

# CCNA Exploration 4.0

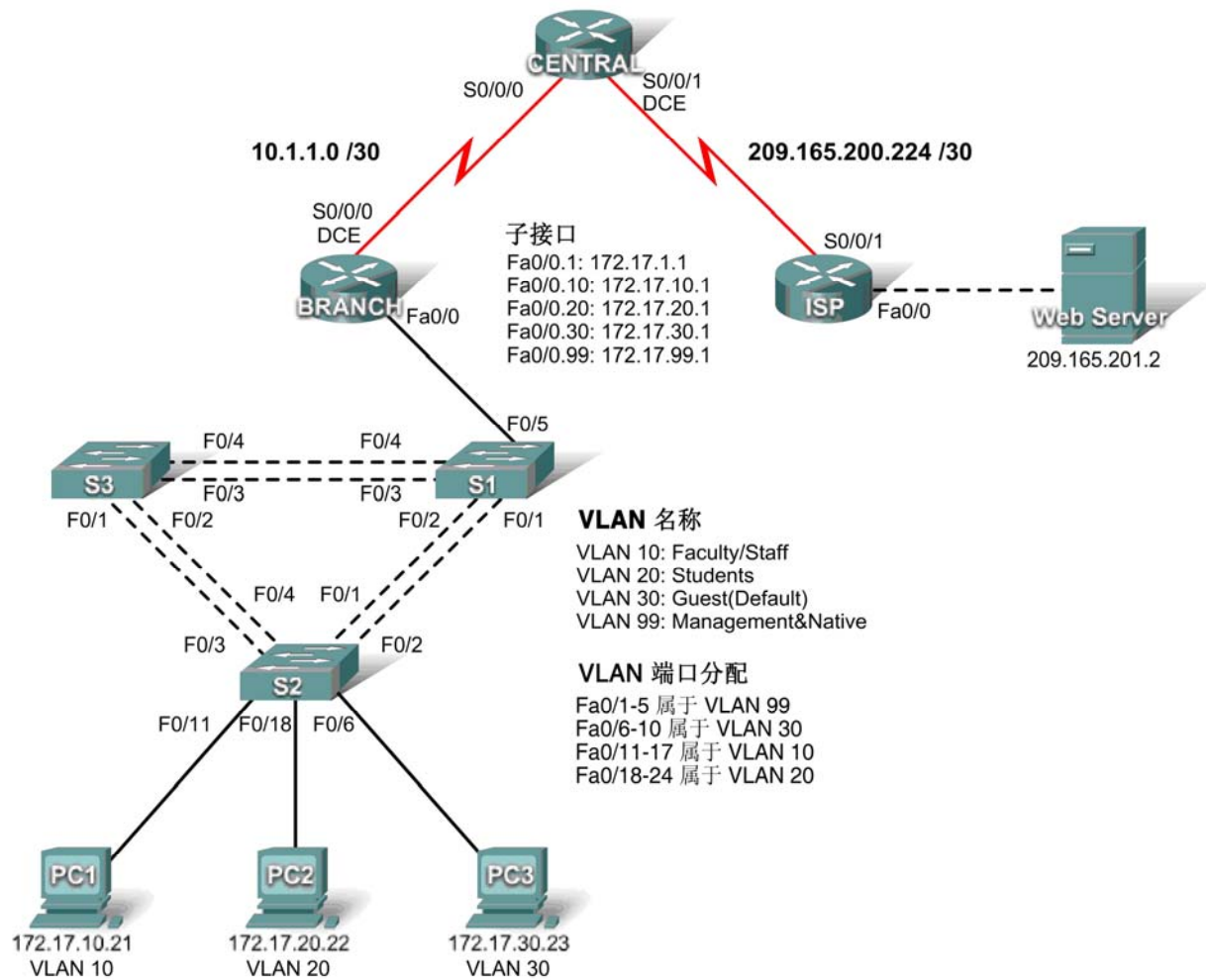
接入 WAN

教师 Packet Tracer 手册

本文档是 Cisco Systems, Inc. 的专有财产，仅允许 Cisco Networking Academy “CCNA Exploration: 接入 WAN” 官方课程中的教师打印或复制本文档并用于非商业分发和内部使用。

## PT 练习 1.5.1: Packet Tracer 综合技能练习 (教师版)

### 拓扑图



## 地址表

设备	接口	IP 地址	子网掩码	默认网关
ISP	S0/0/1	209.165.200.225	255.255.255.252	不适用
	Fa0/0	209.165.201.1	255.255.255.252	不适用
CENTRAL	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	209.165.200.226	255.255.255.252	不适用
BRANCH	S0/0/0	10.1.1.1	255.255.255.252	不适用
	Fa0/0.1	172.17.1.1	255.255.255.0	不适用
	Fa0/0.10	172.17.10.1	255.255.255.0	不适用
	Fa0/0.20	172.17.20.1	255.255.255.0	不适用
	Fa0/0.30	172.17.30.1	255.255.255.0	不适用
	Fa0/0.99	172.17.99.1	255.255.255.0	不适用
S1	VLAN 99	172.17.99.11	255.255.255.0	172.17.99.1
S2	VLAN 99	172.17.99.12	255.255.255.0	172.17.99.1
S3	VLAN 99	172.17.99.13	255.255.255.0	172.17.99.1
PC1	网卡	172.17.10.21	255.255.255.0	172.17.10.1
PC2	网卡	172.17.20.22	255.255.255.0	172.17.20.1
PC3	网卡	172.17.30.23	255.255.255.0	172.17.30.1
Web Server	网卡	209.165.201.2	255.255.255.252	209.165.201.1

## 学习目标

- 配置静态路由和默认路由
- 添加并连接 BRANCH 路由器
- 添加并连接交换机
- 添加并连接 PC
- 执行基本设备配置
- 配置 OSPF 路由
- 配置 STP
- 配置 VTP
- 配置 VLAN
- 检验端到端的连通性

## 简介

本练习覆盖了您在前三门 Exploration 课程中所学的许多技能，包括构建网络、应用编址方案、配置路由、VLAN、STP 和 VTP 以及测试连通性。在继续学习之前，您应先检查这些技能的掌握程度。借此练习机会，您还可以复习有关 Packet Tracer 程序的基本知识。本课程各章都用到了 Packet Tracer。您必须知道如何浏览 Packet Tracer 环境才能完成本课程的学习。如果您需要复习 Packet Tracer 的基本知识，请阅读 Packet Tracer 的 **Help**（帮助）菜单中提供的相关教程。

注：本练习包含 150 多道考题。因此，并非每次输入命令后，您都会看到完成百分比增加。用户执行口令是 **cisco**，特权执行口令是 **class**。

## 任务 1：配置静态路由和默认路由

### 步骤 1. 配置从 ISP 到 CENTRAL 的静态路由。

使用拓扑图为 ISP 配置到达所有网络的静态路由。每个网络都可以通过 ISP 上的 S0/0/1 连通。使用送出接口参数配置到达下列网络的静态路由：

- 10.1.1.0/30
- 172.17.1.0/24
- 172.17.10.0/24
- 172.17.20.0/24
- 172.17.30.0/24
- 172.17.99.0/24

### 步骤 2. 配置从 CENTRAL 到 ISP 的默认路由。

在 CENTRAL 上使用送出接口参数配置默认路由，将所有默认流量发送到 ISP。

### 步骤 3. 测试与 Web Server 的连通性。

CENTRAL 现在应能成功 ping 通 Web Server (209.165.201.2)。

### 步骤 4. 检查结果。

完成比例应为 4%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 2：添加并连接 BRANCH 路由器

### 步骤 1. 添加 BRANCH 路由器。

单击 **Custom Made Devices**（定制设备），将一台 1841 路由器添加到拓扑中。使用 **Config**（配置）选项卡，将 Display Name（显示名称）和 Hostname（主机名）都改为 BRANCH。Display Name（显示名称）区分大小写。

### 步骤 2. 将 BRANCH 连接到 CENTRAL。

- 将 BRANCH 连接到 CENTRAL。
- 配置 BRANCH 和 CENTRAL 之间的链路。
- 时钟频率用 **64000** bps。

### 步骤 3. 检查结果。

完成比例应为 8%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 3: 添加并连接交换机

位置、交换机名称和接口请参照拓扑图。

步骤 1. 使用 2960 型添加 S1、S2 和 S3 交换机。

步骤 2. 将 S1 连接到 BRANCH。

步骤 3. 将 S1 连接到 S2。

步骤 4. 将 S1 连接到 S3。

步骤 5. 将 S2 连接到 S3。

步骤 6. 检查结果。

完成比例应为 28%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 4: 添加并连接 PC

请使用拓扑图和地址表中指定的接口。

步骤 1. 添加 PC1、PC2 和 PC3。

步骤 2. 将 PC1、PC2 和 PC3 连接到 S2。

步骤 3. 配置 PC。

步骤 4. 检查结果。

完成比例应为 41%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 5: 执行基本设备配置

步骤 1. 在 BRANCH、S1、S2 和 S3 上配置基本命令。

基本配置命令应包括主机名、执行模式口令、标语、控制台和 vty 线路。

步骤 2. 在 BRANCH 上配置快速以太网子接口。

不要忘记为每个子接口配置 802.1q 封装和 VLAN 设置。每个子接口地址的第三组二进制八位数与 VLAN 编号对应。例如，子接口 Fa0/0.30 应使用 IP 地址 172.17.30.1，属于 VLAN 30。VLAN 99 为本征 VLAN。

步骤 3. 配置交换机。

- 配置 VLAN 99 接口。
- 配置默认网关。

#### 步骤 4. 检查结果。

完成比例应为 60%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

### 任务 6: 配置 OSPF 路由

#### 步骤 1. 在 **CENTRAL** 上配置 OSPF 并传播默认路由。

- 使用进程 ID 1 配置 OSPF。
- 使用 OSPF 区域 0。
- 仅添加与 **BRANCH** 共享的网络。
- 向 OSPF 邻居传播默认路由。

#### 步骤 2. 在 **BRANCH** 上配置 OSPF。

- 使用进程 ID 1 配置 OSPF。
- 使用 OSPF 区域 0。
- 添加通过 **BRANCH** 路由的所有网络。

#### 步骤 3. 在 **CENTRAL** 和 **BRANCH** 的适当接口上禁用 OSPF 更新。

在所有 LAN 接口和接入 ISP 的接口上禁用 OSPF 更新。

#### 步骤 4. 测试连通性。

**BRANCH** 应该能成功 ping 通 Web Server (209.165.201.2)

#### 步骤 5. 检查结果。

完成比例应为 69%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

### 任务 7: 配置 STP

#### 步骤 1: 确保 **S1** 成为根桥。

将优先级设置为 4096。

#### 步骤 2: 检查 **S1** 是否是根桥。

#### 步骤 3: 检查结果。

完成比例应为 72%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

### 任务 8: 配置 VTP

#### 步骤 1: 在三台交换机上逐一配置 VTP 模式。

将 **S1** 配置为服务器模式。将 **S2** 和 **S3** 配置为客户端模式。

#### 步骤 2: 在三台交换机上逐一配置 VTP 域名。

使用 **CCNA** 作为 VTP 域名。

**步骤 3:** 在三台交换机上逐一配置 VTP 域口令。

使用 **cisco** 作为 VTP 域口令。

**步骤 4:** 检查结果。

完成比例应为 77%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 9: 配置中继

**步骤 1:** 在 **S1**、**S2** 和 **S3** 上配置中继。

将适当的接口配置为中继模式并指定 VLAN 99 为本征 VLAN。

**步骤 2:** 检查结果。

完成比例应为 94%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 10: 配置 VLAN

**步骤 1.** 为 **S1** 配置 VLAN。

VLAN 名称区分大小写。根据以下规定添加四个 VLAN 并为其命名：

- VLAN 10 – **Faculty/Staff**
- VLAN 20 – **Students**
- VLAN 30 – **Guest(Default)**
- VLAN 99 – **Management&Native**

**步骤 2.** 检查 **S2** 和 **S3** 是否已收到 **S1** 传送的 VLAN 配置。

**步骤 3.** 将连接到 PC 的 **S2** 端口配置为接入模式，并将每个端口分配给相应的 VLAN。

**步骤 4.** 检查结果。

完成比例应为 100%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 11: 检验端到端的连通性

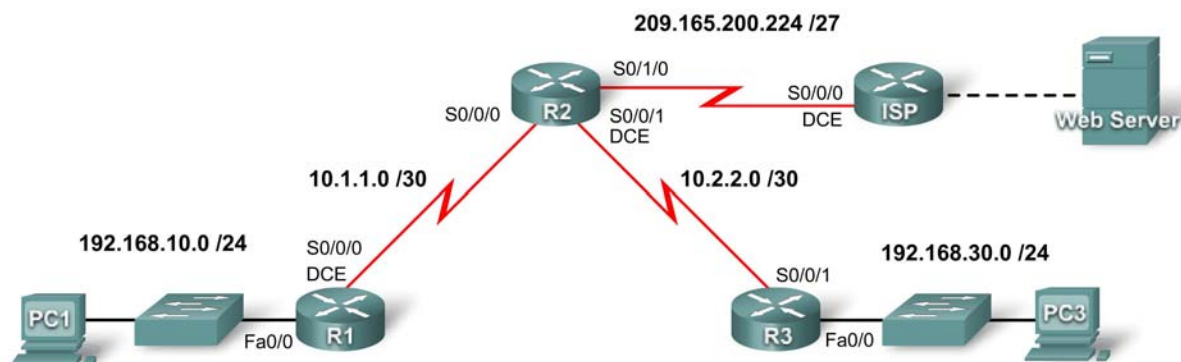
**步骤 1.** 检查 **PC1**、**PC2** 和 **PC3** 能否彼此 ping 通。

**步骤 2.** 检查 **PC1**、**PC2** 和 **PC3** 能否 ping 通 Web Server。



## PT 练习 2.1.7：串行接口故障排除（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.224
	Fa0/0	209.165.200.1	255.255.255.252
Web Server	网卡	209.165.200.2	255.255.255.252
PC1	网卡	192.168.10.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0

### 学习目标

- 测试连通性
- 通过收集数据调查连通性问题
- 实施解决方案并测试连通性



## 简介

在本练习中，您只能访问 PC1 和 PC3 的命令提示符。要排查路由器的故障并实施解决方案，您必须从 PC1 或 PC3 telnet 至路由器。本练习的目标是，排查所有故障，且 PC1 能 ping 通 PC3。

### 任务 1：测试连通性

**步骤 1：使用 ping 命令测试端到端连通性。**

等待 S1 和 S3 上的链路灯从琥珀色变为绿色。然后在 PC1 的命令提示符后 ping PC3。此 ping 命令应该失败。

**步骤 2：使用 traceroute 命令找到存在连通性故障的位置。**

在 PC1 的命令提示符后发出 **tracert** 命令，查找连接失败的位置。

Packet Tracer PC Command Line 1.0  
PC>**tracert 192.168.30.10**

使用组合键 Ctrl-C 中止 **tracert** 命令。最后响应 **tracert** 的是哪一台路由器？

\_\_\_\_\_ 第一阶段中的 R1。

**步骤 3：记录问题的症状。**

\_\_\_\_\_

\_\_\_\_\_

PC1 无法访问自己默认网关以外的位置。

### 任务 2：收集有关问题的数据

**步骤 1：访问最后响应 traceroute 数据包的路由器。**

Telnet 至最后响应 **tracert** 命令的路由器。分别用 **cisco** 和 **class** 作为 telnet 口令和使能口令。

**步骤 2：使用故障排除命令调查此路由器为何无法将 trace 数据包转发到下一跳。**

使用下列命令界定串行接口存在的具体问题：

- **show ip interface brief**
- **show interface serial**
- **show controllers serial**

**show ip interface brief** 命令指示接口配置是否正确，以及是否已使用 **no shutdown** 命令正确启用了接口。

**show interface serial** 命令可提供有关故障接口的详细信息。它会返回以下五种可能状态之一：

- Serial x is down, line protocol is down
- Serial x is up, line protocol is down
- Serial x is up, line protocol is up (looped)
- Serial x is up, line protocol is down (disabled)
- Serial x is administratively down, line protocol is down

**show interface serial** 命令还可显示该接口上使用的封装类型。本练习中的所有路由器都应使用 HDLC 封装。

**show controllers serial** 命令指示接口通道的状态，以及接口是否连接了电缆。

此外，为了检测问题，可能还需要检查连接的路由器是否配置正确。

### 步骤 3: 记录问题并提出建议的解决方案。

串行链路故障可能出于哪些原因？

---

---

---

在 R1 上，学生应注意到 S0/0/0 的状态分别为“up”和“down”。尝试使用 **no shutdown** 命令启用它将无效，因为该接口的物理状态已经为“up”。通过进一步调查，学生应发现，封装类型设置为 PPP。解决方案应该用 **no encap ppp** 命令或 **encap hdlc** 命令将其更改为 HDLC 封装。

在 R2 上，学生应注意到 s0/0/1 的状态分别为“down”和“down”。对接口发出 **no shutdown** 命令将无效。**show interface se 0/0/1** 命令没有显示任何问题，但 **show controllers se 0/0/1** 命令却显示，该接口连接了 DCE 电缆，不过没有设置时钟频率。解决方案是将时钟频率设置为 64000 bps。

在 R3 上，学生应注意到 se0/0/1 的状态分别为“administratively down”和“down”。因此，学生应该立即知道，问题极有可能是该接口缺少 **no shutdown** 命令。

## 任务 3: 实施解决方案并测试连通性

步骤 1: 根据任务 2 中建议的解决方案做出更改。

步骤 2: 使用 **ping** 命令测试端到端连通性。

从路由器或 PC1 的命令行发出 **ping** 和 **tracert** 命令，测试与 PC3 的连通性。

如果 ping 失败，请返回到任务 2 继续排查故障。在有些情况下，故障排查过程可能需要从 PC3 开始。

步骤 3. 检查结果。

单击 **Check Results**（检查结果），然后单击 **Connectivity Tests**（连通性测试）选项卡。Connectivity Tests（连通性测试）现在应成功。

步骤 4. 摘要列出您的结论。

问题 1: \_\_\_\_\_

解决方案 1: \_\_\_\_\_

问题 2: \_\_\_\_\_

解决方案 2: \_\_\_\_\_

问题 3: \_\_\_\_\_

解决方案 3: \_\_\_\_\_

问题 1: R1 serial 0/0/0 封装不匹配

解决方案: 对 s0/0/0 发出 **encapsulation hdlc** 命令

问题 2: R2 serial 0/0/1 缺少时钟频率

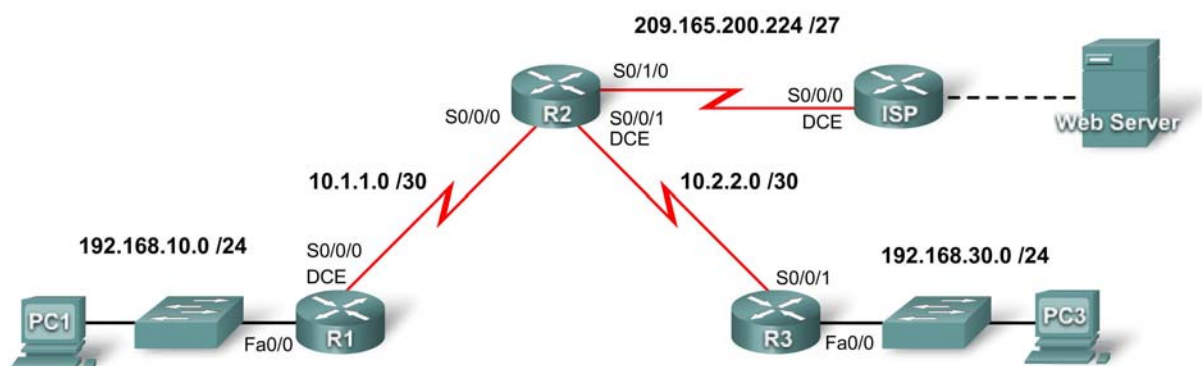
解决方案: 对 s0/0/1 发出 **clock rate 64000** 命令

问题 3: R3 serial 0/0/1 关闭

解决方案: 对 s0/0/1 发出 **no shutdown** 命令

## PT 练习 2.3.4：配置点对点封装（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/0	192.168.10.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
R2	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
	S0/1/0	209.165.200.225	255.255.255.252	不适用
R3	Fa0/0	192.168.30.1	255.255.255.0	不适用
	S0/0/1	10.2.2.2	255.255.255.252	不适用
ISP	S0/0/0	209.165.200.226	255.255.255.252	不适用
	Fa0/0	209.165.200.1	255.255.255.252	不适用
Web Server	网卡	209.165.200.2	255.255.255.252	209.165.200.1
PC1	网卡	192.168.10.10	255.255.255.0	192.168.10.1
PC3	网卡	192.168.30.10	255.255.255.0	192.168.30.1

### 学习目标

- 检查路由配置
- 将 PPP 配置为封装方法
- 将 HDLC 配置为封装方法

## 任务 1: 检查路由配置。

### 步骤 1. 查看所有路由器的运行配置。

记录下静态和动态路由配置。在本章最后的 Packet Tracer 综合技巧练习中，您需要配置这两种类型的路由。

### 步骤 2. 测试计算机和 Web 服务器之间的连通性。

1. 从 PC1 打开命令行窗口。
2. 发出命令 **ping 209.165.200.2**
3. 对 PC3 重复此操作。

两条 **ping** 命令都应该成功。请记住，STP 和 OSPF 需要足够的时间才能收敛。

## 任务 2: 将 PPP 配置为封装方法。

### 步骤 1. 将 R1 配置为与 R2 之间使用 PPP 封装。

```
R1(config)#interface serial0/0/0  
R1(config-if)#encapsulation ppp
```

### 步骤 2. 将 R2 配置为与 R1 和 R3 之间使用 PPP 封装。

### 步骤 3. 将 R3 配置为与 R2 之间使用 PPP 封装。

### 步骤 4. 测试计算机和 Web 服务器之间的连通性。

为什么 OSPF 在封装更改后需要收敛？

---

---

---

当链路一端的封装方法更改后，链路会断开。**dead** 间隔时间过后，路由器会被标记为 **down**，停止接收 Hello 数据包的路由器随后会将拓扑更新泛洪到其相邻设备。从路由表中将清除路由。因此，使用 **PPP** 重新建立连接后，路由器必须创建新的邻接关系，然后发送链路状态更新。

### 步骤 5. 检查结果。

完成比例应为 67%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

### 任务 3: 将 HDLC 配置为封装方法。

#### 步骤 1. 将 ISP 配置为与 R2 之间使用 HDLC 封装。

```
ISP(config)#interface serial0/0/0
ISP(config-if)#encapsulation hdlc
ISP(config-if)#no shutdown
```

#### 步骤 2. 将 R2 配置为与 ISP 之间使用 HDLC 封装。

```
R2(config)#interface serial0/1/0
R2(config-if)#encapsulation hdlc
R2(config-if)#no shutdown
```

注: 虽然 Check Results (检查结果) 可能显示为 100%, 但是如果 R2 和 ISP 上没有配置 **no shutdown** 命令, Connectivity Tests (连通性测试) 仍会失败。

#### 步骤 3. 测试计算机和 Web 服务器之间的连通性。

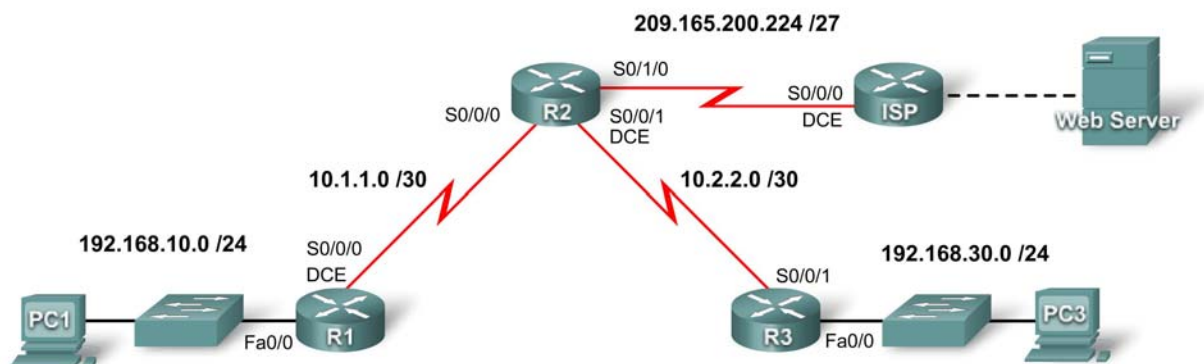
使用 Packet Tracer 简单 PDU 检查连通性。结果应该成功。

#### 步骤 4. 检查结果。

完成比例应为 100%。如果并非如此, 请单击 **Check Results (检查结果)** 查看尚未完成哪些必要部分。

## PT 练习 2.4.6: 配置 PAP 和 CHAP 身份验证 (教师版)

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252
ISP	S0/0/0	209.165.200.226	255.255.255.252
	Fa0/0	209.165.200.1	255.255.255.252
Web Server	网卡	209.165.200.2	255.255.255.252
PC1	网卡	192.168.10.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0

### 学习目标

- 配置 OSPF 路由
- 在 R1 和 R2 之间配置 PAP 身份验证。
- 在 R3 和 R2 之间配置 CHAP 身份验证。

## 简介

PPP 封装支持两种不同类型的身份验证：**PAP**（口令验证协议）和 **CHAP**（挑战握手验证协议）。PAP 使用明文口令，而 CHAP 则调用安全性高于 PAP 的单向哈希。本练习将配置 PAP 和 CHAP 两种验证，同时还要复习 OSPF 路由配置。

### 任务 1: 配置 OSPF 路由

**步骤 1: 在 R1 上启用 OSPF。**

以 **1** 作为 *process-ID*，使用 **router ospf 1** 命令启用 OSPF 路由。

**步骤 2: 在 R1 上配置 network 语句。**

在路由器的配置模式下，使用 **network** 命令添加连接到 R1 的所有网络。在本拓扑结构中，所有 **network** 语句的 OSPF *area-id* 参数均为 **0**。

```
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
```

**步骤 3: 在 R2 和 R3 上配置 network 语句。**

对路由器 R2 和 R3 重复步骤 1 和步骤 2。使用地址表确定正确的语句。在 R2 上，不要通告 209.165.202.224/30 网络。下一步将配置默认路由。

**步骤 4: 建立并重分布 OSPF 默认路由。**

- 在 R2 上，使用命令 **ip route 0.0.0.0 0.0.0.0 s0/1/0** 创建指向 ISP 的静态默认路由。
- 在路由器提示符后发出 **default-information originate** 命令，将该静态路由包括在从 R2 发出的 OSPF 更新中。

**步骤 5: 检验端到端连通性。**

此时在您的配置中，所有设备均应能够 ping 通所有位置。

单击 **Check Results（检查结果）**，然后单击 **Connectivity Tests（连通性测试）**。两项测试的 Status（状态）均应为“Correct（正确）”。R1、R2 和 R3 的路由表均应完整。R1 和 R3 应该有默认路由，与下例 R1 的路由表所示相同。

```
R1#show ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
<output omitted>
```

```
Gateway of last resort is 10.1.1.2 to network 0.0.0.0
```

```
    10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
O       10.2.2.0 [110/128] via 10.1.1.2, 00:03:59, Serial0/0/0
C      192.168.10.0/24 is directly connected, FastEthernet0/0
O      192.168.30.0/24 [110/129] via 10.1.1.2, 00:02:19, Serial0/0/0
O*E2   0.0.0.0/0 [110/1] via 10.1.1.2, 00:02:19, Serial0/0/0
```

