

**中国移动网络云承载网网管&业支CE局数据配置规范（华为）**

版本号：4.0

XXXX-XX-XX实施

XXXX-XX-XX发布

文档说明：本规范为中国移动网络云承载网信令CE局数据配置指导性规范。

编号说明：

（本文档编号依照以下原则进行：

x.y.z x: 大版本更新，文档结构变化

y: 具体方案的更改，部分内容的修正)

文档修改历史

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 版本 | 更新日期 | 修改 | 核定 | 更新说明 | 文档状态 | |
| 1.0 | 2020-03-21 | 杨应雄 | 赖小勤 | 征求意见稿 | 初稿 | |
| 1.1 | 2020-07-08 | 王永刚 | 赖小勤 | 删除上行接口carrier up-hold-time | |  |
| 1.3 | 2021-03 | 于潇 | 王永刚 | 3.4.3 OSPF协议增加上行AR对接BGP和上行AR对接OSPF两种配置方式  3.3.1删除CE-AR互联延时UP 5000 |  | |
| 4.0 | 2023-04 | 王永刚 |  | 4.4 SNMP配置将认证模式和加密算法修改为安全性更高的sha2-512和aes256 |  | |
|  |  |  |  |  |  | |

目 录

[目 录 4](#_Toc28252118)

[1 移动电信云承载网CE组网概述 5](#_Toc28252119)

[1.1 设计内容 5](#_Toc28252120)

[1.2 目标组网 5](#_Toc28252121)

[2 软硬件版本说明 6](#_Toc28252122)

[3 局数据配置规范 7](#_Toc28252123)

[3.1 协议及参数要求 7](#_Toc28252124)

[3.2 关键字说明 7](#_Toc28252125)

[3.3 接口数据规范 10](#_Toc28252126)

[3.4 路由与VPN 17](#_Toc28252127)

[4 网管与安全配置 23](#_Toc28252128)

[4.1 关闭未使用端口与协议 23](#_Toc28252129)

[4.2 SYSLOG配置 23](#_Toc28252130)

[4.3 SNMP配置 24](#_Toc28252131)

[4.4 管理口配置 25](#_Toc28252132)

[4.5 配置本地帐号 25](#_Toc28252133)

[4.6 配置远程访问 25](#_Toc28252134)

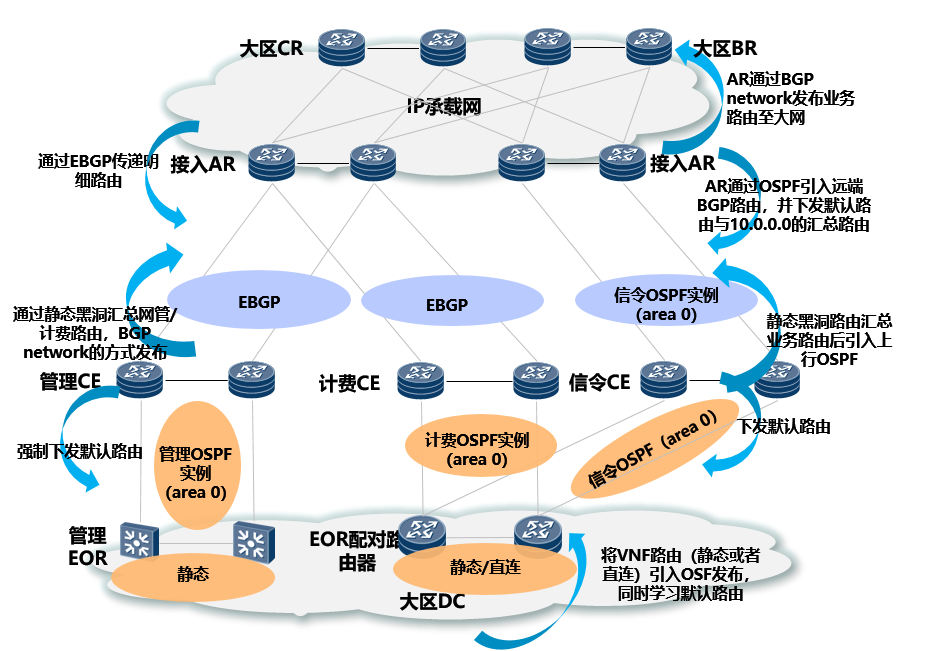
[4.7 NTP配置 26](#_Toc28252135)

# 移动网络云承载网CE组网概述

设计内容

中国移动网络云承载网CE设备作为资源池出口设备对接IP承载网AR，主要承载电信云相关信令、计费、管理等业务，本文档旨在说明承载网信令CE设备及CE与AR、 DC GW、管理EOR等对接的配置规范。

目标组网



注1：CE采用多链路捆绑，同一捆绑组的多个接口应该分布在不同的板卡上

注2： CE之间链路带宽等于AR-CE链路带宽

* 管理、计费和信令CE分别以口字型与IP承载网AR对接，沿用现网对接规范。信令CE与AR间部署OSPF多实例，通过OSPF交互内外部路由。管理与计费CE与AR间部署EBGP（OptionA方式）交互路由；
* AR路由器通过MP-BGP将业务路由发布至大网，针对信令CE，AR将远端通过MP-BGP发布过来的路由引入OSPF并通过OSPF下发默认与汇总路由；针对网管与计费CE，直接通过EBGP将明细路由发布给CE设备；
* 信令、管理、计费CE与DCGW间统一采用OSPF多实例（骨干区域）对接，学习VNF业务网元路由，同时下发默认路由（强制）至DCGW引导上行流量。

# 软硬件版本说明

本规范适用如下软硬件版本：

|  |  |  |  |
| --- | --- | --- | --- |
| 设备厂家 | 设备类型 | 软件版本 | 补丁版本 |
| 路由器 | NE40E | V800R010及以后 |  |
|  |  |  |  |

