交换机配置指南

本手册对应的软件版本为：Release 5.0.x

文档版本号：V1.07

发布时间：2020.12.25

1. 系统管理

1.1. CLI 命令行模式

设备 CLI 管理界面分成若干不同的模式，用户当前所处的命令模式决定了可以使用的命令。在命令提示符下输入问号键（?）可以列出每个命令模式支持使用的命令。当用户登录到设备上时，首先处于用户模式。

模式名称	提示符	切换模式	模式描述
用户模式	(Routing)>	配置 enable 切换到特权模式	支持设备信息显示、调试命令行等
特权模式	(Routing)#	配置 configure 切换到全局模式;配置 exit 切换到用户模式	支持网络测试; 支持功能模块信息查看; 支持配置保存、清空等操作
全局模式	(Routing)(config)#	配置 exit 切换到特权模式；配置 interface 切换到接口模式	支持基于全局的配置命令
接口模式	(Routing)(config-if)#	配置 exit 切换到全局模式;配置 end 切换到特权模式	支持接口模式下配置命令，接口包括物理接口、聚合口、SVI 口

1.2. 配置管理 IP

1.2.1. 配置命令

- 配置设备 Ipv4 管理 IP

命令	(Routing)#network parms ipaddr netmask [gateway]
描述	配置设备 Ipv4 管理 IP

- 配置管理 vlan

命令	(Routing)#network mgmt_vlan [vlan_id} (Routing)#no network mgmt_vlan [vlan_id}
描述	配置/删除设备管理 vlan

- 配置设备 Ipv4 管理 IP DHCP 动态获取

命令	(Routing)#network protocol dhcp client-id
描述	配置 Ipv4 管理 IP

- 配置设备 Ipv6 管理 IP

命令	(Routing)#network ipv6 address ipv6 ipv6-address/prefix-length [eui64] (Routing)#network ipv6 gateway ipv6-address (Routing)#no network ipv6 address ipv6 ipv6-address/prefix-length (Routing)#no network ipv6 gateway
描述	配置/删除设备 Ipv6 管理 IP

- 配置设备 Ipv6 管理 IP DHCP 动态获取

命令	(Routing)#network ipv6 address autoconfig (Routing)#**no network ipv6 address autoconfig**
描述	配置/删除设备 Ipv6 管理 IP

- 查看设备管理 IP 配置

命令	(Routing)#show running-config
描述	查看 ip 配置

1.3. 配置保存/清除操作

- 配置保存命令

命令	(Routing)#write memory
描述	保存配置

- 恢复默认配置命令

命令	((Routing)) #clear config Are you sure you want to clear the configuration? (y/n) y
描述	恢复系统默认配置，设备重启后生效

1.4. 设备热重启操作

- 配置热重启命令

命令	(Routing)#**reload**
描述	设备热重启

1.5. 用户登录管理

- 新增/删除用户、修改用户密码

命令	(Routing)(config)# **username** NAME **password** LINE (Routing)(config)# **no username** NAME
描述	若用户 NAME 不存在则新增用户，若存在则修改用户的密码； 设备出厂默认自带用户"admin"，密码"admin"，支持修改密码、删除操作； 设备最多支持 8 个用户，用户、密码长度为 <8-64>字节； 密码显示采用加密方式； 密码字符区分大小写；

- 配置使能 WEB 管理

命令	(Routing)# `ip http server` (Routing)# `ip http secure-server` (Routing)# **no** `ip http server` (Routing)#no ip http secure-server
描述	配置使能 WEB 管理 默认 enable 状态 支持 Ipv6

- 配置使能 Telnet 管理

命令	(Routing)# ip telnet server enable (Routing)# no ip telnet server enable
描述	配置使能 telnet 管理 默认 disable 状态 支持 Ipv6

- 配置使能 SSH 管理

命令	(Routing)# **ip ssh server enable** (Routing)# **no ip ssh server enable**
描述	配置使能 SSH 管理 默认 disable 状态 支持 Ipv6

显示命令：

```
(Routing) #show users

                                User
User Name                     Access Mode
-----------------------       -----------
admin                         Privilege-15
```

1.6. 配置系统名称

- 配置系统名称

命令	(Routing)(config)# **hostname** WORD
描述	设置系统名称，名称必须由可打印字符组成，长度不能超过64 个字节； 配置即时生效

1.7. 配置系统时间

- 手动配置系统时间

命令	(Routing)(config)# clock set hh:mm:ss (Routing)(config)# clock set mm/dd/yyyy
描述	设置系统时间 例如配置 2017 年 10 月 1 日 15 时 30 分 0 秒: clock set 15:30:00 clock set 10/1/ 2017

- 配置 ntp 服务器

命令	(Routing)(config)# sntp server {ipaddress | ipv6address | hostname} [priority [version] (Routing)(config)#s**ntp server** A.B.C.D
描述	配置 NTP 服务器的 IP 地址(不支持域名配置)。配置完成后，若设备与服务器保持网络连通，设备将自动从服务器同步时间信息，第一次完成时间同步大概耗时 4-8 分钟。

- 配置系统时区

命令	(Routing)(config)# clock timezone {hours} [minutes minutes] [zone acronym]

	(Routing)(config)# `no clock timezone`
描述	配置系统时区，默认为世界标准时间 UTC，支持标准的时区配置，如上海时区关键字“Shanghai”，香港时区关键字” Hong_Kong”等。

- 查看系统时间

命令	(Routing)# **show clock**
描述	查看系统时间

2. 配置接口

2.1. 接口类型概述

交换设备的接口，根据业务层面，可分为以下两大类：二层接口与三层接口。

二层接口(L2 interface)，这里包括普通物理口((Routing) Port)以及聚合口(Port Channel)。

(Routing) Port 由设备上的单个物理端口构成，只有二层交换功能。该端口可以是一个 Access Port、Hybrid Port 或一个 Trunk Port，您可以通过 (Routing) Port 接口配置命令，把一个端口配置为一个 Access Port、Hybrid Port 或者 Trunk Port。

Port Channel 简称 PO，是由多个物理成员端口聚合而成的。我们可以把多个物理链接捆绑在一起形成一个简单的逻辑链接，这个逻辑链接我们称之为一个聚合口。对于二层交换来说聚合口就好像一个高带宽的(Routing) port，它可以把多个端口的带宽叠加起来使用，扩展了链路带宽。

三层接口(L3 interface)，这里主要指 SVI((Routing) virtual interface)口。

SVI 是交换虚拟接口，用来实现三层交换的逻辑 9 接口。SVI 可以做为本机的管理接口，通过管理接口管理员可管理设备。您可通过 interface vlan 接口配置命令来创建 SVI，然后给 SVI 分配 IP 地址来建立 VLAN 之间的路由。

2.2. 配置命令

- 配置端口 range

命令	(Routing)(config)# **interface** <intf-range> (Routing)(config)# **interface** 0/1-0/4 (Routing)(config)# **interface** 0/1 (Routing)(config)# show interface ethernet all

描述	<intf-range> 格式如 0/1-0/4,

- 配置端口描述符

命令	(Routing)(config-if)# **description** <description>
描述	配置接口描述符，最多 80 个字符

- 配置端口使能

命令	(Routing)(config-if)# **shutdown** (Routing)(config-if)# **no shutdown**
描述	关闭端口或使能端口，默认使能； 仅支持物理口上配置

- 配置端口速率

命令	(Routing)(config-if)# **speed** [10G | 1000 | 100 | 10] {half-duplex | `full-duplex}}` (Routing)(config-if)# speed auto-detect (Routing)(config-if)# **speed** auto-neg [10G | 1000 | 100 | 10] {half-duplex | `full-duplex}}`
描述	配置端口速率，当配置成 auto，端口速率进入自协商模式； 默认端口速率自协商；

	不支持在聚合成员口上配置； 不支持在 SVI 口上配置

说明

✦当速率与双工均退出自协商模式时，端口自协商关闭

- 配置端口流控

当本端交换机和对端交换机都开启了流量控制功能后，如果本端交换机发生拥塞：

本端交换机将向对端交换机发送消息，通知对端交换机暂时停止发送报文或减慢发送报文的速度。

对端交换机在接收到该消息后，将暂停向本端发送报文或减慢发送报文的速度，从而避免了报文丢失现象的发生，保证了网络业务的正常运行。

命令	(Routing)(config-if)# **flowcontrol** { **asymmetric | symmetric** } (Routing)(config-if)# no **flowcontrol** ((Routing)) (Interface 0/1)#show flowcontrol 0/1 Admin Flow Control: Inactive Flow Control Flow Control RxPause TxPause Intf Oper Mode

	------- ------------ ------------ -------- -------- 0/1 Inactive Symmetric 0 0 ((Routing)) (Interface 0/1)#
描述	配置端口流控，默认端口流控自协商； 不支持在聚合成员口上配置； 不支持在 SVI 口上配置

- 配置端口 MTU

当端口进行大吞吐量数据交换时，可能会遇到大于以太网标准帧长度的帧，这种帧被称为 jumbo 帧。用户可以通过设置端口的 MTU 来控制该端口允许收发的最大帧长。 MTU 是指帧中有效数据段的长度，不包括以太网封装的开销。 端口收到或者转发的帧，如果长度超过设置的 MTU，将被丢弃。

因芯片限制，MTU 值仅支持偶数，若用户配置为奇数，设备将自动对齐，如配置 MTU 为 127,实际支持 128 长度报文通过。

命令	(Routing)(config-if)# **mtu** LENGTH (Routing)(config-if)# **no mtu**
描述	配置端口 MTU，允许设置的范围为 <1500 to 12270> 字节，缺省为 1518 字节 不支持在聚合成员口上配置；

	不支持在 SVI 口上配置

- 配置端口隔离

部分应用环境下，要求设备部分端口间不能互相通讯，可以通过将这些端口设置为隔离口实现。当端口设为隔离口之后，隔离口之间互相无法通讯，隔离口与非隔离口之间可以正常通讯，非隔离口与非隔离口之间可以正常通讯。

命令	(Routing)(config-if)#(Routing)port protected <0-2> (Routing)(config-if)# **no** (Routing)port protected <0-2>
描述	默认端口为非隔离口； 当前不支持在聚合口、vlan 口上配置隔离功能

- 显示端口光/铜缆模块信息

该命令用于显示光口上插入的的光/铜缆模块的信息。

命令	(Routing)#show fiber-ports optics {all | unit/slot/port} (Routing)#show fiber-ports optics all (Routing)#show fiber-ports optics 0/1
描述	不指定 unit/slot/port 则显示所有端口的模块信息 不指定 info 则显示端口模块的 DDM 信息,指定则显示完整模块信息（基本信息，告警信息，厂商信息）

3. 配置风暴控制

3.1. 风暴控制概述

当 LAN 中存在过量的广播、多播或未知单播数据流时，将导致网络性能下降，甚至网络瘫痪的现象，称为广播风暴。风暴控制针对广播、多播和未知单播数据流进行限速，当交换机端口接收到的广播、未知名多播或未知单播数据流的速率超过所设定的带宽时，设备将只允许通过所设定带宽的数据流，超出带宽部分的数据流将被丢弃，从而避免过量的泛洪数据流进入 LAN 中形成风暴。

3.2. 配置命令

- 配置接口风暴控制策略

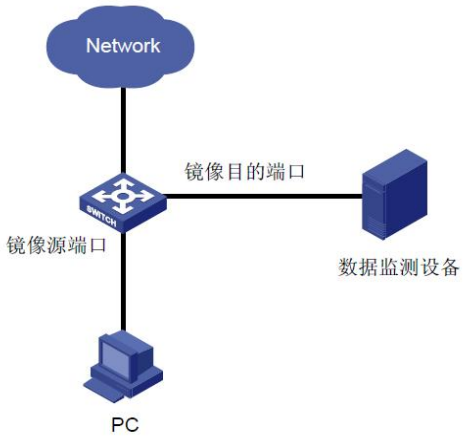
命令	(Routing)(config-if)#storm-control {**broadcast | multicast | unicast | }** (Routing)(config-if)#no storm-control {**broadcast | multicast | unicast | }** (Routing)(config-if)#storm-control {**broadcast | multicast | unicast | }**level threshold (Routing)(config-if)#no storm-control {**broadcast | multicast | unicast | }** level (Routing)(config-if)#storm-control {**broadcast | multicast | unicast | }** rate threshold (Routing)(config-if)#no storm-control {**broadcast | multicast | unicast | }** rate ((Routing)) #show storm-control all
描述	配置/删除端口风暴控制策略； 支持在 broadcast/multicast/unicast/all/unicast-broadcast/ multicast-broadcast 中选择配置，选择配置无法共存;

	其中 multicast 表示未知名多播报文，unicast 表示未知名单播报文； level 数值为端口带宽百分比，rate 为端口速率变动

4. 配置 SPAN

4.1. SPAN 概述

SPAN（Local (Routing)ed Port Analyzer）为本地镜像功能。SPAN 功能将指定端口的报文复制到目的端口，一般 SPAN 目的端口会接入数据检测设，用户利用这些设备分析目的端口接收到的报文，进行网络监控和故障排除。



SPAN 并不影响源端口和目的端口的报文交换，只是将源端口所有进入和输出的报文原样复制了一份到目的端口。当源端口的镜像流量超过目的端口带宽的情况下，例如 100Mbps 目的端口监控 1000Mbps 源端口的流量，可能导致报文被丢弃。

SPAN 基于会话管理，在会话中配置 SPAN 的源端口与目的端口。在一个会话中，只能有一个目的端口，但是可以同时配置多个源端口。

4.2. 配置命令

- 创建会话

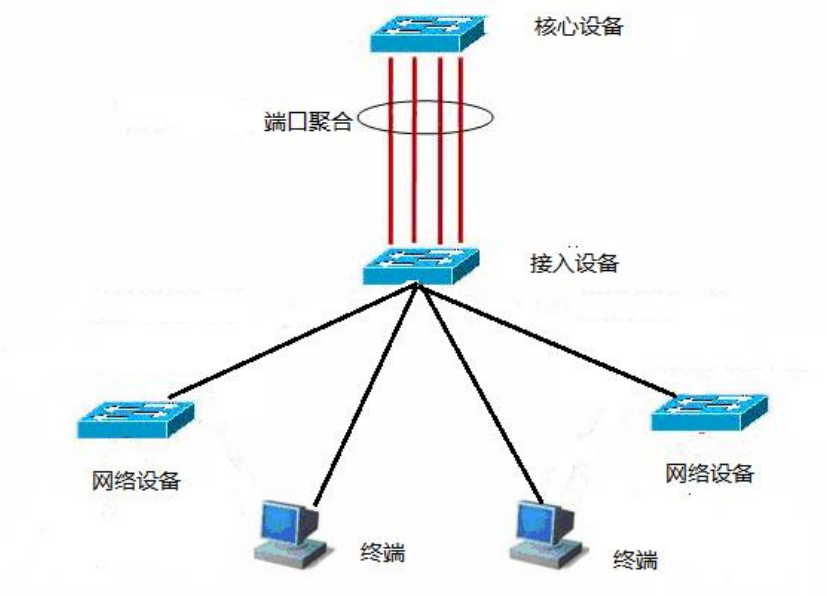
命令	(Routing)(config)#monitor session session-id {source {interface unit/slot/port | cpu || vlan vlan-id | remote vlan vlan-id }[{rx | tx}] | destination {interface

	unit/slot/port |remote vlan vlan-id reflector-port unit/slot/port}| mode | (Routing)(config)#**no monitor session** SESSION-ID ((Routing)) #show monitor session all
描述	创建/删除/显示会话，创建会话同时进入会话模式； 支持会话数 4 个

5. 配置端口聚合

5.1. 聚合口概述

将多个物理链接捆绑在一起建立一个逻辑链接，这个逻辑链接我们称之为聚合口（port-channel，后者 PO 口），该功能称为端口聚合功能。聚合口功能符合 IEEE802.3ad 标准， 它可以用于扩展链路带宽，提供更高的连接可靠性，常用于端口上联，如下图所示。



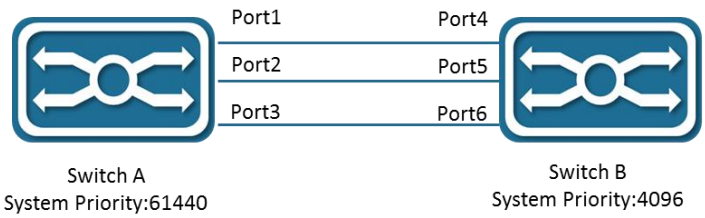
聚合口具备以下几个特性：高带宽，聚合口总带宽为物理成员口带宽总和；支持流量均衡策略，可以根据策略把流量地分配给各成员链路；支持链路备份，当聚合口中的一条成员链路断开时，系统会将该成员链路的流量自动地分配到聚合口中的其它有效成员链路上。

5.2. LACP 概述

基于 IEEE802.3ad 标准的 LACP（Link Aggregation Control Protocol，链路汇聚控制协议）是一种实现链路动态汇聚的协议。如果端口启用 LACP 协议，端口会发送 LACPDU 来通告自己的系统优先级、系统 MAC、端口的优先级、端口号和操作 key 等。相连设备收到对端的 LACP 报文后，根据报文中的系统 ID 比较两端的系统优先级。在系统 ID 优先级较高的一端，将按照端口 ID 优先级从高到低的顺序，设置聚合组内端口处于聚合状态，并发出更新后的 LACP 报文，对端设备收到报文后，也会把相应的端口设置成聚合

状态，从而使双方在端口退出或者加入聚合组上达到一致。只有双方的端口都完成动态聚合绑定操作后，该物理链路才能进行数据报文的转发。

LACP 成员口链路绑定之后，还会进行周期性的 LACP 报文交互，在一段时间没有收到 LACP 报文时，就认为收包超时，成员口链路解除绑定，端口重新处于不可转发状态。这里的超时时间有两种模式:长超时模式和短超时模式.在长超时模式下，端口间隔 30 秒发送一个报文，若 90 秒没有收到对端报文，就处于收包超时；在短超时模式下，端口间隔 1 秒发送一个报文，若 3 秒钟没有收到对端报文，就处于收包超时。



如上图所示，交换机 A 和交换机 B 通过 3 个端口连接在一起。设置交换机 A 的系统优先级为 61440，设置交换机 B 的系统优先级为 4096。在交换机 A 和 B 的 3 个直连端口上打开 LACP 链路聚合，设置 3 个端口的聚合模式为主动模式，设置 3 个端口的端口优先级为默认优先级 32768。

在收到对端的 LACP 报文后，交换机 B 发现自己的系统 ID 优先级比较高(交换机 B 的系统优先级比交换机 A 高)，于是按照端口 ID 优先级的顺序(端口优先级相同的情况下，按照端口号从小到大的顺序)设置端口 4、5、6 处于聚合状态。交换机 A 收到交换机 B 更新后的 LACP 报文后，发现对端的系统 ID 优先级比较高，并且把端口设置成聚合状态了，也把端口 1、2、3 设置成聚合状态了。

5.3. 配置命令

- 端口加入/退出聚合口

命令	加入静态聚合口: (Routing)(config-if)#addport lag <lag-group-id> (Routing)(config-if)#addport lag 1 加入动态聚合(LACP):

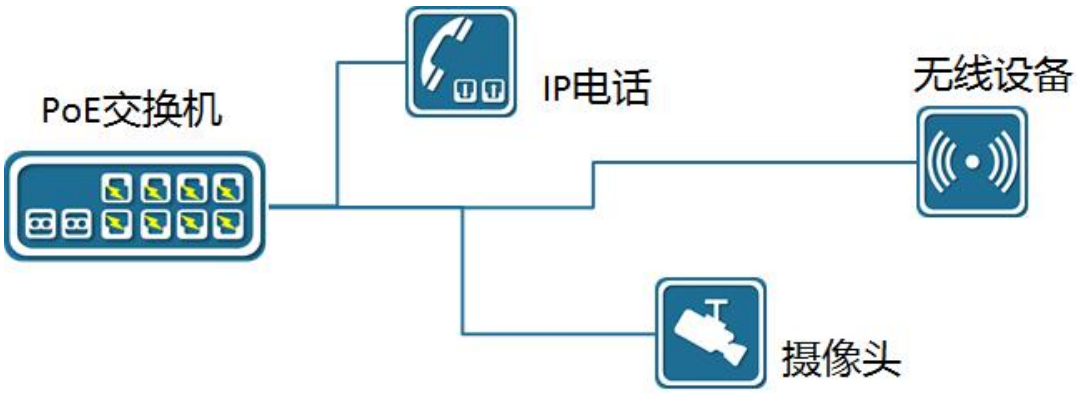
	(Routing)(config)#interface 1/1 (Routing)(Interface 1/1)#no port-channel static 查看端口汇聚 ((Routing)) #show interface lag 1
描述	支持 8 个聚合口<1-8>； 一个聚合口要么是静态的，要么是动态的，由加入的第一个成员口加入方式来决定。 Active 聚合模式表示该端口会主动发起 LACP 聚合运算；Passive 聚合模式表示该端口不会主动发起 LACP 聚合运算，但是在接收到邻居的 LACP 报文后会被动参与 LACP 计算。