**步骤 6: 检查结果。**

完成比例应为 40%。如果并非如此，请单击 **Check Results（检查结果）** 查看尚未完成哪些必要部分。



## 任务 2: 配置 PAP 身份验证。

### 步骤 1: 将 R1 配置为使用 PAP 验证 R2 的身份。

- 在 R1 的全局配置模式下，键入命令 **username R2 password cisco123**。此命令允许远程路由器 R2 使用口令 **cisco123** 连接到 R1。
- 使用 **encapsulation ppp** 命令将 R1 s0/0/0 接口上的封装类型更改为 PPP。
- 在该串行接口的接口配置模式下，使用 **ppp authentication pap** 命令配置 PAP 身份验证。
- 使用 **ppp pap sent-username R1 password cisco123** 命令配置要向 R2 发送的用户名和口令。虽然 Packet Tracer 不对 **ppp pap sent-username R1 password cisco123** 命令评分，但配置 PAP 身份验证时需要使用此命令才能成功。
- 返回到特权执行模式，然后使用 **show ip interface brief** 命令观察 R1 和 R2 之间的链路是否已断开。

```
R1(config)#username R2 password cisco123
R1(config)#interface s0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password cisco123
R1(config-if)#end
%SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	192.168.10.1	YES	manual	up	up
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	10.1.1.1	YES	manual	up	down
Serial0/0/1	unassigned	YES	manual	administratively down	down
Vlan1	unassigned	YES	manual	administratively down	down

### 步骤 2: 将 R2 配置为使用 PAP 验证 R1 的身份。

对 R2 重复步骤 1，使用与 R1 之间的串行链路。

请记住，命令 **username name password password** 中使用的名称始终是远程路由器的名称，但在 **ppp pap sent-username name password password** 命令中，该名称应该是始发路由器的名称。

注：虽然 Packet Tracer 会开通链路，但在实际设备上，您却需要首先对接口发出 **shutdown** 命令，然后再发出 **no shutdown** 命令，促使 PAP 重新验证身份。当然，您也可以重新启动路由器。

### 步骤 3: 测试 PC1 和 Web 服务器之间的连通性。

使用 **show ip interface brief** 命令观察 R1 和 R2 之间的链路现在是否已启用。现在，从 R1 到 Web 服务器的连接应该已恢复。从 PC1 向 Web 服务器发送 ping 命令来测试。

```
R2#show ip interface brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	manual	administratively down	down
FastEthernet0/1	unassigned	YES	manual	administratively down	down
Serial0/0/0	10.1.1.2	YES	manual	up	up
Serial0/0/1	10.2.2.1	YES	manual	up	up
Serial0/1/0	209.165.200.225	YES	manual	up	up
Serial0/1/1	unassigned	YES	manual	administratively down	down
Vlan1	unassigned	YES	manual	administratively down	down

### 步骤 4: 检查结果。

完成比例应为 70%。如果并非如此，请单击 **Check Results（检查结果）** 查看尚未完成哪些必要部分。

### 任务 3: 配置 CHAP 身份验证

**步骤 1:** 将 R3 配置为使用 CHAP 验证 R2 的身份。

- 在 R3 的全局配置模式下，键入 **username R2 password cisco123**。
- 对 s0/0/1 接口发出 **encapsulation ppp** 命令和 **ppp authentication chap** 命令，启用 PPP 封装和 CHAP 身份验证。
- 使用 **show ip interface brief** 命令观察 R2 和 R3 之间的链路是否已断开。

```
R3(config)#username R2 password cisco123
R3(config)#interface s0/0/1
R3(config-if)#encapsulation ppp
R3(config-if)#ppp authentication chap
```

**步骤 2:** 将 R2 配置为使用 CHAP 验证 R3 的身份。

对 R2 重复步骤 1，但用户名应改为 R3，因为 R3 是远程路由器。

**步骤 3:** 测试 PC3 和 Web 服务器之间的连通性。

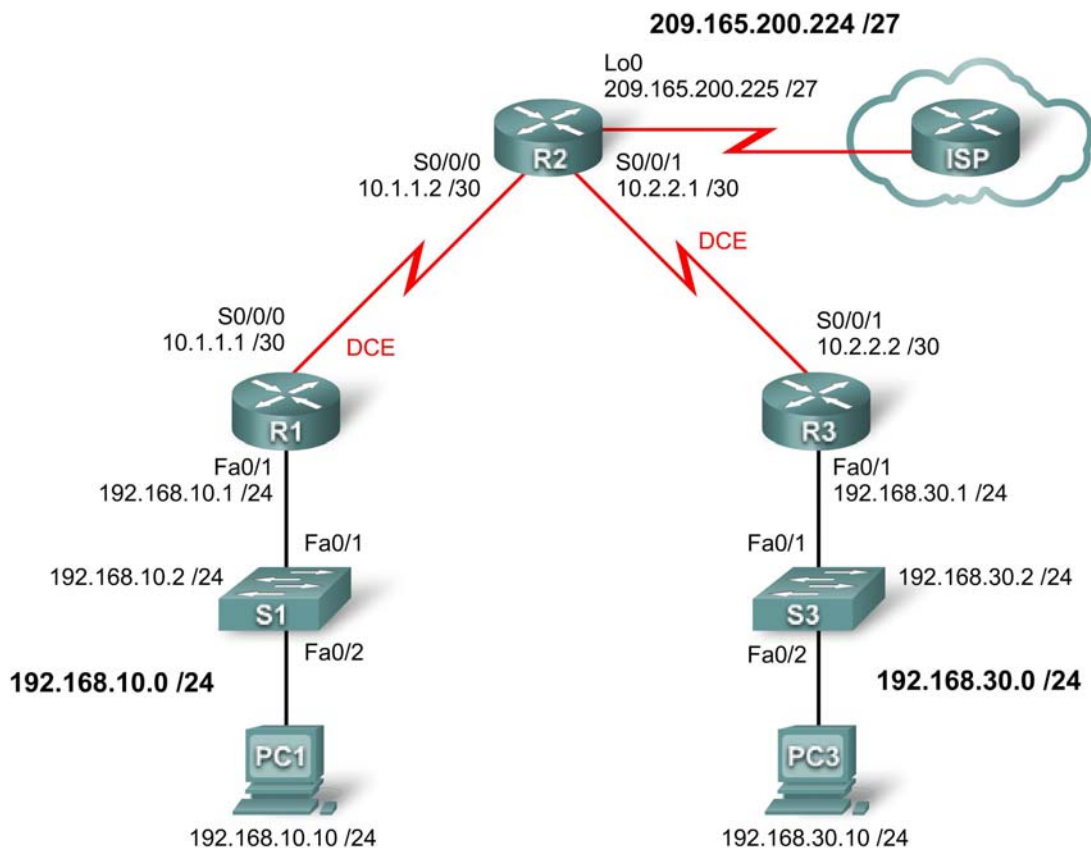
使用 **show ip interface brief** 命令，应该观察到 R2 和 R3 之间的链路现在已启用，而且 PC3 能 ping 通 Web 服务器。

**步骤 4:** 检查结果。

完成比例应为 100%。如果并非如此，请单击 **Check Results（检查结果）** 查看尚未完成哪些必要部分。

## 练习 2.5.1：基本 PPP 配置（教师版）

拓扑图



地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/1	192.168.10.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
R2	Lo0	209.165.200.225	255.255.255.224	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
R3	Fa0/1	192.168.30.1	255.255.255.0	不适用
	S0/0/1	10.2.2.2	255.255.255.252	不适用
PC1	网卡	192.168.10.10	255.255.255.0	192.168.10.1
PC3	网卡	192.168.30.10	255.255.255.0	192.168.30.1

## 学习目标

- 在所有路由器上配置 OSPF 路由
- 在所有串行接口上配置 PPP 封装
- 有意中断然后恢复 PPP 封装
- 配置 PPP PAP 和 CHAP 身份验证
- 有意中断然后恢复 PPP PAP 和 CHAP 身份验证

## 简介

本实验将使用拓扑图中显示的网络学习如何在串行链路上配置 PPP 封装。然后，您还要学习如何将串行链路恢复为其默认的 HDLC 封装。最后，您需要配置 PPP PAP 身份验证和 PPP CHAP 身份验证。

### 任务 1: 在路由器上配置 OSPF

**步骤 1. 在 R1、R2 和 R3 上启用 OSPF 路由。**

以 1 作为进程 ID 发出 **router ospf 1** 命令，进入路由器配置提示符窗口。每台路由器均需通告所有连接的网络。

```
R1(config)#router ospf 1
R1(config-router)#network 192.168.10.0 0.0.0.255 area 0
R1(config-router)#network 10.1.1.0 0.0.0.3 area 0
R1(config-router)#

R2(config)#router ospf 1
R2(config-router)#network 10.1.1.0 0.0.0.3 area 0
R2(config-router)#network 10.2.2.0 0.0.0.3 area 0
R2(config-router)#network 209.165.200.224 0.0.0.31 area 0
R2(config-router)#

R3(config)#router ospf 1
R3(config-router)#network 10.2.2.0 0.0.0.3 area 0
R3(config-router)#network 192.168.30.0 0.0.0.255 area 0
R3(config-router)#
```

**步骤 2. 检查网络是否完全连通。**

使用 **show ip route** 命令和 **ping** 命令检验连通性。

```
R1#show ip route
```

<省略部分输出>

```
10.0.0.0/30 is subnetted, 2 subnets
C    10.1.1.0 is directly connected, Serial0/0/0
O    10.2.2.0 [110/128] via 10.1.1.2, 00:02:22, Serial0/0/0
C    192.168.10.0/24 is directly connected, FastEthernet0/1
O    192.168.30.0/24 [110/129] via 10.1.1.2, 00:00:08, Serial0/0/0
209.165.200.0/32 is subnetted, 1 subnets
O    209.165.200.225 [110/65] via 10.1.1.2, 00:02:22, Serial0/0/0
```

```
R1#ping 192.168.30.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:
!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms  
R1#

R2#**show ip route**

<省略部分输出>

```
      10.0.0.0/30 is subnetted, 2 subnets
C      10.1.1.0 is directly connected, Serial0/0/0
C      10.2.2.0 is directly connected, Serial0/0/1
O      192.168.10.0/24 [110/65] via 10.1.1.1, 00:02:31, Serial0/0/0
O      192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:20, Serial0/0/1
      209.165.200.0/27 is subnetted, 1 subnets
C      209.165.200.224 is directly connected, Loopback0
```

R2#**ping 192.168.30.1**

Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.30.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms  
R2#**ping 192.168.10.1**

Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms  
R2#

R3#**show ip route**

<省略部分输出>

```
      10.0.0.0/30 is subnetted, 2 subnets
O      10.1.1.0 [110/128] via 10.2.2.1, 00:00:34, Serial0/0/1
C      10.2.2.0 is directly connected, Serial0/0/1
O      192.168.10.0/24 [110/129] via 10.2.2.1, 00:00:34, Serial0/0/1
C      192.168.30.0/24 is directly connected, FastEthernet0/1
      209.165.200.0/32 is subnetted, 1 subnets
O      209.165.200.225 [110/65] via 10.2.2.1, 00:00:34, Serial0/0/1
```

R3#**ping 209.165.200.225**

Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.165.200.225, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/16/16 ms  
R3#**ping 192.168.10.1**

Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms  
R3#

## 任务 2: 在串行接口上配置 PPP 封装

### 步骤 1. 使用 **show interface** 命令检查 HDLC 是否默认串行封装。

Cisco 路由器上的默认串行封装是 HDLC。对任意串行接口使用 **show interface** 命令，查看当前的封装类型。

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 10.1.1.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
```

<省略部分输出>

如果检查所有活动的串行接口，其封装均应设置为 HDLC。

### 步骤 2. 将串行接口的封装由 HDLC 改为 PPP。

更改 R1 和 R2 间链路上的封装类型，然后观察其后果。

```
R1(config)#interface serial 0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#
*Aug 17 19:02:53.412: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#
```

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#
```

如果串行链路的一端采用 PPP 封装而链路另一端采用 HDLC 封装，会出现什么情况？

如果在串行链路两端均配置 PPP 封装，又会出现什么情况？

### 步骤 3. 将 R2 和 R3 间串行链路两端的封装均由 HDLC 改为 PPP。

```
R2(config)#interface serial0/0/1
R2(config-if)#encapsulation ppp
R2(config-if)#
*Aug 17 20:02:08.080: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:02:13.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to down
*Aug 17 20:02:58.564: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to up
*Aug 17 20:03:03.644: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
*Aug 17 20:03:46.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to down
R3(config)#interface serial 0/0/1
```

```
R3(config-if)#encapsulation ppp
R3(config-if)#
*Aug 17 20:04:27.152: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to up
*Aug 17 20:04:30.952: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
LOADING to FULL, Loading Done
```

该串行链路上的线路协议何时才会打开并恢复 OSPF 邻接关系？

#### 步骤 4. 检查现在串行接口上的封装类型是否 PPP。

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Internet address is 10.1.1.1/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: CDPCP, IPCP, loopback not set
```

<省略部分输出>

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is GT96K Serial
Internet address is 10.1.1.2/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: CDPCP, IPCP, loopback not set
```

<省略部分输出>

```
R2#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
Hardware is GT96K Serial
Internet address is 10.2.2.1/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: CDPCP, IPCP, loopback not set
```

<省略部分输出>

```
R3#show interface serial 0/0/1
Serial0/0/1 is up, line protocol is up
Hardware is GT96K Serial
Internet address is 10.2.2.2/30
MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: CDPCP, IPCP, loopback not set
```

<省略部分输出>



### 任务 3: 中断然后恢复 PPP 封装

步骤 1. 将 R2 的两个串行接口恢复为其默认的 HDLC 封装。

```
R2(config)#interface serial 0/0/0
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:36:48.432: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from FULL
to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:36:49.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
state to down
R2(config-if)#
*Aug 17 20:36:51.432: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
state to up
R2(config-if)#interface serial 0/0/1
*Aug 17 20:37:14.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
state to down
R2(config-if)#encapsulation hdlc
R2(config-if)#
*Aug 17 20:37:17.368: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
to DOWN, Neighbor Down: Interface down or detached
*Aug 17 20:37:18.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to down
*Aug 17 20:37:20.368: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to up
*Aug 17 20:37:44.080: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to down
```

有意中断配置有何作用？

---

如果您了解用什么方式可以有意中断协议，就可以帮助您明白可能会无意中断协议的情况。当您需要解决故障排除实验中的问题时，您会发现这对您有莫大的帮助。

两个串行接口为什么会先关闭，然后重新打开，最后又再次关闭？

---

接口最初关闭是因为其封装类型不匹配。然后，接口重新打开，试图重新建立连接。当接口无法成功地重新建立连接时，就会再次关闭。

除了使用 `encapsulation hdlc` 命令之外，您能否想到另一种方法，将串行接口的封装由 PPP 更改为默认的 HDLC 封装？（提示：必须使用 `no` 命令。）

```
R2(config)#interface serial 0/0/0
R2(config-if)#no encapsulation ppp
R2(config-if)#interface serial 0/0/1
R2(config-if)#no encapsulation ppp
```

**步骤 2.** 将 R2 的两个串行接口恢复为 PPP 封装。

```
R2(config)#interface s0/0/0
R2(config-if)#encapsulation ppp
*Aug 17 20:53:06.612: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
state to up
R2(config-if)#interface s0/0/1
*Aug 17 20:53:10.856: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
R2(config-if)#encapsulation ppp
*Aug 17 20:53:23.332: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to up
*Aug 17 20:53:24.916: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

#### 任务 4: 配置 PPP 身份验证

**步骤 1.** 在 R1 和 R2 间的串行链路上配置 PPP PAP 身份验证。

```
R1(config)#username R1 password cisco
R1(config)#int s0/0/0
R1(config-if)#ppp authentication pap
R1(config-if)#
*Aug 22 18:58:57.367: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
state to down
*Aug 22 18:58:58.423: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/0 from F
ULL to DOWN, Neighbor Down: Interface down or detached
R1(config-if)#ppp pap sent-username R2 password cisco
```

如果仅在串行链路一端配置 PPP PAP 身份验证，会出现什么情况？

---

接口 **serial 0/0/0** 上的线路协议关闭，而且 **OSPF** 邻接关系进入 **DOWN** 状态。

```
R2(config)#username R2 password cisco
R2(config)#interface Serial0/0/0
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R1 password cisco
R2(config-if)#
*Aug 23 16:30:33.771: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/0, changed
state to up
*Aug 23 16:30:40.815: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on
Serial0/0/0 from LOAD
ING to FULL, Loading Done
```

如果在串行链路两端均配置 PPP PAP 身份验证，会出现什么情况？

---

接口 **serial 0/0/0** 上的线路协议打开并建立 **OSPF** 邻接关系。

**步骤 2. 在 R2 和 R3 间的串行链路上配置 PPP CHAP 身份验证。**

采用 PAP 身份验证时，口令不加密。虽然这无疑强于完全没有身份验证，但较之对链路上传送的口令加密而言，却仍稍逊一筹。CHAP 验证则会对口令加密。

```
R2(config)#username R3 password cisco
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 23 18:06:00.935: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to down
R2(config-if)#
*Aug 23 18:06:01.947: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from FULL
to DOWN, Neighbor Down: Interface down or detached
R2(config-if)#
R3(config)#username R2 password cisco
*Aug 23 18:07:13.074: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to up
R3(config)#int s0/0/1
R3(config-if)#
*Aug 23 18:07:22.174: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from L
OADING to FULL, Loading Done
R3(config-if)#ppp authentication chap
R3(config-if)#
```

请注意，接口 **serial 0/0/1** 上的线路协议甚至在该接口配置 **CHAP** 身份验证之前就已更改为 **UP** 状态。您能猜出原因是什么吗？

**CHAP** 既能执行单向身份验证，也能执行双向身份验证。因此，只要配置了正确的用户名和口令，链路就会进入工作状态。

## 任务 5: 有意中断然后恢复 PPP CHAP 身份验证

### 步骤 1. 中断 PPP CHAP 身份验证。

在 R2 和 R3 间的串行链路上，将接口 **serial 0/0/1** 上的身份验证协议改为 **PAP**。

```
R2#conf t
输入配置命令，每行一条。以 CNTL/Z 结束。
R2(config)#int s0/0/1
R2(config-if)#ppp authentication pap
R2(config-if)#^Z
R2#
*Aug 24 15:45:47.039: %SYS-5-CONFIG_I: Configured from console by console
R2#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R2#reload
将接口 serial 0/0/1 上的身份验证协议改为 PAP 是否会中断 R2 和 R3 之间的身份验证？
```

会。使用 **show ip interface brief** 命令检查协议是否已关闭。如果不重新启动路由器，线路协议会保持打开。

### 步骤 2. 恢复串行链路上的 PPP CHAP 身份验证。

请注意，此更改无需重新启动路由器即可生效。

```
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#int s0/0/1
R2(config-if)#ppp authentication chap
R2(config-if)#
*Aug 24 15:50:00.419: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed
state to up
R2(config-if)#
*Aug 24 15:50:07.467: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on
Serial0/0/1 from LOAD
ING to FULL, Loading Done
R2(config-if)#
```

步骤 3. 在 R3 上更改口令，有意中断 PPP CHAP 身份验证。

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username R2 password ciisco
R3(config)#^Z
R3#
*Aug 24 15:54:17.215: %SYS-5-CONFIG_I: Configured from console by console
R3#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
R3#reload
```

重新启动后，serial 0/0/1 上的线路协议状态是什么？

---

关闭。使用 **show ip interface brief** 命令检查是否如此。

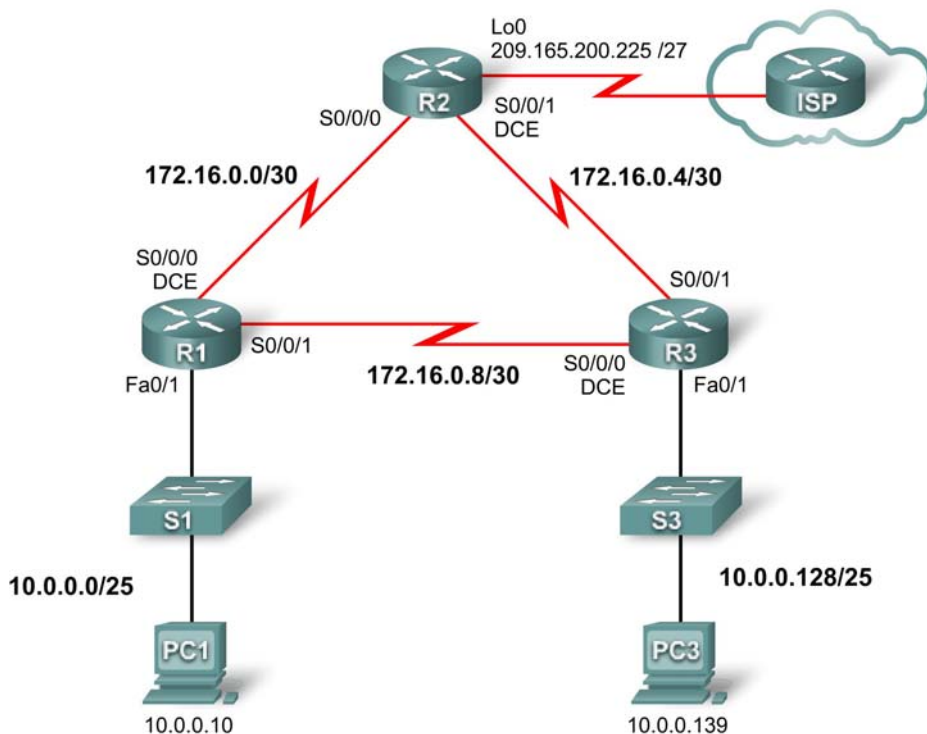
步骤 4. 在 R3 上更改口令，恢复 PPP CHAP 身份验证。

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#username R2 password cisco
R3(config)#
*Aug 24 16:11:10.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Serial0/0/1, changed state to up
R3(config)#
*Aug 24 16:11:19.739: %OSPF-5-ADJCHG: Process 1, Nbr 209.165.200.225 on
Serial0/0/1 from LOADING to FULL, Loading Done
R3(config)#
```

请注意，链路已恢复。从 PC1 ping PC3，以此测试连通性。

## 练习 2.5.2: PPP 配置练习 (教师版)

### 拓扑



### 地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/1	10.0.0.1	255.255.255.128	不适用
	S0/0/0	172.16.0.1	255.255.255.252	不适用
	S0/0/1	172.16.0.9	255.255.255.252	不适用
R2	Lo0	209.165.200.161	255.255.255.224	不适用
	S0/0/0	172.16.0.2	255.255.255.252	不适用
	S0/0/1	172.16.0.5	255.255.255.252	不适用
R3	Fa0/1	10.0.0.129	255.255.255.128	不适用
	S0/0/0	172.16.0.10	255.255.255.252	不适用
	S0/0/1	172.16.0.6	255.255.255.252	不适用
PC1	网卡	10.0.0.10	255.255.255.128	10.0.0.1
PC3	网卡	10.0.0.139	255.255.255.128	10.0.0.129

## 学习目标

- 配置并激活接口
- 在所有路由器上配置 OSPF 路由
- 在所有串行接口上配置 PPP 封装
- 配置 PPP CHAP 身份验证

## 简介

本练习将使用拓扑图中显示的网络在串行链路上配置 PPP 封装。此外还要配置 PPP CHAP 身份验证。如需帮助，可参考“基本 PPP 配置”实验或练习，但应尽量自行完成。

## 任务 1：配置并激活串行地址和以太网地址

**步骤 1. 在 R1、R2 和 R3 上配置接口。**

拓扑图和地址表中列出了编址方案。有些接口提供了地址，但有些接口仅提供了所在网络。如果仅提供了网络地址，则根据 **Packet Tracer** 评分标准，使用指定网络中的任何有效地址均为正确答案。

根据拓扑图配置 R1、R2 和 R3 的接口。串行链路 DCE 端的时钟速率为 64000 位。

### R1

```
!  
interface FastEthernet0/1  
  ip address 10.0.0.1 255.255.255.128  
  no shutdown  
!  
  
interface Serial0/0/0  
  ip address 172.16.0.1 255.255.255.252  
  no shutdown  
  clock rate 64000  
!  
interface Serial0/0/1  
  ip address 172.16.0.9 255.255.255.252  
  no shutdown
```

### R2

```
!  
interface Loopback0  
  ip address 209.165.200.161 255.255.255.224  
!  
!  
interface Serial0/0/0  
  ip address 172.16.0.2 255.255.255.252  
  no shutdown  
!  
interface Serial0/0/1  
  ip address 172.16.0.5 255.255.255.252  
  clock rate 64000  
  no shutdown
```

### R3

```
!  
interface FastEthernet0/1  
  ip address 10.0.0.129 255.255.255.128
```



```
no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.10 255.255.255.252
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.6 255.255.255.252
 clock rate 64000
 no shutdown
```

## 步骤 2. 检验 IP 地址和接口。

检查物理层和数据链路层的所有接口是否均已启用。直连的路由器应该能够彼此 ping 通。

R1#show ip interface brief

Interface	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	manual	administratively down
FastEthernet0/1	10.0.0.1	YES	manual	up
Serial0/0/0	172.16.0.1	YES	manual	up
Serial0/0/1	172.16.0.9	YES	manual	up

R2#show ip interface brief

Interface	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	unset	administratively down
FastEthernet0/1	unassigned	YES	unset	administratively down
Serial0/0/0	172.16.0.2	YES	manual	up
Serial0/0/1	172.16.0.5	YES	manual	up
Loopback0	209.165.200.161	YES	manual	up

R3#show ip interface brief

Interface	IP-Address	OK?	Method	Status
FastEthernet0/0	unassigned	YES	unset	administratively down
FastEthernet0/1	10.0.0.129	YES	manual	up
Serial0/0/0	172.16.0.10	YES	manual	up
Serial0/0/1	172.16.0.6	YES	manual	up

## 步骤 3. 配置 PC1 和 PC3 的以太网接口。

PC1 可使用 10.0.0.2 和 10.0.0.126 之间的任意 IP 地址。PC3 可使用 10.0.0.128 和 10.0.0.254 之间的任意 IP 地址。

## 步骤 4. 测试 PC 之间的连通性。

此时 PC 是否应该能够 ping 通彼此？它们能否 ping 通其默认网关？

## 任务 2: 在路由器上配置 OSPF

### 步骤 1. 在路由器上启用 OSPF 路由。

配置 OSPF 路由时，area-id 使用 0。

```
R1
!
router ospf 1
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
R2
!
router ospf 1
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 209.165.200.160 0.0.0.31 area 0
!
R3
!
router ospf 1
 network 10.0.0.128 0.0.0.127 area 0
 network 172.16.0.4 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
```

### 步骤 2. 检查网络是否完全连通。

所有路由器均应包含到所有网络的路由，而且现在能够 ping 通任何设备。

R1#show ip route

<省略部分输出>

```
      172.16.0.0/30 is subnetted, 3 subnets
C       172.16.0.8 is directly connected, Serial0/0/1
O       172.16.0.4 [110/1562] via 172.16.0.10, 00:09:11, Serial0/0/1
        [110/1562] via 172.16.0.2, 00:09:11, Serial0/0/0
C       172.16.0.0 is directly connected, Serial0/0/0
      209.165.200.0/32 is subnetted, 1 subnets
O       209.165.200.161 [110/782] via 172.16.0.2, 00:09:11, Serial0/0/0
      10.0.0.0/25 is subnetted, 2 subnets
C       10.0.0.0 is directly connected, FastEthernet0/1
O       10.0.0.128 [110/782] via 172.16.0.10, 00:09:11, Serial0/0/1
```

R1#ping 209.165.200.161

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.161, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
R1#ping 10.0.0.129
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.129, timeout is 2 seconds:
```

```
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms  
R2#show ip route
```

<省略部分输出>

```
      172.16.0.0/30 is subnetted, 3 subnets  
O      172.16.0.8 [110/1562] via 172.16.0.6, 00:12:42, Serial0/0/1  
      [110/1562] via 172.16.0.1, 00:12:42, Serial0/0/0  
C      172.16.0.4 is directly connected, Serial0/0/1  
C      172.16.0.0 is directly connected, Serial0/0/0  
      209.165.200.0/27 is subnetted, 1 subnets  
C      209.165.200.160 is directly connected, Loopback0  
      10.0.0.0/25 is subnetted, 2 subnets  
O      10.0.0.0 [110/782] via 172.16.0.1, 00:12:42, Serial0/0/0  
O      10.0.0.128 [110/782] via 172.16.0.6, 00:12:42, Serial0/0/1
```

R2#ping 10.0.0.1

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms  
R2#ping 10.0.0.129
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.0.129, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

R3#show ip route

<省略部分输出>

