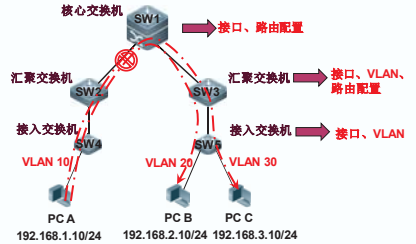




## 访问控制列表（ACL）原理及配置

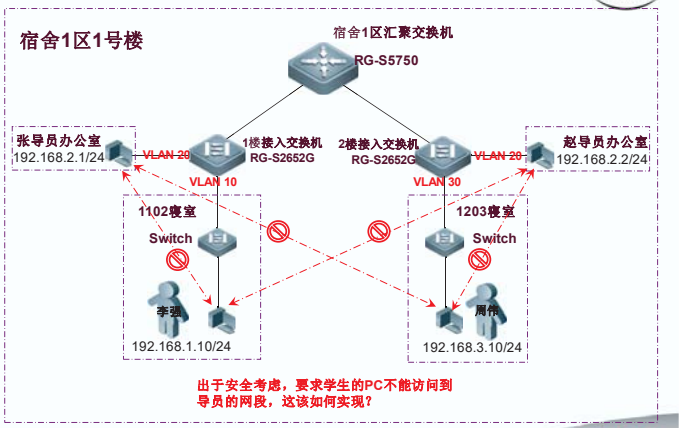
- 什么时候使用访问控制列表？
  - 默认情况下，接入交换机、汇聚交换机、核心交换机完成如下图所示的关键配置，不同VLAN内的PC即可以相互通信，如果想要控制两个VLAN内的数据交互，又不能影响与其他VLAN的数据交互，比如要求PC A只能访问PC B,而不能访问PC C。在这种情况下，就需要使用访问控制列表







## 场景描述

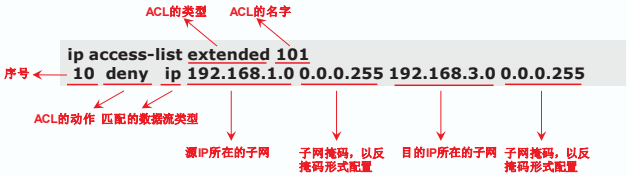





## 访问控制列表（ACL）原理及配置

- 访问控制列表的配置
  - Access Control Lists：简称ACL，最直观的用途是用一些语句来标识数据流
    - 比如禁止PCA 192.168.1.10访问PC B 192.168.3.10的数据流，使用下面的配置方法进行配置
      - 类型、命名、动作、数据流协议类型、源目的IP所在子网、子网掩码等

```
Ruijie(config)#ip access-list extended 101
Ruijie(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
```



## 访问控制列表（ACL）原理及配置

- 常用的访问控制列表的类型
  - › IP标准ACL：只能匹配IP数据包头中的源IP地址
    - » 配置ACL的时候使用"standard"关键字
  - › IP扩展ACL：匹配源IP/目的IP、协议（TCP/IP）、协议信息（端口号、标志代码）等
    - » 配置ACL的时候使用"extended"关键字
  - › 除了上面两种常用的类型外，还存在以下其他的ACL类型及能够匹配的协议类型

| ACL 类型 | 可匹配内容 |
|---|---|
| IP 标准 ACL | 源 IP |
| IP 扩展 ACL | 源 IP，目的 IP，ICMP type，ICMP code，TCP、UDP 端口号 Fragment，TOS，DSCP，Precedence |
| MAC 扩展 ACL | 源 MAC，目的 MAC，COS，协议字段(包括各种协议) |
| 专家级 ACL | IP 扩展可匹配内容，MAC 扩展可匹配内容，VID，inner VID，inner COS |
| 自定义 ACL(ACL80) | 专家级 ACL 可匹配内容，报文前 80 字节的任何内容 |
| IPV6 ACL | 源 IP，目的 IP，ICMP type，ICMP code，TCP、UDP 端口号，fragment，DSCP，flow-label |



## 访问控制列表（ACL）原理及配置

- 访问控制列表的命名
  - › 数字命名
    - » 默认的命名，需要注意标准和扩展两种类型ACL的数字命名范围是不一样的
  - › 自定义名称
    - » 定义更具有代表意义的名称，推荐使用。比如禁止VLAN10内的PC访问VLAN30，可以定义为DENY_VLAN10_TO_VLAN30，这样可以一目了然地知道所配置的ACL是为什么需求服务的。

```
Ruijie(config)#ip access-list standard ?
  <1-99>          IP standard acl
  <1300-1999>   IP standard acl (expanded range)
  WORD            Acl name
```

```
Ruijie(config)#ip access-list extended ?
  <100-199>       IP extended acl
  <2000-2699>   IP extended acl (expanded range)
  WORD            Acl name
```



## 访问控制列表（ACL）原理及配置

- 访问控制列表的动作
  - › 分为两种：permit和deny
    - » permit：允许permit后面语句匹配的数据流通过
    - » deny：禁止deny后面语句匹配的数据流通过



## 访问控制列表（ACL）原理及配置

- 访问控制列表中数据流类型
  - › 标准ACL和扩展ACL能够匹配的数据流类型不同
    - » 标准ACL：仅匹配数据包的源IP地址

```
Ruijie(config)#ip access-list standard 13
Ruijie(config-std-nacl)#permit ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

- » 扩展ACL：能够匹配3层及以上多种协议，并且可以同时匹配源IP和目的IP

```
Ruijie(config)#ip access-list extended 101
Ruijie(config-ext-nacl)#permit ?
  <0-255>  An IP protocol number
  eigrp    Enhanced Interior Gateway Routing Protocol
  gre      General Routing Encapsulation
  icmp     Internet Control Message Protocol
  igmp     Internet Group Managment Protocol
  ip       Any Internet Protocol
  ipinip   IP In IP
  nos      NOS
  ospf     Open Shortest Path First
  tcp      Transmission Control Protocol
  udp      User Datagram Protocol
```



## 访问控制列表（ACL）原理及配置

- 访问控制列表中子网与反掩码配置
  - › 定义数据流的源IP或目的IP所在子网号及掩码
    - » 在访问控制列表中子网号的掩码是采用反掩码的形式，在配置静态路由时，使用的就为“正掩码”

```
ip route 192.168.1.0 255.255.255.0 10.0.0.1
```

正掩码，换算为2进制后，如果某一位为1的话，表示报文目的IP的对应bit位需要与子网号中对应的bit位进行对比

```
Ruijie(config)#ip access-list standard 13
Ruijie(config-std-nacl)#permit 192.168.1.0 0.0.0.255
```

反掩码，换算为2进制后，如果某一位为0的话，表示报文目的IP的对应bit位需要与子网号中对应的bit位进行对比

```
Ruijie(config)#ip access-list standard 13
Ruijie(config-std-nacl)#permit 192.168.1.10 0.0.0.0
```

反掩码配置成全0，表示匹配的是一个主机IP，也可以使用host进行定义

```
Ruijie(config-std-nacl)#permit host 192.168.1.10
```



## 访问控制列表（ACL）原理及配置

- 访问控制列表中子网与反掩码配置
  - › 课堂练习
    - » 192.168.1.0/17和192.168.1.0/25所对应的反掩码分别是多少？

## 访问控制列表（ACL）原理及配置

- 访问控制列表中配置多条语句
  - 若存在多种不同的访问控制需求，就需要在一个ACL中定义多条语句
    - 不允许VLAN10内的PC访问192.168.4.0/24内的所有PC
    - 不允许VLAN10内的PC访问192.168.5.0/24内的所有PC
    - 仅允许VLAN 10内的特定PC（192.168.1.10）访问 192.168.3.0/24内的所有PC
    - 允许VLAN 10内PC仅可以访问10.0.5.5的80端口
    - 其他数据流放行
  - 配置思路
    - 1.首先确定是采用标准还是扩展ACL
    - 2.确定配置ACL中多条语句的顺序
      - 将格式相同（动作、数据流类型、子网号、反掩码等）的语句放置在一起配置
      - 根据需求配置多条语句时，要确认所配置的顺序能否满足需求



## 访问控制列表（ACL）原理及配置

- 访问控制列表中配置多条语句
  - 若存在多种不同的访问控制需求，就需要在一个ACL中定义多条语句
    - 不允许VLAN10内的PC访问192.168.4.0/24内的所有PC
    - 不允许VLAN10内的PC访问192.168.5.0/24内的所有PC
    - 仅允许VLAN 10内的特定PC（192.168.1.10）访问 192.168.3.0/24内的所有PC
    - 允许VLAN 10内PC仅可以访问10.0.5.5的tcp 80端口
    - 其他数据流放行

```
Ruijie(config)#ip access-list extended FOR_VLAN10
Ruijie(config-ext-nacl)#permit ip host 192.168.1.10 192.168.3.0 0.0.0.255
Ruijie(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
Ruijie(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.5.0 0.0.0.255
Ruijie(config-ext-nacl)#permit tcp 192.168.1.0 0.0.0.255 host 10.0.5.5 eq 80
Ruijie(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 host 10.0.5.5
Ruijie(config-ext-nacl)#per ip any any
```



## 访问控制列表（ACL）原理及配置

- 访问控制列表中配置多条语句
  - 序列号的作用
    - 自动生成的序号，默认以10位单位递增。也可以在配置ACL中的语句时提前添加不同的序号。序列号的作用，方便后续添加维护语句

```
ip access-list extended FOR_VLAN10
 10 permit ip host 192.168.1.10 192.168.3.0 0.0.0.255
 20 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
 30 deny ip 192.168.1.0 0.0.0.255 192.168.5.0 0.0.0.255
 40 permit tcp 192.168.1.0 0.0.0.255 host 10.0.5.5 eq www
 50 deny ip 192.168.1.0 0.0.0.255 host 10.0.5.5
 60 permit ip any any
```

    - 新增需求：禁止VLAN 10内的PC访问192.168.6.0/24

```
Ruijie(config)#ip access-list extended FOR_VLAN10
Ruijie(config-ext-nacl)#31 deny ip 192.168.1.0 0.0.0.255 192.168.6.0 0.0.0.255
```