6. 配置 POE

6.1. PoE 概述

Power over Ethernet，简称 PoE，是一个可以在以太网路中通过双绞线与终端进行数据交互同时，提供直流供电的技术。常用对网络电话、WIFI AP、网络摄影机、集线器、电脑等设备进行供电。

按照标准其供电最长距离为 100m。



PSE（Power Sourcing Equipment，供电设备），如上图中 PoE 交换机。PSE 在 PoE 端口的线路上寻找、检测 PD，对 PD 分级，并向其供电。 当检测到 PD 拔出后，PSE 停止供电。PD 是接受 PSE 供电的设备，如上图中 IP 电话、无线设备、摄像头。

PoE 发展经历了两套标准：

IEEE 802.3af(15.4W)是首个 PoE 供电标准，规定了以太网供电标准，是现在 PoE 应用的主流实现标准。它明确规定了远程系统中的电力检测和控制事项，并对路由器、交换机和集线器通过以太网电缆向 IP 电话、安全系统以及无线 LAN 接入点等设备供电的方式进行了规定。IEEE802.3at(25.5W)应大功率终端的需求而诞生，在兼容 802.3af 的基础上，提供更大的供电需求，满足新的需求。根据 IEEE 802.3af 规范，受电设备(PD)上的 PoE 功耗被限制为 12.95W。IEEE 802.3at，它将功率要求高于 12.95W 的设备定义为 Class 4(该级别在 IEEE 802.3af 中有描述，但留作将来使用)，可将功率水平扩展到 25W 或更高。

6.2. 配置命令

- 配置外部电源功率

命令	(Routing)(config)#poe power limit {class-based | none | user-defined maximum-power} (Routing)(config)#no poe power limit [user-defined]
描述	配置外部电源功率 默认电源功率计算方式：PoE 供电端口数与单端口 15.4W 的乘积 若配置功率小于当前设备消耗功率，则对低优先级端口的 PD 设备下电，端口优先级为端口 ID 小的更高优先级。

- 配置端口供电使能

命令	(Routing) (config-if)#**poe** (Routing) (config-if)#**no poe**
描述	配置端口使能供电 默认端口供电使能

- 配置使能兼容模式

命令	(Routing) (config-if)#`poe high-power {legacy | pre-dot3at | dot3at | upoe}` (Routing) (config)#`no poe high-power`
描述	配置 PoE 全局开启关闭兼容模式 在没有接入 PD 设备的端口上使用这个命令，可能导致对端设备被错误的上电烧毁，请确

	保端口在接入 PD 设备的时候使用该命令 不符合标准的 PoE 设备，Class 分级统一显示为 0

7. 配置 VLAN

7.1. VLAN 功能概述

VLAN 是虚拟局域网（Virtual Local Area Network）的简称，它是在一个物理网络上划分出来的逻辑网络。这个网络对应于 ISO 模型的第二层网络。VLAN 的划分不受网络端口的 实际物理位置的限制。VLAN 有着和普通物理网络同样的属性，除了没有物理位置的限制，它和普通局域网一样。第二层的单播、广播和多播帧在一个 VLAN 内转发、扩散，而不会直接进入其它的 VLAN 之中。

基于端口的 VLAN 是最简单的一种 VLAN 划分方法。用户可以将设备上的端口划分到不同的 VLAN 中，此后从某个端口接收的报文将只能在相应的 VLAN 内进行传输，从而实现广播域的隔离和虚拟工作组的划分。

以太网交换机的端口链路类型可以分为三种：Access、Trunk、Hybrid。这三种端口在加入 VLAN 和对报文进行转发时会进行不同的处理。

Access 类型：端口只能属于 1 个 VLAN；一般用于交换机与终端用户之间的连接；

Trunk 类型：端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，但是只有 native VLAN 可以不带 VLAN 标记；一般用于交换机之间的连接；

Hybrid 类型：端口可以属于多个 VLAN，可以接收和发送多个 VLAN 的报文，并且可以根据用户的需要配置相关 VLAN 是否带 VLAN 标记；可以用于交换机之间连接，也可以用于连接用户的计算机。

7.2. 配置命令

- 创建删除 VLAN

命令	(Routing)#vlan database (Routing)(vlan)# **vlan** VLAN_RANGE (Routing)(vlan)# **no vlan** VLAN_RANGE

描述	创建/删除 VLAN

- 配置基于 Access 端口的 VLAN

命令	(Routing)(config)#**interface** 0/1 (Routing)(config-if)#**(Routing)port mode access**
描述	进入以太网端口模式。 配置端口类型为 Access 端口（缺省情况下，端口为 Access 类型）。

命令	(Routing)(config-if)#**(Routing)port access vlan** VLANID (Routing)(config-if)#**no (Routing)port access vlan**
描述	将当前端口加入到指定 VLAN（缺省情况下，所有 Access 端口均属于且只属于 VLAN1），no 命令恢复为缺省。 只有当接口已经配置为 Access 端口后，才能使用如上命令，且指定的 VLAN 必须已经创建。 当配置为非 VLAN1 后，若对应 VLAN 删除，会自动恢复为 VLAN1。

- 配置基于 Trunk 端口的 VLAN

命令	(Routing)(config)#**interface** 0/1 (Routing)(config-if)#**(Routing)port mode trunk**

描述	进入以太网端口模式。 配置端口类型 Trunk 端口。

命令	(Routing)(config-if)#**(Routing)port trunk allowed vlan** { **all** | VLAN_LIST | **none**} (Routing)(config-if)#**no (Routing)port trunk allowed vlan** VLAN_LIST
描述	维护 Trunk 端口的 Allowed VLAN 列表。 只有当接口已经配置为 Trunk 端口后，才能使用如上命令。 All 表示自动模式，自动加入所有已创建的 VLAN，（即使是后续创建，也会自动加入）； None 表示清空 Allowed VLAN 列表，即端口不属于任何 VLAN（包括 native vlan）； VLAN_LIST 表示手动设置 Allowed VLAN 列表，若之前属于 ALL（自动模式），会先清空 Allowed VLAN 列表，再进行 VLAN 列表的添加。VLAN_LIST 支持标准的多 vlan 表示方法(“-”和“,”以及两者组合)； 前面增加 no 关键字时表示从 Allowed VLAN 列表中删除 VLAN_LIST 表示的 VLAN。 设置 all 时，将 Allowed VLAN 列表的维护改为自动模式，其他命令，均修改为手工模式。（缺省情况下，为自动模式，当从其他端口模式切换为 Trunk 端口时，即为自动模式）。 只有已经创建的 VLAN，才能加入 Allowed VLAN 列表；当删除 VLAN 时，Allowed VLAN 列表中对应 VLAN 会自动删除。

命令	(Routing)(config-if)#**(Routing)port trunk native vlan** VLANID (Routing)(config-if)#**no (Routing)port trunk native vlan**
描述	设置 Trunk 端口的 native vlan。（缺省情况下，Trunk 端口的 native VLAN 为 VLAN1），no 命令恢复为缺省。 只有当接口已经配置为 Trunk 端口后，才能使用如上命令。 Native VLAN 的设置跟 Allowed VLAN 是否包含此 VLAN，甚至 VLAN 是否创建没有关系，即 native VLAN 可以设置为一个没有创建的 VLAN。

说明

✦本地设备 Trunk 端口缺省 VLAN ID 和相连的设备的 Trunk 端口的缺省 VLAN ID 必须一致，否则缺省 VLAN 的报文将不能正确传输。

- 配置基于 general 端口的 VLAN

命令	(Routing)(config)#**interface** 0/1 (Routing)(config-if)#**(Routing)port mode general**
描述	进入以太网端口模式。 配置端口类型 general 端口。

命令	(Routing)(config-if)#(Routing)port trunk allowed vlan 2 (Routing)(config-if)#vlan participation include 2,3001 (Routing)(config-if)#vlan tagging 2 (Routing)(config-if)#**no** vlan participation include 2,3001 (Routing)(config-if)#no vlan tagging 2
描述	include :包含的 vlan Tagging：出口打上 tag

说明

✦本地设备 **general** 端口缺省 VLAN ID 和相连的设备的 **general** 端口的缺省 VLAN ID 必须一致，否则缺省 VLAN 的报文将不能正确传输。

7.3. 显示命令

在特权模式下，才可以查看 VLAN 的信息。显示的信息包括 VLAN VID、VLAN 状态、VLAN 成员端口以及 VLAN 配置信息。

- 显示 VLAN

(Routing) #show vlan

```
VLAN ID VLAN Name                                VLAN Type

------- -------------------------------- --------------------

1       default                          Default

2       VLAN0002                         Static

3001    VLAN3001                         Static


(Routing) #
```

8. 配置 QINQ

8.1. QINQ 概述

QinQ 技术〔也称 Stacked VLAN 或 Double VLAN〕。标准出自 IEEE 802.1ad，指在用户报文进入服务提供商网络之前封装上一个服务提供商网络的公网 VLAN Tag，而把用户报文中的私网用户 VLAN Tag 当做数据，使报文带着两层 VLAN Tag 穿越服务提供商网络。

在城域网中需要大量的 VLAN 来隔离用户，IEEE 802.1Q 协议仅支持的 4094 个 VLAN 远远不能满足需求。通过 QinQ 技术双层 Tag 封装，在服务提供商网络中报文只根据公网上分配的唯一外层 VLAN Tag 传播，这样不同的私网用户 VLAN 可以重复使用，扩大了用户可利用的 VLAN Tag 数量，同时提供一种简单的二层 VPN 功能，所以实际上 QINQ 技术是一种 VLAN VPN 技术。

常见的 VLAN VPN 技术除 QINQ 外，还有 VLAN Mapping。两者的区别仅仅在于 QINQ 是对 VLAN 做堆叠（Stacking），VLAN Mapping 是对 VLAN 做映射（Mapping）。

- VLAN Stacking: 从用户网络到提供商网络，单层 tag 变为双层 Tag，C-Tag 保留在报文中，作为内层 Tag；反向，从双层 Tag 变为单层 Tag。

8.2. 配置说明

QINQ 分为三类：

- A 类：基本 QINQ，基于接口开启关闭，当开启基本 QINQ 的接口收到报文时，都当成 untag 报文处理，在原有报文的基础上，增加一层该端口缺省 VLAN 的 VLAN Tag。
- B 类：基于 C-tag 的灵活 QINQ，根据用户侧的 C-VLAN Tag，根据配置的映射策略，在原始报文基础上，增加一层 S-VLAN Tag。该类 QINQ 的配置方式有可选的两种方式，二者只能选择其一。一种方式为接口上直接配置 C-VLAN 和 S-VLAN 的映射关系；一种方式在全局配置 VLAN VPN(其中包含了 C-VLAN 和 S-VLAN 的映射关系)，然后在接口上关联 VPN。对多个接口采用相同映射策略的情况，一般选择后面一种配置方式。对于此类 QINQ，若接口收到的报文为 untag 时，C-tag 为接口的缺省 VLAN Tag。
- C 类：基于 ACL 的灵活 QINQ，根据配置的流策略，来添加外层 Tag。该类 QINQ 的配置放入“QOS”模块中，具体参见“配置 QOS”章节，Policy-map 和 Class-map 的策略对中：“**nest vlan**<1-4094>”即是用于配置基于 ACL 的灵活 QINQ。

如上三类 QINQ 在同一个端口可以同时开启，其优先级关系为：C 类> B 类> A 类。

8.3. 配置命令

- 创建/删除 dvlan-tunnel ethertype

命令	(Routing)(config)#dvlan-tunnel ethertype {802.1Q | vman | custom value} (Routing)(config)#no dvlan-tunnel ethertype (Routing)(config)#dvlan-tunnel ethertype {802.1Q | vman | custom value} [primary-tpid] (Routing)(config)#no dvlan-tunnel ethertype {802.1Q | vman | custom 1–65535} [primary-tpid]
描述	配置和删除 dvlan-tunnel ethertype

- 创建/删除 mode dvlan-tunnel

命令	(Routing)(Interface 0/1)#mode dvlan-tunnel (Routing)(config-vlan-vpn)#**no mode dvlan-tunnel**
描述	配置和删除 dvlan-tunnel

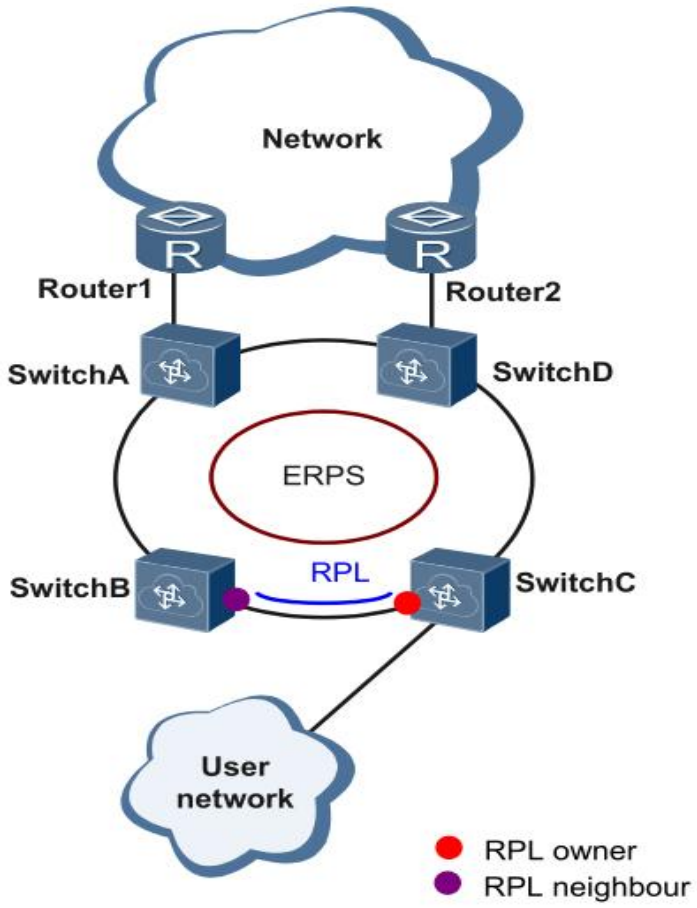
9. 配置 ERPS

9.1. ERPS 功能概述

ERPS（Ethernet Ring Protection (Routing)ing，以太环网保护切换协议）为 ITU 开发的一种环网保护协议，也称 G.8032。它是一个专门应用于以太环网的链路层协议。它在以太环网完整时能够防止数据环路引起的广播风暴，而当以太环网上一条链路断开时能迅速恢复环网上各个节点之间的通信。

目前，解决二层网络环路问题的技术还有 STP。STP 应用比较成熟，但其收敛的时间比较长（秒级）。ERPS 是专门应用于以太环网的链路层协议，二层收敛性能达 50ms 以内，具有比 STP 更快的收敛速度。

ERPS 典型组网：



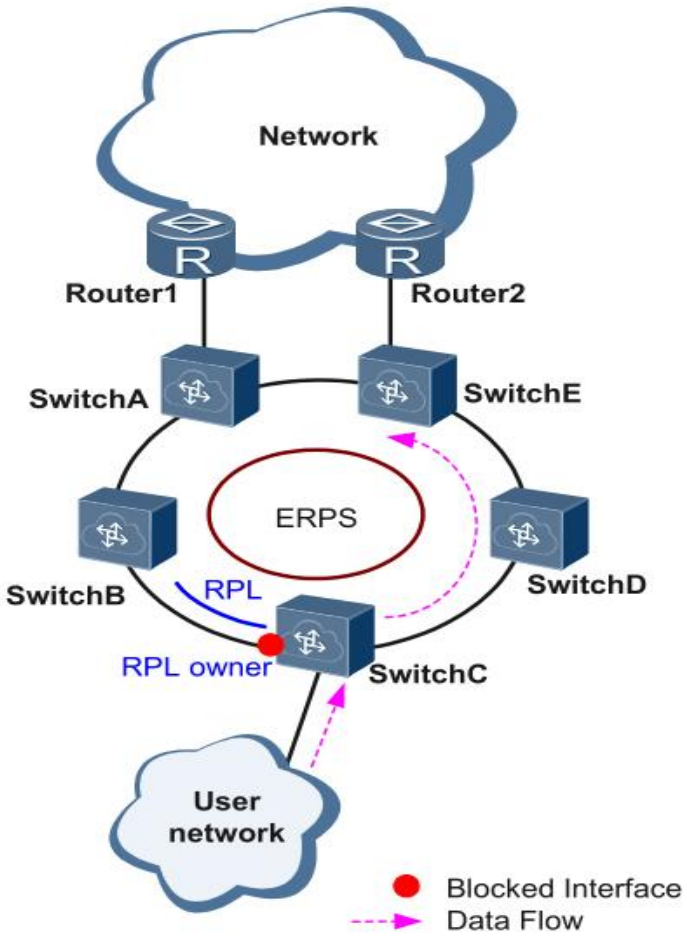
9.2. ERPS 原理简介

ERPS 是一种专用于以太网链路层的标准环网协议，以 ERPS 环为基本单位。每台二层交换设备上只能有两个端口加入同一个 ERPS 环。在 ERPS 环中，为了防止出现环路，可以启动破除环路机制，阻塞 RPL owner 端口，消除环路。当环网发生链路故障时，运行 ERPS 协议的设备可以迅速地放开阻塞端口，进行链路保护倒换，恢复环网上各节点间链路通信。本节主要以示例的形式按照链路正常->链路故障->链路恢复的过程（包括保护倒换操作），介绍基本的单环组网下 ERPS 的实现原理。

链路正常

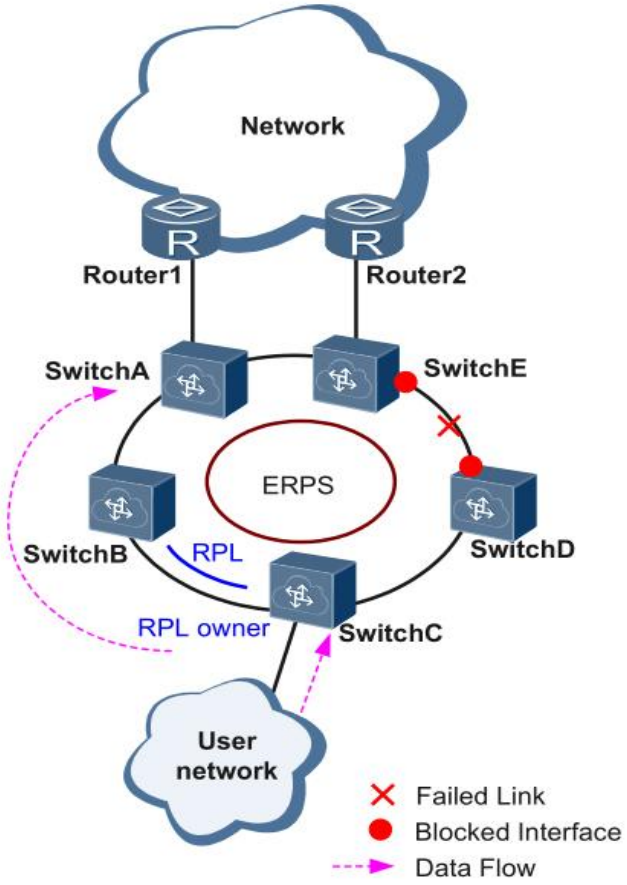
如下图所示，由(Routing)A ~ (Routing)E 组成的环路上各设备通信正常。

