Hcip关键的技术：ospf、bgp（大环境才考虑）、路由策略和策略路由、RSTP、mstp、vrrp、bfd

路由表中判断最佳路由的依据

先判断路由协议优先级

协议相同，再用度量值判断

RIP协议度量值=跳数

Ospf协议度量值=链路总开销cost

ISIS协议度量值=链路总开销cost

DR作用：减少邻接数量，减少ospf报文数量

接口类型必须是：广播、非广播

Interface g0/0/0

Display dr-primity XXXX

Display fib-------转发信息库

是真正指导路由器转发数据的依据

Fib内容必须从IP路由器中得到，

fib记录保存在硬件芯片中，属于数据转发层面，

路由表保存在内存中，属于控制层面

# Ospf多区域

## 表面区别：

区域作用：控制路由学习的范围

## 区域分类

### 骨干区域

要求必须知道全网所有的路由（包括其他协议路由）

区域间的通讯必须经过骨干区域

### 非骨干区域

要求必须和骨干区域直连，才可以学习其他区域的路由

非骨干区域分为5种（利用非骨干区域特性自动减少路由表记录量）

#### 标准区域

路由记录内容=骨干区域路由表内容

特殊区域必须从标准区域转变

Ospf虚链路功能只能在标准区域使用

#### Stub区域，也叫末梢区域

路由记录内容=ospf所有区域的全部路由，非ospf路由默认用缺省替代

#### Totally stub，完全末梢区域

路由记录内容=当前区域所有路由，其他路由自动用缺省代替

建议：标准→末梢→完全末梢

#### Nssa，非纯区域

区域内不止ospf一种路由协议，还有其他路由协议

由stub末梢区域转换得到

只有区域内任何一台路由器执行路由协议，区域就转换为非纯区域

路由记录内容=ospf全部路由，直连的其他路由协议，其他的路由自动被缺省路由替代

#### Totally nssa，完全非纯区

由totally stub完全末梢区转换得到

路由记录内容=当前区域所有路由，直连的其他路由协议，其他路由自动用缺省代替

特殊区域转换命令（在区域视图执行）在区域视图执行

末梢和完全末梢，由abr路由器生成，通告给内部路由器

非纯、完全非纯，由abr和asbr路由器生成，通告给内部路由器

注意：

末梢和完全末梢，要求区域内路由器必须只运行ospf 1种协议

区域必须和骨干直连

非纯和完全非纯，要求区域内至少1台路由器运行2种路由协议

区域必须和骨干直连

## Ospf虚链路

### 作用：

1.把物理上没有直连在骨干区域的区域逻辑上连在一起

2.把分裂的骨干区域在逻辑层面合并在一起

### 要求：

* 中间只能跨越一个非骨干区域
* 中间跨越的非骨干区域类型，必须是标准区域
* 需要在2个ABR路由器上执行，其中一个路由器必须连接骨干区域，另一个必须连接远端区域
* 虚链路命令中，指定对端ABR路由器的routerID

配置命令：必须在中间跨越区域的区域视图内执行

Area 1----中间跨越区域

Vlink-peer XXXX ----XXXX对端routerID

## 特殊区域配置命令

### Stub末梢区域命令

Area 2

Stub

要求：本区域内的所有路由器都要执行，否则邻居关系断开

### Totally Stub完全末梢区域命令

Area 2

Stub no-summary

要求：只需要在ABR路由器执行即可，区域内路由器执行stub命令

### Nssa非纯末梢区域命令

Area 2

Nssa

要求：本区域内的所有路由器都要执行，否则邻居关系断开

### Totally nssa完全非纯末梢区域命令

Area 2

Nssa no-summary

要求：只需要在ABR路由器执行即可，区域内路由器执行nssa命令

减少骨干路由表记录量，需要通过手动配置路由汇总

有2种汇聚方式：

区域间汇总

把非骨干路由汇总后，发送给骨干路由器

必须在ABR路由器非骨干区域视图执行

执行命令：abr-summary 正向掩码

外部汇总

把非ospf的外部路由汇总后发送给ospf路由器

必须在ASBR路由器的ospf视图执行

执行命令：asbr-summary 正向掩码

## Ospf外部路由cost计算方式

有2种cost计算方式，也叫2种外部路由类型

### Type1、1类外部路由

总Cost=ospf外部开销+ospf内部开销

### Type2、2类外部路由

默认方式

总Cost=ospf外部开销

修改命令：

区域视图Import-route rip type类型几

## LSA

链路状态默认老化时间是3600s，过期后自动从LSDB数据库中清除，默认链路状态更新时间是1800s

### LSA处理步骤

* 检查LSA报文序号，与LSDB中的LSA序号是否相同不同则大者为最优
* 序号相同时检查LSA报文的校验和，与LSDB中的LSA校验和是否相同，不同则大者为最优
* 校验和相同时比较LSA报文的age时间，age差值小于15min为相同LSA，超过15min则age小者为最优

### Ospf的6种LSA类型（也叫链路状态通告）

所有的LSA的通告，都是LSU的细分

1. LSA1、路由器LSA ，任何路由器都会发出，通告内容：直连链路信息和开销

任何区域中都有，但是不能跨区域传送

LSA中的linkID、link type、link data，代表一条具体的链路

1. LSA2、网络LSA，只由DR路由器发出，通告内容：邻居routerID和DR自身routerID，任何区域都有，但不能跨区域发送（链路也不可跨）
2. LSA3、网络汇总LSA，只由ABR路由器发出 ，通告内容：某个区域全部的明细路由或汇总路由

必须跨区域传送

特殊LSA3:4种特殊区域内部用LSA3类通告产生缺省路由

1. LSA4、ASBR汇总LSA，只由ABR路由器发出，通过内容：ASBR路由器的routerID

向骨干、标准区域内路由器传送

1. LSA5、AS外部路由，只有ASBR路由器发出，通过内容：外部路由信息

只能在骨干、标准区域间路由器传送；可以跨区传送

1. LSA7、nssa-LSA，只有ASBR路由器发出，通过内容：外部路由信息

只能在非纯、完全非纯区域内路由器传送

注意：LSA7报文在经过ABR路由器传输到骨干区域，自动变为LSA5

骨干和标准中的LSA：LSA1\LSA2\LSA3\LSA4\LSA5

末梢stub区域中的LSA:LSA1\LSA2\LSA3（产生缺省路由和通过其他区域路由）

完全末梢区域的LSA:LSA1\LSA2\LSA3（产生缺省路由，不通过其他区域路由）

非纯nssa区域的LSA:LSA1\LSA2\LSA3\LSA7（产生缺省路由、外部路由）

完全非纯nssa区域的LSA:LSA1\LSA2\LSA3（只产生缺省路由）\LSA7（产生缺省路由、外部路由）

注意：LSA3类通告优先级>LSA7类通告优先级

区域内路由器优先使用LSA3通告的缺省路由

从LSDB中查看LSA通告内容

LSA1：display ospf lsdb router

LSA2：display ospf lsdb network

LSA3：display ospf lsdb summary

LSA4：display ospf lsdb asbr

LSA5：display ospf lsdb ase

LSA7：display ospf lsdb nssa

## ospf的静默接口

作用:直连网段正常宣告、但接口不能收发ospf报文

network宣告命令有2个作用:

a、向其他路由器通告路由

b、相应接口开启报文收发

主要用于连接终端接口

命令：区域视图 silent-interface 接口

## 报文认证方式

### 接口认证

接口视图 ospf authentication-mode md5 1 cipher 认证口令

### 区域认证

区域视图authentication-mode md5 1 cipher 认证口令

注意：2个邻居路由器只要认证模式和密码相同就可以建立邻居关系，不区分认证方式

先判断路由协议，在判断度量值

Rip的度量值叫跳数

Ospf的度量值叫开销

## Ospf防环机制

1. 非骨干与骨干区域直连
2. ABR路由器不会把某个非骨干区域的LSA3，经过骨干再次传回该区域

非骨干→骨干再到非骨干时不学习该报文

1. ABR不会把骨干区域收到的3类LSA经过非骨干再传回骨干

abr路由器把骨干路由经过非骨干区域，再传回给骨干另一台abr后，abr不会重复计算

注意：区域内默认利用SPF算法自动防环

# 路由策略和策略路由

路由策略：控制路由表中记录

策略路由：控制数据包的发送

## 路由控制步骤

### 识别特定路由

常用识别办法：ACL、IP前缀列表

ACL利用IP五元组进行识别

IP前缀列表只能用IP识别。识别IP不区分源或目的（识别多个连续子网有优势）

匹配原则：命中即停止，默认拒绝

### 使用控制工具限制路由学习或者发布

常用路由策略

路由控制策略

**Filter-policy，过滤策略**。可以对接收、发布、引入的路由进行过滤

只能过滤路由信息，无法过滤链路信息

入方向的Filter-policy控制当前路由器的路由表记录，

出方向的Filter-policy控制引入的外部路由能否向邻居通告

**Router-policy，路由策略。**

语法格式：Router-policy 规则链名字 permit/deny node 规则编号

If-match 匹配方式

Apply 修改内容

匹配原则：命中即停止，默认拒绝

注意：没有If-match，表示所有路由；没有Apply，表示不做任何修改。如果有多个If-match，数据必须同时符合所有If-match的要求；如果有多个Apply，执行多项修改

## 策略路由

策略路由优先级 > 路由表

### 策略路由实现手段

#### PBR，标准策略路由

分类

接口PBR

只对接收并转发的数据有效

用在入接口

本地PBR

只能是路由器发起的数据有效

用在系统视图下

#### MQC，扩展策略路由

不光可以策略路由，还可以实现其他功能，如Qos

配置分为4部

关键数据分类别

Traffic classfier aaa

if-match ACL2000

设置不同的控制内容

Traffic behavior aaa

Redirect IP-nexthop ......

利用策略把类别和控制内容捆绑

Traffic policy aaa

classfier aaa behavior aaa

在接口使用MQC策略

Interface g0/0/0

Traffic-policy aaa inbound

# IS-IS（Intermediate System to Intermediate System，中间系统到中间系统）

## 概念

IS-IS是ISO定义的OSI协议栈中的CLNS（ConnectionLess Network Service，无连接网络服务）的一部分。也属于链路状态协议。

## NET（Network Entity Title，网络实体名称）

### 组成

* 区域号
  + 主区域号

主区域号如果是49，表示私有区域

* + 子区域号

没有限制

* SystemID

相当于ospf中的routerID，实际需要routerID转换得到

转化原则：1.把routerid中的”.”去掉

2.4个数字一组，分成3组，得到systemID

全网的systemID不能重复

* 网络类型

表示在什么网络中使用ISIS协议

类型00，表示在IP网络

Net的长度：最长20byte，最短8byte

注意：每个路由器至多设置3个net实体名称

区域号必须区分开，但systemID必须统一

网络类型：广播网络、点到点网络

链路开销：默认为10，与接口带宽无关

## ISIS基础配置

1. 启动ISIS，并设置net实体名称
2. 宣告网段（相当于在接口启动ISIS协议）

[huawei] isis 1

[huawei-isis-1] is-level level-2-----------设置路由器类型

[huawei-isis-1] network-entity 49.0002.0040.0400.4004.00----指定systemID

[huawei-isis-1] quit

[huawei] interface gigabitethernet 0/0/0

[huawei-GigabitEthernet0/0/0] isis enable 1---------接口启动ISIS

## 区域

### 骨干

多区域联合，区域号可以不一样，骨干区域有全网路由

骨干区域依靠路由器类型决定

### 非骨干

单一区域，区域号无要求，只有本区域的路由，利用默认的缺省路由与其他区域通讯

非骨干区域依靠路由器类型决定

注意：ospf特殊区域缺省路由，由ABR路由器生成，向区域内通告

ISIS非骨干区域缺省路由，由区域内路由器独立生成，指向边界路由器

## ISIS路由器类型

* Leve-1路由器，也叫L-1路由器

L-1路由器只出现在非骨干区域

L-1路由器只能和同区域的L-1、L-1-2路由器建邻居（不能跨区域建邻居）

* Leve-2路由器，也叫L-2路由器

L-2路由器只出现在骨干区域

L-2路由器可以和L-2、L-1-2路由器建立邻居关系（可以跨区建邻居）

* Leve-1-2路由器，也叫L-1-2路由器

默认的路由器类型

骨干和非骨干区域都可以出现

在接口视图下 ISIS circuit-level level-2--------可以直接控制接口发送报文的类型

### 邻接关系

* L-1邻接关系

L-1路由器之间、L-1与L-1-2路由器之间

发送L1的ISIS报文，用L1的LSDB保存

* L-2邻接关系

L-2路由器之间、L-2与L-1-2路由器之间

发送L2的ISIS报文，用L2的LSDB保存

注意：2个L-1-2路由器之间，同时建立L1和L2邻接关系

## ISIS 报文类型

* IIH报文（相当于ospf的hello报文）

默认间隔10s，hold（死亡时间）=3\*IIH时间

邻接关系建立时只用到IIH报文，up状态表示邻接关系建立成功。Up状态之后才会发送其他报文，学习链路信息

华为设备在广播网络、点到点网路，都用三次握手来建立邻接关系

* LSP报文，链路状态报文（相当于ospf的LSU报文）
* CSNP报文（相当于ospf的DD报文）

描述LSDB摘要信息

广播网络，周期性（默认间隔10s）发送

点到点网络，只在建立邻接关系的时候发送

* PSNP报文（相当于ospf的LSR\LSAck报文）

点到点网络，PSNP具备确认功能

广播网络，不需要确认

注意：

* Ospf的hello报文目标地址：组播地址

224.0.0.5（所有都要接收）、224.0.0.6（只有DR和BDR可以接收）

* ISIS 的IIH报文的目标地址：Mac地址

L1的IIH报文，必须在非骨干区域传播，目标地址01:80:c2:00:00:14

L2的IIH报文，必须在骨干区域传播，目标地址01:80:c2:00:00:15

## DIS路由器

DIS作用：建立伪节点（虚拟路由器）

伪节点作用：记录邻居路由器systemID

DIS和DR的区别

* DR优先级为0不参与竞选，DIS优先级为0仍参与竞选
* 普通路由器与DR建立邻接关系，普通路由器之间建立DRother关系；普通路由器与DIS建立邻接关系，普通路由器之间也建立邻接关系
* 有DR和BDR之分；DIS路由器只有1台
* DR具有非抢占性；DIS路由器可以随时替换