```
ip access-list extended FOR_VLAN10
 10 permit ip host 192.168.1.10 192.168.3.0 0.0.0.255
 20 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
 30 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
 31 deny ip 192.168.1.0 0.0.0.255 192.168.6.0 0.0.0.255
 40 permit tcp 192.168.1.0 0.0.0.255 host 10.0.5.5 eq www
 50 deny ip 192.168.1.0 0.0.0.255 host 10.0.5.5
 60 permit ip any any
```



## 访问控制列表（ACL）原理及配置

- 访问控制列表中配置多条语句
  - 每一条语句也称为ACE，访问控制表项(Access Control Entry：ACE)
    - ACE匹配的顺序为从上至下，即编号从低到高进行匹配
    - 一旦被某条ACE匹配成功（无论动作是deny或permit），跳出该ACL
    - 如果ACL中没有配置一条ACE，则相当于允许所有数据包
    - 如果ACL中配置了语句，那么将存在一条默认ACL deny ip any any（不显示）

```
ip access-list extended FOR_VLAN10
 10 permit ip host 192.168.1.10 192.168.3.0 0.0.0.255
 20 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
 30 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
 31 deny ip 192.168.1.0 0.0.0.255 192.168.6.0 0.0.0.255
 40 permit tcp 192.168.1.0 0.0.0.255 host 10.0.5.5 eq www
 50 deny ip 192.168.1.0 0.0.0.255 host 10.0.5.5
 60 permit ip any any
```

一个ACL中包含多个ACE



## 访问控制列表（ACL）原理及配置

- 访问控制列表中配置多条语句
  - 多条ACE的配置顺序
    - 不能将编号为60的ACE放到前面，否则一些deny动作的ACE将失去作用
    - 也不能将编号为50的ACE放到40的前面，否则将无法访问10.0.5.5
      - 需求：允许VLAN 10内PC仅可以访问10.0.5.5的80端口

```
ip access-list extended FOR_VLAN10
 10 permit ip host 192.168.1.10 192.168.3.0 0.0.0.255
 20 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
 30 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
 31 deny ip 192.168.1.0 0.0.0.255 192.168.6.0 0.0.0.255
 40 permit tcp 192.168.1.0 0.0.0.255 host 10.0.5.5 eq www
 50 deny ip 192.168.1.0 0.0.0.255 host 10.0.5.5
 60 permit ip any any
```



## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 1.在接口上调用已经配置好的ACL
    - 数据流是从交换机的接口出入，如果所配置的ACL想要发挥作用，就需要将配置好的ACL应用在接口上,接口可以是物理接口也可以是SVI。应用的方向根据ACL的内容以及数据流进入接口的方向进行配置选择

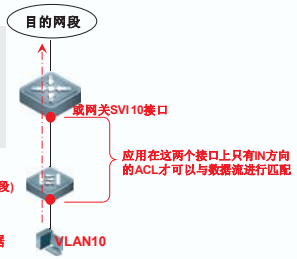
```
Ruijie(config)#int f0/1
Ruijie(config-FastEthernet 0/1)#ip access-group FOR_VLAN10 in
```

```
Ruijie(config)#int vlan 10
Ruijie((config-VLAN 10)#ip access-group FOR_VLAN10 out
```

## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 1.在接口上调用已经配置好的ACL
    - 数据流是从交换机的接口出入，如果所配置的ACL想要发挥作用，就需要将配置好的ACL应用在接口上,接口可以是物理接口也可以是SVI。应用的方向根据ACL的内容以及数据流进入接口的方向进行配置选择

```
ip access-list extended FOR_VLAN10
 10 permit ip host 192.168.1.10 192.168.3.0 0.0.0.255
 20 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
 30 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
 31 deny ip 192.168.1.0 0.0.0.255 192.168.6.0 0.0.0.255
 40 permit tcp 192.168.1.0 0.0.0.255 host 10.0.5.5 eq www
 50 deny ip 192.168.1.0 0.0.0.255 host 10.0.5.5
 60 permit ip any any
```



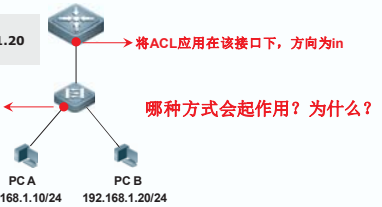

接口上配置in方向的ACL会对流入该接口的数据流进行匹配，在实际中多采用in方向应用ACL



## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 2.在什么设备上配置ACL
    - 二层交换机（接入）、三层交换机（汇聚网关）均支持ACL配置，那么在哪台设备上应用ACL呢？需要结合实际的需求来判断将ACL应用在什么层次的设备上
      - 控制VLAN内的数据流，则需要在接入交换机上配置ACL

```
ip access-list extended FOR_VLAN10
 10 deny ip host 192.168.1.10 host 192.168.1.20
 20 permit ip any any
```




哪种方式会起作用？为什么？

控制PC A无法访问PC B



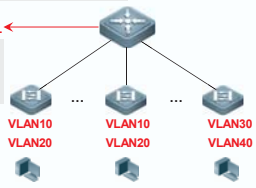
## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 2.在什么设备上配置ACL
    - 二层交换机（接入）、三层交换机（汇聚网关）均支持ACL配置，那么在哪台设备上应用ACL呢？需要结合实际的需求来判断将ACL应用在什么层次的设备上
      - 控制跨网段转发的数据路，建议在汇聚网关上配置ACL，这样可以减少配置量

```
ip access-list extended FOR_VLAN10（为VLAN20配置的ACL略）
 10 deny ip 192.168.1.0 0.0.0.255  192.168.3.0 0.0.0.255
 20 permit ip any any
```

在网关交换机的SVI下配置ACL

```
Ruijie(config)#int vlan 10
Ruijie((config-VLAN 10)#ip access-group FOR_VLAN10 in
Ruijie(config)#int vlan 20
Ruijie((config-VLAN 20)#ip access-group FOR_VLAN20 in
```




仅需要在网关交换机的网关SVI接口下配置，配置工作量大大减少，并方便维护

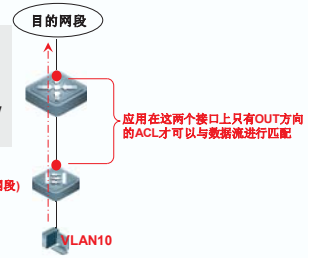
控制VLAN 10内的PC不能访问VLAN 30
控制VLAN 20内的PC不能访问VLAN 40



## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 1.在接口上调用已经配置好的ACL
    - 数据流是从交换机的接口出入，如果所配置的ACL想要发挥作用，就需要将配置好的ACL应用在接口上,接口可以是物理接口也可以是SVI。应用的方向根据ACL的内容以及数据流进入接口的方向进行配置选择

```
ip access-list extended FOR_VLAN10
 10 permit ip host 192.168.1.10 192.168.3.0 0.0.0.255
 20 deny ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255
 30 deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255
 31 deny ip 192.168.1.0 0.0.0.255 192.168.6.0 0.0.0.255
 40 permit tcp 192.168.1.0 0.0.0.255 host 10.0.5.5 eq www
 50 deny ip 192.168.1.0 0.0.0.255 host 10.0.5.5
 60 permit ip any any
```




接口上配置OUT方向的ACL会对流出该接口的数据流进行匹配



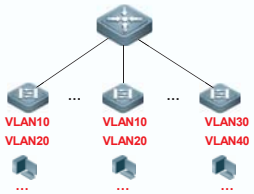
## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 2.在什么设备上配置ACL
    - 二层交换机（接入）、三层交换机（汇聚网关）均支持ACL配置，那么在哪台设备上应用ACL呢？需要结合实际的需求来判断将ACL应用在什么层次的设备上
      - 控制跨网段转发的数据路，建议在汇聚网关上配置ACL，这样可以减少配置量

```
ip access-list extended FOR_VLAN10（为VLAN20配置的ACL略）
 10 deny ip 192.168.1.0 0.0.0.255  192.168.3.0 0.0.0.255
 20 permit ip any any
```

如果将ACL配置在接入交换机上
1.需要在多台交换机上配置
2.需要明确接入交换机哪个端口属于VLAN10，哪个端口属于VLAN20

配置工作量较大，而且容易出错




控制VLAN 10内的PC不能访问VLAN 30
控制VLAN 20内的PC不能访问VLAN 40



## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 3.ACL是在靠近源的设备上应用还是靠近目的的设备上应用
    - 需要结合ACL的类型以及实际的应用、配置的工作量进行考虑
      - 标准ACL（匹配源地址），在靠近报文目的的设备上进行配置


如果应用在靠近数据源的设备上，会有什么问题？

使用标准ACL控制PCA不能访问PC B

```
ip access-list standard AtoB
 10 deny 192.168.1.0 0.0.0.255
 20 permit ip any any
```

## 访问控制列表（ACL）原理及配置

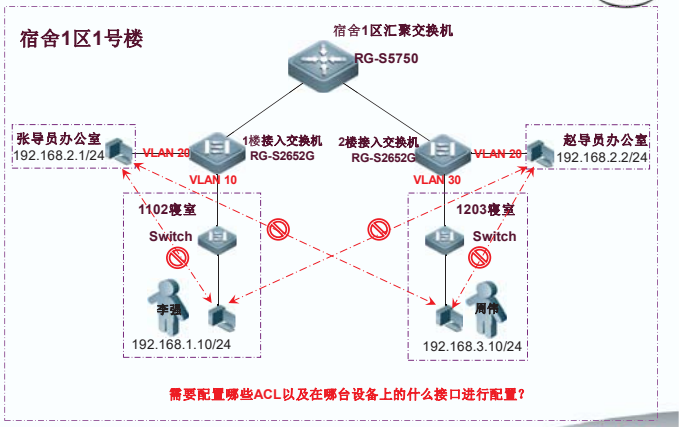
- 访问控制列表的应用位置
  - 3.ACL是在靠近源的设备上应用还是靠近目的的设备上应用
    - 需要结合ACL的类型以及实际的应用、配置的工作量进行考虑
      - 扩展ACL（匹配目的地址），建议在靠近报文源的设备上进行配置


使用扩展ACL控制PCA不能访问PC B

```
ip access-list extended AtoB
10 deny ip 192.168.1.0 0.0.0.255  10.1.1.0 0.0.0.255
20 permit ip any any
```



## 场景回顾与思考




需要配置哪些ACL以及在哪台设备上的什么接口进行配置？



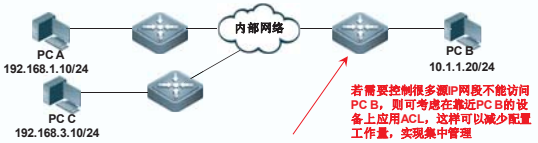
## 访问控制列表（ACL）原理及配置

- 基于时间的ACL
  - 可以实现所配置的ACL只在一个特定的时间段内生效
    - 如在办公时间（9：00-18：00）只允许访问WEB网页，其他应用则被禁止。除了办公时间外，任何网络应用都可以使用
      - 注，类似这种基于时间的应用控制，由于实际中涉及的应用类型比较复杂，因此多在出口位置采用专用的设备进行控制
    - 配置方法
      - 1.正确配置设备时间
        - 在#模式下使用clock set命令设置
      - 2.定义时间段
      - 3.为ACL中的特定ACE关联定义好的时间段



## 访问控制列表（ACL）原理及配置

- 访问控制列表的应用位置
  - 3.ACL是在靠近源的设备上应用还是靠近目的的设备上应用
    - 需要结合ACL的类型以及实际的应用、配置的工作量进行考虑
      - 扩展ACL（匹配目的地址），建议在靠近报文源的设备上进行配置
        - 如果想集中控制的话，也可以在报文目的设备上进行配置




使用扩展ACL控制PCA和PC C 不能访问PC B

