名称和描述信息，单击“确认”。

步骤4 在“选择端口”页面，勾选FusionSphere节点与TOR连接的端口，点击“下一步”。

步骤5 在“VXLAN”页面，点击“创建”，填写VXLAN相关信息，点击“下一步”。

说明

设置的VLAN号必须在“zh-cn_topic_0059220302.xml#ZH-CN_TOPIC_0059220302/zh-cn_topic_0050147978_ZH-CN_TOPIC_0050147978”中设置的VLAN范围以内。

步骤6 单击“完成”，完成L2BR的配置。

步骤7 在网关设备上，将FusionSphere OpenStack的管理网段在路由协议中宣告。

```
[~Gateway-CE12808-1] BGP 65000
[*Gateway-CE12808-1-bgp] ipv4-family unicast
[*Gateway-CE12808-1-bgp-af-ipv4] network 10.100.1.0 255.255.255.0
[*Gateway-CE12808-1-bgp-af-ipv4] network 10.100.2.0 255.255.255.0
[*Gateway-CE12808-1-bgp-af-ipv4] quit
[*Gateway-CE12808-1-bgp] quit
[*Gateway-CE12808-1] commit

[~Gateway-CE12808-2] BGP 65001
[*Gateway-CE12808-2-bgp] ipv4-family unicast
[*Gateway-CE12808-2-bgp-af-ipv4] network 10.100.1.0 255.255.255.0
[*Gateway-CE12808-2-bgp-af-ipv4] network 10.100.2.0 255.255.255.0
[*Gateway-CE12808-2-bgp-af-ipv4] quit
```

```
[*Gateway-CE12808-2-bgp] quit
[*Gateway-CE12808-2] commit
```

----结束

4.2.6.2 安装与配置 FusionSphere OpenStack

FusionSphere OpenStack侧的安装和配置操作由华为IT工程师实施。

FusionSphere OpenStack安装和配置的详细操作步骤请参见《**FusionSphere V100R006C00 产品文档 (云数据中心)**》的“安装与配置”。

4.2.6.3 安装对接插件

分别在AC-DCN和FusionSphere OpenStack侧安装用于对接的插件，插件信息参见下表。

安装端	插件类别	插件名称示例	插件发布源
AC-DCN	eSDK插件，用于和FusionSphere云平台对接	hw_plugin_ac.zip	AC-DCN
FusionSphere OpenStack	L2服务包	ACMECHANISMDRIVERV100R006C00RC3.tar.gz	FusionSphere
	L3服务包	ACROUTERAGENTV100R006C00RC3.tar.gz	FusionSphere
	L4~L7服务包	NEUTRONACPLUGINV100R001C00B752.tar.gz	AC-DCN

步骤1 在AC-DCN侧安装插件。

详细操作步骤请参考《**Agile Controller-DCN V200R001C00产品文档**》中的“安装与Underlay网络部署-软件安装--安装插件-与云平台（FusionSphere）协同的网络业务发放场景-在AC-DCN安装插件”。

步骤2 在FusionSphere侧安装插件。

详细操作步骤请参考《**FusionSphere V100R006C00 产品文档 (云数据中心)**》中的“软件安装指南-安装与配置-*（可选）配置FusionSphere OpenStack对接Agile Controller*”。

步骤3 验证对接结果。在FusionSphere OpenStack主机中，执行命令**neutron net-create** *XXX*

创建一个网络，其中XXX表示网络名称，可自定义。

出现如下图所示回显时，表示网络创建成功，意味着AC-DCN与FusionSphere对接成功。

```
+---------------------------+--------------------------------------+
| Field                     | Value                                |
+---------------------------+--------------------------------------+
| admin_state_up            | True                                 |
| id                        | 73eb2ffe-507a-4bf5-8d30-b3e5f826c949 |
| name                      | xxx                                  |
| provider:network_type     | vxlan                                |
| provider:physical_network |                                      |
| provider:segmentation_id  | 29987                                |
| router:external           | False                                |
| shared                    | False                                |
| status                    | ACTIVE                               |
| subnets                   |                                      |
| tenant_id                 | ff98d04ea514442da1fc866fa735ce4d     |
+---------------------------+--------------------------------------+
```

----结束

4.2.6.4 创建北向接口用户

北向接口用户用于AC-DCN与FusionSphere OpenStack的对接配置。FusionSphere OpenStack上配置的AC-DCN北向用户的用户名和密码需要和AC-DCN上创建的北向用户的用户名和密码保持一致。