### DIS路由器选举过程

先比较优先级，越大越优先、

优先级相同比较Mac，越大越优先

DIS发送hello报文的间隔：1/3\*IIH时间

确认DIS路由器做法：查看LSDB记录

例如：0000.0000.0002.02-00

0000.0000.0002-----路由器systemID

02----伪节点标志，非0代表伪节点信息

-00---ISIS分片信息

## 路由渗透

其实就是路由引入

作用：把骨干的网段通过给非骨干路由器，非骨干路由器选择最佳路径到达

命令：

[R2] **ip ip-prefix 1 permit 192.168.10.0 24**

[R2] **isis 1**

[R2-isis-1] **import-route isis level-2 into level-1 filter-policy ip-prefix 1**

## IS-IS认证

IS-IS认证是基于网络安全性的要求而实现的一种认证手段，通过在IS-IS报文中增加认证字段对报文进行认证。

### 根据报文的种类，认证可以分为以下三类：

* 接口认证：在接口视图下配置，对Level-1和Level-2的Hello报文进行认证。
* 区域认证：在IS-IS进程视图下配置，对Level-1的CSNP、PSNP和LSP报文进行认证。
* 路由域认证：在IS-IS进程视图下配置，对Level-2的CSNP、PSNP和LSP报文进行认证。

### 根据报文的认证方式，可以分为以下四类：

* 简单认证：将配置的密码直接加入报文中，这种加密方式安全性较其他两种方式低。
* MD5认证：通过将配置的密码进行MD5算法加密之后再加入报文中，提高密码的安全性。
* Keychian认证：通过配置随时间变化的密码链表来进一步提升网络的安全性。
* HMAC-SHA256认证：通过将配置的密码进行HMAC-SHA256算法加密之后再加入报文中，提高密码的安全性。

# BGP（Border Gateway Protocol，边界网关协议）

工作重心：控制最佳路由、新功能支持

BGP路由器必须且只属于1个区域

BGP，建立在TCP之上的路由协议。BGP在建立邻居前，需要先进行TCP三次握手

BGP端口号：TCP179

优点：

区域内路由器使用相同的最佳路由

路由器经过的区域数量，选择最佳路由

## AS（Autonomous System，自治系统）

### 概念

AS 是在单一技术管理体系下由唯一自治系统号标识的多个路由器的集合；是具有（同种或多种）路由协议策略的巨型网络或网络群组。

### ASN

自治系统的编号称为ASN：1-65535

公有AS （1-64511）

私有AS（64512-65535）

一般用在BGP区域联盟内部

Ospf协议路由器可以知道全网的路由

BPG不根据路由器数量、链路数量选路

## BGP邻居关系（对等体peer）

* IBGP邻居关系，也叫做IBGP对等体

邻居路由器在同一个区域

建立邻居时，通常使用回环口IP（物理口不稳定，回环口永远开启）需要通过IGP协议学习邻居回环口IP

建立邻居时，IBGP邻居无需直连

现阶段，IBGP邻居需要做全互联，因为受到BGP通告原则影响

区域边界路由器尽量修改外部路由下一跳为自身回环口IP

* EBGP邻居关系，也叫做EBGP对等体

邻居路由器不在同一个区域

通常，EBGP邻居要直连，使用物理口IP建立邻居关系

如果EBGP邻居没有物理直连，需要专门的配置，修改EBGP报文的TTL值

默认EBGP报文TTL=1

修改EBGP多跳命令------[BGP视图下] Peer IP地址 EBGP-max-top <1-255>默认255

## BGP通告原则

1. 只发布最优且有效路由
2. 从EBGP邻居学习到的路由，通告给所有邻居
3. 从IBGP邻居学习到的路由，不会通告给其他IBGP邻居。也叫IBGP水平分割原则
4. 从IBGP邻居学习到的路由，向EBGP邻居通告时，必须保证该路由在IGP、BGP协议中都通告（默认关闭）

路由表中没有该路由，如何判断路路由器的接收，通告

使用命令：display BGP routing-table peer 192.168.1.2 advertised-routes

----------------------查看该路由通过详情

display BGP routing-table peer 192.168.1.2 received-routes

----------------------查看该路由接收详情

## BGP配置思路

1. 接口IP、回环口IP
2. 配置IGP协议，学习回环口IP----可以使用IGP协议下的任何协议
3. 启动BGP，指定所属区域-----BGP 区域号
4. 指定邻居路由器、及邻居所在区域----peer 邻居回环地址 as-number 区域号

如果是IBGP邻居，指定邻居回环口IP，并配置利用本地回环口和邻居回环口建立邻居关系

-----peer 邻居回环地址 connect-interface 回环口地址

1. 用network宣告网段（非标准网段必须写掩码，标准网段可以不写）

实际中，BGP协议只需要宣告PC网段即可

注意：BGP向内部IBGP邻居通告EBGP路由时，保持下一跳地址不变

BGP的network，可以把IP路由表中的任何路由，宣告给邻居

## BGP报文类型

* Open报文，作用：协商、建立邻居关系
* Keepalive报文，作用：维持邻居关系

默认发送间隔：60s

默认邻居死亡时间：180s

* Update报文，作用：路由的学习更新
* Notification报文，作用：故障后中断邻居关系
* route-refresh报文，作用：路由属性改变后，可以立即更新

默认IBGP更新间隔15s，EBGP更新间隔30s

## BGP状态机

1. Idle 空闲状态，配置邻居命令后的状态
2. Connect 连接状态，发送TCP三次握手，建立TCP连接
3. Active 活动状态，TCP三次握手失败，重复执行三次握手
4. Opensent 发送open报文，TCP连接成功后，发送BGP的open报文
5. Openconfirm 确认状态报文，收到open报文，同意BGP参数，发送Keeplive报文
6. Established确定状态报文，BGP邻居成功，发送update更新报文

## BGP路由聚合

可以在任何路由器执行聚合操作

默认执行聚合后，明细路由不会丢弃，需要用参数强制丢弃明细路由

命令：

[BGP视图下]aggregate 聚合后网段 聚合后掩码 detail-suppressed

detail-suppressed参数用来抑制明细路由

## BGP属性

### 公认属性（所有路由器认可、识别的属性）

#### 公认必遵属性（Update更新报文必须要有该属性）

##### As-path区域路径属性

1. **概念：**

记录了从源到目的地所经过的所有自治系统编号（AS）

1. **作用：**

* 保存到达目标网段经过的所有区域号
* 区域间防环
* 优选区域数量少的路径作为最优路径
* 路由过滤（正则表达式）

1. **AS Path属性的类型**

* AS\_SEQUENCE：

这种类型的AS Path属性按顺序排列AS编号，最近的本地AS排在前面，其他AS按顺序依次排列。

* AS\_SET：

这种类型的AS Path属性不考虑顺序，只是简单罗列所有经过的AS编号

在执行抑制明细路由的聚合操作时，可能会产生环路

为了避免环路，聚合操作需要使用as-set参数，该参数会把明细路由的as路径添加到聚合路由的as-path中，并且聚合路由的as-path中，as号是乱序

1. **通过router-policy修改路径，可以以下参数**

* Additive

作用:在原有as-path基础上，新增域号

* Overwrite

作用:用手动配置区域号，替换原有as-path内容

* none overwrite

作用:清空as-path内容

AS号写入AS-path时，向EBGP通告路由再添加

1. **正则表达式过滤**

作用：模糊匹配特定内容

常用的语法：

. 匹配任意单个的字符，包括空格

^ 匹配行首必须是特定格式内容

$ 匹配行尾必须是特定格式内容

\_ 匹配单个符号，不能匹配字母、数字

| 匹配从给定的多个选择中必须匹配任意一项

- 匹配给定的连续范围

\ 转义符，表示后面的符号不具有特殊用途，只是单纯符号

\* 匹配前面的字符出现0次或多次

+ 匹配前面的字符至少出现1次

? 匹配前面的字符最多出现1次

[xxx] 匹配内部多个字符中任意一项

[^xxx] 匹配除了内部指定字符以外的其他任意字符

{数字} 匹配前面字符出现的次数

{数字1，数字2} 匹配前面字符出现的次数范围

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

命令

系统视图

ip as-path-filter ddd deny 正则表达式

ip as-path-filter ddd permit 正则表达式

BGP视图

peer 192.168.3.2 as-path-filter ddd import

##### origin（起源属性）

表示路由进入bgp的方式

* igp方式，表示通过network或聚合方式

在bgp路由表中用i表示（全称IGP）

* egp方式，表示通过egp协议，早已放弃

在bgp路由表中用e表示

* incomplete方式，表示通过import-route方式

在bgp路由表中用?表示

当去往同一个目的地存在多条不同Origin属性的路由时，在其他条件都相同的情况下，BGP将按如Origin的下顺序优选路由：IGP > EGP > Incomplete

##### next-hop（下一跳属性）

* 作用：指定到达目标网段的下一跳地址
* 默认原则：

1. 向ebgp邻居通告路由时，下一跳修改为自身ip
2. 向ibgp邻居通告外部路由时，下一跳保持不变
3. 如果路由器收到某条BGP路由，该路由的Next\_Hop属性值与EBGP对等体（更新对象）同属一个网段，那么该条路由的Next\_Hop地址将保持不变并传递给它的BGP对等体。

* 建议：bgp向内部ibgp邻居通告ebgp路由时，把下一跳改为自身回环口ip

#### 公认任意属性（Update更新报文可以有该属性）

##### local\_preference（本地优先级属性）

作用:向ibgp邻居通告，离开本AS的最佳路由

原则：

* 该属性由边界路由器添加，并只能向ibgp邻居通告，且默认不会改变
* 该属性值越大越优先，默认为100
* 配置时注意次优路径

##### atomic\_aggregate

作用：标明该聚合路由抑制明细路由

公认自由决定属性，它只相当于一种预警标记，而并不承载任何信息。

### 可选属性（部分路由器不认可的属性）

#### 可选过渡属性（路由器不认可属性，可转发给邻居）

##### Community属性

作用：具有相同属性的目的地编组。

属性值用MM：NN形式表示（MM一般为团体标记的区域号，NN自行设置）

路由添加团体标记后，可以控制邻居路由器是否可以通告给其他邻居

**团体标记路由发布控制方式：**

* Internet（默认方式）

带团体标记路由可以通告给所有邻居

* No\_advertise

带团体标记路由不通告给任何邻居。设备收到具有此属性的路由后，将不向任何BGP对等体发送该路由

* No\_export

带团体标记路由只能发给内部邻居（不是IBGP邻居）。设备收到具有此属性的路由后，将不向AS外发送该路由

* No\_Export\_Subconfed

在联盟的环境下，带团体标记路由只能发给IBGP邻居，联盟内其他AS的EBGP邻居也不通告。设备收到具有此属性的路由后，将不向AS外发送该路由，也不向AS内其他子AS发布此路由

**好处：**

Community是一种路由标记，用于简化路由策略的执行。

可以将某些路由分配一个特定的Community属性值，之后就可以基于Community值而不是网络前缀/掩码信息来匹配路由并执行相应的策略了。

###### community filter，团体过滤器

针对community团体标记过滤路由

* 基本团体过滤器

针对指定的团体标记过滤

* 高级团体过滤器

使用正则表达式匹配特殊的团体标记

###### 配置community filter

R2传递路由给EBGP对等体R3，在R2上部署路由策略，过滤掉携带101:1的Community属性值的路由

[R2] ip community-filter 1 permit 101:1

[R2] route-policy Community deny node 10

[R2-route-policy] if-match community-filter 1

[R2-route-policy] quit

[R2] route-policy Community permit node 20

[R2-route-policy] quit

[R2] bgp 102

[R2-bgp] peer 10.1.23.3 route-policy Community export

##### Aggregator（聚合属性）

作用：标明该路由是聚合路由，记录本地AS号及自己的Router-ID

可选传递属性

#### 可选非过渡属性（路由器不认可属性，不转发给邻居）

##### MED（多出口鉴别属性）

作用:控制进入本AS的首选路径

* 在2个相邻AS之间通告时修改，ibgp邻居间通告时保持不变
  + 该属性值越小越优先，默认为0。其属性值=cost

注意:默认情况下，MED只能对比来自同一个As的多条路径

如果需要对比来自不同AS的MED值，需要专门的命令：compare-different-as-med

通告时是否携带MED的原则:

* ibgp邻居间携带该属性，且保持不变
* 本地始发的路由，向ebgp邻居通告时携带属性
* 学习的路由，向ebgp邻居通告时不携带属性

##### cluster\_list（集群列表属性）

保存反射器cluster-id，即簇id。簇id默认是反射器的routerID

在一个AS内，每个路由反射器使用唯一的Cluster ID作为标识。当一条路由通过多个反射器时，这些反射器会将其Cluster ID依次添加到Cluster\_List属性中。

##### originator\_ID（起源ID）

定义：

记录该路由起始路由器的routerID

作用：

* 当一条路由第一次被路由反射器（RR）反射时，RR会将该路由的Originator\_ID属性设置为始发路由器的Router ID。
* 在BGP更新消息中，如果发现一条路由的Originator\_ID属性与本地的Router ID相同，则认为该条路由存在环路并丢弃该路由
* 为反射器客户端和非客户端防环，反射器学到的路由，在反弹时添加，内部通告时保持不变

任何update报文都携带属性吗？

只有新增路由的update报文携带属性

撤销路由不携带update报文的任何属性

### Preferred-Value协议首选值属性（华为专属）

该属性只对当前路由器有效，不会通告给任何邻居

作用:离开本路由器到最佳网段的最佳路由

该属性值越大越优先，默认为0

该属性在做路由优选时，使用优先级最高，可覆盖其他属性设置

## AS内IBGP数量过多，解决办法

### 路由反射器（优先考虑）

反射器建立要求：路由器之间必须是IBGP

#### 配置反射器后路由器角色

1. 反射器路由器

破坏IBGP水平分割原则，从IBGP学习的路由，会反弹给其他的IBGP邻居

As内路由器只需和反射器做IBGP邻居即可

1. 客户端

与路由反射器形成IBGP邻居关系的设备，在AS内部只需要与RR直连

1. 非客户端

既不是RR也不是客户机的IBGP设备，它们之间需要完全互连

**反射器配置**

内容：只在反射路由器配置，其他IBGP邻居不做任何操作

命令：peer 邻居IP reflect-client -----指定客户端型IBGP邻居

#### 路由反射规则

1. 从非客户端学习的IBGP路由，反弹给客户端和EBGP邻居
2. 从客户端学习到的IBGP路由，反弹给所有邻居
3. 从EBGP学的EBGP路由，反弹给所有邻居

建议：

As内部配置2个反射器，互为客户端

配置多个反射器的防环操作利用Originator\_ID、Cluster\_List属性来防环

### BGP联盟

#### 联盟对等体类型

1. 联盟外EBGP
2. 联盟内子区域间EBGP
3. 联盟内子区域内IBGP

联盟有联盟as号，联盟内有联盟子as号

使用联盟后，外部路由的as-path中，只有联盟的as号，没有联盟内的子as区域号

命令：

BGP 65000-----------------------------------------联盟内部子区域号

confederation id 200-------------------------联盟号，内部路由器都要配置

confederation peer-as 65001---------------联盟内部其他EBGP邻居

## BGP路由选优规则

1. 丢弃下一跳不可达路由

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

1. 优选Preferred-Value属性值最大的路由。
2. 优选Local\_Preference属性值最大的路由。

↑ 取值越大越优先

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

↓ 取值越小越优先

1. 本地始发的BGP路由优于从其他对等体学习到的路由，

本地始发的路由优先级：优选手动聚合> 自动聚合> network> import> 从对等体学到的。

1. 优选AS\_Path属性值最短的路由。
2. 优选Origin属性最优的路由。Origin属性值按优先级从高到低的排列是：IGP、EGP及Incomplete。
3. 优选MED属性值最小的路由。
4. 优选从EBGP对等体学来的路由（EBGP路由优先级高于IBGP路由）。
5. 优选到Next\_Hop的IGP度量值最小的路由。
6. 优选Cluster\_List最短的路由。
7. 优选Router ID（Orginator\_ID）最小的设备通告的路由。
8. 优选具有最小IP地址的对等体通告的路由。

## ORF（Outbound Route Filters，出口路由过滤器）

### 基本原理

如果设备希望只接受自己需要的路由，可以通过配置BGP基于前缀的ORF（Outbound Route Filters出口路由过滤器），ORF通过BGP Refresh报文告诉对等体路由过滤需求，对等体收到后，就只会给设备发送X.X.X.X的路由

注意：相邻路由器必须都要配置ORE，只是1端发出ORE需求而另一端接收ORE需求

### 优点

避免了本端设备接收大量无用路由，降低了链路带宽的占用率

### ORF与Router-policy的区别

ORF：我直接告诉对端需要的路由，对端只给我发送这条路由

Router-policy：对端把所有的路由都发给我，我自己过滤出我想要的路由

### 配置举例

告诉邻居

[R2] ip ip-prefix 1 permit 10.1.1.1 32

[R2] bgp 102

[R2-bgp] peer 10.1.12.1 as-number 101

[R2-bgp] peer 10.1.12.1 ip-prefix 1 import

[R2-bgp] peer 10.1.12.1 capability-advertise orf ip-prefix send

接收要求

[R1] bgp 101

[R1-bgp] peer 10.1.12.2 as-number 102

[R1-bgp] peer 10.1.12.2 capability-advertise orf ip-prefix receive

## 对等体组

作用:为多个同类型邻居路由器批量配置相同操作，邻居加入对等体组，会自动获得对等体组的全部配置

对等体组也分2种:

a、ibgp对等体组---------常用

b、ebgp对等体组

注意:针对邻居的单独配置，会覆盖对等体组的批量配置

配置步骤:

1. 创建对等体组
2. 对等体组内添加邻居路由器
3. 针对对等体组，配置各种设置

# RSTP（Rapid Spanning Tree Protocol，快速生成树协议）

## STP的不足：

1. STP没有细致区分端口状态和端口角色，不利于初学者学习及部署。

从用户角度来讲，Listening、Learning和Blocking状态并没有区别，都同样不转发用户流量。

从使用和配置角度来讲，端口之间最本质的区别并不在于端口状态，而是在于端口扮演的角色。

1. STP算法是被动的算法，依赖定时器等待的方式判断拓扑变化，收敛速度慢。
2. STP算法要求在稳定的拓扑中，根桥主动发出配置BPDU报文，而其他设备再进行处理，最终传遍整个STP网络。

## RSTP对STP的改进：

1. 通过端口角色的增补，简化了生成树协议的理解及部署；

* 替代端口：备用的根端口

根端口不可用时，替代口立即变为根端口

* 备份端口：备用的指定端口

提供了另一条从根桥到相应网段的备份通路

* 边缘端口：不向外发送BPDU报文，但可以接收BPDU。

通常连接PC、路由设备（因为不参与计算）

收到BPDU报文，重新参与stp计算，导致网络动荡

1. 端口状态的重新划分；

* Discarding状态：不转发用户流量也不学习MAC地址；
* Learning状态：不转发用户流量但是学习MAC地址；
* Forwarding状：既转发用户流量又学习MAC地址。

1. 配置BPDU格式的改变，充分利用了报文中的Flag字段，明确了端口角色；（拓展标志位）

Type字段：配置BPDU类型不再是0而是2，所以运行STP的设备收到RSTP的配置BPDU时会丢弃。

Flag字段：使用了原来保留的中间6位，这样改变的配置BPDU叫做RST BPDU。

1. 配置BPDU的处理发生变化；

* 所有交换机都能主动发送配置BPDU
* 配置BPDU发送间隔2s，过期时间=3\*hello时间
* 如果收到旧版BPDU，丢弃并回应自身的BPDU，更新邻居的BPDU信息

1. 增加保护功能。

* BPDU保护：针对边缘端口保护，保证现有stp结构稳定不变

保护原理：边缘端口收到BPDU报文，端口状态变为error-down状态，边缘端口特性不变

Error-down恢复方式

通过定时器自动恢复

手动恢复，恢复办法：接口视图，先shutdown再undo shutdown

* 根保护：针对指定端口，保证指定端口不能变为新的根端口

保护原理：指定端口收到更优的BPDU报文时，端口状态变为discarding，等待30s自动恢复

* 环路保护：针对备用端口，即替代端口，保证替代端口不会变为根端口

保护原理：根端口收不到BPDU报文，替代端口仍处于discarding状态

* 防止TC-BPDU攻击：针对拓扑变更的次数

保护原理：在规定时间内收到小于变更次数的TC-BPDU报文，交换机处理超过次数的变更，交换机不再处理

1. 新增P/A机制

作用：交换机接口尽快进入转发状态

协商过程：

* 交换机之间互相发送配置BPDU，互联口变为discarding状态的指定口
* 交换机收到的BPDU更优，把互联口立即变为根端口，边缘、备用端口保持不变，其他接口变为discarding状态的指定口；接口状态改变时，清空Mac表记录；向新根桥发送A标志位置位的BPDU报文
* 如果交换机收到的BPDU报文次优，自身为新根桥，把互联口立即变为转发状态的指定口；启动定时器，周期性发送P标志位置位的BPDU报文
* 非根桥继续用P/A机制与其他交换机更新BPDU信息

# MSTP（Multiple Spanning Tree Protocol，多生成树协议）

## 背景

为了弥补RSTP/STP的缺陷，IEEE于2002年发布的802.1S标准定义了MSTP。MSTP兼容STP和RSTP，通过建立多棵无环路的树，解决广播风暴并实现冗余备份。

## 工作原理

MSTP通过将交换机和桥接器分成多个区域（Region），每个区域可以包含多个独立的生成树实例（MSTI）。这些区域由相同的MST-Region ID标识，并且区域内的接口被视为一个整体。每个MST实例（MSTI）负责管理特定VLAN的流量，确保数据包被正确地映射到相应的路径上

## 优势

1. 负载均衡：MSTP可以在冗余链路上分配不同的数据流，从而实现负载均衡，提高带宽利用率。
2. 快速收敛：MSTP能够迅速响应拓扑变化，减少因拓扑变动带来的延迟。
3. VLAN感知：与RSTP相比，MSTP是VLAN感知的，能够根据不同的VLAN分配不同的数据路径，这使得网络配置更加灵活。
4. 兼容性：MSTP与STP和RSTP兼容，可以通过BPDU交换信息，支持混合环境下的操作

## 基本概念

### MST Region

同一MSTP域设备的特点

* 都启动MSTP
* 具有相同的域名
* 具有相同的VLAN到生成树实例映射配置
* 具有相同的MSTP修订级别配置

一个MSTP网络可以存在多个MST域，各MST域之间在物理上直接或间接相连。用户可以通过MSTP配置命令把多台交换设备划分在同一个MST域内。

### MSTI-基于Instance的生成树

MSTI是指MST域内的生成树。一个MST域内可以通过MSTP生成多棵生成树，各棵生成树之间彼此独立。一个MSTI可以与一个或者多个VLAN对应，但一个VLAN只能与-个MSTI对应。

### IST -内部生成树

IST是各个MST域内部的一棵生成树，是仅针对具体的MST域来计算的。但它是一个特殊的MSTI，其MSTIID为0，即IST通常称为MSTI0。每个MST域中只有一个IST，包括对应MST域中所有互联的交换机。

### CST - 公共生成树

CST：是连接整个MSTP网络内所有MST域的一棵单生成树，是针对整个MSTP网络来计算的，每个网络中只有一个CST，每个MST域中的IST是整个MSTP网络CIST在对应MST与中的一个片段

### CIST - 公共和内部生成树

CIST是通过STP或RSTP协议计算生成的，连接整个MSTP网络内所有交换机的单生成树，由IST和CST共同构成。这里要注意了，上面介绍的CST是连接交换网络中所有MST域的单生成树，而此处的CIST则是连接交换网络内的所有交换机的单生成树。即每个MSTP网络中也只有一个CIST。交换网络中的所有MST域的IST和CST一起构成一棵完整的生成树，也就是这里的CIST。

### SST-单生成树

构成SST（生成树）有两种情况

* 运行STP或RSTP生成树协议的交换机只属于一个生成树
* MST与中只有一个交换机，这个交换机构成了生成树

### 根桥分类

#### 总根

总根是CIST生成树的根桥，通常是交换网络中最上层的交换机，一个MSTP网络只有一个总根

#### 域根

域根（Regional Root）分为IST域根和MSTI域根。

在MST域中IST生成树中距离总根（CIST Root）最近的交换设备是IST域根。

一个MST域内可以生成多棵生成树，每棵生成树都称为一个MSTI。MSTI域根是每个多生成树实例的树根。如图2所示，域中不同的MSTI有各自的域根。

#### 主桥

主桥（Master Bridge）也就是IST Master，它是域内距离总根最近的交换设备。

如果总根在MST域中，则总根为该域的主桥。

### 端口类型

根端口、指定端口、Alternate端口、Backup 端口、边缘端口、Master 端口和域边缘端口。

* Master 端口：

是 MST 域和总根相连的所有路径中最短路径上的端口，它是交换设备上连接 MST 域到总根的端口。 如果ERPC路径开销相同，则比较上行链路的MST域中instance 0的域根bid的大小。