```
ip access-list extended toB
10 deny ip 192.168.1.0 0.0.0.255  10.1.1.0 0.0.0.255
20 deny ip 192.168.3.0 0.0.0.255  10.1.1.0 0.0.0.255
30 permit ip any any
```



## 访问控制列表（ACL）原理及配置

- 访问控制列表的其他用途
  - 防病毒应用
    - 在实际中除了使用ACL控制网段之间的互访外，还有一种比较常见的用法，就是封闭常见的病毒或木马占用的端口，并在三层网关SVI接口下应用，如下的防病毒ACL配置。
      - 防病毒的ACL也可能会与某些应用的端口号重合，实施时需要注意
      - 控制互访和防病毒两种应用在实际中也多结合在一起，因此在配置的时候需要注意ACE的先后顺序

```
ip access-list extended antivirus
 10 deny tcp any any eq 1068
 20 deny tcp any any eq 5554
 30 deny tcp any any eq 9995
 40 deny tcp any any eq 9996
 50 deny tcp any any eq 1022
 60 deny tcp any any eq 1023
 70 deny tcp any any eq 445
 80 deny tcp any any eq 135
 90 deny tcp any any eq 4444
 100 deny tcp any any eq 1080
 110 deny tcp any any eq 3128
...(省略部分)
280 permit ip any any
```



## 访问控制列表（ACL）原理及配置

- 基于时间的ACL
  - 可以实现所配置的ACL只在一个特定的时间段内生效
    - 配置方法
      - 2.定义时间段

```
Ruijie(config)#time-range WORK_TIME
Ruijie(config-time-range)#periodic ?
  Daily      Every day of the week
  Friday     Friday
  Monday     Monday
  Saturday   Saturday
  Sunday     Sunday
  Thursday   Thursday
  Tuesday    Tuesday
  Wednesday  Wednesday
  Weekdays   Monday through Friday
  Weekend    Saturday and Sunday
Ruijie(config-time-range)#periodic weekdays 9:00 to 18:00
```

## 访问控制列表（ACL）原理及配置

- 基于时间的ACL
  - 可以实现所配置的ACL只在一个特定的时间段内生效
    - 配置方法
      - 3.为ACL中的特定ACE关联定义好的时间段
        - 当不在WORK_TIME定义的时间范围内，则所配置的两条ACE语句不生效

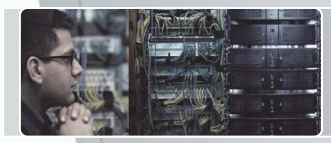
```
ip access-list extended OA
 10 permit tcp any any eq www time-range WORK_TIME
 20 deny ip any any time-range WORK_TIME
```



## 访问控制列表（ACL）原理及配置

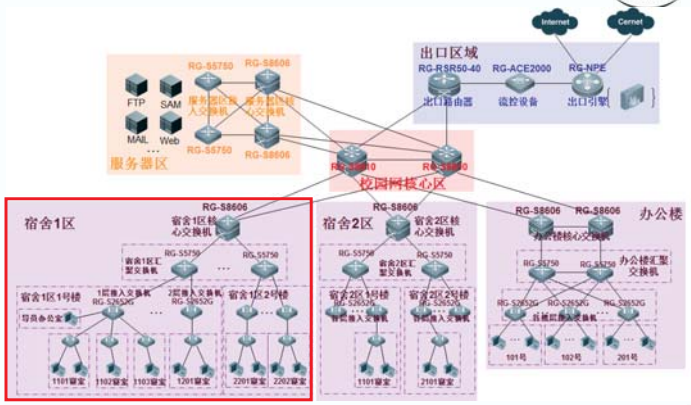
- 关键知识点回顾
  - 1.标准ACL和扩展ACL有什么区别？
  - 2.反掩码的匹配原理
  - 3.ACL在接口上的应用方向与数据流、接口的关系
  - 4.ACL中若存在多条ACE语句，那么匹配的规则是什么样的？





## 2、接入安全

## 场景回顾



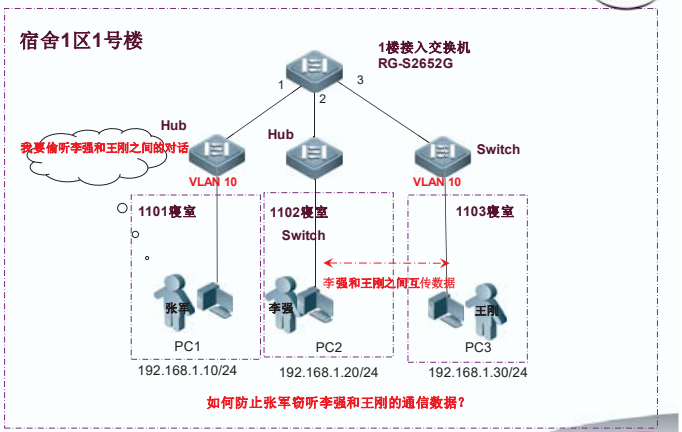



## 课程内容

- **端口安全和全局安全地址**
- DHCP安全特性
- 防ARP欺骗



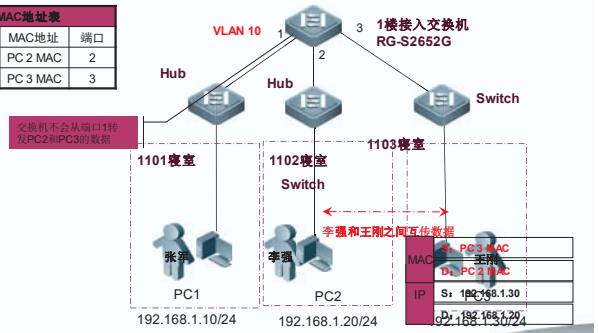
## 场景描述



## 端口安全和全局安全地址

- 交换机工作原理回顾
  - 交换机基于源MAC地址学习，生成MAC地址表项
  - 报文基于目标MAC转发，未知单播和广播从接收端口之外同一VLAN的所有端口洪泛

| MAC地址表 | | |
|---|---|---|
| VLAN | MAC地址 | 端口 |
| 10 | PC 2 MAC | 2 |
| 10 | PC 3 MAC | 3 |





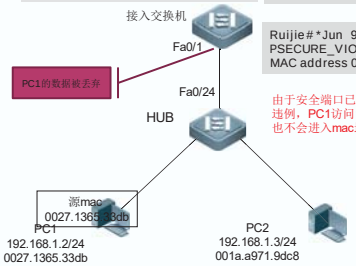

## 端口安全和全局安全地址

- 配置端口最大安全地址数，防范MAC表溢出攻击

当PC2接入网络后，由于fa0/1的安全地址没有达到最大安全地址数，PC2的地址会作为安全地址绑定到fa0/1上

```
int vlan 1
ip add 192.168.1.1 255.255.255.0
Int fa0/1
Switchport port-security
Switchport port-security maximum 1
```

```
Ruijie#sh port-security address
Vlan Mac Address   IP Address   Type      Port     Remaining Age
                                                    (mins)
---- ------------- ------------ --------- -------- -------------
1    001a.a97e.9dc8             Dynamic   Fa0/1
```




```
Ruijie#*Jun  9 12:11:35: %PORT_SECURITY-2-
PSECURE_VIOLATION: Security violation occurred, caused by
MAC address 0027.1365.33db on port FastEthernet 0/1.
```

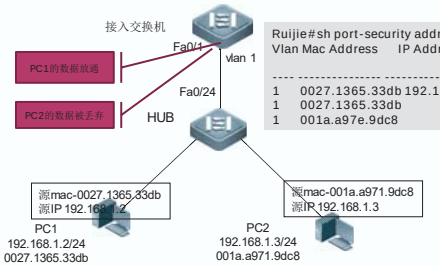
由于安全端口已经达到最大安全地址数，PC1的接入，导致fa0/1接口安全违例，PC1访问192.168.1.1的数据被丢弃，PC1的地址不会成为安全地址，也不会进入mac地址表



## 端口安全和全局安全地址

- 配置端口和安全地址的绑定关系，防止非法用户接入

```
int vlan 1
ip add 192.168.1.1 255.255.255.0
Int fa0/1
Switchport port-security
Switchport port-security binding  0027.1365.33db vlan 1 192.168.1.2
```




