

King Lab CCIE实验室 Switch V1.0试验分解指南

前言:

为了更好的满足广大网络技术爱好者学习的需求，KING LAB网络实验室CCIE专家老师特别制作了这份最新版本的CCNP试验手册。请大家多多支持king lab网络实验室！

更多技术请关注QQ技术讨论群：80990677

网址：www.kinglab.cn

QQ: 1090336027

目录:

1、VLAN 创建	P3
2、交换机端口操作模式设置	P5
3、VLAN 端口划分	P7
4、VTP 设置	P8
5、STP 实验	P12
6、PVST+&RSTP	P15
7、STP 防护	P17
8、SVI 实验	P19
9、etherchannel	P21
10、HSRP	P24
11、DHCP	P27
12、dhcp 中继	P29
13、IP SLA 实验	P31
14、port-Security	P33
15、基于端口的 802.1x	P35
16、dynamic ARP inspect	P41
17、VLAN ACL	P43

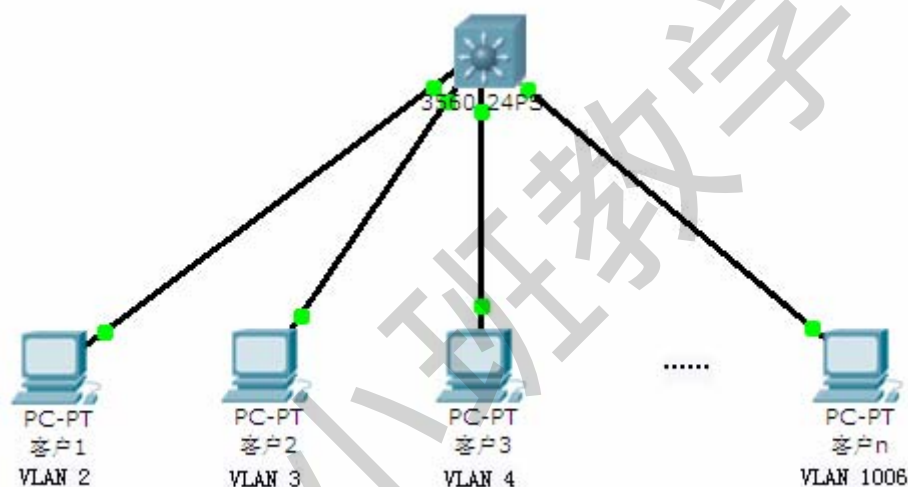
VLAN 的创建

一、实验目的

- 1、掌握标准 VLAN 的创建方法
- 2、掌握扩展 VLAN 的创建方法

二、实验内容

拓扑图：



需求：

为不同的客户划分 VLAN

三、实验配置

配置：

- 1、查看 VTP 的操作模式

```
Switch#show vtp status
```

```
VTP Version           : running VTP1 (VTP2 capable)
Configuration Revision : 0
Maximum VLANs supported locally : 1005
Number of existing VLANs : 5
VTP Operating Mode     : Server
VTP Domain Name       :
```

- 2、配置标准 VLAN

```
Switch(vlan)#vlan database
```

```
Switch(vlan)#vlan 1 （创建 VLAN 1）
```

```
VLAN 1 modified:
```

```
Switch(vlan)#vlan 2
```

```
VLAN 2 added:
```

```
Name: VLAN0002
```

```
Switch(vlan)#vlan 3 name customer (创建 VLAN , 并且设置 VLAN 的名字)
```

```
VLAN 3 modified:
```

```
Name: customer
```

```
Switch(vlan)#exit (一定要使用 exit 退出 VLAN database)
```

3、创建扩展 VLAN (1006~4095)

错误方式:

```
Switch(vlan)#vlan 1006
```

```
% Invalid input detected at '^' marker.
```

```
Switch(config)#vlan 1006
```

```
Switch(config-vlan)#exit
```

```
% Failed to create VLANs 1006
```

```
Extended VLAN(s) not allowed in current VTP mode.
```

(在 VLAN Database 中不能创建扩展 VLAN, 只能在配置模式下, 并且是 VTP 透明模式下才能创建)

正确方式:

```
Switch(config)#vtp mode transparent
```

```
Switch(config)#vlan 1006
```

验证:

```
Switch#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12
2	VLAN0002	active	
3	customer	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	
1006	VLAN1006	active	

```
Switch#show vtp status
```

```
VTP Version : running VTP1 (VTP2 capable)
```

```
Configuration Revision : 0
```

```
Maximum VLANs supported locally : 1005
```

```
Number of existing VLANs : 7
```

VTP Operating Mode : Transparent

VTP Domain Name :

四、应用场景

在大型网络环境或在运营商网络环境下分配 VLAN 时要用到扩展 VLAN（1006~4095）的情况下。

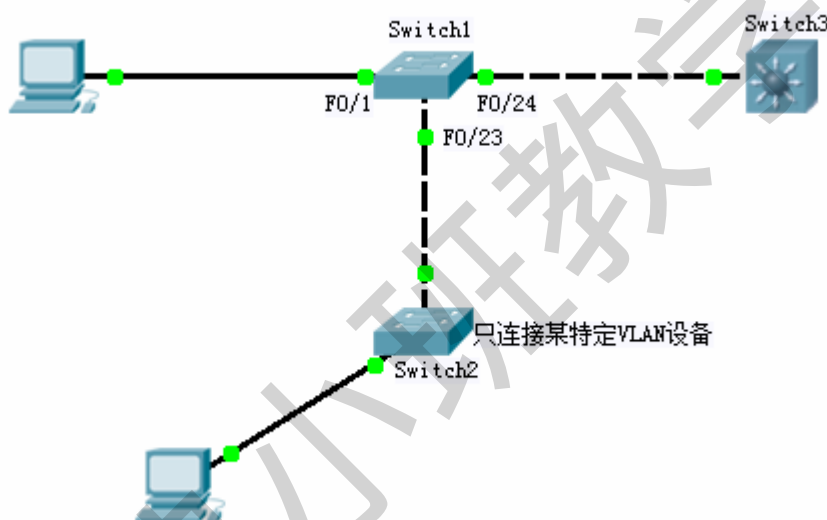
交换机端口操作模式设置

一、实验目的

- 1、掌握交换机端口各操作模式的作用
- 2、掌握交换机端口各操作模式的配置

二、实验内容

拓扑图：



需求：

根据实际情况，为交换机各端口指定符合需求的操作模式。

三、实验配置

知识点链接：

交换机端口的操作模式：

Access: 常用于连接终端设备；特点是只能承载一个 VLAN 的信息

Trunk: 常用于交换机间连接；特点是不属于任何 VLAN，但能承载所有 VLAN 信息

Dynamic: 通过 DTP 协议，动态协商为 access 或 trunk 模式；DTP 有四种协商模式，分别为：on、off、desirable、auto

配置：

- 1、查看交换机端口默认工作模式

```
Switch#show running-config interface fastEthernet 0/1
```

```
interface FastEthernet0/1
```

```
switchport mode dynamic desirable
```

 (端口默认的操作模式)

```
Switch1#show interfaces fastEthernet 0/1 switchport
```

```
Name: Fa0/1
```

```
Switchport: Enabled
```

```
Administrative Mode: dynamic desirable (端口默认的操作模式)
```

```
Operational Mode: static access (动态协商后的操作模式为: Access)
```

2、修改交换机端口的操作模式

```
Switch1(config)#interface fastEthernet 0/1
```

```
Switch1(config-if)#switchport mode access (手动指定交换机的端口操作模式为: access)
```

```
Switch1(config)#interface fastEthernet 0/23
```

```
Switch1(config-if)#switchport mode access
```

```
Switch1(config)#interface fastEthernet 0/24
```

```
Switch1(config-if)#switchport mode trunk (手动指定交换机的端口操作模式为: trunk)
```

```
Switch3(config)#interface fastEthernet 0/24
```

★

```
Switch3(config-if)#switchport trunk encapsulation dot1q
```

```
Switch3(config-if)#switchport mode trunk
```

Cisco 3550、3560 交换机端口的操作模式改为 Trunk 时，应先修改端口的封装类型为：802.1Q 或 ISL

验证：

```
Switch1#show interfaces fa0/1 switchport
```

```
Name: Fa0/1
```

```
Switchport: Enabled
```

```
Administrative Mode: static access
```

```
Operational Mode: static access
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: native
```

```
Negotiation of Trunking: Off
```

```
Switch1#show interfaces fa0/24 switchport
```

```
Name: Fa0/24
```

```
Switchport: Enabled
```

```
Administrative Mode: trunk
```

```
Operational Mode: trunk
```

```
Administrative Trunking Encapsulation: dot1q
```

```
Operational Trunking Encapsulation: dot1q
```

```
Negotiation of Trunking: On
```

Cisco 2950、2960 交换机 trunk 端口的默认封装类型为（仅为）802.1Q

四、应用场景

在交换网络中，为保证二层网络的安全性，最好手动指定各端口的操作模式（虽然动态协商能简化配置），关闭其他不用端口。

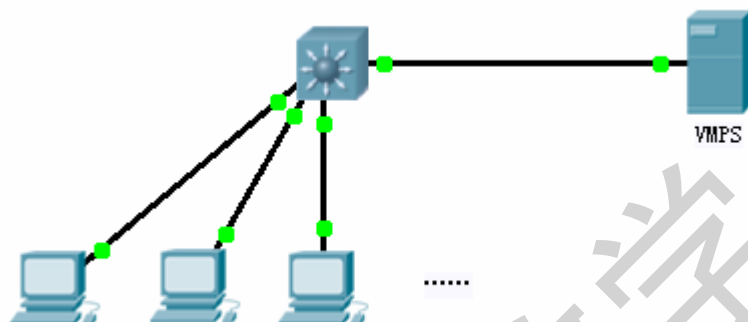
VLAN 端口划分

一、实验目的

- 1、掌握交换机端口划分到 VLAN 的方法

二、实验内容

拓扑图：



需求：

为不同的客户划分 VLAN

三、实验配置

配置：

- 1、手动为端口划分 VLAN

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
```

- 2、动态为端口划分 VLAN (VMPS)

```
Switch(config)#interface range fastEthernet 0/1 - 20 (对一组端口操作)
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport access vlan dynamic
```

验证：

```
Switch#show vlan brief
```

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12
2 VLAN0002	active	
3 customer	active	
10 VLAN0010	active	Fa0/1