步骤1 使用admin账号登录到AC-DCN，在主菜单中选择“系统 > 管理员 > 管理员”。

步骤2 单击“创建”，设置北向用户的基本信息。

步骤3 在“账号”栏输入北向用户的用户名和密码，用户名建议为fsp@huawei.com。

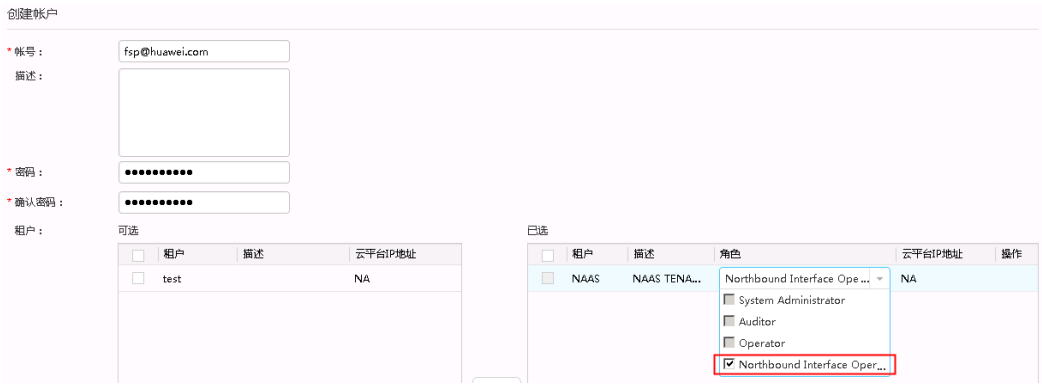
说明

此处北向用户名，需要与FusionSphere中配置的与AC-DCN对接的参数值“ac_username”一致。

此处设置的密码，不能设置成规划中的最终密码，下述步骤8中有强制修改密码的操作。

步骤4 在“角色”下拉列表中，勾选用户角色为“Northbound Interface Operator”。

步骤5 单击“确定”。



步骤6 单击页面右上角，注销当前账户。

步骤7 使用新创建的北向用户重新登录AC-DCN。

步骤8 登录成功后，根据提示完成密码修改，修改密码，如：Huawei@123。

说明

此步骤中设置的密码，需要与FusionSphere中配置的与AC-DCN对接的参数值“ac_password”一致。

步骤9 密码修改完毕后，系统会在5秒后自动跳转到登录页面。使用北向用户重新登录AC-DCN，验证修改的密码是否正确。

显示如下图所示界面，提示权限不足，说明北向用户创建并修改密码成功。

----结束

4.2.6.5 创建云平台

在AC-DCN上创建一个云平台，配置要对接的云平台的相关信息。

步骤1 选择“系统 > 系统设置 > 云平台”，单击“创建”。

步骤2 配置与云管理平台对接参数，与云管理平台建立对接。

- “代理名称”：FusionSphere物理网络名称，默认名称为“physnet1”，可登录FusionSphere OpenStack安装部署界面，在“资源 > 网络 > 物理网络”中查看所需使用的物理网络的名称（即与云平台的ac_service_name参数保持一致）。
- “账号”：北向用户的账号，如fsp@huawei.com。
- “驱动插件IP”、“云平台IP”：一般设置为云管理平台反向代理IP地址。

----结束

4.2.6.6 将云平台绑定到 POD

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 选择“全局配置”，页面，在“连接云平台”一栏，勾选指定代理名称的云管理平台，单击“应用”。

----结束

4.2.6.7 将服务器添加到 POD

完成FusionSphere、FusionCompute安装部署之后，所有FusionSphere节点、CAN节点和虚拟化服务器全部使能LLDP，在AC上重新发现链路，主要是发现接入交换机与服务器节点之间的拓扑信息，并将发现上来服务器添加到POD中。

- 完成FusionSphere安装之后，所有FusionSphere节点的全部使能LLDP，在AC-DCN上可以自动重新发现链路。
- 物理服务器和一些不开启LLDP的服务器，需要通过手动添加的方式关联到它们连接的TOR上。

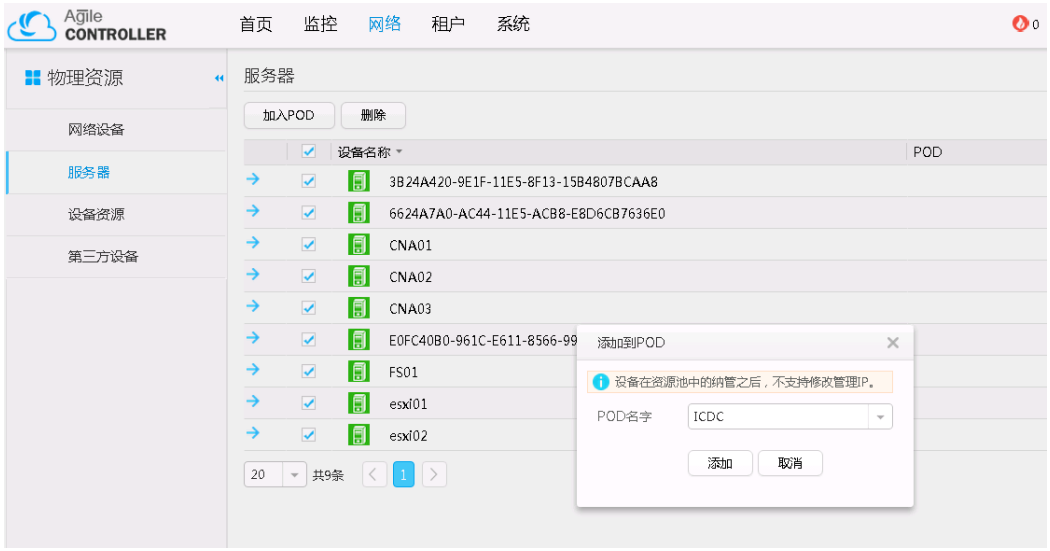
自动发现并添加节点

步骤1 在主菜单中选择“网络 > 链路管理 > 链路”。

步骤2 单击“链路发现”，全选设备，将“LLDP使能”设置为“ON”，然后单击“发现”，重新对设备做链路自动发现。

步骤3 当进度条达成100%时，单击“完成”。此时，交换机与服务器之间的链路发现成功。

步骤4 选择“网络 > 物理资源 > 服务器”，选择需要添加到POD中的主机，单击“加入POD”，将服务器节点添加到POD中。



说明

需要将云平台所有服务器、虚拟化服务器添加到POD。

----结束

手动添加服务器

如果服务器不开启LLDP功能或不支持LLDP功能（如物理服务器），TOR和HOST的对应关系需要在AC-DCN界面上手动添加。

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 单击“交换机”，选择“L2交换机-Host服务器”页签，单击“增加”。

步骤4 在“增加”窗口中选择TOR交换机和对应的物理接口，填写服务器名称，单击“确定”。

步骤5 添加完成后，单击对应TOR“设备名称”前的⊞，检查TOR与HOST服务器之间的链路，确保与规划的链路链接一致。

----结束

配置裸金属服务器接入网络

当网络中规划了裸金属服务器时，需要在裸金属服务器与接入交换机连接的接口上，预置好PXE网络。PXE网络是裸金属服务器业务发放的初始网络。

前提条件：

- 在FusionSphere CPS上已完成裸金属服务部署并成功对接FusionSphere OpenStack。
- 已将裸金属服务器接入PXE网络，并完成BMC Base和Provision网络配置。