# 局数据配置规范

协议及参数要求

IP承载网AR（PE）与CE之间互连参数规范如下表，包括AR-CE互连路由协议参数、CE-CE互连路由协议参数、路由策略、VPN配置等，详细内容请参见《**承载网PE－电信云CE间参数规范》**。

关键字说明

|  |  |  |
| --- | --- | --- |
| **关键字** | **用途** | **规则** |
| CE主机名 | 定义设备名 | 按照承载网CE命名规范已经前期同资管组确定的《中国移动数据网资源标准命名规范》，对网络云CE命名遵照如下格式：   |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | |  | **省名** | **地市名** | **-** | **业务系统分类** | **-** | **CE** | **序号** | **-** | **设备型号** | | 符号 | 字符 | 字符 | 字符 | 字符/数字 | 字符 | 字符 | 数字 | 字符 | 字符/数字 | | 字符数 | 2（大写字母） | 2或3（大写字母） | 1 | ≤15(大写字母或数字) | 1 | 2 | 2 | 1 | ≤10(大写字母、小写字母、数字或／) |   说明：**设备型号** 长度≤10，因此华为NE40E设备统一为HWNE40EX16。  C:\Users\y00294207\AppData\Roaming\eSpace_Desktop\UserData\y00294207\imagefiles\0C933019-43C9-43C2-84A6-68EC9FCE0E39.png  NETNMS 用于标识网络云网管域CE  NETBOSS 用于标识网络云业支域CE  NETCN+数字 用于标识网络云业务域CE、其中NETCN后接数字需与业务CE所属资源池编号相同  资源池机房编号+RT+数字 用于标识CMNET接入路由器CE   举例：  “ZJJIH-NETNMS-CE01-HWNE40EX16” 浙江金华网络云网管CE01  “ZJJIH-NETBOSS-CE01-HWNE40EX16”浙江金华网络云业支CE01  “ZJJIH-NETCN01-CE01-HWNE40EX16”浙江金华网络云业务01资源池CE01  “NFV-D-HDNJIH-03A-1203-0F07-N-RT-01”浙江金华网络云203机房CMNET接入路由器01  C:\Users\y00294207\AppData\Roaming\eSpace_Desktop\UserData\y00294207\imagefiles\0F099678-3A6F-4918-A907-5FB9EDDF438C.png |
| 端口描述 | 定义端口描述 | 参见“中国移动集中网络云网络设备参数规范” |
| 路由策略 | 控制发布与引入BGP的路由策略 | 接收CMNet路由策略命令：CMNET\_TO\_XXX\_TIC（XXX为大区资源池名称）  发布CMNet路由策略命令： XXX\_TIC\_TO\_CMNET（XXX为大区资源池名称） |
| Prefix-List | 控制路由发布 | 1. 路由策略的prefix-list建议命名：prefix\_Tic\_XX\_YY（XX为大区缩写,YY为业务缩写） 2. node：从10开始，以10为步长递增；node 1000固定策略为deny |
| VLAN规划 | 资源池内部网络设备之间VLAN规划 | DCGW-CE对接VLAN编号为CE-AR对接编号+1000，如某业务CE-AR vlan是30，则DCGW-CE对接vlan使用1030。 |
| ospf密钥 | 建立ospf、ospfv3邻居配置密钥协商 | ospfv2对接大网密码由大网侧统一分配，资源池内使用：WLY-大区缩写（大写）@10086。  ospfv3与友商设备对接不配置密钥。 |
| ospf进程号 | 集团对ospf进程号分配要求 | 一、对于CE与AR间使用OSPF的场景：  （1）CE上行OSPF进程（CE-AR方向）使用与承载网相同的OSPF号进程，如承载网OSPF进程使用15，则CE上行OSPF进程也使用15  （2）CE下行OSPF进程（CE-DCGW方向）使用承载网OSPF号进程+100，如承载网OSPF进程使用15，则CE下行OSPF进程使用115  如果后续出现进程号冲突（例如后续大网启用了115，而此时CE上已经有进程115了），则CE上行进程号再+10，即CE上行AR方向进程号使用125，下行到DC-GW方向进程号使用225  二、对于CE与AR间使用BGP的场景  CE下行OSPF进程（CE-DCGW/EOR方向）使用承载网分配的私有AS号码作为进程号码，如承载网对接分配的私有AS号为65233，则CE下行OSPF进程号也使用65233  三、对于DCGW到CE的OSPF进程号，与CE的下行OSPF进程号保持一致  四、对于DCGW到防火墙的OSPF进程号，直接从10开始顺序分配，步长为10（即进程号为10/20/30……）  五、对于防火墙到CMNet CE的OSPF进程号，使用CMNet分配的私有AS号码作为进程号码 |
| bgp as号 | 集团对bgp AS分配要求 | 一、BGP AS号，由于每个对接VPN集团都会分配一个对应的私有AS号，网管CE与业支CE采用如下原则选取自身的AS号  顺序如下：网管VPN优于计费VPN优于业务开通VPN，同一类VPN中V4的AS号优于V6的AS号  按照该原则，选定一个最优的AS号作为CE设备的AS号。  AS号选定后，即使后面再有更优的VPN开通，也不再更换AS号。  二、CE设备与IP承载网对接，需要满足每个VPN的私有AS号分配要求。因此在CE上除了选定的AS号对应的VPN外，其他VPN对接使用fake-as技术对接，以保证承载网AR上每个VPN对接的AS号均不同，符合规范要求。  三、CMNet侧AS号，由移动集团需求部门向网络部申请。建议每个资源池使用不同的AS号。 |