开启端口动态 VLAN 划分。
注：需在 VMPS 服务器上构建 VLAN-MAC 的映射数据库

四、应用场景

在大型网络环境下分配 VLAN 时，通过动态 VLAN 可以简化配置，并可提高网络的安全性。

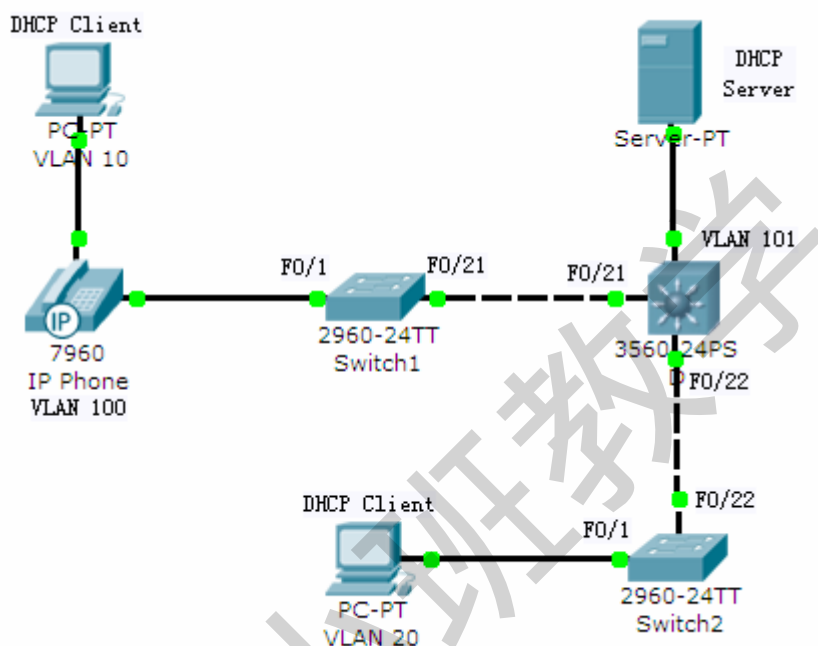
VLAN VTP 设置

一、实验目的

- 1、掌握交换机 VTP 的应用及配置

二、实验内容

拓扑图：



需求：

- 1、简化 VLAN 的配置
- 2、减少 VLAN 的泛洪
- 3、确保 VLAN 信息的安全

三、实验配置

配置：

- 1、在 3560 上查看 VTP 信息

Switch#show vtp status

```
VTP Version : 2 (VTP 协议版本号, V2 版本增加对令牌环网的支持)
Configuration Revision : 0 (VTP 的配置版本号, 指示 VLAN 的变更信息)
Maximum VLANs supported locally : 1005 (指示交换机最多能够配置的 VLAN 数量)
Number of existing VLANs : 5 (指示现有 VLAN 的数量)
VTP Operating Mode : Server (VTP 的操作模式: Server、Client、Transparent)
VTP Domain Name : (VTP 的管理域, 缺省为空 (Null))
VTP Pruning Mode : Disabled (VTP 的修剪模式, 处于关闭状态)
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x7D 0x5A 0xA6 0x0E 0x9A 0x72 0xA0 0x3A (VTP 加密信息)
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```


Local updater ID is 0.0.0.0 (no valid interface found)

2 配置 VLAN (略)

3、配置交换机间 Trunk 链路 (略; 注: VTP 工作在 Trunk 链路上)

4、在核心交换机上配置 VTP 相关参数

SW3560#vlan database (进入 VLAN Database 模式下配置; 但建议在全局模式下配置)

SW3560(config)#vtp mode server (修改 VTP 的操作模式为 Server)

SW3560(config)#vtp domain kinglab (修改 VTP 的管理域 (Domain) 为 kinglab)

Changing VTP domain name from NULL to kinglab (默认 VTP 的 Domain 为空 (Null))

SW3560(config)#vtp pruning (开启 VTP 修剪功能, 防止 VLAN 数据泛洪, 提高有效带宽)

Pruning switched on

SW3560(config)#vtp password kinglab (设置 VTP 密码, 保护 VTP 信息)

Setting device VLAN database password to kinglab

5、在其他交换机上配置 VTP 相关参数 (配置同上, 略; 注: VTP 模式改为 Client)

验证:

SW3560#show vtp status

VTP Version : running VTP1 (VTP2 capable)

Configuration Revision : 3

Maximum VLANs supported locally : 1005

Number of existing VLANs : 7

VTP Operating Mode : Server

VTP Domain Name : kinglab

VTP Pruning Mode : Enabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0xF8 0x24 0xC2 0xE0 0x9B 0x33 0x92 0x0E

*** MD5 digest checksum mismatch on trunk: Fa0/21 *** (其他交换机没配置 password 时)

*** MD5 digest checksum mismatch on trunk: Fa0/22 ***

*** MD5 digest checksum mismatch on trunk: Fa0/23 ***

*** MD5 digest checksum mismatch on trunk: Fa0/24 ***

Configuration last modified by 0.0.0.0 at 3-1-93 00:04:49

Local updater ID is 0.0.0.0 (no valid interface found)

SW2960#show vtp status

VTP Version : 2

Configuration Revision : 3

Maximum VLANs supported locally : 128

Number of existing VLANs : 7

VTP Operating Mode : Client

VTP Domain Name : kinglab

```
VTP Pruning Mode           : Enabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x8A 0x4E 0xDA 0x4F 0x09 0xCC 0x50 0x04
Configuration last modified by 0.0.0.0 at 3-1-93 01:57:45
```

四、应用场景

通过 VTP 的配置，可以大大简化企业 VLAN 的部署，但是请尽量避免使用 VTP 部署方法。确实要部署请一定要注意 vtp Revision 的问题。

经典小班教学

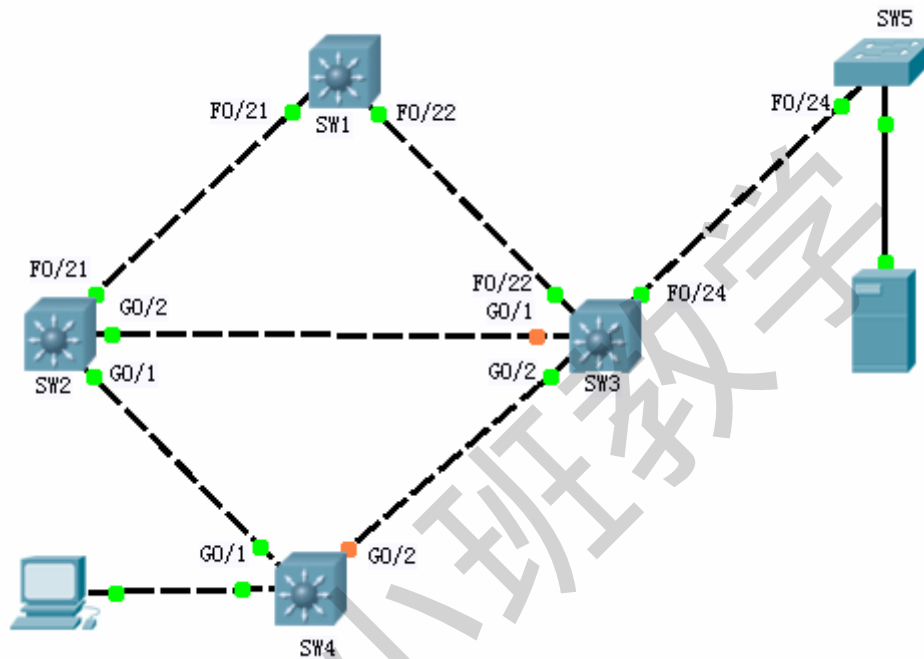
Spanning Tree Protocol (STP 802.1D)

一、实验目的

- 1、掌握标准生成树（STP）的应用及配置

二、实验内容

拓扑图：



需求：

- 1、确保 PC 和服务间通信路径最短（注：橙色端口为阻塞端口）

三、实验配置

配置：

- 1、查看生成树

SW1#show spanning-tree （查看生成树）

VLAN0001 （VLAN1 的生成树实例）

Spanning tree enabled protocol ieee （生成树的模式为 802.1D 标准生成树）

Root ID Priority 32769 （指示生成树根的 Root ID，SW1 为根桥）

Address 0004.9A8B.7C69

This bridge is the root （指示此交换机为 Vlan1 生成树的根）

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec （生成树计时器）

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1) （指示此交换机的 BridgeID）

Address 0004.9A8B.7C69

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Aging Time 20

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----------	------	-----	------	-------	-----	------

```

Fa0/21      Desg FWD 19      128.21  P2p      (端口角色、状态及端口优先级)
Fa0/22      Desg FWD 19      128.22  P2p

```

SW3#show spanning-tree (SW3 为非根桥)

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      32769
Address      0004.9A8B.7C69
Cost         19
Port         22(FastEthernet0/22)
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

```

```

Bridge ID    Priority      32769 (priority 32768 sys-id-ext 1)
Address      00E0.A39D.C5A3
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   20

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/22	Root	FWD	19	128.22	P2p
Fa0/24	Desg	FWD	19	128.24	P2p
Gi0/1	Altn	BLK	4	128.25	P2p
Gi0/2	Desg	FWD	4	128.26	P2p

2、根据需求，应该让 SW3 为 STP 的 Root 最为合理

SW3(config)#spanning-tree vlan 1 root primary (修改 SW3 的 VLAN1 生成树实例为根桥)

验证:

SW3#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

```

Root ID      Priority      24577
Address      00E0.A39D.C5A3

```

This bridge is the root

```

Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

```

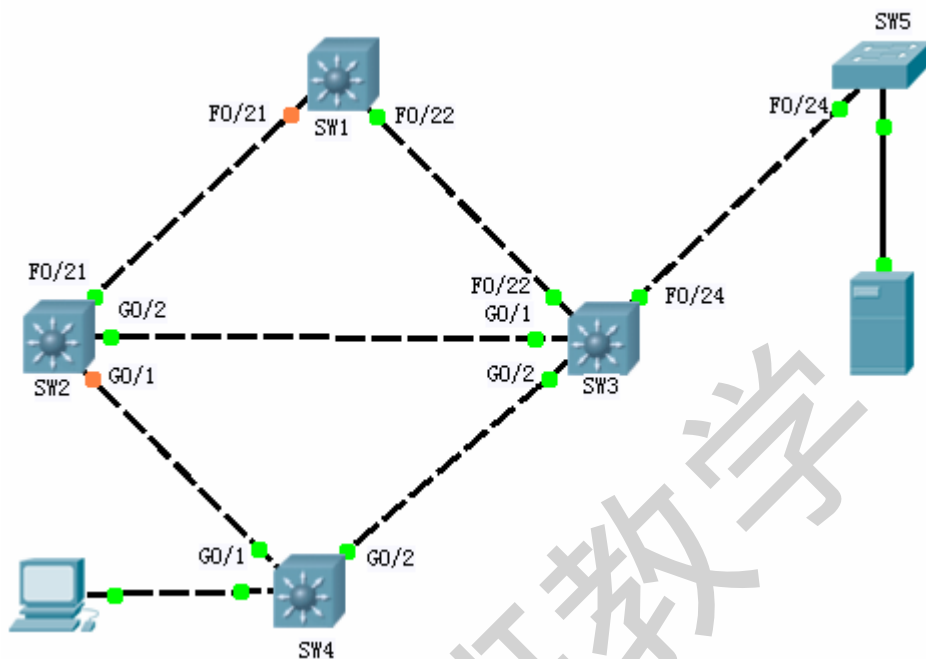
```