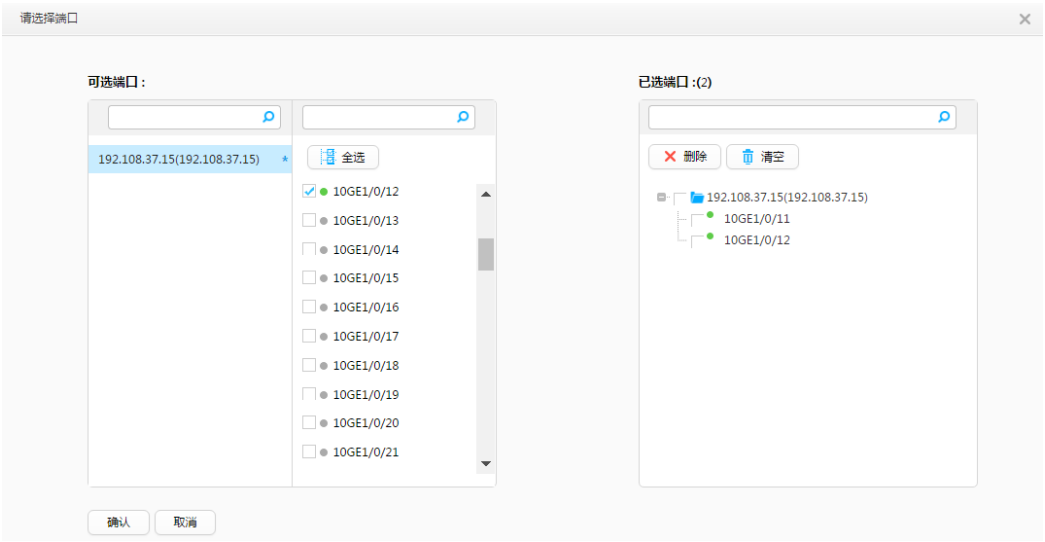
AC-DCN上配置PXE网络步骤如下：

步骤1 选择“网络 > POD管理 > POD”，在POD列表中，选择指定的POD，进入到POD管理页面。

步骤2 在“全局配置”页面中，选择“PXE网络”，配置PXE网络的VLAN和VNI。

VNI的配置需要和PXE服务器上PXE网络配置保持一致。

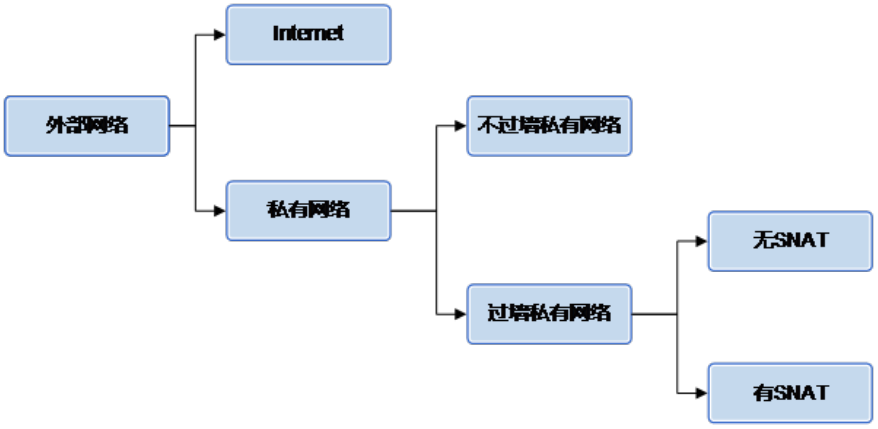
步骤3 填写VNI，单击“创建”。勾选接入交换机上连接裸金属服务器的接口，单击“确认”。



----结束

4.2.6.8 创建外部网络

外部网络主要分为Internet类型和私有类型两大类。在云网一体化场景中只有Internet类型的外部网络。



外部网络类型为 Internet

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 选择“服务配置”，在“外部网络”栏中单击“创建”。

步骤4 填写外部网络基本信息。单击“下一步”。

步骤5 填写网关信息，单击“下一步”。

- 网关类型选择为多活。
- 选择网关组的组名。
- 选择网关IP。

步骤6 检查并确认配置。

步骤7 在云平台上添加外部网络时，外部网络可以有多个，但是必须以AC-DCN上定义的外部网络的名称为前缀。例如：AC-DCN上定义的外部网络名称是ext，则云平台上定义的外部网络名称可以是ext01、ext02等。

----结束

4.2.6.9 配置 FusionSphere 与 VMM 对接

将vCenter作为虚拟化资源池接入到FusionSphere OpenStack中，以便FusionSphere OpenStack对各种虚拟化资源进行统一管理。此处操作由云平台提供方实施。

步骤1 安装VMM。

以vCenter虚拟化平台为例，其安装步骤包括ESXi主机安装与配置、vCenter安装与配置、创建VDS和配置共享存储。详细的配置步骤请浏览**VMware官方网站**，进入“支持 > 支持资源 > 产品文档”中获取。

说明

安装ESXi主机安装时，牢记设置的ESXi主机登录密码。使用root用户登录vCenter客户端时，需要使用该密码。一旦忘记密码，无法重置，只能重装后重新设置密码。

步骤2 配置FusionSphere与vCenter对接。

FusionSphere与vCenter的对接详细操作请参考《**FusionSphere V100R006C00 产品文档(云数据中心)**》中的“软件安装指南-安装与配置-配置vCenter接入FusionSphere OpenStack”。

----结束

4.2.7 配置 AC-DCN 对接开源 OpenStack

4.2.7.1 创建 OpenStack 管理网络

AC-DCN与OpenStack云平台对接一般采用带内管理模式，即OpenStack的管理网络由AC-DCN下发L2BR来配置。

AC-DCN通过VLAN方式接入，在TOR或网关上创建三层VLANIF接口，将AC-DCN控制器和OpenStack的管理网段引入路由域，打通AC-DCN与OpenStack管理平面之间的路由。

通过AC-DCN下发L2BR打通OpenStack各个节点的管理网络。

OpenStack网络平面规划以下表为例。

L2BR名称	类别/名称	接入类型	VNI	VLAN	网关类型	网关地址
Ops	External_OM	untag	29901	1998	多活	10.100.2.254/24

步骤1 选择“网络 > POD管理 > POD”。在资源池列表中，选择指定的资源池，进入到资源池管理页面。

步骤2 在“服务配置”页面中，选择“L2BR端口组”，单击“创建”，创建L2BR。

步骤3 在“基本信息”页面，填写L2BR名称和描述信息，单击“确认”。

步骤4 在“选择端口”页面，勾选OpenStack节点与TOR连接的端口，点击“下一步”。

步骤5 在“VXLAN”页面，点击“创建”，填写VXLAN相关信息，点击“下一步”。

说明

如果接入类型是Tag模式，则设置的VLAN号必须在“配置VNI/VLAN/BD的可用范围”中设置的VLAN范围以内。

步骤6 单击“完成”，完成L2BR的配置。

步骤7 在网关设备上，将OpenStack的管理网段在路由协议中宣告。

```
[~Gateway-CE12808-1] BGP 65000
[*Gateway-CE12808-1-bgp] ipv4-family unicast
[*Gateway-CE12808-1-bgp-af-ipv4] network 10.100.2.0 255.255.255.0
[*Gateway-CE12808-1-bgp-af-ipv4] quit
[*Gateway-CE12808-1-bgp] quit
[*Gateway-CE12808-1] commit

[~Gateway-CE12808-2]BGP 65001
[*Gateway-CE12808-2-bgp] ipv4-family unicast
[*Gateway-CE12808-2-bgp-af-ipv4] network 10.100.2.0 255.255.255.0
[*Gateway-CE12808-2-bgp-af-ipv4] quit
```

```
[*Gateway-CE12808-2-bgp] quit
[*Gateway-CE12808-2] commit
```