```
Ruijie#sh port-security address
Vlan Mac Address    IP Address      Type       Port     Remaining Age
                                                        (mins)
---- -------------- --------------- ---------- -------- -------------
1    0027.1365.33db 192.168.1.2     Configured Fa0/1    -
1    0027.1365.33db                 Dynamic    Fa0/1    -
1    001a.a97e.9dc8                 Dynamic    Fa0/1
```

注意：由于配置最大安全地址数，安全地址缺省为128，PC2的数据被丢弃，但它的地址仍可以成为安全地址，可以进入mac地址表

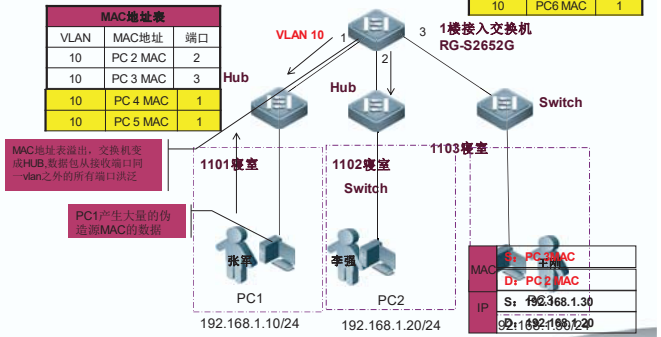


## 端口安全和全局安全地址

- MAC地址表溢出攻击
  - MAC表容量有限
  - 攻击主机产生大量的伪造源MAC的数据包，导致MAC表溢出

| MAC地址表 | | |
|---|---|---|
| VLAN | MAC地址 | 端口 |
| 10 | PC 2 MAC | 2 |
| 10 | PC 3 MAC | 3 |
| 10 | PC 4 MAC | 1 |
| 10 | PC 5 MAC | 1 |

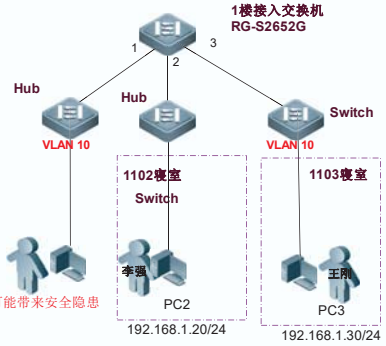
| MAC地址表 | | |
|---|---|---|
| VLAN | MAC地址 | 端口 |
| 10 | PC 4MAC | 1 |
| 10 | PC 5 MAC | 1 |
| 10 | PC6 MAC | 1 |






## 场景描述

**宿舍1区1号楼**




外来用户随意接入，可能带来安全隐患

以太网具有即插即入的特性

网络管理员如何防止外来用户随意接入网络？



## 端口安全和全局安全地址

- 端口安全
  - 交换机上的认证是基于用户数据包的源地址（MAC、IP）实现的，端口安全就是在交换机上建立端口和地址的绑定关系
    - 限制端口能接入的最大主机数，防止MAC地址表溢出攻击
    - 针对端口绑定MAC地址、IP地址、IP+MAC地址，对接入主机进行控制，防止非授权用户随意接入，防止MAC地址欺骗、IP地址欺骗、ARP欺骗等地址欺骗攻击

## 端口安全和全局安全地址

- 端口安全介绍
  - 安全端口
    - 开启了端口安全功能的端口
  - 安全地址
    - 在安全端口上绑定的地址
    - 安全地址可以手工配置，也可以通过数据包的源地址动态学习
    - 安全地址可以是二层地址（MAC地址），也可以是三层地址（IP或IP+MAC）
      - 二层安全地址可以是静态绑定，也可以是动态绑定
      - 三层安全地址只能是静态绑定



## 端口安全和全局安全地址

- 配置步骤
  - 开启端口安全

```
Switch(config-if)#switchport port-security
```

  - 配置安全端口和安全地址的绑定关系

```
Switch(config-if)#switchport port-security binding 0006.1bde.13b4 vlan 10 192.168.1.10
```



## 端口安全和全局安全地址

- 设置端口违例处理方式(可选)

```
Switch(config)#interface fastethernet 0/1
Switch(config-if)#switchport port-security violation { protect |restric | shutdown }
```

› 如果安全端口的安全地址达到允许的最大个数，或者收到的数据源地址不是安全地址，则产生安全违例事件，按照配置进行违例处理
  - » Protect 丢弃违例数据 缺省的违例处理方式
  - » Restric 丢弃违例数据，并发送trap通知
  - » Shutdown 关闭端口，并发送trap通知，必须在全局下使用errdisable recovery才能恢复端口



## 端口安全和全局安全地址

- 配置步骤
  - 开启端口安全

```
Switch(config-if)#switchport port-security
```

  - 配置最大安全地址数

```
Switch(config-if)# switchport port-security maximum 4
```

安全地址的个数

    - 最大安全地址数指动态学习和静态配置的安全地址总数，安全端口如果没有配置最大安全地址数，缺省为128
    - 端口下安全地址没有达到最大安全地址数，可以基于接收到的数据包的源地址动态学习和静态配置；达到最大安全地址数，如果有新的用户接入，则产生安全违例事件，丢弃该用户的数据



## 端口安全和全局安全地址

- 在端口绑定安全地址（根据需要绑定二层或者三层安全地址）

› 针对端口进行MAC地址绑定（只绑定并检查二层源MAC）

```
Switch(config-if)#switchport port-security mac-address 0006.1bde.13b4 vlan 10
```

绑定的源MAC　源MAC所属vlan

› 针对端口绑定IP(只绑定并检查源IP)

绑定的源IP

```
Switch(config-if)#switchport port-security binding 192.168.1.10
```

› 针对端口绑定IP+MAC（绑定并检查源MAC和源IP）

绑定的源IP

```
Switch(config-if)#switchport port-security binding 0006.1bde.13b4 vlan 10 192.168.1.10
```

绑定的源MAC　源MAC所属vlan

» 该命令的等价命令

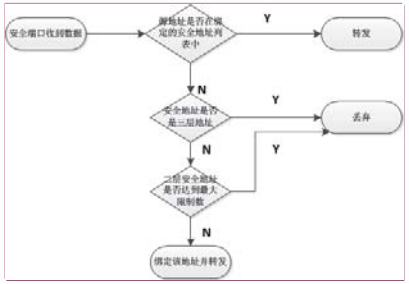
```
Switch(config)#switchport port-security binding interface fa0/1 0006.1bde.13b4 vlan 10 192.168.1.10
```

绑定的接口



## 端口安全和全局安全地址

- 端口安全原理
  - 开启端口安全功能的端口，会根据配置建立安全端口和安全地址的对应关系，并检查接收到的数据包的源地址，和安全地址匹配，决定如何处理该数据
  - 安全检查逻辑：先检查MAC地址，如果匹配，再检查



## 端口安全和全局安全地址

- 结果查看

```
Ruijie#show port-security
Secure Port  MaxSecureAddr  CurrentAddr  MaxIPSecureAddr  CurrentIPAddr  Security Action
                 (Count)      (Count)       (Count)          (Count)
-----------  ------------  -----------  ---------------  -------------  ---------------
  Fa0/3          128             0            128              0           Protect
  Fa0/7          128             4            128              1           Protect
```

查看所有安全端口的安全信息

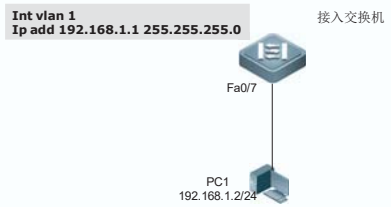
```
Ruijie#sh port-security address int fa0/7
  Vlan Mac Address       IP Address          Type          Port          Remaining Age
                                                                           (mins)
  ---- --------------- --------------- --------------  ---------  -------------
  1    0027.1365.33db  192.168.1.2     Configured      Fa0/7             -
  1    0027.1365.33db                  Dynamic         Fa0/7             -
  1    001a.a97e.9dc8                  Dynamic         Fa0/7             -
  1    0022.2333.3333                  Configured      Fa0/7             -
  1    0001.3333.2222                  Configured      Fa0/7             -
```

查看安全地址信息，一个端口配置为安全端口之后，该端口和mac地址的绑定关系不在mac地址表中，只能通过show port-security address int 接口号查看



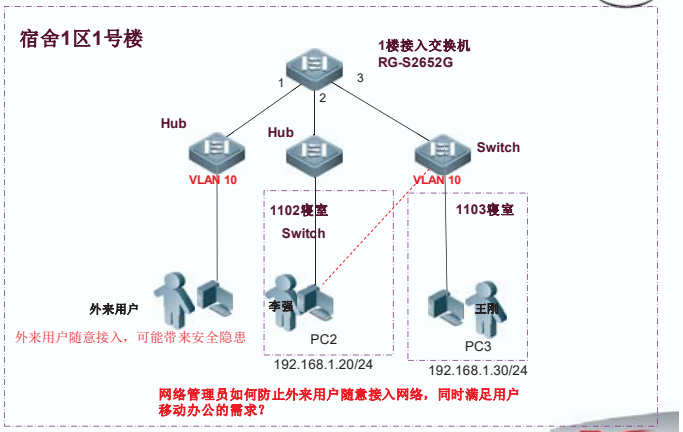
## 端口安全和全局安全地址

- 课堂练习
  - 网络管理员为每一位员工的主机分配固定的IP地址，其中PC1连接端口fa0/7，IP地址192.168.1.2,MAC地址使用用户主机的真实MAC。保证只有员工主机可以使用网络，其他用户不能随意接入网络






## 场景描述






## 端口安全和全局安全地址

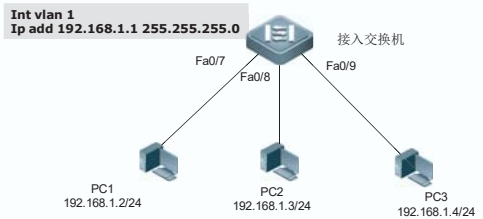
- 端口安全补充说明
  - 安全端口必须是二层端口，不能是镜像的目的端口
  - 和802.1x的认证功能互斥
    - 802.1x认证功能和端口安全功能都可以保证网络使用者的合法性，使能其一就可以达到控制端口接入的目
  - 安全地址的格式保持一致，即一个端口上的安全地址要么全绑定了IP地址（IP，IP+MAC），要么都不绑定IP地址(MAC)。如果一个端口同时包含这两种格式的安全地址，则不绑定IP地址的安全地址将失效(绑定IP地址的安全地址优先级更高)。



## 端口安全和全局安全地址

- 课堂练习

```
int fa0/7
switchport port-security binding 0027.1365.33db vlan 1 192.168.1.2
```




1、如果把PC1的IP地址修改为192.168.1.3或者更改MAC地址，是否能ping通192.168.1.1
2、保证fa0/8、fa0/9这两个端口只能接入如图所示的用户PC2、PC3？
3、如果PC2、PC3都通过HUB连接fa0/7，如何配置？
4、完成以上配置后用户是否能够接入其他已配置了安全地址的安全端口？非安全端口呢？如何既防止非法用户接入，又保证合法用户可以随意接入该交换机任何一个端口？



## 端口安全和全局安全地址

- 解决方案
  - 端口安全
    - 安全地址必须和特定的接口绑定，意味着用户只能接入绑定的安全端口
  - 全局安全地址
    - 交换机全局绑定IP+MAC地址，只有源地址满足绑定关系的用户才能通过该交换机接入网络，防止非授权用户接入，用户接入不再受限于特定的 端口。

## 端口安全和全局安全地址

- 配置全局绑定地址
  - Ruijie(config)#address-bind 192.168.1.2 0027.1365.33db
- 配置全局绑定地址上联口
  - Ruijie(config)# address-bind uplink gi 0/25
- 开启全局绑定地址功能
  - Ruijie(config)#address-bind install
- 查看全局绑定地址
  - Ruijie#show address-bind

绑定的IP和MAC

配置全局绑定后，缺省所有接口都会检查数据的源地址，并匹配配置的安全地址，上联口不会检查

使全局安全地址功能生效