Bridge ID    Priority      24577 (priority 24576 sys-id-ext 1)
Address      00E0.A39D.C5A3
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   20

```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/22	Desg	FWD	19	128.22	P2p

Fa0/24	Desg FWD 19	128.24	P2p
Gi0/1	Desg FWD 4	128.25	P2p
Gi0/2	Desg FWD 4	128.26	P2p



四、应用场景

STP 协议对用户是透明的。自动会选举出 block 端口，阻止环路。但我们一定注意 STP 选举有可能选择出的路径不是最优的。这时候我们就要调整 STP 参数。达到流量优化的目的。

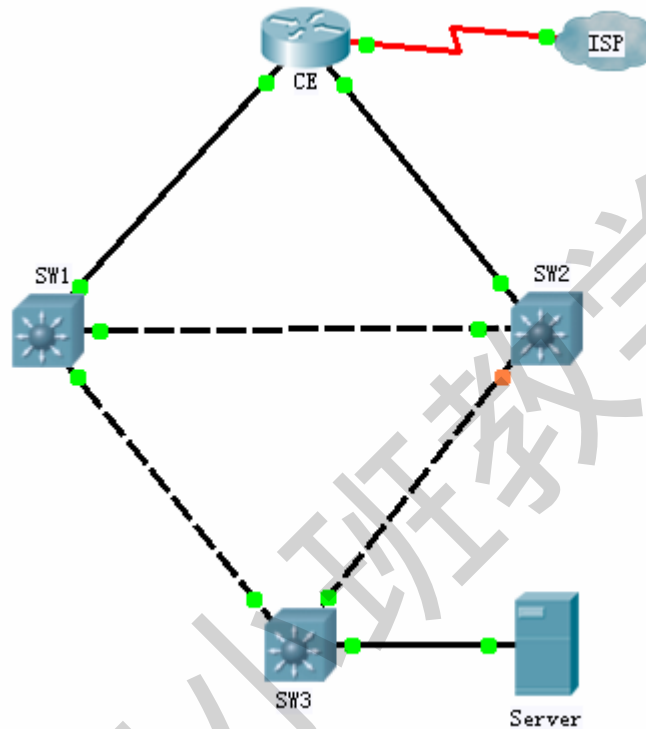
PVST+ & RSTP

一、实验目的

- 1、掌握 PVST+ 的应用及配置
- 2、掌握 RSTP 的应用及配置

二、实验内容

拓扑图：



需求：

- 1、加快 STP 的收敛，匹配动态路由的收敛（注：在内网运行 OSPF）

三、实验配置

配置：

- 1、在所有连接非交换机的端口配置快速端口

SW3(config)#spanning-tree portfast default （在全局下开启 PVST+ 的快速端口）

SW3(config)#interface fastEthernet 0/1

SW3(config-if)#switchport mode access

SW3(config-if)#spanning-tree portfast （在端口下开启 PVST+ 的快速端口）

- 2、开启快速上行链路

SW1(config)#spanning-tree uplinkfast （在全局下开启快速上行链路，其他交换机同配置）

- 3、开启快速骨干链路

Switch(config)#spanning-tree backbonefast （在全局下开启快速骨干链路，其他交换机同配置）

4、或者替代步骤 2、3；启用 RSTP

Switch(config)#spanning-tree mode rapid-pvst (开启 RSTP 生成树模式)

验证：

1、观察

开启 Portfast 功能的端口，连上 PC 后，端口颜色立马变成绿色（没开启时，端口颜色由橙色变绿色，一般需 30 秒）

2、查看生成树

Switch#show spanning-tree

VLAN0001

Spanning tree enabled protocol rstp (生成树模式为 RSTP)

```
Root ID    Priority    32769
  Address   0009.7ca7.7d00
    Cost    3019
    Port    23 (FastEthernet0/23)
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
```

```
Bridge ID  Priority    49153 (priority 49152 sys-id-ext 1)
  Address   0011.9391.2680
  Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Aging Time 300
```

UplinkFast enabled but inactive in rapid-pvst mode

Interface	Role	Sts	Cost	Prio.	Nbr	Type
-----	-----	-----	-----	-----	-----	-----
Fa0/21	Altn	BLK	3019	128.	21	P2p Peer (STP)
Fa0/22	Altn	BLK	3019	128.	22	P2p Peer (STP)
Fa0/23	Root	FWD	3019	128.	23	P2p Peer (STP)
Fa0/24	Altn	BLK	3019	128.	24	P2p Peer (STP)

四、应用场景

加快应网络拓扑发生变化而导致的收敛速度

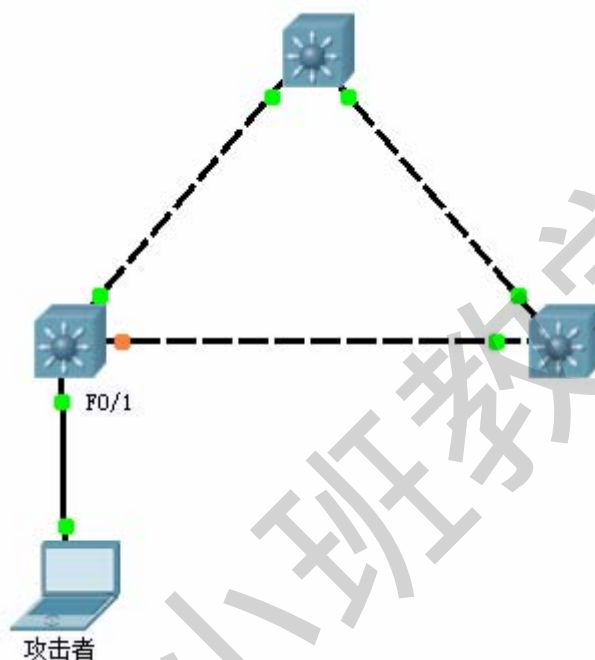
生成树防护 (STP Guard)

一、实验目的

- 1、掌握生成树防护的应用及配置

二、实验内容

拓扑图：



需求：

- 1、防止攻击者使用 STP 攻击网络

三、实验配置

配置：

```
Switch(config)#interface fastEthernet 0/1
```

```
Switch(config-if)#switchport mode access
```

```
Switch(config-if)#spanning-tree bpduguard enable
```

(启用 BPDU 过滤功能，在此端口不接受/发送 BPDU 报文)

```
Switch(config-if)#spanning-tree bpduguard enable
```

(启用 BPDU 防护功能，在此端口不接受 BPDU；收到 BPDU，端口禁用)

```
Switch(config-if)#spanning-tree guard root
```

(启用 STP 根防护功能，在此端口不接受拥有更优 BID 的 BPDU 报文)

验证：

1、Switch#show spanning-tree interface fastEthernet 0/24 detail

Port 24 (FastEthernet0/24) of VLAN0001 is designated forwarding
Port path cost 3019, Port priority 128, Port Identifier 128.24.
Designated root has priority 32769, address 0009.7ca7.7d00
Designated bridge has priority 49153, address 0011.9391.2680
Designated port id is 128.24, designated path cost 3019
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
Bpdu guard is enabled (端口启用 BPDU 防护)
Bpdu filter is enabled (端口启用了 BPDU 过滤)
Root guard is enabled on the port (端口启用根防护)
BPDU: sent 0, received 0 (在此端口没收发任何 BPDU 报文)

经典小班教学

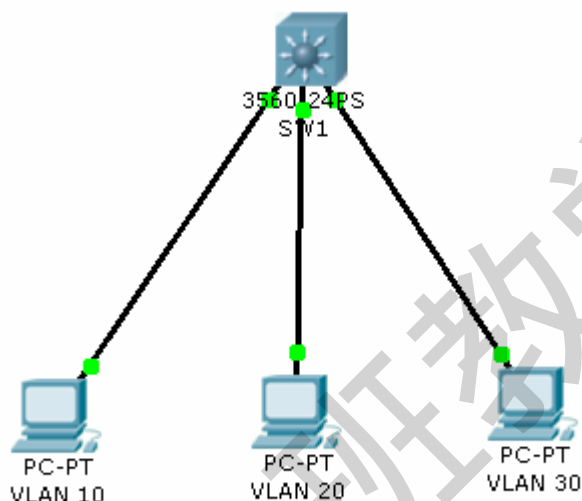
SVI 实验

一、实验目的

掌握多层交换机 SVI 接口的配置方法

二、实验内容

拓扑图：



需求：3 台 PC 分别在 3 个 VLAN 分别是 VLAN 10.20.30 在交换机配置

SVI 三层接口让 VLAN 之间能够互相访问。

三、实验配置

SW (config) #interface fa0/1 把连接 VLAN10 的主机划入 VLAN10

SW(config-if)#switchport mode access

SW(config-if)#switchport access vlan 10

SW (config) #interface fa0/2 把连接 VLAN20 的主机划入 VLAN20

SW(config-if)#switchport mode access

SW(config-if)#switchport access vlan 20

SW (config) #interface fa0/3 把连接 VLAN30 的主机划入 VLAN30

SW(config-if)#switchport mode access

SW(config-if)#switchport access vlan 30

SW (config) #interface vlan 10 进入三层 SVI 接口

SW(config-if)#ip address 10.1.1.254 255.255.255.0

SW (config) #interface vlan 20 进入三层 SVI 接口

SW(config-if)#ip address 20.1.1.254 255.255.255.0

SW (config) #interface vlan 30 进入三层 SVI 接口

SW(config-if)#ip address 30.1.1.254 255.255.255.0

主机配置：

主机配置好对应 VLAN 的 IP 地址，网关全部指向 SVI 接口。

验证：

所有不同的 VLAN 主机可以互相 ping 通。

四、应用场景

在园区网内部实现 VLAN 之间的访问。

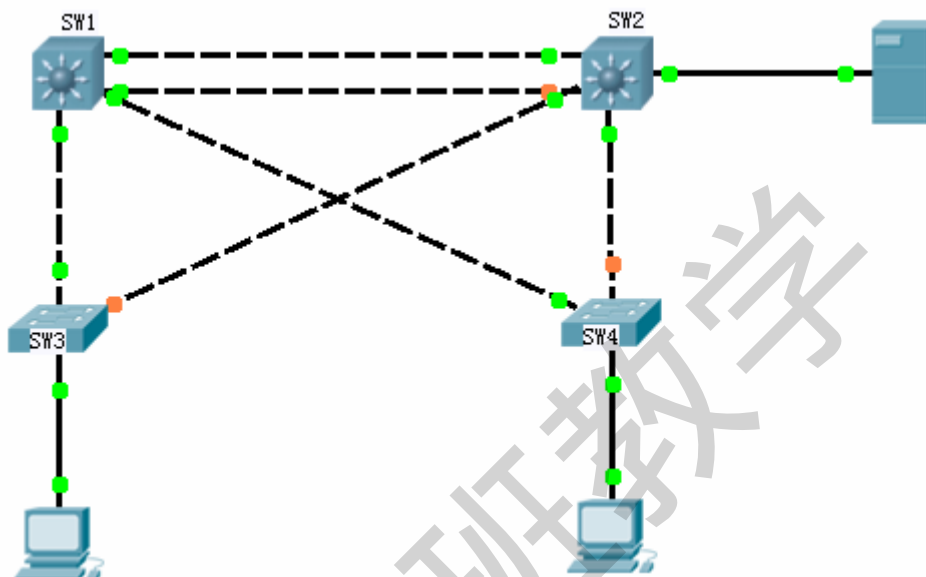
EtherChannel

一、实验目的

- 1、掌握 EtherChannel 的应用及配置

二、实验内容

拓扑图：



需求：

- 1、启用 Etherchannel，实现多链路捆绑及负载均衡

三、实验配置

配置：

1、Layer2 Etherchannel 配置

