

## 《计算机网络》路由交换系列实验-2

### 一、实验名称：VLAN、静态路由、DHCP

### 二、实验学时：4 学时

### 三、实验目的

1. 掌握如何在交换机上划分基于端口的 VLAN、如何给 VLAN 内添加端口，理解跨交换机之间 VLAN 的特点以及掌握 VLAN 间路由的方法；
2. 理解路由器的工作原理，掌握路由器的基本操作以及简单的动态路由；
3. 通过对交换机的各种安全操作，提高网络安全意识。

### 四、实验原理

#### 1. VLAN 与 VLAN 中继

虚拟局域网（Virtual Local Area Network，VLAN）是一种可极大改善网络性能的技术。

##### ● 切割广播域

VLAN 能将大型广播域划分成较小的广播域。较小的广播域能够限制参与广播的设备数量，并允许将设备分成各个工作组。这使得管理者可以不依赖于主机的物理位置，而是以逻辑的方式分隔不同功能/用途/部门的主机，使之在数据链路层逻辑上相互隔离互通。

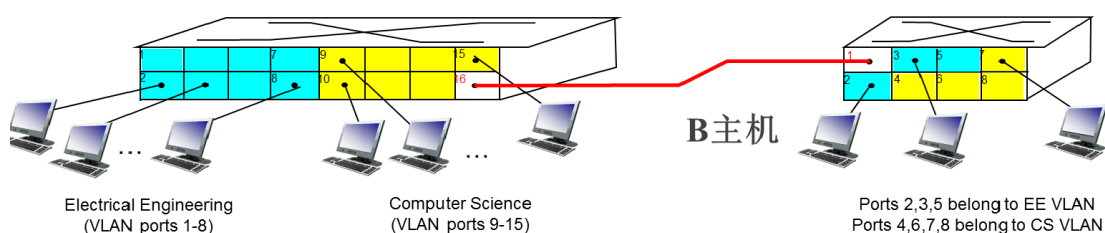
##### ● 逻辑上独立的 IP 子网

VLAN 是一个逻辑上独立的 IP 子网。多个 IP 网络可以通过 VLAN 存在于同一个交换网络中。为了让同一个 VLAN 上的计算机能相互通信，**每台计算机必须具有与该 VLAN 一致的 IP 地址和子网掩码**。其中的交换机必须配置 VLAN，并且必须将位于 VLAN 中的每个端口分配给 VLAN。配置了单个 VLAN 的交换机端口称为接入 ACCESS 端口。

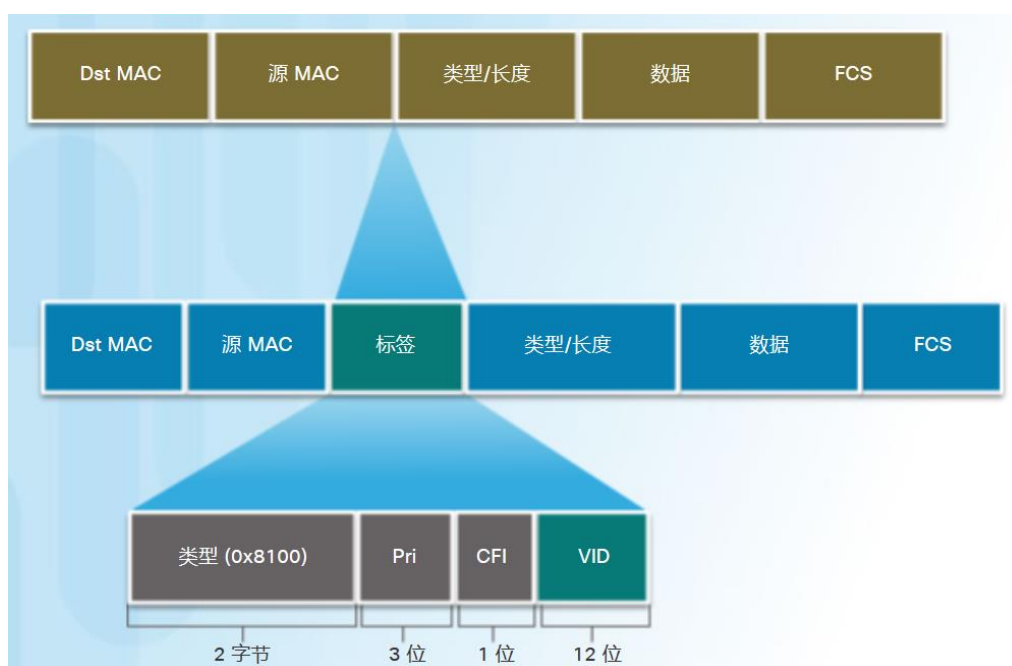
注意，如果两台计算机只是在物理上连接到同一台交换机，并不表示它们能够通信。无论是否使用 VLAN，两个不同网络和子网上的设备必须通过路由器（第 3 层）才能通信。要将多个网络和子网组织到一个交换网络中，不一定要使用 VLAN，但是使用 VLAN 会更简单与方便。

## ● VLAN 中继与 802.1Q 协议（参考课件）

VLAN 和 VLAN 中继有着密不可分的联系。如果没有 VLAN 中继，现代交换 LAN 中的 VLAN 实际上没有任何用处。VLAN 中继是以太网交换机接口和另一个联网设备（如路由器或交换机）的以太网接口之间的点对点链路，负责在单个链路上传输多个 VLAN 的流量。VLAN 中继通过在以太网帧头部中标记的方式实现，主要是通过通过在以太网帧头增加 802.1Q 字段，用以记录帧所属 VLAN，帮助交换机识别 VLAN 中继 Trunk 链路上传输的到底是哪个 VLAN 的帧。



VLAN EE 的两个主机如果都连接到左侧交换机，则他们之间通信是采用普通的以太帧；如果 VLAN EE 的两个主机是分别接入左侧交换机和右侧交换机，他们通信的以太帧，需要通过左侧交换机的 16 号端口和右侧交换机 1 号端口的 trunk 链路，当以太帧需要发送到 trunk 链路时，需要在以太帧中加入 802.1Q 的标识符，以帮助交换机确认这个以太帧是属于哪个 VLAN 的。【注意 trunk 链路上允许传输不同 VLAN 的 802.1Q 以太帧。每个主机与交换机端口之间发送的都是普通的以太帧】



## 2. VLAN 与 VLAN 中继配置应用

### ● VLAN 编号与配置存储

每一个 VLAN 都有一个 VLAN ID，一般也可以对 VLAN 进行命名。VLAN ID 的选择有两种范围：普通范围的 VLAN ID 是 1-1001，扩展范围的 VLAN ID 是 1006-4094。而 VLAN 1 和 VLAN 1002-1005 是保留 ID 号。在配置普通范围 VLAN 时，配置细节会自动存储在交换机闪存内一个名为 vlan.dat 的文件中，把运行配置文件的修改保存到启动配置文件。

### ● VLAN 创建

IOS 命令向交换机添加 VLAN 的过程如下（在全局配置模式下）：

//创建 ID 为<vlan\_id>的 VLAN，之后 CLI 会切换到此 VLAN 的配置模式

```
S1(config)#vlan <vlan_id>
```

//指定唯一的 VLAN 名称标识 VLAN（可选，默认名称为 VLAN 后面加若干个 0 再加上 VLAN 号，如 VLAN0001）

```
S1(config-vlan)#name <vlan_name>
```

//返回特权执行模式，此时配置会保存在 vlan.dat 文件中，同时配置生效

```
S1(config-vlan)#end
```

在特权执行模式下使用 show vlan 可以看到当前设备的 VLAN 状态：

```
show vlan [brief|id <vlan-id>|name <vlan-name>|summary]
```

### ● 交换机接口VLAN模式

交换机接口的模式有以下三种：Access、Dynamic、Trunk。Access 型接口只能属于 1 个 VLAN，一般用于连接计算机的端口，连接 Access 接口链路通常称为 Access Link；Trunk 型的接口可以属于多个 VLAN，通过给以太网帧头打标记(tag)的方式支持接收和发送多个 VLAN 的数据，一般用于交换机之间连接的端口，即支持 VLAN 中继【也用于连接交换机和路由器的接口】；Dynamic 型端口支持端口之间通过自动协商确认是采用 Access 型还是 Trunk 型【本实验中不涉及】。

### ● 指定VLAN的接口添加或删除

默认情况下所有接口都在 VLAN 1 下，添加接口至单个指定 VLAN 的方法范例

如下：

```
//进入 f0/10 接口的配置模式
S1(config)#interface f0/1
//强制修改端口为接入模式。
S1(config-if)#switchport mode access
//将接口添加到 VLAN 20 中，端口在 access 模式下允许 vlan 20 通过
S1(config-if)#switchport access vlan 20
S1(config-if)#end
//删除 VLAN 成员资格需要在接口配置模式下使用 no switchport access
```

vlan 命令：

```
S1(config)# interface f0/10
S1(config-if)# no switchport mode access
S1(config-if)#end
```