* 域边缘端口：

域边界端口。是指位于 MST 域的边缘并连接其它 MST 域或 SST 的端口。

## MSTP配置过程

* 区域配置和实例划分

注意：区域内所有交换机配置必须完全一致

具体配置内容：

1. 划分区域，配置区域名
2. 划分实例，vlan归属实例
3. 激活区域配置

* 给实例指定根桥

1区域配置和实例划分命令：

[SW1] stp region-configuration------------进入MST域视图

[SW1-mst-region] region-name 1-------给域命名

[SW1-mst-region] instance 1 vlan 2-----配置多生成树实例与VLAN的映射关系

[SW1-mst-region] instance 2 vlan 3

[SW1-mst-region] active region-configuration------激活MSTP域配置

[SW1-mst-region] quit

2指定根桥命令：

[Huawei] stp instance 1 root primary

[Huawei] stp instance 2 root secondary

# VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议）

## 概念

一种由IETF提出的网络层协议，旨在提高局域网中配置静态网关时的可靠性和可用性。其主要功能是通过将多台路由器虚拟成一个虚拟路由器，并使用一定的机制来保证当主路由器发生故障时，能够及时将业务切换到其他备份路由器上，从而保持通讯的连续性和可靠性

## 基本概念

### VRRP组：也称为虚拟路由器组或备份组，

由一组在同一局域网内、具有相同VRRP ID和虚拟IP地址的路由器组成。这些路由器共同工作，但只有一个处于Master状态，负责转发数据流量。

### 虚拟IP地址：

所有组内的路由器共享一个虚拟IP地址，这个地址被用作局域网内其他主机的默认网关。当主路由器发生故障时，其他备份路由器可以自动接管并继续处理数据流量。

关于虚拟ip和虚拟mac的几点注意事项：

虚拟ip配置时没有掩码

虚拟ip必须和接口ip在同网段

虚拟mac格式固定为：0000-5e00-01xx ，xx是vrid编号

### Master和Backup路由器：

* 在VRRP组中，有一个主路由器（Master）和多个备份路由器（Backup）。主路由器负责正常的数据包转发，而当主路由器失效时，备份路由器会自动接替其工作。
* 2种路由器都能收到发给网关的报文，但是backup路由器不做任何回复。
* 特殊的master路由器，叫IP地址拥有者路由器

vrrp的虚拟ip = 某个路由器接口ip

该路由器就是master路由器。优先级默认是255

尽量不用，会导致某些需要主备自动切换的功能失效

* master失效时间

vrrp维持状态的报文由master发送，发送间隔1s

master失效时间在3-4s之间

### 优先级机制：

每个VRRP路由器都有一个优先级值，优先级越高，越有可能成为Master路由器。如果当前的Master路由器失效，其他路由器会根据优先级重新选举新的Master路由器

## 工作原理

1. 角色划分：在VRRP组中，路由器根据优先级确定自己在组中的角色。优先级最高的路由器成为主用路由器（Master），负责转发数据包到虚拟IP地址；其他路由器则作为备用路由器（Backup）。

master竞选过程：

a、修改vrrp优先级，越大越优先。默认是100

b、优先级相同对比ip地址，越大越优先

2. 通告报文：主用路由器会定期发送VRRP通告报文，通知备份组内的其他路由器自己工作正常。如果备用路由器在一定时间内未收到主用路由器的通告报文，则认为主用路由器已经无法正常工作，此时备用路由器将接管数据传输任务。

vrrp报文目的ip，是224.0.0.18

vrrp报文TTL=255

hsrp(叫热备份路由选择协议)报文TTL=1

1. 抢占与非抢占模式：VRRP支持抢占和非抢占两种模式。在抢占模式下，如果备用路由器的优先级高于当前的主用路由器，它将立即成为新的主用路由器。在非抢占模式下，即使备用路由器的优先级更高，只要当前的主用路由器仍在工作，它就不会成为新的主用路由器。

如果抢占模式没开使用：vrrp vrid 编号 preempt-mode delay xxx秒

## 监视特定口、特定链路状态

特定口、特定链路状态有误，主动执行主备切换

监视原理:端口或链路故障，master主动降低优先级，从而backup路由器优先级高

一般监视master设备的接口或链路

监视接口状态：

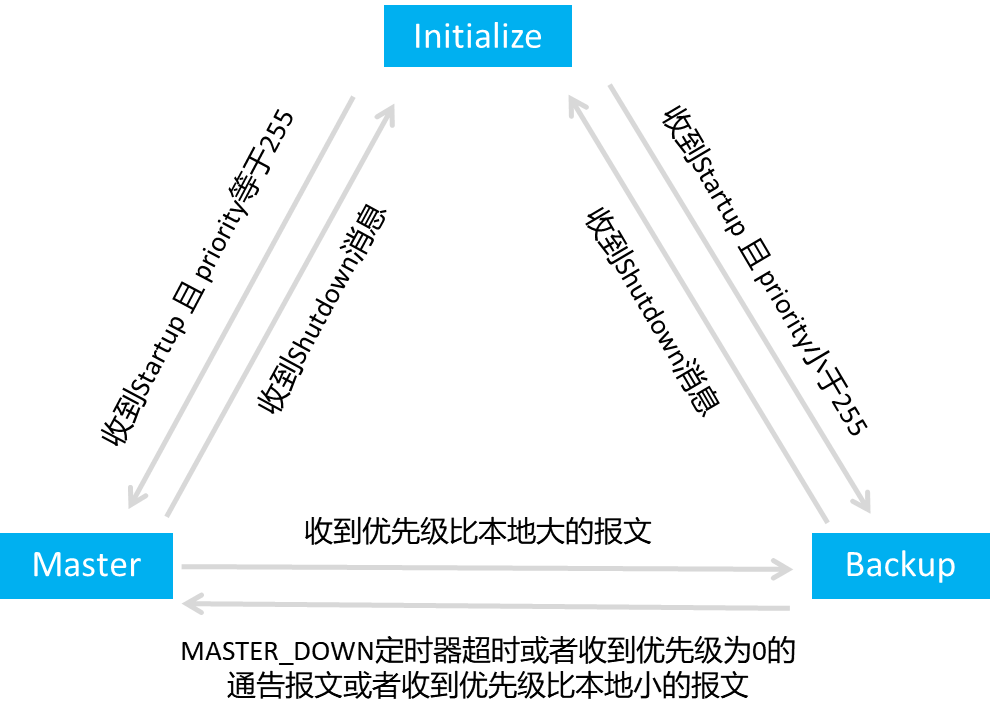
vrrp vrid 编号 track interface 接口 reduce 减少的数值

监视链路状态：

vrrp vrid 编号 track bfd-session bfd号

## VRRP协议状态机

Initialize（初始状态）、Master（活动状态）、Backup（备份状态）。



单一路由器的状态为Initialize原因是什么？

接口没IP或者说接口没开启是down状态

# [BFD](https://blog.csdn.net/Junior_engineer/article/details/111321416?spm=1001.2101.3001.6650.3&utm_medium=distribute.pc_relevant.none-task-blog-2%7Edefault%7ECTRLIST%7ECtr-3-111321416-blog-125501721.235%5Ev43%5Epc_blog_bottom_relevance_base5&depth_1-utm_source=)**（Bidirectional Forwarding Detection，双向转发检测）**

## 简述

BFD（Bidirectional Forwarding Detection，双向转发检测）是一个通用的、标准化的、介质无关和协议无关的快速故障检测机制，用于检测IP网络中链路的连通状况，保证设备之间能够快速检测到通信故障，以便能够及时采取措施，保证业务持续运行。

注意：

监视发包间隔以ms为单位

BFD不可单用，必须结合其他功能，为其他功能提供切换依据

## 分类

### 静态BFD

一般在2个远端设置之间手动配置BFD。需要手动配置本端和对端的标识

命令：

[R1]bfd

[R1]bfd 12 bind peer 10.0.12.2 interface GigabitEthernet 0/0/1

[R1-bfd-session-12]discriminator local 10

[R1-bfd-session-12]discriminator remote 20

[R1-bfd-session-12]commit ------提交保存

[R2]bfd

[R2]bfd 21 bind peer 10.0.12.1 interface GigabitEthernet 0/0/1

[R2-bfd-session-21]discriminator local 20

[R2-bfd-session-21]discriminator remote 10

[R2-bfd-session-21]commit

在R1上配置静态路由并绑定BFD会话

[R1] ip route-static 4.4.4.4 32 10.0.12.2 track bfd-session 12

[R1] ip route-static 4.4.4.4 32 10.0.13.2 preference 100

### 动态BFD

一般在2个相邻设备之间自动配置BFD。通常在路由协议中使用

命令：

[R1]bfd

[R1-ospf-1]bfd all-interfaces enable

## BFD检测方式

### 异步模式

双方都支持BFD使用

双方周期性发送检测报文，收到对端的检测报文，表示链路正常

发送时间 = 本地配置发送时间、对端配置接收时间的最大值

接收时间 = 本地配置接收时间、对端配置发送时间的最大值

检测次数 = 对端配置的检测次数

### 查询模式，也叫回声模式（不建议使用）

当一方设备支持BFD但另一方不支持使用

只在需要检测时，连续发送多次

检测次数 = 本端配置的检测次数

# 组播

## 组播地址

|  |  |
| --- | --- |
| 范围 | 含义 |
| 224.0.0.0—224.0.0.255 | 为路由协议预留的永久组地址 |
| 224.0.1.0—231.255.255.255  233.0.0.0—238.255.255.255 | Any-Source临时组播组地址 |
| 232.0.0.0—232.255.255.255 | Source-Specific临时组播组地址 |
| 239.0.0.0—239.255.255.255 | 本地管理的Any-Source临时组播组地址 |

### 特殊组播地址

224.0.0.1---------------任何设备都可以接收的组播地址

224.0.0.2---------------只有路由设备才能接收的组播地址

224.0.0.5---------------所有运行OSPF进程的路由器的组播地址

224.0.0.6---------------多路访问网络中DR（指定路由器）和BDR（备份指定路由器）的组播接收地址

224.0.0.18-------------VRRP协议用到的组播地址

## 组播Mac地址

IANA规定，IPv4组播MAC地址的高24位为0x01005e，第25位为0，低23位为IPv4组播地址的低23位，例如组播组地址224.0.1.1对应的组播MAC地址为01-00-5e-00-01-01。

## 组播网络基本架构

* 源端网络：将组播源产生的组播数据发送至组播网络。
* 组播转发网络：形成无环的组播转发路径，该转发路径也被称为组播分发树（Multicast Distribution Tree）。
* 成员端网络：让组播网络感知组播组成员位置与加入的组播组。

## 组播服务模型

组播组成员在接收组播数据时可以对于组播数据源进行选择，因此产生了ASM（Any-Source Multicast，任意源组播）和SSM（Source-Specific Multicast，指定源组播）两种组播服务模型。

ASM：组成员加入组播组以后，组成员可以接收到任意源发送到该组的数据。

SSM：组成员加入组播组以后，组成员只会收到指定源发送到该组的数据。

## 组播协议

### 组播成员关系协议

#### IGMP（Internet Group Management Protocol）

用于IPv4环境，是最早出现的组播成员关系协议。它通过路由器与主机之间的交互来管理组播组成员关系。当一个主机希望加入某个组播组时，它会发送IGMP加入报文，而路由器则根据这些报文更新其维护的组播组成员表。

客户端需要加入组播环境，路由器才会创建IGMP组播路由表

路由器同时创建IGMP组表，记录接收组播数据的最后一个PC地址

##### IGMP组表项与路由表项

* IGMP组表项是由用户主机发送的IGMP加入报文触发创建的，用于维护组加入信息并通知组播路由协议（通常所说的为PIM协议）创建相应(\*,G)表项。
* IGMP路由表项的作用主要是用来扩展组播路由表项的出接口。

IGMP路由表项与IGMP组表项能为组播协议路由表提供组播组地址信息与出接口信息。

##### IGMP版本

IGMPv1

主要基于查询和响应机制完成组播组管理。

* 普遍组查询报文（General Query）：查询器向共享网络上所有主机和路由器发送的查询报文，用于查询哪些组播组存在成员。

默认发送间隔 60 s

成员关系报告报文（Report）：主机向查询器发送的报告报文，用于申请加入某个组播组或者应答查询报文。

IGMPv2

在IGMPv1的基础上新增2种报文

* 成员离开报文（Leave）：成员离开组播组时主动向查询器发送的报文，用于宣告自己离开了某个组播组。成员离开报文目的地址为224.0.0.2。
* 特定组查询报文（Group-Specific Query）：查询器向共享网段内指定组播组发送的查询报文，用于查询该组播组是否存在成员。特定组查询报文目的地址为所查询组播组的组地址。

IGMPv2查询器：IP地址最小的路由器成为查询器

IGMPv3

查询报文共有三类：

* 普遍组查询报文（General Query）。该报文作用与IGMPv1,IGMPv2中的普遍组查询报文作用一致。
* 特定组查询报文（Group-Specific Query） 。该报文作用与IGMPv2中的特定组查询报文作用一致。
* 特定源组查询报文（Group-and-Source-Specific Query）。该报文用于查询该组成员是否愿意接收特定源发送的数据。特定源组查询通过在报文中携带一个或多个组播源地址来达到这一目的。

##### IGMP Snooping

IGMP Snooping可以实现组播数据在数据链路层的转发和控制。

工作原理：IGMP Snooping设备通过监听IGMP报文，形成二层组播转发表，并决定接口类型

**二层组播转发表项中存在两类接口：**

* 路由器端口（Router Port）：二层组播设备上朝向三层组播设备（DR或IGMP查询器）一侧的接口，二层组播设备从此接口接收组播数据报文。
* 成员端口（Member Port）：又称组播组成员端口，表示二层组播设备上朝向组播组成员一侧的端口，二层组播设备往此接口发送组播数据报文。