```
SW1(config)#interface port-channel 1 （创建以太通道端口）
```

```
SW1(config-if)#channel-group 1 mode desirable （配置以太通道协议 PAGP 的操作模式为：协商）
```

```
SW1(config-if)#channel-protocol pagp （配置以太通道的协议模式为 pagp，可选）
```

```
SW1(config)# interface range gigabitEthernet 0/1 - 2
```

```
SW1(config-if)#channel-group 1 mode desirable （在端口关联以太通道端口）
```

注：以上是先创建后关联

```
SW2(config)#interface range gigabitEthernet 0/1 - 2
```

```
SW2(config-if-range)#switchport trunk encapsulation dot1q
```

```
SW2(config-if-range)#switchport mode trunk
```

```
SW2(config-if-range)#channel-group 1 mode desirable
```

```
SW2(config-if-range)#channel-protocol pagp
```

注：以上配置是直接在端口关联以太通道，系统会自动创建以太通道

2、Layer3 Etherchannel 配置

```
SW2(config)#interface range gigabitEthernet 0/1 - 2
```

```
SW2(config-if-range)#no switchport (关键，开启接口三层端口)
```

```
SW2(config-if-range)#channel-group 1 mode desirable
```

```
SW2(config-if-range)#channel-protocol pagp
```

```
SW2(config)#interface port-channel 1
```

```
SW2(config-if)#no switchport (关键，开启三层以太通道端口；注意确保接口的二层端口开启)
```

```
SW2(config-if)#ip address X.X.X.X 255.255.255.0
```

注：Layer3 Etherchannel 要注意配置次序

3、Etherchannel 负载均衡方式

```
Switch(config)#port-channel load-balance ? (修改 Etherchannel 的负载均衡方式)
```

```
dst-ip      Dst IP Addr
dst-mac     Dst Mac Addr
src-dst-ip  Src XOR Dst IP Addr
src-dst-mac Src XOR Dst Mac Addr
src-ip      Src IP Addr
src-mac     Src Mac Addr
```

验证：

```
Switch#show etherchannel port-channel (查看 Etherchannel 的相关参数)
```

```
Channel-group listing:
```

```
Group: 1
```

```
Port-channels in the group:
```

```
Port-channel: Po1
```

```
Age of the Port-channel = 00d:00h:32m:28s
```

```
Logical slot/port = 2/1 Number of ports = 2
```

```
GC = 0x00000000 HotStandBy port = null
```

```
Port state = Port-channel (Etherchannel 协议状态，现在为 L2)
```

```
Protocol = PAGP (Etherchannel 协议类型)
```

```
Port Security = Disabled
```

```
Ports in the Port-channel:
```

```
Index Load Port EC state No of bits
```

```
-----+-----+-----+-----+-----+
0      00      Gig0/1  Desirable-Sl      0      (Etherchannel 协议协工作模式)
0      00      Gig0/2  Desirable-Sl      0
Time since last port bundled:    00d:00h:25m:12s    Gig0/2
```

四、应用场景

网络骨干链路上实现高带宽、链路备份、负载均衡

经典小班教学

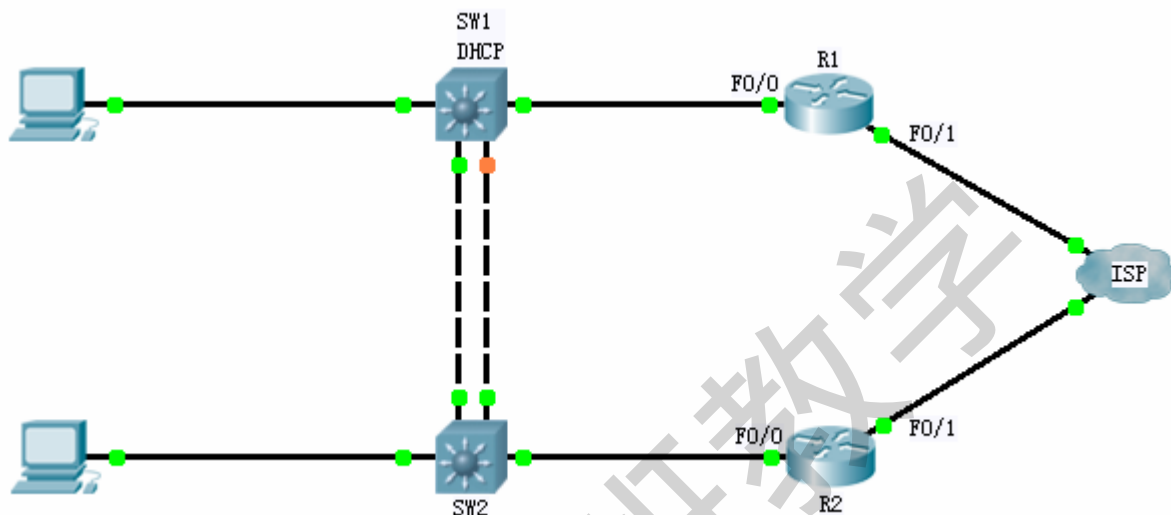
Hot Standby Router Protocol (HSRP)

一、实验目的

- 1、掌握 HSRP 的应用及配置

二、实验内容

拓扑图：



需求：

- 1、实现链路、设备热备

三、实验配置

配置：

PC 上设置好正确的 IP 地址，注意网关指向 HSRP 的虚拟地址（192.168.1.254）

- 1、在 R1 上配置 HSRP

```
R1(config)#interface fastEthernet 0/0
```

```
R1(config-if)#standby 1 ip 192.168.1.254
```

（设置 HSRP 虚拟路由器的 IP 地址为：192.168.1.254）

```
R1(config-if)#standby 1 priority 105
```

（设置 HSRP 的优先级值；值越大优先级越高）

```
R1(config-if)#standby 1 preempt
```

（设置 HSRP 根据优先级值抢占 Active 角色功能）

```
R1(config-if)#standby 1 track fa0/1
```

（开启 HSRP 对接口的 Track 功能）

- 2、在 R2 上配置 HSRP

```
R2(config)#interface fastEthernet 0/0
```

```
R2(config-if)#standby 1 ip 192.168.1.254
```

```
R2(config-if)#standby 1 priority 100
```

（设置 HSRP 的优先级值；缺省为 100，可以不设）

```
R2(config-if)#standby 1 preempt
```

```
R2(config-if)#standby 1 track fa0/1
```

3、在 SW1 上配置 DHCP，宣告 PC 的网关地址为 192.168.1.254 （略）

验证：

1、查看 HSRP 协议相关信息

R1#show standby

FastEthernet0/0 - Group 1

State is Active （路由器 HSRP 的状态）

2 state changes, last state change 00:00:06

Virtual IP address is 192.168.1.254 （HSRP 的虚拟 IP 地址，需手动指定）

Active virtual MAC address is 0000.0c07.ac01 （HSRP 的虚拟 MAC 地址，系统自动分配）

Local virtual MAC address is 0000.0c07.ac01 (v1 default)

Hello time 3 sec, hold time 10 sec （HSRP 的 Hello 时间）

Next hello sent in 1.924 secs

Preemption enabled （HSRP 抢占功能开启）

Active router is local

Standby router is 192.168.1.2, priority 100 （192.168.1.2 为 HSRP 的 Standby 路由器）

Priority 105 (configured 105) （配置的优先级值为 105）

Track interface FastEthernet0/1 state Up decrement 10 （开启了 Track 功能，惩罚值为 10）

Group name is "hsrp-Fa0/0-1" (default) （HSRP 热备组名称）

2、Debug HSRP 的交互报文

R1#debug standby

*Mar 1 01:03:48.015: HSRP: Fa0/0 Grp 1 Hello out 192.168.1.1 Active pri 105 vIP 192.168.1.254

*Mar 1 01:03:48.683: HSRP: Fa0/0 Grp 1 Hello in 192.168.1.2 Standby pri 100 vIP 192.168.1.254

*Mar 1 01:03:49.135: HSRP: Fa0/0 Grp 1 Hello out 192.168.1.1 Active pri 105 vIP 192.168.1.254

当 R1 的 F0/1 端口发生故障

*Mar 1 01:07:13.283: %TRACKING-5-STATE: 1 interface Fa0/1 line-protocol Up->Down

*Mar 1 01:07:13.283: HSRP: Fa0/0 Grp 1 Track 1 object changed, state Up -> Down

*Mar 1 01:07:13.283: HSRP: Fa0/0 Grp 1 Priority 105 -> 95

*Mar 1 01:07:13.291: HSRP: Fa0/0 Grp 1 Hello in 192.168.1.2 Standby pri 100 vIP 192.168.1.254

*Mar 1 01:07:14.487: HSRP: Fa0/0 Grp 1 Hello out 192.168.1.1 Active pri 95 vIP 192.168.1.254

*Mar 1 01:07:19.407: HSRP: Fa0/0 Interface adv in, Active, active 1, passive 0, from 192.168.1.2

*Mar 1 01:07:19.411: HSRP: Fa0/0 Grp 1 Active router is 192.168.1.2, was local

*Mar 1 01:07:19.411: HSRP: Fa0/0 Nbr 192.168.1.2 active for group 1

*Mar 1 01:07:19.415: HSRP: Fa0/0 Grp 1 Standby router is unknown, was 192.168.1.2

*Mar 1 01:07:19.415: HSRP: Fa0/0 Nbr 192.168.1.2 no longer standby for group 1 (Active)