此时接口会被重新分配给 VLAN 1。

### ● 删除已创建的VLAN

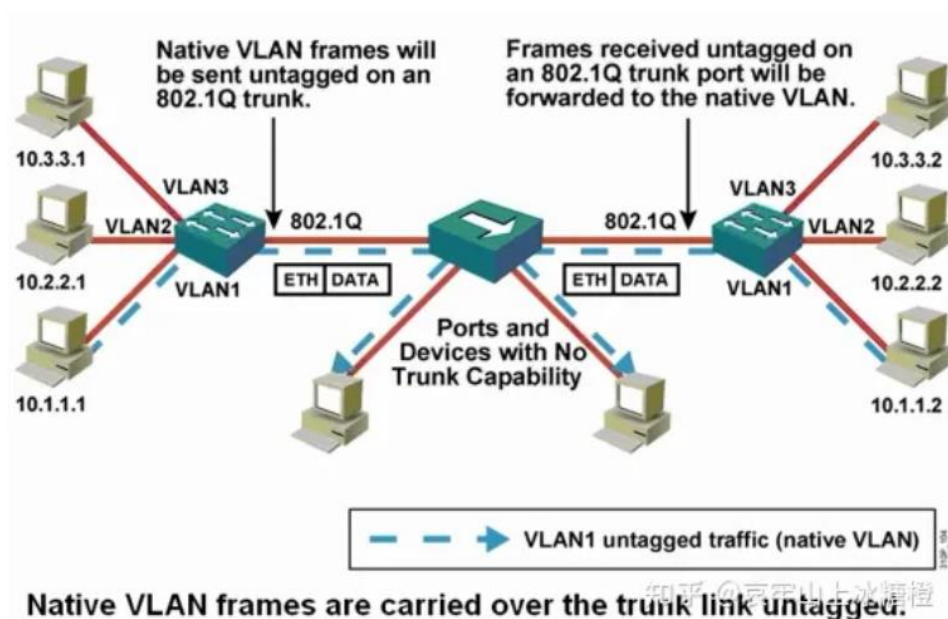
删除 VLAN 需要在全局配置模式下使用命令 `no vlan <vlan_id>`。需要注意，删除 VLAN 不会将此 VLAN 下的接口转移到其他 VLAN 下。

### ● 配置VLAN中继接口

使用 `switchport mode trunk` 命令。在交换机端口上输入该命令，接口即更改为永久中继模式，并且端口会进入 DTP（Dynamic Trunking Protocol）协商，以将链路转换为中继链路。默认情况下中继接口允许所有 VLAN 通过，如果需要限制中继接口允许的 VLAN，则需在接口配置模式下使用命令 `switchport trunk allowed vlan add <vlan_list>`，删除这一限制可以在接口配置模式下使用命令 `no switchport trunk allowed vlan`。将接口重置为静态接入模式可以在接口配置模式下使用命令 `switchport mode access`。

### ● Native VLAN

在 802.1Q 中，设置了 native vlan，一旦把 vlan 设置成 native vlan，那个这个 vlan 就不用打 tag 标记了。



交换机 A 上将 vlan1 设置成 native vlan , 交换机 B 上也将 vlan1 设置成 native vlan, 交换机 A 向交换机 B 发数据帧, 在 trunk 口上, vlan 2 和 vlan3 都要打各自的 tag 标记, 标识所属 vlan。vlan1 就不用打 tag 标记, 也不用管所属 vlan, 交换机 B 收到后数据帧后, 对 vlan2、vlan3 解封装, 转发数据到相应 vlan 端口, 对 vlan1 不用解封装, 直接转发到 native vlan 端口。

Trunk 两端的交换机 native vlan 必须相同, 并且 native vlan 只能有一个。

思科交换机上, 默认 vlan1 就是 native vlan。

switchport trunk native vlan <vlan id>

### 3. VLAN 间路由

VLAN 和中继用于把 LAN 分段。用 VLAN 分段功能限定 LAN 中各广播域的范围, 可提高整个网络的性能和安全。VLAN 间路由则可以使属于不同 VLAN 的设备进行通信。VLAN 间路由有多种方式:

- 每个路由器的路由接口对应一独立 VLAN

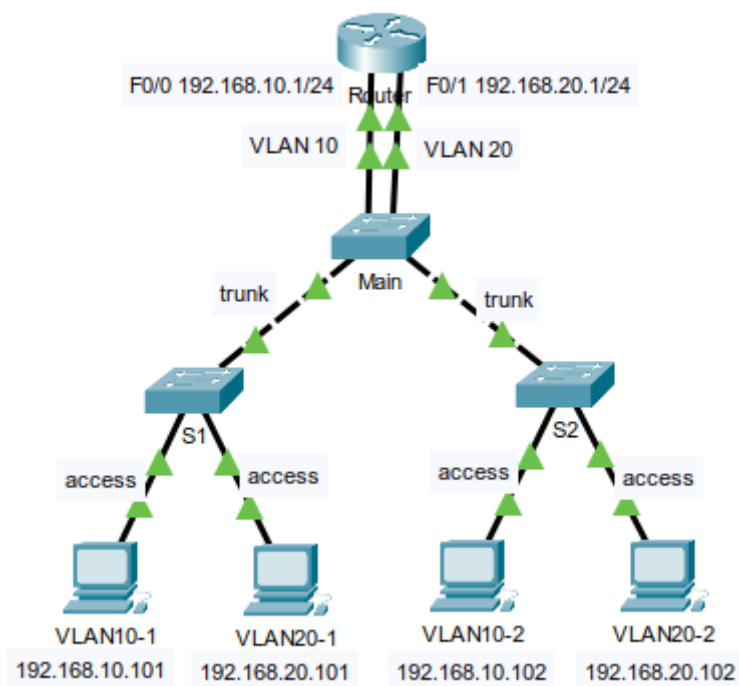


图1 每个路由器接口对应一个VLAN的情形

图 1 的拓扑结构在逻辑上与图 2 的逻辑结构一致。

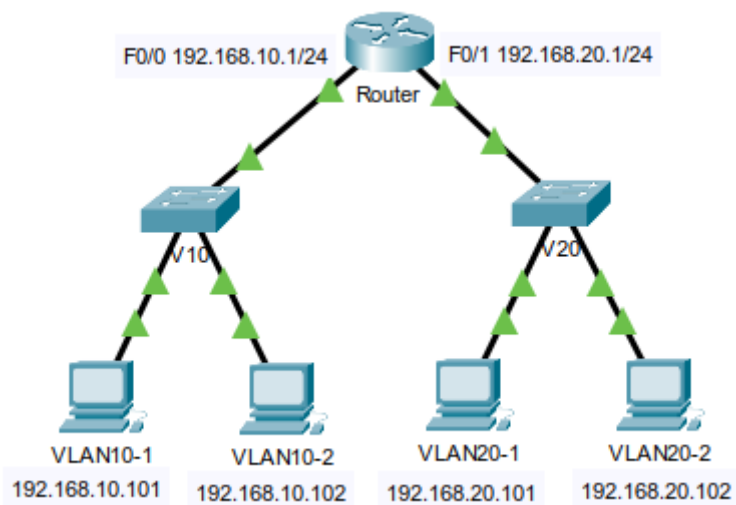


图2 每个路由器接口对应一个VLAN的逻辑情形

### ● 单臂路由器（单路由器接口支持多 VLAN）【本实验的方法】

单臂路由器只需要一个接口就可完成所有的工作，下面主要介绍单臂路由器的配置。单臂路由器路由需使用虚拟子接口和中继链路。子接口是基于软件的虚拟接口，可分配到各物理接口。每个子接口配置有自己的 IP 地址、子网掩码和唯一的 VLAN 分配，使单个物理接口可同时属于多个逻辑网络。这种方法适用于在网络中有多个 VLAN 但只有少数路由器物理接口的 VLAN。

使用单臂路由器模式配置 VLAN 间路由时，路由器的物理接口必须与相邻交换机的中继链路（Trunk）相连接。针对网络上每个唯一的 VLAN/子网创建子接口。每个子接口都分配有所属子网的 IP 地址，并对与其交互的 VLAN 帧添加 VLAN 标记。这样，路由器可以在流量通过中继链路返回交换机时区分不同子接口的流量。假设有如图 3 所示拓扑。图 3 的拓扑结构在逻辑上与图 4 的拓扑结构一致。

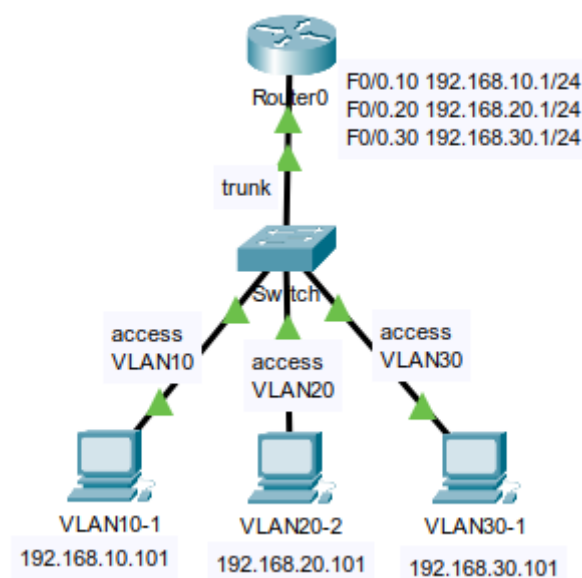


图3 单臂路由器拓扑示例

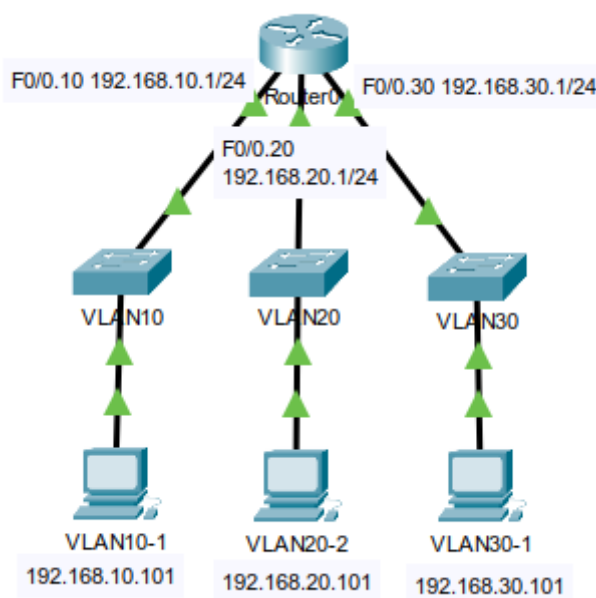


图4 单臂路由器的逻辑拓扑

在上图中，VLAN 10 中的主机的 IP 地址是 192.168.10.101/24，VLAN 20 中的主机的 IP 地址是 192.168.20.101/24。这两个主机进行通信，VLAN 10 的主机