##### IGMP SSM Mapping

IGMP SSM Mapping通过静态的将组播源与组播组进行绑定，使得IGMPv1与IGMPv2的组成员也能接入SSM组播网络。

**工作原理：**

在IGMP查询器上静态配置SSM地址的映射规则，将IGMPv1或IGMPv2成员关系报告中的组信息映射为源组信息。

##### IGMP Proxy

为了缓解IGMP查询器压力，IGMP Proxy设备将成员关系报告/离开报文汇聚后统一上送给IGMP查询器。

IGMP Proxy设备也可以代理IGMP查询器向成员主机发送查询报文，维护组成员关系，基于组成员关系进行组播转发。

**为了实现以上功能，IGMP Proxy定义了两类接口：**

* 主机接口（Host Interface）：IGMP Proxy设备上配置IGMP Proxy功能的接口，该接口一般面向IGMP查询器。
* 路由器接口（Router Interface）：IGMP Proxy设备上配置IGMP功能的接口，该接口一般面向组成员。

##### 命令：

[RTA]multicast routing-enable

[RTA]interface g0/0/1

[RTA-GigabitEthernet0/0/1]ip address 192.168.1.1 24

[RTA-GigabitEthernet0/0/1]igmp enable

[RTA-GigabitEthernet0/0/1]igmp version 2

IGMP通常连接客户端

#### MLD（Multicast Listeners Discovery Protocol）

用于IPv6环境，功能类似于IGMP，但专为IPv6设计。MLD同样通过路由器与主机之间的交互来管理组播组成员关系

### 组播路由协议

#### PIM（Protocol Independent Multicast，协议无关组播）

协议主要作用是生成AS域内的组播分发树。

##### Pim模式

* PIM-DM（PIM-Dense Mode，PIM密集模式）

工作原理：先向全网扩散组播，收集PC配置，形成组播分发树

适合环境：适合小型网络、组播客户端集中的环境

* PIM-SM（PIM-Sparse Mode，PIM稀疏模式）

工作原理：先收集PC配置，形成组播分发树，再发送组播数据

适合环境：适合大型网络、组播客户端分散的环境

该模式中，必须有RP（汇聚点）路由器

RP必须和组播源构建组播接收路径

RP必须和末端路由器构建组播分发路径

##### Pim分发树

* SPT 共享树

以组播源为根，组播组成员为叶子的组播分发树。在PIM-DM与PIM-SM中均有使用。

* RPT源树

以RP（Rendezvous Point）为根，组播组成员为叶子的组播分发树。在PIM-SM中使用。

##### PIM路由表项

（S，G）路由表项主要用于在PIM网络中建立SPT。对于PIM-DM网络和PIM-SM网络适用。

（\*，G）路由表项主要用于在PIM网络中建立RPT。对于PIM-SM网络适用。

##### PIM-DM机制

1. **扩散（Flooding）机制**

组播数据包向所有的PIM邻居泛洪，同时组播路由器产生组播路由表项。

1. **剪枝（Prune）机制**

如果组播路由器下没有组成员，则将源到该组播路由器的组播转发路径剪枝。

1. **邻居发现（Neighbor Discovery）机制**

组播转发路径只能在PIM邻居之间建立，因此邻居发现是形成组播分发树的先决条件。

邻居发现主要通过PIM Hello包完成。

1. **嫁接（Graft）机制**

PIM-DM通过嫁接机制，使有新组成员加入的网段快速得到组播报文。

叶子路由器通过IGMP了解到与其相连的用户网段上，组播组G有新的组成员加入。随后叶子路由器会基于本地的组播路由表向上游发送Graft报文，请求上游路由器恢复相应出接口转发，将其添加在（S，G）表项下游接口列表中。

1. **断言（Assert）机制**

当组播转发过程中存在多路访问网络，则需要选举出一个组播转发路由器，避免重复组播报文。

1. **状态刷新（State Refresh）机制。**

在PIM-DM网络中，为了避免被裁剪的接口因为“剪枝定时器”超时而恢复转发，离组播源最近的第一跳路由器会周期性地触发State Refresh报文在全网内扩散。

收到State Refresh报文的PIM路由器会刷新剪枝定时器的状态。被裁剪接口的下游叶子路由器如果一直没有组成员加入，该接口将一直处于抑制转发状态。

##### 命令：

[R3]multicast routing-enable

[R3]interface g0/0/0

[R3-GigabitEthernet0/0/0]pim dm

路由器之间，

#### MSDP（Multicast Source Discovery Protocol，组播源发现协议）

主要作用是帮助生成AS域间的组播分发树。

#### MBGP（Multicast BGP，组播BGP）

主要作用是帮助跨域组播流进行RPF校验。

### 其他相关的组播协议和技术

#### BIER（Bit Index Explicit Replication）

一种支持IPv6的显式复制组播技术，主要用于视频直播、视频监控等场景

#### 组播密钥管理

涉及簇生成协议、成员发现协议和密钥服务器等，用于提高系统的可扩展性、健壮性和可预测性

## RPF检查（Reverse Path Forwarding）

用于确定数据包到达的接口是否是通往组播源的最佳路径。其主要作用是防止循环和泛滥，确保数据包能够正确地从组播源传输到接收者。

### RPF路由选举规则

如果配置了按照最长匹配选择路由，则从这三条路由中选出最长匹配的那条路由；

如果这三条路由的掩码一样，则选择优先级最高的那条路由；

如果它们的优先级也相同，则按照组播静态路由、MBGP路由、单播路由的顺序进行选择。

## 组播分发树

通过RPF机制与组播路由协议，组播网络可以最终形成无环、无次优且无重复包的组播转发路径，该路径可以被称为组播分发树。

组播分发树以组播源为根，以组成员为叶子形成转发路径，组播数据在转发时都基于组播分发树进行转发。

## 应用场景

组播技术广泛应用于多种场景，如视频直播、视频监控、远程教育、软件分发等。例如，在视频会议和远程教学中，通过组播技术可以实现多点到多点的实时数据传输。

# 防火墙

## 基本概念

### 定义

在通信领域，防火墙是一种安全设备。它用于保护一个网络区域免受来自另一个网络区域的攻击和入侵，通常被应用于网络边界。

### 分类

#### 包过滤防火墙

原理：利用IP五元组过滤数据

缺点：必须配置双向规则，过滤数据不全面

#### 状态检测防火墙（基础类型）

特点：针对网络层、传输层、应用层过滤；只需要配置单向规则，返回的数据自动被放过

配置出向规则后，数据流过防火墙时，在会话表中自动生成记录，回传的数据按照会话表记录自动放通

#### AI防火墙

华为AI防火墙，内置的恶意文件检测引擎CDE、诱捕Sensor、APT检测引擎和探针，支持与沙箱和华为大数据分析平台CIS联动检测，打造智能防御体系。

#### WAF防火墙（web防火墙）

过滤网站访问数据

#### 代理防火墙

过滤传输层、应用层数据，利用缓存加快访问速度

### 区域

通过区域划分，决定防火墙连接网络的安全程度

**区域划分**

* 受信区域（trust）

连接内网

较高安全级别区域，优先级为85

* 非受信区域（untrust）

连接外网

低安全级别区域，优先级为5。

* 非军事化区域（dmz）

只能存放对外开放访问的服务器

中等安全级别区域，优先级为50

* 本地区域（local）

代表防火墙自身

默认防火墙所有接口都在1ocal区域，且不可修改

最高安全级别区域，优先级为100。

### 安全策略

* 安全策略是控制防火墙对流量转发以及对流量进行内容安全一体化检测的策略。
* 当防火墙收到流量后，对流量的属性（五元组、用户、时间段等）进行识别，然后与安全策略的条件进行匹配。如果条件匹配，则此流量被执行对应的动作。
* 安全策略的组成有匹配条件、动作和安全配置文件（可选）
* 安全策略的配置顺序很重要，需要先配置条件精确的策略，再配置宽泛的策略

### 会话表

会话表是用来记录TCP、UDP、ICMP等协议连接状态的表项，是防火墙转发报文的重要依据。

防火墙采用了基于“状态”的报文控制机制：只对首包或者少量报文进行检测就确定一条连接的状态，大量报文直接根据所属连接的状态进行控制。这种状态检测机制迅速提高了防火墙的检测和转发效率。

为了解决多通道协议的问题，防火墙需要识别协议在应用层协商的地址和端口。需要开启ASPF （Application Specific Packet Filter，针对应用层的包过滤）功能。ASPF会生成Server-map表。在流量真实到达防火墙时，防火墙会基于Server-map表生成会话表，然后执行转发。

### 使用位置

替换出口路由器：进行全网数据过滤

服务器前面：只过滤对服务器的访问

放置方法：

* 直接接入网络

适用于新网络

* 旁挂到网络

适用于现有网络

## 防火墙配置步骤

1. 接口加入某个区域（接口下的某一个网络加入某个区域）
2. 接口配置IP
3. 配置路由表
4. 配置安全规则

# VPN（Virtual Private Network，虚拟专用网络）

## VPN概念

虚拟专用网VPN,

作用:通过互联网，在2个设备之间安全传输数据

常用于:出差员工访问公司内部资源总部与分部之间传输数据

## VPN使用场景

a、远程访问VPN，也叫accessVPN、端到端VPN特点:互联网上单台PC，连接公司VPN设备，并能访问内部资源

点到点VPNb、特点:2个公司之间通过互联网安全传输数据只能在网络设备上配置

注意:三层交换不支持VPN和NAT

## VPN协议分类

### 远程访问VPN（Remote Access VPN）

常见RA-VPN协议: PPTP VPN、L2TP VPN、 SSTP VPN、EZvpn/ easyvpn（思科私有）、 SSL VPN（目前比较流行）

二层VPN

a、常用的有:PPTP(点到点隧道协议)、L2TP(第二层隧道协议)可以实现远程访问VPN

安全性差，很少使用

七层VPN

常用的有:SSL VPN可以实现远程访问VPN

使用较多，直接通过浏览器实现 L2TP都需要在Pc配置PPTP、

### 点到点VPN

常见的点到点VPN：IPsecVPN

三层VPN

常用的有:IPSec VPN

可以实现点到点VPN，需要双方配置最常使用，用来连接网络和网络

## VPN隧道技术

隧道技术（Tunneling）是网络基础设置在网络之间传递数据的方式，使用隧道技术传递可以是不同协议的数据包，隧道协议将这些其他协议的数据包重新封装在新的包头中发送。被封装的数据包在隧道的两个端点之间通过网络进行路由，被封装数据包在网络上传递时所经历的逻辑路径称为隧道。

简单来说，隧道技术是一类网络协议，是将一个数据包封装在另一个数据包中进行传输的技术；使用隧道的原因是在不兼容的网络上传输数据，或在不安全网络上提供一个安全路径。通过网络隧道技术，可以使隧道两端的网络组成一个更大的内部网络。（把不支持的协议数据包打包成支持的协议数据包之后进行传输）。

### 常见的隧道协议

#### 基于数据包的隧道协议

1. IPsec： 提供加密和认证，确保数据的完整性和保密性。IPsec是一套协议包，而不是单一协议，包含了AH（认证首部）和ESP（封装安全载荷）等多个子协议。
2. GRE（通用路由封装协议）： 支持多种网络层协议和多路技术。
3. IP in IP： 适合只有一个IP流的情况，负载头更小。
4. L2TP（第二层隧道协议）： 结合了PPTP和L2F的优点，支持多种协议。L2TP允许用户从客户端或访问服务器端建立VPN连接。
5. MPLS（多协议标签交换）： 用于高效的数据包转发。MPLS通过标签进行数据包转发，避免了复杂的路由查找。
6. PPTP（点对点隧道协议）： 通过PPP帧在互联网上建立虚拟专用网（VPN）。PPTP采用了基于RSA公司的RC4加密方法，保证了虚拟连接通道的安全。
7. PPPoE（基于以太网的点对点隧道）： 用于DSL宽带连接。
8. IPv6穿隧（如6to4、6in4、Teredo）： 帮助IPv6数据包在IPv4网络中传输。

#### 基于流的隧道协议

1. 传输层安全（TLS）： 提供加密的传输层安全，用于保护在两个应用程序之间传输的数据。
2. SSH（安全外壳协议）： 通过加密通道进行安全数据传输，常用于远程登录。
3. SOCKS： 用于代理服务器的通用协议，能够代理TCP和UDP请求。
4. HTTP CONNECT 命令： 通过HTTP代理建立隧道，用于传输加密数据。

## IPSec

IPSec（IP Security）是一组开放的网络安全协议，是对IP的安全性补充，其工作在IP层，为IP网络通信提供透明的安全服务。它并不是一个单独的协议，而是一系列为IP网络提供安全性的协议和服务的集合，这些协议和服务包括认证头AH（Authentication Header）和封装安全载荷ESP（Encapsulating Security Payload）两个安全协议、密钥交换和用于验证及加密的一些算法等。