----结束

4.2.7.2 安装与配置 OpenStack

说明

一般情况下，开源云平台OpenStack的安装和操作由客户或第三方云平台厂家实施。

步骤1 安装服务器的操作系统。

步骤2 修改服务器的网络配置。

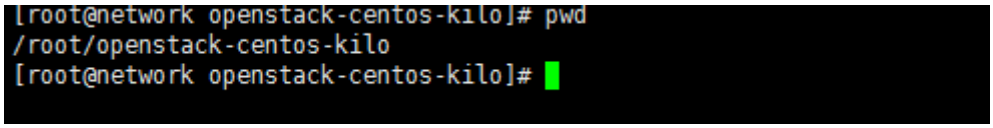
1. 以root用户身份登录系统。
2. 执行如下命令编辑网络配置文件。

```
vi /etc/sysconfig/network-scripts/ifcfg-ens33 // ens33为实际物理网卡名称
```

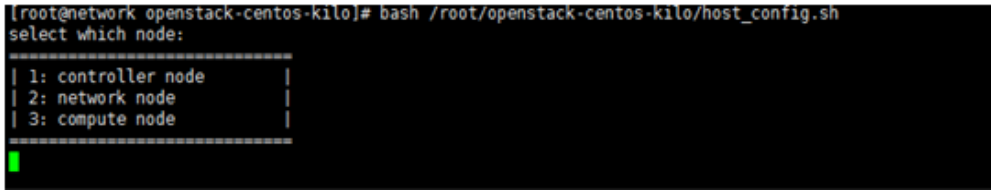
3. 单击**a**键，进入编辑模式，按方向键移动光标对文件中如下修改项进行修改：
   - BOOTPROTO修改为**static**
   - ONBOOT修改为**yes**
   - 添加IP地址（IPADDR）、掩码（NETMASK）和网关（GATEWAY）
4. 按esc键退编辑模式。
5. 执行命令**:wq!**保存该文件。
6. 执行命令**reboot**重启系统。

步骤3 配置主机。

1. 使用root用户登录操作系统，使用SFTP工具（如XSHELL）拷贝openstack-centos-kilo到root路径下。



2. 执行脚本bash /root/openstack-centos-kilo/host_config.sh，配置主机。

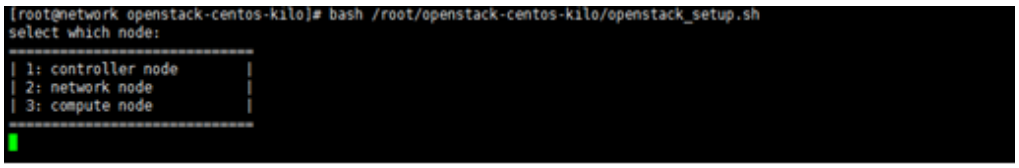


3. 选择当前服务器将要安装的角色

   如果选择2或者3，需要输入控制节点的IP。

4. 等待配置完成后，执行命令**reboot**，重启服务器。

步骤4 执行脚本bash /root/openstack-centos-kilo/openstack_setup.sh，安装Openstack。



步骤5 选择当前服务器将要安装的角色（与步骤3的选择保持一致），进行安装。

安装的详细日志记录在/var/log/opsinstall目录下。

----结束

4.2.7.3 安装对接插件

步骤1 在AC-DCN侧安装对接插件。

详细操作步骤请参考《**Agile Controller-DCN V200R001C00产品文档**》中的“安装与Underlay网络配置-软件安装-安装插件-与云平台（OpenStack）协同的网络业务发放场景-在AC-DCN安装插件”。

步骤2 在OpenStack侧安装插件

详细操作步骤的参考链接同上。

----结束

4.2.7.4 在 OpenStack 上执行对接操作

步骤1 通过ovs创建bond端口（此步骤要在所有计算和网络节点进行配置，且服务器双网卡与tor连接）。

1. 首先配置需要绑定成bond的端口为激活状态。

   不同的系统或系统版本命令可能存在差异，此处以Ubuntu 14.04.1举例（注：如果没有下一步中的网卡配置文件，此步骤可以忽略，直接执行第2大步骤）。

2. 执行命令**vi /etc/network/interfaces**编辑网卡配置文件。

3. 修改eth1和eth2的配置。

   ```
   auto eth1
   iface eth1 inet manual

   auto eth2
   iface eth2 inet manual
   ```

4. 保存退出后，执行命令**sudo /etc/init.d/networking restart**重启网络服务。

   如果无法生效可以使用以下命令一个个重启网卡。

   ```
   ifdown eth1
   ifup eth1
   ```

   如果还是不行，重启系统。

步骤2 使用ovs命令绑定bond。

1. 执行命令**ovs-vsctl del-br br-eth1**删除默认网桥br-eth1。
2. 执行命令**ovs-vsctl add-br br-bond1**创建网桥br-bond1。
3. 执行命令**ovs-vsctl add-bond br-bond1 bond1 eth1 eth2**网桥绑定物理端口（主备模式到这里结束）。
4. （选配）如果是负载均衡模式，再增加配置命令**ovs-vsctl set Port bond1 bond_mode=balance-slb lacp=active**。
5. 执行命令**ovs-vsctl show**检查并确认ovs的配置。

步骤3 配置Openstack业务网桥为br-bond1。

1. 备份ml2配置文件。
2. 执行命令**vi /etc/neutron/plugins/ml2/ml2_conf.ini**修改ml2配置文件。
3. 找到bridge_mappings配置：

   ```
   bridge_mappings = physnet1:br-eth1
   ```

   修改为br-bond1：

   ```
   bridge_mappings = physnet1:br-bond1
   ```

   如果没有此语句，添加上：

   ```
   bridge_mappings = physnet1:br-bond1
   ```

   “local_ip”为本机IP地址，确保此句在“[ovs]”下面，如下所示。

   ```
   [ovs]
   local_ip = 192.168.12.162
   #bridge_mappings = external:br-ex
   bridge_mappings = physnet1:br-bond1
   [agent]
   ```

4. 执行命令**service neutron -openvswitch-agent restart**重启neutron -openvswitch-agent服务，服务重启后检测下业务是否OK。
5. 执行命令**ovs-appctl bond/show**查看如下状态说明已配置好了。

   ```
   [root@network neutron]# ovs-appctl bond/show
   ---- bond1 ----
   bond_mode: active-backup
   bond may use recirculation: no, Recirc-ID : -1
   bond-hash-basis: 0
   updelay: 0 ms
   downdelay: 0 ms
   lacp_status: off
   active slave mac: a4:dc:be:f1:0f:25(enp2s0f3)

   slave enp2s0f2: enabled
           may_enable: true

   slave enp2s0f3: enabled
           active slave
           may_enable: true
   ```