为防止环路产生，ERPS 首先会阻塞 RPL owner 端口，如果配置了 RPL neighbour 端口，该端口同样会被阻塞，其他端口可以正常转发业务流量。



链路故障

如图所示，当(Routing)D 和(Routing)E 之间的链路发生故障时，ERPS 协议启动保护倒换机制，将故障链路的两端端口阻塞，然后放开 RPL owner 端口，这两个端口重新恢复用户流量的接收和发送，从而保证了流量不中断。



链路恢复

链路恢复正常后，如果 ERPS 环配置的是回切模式，RPL owner 端口所在设备会重新阻塞 RPL 链路上的流量，故障链路重新被用来完成用户流量的传送。

9.3. 配置命令

- 创建环

命令	(Routing)(config)#**erps domain ring** <1-16>

	(Routing)(config)#**no erps domain ring** <1-16> (Routing) (Config-erps-domain-1)#role-mode none-interconnection (Routing) (Config-erps-domain-1)#ring <1-16>
描述	创建/删除 ERPS 环； ERPS 环是由一组配置了相同的控制 VLAN 且互连的二层交换设备构成，是 ERPS 协议的基本单位，环中的每台设备上都需要配置。 环编号为 ERPS 环的唯一标识。

- 关联 ERPS 实例和环

命令	(Routing)(Config-erps-ring-1)#**erps ring** <1-16>
描述	配置 ERPS 实例和环的对应关系；

- 配置 ERPS 实例等级

命令	(Routing)(Config-erps-ring-1)#**raps-mel** <0-7>
描述	配置 ERPS 实例等级；

- 配置 ERPS 实例中 RPL 角色

命令	(Routing)(Config-erps-ring-1)#**ring-port rpl** NAME (Routing)(Config-erps-ring-1)#**ring-port** rl
描述	配置 ERPS 实例 RPL 角色；

	一个 ERPS 环只有一个 RPL owner 端口，由用户配置决定，通过阻塞 RPL owner 端口转发用户流量来防止 ERPS 环中产生环路。

- 配置实例保护的管理 VLAN

命令	(Routing)(Config-erps-ring-1))#**raps-vlan** <2-4094> (Routing)(Config-erps-ring-1)#**no raps-vlan**
描述	配置/删除 ERPS 实例的管理 VLAN/数据 VLAN； 每个 ERPS 环必须配置控制 VLAN。不同 ERPS 环不能使用相同 ID 的控制 VLAN。

- 配置 ERPS 回切模式

命令	(Routing)(config-erps-prof)#**revertive enable | non-revertive enable**
描述	配置 ERPS 自动回切/不回切；

- 配置 ERPS 定时器参数

命令	(Routing)(config-erps-prof)#wtr-time <1-12>
描述	配置 ERPS 定时器参数； <1-12>: 单位分钟；故障恢复后的回切时间，默认为 5 分钟

9.4. 显示命令

- 显示 ERPS 环信息

((Routing)) #show erps

D : Discarding

F : Forwarding

FS : Forced (Routing)

MS : Manual (Routing)

Domain ID	Ring ID	Control VLAN	WTR Timer (min)	Guard Timer (msec)	RL Port	RPL Port
1	1	3001	1	500	0/9(B)	0/10(B)

Total number of rings configured = 1

Loacal ring node id: cc:52:91:0a:02:10

((Routing)) #show erps detail

Domain ID : 1

Ring ID : 1

Ring Topology mode : major-ring

Node Type mode : rpl-owner-node

RAPS Level : 0

Control Vlan : 3001

Protected Instance : 0

Service Vlan : 0-4092

WTR Timer Setting (min) : 1

Guard Timer Setting (msec) : 500

Holdoff Timer Setting (msec) : 0

WTB Timer Setting (sec) : 5

Ring State : protection

Revertive Mode : revertive

Time since last topology change : before 1175sec.

Forced (Routing) Port : NULL

Manual (Routing) Port : NULL

RL Port : 0/9(Block)

RPL Port : 0/10(Block)

((Routing)) #show erps statistics

Ring	Port	RX/TX	SF	NR	NRRB	FS	MS	EVENT

---- ------ ------ -------- ---------- ---------- ---------- ---------- ----------

1	0/9	RX	0	0	0	0	0	0
1	0/9	TX	0	0	0	0	0	0
1	0/10	RX	0	0	0	0	0	0
1	0/10	TX	0	0	0	0	0	0

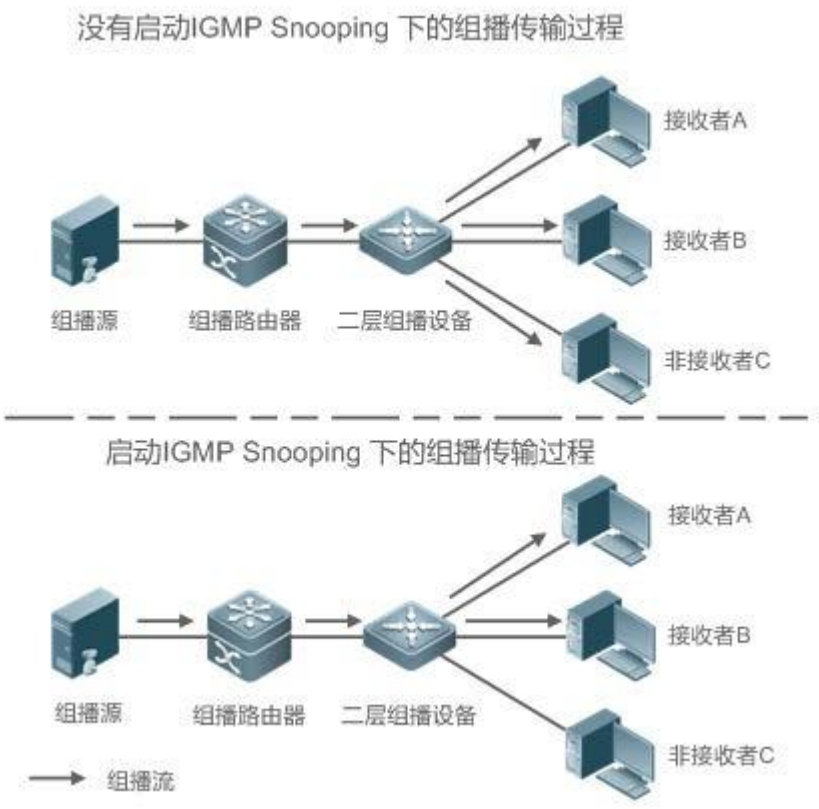
10. 配置 IGMP SNOOPING

10.1. 概述

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束的机制，用于管理和控制组播组。

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。

如下图所示，当二层组播设备没有运行 IGMP Snooping 时，IP 组播报文在 VLAN 内被广播；当二层组播设备运行了 IGMP Snooping 后，IP 组播报文只发给组成员接收者。



10.2. 配置命令

- 启用 IGMP Snooping

命令	(Routing)(config)#**set igmp** (Routing)(config)#**no set igmp** (Routing)(config)#**set igmp**［*vlan-id*］ (Routing)(config)#**no set igmp**［*vlan-id*］
描述	启用/关闭 IGMP Snooping 功能；默认关闭。 全局模式。

- 配置 IGMP Snooping 端口

命令	(Routing)(config)#set igmp interfacemode (Routing)(config#no set igmp interfacemode
描述	开启/关闭 IGMP Snooping 端口；可选配置。

- 配置 IGMP Snooping 查询

命令	(Routing)(config)set igmp querier 1 (Routing)(config)set igmp querier election participate 1
描述	配置/删除 IGMP Snooping 查询器

- 配置 IGMP Snooping 快速离开

命令	(Routing)(config)#`set igmp fast-leave [`*vlan-id*`]` (Routing)(config)#**no** `set igmp fast-leave [`*vlan-id*`]`
描述	配置/删除 IGMP Snooping 快速离开功能；可选配置。 SVI 接口模式。

- 配置 IGMP Snooping 老化时间

命令	(Routing)(config)#`set igmp groupmembership-interval [`*vlan-id*`]` *second* (Routing)(config)#**no** `set igmp groupmembership-interval [`*vlan-id*`]` *second*
描述	配置/删除 IGMP Snooping 老化时间；可选配置

- 配置 IGMP Snooping 最大响应时间

命令	(Routing)(config)#`set igmp maxresponse [`*vlan-id*`]` *seconds* (Routing)(config)#**no** `set igmp maxresponse [`*vlan-id*`]` *seconds*
描述	配置/删除 IGMP Snooping 响应时间；可选配置

- 配置 IGMP Snooping mrouter

命令	(Routing)(config-0/1)#set igmp mrouter *vlan-id* (Routing)(config-0/1)#**no** set igmp mrouter *vlan-id* (Routing)(config-0/1)#set igmp mrouter interface (Routing)(config-0/1)#no set igmp mrouter interface
描述	配置/删除 mrouter；可选配置

10.3. 显示命令

- 查看 IGMP Snooping 组播组

```
(Routing) #show igmpsnooping 1

VLAN ID..................................... 1
IGMP Snooping Admin Mode.................... Enabled
Fast Leave Mode............................. Enabled
Group Membership Interval (secs)............ 260
Max Response Time (secs).................... 10
Multicast Router Expiry Time (secs)......... 0
Report Suppression Mode..................... Disabled

(Routing) #
(Routing) #show igmpsnooping

Admin Mode.................................. Enable
Multicast Control Frame Count............... 15
IGMP header validation...................... Enabled
Interfaces Enabled for IGMP Snooping........ 0/1
                                             0/2
                                             0/3
                                             0/4
                                             0/5
                                             0/6
                                             0/7
                                             0/8
```

```
                                                0/9
                                                0/10
                                                0/11
                                                0/12
                                                1/1
                                                1/2
                                                1/3
                                                1/4
                                                1/5
                                                1/6
                                                1/7
                                                1/8
VLANs enabled for IGMP snooping..... 1

(Routing) #show igmpsnooping mrouter

Command not found / Incomplete command. Use ? to list commands.

(Routing) #show igmpsnooping querier

Global IGMP Snooping querier status
-----------------------------------
IGMP Snooping Querier Mode..... Enable
Querier Address..... 0.0.0.0
IGMP Version..... 2
Querier Query Interval..... 60
Querier Expiry Interval..... 125
```

11. 配置 STP 生成树协议

11.1. 概述

生成树协议是一种二层管理协议，它通过选择性地阻塞网络中的冗余链路来消除二层环路，同时还具备链路备份的功能。

与众多协议的发展过程一样，生成树协议也是随着网络的发展而不断更新的，从最初的 STP（Spanning Tree Protocol，生成树协议）到 RSTP（Rapid Spanning Tree Protocol，快速生成树协议），再到最新的 MSTP（Multiple SpanningTree Protocol，多生成树协议）。

对二层以太网来说，两个 LAN 间只能有一条活动着的通路，否则就会产生广播风暴。但是为了加强一个局域网的可靠性，建立冗余链路又是必要的，其中的一些通路必须处于备份状态，如果当网络发生故障，另一条链路失效时，冗余链路就必须被提升为活动状态。手工控制这样的过程显然是一项非常艰苦的工作，STP 协议就自动地完成这项工作。它能使一个局域网中的设备起以下作用：

发现并启动局域网的一个最佳树型拓朴结构。

发现故障并随之进行恢复，自动更新网络拓朴结构，使在任何时候都选择了可能的最佳树型结构。

11.2. 配置命令

- 配置 STP 模式

命令	(Routing)(config)#**spanning-tree mode** {**stp | rstp | mst**}
描述	stp：Spanning tree protocol(IEEE 802.1d) rstp：Rapid spanning tree protocol(IEEE 802.1w) mst：Multiple spanning tree protocol(IEEE 802.1s) 默认为 mstp 模式，模式切换后生成树协议默认关闭，需要重新启用。

	全局模式。

- 启用生成树协议

命令	(Routing)(config)#**spanning-tree** (Routing)(config)#**no spanning-tree**
描述	启用/关闭 STP 功能；默认关闭。 全局模式。

- 配置设备优先级

命令	(Routing)(config)#**spanning-tree priority** <0-4094> <0-61440> (Routing)(config)#**no spanning-tree priority** <0-4094>
描述	配置/删除 STP 系统优先级；默认 32768。可选配置。 全局模式。

- 配置 Forward-Delay Time

命令	(Routing)(config)#**spanning-tree forward-time** <4-30> (Routing)(config)#**no spanning-tree forward-time**
描述	配置/重置 STP 端口转发状态延迟时间，单位为秒；默认为 15s。可选配置。 全局模式。

- 配置 Max-Age Time

命令	(Routing)(config)#**spanning-tree max-age** <6-40> (Routing)(config)#**no spanning-tree max-age**
描述	配置/重置 BPDU 报文的生命周期，单位为秒；默认为 20s。可选配置。 Hello Time、Forward-Delay Time、Max-Age Time 需要遵循条件：2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0seconds)，否则有可能导致拓扑不稳定。 STP/RSTP 网络最长路径受本参数影响，默认最长路径为 20 台，当超出 20 台设备时，需要修改配置(可以配置 forward-delay 21s，max-age 40s)，最大支持最长路径 40 台。 全局模式。

- 配置 Max-Hops

命令	(Routing)(config)#**spanning-tree max-hops** <6-40> (Routing)(config)#**no spanning-tree max-hops**
描述	配置/重置 BPDU 报文的最大跳数；默认为 20。可选配置。 MSTP 网络最长路径受本参数影响，当超过 20 台设备时需要修改配置，最大 40。 MSTP 兼容 max-age 功能，需要同时调整 max-age 参数，参考对应命令。 全局模式。

- 配置 Transmit-Holdcount

命令	(Routing)(config)#**spanning-tree transmit hold-count** <1-10> (Routing)(config)#**no spanning-tree transmit hold-count**

描述	配置/重置每秒最多发送的 BPDU 数；默认为 6 个。可选配置。 全局模式。

- 创建 instance

命令	(Routing)(config)#**spanning-tree mst instance** <1-4094> (Routing)(config)#**no spanning-tree mst instance** <1-4094>
描述	创建/删除 instance 实例。 全局模式。

- 配置 MST VLAN 和 instance 的对应关系

命令	(Routing)(config)# **spanning-tree mst vlan** <1-4094> <1-4094> (Routing)(config)# **no spanning-tree mst vlan** <1-4094> <1-4094>
描述	配置/删除 MST 实例和 VLAN 的关联；可选配置。 全局模式。

- 配置 MST 区域名

命令	(Routing)(config)#**spanning-tree configuration name** NAME (Routing)(config)#**no spanning-tree configuration name** NAME
描述	配置/删除 MST 区域名；可选配置。 全局模式。

- 配置 MST 版本号

命令	(Routing)(config)#**spanning-tree configuration revision** <0-65535>
描述	配置/删除 MST 版本号，默认为 0；可选配置。 全局模式。

- 配置端口优先级

命令	(Routing)(config-if)#**spanning-tree port-priority** <0-240> (Routing)(config-if)#**spanning-tree instance** <1-4094> **port-priority**<0-240>
描述	配置端口 STP 优先级；默认 128。可选配置。 接口配置模式。

- 配置端口路径花费

命令	(Routing)(config-if)#**spanning-tree cost** <1-200000000> (Routing)(config-if)#**no spanning-tree cost**
描述	配置/重置端口的路径花费；可选配置。 接口配置模式。

- 配置 Protocol Migration 处理

命令	(Routing)(config-if)#**clear spanning-tree detected protocols**
描述	对所有端口强制进行版本检查。

	特权模式。

- 配置 Edge Port

命令	(Routing)(config-if)#**spanning-tree {edgeport | auto-edge}** (Routing)(config-if)#**no spanning-tree {edgeport | auto-edge}**
描述	配置/删除端口 Edge Port；配置为 edgeport 表示该端口直连设备不是网桥设备，可以快速 forward；配置为 autoedge 表示该端口依据 BPDU 自动识别是否边缘端口；默认关闭；可选配置。 接口配置模式。

- 配置 Root Guard

命令	(Routing)(config-if)# **spanning-tree guard root** (Routing)(config-if)#**no spanning-tree guard root**
描述	配置/删除端口 Root Guard；接口打开 Root Guard 功能时，强制其在所有实例上的端口角色为指定端口，一旦该端口收到优先级更高的配置信息时，Root Guard 功能会将该接口置为 blocked 状态；默认关闭；可选配置。 接口配置模式。

- 配置 BPDU Filter

命令	(Routing)(config)#**spanning-tree bpdufilter** (Routing)(config)#**no spanning-tree bpdufilter**

描述	配置/删除 BPDU Filter；端口打开 BPDU Filter 后，既不发送 BPDU，也不接收 BPDU 报文；可选配置。 接口配置模式。

11.3. 显示命令

- 查看 STP 状态

```
(Routing)#show spanning-tree
```

- 查看 MSTP 实例状态

```
(Routing)#show spanning-tree mst detailed <0-4094>
```

12. MAC 地址管理

12.1. MAC 地址概述

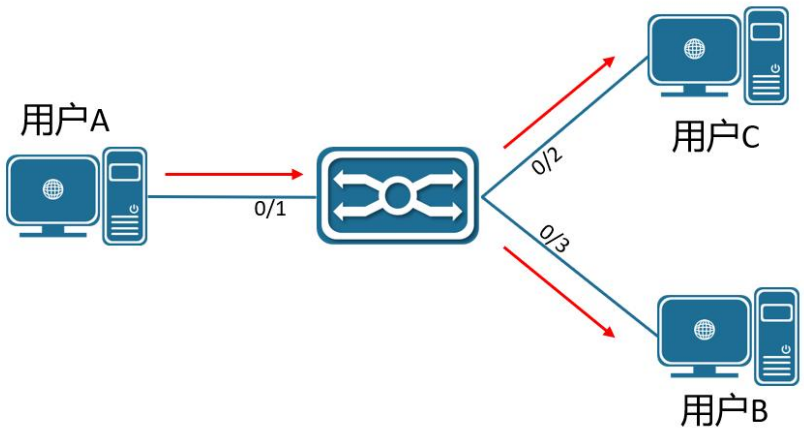
以太网交换机通过解析报文所携带的目的 MAC 地址，查询 MAC 地址表，将报文发送到相应的端口。MAC 地址表记录了与该设备相连的设备的 MAC 地址、接口以及所属的 VLAN ID 信息。以太网交换机根据 MAC 地址表查找的结果决定采用知名单播或未知名广播的转发方式。

知名单播：以太网交换机在 MAC 地址表中查到与报文的目的 MAC 地址和 VLAN ID 相对应的表项并且表项中的输出端口是唯一的，报文直接从表项对应的端口输出。

未知名广播：以太网交换机在地址表中没有找到目标 MAC 地址对应的表项，报文被送到所属的 VLAN 中除报文输入端口外的其他所有端口输出。

以太网交换机的 MAC 地址可通过动态获取或静态配置，一般情况下通过动态获取得到。下面通过分析用户 A 与用户 C 交互过程，给出 MAC 地址动态学习的工作原理。

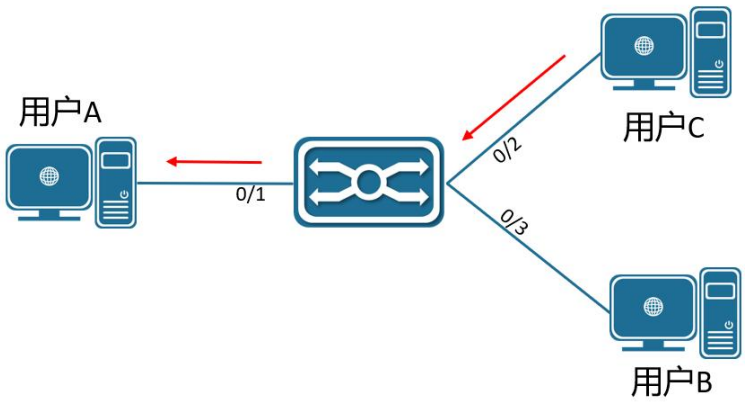
用户 A 发送报文到交换机的端口 gigabitEthernet0/1，此时以太网交换机将用户 A 的 MAC 地址学习到 MAC 地址表中。由于地址表中没有用户 C 的源 MAC 地址，因此以太网交换机以广播的方式将报文发送到除连接用户 A 的 gigabitEthernet0/1 以外的同属 VLAN1 的所有端口，包括用户 B 与用户 C 的端口，此时用户 B 能够收到用户 A 所发出的不属于它的报文。