端口号：UDP500

### IPsec可提供安全服务

1. 数据加密：IPsec协议使用加密技术对数据进行加密，确保数据在传输过程中的机密性。它提供了两种加密方式：ESP（Encapsulating Security Payload）和AH（Authentication Header）。ESP协议负责数据的加密，而AH协议则提供数据的完整性校验和源验证功能。通过这些加密技术，IPsec可以保护TCP/IP协议簇中传输的数据，防止数据被窃取或篡改。
2. 认证机制：IPsec协议提供了认证机制，用于验证数据的完整性和来源。AH协议通过在每个数据包中添加一个认证头来实现这一功能。认证头包含了用于验证数据完整性的哈希值和用于验证数据来源的公钥或预共享密钥。通过验证认证头，接收方可以确保接收到的数据是完整且来自可信的发送方。
3. 防止重放攻击：IPsec协议通过使用序列号和时间戳来防止重放攻击。每个IPsec数据包都包含一个唯一的序列号，接收方可以检查序列号的连续性来识别重放的数据包。此外，时间戳也可以用来验证数据包的时效性，确保数据包不是在过去某个时间截取的。
4. 访问控制：IPsec协议支持访问控制功能，可以根据策略规则来允许或拒绝特定的通信连接。通过配置IPsec策略，可以实现基于源IP地址、目标IP地址、端口号等条件的访问控制，增强网络的安全性。

#### 主要功能详解

a、加密协议采用对称加密协议，使用DES、3DES、AES算法

加密的2种类型:

1. 对称加密

加密、解密采用相同的密钥与算法

加密速度快

2)非对称加密

加密和解密使用不同的密钥与算法

安全性最高，加密速度慢

b、数据完整性协议

采用hash散列算法，使用MD5、SHA算法

特点:只能从一种形式转换成另一种形式，不可逆推

1. 身份验证方法

可用:预共享密钥、数字证书

d、抗重放攻击

E、密匙交换协议，也叫IKE协议

特点：协商上面各种协议，自动生成加密密匙

### 数据封装协议

#### AH协议：（认证头协议、鉴别头协议）

AH（Authentication Header）协议是一种为IP数据包提供数据完整性验证和数据源身份认证的安全协议。

AH协议号:51

##### AH提供的安全服务：

1. 数据源验证：AH协议通过验证数据包的完整性和身份来确保数据来自可信的源。它使用公钥加密或预共享密钥来对数据包进行加密和签名，以验证发送方的身份和数据包的完整性。
2. 数据完整性校验：AH协议使用哈希算法（如MD5或SHA-1）来计算数据包的哈希值，并将该哈希值附加在数据包的AH头认证数据字段中。接收方在接收到数据包后，使用相同的哈希算法重新计算哈希值，并与数据包中的哈希值进行比较，以验证数据包的完整性。
3. 防报文重放：AH协议通过序列号和时间戳等机制来防止重放攻击。每个AH数据包都包含一个唯一的序列号，接收方可以检查序列号的连续性来识别重放的数据包。此外，时间戳也可以用来验证数据包的时效性，确保数据包不是在过去某个时间截取的。

##### AH数据封装位置：

在原始ip包头与传输层数据之间添加AH头部

##### AH认证范围：

所有的ip数据包信息

#### ESP协议，数据封装载荷协议

ESP（Encapsulating Security Payload）协议是IPsec协议族中的一个重要组件，主要用于为IP数据包提供加密、数据源认证、数据完整性校验和防报文重放等功能。与AH协议不同，ESP协议主要关注数据的机密性，通过加密技术来保护数据的内容不被泄露。

ESP协议号:50

##### ESP提供的安全服务：

1. 数据机密性保护：ESP协议使用对称加密算法（如DES、3DES、AES等）对IP数据包的内容进行加密，确保数据在传输过程中不被未授权访问。加密后的数据以密文形式传输，只有拥有正确密钥的接收方才能解密并获取原始数据。这提供了数据的机密性保护，防止了数据的泄露和非法获取。
2. 数据源认证：ESP协议还提供了数据源认证功能，用于验证数据包的来源。这通过使用公钥加密或预共享密钥来生成认证标签（通常是哈希值）实现。发送方在生成ESP报文时，会将认证标签附加在ESP尾中。接收方收到报文后，会使用相同的密钥和算法重新计算认证标签，并与报文中的标签进行比较。如果两者一致，则说明数据包来自可信的发送方，没有被篡改。
3. 数据完整性校验：ESP协议使用哈希算法（如MD5或SHA-1）来计算数据包的哈希值，并将其附加在ESP尾中。这个哈希值用于校验数据包的完整性，确保数据在传输过程中没有被篡改。接收方在收到数据包后，会使用相同的哈希算法重新计算哈希值，并与报文中的哈希值进行比较。如果哈希值一致，则说明数据包的内容没有被篡改，保持了数据的完整性。
4. 防报文重放：ESP协议通过序列号机制来防止报文的重放攻击。每个ESP数据包都包含一个唯一的序列号，接收方可以检查序列号的连续性来识别重放的数据包。这种机制确保了每个数据包都是新鲜的，没有被重复发送，从而防止了重放攻击。

ESP的认证不如AH全面高安全环境下，ESP+AH同时使用

##### Esp数据封装位置:

在原始ip包头与传输层数据之间添加ESP头部在传输层后面添加ESP尾部在ESP尾部后面，添加ESP认证信息

##### ESP加密范围:

从ESP头部后面，直到ESP尾部

##### ESP认证范围:

从ESP头部开始，直到ESP尾部

注意:如果VPN设备在内网，VPN通讯需要经过NAT转换，封装协议只能选择ESP

出口设备做VPN任何封装方式都可以

#### ESP和AH对比

ESP（Encapsulating Security Payload，封装安全载荷）和AH（Authentication Header，认证头标）是IPSec协议中的两个核心协议，它们在功能和应用方面存在显著区别。

##### 加密功能：

ESP提供了加密功能，可以隐藏数据内容，防止窃听。

AH则没有提供加密功能，仅用于验证数据包的完整性和来源。

##### 验证范围：

ESP的验证范围不包括IP报头，只对数据部分进行加密和认证。这意味着在传输模式下，ESP不会保护原始IP报头的内容。

AH的验证范围更广，它不仅验证数据部分，还验证整个IP报头。这使得AH能够确保整个数据包的完整性。

##### 资源消耗：

AH由于其简单的结构和算法，通常需要较少的CPU、内存和网络资源。

ESP由于其复杂的加密机制，需要更多的计算资源，因此在性能上可能稍逊一筹。

##### 应用场景：

如果需要数据加密和完整性保护，可以选择使用ESP。例如，在需要高安全性的场景中，ESP是更好的选择。

在对安全性要求较高的情况下，可以联合使用AH和ESP协议，以弥补各自不足。

总结来说，ESP和AH各有优缺点。如果需要全面的数据保护（包括加密和完整性），应优先选择ESP；而在对资源消耗敏感且不需要加密的情况下，可以选择AH来实现基本的安全需求。

#### IKE（Internet Key Exchange）协议

即因特网密钥交换协议，是一种为IPSec（Internet Protocol Security）提供自动协商交换密钥、建立安全联盟（Security Association，SA）的协议。

##### IKE协议的基本概念

定义：IKE协议建立在ISAKMP（Internet Security Association and Key Management Protocol）框架之上，是基于UDP的应用层协议。它为IPSec提供了自动协商密钥、建立IPSec安全联盟的服务，从而简化了IPSec的使用和管理。

作用：IKE协议能够自动协商和分发密钥，验证通信双方的身份，并在不安全的网络上安全地建立IPSec安全联盟。

##### IKE包含的组件

1. SKEME：实现公钥加密认证的机制
2. Oakley：基于到达两个对等体间的加密密钥的机制
3. ISAKMP：在两个实体间进行分组格式及状态转换的消息交换的体系结构。

##### IKEv1和IKEv2版本区别

###### 协商过程不同。

− IKEv1

IKEv1协商安全联盟主要分为两个阶段。

IKEv1阶段1的目的是建立IKE SA，它支持两种协商模式：主模式和野蛮模式。主模式用6条ISAKMP消息完成协商。野蛮模式用3条ISAKMP消息完成协商。野蛮模式的优点是建立IKE SA的速度较快。但是由于野蛮模式密钥交换与身份认证一起进行无法提供身份保护。

IKEv1阶段2的目的就是建立用来传输数据的IPSec SA，通过快速交换模式（3条ISAKMP消息）完成协商。

− IKEv2

IKEv2简化了安全联盟的协商过程。IKEv2正常情况使用2次交换共4条消息就可以完成一个IKE SA和一对IPSec SA，如果要求建立的IPSec SA大于一对时，每一对SA只需额外增加1次交换，也就是2条消息就可以完成。

###### 认证方法不同。

IKEv2支持EAP身份认证。IKEv2可以借助认证服务器对远程接入的PC、手机等进行身份认证、分配私网IP地址。IKEv1无法提供此功能，必须借助L2TP来分配私网地址。

###### IKE SA的完整性算法支持情况不同。

IKE SA的完整性算法仅IKEv2支持，IKEv1不支持。

###### DPD中超时重传实现不同。

retry-interval参数仅IKEv1支持。表示发送DPD报文后，如果超过此时间间隔未收到正确的应答报文，DPD记录失败事件1次。当失败事件达到5次时，删除IKE SA和相应的IPSec SA。直到隧道中有流量时，两端重新协商建立IKE SA。

对于IKEv2方式的IPSec SA，超时重传时间间隔从1到64以指数增长的方式增加。在8次尝试后还未收到对端发过来的报文，则认为对端已经下线，删除IKE SA和相应的IPSec SA。

###### IKE SA超时时间手工调整功能支持不同。

IKEv2的IKE SA软超时为硬超时的9/10±一个随机数，所以IKEv2一般不存在两端同时发起重协商的情况，故IKEv2不需要配置软超时时间。

###### IPSec SA超时时间手工调整功能支持不同。

IKEv2的IKE SA软超时为硬超时的9/10±一个随机数，所以IKEv2一般不存在两端同时发起重协商的情况，故IKEv2不需要配置软超时时间。

##### IKE协议的安全机制

* 密钥交换：IKE协议通过Diffie-Hellman（DH）交换技术来生成共享密钥，而不是直接在网络上传输密钥。这样，即使第三者截获了用于计算密钥的所有交换数据，也无法计算出真正的密钥。
* 身份验证：IKE支持多种身份验证方法，包括预共享密钥认证、数字证书认证等。这些方法确保了通信双方的身份真实性。
* 数据验证：IKE协议通过验证数据的完整性来确保数据在传输过程中未被篡改。
* 前向安全性（PFS）：PFS是一种安全特性，指一个密钥被破解后，不影响其他密钥的安全性。IKE通过执行额外的DH交换来保证PFS。

##### IKE协议的工作流程

###### 阶段一：协商IKE SA

在此阶段，通信各方建立一个已通过身份验证和安全保护的通道，即ISAKMP SA（也可称IKE SA）。

支持两种协商模式：主模式（Main Mode）和野蛮模式（Aggressive Mode）。主模式需要更多的消息交换来提供更强的身份保护，而野蛮模式则通过减少消息交换次数来提高效率，但牺牲了部分身份保护。

**主模式**

双方需要交换6个报文才能协商成功

* 报文1:发起者发送支持的各种安全参数
* 报文2:接受者采用双方都支持的最高安全参数，并反馈给发起者
* 报文3:双方互发密钥生成资料，并携带临时的对称密钥
* 报文4:根据对方要求，在本地生成长期使用对称密钥(有效期1天)

2个报文都是在本地生成加密密钥

* 报文5:双方利用长期使用对称密钥加密自身信息，发送给对方
* 报文6:验证接收到的身份信息，验证长期使用对称密钥是否可用

注意:前4个报文明文、后2个身份认证报文密文长期使用的对称密钥，不能用于数据加密

3次交换过程，6个消息交互

1. SA交换[报文1和报文2]：发送本端的IKE策略信息，接收对端的确认策略
2. 密匙交换（DH交换）[报文3和报文4]：发送本地密匙生成信息，密匙生成
3. ID交换及验证[报文5和报文6]：发送本端身份和验证信息，身份验证和交换过程验证

**野蛮模式**

双方需要交换3个报文才能协商成功

* 报文1:发送所有的安全参数、身份信息、密钥生成要求
* 报文2:在本地生成长期使用对称密钥，并向发送者也发送报文1内容
* 报文3:发送者在本地生成长期使用对称密钥，并做简单验证

注意:前2个报文明文、后1个报文密文

注意:身份信息在主模式下只能用ip地址表示身份信息在野蛮模式下，可以用ip地址、也可以自定义在有NT地址转换情况下，只能用野蛮模式协商

主模式、野蛮模式区别:

1. 主模式使用6个报文、野蛮模式使用3个报文
2. 主模式协商慢但安全性高、野蛮模式协商快但安全性较低
3. 主模式只能用IP地址标识身份、野蛮模式可以用IP或自定义字符串形式标识身份

总结:在有NAT存在时，只能使用ESP封装+隧道模式+IKE阶段一采用野蛮模式

###### 阶段二：协商IPSec SA

在第一阶段建立的安全通道内，IKE为IPSec协商具体的安全联盟，即IPSec SA。

IPSec SA用于最终的IP数据安全传送。

只有1种协商办法:快速模式

使用3个报文完成协商:

报文一和报文二:双方交换各自的安全配置

注意:使用阶段一生成的加密密钥，加密交换的安全配置内容

报文三:双方生成加密数据用的对称密钥，验证对称密钥是否可用

注意:该对称密钥用来加密通讯双方正式的通讯数据密钥有效期:3600s

阶段二的所有数据全部采用密文

阶段二可以使用阶段一的对称密钥加密数据，阶段二如果想使用单独的对称密钥，必须配置PES技术(叫完美向前保密)