步骤4 单网卡配置br-int（所有网络和计算节点上）。

1. 执行命令**ovs-vsctl list-br**查看是否有br-eth1。

   如果br-eth1被删掉，先执行命令**ovs-vsctl add-br br-eth1**添加网桥，然后再执行命令**ovs-vsctl list-br**查看一下是否真正添加成功。
2. 执行命令**ovs-vsctl del-br br-tun**删除br-tun网桥口。
3. 执行命令**vi /etc/neutron/plugins/ml2/ml2_conf.ini**修改配置文件。

4. 找到bridge_mappings配置，修改为br-eth1（如果没有添加上此语句）。

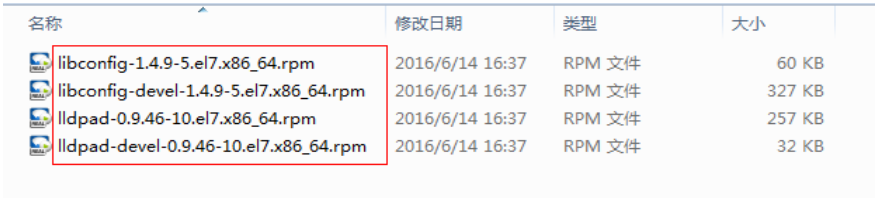
```
[ovs]
local_ip = 172.168.10.16
bridge_mappings = physnet1:br-eth1
```

其中“local_ip”为本机IP地址。

5. 执行命令**service neutron -openvswitch-agent restart**重启neutron -openvswitch-agent服务。

步骤5 配置计算和网络节点服务器使能LLDP。

1. 将LLDP的RPM包上传到计算和网络节点。



名称	修改日期	类型	大小
libconfig-1.4.9-5.el7.x86_64.rpm	2016/6/14 16:37	RPM 文件	60 KB
libconfig-devel-1.4.9-5.el7.x86_64.rpm	2016/6/14 16:37	RPM 文件	327 KB
lldpad-0.9.46-10.el7.x86_64.rpm	2016/6/14 16:37	RPM 文件	257 KB
lldpad-devel-0.9.46-10.el7.x86_64.rpm	2016/6/14 16:37	RPM 文件	32 KB

2. 进入目录下，依次执行如下命令进行安装。

```
rpm -ivh libconfig-1.4.9-5.el7.x86_64.rpmrpm -ivh libconfig-devel-1.4.9-5.el7.x86_64.rpmrpm -ivh lldpad-0.9.46-10.el7.x86_64.rpmrpm -ivh lldpad-devel-0.9.46-10.el7.x86_64.rpm
```

3. 四个命令执行完成后，在对应的网口使能LLDP，其中“**enp2s0f2**”为网卡名称。

```
lldpad -dlldptool set-lldp -i enp2s0f2 adminStatus=rxtxlldptool -T -i enp2s0f2 -V sysName enableTx=yeslldptool -T -i enp2s0f2 -V portDesc enableTx=yeslldptool -T -i enp2s0f2 -V sysDesc enableTx=yes
```

如果是双网卡连接TOR，两个网卡都要顺序执行以上命令，注意把“enp2s0f2”换成对应连接交换机的网卡名。

步骤6 修改网络类型（VXLAN网络下发）。

1. 执行命令**vim /etc/neutron/plugins/ml2/ml2_conf.ini**修改控制节点对应节点文件，按照以下截图修改。

```
[ml2]
type_drivers = flat,vlan,gre,vxlan
tenant_network_types = vxlan,vlan
#mechanism_drivers = huawei,l2population
mechanism_drivers = huawei,openvswitch

[ml2_type_gre]
tunnel_id_ranges = 1:1000

[ml2_type_vlan]
network_vlan_ranges = physnet1:600:700

[securitygroup]
enable_security_group = True
enable_ipset = True
firewall_driver = neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver
[ml2_type_vxlan]
vni_ranges =4096:99999
~
~
~
~
~
~
~
```

此vlan为外部网络指定vlan值，不是内部网络指定值

2. 执行命令**systemctl restart neutron-server.service**重启服务。
3. 执行命令**vim /etc/neutron/plugins/ml2/ml2_conf.ini**修改网络节点对应配置文件，按照以下截图修改（local_ip除外）。

```
[ml2]
type_drivers = flat,vlan,gre,vxlan
tenant_network_types = vxlan
mechanism_drivers = openvswitch

[ml2_type_flat]
flat_networks = external

[ml2_type_gre]
tunnel_id_ranges = 4096:99999

[ml2_type_vxlan]
vni_ranges =4096:99999

[securitygroup]
enable_security_group = True
enable_ipset = True
firewall_driver = neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver

[ovs]
local_ip = 192.168.12.162
#bridge_mappings = external:br-ex
bridge_mappings = physnet1:br-bond1
[agent]
tunnel_types = vxlan
~
~
~
~
~
~
```

4. 执行命令**systemctl restart neutron-openvswitch-agent.service**重启服务。
5. 执行命令**vim /etc/neutron/plugins/ml2/ml2_conf.ini**修改计算节点对应配置文件，按照以下截图修改（local_ip除外）。

```
[ml2]
type_drivers = flat,vlan,gre,vxlan
tenant_network_types = vxlan
mechanism_drivers = openvswitch

[ml2_type_gre]
tunnel_id_ranges = 4096:99999

[ml2_type_vxlan]
vni_ranges =4096:99999

[securitygroup]
enable_security_group = True
enable_ipset = True
firewall_driver = neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver

[ovs]
local_ip = 192.168.12.160
bridge_mappings = physnet1:br-bond1
[agent]
tunnel_types = vxlan
~
~
~
~
~
```

执行命令**systemctl restart neutron-openvswitch-agent.service**重启服务。

步骤7 修改网络类型（VLAN网络下发）。

1. 在控制节点执行命令**vim /etc/neutron/plugins/ml2/ml2_conf.ini**修改配置文件，按照以下截图修改。

```
[ml2]
type_drivers = flat,vlan,gre,vxlan
tenant_network_types = vlan
#tenant_network_types = vxlan
mechanism_drivers = huawei,openvswitch

[ml2_type_gre]
tunnel_id_ranges = 1:1000

[securitygroup]
enable_security_group = True
enable_ipset = True
firewall_driver = neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver

[ml2_type_vlan]
network_vlan_ranges = physnet1:2:4094

#[ml2_type_vxlan]
#vni_ranges = 10000:11000
~
~
~
```