```
      172.16.0.0/30 is subnetted, 3 subnets  
C      172.16.0.8 is directly connected, Serial0/0/0  
C      172.16.0.4 is directly connected, Serial0/0/1  
O      172.16.0.0 [110/1562] via 172.16.0.9, 00:14:14, Serial0/0/0  
      [110/1562] via 172.16.0.5, 00:14:14, Serial0/0/1  
      209.165.200.0/32 is subnetted, 1 subnets  
O      209.165.200.161 [110/782] via 172.16.0.5, 00:14:14, Serial0/0/1  
      10.0.0.0/25 is subnetted, 2 subnets  
O      10.0.0.0 [110/782] via 172.16.0.9, 00:14:14, Serial0/0/0  
C      10.0.0.128 is directly connected, FastEthernet0/1
```

R3#ping 209.165.200.161

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.165.200.161, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms  
R3#ping 10.0.0.1
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/32 ms
```

### 任务 3: 在串行接口上配置 PPP 封装

#### 步骤 1. 逐一在三台路由器的串行接口上配置 PPP。

所有串行链路上的封装目前均设置为 HDLC。为了稍后配置身份验证，必须将封装类型设置为 PPP。

##### R1

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

##### R2

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

##### R3

```
interface Serial0/0/0
 encapsulation ppp
!
interface Serial0/0/1
 encapsulation ppp
```

#### 步骤 2. 检查所有串行接口是否都在使用 PPP 封装。

如果连接的串行接口封装不匹配，链路就会中断。因此，要确保所有接口都设置为 PPP 封装。

```
R1#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.1/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

```
R1#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.9/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

## R2

```
R2#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.2/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

```
R2#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.5/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

## R3

```
R3#show interface serial0/0/0
Serial0/0/0 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.10/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

```
R3#show interface serial0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is GT96K Serial
  Internet address is 172.16.0.6/30
  MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation PPP, LCP Open
  Open: CDPCP, IPCP, loopback not set
```

## 任务 4: 配置 PPP CHAP 身份验证

CHAP 身份验证的口令为 cisco。

步骤 1. 在所有串行链路上配置 PPP CHAP 身份验证。

### R1

```
username R2 password cisco
username R3 password cisco
interface serial0/0/0
  ppp authentication chap
interface serial0/0/1
  ppp authentication chap
```

### R2

```
username R1 password cisco
username R3 password cisco
interface serial0/0/0
  ppp authentication chap
interface serial0/0/1
  ppp authentication chap
```

### R3

```
username R1 password cisco
username R2 password cisco
interface serial0/0/0
  ppp authentication chap
interface serial0/0/1
  ppp authentication chap
```

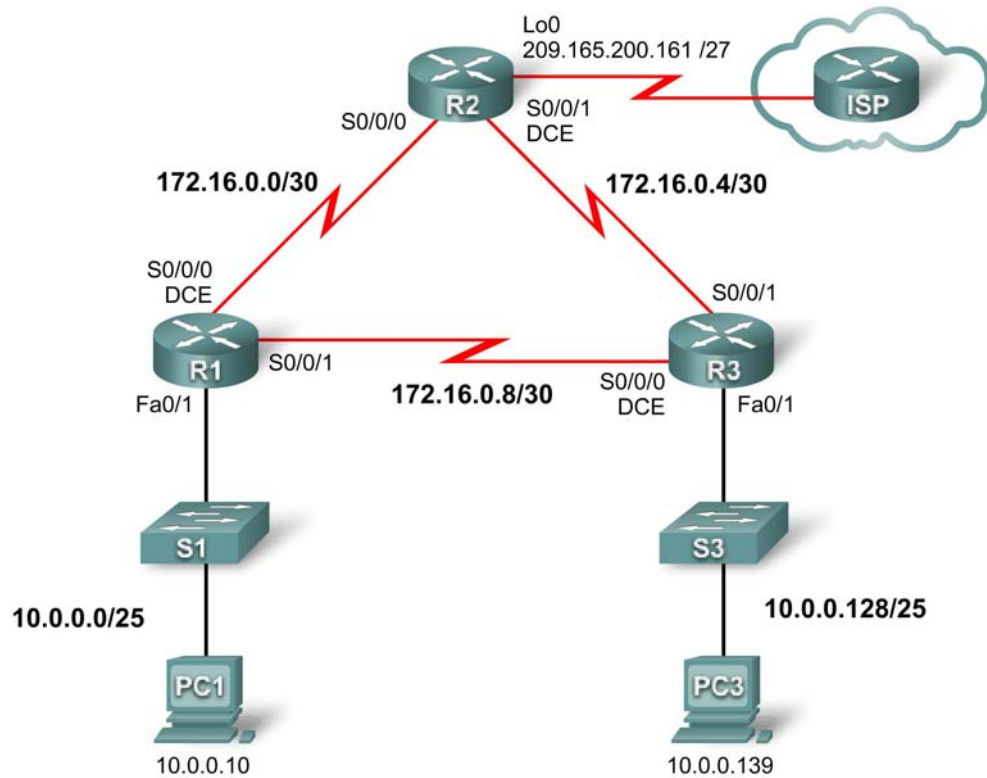
步骤 2. 检验所有串行链路上的 PPP CHAP 身份验证。

所有路由器是否都能相互通信？PC1 能否 ping 通 PC3？

以上两道问题的回答都应该为能。

## 练习 2.5.3: PPP 配置故障排除 (教师版)

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/1	10.0.0.1	255.255.255.128	不适用
	S0/0/0	172.16.0.1	255.255.255.252	不适用
	S0/0/1	172.16.0.9	255.255.255.252	不适用
R2	Lo0	209.165.200.161	255.255.255.224	不适用
	S0/0/0	172.16.0.2	255.255.255.252	不适用
	S0/0/1	172.16.0.5	255.255.255.252	不适用
R3	Fa0/1	10.0.0.129	255.255.255.128	不适用
	S0/0/0	172.16.0.10	255.255.255.252	不适用
	S0/0/1	172.16.0.6	255.255.255.252	不适用
PC1	网卡	10.0.0.10	255.255.255.128	10.0.0.1
PC3	网卡	10.0.0.139	255.255.255.128	10.0.0.129



## 学习目标

- 查找并纠正网络错误
- 记录纠正后的网络

## 场景

配置贵公司路由器的网络工程师缺乏经验，因此，若干配置错误导致了连通性问题。上级要求您排除故障并纠正配置错误，然后记录纠正后的网络。请运用您掌握的 PPP 知识和标准测试方法查找并纠正错误。您要确保所有串行链路均采用 PPP CHAP 身份验证，而且所有网络都可连通。

### 任务 1：查找并纠正网络错误

- 所有时钟频率均使用 **64000**。
- 所有 CHAP 口令均使用 **cisco**。

### 任务 2：记录纠正后的网络

[教师注意事项：以下脚本逐一显示了三台路由器的正确配置。]

**R1**

**R1#show run**

```
!<省略部分输出>
!
hostname R1
!
!
enable secret cisco
!
!
no ip domain lookup
!
username R3 password 0 cisco
username R2 password 0 cisco
!
!
interface FastEthernet0/1
 ip address 10.0.0.1 255.255.255.128
 no shutdown
!
interface Serial0/0/0
 ip address 172.16.0.1 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.9 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
!
```

```
router ospf 1
 network 10.0.0.0 0.0.0.127 area 0
 network 172.16.0.0 0.0.0.3 area 0
 network 172.16.0.8 0.0.0.3 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
 exec-timeout 0 0
 password cisco
 logging synchronous
 login
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

## R2

R2#show run

```
!<省略部分输出>
!
hostname R2
!
!
enable secret cisco
!
!
no ip domain lookup
!
username R1 password 0 cisco
username R3 password 0 cisco
!
!
!
interface Loopback0
 ip address 209.165.200.161 255.255.255.224
!
!
interface Serial0/0/0
 ip address 172.16.0.2 255.255.255.252
 encapsulation ppp
 ppp authentication chap
 no shutdown
!
interface Serial0/0/1
 ip address 172.16.0.5 255.255.255.252
 encapsulation ppp
 clockrate 64000
 ppp authentication chap
 no shutdown
!
```

```
!  
router ospf 1  
  network 172.16.0.0 0.0.0.3 area 0  
  network 172.16.0.4 0.0.0.3 area 0  
  network 209.165.200.160 0.0.0.31 area 0  
!  
!  
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the  
full extent of the law^C  
!  
line con 0  
  exec-timeout 0 0  
  password cisco  
  logging synchronous  
  login  
line aux 0  
line vty 0 4  
  password cisco  
  login  
!  
end
```

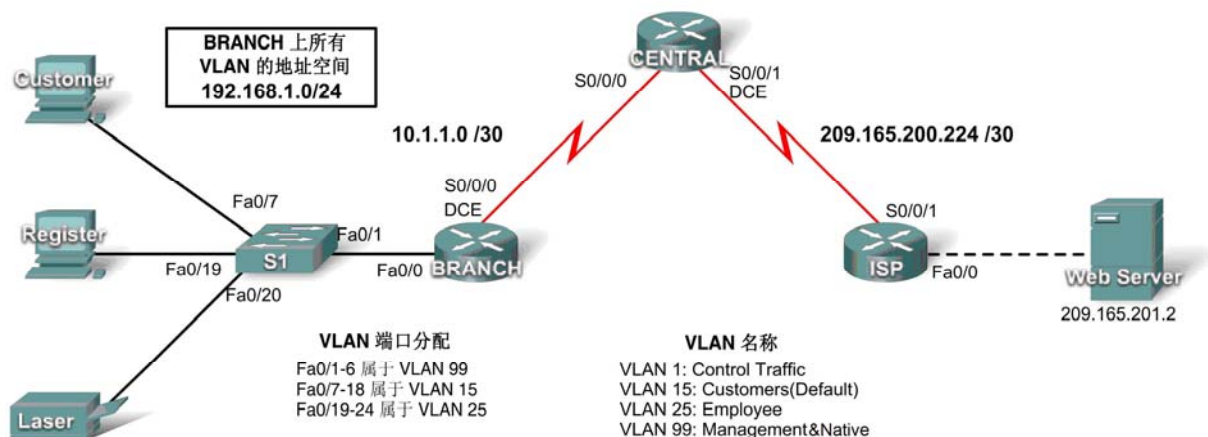
### R3

```
R3#show run  
!<省略部分输出>  
!  
hostname R3  
!  
!  
enable secret cisco  
!  
!  
no ip domain lookup  
!  
username R1 password 0 cisco  
username R2 password 0 cisco  
!  
!  
interface FastEthernet0/1  
  ip address 10.0.0.129 255.255.255.128  
  no shutdown  
!  
interface Serial0/0/0  
  ip address 172.16.0.10 255.255.255.252  
  encapsulation ppp  
  clockrate 64000  
  ppp authentication chap  
  no shutdown  
!  
interface Serial0/0/1  
  ip address 172.16.0.6 255.255.255.252  
  encapsulation ppp  
  ppp authentication chap  
  no shutdown  
!  
router ospf 1
```

```
network 10.0.0.128 0.0.0.127 area 0
network 172.16.0.4 0.0.0.3 area 0
network 172.16.0.8 0.0.0.3 area 0
!
!
banner motd ^CCUnauthorized access strictly prohibited and prosecuted to the
full extent of the law^C
!
line con 0
  exec-timeout 0 0
  password cisco
  logging synchronous
  login
line aux 0
line vty 0 4
  password cisco
  login
!
end
```

## PT 练习 2.6.1: Packet Tracer 综合技能练习（教师版）

拓扑图



地址表

设备	接口	IP 地址	子网掩码	默认网关
CENTRAL	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	209.165.200.226	255.255.255.252	不适用
ISP	S0/0/1	209.165.200.225	255.255.255.252	不适用
	Fa0/0	209.165.201.1	255.255.255.252	不适用
BRANCH	Fa0/1	192.168.1.193	255.255.255.224	不适用
	Fa0/15	192.168.1.1	255.255.255.128	不适用
	Fa0/25	192.168.1.129	255.255.255.192	不适用
	Fa0/99	192.168.1.225	255.255.255.224	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
S1	VLAN99	192.168.1.226	255.255.255.224	192.168.1.225
Customer	网卡	192.168.1.2	225.255.255.128	192.168.1.1
Register	网卡	192.168.1.130	225.255.255.192	192.168.1.129
Laser	网卡	192.168.1.190	225.255.255.192	192.168.1.129
Web Server	网卡	209.165.201.2	255.255.255.252	209.165.201.1

## 学习目标

- 配置静态路由和默认路由
- 添加并连接路由器
- 设计一个编址方案并记录下来
- 添加并连接位于一个地址空间中的设备
- 配置设备的基本设置
- 使用 CHAP 配置 PPP 封装
- 配置 OSPF 路由
- 配置 VLAN
- 检验连通性

### 任务 1: 配置静态路由和默认路由

#### 步骤 1. 配置从 ISP 到 CENTRAL 的静态路由。

使用口令 **cisco** 和 **class** 访问路由器 CLI 的执行模式。在 ISP 上使用通向下述网络的送出接口参数配置两条静态路由：

- 10.1.1.0/30
- 192.168.1.0/24

#### 步骤 2. 配置从 CENTRAL 到 ISP 的默认路由。

在 CENTRAL 上使用送出接口参数配置默认路由，将所有默认流量发送到 ISP。

#### 步骤 3. 测试与 Web 服务器的连通性。

CENTRAL 应该能成功 ping 通 Web 服务器 (209.165.201.2)

#### 步骤 4. 检查结果。

完成比例应为 4%。如果并非如此，请单击 **Check Results** (检查结果) 查看尚未完成哪些必要部分。

### 任务 2: 添加并连接路由器

#### 步骤 1. 添加 BRANCH 路由器。

单击 Custom Made Devices (定制设备)，然后将一台 1841 路由器添加到拓扑中。使用 Config (配置) 选项卡，将 Display Name (显示名称) 改为 BRANCH。显示名称区分大小写。目前不要更改主机名。

#### 步骤 2. 将 BRANCH 连接到 CENTRAL。

根据拓扑中显示的接口，选择正确的电缆将 BRANCH 连接到 CENTRAL。

#### 步骤 3. 检查结果。

完成比例应为 9%。如果并非如此，请单击 **Check Results** (检查结果) 查看尚未完成哪些必要部分。如果在步骤 2 中更改了主机名，则完成比例会更高。

### 任务 3: 设计一个编址方案并记录下来

#### 步骤 1. 设计编址方案。

根据拓扑和下列要求设计一个编址方案:

- 所有 WAN 链路使用规定的地址。
- 连接到 **BRANCH** 的 VLAN 使用地址空间 192.168.1.0/24。从需要主机数量最多的 VLAN 开始, 按下列顺序为所有 VLAN 分配子网。
  - VLAN 15 需要可容纳 100 台主机的空间 \_\_\_\_\_ 192.168.1.0/25
  - VLAN 25 需要可容纳 50 台主机的空间 \_\_\_\_\_ 192.168.1.128/26
  - VLAN 1 需要可容纳 20 台主机的空间 \_\_\_\_\_ 192.168.1.192/27
  - VLAN 99 需要可容纳 20 台主机的空间 \_\_\_\_\_ 192.168.1.224/27

#### 步骤 2. 记录编址方案。

- 根据以下说明完成地址表。下一个任务将添加其余设备。
  - 将每个 VLAN 中的第一个地址分配给相应的 **BRANCH** 子接口。子接口编号与 VLAN 编号匹配。
  - 将 VLAN 99 中的第二个地址分配给 **S1**。
  - 将 VLAN 15 中的第二个地址分配给 **Customer PC**。
  - 将 VLAN 25 中的第二个地址分配给 **Register PC**。
  - 将 VLAN 25 中的最后一个地址分配给激光打印机。
- 请务必记录下每个地址的相应子网掩码和默认网关。

### 任务 4: 添加并连接地址空间中的设备

#### 步骤 1. 添加 192.168.1.0/24 地址空间中的 **S1**、**Customer PC**、**Register PC** 和激光打印机。

- **S1** 是 2960 交换机。请将一台 2960 交换机添加到拓扑中并将显示名称改为 **S1**。显示名称区分大小写。目前不要更改主机名。
- **PC** 和打印机列于 **End Devices** (终端设备) 中。添加两台 **PC** 和一台打印机。按照拓扑图更改 **PC** 和打印机的显示名称。

#### 步骤 2. 将 **S1** 连接到 **BRANCH**。

根据拓扑中显示的接口, 选择正确的电缆将 **S1** 连接到 **BRANCH**。

#### 步骤 3. 将 **Customer PC**、**Register PC** 和激光打印机连接到 **S1**。

根据拓扑中显示的接口, 选择正确的电缆将 **PC** 和打印机连接到 **S1**。

#### 步骤 4. 检查结果。

完成比例应为 22%。如果并非如此, 请单击 **Check Results** (检查结果) 查看尚未完成哪些必要部分。如果在步骤 1 中更改了 **S1** 的主机名, 则完成比例会更高。

## 任务 5: 配置设备的基本设置

### 步骤 1. 配置 BRANCH 和 S1。

根据您的记录设置 BRANCH 和 S1 的基本配置，包括地址。使用 **cisco** 作为线路口令，并使用 **class** 作为加密口令。使用 64000 作为时钟频率。基本配置中予以评分的部分包括：

- 主机名，区分大小写。
- 为接口分配地址并激活接口。时钟频率设置为 64000 bps。
- 对于接口 Fa0/0.99，将 VLAN 99 配置为本征 VLAN。
- 在 S1 上创建 VLAN 99 并为其分配地址。在本练习稍后配置了中继之后再激活 VLAN 99。

### 步骤 2. 配置其余设备。

根据您的记录，用正确的地址配置 PC 和打印机。

### 步骤 3. 测试 BRANCH 和 CENTRAL 之间的连通性。

CENTRAL 此时应该能成功 ping 通 BRANCH。S1 在配置中继前无法 ping 通。

### 步骤 4. 检查结果。

完成比例应为 63%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 6: 使用 CHAP 身份验证配置 PPP 封装

### 步骤 1. 配置 CENTRAL，使其通向 BRANCH 的链路使用 PPP 封装并采用 CHAP 身份验证。

CHAP 身份验证的口令是 **cisco123**。链路将断开。

### 步骤 2. 配置 BRANCH，使其通向 CENTRAL 的链路使用 PPP 封装并采用 CHAP 身份验证。

CHAP 身份验证的口令是 **cisco123**。链路将恢复。

### 步骤 3. 测试 BRANCH 和 CENTRAL 之间的连通性。

Packet Tracer 重新打开接口所需的时间可能比实际设备稍长。一旦接口打开，CENTRAL 应该能成功 ping 通 BRANCH。

### 步骤 4. 检查结果。

完成比例应为 71%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 7: 配置 OSPF 路由

### 步骤 1. 在 CENTRAL 上配置 OSPF。

- 使用进程 ID 1 配置 OSPF。
- 仅添加与 BRANCH 共享的网络。
- 向 OSPF 相邻设备传播默认路由。
- 在接入 ISP 的接口上禁用 OSPF 更新。



## 步骤 2. 在 BRANCH 上配置 OSPF。

- 使用进程 ID 1 配置 OSPF。
- 添加通过 BRANCH 路由的所有活动网络。
- 在接入 VLAN 的接口上禁用 OSPF 更新。

## 步骤 3. 测试与 Web 服务器的连通性。

BRANCH 现在应能成功 ping 通 Web 服务器 (209.165.201.2)。

## 步骤 4. 检查结果。

完成比例应为 86%。如果并非如此，请单击 **Check Results** (检查结果) 查看尚未完成哪些必要部分。

## 任务 8: 配置 VLAN

### 步骤 1. 为 S1 添加 VLAN。

VLAN 名称区分大小写。根据以下规定添加四个 VLAN 并为其命名：

- VLAN 15; 名称为 **Customers** (默认)
- VLAN 25; 名称为 **Employee**
- VLAN 99; 名称为 **Management** (本征)

### 步骤 2. 将端口分配到相应的 VLAN 并激活接口 VLAN 99。

- 根据拓扑图中显示的“VLAN 端口分配”，配置连接到终端设备的接入端口并将每个端口分配到正确的 VLAN。
- 对 Fa0/1 端口启用中继并将其配置为使用 VLAN 99 作为本征 VLAN。
- 根据需要激活接口 VLAN 99。它应该已经启用。

### 步骤 3. 检查结果。

完成比例应为 100%。如果并非如此，请单击 **Check Results** (检查结果) 查看尚未完成哪些必要部分。

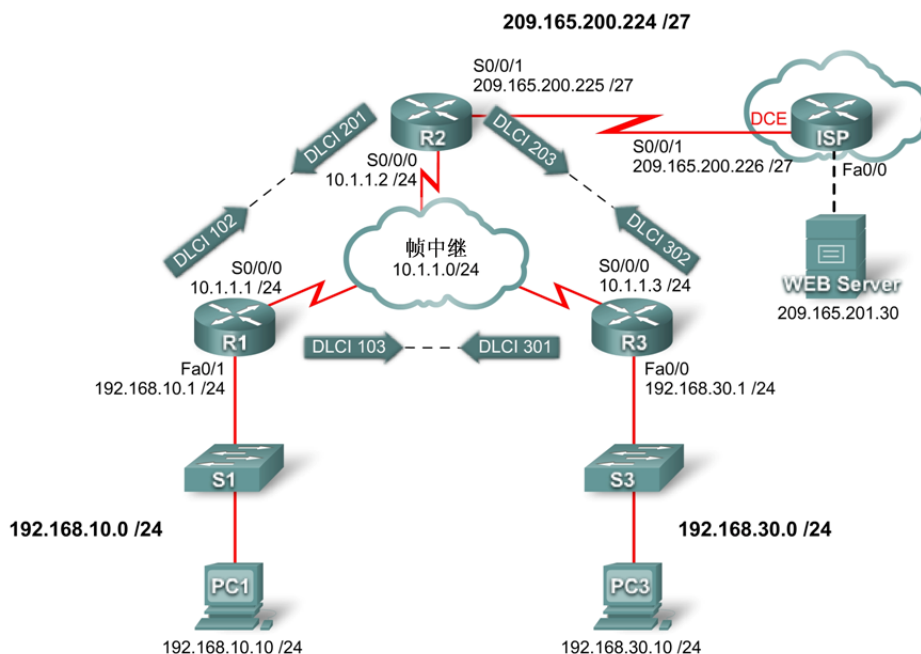
## 任务 9: 检验连通性

### 步骤 1. 检查 Customer PC、Register PC 和激光打印机能否彼此 ping 通。

### 步骤 2. 检查 Customer PC、Register PC 和激光打印机能否 ping 通 Web 服务器。

## PT 练习 3.2.2：使用静态映射配置基本帧中继（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/0	192.168.10.1	255.255.255.0
	S0/0/1	10.10.10.1	255.255.255.0
R2	S0/0/0	10.10.10.2	255.255.255.0
	S0/0/1	209.165.200.225	255.255.255.224
R3	Fa0/0	192.168.30.1	255.255.255.0
	S0/0/0	10.10.10.3	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.224

### 学习目标

- 配置帧中继
- 配置静态帧中继映射
- 配置帧中继 LMI 类型

## 简介

在本练习中，您将在路由器 R1、R2 和 R3 的 Serial 0/0/0 接口上配置帧中继。此外，您还将在每台路由器上配置两个帧中继静态映射以便访问其它两台路由器。尽管路由器可以自动感知 LMI 类型，但您仍将手动配置 LMI 来静态指定 LMI 类型。

路由器 R1、R2 和 R3 已经预先配置了主机名和所有接口的 IP 地址。路由器 R1 和 R3 的快速以太网接口处于活动状态，R2 的 S0/0/1 接口处于活动状态。

## 任务 1: 配置帧中继

**步骤 1. 在 R1 的 Serial 0/0/0 接口上配置帧中继封装。**

```
R1(config)#interface serial0/0/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#no shutdown
```

**步骤 2. 在 R2 和 R3 的 Serial 0/0/0 接口上配置帧中继封装。**

**步骤 3. 测试连通性。**

在 PC1 的命令行中，使用 **ping** 命令检验与 PC3 主机（地址为 192.168.30.10）的连通性。

由于 R1 路由器不知道 192.168.30.0 网络在哪里，因此从 PC1 ping PC3 应该失败。R1 必须配置有帧中继映射才能找到连接该网络的下一跳目的地址。

**步骤 4. 检查结果。**

完成百分比应当为 40%。如果不是，请单击 **Check Results（检查结果）** 查看哪些需要的组件尚未完成。

## 任务 2: 配置静态帧中继映射

注：Packet Tracer 不对 map 语句评分，但您仍然必须配置这些命令。

**步骤 1. 在 R1、R2 和 R3 上配置静态映射。**

每台路由器需要两个静态映射来访问另两台路由器。用于访问这些路由器的 DLCI 如下：

路由器 R1:

- 要访问路由器 R2，应使用位于 IP 地址 10.10.10.2 的 DLCI 102。
- 要访问路由器 R3，应使用位于 IP 地址 10.10.10.3 的 DLCI 103。

路由器 R2:

- 要访问路由器 R1，应使用位于 IP 地址 10.10.10.1 的 DLCI 201。
- 要访问路由器 R3，应使用位于 IP 地址 10.10.10.3 的 DLCI 203。

路由器 R3:

- 要访问路由器 R1，应使用位于 IP 地址 10.10.10.1 的 DLCI 301。
- 要访问路由器 R2，应使用位于 IP 地址 10.10.10.2 的 DLCI 302。

路由器还必须支持 RIP；因此需要使用关键字 **broadcast**。

在路由器 R1 上，如下配置静态帧中继映射：

```
R1(config-if)#frame-relay map ip 10.10.10.2 102 broadcast  
R1(config-if)#frame-relay map ip 10.10.10.3 103 broadcast
```

使用上面提供的信息配置路由器 R2 和 R3。

## 步骤 2. 检查结果。

完成百分比应当为 80%。如果不是，请单击 **Check Results**（检查结果）查看哪些需要的组件尚未完成。

## 任务 3：配置帧中继 LMI 类型

帧中继网云中包含 LMI 类型为 ANSI 的交换机。因此，必须将所有帧中继链路都手工配置为使用 ANSI。

### 步骤 1. 将 ANSI 配置为 R1、R2 和 R3 上的 LMI 类型。

对每台路由器的串行接口输入下列命令。

```
R1(config-if)#interface s0/0/0  
R1(config-if)#frame-relay lmi-type ansi
```