当前动态 MAC 地址表信息：

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	gigabitEthernet0/1

用户 B 收到报文后将回应报文通过以太网交换机的端口 gigabitEthernet0/2，发送给用户 A，此时以太网交换机的 MAC 地址表中已存在用户 A 的 MAC 地址，报文被以单播的方式转发到 gigabitEthernet0/1 端口，同时以太网交换机将学习用户 C 的 MAC 地址，与前面所不同的是用户 B 此时接收不到用户 C 发送给用户 A 的报文。



当前动态 MAC 地址表信息：

用户	VLAN	MAC 地址	端口
用户 A	1	000E.C6C1.C8AB	gigabitEthernet0/1
用户 C	1	000E.C6C1.C8AD	gigabitEthernet0/2

通过用户 A 与用户 C 的一次交互过程后，设备学习到了用户 A 与用户 C 的源 MAC 地址，之后用户 A 与用户 C 之间的报文交互则采用单播的方式进行转发，此后用户 B 将不再接收到用户 A 与用户 C 之间的交互报文。

12.2. 配置命令

- 配置动态 MAC 地址老化时间

命令	(Routing)(config)#**bridge aging-time** <10-1000000> (Routing)(config)#**no bridge aging-time**
描述	配置 MAC 地址老化时间，范围 10-1000000 秒； 默认 MAC 地址老化时间 300 秒；

- 配置静态 MAC 地址

命令	(Routing)(config-0/1)#**port-security mac-address** MAC_ADDR VLANID (Routing)(config-0/1)#**no port-security mac-address** MAC_ADDR VLANID
描述	配置静态 MAC 地址； 当设备在 VLANID 指定 的 VLAN 上接收到以 MAC_ADDR 为目的地址的报文时

- 清除动态 MAC 地址

命令	(Routing)**#clear mac-address-table all** (Routing)**#clear mac-address-table interface** (Routing)**#clear mac-address-table vlan**
描述	动态 MAC 地址清除操作; 支持全部、基于 VLAN、基于端口的 MAC 地址清除操作

12.3. 显示命令

- 显示 MAC 地址

```
((Routing)) #show mac-addr-table all

VLAN ID  MAC Address         Interface             IfIndex  Status
-------  ------------------  --------------------  -------  ------------
1        00:E0:4C:1D:65:FE   0/3                   3        Learned
1        C8:39:0D:01:DC:99   0/1                   1        Static
1        C8:39:0D:01:DC:A0   3/1                   65       Management

((Routing)) #
```

- 显示 MAC 地址个数统计

```
((Routing)) #show mac-addr-table count

Dynamic Address count..................... 2
Static Address (User-defined) count..... 1
Total MAC Addresses in use..... 3
Total MAC Addresses available..... 32768
```

13. 配置 LLDP

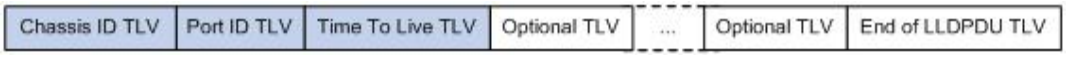
1.1. 协议概述

LLDP（Link Layer Discovery Protocol，链路层发现协议）提供了一种标准的链路层发现方式，使不同厂商的设备能够在网络中相互发现并交互各自的系统及配置信息。LLDP 将本端设备的信息（包括主要能力、管理地址、设备标识、接口标识等）封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB 的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

LLDPDU

LLDPDU 是封装在 LLDP 报文数据部分的数据单元。在组成 LLDPDU 之前，设备先将本地信息封装成 TLV 格式，再由若干个 TLV 组合成一个 LLDPDU 封装在 LLDP 报文的数据部分进行传送。

图 22-1 LLDPDU 的封装格式



如图 22-1 所示，蓝色的 Chassis ID TLV、Port ID TLV、Time To Live TLV 是每个 LLDPDU 都必须携带的，其余的 TLV 则为可选携带。每个 LLDPDU 最多可携带 32 种 TLV。

TLV

TLV 是组成 LLDPDU 的单元，每个 TLV 都代表一个信息。LLDP 可以封装的 TLV 包括基本 TLV、802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED（Link Layer Discovery Protocol Media Endpoint Discovery，链路层发现协议媒体终端发现）TLV。

基本 TLV

基本 TLV 是网络设备管理基础的一组 TLV，802.1 组织定义 TLV、802.3 组织定义 TLV 和 LLDP-MED TLV 则是由标准组织或其他机构定义的 TLV，用于增强对网络设备的管理，可根据实际需要选择是否在 LLDPDU 中发送。

在基本 TLV 中，有几种 TLV 对于实现 LLDP 功能来说是必选的，即必须在 LLDPDU 中发布，如表 22-1 所示。

表 22-1 基本 TLV

TLV 名称	说明	是否必须发布
Chassis ID	发送设备的桥 MAC 地址	是
Port ID	标识 LLDPDU 发送端的端口。如果 LLDPDU 中携带有 LLDP-MED TLV，其内容为端口的 MAC 地址；否则，其内容为端口的名称	是
Time To Live	本设备信息在邻居设备上的存活时间	是

TLV 名称	说明	是否必须发布
End of LLDPDU	LLDPDU 的结束标识，是 LLDPDU 的最后一个 TLV	否
Port Description	端口的描述	否
System Name	设备的名称	否
System Description	系统的描述	否
System Capabilities	系统的主要功能以及已开启的功能项	否
Management Address	管理地址，以及该地址所对应的接口号和 OID（Object Identifier，对象标识符）	否

802.1 组织定义 TLV

IEEE 802.1 组织定义 TLV 的内容如表 22-2 所示。

目前，H3C 设备不支持发送 Protocol Identity TLV 和 VID Usage Digest TLV，但可以接收这两种类型的 TLV。

三层以太网接口仅支持 Link Aggregation TLV。

表 22-2 IEEE 802.1 组织定义的 TLV

TLV 名称	说明
Port VLAN ID(PVID)	端口 VLAN ID
Port and protocol VLAN ID(PPVID)	端口协议 VLAN ID
VLAN Name	端口所属 VLAN 的名称
Protocol Identity	端口所支持的协议类型
DCBX	数据中心桥能力交换协议（Data Center Bridging Exchange Protocol）
EVB 模块	（暂不支持）边缘虚拟桥接（Edge Virtual Bridging）模块，具体包括 EVB TLV 和 CDCP（S-Channel Discovery and Configuration Protocol，S 通道发现和配置协议） TLV 这两种 TLV。有关这两种 TLV 的详细介绍，请参见“EVB 配置指导”
Link Aggregation	端口是否支持链路聚合以及是否已开启链路聚合
Management VID	管理 VLAN
VID Usage Digest	包含 VLAN ID 使用摘要的数据
ETS Configuration	增强传输选择（Enhanced Transmission Selection）配置
ETS Recommendation	增强传输选择推荐
PFC	基于优先级的流量控制（Priority-based Flow Control）

TLV 名称	说明
APP	应用协议（Application Protocol）
QCN	（暂不支持）量化拥塞通知（Quantized Congestion Notification）

802.3 组织定义 TLV

IEEE 802.3 组织定义 TLV 的内容如表 22-3 所示。

Power Stateful Control TLV 是在 IEEE P802.3at D1.0 版本中被定义的，之后的版本不再支持该 TLV。H3C 设备只有在收到 Power Stateful Control TLV 后才会发送该类型的 TLV。

表 22-3 IEEE 802.3 组织定义的 TLV

TLV 名称	说明
MAC/PHY Configuration/Status	端口支持的速率和双工状态、是否支持端口速率自动协商、是否已开启自动协商功能以及当前的速率和双工状态
Link Aggregation	端口是否支持链路聚合以及是否已开启链路聚合
Power Via MDI	端口的供电能力，包括 PoE（Power over Ethernet，以太网供电）的类型（包括 PSE（Power Sourcing Equipment，供电设备）和 PD（Powered Device，受电设备）两种）、PoE 端口的远程供电模式、是否支持 PSE 供电、是否已开启 PSE 供电、供电方式是否可控、供电类型、功率来源、功率优先级、PD 请求功率值、PSE 分配功率值
Maximum Frame Size	端口支持的最大帧长度
Power Stateful Control	端口的电源状态控制，包括 PSE/PD 所采用的电源类型、供/受电的优先级以及供/受电的功率
Energy-Efficient Ethernet	节能以太网

管理地址

管理地址是供网络管理系统标识网络设备并进行管理的地址。管理地址可以明确地标识一台设备，从而有利于网络拓扑的绘制，便于网络管理。管理地址被封装在 LLDP 报文的 Management Address TLV 中向外发布。

LLDP 的工作模式

在指定类型的 LLDP 代理下，LLDP 有以下四种工作模式：

- TxRx：既发送也接收 LLDP 报文。
- Tx：只发送不接收 LLDP 报文。
- Rx：只接收不发送 LLDP 报文。
- Disable：既不发送也不接收 LLDP 报文。

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

协议规范

与 LLDP 相关的协议规范有：

- IEEE 802.1AB-2005：Station and Media Access Control Connectivity Discovery
- IEEE 802.1AB 2009：Station and Media Access Control Connectivity Discovery
- ANSI/TIA-1057：Link Layer Discovery Protocol for Media Endpoint Devices
- IEEE Std 802.1Qaz-2011：Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks-Amendment 18: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes

1.2. 配置命令

1.2.1. **开关和工作模式配置**

- 配置 LLDP 接口的开关工作模式

命令	(Routing)(Interface 0/1)# **lldp** { receive | transmit } (Routing)(Interface 0/1)# **lldp disable**
描述	LLDP 接口配置模式。 配置 LLDP 接口的工作模式。 可选。

1.2.2. **可选基本参数配置**

- 配置系统名称等参数

命令	(Routing)(Interface 0/1)#lldp transmit-tlv sys-name (Routing)(Interface 0/1)#lldp transmit-tlv sys-desc (Routing)(Interface 0/1)#lldp transmit-tlv sys-cap

	(Routing)(Interface 0/1)#lldp transmit-mgmt (Routing)(Interface 0/1)#lldp notification (Routing)(Interface 0/1)#lldp med
描述	接口模式。 配置/重置系统名称。 可选。

1.2.3. **可选状态机参数配置**

- 配置 LLDP 接口的 hold 参数

命令	((Routing)) (Config)#lldp timers <cr> Press enter to execute the command. hold The interval multiplier to set local LLDP data TTL. interval The interval in seconds to transmit local LLDP data. reinit The delay before re-initialization.
描述	全局模式 Lldp 发送间隔等 可选。

- 配置 LLDP 通告参数

命令	(Routing)(lldp)# notification-interval <5 - 3600> (Routing)(lldp)#
描述	全局配置模式。

1.3. 显示命令

- 显示 LLDP 接口的状态

```
#show lldp interface 0/1

((Routing)) #show lldp interface 0/1

LLDP Interface Configuration

Interface  Link    Transmit  Receive   Notify    TLVs     Mgmt
---------  ------  --------  --------  --------  -------  ----
0/1        Down    Enabled   Enabled   Enabled   1,2,3    Y

TLV Codes: 0- Port Description,   1- System Name
           2- System Description, 3- System Capabilities
```

- 显示 LLDP 接口邻居

```
#((Routing)) #show lldp remote-device int 0/1
```

14. 配置 L3

14.1. L3 概述

L3 功能包括三层口管理，ARP 管理以及路由管理。路由管理不包含动态路由管理。

- 三层口管理：

三层口是针对二层（交换）口而言的，一般分为路由口（普通物理端口或者聚合口切换为三层口）或者 SVI 口（(Routing) Virtual Interface，与一个 VLAN 相对应）。SVI 口是一个逻辑接口，架构在对应 VLAN 所包含的所有成员端口之上，与路由口不同，经过 SVI 进行三层转发的报文，在输入时会先经过二层（比如 VLAN 过滤，地址学习）再经过三层，在输出时先经过三层再经过二层（比如 VLAN 输出规则）。

因特网协议（Internet Protocol，IP）使用逻辑虚拟的地址将数据包从源方发送到目的方，即 IP 地址。在网络层，路由设备使用 IP 地址完成数据包转发。（协议规范：RFC 1918：Address Allocation for Private Internets， RFC 1166：Internet Numbers）

三层口管理也包含三层口的 IP 地址维护。IP 地址由 32 位二进制组成，为了书写和描述方便，一般用点分十进制表示。点分十进制表示时，分为四组，每组 8 位，范围从 0~255，组之间用“.”号隔开，比如“192.168.1.1”就是用十进制表示的 IP 地址。IP 地址顾名思义，自然是 IP 层协议的互连地址。32 位的 IP 地址由两个部分组成：1）网络地址部分，表明是哪个网络；2）主机地址部分，表明是网络中的哪个主机。IP 地址的网络地址部分和主机地址地址部分由网络掩码来划分，网络掩码也是一个 32 比特的数值，由前面若干个比特“1”和后面若干个比特“0”组成，IP 地址与网络掩码相与得到的就是对应网络地址部分。同样，网络掩码也可以直接通过掩码长度来表示。比如“192.168.1.1 255.255.255.0”和“192.168.1.1/24”表示相同的 IP 地址。

本设备三层口不支持配置 second IP 地址，即一个三层口最多配置一个 IP 地址。当一个三层口配置了 IP 地址，就确定了一个网段，同台设备的不同三层口必须属于不同的网段，不同三层口配置的 IP 地址必须属于不同网段。SVI 表示的三层口，对应的 VLAN 作为该三层口的唯一标识。

设备的不同三层口划分了不同网段后，这些不同网段（比如 VLAN1 和 VLAN2）间的转发就称为“三层转发”（跨越网段，或者说跨越了不同 VLAN）。

- ARP 管理：

在局域网中，每个 IP 网络设备都有两个地址：1）本地地址，由于它包含在数据链路层的帧头中，更准确地说应该是数据链路层地址，但实际上对本地地址进行处理的是数据链路层中的 MAC 子层，因此习惯上称为 MAC 地址，MAC 地址在局域网上代表着 IP 网络设备；2）网络地址，在互联网上代表着 IP 网络设备，同时它也说明了该设备所属的网络。

局域网上两台 IP 设备之间需要通信，必须要知道对方的 48 比特的 MAC 地址。根据 IP 地址来获知 MAC 地址的过程称为地址解析。地址解析的方式有两类：1) 地址解析协议 (ARP)；2) 代理地址解析协议 (Proxy ARP）。关于 ARP 、Proxy ARP，分别在 RFC 826，RFC 1027 文档中描述。

ARP(Address Resolution Protocol，地址解析协议)是用来绑定 MAC 地址和 IP 地址的，以 IP 地址作为输入，ARP 能够知道其关联的 MAC 地址。一旦知道了 MAC 地址，IP 地址与 MAC 地址对应关系就会保存在设备的 ARP 缓存中。有了 MAC 地址，IP 设备就可以封装链路层的帧，然后将数据帧发送到局域网上去。以太网上 IP 和 ARP 的封装为 Ethernet II 类型。

ARP 表项分为两类：来源于 ARP 协议生成的动态表项，来源于静态配置的静态表项。动态 ARP 表项靠 IP 报文触发打通形成，打通过程是一个 ARP 请求/应答的过程，打通后形成的 ARP 表项，若后续不可达，会自动老化。静态 ARP 表项不需要打通，也不会老化。

- 路由管理：

路由管理负责管理路由表，整合各种路由协议下发的路由，进行优选。路由表中根据来源不同，通常分为以下三类：

- 直连路由：链路层协议发现的路由，也称为接口路由。直连路由由三层口配置 IP 地址时自动生成，路由前缀为该三层口直连的网络。
- 静态路由：网络管理员手工配置的。
- 动态路由：动态路由协议（比如 RIP， OSPF）发现的路由。

本设备不支持动态路由协议，因此，也不支持动态路由。

路由表项由两个部分组成：

- 前缀：由一个 IP 地址及网络掩码(或者掩码长度)来表示，指路由表项所确定的目的网络或者主机（当掩码长度为 32 表示主机）。

- 直连或者下一跳：直连表示目的网络或者主机属于直连网络，直连路由即属于此情况，在配置静态路由时，指定三层口而非 IP 地址，也会生成此类路由表项；下一跳由一个 IP 主机地址来表示，表示了要到达目的网络或主机，需要先转发到该 IP 地址表明的 IP 网络设备。

根据路由表项进行 IP 报文转发时，若该路由表项指定的是下一跳，链路层封装查询 ARP 时，使用下一跳的 IP，即链路层封装的目的 MAC 地址为下一跳的目的 MAC 地址。若该路由表项为直连的，则直接使用报文的目的 IP 进行 ARP 查询，即链路层封装的目的 MAC 地址为报文最终目的的 MAC 地址。不管哪种方式，若 ARP 查询不到，则会触发路由打通（生成动态 ARP 表项），若无法打通，IP 报文无法完成转发，将被丢弃。

路由表项间可能存在包含关系（根据掩码长度不同），所以，路由查找过程满足 LPM（Longest Prefix Match，最长前缀匹配）。即 IP 报文转发进行路由查找时，若同时命中多个路由表项，则选择前缀的掩码长度最长的那个路由表项。

14.2. 配置命令

14.2.1. **配置/删除 route 模式**

命令	**配置路由模式：** (Routing)(config)#**interface** 0/1 (Routing)(config-0/1)#ip routing **删除路由模式：** (Routing)(config-if)#no ip routing
描述	开启/删除路由模式

14.2.2. **配置/删除 SVI 口 IP 地址**

命令	**配置三层口 IP 地址：** (Routing)(config)#vlan routing 10 1 (Routing)(config)#int vlan 10 (Routing)(config-if)#**ip address** IPADDR MASK **删除三层口 IP 地址：** (Routing)(config)#int vlan10 (Routing)(config-if)#**no ip address** IPADDR MASK **查看三层口 IP 地址：** (Routing)#**show ip interface brief**
描述	在 SVI 的接口模式下进行配置。 当 VLAN 创建时，SVI 自动创建，VLAN 删除时，SVI 自动删除。int vlanXX 是进入该 SVI 的接口模式，而非创建 SVI 口，因此，当 SVI 不存在（对应 VLAN 不存在）时，进入该 SVI 的接口模式将会失败。同时，当 SVI 删除时，其上配置的 IP 地址会自动清除。 三层口支持进行 IP 地址配置更新，与删除再配置效果一样。不同三层口配置的 IP 地址必须属于不同网段。 三层口不支持配置 second ip。

	注意：配置本命令后，系统会将管理 IP 配置清除(参考:配置管理 IP)，转而使用三层口 IP 地址作为设备管理 IP。

14.2.3. **配置/删除路由口 IP 地址**

命令	**配置路由口 IP 地址：** (Routing)(config)#**interface** 0/1 (Routing)(config-0/1)#ip address IP(A.B.C.D) MASK(A.B.C.D) **删除三层口 IP 地址：** (Routing)(config-if)#no ip address IP(A.B.C.D) MASK(A.B.C.D)
描述	在接口模式下进行配置。 在配置路由口 IP 前，由于接口的默认属性是二层端口属性，因此需要使用 no (Routing)port 命令将端口从二层端口属性切换成三层的路由口属性，然后再使用 ip address 命令进行路由口的 IP 配置，反之，将路由口切换会二层端口属性，使用(Routing)port 命令。 三层口支持进行 IP 地址配置更新，与删除再配置效果一样。不同三层口配置的 IP 地址必须属于不同网段。 三层口不支持配置 second ip。

14.2.4. **配置/删除静态 ARP 表项**

命令	(Routing)(config)#**arp** IPADDR MACADD (Routing)(config)#**no arp** IPADDR

描述	在全局配置模式下进行配置。 静态 ARP 配置的 IP 地址必须属于直连网段，否则配置失败。 静态 ARP 优先级高于动态 ARP，当两者冲突，以静态 ARP 生效。 当三层口的 IP 地址删除或者三层口删除，若静态 ARP 的 IP 地址属于该三层口的直连网段，则该静态 ARP 失效（通过 show arp 可以看到不存在该表项，但 show run 可以看到配置还在）；同样，当某个三层口配置 IP 地址，其 IP 地址属于该三层口的直连网段的 ARP 表项将会从无效状态变为有效状态。(通过 show arp 可以看到 ARP 表项存在)。

14.2.5. **清除 ARP 缓存**

命令	(Routing)#**clear arp-cache**
描述	在特权模式下进行 ARP 缓存的清除。 该命令只是清除动态 ARP 表项，静态 ARP 表项不会被清除。