2. 在网络节点执行命令**vim /etc/neutron/plugins/ml2/ml2_conf.ini**修改对应配置文件，按照以下截图修改（local_ip除外）。

```
[ml2]
type_drivers = flat,vlan,gre,vxlan
#tenant_network_types = vxlan
tenant_network_types = vlan
mechanism_drivers = openvswitch

[ml2_type_flat]
flat_networks = external

[ml2_type_gre]
tunnel_id_ranges = 1:1000

[ml2_type_vlan]
network_vlan_ranges = physnet1:2:4094

[securitygroup]
enable_security_group = True
enable_ipset = True
firewall_driver = neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver

[ovs]
local_ip = 189.193.64.121
bridge_mappings = physnet1:br-eth1

#[agent]
#tunnel_types = vxlan
~
~
~
~
```

3. 在计算节点执行命令**vim /etc/neutron/plugins/ml2/ml2_conf.ini**修改对应配置文件，按照以下截图修改（local_ip除外）。

```
[ml2]
type_drivers = flat,vlan,gre,vxlan
#tenant_network_types = vxlan
tenant_network_types = vlan
mechanism_drivers = openvswitch

[ml2_type_vlan]
network_vlan_ranges = physnet1:2:4094

[ml2_type_gre]
tunnel_id_ranges = 1:1000

[securitygroup]
enable_security_group = True
enable_ipset = True
firewall_driver = neutron.agent.linux.iptables_firewall.OVSHybridIptablesFirewallDriver

[ovs]
local_ip = 189.193.64.118
bridge_mappings = physnet1:br-eth1

#[agent]
#tunnel_types = gre
~
~
~
```

----结束

4.2.7.5 创建北向接口用户

用户最终使用北向用户的用户名，必须设置为：“esdk@huawei.com”，密码必须设置为：“Huawei@123”。因为在云平台的插件中的配置文件中已经保存了AC-DCN北向用户使用的用户名和密码。

步骤1 使用admin账号登录到AC-DCN。

步骤2 在主菜单选择“系统 > 管理员 > 管理员”。

步骤3 创建北向用户。单击“创建”，设置北向用户的基本信息。

1. 设置“帐号”为“esdk@huawei.com”。
2. 设置“密码”为“Admin@1234”。

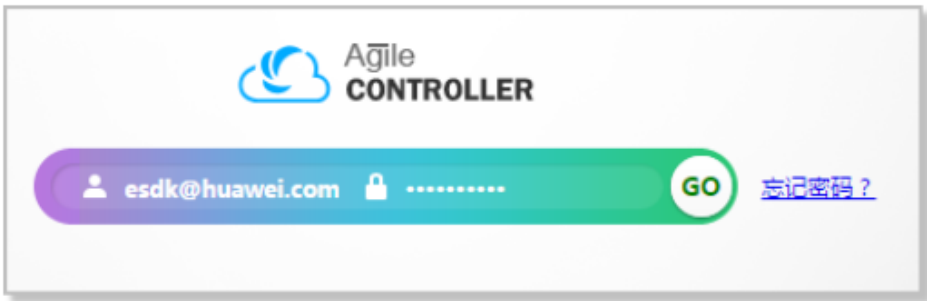
   说明

   初次创建的北向用户的密码可以任意设置，但是不能设置为最终使用的密码为“Huawei@123”。AC-DCN要求初次登录的用户必须修改密码。
3. 设置“确认密码”为“Admin@1234”。

4. 在“角色”中，选择“Northbound Interface Operator”。
5. 单击“确定”。

步骤4 单击页面右上角，注销当前账户。

步骤5 使用新创建的北向用户重新登录AC-DCN。



步骤6 登录成功后，根据提示完成密码修改，修改密码为：“Huawei@123”。

步骤7 密码修改完毕后，系统会在5秒后自动跳转到登录页面。使用北向用户重新登录AC-DCN，验证修改的密码是否正确。

显示如下图所示界面，提示权限不足，说明北向用户创建并修改密码成功。

----结束

4.2.7.6 创建云平台

绑定云管理平台和AC-DCN的POD，使云管理平台网络业务通过AC-DCN完成自动化部署。

步骤1 选择“系统 > 系统设置 > 云平台”，单击“创建”。

步骤2 配置与云管理平台对接参数，与云管理平台建立对接。

- “代理名称”：OpenStack（Kilo）的代理名称。需要跟OpenStack（Kilo）控制节点根目录下的“config.ini”配置文件中的设置保持一致，查看代理名称，执行如下命令。

```
[root@controller neutron] # more /etc/neutron/config.ini
[opensdk]
service_name=physnet1
```

  OpenStack（Kilo）配置文件中代理名称默认为“physnet1”，如果使用其他名称，需要同时修改配置文件中的名称。在OpenStack（Kilo）控制节点根目录下，修改代理名称，执行如下操作。

  a. 进入控制节点根目录，执行如下命令：**# vim /etc/neutron/config.ini**
  b. 按“i”键，进入编辑模式。将“service_name”修改成用户使用的代理名称。
  c. 按“Esc”键，退出编辑模式。
  d. 输入“:wq!”，保存修改。

  - “帐号”：北向用户的帐号，设置为“esdk@huawei.com”。
  - “驱动插件IP”：AC-DCN通过插件与云平台对接时，安装插件的服务器IP地址就是驱动插件IP; 如果不是插件方式对接，此项可以填写云平台IP地址。
  - “云平台IP”：云管理平台IP地址。

----结束

4.2.7.7 将云平台绑定到 POD

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 选择“全局配置”，页面，在“连接云平台”一栏，勾选指定代理名称的云管理平台，单击“应用”。

----结束

4.2.7.8 将服务器添加到 POD

完成云平台安装部署后，所有物理服务器和虚拟化服务器全部使能LLDP，在AC-DCN上重新发现链路，主要是发现接入交换机与服务器节点之间的拓扑信息，并将发现上来服务器添加到POD中。