接口数据规范

### 3.3.1 CE-AR互联

**配置说明：**

#### 1）CE-AR间链路捆绑配置：

配置CE-AR链路捆绑逻辑接口，不同业务之间的隔离使用TRUNK子接口。ETH-Trunk编号对接AR从3开始使用。

interface Eth-Trunk3 //进入Eth-Trunk视图

description ***TO-[对端主机名]-Eth-Trunk****<****编号****>****-N\*链路带宽***  //配置端口描述

undo shutdown

mode lacp-static

lacp timeout fast //与AR侧接口保持一致

ipv6 mtu 4470 spread //设置子接口ipv6 MTU值，与AR保持一致

mtu 4470 spread //设置子接口ipv4 MTU值，与AR保持一致

#

interface GigabitEthernet***<端口编号>/100GE<端口编号>***  //进入端口视图

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

carrier down-hold-time 200 //延迟200ms DOWN

undo shutdown

eth-trunk *<****编号>*** //把端口划分到Eth-Trunk端口

#

#### 2）网管CE对接AR子接口 (eBGP)：

interface Eth-Trunk3.***<子接口>*** //进入子端口视图（ipv4子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4 VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

#

interface Eth-Trunk3.***<子接口>*** //进入子端口视图（ipv6子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv6 VPN实例

ipv6 enable

ipv6 address ***<IPv6 网段>/<前缀长度>***  //配置端口Ipv6地址

#

#### 3）网管CE对接AR子接口(OSPF)：

interface Eth-Trunk3.***<子接口>*** //进入子端口视图（ipv4子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4 VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ospf authentication-mode md5 1 ***<密码>*** //配置OSPFv2 MD5认证

ospf network-type p2p //配置OSPF端口为P2P工作模式。

ospf cost 10 //强制AR-CE、CE-CE互连接口OSPF cost值为10

ospf hello timer 1 //配置CE-AR对接hello timer，与AR侧保持一致

#

interface Eth-Trunk3.***<子接口>*** //进入子端口视图（ipv6子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance **<VPN名称>**//绑定对应业务的ipv6 VPN实例

ipv6 enable

ipv6 address ***<IPv6 网段>/<前缀长度>***  //配置端口IPv6地址

ospfv3 ***<ID>*** area 0.0.0.0 //绑定OSPFv3，不认证

ospfv3 cost 10 //指定链路COST

ospfv3 network-type p2p //指定链路类型

ospfv3 hello timer 1 //配置CE-AR对接hello timer，与AR侧保持一致

#

#### 4）业支CE对接AR子接口(eBGP)：

interface Eth-Trunk3.***<子接口>*** //进入子端口视图（ipv4/ipv6双栈子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance***<VPN名称>*** //绑定对应业务的双栈VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ipv6 enable

ipv6 address ***<IPv6 网段>/<前缀长度>*** //配置端口Ipv6地址

#

### 3.3.2 CE-CE互联

**配置说明：**CE-CE之间使用多链路捆绑（是否使用聚合端口以现网为准）,不同业务通过vpn实例方式实现隔离。

#### 1）配置CE-CE对接逻辑接口

**【注意：如果AR-CE的VRF使用OSPF对接，CE-CE间需要分别配置对AR方向子接口和对DCGW/管理EOR方向子接口；如果AR-CE的VRF使用BGP对接，CE-CE间仅配置对DCGW/管理EOR方向子接口】**

interface Eth-Trunk1//进入Eth-Trunk视图，建议与CE互联使用trunk编号1

description ***TO-[端口主机名]-Eth-Trunk****<****编号****>****-N\*端口带宽***  //配置端口描述

mode lacp-static //开启LACP监测

lacp timeout fast //配置为LACP快检测

ipv6 mtu 4470 spread //设置子接口ipv6 MTU值，横连取MTU大值与AR保持一致

mtu 4470 spread //设置子接口ipv4 MTU值，横连取MTU大值与AR保持一致

#

interface GigabitEthernet***<端口编号>***  //进入端口视图

description ***TO-[对端设备]-端口-端口带宽*** //配置端口描述

eth-trunk *<****编号>*** //把端口划分到Eth-Trunk端口

#

#### 2）配置网管CE-CE互联子接口(eBGP)

// AR-CE的VRF使用BGP对接，CE-CE间仅配置对DCGW/管理EOR方向子接口

interface Eth-Trunk1.***<子接口>*** //进入子端口视图（ipv4子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q。

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4 VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ospf authentication-mode md5 1 ***<密码>*** //配置OSPF Hello MD5认证

ospf network-type **p2p** //配置OSPF端口为P2P工作模式。

ospf cost **10** //强制AR-CE、CE-CE互连接口OSPF cost值为10

#

interface Eth-Trunk1.***<子接口>*** //进入子端口视图（ipv6子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv6 VPN实例

ipv6 enable

ipv6 address ***<IPv6 网段>/<前缀长度>***  //配置端口Ipv6地址

ospfv3 ***<ID>*** area 0.0.0.0 //绑定OSPFv3

ospfv3 cost 10 //指定链路COST

ospfv3 network-type p2p //指定链路类型

ospfv3 authentication-mode hmac-sha256 key-id 1 cipher ***<密码>***

//配置OSPF认证Key ID和密码

#

#### 3）配置网管CE-CE互联子接口(OSPF)

对接上行CE-AR进程CE互联子接口

interface Eth-Trunk1.***<子接口>*** //进入子端口视图（ipv4子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q。

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4 VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ospf authentication-mode md5 1 ***<密码>*** //配置OSPF Hello MD5认证

ospf network-type **p2p** //配置OSPF端口为P2P工作模式。

ospf cost **20** //CE-CE对上互联COST值为20

ospf bfd enable //对接AR的OSPF进程无BFD，接口下使能BFD For OSPF

ospf bfd min-rx-interval 300 min-tx-interval 300 detect-multiplier 4

#

interface Eth-Trunk1.***<子接口>*** //进入子端口视图（ipv6子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv6 VPN实例

ipv6 enable

ipv6 address ***<IPv6 网段>/<前缀长度>***  //配置端口Ipv6地址

ospfv3 ***<ID>*** area 0.0.0.0 //绑定OSPFv3

ospfv3 cost 20 // CE-CE对上互联COST值为20

ospfv3 network-type p2p //指定链路类型

ospfv3 authentication-mode hmac-sha256 key-id 1 cipher ***<密码>***

//配置OSPF认证Key ID和密码

ospfv3 bfd enable //对接AR的OSPF进程无BFD，接口下使能BFD For OSPF

ospfv3 bfd min-transmit-interval 300 min-receive-interval 300 detect-multiplier 4