```
*Mar 1 01:07:19.415: HSRP: Fa0/0 Grp 1 Active: g/Hello rcvd from higher pri Active router
(100/192.168.1.2)
*Mar 1 01:07:19.415: HSRP: Fa0/0 Grp 1 Active -> Speak
*Mar 1 01:07:19.419: HSRP: Fa0/0 Interface adv out, Passive, active 0 passive 1
*Mar 1 01:07:19.419: HSRP: Fa0/0 Grp 1 Redundancy "hsrp-Fa0/0-1" state Active -> Speak
*Mar 1 01:07:19.419: HSRP: Fa0/0 Grp 1 Resign out 192.168.1.1 Speak pri 95 vIP 192.168.1.254
*Mar 1 01:07:19.427: HSRP: Fa0/0 Grp 1 Deactivating MAC 0000.0c07.ac01
*Mar 1 01:07:19.427: HSRP: Fa0/0 Grp 1 Removing 0000.0c07.ac01 from MAC address filter
*Mar 1 01:07:19.431: HSRP: Fa0/0 Grp 1 MAC addr update Delete from SMF 0000.0c07.ac01
*Mar 1 01:07:19.431: HSRP: Fa0/0 Grp 1 Hello out 192.168.1.1 Speak pri 95 vIP 192.168.1.254
*Mar 1 01:07:19.435: HSRP: Fa0/0 IP Redundancy "hsrp-Fa0/0-1" update, Active -> Speak
*Mar 1 01:07:19.459: HSRP: Fa0/0 Interface adv in, Passive, active 0, passive 1, from 192.168.1.2
*Mar 1 01:07:19.463: HSRP: Fa0/0 Grp 1 Resign in 192.168.1.2 Speak pri 100 vIP 192.168.1.254
*Mar 1 01:07:19.463: HSRP: Fa0/0 Grp 1 Active router is unknown, was 192.168.1.2
*Mar 1 01:07:19.463: HSRP: Fa0/0 Nbr 192.168.1.2 no longer active for group 1 (Speak)
*Mar 1 01:07:19.467: HSRP: Fa0/0 Nbr 192.168.1.2 Was active or standby - start passive holddown
*Mar 1 01:07:19.467: HSRP: Fa0/0 Grp 1 Hello in 192.168.1.2 Speak pri 100 vIP 192.168.1.254
*Mar 1 01:07:19.467: HSRP: Fa0/0 Grp 1 Speak: f/Hello rcvd from higher pri Speak router
(100/192.168.1.2)
*Mar 1 01:07:19.471: HSRP: Fa0/0 Grp 1 Speak -> Listen
*Mar 1 01:07:19.471: HSRP: Fa0/0 Grp 1 Redundancy "hsrp-Fa0/0-1" state Speak -> Backup
*Mar 1 01:07:19.471: HSRP: Fa0/0 Interface adv in, Active, active 1, passive 1, from 192.168.1.2
*Mar 1 01:07:19.471: HSRP: Fa0/0 Nbr 192.168.1.2 Adv in, active 1 passive 1
*Mar 1 01:07:19.475: HSRP: Fa0/0 Nbr 192.168.1.2 is no longer passive
*Mar 1 01:07:19.475: HSRP: Fa0/0 Nbr 192.168.1.2 destroyed
*Mar 1 01:07:19.475: HSRP: Fa0/0 Grp 1 Coup in 192.168.1.2 Speak pri 100 vIP 192.168.1.254
*Mar 1 01:07:19.475: HSRP: Fa0/0 Grp 1 Active router is 192.168.1.2
*Mar 1 01:07:19.479: HSRP: Fa0/0 Nbr 192.168.1.2 created
*Mar 1 01:07:19.479: HSRP: Fa0/0 Nbr 192.168.1.2 active for group 1
*Mar 1 01:07:19.479: HSRP: Fa0/0 Interface adv out, Passive, active 0 passive
*Mar 1 01:07:19.483: HSRP: Fa0/0 Interface adv in, Active, active 1, passive 0, from 192.168.1.2
*Mar 1 01:07:19.483: HSRP: Fa0/0 IP Redundancy "hsrp-Fa0/0-1" update, Speak -> Backup
*Mar 1 01:07:19.879: HSRP: Fa0/0 Grp 1 Hello in 192.168.1.2 Active pri 100 vIP 192.168.1.254
```

四、应用场景

网络骨干链路上实现双出口链路、设备热备、负载均衡功能

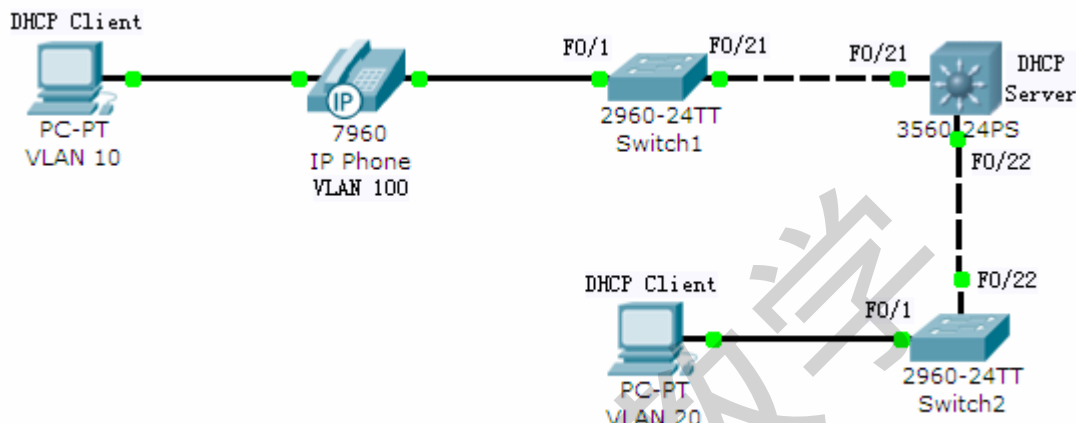
动态地址分配 (DHCP)

一、实验目的

- 1、掌握 DHCP Server 的配置及应用

二、实验内容

拓扑图：



需求：

- 1、3560-24PS 为 DHCP Server；
- 2、分别为 VLAN10、VLAN20 内的 PC 动态分配 IP 地址；
- 3、为 VLAN100 内的 IP Phone 绑定 IP 地址，并设置 TFTP 为 192.168.100.253 。

三、实验配置

配置：

- 1、开启 DHCP Server 功能

```
Switch(config)#service dhcp
```

- 2、排除已分配的固定 IP 地址

```
Switch(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.100
```

- 3、创建 DHCP 地址池

```
Switch(config)#ip dhcp pool VLAN10 (对 VLAN 10 配置地址池)
```

```
Switch(dhcp-config)#network 192.168.10.0 /24 (设置地址池网段)
```

```
Switch(dhcp-config)#default-router 192.168.10.254 (设置默认网关地址)
```

```
Switch(dhcp-config)#dns-server 202.96.209.133 202.96.209.134 (设置 DNS 地址)
```

```
Switch(dhcp-config)#lease 0 8 (设置 IP 地址租期：8 小时)
```

```
Switch(config)#ip dhcp pool VLAN20
```

```
Switch(dhcp-config)#network 192.168.20.0 /24
```

```
Switch(dhcp-config)#default-router 192.168.20.254
```

```
Switch(dhcp-config)#dns-server 202.96.209.133 202.96.209.134
```

```
Switch(dhcp-config)#lease 0 8
```

```
Switch(config)#ip dhcp pool Phone8001
```

```
Switch(dhcp-config)#hardware-address aabb.ccdd.eeff (绑定 Phone/PC 的 MAC 地址)
```

```
Switch(dhcp-config)#host 192.168.100.1 /24 (绑定 IP 地址)
```

```
Switch(dhcp-config)#default-router 192.168.20.254
```

```
Switch(dhcp-config)#option 150 ip 192.168.100.253 (设置 CISCO VOIP 的 TFTP Server 地址)
```

```
Switch(dhcp-config)#lease infinite
```

验证:

```
Switch#show ip dhcp binding
```

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.10.101	0100.2264.4bab.eb	Mar 01 1993 08:22 AM	Automatic
192.168.100.1	aabb.ccdd.eeff	Infinite	Manual

四、应用场景

此 DHCP 配置方案主要应用在中大型网络中;

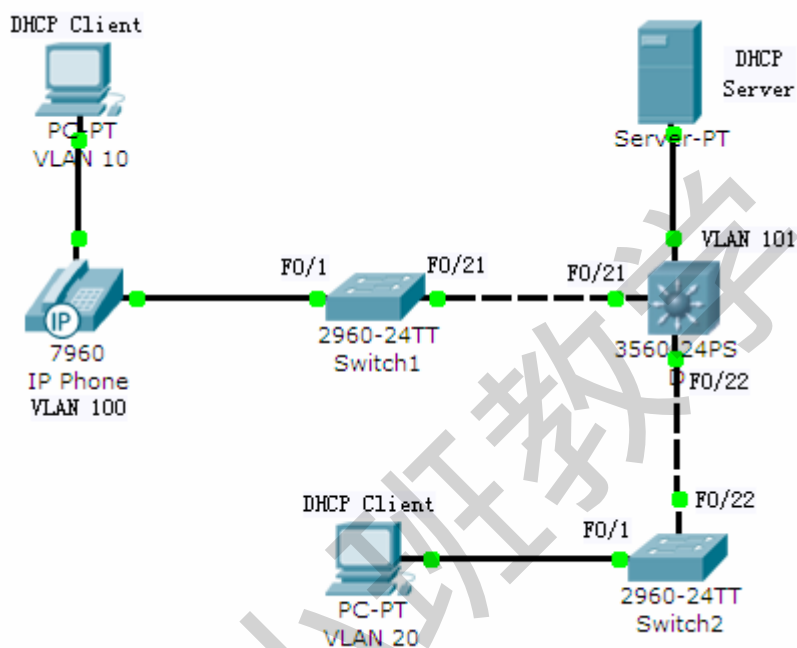
DHCP 中继

一、实验目的

- 1、掌握 DHCP 中继的应用

二、实验内容

拓扑图：



需求：

- 1、VLAN 10、VLAN 20 内的 PC 能够从 DHCP Server (Server-PT) 动态获得 IP 地址；
- 2、DHCP Server (Server-PT) 属于 VLAN 101；

三、实验配置

配置思路：

DHCP 工作时使用广播地址，同时 PC 和 DHCP Server 又不在同一 VLAN 中，而 VLAN 拥有分割广播域的作用，从而导致 PC 不能从 DHCP Server 获取 IP 地址。这就需要在负责 VLAN 间路由的 3560-24PS 的交换机上启用 DHCP 中继来解决问题。

配置

- 1、开启 3560-24PS 的 DHCP 服务功能