```
Ruijie#sh address-bind
Total Bind Addresses in System : 1
IP Address          Binding MAC Addr
---------------     ---------------
   192.168.1.2      0027.1365.33db
```



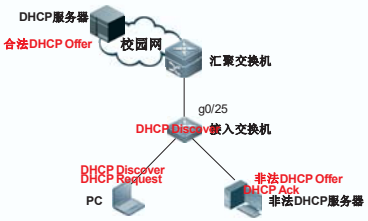
## 课程内容

- 端口安全和全局安全地址
- **DHCP安全特性**
- 防ARP欺骗



## 场景描述

- 如何防止下联用户架设非法DHCP服务器
  - 由于DHCP中继的存在，非法的DHCP服务器必须和客户端在同一VLAN
  - 客户端选择第一个提供offer的服务器（非法DHCP服务器）的IP地址




问题的关键就是在从连接用户的下联端口接收并转发了DHCP响应报文



## 端口安全和全局安全地址

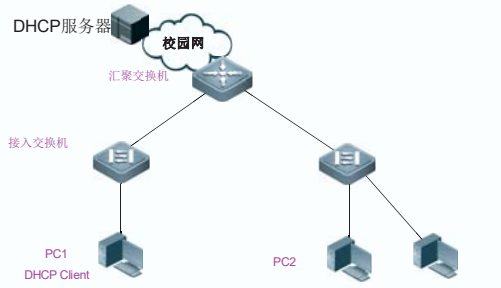
- 全局安全地址补充说明
  - 全局安全地址优先于端口安全、802.1X、ACL
  - 全局安全地址通过IPv4地址进行配置，IPv6报文转发受地址绑定模式影响
  - 配置地址绑定模式（可选）

```
Switch（config）#address-bind ipv6-mode {  compatible |loose | strict  }
```

  - Compatible 兼容模式，源mac为绑定mac的ipv6报文转发
  - loose 宽松模式 所有ipv6报文都转发
  - strict 严格模式 所有IPv6报文都不转发，缺省模式



## 场景描述




如何防范非法DHCP服务器



## DHCP安全特性

- 解决方案
  - 在接入交换机部署DHCP Snooping

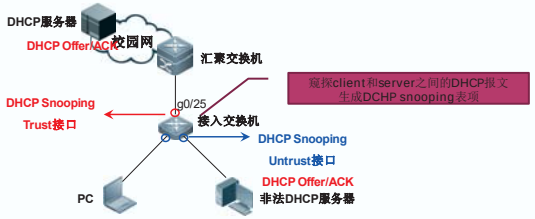
```
Ruijie(config)#ip dhcp snooping
```

  - 上联口配置为trust口

```
Ruijie(config)#int g0/25
Ruijie(config-GigabitEthernet 0/25)#ip dhcp snooping trust
```

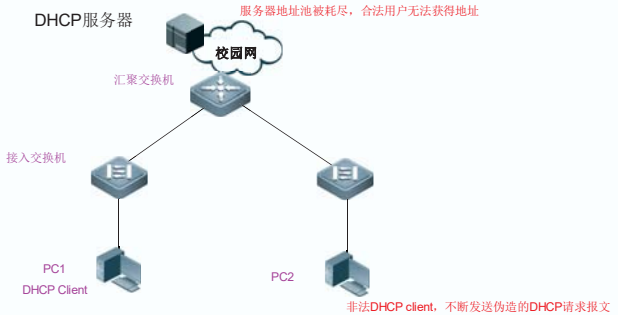
## DHCP安全特性

- DHCP snooping原理
  - 开启DHCP snooping的交换机所有接口缺省为untrust口
  - 只转发从trust口收到的DHCP响应报文（offer、ACK、NAK）
  - 窥探并记录DHCP报文中的信息，记录用户IP、MAC、交换机端口、租约时间、vlanID等信息，做为安全检查的依据






## 场景描述

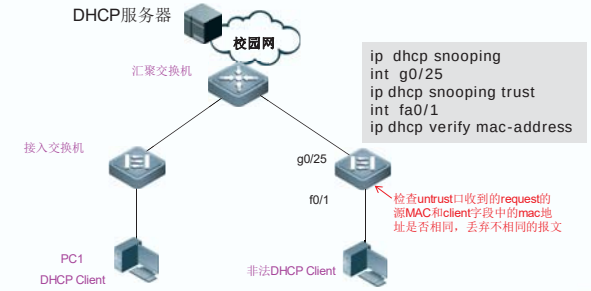



如何防范DHCP地址池耗尽攻击



## DHCP安全特性

- 解决方案
  - 在接入层交换机untrust口部署DHCP源MAC检查
    - 攻击者发送的DHCP报文的源MAC和Client字段中的MAC地址可能不匹配






## DHCP安全特性

- 结果查看

显示DHCP snooping的配置信息

```
Ruijie#sh ip dhcp snooping

Switch DHCP snooping  status                 :  ENABLE
DHCP snooping  Verification of hwaddr status    :  DISABLE
DHCP snooping database write-delay time      :  0 seconds
DHCP snooping option 82 status               :  DISABLE
DHCP snooping Support bootp bind status      :  DISABLE
Interface                Trusted      Rate limit (pps)
-------------------------  -------  -----------------
GigabitEthernet 0/25       YES          unlimited
```

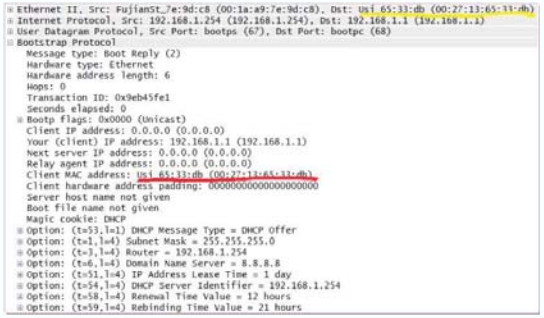
```
Ruijie#sh ip dhcp snooping binding

Total number of bindings: 1

MacAddress          IpAddress       Lease(sec)   Type           VLAN  Interface
------------------ --------------- ---------- ------------- ----- --------------------
0027.1365.33db     172.16.10.1     86397        dhcp-snooping  1     FastEthernet 0/1
```

显示DHCP snooping绑定数据库的信息



## DHCP安全特性

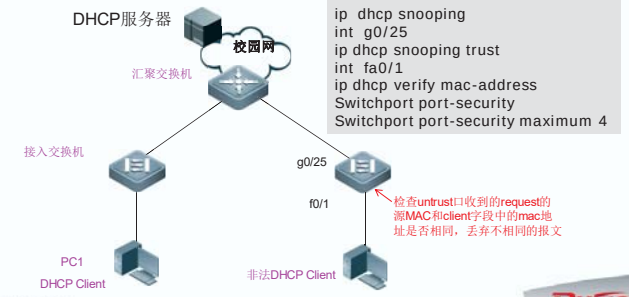
- DHCP 地址耗尽攻击原理
  - Server基于client字段中的MAC地址为客户端分配地址，并且没有认证机制
  - 客户端可以通过变更地址，不断的申请地址，耗尽服务器地址池中的地址





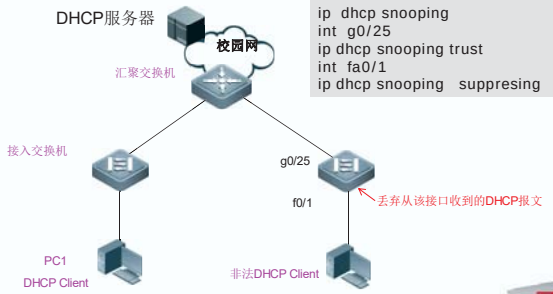

## DHCP安全特性

- 解决方案
  - 在接入层交换机untrust口部署DHCP源MAC检查
    - 攻击者发送的DHCP报文的源MAC和Client字段中的MAC地址可能不匹配
    - 如果两个MAC地址相同，可以通过端口安全限制该端口的最大安全地址数



## DHCP安全特性

- 解决方案
  - 在连接非法客户端的接口配置DHCP报文抑制，丢弃从该接口收到的DHCP报文

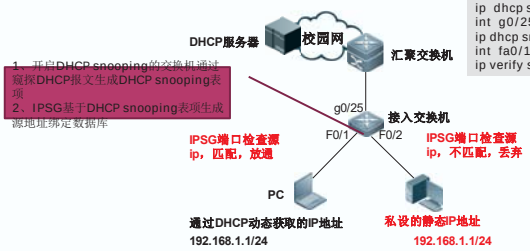



```
ip dhcp snooping
int g0/25
ip dhcp snooping trust
int fa0/1
ip dhcp snooping suppresing
```



## DHCP安全特性

- 如何防止用户私设IP
  - 部署IPSG(ip source guard)
    - IPSG维护IP源地址绑定数据库，该数据库来源于DHCP snooping数据库或者手工静态配置
    - 开启IPSG的端口基于IP源地址绑定数据库，检查接收到的所有非DHCP的IP报文的源IP或源IP+MAC，丢弃不匹配的数据




```
ip dhcp snooping
int g0/25
ip dhcp snooping trust
int fa0/1
ip verify source port-security
```



## DHCP安全特性

- 结果查看

显示DHCP snooping绑定数据库的信息

```
Ruijie#sh ip dhcp snooping binding
Total number of bindings: 1
MacAddress          IpAddress       Lease(sec)     Type           VLAN  Interface
------------------  --------------  -------------  -------------  ----  --------------------
0027.1365.33db      192.168.1.1     84437          dhcp-snooping  1     FastEthernet 0/1
```

显示IP源地址绑定数据库的信息

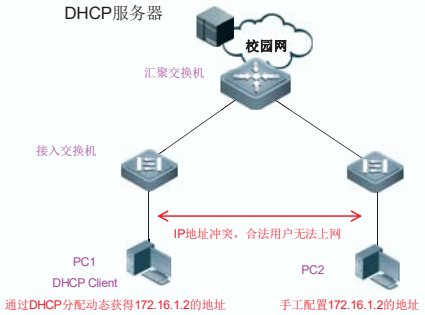
```
Ruijie#sh ip source binding
MacAddress          IpAddress       Lease(sec)     Type           VLAN  Interface
------------------  --------------  -------------  -------------  ----  --------------------
0027.1365.33db      192.168.1.1     84385          dhcp-snooping  1     FastEthernet 0/1
0027.1365.3425      192.168.1.2     infinite       static         1     FastEthernet 0/3
Total number of bindings: 2
```

显示IPSG的地址过滤表项

```
Ruijie#sh ip verify source
Interface           Filter-type  Filter-mode  Ip-address      Mac-address       VLAN
------------------  -----------  -----------  --------------  ----------------  ----
FastEthernet 0/1    ip+mac       active       192.168.1.1     0027.1365.33db    1
FastEthernet 0/1    ip+mac       active       deny-all        deny-all
FastEthernet 0/2    ip+mac       active       deny-all        deny-all
FastEthernet 0/3    ip+mac       active       192.168.1.2     0027.1365.3425    1
```



## 场景描述




如何防范用户私设IP



## DHCP安全特性

- 部署IPSG防止用户私设IP
  - 在DHCP snooping的untrust口开启IPSG功能