- 完成OpenStack安装之后，所有OpenStack节点的全部使能LLDP，在AC-DCN上可以自动重新发现链路。

- 物理服务器和一些不开启LLDP的服务器，需要通过手动添加的方式关联到它们连接的TOR上。

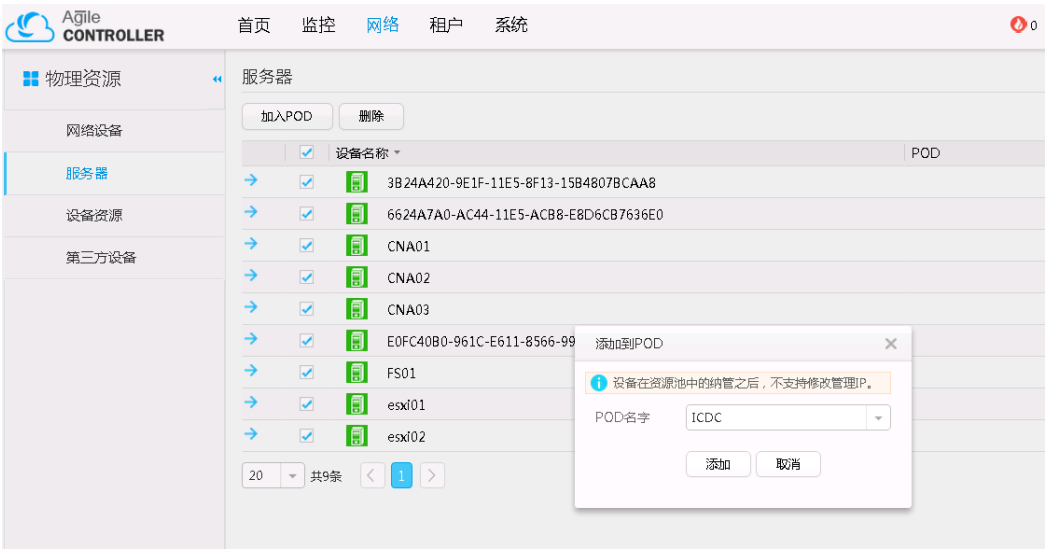
自动发现并添加节点

步骤1 在主菜单中选择“网络 > 链路管理 > 链路”。

步骤2 单击“链路发现”，全选设备，将“LLDP使能”设置为“ON”，然后单击“发现”，重新对设备做链路自动发现。

步骤3 当进度条达成100%时，单击“完成”。此时，交换机与服务器之间的链路发现成功。

步骤4 选择“网络 > 物理资源 > 服务器”，选择需要添加到POD中的主机，单击“加入POD”，将服务器节点添加到POD中。



说明

需要将云平台所有服务器、虚拟化服务器添加到POD。

----结束

手动添加服务器

如果服务器不开启LLDP功能或不支持LLDP功能（如物理服务器），TOR和HOST的对应关系需要在AC-DCN界面上手动添加。

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 单击“交换机”，选择“L2交换机-Host服务器”页签，单击“增加”。

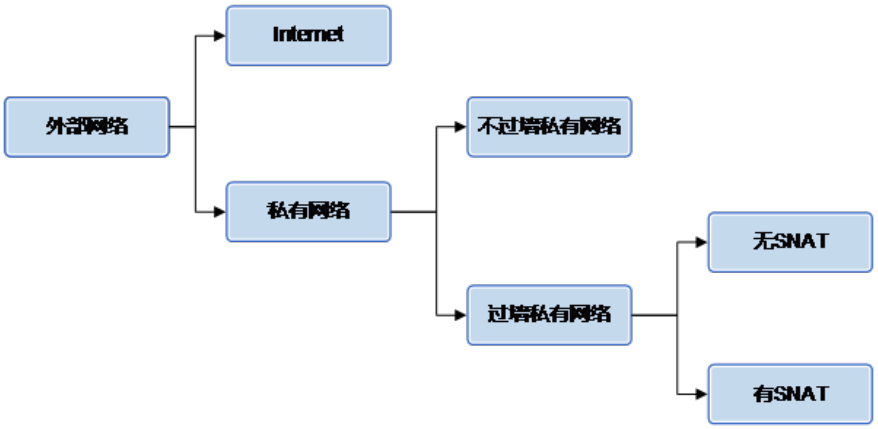
步骤4 在“增加”窗口中选择TOR交换机和对应的物理接口，填写服务器名称，单击“确定”。

步骤5 添加完成后，单击对应TOR“设备名称”前的，检查TOR与HOST服务器之间的链路，确保与规划的链路链接一致。

----结束

4.2.7.9 创建外部网络

外部网络主要分为Internet类型和私有类型两大类。具体分类参见下图。在云网一体化场景中只有Internet类型的外部网络。



外部网络类型为 Internet

步骤1 选择“网络 > POD管理 > POD”。

步骤2 在POD列表中，选择指定的POD，进入到POD管理页面。

步骤3 选择“服务配置”，在“外部网络”栏中单击“创建”。

步骤4 填写外部网络名称，并选择外部网络类型是“Internet”。单击“下一步”。

步骤5 填写网关信息，选择多活网关组，单击“下一步”。

步骤6 检查并确认配置。

步骤7 在云平台上添加外部网络时，外部网络可以有多个，但是必须以AC-DCN上定义的外部网络的名称为前缀。例如：AC-DCN上定义的外部网络名称是ext，则云平台上定义的外部网络名称可以是ext01、ext02等。

----结束

4.2.7.10 配置 OpenStack 与 VMM 对接

由客户或第三方云平台厂商实施。可登录**OpenStack官方网站**，获取文档支撑。

4.2.8 部署 Overlay 网络

网络和业务的创建、下发，在云平台的Protal上实现。

- 如果云平台是华为FusionSphere OpenStack，则Protal操作在ManageOne上由IT侧实施，具体的操作步骤请参见《**ManageOne 3.0 产品文档**》中的“运营指引”。
- 如果是在开源OpenStack云平台上下发业务，由客户或第三方云平台厂商实施。可登录**OpenStack官方网站**，获取文档支撑。

4.2.9 常用操作指导

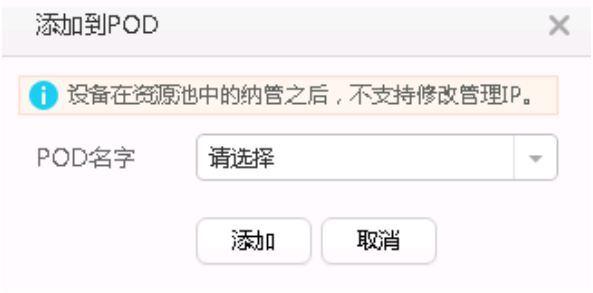
4.2.9.1 扩容设备

步骤1 登录AC-DCN，在主菜单中选择“网络 > 物理资源 > 网络设备”，单击“自动发现”。

步骤2 填写新增设备的IP网段及SNMPv3发现协议参数，单击“开始”，将新增设备发现到AC-DCN中。

步骤3 在主菜单中选择“网络 > 物理资源 > 网络设备”，选择新发现上来的TOR节点，点击“加入POD”。

步骤4 在“添加到POD”对话框中选择POD的名字，将新增设备添加到改资源池中。



步骤5 自动发现新增TOR的链路，在主菜单中选择“网络 > 链路管理 > 链路”；单击“链路发现”。勾选所有设备后单击“发现”，重新对设备做链路自动发现。

步骤6 进入创建的POD资源池，点击“设备”标签，点击“交换机”，点击新增的TOR节点后面的“Netconf”，填写netconf相关参数（端口号为22）。

步骤7 设置TOR在POD中的角色。

可以在以下两种方式中，选择其中一种，配置POD中各个设备的角色。

- （推荐）在POD的“拓扑”页面中，右键对应的设备图标，设置设备的角色。
  本例中右键新增的TOR后，单击“设置为接入交换机”。
- 在POD“设备”页面中，选择“物理网络设备”，在物理网络设备列表中，配置POD设备的角色。