### 数据传输类型

#### 传输模式

传输模式用于直接连接两个主机或者终端设备之间的安全通信。在传输模式下，只有 IP 数据包的有效载荷部分被加密和认证，而 IP 头部保持原样。

传输模式适用于端到端的通信，例如主机到主机之间的通信或者主机到网关的通信。

#### 隧道模式

隧道模式用于在两个网络之间创建安全的通信隧道，将整个 IP 数据包（包括 IP 头部和有效载荷）都加密和认证后传输。通常，在一个网络设备（例如 VPN 网关）到另一个网络设备之间建立隧道连接。

隧道模式适用于网关到网关的通信，其中整个通信流量需要加密，并且可能需要跨越不受信任的网络进行传输。

### IPSec安全数据库

#### 安全策略数据库SPD

IPSec中的安全策略数据库（Security Policy Database，SPD）的作用是存储和管理与IPSec相关的安全策略信息。SPD中包含了一系列规则，用于定义如何对特定的网络流量进行加密、认证和访问控制。

SPD用于指定哪些流量需要被保护，哪些流量需要被拒绝，以及如何对这些流量进行处理。通过配置SPD，管理员可以定义允许或禁止特定的IP地址、协议、端口等相关信息，以确保网络流量的安全性。

SPD的作用包括：

1. IP选择：SPD可以定义哪些IP地址或地址范围可以被接受或拒绝。
2. 安全协议选择：SPD可以指定所使用的加密和认证协议，如ESP（Encapsulating Security Payload）和AH（Authentication Header），以保护IPSec通信。
3. 安全服务选择：SPD可以定义要应用的安全服务，如加密、认证和完整性保护。
4. 流量筛选：SPD可以基于源IP地址、目标IP地址、协议类型、端口号等参数对网络流量进行筛选和匹配。
5. 流量处理：SPD可以定义对匹配规则的流量的处理方式，如允许通过、拒绝、加密、解密等。

#### 安全关联数据库SAD

在IPSec协议中，安全关联数据库（SAD）存放了与IPSec安全通信相关的关键信息。这些信息对于确保通信的安全性和完整性至关重要。

SAD中存放的主要信息：

1. 安全关联（SA）条目：每一个安全关联在SAD中都有唯一的记录。这些记录包括SPI（安全参数索引）、目的IP地址和安全协议等标识信息，用于定位特定的安全关联。
2. 密钥信息：这是SAD中最关键的信息之一，包括用于加密和解密的密钥，以及用于完整性验证的密钥。这些密钥是在通信双方建立安全关联时协商确定的，用于保障数据的机密性和完整性。
3. 算法信息：SAD存储了当前安全关联所使用的加密算法和完整性校验算法。这些算法的选择对于通信的安全级别和性能有重要影响。
4. 包序列号：为了防止重放攻击，IPSec使用包序列号来确保每个数据包都是新鲜且未被篡改的。SAD中存储了每个安全关联的当前包序列号，以便在接收数据包时进行验证。

安全关联的生命周期：这包括安全关联的开始时间和结束时间，以及可能的软/硬限制（如数据包数量或字节数限制）。当安全关联达到其生命周期的终点或超过限制时，它将被视为无效，需要进行重新协商或更新

## MPLS VPN

### 定义

MPLS VPN使用BGP在运营商骨干网（IP网络）上发布VPN路由，使用MPLS在运营商骨干网上转发VPN报文。BGP/MPLS IP VPN又被简称为MPLS VPN，是一种常见的L3VPN（Layer 3 VPN）技术。

### MPLS VPN的网络结构

运营商和客户的路由器分为3类

* CE：用户网络边缘设备，用户网络直接与运营商网络相连。CE可以是路由器或交换机，也可以是一台主机。通常情况下，CE“感知”不到VPN的存在，也不需要支持MPLS。
* PE：运营商边缘路由器，是运营商网络的边缘设备，与CE直接相连。在MPLS网络中，对VPN的所有处理都发生在PE上，对PE性能要求较高。
* P：运营商网络中的骨干路由器，不与CE直接相连。P设备只需要具备基本MPLS转发能力，不维护VPN相关信息。

### MPLS VPN技术架构

* MP-BGP：负责在PE与PE之间传递站点内的路由信息。
* LDP：负责PE与PE之间的隧道建立
* VRF：负责PE的VPN用户管理。
* 静态路由、IGP、BGP：负责PE与CE之间的路由信息交换。

### MPLS VPN常见组网

* Intranet：一个VPN中的所有用户形成闭合用户群，同一VPN站点之间可以互访，不同VPN站点间不能互访。
* Extranet：适用于一个VPN用户希望提供部分本VPN的站点资源给其他VPN的用户访问的场景。
* Hub&Spoke：如果希望在VPN中设置中心访问控制设备，其它用户的互访都通过中心访问控制设备进行，可采用Hub&Spoke组网方案。

### MPLS VPN路由交互

#### 本地CE到入口PE

CE与PE之间可以使用静态路由、OSPF、IS-IS或BGP交换路由信息。无论使用哪种路由协议，CE和PE之间交换的都是标准的IPv4路由。

#### 入口PE到出口PE

##### VRF

VRF（Virtual Routing and Forwarding，虚拟路由转发），又称VPN实例，是MPLS VPN架构中的关键技术，每个VPN实例使用独立的路由转发表项，实现VPN之间的逻辑隔离。

##### RD（路由标识符）

必须在PE路由器的vpn实例中配置

作用:表示xxx用户

RD只对当前路由器有效

可以借助BGP把RD值传递给其他路由器，但其他路由器只记录但不起任何作用

RD值由2部分组成:

xxx:yyy

##### RT（路由标记）

作用:接收对端PE发来的数据，引入到某个vpn实例路由器

在PE上，每一个VPN实例都会与一个或多个VPN Target属性绑定，有两类VPN Target属性：

* Export Target（ERT）：本地PE从直接相连站点学到IPv4路由后，转换为VPN IPv4路由，并为这些路由添加Export Target属性。Export Target属性作为BGP的扩展团体属性随路由发布。
* Import Target（IRT）：PE收到其它PE发布的VPN-IPv4路由时，检查其Export Target属性。当此属性与PE上某个VPN实例的Import Target匹配时，PE就把路由加入到该VPN实例的路由表。
* 一边的出方向 = 另一边的入方向

该属性，随着BGP路由学习，通告给其他路由器。

RT值要求：2个PE设备之间配置一致

RT外观和配置位置与RD一样

BGP协议从VPN实例接收路由时，给路由添加扩展团体属性RT值。PE路由器利用VPNV4（MP-BGP）保持RT值不变，传送给另一端PE，PE利用BGP协议从VPN实例，向客户端传输路由时，会剥离RT值。

路由器添加和剥离RT值同时，会添加和剥离MPLS标签

#### 出口PE到远端CE

### 注意事项

MPLS VPN正式通讯时，在P向P设备传输数据时，携带2层标签

内层标签，PE用vpn实例，接收CE传来数据时，自动添加也叫v标，私网路由标签

使用BGP协议封装

外层标签，PE向P设备传来数据时，自动添加也叫T标，公网路由标签

使用MPLS LDP协议封装

### 配置步骤

#### 所有设备打通BGP

#### 路由器之间开启MPLS动态功能

系统视图

MPLS lsr-id X.X.X.X

MPLS

MPLS LDP

接口视图

MPLS

MPLS LDP

#### 2个路由器之间开通mp-bgp功能

BGP视图

ipv4-family vpnv4

Peer X.X.X.X enable

#### 配置用户RD值

IP vpn-instance bbb

ipv4-family

route-distinguisher 22:22

#### 配置RT值

IP vpn-instance bbb

ipv4-family

vpn-target 666：999 both

#### 如果PE与CE之间启用的是动态协议，需要从VPN实例中进入宣告

Ospf 1 vpn-instance bbb

A 0

Network x.x.x.x 反掩码

其他动态协议类似

#### 将VPN实例路由引入IGP路由

BGP视图

ipv4-family vpn-instance bbb

import-route ospf 1

**若是BGP邻居，直接将67合并，配置如下**

BGP视图

ipv4-family vpn-instance bbb

Peer x.x.x.x as-number 200

# MPLS（Multi-Protocol Label Switching，多协议标签交换）

## 基本概念

MPLS位于TCP/IP协议栈中的链路层和网络层之间（2.5层），用于向IP层提供连接服务，同时又从链路层得到服务。MPLS以标签交换替代IP转发。为其他高端能力提供数据转发基础。

## MPLS标签

标签是一个短而定长的、只具有本地意义的标识符，用于唯一标识一个分组所属的FEC。

Label

EXP

S

TTL

Label：20bit，标签值域。

Exp：3bit，用于扩展。现在通常用做CoS（Class of Service），其作用与Ethernet802.1p的作用类似。

BoS：1bit，栈底标识。MPLS支持多层标签，即标签嵌套。S值为1时表明为最底层标签。

TTL：8bit，和IP分组中的TTL（Time To Live）意义相同。

### MPLS标签栈

MPLS支持一层或多层标签头部，这些标签头部的有序集合被称为标签栈（Label Stack）。

当标签栈中存在多个标签时，这些标签的顺序是非常讲究的：

最靠近二层头部的标签是栈顶标签，标签中的S字段为0。

最靠近IP头部的标签是栈底标签，标签中的S字段为1。

### 标签空间

标签是一个短而定长的、只具有本地意义的标识符。标签空间就是指标签的取值范围。标签值的范围及规划如下：

|  |  |
| --- | --- |
| 标签值 | 描述 |
| 0~15 | 特殊标签值。例如0被定义为IPv4显式空标签（IPv4 Explicit NULL Label），标签值3被定义为隐式空标签（Implicit NULL Label） |
| 16~1023 | 用于静态LSP、静态CR-LSP的共享标签空间 |
| 1024~1048575 | LDP、RSVP-TE、MP-BGP等动态信令协议的标签空间；  动态信令协议的标签空间不是共享的，而是独立且连续的，互不影响 |

## LSR（Label Switching Router，标签交换路由器）

LSR，支持mpls功能的路由器

每个路由器为目标网段分配的标签可以不同

标签必须让路由器和邻居路由器有效

### ingress路由器

也叫入站路由器

作用:在ip头部前面添加MPLS标签，该操作也叫压入

### transit路由器

也叫中转路由器

作用:更换标签信息，该操作也叫交换、替换

### egress路由器

也叫出站路由器

作用:剥离MPLS标签还原成普通ip数据包，该操作也叫弹出

注意:路由器必须先在ip路由表中有记录，才能给目标网段分配标签

## FEC（Forwarding Equivalence Class，转发等价类）

每个路由器为相同的FEC分配的标签，合并形成标签数据传输路径

* 相当于最优路由
* LSP是单向的，需要建立双向的LSP路径

## LSP（Label Switched Path，标签交换路径）

标签报文穿越MPLS网络到达目的地所走的路径。

### 静态LSP

#### 基本概念：

静态LSP是用户通过手工为各个FEC分配标签而建立的。

静态LSP不使用标签发布协议，不需要交互控制报文，因此消耗资源比较小。

通过静态方式建立的LSP不能根据网络拓扑变化动态调整，需要管理员干预。

#### 应用场景：

适用于拓扑结构简单并且稳定的小型网络。

#### 标签分配原则：

前一节点出标签的值等于下一个节点入标签的值。

### 动态LSP

#### 基本概念：

动态LSP通过标签发布协议动态建立。

标签发布协议是MPLS的控制协议（也可称为信令协议），负责FEC的分类、标签的分发以及LSP的建立和维护等一系列操作。

#### 标签分发协议 (LDP)

##### 定义

LDP是多协议标签交换MPLS的一种控制协议，负责转发等价类FEC的分类、标签的分配以及标签交换路径LSP的建立和维护等操作。

##### LDP ID组成

1. LSR ID（32bit）
2. 16bit标签空间标识符（Label Space ID）16bit

标签空间标识一般存在两种形态：

* 值为0：表示基于设备（或基于平台）的标签空间；

意味着向所有邻居通告同一个Ec时，标签号一样

* 值非0：表示基于接口的标签空间。

意味着向不同邻居通告同一个FEC时，标签号不同

##### LDP报文

1. 发现消息（Discovery Message）
2. 会话消息（Session Message）
3. 通告消息（Advertisement Message）
4. 通知消息（Notification Message）

发现消息he1llo报文，作用:发现1dp邻居基于UDP协议，端口号646

其余LDP报文，都是基于TCP协议，端口号646

##### 标签的发布和管理

###### 标签分配方式

作用:哪台路由器为目标网段分配标签

独立方式（Independent）

特点:无需接收下游LSR路由器发出的标签，主动向上游通告目标网段标签

有序方式（Ordered）

默认方式

特点:从最下游LSR路由器开始，依次向土游通告目标网段标签

###### 标签发布方式

作用:路由器如何向邻居通告标签

下游自主方式（Downstream Unsolicited，DU）

默认模式

特点:下游路由器主动把目标网段标签，通告给上游路由器

下游按需方式（Downstream on Demand，DoD）

特点:下游路由器收到上游路由器请求后，把目标网段标签通告给上游

###### 标签保存方式

作用:路由器如何保存学到的标签

自由方式（Liberal）

保存从任何邻居学到的标签

保守方式（Conservative）

只保存从最优下一跳路由器发送的目标网段标签

#### PHP（Penultimate Hop Popping，次末跳弹出）

最末端出站路由器，把目标网段设置为特殊标签3(叫隐式空标签)，并通告给倒数第二跳路由器，倒数第二跳路由器把数据包中的标签剥离后，发送给末端出站路由器。

上述操作会导致MPLS标签在向末端路由器发送时，失去Qos分类功能

解决办法：

向末端路由器发送报文保持带标签，使用Qos分类功能需要把标签改为0(叫显式空标签)