```
Ruijie(config-FastEthernet 0/1)#ip verify source ?
  port-security  Port security
  <cr>
```

Ip verify source 只检查源IP

Ip verify source port-security 检查源IP+源MAC

  - 配置静态源地址绑定

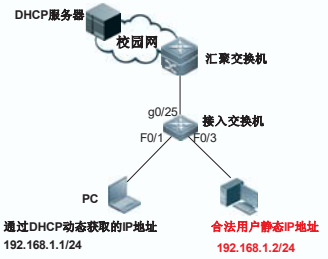
```
Ruijie(config)#ip source binding 0027.1365.33db vlan 1 192.168.1.2 interface fa0/1
```

源MAC　VLAN ID　源IP　绑定的接口



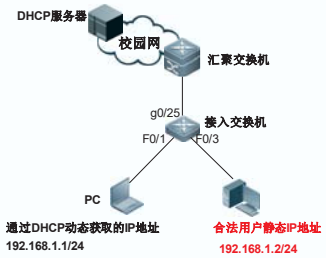
## DHCP安全特性

- 课堂练习
  - 防止私设服务器，防止用户私设IP，其中f0/3接口连接的合法用户的地址是静态配置



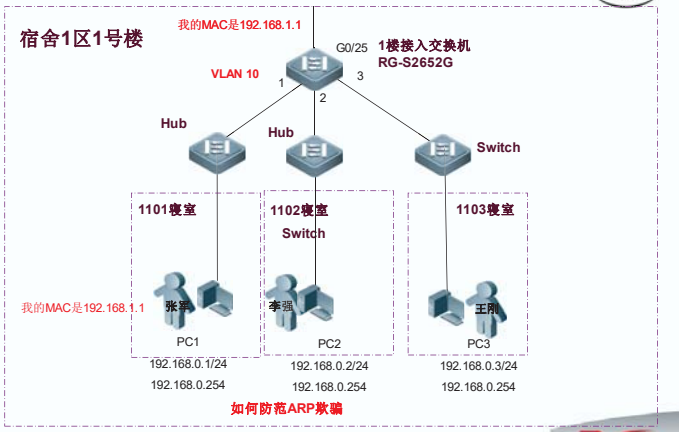
## DHCP安全特性

- 课堂练习
  - 防止私设服务器，防止用户私设IP，其中f0/3接口连接的合法用户的地址是静态配置





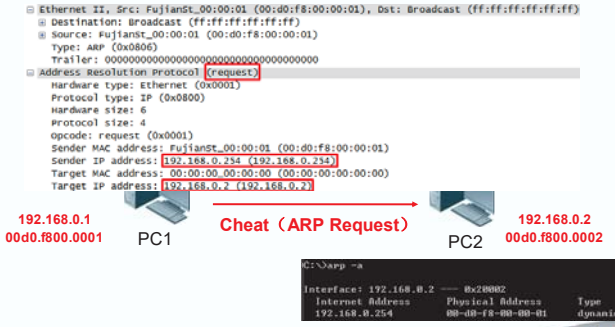

## 场景描述






## 防ARP欺骗

- ARP Request报文更新ARP表的条件
  - ARP报文中Target IP为自己
  - 用ARP报文中的Sender MAC与Sender IP更新自己的ARP表





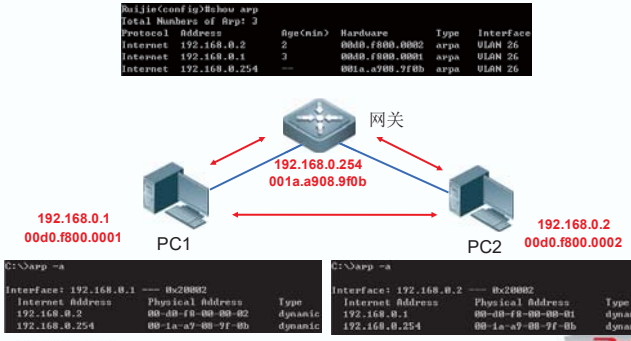

## 课程内容

- 端口安全和全局安全地址
- DHCP安全特性
- 防ARP欺骗



## 防ARP欺骗

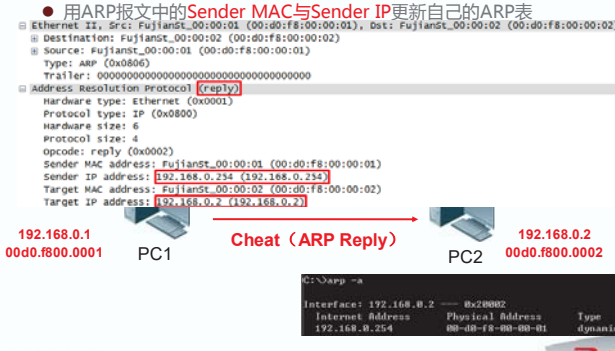
- ARP回顾
  - PC与设备之间相互通信后形成的ARP表
  - ARP表决定后续报文如何封装






## 防ARP欺骗

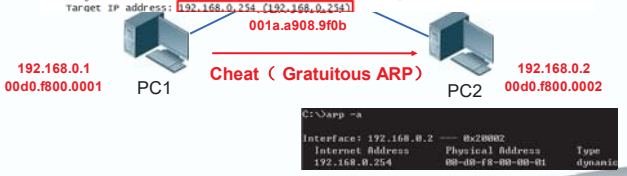
- ARP Reply报文更新ARP表的条件
  - ARP报文中Target IP为自己
  - 当前ARP表中已存在Sender IP的表项
  - 用ARP报文中的Sender MAC与Sender IP更新自己的ARP表



## 防ARP欺骗

- Gratuitous ARP报文更新ARP表的条件
  - Gratuitous ARP是一种特殊的ARP Request/Replay报文，即Sender IP与Target IP一致

```
Ethernet II, Src: FujianSt_00:00:01 (00:d0:f8:00:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: FujianSt_00:00:01 (00:d0:f8:00:00:01)
  Type: ARP (0x0806)
  Trailer: 00000000000000000000000000000000000000000000
Address Resolution Protocol (request/gratuitous ARP)
  Hardware type: Ethernet (0x0001)
  Protocol type: IP (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (0x0001)
  Sender MAC address: FujianSt_00:00:01 (00:d0:f8:00:00:01)
  Sender IP address: 192.168.0.254 (192.168.0.254)
  Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.0.254 (192.168.0.254)
```

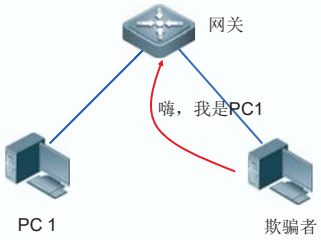



```
C:\>arp -a

Interface: 192.168.0.2 --- 0x20002
  Internet Address      Physical Address      Type
  192.168.0.254         00-d0-f8-00-00-01     dynamic
```



## 防ARP欺骗

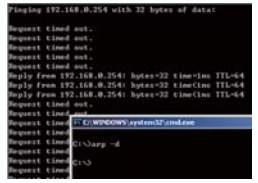
- ARP欺骗—网关型ARP欺骗
  - 欺骗者主机冒充其他主机对网关设备进行欺骗






## 防ARP欺骗

- 怎样判断是否受到了ARP欺骗攻击？
  - 网络时断时续或网速特别慢
  - 在命令行提示符下执行“arp –d”命令就能好上一会
  - 在命令行提示符下执行“arp –a”命令查看网关对应的MAC地址发生了改变

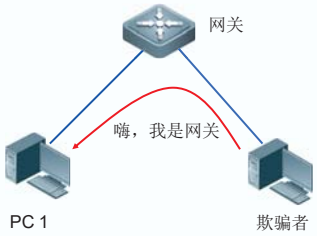


```
C:\>arp -a

Interface: 192.168.0.2 --- 0x20002
  Internet Address      Physical Address      Type
  192.168.0.254         00-d0-f8-00-00-01     dynamic
```



## 防ARP欺骗

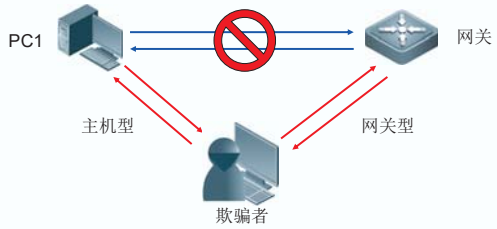
- ARP欺骗—主机型ARP欺骗
  - 欺骗者主机冒充网关设备对其他主机进行欺骗






## 防ARP欺骗

- 为什么产生ARP欺骗攻击？
  - 表象：网络通讯中断
  - 真实目的：截获网络通讯数据






## 防ARP欺骗

- 网关设备怎样判断是否受到了ARP欺骗攻击？
  - ARP表中同一个MAC对应许多IP地址