本例中勾选新增的TOR后，单击“设置为接入交换机”，再单击“保存配置”。

步骤8 在主菜单中选择“网络 > POD管理 > POD”。在“设备”页面中，选择“虚拟网络节点”，选中新增的网络设备，点击“读设备VTEP IP”。

----结束

4.2.9.2 替换设备

执行设备替换的前提条件是：

- 新设备的设备型号、接口等硬件信息与旧设备完全一致。
- 新设备的软件版本与旧设备相同或高于旧设备。
- 新设备已经加载License，且License的规格不低于旧设备。
- 新设备当前未被AC-DCN管理，未与AC-DCN建立连接。
- 新设备的内存足够保存最新的配置文件。

设备替换操作即旧设备的离线和新设备的上线，AC-DCN相当于感知了一次设备的重启操作。

步骤1 在AC-DCN选择“网络 > 物理资源 > 网络设备”，勾选待替换的设备，单击“替换”，进入设备替换向导界面。

步骤2 参考前提条件进行设备替换前的检查，单击“下一步”。

步骤3 登录旧设备命令行，备份设备配置文件。

注意

保存配置文件后，请立即进行旧设备下电和移除，不要再向设备下发业务，否则会导致部分未在配置文件中保存的业务无法恢复。请不要修改该配置文件。如果设备创建了VS，请另行备份和恢复非VS0的配置文件。

步骤4 将旧设备下电，从网络中移除。

步骤5 在设备替换向导界面单击“清除公钥”。

步骤6 将新设备接入网络，请确保设备上的所有物理连线与旧设备保持一致。

步骤7 将新设备上电，导入备份的配置文件，并将其设置为下次启动时的配置文件。

步骤8 重启新设备，重启时选择不保存当前配置。设备重启成功后，将自动在AC-DCN中上线。

说明

重启后，设备将自动进行配置恢复，配置恢复需要一段时间，请耐心等待5~10分钟。

步骤9 新设备配置恢复后，执行命令**rsalocal-key-pair create**生成本地RSA密钥对，用于与AC-DCN建立NETCONF连接，该密钥对在设备重启后不会丢失。

密钥对生成后，可以执行命令**display rsa local-key-pair public**查看本地密钥对中的公钥部分信息。

步骤10 在设备替换向导界面单击“清除公钥”，重新清除设备公钥。

步骤11 在设备替换向导界面单击“检查连接”，确认AC-DCN与设备的NETCONF连接正常，单击“下一步”。

说明

如果设备的NETCONF连接失败，请重新配置:

1. 配置设备侧NETCONF参数。
2. 在AC-DCN上选择“网络 > POD管理 > POD”，选择“设备”页签。
3. 根据设备角色选择“接入交换机”或“汇聚交换机”页签，找到目标设备并单击“Netconf”。
4. 在“Netconf配置”窗口设置连接参数，与设备侧的配置保持一致。

步骤12 单击“设备审计”，检查新设备配置审计结果，确认业务正常恢复。

- 如果审计结果正常，表示新设备业务恢复成功。
- 如果审计结果有异常，请逐一确认是否要修复设备上的配置。

----结束

4.2.9.3 删除设备

当用户组网中的物理设备不再继续使用时，需要将该设备从POD中删除。在从POD删除设备前，必须先将上层业务占用的设备资源释放掉，删除相应业务即可释放资源。在POD删除具体的网络设备时，页面将提示当前设备的哪些资源被业务占用了，请参考下表来释放资源。

表1-6 不同资源项的释放指导

资源项	对应业务	资源释放操作
VLAN资源	DHCP Neutron Port业务	1. 在AC-DCN界面选择“租户 > 租户管理 > 租户”。 2. 单击租户名称，选择“端口”。 3. 查看端口详情中的接入设备信息，如果接入设备是待删除设备，请记录端口名称。 4. 登录云管理平台，删除记录的端口。
	裸金属服务器Neutron Port业务	在云管理平台释放裸金属服务器
	VM的Neutron Port业务	选择“网络 > POD管理 > POD > 设备 > 虚拟机”，查看虚拟机接入的交换机。 删除接入在待删除交换机上的所有虚拟机。
	LB的Neutron Port业务	在AC-DCN界面选择“租户 > 租户管理 > 租户”。 单击租户名称，选择“端口”。 查看端口详情中的接入设备信息，如果接入设备是待删除设备，请记录端口名称。 登录云管理平台，删除记录的端口。
	L2BR Port业务	删除关联在待删除设备上的L2BR Port
	PXE预配置Port业务	删除关联在待删除设备上的PXE Port
BD资源	DHCP Neutron Port业务	1. 在AC-DCN界面选择“租户 > 租户管理 > 租户”。 2. 单击租户名称，选择“端口”。 3. 查看端口详情中的接入设备信息，如果接入设备是待删除设备，请记录端口名称。 4. 登录云管理平台，删除记录的端口。
	裸金属服务器Neutron Port业务	在云管理平台释放裸金属服务器
	VM的Neutron Port业务	1. 选择“网络 > POD管理 > POD > 设备 > 虚拟机”，查看虚拟机接入的交换机。 2. 删除接入在待删除交换机上的所有虚拟机。

资源项	对应业务	资源释放操作
	LB的Neutron Port业务	1. 在AC-DCN界面选择“租户 > 租户管理 > 租户”。 2. 单击租户名称，选择“端口”。 3. 查看端口详情中的接入设备信息，如果接入设备是待删除设备，请记录端口名称。 4. 登录云管理平台，删除记录的端口。
	L2BR Port业务	删除关联在待删除设备上的L2BR Port
	PXE预配置Port业务	删除关联在待删除设备上的PXE Port
	vRouter关联内部接口	删除vRouter绑定的内部接口
vFW资源	vRouter关联外部网关	1. 删除vFW业务（包含EIP、SNAT、VPN、安全策略）。 2. vRouter取消关联外部网关。
	vFW业务（包含EIP、SNAT、VPN、安全策略）	
接口互联资源	vRouter关联外部网关	1. 删除vFW业务（包含EIP、SNAT、VPN、安全策略）。 2. vRouter取消关联外部网关。
	vFW业务（包含EIP、SNAT、VPN、安全策略）	
VPN资源	创建VPC	1. 删除vFW业务（包含EIP、SNAT、VPN、安全策略）。 2. vRouter取消关联外部网关。 3. vRouter取消关联内部接口。
	vRouter关联外部网关	
	vRouter关联内部接口	