#

#### 4）对接下行CE-DCGW/EOR进程CE互联子接口

interface Eth-Trunk1.***<子接口>*** //进入子端口视图（ipv4子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q。

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4 VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ospf authentication-mode md5 1 ***<密码>*** //配置OSPF Hello MD5认证

ospf network-type **p2p** //配置OSPF端口为P2P工作模式。

ospf cost **10** //强制AR-CE、CE-CE互连接口OSPF cost值为10

#

interface Eth-Trunk1.***<子接口>*** //进入子端口视图（ipv6子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv6 VPN实例

ipv6 enable

ipv6 address***<IPv6 网段>/<前缀长度>***  //配置端口Ipv6地址

ospfv3 ***<ID>*** area 0.0.0.0 //绑定OSPFv3

ospfv3 cost 10 //指定链路COST

ospfv3 network-type p2p //指定链路类型

ospfv3 authentication-mode hmac-sha256 key-id 1 cipher ***<密码>***

//配置OSPF认证Key ID和密码

#

#### 5）配置业支CE-CE互联子接口

interface Eth-Trunk1.***<子接口>*** //进入子端口视图（ipv4/ipv6双栈子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4/ipv6双栈VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ospf authentication-mode md5 1 ***<密码>*** //配置OSPF Hello MD5认证

ospf network-type **p2p** //配置OSPF端口为P2P工作模式。

ospf cost **10** //强制AR-CE、CE-CE互连接口OSPF cost值为10

ipv6 enable

ipv6 address***<IPv6 网段>/<前缀长度>***  //配置端口Ipv6地址

ospfv3 ***<ID>*** area 0.0.0.0 //绑定OSPFv3

ospfv3 cost 10 //指定链路COST

ospfv3 network-type p2p //指定链路类型

ospfv3 authentication-mode hmac-sha256 key-id 1 cipher ***<密码>***

//配置OSPF认证Key ID和密码

~~#~~

### 3.3.3 CE-DC GW/管理EOR

**配置说明：**CE-DC GW/管理EOR之间使用多链路捆绑成Eth-trunk聚合口，不同业务之间的隔离使用子接口。Eth-trunk端口号建议从11开始使用。

#### 1) 配置eth-trunk接口

interface Eth-Trunk11 //进入Eth-Trunk视图

description***TO-[端口主机名]-Eth-Trunk****<****编号****>****-N\*10G***  //配置端口描述

ip address 192.168.1.5 255.255.255.252

mode lacp-static //开启LACP监测

lacp timeout fast //配置为LACP快检测

ipv6 mtu 4000 spread //设置子接口ipv6 MTU值，CE对资源池内部使用mtu 4000

mtu 4000 spread //设置子接口ipv4 MTU值，CE对资源池内部使用mtu 4000

#

interface GigabitEthernet***<端口编号>*** //进入端口视图

description ***TO-[对端设备]-端口-端口带宽*** //配置端口描述

eth-trunk *<****编号>*** //把端口划分到Eth-Trunk端口

#

#### 2）配置网管CE-I类资源池管理EOR接口/II类资源池DCGW接口

interface Eth-Trunk11.***<子接口>*** //进入子端口视图（ipv4子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4 VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ospf authentication-mode md5 1 ***<密码>*** //配置OSPF Hello MD5认证

ospf network-type **p2p** //配置OSPF端口为P2P工作模式。

ospf cost **10** //强制AR-CE、CE-CE互连接口OSPF cost值为10

#

interface Eth-Trunk11.***<子接口>*** //进入子端口视图（ipv6子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q，根据《承载网PE－电信云CE间参数规范.xls》定义。

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv6 VPN实例

ipv6 enable

ipv6 address ***<IPv6 网段>/<前缀长度>*** //配置端口Ipv6地址

ospfv3 ***<ID>***area 0.0.0.0 //绑定OSPFv3

ospfv3 cost 10 //指定链路COST

ospfv3 network-type p2p //指定链路类型

ospfv3 authentication-mode hmac-sha256 key-id 1 cipher ***<密码>***

//配置OSPF认证Key ID和密码

#

#### 3）配置业支CE-I类资源池DCGW接口：

interface Eth-Trunk11.***<子接口>*** //进入子端口视图（ipv4/ipv6双栈子接口）

description ***TO-[对端设备]-端口编号-端口带宽*** //配置端口描述

vlan-type dot1q ***<子接口VLAN号>*** //配置端口封装类型802.1Q

ip binding vpn-instance ***<VPN名称>*** //绑定对应业务的ipv4/ipv6双栈VPN实例

ip address ***<IP地址> <掩码>*** //配置端口ipv4地址

ospf authentication-mode md5 1 ***<密码>*** //配置OSPF Hello MD5认证

ospf network-type **p2p** //配置OSPF端口为P2P工作模式。

ospf cost **10** //强制AR-CE、CE-CE互连接口OSPF cost值为10

ipv6 enable

ipv6 address***<IPv6 网段>/<前缀长度>***  //配置端口Ipv6地址

ospfv3 ***<ID>*** area 0.0.0.0 //绑定OSPFv3

ospfv3 cost **10** //指定链路COST

ospfv3 network-type p2p //指定链路类型

ospfv3 authentication-mode hmac-sha256 key-id 1 cipher ***<密码>***

//配置OSPF认证Key ID和密码（密码由集团统一分配）

#

路由与VPN

### 3.4.1 VPN配置

配置说明：CE设备启用VRF多实例，不同VPN之间的路由隔离通过VPN实例（VPN-instance）实现。

ip vpn-instance ***NFV-DM-Mgmt*** //硬集定义VRF的名字  
ipv6-family  
route-distinguisher 8086:0080 //定义VRF的RD