```
Ruijie#show arp
Total Numbers of Arp: 52
Protocol  Address          Age(min)  Hardware        Type
Internet  192.168.0.41     0         00d0.f800.0001  arpa
Internet  192.168.0.40     0         00d0.f800.0001  arpa
Internet  192.168.0.39     0         00d0.f800.0001  arpa
Internet  192.168.0.38     0         00d0.f800.0001  arpa
Internet  192.168.0.37     0         00d0.f800.0001  arpa
Internet  192.168.0.36     0         00d0.f800.0001  arpa
Internet  192.168.0.35     0         00d0.f800.0001  arpa
Internet  192.168.0.34     0         00d0.f800.0001  arpa
```

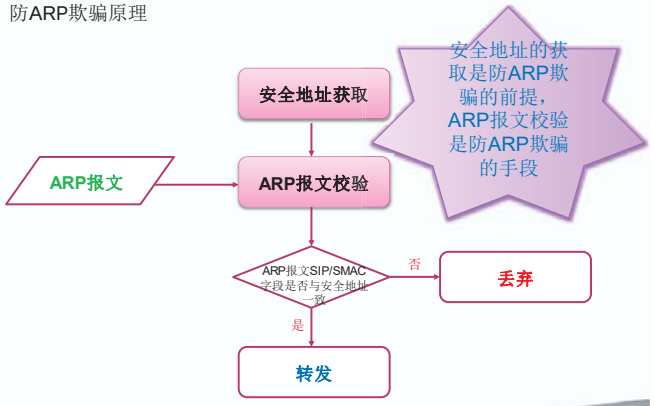
## 防ARP欺骗

- 防ARP欺骗原理
  - ARP欺骗就是伪造ARP报文中的sender IP和sender MAC
  - 安全地址
    - 主机真实的IP与MAC地址
    - 在主机发送ARP报文前获得，可以
    - 可以动态学习或者手工配置
  - ARP报文校验
    - 检查ARP报文中Sender’s MAC与安全地址中的MAC是否一致，否则丢弃
    - 检查ARP报文中Sender’s IP与安全地址中的IP是否一致，否则丢弃



## 防ARP欺骗

- 防ARP欺骗原理





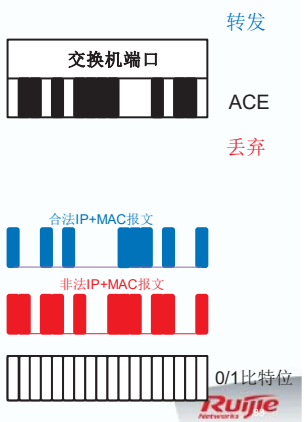

## 防ARP欺骗

- 安全地址获取方式
  - 主机的真实信息，由IP+MAC地址组成
  - 手工指定
    - port-security
  - 自动获取
    - DHCP Snooping
    - Dot1x认证
- ARP报文校验方法
  - ARP-check
  - DAI



## 防ARP欺骗

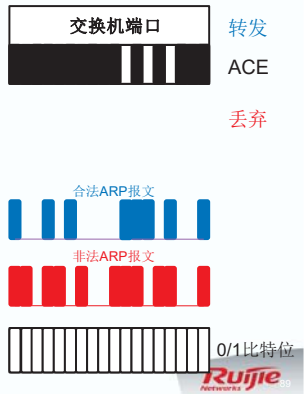
- 什么是ACE
  - 交换机端口形成的硬件资源表项
  - 通过硬件对报文的转发进行判断
- 端口策略
  - 未配置安全地址时
    - permit any any any any
  - 配置安全地址后
    - permit mac1 ip1 any any
    - permit mac2 ip2 any any
    - permit macN ipN any any
    - deny any any any any






## 防ARP欺骗

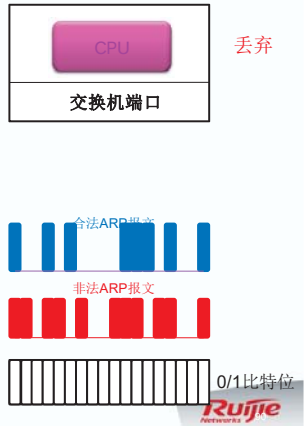
- **锐捷ARP报文校验方式一（ARP-check）**
  - ARP-check
    - 原理：
      - 提取ACE中IP+MAC对的信息
      - 在原有ACE（过滤IP+MAC）的基础上形成新的ACE（过滤ARP）
    - 应用后端口策略
      - permit mac1 ip1 any any
      - permit arp 源MAC1 源IP1 any any
      - deny any any any any
    - 注意事项：ARP-check功能开启后，如果ACE中不存在安全地址，则所有的ARP报文将被丢弃






## 防ARP欺骗

- **锐捷ARP报文校验方式二（DAI）**
  - DAI
    - 原理：
      - 提取DHCP Snooping表中的IP+MAC信息
      - 通过CPU过滤源MAC/源IP不在Snooping表中的ARP报文
    - 注意事项：DAI功能开启开启后，如果DHCP Snooping表为空，则所有的ARP报文将被丢弃
    - 缺省开启DAI检查的VLAN的所有接口都是untrust口，会检查收到的ARP报文，需要把接入交换机的上联口配置为trust口



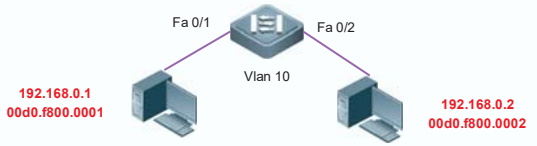
## 防ARP欺骗

- **方案一：port-security + ARP-check**
  - 原理
    - 通过port-security功能将用户正确的IP与MAC写入交换机端口ACE
    - 使用ARP-check功能校验ARP报文的正确性
  - 应用场景
    - 用户使用静态IP地址
    - 无安全认证措施
  - 缺点
    - 需要收集所有用户的IP、MAC，将其配置到端口上
    - 当用户接入端口发生变化时，需重新设置安全地址



## 防ARP欺骗

- **方案一：port-security + ARP-check实施**




```
interface FastEthernet 0/1
 switchport port-security binding 00d0.f800.0001 vlan 10 192.168.0.1
 switchport port-security
 arp-check
!
interface FastEthernet 0/2
 switchport port-security binding 00d0.0000.0002 vlan 10 192.168.0.2
 switchport port-security
 arp-check
```



## 防ARP欺骗

- 结果查看

查看安全地址与端口的绑定关系

```
Ruijie#sh port-security address
Vlan   Mac Address       IP Address                Type            Port     Remaining Age
                                                                                (mins)
----   -----------       ----------                ----            ----     -------------
10   00d0.f800.0001    192.168.0.1               Configured      Fa0/1       -
10   00d0.0000.0002    192.168.0.2               Configured      Fa0/2       -
```

```
Ruijie#sh int arp-check list
Interface  Sender MAC       Sender IP      Policy Source
---------- --------------- --------------- --------------------
Fa0/1      00d0.f800.0001  192.168.0.1     port-security
Fa0/2      00d0.0000.0002  192.168.0.2     port-security
```

显示arp-check所检查的表项信息



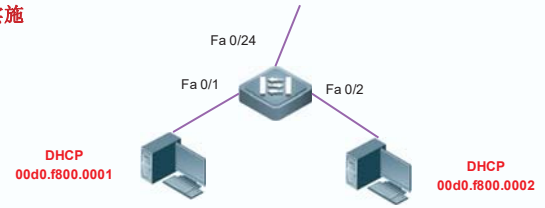
## 防ARP欺骗

- **方案二：DHCP Snooping + IP Source guard + ARP-check方案**
  - 原理
    - 通过DHCP Snooping功能将用户正确的IP与MAC写入交换机的DHCP Snooping表
    - 通过IP Source guard将DHCP Snooping表的写入交换机的ACE（类似端口安全）
    - 使用ARP-check功能校验ARP报文的正确性
  - 应用场景
    - 用户使用动态IP地址
    - 同样适用于SAM认证环境
    - 动态环境下如果使用安全通道，请勿在安全通道中允许ARP报文通过
  - 缺点
    - 无



## 防ARP欺骗

- **方案二：DHCP Snooping + IP Source guard + ARP-check实施**

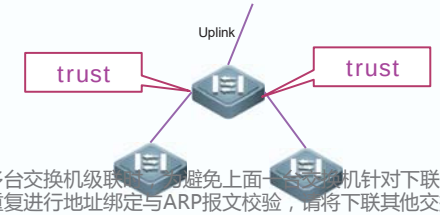



```
ip dhcp snooping
!
interface FastEthernet 0/1
 ip verify source port-security
 arp-check
!
interface FastEthernet 0/2
 ip verify source port-security
 arp-check
!
interface FastEthernet 0/24
 ip dhcp snooping trust
```



## 防ARP欺骗

- **方案二：DHCP Snooping + IP Source guard + ARP-check级联优化**




- 多台交换机级联时，为避免上面一级交换机针对下联交换机上的用户重复进行地址绑定与ARP报文校验，请将下联其他交换机的接口启用 ip dhcp snooping trust

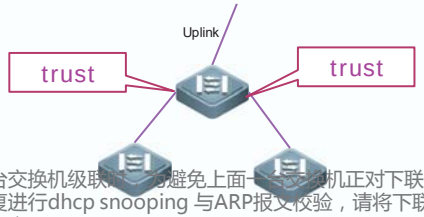
## 方案三： DHCP Snooping + DAI

- 原理
  - 通过DHCP Snooping功能将用户正确的IP与MAC写入交换机的DHCP Snooping表
  - 使用DAI功能校验ARP报文的正确性
- 应用场景
  - 用户使用动态IP地址
  - 同样适用于SAM认证环境
  - 动态环境下如果使用安全通道，请勿在安全通道中允许ARP报文通过
- 缺点
  - DAI功能需通过CPU处理，大量的ARP报文可能导致CPU过高





## 方案三： DHCP Snooping + DAI级联优化

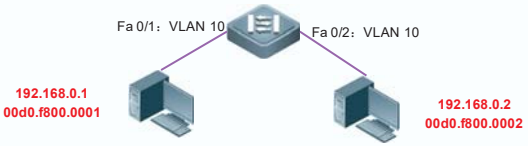



- 多台交换机级联时，为避免上面一台交换机正对下联交换机上的用户重复进行dhcp snooping 与ARP报文校验，请将下联其他交换机的接口启用ip dhcp snooping trust及ip arp inspection trust





## 方案四： SAM + Supplicant实施

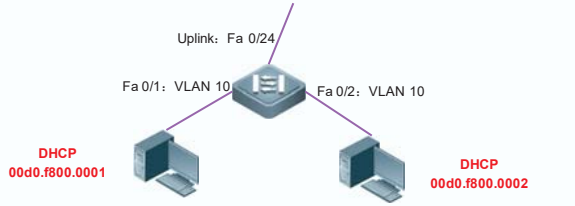



```
aaa authorization ip-auth-mode supplicant
!
interface FastEthernet 0/1
 switchport access vlan 10
 arp-check
 dot1x port-control auto
!
interface FastEthernet 0/2
 switchport access vlan 10
 arp-check
 dot1x port-control auto
```





## 方案三： DHCP Snooping + DAI实施