### 步骤 2. 检查结果。

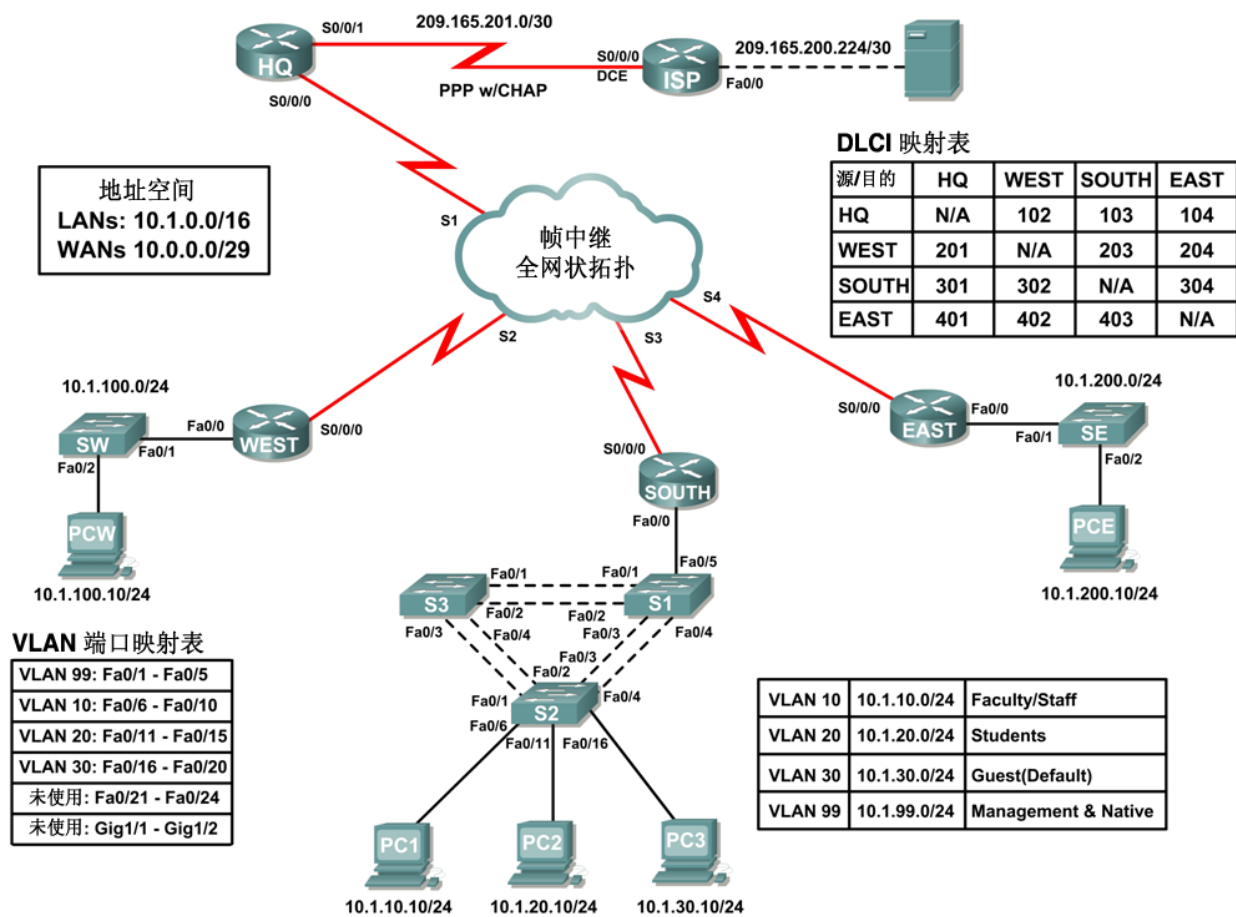
完成百分比应当为 100%。如果不是，请单击 **Check Results**（检查结果）查看哪些需要的组件尚未完成。

### 步骤 3. 测试连通性。

在练习完成比例为 100% 的情况下，仍有可能无法连通。PC1 和 PC3 现在应能成功 ping 通彼此，也能 ping 通 Web Server。若非如此，请检查您输入的所有命令是否与上述步骤中指定的命令完全相同。

## PT 练习 3.6.1: Packet Tracer 综合技能练习 (教师版)

### 拓扑图



## 地址表

设备	接口	IP 地址	子网掩码
HQ	S0/0/1	209.165.201.2	255.255.255.252
	S0/0/0	10.0.0.1	255.255.255.248
WEST	S0/0/0	10.0.0.2	255.255.255.248
	Fa0/0	10.1.100.1	255.255.255.0
SOUTH	S0/0/0	10.0.0.3	255.255.255.248
	Fa0/0.10	10.1.10.1	255.255.255.0
	Fa0/0.20	10.1.20.1	255.255.255.0
	Fa0/0.30	10.1.30.1	255.255.255.0
	Fa0/0.99	10.1.99.1	255.255.255.0
EAST	S0/0/0	10.0.0.4	255.255.255.248
	Fa0/0	10.1.200.1	255.255.255.0
ISP	S0/0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.200.225	255.255.255.252
Web Server	网卡	209.165.200.226	255.255.255.252
S1	VLAN99	10.1.99.11	255.255.255.0
S2	VLAN99	10.1.99.12	255.255.255.0
S3	VLAN99	10.1.99.13	255.255.255.0

## 学习目标

- 配置采用 CHAP 的 PPP
- 配置全网状帧中继
- 配置静态路由和默认路由
- 配置并测试 VLAN 间路由
- 在交换机上配置 VTP 和中继
- 在交换机上配置 VLAN
- 配置并检验接口 VLAN 99
- 将交换机配置为所有生成树的根桥
- 将端口分配给 VLAN
- 测试端到端连通性

## 简介

通过本练习，您可以演练各种技能，包括配置帧中继、采用 CHAP 的 PPP、静态路由和默认路由、VTP 和 VLAN。由于本练习中包含将近 150 个评分项目，因此，并非每次配置完一个参与评分的命令之后，您都会看到完成百分比会增加。本练习中，随时都可单击 **Check Results（检查结果）** 和 **Assessment Items（考试试题）** 来查看您是否输入正确的评分命令。

## 任务 1：配置在设备间采用 CHAP 身份验证的 PPP

步骤 1. 在 HQ 上配置并激活 Serial 0/0/1。

步骤 2. 在 HQ 上为其与 ISP 之间共享的链路配置 PPP 封装。

步骤 3. 在 HQ 上配置 CHAP 身份验证。

使用 **cisco** 作为口令。

步骤 4. 检验 HQ 和 ISP 之间的连通性。

现在，HQ 和 ISP 之间的链路应该处于工作状态，因此您应该能 ping 通 ISP。不过在 Packet Tracer 中，链路进入工作状态可能需要几分钟。要加速这一过程，请在 Simulation（模拟）模式和 Realtime（实时）模式之间切换三四次。

步骤 5. 检查结果。

完成百分比应当为 4%。如果不是，请单击 **Check Results**（检查结果）查看哪些需要的组件尚未完成。

## 任务 2：配置全网状帧中继

上面的拓扑图和下表都显示了此全网状帧中继配置中使用的 DLCI 映射。请从左至右阅读下表。例如，在 HQ 上配置的 DLCI 映射应为：102 映射到 WEST；103 映射到 SOUTH；104 映射到 EAST。

DLCI 映射				
从/到	HQ	WEST	SOUTH	EAST
HQ	不适用	102	103	104
WEST	201	不适用	203	204
SOUTH	301	302	不适用	304
EAST	401	402	403	不适用

注：HQ、WEST 和 SOUTH 均使用默认的帧中继封装 **cisco**。但 EAST 使用的封装类型是 IETF。

步骤 1. 在 HQ 上配置并激活 Serial 0/0/0 接口。

使用以下信息配置该接口：

- IP 地址
- 帧中继封装
- 到 WEST、SOUTH 和 EAST 的映射（EAST 使用 IETF 封装）
- LMI 类型为 ANSI

步骤 2. 在 WEST 上配置并激活 Serial 0/0/0 接口。

使用以下信息配置该接口：

- IP 地址
- 帧中继封装
- 到 HQ、SOUTH 和 EAST 的映射（EAST 使用 IETF 封装）
- LMI 类型为 ANSI

### 步骤 3. 在 SOUTH 上配置并激活 Serial 0/0/0 接口。

使用以下信息配置该接口：

- IP 地址
- 帧中继封装
- 到 HQ、WEST 和 EAST 的映射（EAST 使用 IETF 封装）
- LMI 类型为 ANSI

### 步骤 4. 在 EAST 上配置并激活 Serial 0/0/0 接口。

使用以下信息配置该接口：

- IP 地址
- 帧中继封装使用 IETF
- 到 HQ、WEST 和 SOUTH 的映射
- LMI 类型为 ANSI

注：Packet Tracer 不对 map 语句评分，但您仍然必须配置这些命令。现在，帧中继路由器之间应该完全连通。

### 步骤 5. 检验帧中继路由器之间的连通性。

HQ 上的映射应类似下例。请确保所有路由器的映射完整。

```
Serial0/0/0 (up): ip 10.0.0.2 dlci 102, static, broadcast, CISCO, status  
defined, active  
Serial0/0/0 (up): ip 10.0.0.3 dlci 103, static, broadcast, CISCO, status  
defined, active  
Serial0/0/0 (up): ip 10.0.0.4 dlci 104, static, broadcast, IETF, status  
defined, active
```

检查 HQ、WEST、SOUTH 和 EAST 现在能否 ping 通彼此。

### 步骤 6. 检查结果。

完成百分比应当为 28%。如果不是，请单击 **Check Results**（检查结果）查看哪些需要的组件尚未完成。

## 任务 3：配置静态路由和默认路由

本拓扑中未使用任何路由协议。所有路由均通过静态路由和默认路由完成。

### 步骤 1. 在 HQ 上配置静态路由和默认路由。

- HQ 需要通往本拓扑中六个远程 LAN 的六条静态路由。请在静态路由配置中使用 *下一跳 ip 地址* 参数。
- HQ 还需要一条默认路由。请在默认路由配置中使用 *送出接口* 参数。

### 步骤 2. 在 WEST 上配置静态路由和默认路由。

- WEST 需要通往本拓扑中五个远程 LAN 的五条静态路由。请在静态路由配置中使用 *下一跳 ip 地址* 参数。
- WEST 还需要一条默认路由。请在默认路由配置中使用 *下一跳 ip 地址* 参数。



### 步骤 3. 在 SOUTH 上配置静态路由和默认路由。

- SOUTH 需要通往本拓扑中两个远程 LAN 的两条静态路由。请在静态路由配置中使用 *下一跳 ip 地址* 参数。
- SOUTH 还需要一条默认路由。请在默认路由配置中使用 *下一跳 ip 地址* 参数。

### 步骤 4. 在 EAST 上配置静态路由和默认路由。

- EAST 需要通往本拓扑中五个远程 LAN 的五条静态路由。请在静态路由配置中使用 *下一跳 ip 地址* 参数。
- EAST 还需要一条默认路由。请在默认路由配置中使用 *下一跳 ip 地址* 参数。

### 步骤 5. 检验从 EAST LAN 和 WEST LAN 到 Web Server 的连通性。

- 所有路由器现在均应能 ping 通 Web Server。
- WEST PC (PCW) 和 EAST PC (PCE) 现在应能 ping 通彼此，也能 ping 通 Web Server。

### 步骤 6. 检查结果。

完成百分比应当为 43%。如果不是，请单击 **Check Results（检查结果）** 查看哪些需要的组件尚未完成。

## 任务 4：配置并测试 VLAN 间路由

### 步骤 1. 在 SOUTH 上配置 VLAN 间路由。

根据地址表，在 SOUTH 上激活 FastEthernet 0/0 接口并配置 VLAN 间路由。子接口编号与 VLAN 编号对应。VLAN 99 为本征 VLAN。

### 步骤 2. 测试 SOUTH 上的 VLAN 间路由。

HQ、WEST 和 EAST 现在应能 ping 通 SOUTH 的每个子接口。

### 步骤 3. 检查结果。

完成百分比应当为 56%。如果不是，请单击 **Check Results（检查结果）** 查看哪些需要的组件尚未完成。路由器的配置现在已完整。

## 任务 5：在交换机上配置 VTP 和中继

### 步骤 1. 在 S1、S2 和 S3 上配置 VTP 设置。

- S1 是服务器。S2 和 S3 是客户端。
- 域名是 **CCNA**。
- 口令是 **cisco**。

### 步骤 2. 在 S1、S2 和 S3 上配置中继。

S1、S2 和 S3 的中继端口均为连接到其它交换机或路由器的端口。将所有中继端口设置为中继模式并将 VLAN 99 指定为本征 VLAN。

### 步骤 3. 检查结果。

完成百分比应当为 81%。如果不是，请单击 **Check Results（检查结果）** 查看哪些需要的组件尚未完成。

## 任务 6：在交换机上配置 VLAN

### 步骤 1. 创建并命名 VLAN。

仅在 S1 上创建以下 VLAN 并为其命名：

- VLAN 10, 名称 = **Faculty/Staff**
- VLAN 20, 名称 = **Students**
- VLAN 30, 名称 = **Guest(Default)**
- VLAN 99, 名称 = **Management&Native**

### 步骤 2. 检查这些 VLAN 是否已发送到 S2 和 S3。

什么命令会显示以下输出？ \_\_\_\_\_ **show vtp status**

```
VTP Version                : 2
Configuration Revision      : 8
Maximum VLANs supported locally : 64
Number of existing VLANs    : 9
VTP Operating Mode          : Client
VTP Domain Name             : CCNA
VTP Pruning Mode            : Disabled
VTP V2 Mode                 : Disabled
VTP Traps Generation        : Disabled
MD5 digest                  : 0xF5 0x50 0x30 0xB6 0x91 0x74 0x95 0xD9
Configuration last modified by 0.0.0.0 at 3-1-93 00:12:30
```

什么命令会显示以下输出？ \_\_\_\_\_ **show vlan brief**

VLAN	Name	Status	Ports
1	default	active	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 Gig1/1, Gig1/2
10	Faculty/Staff	active	
20	Students	active	
30	Guest(Default)	active	
99	Management&Native	active	

<省略部分输出>

### 步骤 3. 检查结果。

完成百分比应当为 84%。如果不是，请单击 **Check Results**（检查结果）查看哪些需要的组件尚未完成。

## 任务 7：配置并检验 VLAN 99

步骤 1. 在 S1、S2 和 S3 上完成下列步骤：

- 配置并激活 VLAN 99
- 配置默认网关
- 检查 S1、S2 和 S3 现在能否 ping 通 SOUTH 的 10.1.99.1 接口

步骤 2. 检查结果。

完成百分比应当为 92%。如果不是，请单击 **Check Results**（检查结果）查看哪些需要的组件尚未完成。

## 任务 8：将 S1 配置为所有生成树的根桥

步骤 1. 将 S1 配置为所有生成树（包括 VLAN 1、VLAN 10、VLAN 20、VLAN 30 和 VLAN 99）的根桥。

请注意，S3 已在根桥选举中当选，目前是所有生成树的根桥。将 S1 在所有生成树中的优先级均设置为 4096。

步骤 2. 检查 S1 现在是否是所有生成树的根桥。

以下仅显示了 VLAN 1 的输出，但 S1 应该是所有生成树的根桥。什么命令会显示以下输出？

```
_____ show spanning-tree vlan 1
```

```
VLAN0001
Spanning tree enabled protocol ieee
Root ID    Priority    4097
           Address    00D0.BC79.4B57
           This bridge is the root
           Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID  Priority    4097 (priority 4096 sys-id-ext 1)
           Address    00D0.BC79.4B57
           Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/1	Desg	FWD	19	128.3	Shr
Fa0/2	Desg	FWD	19	128.3	Shr
Fa0/3	Desg	FWD	19	128.3	Shr
Fa0/4	Desg	FWD	19	128.3	Shr
Fa0/5	Desg	FWD	19	128.3	Shr

<省略部分输出>

步骤 3. 检查结果。

完成百分比应当为 96%。如果不是，请单击 **Check Results**（检查结果）查看哪些需要的组件尚未完成。

## 任务 9：将端口分配给 VLAN

### 步骤 1. 将 S2 的端口分配给 VLAN。

Packet Tracer 仅对连接到 PC1、PC2 和 PC3 的端口评分。

- 将端口配置为接入模式
- 将端口分配给相应 VLAN

VLAN 端口映射如下：

- VLAN 99: Fa0/1 – Fa0/5
- VLAN 10: Fa0/6 – Fa0/10
- VLAN 20: Fa0/11 – Fa0/15
- VLAN 30: Fa0/16 – Fa0/20
- 未使用: Fa0/21 – Fa0/24; Gig1/1; Gig1/2

出于安全考虑，应关闭未使用的端口。

### 步骤 2. 检查 VLAN 端口分配。

使用什么命令可获得显示 VLAN 分配的下列输出？

**show vlan brief**

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
10	Faculty/Staff	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
20	Students	active	Fa0/11, Fa0/12, Fa0/13, Fa0/14 Fa0/15
30	Guest(Default)	active	Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20
99	Management&Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

### 步骤 3. 检查结果。

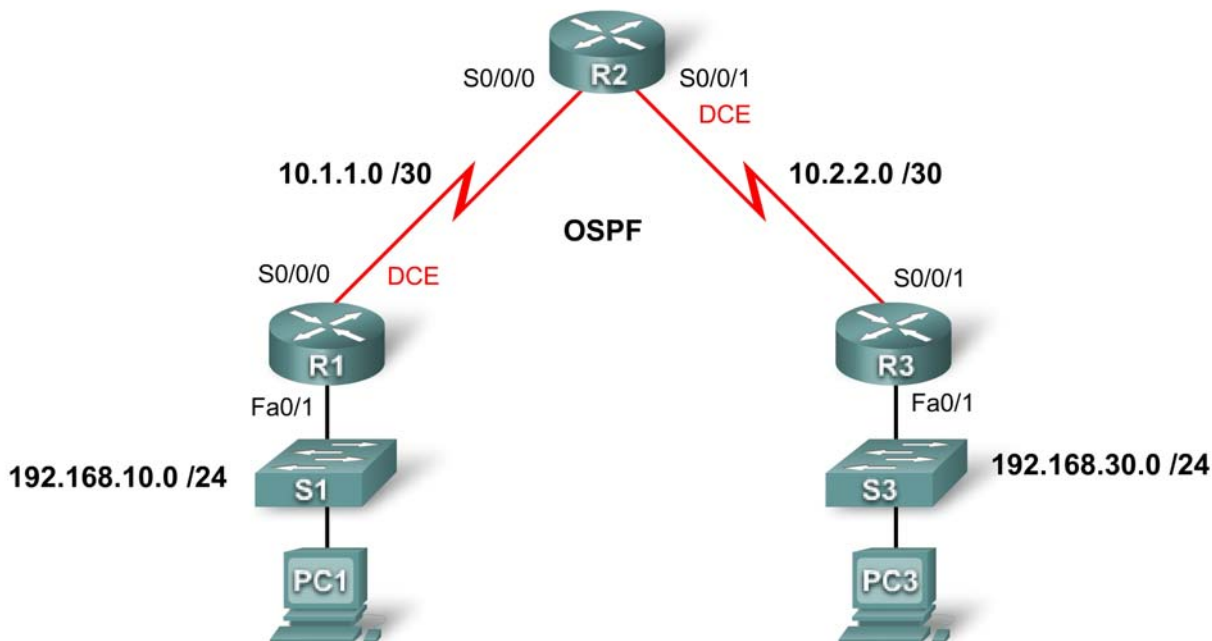
完成百分比应当为 100%。如果不是，请单击 **Check Results（检查结果）** 查看哪些需要的组件尚未完成。

## 任务 10：测试端到端连通性

虽然 Packet Tracer 可能需要一段时间才能收敛，但从 PC1、PC2 和 PC3 发出的 ping 命令最终应成功。请测试与 PCW、PCE 和 Web Server 之间的连通性。如果需要，可以通过切换 **Simulation（模拟）** 模式和 **Realtime（实时）** 模式来加快收敛。

## PT 练习 4.3.2: 配置 OSPF 身份验证 (教师版)

拓扑图



地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	网卡	192.168.10.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0

学习目标

- 配置 OSPF 简单身份验证
- 配置 OSPF MD5 身份验证
- 测试连通性

## 简介

本练习涵盖 OSPF 简单身份验证和 OSPF MD5（消息摘要 5）身份验证。您可以在 OSPF 中启用身份验证，以便通过安全方式交换路由更新信息。使用简单身份验证时，口令在网络中以明文方式发送。当区域内的设备不支持更安全的 MD5 身份验证时，则使用简单身份验证。如果使用 MD5 身份验证，则口令不会通过网络发送。MD5 被认为是最安全的 OSPF 身份验证模式。当配置身份验证时，您必须在整个区域中配置相同类型的身份验证。在本练习中，您将在 R1 和 R2 之间配置简单身份验证，在 R2 和 R3 之间配置 MD5 身份验证。

### 任务 1：配置 OSPF 简单身份验证

#### 步骤 1. 将 R1 配置为使用 OSPF 简单身份验证。

要在 R1 上启用简单身份验证，请在全局配置提示符下使用 **router ospf 1** 命令进入路由器配置模式。然后发出 **area 0 authentication** 命令以启用身份验证。

```
R1(config)#router ospf 1
R1(config-router)#area 0 authentication
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:02:30: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/0 from FULL to
Down: Interface down or detached
```

最后，您将看到一条说明 R1 与 R2 的相邻关系已解除的控制台消息。R1 路由表中的所有 OSPF 路由全都消失，直至它能够向 R2 验证路由。即使未配置口令，R1 仍会要求所有邻居在 OSPF 路由消息和更新中使用身份验证。

**area 0 authentication** 命令可对区域 0 中的所有接口启用身份验证。通常，在 R1 上只需使用该命令便可成功配置身份验证，因为 R1 无须支持任何其它类型的身份验证。

要为 R1 配置简单身份验证口令，请进入连接到 R2 的链路所对应的接口配置模式。然后发出 **ip ospf authentication-key cisco123** 命令。该命令将身份验证口令设置为 **cisco123**。

```
R1(config-router)#interface S0/0/0
R1(config-if)#ip ospf authentication-key cisco123
```

#### 步骤 2. 将 R2 配置为使用 OSPF 简单身份验证。

您已经在 R1 上为整个区域配置了身份验证。由于 R2 同时支持简单身份验证和 MD5 身份验证，因此应在接口级别输入命令。

进入接口 S0/0/0 的接口配置模式。利用 **ip ospf authentication** 命令指明您要使用简单身份验证。然后发出 **ip ospf authentication-key cisco123** 命令将身份验证口令设置为 **cisco123**。

```
R2(config)#interface S0/0/0
R2(config-if)#ip ospf authentication
R2(config-if)#ip ospf authentication-key cisco123
00:07:45: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.10.1 on Serial0/0/0 from
EXCHANGE to FULL, Exchange Done
```

完成上述配置任务之后，您应该会看到一条控制台消息，该消息表明 R1 与 R2 之间的相邻关系已重新建立。OSPF 路由重新加入路由表中。

#### 步骤 3. 检查结果。

完成比例应为 50%。如果不是，请单击 **Check Results（检查结果）**，了解哪些必需的组件尚未完成。

## 任务 2：配置 OSPF MD5 身份验证

### 步骤 1. 将 R3 配置为使用 OSPF MD5 身份验证。

要在 R3 上启用 MD5 身份验证，请在全局配置提示符下使用 **router ospf 1** 命令进入路由器配置模式。然后发出 **area 0 authentication message-digest** 命令以启用身份验证。

```
R3(config)#router ospf 1
R3(config-router)#area 0 authentication message-digest
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
DOWN, Neighbor Down: Dead timer expired
00:10:00: %OSPF-5-ADJCHG: Process 1, Nbr 10.2.2.1 on Serial0/0/1 from FULL to
Down: Interface down or detached
```

最后，您将看到一条说明与 R2 的相邻关系已解除的控制台消息。R3 路由表中的所有 OSPF 路由全都消失，直至它能够向 R2 验证路由。

要为 R3 配置 MD5 身份验证口令，请进入连接至 R2 的链路所对应的接口配置模式。然后发出 **ip ospf message-digest-key 1 md5 cisco123** 命令。该命令将 OSPF 身份验证口令设置为 **cisco123**，并使用 MD5 算法加以保护。

```
R3(config-router)#interface S0/0/1
R3(config-if)#ip ospf message-digest-key 1 md5 cisco123
```

### 步骤 2. 将 R2 配置为使用 OSPF MD5 身份验证。

在 R2 上，进入连接至 R3 的链路所对应的接口配置模式。发出 **ip ospf authentication message-digest** 命令以启用 MD5 身份验证。您需要在 R2 上执行该命令，因为该路由器同时使用两种类型的身份验证。

接下来，发出 **ip ospf message-digest-key 1 md5 cisco123** 命令设置身份验证口令。

```
R2(config)#interface S0/0/1
R2(config-if)#ip ospf authentication message-digest
R2(config-if)#ip ospf message-digest-key 1 md5 cisco123
00:13:51: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.30.1 on Serial0/0/1 from
EXCHANGE to FULL, Exchange Done
```

在输入该命令后，路由器需要经过一段时间才能收敛。在 R2 和 R3 上您都应该会看到一条控制台消息，该消息表明相邻关系已重新建立。您可以确认 R2 已重新添加该 OSPF 路由，并且 R3 是 R2 的 OSPF 邻居。

```
R2#show ip route
<省略部分输出>
```

```
Gateway of last resort is not set
```

```
    10.0.0.0/30 is subnetted, 2 subnets
C       10.1.1.0 is directly connected, Serial0/0/0
C       10.2.2.0 is directly connected, Serial0/0/1
O       192.168.10.0/24 [110/65] via 10.1.1.1, 00:06:13, Serial0/0/0
O       192.168.30.0/24 [110/65] via 10.2.2.2, 00:00:07, Serial0/0/1
```

```
R2#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.10.1	1	FULL/-	00:00:32	10.1.1.1	Serial0/0/0
192.168.30.1	1	FULL/-	00:00:37	10.2.2.2	Serial0/0/1

### 步骤 3. 检查结果。

完成比例应为 100%。如果不是，请单击 **Check Results**（检查结果），了解哪些必需的组件尚未完成。

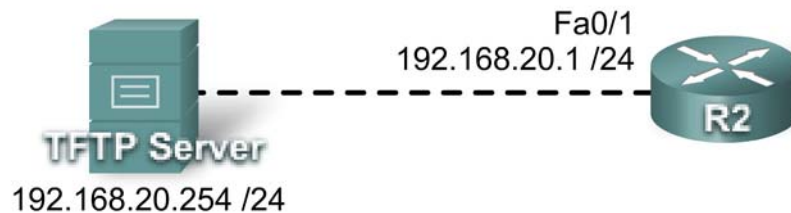
### 任务 3：测试连通性

现在，应该已在所有三台路由器上正确配置了身份验证，因此 PC1 应该能够 ping 通 PC3。单击 **Check Results**（检查结果），然后单击 **Connectivity Tests**（连通性测试）检查能否 ping 通。



## PT 练习 4.5.4: 使用 TFTP 服务器升级 Cisco IOS 映像 (教师版)

### 拓扑图



### 学习目标

- 检查当前的 Cisco IOS 映像
- 配置连接以访问 TFTP 服务器
- 上传新的 Cisco IOS 映像
- 配置 **boot system** 命令
- 测试新的 Cisco IOS 映像

### 简介

在本练习中，您将配置连接以访问 TFTP 服务器，并上传更新、更高级的 Cisco IOS 映像。虽然 Packet Tracer 会模拟在路由器上升级 Cisco IOS 映像，但是不会模拟将 Cisco IOS 映像备份到 TFTP 服务器中。此外，虽然您要升级到的映像更为高级，但 Packet Tracer 模拟过程不会通过启用更高级的命令来反映这一升级。既有的 Packet Tracer 命令集仍然有效。

### 任务 1: 检查当前的 Cisco IOS 映像

**步骤 1.** 使用 **show version** 命令检查 RAM 中当前所加载的映像版本。

```

R2#show version
Cisco IOS Software, 1841 Software (C1841-IPBASE-M), Version 12.3(14)T7,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 15-May-06 14:54 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-ipbase-mz.123-14.T7.bin"
<省略部分输出>
  
```

RAM 中当前所加载的映像不支持 SSH 及其它许多高级功能。

**步骤 2. 使用 `show flash` 命令检验闪存中当前是否有可用的映像。**

R2#**show flash**

```
System flash directory:
File Length Name/status
  1  13832032 c1841-ipbase-mz.123-14.T7.bin
[13832032 bytes used, 18682016 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)
```

只有一个 Cisco IOS 映像可用。您必须将映像升级至更高版本才能使用 SSH 和其它安全功能。

## 任务 2：配置连接以访问 TFTP 服务器

您需要建立连接，使 R2 连接到含有所需 Cisco IOS 映像的 TFTP 服务器。

**步骤 1. 连接 R2 和 TFTP 服务器。**

请参照拓扑图找到正确的接口。

**步骤 2. 配置 R2 的 IP 地址。**

请参照拓扑图获得正确的 IP 编址信息。

**步骤 3. 配置 TFTP 服务器的 IP 地址和默认网关。**

请参照拓扑图获得正确的 IP 编址信息。

**步骤 4. 测试连通性。**

R2 应该能成功 ping 通 TFTP 服务器。否则，请检查电缆连接和编址情况。

**步骤 5. 检查结果。**

完成比例应为 80%。如果不是，请单击 **Check Results**（检查结果），了解哪些必需的组件尚未完成。

## 任务 3：上传新的 Cisco IOS 映像

**步骤 1. 检查 TFTP 服务器上的 Cisco IOS 映像。**

单击 TFTP 服务器，然后单击 **Config**（配置）选项卡。您会注意到有多个可用的映像。您需要将映像 c1841-ipbasek9-mz.124-12.bin 上传到 R2。

**步骤 2. 将映像 c1841-ipbasek9-mz.124-12.bin 上传到 R2。**

- 在 R2 上，使用 **copy tftp flash** 命令开始上传过程。
- 输入 TFTP 服务器的 IP 地址。
- 输入该 Cisco IOS 映像的完整文件名。

```
R2#copy tftp flash
Address or name of remote host []? 192.168.20.254
Source filename []? c1841-ipbasek9-mz.124-12.bin
Destination filename [c1841-ipbasek9-mz.124-12.bin]? Enter
Accessing tftp://192.168.20.254/c1841-ipbasek9-mz.124-12.bin...
Loading c1841-ipbasek9-mz.124-12.bin from 192.168.20.254:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 16599160 bytes]

16599160 bytes copied in 13.047 secs (284682 bytes/sec)
R2#
```

步骤 3. 检验新的映像是否已在闪存中。

```
R2#show flash

System flash directory:
File Length Name/status
  1  13832032 c1841-ipbase-mz.123-14.T7.bin
  2  16599160 c1841-ipbasek9-mz.124-12.bin
[30431192 bytes used, 2082856 available, 32514048 total]
32768K bytes of processor board System flash (Read/Write)

R2#
```

步骤 4. 检查结果。

完成比例应为 90%。如果不是，请单击 **Check Results（检查结果）**，了解哪些必需的组件尚未完成。

#### 任务 4：配置 boot system 命令

默认情况下，路由器的启动序列会加载闪存中所列出的第一个 Cisco IOS 映像。保证路由器加载新映像的方法之一是配置 **boot system flash** 命令。在 R2 上，输入以下命令：

```
R2(config)#boot system flash c1841-ipbasek9-mz.124-12.bin
```

该命令现在属于运行配置的一部分。但是，必须将运行配置保存到 NVRAM 中；否则，下次重新启动路由器时该配置会被改写。

```
R2(config)#end
R2#copy running-config startup-config
```

完成比例应为 100%。如果不是，请单击 **Check Results（检查结果）**，了解哪些必需的组件尚未完成。

## 任务 5：测试新映像

重新加载 R2 并等它重新启动。路由器重新启动后，请使用 **show version** 命令检验新的映像是否已位于 RAM 中。

R2#**reload**

Proceed with reload? [confirm]**[Enter]**

%SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload Command.