#

ip vpn-instance ***<VPN名称>***  //业支CE、CBOSS及YWKT使用双栈VPN

ipv4-family

ip frr //CE与DC-GW之间的VPN需要配置

route-distinguisher***24059:xxxx*** //配置ipv4 RD

ipv6-family

ipv6 frr //CE与DC-GW之间的VPN需要配置

route-distinguisher ***24059:xxxxxx*** //配置ipv6 RD

#

ip vpn-instance ***<VPN名称>***  //配置IPv4单栈VRF

ipv4-family

ip frr //CE与DC-GW之间的VPN需要配置

route-distinguisher ***24059:xxxx*** //配置RD

#

ip vpn-instance ***<VPN名称>***  //配置IPv6单栈VRF

ipv6-family

ipv6 frr //CE与DC-GW之间的VPN需要配置

route-distinguisher ***24059:xxxx*** //配置RD

#

### 3.4.2 LOOPBACK配置

**配置说明：**CE设备启用VRF多实例，需要创建LOOPBACK作为对应OSPF实例的routeid。根据设备承载的业务选择配置。

**1）配置v4 loopback：**

interface LoopBack***<ID>*** //loopback接口号可根据情况自行设置，建议与ospf进程号一致

description ***Loopback For OSPFXX***  //XX为OSPF进程号

ip binding vpn-instance ***<VPN名称>***  //绑定对于的OSPF进程

ip address ***<LOOPBACK>*** 255.255.255.255

#

**2）配置v6 loopback：**

interface LoopBack***<ID>*** //loopback接口号可根据情况自行设置，建议与ospf进程号一致

description ***Loopback For OSPFXX*** //XX为OSPF进程号

ip binding vpn-instance ***<VPN名称>***  //绑定对于的OSPF进程

ipv6 enable

ipv6 address ***<LOOPBACK>/128***

ospfv3 ***<ID>*** area0instance XXX //Loopback口使能OSPFV3

#

### 3.4.3 OSPF协议

**配置说明：**网管&业支CE与AR对接协议有EBGP和OSPF两种方式，根据VPN类型不同对接协议不同。根据CE-AR对接VPN使用协议不同CE到DCGW有两种不同配置方式；

#### 1）CE与AR VPN对接采用EBGP方式对接，

CE创建一个OSPF/OSPFv3进程，CE-CE之间的OSPF与CE-DCGW/管理EOR运行在同一进程的area0中，AR EBGP不会下发缺省路由，需要OSPF强制下发缺省路由引导流量上行，EBGP不引入OSPF路由，通过network+黑洞路由方式发布汇总路由，配置OSPF+BFD方式。

**创建CE-CE之间、CE-DCGW/管理EOR的OSPF&OSPFv3进程：**

ospf ***<ID>*** router-id ***<RouterID>*** vpn-instance ***<VPN名称>*** //配置OSPF多实例

vpn-instance-capability simple //配置OSPF 忽略环路检查

bfd all-interfaces enable

bfd all-interfaces min-tx-interval 300 min-rx-interval 300 detect-multiplier 4

spf-schedule-interval intelligent-timer 50 50 50//配置OSPF 路由计算时间间隔

lsa-originate-interval intelligent-timer 500 50 100//配置OSPF LSA被接收的时间间隔

lsa-arrival-interval intelligent-timer 50 50 50//配置OSPF LSA的更新时间间隔

**default-route-advertise always type 1**  **//业支CE对接DCGW和网管CE对接管EOR:向管理EOR强制下发默认路由**

frr

loop-free-alternate //使能frr功能

area 0.0.0.0

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE之间互连网段路由

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE loopback地址路由

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE下行到DC-GW的网段路由

#

ospfv3***<ID>*** vpn-instance ***<VPN名称>*** //配置OSPFv3多实例

vpn-instance-capability simple //配置OSPF 忽略环路检查

bfd all-interfaces enablebfd all-interfaces min-transmit-interval 300 min-receive-interval 300 detect-multiplier 4

router-id ***<Loopback>*** //针对v6的VPN，ospfv3 router-id标识需使用ipv4地址格式

spf-schedule-interval intelligent-timer 50 50 50//配置OSPF 路由计算时间间隔

lsa-originate-interval intelligent-timer 500 50 100//配置OSPF LSA被接收的时间间隔

lsa-arrival-interval intelligent-timer 50 50 50//配置OSPF LSA的更新时间间隔

**default-route-advertise always type 1** **//业支CE对接DCGW和网管CE对接管理EOR:向管理EOR强制下发默认路由**

frr

loop-free-alternate //使能frr功能

area 0.0.0.0

#

#### 2）CE与AR VPN对接采用OSPF方式

CE创建两个OSPF/OSPFv3进程分别对接AR和DCGW/EOR，CE-CE之间的OSPF与CE-DCGW/管理EOR运行在同一进程的area0中，AR通过OSPF下发缺省路由，上行进程引入汇总静态路由，下行进程通过OSPF非强制下发缺省路由引导流量上行，两个OSPF进程不互相引入路由避免路由环路，同时下行OSPF进程配置路由策略过滤下行缺省路由，避免路由环路。