发送数据报给 VLAN 20 的主机,则该主机首先判断目的 IP 与自己不在一个子网,则这个数据报要首先发送给网关路由器,这里 VLAN 10 主机的默认网关是 192.168.10.1,它属于 VLAN 10,则 VLAN 10 主机发送的数据帧的源 MAC 地址是自己的 MAC 地址,目的 MAC 地址是路由器的虚拟子接口 F0/0.10 的 MAC 地址【以太网接口 F0/0 的 MAC 地址】。

交换机收到这个以太帧,将其通过自己与路由器相连的 Trunk 链路转发到路由器接口,注意 Trunk 链路上传输的是 802.1Q 帧,带有 VLAN 10 的标记。

路由器接口 F0/0 收到这个数据帧,首先根据 VLAN 10 的标记将其交给虚拟子接口 F0/0.10,通过路由转发表,这个数据报需要转发到 192.168.20.0/24 子网,则需要通过 VLAN 20 的子接口 F0/0.20 转发,重新封装成 802.1Q 以太帧,源 MAC 是 F0/0 的 MAC 地址,目的 MAC 是 VLAN 20 主机的 MAC 地址,注意这个以太帧带有 VLAN 20 的标识,发送这个数据帧的端口是属于 VLAN 20 的。

交换收到这个 802.1Q 以太帧,通过查转发表,将它发送给 VLAN 20 主机。

假设已经划分好 VLAN,并分配相应的端口,首先需配置交换机与路由器之间的链路为 Trunk:

```
S1(config)#interface f0/4
S1(config-if)#switchport mode trunk
S1(config-if)#end
```

接下来配置路由器以实现 VLAN 间路由。不同于物理接口配置,全局配置模式下使用 interface<interface\_id.subinterface\_id>命令创建各个子接口。子接口创建后,在子接口配置模式下运行 encapsulation dot1q <vlan\_id>命令分配 VLAN ID。然后运行 ip address<ip\_address><subnet\_mask>子接口配置模式命令为该子接口分配 IP 地址:

```
R1(config)#interface f0/0.10
R1(config-subif)#encapsulation dot1q 10
R1(config-subif)#ip address 192.168.10.101 255.255.255.0
R1(config-subif)#exit
R1(config)#interface f0/0.20
R1(config-subif)# encapsulation dot1q 20
```



```
R1(config-subif)# ip address 192.168.20.101 255.255.255.0
R1(config-subif)#exit
R1(config)#interface f0/0.30
R1(config-subif)#encapsulation dot1q 30
R1(config-subif)#ip address 192.168.30.101 255.255.255.0
R1(config-subif)#exit
R1(config)#interface f0/0
R1(config-if)#no shutdown //启动 f0/0 接口
R1(config-if)# end
```

现在可以使用 show ip route 命令检查路由表，并在主机上使用 ping 命令测试网络。

#### 4. 交换机虚拟接口 SVI

交换机虚拟端口（Switch Virtual Interface, SVI）是交换机上的逻辑第三层接口（功能上等价于路由器的路由端口），配置 SVI 的目的包括：

- 为 VLAN 提供默认网关，允许流量在 VLAN 之间路由（主要用在三层交换机）；
- 提供 fallback bridging；
- 提供到交换机的第 3 层 IP 连接；
- 支持桥接配置和路由协议。

一个 SVI 代表一个由交换端口构成的 VLAN，以便于实现系统中路由和桥接的功能。SVI 接口即通常所谓的 VLAN 接口，不过它是虚拟的，用于连接整个 VLAN，所以也经常被称为逻辑三层接口。一个 VLAN 仅可以有一个 SVI。

在交换机的管理 VLAN 上配置 IP 地址和子网掩码的步骤如下（假设 VLAN 4 为管理 VLAN）：

```
//进入 VLAN 4 的接口配置模式
S1(config)#interface vlan 4
//配置接口 IP 地址
S1(config-if)#ip address <ip_address> <netmask>
//启动接口
```

```
S1(config-if)#no shutdown
```

```
S1(config-if)#end
```

之后就可以为这一 VLAN 分配端口了。

## 5. 交换机端口安全性配置

未提供端口安全性的交换机将允许攻击者连接到系统上未使用的已启用端口，并执行信息收集或攻击。配置端口安全性的一些方法如下：

启用端口安全性时，在端口配置模式下使用命令 `switchport port-security` 即可，需注意首先把接口设置为 `access` 模式，动态端口不可配置为安全端口。设置最大允许的安全地址数量的命令为：

```
switchport port-security maximum <num>。
```

## 6. 端口聚合 EtherChannel

端口聚合又称为以太通道，是由 Cisco 研发的，应用于交换机之间的多链路捆绑技术。它的基本原理是：将两个设备间多条物理链路捆绑在一起组成一条逻辑链路，从而达到带宽倍增的目的（这条逻辑链路带宽相当于物理链路带宽之和）。除了增加带宽外，端口聚合还可以在多条链路上均衡分配流量，起到负载分担的作用；当一条或多条链路故障时，只要还有链路正常，流量将转移到其它的链路上，整个过程在几毫秒内完成，从而起到冗余的作用，增强了网络的稳定性和安全性。两台交换机之间是否形成 EtherChannel 可以用协议自动协商。目前有两个协商协议：PAgP 和 LACP，PAgP（端口汇聚协议 Port Aggregation Protocol）是 Cisco 私有的协议，而 LACP（链路汇聚控制协议 Link Aggregation Control Protocol）是基于 IEEE 802.3ad 的国际标准，是一种实现链路动态聚合的协议。

【在本实验中要求按照 LACP】

```
//创建一个通道，通道号为 1
```

```
S1(config)#interface port-channel 1
```

```
//全局模式下进入 Fa0/1-2 端口
```

```
S1(config)#interface range f0/1-2
```

//创建虚拟通道 channel-group 1 并设置模式为[desirable/active]封装协议为 LACP

```
S1(config-if-range)#channel-group 1 mode active
```

## 7. 静态路由

从一个网络路由到末节网络（只能通过单条路由访问的网络），一般使用静态路由。配置静态路由采用如下命令：

```
R1(config)#ip route <dest_address> <subnet-mask>
<ip-address|exit_interface> [administrative_distance]
```

- **dest\_address**: 要加入路由表的远程网络的目的网络地址；
- **subnet-mask**: 要加入路由表的远程网络的子网掩码；
- **ip-address**: 指定可用于到达该网络的下一跳路由器的 IP 地址；
- **exit\_interface**: 将数据包转发到目的网络时使用的送出接口；
- **administrative\_distance**(可选参数): 管理距离(也称为路由优先级)，代表路由的可信度，有效范围是 1–255，默认值为 1。如果有多条路径可以到达目的地，路由器会选择管理距离最小的路径。

这一语句可以理解为：若待转发 IP 报文的目的 IP 符合 dest\_address 与 mask 定义的网段，则将该 IP 数据报发往下一跳 IP 地址为 ip-address 的邻居路由器，或直接从本地 exit\_interface 接口发出。

IPv6 静态路由的配置与 IPv4 有一些差别，首先在配置 IPv6 的静态路由时要使用命令 ipv6 unicast-routing 启动 IPv6 的数据包转发功能，否则静态路由无法完成。ipv6 静态路由配置命令如下：

```
ipv6 route <dest_ipv6_address>/<prefix-length> [<ipv6-address> |
<exit_interface> ] [administrative_distance]
```

指定 IPv6 网段时，掩码使用前缀长度表达法。

### • 默认路由

默认路由是一类特殊的静态路由，默认路由使用零或者没有比特匹配的方法来表示全部路由。换言之，如果路由表中没有其他路由与数据包的目标 IP 地址匹配，那么默认路由就将被匹配。配置默认路由的语法类似于配置其他静态路由，但网络地址和子网掩码均为 0.0.0.0：

```
R1(config)#ip route 0.0.0.0 0.0.0.0 <ip-address|exit_interface>
[metric-value]
```

IPv4: 0.0.0.0 0.0.0.0 四个八位组 (Octet) 全零的网络地址和掩码也称为全零路由。

IPv6: 全零路由地址为 ::/0

## 8. 动态地址配置 DHCP

路由器一般均可用作 DHCP 服务器。DHCP 服务器从路由器的地址池中分配 IP 地址给 DHCP 客户端，并管理这些 IP 地址。一般而言 DHCP 是默认启动的，如需禁用服务，可使用命令 `no service dhcp`。使用全局配置命令 `service dhcp` 则可重新启动 DHCP 服务。下面是将路由器配置成 DHCP 服务器的一般步骤：

- **指定待排除的地址**

可避免 DHCP 分配保留的地址。这些地址通常是保留供路由器接口、交换机管理以及服务器和本地网络打印机使用的静态地址。下面命令可以排除一个地址，也可以排除从 `low_address` 到 `high_address` 范围的 IP 地址。

```
R1(config)#ip dhcp excluded-address <low_address> [<high_address>]
```

注意：`high_address` 为可选参数，如果不输入这个参数值，则只排除 `low_address`

- **建立待分配地址池**

下面命令可以建立地址池并为其命名，执行命令后会进入 DHCP 配置模式。

```
R1(config)#ip dhcp pool <pool_name>
```

- **配置可用网段信息**

指定子网号和子网掩码，同时配置默认网关地址。

```
R1(dhcp-config)#network <network_number> [<mask>]//定义可用地址范围
```

```
R1(dhcp-config)#default-router <address> [<address2>...<address8>]
//定义默认网关（路由器），至少指定一个，最多可指定 8 个
```

下面是其他一些可选网络信息配置，包括指定 DNS 服务器、指定域名等：

```
R1(dhcp-config)#dns-server <address> [<address2>...<address8>] //
指定 DNS 服务器，最多可指定 8 个
```