<省略部分输出>

R2>**show version**

Cisco IOS Software, 1841 Software (C1841-IPBASEK9-M), Version 12.4(12),  
RELEASE SOFTWARE (fc1)

Technical Support: <http://www.cisco.com/techsupport>

Copyright (c) 1986-2006 by Cisco Systems, Inc.

Compiled Mon 15-May-06 14:54 by pt\_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

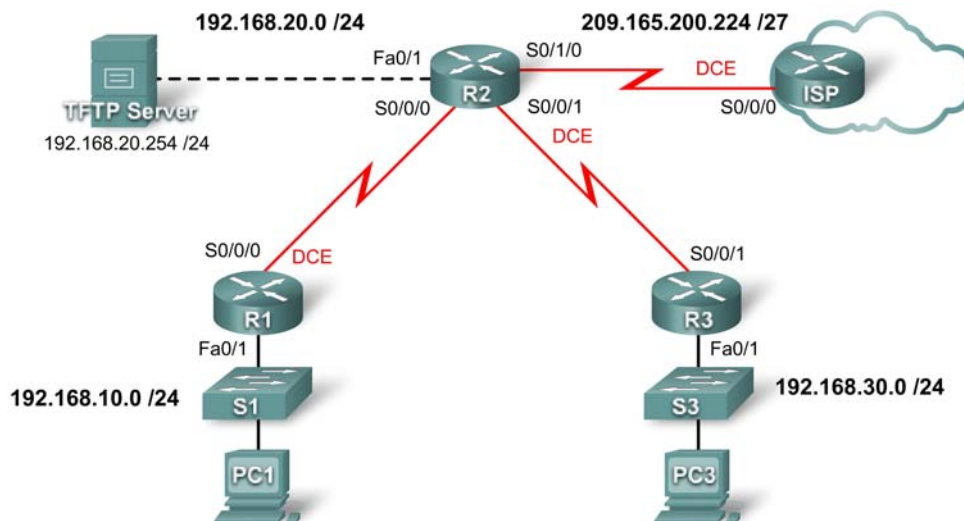
System returned to ROM by power-on

System image file is "flash:c1841-ipbasek9-mz.124-12.bin"

<省略部分输出>

## PT 练习 4.7.1: Packet Tracer 综合技能练习（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
ISP	S0/0/0	209.165.200.226	255.255.255.252
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/1	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.252
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
PC1	网卡	192.168.10.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0
TFTP Server	网卡	192.168.20.254	255.255.255.255

### 学习目标

- 配置路由
- 配置 OSPF 身份验证
- 升级 Cisco IOS 映像

## 简介

本练习总结性复习本章的内容，包括 OSPF 路由、身份验证以及 Cisco IOS 映像升级。

### 任务 1：配置路由

**步骤 1. 配置到达 ISP 的默认路由。**

在 R2 上，使用送出接口参数配置到达 ISP 的默认路由。

**步骤 2. 配置 R1、R2 和 R3 之间的 OSPF 路由。**

在所有三台服务器上配置 OSPF 路由。请使用进程 ID 1。在相应接口上禁用 OSPF 更新。

**步骤 3. 传播默认路由。**

**步骤 4. 检查结果。**

完成比例应为 59%。如果不是，请单击 **Check Results**（检查结果），了解哪些必需的组件尚未完成。

### 任务 2：配置 OSPF 身份验证

**步骤 1. 在 R1、R2 和 R3 之间配置 MD5 身份验证。**

使用 1 作为密钥值并使用 **cisco123** 作为口令，在 R1、R2 和 R3 之间配置 OSPF MD5 身份验证。

**步骤 2. 检查结果。**

完成比例应为 91%。如果不是，请单击 **Check Results**（检查结果），了解哪些必需的组件尚未完成。

### 任务 3：升级 Cisco IOS 映像

**步骤 1. 将更新版本的映像从 TFTP 服务器复制到 R2 上的闪存中。**

查看 TFTP 服务器的 Config（配置）选项卡，以确定更新版本的 Cisco IOS 映像的名称。然后将更新版本的映像复制到 R2 上的闪存中。

**步骤 2. 配置 R2 使其在启动时加载新的映像。**

**步骤 3. 保存配置并重新启动。**

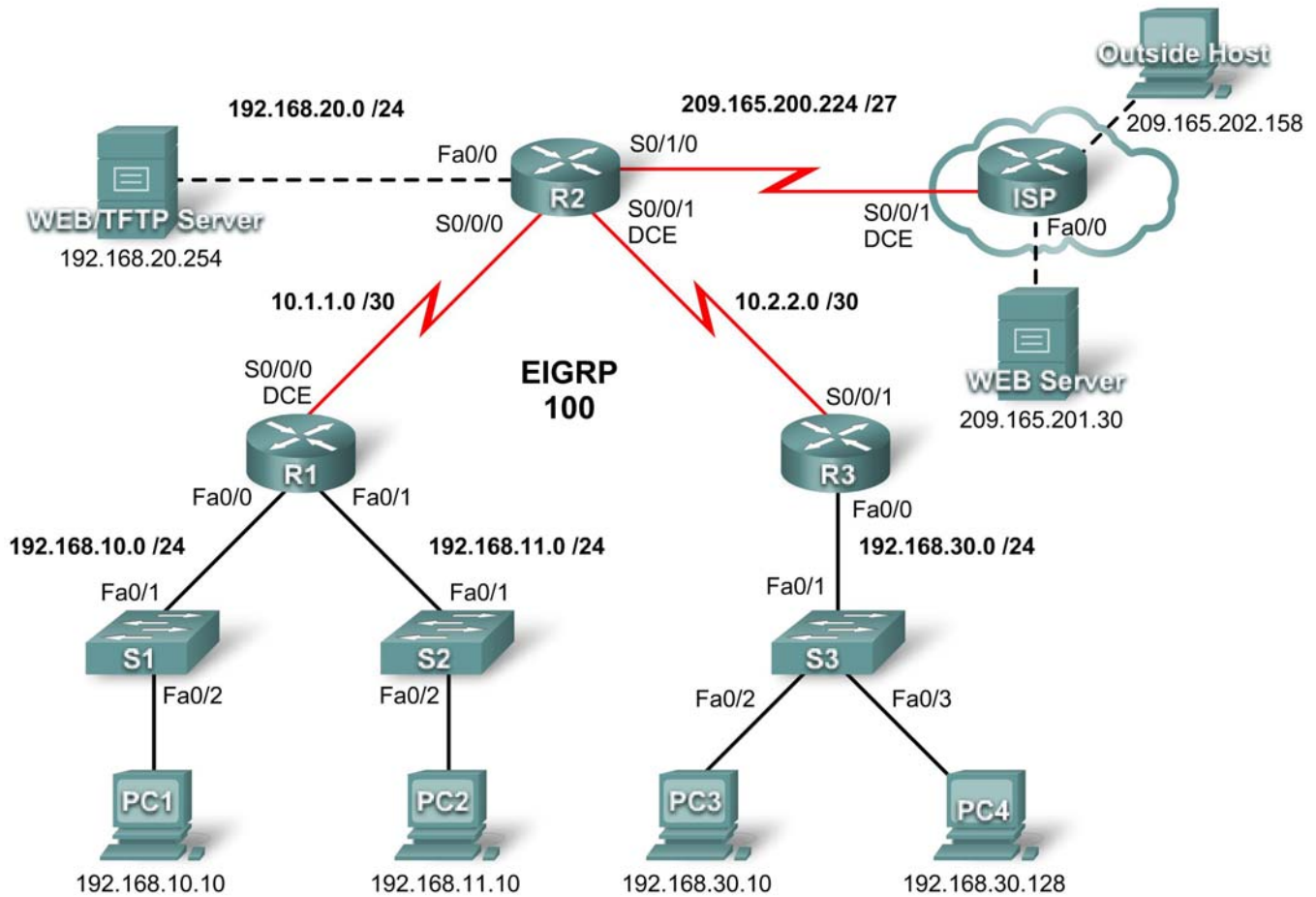
检验新的映像是否已加载到 RAM 中。

**步骤 4. 检查结果。**

完成比例应为 100%。如果不是，请单击 **Check Results**（检查结果），了解哪些必需的组件尚未完成。

## PT 练习 5.2.8: 配置标准 ACL (教师版)

拓扑图



## 地址表

设备	接口	IP 地址	子网掩码
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	S0/0/1	10.2.2.2	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	网卡	192.168.10.10	255.255.255.0
PC2	网卡	192.168.11.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0
PC4	网卡	192.168.30.128	255.255.255.0
WEB/TFTP Server	网卡	192.168.20.254	255.255.255.0
WEB Server	网卡	209.165.201.30	255.255.255.224
Outside Host	网卡	209.165.202.158	255.255.255.224

## 学习目标

- 检查当前的网络配置
- 评估网络策略并规划 ACL 实施
- 配置采用数字编号的标准 ACL
- 配置命名标准 ACL

## 简介

标准 ACL 是一种路由器配置脚本，根据源地址来控制路由器应该允许还是应该拒绝数据包。本练习的主要内容是定义过滤标准、配置标准 ACL、将 ACL 应用于路由器接口并检验和测试 ACL 实施。路由器已经过配置，包括 IP 地址和 EIGRP 路由。用户执行口令是 **cisco**，特权执行口令是 **class**。



## 任务 1: 检查当前的网络配置

### 步骤 1. 查看路由器的运行配置。

逐一在三台路由器的特权执行模式下使用 **show running-config** 命令查看运行配置。请注意，接口和路由已配置完整。将 IP 地址配置与上面的地址表相比较。此时，路由器上应该尚未配置任何 ACL。

本练习不需要配置 ISP 路由器。假设 ISP 路由器不属于您的管理范畴，而是由 ISP 管理员配置和维护。

### 步骤 2. 确认所有设备均可访问所有其它位置。

将任何 ACL 应用于网络中之前，都必须确认网络完全连通。如果应用 ACL 之前不测试网络连通性，排查故障可能会更加困难。

有助于连通性测试的一个步骤是查看每台设备上的路由表，确保列出了每个网络。在 R1、R2 和 R3 上发出 **show ip route** 命令。输出应该显示，每台设备都有路由通往其连接的网络，并且有到所有其它远程网络的动态路由。所有设备均可访问所有其它位置。

虽然路由表有助于评估网络状态，但仍应使用 **ping** 命令测试连通性。完成以下测试：

- 从 PC1 ping PC2。
- 从 PC2 ping Outside Host。
- 从 PC4 ping Web/TFTP Server。

这些连通性测试都应该成功。

## 任务 2: 评估网络策略并规划 ACL 实施

### 步骤 1. 评估 R1 LAN 的策略。

- 允许 192.168.10.0/24 网络访问除 192.168.11.0/24 网络外的所有位置。
- 允许 192.168.11.0/24 网络访问所有目的地址，连接到 ISP 的所有网络除外。

### 步骤 2. 为 R1 LAN 规划 ACL 实施。

- 用两个 ACL 可完全实施 R1 LAN 的安全策略。
- 在 R1 上配置第一个 ACL，拒绝从 192.168.10.0/24 网络发往 192.168.11.0/24 网络的流量，但允许所有其它流量。
- 此 ACL 应用于 Fa0/1 接口的出站流量，监控发往 192.168.11.0 网络的所有流量。
- 在 R2 上配置第二个 ACL，拒绝 192.168.11.0/24 网络访问 ISP，但允许所有其它流量。
- 控制 S0/1/0 接口的出站流量。
- ACL 语句的顺序应该从最具体到最概括。拒绝网络流量访问其它网络的语句应在允许所有其它流量的语句之前。

### 步骤 3. 评估 R3 LAN 的策略。

- 允许 192.168.30.0/10 网络访问所有目的地址。
- 拒绝主机 192.168.30.128 访问 LAN 以外的地址。

#### 步骤 4. 为 R3 LAN 规划 ACL 实施。

- 一个 ACL 即可完全实施 R3 LAN 的安全策略。
- 在 R3 上配置该 ACL，拒绝主机访问 LAN 以外的地址，但允许 LAN 中的所有其它主机发出的流量。
- 此 ACL 将应用于 Fa0/0 接口的入站流量，监控尝试离开 192.168.30.0/10 网络的所有流量。
- ACL 语句的顺序应该从最具体到最概括。拒绝 192.168.30.128 主机访问的语句应在允许所有其它流量的语句之前。

### 任务 3: 配置采用数字编号的标准 ACL

#### 步骤 1. 确定通配符掩码。

ACL 语句中的通配符掩码用于确定要检查的 IP 源地址或 IP 目的地址的数量。若某个位为 0，则表示匹配地址中该位的值，若为 1 则忽略地址中该位的值。请记住，标准 ACL 仅检查源地址。

- 由于 R1 上的 ACL 拒绝所有 192.168.10.0/24 的网络流量，因此以 192.168.10 开头的任何源 IP 地址都应拒绝。鉴于 IP 地址的最后一组二进制八位数可以忽略，所以正确的通配符掩码应为 0.0.0.255。此掩码中的每组二进制八位数可以理解为“检查、检查、检查、忽略”。
- R2 上的 ACL 还要拒绝 192.168.11.0/24 网络流量。可以使用同样的通配符掩码 0.0.0.255。

#### 步骤 2. 确定语句。

- 应在全局配置模式下配置 ACL。
- 标准 ACL 使用介于 1 和 99 之间的编号。R1 上的此列表使用编号 10，有助于记住此 ACL 监控的是 192.168.10.0 网络。
- 在 R2 上，访问列表 11 将拒绝从 192.168.11.0 网络发往任何 ISP 网络的流量，因此使用网络 192.168.11.0 和通配符掩码 0.0.0.255 设置 deny 选项。
- 由于 ACL 末尾有隐式“deny any”语句，因此必须用 permit 选项允许所有其它流量。any 选项用于指定任何源主机。

在 R1 上执行下列配置：

```
R1(config)#access-list 10 deny 192.168.10.0 0.0.0.255
R1(config)#access-list 10 permit any
```

注：ACL 配置只有按正确顺序输入所有语句后，才会获得 Packet Tracer 的评分。

现在，请在 R2 上创建拒绝 192.168.11.0 网络并允许所有其它网络的 ACL。此 ACL 使用编号 11。在 R2 上执行下列配置：

```
R2(config)#access-list 11 deny 192.168.11.0 0.0.0.255
R2(config)#access-list 11 permit any
```

#### 步骤 3. 将语句应用到接口。

在 R1 上，进入 Fa0/1 接口的配置模式。

发出 ip access-group 10 out 命令，将标准 ACL 应用于该接口的出站流量。

```
R1(config)#interface fa0/1
R1(config-if)#ip access-group 10 out
```

在 R2 上, 进入 S0/1/0 接口的配置模式。

发出 **ip access-group 11 out** 命令, 将标准 ACL 应用于该接口的出站流量。

```
R2(config)#interface s0/1/0
R2(config-if)#ip access-group 11 out
```

#### 步骤 4. 检验和测试 ACL。

配置并应用 ACL 后, PC1 (192.168.10.10) 应该无法 ping 通 PC2 (192.168.11.10), 因为 ACL 10 在 R1 上应用于 Fa0/1 的出站流量。

PC2 (192.168.11.10) 应该无法 ping 通 Web Server (209.165.201.30) 或 Outside Host (209.165.202.158), 但应能 ping 通其它所有位置, 因为 ACL 11 在 R2 上应用于 S0/1/0 的出站流量。但 PC2 无法 ping 通 PC1, 因为 R1 上的 ACL 10 会阻止 PC1 向 PC2 发送的应答。

#### 步骤 5. 检查结果。

完成比例应为 67%。如果并非如此, 请单击 **Check Results (检查结果)** 查看尚未完成哪些必要部分。

### 任务 4: 配置命名标准 ACL

#### 步骤 1. 确定通配符掩码。

- R3 的访问策略规定, 应该拒绝 192.168.30.128 主机访问本地 LAN 以外的任何地址。允许 192.168.30.0 网络中的所有其它主机访问所有其它位置。
- 要检查一台主机, 就需要检查完整的 IP 地址, 可使用关键字 **host** 来实现。
- 不匹配 **host** 语句的所有数据包都应允许。

#### 步骤 2. 确定语句。

- 在 R3 上进入全局配置模式。
- 发出 **ip access-list standard NO\_ACCESS** 命令, 创建名为 NO\_ACCESS 的命名 ACL。您将进入 ACL 配置模式。所有 **permit** 和 **deny** 语句都在此配置模式下配置。
- 使用 **host** 选项拒绝来自 192.168.30.128 主机的流量。
- 使用 **permit any** 允许所有其它流量。

在 R3 上配置以下命名 ACL:

```
R3(config)#ip access-list standard NO_ACCESS
R3(config-std-nacl)#deny host 192.168.30.128
R3(config-std-nacl)#permit any
```

#### 步骤 3. 将语句应用到正确的接口。

在 R3 上, 进入 Fa0/0 接口的配置模式。

发出 **ip access-group NO\_ACCESS in** 命令, 将命名 ACL 应用于该接口的入站流量。应用之后, 即会根据该 ACL 检查从 192.168.30.0/24 LAN 进入 Fa0/0 接口的所有流量。

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group NO_ACCESS in
```

#### 步骤 4. 检验和测试 ACL。

单击 **Check Results**（检查结果），然后单击 **Connectivity Tests**（连通性测试）。以下测试会失败。

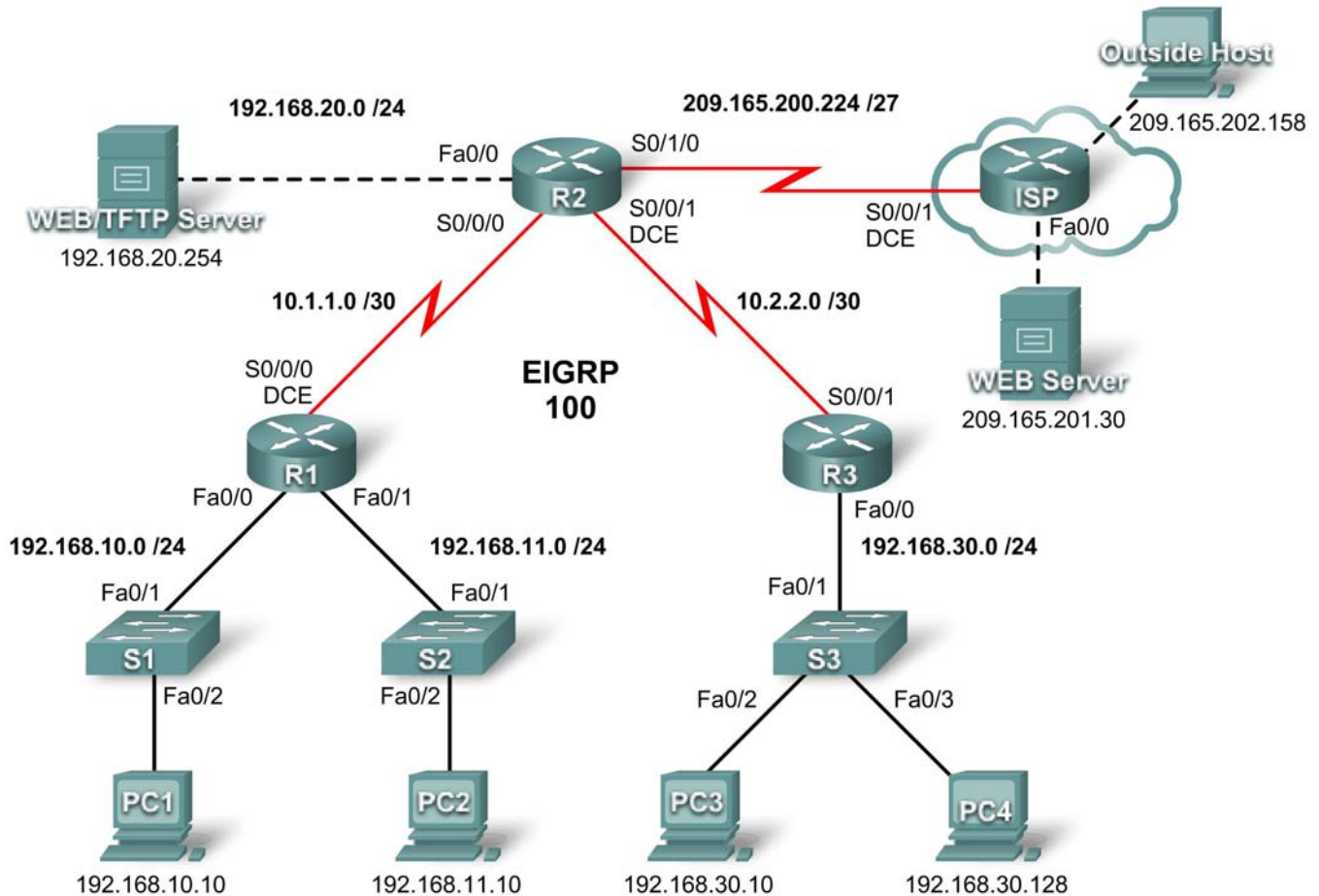
- PC1 到 PC2
- PC2 到 Outside Host
- PC2 到 Web Server
- 除 PC3 和 PC4 之间的 ping 以外，从 PC4 或向 PC4 发出的所有 ping

#### 步骤 5. 检查结果。

完成比例应为 100%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## PT 练习 5.3.4: 配置扩展 ACL (教师版)

拓扑图



## 地址表

设备	接口	IP 地址	子网掩码
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.2	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	S0/0/1	10.2.2.1	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	网卡	192.168.10.10	255.255.255.0
PC2	网卡	192.168.11.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0
PC4	网卡	192.168.30.128	255.255.255.0
WEB/TFTP Server	网卡	192.168.20.254	255.255.255.0
WEB Server	网卡	209.165.201.30	255.255.255.224
Outside Host	网卡	209.165.202.158	255.255.255.224

## 学习目标

- 检查当前的网络配置
- 评估网络策略并规划 ACL 实施
- 配置采用数字编号的扩展 ACL
- 配置命名扩展 ACL

## 简介

扩展 ACL 是一种路由器配置脚本，根据源地址、目的地址，以及协议或端口来控制路由器应该允许还是应该拒绝数据包。扩展 ACL 比标准 ACL 更加灵活而且精度更高。本练习的主要内容是定义过滤标准、配置扩展 ACL、将 ACL 应用于路由器接口并检验和测试 ACL 实施。路由器已经过配置，包括 IP 地址和 EIGRP 路由。用户执行口令是 **cisco**，特权执行口令是 **class**。

## 任务 1: 检查当前的网络配置

### 步骤 1. 查看路由器的运行配置。

逐一在三台路由器的特权执行模式下使用 **show running-config** 命令查看运行配置。请注意，接口和路由已配置完整。将 IP 地址配置与上面的地址表相比较。此时，路由器上应该尚未配置任何 ACL。

本练习不需要配置 ISP 路由器。假设 ISP 路由器不属于您的管理范畴，而是由 ISP 管理员配置和维护。

### 步骤 2. 确认所有设备均可访问所有其它位置。

将任何 ACL 应用于网络中之前，都必须确认网络完全连通。如果应用 ACL 之前不测试网络连通性，排查故障会非常困难。

要确保整个网络连通，请在不同的网络设备之间使用 **ping** 命令和 **tracert** 命令检验连接。

## 任务 2: 评估网络策略并规划 ACL 实施

### 步骤 1. 评估 R1 LAN 的策略。

- 对于 192.168.10.0/24 网络，阻止 telnet 访问所有位置，并且阻止通过 TFTP 访问地址为 192.168.20.254 的企业 Web/TFTP Server。允许所有其它访问。
- 对于 192.168.11.0/24 网络，允许通过 TFTP 和 Web 访问地址为 192.168.20.254 的企业 Web/TFTP Server。阻止从 192.168.11.0/24 网络发往 192.168.20.0/24 网络的所有其它流量。允许所有其它访问。

### 步骤 2. 为 R1 LAN 规划 ACL 实施。

- 用两个 ACL 可完全实施 R1 LAN 的安全策略。
- 第一个 ACL 支持策略的第一部分，配置在 R1 上并应用于 Fast Ethernet 0/0 接口的入站流量。
- 第二个 ACL 支持策略的第二部分，配置在 R1 上并应用于 Fast Ethernet 0/1 接口的入站流量。

### 步骤 3. 评估 R3 LAN 的策略。

- 阻止 192.168.30.0/24 网络的所有 IP 地址访问 192.168.20.0/24 网络的所有 IP 地址。
- 允许 192.168.30.0/24 的前一半地址访问所有其它目的地址。
- 允许 192.168.30.0/24 的后一半地址访问 192.168.10.0/24 网络和 192.168.11.0/24 网络。
- 允许 192.168.30.0/24 的后一半地址通过 Web 访问和 ICMP 访问所有其余目的地址。
- 明确拒绝所有其它访问。

### 步骤 4. 为 R3 LAN 规划 ACL 实施。

本步骤需要在 R3 上配置一个 ACL 并应用于 FastEthernet 0/0 接口的入站流量。

### 步骤 5. 评估通过 ISP 进入的 Internet 流量的策略。

- 仅允许 Outside Host 通过端口 80 与内部 Web Server 建立 Web 会话。
- 仅允许已建立 TCP 会话进入。
- 仅允许 ping 应答通过 R2。

### 步骤 6. 为通过 ISP 进入的 Internet 流量规划 ACL 实施。

本步骤需要在 R2 上配置一个 ACL 并应用于 Serial 0/1/0 接口的入站流量。



### 任务 3: 配置采用数字编号的扩展 ACL

#### 步骤 1. 确定通配符掩码。

在 R1 上实施访问控制策略需要两个 ACL。这两个 ACL 将用于拒绝整个 C 类网络。您需要配置一个通配符掩码，匹配这些 C 类网络中每个网络的所有主机。

例如，要匹配整个 192.168.10.0/24 子网，通配符掩码就应为 0.0.0.255。此掩码可以理解为“检查、检查、检查、忽略”，实质上能匹配整个 192.168.10.0/24 网络。

#### 步骤 2. 为 R1 配置第一个扩展 ACL。

在全局配置模式下，使用编号 110 配置第一个 ACL。首先需要阻止 192.168.10.0/24 网络中的所有 IP 地址 telnet 至任何位置。

编写语句时，请确定您目前处于全局配置模式下。