**创建CE-AR的OSPF进程：**

ospf***<ID>*** router-id ***<RouterID>*** vpn-instance ***<VPN名称>***//配置OSPF多实例

spf-schedule-interval intelligent-timer 50 50 50//配置OSPF 路由计算时间间隔

lsa-originate-interval intelligent-timer 500 50 100//配置OSPF LSA被接收的时间间隔

lsa-arrival-interval intelligent-timer 50 50 50//配置OSPF LSA的更新时间间隔

import-route static type 1 route-policy ***TIC-to-IPNET\_v4***

//配置引入静态汇聚路由，策略名可根据实际情况添加vpn名称信息

vpn-instance-capability simple//配置OSPF 忽略环路检查

area 0.0.0.0

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE之间互连网段路由

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE上行到AR的网段路由

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE loopback地址路由

#

ospfv3 ***<ID>*** vpn-instance ***<VPN名称>*** //配置OSPFv3多实例

router-id ***<Loopback>***

spf-schedule-interval intelligent-timer 50 50 50//配置OSPF 路由计算时间间隔

lsa-originate-interval intelligent-timer 500 50 100//配置OSPF LSA被接收的时间间隔

lsa-arrival-interval intelligent-timer 50 50 50//配置OSPF LSA的更新时间间隔

import-route static type 1 route-policy ***TIC-to-IPNET\_v6*** //配置引入静态汇聚路由，策略名可根据实际情况添加vpn名称信息

vpn-instance-capability simple //配置OSPF 忽略环路检查

#

#### 3）创建CE-DC-GW的OSPF进程：

ospf ***<ID>*** router-id *<****IPv4****>* vpn-instance ***<VPN名称>***//配置OSPF多实例

bfd all-interfaces enable

bfd all-interfaces min-tx-interval 300 min-rx-interval 300 detect-multiplier 4

spf-schedule-interval intelligent-timer 50 50 50//配置OSPF 路由计算时间间隔

lsa-originate-interval intelligent-timer 500 50 100//配置OSPF LSA被接收的时间间隔

lsa-arrival-interval intelligent-timer 50 50 50//配置OSPF LSA的更新时间间隔

default-route-advertise type 1 //**网管CE对接DCGW:**向DC-GW非强制下发默认路由

filter-policy ip-prefix ***deny\_default*** import //**网管CE对接DCGW:**向DC-GW下行ospf进程过滤缺省路由

vpn-instance-capability simple//配置OSPF 忽略环路检查

frr

loop-free-alternate //使能frr功能

area 0.0.0.0

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE之间互连网段路由

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE下行到DC-GW的网段路由

network ***<IP 网段> <反掩码>*** //配置OSPF发布CE loopback地址路由

#

ospfv3 ***<ID>*** vpn-instance ***<VPN名称>*** //配置OSPFv3多实例

router-id ***<Loopback>***

bfd all-interfaces enable

bfd all-interfaces min-transmit-interval 300 min-receive-interval 300 detect-multiplier 4

spf-schedule-interval intelligent-timer 50 50 50//配置OSPF 路由计算时间间隔

lsa-originate-interval intelligent-timer 500 50 100//配置OSPF LSA被接收的时间间隔

lsa-arrival-interval intelligent-timer 50 50 50//配置OSPF LSA的更新时间间隔

default-route-advertise type 1 //向DC-GW非强制下发默认路由

filter-policy ipv6-prefix deny\_default import //下行ospf进程过滤缺省路由

vpn-instance-capability simple //配置OSPF 忽略环路检查

frr

loop-free-alternate //使能frr功能

area 0.0.0.0

#

ip ip-prefix ***deny\_default*** index 10 deny 0.0.0.0 0

ip ip-prefix ***deny\_default*** index 20 permit 0.0.0.0 0 less-equal 32//过滤缺省路由

#

ip ipv6-prefix ***deny\_default*** index 10 deny :: 0

ip ipv6-prefix ***deny\_default*** index 20 permit :: 0 less-equal 128//过滤缺省路由

#

### 3.4.4 BGP协议

配置说明：与AR互联建立BGP邻居，通过EBGP和承载网之间实现路由交互。

bgp***<ID>*  //BGP AS根据统一规划配置**

router-id ***<IPv4地址>***

#

ipv4-family unicast

undo synchronization

maximum load-balancing 32

#

ipv4-family vpn-instance ***<VPN名称>***

network ***<IP 网段> <掩码>* //发布汇总后的v4业务网段**

network ***<IP 网段> <掩码>*  //发布汇总后的v4业务网段**

maximum load-balancing 32

group ***IPNET-AR-V4*** external //与AR的ipv4 ebgp邻居

peer ***IPNET-AR-V4*** as-number ***<AS-NUMBER>***

peer ***IPNET-AR-V4*** password cipher ***<密码>*** //协商密钥由大网分配

peer ***IPNET-AR-V4*** connect-interface ***<Eth-TrunkXXXX>***

//使用接口地址与IP承载网建立 bgp邻居

peer ***IPNET-AR-V4*** route-policy ***TIC-to-IPNET\_v4*** export

peer ***IPNET-AR-V4***advertise-community

peer ***IPNET-AR-V4*** advertise-ext-community

peer ***<AR IP地址>***  group IPNET-AR-V4

peer***<AR IP地址>***description ***<邻居描述>***

peer ***<AR IP地址>***  timer keepalive 10 hold 30 //对接承载网AR要求，命令执行后要输入y

peer IPNET-AR-V4 fake-as ***<AS-Number>***

//需要满足每个VPN的私有AS号分配要求。因此在CE上除了选定的AS号对应的VPN外，其他VPN对接使用fake-as技术对接

#

group ***TIC\_XX\_V4*** internal //CE间的ipv4 iBGP邻居

peer ***TIC\_XX\_V4*** password cipher ***<密码>***

peer ***TIC\_XX\_V4*** connect-interface ***LoopBackXXX*** //使用同VPN OSPFxxx使用的Loopback口建立CE间的iBGP Peer