R1(dhcp-config)#domain-name <domain> //指定域名

### • 查看 DHCP 配置应用

查看当前 DHCP 配置可以使用命令 show ip dhcp binding。该命令会显示 DHCP 服务器提供的所有 IP 地址到 MAC 地址的绑定：

R1#show ip dhcp binding

IP address	Client-ID/ Hardware address	Lease expiration	Type
192.168.1.4	00D0.BA28.71D3	--	Automatic
192.168.1.3	000C.CFAD.5238	--	Automatic

而 show ip dhcp pool <pool\_name>则可查看当前 IP 池状态：

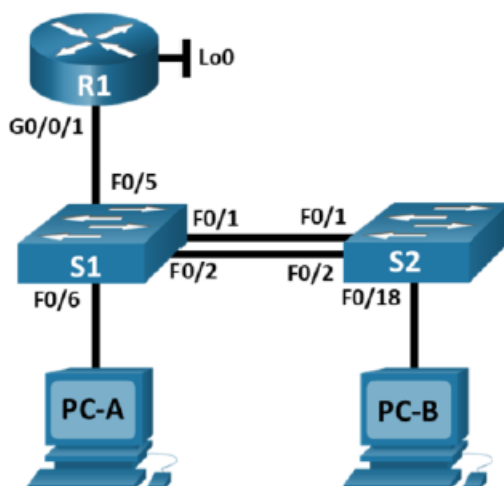
Router#show ip dhcp pool

```
Pool LAN1-POOL :
Utilization mark (high/low)      : 100 / 0
Subnet size (first/next)          : 0 / 0
Total addresses                   : 254
Leased addresses                  : 2
Excluded addresses                : 1
Pending event                    : none

1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.1.1       192.168.1.1 - 192.168.1.254    2 / 1 / 254
```

## 五、实验内容

实验题目如下：



题目给出的逻辑上的拓扑结构，主机 A 和交换机 S1 相连，主机 B 和交换机 S2 相连，两个交换机由 2 条链路相连，因此本实验中的链路聚合是指的这里 2 条链路的聚合。交换机 S1 与路由器 R1 相连。路由器有个还回接口 Lo0。【这里

显然可以看出这个实验的 VLAN 间路由是通过单臂路由实现的。G0/0/1 接口上要创建多个子接口】

题目给出了物理设备，要求按照逻辑拓扑结构的来手动连接这些设备。

题目给出了一个 VLAN 分配表，需要在交换机上和路由器上配置多个 VLAN，这个表给出了这些 VLAN 的名字。

**VLAN Table**

VLAN	Router Subinterface	VLAN Name
2	G0/0/1.2	Bikes
3	G0/0/1.3	Trikes
4	G0/0/1.4	Management
5	N/A	Parking
6	G0/0/1.6	Native

题目中给出了 IP 地址，路由器子接口、还回端口，交换机的虚拟接口，两个 PC 的地址。注意 IPv6 地址是直接在表中给出的。两个 PC 的 IPv4 地址是通过 DHCP 配置的，因此不需要手动设置。

Addressing Table

Device / Interface	IP Address/Prefix/Link Local Address	Default Gateway
R1 G0/0/1.2	10.19.8.1 /26	N/A
	2001:db8:acad:a::1 /64	N/A
	fe80::1	N/A
R1 G0/0/1.3	10.19.8.65 /27	N/A
	2001:db8:acad:b::1 /64	N/A
	fe80::1	N/A
R1 G0/0/1.4	10.19.8.97 /29	N/A
	2001:db8:acad:c::1 /64	N/A
	fe80::1	N/A
R1 G0/0/1.6	N/A	N/A
R1 Loopback0	209.165.201.1 /27	N/A
	2001:db8:acad:209::1 /64	N/A
	fe80::1	N/A
S1 VLAN 4 SVI	10.19.8.98 /29	10.19.8.97
S2 VLAN 4 SVI	10.19.8.99 /29	10.19.8.97
PC-A NIC	DHCP for IPv4 address	DHCP for IPv4 default gateway
	2001:db8:acad:a::50 /64	fe80::1
PC-B NIC	DHCP for IPv4 address	DHCP for IPv4 default gateway
	2001:db8:acad:b::50 /64	fe80::1

**Note:** There is no interface on the router that supports VLAN 5.

在本实验中，学生需要配置一个路由器、两个交换机、两个 PC 主机以支持这些设备之间在 IPV4 和 IPV6 协议上的互通性【互通即互相可以 ping 通】。路由器和交换机必须进行安全管理。也需要配置 VLAN 域间路由，DHCP，Etherchannel 和 port-security。所有这些任务都在 PT Physical Mode 下完成。网络设备的配置需要通过一个直连的 console 连接。

## 六、实验器材

Packet Tracer

## 七、实验步骤

### Part 1: Build the Network

- Move the required devices into the equipment rack.
- Place the PCs on the table.
- Connect the devices according to the topology diagram.

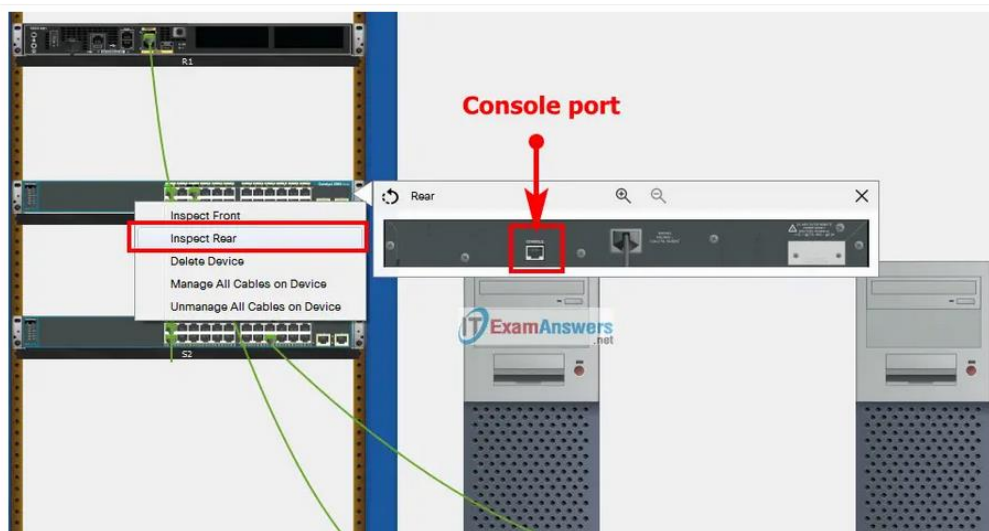
题目理解：

- 将所需设备移动到机架上。【直接拖动即可】
- 将两个 PC 机放到桌面上。
- 按照逻辑拓扑结构连线。【设备之间互连的线选择 Copper Straight-Through cable】【console 线连接的设备的 console 端口和 PC 机的 RS232 端口】【难点：找到设备上的这些端口。交换机的 console 端口在背面，通过点击右键，选择 Inspect Rear 来找到这个端口】【最后是加电，路由器、主机都需要开机，交换机不需要开机】【由于只有 2 个 PC，因此在配置过程中，可以先配置路由器，再把 console 线换到交换机 S2 上。配置交换机时，先配置 S1 更优】

- Use Copper Straight-Through cable to connect all devices



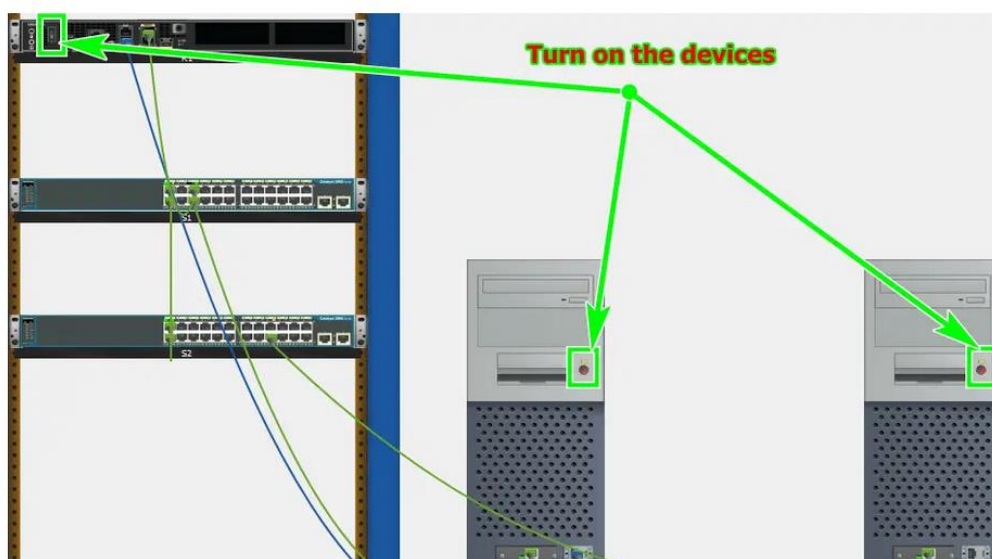
SRWE Final PT Skills Assessment (PTSA)



SRWE Final PT Skills Assessment (PTSA)



Turn on the devices PCs and Router



## Part 2: Configure Initial Device Settings

所有的 IOS 设备配置必须通过一个直连的 console 线。

### Step 1: 配置 R1 的基本信息和设备安全加固

a. Configure basic settings.