```
Switch(config)#service dhcp
```

- 2、开启路由功能

```
Switch(config)#ip routing
```

- 3、开启 DHCP 中继功能

```
Switch(config)#ip dhcp relay information option
```

```
Switch(config)#interface vlan 10
```

```
Switch(config-if)#ip helper-address 192.168.101.1 (设置中继目标地址为 DHCP Server )
```

验证:

```
Switch#debug ip dhcp server packet
```

```
*Mar 1 01:42:58.663: DHCPD: incoming interface name is Vlan10
*Mar 1 01:42:58.663: DHCPD: Looking up binding using address 192.168.10.254
*Mar 1 01:42:58.663: DHCPD: setting giaddr to 192.168.10.254.
*Mar 1 01:42:58.663: DHCPD: adding relay information option.
*Mar 1 01:42:58.663: DHCPD: BOOTREQUEST from 0100.2264.4bab.eb forwarded to 192.168.20.1.
*Mar 1 01:42:58.667: DHCPD: incoming interface name is Vlan20
*Mar 1 01:42:58.667: DHCPD: forwarding BOOTREPLY to client 0022.644b.abeb.
*Mar 1 01:42:58.667: old_giaddr = 0.0.0.0, giaddr=0.0.0.0, flag=0
*Mar 1 01:42:58.667: DHCPD: Option82 is currently:
*Mar 1 01:42:58.667: 020c020a0000c0a80afe0a000000
*Mar 1 01:42:58.667: DHCPD: Removing option82 information
*Mar 1 01:42:58.667: DHCPD: Option82 is removed
*Mar 1 01:42:58.667: DHCPD: broadcasting BOOTREPLY to client 0022.644b.abeb.
*Mar 1 01:43:02.731: DHCPD: incoming interface name is Vlan10
*Mar 1 01:43:02.731: DHCPD: Looking up binding using address 192.168.10.254
*Mar 1 01:43:02.731: DHCPD: setting giaddr to 192.168.10.254.
*Mar 1 01:43:02.731: DHCPD: adding relay information option.
*Mar 1 01:43:02.731: DHCPD: BOOTREQUEST from 0100.2264.4bab.eb forwarded to 192.168.20.1.
*Mar 1 01:43:02.735: DHCPD: incoming interface name is Vlan20
*Mar 1 01:43:02.735: DHCPD: forwarding BOOTREPLY to client 0022.644b.abeb.
*Mar 1 01:43:02.735: old_giaddr = 0.0.0.0, giaddr=0.0.0.0, flag=0
*Mar 1 01:43:02.735: DHCPD: Option82 is currently:
*Mar 1 01:43:02.735: 020c020a0000c0a80afe0a000000
*Mar 1 01:43:02.735: DHCPD: Removing option82 information
*Mar 1 01:43:02.735: DHCPD: Option82 is removed
*Mar 1 01:43:02.735: DHCPD: broadcasting BOOTREPLY to client 0022.644b.abeb.
```

四、应用场景

当使用 Windows2003、Windows2008、Linux 等为 DHCP Server，并且和 PC 不在同一网段时；

IP SLA

一、实验目的

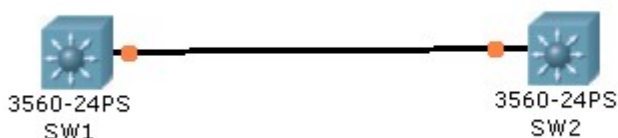
1、掌握 IP SLA 的应用

知识点链接：

SLA (Service Level Agreement) 在接入层交换机就可以提供此服务。主要作用是网络中发出的各种数据包进行探测，然后进行统计看网络数据包的状况。当然还可以和 HSRP 静态路由结合做 track 服务。

二、实验内容

拓扑图：



需求：

- 1、在 SW1/SW2 创建 no switchport 三层接口
- 2、SW1 作为 source 方，模拟发出 UDP 报文，端口 2005。SW2 作为接收方。报文每 2S 发送一次 Timeout 为 500 毫秒。然后查看 SLA 统计情况。

三、实验配置

```
SW1(config)#interface fastEthernet 0/24
```

```
SW1(config-if)#no switchport 关闭 2 层接口，开启三层接口
```

```
SW1(config-if)#ip address 10.1.1.1 255.255.255.0
```

```
SW2(config)#inter f0/24
```

```
SW1(config-if)#no switchport 关闭 2 层接口，开启三层接口
```

```
SW2(config-if)#ip address 10.1.1.2 255.255.255.0
```

```
SW1(config)#do ping 10.1.1.2 ping SW2 确保能够通讯
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:

!!!!

SW1(config)#ip sla 1	进入 SLA 配置模式，编号为 1
SW1(config-ip-sla)#udp-echo 10.1.1.2 2005	对目的地 10.1.1.2 发送 udp echo 报文。端口 2005
SW1(config-ip-sla-udp)#timeout 500	超时时间是 500 毫秒
SW1(config-ip-sla-udp)#frequency 2	发送频率是每 2 秒发送一次
SW1(config)#ip sla schedule 1 life forever	一直不停的发送报文
SW1(config)#ip sla schedule 1 start-time now	立即开始发送
SW2(config)#ip sla responder	SW2 作为相应端，相应 SW1 的 UDP 报文
SW2(config)#ip sla responder udp-echo port 2005	

SW1#show ip sla statistics 查看 SLA 统计信息

Round Trip Time (RTT) for Index 1

Latest RTT: 3 ms

Latest operation start time: *00:31:00.699 UTC Mon Mar 1 1993

Latest operation return code: OK

Number of successes: 32

Number of failures: 8

Operation time to live: Forever

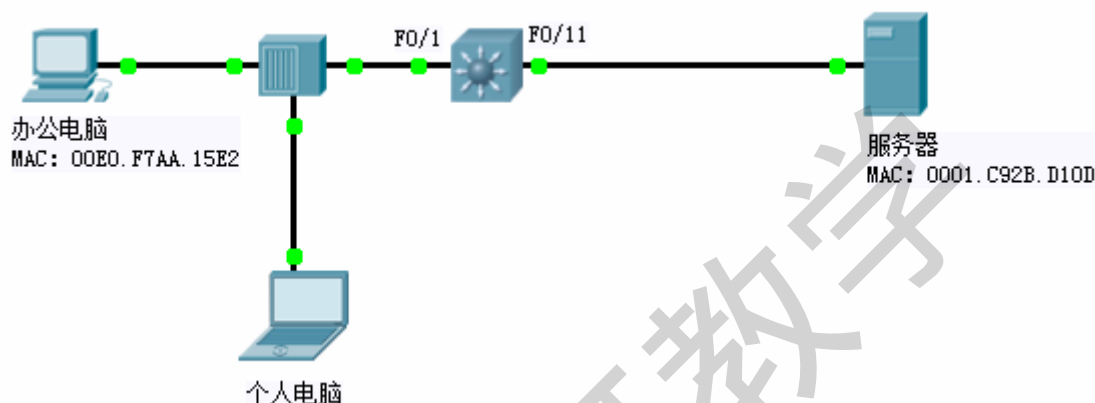
交换机端口安全

一、实验目的

- 1、掌握交换机端口安全的应用及配置

二、实验内容

拓扑图：



需求：

- 1、确保在企业网络内，外来电脑不能接入，防止针对交换机 MAC 地址的攻击

三、实验配置

配置：

- 1、查看交换机 MAC 地址表

```
Switch#show mac-address-table
```

Mac Address Table

Vlan	Mac Address	Type	Ports
1	0001.c92b.d10d	DYNAMIC	Fa0/11 （服务器，动态获得）
1	0004.9a54.52c7	DYNAMIC	Fa0/1 （个人电脑，外来，应禁用）
1	00e0.f7aa.15e2	DYNAMIC	Fa0/1 （办公电脑）

- 2、配置端口安全

```
Switch(config)#interface fastEthernet 0/11
```

```
Switch(config-if)#shutdown （配置端口安全之前先关闭端口）
```

```
Switch(config-if)#switchport mode access （在动态操作模式下，不能启用端口安全功能）
```

```
Switch(config-if)#switchport port-security （启用端口安全）
```

```
Switch(config-if)#switchport port-security maximum 1 （修改端口允许接入设备数为 1）
```

```
Switch(config-if)#switchport port-security mac-address 0001.c92b.d10d
```


(设置允许接入设备的 MAC 地址)

SW3560(config-if)#switchport port-security violation restrict (设置违规惩罚规则)

Switch(config-if)#no shutdown

注: Switch 的 F0/1 端口配置同 F0/11

验证:

1、Switch#show mac-address-table

Mac Address Table

Vlan	Mac Address	Type	Ports
1	0001.c92b.d10d	STATIC	Fa0/11 (服务器, 动态获得)
1	00e0.f7aa.15e2	STATIC	Fa0/1 (办公电脑)