```
R1(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```

接下来要阻止 192.168.10.0/24 网络中的所有 IP 地址通过 TFTP 访问地址为 192.168.20.254 的主机。

```
R1(config)#access-list 110 deny udp 192.168.10.0 0.0.0.255 host  
192.168.20.254 eq tftp
```

最后要允许所有其它流量。

```
R1(config)#access-list 110 permit ip any any
```

#### 步骤 3. 为 R1 配置第二个扩展 ACL。

用编号 111 配置第二个 ACL。允许 192.168.11.0/24 网络中的任何 IP 地址通过 WWW 访问地址为 192.168.20.254 的主机。

```
R1(config)#access-list 111 permit tcp 192.168.11.0 0.0.0.255 host  
192.168.20.254 eq www
```

然后，允许 192.168.11.0/24 网络中的任何 IP 地址通过 TFTP 访问地址为 192.168.20.254 的主机。

```
R1(config)#access-list 111 permit udp 192.168.11.0 0.0.0.255 host  
192.168.20.254 eq tftp
```

阻止从 192.168.11.0/24 网络发往 192.168.20.0/24 网络的所有其它流量。

```
R1(config)#access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0  
0.0.0.255
```

最后，允许任何其它流量。此语句用于确保不会阻止来自其它网络的流量。

```
R1(config)#access-list 111 permit ip any any
```



#### 步骤 4. 检验 ACL 配置。

在 R1 上发出 **show access-lists** 命令，确认您的配置。输出应类似下例：

```
R1#show access-lists
Extended IP access list 110
  deny tcp 192.168.10.0 0.0.0.255 any eq telnet
  deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
  permit ip any any
Extended IP access list 111
  permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
  permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
  deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
  permit ip any any
```

#### 步骤 5. 将语句应用到接口。

要将 ACL 应用到某个接口，请进入该接口的接口配置模式。配置 **ip access-group access-list-number {in | out}** 命令，将相应 ACL 应用于该接口。

每个 ACL 都用于过滤入站流量。将 ACL 110 应用于 Fast Ethernet 0/0 接口，ACL 111 应用于 Fast Ethernet 0/1 接口。

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group 110 in
R1(config-if)#interface fa0/1
R1(config-if)#ip access-group 111 in
```

确认这两个 ACL 显示于 R1 的运行配置中而且已应用到正确的接口。

#### 步骤 6. 测试 R1 上配置的 ACL。

配置和应用 ACL 后，必须测试是否能按照预期阻止或允许流量。

- 尝试从 PC1 telnet 访问任何设备。此流量应该阻止。
- 尝试从 PC1 通过 HTTP 访问企业 Web/TFTP Server。此流量应该允许。
- 尝试从 PC2 通过 HTTP 访问 Web/TFTP Server。此流量应该允许。
- 尝试从 PC2 通过 HTTP 访问外部 Web Server。此流量应该允许。

根据您掌握的 ACL 知识，尝试从 PC1 和 PC2 执行一些其它的连通性测试。

#### 步骤 7. 检查结果。

Packet Tracer 不支持测试 TFTP 访问，因此您无法检验该策略。不过，完成比例应为 50%。如果并非如此，请单击 **Check Results（检查结果）** 查看尚未完成哪些必要部分。

## 任务 4: 为 R3 配置命名扩展 ACL

### 步骤 1. 确定通配符掩码。

192.168.30.0/24 网络中前一半 IP 地址的访问策略有如下要求:

- 拒绝其访问 192.168.20.0/24 网络
- 允许其访问所有其它目的地址

对 192.168.30.0/24 网络中的后一半 IP 地址有如下限制:

- 允许其访问 192.168.10.0 和 192.168.11.0
- 拒绝其访问 192.168.20.0
- 允许其对所有其它位置的 Web 访问和 ICMP 访问

要确定通配符掩码, 应考虑 ACL 在匹配 IP 地址 0–127 (前一半) 或 128–255 (后一半) 时需要检查哪些位。

我们学过, 确定通配符掩码的方法之一是从 255.255.255.255 中减去标准网络掩码。对 C 类地址而言, IP 地址 0–127 和 128–255 的标准掩码是 255.255.255.128。用减法可得出正确的通配符掩码:

```
255.255.255.255
- 255.255.255.128
-----
0. 0. 0.127
```

### 步骤 2. 在 R3 上配置扩展 ACL。

在 R3 上, 进入全局配置模式并以 130 作为访问列表编号配置 ACL。

第一条语句用于阻止 192.168.30.0/24 访问 192.168.30.0/24 网络中的所有地址。

```
R3(config)#access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

第二条语句用于允许 192.168.30.0/24 网络的前一半地址访问任何其它目的地址。

```
R3(config)#access-list 130 permit ip 192.168.30.0 0.0.0.127 any
```

其余的语句则明确允许 192.168.30.0/24 网络的后一半地址访问网络策略允许的网络和服务。

```
R3(config)#access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0
0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0
0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

### 步骤 3. 将语句应用到接口。

要将 ACL 应用到某个接口, 请进入该接口的接口配置模式。配置 **ip access-group access-list-number {in | out}** 命令, 将相应 ACL 应用于该接口。

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group 130 in
```

#### 步骤 4. 检验和测试 ACL。

配置和应用 ACL 后，必须测试是否能按照预期阻止或允许流量。

- 从 PC3 ping Web/TFTP Server。此流量应该阻止。
- 从 PC3 ping 任何其它设备。此流量应该允许。
- 从 PC4 ping Web/TFTP Server。此流量应该阻止。
- 从 PC4 通过 192.168.10.1 或 192.168.11.1 接口 telnet 至 R1。此流量应该允许。
- 从 PC4 ping PC1 和 PC2。此流量应该允许。
- 从 PC4 通过 10.2.2.2 接口 telnet 至 R2。此流量应该阻止。

经过测试并得出正确结果后，在 R3 上使用 **show access-lists** 特权执行命令检查 ACL 语句是否存在匹配。

根据您掌握的 ACL 知识执行其它测试，检查每条语句匹配的流量是否正确。

#### 步骤 5. 检查结果。

完成比例应为 75%。如果并非如此，请单击 **Check Results（检查结果）** 查看尚未完成哪些必要部分。

### 任务 5: 配置命名扩展 ACL

#### 步骤 1. 在 R2 上配置命名扩展 ACL。

前面讲过，R2 上配置的策略将用于过滤 Internet 流量。由于 R2 连接到 ISP，因此它是配置 ACL 的最佳位置。

在 R2 上使用 **ip access-list extended name** 命令配置名为 FIREWALL 的命名 ACL。此命令使路由器进入扩展命名 ACL 配置模式。请留意路由器提示符已更改。

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#
```

在 ACL 配置模式下添加语句，按照策略中所述的要求过滤流量：

- 仅允许 Outside Host 通过端口 80 与内部 Web Server 建立 Web 会话。
- 仅允许已建立 TCP 会话进入。
- 允许 ping 应答通过 R2。

```
R2(config-ext-nacl)#permit tcp any host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#deny ip any any
```

在 R2 上配置了 ACL 后，使用 **show access-lists** 命令确认该 ACL 语句正确。

#### 步骤 2. 将语句应用到接口。

使用 **ip access-group name {in | out}** 命令，将 ACL 应用于 ISP 的入站流量，面向 R2 的接口。

```
R3(config)#interface s0/1/0
R3(config-if)#ip access-group FIREWALL in
```

### 步骤 3. 检验和测试 ACL。

执行下列测试，确保 ACL 能达到预期效果。

- 从 Outside Host 打开内部 Web/TFTP Server 中的网页。此流量应该允许。
- 从 Outside Host ping 内部 Web/TFTP Server。此流量应该阻止。
- 从 Outside Host ping PC1。此流量应该阻止。
- 从 PC1 ping 地址为 209.165.201.30 的外部 Web Server。此流量应该允许。
- 从 PC1 打开外部 Web Server 中的网页。此流量应该允许。

经过测试并得出正确结果后，在 R2 上使用 **show access-lists** 特权执行命令检查 ACL 语句是否存在匹配。

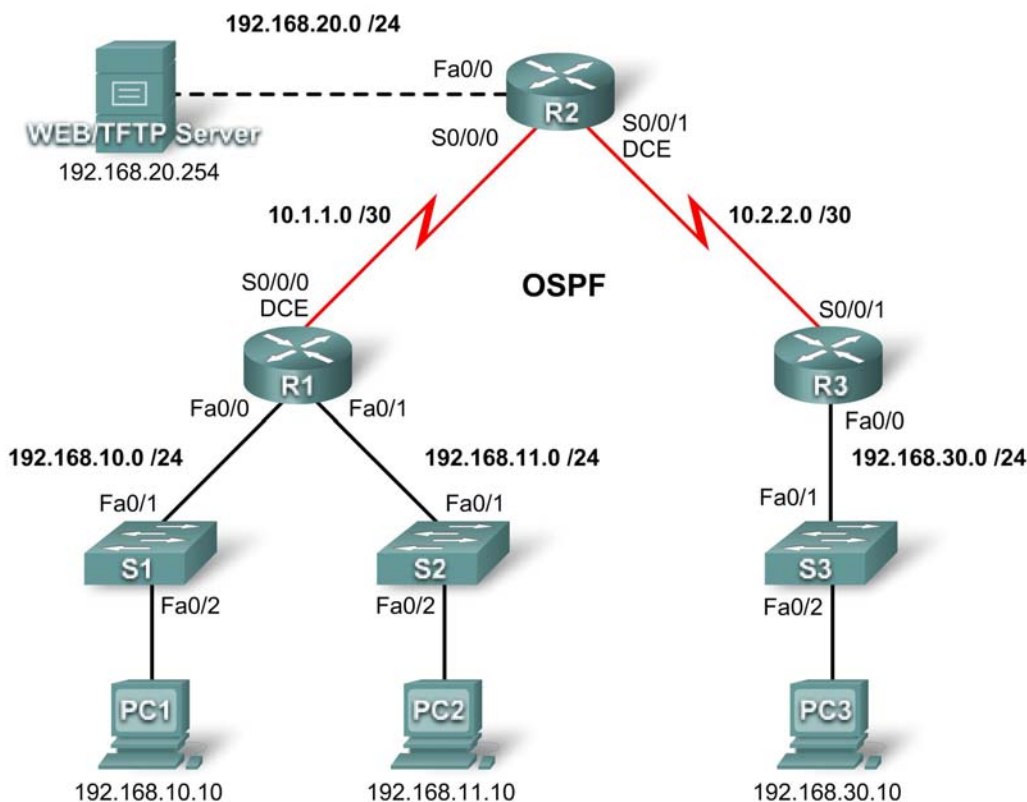
根据您掌握的 ACL 知识执行其它测试，检查每条语句匹配的流量是否正确。

### 步骤 4. 检查结果。

完成比例应为 100%。如果并非如此，请单击 **Check Results（检查结果）** 查看尚未完成哪些必要部分。

## PT 练习 5.5.1：基本访问控制列表（教师版）

拓扑图



地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/0	192.168.10.1	255.255.255.0	不适用
	Fa0/1	192.168.11.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
R2	Fa0/0	192.168.20.1	255.255.255.0	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
	Lo0	209.165.200.225	255.255.255.224	不适用
R3	Fa0/0	192.168.30.1	255.255.255.0	不适用
	S0/0/1	10.2.2.2	255.255.255.252	不适用

地址表接下一页

地址表 (续)

<b>S1</b>	<b>VLAN 1</b>	192.168.10.2	255.255.255.0	192.168.10.1
<b>S2</b>	<b>VLAN 1</b>	192.168.11.2	255.255.255.0	192.168.11.1
<b>S3</b>	<b>VLAN 1</b>	192.168.30.2	255.255.255.0	192.168.30.1
<b>PC1</b>	网卡	192.168.10.10	255.255.255.0	192.168.10.1
<b>PC2</b>	网卡	192.168.11.10	255.255.255.0	192.168.11.1
<b>PC3</b>	网卡	192.168.30.10	255.255.255.0	192.168.30.1
<b>Web Server</b>	网卡	192.168.20.254	255.255.255.0	192.168.20.1

## 学习目标

- 执行基本的路由器和交换机配置
- 配置标准 ACL
- 配置扩展 ACL
- 使用标准 ACL 控制对 vty 线路的访问
- 排查 ACL 问题

## 简介

本练习将设计、应用、测试访问列表配置并排查问题。

## 任务 1: 执行基本的路由器和交换机配置

根据以下说明配置 R1、R2 和 R3 路由器以及 S1、S2 和 S3 交换机:

- 依照拓扑图配置主机名。
- 禁用 DNS 查找。
- 配置执行模式加密口令 **class**。
- 配置当日消息标语。
- 为控制台连接配置口令 **cisco**。
- 为 vty 连接配置口令 **cisco**。
- 在所有设备上配置 IP 地址和掩码。时钟频率为 **64000**。
- 使用进程 ID 1 在所有路由器上为所有网络启用 OSPF。
- 在 R2 上配置环回接口。
- 在每台交换机上配置 VLAN 1 接口的 IP 地址。
- 使用相应的默认网关配置每台交换机。
- 使用 **ping** 命令检验 IP 是否完全连通。

## 任务 2: 配置标准 ACL

标准 ACL 只能根据源 IP 地址过滤流量。本任务要配置一个标准 ACL，阻止来自 192.168.11.0 /24 网络的流量。此 ACL 将应用于 R3 串行接口的入站流量。请记住，每个 ACL 都有一条隐式的“deny all”语句，这会导致不匹配 ACL 中任何语句的所有流量都受到阻止。因此，请在该 ACL 末尾添加 **permit any** 语句。

### 步骤 1. 创建 ACL。

在全局配置模式下，创建名为 **std-1** 的标准命名 ACL。

```
R3(config)#ip access-list standard std-1
```

在标准 ACL 配置模式下，添加一条语句，拒绝源地址为 192.168.11.0/24 的任何数据包，并在控制台显示匹配该语句的每个数据包的日志消息。

```
R3(config-std-nacl)#deny 192.168.11.0 0.0.0.255
```

允许所有其它流量。

```
R3(config-std-nacl)#permit any
```

### 步骤 2. 应用 ACL。

应用 ACL std-1，过滤通过串行接口 0/0/1 进入 R3 的数据包。

```
R3(config)#interface serial 0/0/1
R3(config-if)#ip access-group std-1 in
```

### 步骤 3. 测试 ACL。

从 PC2 ping PC3，以此测试该 ACL。由于该 ACL 的目的是阻止源地址属于 192.168.11.0/24 网络的流量，因此 PC2 (192.168.11.10) 应该无法 ping 通 PC3。

在 R3 的特权执行模式下，发出 **show access-lists** 命令。屏幕上显示的输出应类似下例。ACL 每行都有一个关联的计数器，显示匹配该规则的数据包数量。

```
Standard IP access list std-1
    deny 192.168.11.0 0.0.0.255 (3 match(es))
    permit any
```

## 任务 3: 配置扩展 ACL

需要更高的精度时，应该使用扩展 ACL。扩展 ACL 过滤流量的依据不仅仅限于源地址。扩展 ACL 可以根据协议、源 IP 地址、目的 IP 地址，以及源端口号和目的端口号过滤流量。

此网络的另一条策略规定，只允许 192.168.10.0/24 LAN 中的设备访问内部网络，而不允许此 LAN 中的计算机访问 Internet。因此，必须阻止这些用户访问 IP 地址 209.165.200.225。由于此要求的实施涉及源地址和目的地址，因此需要使用扩展 ACL。

本任务需要在 R1 上配置扩展 ACL，阻止 192.168.10.0/24 网络中任何设备发出的流量访问 209.165.200.255 主机。此 ACL 将应用于 R1 Serial 0/0/0 接口的出站流量。

### 步骤 1. 配置命名扩展 ACL。

在全局配置模式下，创建名为 **extend-1** 的命名扩展 ACL。

```
R1(config)#ip access-list extended extend-1
```

请注意，路由器提示符会改变，表示现在处于扩展 ACL 配置模式下。在此提示符后添加必要的语句，阻止从 192.168.10.0/24 到该主机的流量。定义目的地址时要使用关键字 **host**。

```
R1(config-ext-nacl)#deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225
```

前面讲过，如果没有 **permit** 语句，隐式“deny all”语句会阻止所有其它流量。因此，应添加 **permit** 语句，确保其它流量不会受到阻止。

```
R1(config-ext-nacl)#permit ip any any
```

### 步骤 2. 应用 ACL。

如果是标准 ACL，最好将其应用于尽量靠近目的地址的位置。而扩展 ACL 则通常应用于靠近源地址的位置。**extend-1** ACL 将应用于串行接口并过滤出站流量。

```
R1(config)#interface serial 0/0/0  
R1(config-if)#ip access-group extend-1 out
```

### 步骤 3. 测试 ACL。

从 PC1 或 192.168.10.0/24 网络中的任何其它设备 ping R2 的环回接口。这些 ping 会失败，因为来自 192.168.10.0/24 网络的流量只要目的地址为 209.165.200.225，都会被过滤掉。如果 ping 任何其它目的地址，则应该成功。从 192.168.10.0/24 网络的设备 ping R3，确认此点。

要进一步检查，可于 ping 操作后在 R1 上发出 **show ip access-list** 命令。

该 ACL 的两条规则都应该存在匹配。这是因为从 PC1 向 R2 环回接口发出的 ping 会被拒绝，而向 R3 发出的 ping 会被允许。

```
R1#show ip access-list  
Extended IP access list extend-1  
    deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225 (4 match(es))  
    permit ip any any (4 match(es))
```

## 任务 4: 使用标准 ACL 控制对 vty 线路的访问

限制对路由器 vty 线路的访问是远程管理的良做法。ACL 可应用于 vty 线路，从而限制对特定主机或网络的访问。本任务将配置标准 ACL，允许两个网络中的主机访问 vty 线路。拒绝所有其它主机。

检查是否可从 R1 和 R3 telnet 至 R2。

### 步骤 1. 配置 ACL。

在 R2 上配置命名标准 ACL，允许来自 10.2.2.0/29 和 192.168.30.0/24 的流量，拒绝所有其它流量。将该 ACL 命名为 **Task-4**。

```
R2(config)#ip access-list standard Task-4  
R2(config-std-nacl)#permit 10.2.2.0 0.0.0.3  
R2(config-std-nacl)#permit 192.168.30.0 0.0.0.255
```



## 步骤 2. 应用 ACL。

进入 vty 线路 0-4 的线路配置模式。

```
R2(config)#line vty 0 15
```

使用 **access-class** 命令将该 ACL 应用于这些 vty 线路的入站方向。请注意，此命令与将 ACL 应用于其它接口的命令不同。

```
R2(config-line)#access-class Task-4 in
```

## 步骤 3. 测试 ACL。

从 R1 telnet 至 R2。请注意，R1 的地址不在 ACL Task-4 permit 语句中列出的地址范围内。因此，连接尝试应失败。

从 R3 telnet 至 R2 或 192.168.30.0 /24 网络中的任何设备。屏幕上将显示要求输入 vty 线路口令的提示。

从其它网络尝试连接时，即使这些网络未在 ACL 中具体列出，尝试也会失败，原因是什么？

---

所有 ACL 都包含隐式的 **deny all** 语句，作为最后一条语句。未明确允许的所有流量都会被丢弃。

---

## 任务 5: 排查 ACL 问题

当 ACL 配置不正确或应用到错误接口或错误方向时，可能会对网络流量造成不当的影响。

### 步骤 1. 测试 ACL。

前面的任务在 R3 上创建并应用了一个命名标准 ACL。使用 **show running-config** 命令查看该 ACL 及其位置。输出应显示，配置的 ACL 名为 **std-1**，应用于 Serial 0/0/1 的入站流量。不要忘记，此 ACL 旨在阻止源地址属于 192.168.11.0/24 网络的所有网络流量访问 R3 上的 LAN。

要删除该 ACL，请在 R3 上进入 Serial 0/0/1 的接口配置模式。

```
R3(config)#interface serial 0/0/1
```

使用 **no ip access-group std-1 in** 命令从该接口删除 ACL。

```
R3(config-if)#no ip access-group std-1 in
```

使用 **show running-config** 命令确认已从 Serial 0/0/1 删除该 ACL。

### 步骤 2. 将 ACL std-1 应用于 S0/0/1 的出站流量。

为了检验 ACL 过滤方向的重要性，请重新将 **std-1** ACL 应用于 Serial 0/0/1 接口。但这次该 ACL 将用于过滤出站流量而非入站流量。应用 ACL 时请记住使用关键字 **out**。

```
R3(config-if)#ip access-group std-1 out
```

### 步骤 3. 测试 ACL。

从 PC2 ping PC3，以此测试该 ACL。也可从 R1 使用扩展 ping 命令。请注意，这次不仅 ping 会成功，而且 ACL 计数器不会增加。在 R3 上发出 **show ip access-list** 命令确认此点。

#### 步骤 4. 将 ACL 恢复为其原始配置。

从出站方向删除该 ACL，然后重新将其应用于入站方向。

```
R3(config)#interface serial 0/0/1
R3(config-if)#no ip access-group std-1 out
R3(config-if)#ip access-group std-1 in
```

#### 步骤 5. 将 Task-4 应用于 R2 Serial 0/0/0 接口的入站流量。

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip access-group Task-4 in
```

#### 步骤 6. 测试 ACL。

尝试从 R1 或其连接的网络与连接到 R2 或 R3 的任何设备通信。请注意，所有通信都会受到阻止，但 ACL 计数器不会增加。这是因为每个 ACL 末尾都有隐式 “deny all” 语句。

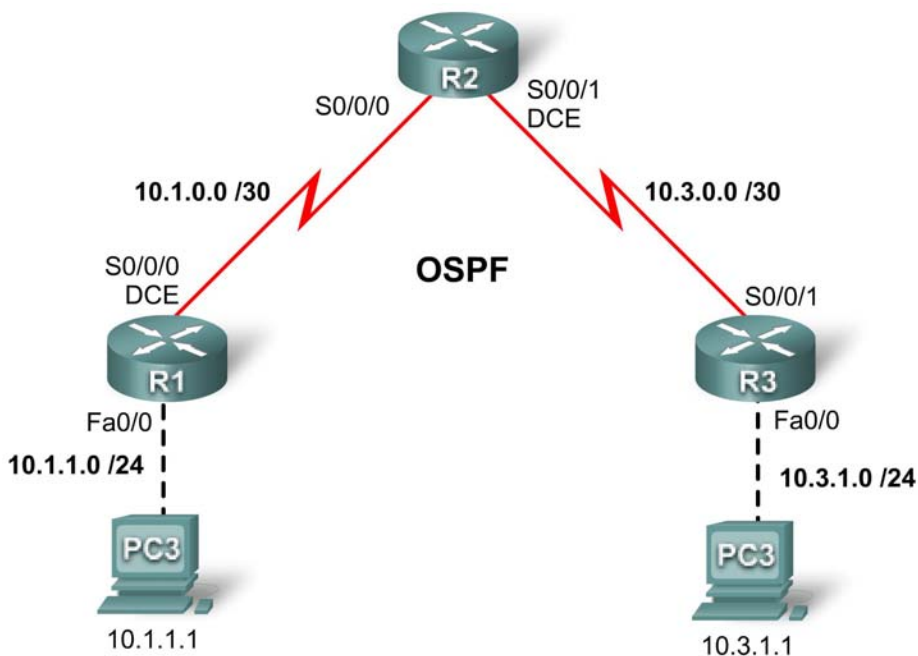
OSPF dead 计时器到期后，R1 和 R2 的控制台应显示类似下列的消息：

```
*Sep  4 09:51:21.757: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.11.1 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
```

从该接口删除 ACL Task-4。

## PT 练习 5.5.2：访问控制列表练习（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	S0/0/0	10.1.0.1	255.255.255.252	不适用
	Fa0/0	10.1.1.254	255.255.255.0	不适用
R2	S0/0/0	10.1.0.2	255.255.255.252	不适用
	S0/0/1	10.3.0.1	255.255.255.252	不适用
R3	S0/0/1	10.3.0.2	255.255.255.252	不适用
	Fa0/0	10.3.1.254	255.255.255.0	不适用
PC1	网卡	10.1.1.1	255.255.255.0	10.1.1.254
PC2	网卡	10.3.1.1	255.255.255.0	10.3.1.254

### 学习目标

- 执行基本路由器配置
- 配置标准 ACL
- 配置扩展 ACL
- 检验 ACL

## 简介

本练习将设计、应用、测试访问列表配置并排查问题。

### 任务 1: 执行基本的路由器配置

根据以下说明配置所有设备:

- 配置路由器主机名。
- 禁用 DNS 查找。
- 配置执行模式加密口令 **class**。
- 配置当日消息标语。
- 为控制台连接配置口令 **cisco**。
- 为 vty 连接配置口令 **cisco**。
- 在所有设备上配置 IP 地址和掩码。时钟频率为 **64000**。
- 使用进程 ID 1 在所有路由器上为所有网络启用 OSPF。
- 使用 **ping** 命令检验 IP 是否完全连通。

### 任务 2: 配置标准 ACL

对 R1 和 R3 的 vty 线路配置标准命名 ACL, 允许直接连接到其 FastEthernet 子网的主机获得 telnet 访问权。拒绝所有其它的连接尝试。将这些标准 ACL 命名为 **VTY-Local** 并应用于所有 telnet 线路。记录 ACL 配置。

---

---

---

---

---

---

---

---

R1 和 R3 上均应如下配置。所示仅为 R1 的配置。

```
R1(config)#ip access-list standard VTY-Local
R1(config-std-nacl)#permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)#deny any
R1(config-std-nacl)#line vty 0 4
R1(config-line)#access-class VTY-Local in
```

### 任务 3: 配置扩展 ACL

在 R2 上通过应用扩展 ACL 满足下列要求:

- 将该 ACL 命名为 block
- 阻止从连接到 R1 的子网发出的流量到达连接到 R3 的子网。
- 阻止从连接到 R3 的子网发出的流量到达连接到 R1 的子网。
- 允许所有其它流量。

记录 ACL 配置

```
R2(config)#ip access-list extended block
R2(config-ext-nacl)#deny ip 10.1.1.0 0.0.0.255 10.3.1.0 0.0.0.255
R2(config-ext-nacl)#deny ip 10.3.1.0 0.0.0.255 10.1.0.0 0.0.0.255
R2(config-ext-nacl)#permit ip any any
R2(config-ext-nacl)#int s0/0/0
R2(config-if)#ip access-group block in
R2(config-if)#int s0/0/1
R2(config-if)#ip access-group block in
```