peer ***TIC\_XX\_V4*** next-hop-local //设置向横连对端CE通告路由时，把下一跳属性设为自身的IP地址

peer ***<CE IP地址>*** group ***TIC\_XX\_V4***

peer ***<CE IP地址>*** description ***<邻居描述>***

#

ipv6-family vpn-instance ***<VPN名称>***

network ***<IPv6 网段> <掩码>*  //发布汇总后的v6业务网段**

network ***<IPv6 网段> <掩码>*  //发布汇总后的v6业务网段**

maximum load-balancing 32

group ***IPNET-AR-V6*** external

peer ***IPNET-AR-V6***as-number ***<AS-Number>***

peer ***IPNET-AR-V6***password cipher***<密码>***//协商密钥由大网分配

peer ***IPNET-AR-V6*** connect-interface ***<Eth-TrunkXXXX>*** //使用接口地址与IP承载网建立 bgp邻居

peer ***IPNET-AR-V6*** route-policy ***TIC-to-IPNET\_v6*** export

peer ***IPNET-AR-V6***advertise-community

peer ***IPNET-AR-V6*** advertise-ext-community

peer ***<IPv6地址>*** group ***IPNET-AR-V6***

peer***<IPv6地址>***description ***<邻居描述>***

peer ***IPNET-AR-V6*** fake-as***<AS-Number>***

//需要满足每个VPN的私有AS号分配要求。因此在CE上除了选定的AS号对应的VPN外，其他VPN对接使用fake-as技术对接

peer***<IPv6地址>*** next-hop-local //设置向CE通告ipv6路由时，把下一跳属性设为自身的IP地址

#

group ***TIC\_XX\_V6*** internal //CE间的ipv6 iBGP邻居

peer ***TIC\_XX\_V6*** password cipher***<密码>***

peer ***TIC\_XX\_V6*** connect-interface ***LoopBackXXX*** //使用同VPN OSPFxxx使用的Loopback口建立CE间的iBGP Peer

peer ***TIC\_XX\_V6*** next-hop-local //设置向横连对端CE通告路由时，把下一跳属性设为自身的IP地址

peer ***<CE IPv6地址>*** group TIC\_XX\_V6

peer ***<CE IPv6地址>*** description ***<邻居描述>***

#

### 3.4.5 静态路由协议

**配置说明：**业务网段黑洞路由，用于BGP network发布业务网段路由。

ip route-static ***<VPN实例> <目的IP地址> <掩码>*** **Null0** track bfd-session ***<BFD会话名称>***description ***<描述>***

//配置业务网段汇总黑洞路由并绑定CE-DCGW间BFD会话

ipv6 route-static :: 0 ***g0/0/0*** ***<下一跳地址>***

//带外网管，打通至硬件管理TOR：配置ipv6地址的默认路由，下一跳为网关地址

### 3.4.6 路由策略

**配置说明：**配置允许引入到AR-CE的OSPF/BGP中的路由策略，策略名称和路由前缀名可以自行定义。

route-policy ***TIC-to-IPNET\_v4*** permit node **10**

//配置路由策略，策略名可根据实际情况添加vpn名称信息。

if-match ip-prefix ***TIC-to-IPNET\_v4*** //配置允许发布的IPV4地址前缀列表

#

route-policy ***TIC-to-IPNET\_v6*** permit node **10** //配置路由策略

if-match ipv6 address prefix-list ***TIC-to-IPNET\_v6*** //配置允许发布的IPV6地址前缀列表

#

**ip prefix**配置规范：

ip ip-prefix ***<prefix名称>***index ***10*** permit ***<IP 网段> <掩码>***

//index以10为步长增加。

ip ipv6-prefix ***<prefix名称>***index***10*** permit ***<IP 网段> <掩码>***

//index以10为步长增加。

#

### 3.4.7 路由聚合+BFD协议

配置说明：**要求在网管/业支CE设备上针对不同资源池分别进行地址汇总发布**，对应分别关联CE至不同资源池的管理EOR/DCGW的bfd。

bfd //使能BFD

bfd ***v4\_NMSCE\_01EOR*** bind peer-ip ***192.168.1.6*** source-ip ***192.168.1.5*** auto //V4 BFD，v4\_CE类型(业务CE:CNCE 业支CE:BOSSCE 网管CE:NMSCE)\_ 01DCGW(资源池编号+DCGW或者资源池编号+NMSEOR)，网管和业支CE到管理EOR或者DCGW均配置BFD

detect-multiplier 4

min-tx-interval 500

min-rx-interval 500

#

ip route-static vpn-instance ***<VPN名称>******<IP 网段> <掩码>*** **NULL0** *track bfd-session* ***v4\_NMSCE\_01EOR*** description ***Summay-[业务类型]***

ipv6 route-static vpn-instance ***<VPN名称>******<IP 网段> <掩码>*** **NULL0** *track bfd-session* ***v4\_ NMSCE\_01EOR*** description ***Summay-[业务类型]***

//在CE上配置业务地址段汇聚路由，并引入OSPF或者通过BGP network发布。要求不同资源池的管理EOR或者DCGW分别进行汇总发布，对应分别关联CE至不同资源池的管理EOR/DCGW的bfd。此处仅举例到管理EOR配置，实际配置需要增加到DCGW配置。

### 3.4.8 端口联动

**配置说明：**

**1.如果AR-CE的VRF使用OSPF对接，那么无需配置端口联动配置**

**2.如果AR-CE的VRF使用BGP对接，那么需要在全局端口联动配置及在VRF所属的CE下行口增加端口联动配置**

网管/业支CE上联口和横联口加入monitor-group，下联口联动monitor-troup的状态。实现监测上联、互联端口链路状态，同步联动CE所有下行端口关闭。

**全局端口联动配置：**

monitor-group ***User\_bind\_down***

monitor enable

binding interface ***Eth-Trunk3*** down-weight 50 //监测上行端口状态

binding interface ***Eth-Trunk1*** down-weight 50 //监测互联端口状态

trigger-up-delay 30

**接口下端口联动配置：**

interface ***Eth-Trunk11***

track monitor-group ***User\_bind\_down*** trigger-down-weight 100 //将涉及下行端口配置为track接口

interface Eth-Trunk12

track monitor-group ***User\_bind\_down*** trigger-down-weight 100 //将涉及下行端口配置为track接口

interface Eth-Trunk13

track monitor-group ***User\_bind\_down*** trigger-down-weight 100 //将涉及下行端口配置为track接口