```
ip dhcp snooping
!
ip arp inspection vlan 10
!
interface FastEthernet 0/1
!
interface FastEthernet 0/2
!
interface FastEthernet 0/24
 ip dhcp snooping trust
 ip arp inspection trust
```

指定需要开启DAI检查的VLAN

把上联口配置为DAI的trust口





## 方案四： SAM + Supplicant授权

- 原理
  - 用户通过SAM认证后，交换机会将用户的MAC信息写入ACE
  - 交换机开启Supplicant授权，supplicat把IP地址告诉交换机，交换机会将用户的IP信息写入ACE
  - 使用ARP-check功能校验ARP报文的正确性
- 应用场景
  - 用户使用静态IP地址
  - 用户使用SAM认证
- 缺点
  - 不能使用安全通道功能





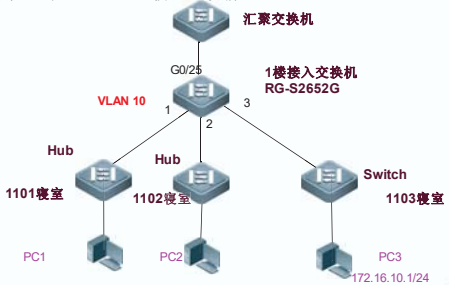
## 各种防ARP欺骗方案比较

| 环境/方案 | port-security +ARP-check | DHCP Snooping +IP Source guard +ARP-check | DHCP Snooping +DAI | Supplicant授权 +ARP-check |
|---|---|---|---|---|
| 静态IP | √ | | | |
| 静态IP+SAM | | | | √ |
| 动态IP | | √ | √ | |
| 动态IP+SAM | | √ | √ | |

## 防ARP欺骗

**课堂练习**

- 汇聚交换机作为DHCP服务器，为用户分配IP地址。地址段172.16.10.0/24，网关172.16.10.254，DNS地址8.8.8.8，其中PC3的用户地址静态分配，地址172.16.10.1
- 分别使用DAI和ARP-check防ARP欺骗



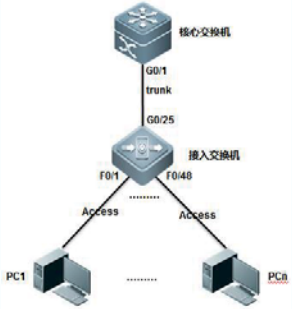



## 3、NFPP

## NFPP(Network Foundation Protection Policy)
## FPP实验

一、组网需求

核心设备下挂3000个用户，其中一个端口最大用户数为200个，接入交换机所携带的用户数不超过200，接入交换机的每个端口最大用户数6个，所有的接入设备都启用DHCP Snooping+DAI功能防ARP欺骗。为了防止非法攻击，占用交换机的CPU资源，需要调整NFPP的相关参数实现防攻击






## 防ARP欺骗

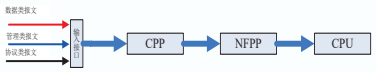
- 主要知识点回顾
  - 1.端口安全和全局安全地址的区别在哪里？
  - 2.如何防范DHCP服务器欺骗？如何防范用户私设IP
  - 3.使用DAI防范ARP欺骗时安全地址如何获得？使用ARP-check防范ARP欺骗时安全地址如何获得？



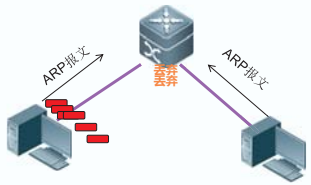
## NFPP(Network Foundation Protection Policy)
## 网络基础保护策略

- 作用
  - 在CPP基础上进一步保护交换机管理面安全，设备能够在恶意攻击时保持稳定
  - CPP对ARP报文进行整体限速，NFPP可基于主机进行限速
  - 支持ARP、ICMP、DHCP、IP扫描、ND抗攻击
- 原理
  - 对特定的协议报文基于MAC/IP/端口进行限速及攻击检测识别，并可对攻击源隔离

注意：设备默认开启




基于IP/MAC ：限速4PPS
：攻击8PPS






## NFPP(Network Foundation Protection Policy)
## FPP实验

二、配置要点

1、根据需求调整接入交换机NFPP功能参数，由于接入交换机开启了DAI功能，网关发送的ARP报文到接入交换机后都需要送CPU处理，为了防止正常的ARP等报文被NFPP丢弃，需要关闭上联口的NFPP相关功能，并放大接入交换机的CPP限速（默认限速180PPS在DAI场景中偏小）

2、根据核心的用户数量，调整核心交换机NFPP基于端口的限速/攻击检测参数

3、为了避免NFPP产生的LOG太多，通过命令调整LOG打印速率

## NFPP(Network Foundation Protection Policy) FPP实验

二、配置要点

1、根据需求调整接入交换机NFPP功能参数，由于接入交换机开启了DAI功能，网关发送的ARP报文到接入交换机后都需要送CPU处理，为了防止正常的ARP等报文被NFPP丢弃，需要关闭上联口的NFPP相关功能，并放大接入交换机的CPP限速（默认限速180PPS在DAI场景中偏小）

2、根据核心的用户数量，调整核心交换机NFPP基于端口的限速/攻击检测参数

3、为了避免NFPP产生的LOG太多，通过命令调整LOG打印速率



## NFPP(Network Foundation Protection Policy) FPP实验

三、配置步骤

接入交换机配置：

1、配置交换机的防ARP欺骗功能，具体也可以参见DHCP环境防ARP欺骗章节中DHCP Snooping+DAI方案。

```
Ruijie#configure terminal
Ruijie(config)#vlan 10
Ruijie(config-vlan)#exit
Ruijie(config)#ip arp inspection vlan 10
Ruijie(config)#ip dhcp snooping
Ruijie(config)#interface gigabitEthernet 0/25
Ruijie(config-if-GigabitEthernet 0/25)#switchport mode trunk
Ruijie(config-if-GigabitEthernet 0/25)#ip dhcp snooping trust
Ruijie(config-if-GigabitEthernet 0/25)#ip arp inspection trust
Ruijie(config-if-GigabitEthernet 0/25)#exit
Ruijie(config)#interface range fastEthernet 0/1-24
Ruijie(config-if-range)#switchport access vlan 10
```



## NFPP(Network Foundation Protection Policy) FPP实验

2、NFPP功能配置：

1）全局NFPP配置

默认交换机的NFPP功能是开启的，二层交换机参数无需调整，只需将上联口NFPP关闭并由于DAI原因调整放大CPP即可（

Ruijie(config)#cpu-protect type arp pps 500 ，如果没有使用DAI，CPP也无需调整。

全局下的NFPP调整参数如下

Ruijie(config-nfpp)#log-buffer entries 1024 ------>设置NFPP log缓存的容量为1024条（默认256）

Ruijie(config-nfpp)#log-buffer logs 1 interval 300 ------>为避免NFPP产生的LOG太多，调整每次打印一条相同log信息的阀值为300秒

Ruijie(config-nfpp)#exit

Ruijie(config)#



## NFPP(Network Foundation Protection Policy) FPP实验

2）接口NFPP配置

为了防止大量网关发送的正常的相关报文（特别是网关发送的ARP请求或回应报文）被接入交换机误认为是攻击被丢弃，从而导致下联用户无法获取网关的ARP信息而无法上网，需要将上联口的NFPP功能关闭

Ruijie(config)#int g0/25

Ruijie(config-if-GigabitEthernet 0/25)#no nfpp arp-guard enable ------>关闭接口的ARP-guard功能，关闭该功能后，该接口进入的数据报文不进行NFPP检测

Ruijie(config-if-GigabitEthernet 0/25)#no nfpp dhcp-guard enable ------>关闭接口的dhcp-guard功能，关闭该功能后，该接口进入的数据报文不进行NFPP检测

Ruijie(config-if-GigabitEthernet 0/25)#no nfpp dhcpv6-guard enable ------>关闭接口的dhcpv6-guard功能，关闭该功能后，该接口进入的数据报文不进行NFPP检测



## NFPP(Network Foundation Protection Policy) FPP实验

2）接口NFPP配置

Ruijie(config-if-GigabitEthernet 0/25)#no nfpp icmp-guard enable ------>关闭接口的icmp-guard功能，关闭该功能后，该接口进入的数据报文不进行NFPP检测

Ruijie(config-if-GigabitEthernet 0/25)#no nfpp ip-guard enable ------>关闭接口的ip-guard功能，关闭该功能后，该接口进入的数据报文不进行NFPP检测

Ruijie(config-if-GigabitEthernet 0/25)#no nfpp nd-guard enable ------>关闭接口的nd-guard功能，关闭该功能后，该接口进入的数据报文不进行NFPP检测

Ruijie(config-if-GigabitEthernet 0/25)#exit

Ruijie(config)#



## NFPP(Network Foundation Protection Policy) FPP实验

核心交换机NFPP配置：

只做下述调整即可：

Ruijie(config)#nfpp

Ruijie(config-nfpp)#arp-guard attack-threshold per-port 800 ------>设置每个端口的攻击阀值为800个，超过此值丢弃并打印攻击日志

Ruijie(config-nfpp)#arp-guard rate-limit per-port 500 ------>每个端口每秒限速500个arp报文，多余的ARP报文将被丢弃（默认限速阀值是100个偏小）

Ruijie(config-nfpp)#log-buffer entries 1024 ------>设置NFPP log缓存的容量为1024条（默认256）

Ruijie(config-nfpp)#log-buffer logs 1 interval 300 ------>调整log打印频率为300S打印1次

## NFPP(Network Foundation Protection Policy)
## FPP实验

用户隔离信息

Ruijie(config)#nfpp ------>进入NFPP配置模式

Ruijie(config-nfpp)#arp-guard isolate-period 600 ------>超过ARP攻击阀值后，对用户进行隔离，设置隔离时间为600秒

Ruijie(config-nfpp)#arp-guard attack-threshold per-src-mac 30 ------>设置每个mac的攻击阀值为10个，如果交换机检测每个mac发送的ARP报文大于10个，那么交换机会把该用户放入ARP攻击表，可以对这些用户进行硬件隔离（默认不进行硬件隔离，可以进行配置隔离时间进行隔离，设置隔离时间后会占用硬件表项资源。默认每MAC的攻击阀值是8个）

Ruijie(config-nfpp)#arp-guard attack-threshold per-src-ip 30 ------>设置每个IP的攻击阀值为10个，如果交换机检测每个IP发送的ARP报文大于10个，那么交换机会把该用户放入ARP攻击表，可以对这些用户进行硬件隔离（默认不进行硬件隔离，可以进行配置隔离时间进行隔离，设置隔离时间后会占用硬件表项资源。默认每IP的攻击阀值是8个）




Ruijie Networks Certification Center
Addr: 北京海淀区复兴路29号中意鹏奥大厦东塔A座11层 邮编：100036
university.ruijie.com.cn

## NFPP(Network Foundation Protection Policy)
## FPP实验

Ruijie(config-nfpp)#arp-guard rate-limit per-src-mac 20 ------>每个mac每秒限速6个arp报文，多余的ARP报文将被丢弃（默认限速阀值是4个）

Ruijie(config-nfpp)#arp-guard rate-limit per-src-ip 20 ------>每个IP每秒限速6个arp报文，多余的ARP报文将被丢弃（默认限速阀值是4个）

Ruijie(config-nfpp)#ip-guard attack-threshold per-src-ip 80 ------>设置IP攻击阀值为40个每IP

Ruijie(config-nfpp)#ip-guard isolate-period 600 ------>超过IP攻击阀值后，对用户进行隔离，设置隔离时间为600秒