14.2.6. **配置/删除静态路由**

命令	(Routing)(config)#**ip route** { IPADDR MASK} {NH_IPADDR | <1-255> } (Routing)(config)#**no ip route** { IPADDR MASK} {NH_IPADDR | <1-255> }
描述	在全局配置模式下进行配置。 不支持递归路由（配置的下一跳 IP 必须属于直连网段）； 路由前缀不能属于直连网段（即直连路由自动生成，不能静态配置）。 当三层口配置 IP 地址时，若某条静态路由表项的前缀属于该三层口的直连网段，则该静态路由自动删除，以 LOG 方式提示；

	当三层口删除 IP 地址或者三层口删除时，若某条静态路由表项的下一跳 IP 属于该三层口的直连网段，则该静态路由自动删除，以 LOG 方式提示。

14.3. 显示命令

- 显示 ARP 表项

```
(Routing)#show arp
Address                  HWaddress              Interface      Type
192.168.1.238        00:00:00:00:04:86       vlan2          Static
192.168.2.46          00:00:00:00:05:45       vlan3          Static
192.168.3.110        00:00:00:00:08:59       vlan4          Static
192.168.0.12          00:00:00:00:00:09       vlan1          Static
192.168.0.1            00:0e:c6:d8:c7:f7         vlan1          Dynamic
10.100.2.2             00:01:a0:00:10:11       GiE0/2         Dynamic
```

- 显示路由表项

```
(Routing)#show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
       B - BGP Derived, IA - OSPF Inter Area
       E1 - OSPF External Type 1, E2 - OSPF External Type 2
       N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
       P - Net Prototype
```

15. 配置 OSPFv2

15.1. OSPFv2 概述

OSPF（Open Shortest Path First）是 IETF OSPF 工作组开发的一种基于链路状态的内部网关路由协议。OSPF 是专为 IP 开发的路由协议，直接运行在 IP 层，协议号为 89，采用组播方式进行 OSPF 包交换，组播地址为 224.0.0.5 (全部 OSPF 设备) 和 224.0.0.6 (指定设备)。它应用在 AS（Autonomous System，自治系统）内部。

一组运行 OSPF 路由协议的设备，组成了 OSPF 路由域的自治域系统。

一个自治域系统是指由一个组织机构控制管理的所有设备，自治域系统内部只运行一种 IGP 路由协议，自治域系统之间通常采用 BGP 路由协议进行路由信息交换。不同的自治域系统可以选择相同的 IGP 路由协议，如果要连接到互联网，每个自治域系统都需要向相关组织申请自治域系统编号。

当 OSPF 路由域规模较大时，一般采用分层结构，即将 OSPF 路由域分割成几个区域（area），区域之间通过一个骨干区域互联，每个非骨干区域都需要直接与骨干区域连接。

在 OSPF 路由域中，根据设备的部署位置，有三种设备角色：

- 区域内部设备：该设备的所有接口网络都属于一个区域；
- 区域边界设备：即 ABR（Area Border Routers）。该设备的接口网络至少属于两个区域，其中一个必须为骨干区域。
- 自治域边界设备：即 ASBR（Autonomous System Boundary Routers），是 OSPF 路由域与外部路由域进行路由交换的必经之路。

链路状态算法是一种与哈夫曼向量算法（距离向量算法）完全不同的算法，应用哈夫曼向量算法的传统路由协议为 RIP，而 OSPF 路由协议是链路状态算法的典型实现。与 RIP 路由协议对比，OSPF 除了算法上的不同，还引入了路由更新认证、VLSMs(可变长子网掩码)、路由汇聚等新概念。RIP 协议存在两个致命弱点：收敛速度慢、网络规模受限制（最大跳数不超过 16）。OSPF 克服了 RIP 的弱点，可以胜任中大型、较复杂的网络环境。

OSPF 路由协议利用链路状态算法建立和计算到每个目标网络的最短路径，该算法本身较复杂，以下简单地、概括性地描述了链路状态算法工作的总体过程：

- 初始化阶段，设备将产生链路状态通告，该链路状态通告包含了该设备全部链路状态；
- 所有设备通过组播的方式交换链路状态信息，每台设备接收到链路状态更新报文时，将拷贝一份到本地数据库，然后再传播给其它设备；
- 当每台设备都有一份完整的链路状态数据库时，设备应用 Dijkstra 算法针对所有目标网络计算最短路径树，结果内容包括：目标网络、下一跳地址、花费，是 IP 路由表的关键部分。

如果没有链路花费、网络增删变化，OSPF 将会十分安静，如果网络发生了任何变化，OSPF 通过链路状态进行通告，但只通告变化的链路状态，变化涉及到的设备将重新运行 Dijkstra 算法，生成新的最短路径树。

15.2. 配置命令

15.2.1. **创建 OSPF 进程**

命令	(Routing)(config)#**router ospf** (Routing)(config-router)#**router-id** *router-id*

	(Routing)(config-router)# **network** *IP(A.B.C.D) MASK(A.B.C.D)* **area** *area-id*
描述	要运行 OSPF 路由协议，需要先创建 OSPF 路由进程，并将对应的网络与 OSFP 路由进程进行关联。 router router 命令即为创建 OSPF 路由进程,process-id 为 OSPF 路由进程的实例号,未配置时表示进程实例 1。 router-id 命令为设置路由设备的 ID，以 IP 地址的形式表示。每个 OSPF 进程使用不同的 Router ID 进行区分。 network 命令即表示 OSPF 命令对外通告的关联网络的路由信息，也表示只在关联网络对应的接口上进行协议的通告和路由信息的更新。 IP 和 MASK 共同构成了地址范围。 area-id 时 OSPF 区域标识，它总是与一个 IP 地址范围关联，通常为了管理方便，会使用子网掩码作为 OSPF 区域的标识。

15.2.2. **接口网络类型配置**

命令	(Routing)(config-if)#**ip ospf network** {broadcast|point-to-point }
描述	broadcast 表示广播类型，以组播方式发送 OSPF 报文，能自动发现邻居，并选举出 DR（Designated Router）和 BDR（Backup Designated Router）。 point-to-point 表示点对点连接,要求接口 1 对 1 的方式方式互联,以组播方式发送 OSPF 报文，会自动发现邻居，不需要 DR/BDR 选举。

命令	(Routing)(config-if)#**ip ospf priority** *priority*

描述	priority 用于指定接口的优先级，值越大优先级越高，缺省为 1。

DR（Designated Router）：指定路由器。

BDR（Designated Router）：备份指定路由器。

在 OSPF 组网中，只有 DR 设备对外通告网络的链路状态，其它所有设备之间都保持邻居关系，但所有设备只和 DR/BDR 保持邻接关系，即除 DR/BDR 外的设备只和 DR/BDR 设备进行链路状态数据包的交互，DR 汇总计算后再通告给其它设备，OSPF 协议使用该机制来确保组网中的所有设备的链路状态数据是保持一致的。

DR 通过接口优先级比较进行选举，优先级最高的设备会被选举为 DR 设备，优先级设置为 0 的设备为放弃选举资格的设备。OSPF 邻居在一定时间没有接收到 DR 的 hello 报文会认为 DR 宕机，才会重新发起新一轮的 DR 选举，这是 DR 选举的唯一条件。设备动态修改优先级并不会立即生效，只有新一轮选举被触发才会生效。

15.2.3. **协议控制配置**

- 配置 hello 报文间隔

命令	(Routing)(config-if)#**ip ospf hello-interval** *seconds*
描述	hello-interval 用于设置接口上 hello 报文的发送间隔，邻居两端取值需要相同。

- 配置 dead 判定间隔

命令	(Routing)(config-if)#**ip ospf dead-interval** *seconds*
描述	dead-interval seconds 用于设置接口上判定邻居死亡的时间间隔，邻居两端取值需要相同

- 关闭 mtu 校验

命令	(Routing)(config-if)#**ip ospf mtu-ignore**

描述	mtu-ignore 用于设置关闭 OSPF 的 MTU 校验。OSPF 协议在接收数据库描述报文时会对邻居接口的 MTU 进行校验，如果接收数据库描述报文中所指示的接口的 MTU 大于接收接口的 MTU，则无法建立邻接关系，此时除了修改 mtu 值外，还可以将使用此配置将 mtu 校验关闭来解决问题。

- 禁止发出 LSA

命令	(Routing)(config-if)#**ip ospf database-filter all out**
描述	mtu-ignore 用于设置关闭 OSPF 的 MTU 校验。OSPF 协议在接收数据库描述报文时会对邻居接口的 MTU 进行校验，如果接收数据库描述报文中所指示的接口的 MTU 大于接收接口的 MTU，则无法建立邻接关系，此时除了修改 mtu 值外，还可以将使用此配置将 mtu 校验关闭来解决问题。

- 配置 lsu 报文发送延迟

lsu 报文中的包含了 LSAs(链路状态描述)的 Age 字段，该字段会再 LSU 报文发送之前递增。当 Age 达到 3600 时，会对 lsu 报文进行重传或者请求重传，如果没有得到及时的刷新，超时的 LSA 会被从链路状态数据库中删除掉。对于低速线路，由于接口发送和线路传播时延大，需要将 Age 字段递增加快，此时需要将 lsu 报文发送延迟配大，增加 Age 字段的递增步进来触发重传。

命令	(Routing)(config-if)#**ip ospf tramsmit-delay** *seconds*
描述	transmit-delay 用于设置接口上 lsu 报文的延时，单位为秒。

- 配置 lsu 报文重传间隔

设备发送一个 lsu 报文后，lsu 报文可能由于各种原因无法送达或无法收到对方确认应答，此时需要对 lsu 报文进行重传，通过配置 lsu 报文重传间隔来设定重传的时间。

命令	(Routing)(config-if)#**ip ospf retransmit-interval** *seconds*
描述	retransmit-interval 用于设置接口上 lsu 报文的重传时间间隔，单位为秒。时间需要大于邻居之间数据包往返传输的时延。

- 配置 SPF 刷新延时

命令	(Routing)(config-router)#**timers spf** *spf-holdtime*
描述	spf-delay 表示从网络拓扑变化到 SPF 开始计算需要延迟的时间，用于设置 SPF 计算对网络拓扑变化感知的灵敏度。 spf-holdtime 表示第一次触发 SPF 计算到第二次触发 SPF 计算的最小时间间隔。

如果链路震荡只是偶发，则将 spf-delay 值配置小，利于加快 OSPF 收敛速度；将值配置大则可以防止链路快速震荡导致 CPU 资源被大量消耗。

15.2.4. **被动接口配置**

被动接口配置可以用于禁止本设备的路由信息被其它设备学习到。可以基于整机或者指定接口设备被动接口及地址进行设置。被动接口/被动地址不能建立邻居，无法进行 OSPF 报文的交互，但被动地址的路由信息是可以通过非被动地址进行发布并被邻居所学习的。

命令	(Routing)(config-router)#**passive-interface default** (Routing)(config-router)#**passive-interface** <slot/port> (Routing)(config-router)#**passive-interface** vlan
描述	default 表示所有接口设置为被动接口。 slot/port 表示将指定的接口配置为被动接口。 vlan 表示配置被动 vlan。 no 表示删除被动接口。

15.2.5. **缺省路由发布配置**

命令	(Routing)(config-router)#**default-information originate** [always] [metric metric] [metric-type *type*]

描述	always 表示不管本地是否有缺省路由，OSPF 也会无条件产生缺省路由。 metric 表示缺省路由的度量值。 metric-type 表示缺省路由的类型。OSPF 的外部路由有两种类型：类型 1 的外部路由在不同路由设备上的度量值是不同的；类型 2 的外部路由在所有路由设备上的度量值是一样的。

配置 default-information originate 命令后，设备会自动变成 ASBR。

STUB 区域的 ABR 会自动向 STUB 区域发布缺省路由。

NSSA 区域的 ABR 会自动向 NSSA 区域发布缺省路由。

15.2.6. **路由重发布配置**

命令	(Routing)(config-router)# **redistribute** {bgp | connected | rip | static} [metric *value*] [metric-type {1 | 2}] [route-map *map-name*] [subnets] [tag *value*]
描述	该命令用来在 ASBR 设备上配置向 OSPF 进程引入外部路由（包括 OSPF 的其它进程/静态路由/其它路由协议的路由）。

15.2.7. **路由汇聚配置**

- 配置区域间路由汇聚

命令	(Routing)(config-router)#**area area-id range** *ip-address/mask* [advertise|not-advertise]
描述	area-id 表示路由汇聚的 OSPF 域 id。 ip-address 和 mask 表示汇聚路由的网段 ip 和掩码。 advertise 和 not-advertise 表示是否需要公布该汇聚路由。

这条命令只在 ABR 设备上有效，作用是把区域的多条路由进行合并汇聚变成一条路由后再将其通告到其它区域。由于汇聚只发生在 ABR 设备，所以区域内部路由看到的是具体的路由信息，但对于区域外的其它设备则只能看到汇聚后的一条路由。可以同时定义多个区域汇聚路由。路由汇聚可以使得整个路由域的路由得到精简。

- 配置外部路由汇聚

命令	(Routing)(config-router)#**summary-address** *ip-address mask* [not-advertise|tag *tag-value*]
描述	area-id 表示路由汇聚的 OSPF 域 id。 ip-address 和 mask 表示汇聚路由的网段 ip 和掩码。 not-advertise 表示不公布该汇聚路由,未使用该参数表示发布。 tag-value 表示路由的 tag 值。

其它路由进程发布给 OSPF 路由进程的路由都是以外部链路状态的方式通告给 OSPF 的，若注入的路由是连续的地址空间，AS 域便捷设备路由设备可以将连续地址空间的多条路由汇聚成一条路由进行通告，这样可以减小域内路由设备的路由表规模。

summary-address 配置在 NSSA 域的 ABR 上时，只对重分发的路由和 LSA 7 类转 5 类的路由进行汇聚，当配置在 ASBR 时，则只对重分发的路由进行汇聚。

summary-address 和 area range 的区别是，area range 是对 OSPF 域内的路由进行汇聚，summary-address 是对 OSPF 域外的路由进行汇聚。

15.2.8. **最短路径配置**

- 配置接口出方向的度量值

接口出方向的度量值的配置有三种方式：

- 一种是通过配置参考带宽的方式利用自动计算参考带宽与接口带宽的比值作为接口出方向的度量值，假设接口带宽为 100Mbps，我们配置参考带宽为 1000Mbps，则接口的缺省 cost 值就为 1000/100=10。

命令	(Routing)(config-router)#**auto-cost reference-bandwidth** *ref-bw*

描述	ref-bw 表示参考带宽。

➢ 另外一种是根据链路带宽、时延等元素考虑直接在接口上配置度量值。

命令	(Routing)(config-if)#**ip ospf cost** *cost-value*
描述	cost-value 表示度量值。

- 配置 STUB/NSSA 区域缺省路由度量值

ABR 设备发送给 STUB/NSSA 区域的缺省路由度量值默认为 1，可以通过配置指定度量值。

命令	(Routing)(config-router)#**area** *area-id* **default-cost** *cost-value*
描述	area-id 表示 OSPF 域 id。 cost-value 表示度量值。

- 配置重发布路由缺省度量值

ASBR 设备重发布的 BGP 路由的 metric 值默认为 1，重发布的的其它路由的 metric 值默认为 20，可以通过配置指定度量值，但需要和 redistribute 命令配合使用。

命令	(Routing)(config-router)#**default-metric** *metric-value*
描述	cost-value 表示度量值。

- 配置路由管理距离值

路由管理距离是指路由来源的可信度，它是一个介于 0 到 255 的数值，数据越大表示可信度越低，OSPF 在选择路由时会优先选择管理距离小即可信度高的路由。OSPF 管理距离缺省值为 110。

命令	(Routing)(config-router)#**distance** {*distance* | ospf {intra-area distance|inter-area distance|external *distance*}}

描述	intra-area 表示区域内路由。 inter-area 表示区域间路由。 external 表示外部路由。 distance 表示度量值。

15.3. 显示命令

- 显示路由信息

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

- 仅显示 OSPF 路由信息

```
(Routing) #show ip route ospf

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype



(Routing) #
```

- 其它 OSPF 信息

命令	作用
show ip ospf	显示 OSPF 概要信息
show ip ospf asbr	显示 OSPF 的边界和边界路由器信息
show ip ospf database	显示 OSPF 的数据库信息
show ip ospf interface	显示 OSPF 的接口相关信息
show ip ospf neighbor	显示 OSPF 的邻居信息

16. 配置 BGP

16.1. BGP 概述

BGP（Border Gateway Protocol）是一种不同自治系统的路由设备之间进行通信的外部网关协议(Exterior Gateway Protocol，EGP)，其主要功能是在不同的自治系统(Autonomous Systems，AS)之间交换网络可达信息，并通过协议自身机制来消除路由环路。

BGP 使用 TCP 协议作为传输协议，通过 TCP 协议的可靠传输机制保证 BGP 的传输可靠性。

运行 BGP 协议的 Router 称为 BGP Speaker，建立了 BGP 会话连接(BGP Session)的 BGP Speakers 之间被称作对等体 (BGP Peers)。

BGP Speaker 之间建立对等体的模式有两种：IBGP(Internal BGP)和 EBGP(External BGP)。IBGP 是指在相同 AS 内建立的 BGP 连接，EBGP 是指在不同 AS 之间建立的 BGP 连接。二者的作用简而言之就是：EBGP 是完成不同 AS 之间路由信息的交换，IBGP 是完成路由信息在本 AS 内的过渡。

16.2. 配置命令

16.2.1. **创建 BGP 进程**

命令	(Routing)(config)#**router bgp** *as-number* (Routing)(config-router)# **bgp router-id** *router-id*
描述	创建进程，并配置唯一标识。

16.2.2. **BGP 地址族配置**

命令	(Routing)(config-router)#address-family ipv4 [unicast | multicast]
描述	BGP 的路由模式位于 IPv4 单播地址族。对于分地址族配置的命令，在 BGP 路由模式下配置，将作用于 IPv4 单播地址族。

16.2.3. **BGP 邻居配置**

BGP 邻居需要手动配置，且需要在 BGP 会话者两端同时配置对端为本端邻居，因此 BGP 邻居也叫 BGP 对等体。

- 配置对等体

命令	(Routing)(config-router)# [**no**] **neighbor** *address* **remote-as** *as-number*
描述	address 表示 BGP 对等体的地址。 as-number 表示 as 号，范围为 1 – 4294967295。

16.2.4. **反射器配置**

一个 AS 中的所有的 BGP Speaker 之间需要建立全连接，因此随着 AS 中的 BGP Speaker 的数量增加，Speaker 之间需要维护的连接也相应增加，就会加重 Speaker 的资源消耗。为了降低这种消耗，可以使用 BGP 路由反射器的方式来设计网络。

在路由反射器使用中，可以根据类型将 BGP Speaker 设备分为客户端和非客户端。路由反射器与其客户端（不止于一个）之间组成一个群。对于路由反射器的客户端只跟反射器建立连接，客户端和客户端之间不建立连接，客户端与群外的 Speaker 之间也不建立连接，基于以上原理，BGP 路由反射器可以减少 AS 中 IBGP 对等体的连接数量。

将一台路由器配置为反射器就是为其指定哪些邻居作为客户端。

路由反射器对于路由学习的规则如下：

- 通过客户端学习到的路由，会同步给其它客户端以及其它非客户端；
- 通过 IBGP 非客户端学习到的路由，会同步给其它客户端。
- 通过 EBGP Speaker 学习到的路由，会同步给其它客户端以及其它非客户端；

如果一个群内有多个路由反射器，则需要为群配置一个群 ID，如果只有一个这可以不需要配置，群使用反射器的 Router-id 识别。

- 配置设备为路由反射器，并指定客户端

命令	(Routing)(config-router)# [**no**] **neighbor** {**address** } **route-reflector-client**
描述	address 表示对等体 IP 地址。 group-name 表示对等体组地址。

- 配置路由反射器群 ID

命令	(Routing)(config-router)#**bgp cluster-id** *cluster-id*
描述	cluster-id 表示路由反射器的群 ID。

- 配置取消客户端之间的路由反射

命令	(Routing)(config-router)#**no bgp client-to-client reflection**
描述	取消客户端之间的路由反射。