#

# 网管与安全配置

主机名称配置

配置规范：

system-view

sysname HAZZ-NETCN05-CE02-HWNE40EX8C //配置设备名称

关闭未使用端口与协议

**配置说明：**关闭所有未使用接口。

interface***GigabitEthernetX/X/X*** //进入端口视图，包括GE、FE、POS等

shutdown //关闭所有未使用端口

#

undo ftp server //关闭ftp服务

undo ftp ipv6 server

undo telnet server enable

undo telnet ipv6 server enable

#

undo dhcp enable //关闭dhcp服务

#

SYSLOG配置

**配置规范：**

info-center enable

info-center loghost source ***<源接口>***  //建议使用SYSLOG服务器所在VPN的loopback地址

info-center loghost ipv6 ***<IP地址1>***  vpn-instance ***NFV-DM-Mgmt***  //设置接收SYSLOG服务器1地址

info-center loghost ipv6 ***<IP地址2>***  vpn-instance ***NFV-DM-Mgmt*** //设置接收SYSLOG服务器2地址

info-center logbuffer size 1024

info-center timestamp log date without-timezone //配置发送日志内容不带时区,与syslog服务器对接时协商参数格式，按需配置

info-center timestamp trap date without-timezone //配置发送trap日志内容不带时区,与syslog服务器对接时协商参数格式，按需配置

#

SNMP配置

**配置说明：**配置SNMP ACL以及SNMP信息。

acl ipv6 number ***2000***  //配置SNMP ACL

description ***For-snmp\_v6***

rule 5 permit vpn-instance ***NFV-DM-Mgmt*** source ***<IP地址1>/掩码***  //网管服务器地址1

rule 10 permit vpn-instance ***NFV-DM-Mgmt***  source ***<IP地址2>/掩码***  //网管服务器地址2

rule 500 deny //Deny其它访问

#

snmp-agent

snmp-agent sys-info location ***<设备安装局址>***

snmp-agent sys-info version v3 //统一使用v3

snmp-agent usm-user v3 ***uhmroot*** //账号与esight保持一致

snmp-agent usm-user v3 ***uhmroot*** group ***dc-admin***

snmp-agent usm-user v3 ***uhmroot*** acl 2000 //关联上述创建的ACL

snmp-agent usm-user v3 uhmroot authentication-mode ***sha2-512***

Please configure the authentication password (8-255)

Enter Password: //输入认证密码

Confirm Password: //确认认证密码

snmp-agent usm-user v3 uhmroot 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

#

snmp-agent mib-view included iso-view iso

snmp-agent mib-view included nt iso

snmp-agent mib-view included rd iso

snmp-agent mib-view included wt iso

snmp-agent group v3 dc-admin privacy read-view rd write-view wt notify-view nt

**snmp-agent trap enable**

**snmp-agent protocol source-status ipv6 all-interface**

**snmp-agent trap source *GigabitEthernet0/0/0***

**对接华为esight配置命令：**

snmp-agent target-host trap ipv6 address udp-domain ***<IP地址1>*** vpn-instance ***NFV-DM-Mgmt*** source ***GigabitEthernet0/0/0*** params securityname uhmroot v3 privacy private-netmanager ext-vb

**#**

管理口配置

**配置规范：**

interface ***GigabitEthernet0/0/0***

description TO-[对端设备]-端口-端口带宽

ip binding vpn-instance ***NFV-DM-Mgmt***

ipv6 enable  
ipv6 address ***2409:8086:XXXXXXXX/64*** //根据实际规划配置管理ip地址

配置本地帐号

**配置说明：**配置本地帐号

aaa

local-user ***tempadmin*** password irreversible-cipher ***<密码>***

//配置用户名和密码为临时调测

local-user ***tempadmin*** service-type ssh telnet

local-user ***tempadmin*** level 3

#

rsa local-key-pair create

stelnet ipv6 server enable

ssh user ***tempadmin***

ssh user ***tempadmin*** authentication-type password

ssh user ***tempadmin*** service-type stelnet

ssh ipv6 server acl ***2007***

配置远程访问

**配置说明：**配置远程登陆限制以及远程访问参数

acl ipv6 number ***2007***

description ***For-SSH\_v6***

rule 999 permit vpn-instance ***NFV-DM-Mgmt*** source ***2409:8086::/32***

//调测临时放开，后续添加实际明细路由，此条删除

rule 1000 deny

#

user-interface con 0

authentication-mode password //配置认证方式

set authentication password cipher ***<密码>*** //配置登录密码

#

user-interface maximum-vty 21

user-interface vty 0 20

authentication-mode aaa

user privilege level 3

protocol inbound ssh

idle-timeout 15 0

acl ipv6 2007 inbound //配置acl限制登录

#

ssh ipv6 server-source all-interface

ssh authorization-type default aaa

#

NTP配置

ntp-service server disable //关闭ipv4 ntp server功能

ntp-service ipv6 server disable //关闭ipv6 ntp server功能

#

ntp-service ipv6 source-interface ***GigabitEthernet0/0/0*** vpn-instance ***NFV-DM-Mgmt***  //指定源接口

ntp-service unicast-server ipv6 ***<NTP服务器地址1>*** authentication-keyid 1 vpn-instance ***NFV-DM-Mgmt*** preference

ntp-service unicast-server ipv6 ***<NTP服务器地址2>*** authentication-keyid 1 vpn-instance ***NFV-DM-Mgmt***（多台服务器则按需配置）

配置时区

clock timezone BeiJing add 08:00:00