四、应用场景

主要应用在 access 接口模式下, 防护攻击者对交换机 MAC 地址的攻击, 同时只允许合法的 MAC 地址才可以接入公司网络。

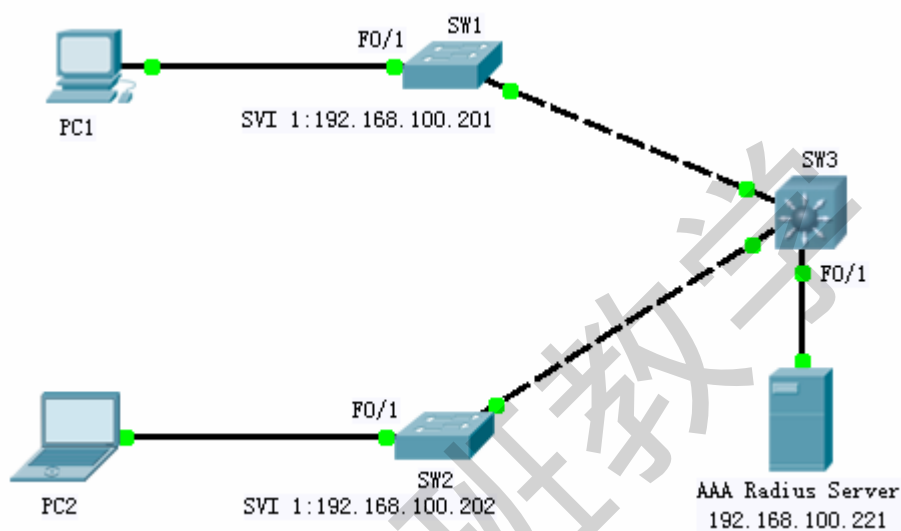
基于端口的 802.1X 认证

一、实验目的

- 1、掌握 AAA 服务器的配置
- 2、掌握基于 802.1x 认证的应用及配置

二、实验内容

拓扑图：



需求：

- 1、对用户接入网络做 802.1x 认证，并根据认证结果划分到特定 VLAN 中

三、实验配置

配置：

- 1、安装、配置 AAA 服务器

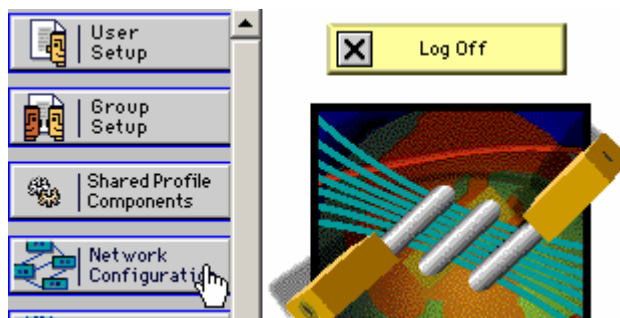
1)、软件需求：

AAA 软件：Cisco ACS 4.2

Java 软件：JRE 1.6

2)、CISCO ACS 配置

关联 ACS 客户端设备：



点击“Network Configuration”

AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
None Defined		
Add Entry		Search

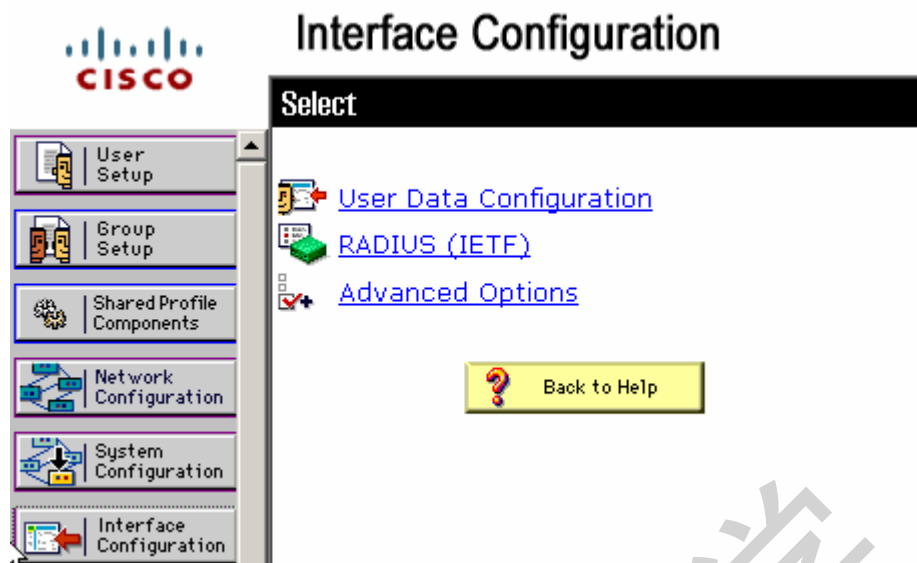
点击“Add Entry”

AAA Client Hostname	SW1
AAA Client IP Address	192.168.100.221
Shared Secret	kinglab

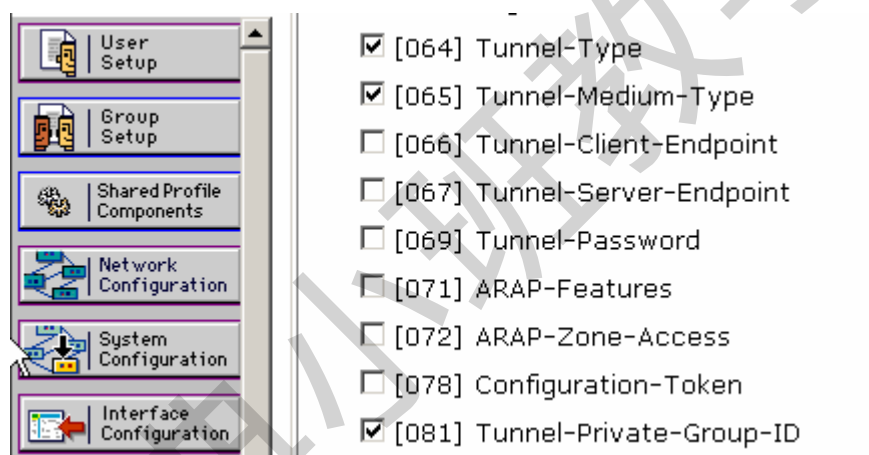
根据上图，添加 ACS 客户设备

Authenticate Using	RADIUS (IETF)
<input type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure) <input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client <input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client <input type="checkbox"/> Replace RADIUS Port info with Username from this AAA Client <input type="checkbox"/> Match Framed-IP-Address with user IP address for accounting packets from this AAA Client	
Submit Submit + Apply Cancel	

修改认证方式为“RADIUS (IETF)”并点击“Submit+Apply”



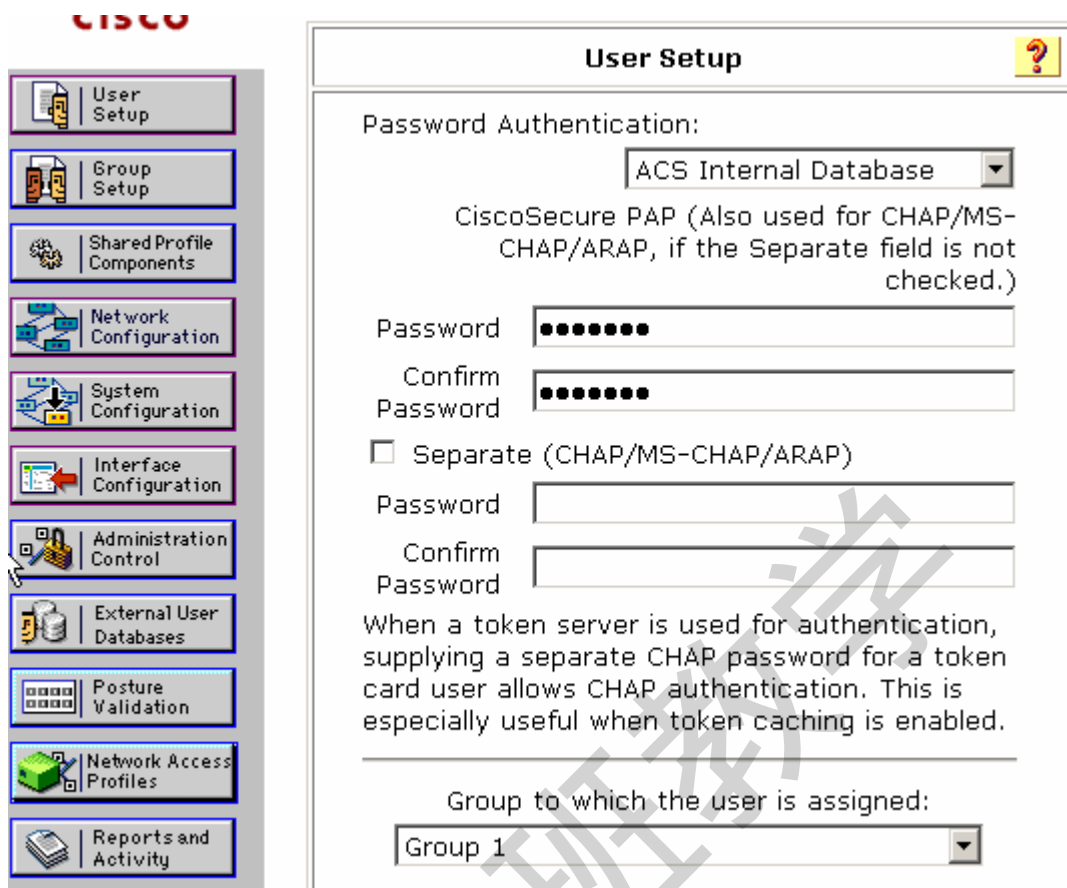
点击“Interface Configuration” → “RADIUS (IETF)”



确保“[064]/[065]/[081]”选项打钩，并点击“Submit”



点击“User Setup”在“User”栏中输入用户名，点击“Add/Edit”



User Setup

Password Authentication:

ACS Internal Database

CiscoSecure PAP (Also used for CHAP/MS-CHAP/ARAP, if the Separate field is not checked.)