16.2.5. **路由汇聚配置**

命令	(Routing)(config-router)#**aggregate-address** *address mask* [as-set] [summary-only]
描述	address 和 mask 参数表示配置的聚合地址。 as-set 参数表示若配置该参数，会保留聚合地址范围内路径的 AS 路径信息。 summary-only 参数表示若配置该参数，则只会将聚合后的路径通告出去。默认是将聚合前后的所有路径信息都通告。

16.2.6. **管理距离配置**

管理距离是用于评价路由来源可信度的属性，管理距离越小，路由越优先。

命令	(Routing)(config-router)#**distance bgp** *external-distance internal-distance local-distance*
描述	external-distance 参数表示从 EBGP 对等体学到的路由的管理距离。 internal-distance 参数表示从 IBGP 对等体学到的路由的管理距离。 local-distance 参数表示从对等体学到，但被认为存在可以从 IGP 学到更优的路由的管理距离，通常这些路由是通过 network backdoor 命令进行表示的。

如果把一条路由配置成后门路由，如果 IGP 和 EBGP 都学到这条路由，则优先使用 IGP 的路由，但 IGP 学习到该路由并不会被通告出去。

命令	(Routing)(config-router)#**network** *address mask* **backdoor**
描述	address 和 mask 参数表示网段地址。 backdoor 参数表示这条路由为后门路由。

16.2.7. **多径负载均衡配置**

如果到达统一网段的路径有多条，数据可以通过这多条路径进行均衡转发就叫做多径负载均衡，可以通过启用/关闭多径负载均衡配置启用或关闭此功能。BGP 中，EBGP 的路由可以和 EBGP 的路由形成多径负载均衡，但不能和 IBGP 的路由组成多径负载均衡，IBPG 同理也不能和 EBGP 路由组成多径负载均衡。

- IBGP 多径负载均衡

命令	(Routing)(config-router)#**maximum-paths ibgp** *number*
描述	number 表示支持等价一下跳的个数，范围为 1-32。

- AS-path 宽松比较

在默认情况下，两条路由想要组合成等价路由形成多径负载均衡需要满足 AS-path 所有属性完全相等的条件。如果希望降低以上的苛刻条件形成多径负载均衡，可以通过启用 AS-path 宽松比较来达成。AS-path 宽松比较只需要在同路由多径的前提下满足 AS-path 长度和联盟 AS-path 长度分别相等的条件即可达成多径负载均衡。

命令	(Routing)(config-router)#**bgp bestpath as-path ignore**
描述	命令表示启用 BGP AS-path 宽松比较模式

16.2.8. **路由重分发配置**

- 路由注入

命令	(Routing)(config-router)# **redistribute** { connected | isis [area-tag] | ospf process-id | rip | static} [metric value] [metric-type {1 | 2}] [route-map map-name] [subnets] [tag value]
描述	该命令用来向 BGP 进程注入外部路由（包括静态路由/其它路由协议的路由）。

- 默认路由注入

命令	(Routing)(config-router)#**default-informnation originate**
描述	使用此命令将默认路由注入 BGP，通过协议分发。

16.2.9. **协议参数配置**

- 配置邻居保活定时器

命令	(Routing)(config-router)#**timer bgp** *holdtime*
描述	keepalive 参数是指对等体保持有效连接的周期，单位为秒，范围为 0-65535，默认值为 60。协议在 keepalive 周期内会发送 keepalive 报文对连接进行保持。 holdtime 参数是判断对等体是否有效的周期，单位为秒，范围为 0-65535，默认值为 180。如果设备在 holdtime 时间内没有收到对等体的 keepalive 报文则认为对等体连接无效。

当 BGP Speakers 之间建立 BGP 连接后，会对 holdtime 进行协商，两者之间会选出小的那个 holdtime 作为生效配置。keepalive 的生效值则会再 holdtime 协商完成后，基于协商生效的 holdtime 值取 1/3，与配置的 keepalive 值进行比较，使用两者中的较小值作为 keepalive 的生效配置。

还可以基于 BGP 对等体（组）配置 keepalive 和 holdtime 值。

命令	(Routing)(config-router)#**neighbor** {address | group-name} times
描述	adress 表示对等体的地址。 group-name 表示对等体组的名称。

- 配置邻居重连定时器

设备与对等体连接失效后需要尝试重新连接，可以通过配置重连定时器来指定重连周期。

命令	(Routing)(config-router)#**neighbor** {address | group-name} **timer connect** *connect-retry*
描述	adress 表示对等体的地址。 group-name 表示对等体组的名称。 connect-retry 表示重连周期，单位为秒，范围为 1-65535，默认值为 15 秒。

- 配置路由通告定时器

当设备本地产生路由变动时需要将更新的路由通告给对等体（组），可以通过路由通告定时器的配置来设置通告的频率。

命令	(Routing)(config-router)#**neighbor** {address | group-name} **advertisemet-interval** *interval-time*

描述	adress 表示对等体的地址。 group-name 表示对等体组的名称。 interval-time 表示发送路由更新的最小间隔，单位为秒，范围为 1-600，对于 IBGP 对等体默认值为 5 秒，对于 EBGP 对等体默认值为 30 秒。

16.3. 显示命令

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

- 仅显示 BGP 路由信息

```
(Routing) #show ip route bgp

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
```

- 其它 BGP 信息

命令	作用
show ip bgp	显示 BGP 的概要信息
show ip bgp summary	显示 BGP 的连接汇总信息
show ip bgp neighbors	显示 BGP 的邻居详细信息

17. 配置 RIP

17.1. RIP 概述

RIP(Routing Information Protocol)路由协议是一种使用距离向量算法的路由协议，主要使用在小型网络中。分别有 RIPv1 和 RIPv2 两个版本（RIPv1 在 RFC 1058，RIPv2 在 RFC 2453 文档中定义）。
RIP 协议报文是基于 UDP 协议的报文，UDP 端口号为 520。RIPv1 报文一般采用广播报文的形式；RIPv2 报文采用组播报文的形式，组播地址为 224.0.0.9；

RIP 协议每隔 30 秒向外发送更新报文，若 180 秒没有收到对端的路由更新报文则本机将所有来自对端此设备的路由标记为不可达，此状态后，再在 120 秒后仍未收到更新报文本机会将对端设备所通告的这些路由从路由表中删除。

RIP 的路由度量是指用于衡量达到目的地距离的跳数。直连网络的跳数标记为 0，每经过一个设备可达的网络跳数为 1；不可达网络的跳数为 16。

RIP 路由进程只会向与进程关联的网络接口发送更新报文。

17.2. 配置命令

17.2.1. **创建 RIP 进程**

命令	(Routing)(config)#router rip
描述	要运行 RIP 路由协议，需要先创建 RIP 路由进程，并将对应的网络与 RIP 路由进程进行关联。 router rip 命令即为创建 RIP 路由进程。 network 命令即表示 rip 命令对外通告的关联网络的路由信息，也表示只在关联网络对应的接口上进行协议的通告和路由信息的更新。 IP 和 MASK 共同构成了地址范围。

17.2.2. **配置 RIP 版本**

产品支持 RIP 的版本 1 和 2。版本 2 支持认证，路由汇聚，密钥管理。

默认情况下产品可以接收版本 1 和版本 2 的 RIP 数据包，但只会发送版本 1 的数据包。

产品支持基于整机指定接收和发送的 RIP 版本的数据包或者基于端口指定。

基于端口指定发送的 RIP 版本：

命令	(Routing)(config-if)# ip rip send version {1|2} {1|2}
描述	可以通过此命令来指定端口只发送所指定版本的数据包。

基于端口指定接收的 RIP 版本：

命令	(Routing)(config-if)# ip rip receive version {1|2} {1|2}
描述	可以通过此命令来指定端口只发送所指定版本的数据包。

17.2.3. **路由重发布配置**

命令	(Routing)(config-router)# redistribute {bgp | connected [area-tag] | ospf process-id | rip | static} [metric value] [metric-type {1 | 2}] [route-map map-name] [subnets] [tag value]
描述	该命令用来在 ASBR 设备上配置向 OSPF 进程引入外部路由（包括 OSPF 的其它进程/静态路由/其它路由协议的路由）。

17.2.4. **配置路由汇聚**

当子网路由穿越有类路由的网络边界时，可以将子网路由汇聚成有类网络路由，这样可以提高网络的伸缩性和有效性，即在路由表中看不到包含在汇聚路由内的子路由，这样可以大大缩小路由表的规模。RIP 的版本 2 缺省情况下会自动进行路由汇聚，版本 1 不支持此功能。

命令	(Routing)(config)#router rip (Routing)(config-router)#[no] auto-summary
描述	auto-summary 表示开启路由自动汇聚。 no 关键字表示关闭路由自动汇聚。

17.2.5. **配置水平分割**

距离向量路由协议由于其自身的机制导致当多台设备连接在 IP 广播类型网络上时，会经常出现路由环路。而水平分割机制就是用于避免路由环路的形成。

水平分割机制是通过阻止某些路由信息从学习到该路由信息的接口通告出去的方式来优化多设备之间的路由信息交换。但该机制对于非广播多路访问网络（如 X.25 网络、帧中继网路等）会由于通告被阻止而无法学习到完整的路由信息，因此就不适合开启水平分割。

毒性逆转是水平分割技术的一种改进机制，开启带毒性逆转的水平分割时，设备中学习到对于路由信息的接口仍然会将这些路由信息通告出去，但是会将路由信息中的度量值属性设置成不可达，这样对端在接收到这类的路由信息后，会立刻抛弃该路由，而不等待其老化时间到，加速路由的收敛。

水平分割是在全局模式下进行配置的。

命令	(Routing)(config)#[no] ip rip split-horizon {poisoned-reverse}
描述	split-horizon 关键字表示开启 rip 的水平分割。 poisoned-reverse 关键字表示毒性逆转。

17.2.6. **配置缺省路由通告**

可以基于接口指定路由更新报文中产生一条默认路由。也可以指定只通过该默认路由而不通告其它的路由。

命令	(Routing)(config-if)#ip rip default-information {originate | only} [metric metric-value]

	(Routing)(config)#default-information originate
描述	originate 关键字表示除了通告默认路由外，也通告其它路由。 only 关键字表示只通告本接口的默认路由，不通告其它路由。

注意： RIP 进程中配置的 default-information 和接口下配置的 ip rip default-information 之间，接口配置优先级高于 RIP 进程配置，即两种都存在的情况下，通告接口下配置的默认路由。

17.3. 显示命令

- 显示路由信息

```
(Routing) #show ip route

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

- 仅显示 RIP 路由信息

```
(Routing) #show ip route rip

Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static
        B - BGP Derived, IA - OSPF Inter Area
        E1 - OSPF External Type 1, E2 - OSPF External Type 2
        N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
        P - Net Prototype
```

- 其它 RIP 信息

命令	作用
show ip rip	显示 RIP 数据库
show ip rip interface	显示 RIP 的相关接口信息

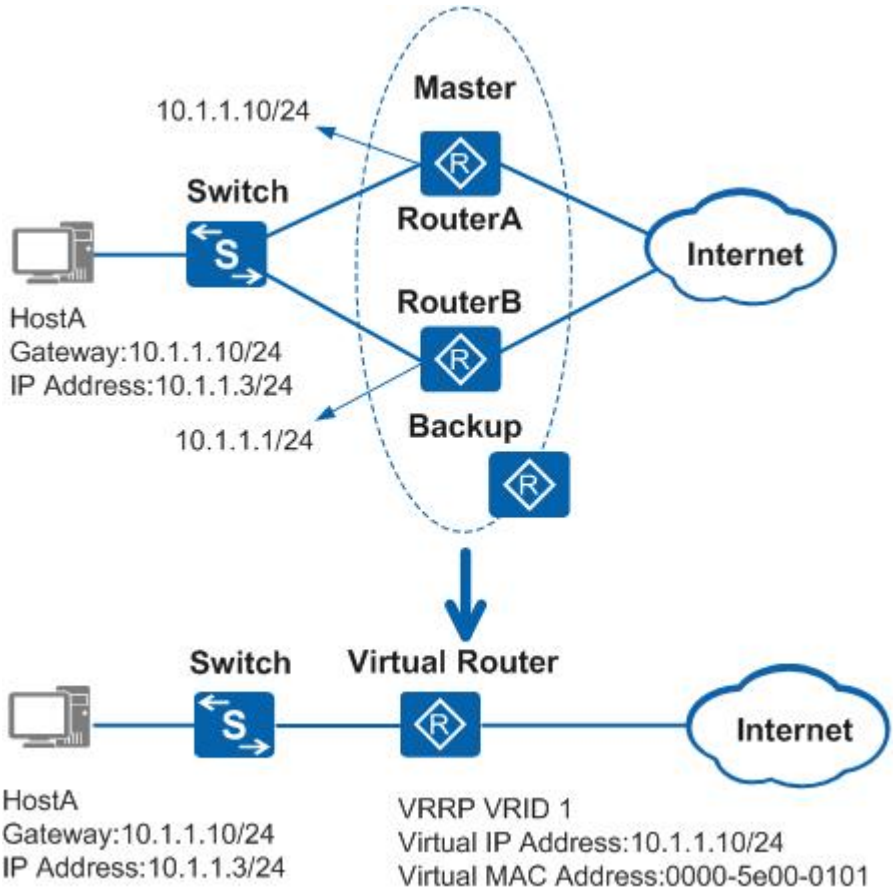
18. 配置 VRRP

18.1. 协议概述

虚拟路由冗余协议 VRRP（Virtual Router Redundancy Protocol）通过把几台路由设备联合组成一台虚拟的路由设备，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。

本设备仅支持 VRRPv2 功能。

组网拓扑



术语定义

- VRRP 路由器（VRRP Router）：运行 VRRP 协议的设备，它可能属于一个或多个虚拟路由器，如 RouterA 和 RouterB。

- 虚拟路由器（Virtual Router）：又称 VRRP 备份组，由一个 Master 设备和多个 Backup 设备组成，被当作一个共享局域网内主机的缺省网关。如 RouterA 和 RouterB 共同组成了一个虚拟路由器。
- Master 路由器（Virtual Router Master）：承担转发报文任务的 VRRP 设备，如 RouterA。
- Backup 路由器（Virtual Router Backup）：一组没有承担转发任务的 VRRP 设备，当 Master 设备出现故障时，它们将通过竞选成为新的 Master 设备，如 RouterB。
- VRID：虚拟路由器的标识。如 RouterA 和 RouterB 组成的虚拟路由器的 VRID 为 1。
- 虚拟 IP 地址(Virtual IP Address)：虚拟路由器的 IP 地址，一个虚拟路由器可以有一个或多个 IP 地址，由用户配置。如 RouterA 和 RouterB 组成的虚拟路由器的虚拟 IP 地址为 10.1.1.10/24。
- IP 地址拥有者（IP Address Owner）：如果一个 VRRP 设备将虚拟路由器 IP 地址作为真实的接口地址，则该设备被称为 IP 地址拥有者。如果 IP 地址拥有者是可用的，通常它将成为 Master。如 RouterA，其接口的 IP 地址与虚拟路由器的 IP 地址相同，均为 10.1.1.10/24，因此它是这个 VRRP 备份组的 IP 地址拥有者。
- 虚拟 MAC 地址（Virtual MAC Address）：虚拟路由器根据虚拟路由器 ID 生成的 MAC 地址。一个虚拟路由器拥有一个虚拟 MAC 地址，格式为：00-00-5E-00-01-{VRID}(VRRP for IPv4)；00-00-5E-00-02-{VRID}(VRRP for IPv6)。当虚拟路由器回应 ARP 请求时，使用虚拟 MAC 地址，而不是接口的真实 MAC 地址。如 RouterA 和 RouterB 组成的虚拟路由器的 VRID 为 1，因此这个 VRRP 备份组的 MAC 地址为 00-00-5E-00-01-01。

18.2. 配置命令

- 创建/删除 VRRP 组

命令	(Routing)(config)# **ip vrrp** (Routing)(config)#**no ip vrrp**
描述	全局配置模式。 创建/删除一个 VRRP 组。

- 关联 VRRP 接口

命令	(Routing)(inteface0/1)#ip vrrp 1 (Routing)(inteface0/1)#ip vrrp 1 accept-mod

描述	VRRP 组配置模式。 配置/删除 VRRP 组关联的三层口。支持 SVI 口，比如 vlan1；不支持二层口，比如未配置为三层口的 gigabitEthernet0/1。

- 配置/删除 VRRP 虚拟地址

命令	(Routing)(Interface 0/1)#ip vrrp 1 ip A.B.C.D
描述	VRRP 组配置模式。 虚拟地址为虚拟路由器网关地址。 配置为 master 角色必须保证虚拟 IP 为组关联的接口 IP。

- 配置/删除 VRRP 优先级

命令	(Routing)(Interface 0/1)#**ip vrrp 1 priority <1-254>** (Routing)(Interface 0/1)#no **ip vrrp 1 priority <1-254>**
描述	VRRP 组配置模式。可选配置。 优先级 0 被系统保留作为特殊用途；优先级值 255 保留给 IP 地址拥有者。 缺省情况下，backup 路由器优先级的取值是 100。数值越大，优先级越高。

- 配置/重置 VRRP 组通告间隔

命令	(Routing)(Interface 0/1)#**ip vrrp 1 timers advertise <1-255>** (Routing)(config-vrrp)#**no ip vrrp 1 timers advertise**

描述	VRRP 组配置模式。 可选配置，单位为秒，默认为 1。

- 配置/删除抢占模式

命令	(Routing)(config-vrrp)#ip vrrp 1 preempt (Routing)(config-vrrp)#no ip vrrp 1 preempt
描述	VRRP 组配置模式。 可选配置，默认开启抢占。

- 配置认证功能

命令	(Routing) (Interface 0/1)#ip vrrp 1 authentication simple
描述	VRRP 组配置模式。 可选配置，默认免认证模式。 VRRPv1 支持免认证模式、简单密钥认证模式、md5 认证模式，但是并不能提升安全性；VRRPv2 兼容 v1 的认证模式；VRRPv3 取消了安全性字段。 设备不建议配置认证功能。

18.3. 显示命令

- 显示 vrrp 组信息

```
#show vrrp
 ---------------- VRRP 1 ----------------
```

```
ID:                     1
State:                  Master (Enabled)
Virtual IP:             2.2.1.1/24 (Not IP owner)
Last Master:            2.2.1.3 (63510s ago)
Interface:              vlan100
Priority:               100 (conf.-1)
Advertisement interval: 1 sec
Preempt mode:           TRUE
Authentication:         none
---------------- VRRP 2 ----------------
ID:                     2
State:                  Backup (Enabled)
Virtual IP:             2.2.2.1/24 (Not IP owner)
Last Master:            2.2.2.3 (0s ago)
Interface:              vlan200
Priority:               90 (conf.90)
Advertisement interval: 1 sec
Preempt mode:           TRUE
Authentication:         none
```

19. 配置 ACL

19.1. ACL 概述

ACL（Access Control List，访问控制列表）通过配置对报文的匹配规则和处理操作来实现包过滤的功能。可以有效防止非法用户对网络的访问，同时也可以控制流量，节约网络资源。

由 ACL 定义的数据包匹配规则，也可以被其它需要对流量进行区分的功能引用，如 QoS 中流分类规则的定义。

ACL 通过一系列匹配条件对数据包进行分类，这些条件可以是数据包的 SMAC、DMAC、SIP、DIP 等。根据匹配条件，可将 ACL 分为以下几种：

基于 IP 的标准 ACL：只根据数据包的源 IP 地址制定规则。

基于 IP 的扩展 ACL：根据数据包的源 IP 地址、目的 IP 地址、ETYPE、protocol 制订规则。

基于 MAC 的 ACL：根据数据包的源 MAC 地址、目的 MAC 地址制订规则。

可命名 ACL：制订规则同基于 IP 的标准 ACL、扩展 ACL。

19.2. 配置命令

- 配置基于 IP 的标准 ACL

命令	(Routing)(config)#**ip-access-list** {<1-99>} {**permit** | **deny**} {every | **any**} (Routing)(config)#**no ip-access-list** {<1-99>} {**permit** | **deny**} {every | **any**}
描述	创建/删除基于 IP 的标准 ACL

- 配置基于 IP 的扩展 ACL

命令	(Routing)(config)# **ip-access-list** {<100-199> |} {**permit** **| deny**} {TYPE} {SIPADDR SIPADDRMASK | **any**} {DIPADDR DIPADDRMASK | **any**} (Routing)(config)#**no** **ip-access-list** {<100-199> } {**permit** **| deny**} TYPE {SIPADDR SIPADDRMASK | **any**} {DIPADDR DIPADDRMASK | **any**} (Routing)(config)# **no ip-access-list** {<100-199> }
描述	创建/删除基于 IP 的扩展 ACL TYPE 列表： <0-255>：指定 protocol 的 ID any：任意 protocol 报文 gre：GRE 报文 IGMP：IGMP 报文 IP：IPv4 报文 ipcomp：IPComp 报文 ospf：OSPF 报文 pim： PIM 报文 rsvp：RSVP 报文 tcp：TCP 报文 udp：UDP 报文

	vrrp：VRRP 报文

- 配置基于 MAC 的 ACL

命令	(Routing)(config)#mac access-list extended h (Routing)(config)#permit any any (Routing)(config)#**no** mac access-list extended h
描述	创建/删除基于 MAC 的 ACL

- 配置 ACL 应用在端口上

命令	(Routing)(config-if)#mac access-group h in 1 (Routing)(config-if)#**no** mac access-group h in 1
描述	配置/删除 ACL 应用在端口上

说明

✦ 当 ACL 已经应用在端口上时，若需要添加删除规则，需先从端口解应用；

19.3. 显示命令

- 显示 ACL