- 1) 防止路由器将不正确的输入命令解析为域名。
- 2) 配置 R1 路由器的名字。
- 3) 配置一个适当的 MOTD banner.

```
Router(config)#no ip domain lookup
Router(config)#hostname R1
R1(config)#banner motd #Unauthorized Access is Prohibited#
```

b. Configure password security. 配置密码安全性

- 1) 配置控制台密码并启用连接。
- 2) 配置 enable 启用密码。
- 3) 加密所有明文密码。
- 4) 将新创建的密码的最小长度设置为 10 个字符。

```
R1(config)#line console 0
R1(config-line)#password ciscoconpass
R1(config-line)#login
R1(config-line)#exit

R1(config)#enable secret ciscoenpass

R1(config)#service password-encryption

R1(config)#security passwords min-length 10
```

### c. Configure SSH.

- 1) 在本地用户数据库中创建一个管理员用户

Username: **admin**

Encrypted Password: **admin1pass**

- 2) 配置域名为 **ccna-pts.com**
- 3) 创建一个模数为 **1024** 比特的 **RSA** 加密密钥。
- 4) 确保将使用更安全的 SSH 版本。
- 5) 配置 vty 线，根据本地用户数据库验证登录。
- 6) 配置 vty 线路，只接受通过 SSH 的连接。

```
R1(config)#username admin secret admin1pass

R1(config)#ip domain name ccna-pts.com

R1(config)#crypto key generate rsa
1024

R1(config)#ip ssh version 2

R1(config)#line vty 0 15
R1(config-line)#login local
R1(config-line)#transport input ssh
R1(config-line)#exit
```

## Step 2: 配置路由器接口

- a. Configure R1 with a loopback interface. Configure the **loopback0** with IPv4 and IPv6 addressing according to the addressing table. 【给 R1 配置一个环回接口。根据寻址表，用 IPv4 和 IPv6 寻址配置 loopback0。】

```
R1(config)#interface Loopback 0
R1(config-if)#description Loopback
R1(config-if)#ip address 209.165.201.1 255.255.255.224
R1(config-if)#ipv6 address 2001:db8:acad:209::1/64
R1(config-if)#ipv6 address fe80::1 link-local
R1(config-if)#exit
```

#### b. Configure Router Subinterfaces 【配置路由器子接口】

- 1) 准备在路由器的接口上配置 IPv6 地址。
- 2) 使用地址表和 VLAN 表中的信息，在 R1 上配置子接口：
  - 接口应配置为 IPv4 和 IPv6 寻址。
  - 所有寻址的接口都应使用 **fe80::1** 作为 link local 地址。
  - 使用 VLAN 表给予接口分配 VLAN 成员。
- 3) 必须配置 native VLAN 接口。
- 4) 为所有的(子)接口配置 description 信息.

```
R1(config)#ipv6 unicast-routing

R1(config)#interface g0/0/1.2
R1(config-subif)#encapsulation dot1Q 2
R1(config-subif)#description Bikes
R1(config-subif)#ip address 10.19.8.1 255.255.255.192
R1(config-subif)#ipv6 address 2001:db8:acad:a::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#interface g0/0/1.3
R1(config-subif)#encapsulation dot1Q 3
R1(config-subif)#description Trikes
R1(config-subif)#ip address 10.19.8.65 255.255.255.224
R1(config-subif)#ipv6 address 2001:db8:acad:b::1/64
R1(config-subif)#ipv6 address fe80::1 link-local
```

```
R1(config)#interface g0/0/1.3
```

```
R1(config-subif)#interface g0/0/1.4
R1(config-subif)#encapsulation dot1Q 4
R1(config-subif)#description Management
R1(config-subif)#ip address 10.19.8.97 255.255.255.248
R1(config-subif)#ipv6 address 2001:db8:acad:c::1/64
R1(config-subif)#ipv6 address fe80::1 link-local

R1(config-subif)#interface g0/0/1.6
R1(config-subif)#encapsulation dot1Q 6 native
R1(config-subif)#description Native

R1(config)#interface g0/0/1
R1(config-if)#no shutdown
```

### Step 3: Configure S1 and S2 with Basic Settings and Device Hardening.

交换机 S1 和 S2 的配置要求如下；【为了能同时配置 S1 和 S2，要把连路由器的 console 线连到 S2 上，后面需要配置路由器时，再接回路由器】

#### a. 在 S1 和 S2 上进行基本信息配置

- 1) 防止交换机试图将错误输入的命令解析为域名。
- 1) 配置 S1 或 S2 名字。
- 3) 为两个交换机各配置一个适当的 MOTD banners.

```
Switch1(config)#no ip domain lookup
Switch1(config)#hostname S1
S1(config)#banner motd #Unauthorized Access is Prohibited!#
```

```
Switch2(config)#no ip domain lookup
Switch2(config)#hostname S2
S2(config)#banner motd #Unauthorized Access is Prohibited!#
```

#### b. Configure Device Hardening on S1 and S2

- 1) 配置 console 密码 and enable connections.
- 2) 配置 enable secret password.
- 3) 加密所有的明文密码.

```
S1(config)#line console 0
S1(config-line)#password ciscoconpass
S1(config-line)#login
S1(config-line)#exit

S1(config)#enable secret ciscoenpass

S1(config)#service password-encryption
```

```
S2(config)#line console 0
S2(config-line)#password ciscoconpass
S2(config-line)#login
S2(config-line)#exit

S2(config)#enable secret ciscoenpass

S2(config)#service password-encryption
```

c. Configure SSH on S1 and S2。

1) 在本地的用于数据库中创建一个管理员用户。

Username: admin

Password: admin1pass

2) 配置域名为 ccna-pts.com

3) 创建一个模数为 1024 比特的 RSA 加密密钥。

4) 确保将使用更安全的 SSH 版本。

5) 配置 vty 线，根据本地用户数据库验证登录。

6) 配置 vty 线，只接受通过 SSH 的连接。

```
S1(config)#username admin secret admin1pass

S1(config)#ip domain name ccna-pts.com

S1(config)#crypto key generate rsa
1024

S1(config)#ip ssh version 2

S1(config)#line vty 0 15
S1(config-line)#login local
S1(config-line)#transport input ssh
S1(config-line)#exit
```

```
S2(config)#username admin secret admin1pass

S2(config)#ip domain name ccna-pts.com

S2(config)#crypto key generate rsa
1024

S2(config)#ip ssh version 2

S2(config)#line vty 0 15
S2(config-line)#login local
S2(config-line)#transport input ssh
S2(config-line)#exit
```

#### Step 4: Configure SVIs on S1 and S2

配置两个交换机上的 SVIs 接口

- 使用寻址表中的信息，在 S1 和 S2 上为 Management VLAN 配置 SVI。
- 配置交换机，使来自其它网络的数据帧可以通过 Management VLAN 到啊 SVI。

【Management VLAN 就是 VLAN 4，首先进入 VLAN 4 的接口，配置这个接口的 IP 地址。网络前缀 29 等价于  $255.255.255.255.11111000=248$ 】

	IP地址	网关
S1 VLAN 4 SVI	10.19.8.98 /29	10.19.8.97
S2 VLAN 4 SVI	10.19.8.99 /29	10.19.8.97

```
S1(config)#interface vlan 4
S1(config-if)#ip address 10.19.8.98 255.255.255.248
S1(config-if)#description Management Interface
S1(config-if)#no shutdown
S1(config-if)#exit

S1(config)#ip default-gateway 10.19.8.97
```

```
S2(config)#interface vlan 4
S2(config-if)#ip address 10.19.8.99 255.255.255.248
S2(config-if)#description Management Interface
S2(config-if)#no shutdown
S2(config-if)#exit

S2(config)#ip default-gateway 10.19.8.97
```

### Part 3: Configure Network Infrastructure Settings (VLANs, Trunking, EtherChannel)

在交换机 S1 和 S2 上进行配置

#### Step 1: Configure VLANs and Trunking.

- a. 根据 VLAN 表创建 VLAN.

```
S1(config)#vlan 2
S1(config-vlan)#name Bikes
S1(config-vlan)#vlan 3
S1(config-vlan)#name Trikes
S1(config-vlan)#vlan 4
S1(config-vlan)#name Management
S1(config-vlan)#vlan 5
S1(config-vlan)#name Parking
S1(config-vlan)#vlan 6
S1(config-vlan)#name Native
```

```
S2(config)#vlan 2
S2(config-vlan)#name Bikes
S2(config-vlan)#vlan 3
S2(config-vlan)#name Trikes
S2(config-vlan)#vlan 4
S2(config-vlan)#name Management
S2(config-vlan)#vlan 5
S2(config-vlan)#name Parking
S2(config-vlan)#vlan 6
S2(config-vlan)#name Native
```

- b. Create 802.1Q VLAN trunks on ports **F0/1** and **F0/2**. On S1, **F0/5** should also be configured as a trunk. Use **VLAN 6 as the native VLAN**.

```
S1(config)#interface range f0/1-2
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 6
S1(config-if-range)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if-range)#exit
```

```
S1(config)#interface f0/5
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 6
S1(config-if)#switchport trunk allowed vlan 2,3,4,5,6
S1(config-if)#exit
```



```
S2(config)#interface range f0/1-2
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 6
S2(config-if-range)#switchport trunk allowed vlan 2,3,4,5,6
S2(config-if-range)#exit
```

### Step 2: Configure Etherchannel. 链路聚合

Create Layer 2 EtherChannel **port group 1** that uses **interfaces F0/1 and F0/2 on S1 and S2**. Both ends of the channel should negotiate the **LACP** link.

```
S1(config)#interface range f0/1-2
S1(config-if-range)#channel-group 1 mode active
S1(config-if-range)#interface port-channel 1
S1(config-if-range)#exit
```

```
S2(config)#interface range f0/1-2
S2(config-if-range)#channel-group 1 mode active
S2(config-if-range)#interface port-channel 1
S2(config-if-range)#exit
```