### 任务 4: 检验 ACL

步骤 1. 测试 telnet 访问。

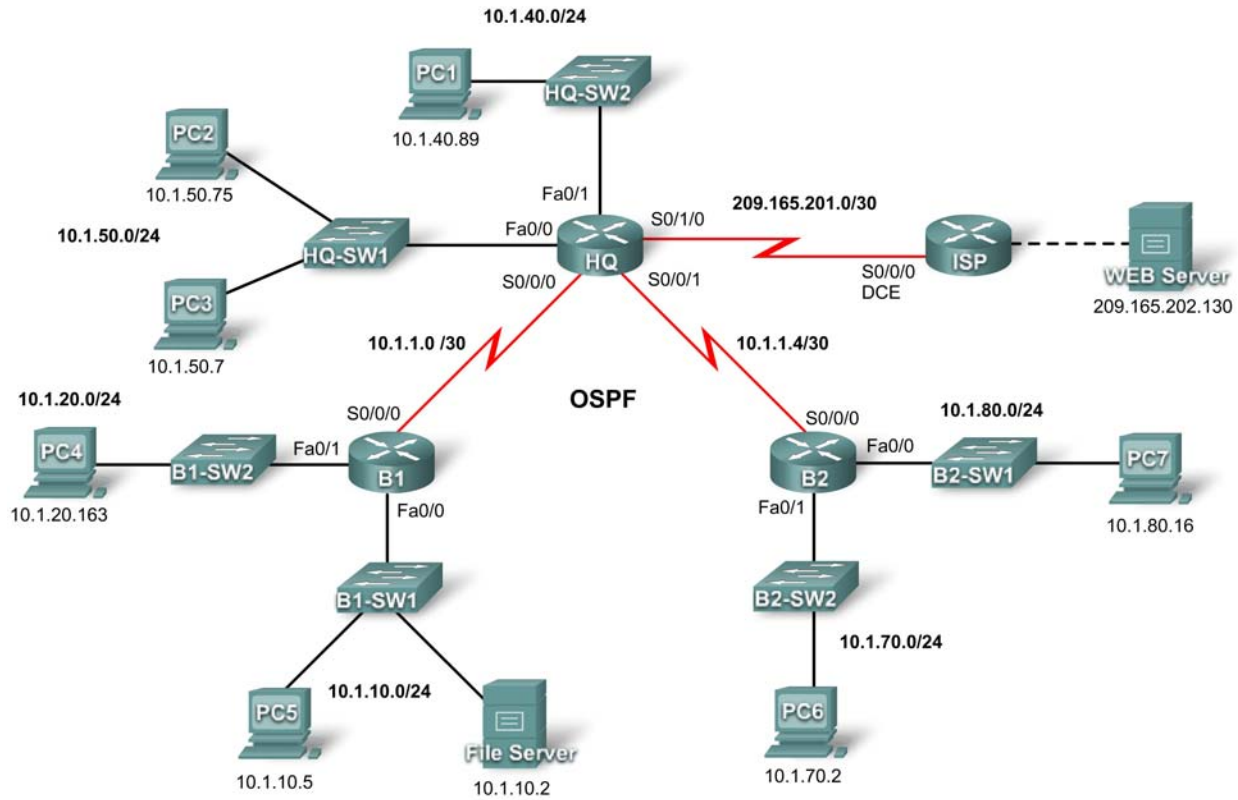
- PC1 应能通过 telnet 登录 R1
- PC3 应能通过 telnet 登录 R3
- R2 对 R1 和 R3 的 telnet 访问应被拒绝

步骤 2. 测试流量。

PC1 和 PC3 之间的 ping 应失败。

## PT 练习 5.6.1: Packet Tracer 综合技能练习 (教师版)

拓扑图



## 地址表

设备	接口	IP 地址	子网掩码
HQ	S0/0/0	10.1.1.1	255.255.255.252
	S0/0/1	10.1.1.5	255.255.255.252
	S0/1/0	209.165.201.2	255.255.255.252
	Fa0/0	10.1.50.1	255.255.255.0
	Fa0/1	10.1.40.1	255.255.255.0
B1	S0/0/0	10.1.1.2	255.255.255.252
	Fa0/0	10.1.10.1	255.255.255.0
	Fa0/1	10.1.20.1	255.255.255.0
B2	S0/0/0	10.1.1.6	255.255.255.252
	Fa0/0	10.1.80.1	255.255.255.0
	Fa0/1	10.1.70.1	255.255.255.0
ISP	S0/0/0	209.165.201.1	255.255.255.252
	Fa0/0	209.165.202.129	255.255.255.252
Web Server	网卡	209.165.202.130	255.255.255.252

## 学习目标

- 配置带有 CHAP 身份验证的 PPP
- 配置默认路由
- 配置 OSPF 路由
- 实施并检验多项 ACL 安全策略

## 简介

在本练习中，您需要演练配置实施五项安全策略的 ACL 的技能。此外，您还要配置 PPP 和 OSPF 路由。设备已配置了 IP 地址。用户执行口令是 **cisco**，特权执行口令是 **class**。

## 任务 1: 配置带有 CHAP 身份验证的 PPP

步骤 1. 将 HQ 和 B1 之间的链路配置为使用带有 CHAP 身份验证的 PPP 封装。

CHAP 身份验证的口令是 **cisco123**。

```
HQ(config)#username B1 password cisco123
HQ(config)#interface s0/0/0
HQ(config-if)#encapsulation ppp
HQ(config-if)#ppp authentication chap
```

```
B1(config)#username HQ password cisco123
B1(config)#interface s0/0/0
B1(config-if)#encapsulation ppp
B1(config-if)#ppp authentication chap
```

**步骤 2. 将 HQ 和 B2 之间的链路配置为使用带有 CHAP 身份验证的 PPP 封装。**

CHAP 身份验证的口令是 **cisco123**。

```
HQ(config)#username B2 password cisco123
HQ(config)#interface s0/0/1
HQ(config-if)#encapsulation ppp
HQ(config-if)#ppp authentication chap
```

```
B2(config)#username HQ password cisco123
B2(config)#interface s0/0/0
B2(config-if)#encapsulation ppp
```

**步骤 3. 检查路由器之间是否已恢复连通性。**

HQ 应能 ping 通 B1 和 B2。接口恢复可能需要几分钟。在 **Realtime**（实时）模式和 **Simulation**（模拟）模式之间来回切换可加快此过程。要让 **Packet Tracer** 加快此过程，另一种可行的方法是对接口使用 **shutdown** 和 **no shutdown** 命令。

注：由于 **Packet Tracer** 程序缺陷，接口可能会在练习期间的任何时候随机关闭。请等待几秒钟，通常接口会自行重新打开。

**步骤 4. 检查结果。**

完成比例应为 29%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 2：配置默认路由

**步骤 1. 配置从 HQ 到 ISP 的默认路由。**

在 HQ 上使用送出接口参数配置默认路由，将所有默认流量发送到 ISP。

```
HQ(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
```

**步骤 2. 测试与 Web Server 的连通性。**

从 HQ 的 Serial0/1/0 接口发出 ping。HQ 应该能成功 ping 通 Web Server (209.165.202.130)。

**步骤 3. 检查结果。**

完成比例应为 32%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 3：配置 OSPF 路由

**步骤 1. 在 HQ 上配置 OSPF。**

- 使用进程 ID 1 配置 OSPF。
- 通告除 209.165.201.0 网络外的所有子网。
- 向 OSPF 相邻设备传播默认路由。
- 在接入 ISP 和接入 HQ LAN 的接口上禁用 OSPF 更新。

```
HQ(config)#router ospf 1
HQ(config-router)#network 10.1.1.0 0.0.0.3 area 0
HQ(config-router)#network 10.1.1.4 0.0.0.3 area 0
HQ(config-router)#network 10.1.40.0 0.0.0.255 area 0
HQ(config-router)#network 10.1.50.0 0.0.0.255 area 0
```



```
HQ(config-router)#default-information originate
HQ(config-router)#passive-interface fa0/0
HQ(config-router)#passive-interface fa0/1
HQ(config-router)#passive-interface s0/1/0
```

## 步骤 2. 在 B1 和 B2 上配置 OSPF。

- 使用进程 ID 1 配置 OSPF。
- 在每台路由器上配置适当的子网。
- 在接入 LAN 的接口上禁用 OSPF 更新。

```
B1(config)#router ospf 1
B1(config-router)#network 10.1.1.0 0.0.0.3 area 0
B1(config-router)#network 10.1.10.0 0.0.0.255 area 0
B1(config-router)#network 10.1.20.0 0.0.0.255 area 0
B1(config-router)#passive-interface fa0/0
B1(config-router)#passive-interface fa0/1
```

```
B1(config)#router ospf 1
B1(config-router)#network 10.1.1.4 0.0.0.3 area 0
B1(config-router)#network 10.1.70.0 0.0.0.255 area 0
B1(config-router)#network 10.1.80.0 0.0.0.255 area 0
B1(config-router)#passive-interface fa0/0
B1(config-router)#passive-interface fa0/1
```

## 步骤 3. 测试整个网络的连通性。

现在，网络应该实现了完全的端到端连通性。所有设备均应能够成功 ping 通所有其它设备，包括地址为 209.165.202.130 的 Web Server。

## 步骤 4. 检查结果。

完成比例应为 76%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

## 任务 4: 实施多项 ACL 安全策略

### 步骤 1. 实施第一项安全策略。

阻止 10.1.10.0 网络访问 10.1.40.0 网络。允许对 10.1.40.0 的所有其它访问。在 HQ 上使用 ACL 编号 10 配置 ACL。

- 使用标准 ACL 还是扩展 ACL? \_\_\_\_\_ 标准
- 将 ACL 应用到哪个接口? \_\_\_\_\_ Fa0/1
- 将 ACL 应用于哪个方向? \_\_\_\_\_ 出站方向

---

---

---

---

---

---

```
HQ(config)#access-list 10 deny 10.1.10.0 0.0.0.255
HQ(config)#access-list 10 permit any
HQ(config)#int fa0/1
HQ(config-if)#ip access-group 10 out
```

**步骤 2. 检查第一项安全策略是否已实现。**

从 PC5 ping PC1 应该失败。

**步骤 3. 检查结果。**

完成比例应为 80%。如果并非如此，请单击 **Check Results** (检查结果) 查看尚未完成哪些必要部分。

**步骤 4. 实施第二项安全策略。**

拒绝主机 10.1.10.5 访问主机 10.1.50.7。允许所有其它主机访问 10.1.50.7。在 B1 上使用 ACL 编号 115 配置 ACL。

- 使用标准 ACL 还是扩展 ACL? \_\_\_\_\_ 扩展
  - 将 ACL 应用到哪个接口? \_\_\_\_\_ Fa0/0
  - 将 ACL 应用于哪个方向? \_\_\_\_\_ 入站方向
- 
- 
- 
- 
- 

```
B1(config)#access-list 115 deny ip host 10.1.10.5 host 10.1.50.7
B1(config)#access-list 115 permit ip any any
B1(config)#int fa0/0
B1(config-if)#ip access-group 115 in
```

**步骤 5. 检查第二项安全策略是否已实现。**

从 PC5 ping PC3 应该失败。

**步骤 6. 检查结果。**

完成比例应为 85%。如果并非如此，请单击 **Check Results** (检查结果) 查看尚未完成哪些必要部分。

**步骤 7. 实施第三项安全策略。**

拒绝从 10.1.50.1 到 10.1.50.63 的主机通过 Web 访问地址为 10.1.80.16 的内部网服务器。允许所有其它访问。在适当的路由器上使用 ACL 编号 101 配置 ACL。

- 使用标准 ACL 还是扩展 ACL? \_\_\_\_\_ 扩展
- 在哪台路由器上配置该 ACL? \_\_\_\_\_ HQ
- 将 ACL 应用到哪个接口? \_\_\_\_\_ Fa0/0
- 将 ACL 应用于哪个方向? \_\_\_\_\_ 入站方向

---

---

---

---

```
HQ(config)#access-list 101 deny tcp 10.1.50.0 0.0.0.63 host 10.1.80.16 eq www
HQ(config)#access-list 101 permit ip any any
HQ(config)#interface fa0/0
HQ(config-if)#ip access-group 101 in
```

#### 步骤 8. 检查第三项安全策略是否已实现。

要测试此策略，请单击 **PC3**，然后单击 **Desktop（桌面）** 选项卡，再单击 **Web Browser（Web 浏览器）**。URL 应键入内部网服务器的 IP 地址 10.1.80.16，然后按 **Enter**。几秒后应收到 Request Timeout（请求超时）消息。PC2 和该网络中的所有其它 PC 都应该能够访问内部网服务器。

#### 步骤 9. 检查结果。

完成比例应为 90%。如果并非如此，请单击 **Check Results（检查结果）** 查看尚未完成哪些必要部分。

#### 步骤 10. 实施第四项安全策略。

使用名称 **NO\_FTP** 配置命名 ACL，阻止 10.1.70.0/24 网络访问文件服务器（10.1.10.2）上的 FTP 服务（端口 21）。所有其它访问都应允许。

注意：名称区分大小写。

- 使用标准 ACL 还是扩展 ACL? \_\_\_\_\_ 扩展
  - 在哪台路由器上配置该 ACL? \_\_\_\_\_ B2
  - 将 ACL 应用到哪个接口? \_\_\_\_\_ Fa0/1
  - 将 ACL 应用于哪个方向? \_\_\_\_\_ 入站方向
- 
- 
- 
- 

```
B2(config)#ip access-list extended NO_FTP
B2(config-ext-nacl)#deny tcp 10.1.70.0 0.0.0.255 host 10.1.10.2 eq ftp
B2(config-ext-nacl)#permit ip any any
B2(config-ext-nacl)#interface fa0/1
B2(config-if)#ip access-group NO_FTP in
```

### 步骤 11. 检查结果。

Packet Tracer 不支持测试 FTP 访问，因此您无法检验此策略。不过，完成比例应为 95%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

### 步骤 12. 实施第五项安全策略。

由于 ISP 代表与 Internet 之间的连通性，因此请按照下列顺序配置名为 **FIREWALL** 的命名 ACL：

1. 仅允许来自 ISP 和来自 ISP 之外任何源地址的入站 ping 应答。
2. 仅允许来自 ISP 和来自 ISP 之外任何源地址的已建立 TCP 会话。
3. 明确阻止来自 ISP 和来自 ISP 之外任何源地址的所有其它入站访问。

- 使用标准 ACL 还是扩展 ACL? \_\_\_\_\_ 扩展
- 在哪台路由器上配置该 ACL? \_\_\_\_\_ HQ
- 将 ACL 应用到哪个接口? \_\_\_\_\_ S0/1/0
- 将 ACL 应用于哪个方向? \_\_\_\_\_ 入站方向

```
HQ(config)#ip access-list extended FIREWALL
HQ(config-ext-nacl)#permit icmp any any echo-reply
HQ(config-ext-nacl)#permit tcp any any established
HQ(config-ext-nacl)#deny ip any any
HQ(config-ext-nacl)#interface s0/1/0
HQ(config-if)#ip access-group FIREWALL in
```

### 步骤 13. 检查第五项安全策略是否已实现。

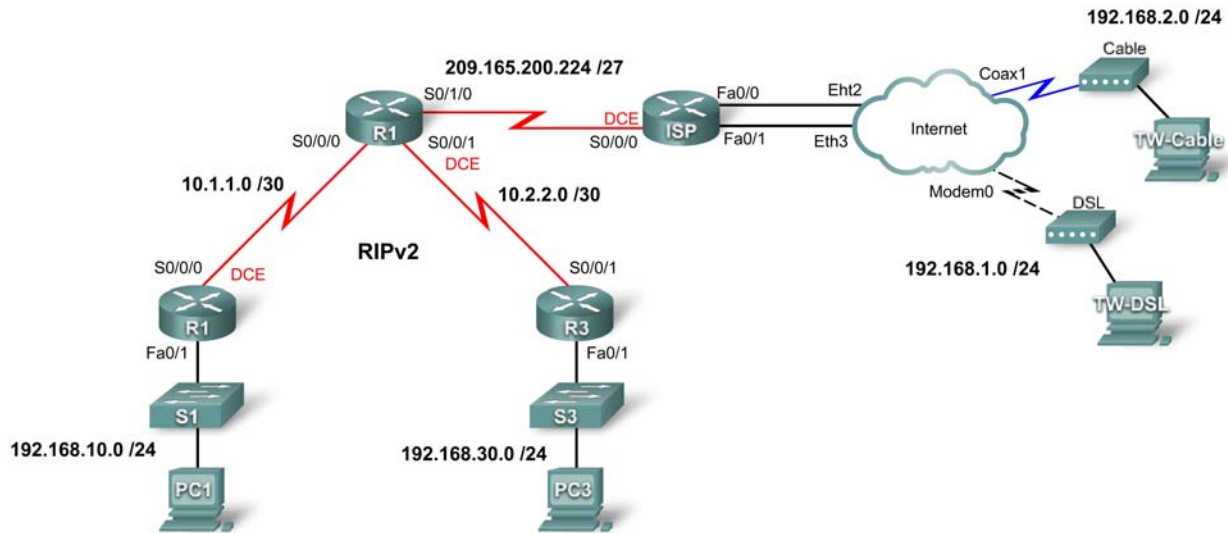
此策略的测试结果应该是任何 PC 都能 ping 通 ISP 或 Web Server。但 ISP 和 Web Server 应该都无法 ping 通 HQ 或 ACL **FIREWALL** 后的任何其它设备。

### 步骤 14. 检查结果。

完成比例应为 100%。如果并非如此，请单击 **Check Results**（检查结果）查看尚未完成哪些必要部分。

### PT 练习 6.2.4: 宽带服务 (教师版)

## 拓扑图



## 学习目标

- 将 ISP 连接至 Internet 网云
- 添加 WAN 设备
- 将 WAN 设备连接至 Internet 网云
- 将远程工作者 PC 连接至 WAN 设备
- 测试连通性

## 简介

在本练习中，您需要演练为 **Packet Tracer** 添加宽带设备和连接的技能。尽管您无法配置 DSL 调制解调器和电缆调制解调器，却可以模拟与远程工作者设备的端到端连接。

### 任务 1：将 ISP 连接至 Internet 网云

步骤 1. 通过拓扑图所示的接口进行连接。

- 将 ISP 的 Fa0/0 接口连接至 Internet 网云的 Eth2
- 将 ISP 的 Fa0/1 接口连接至 Internet 网云的 Eth3

## 步骤 2. 检查结果。

完成比例应为 25%。如果不是，请单击 **Check Results** (检查结果)，了解哪些必需的组件尚未完成。

## 任务 2：添加 WAN 设备

步骤 1. 添加 DSL 设备和电缆设备。

**DSL Modem**（DSL 调制解调器）和 **Cable Modem**（电缆调制解调器）设备位于 **WAN Emulation**（WAN 仿真）菜单中。请像安置任意其它设备一样将它们安置好。

步骤 2. 命名 WAN 设备。

用 **Config**（配置）选项卡将每台 WAN 设备的显示名称分别更改为 **Cable** 和 **DSL**。

## 任务 3：将 WAN 设备连接至 Internet 网云

步骤 1. 将电缆调制解调器连接至 Internet 网云。

从 **Connection**（连接）菜单中选择 **Coaxial**（同轴）连接类型。

步骤 2. 将 DSL 调制解调器连接至 Internet 网云。

从 **Connection**（连接）菜单中选择 **Phone**（电话）连接类型。

步骤 3. 检查结果。

完成比例应为 75%。如果不是，请单击 **Check Results**（检查结果），了解哪些必需的组件尚未完成。

## 任务 4：将远程工作者 PC 连接至 WAN 设备

步骤 1. 将 TW-Cable 连接至 Cable。

步骤 2. 将 TW-DSL 连接至 DSL。

步骤 3. 检查结果。

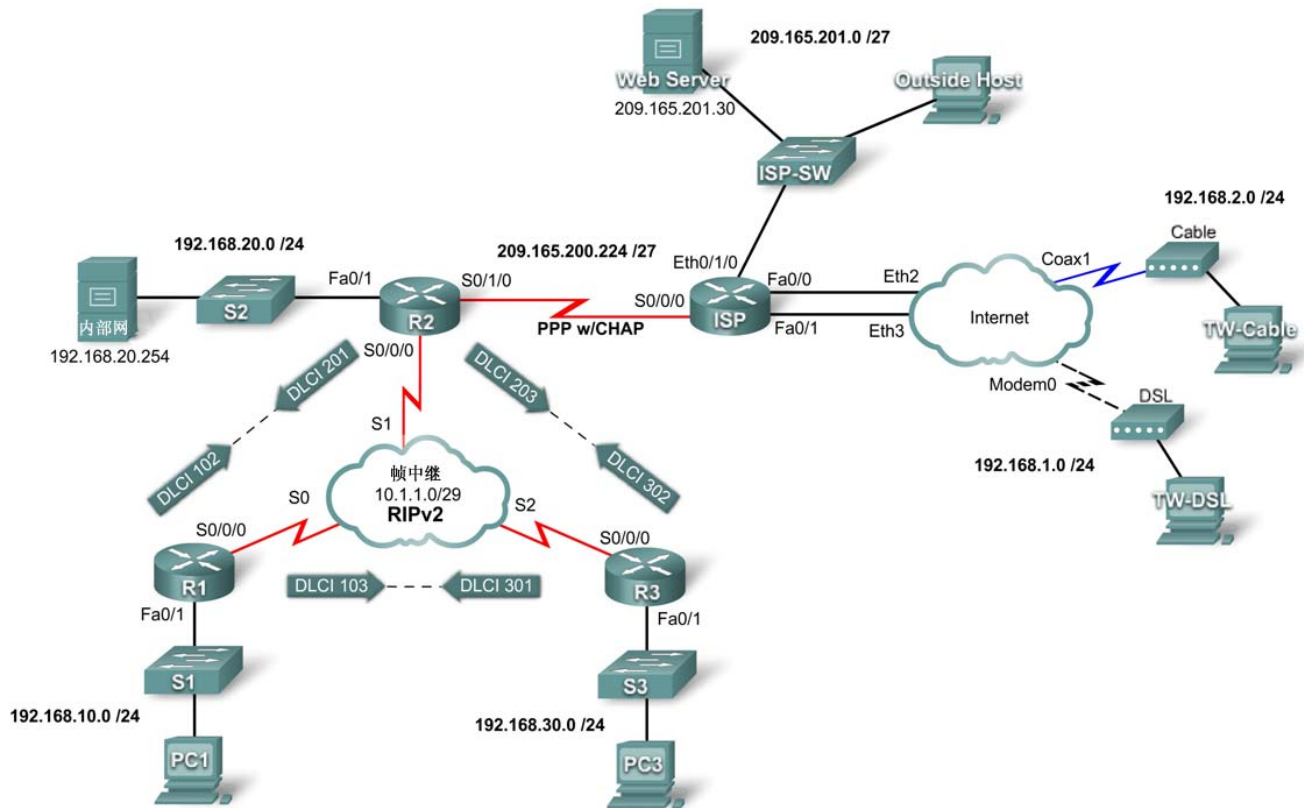
完成比例应为 100%。如果不是，请单击 **Check Results**（检查结果），了解哪些必需的组件尚未完成。

## 任务 5：测试连通性

单击 **Check Results**（检查结果），然后单击 **Connectivity Tests**（连通性测试）选项卡，检查远程工作者设备与内部 PC 间能否通信。

## PT 练习 6.4.1: Packet Tracer 综合技能练习 (教师版)

拓扑图



## 地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.248
R2	Fa0/1	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.248
	S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/0	10.1.1.3	255.255.255.248
ISP	S0/0/0	209.165.200.226	255.255.255.224
	Eth0/1/0	209.165.201.1	255.255.255.224
	Fa0/0	192.168.1.1	255.255.255.0
	Fa0/1	192.168.2.1	255.255.255.0
PC1	网卡	192.168.10.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0
Intranet	网卡	192.168.20.254	255.255.255.0
TW-DSL	网卡	192.168.1.10	255.255.255.0
TW-Cable	网卡	192.168.2.10	255.255.255.0
Web Server	网卡	209.165.201.30	255.255.255.224
Outside Host	网卡	209.165.201.10	255.255.255.224

## 学习目标

- 应用基本的路由器配置
- 配置动态路由和默认路由
- 建立远程办公服务
- 在配置 ACL 之前测试连通性
- 应用 ACL 策略
- 在配置 ACL 之后测试连通性

## 简介

本练习要求您配置一个默认路由以及使用 RIP 第 2 版的动态路由。您还要为网络添加宽带设备。最后，您要在两台路由器上设置 ACL 来控制网络流量。由于 Packet Tracer 在对 ACL 的评分方式上非常严格，因此需要按给定的顺序来配置 ACL 规则。



## 任务 1：应用基本的路由器配置

用拓扑图和地址表中的信息来配置 R1、R2 和 R3 上的基本设备配置。主机名已配置好。

包括以下内容：

- 控制台线路和 vty 线路
- 标语
- 禁用域名查询
- 接口描述

## 任务 2：配置动态路由和默认路由

### 步骤 1. 配置默认路由。

R2 需要有默认路由。请在默认路由配置中采用送出接口参数。

```
R2(config)#ip route 0.0.0.0 0.0.0.0 s0/1/0
```

### 步骤 2. 配置动态路由。

在 R1、R2 和 R3 上针对所有可用网络配置 RIPv2。R2 需要将其默认网络配置传递给其它路由器。此外，请务必对所有未用于路由的活动接口使用 **passive-interface** 命令。

```
R1(config)#router rip
R1(config-router)#version 2
R1(config-router)#network 192.168.10.0
R1(config-router)#network 10.0.0.0
R1(config-router)#passive-interface fa0/1
```

```
R2(config)#router rip
R2(config-router)#version 2
R2(config-router)#no auto-summary
R2(config-router)#network 192.168.20.0
R2(config-router)#network 10.0.0.0
R2(config-router)#default-information originate
R2(config-router)#passive-interface fa0/1
R2(config-router)#passive-interface s0/1/0
```

```
R3(config)#router rip
R3(config-router)#version 2
R3(config-router)#no auto-summary
R3(config-router)#network 192.168.30.0
R3(config-router)#network 10.0.0.0
R3(config-router)#passive-interface fa0/1
```

### 步骤 3. 检查结果。

完成比例应为 59%。如果不是，请单击 **Check Results（检查结果）**，了解哪些必需的组件尚未完成。

### 任务 3：建立远程办公服务

#### 步骤 1. 添加 WAN 设备。

根据拓扑图，添加一台 DSL 调制解调器和一台电缆调制解调器。

#### 步骤 2. 命名 WAN 设备。

用 **Config（配置）** 选项卡将每台 WAN 设备的显示名称分别更改为 **Cable** 和 **DSL**。

#### 步骤 3. 连接 WAN 设备。

使用适当的电缆和接口将 WAN 设备连接至相应的 PC 和 Internet。

#### 步骤 4. 检查结果。

完成比例应为 86%。如果不是，请单击 **Check Results（检查结果）**，了解哪些必需的组件尚未完成。

### 任务 4：在配置 ACL 之前测试连通性

此时，拓扑的所有分支都应相互连通。在 **Simulation（模拟）** 模式和 **Realtime（实时）** 模式之间切换可加快收敛。

### 任务 5：应用 ACL 策略

#### 步骤 1. 创建并应用第一项安全策略。

使用 ACL 编号 101 来实施以下 ACL 规则：

1. 允许 192.168.30.0/24 网络上的主机通过 Web 访问任意目的地。
2. 允许 192.168.30.0/24 网络上的主机通过 ping 访问任意目的地。
3. 拒绝来自网络的任何其它访问。

```
R3(config)#access-list 101 permit tcp 192.168.30.0 0.0.0.255 any eq www
R3(config)#access-list 101 permit icmp 192.168.30.0 0.0.0.255 any
R3(config)#access-list 101 deny ip any any
R3(config)#interface fa0/1
R3(config-if)#ip access-group 101 in
```