```
Routing) #show access-lists interface 0/1 in
```

```
ACL Type              ACL ID                Sequence Number
--------  ------------------------------  ---------------


(Routing) #
```

20. 配置 QOS

20.1. QOS 概述

QoS（Quality of Service，服务质量）指一个网络能够利用各种基础技术，为指定的网络通信提供更好的服务能力。

传统网络采用“尽力而为”的转发机制，当网络带宽充裕的时候，所有的数据流都得到了较好的处理，当网络发生拥塞的时候，所有的数据流都有可能被丢弃。为满足不同应用不同服务质量的要求，需要网络能根据用户的要求分配和调度资源，对不同的数据流提供不同的服务质量。

支持 QoS 功能的设备，能够提供传输品质服务，针对某种类别的数据流，可以为它赋予某个级别的传输优先级，来标识它的相对重要性，并使用设备所提供的各种优先级转发策略、拥塞避免等机制为这些数据流提供特殊的传输服务。

配置了 QoS 的网络环境，增加了网络性能的可预知性，并能够有效地分配网络带宽，更加合理地利用网络资源。

20.2. 配置命令

- 全局开启/关闭 QOS

命令	(Routing)(config)#classofservice dot1p-mapping *userpriority trafficclass* (Routing)(config)#no classofservice ip-dscp-mapping (Routing)(config)#no classofservice ip-dscp-mapping (Routing)(config)#classofservice trust {dot1p | ip-dscp | untrusted} (Routing)(config)#no classofservice trust

(Routing)(config)#cos-queue min-bandwidth *bw-0 bw-1 … bw-n*

(Routing)(config)#no cos-queue min-bandwidth

(Routing)(config)#cos-queue random-detect *queue-id-1* [*queue-id-2 …*

queue-id-n]

(Routing)(config)#no cos-queue random-detect *queue-id-1* [*queue-id-2 …*

queue-id-n]

(Routing)(config)#cos-queue strict *queue-id-1* [*queue-id-2 … queue-id-n*]

(Routing)(config)#no cos-queue strict *queue-id-1* [*queue-id-2 … queue-id-n*]

描述	全局开启、关闭 QOS 功能 默认关闭

命令	(Routing)(config-pmap-c)**#police cir** <32-1000000> **cbs** <4-31250> **exceed-action drop** (Routing)(config-pmap-c)**#no police**
描述	配置/删除策略 Cir 是限速水线，单位 kbps Cbs 是 burst 能力，单位 Kbyte

说明

✦ cir 数值是可确定的，比如限速 1M，那么 cir 数值为 1024，但是 cbs 的数值却取自经验数值。当 cbs 数值配大，流量尖峰更高，限速较稳定，但平均速率可能高于限速值；当 cbs 数值配小，流量尖峰较低，限速波动较大，平均速率可能小于限速值。建议 cbs 配置取 cir 的 4 倍值与 31250 的小值。

- 配置 policy-map 在接口上应用

命令	(Routing)(config-if)#**service-policy input** PNAME (Routing)(config-if)#**no service-policy input**
描述	配置/删除策略在接口上的应用 一个接口上只能应用一条 policy-map

- 配置端口入口限速

命令	(Routing)(config-if)#**rate-limit input** <64-1000000> <32-16384> (Routing)(config-if)#**no rate-limit input**
描述	配置/删除端口入口限速 第一个参数为 limit，单位 kbps 第二个参数为 burst，单位 Kbyte

- 配置端口出入口限速

命令	(Routing)(config-if)#**rate-limit output** <64-1000000> <32-16384> (Routing)(config-if)#**no service-policy output**
描述	配置/删除端口出口限速 第一个参数为 limit，单位 kbps 第二个参数为 burst，单位 Kbyte

说明

✦ limit 数值是可确定的，比如限速 1M，那么 limit 数值为 1024，但是 burst 的数值却取自经验数值。当 burst 数值配大，流量尖峰更高，限速较稳定，但平均速率可能高于限速值；当 burst 数值配小，流量尖峰较低，限速波动较大，平均速率可能小于限速值。建议 burst 配置取 limit 的 4 倍值与 16384 的小值。

20.3. 显示命令

- 显示 cos-map 配置信息

```
show interfaces cos-queue [unit/slot/port]
```

- 显示端口配置信息

```
show classofservice ip-precedence-mapping [unit/slot/port]

show classofservice trust [unit/slot/port]
```

- 显示 class-map 配置信息

```
show classofservice dot1p-mapping [unit/slot/port]
```

- 显示 policy-map 配置信息

```
show classofservice ip-dscp-mapping
```

- 显示端口限速配置信息

```
(Routing)#show rate-limit
-------------------------------------------------------
Interface     In limit  In burst  Out limit  Out burst
-------------------------------------------------------
```

GiE0/1	--	--	--	--
GiE0/2	--	--	--	--
GiE0/3	1024	4096	--	--
GiE0/4	--	--	--	--
GiE0/5	--	--	--	--
GiE0/6	--	--	--	--
GiE0/7	--	--	--	--
GiE0/8	--	--	--	--
GiE0/9	--	--	--	--
GiE0/10	--	--	1024	4096

21. 配置 DHCP SNOOPING

21.1. DHCP SNOOPING 概述

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议， 被广泛用来动态分配可重用的网络资源，是一种用户或者内部网络管理员对所有计算机作中央管理的手段。

DHCP Snooping 是 DHCP 安全技术，通过侦测管理 DHCP 交互报文，实现对非法 DHCP Server 的隔离功能。DHCP Snooping 把端口分为两种类型，TRUST 口和 UNTRUST 口，设备只转发 TRUST 口收到的 DHCP Offer 报文，而丢弃所有来自 UNTRUST 口 DHCP Offer 报文，从而实现对非法 DHCP Server 的屏蔽。

21.2. 配置命令

- 全局开启/关闭 DHCP Snooping

命令	(Routing)(config)#**ip dhcp snooping** (Routing)(config)#**no ip dhcp snooping**
描述	全局开启、关闭 DHCP Snooping 功能

- 配置信任口

命令	OLT(config-if)#**ip dhcp snooping trust** OLT(config-if)#**no ip dhcp snooping trust**
描述	设置端口为 TRUST/UNTRUST 口

21.3. 显示命令

- 显示 DHCP Snooping 配置信息

```
(Routing) #show ip dhcp snooping

DHCP snooping is Disabled
```

```
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:


 Interface    Trusted     Log Invalid Pkts
-----------  ----------   ----------------


(Routing) #
```

22. 配置 802.1X 认证

22.1. 协议概述

IEEE802 LAN/WAN 委员会为解决无线局域网网络安全问题，提出了 802.1X 协议。后来，802.1X 协议作为局域网端口的一个普通接入控制机制在以太网中被广泛应用，主要解决以太网内认证和安全方面的问题。

802.1X 协议是一种基于端口的网络接入控制协议（port based network access control protocol）。“基于端口的网络接入控制”是指，在局域网接入设备的端口这一级，对所接入的用户设备通过认证来控制对网络资源的访问。

22.1.1. 802.1X 的体系结构

802.1X 系统为典型的 Client/Server 结构，如图 1-1 所示，包括三个实体：客户端（Client）、设备端（Device）和认证服务器（Server）。

图 1-1 802.1X 认证系统的体系结构

- 客户端是位于局域网段一端的一个实体，由该链路另一端的设备端对其进行认证。客户端一般为一个用户终端设备，用户可以通过启动客户端软件发起 802.1X 认证。客户端必须支持 EAPOL（Extensible Authentication Protocol over LAN，局域网上的可扩展认证协议）。
- 设备端是位于局域网段一端的另一个实体，对所连接的客户端进行认证。设备端通常为支持 802.1X 协议的网络设备，它为客户端提供接入局域网的端口，该端口可以是物理端口，也可以是逻辑端口。
- 认证服务器是为设备端提供认证服务的实体。认证服务器用于实现对用户进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。

22.1.2. 802.1X 的认证方式

802.1X 认证系统使用 EAP（Extensible Authentication Protocol，可扩展认证协议），来实现客户端、设备端和认证服务器之间认证信息的交换。

- 在客户端与设备端之间，EAP 协议报文使用 EAPOL 封装格式，直接承载于 LAN 环境中。

- 在设备端与 RADIUS 服务器之间，可以使用两种方式来交换信息。一种是 EAP 协议报文由设备端进行中继，使用 EAPOR（EAP over RADIUS）封装格式承载于 RADIUS 协议中；另一种是 EAP 协议报文由设备端进行终结，采用包含 PAP（Password Authentication Protocol，密码验证协议）或 CHAP（Challenge Handshake Authentication Protocal，质询握手验证协议）属性的报文与 RADIUS 服务器进行认证交互。

22.1.3. 802.1X 的基本概念

22.1.3.1. 受控/非受控端口

设备端为客户端提供接入局域网的端口，这个端口被划分为两个逻辑端口：受控端口和非受控端口。任何到达该端口的帧，在受控端口与非受控端口上均可见。

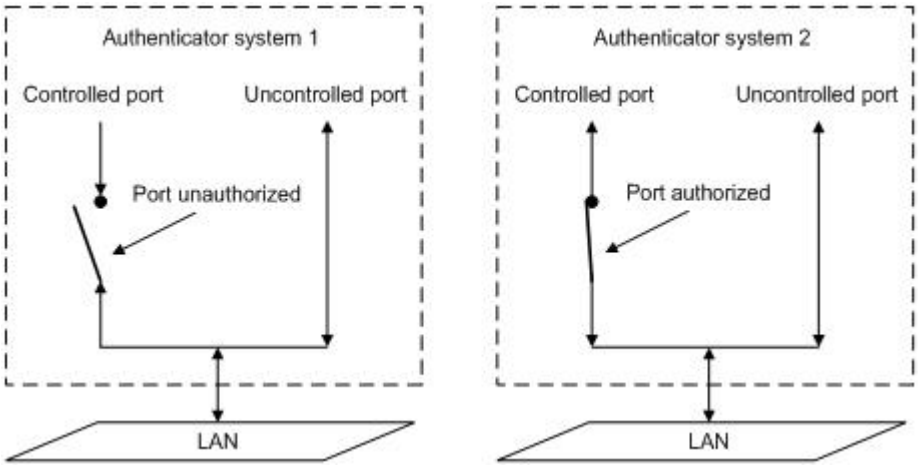
- 非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，保证客户端始终能够发出或接收认证报文。
- 受控端口在授权状态下处于双向连通状态，用于传递业务报文；在非授权状态下禁止从客户端接收任何报文。

22.1.3.2. 授权/非授权状态

设备端利用认证服务器对需要接入局域网的客户端执行认证，并根据认证结果（Accept 或 Reject）对受控端口的授权/非授权状态进行相应地控制。

图 1-2 显示了受控端口上不同的授权状态对通过该端口报文的影响。图中对比了两个 802.1X 认证系统的端口状态。系统 1 的受控端口处于非授权状态（相当于端口开关打开），系统 2 的受控端口处于授权状态（相当于端口开关关闭）。

图 1-2 受控端口上授权状态的影响



用户可以通过在端口下配置的接入控制的模式来控制端口的授权状态。端口支持以下三种接入控制模式：

- 强制授权模式（**authorized-force**）：表示端口始终处于授权状态，允许用户不经认证授权即可访问网络资源。
- 强制非授权模式（**unauthorized-force**）：表示端口始终处于非授权状态，不允许用户进行认证。设备端不对通过该端口接入的客户端提供认证服务。
- 自动识别模式（**auto**）：表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果认证通过，则端口切换到授权状态，允许用户访问网络资源。这也是最常见的情况。

22.1.3.3. 受控方向

在非授权状态下，受控端口可以被设置成单向受控和双向受控。

- 实行双向受控时，禁止帧的发送和接收；
- 实行单向受控时，禁止从客户端接收帧，但允许向客户端发送帧。

22.1.4. **802.1X 的认证过程**

802.1X 系统支持 EAP 中继方式和 EAP 终结方式与远端 RADIUS 服务器交互完成认证。以下关于两种认证方式的过程描述，都以客户端主动发起认证为例。

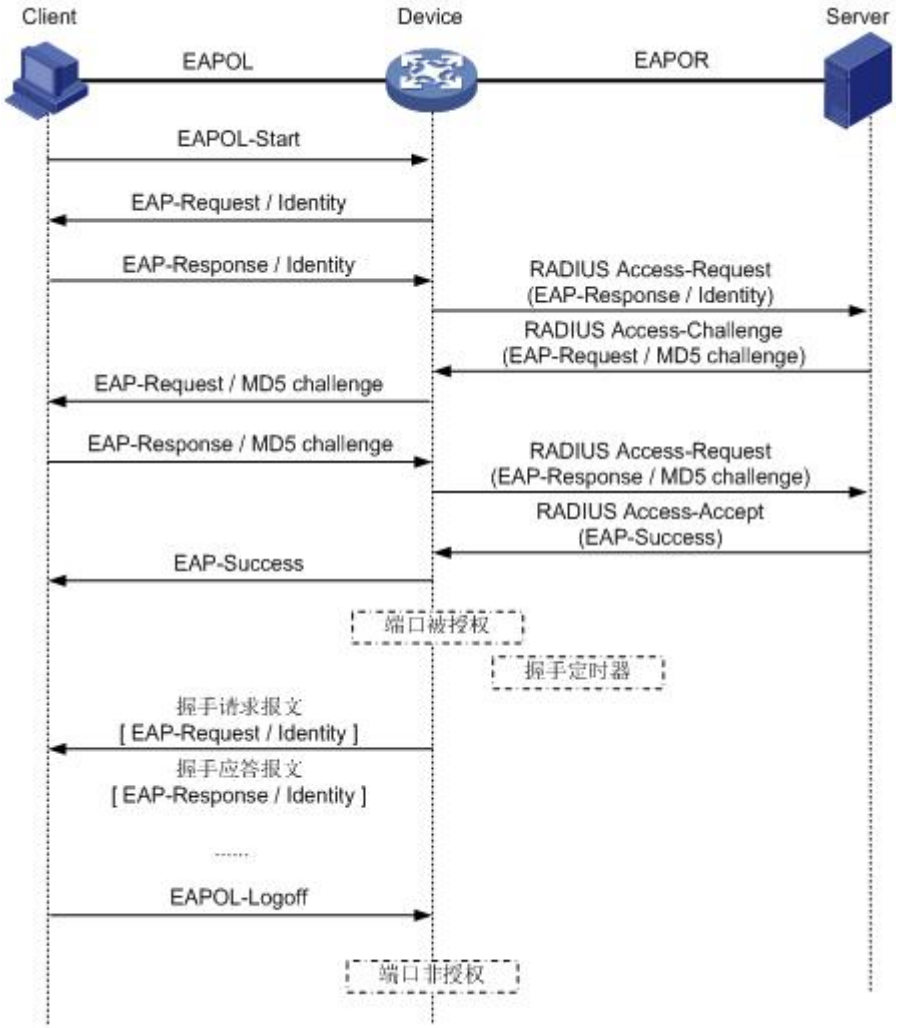
22.1.4.1. EAP 中继方式

这种方式是 IEEE 802.1X 标准规定的，将 EAP（可扩展认证协议）承载在其它高层协议中，如 EAP over RADIUS，以便扩展认证协议报文穿越复杂的网络到达认证服务器。一般来说，EAP 中继方式需要 RADIUS

服务器支持 EAP 属性：EAP-Message 和 Message-Authenticator，分别用来封装 EAP 报文及对携带 EAP-Message 的 RADIUS 报文进行保护。

下面以 EAP-MD5 方式为例介绍基本业务流程，如图 1-3 所示。

图 1-3 IEEE 802.1X 认证系统的 EAP 中继方式业务流程



认证过程如下：

1) 当用户有访问网络需求时打开 802.1X 客户端程序，输入已经申请、登记过的用户名和密码，发起连接请求（EAPOL-Start 报文）。此时，客户端程序将发出请求认证的报文给设备端，开始启动一次认证过程。
2) 设备端收到请求认证的数据帧后，将发出一个请求帧（EAP-Request/Identity 报文）要求用户的客户端程序发送输入的用户名。

3) 客户端程序响应设备端发出的请求，将用户名信息通过数据帧（EAP-Response/Identity 报文）发送给设备端。设备端将客户端发送的数据帧经过封包处理后（RADIUS Access-Request 报文）送给认证服务器进行处理。

4) RADIUS 服务器收到设备端转发的用户名信息后，将该信息与数据库中的用户名表对比，找到该用户名对应的密码信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过 RADIUS Access-Challenge 报文发送给设备端，由设备端转发给客户端程序。

5) 客户端程序收到由设备端传来的加密字（EAP-Request/MD5 Challenge 报文）后，用该加密字对密码部分进行加密处理（此种加密算法通常是不可逆的），生成 EAP-Response/MD5 Challenge 报文，并通过设备端传给认证服务器。

6) RADIUS 服务器将收到的已加密的密码信息（RADIUS Access-Request 报文）和本地经过加密运算后的密码信息进行对比，如果相同，则认为该用户为合法用户，反馈认证通过的消息（RADIUS Access-Accept 报文和 EAP-Success 报文）。

7) 设备收到认证通过消息后将端口改为授权状态，允许用户通过端口访问网络。在此期间，设备端会通过向客户端定期发送握手报文的方法，对用户的在线情况进行监测。缺省情况下，两次握手请求报文都得不到客户端应答，设备端就会让用户下线，防止用户因为异常原因下线而设备无法感知。

8) 客户端也可以发送 EAPOL-Logoff 报文给设备端，主动要求下线。设备端把端口状态从授权状态改变成未授权状态，并向客户端发送 EAP-Failure 报文。

22.2. 配置命令

- 全局开启/关闭 802.1X 认证

命令	(Routing)(config)# **dot1x system-auth-control** (Routing)(config)#**no dot1x system-auth-control**
描述	全局开启、关闭 802.1X 功能。

- 端口开启/关闭 802.1X 认证

命令	(Routing)(config-if)# **dot1x port-control force-unauthorized** (Routing)(config-if)#**no dot1x port-control force-unauthorized**

	(Routing)(config-if)#**dot1x port-control force-authorized** (Routing)(config-if)#**no dot1x port-control force-authorized** (Routing)(config-if)#**dot1x port-control auto** (Routing)(config-if)#**no dot1x port-control auto**
描述	端口开启、关闭 802.1X 功能。

- 配置 RADIUS 服务器

命令	(Routing)(config)# **radius-server host** A.B.C.D **auth-port** <0-65535> **acct-port** <0-65535> **key** WORD (Routing)(config)# aaa authentication dot1x default radius (Routing)(config)# radius server host auth "192.168.10.1" name "rad" (Routing)(config)# radius server key auth "192.168.10.1" encrypted e9dc904557361f19ac7716c3bd5429f1e2d061dea16e5d46c3cf45a54d523a470c792e7a504198810a118cb67a633236be8ccd8fa8191f762791f53dc3ceeb45 (Routing)(config)# radius server primary "192.168.10.1" (Routing)(config)#**no radius-server** primary A.B.C.D
描述	配置认证服务器信息。

	默认认证端口为 1812，记账端口为 1813。 请确保 RADIUS 服务器和设备管理地址互通。

22.3. 显示命令

- 显示 802.1X 端口认证信息