Password: [Redacted]

Confirm Password: [Redacted]

☐ Separate (CHAP/MS-CHAP/ARAP)

Password: [Redacted]

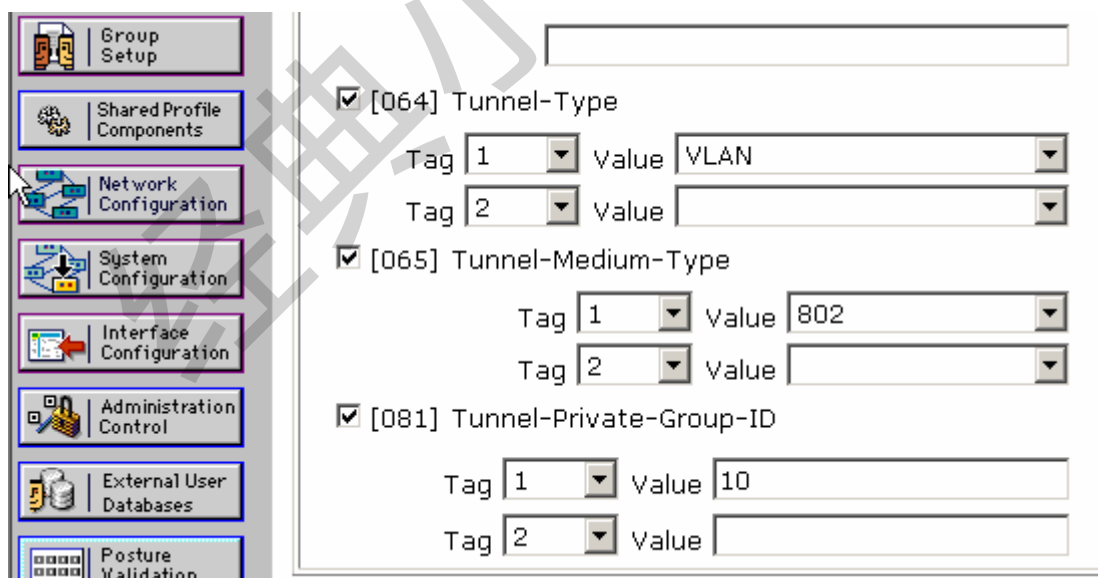
Confirm Password: [Redacted]

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

Group to which the user is assigned:

Group 1

输入用户密码及修改用户所在组为“Group 1”，点击“Submit”；同上添加用户第二个用户



Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Posture Validation

☒ [064] Tunnel-Type

Tag 1 Value VLAN

Tag 2 Value [Redacted]

☒ [065] Tunnel-Medium-Type

Tag 1 Value 802

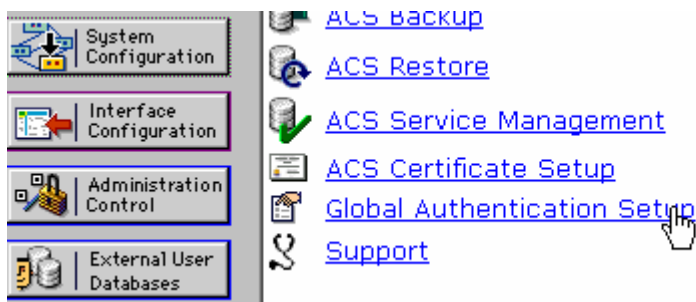
Tag 2 Value [Redacted]

☒ [081] Tunnel-Private-Group-ID

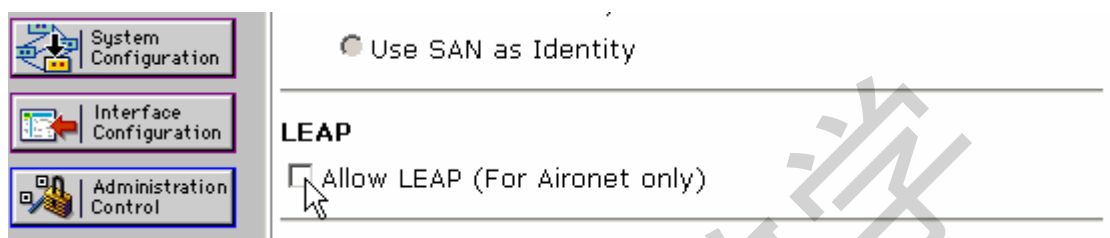
Tag 1 Value 10

Tag 2 Value [Redacted]

点击“Group Setup”修改“Group1”，“Group2”组的策略，如图，并点击“Submit+Restart”；“Group1” [081]选项值为“10”，“Group2” [081]选项值为“20”



点击“System Configuration” -> “Global Authentication Setup”



去掉选项“Allow LEAP (For Aironet only)”前面的钩，并且点击“Submit+Restart”

2、交换机配置

SW1(config)#interface vlan 1 (配置交换机和 ACS 的通信地址)

SW1(config-if)#ip address 192.168.100.201 255.255.255.0

SW1(config)#aaa new-model (启用 AAA 功能)

SW1(config)#aaa authentication login default none (设置不对网络设备做登陆认证)

SW1(config)#aaa authentication dot1x default group radius (启用对 dot1x 使用 Radius 认证)

SW1(config)#aaa authorization network default group radius (启用对 dot1x 使用 Radius 授权)

SW1(config)#radius-server host 192.168.100.221 key cisco (设置 Radius 服务器地址及密钥)

SW1(config)#radius-server vsa send (向 Radius 服务器发送 CISCO 私有属性集)

SW1(config)#dot1x system-auth-control (启用 dot1x 的认证控制)

SW1(config)#interface range fa0/1 - 20

SW1(config-if-range)#switchport mode access

SW1(config-if-range)#spanning-tree portfast

SW1(config-if-range)#dot1x port-control auto (启用端口的 dot1x 认证控制)

SW1(config)#vlan 10

SW1(config-vlan)#vlan 20

注：SW2 的配置同 SW1

验证：

在 PC1 没认证之前，SW1 中 VLAN 的配置信息

SW1#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24
10 VLAN0010	active	
20 VLAN0020	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

在 PC1 的交互窗口输入用户名：“zhang san”，密码：“kinglab”认证通过后，SW1 中 VLAN 的配置信息：

SW1#show vlan brief

VLAN Name	Status	Ports
1 default	active	Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24
10 VLAN0010	active	Fa0/1
20 VLAN0020	active	
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

四、应用场景

在企业中为了简化 VLAN 的配置及确保合法授权用户接入网络

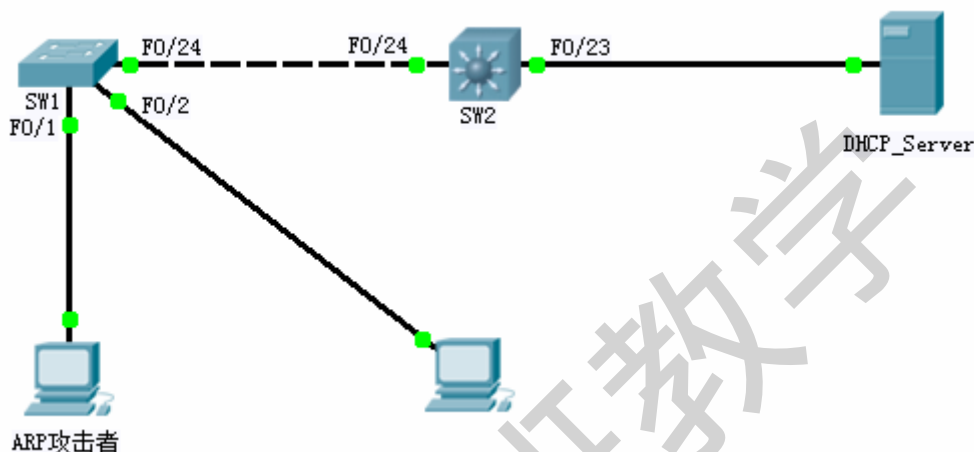
Dynamic ARP Inspect

一、实验目的

- 1、掌握 DHCP Snooping 的应用及配置
- 2、掌握 DAI 的应用及配置

二、实验内容

拓扑图：



需求：

- 1、防止使用 ARP 攻击网络

三、实验配置

配置：

```
SW1(config)#ip dhcp snooping (全局下启用 DHCP Snooping 功能)
```

```
SW1(config)#ip dhcp snooping vlan 1 (全局下对 VLAN1 开启 DHCP Snooping)
```

```
Switch(config)#ip arp inspection vlan 1 (全局下启用对 VLAN1 的 ARP 检查功能)
```

```
SW1(config)#interface range fastEthernet 0/1 - 20
```

```
SW1(config-if-range)#ip dhcp snooping limit rate 100
```

```
SW1(config)#interface fastEthernet 0/24
```

```
SW1(config-if)#ip dhcp snooping trust (设置接口为 DHCP Snooping 信任接口)
```

```
SW1(config-if)#ip arp inspection trust (设置接口为 ARP Inspect 信任接口)
```

(设置接口为 DHCP Snooping 不信任接口，并设置允许速率为每秒 100 报文)

```
SW2(config)#ip dhcp snooping
```

```
SW2(config)#ip dhcp snooping vlan 1
```

```
Switch(config)#ip arp inspection vlan 1
```



```
SW2(config)#interface range fastEthernet 0/23 - 24
```

```
SW1(config-if-range)# ip dhcp snooping trust
```

```
SW1(config-if-range)#ip arp inspection trust
```

注：在所有 Trunk 接口及关联 DHCP Server 的接口应设置为 DHCP Snooping、ARP Inspect 的信任接口

验证：

```
Switch#show ip dhcp snooping binding
```

MacAddress	IpAddress	Lease(sec)	Type	VLAN	Interface
00:22:64:4B:AB:EB	192.168.100.100	603676	dhcp-snooping	1	FastEthernet0/1
00:21:64:4B:AB:EA	192.168.100.101	603676	dhcp-snooping	1	FastEthernet0/2

Total number of bindings: 2

四、应用场景

针对企业常见的 DHCP 攻击和 ARP 攻击进行防护。

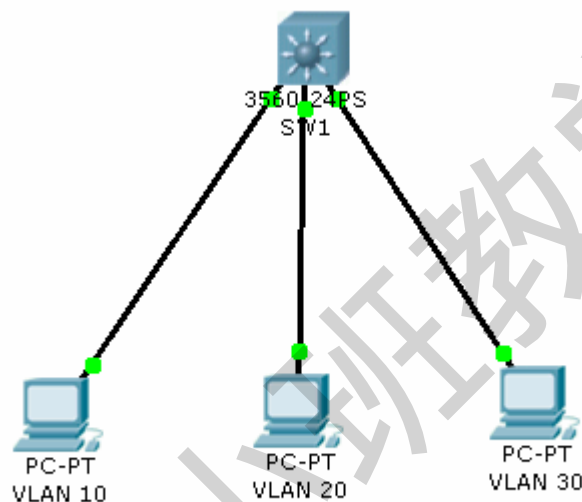
VLAN ACL

一、实验目的

1. 掌握多层交换机 SVI 接口的配置方法
2. 掌握控制 VLAN 之间访问控制的 VACL 配置方法

二、实验内容

拓扑图：



需求：3 台 PC 分别在 3 个 VLAN 分别是 VLAN 10. 20. 30 在交换机配置

SVI 三层接口让 VLAN 之间能够互相访问。

通过配置 VACL 技术限制 VLAN 10 和 VLAN30 之间的访问。

三、实验配置

SVI 的配置可以参考上面 SVI 实验。

VACL 配置

```

vlan access-map cisco 10
  action drop          匹配ACL101的流量DROP掉
  match ip address 101 匹配ACL101
vlan access-map cisco 20
  action forward        其他流量全部forward
vlan filter cisco vlan-list 10
  
```

```
access-list 101 permit ip host 10.1.1.1 host 30.1.1.1
```

主机配置:

主机配置好对应 VLAN 的 IP 地址，网关全部指向 SVI 接口。

验证:

VLAN 和 VLAN 30 之间的主机不能 ping 通，其他的可以 ping 通

经典小班教学