### Step 3: Configure Switchports.

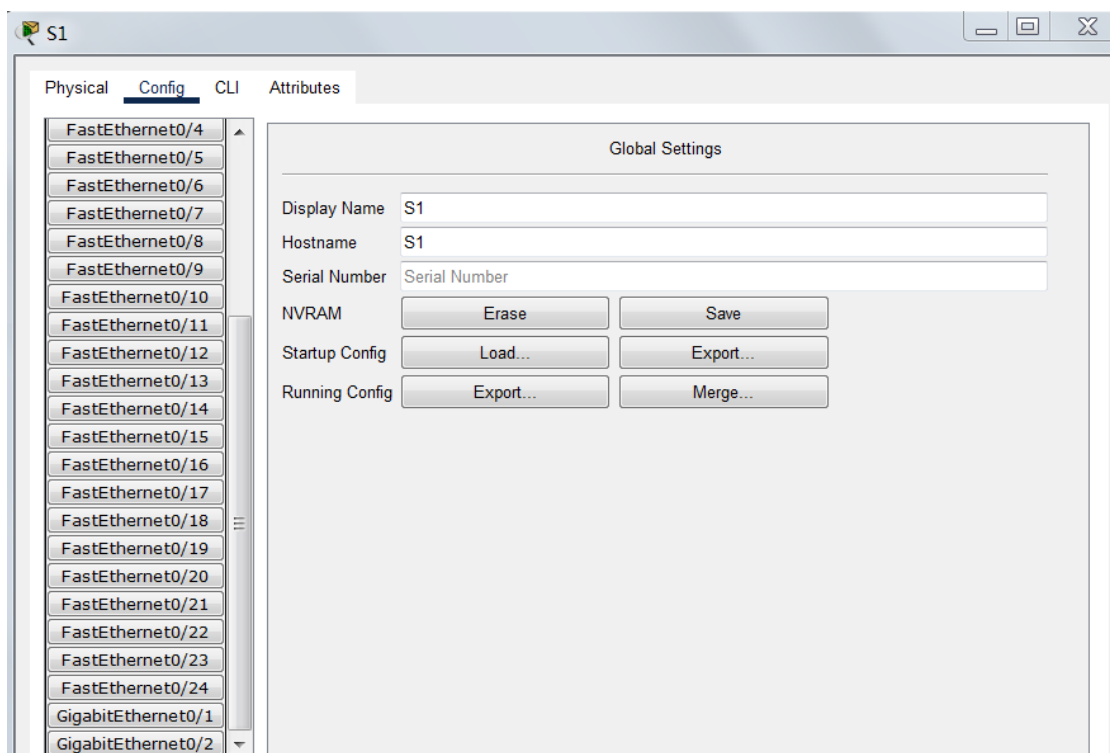
- 在 S1 上，将连接到主机 PC-A 的端口配置为 VLAN 2 的静态访问模式。
- 在 S2 上，将连接到主机 PC-B 的端口配置为 VLAN 3 的静态访问模式。
- 在 S1 和 S2 active access 端口上配置端口安全，只接受三个学习的 MAC 地址。  
【3 个 MAC 地址，分别是 PC-A，PC-B，路由器 G0/0/1 端口的 MAC 地址】
- 将所有未使用的交换机端口分配给两个交换机上的 VLAN 5，并关闭这些端口。
- 在未使用的端口上配置一个与其状态相关的描述。

```
S1(config)#interface f0/6
S1(config-if)#description host
S1(config-if)#switchport mode access
S1(config-if)#switchport access vlan 2
S1(config-if)#switchport port-security
S1(config-if)#switchport port-security maximum 3

S1(config)#interface range f0/3-4, f0/7-24, g0/1-2
S1(config-if-range)#switchport mode access
S1(config-if-range)#switchport access vlan 5
S1(config-if-range)#description Unused Interfaces
S1(config-if-range)#shutdown
```



【可以从交换机的图像界面，看到这个交换机上的所有端口】



```
S2(config)#interface f0/18
S2(config-if)#switchport mode access
S2(config-if)#switchport port-security
S2(config-if)#switchport access vlan 3
S2(config-if)#switchport port-security maximum 3

S2(config)#interface range f0/3-17, f0/19-24, g0/1-2
S2(config-if-range)#switchport mode access
S2(config-if-range)#switchport access vlan 5
S2(config-if-range)#description Unused Interfaces
S2(config-if-range)#shutdown
```

#### Part 4: Configure Host Support

##### Step 1: Configure Default Routing on R1

- 配置一个 IPv4 默认路由，使用 Lo0 接口作为出口接口。
- 配置一个 IPv6 默认路由，使用 Lo0 接口作为出口接口。

【这里出口接口指对于在路由转发表上无法匹配的 IP 数据报都转发到出口接口】

```
R1(config)#ip route 0.0.0.0 0.0.0.0 loopback 0
R1(config)#ipv6 route ::/0 loopback 0
```

##### Step 2: Configure IPv4 DHCP for VLAN 2

a. On R1, create a **DHCP pool** called **CCNA-A** that consists of the last 10 host addresses in the VLAN 2 subnet only.

【解析；包含 VLAN 2 对应的子网中最后 10 个可分配主机地址。首先分析 VLAN 2 包含的可分配地址。】

根据地址表中，VLAN 2 对应的路由器子接口的 IP 地址；10.19.8.1 /26。可以推断，VLAN 2 对应的子网是 10.19.8.0，255.255.255.11000000=192

地址范围是；10.19.8.1-10.19.8.62 【10.19.8.0 是网络号，10.19.8.63 是这个子网的广播地址】因此可分配的最后 10 个 IP 地址是 10.19.8.53-10.19.8.62。因此这个地址池排除的 IP 地址范围是 10.19.8.1-10.19.8.52

b. Configure the correct default gateway address in the pool. 【配置默认网关】

c. Configure the domain name of ccna-a.net. 【配置域名】

```
R1(config)#ip dhcp excluded-address 10.19.8.1 10.19.8.52
R1(config)#ip dhcp pool CCNA-A
R1(dhcp-config)#network 10.19.8.0 255.255.255.192
R1(dhcp-config)#default-router 10.19.8.1
R1(dhcp-config)#domain-name ccna-a.net
R1(dhcp-config)#exit
```

### Step 3: Configure IPv4 DHCP for VLAN 3

a. On R1, create a DHCP pool called CCNA-B that consists of the last 10 host addresses in the VLAN 3 subnet only.

b. Configure the correct default gateway address in the pool.

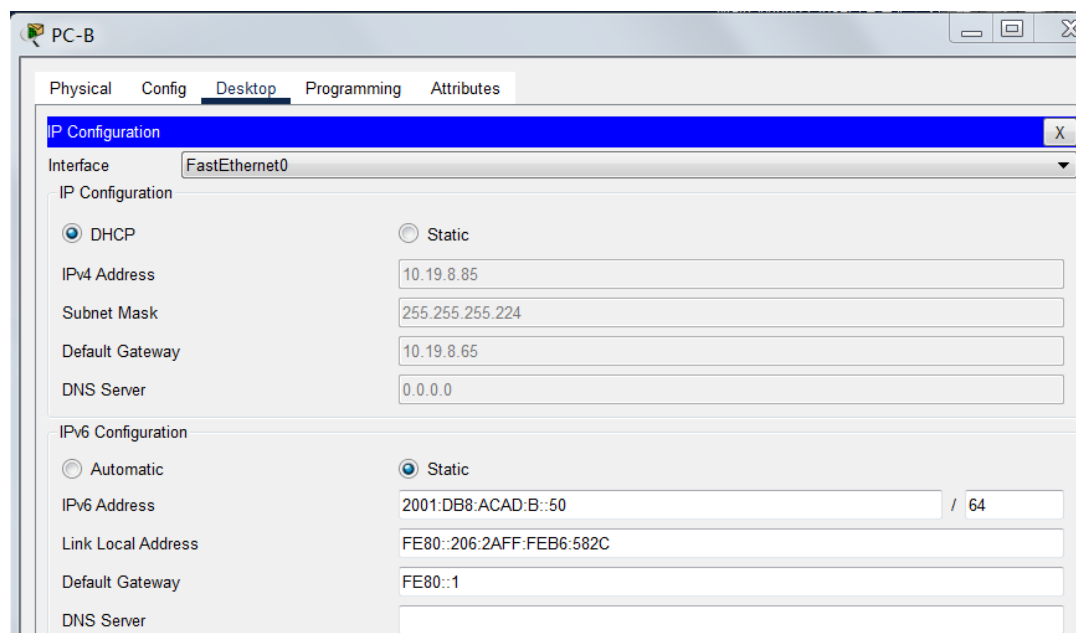
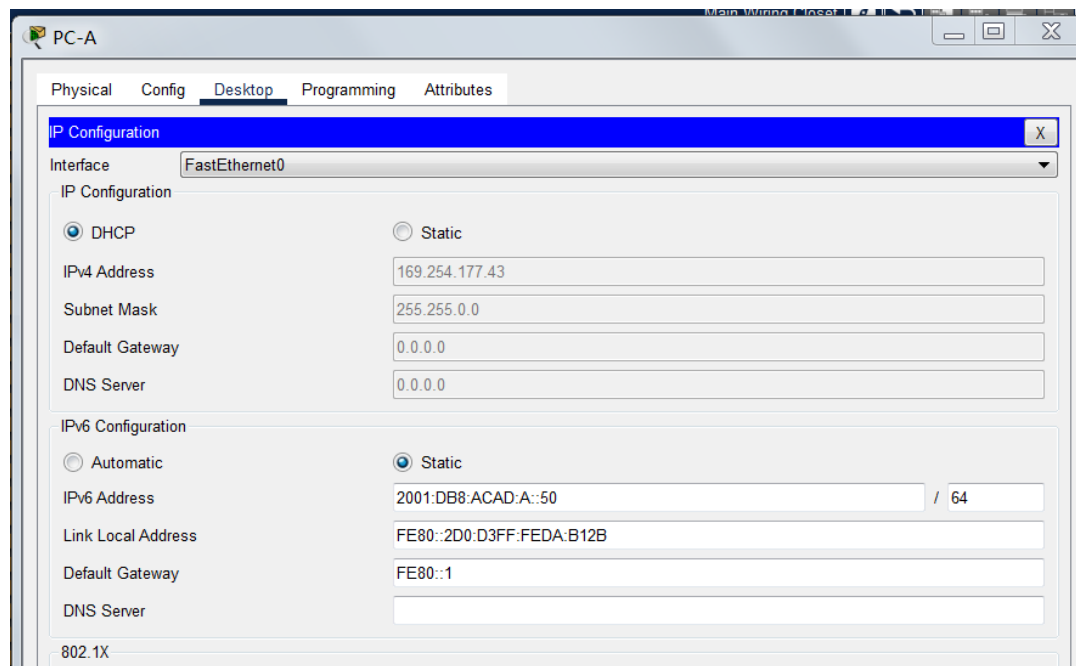
c. Configure the domain name of ccna-b.net.