末端路由器不做任何检查，直接剥离标签

出口路由器配置命令

[r1-mpls]label advertise explicit-null --配置显式空标签

[r1-mpls]label advertise implicit-null --配置隐式空标签

[r1-mpls]label advertise non-null --使用正常标签

## MPLS标签转发（3个表）

### FTN（FEC-to-NHLFE）

作用:判断是否需要添加标签

只用在入站LSR路由器

入站LSR路由器根据FIB(转发信息库)中，目标网段的tunnelrp字段，判断是否需要执行标签转发

tunnelID不等于0，表示执行MPLS标签转发

tunnelIp等于0，表示执行标准的ip路由

### 下一跳标签转发表项NHLFE（Next Hop Label Forwarding Entry）

作用:添加、更换标签

入站LSR、中转LSR路由器都需要用到

### 入标签映射ILM（Incoming Label Map）

作用:更换、剥离标签

中转LSR、出站LSR路由器都需要用到

操作时，主要看FIB表，LSP标签转发表

## MPLS体系结构

### 控制平面

控制平面是无连接的，主要功能是负责产生和维护路由信息以及标签信息。

控制平面包括：

路由信息表RIB（Routing Information Base）：由IP路由协议（IP Routing Protocol）、静态路由和直连路由共同生成，用于选择路由。

标签信息表LIB（Label Information Base）：用于管理标签信息，LIB中的表项可由标签交换协议（LDP、RSVP等协议）或静态配置生成。

### 转发平面

转发平面也称为数据平面，是面向连接的， 主要功能是负责普通IP报文的转发以及带MPLS标签报文的转发。

转发平面包括：

转发信息表FIB（Forwarding Information Base）：从RIB提取必要的路由信息生成，负责普通IP报文的转发。

标签转发信息表LFIB（Label Forwarding Information Base）：简称标签转发表，负责带MPLS标签报文的转发。

## 静态MPLS配置步骤：

a、系统视图下，启动mpls

b、接口视图下，开启mpls转发能力

注意：只需要在非终端接口开启

b、给目标网段手动指定标签



[R1]mpls lsr-id 10.1.1.1

[R1]mpls

[R1-mpls]quit

[R1]interface GigabitEthernet 0/0/0

[R1-GigabitEthernet0/0/0]mpls

[R1-GigabitEthernet0/0/0]quit]

[R1] static-lsp ingress 1 destination 3.3.3.3 24 nexthop 10.0.12.2 out-label 200

[R1] static-lsp egress 2 incoming-interface GigabitEthernet 0/0/0 in-label 200

[R2] static-lsp transit 1 incoming-interface GigabitEthernet 0/0/0 in-label 200 nexthop 10.0.23.3 out-label 300

[R2] static-lsp transit 2 incoming-interface GigabitEthernet 0/0/1 in-label 300 nexthop 10.0.12.1 out-label 200

[R3] static-lsp egress 1 incoming-interface GigabitEthernet 0/0/0 in-label 300

[R3]static-lsp ingress 2 destination 1.1.1.1 24 nexthop 10.0.23.2 out-label 300

# VRF（Virtual Routing and Forwarding，虚拟路由转发）

## 概念

VRF（Virtual Routing and Forwarding，虚拟路由转发）技术通过在一台三层转发设备上创建多张路由表实现数据或业务的隔离，常用于MPLS VPN、防火墙等一些需要实现隔离的应用场景。

## VRF的实现过程

VRF是对物理设备的一个逻辑划分，每个逻辑单元都被称为一个VPN实例，实例之间在路由层面是隔离的。VRF实现过程如下：

1. 创建实例，并将三层接口（可以是路由器的物理接口或者子接口，也可以是VLANIF接口）绑定到实例；
2. （可选）配置与实例绑定的路由协议或静态路由；
3. 基于与实例绑定的接口和路由协议等建立实例路由表并基于实例路由表转发数据，实现实例间隔离。

# 以太网交换安全

## DHCP Snooping

### 概述

DHCP Snooping是DHCP的一种安全特性，用于保证DHCP客户端从合法的DHCP服务器获取IP地址。DHCP 服务器记录DHCP客户端IP地址与MAC地址等参数的对应关系，防止网络上针对DHCP攻击。

### DHCP Snooping信任功能

#### 信任接口

信任接口正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文。

#### 不可信接口

非信任接口收到的DHCP Server发送的DHCP OFFER、DHCP ACK、DHCP NAK报文会被直接丢弃。M

#### 命令

系统视图

DHCP enable

dhcp snooping enable ipv4

接口视图

[Huawei-Ethernet0/0/2]dhcp snooping enable

[Huawei-Ethernet0/0/2]dhcp snooping trusted

[Huawei-Ethernet0/0/3]dhcp snooping enable

注意：开启snooping后，接口默认是不可信状态

### DHCP饿死攻击

攻击原理：

攻击者持续大量地向DHCP Server申请IP地址，直到耗尽DHCP Server地址池中的IP地址，导致DHCP Server不能给正常的用户进行分配。

解决方法：

对于饿死攻击，可以通过DHCP Snooping的MAC地址限制功能来防止。该功能通过限制交换机接口上允许学习到的最多MAC地址数目，防止通过变换MAC地址，大量发送DHCP请求。

### 改变CHADDR值的DoS攻击

攻击原理：

攻击者持续大量地向DHCP Server申请IP地址，直到耗尽DHCP Server地址池中的IP地址，导致DHCP Server不能给正常的用户进行分配。

解决方法：

为了避免受到攻击者改变CHADDR值的攻击，可以在设备上配置DHCP Snooping功能，检查DHCP Request报文中CHADDR字段。如果该字段跟数据帧头部的源MAC相匹配，转发报文；否则，丢弃报文。从而保证合法用户可以正常使用网络服务。

### DHCP中间人攻击

攻击原理：

攻击者利用ARP机制，让Client学习到DHCP Server IP与Attacker MAC的映射关系，又让Server学习到Client IP与Attacker Mac的映射关系。

解决方法：

为防御中间人攻击与IP/MAC Spoofing攻击，可使用DHCP Snooping的绑定表工作模式，当接口接收到ARP或者IP报文，使用ARP或者IP报文中的“源IP+源MAC”匹配DHCP Snooping绑定表。如果匹配就进行转发，如果不匹配就丢弃。

## IP源防攻击（IPSG，IP Source Guard）

### 基本概念

是一种基于二层接口的源IP地址过滤技术。它能够防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址的方式来访问网络或攻击网络。

### 工作原理

IPSG利用绑定表（源IP地址、源MAC地址、所属VLAN、入接口的绑定关系）去匹配检查二层接口上收到的IP报文，只有匹配绑定表的报文才允许通过，其他报文将被丢弃。常见的绑定表有静态绑定表和DHCP Snooping动态绑定表。

### IPSG应用场景

#### 通过IPSG防止PC私自更改IP地址。

PC只能使用DHCP Server分配的IP地址或者管理员配置的静态地址，随意更改IP地址后无法访问网络，防止PC非法取得上网权限。

#### 小型网络IP地址是静态分配时，通过IPSG限制非法PC接入。

外来人员自带电脑不能随意接入内网，防止内网资源泄露。

## 交换机端口镜像

作用:

把某些接口的数据复制到另一个接口上

使用场景:

监控网络数据、检验数据是否异常、流量审计

交换机接口分2类:

a、镜像口

被监控的接口，提供原始的数据

b、监视口

接收镜像口数据，发送给监控主机

# 网络割接

割接的流程步骤

1. 网络规划：在进行网络割接之前，需要对现有网络进行规划和评估，确定网络割接的具体方案。这包括确定升级的网络架构、设备需求以及业务迁移计划等。
2. 预备工作：在进行网络割接之前，需要完成一系列的预备工作，例如备份数据、调整路由和优化网络配置等。这些工作的目的是确保网络割接过程的稳定性和安全性。
3. 割接测试：在正式进行网络割接之前，需要进行详细的测试和模拟操作，以检测系统是否能够正常工作。这包括网络连接测试、业务功能测试和数据传输测试等，以确保网络割接不会影响到用户的正常使用。
4. 割接过程：在进行网络割接过程中，需要按照预先制定的计划逐步进行。这意味着需要有一个明确的时间表和步骤，以确保业务连续性和数据安全性。同时，需要密切监控割接过程中的变化和问题，并及时采取措施进行修复。
5. 后续检测和维护：在完成网络割接之后，需要进行详细的检测和维护工作。这包括监测网络性能、检查业务连通性以及及时修复可能存在的问题。这一步骤的目的是确保网络的稳定性和可用性。

网络割接的好处是显而易见的。它可以帮助企业顺利升级网络架构，提升网络的稳定性和可用性。同时，网络割接也为企业实现业务的迁移和扩展提供了便利。

然而，网络割接也存在一定的风险。如果割接不当，可能会导致业务中断和数据丢失等问题。因此，在进行网络割接时需要格外谨慎，确保每个步骤都经过充分的测试和备份，并及时修复可能存在的问题。

# QoS，服务质量

延时时间，达标小于200ms

网络稳定，丢包率小于5%

## 设备转发数据的3种方案：

a、尽力而为型

默认转发方案，按照先进先出方式转发数据

b、区分服务型

实现把数据分类，并提前预留足够资源

缺点：预留的资源不能被其他类型数据使用

c、差分服务型

数据分类并设置转发时使用的资源

## QoS设置2种对象：

a、限速

b、资源最小使用带宽

## 华为QoS限速手段有3种

a、接口限速

针对所有类型数据设置限速值

b、流量整形

针对出口的速率做限速

特点：超出限制的数据放入缓冲区，稍后发送

也叫消峰填谷

c、流量监管

可以在入口、出口上做限速

特点：超出限制的数据可以直接丢弃

## 流量整形、流量监管的限速原理

利用令牌桶生成令牌速度限速

令牌是数据传输的依据

### 令牌桶限速有3种类型

a、单速单桶

数据从1个令牌桶取令牌，有足够令牌数据标记为绿色并放行

没有足够令牌数据标记为红色并禁止通行

不适合突发流量场景

b、单速双桶

有2个令牌桶：C桶和E桶

使用1个令牌生成速度向2个桶补充令牌

令牌生成速度，叫CIR（信息承诺速率）

原理：

a、数据先从C桶取令牌，如果有足够令牌，数据标记为绿色并放行

b、C桶令牌不足时，从E桶取足够的令牌，数据标记为黄色并放行

c、C桶和E桶令牌不足时，数据标记为红色并禁止通行

c、双速双桶

通常双筒中另一个令牌桶会比较大，可以应对突发大流量

### 流量整形、流量监管配置命令

a、接口直接配置

b、利用MQC配置

## 拥塞避免，数据拥堵时如何缓解

拥塞避免实现的办法有2种：

a、尾丢弃

拥堵之后的数据全部丢弃

默认方法

会导致TCP连接不稳定、不断重复

b、加权随机预丢弃

特点：从排队的队列中，随机丢弃低优先级的数据

为队列设置不同优先级数据，丢弃概率和丢弃阈值

丢弃阈值，队列拥堵程度，开始丢弃数据

丢弃概率，丢弃数据的程度，一般设置下限值和上限值

当队列拥挤程度不到100%，执行丢弃上限值

当队列拥挤程度100%，执行100%丢弃

### 拥塞管理

数据按照条件分队列

队列分2种：

a、内部优先级队列

=接口的队列

所有接口内置8个队列，编号0-7

b、外部优先级队列

=数据包中的队列值

现阶段，只有IP数据包、VLAN数据包、MPLS数据包，内置优先级字段

MPLS和VLAN数据包，包头中优先级字段总长3bit，共8种组合

与接口队列一一对应

其中，VLAN数据包如果有优先级设置，该数据包用802.1p封装

IP数据包优先级字段，总长8bit，细分2种使用方式

1）只使用前3bit

早期的方式

也叫IP优先级

2）使用前6bit

新型方式

也叫DSCP，差分服务代码点

### 外部优先级队列设置名称：

a、CS6和CS7

最高级的队列

通常用来传递路由控制报文

b、CS5

也叫EF，快速转发队列

通常用来传输语音数据

c、CS4

d、CS3

e、CS2

f、CS1

CS4-CS1，也叫AF，确保转发队列

AF队列由2个数字组成

AF11中，第一个数字表示队列，第二个数字表示丢弃概率，数字越大丢弃概率越高

g、CS0

也叫BF，尽力而为队列

各队列之间通过调度，控制队列数据发送顺序

### 常见的调度算法有3种：

a、RR轮询算法

所有队列依次使用接口发送相同大小的数据

b、PQ，优先级队列算法

特点：先发送高优先级队列数据，高优先级队列空时，再发低优先级队列数据

c、WFQ，加权公平队列算法

特点：每个队列设置权重，根据权重比例决定发送的数据量

动态根据队列数据量，调整队列占用的带宽

通常情况下，CS6和CS7队列使用PQ调度法，其他队列使用WFQ调度法