```
(Routing) #show dot1x

Administrative Mode.............. Disabled
VLAN Assignment Mode............. Disabled
Dynamic VLAN Creation Mode........ Disabled
Monitor Mode..................... Disabled
EAPOL Flood Mode................. Disabled
```

23. 配置 PORT SECURITY

23.1. PORT SECURITY 功能概述

Port Security 功能通过对端口合法 MAC 地址个数限制，达到限制非法用户对该端口访问的目的，对于非合法 MAC 的报文，将直接丢弃。

合法 MAC 可通过静态或动态的方式生成。静态合法 MAC 通过用户命令行配置生成；动态合法 MAC 则通过 MAC 地址学习功能动态生成。

当端口上安全地址个数已经达到最大安全地址个数配置值后，新 MAC 访问端口将认定为非法 MAC，产生违例事件，用户可配置违例事件产生时的应对操作，分别为 restrict 或 shutdown 端口。

Restrict：禁止非法 MAC 数据通过，并产生告警 log 提示信息。非法 MAC 将在 MAC 地址老化时间内禁止访问端口。通过 shutdown、no shutdown 端口可恢复。

Shutdown：强制端口 down 掉，并可配置端口恢复时间，时间到了端口自动恢复；也可通过 shutdown，no shutdown 命令恢复。

若希望将动态安全用户转换为静态安全用户，可开启端口上 sticky 功能。端口开启 sticky 功能，端口上学习到的动态用户将以静态用户的方式存在，若保存配置，设备重启后依然存在。

限制说明

- 仅支持 L2 端口配置端口安全，如普通物理口，AP 口。
- 仅支持在 access 模式下配置端口安全功能。
- 不支持 AP 成员口配置端口安全功能。
- 不支持 SPAN 的目的端口配置端口安全功能。
- 不支持在已配置静态 MAC 地址端口欹之端口安全功能。

23.2. 配置命令

- 全局模式开启端口安全

命令	(Routing)(config)#**port-security** (Routing)(config)#**no port-security**
描述	使能/关闭接口上端口安全功能

-
- 使能端口安全功能

命令	(Routing)(config-if)#**port-security** (Routing)(config-if)#**no port-security**
描述	使能/关闭接口上端口安全功能

- 配置端口最大安全地址个数

命令	(Routing)(config-if)#**port-security max-dynamic** VALUE (Routing)(config-if)#**no port-security max-dynamic**
描述	默认最大安全地址个数为 1 范围<1 1024>

- 配置静态安全地址

命令	(Routing)(config-if)#**port-security max-static** MAC_ADDR (Routing)(config-if)#**no port-security max-static** MAC_ADDR
描述	安全地址格式：XX：XX：XX：XX：XX：XX

	安全地址不能是广播或组播地址

23.3. 显示命令

在特权模式下，可以查看端口安全配置信息、安全地址信息等。

- 显示所有端口端口安全概要信息

```
(Routing) #show port-security all

          Admin    Dynamic     Static    Violation  Violation  Sticky
 Intf     Mode      Limit      Limit     Trap Mode  Shutdown   Mode
-------- -------- ----------  ---------- ---------- ---------- --------
0/1      Disabled 600         20         Disabled   Disabled   Disabled
0/2      Disabled 600         20         Disabled   Disabled   Disabled
0/3      Enabled  600         20         Disabled   Disabled   Disabled
0/4      Disabled 600         20         Disabled   Disabled   Disabled
0/5      Disabled 600         20         Disabled   Disabled   Disabled
0/6      Disabled 600         20         Disabled   Disabled   Disabled
0/7      Disabled 600         20         Disabled   Disabled   Disabled
0/8      Disabled 600         20         Disabled   Disabled   Disabled
0/9      Disabled 600         20         Disabled   Disabled   Disabled
0/10     Disabled 600         20         Disabled   Disabled   Disabled
0/11     Disabled 600         20         Disabled   Disabled   Disabled
0/12     Disabled 600         20         Disabled   Disabled   Disabled
1/1      Disabled 600         20         Disabled   Disabled   Disabled
1/2      Disabled 600         20         Disabled   Disabled   Disabled
1/3      Disabled 600         20         Disabled   Disabled   Disabled
1/4      Disabled 600         20         Disabled   Disabled   Disabled
1/5      Disabled 600         20         Disabled   Disabled   Disabled
1/6      Disabled 600         20         Disabled   Disabled   Disabled
1/7      Disabled 600         20         Disabled   Disabled   Disabled
1/8      Disabled 600         20         Disabled   Disabled   Disabled
```

24. 配置 IP SOURCE GUARD

24.1. IP SOURCE GUARD 功能概述

Ip Source Guard 绑定功能，允许符合 IP+MAC 绑定的 IP 报文通过端口，不符合的报文则直接丢弃，从而达到防止 IP/MAC 欺骗攻击的目的。

Ip Source Guard 的绑定条目，主要有两个来源：用户静态配置与 ip dhcp snooping 环境中动态获取。

用户静态配置：主要应对局域网络中 IP 地址静态配置的主机用户。

Ip dhcp snooping 动态获取：主要应对局域网络中通过 dhcp 动态获取到 IP 地址的主机用户。

IP/MAC 欺骗攻击：非法 MAC 用户，发送带合法源 IP 的 IP 报文，实现访问身份的合法化。

限制说明

- 当前软件版本仅支持绑定条目用户静态配置方式。
- 不支持 AP 成员口配置 Ip Source Guard 功能。

24.2. 配置命令

- 使能 Ip Source Guard 功能

命令	(Routing)(config-if)#**ip verify source** (Routing)(config-if)#**no ip verify source**
描述	使能/关闭接口上 Ip Source Guard 功能

- 配置绑定表项

命令	(Routing)(config)# **ip verify binding** xx:xx:xx:xx:xx:xx vlan 1 A.B.C.D **interface 0/1** (Routing)(config)#**no ip verify binding** xx:xx:xx:xx:xx:xx vlan 1 A.B.C.D **interface 0/1**
描述	安全地址格式：xx:xx:xx:xx:xx:xx IP 地址格式：A.B.C.D 单端口最多配置 128 条表项

24.3. 显示命令

在特权模式下，可以查看 ip verify source 生效规则与 ip source binding 绑定项。

- 查看 ip verify source 生效规则

```
(Routing) #show ip source binding dhcp-snooping

MAC Address           IP Address        Type            VLAN  Interface
-----------------  ---------------  -------------  -----  -------------
```

- 显示 ip source binding 表项

```
(Routing) #show ip source binding
interface   vlan   IP-address       Mac-address      Lease      Type
-------------------------------------------------------------------------------------------
GiE0/1       1       1.1.1.1          0001.0001.0001 infinite     static
GiE0/2       1       1.1.2.1          0001.0002.0001 infinite     static
```

25. 配置 SNMP 网管

25.1. 概述

SNMP 是 Simple Network Management Protocol（简单网络管理协议）的缩写，在 1988 年 8 月就成为一个网络管理标准 RFC1157。到目前，因众多厂家对该协议的支持，SNMP 已成为事实上的网管标准，适合于在多厂家系统的互连环境中使用。

利用 SNMP 协议，网络管理员可以对网络上的节点进行信息查询、网络配置、故障定位、容量规划，网络监控和管理是 SNMP 的基本功能。

目前 SNMP 存在以下版本：

SNMPv1 ：简单网络管理协议的第一个正式版本，在 RFC1157 中定义。

SNMPv2C：基于共同体（Community-Based）的 SNMPv2 管理架构，在 RFC1901 中定义。

SNMPv3 ：通过对数据进行鉴别和加密，提供了以下的安全特性：

1)确保数据在传输过程中不被篡改。
2)确保数据从合法的数据源发出。
3)加密报文，确保数据的机密性。

25.2. 配置命令

- 配置通信团体字

命令	(Routing)(config)#**snmp-server enable 全局开启** (Routing)(config)#**snmp-server community** COMMUNITY **{ro | rw}** (Routing)(config)#**no snmp-server community** COMMUNITY
描述	配置/删除 SNMP 通信团体字；

	ro: 只读标识，将团体字配置为只有读权限的团体字；默认配置为同时具备读写权限的团体字； 支持同时配置多个团体字

- 配置 SNMPv3 视图

命令	(Routing)(config)# **snmp-server view** NAME OID **{include | exclude}** (Routing)(config)# **no snmp-server view** NAME
描述	配置/删除 SNMPv3 视图； 支持同时配置多个视图，支持单个视图配置多个规则； 系统默认存在 all 和 none 视图，不可修改

- 配置 SNMP 组

命令	(Routing)(config)# **snmp-server group** NAME **{v3 | } {noAuthNoPriv | authNoPriv | authPriv} read** RVIEW **write** WVIEW (Routing)(config)# **snmp-server group** NAME **{v1 | v2c} read** RVIEW **write** WVIEW (Routing)(config)# **no snmp-server group** NAME
描述	配置/删除 SNMP 组； 支持同时配置多个组； SNMPv1 SNMPv2c 在配置 community 时为了兼容旧的配置，会自动创建组信息，通常无需额外关注

- 配置 SNMPv3 用户

命令	(Routing)(config)# **snmp-server user** NAME GROUPNAME **auth {md5 | sha}** {AUTHPASS} **priv {aes | des}** PRIVPASS (Routing)(config)# **no snmp-server user** NAME
描述	配置/删除 SNMP 用户； 支持同时配置多个用户；

- 配置 SNMP Host 通告服务器

命令	(Routing)(config)# **snmp-server host** IPADDR **informs** community (Routing)(config)# **no snmp-server host** NAME
描述	配置/删除 SNMP 服务器； 支持同时配置多个服务器；

26. 配置 RMON

26.1. 概述

SNMP 是互联网络中使用最广泛的网管协议，通过嵌入到设备中的代理软件来实现对网络通信信息的收集和统计。管理软件通过轮询方式向代理的 MIB 发出查询信号得到这些信息，通过得到的信息实现对网络的管理。虽然 MIB 计数器把统计数据的总和记录下来了，但它无法对日常的通信情况进行历史分析。为了能全面的查看一天中的流量和流量的变化情况，网管软件需要不断的轮询，才能通过得到的信息分析出网络的状况。

采用 SNMP 进行轮询有两个明显的缺点：

- 占用了大量的网络资源，在大型的网络中，通过轮询的方式会产生大量的网络通信报文，这样将会导致网络的拥塞甚至于会引起网络的阻塞，故 SNMP 不适合管理大型的网络，不适合回收大量的数据，如路由表信息。
- 加重了管理者的负担，在 SNMP 轮询中收集数据的任务是由网络管理者通过网管软件完成的，如果网络管理者监控了 3 个以上的网段，就有可能出现由于负担过重，网络管理者无法完成任务的情况。

为了提高管理信息的可用性、减少管理站的负担、满足网络管理员监控多个网段性能的需求，IETF 开发了 RMON 用以解决 SNMP 在日益扩大的分布式互联中的局限性，主要实现对一个网段乃至整个网络的数据流量的监视功能。以下是 RMON 的特点：

- SNMP 是 RMON 实现的基础，RMON 是 SNMP 功能的增强。

RMON 基于 SNMP 体系结构实现，与现存 SNMP 框架兼容，仍然是网管工作站 NMS 和运行在各网络设备上的代理 Agent 两部分组成。由于 RMON 没有使用另外一套机制，网管工作站 NMS 和 SNMP 共用，网络管理人员无需进行额外的学习，因此实现比较简单。

- RMON 使 SNMP 能更有效、更积极主动地监测远程网络设备，为监控网络的运行提供了一种高效的手段。

RMON 协议规定达到告警阈值时被管理设备能自动发送 Trap 信息，所以管理设备不需要多次通过轮询获取 MIB 变量的值进行比较，从而能够减少管理设备同被管理设备的通信流量，达到简便而有效地管理大型互连网络的目的。

RMON 允许有多个监控者，监控者可用如下两种方法收集数据：

- 通过专用的 RMON Probe（探测仪），NMS 直接从 RMON Probe 获取管理信息并控制网络资源，这种方式可以获取 RMON MIB 的全部信息。
- 将RMON Agent直接嵌入网络设备中，使它们成为带RMON Probe功能的网络设备。NMS使用SNMP与其交换数据信息，收集网络管理信息。这种方式受设备资源限制，一般无法获取 RMON MIB 的所有数据，基本上只收集四个组（告警、事件、历史和统计）的信息。

我司设备采用第二种方法，在设备上实现了 RMON Agent 功能。通过该功能，管理设备可以获得与被管网络设备接口相连的网段上的整体流量、错误统计和性能统计等信息，进而实现对网络的监控。

26.2. 原理

在配置 RMON 之前，需要了解 RMON 规范定义的统计、历史、告警和事件四个组的基本概念。

RMON 特性

RMON 主要实现了统计和告警功能，用于网络中管理设备对被管理设备的远程监控和管理。

RMON 的统计功能可以通过 RMON 统计组或者 RMON 历史组来实现，分为以太网统计功能和历史统计功能。

- 以太网统计功能（对应 RMON MIB 中的统计组）：系统统计被监控的每个网络的基本统计信息。系统将持续的统计某一网段的流量和各种类型包的分布，或者各种类型的错误帧数、碰撞次数等，统计对象包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。
- 历史统计功能（对应 RMON MIB 中的历史组）：系统定期采样收集网络状态统计信息并存储，以便后续的处理。系统将按周期定时对各种流量信息进行统计，统计数据包括带宽利用率、错误包数和总包数等。

RMON 告警功能包含事件定义功能和设置告警阈值功能，由这两个子功能的组合使用来实现了 RMON 告警功能。

- 事件定义功能 (对应 RMON MIB 中的事件组)：事件组控制从设备来的事件和提示，提供关于 RMON Agent 所产生的所有事件。当某事件发生时，可以记录日志或发送 Trap 到网管站。

- 设置告警阈值功能（对应 RMON MIB 中的告警组）：系统针对指定的告警变量（任意告警对象对应的 OID）进行监控。在用户预先定义指定告警的一组阈值和采样时间后，系统会按照定义的时间周期去获取指定告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件。RMON Agent 会将上述监控到的状态记录为日志或者把 Trap 发往网管站。

RMON 规范（RFC2819）中定义了多个 RMON 组，设备实现了公有 MIB 中支持的统计、历史、告警和事件四个组。下面对这几个组分别进行介绍。

- 统计组

统计组规定系统将持续地对以太网接口的各种流量信息进行统计，并将统计结果存储在以太网统计表（etherStatsTable）中以便管理设备随时查看。统计信息包括网络冲突数、CRC 校验错误报文数、过小（或超大）的数据报文数、广播、多播的报文数以及接收字节数、接收报文数等。

在指定接口下创建统计表项成功后，统计组就对当前接口的报文数进行统计，它统计的结果是一个连续的累加值。

- 历史组

历史组定期收集网络状态统计信息并存储，以便后续的处理。

历史组包含两个表：

  - 历史控制表（historyControlTable）：主要用来设置采样间隔时间等控制信息。
  - 以太网历史表（etherHistoryTable）：主要用来存储历史组定期收集网络状态统计信息，为网络管理员提供有关网段流量、错误包、广播包、利用率以及碰撞次数等其他统计信息的历史数据。
- 事件组

事件组定义的事件用于告警组配置项和扩展告警组配置项中，当监控对象达到告警条件时，就会触发事件。RMON 事件管理即是在事件表的指定行添加事件，并定义事件的处理方式：

  - log：只发送日志
  - trap：只向 NMS 发送 Trap 消息
  - log-trap：既发送日志同时也向 NMS 发送 Trap 消息
  - none：不做任何处理

- 告警组

告警组允许针对告警变量（可以是本地 MIB 的任意对象）预先定义一组阈值进行监视。用户定义了告警表项（alarmTable）后，系统会按照定义的时间周期去获取被监视的告警变量的值，当告警变量的值大于或等于上限阈值时，触发一次上限告警事件；当告警变量的值小于或等于下限阈值，触发一次下限告警事件，告警管理将按照事件的定义进行相应的处理。

26.3. 配置命令

- 配置历史组

命令	(Routing)(config)# **rmon hcalarm** <1-65535> **interface** IFNAME **buckets** <1-65535> **interval** <1-3600> **{owner** OWNERNAME **|}** (Routing)(config-if)#**no rmon history** <1-65535>
描述	配置/删除历史组； <1-65535>: 组索引 IFNAME：接口名称 <1-65535>：历史桶大小 <1-3600>：记录周期；单位为秒 OWNERNAME：所有者信息

- 配置事件组

命令	(Routing)(config)# **rmon event** <1-65535> **{description** DESCRIPTION **|} {log | trap** COMMUNITY **| log-trap** COMMUNITY **| none} {owner** OWNERNAME **|}** (Routing)(config-if)#**no rmon event** <1-65535>

描述	配置/删除事件组； <1-65535>：组索引 DESCRIPTION：事件描述 COMMUNITY：Trap 通信团体字 OWNERNAME：所有者信息

- 配置告警组

命令	(Routing)(config)# **rmon alarm** <1-65535> **object** STRING <1-65535> **{absolute | delta} rising-threshold** <1-2147483645> <1-65535> **falling-threshold** <1-2147483645> <1-65535> **{owner** OWNERNAME **|}** (Routing)(config-if)#**no rmon alarm** <1-65535>
描述	配置/删除告警组； <1-65535>：组索引 STRING：告警监控的 OID；比如 1.3.6.1.2.1.2.2.1.10.1 表示监控接口 1 收到的字节数 <1-65535>：监控周期；单位为秒 <1-2147483645>：上升阈值 <1-65535>：上升事件索引；对应事件组中的索引 <1-2147483645>：下降阈值 <1-65535>：下降事件索引；对应事件组中的索引

	OWNERNAME：所有者信息

26.4. 显示命令

- 显示事件组日志

```
(Routing) #show rmon ?

alarm                    Show RMON alarm entries.
alarms                   Display the alarm table.
collection               Displays the configured requested group of
statistics.
events                   Displays the RMON event table.
hcalarm                  Show RMON high capacity alarm entries
hcalarms                 Displays the high capacity alarm table.
history                  Displays the RMON history ethernet statistics.
log                      Display the RMON logging table.
statistics               Display RMON ethernet statistics.
```

27. 配置 DHCP 服务器

27.1. 协议概述

DHCP（Dynamic Host Configuration Protocol，动态主机设置协议）是一个局域网的网络协议，使用 UDP 协议工作，被广泛用来动态分配可重用的网络资源，如 IP 地址。

DHCP 是基于 Client/Server 工作模式，DHCP 客户端通过发送请求消息向 DHCP 服务器获取 IP 地址，等其他配置信息。当 DHCP 客户端与服务器不在同一个子网上，必须有 DHCP 中继代理（DHCP Relay）来转发 DHCP 请求和应答消息。

27.1.1. **协议标准**

RFC2132 DHCP Options and BOOTP Vendor Extensions. S. Alexander, R. Droms. March 1997. (Format: TXT, HTML) (Obsoletes RFC1533) (Updated by RFC3442, RFC3942, RFC4361, RFC4833, RFC5494) (Status: DRAFT STANDARD) (DOI: 10.17487/RFC2132)

27.2. 配置命令

27.2.1. **全局配置命令**

- 全局开启/关闭 DHCP 服务器

命令	(Routing)(config)# **service dhcp** (Routing)(config)#**no service dhcp**
描述	全局开启、关闭 DHCP 服务器。

- 配置全局参数

命令	(Routing)(config)# **ip dhcp pool** NAME (Routing)(config)# lease infinite (Routing)(config)#network A.B.C.D mask (Routing)(config)#dns-server A.B.C.D (Routing)(config)#default-router A.B.C.D (Routing)(config)#ip dhcp excluded-address A.B.C.D A.B.C.D
描述	全局参数配置。参数值冲突时，全局参数优先级低于范围更精确的子网和地址池的参数。 默认的租约时间：43200s/12h 可选配置。

27.3. 配显示命令

- 显示 DHCP 服务器状态信息

```
show ip dhcp server statistics
```

28. 故障诊断

28.1. PING/TRACEROUT

- 执行 ping 功能

命令	(Routing)#**ping {ip** IPADDR **| ipv6** IPV6ADDR**}**
描述	执行 ping 命令

- 执行 traceroute 功能

命令	(Routing)# **traceroute {ip** IPADDR **| ipv6** IPV6ADDR **}**
描述	执行 traceroute 命令