【解析，同理 VLAN 3 对应的路由器的子接口的 IP 地址 10.19.8.65/27，65=01000001，由此可知 VLAN 3 对应的子网的网络号是 10.19.8.64=010 00000，子网掩码为 255.255.255.11100000 =224。VLAN 3 的子网的可分配地址范围是 10.19.8.65-10.19.8.94，因此最后可分配 IP 地址是 10.19.8.85-10.19.8.94，建立地址池需要排除的地址范围是 10.19.8.64-10.19.8.84】 fe80::

```
R1(config)#ip dhcp excluded-address 10.19.8.65 10.19.8.84
R1(config)#ip dhcp pool CCNA-B
R1(dhcp-config)#network 10.19.8.64 255.255.255.224
R1(dhcp-config)#default-router 10.19.8.65
R1(dhcp-config)#domain-name ccna-b.net
R1(dhcp-config)#exit
```

#### Step 4: Configure host computers.

- 配置主机以使用 DHCP 进行 IPv4 寻址。
- 使用寻址表中的值静态分配 IPv6 GUA 和默认网关地址。



【注意：IPV4 地址是动态配置的】

**Part5: 利用 PC-A 和 PC-B 进行连通性测试**

From	To	Protocol	IP Address	Ping Results
PC-A	R1, G0/0/1.2	IPv4	10.19.8.1	同一个子网
		IPv6	2001:db8:acad:a::1	
	R1, G0/0/1.3	IPv4	10.19.8.65	不同子网，通过 路由器中转
		IPv6	2001:db8:acad:b::1	
	R1, G0/0/1.4	IPv4	10.19.8.97	不同子网，通过 路由器中转
		IPv6	2001:db8:acad:c::1	
	S1, VLAN 4	IPv4	10.19.8.98	不同子网，通过 路由器中转 g0/0/1.4
	S2, VLAN 4	IPv4	10.19.8.99	不同子网，通过 路由器中转 g0/0/1.4 到达 S1,S1 再通过聚 合链路发送给 S2
	PC-B	IPv4	IP address will vary.	不同子网，通过 路由器中转 g0/0/1.3，到 S1 加 VLAN 3 标 记，通过聚合链 路发送给 S2，S2 发送给 PC-B
		IPv6	2001:db8:acad:b::50	
PC-B	R1 Loop0	IPv4	209.165.201.1	不同子网，路由 器直接转发给还 回端口
		IPv6	2001:db8:acad:209::1	
	R1, G0/0/1.2	IPv4	10.19.8.1	
		IPv6	2001:db8:acad:a::1	
	R1, G0/0/1.3	IPv4	10.19.8.65	
		IPv6	2001:db8:acad:b::1	
	R1, G0/0/1.4	IPv4	10.19.8.97	

From	To	Protocol	IP Address	Ping Results
		IPv6	2001:db8:acad:c::1	
	S1, VLAN 4	IPv4	10.19.8.98	
	S2, VLAN 4	IPv4	10.19.8.99	

## 八、思科得分点

Performance Component: Build the Network

Description:

Maximum Points = 3

Work Product Feature	Student Result	Earned Points	Max Points
Build the Network			3
Assemble the Network			1
Network:R1:Power 【加电】			
Network:S1:Power 【加电】			
Network:S2:Power 【加电】			
Network:PC-A:Power 【加电】			
Network:PC-B:Power 【加电】			
Connect Devices			2
Network:R1:Ports:GigabitEthernet0/0/1:Link to S1:Connects to FastEthernet0/5			
Network:R1:Ports:GigabitEthernet0/0/1:Link to S1:Type			
Network:S1:Ports:FastEthernet0/1:Link to S2:Connects to FastEthernet0/1			
Network:S1:Ports:FastEthernet0/1:Link to S2:Type			
Network:S1:Ports:FastEthernet0/2:Link to S2:Connects to FastEthernet0/2			
Network:S1:Ports:FastEthernet0/2:Link to S2:Type			
Network:S1:Ports:FastEthernet0/6:Link to PC-A:Connects to FastEthernet0			
Network:S1:Ports:FastEthernet0/6:Link to PC-A:Type			
Network:S2:Ports:FastEthernet0/18:Link to PC-B:Connects to FastEthernet0			
Network:S2:Ports:FastEthernet0/18:Link to PC-B:Type			

### Performance Component: Configure Host Computers

Description:

Maximum Points = 2

Work Product Feature	Student Result	Earned Points	Max Points
Configure Host Computers			2
IPv4 DHCP Client Configuration			2
<i>Network:PC-A:Ports:FastEthernet0:DHCP client enable</i>			
<i>Network:PC-B:Ports:FastEthernet0:DHCP client enable</i>			

### Performance Component: Configure Initial Settings on IOS Devices

Description:

Maximum Points = 13

Work Product Feature	Student Result	Earned Points	Max Points
Configure Initial Settings on IOS Devices			13
Configure S1 Basic Settings			3
<i>Network:S1:Host Name</i>			
<i>Network:S1:Enable Secret</i>			
<i>Network:S1:Banner motd</i>			
<i>Network:S1:Console Line:Password</i>			
<i>Network:S1:Console Line:Login</i>			
<i>Network:S1:DNS:IP Domain Lookup</i>			
Configure Inactive S1 Port Descriptions			2
<i>Network:S1:Ports:FastEthernet0/3:Description</i>			
<i>Network:S1:Ports:FastEthernet0/4:Description</i>			
<i>Network:S1:Ports:FastEthernet0/7:Description</i>			
<i>Network:S1:Ports:FastEthernet0/8:Description</i>			
<i>Network:S1:Ports:FastEthernet0/9:Description</i>			
<i>Network:S1:Ports:FastEthernet0/10:Description</i>			
<i>Network:S1:Ports:FastEthernet0/11:Description</i>			
<i>Network:S1:Ports:FastEthernet0/12:Description</i>			
<i>Network:S1:Ports:FastEthernet0/13:Description</i>			
<i>Network:S1:Ports:FastEthernet0/14:Description</i>			
<i>Network:S1:Ports:FastEthernet0/15:Description</i>			
<i>Network:S1:Ports:FastEthernet0/16:Description</i>			

<i>Network:S1:Ports:FastEthernet0/17:Description</i>			
<i>Network:S1:Ports:FastEthernet0/18:Description</i>			
<i>Network:S1:Ports:FastEthernet0/19:Description</i>			
<i>Network:S1:Ports:FastEthernet0/20:Description</i>			
<i>Network:S1:Ports:FastEthernet0/21:Description</i>			
<i>Network:S1:Ports:FastEthernet0/22:Description</i>			
<i>Network:S1:Ports:FastEthernet0/23:Description</i>			
<i>Network:S1:Ports:FastEthernet0/24:Description</i>			
<i>Network:S1:Ports:GigabitEthernet0/1:Description</i>			
<i>Network:S1:Ports:GigabitEthernet0/2:Description</i>			
Configure S2 Basic Settings			3
<i>Network:S2:Host Name</i>			
<i>Network:S2:Enable Secret</i>			
<i>Network:S2:Banner motd</i>			
<i>Network:S2:Console Line:Password</i>			
<i>Network:S2:Console Line:Login</i>			
<i>Network:S2:DNS:IP Domain Lookup</i>			
Configure Inactive S2 Port Descriptions			2
<i>Network:S2:Ports:FastEthernet0/3:Description</i>			
<i>Network:S2:Ports:FastEthernet0/4:Description</i>			
<i>Network:S2:Ports:FastEthernet0/5:Description</i>			
<i>Network:S2:Ports:FastEthernet0/6:Description</i>			
<i>Network:S2:Ports:FastEthernet0/7:Description</i>			
<i>Network:S2:Ports:FastEthernet0/8:Description</i>			
<i>Network:S2:Ports:FastEthernet0/9:Description</i>			
<i>Network:S2:Ports:FastEthernet0/10:Description</i>			
<i>Network:S2:Ports:FastEthernet0/11:Description</i>			
<i>Network:S2:Ports:FastEthernet0/12:Description</i>			
<i>Network:S2:Ports:FastEthernet0/13:Description</i>			
<i>Network:S2:Ports:FastEthernet0/14:Description</i>			
<i>Network:S2:Ports:FastEthernet0/15:Description</i>			
<i>Network:S2:Ports:FastEthernet0/16:Description</i>			
<i>Network:S2:Ports:FastEthernet0/17:Description</i>			
<i>Network:S2:Ports:FastEthernet0/19:Description</i>			
<i>Network:S2:Ports:FastEthernet0/20:Description</i>			
<i>Network:S2:Ports:FastEthernet0/21:Description</i>			
<i>Network:S2:Ports:FastEthernet0/22:Description</i>			
<i>Network:S2:Ports:FastEthernet0/23:Description</i>			
<i>Network:S2:Ports:FastEthernet0/24:Description</i>			

<i>Network:S2:Ports:GigabitEthernet0/1:Description</i>			
<i>Network:S2:Ports:GigabitEthernet0/2:Description</i>			
Configure R1 Basic Settings			3
<i>Network:R1:Host Name</i>			
<i>Network:R1:Enable Secret</i>			
<i>Network:R1:Banner motd</i>			
<i>Network:R1:Console Line:Password</i>			
<i>Network:R1:Console Line:Login</i>			
<i>Network:R1:DNS:IP Domain Lookup</i>			

### Performance Component: Configure Router Interfaces

Description:

Maximum Points = 7

Work Product Feature	Student Result	Earned Points	Max Points
Configure Router Interfaces			7
Configure R1 Loopback IPv4 Addressing			2
<i>Network:R1:Ports:Loopback0:IP Address</i>			
<i>Network:R1:Ports:Loopback0:Subnet Mask</i>			
<i>Network:R1:Ports:Loopback0:Power</i>			
Configure R1 Subinterface IPv4 Addressing			5
<i>Network:R1:Ports:GigabitEthernet0/0/1.2:IP Address</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1.2:Subnet Mask</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1.3:IP Address</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1.3:Subnet Mask</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1.4:IP Address</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1.4:Subnet Mask</i>			

### Performance Component: Configure Secure Remote Management Access

Description:

Maximum Points = 18

Work Product Feature	Student	Earned	Max
----------------------	---------	--------	-----



	Result	Points	Points
Configure Secure Remote Management Access			18
R1 SSH Configuration			4
Network:R1:IP Domain Name			
Network:R1:User Names:admin			
Network:R1:VTY Lines:0:Transport Input			
Network:R1:VTY Lines:0:Login			
Network:R1:Security:Modulus Bits			
Network:R1:SSH Server:SSH Server Version			
Network:R1:DNS:IP Domain Name			
S1 SSH Configuration			4
Network:S1:DNS:IP Domain Name			
Network:S1:User Names:admin			
Network:S1:VTY Lines:0:Transport Input			
Network:S1:VTY Lines:0:Login			
Network:S1:Security:Modulus Bits			
Network:S1:IP Domain Name			
Network:S1:SSH Server:SSH Server Version			
S2 SSH Configuration			4
Network:S2:DNS:IP Domain Name			
Network:S2:User Names:admin			
Network:S2:VTY Lines:0:Transport Input			
Network:S2:VTY Lines:0:Login			
Network:S2:Security:Modulus Bits			
Network:S2:IP Domain Name			
Network:S2:SSH Server:SSH Server Version			
Configure S1 SVI			3
Network:S1:Ports:Vlan4:Power			
Network:S1:Ports:Vlan4:IP Address			
Network:S1:Ports:Vlan4:Subnet Mask			
Network:S1:Default Gateway			
Configure S2 SVI			3
Network:S2:Ports:Vlan4:Power			
Network:S2:Ports:Vlan4:IP Address			
Network:S2:Ports:Vlan4:Subnet Mask			
Network:S2:Default Gateway			

## Performance Component: Configure VLANs and Trunks

Description:

Maximum Points = 21

Work Product Feature	Student Result	Earned Points	Max Points
Configure VLANs and Trunks			21
Configure S1 VLANs			3
<i>Network:S1:VLANs:2:VLAN Name</i>			
<i>Network:S1:VLANs:3:VLAN Name</i>			
<i>Network:S1:VLANs:4:VLAN Name</i>			
<i>Network:S1:VLANs:5:VLAN Name</i>			
<i>Network:S1:VLANs:6:VLAN Name</i>			
Configure S2 VLANs			3
<i>Network:S2:VLANs:2:VLAN Name</i>			
<i>Network:S2:VLANs:3:VLAN Name</i>			
<i>Network:S2:VLANs:4:VLAN Name</i>			
<i>Network:S2:VLANs:5:VLAN Name</i>			
<i>Network:S2:VLANs:6:VLAN Name</i>			
Configure Active Access Port VLAN Membership		0	3
<i>Network:S1:Ports:FastEthernet0/6:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/18:Access VLAN</i>			
Configure S1 Inactive Port VLAN Membership		0	4
<i>Network:S1:Ports:FastEthernet0/3:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/4:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/7:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/8:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/9:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/10:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/11:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/12:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/13:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/14:Access VLAN</i>			

<i>Network:S1:Ports:FastEthernet0/15:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/16:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/17:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/18:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/19:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/20:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/21:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/22:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/23:Access VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/24:Access VLAN</i>			
<i>Network:S1:Ports:GigabitEthernet0/1:Access VLAN</i>			
<i>Network:S1:Ports:GigabitEthernet0/2:Access VLAN</i>			
Configure S2 Inactive Port VLAN Membership			4
<i>Network:S2:Ports:FastEthernet0/3:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/4:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/5:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/6:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/7:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/8:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/9:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/10:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/11:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/12:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/13:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/14:Access</i>			

<i>VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/15:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/16:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/17:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/19:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/20:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/21:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/22:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/23:Access VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/24:Access VLAN</i>			
<i>Network:S2:Ports:GigabitEthernet0/1:Access VLAN</i>			
<i>Network:S2:Ports:GigabitEthernet0/2:Access VLAN</i>			
Configure Trunk Ports		0	4
<i>Network:S1:Ports:FastEthernet0/5:Port Mode</i>			
<i>Network:S1:Ports:FastEthernet0/5:Native VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/1:Port Mode</i>			
<i>Network:S1:Ports:FastEthernet0/1:Native VLAN</i>			
<i>Network:S1:Ports:FastEthernet0/2:Port Mode</i>			
<i>Network:S1:Ports:FastEthernet0/2:Native VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/1:Port Mode</i>			
<i>Network:S2:Ports:FastEthernet0/1:Native VLAN</i>			
<i>Network:S2:Ports:FastEthernet0/2:Port Mode</i>			
<i>Network:S2:Ports:FastEthernet0/2:Native VLAN</i>			

Performance Component: Configure Router Subinterfaces for Inter-VLAN Routing

Description:

Maximum Points = 5

Work Product Feature	Student	Earned	Max
----------------------	---------	--------	-----

	Result	Points	Points
Configure Router Subinterfaces for Inter-VLAN Routing			5
Create and Encapsulate R1 Subinterfaces			3
<i>Network:R1:Ports:GigabitEthernet0/0/1:Power</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 2:Power</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 2:802. 1Q:VLAN ID</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 3:Power</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 3:802. 1Q:VLAN ID</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 4:Power</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 4:802. 1Q:VLAN ID</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 6:Power</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 6:802. 1Q:VLAN ID</i>			
Configure R1 Subinterfaces Native VLAN		2	2
<i>Network:R1:Ports:GigabitEthernet0/0/1. 2:802. 1Q:Native VLAN</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 3:802. 1Q:Native VLAN</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 4:802. 1Q:Native VLAN</i>			
<i>Network:R1:Ports:GigabitEthernet0/0/1. 6:802. 1Q:Native VLAN</i>			

## Performance Component: Configure Etherchannel

Description:

Maximum Points = 10

Work Product Feature	Student Result	Earned Points	Max Points
Configure Etherchannel		0	10
Configure Channel Groups		0	5
<i>Network:S1:Ports:FastEthernet0/1:Channel Group</i>			
<i>Network:S1:Ports:FastEthernet0/2:Channel Group</i>			
<i>Network:S2:Ports:FastEthernet0/1:Channel Group</i>			

<i>Network:S2:Ports:FastEthernet0/2:Channel Group</i>			
Configure Channel Mode	0	5	
<i>Network:S1:Ports:FastEthernet0/1:Channel mode</i>			
<i>Network:S1:Ports:FastEthernet0/2:Channel mode</i>			
<i>Network:S2:Ports:FastEthernet0/1:Channel mode</i>			
<i>Network:S2:Ports:FastEthernet0/2:Channel mode</i>			

### Performance Component: Configure a Router as a DHCP Server

Description:

Maximum Points = 11

Work Product Feature	Student Result	Earned Points	Max Points
Configure a Router as a DHCP Server			11
Configure R1 DHCP Server Excluded Addresses			3
<i>Network:R1:DHCP Server:Excluded Addresses:10. 19. 8. 1 10. 19. 8. 52</i>			
<i>Network:R1:DHCP Server:Excluded Addresses:10. 19. 8. 65 10. 19. 8. 84</i>			
Configure R1 DHCP Pool A	0	4	
<i>Network:R1:DHCP Server:Pools:CCNA-A:Default Gateway</i>			
<i>Network:R1:DHCP Server:Pools:CCNA-A:Network Address</i>			
<i>Network:R1:DHCP Server:Pools:CCNA-A:Subnet mask</i>			
<i>Network:R1:DHCP Server:Pools:CCNA-A:Domain Name</i>			
Configure R1 DHCP Pool B	0	4	
<i>Network:R1:DHCP Server:Pools:CCNA-B:Default Gateway</i>			
<i>Network:R1:DHCP Server:Pools:CCNA-B:Network Address</i>			
<i>Network:R1:DHCP Server:Pools:CCNA-B:Subnet mask</i>			

<i>Network:R1:DHCP Server:Pools:CCNA-B:Domain Name</i>			
--	--	--	--

### Performance Component: Configure Device Security

Description:

Maximum Points = 12

Earned Points = 2

Work Product Feature	Student Result	Earned Points	Max Points
Configure Device Security		2	12
Configure S1 Port Security		0	4
<i>Network:S1:Ports:FastEthernet0/6:Port Security:Enabled</i>			
<i>Network:S1:Ports:FastEthernet0/6:Port Security:Max Secure Mac</i>			
Configure S2 Port Security		0	4
<i>Network:S2:Ports:FastEthernet0/18:Port Security:Enabled</i>			
<i>Network:S2:Ports:FastEthernet0/18:Port Security:Max Secure Mac</i>			
Configure R1 Enhanced Password Security		2	2
<i>Network:R1:Service Password Encryption</i>			
<i>Network:R1:Security Password Min-Length</i>			
Configure S1 Enhanced Password Security		0	1
<i>Network:S1:Service Password Encryption</i>			
Configure S2 Enhanced Password Security		0	1
<i>Network:S2:Service Password Encryption</i>			

### Performance Component: Configure Static Routes

Description:

Maximum Points = 5

Work Product Feature	Student Result	Earned Points	Max Points
Configure Static Routes		0	5
Configure IPv6 Static Route		0	5
<i>Network:R1:Routesv6:Ipv6 Unicast Routing</i>			
<i>Network:R1:Routesv6:Static RoutesV2:Route0</i>			