#### 步骤 2. 创建并应用第二项安全策略。

由于 ISP 提供通往 Internet 的连接，因此请按照下列顺序配置名为 **FIREWALL** 的命名 ACL：

1. 允许 TW-DSL 通过 Web 访问 Intranet 服务器。
2. 允许 TW-Cable 通过 Web 访问 Intranet 服务器。
3. 仅允许来自 ISP 和来自 ISP 之外任何源地址的入站 ping 应答。
4. 仅允许来自 ISP 和来自 ISP 之外任何源地址的已建立 TCP 会话。
5. 明确阻止来自 ISP 和来自 ISP 之外任何源地址的所有其它入站访问。

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#permit tcp host 192.168.1.10 host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp host 192.168.2.10 host 192.168.20.254 eq www
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#deny ip any any
R2(config-ext-nacl)#interface s0/1/0
R2(config-if)#ip access-group FIREWALL in
```

### 步骤 3. 检查结果。

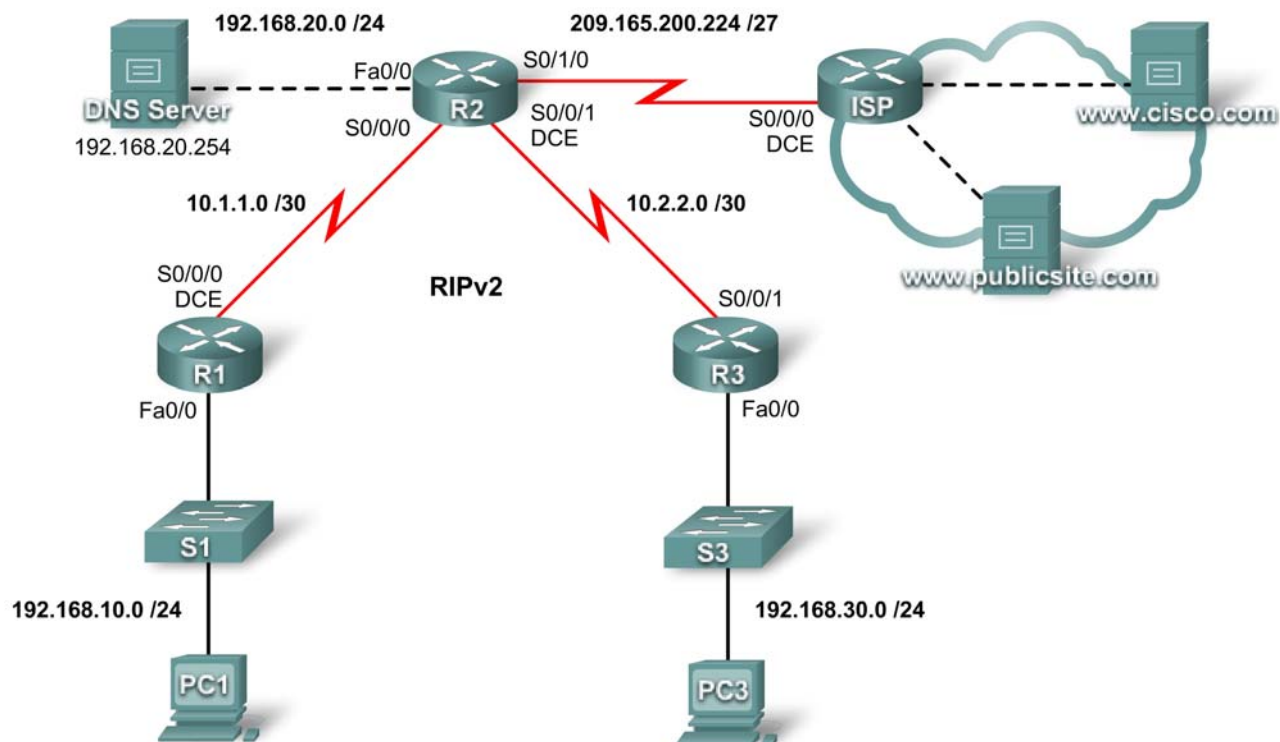
完成比例应为 100%。如果不是，请单击 **Check Results（检查结果）**，了解哪些必需的组件尚未完成。

## 任务 6： ACL 之后测试连通性

远程工作者应该无法 ping 通 Intranet 服务器，但是应该能通过 Web 浏览器访问其 HTTP 服务器。本练习包括三个 PDU，其中两个应该会失败，另一个则会成功。查看 **Check Results（检查结果）** 菜单中的 **Connectivity Tests（连通性测试）**，确保完成结果为 100%。

## PT 练习 7.1.8: 使用 Easy IP 配置 DHCP (教师版)

拓扑图



地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

## 学习目标

- 使用 Easy IP 配置路由器
- 检验 PC 是否自动配置了地址信息
- 利用 DNS 条目配置 DNS Server
- 测试 PC 到域名的连通性

## 简介

DHCP 动态分配 IP 地址和其它重要的网络配置信息。作为一种选择, Cisco 路由器可以使用 Cisco IOS 功能集 Easy IP 来提供全功能的 DHCP 服务。Easy IP 租用配置的默认期限是 24 小时。本练习中, 您将在两台路由器上配置 DHCP 服务, 并测试您的配置。

### 任务 1: 使用 Easy IP 配置路由器

#### 步骤 1. 配置 R1 和 R3 的排除地址。

服务器、路由器和打印机等设备需要静态地址, 定义一个保留给这些主机使用的地址集。可供分配给 DHCP 客户端的地址池中不包括这些地址。对于 R1 和 R3, 排除 DHCP 池中的前九个地址。

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.9
R1(config)#
```

```
R3(config)#ip dhcp excluded-address 192.168.30.1 192.168.30.9
R3(config)#
```

#### 步骤 2. 配置 R1 的地址池。

定义地址池, DHCP 将把该地址池中的地址分配给 R1 LAN 上的 DHCP 客户端。可用地址为 192.168.10.0 网络上除步骤 1 排除地址以外的所有地址。

在 R1 上, 将地址池命名为 R1LAN。为请求 DHCP 服务的客户端设备指定地址池、默认网关和 DNS 服务器。

```
R1(config)#ip dhcp pool R1LAN
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
R1(dhcp-config)#default-router 192.168.10.1
R1(dhcp-config)#dns-server 192.168.20.254
```

#### 步骤 3. 配置 R3 的地址池。

在 R3 上, 将地址池命名为 R3LAN。为请求 DHCP 服务的客户端设备指定地址池、默认网关和 DNS 服务器。

```
R3(config)#ip dhcp pool R3LAN
R3(dhcp-config)#network 192.168.30.0 255.255.255.0
R3(dhcp-config)#default-router 192.168.30.1
R3(dhcp-config)#dns-server 192.168.20.254
```

#### 步骤 4. 检查结果。

完成比例应为 43%。如果不是, 请单击 **Check Results (检查结果)**, 查看哪些需要的组件尚未完成。

## 任务 2: 检验 PC 已自动配置

### 步骤 1. 配置 PC1 和 PC3 的 DHCP 配置。

在每台 PC 的 **Desktop** (桌面) 选项卡上, 单击 **IP Configuration** (IP 配置), 然后选择 **DHCP**。IP 配置信息应会立即更新。

### 步骤 2. 检查路由器的 DHCP 运行情况。

要检验路由器的 DHCP 运行情况, 请发出 **show ip dhcp binding** 命令。结果应显示每台路由器上都绑定了一个 IP 地址。

### 步骤 3. 检查结果。

完成比例应为 86%。如果不是, 请单击 **Check Results** (检查结果), 查看哪些需要的组件尚未完成。

## 任务 3: 利用 DNS 条目配置 DNS Server

### 步骤 1. 配置 DNS Server。

要在 DNS Server 上配置 DNS, 请单击 **Config** (配置) 选项卡上的 **DNS** 按钮。

确保 DNS 已启动, 输入以下 DNS 条目:

- **www.cisco.com**                209.165.201.30
- **www.publicsite.com**        209.165.202.158

### 步骤 2. 检查结果。

完成比例应为 100%。如果不是, 请单击 **Check Results** (检查结果), 查看哪些需要的组件尚未完成。

## 任务 4: 测试 PC 到域名的连通性

### 步骤 1. 检验 PC1 可以使用域名连接到服务器。

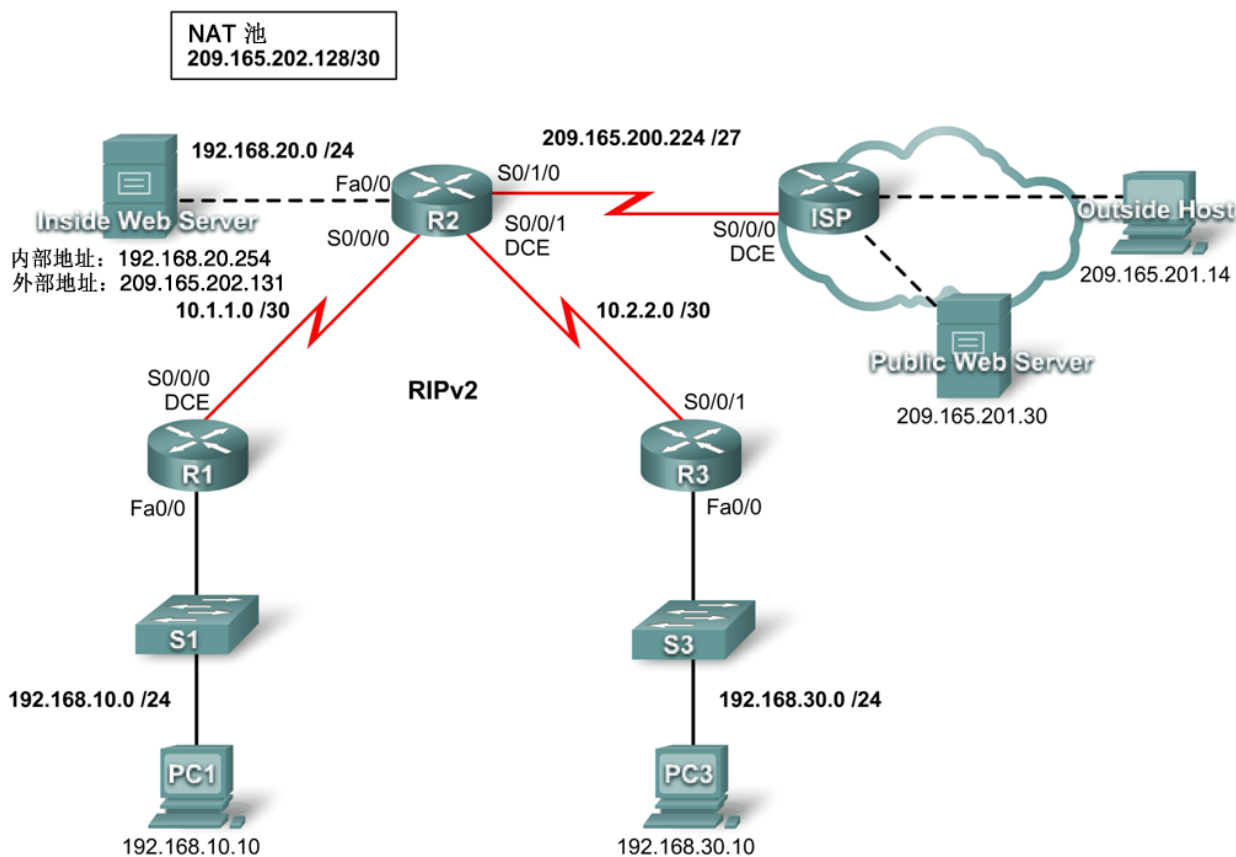
在 PC1 上打开 Web 浏览器, 在地址栏中输入 **www.cisco.com**。应会显示一个网页。

### 步骤 2. 检验 PC3 可以使用域名连接到服务器。

在 PC3 上打开 Web 浏览器, 在地址栏中输入 **www. publicsite.com**。应会显示一个网页。

## PT 练习 7.2.8：利用 NAT 扩展网络（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/1	192.168.10.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/0	10.2.2.2	255.255.255.252

地址表接下页

地址表 (续)

Inside Web Server	网卡	本地: 192.168.20.254	255.255.255.252
	网卡	全局: 209.165.202.131	255.255.255.252
PC1	网卡	192.168.10.10	255.255.255.0
PC3	网卡	192.168.30.10	255.255.255.0
Outside Host	网卡	209.165.201.14	255.255.255.240
Public Web Server	网卡	209.265.201.30	255.255.255.240

## 学习目标

- 配置 ACL 以规定可以进行 NAT 的地址
- 配置静态 NAT
- 配置动态 NAT 过载
- 利用静态路由配置 ISP 路由器
- 测试连通性

## 简介

NAT 将不可路由的私有内部地址转换成可路由的公有地址。NAT 还能在一定程度上增加网络的私密性和安全性,因为它对外部网络隐藏了内部 IP 地址。本练习中,您将配置动态 NAT 和静态 NAT。

## 任务 1: 配置 ACL 以规定可以进行 NAT 的地址

### 步骤 1. 创建命名标准 ACL。

要定义在 NAT 过程中被转换为公有地址的内部地址,请创建一个命名标准 ACL,称为 R2NAT。下面的 NAT 配置步骤将使用此列表。

```
R2(config)#ip access-list standard R2NAT
R2(config-std-nacl)# permit 192.168.10.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.20.0 0.0.0.255
R2(config-std-nacl)# permit 192.168.30.0 0.0.0.255
```

### 步骤 2. 检查结果。

完成比例应为 11%。如果不是,请单击 **Check Results (检查结果)**, 查看哪些需要的组件尚未完成。

## 任务 2: 配置静态 NAT

### 步骤 1. 为内部 Web 服务器配置静态 NAT。

Inside Web Server 需要一个不会改变的公有 IP 地址,以便能从网络外部访问它。配置静态 NAT 地址允许 Web 服务器配置私有内部地址。然后, NAT 过程将始终把使用该服务器公有地址的数据包映射到私有地址。

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.202.131
```

### 步骤 2. 检查结果。

完成比例应为 22%。如果不是,请单击 **Check Results (检查结果)**, 查看哪些需要的组件尚未完成。



### 任务 3: 配置动态 NAT 过载

除分配给 Inside Web Server 的公有 IP 地址外, ISP 还分配了三个公有地址供您使用。这些地址被映射到所有其它访问 Internet 的内部主机。

要允许三台以上内部主机同时访问 Internet, 请配置 NAT 过载来容纳额外的主机。NAT 过载也称为端口地址转换 (PAT), 它使用端口号区分来自不同主机的数据包, 这些不同主机被分配了同一公有 IP 地址。

#### 步骤 1. 定义地址池并配置动态 NAT。

输入下列命令来配置公有地址池, 它可动态映射到内部主机。

第一个命令定义了由三个公有地址组成的地址池。

第二个命令指示 NAT 过程将池中的地址映射到任务 1 所创建访问列表中定义的地址。

```
R2(config)#ip nat pool R2POOL 209.165.202.128 209.165.202.130 netmask  
255.255.255.252  
R2(config)#ip nat inside source list R2NAT pool R2POOL overload
```

#### 步骤 2. 配置 R2 上的接口以应用 NAT。

在 R2 上的接口配置模式下, 使用 **ip nat {inside | outside}** 命令配置各接口。因为内部地址位于与 Fa0/0、Serial 0/0/0 和 Serial 0/0/1 接口连接的网络上, 所以配置这些接口时请使用 **ip nat inside** 命令。Internet 与 Serial 0/1/0 接口相连, 因此配置此接口时请使用 **ip nat outside** 命令。

#### 步骤 3. 检查结果。

完成比例应为 89%。如果不是, 请单击 **Check Results (检查结果)**, 查看哪些需要的组件尚未完成。

### 任务 4: 利用静态路由配置 ISP

#### 步骤 1. 利用到 R2 的静态路由配置 ISP。

ISP 需要一个静态路由到 R2 的公有地址。使用以下命令配置此路由。

```
ISP(config)#ip route 209.165.202.128 255.255.255.224 serial0/0/0
```

#### 步骤 2. 检查结果。

完成比例应为 100%。如果不是, 请单击 **Check Results (检查结果)**, 查看哪些需要的组件尚未完成。

### 任务 5: 测试连通性

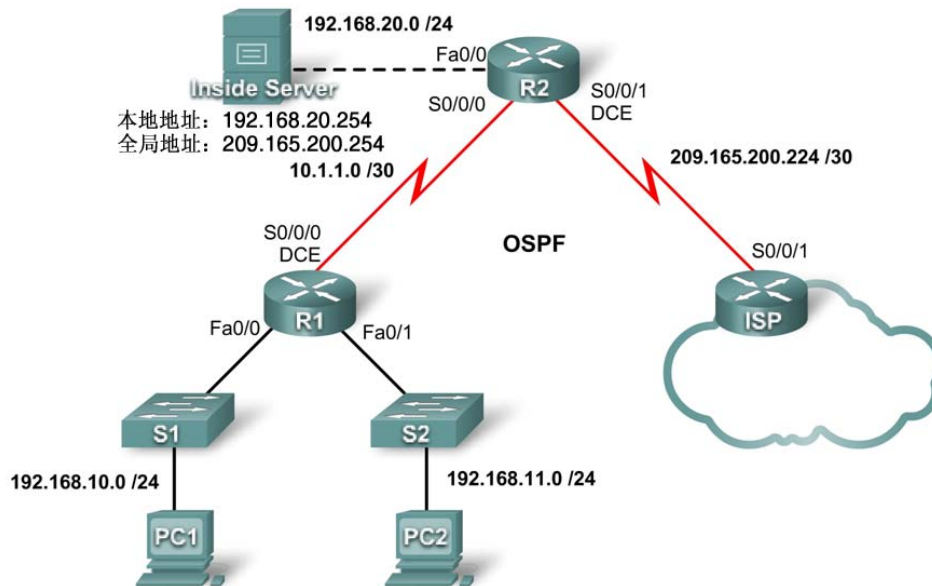
现在应能从任何内部主机 ping 通 Outside Host 或 Public Web Server。

要查看 NAT 对特定数据包的影响, 请进入仿真模式, 观察源自 PC1 的数据包。

当数据包从 R1 传到 R2 时, 单击与该数据包相关的彩色信息框。单击 **Inbound PDU Details (入站 PDU 详细信息)**, 应看到源地址为 192.168.10.10。单击 **Outbound PDU Details (出站 PDU 详细信息)**, 应看到源地址已被转换为 209.165.x.x 地址。

## 练习 7.4.1：基本 DHCP 与 NAT 配置（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	S0/0/0	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	209.165.200.225	255.255.255.252
	Fa0/0	192.168.20.1	255.255.255.0
ISP	S0/0/1	209.165.200.226	255.255.255.252

## 学习目标

完成本实验后，您将能够：

- 准备网络
- 执行基本路由器配置
- 配置 Cisco IOS DHCP 服务器
- 配置静态路由和默认路由
- 配置静态 NAT
- 利用地址池配置动态 NAT
- 配置 NAT 过载

## 场景

本实验中，您将配置 DHCP 与 NAT IP 服务。一台路由器为 DHCP 服务器。另一台路由器将 DHCP 请求转发到 DHCP 服务器。您还将配置静态和动态 NAT 配置，包括 NAT 过载。完成配置后，请检验内部地址与外部地址之间的连通性。

## 任务 1: 执行基本路由器配置

根据以下说明配置 R1、R2 和 ISP 路由器：

- 配置设备主机名。
- 禁用 DNS 查找。
- 配置特权执行模式口令。
- 配置当日消息标语。
- 为控制台连接配置口令。
- 为所有 vty 连接配置口令。
- 在所有路由器上配置 IP 地址。本练习中，PC 稍后将从 DHCP 接收 IP 编址信息。
- 在 R1 和 R2 上使用进程 ID 1 启用 OSPF。请勿通告 209.165.200.224/27 网络。

### 对所有设备：

```
enable
conf t
no ip domain-lookup
enable secret class
banner motd $Authorized Access Only!$
!
line con 0
logging synchronous
password cisco
login
!
line vty 0 4
password cisco
login
end
copy run start
```

### R1:

```
hostname R1
int fa0/0
 ip address 192.168.10.1 255.255.255.0
 no shut
int fa0/1
 ip address 192.168.11.1 255.255.255.0
 no shut
int s0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 125000
 no shut
!
router ospf 1
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.3 area 0
```

### R2:

```
hostname R2
int fa0/0
 ip address 192.168.20.1 255.255.255.0
 no shut
int s0/0/0
 ip address 10.1.1.2 255.255.255.252
 no shut
int s0/0/1
 ip address 209.165.200.225 255.255.255.252
 clock rate 125000
 no shut
!
router ospf 1
 network 10.1.1.0 0.0.0.3 area 0
```

### ISP:

```
hostname ISP
int s0/0/1
 ip address 209.165.200.226 255.255.255.252
 no shut
!
```

## 任务 2: 配置 Cisco IOS DHCP 服务器

### 步骤 1: 排除静态分配的地址。

DHCP 服务器假定 DHCP 地址池子网中的所有 IP 地址均可供分配给 DHCP 客户端。对于 DHCP 服务器不应分配给客户端的 IP 地址，必须特别指定。这些 IP 地址通常是保留给路由器接口、交换机管理 IP 地址、服务器和本地网络打印机使用的静态地址。**ip dhcp excluded-address** 命令防止路由器分配所配置范围内的 IP 地址。下列命令排除与 R1 相连的各 LAN 地址池中的前 10 个 IP 地址。这些地址不会被分配给任何 DHCP 客户端。

```
R1(config)#ip dhcp excluded-address 192.168.10.1 192.168.10.10
R1(config)#ip dhcp excluded-address 192.168.11.1 192.168.11.10
```

## 步骤 2: 配置地址池。

使用 **ip dhcp pool** 命令创建 DHCP 地址池，并将它命名为 **R1Fa0**。

```
R1(config)#ip dhcp pool R1Fa0
```

指定分配 IP 地址时使用的子网。DHCP 地址池会根据 **network** 语句自动与接口关联。现在路由器相当于 DHCP 服务器，分配 192.168.10.0/24 子网中的地址，从 192.168.10.1 开始分配。

```
R1(dhcp-config)#network 192.168.10.0 255.255.255.0
```

配置网络的默认路由器和域名服务器。客户端通过 DHCP 接收这些设置以及 IP 地址。

```
R1(dhcp-config)#dns-server 192.168.11.5
```

```
R1(dhcp-config)#default-router 192.168.10.1
```

注：地址 192.168.11.5 上并没有 DNS 服务器。配置此地址仅用于练习目的。

```
R1(config)#ip dhcp pool R1Fa1
```

```
R1(dhcp-config)#network 192.168.11.0 255.255.255.0
```

```
R1(dhcp-config)#dns-server 192.168.11.5
```

```
R1(dhcp-config)#default-router 192.168.11.1
```

## 步骤 3: 检验 DHCP 配置。

可以通过几种不同的方式检验 DHCP 服务器配置。最基本的方式是配置子网上的一台主机通过 DHCP 接收 IP 地址。然后在路由器上发出命令，以便获得更多信息。**show ip dhcp binding** 命令提供关于目前已分配的所有 DHCP 地址的信息。例如，以下输出显示 IP 地址 192.168.10.11 已被分配给 MAC 地址 3031.632e.3537.6563。该 IP 租用于 2007 年 9 月 14 日下午 7:33 到期。

```
R1#show ip dhcp binding
```

```
IP address Client-ID/ Lease expiration Type
```

```
Hardware address
```

```
192.168.10.11 0007.EC66.8752 -- Automatic
```

```
192.168.11.11 00E0.F724.8EDA -- Automatic
```

## 任务 3: 配置静态路由和默认路由

ISP 使用静态路由到达 R2 以外的所有网络。不过，给 ISP 发送流量之前，R2 会将私有地址转换成公有地址。因此，必须以公有地址配置 ISP，这些公有地址是 R2 上 NAT 配置的一部分。在 ISP 上输入以下静态路由：

```
ISP(config)#ip route 209.165.200.240 255.255.255.240 serial 0/0/1
```

此静态路由包括所有分配给 R2 的公有地址。

在 R2 上配置默认路由，并在 OSPF 中传播此路由。

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.200.226
```

```
R2(config)#router ospf 1
```

```
R2(config-router)#default-information originate
```

给 R1 几秒钟时间从 R2 学习默认路由，然后检查 R1 的路由表。或者也可以使用 **clear ip route \*** 命令清除路由表。R1 路由表中应出现指向 R2 的默认路由。从 R1 ping R2 上的 serial 0/0/1 接口 (209.165.200.225)。ping 应当能成功。如果 ping 不成功，请排除故障。

## 任务 4: 配置静态 NAT

### 步骤 1: 静态映射公有 IP 地址到私有 IP 地址。

ISP 以外的外部主机可以访问与 R2 相连的内部服务器。将公有 IP 地址 209.165.200.254 静态指定为 NAT 用来映射数据包到内部服务器私有 IP 地址 192.168.20.254 的地址。

```
R2(config)#ip nat inside source static 192.168.20.254 209.165.200.254
```

### 步骤 2: 指定内部和外部 NAT 接口。

NAT 工作之前, 必须指定哪些接口是内部接口, 哪些接口是外部接口。

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

### 步骤 3: 检验静态 NAT 配置。

从 ISP ping 公有 IP 地址 209.165.200.254。

## 任务 5: 利用地址池配置动态 NAT

静态 NAT 建立了内部地址与特定公有地址之间的永久性映射。而动态 NAT 则是将私有 IP 地址临时映射到公有地址, 这些公有 IP 地址源自 NAT 地址池。

### 步骤 1: 定义全局地址池。

创建一个地址池, 以便将符合条件的源地址转换为其中的地址。以下命令创建名为 **MY-NAT-POOL** 的地址池, 符合条件的源地址将被转换为 209.165.200.241 - 209.165.200.246 范围内的可用 IP 地址。

```
R2(config)#ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
```

### 步骤 2: 创建标准访问控制列表, 以便确定需要的转换内部地址。

```
R2(config)#ip access-list extended NAT
R2(config-std-nacl)#permit ip 192.168.10.0 0.0.0.255 any
R2(config-std-nacl)#permit ip 192.168.11.0 0.0.0.255 any
```

### 步骤 3: 将地址池与访问控制列表绑定, 建立动态源地址转换。

一台路由器可以具有一个以上的 NAT 池和一个以上的 ACL。以下命令告知路由器使用哪个地址池来转换 ACL 允许的主机。

```
R2(config)#ip nat inside source list NAT pool MY-NAT-POOL
```

### 步骤 4: 指定内部和外部 NAT 接口。

您已经指定静态 NAT 配置的内部接口和外部接口。现在将链接到 R1 的串行接口添加为内部接口。

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

### 步骤 5: 检验配置。

从 PC1 和 PC2 ping ISP。然后在 R2 上使用 **show ip nat translations** 命令检验 NAT。

```
R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.200.241      192.168.10.11    ---               ---
---  209.165.200.242      192.168.11.11    ---               ---
---  209.165.200.254      192.168.20.254   ---               ---
```

## 任务 6: 配置 NAT 过载

上例中, 如果您需要六个以上公有 IP 地址, 多于地址池允许的地址, 将会发生什么情况?

通过跟踪端口号, NAT 过载允许多位内部用户重用公有 IP 地址。

本任务中, 您将删除前一任务中配置的地址池和映射语句。然后在 R2 上配置 NAT 过载, 以便连接任何外部设备时, 所有内部 IP 地址能被转换为 R2 S0/0/1 地址。

### 步骤 1: 删除 NAT 地址池和映射语句。

使用以下命令删除 NAT 地址池和到 NAT ACL 的映射。

```
R2(config)#no ip nat pool MY-NAT-POOL 209.165.200.241 209.165.200.246 netmask
255.255.255.248
R2(config)#no ip nat inside source list NAT pool MY-NAT-POOL
```

如果接收到以下消息, 请清除 NAT 转换。

```
%Pool MY-NAT-POOL in use, cannot destroy
R2#clear ip nat translation *
```

### 步骤 2: 使用 serial 0/0/1 接口公有 IP 地址在 R2 上配置 PAT。

配置与动态 NAT 相似, 不同之处在于不是使用地址池, 而是使用 **interface** 关键字来识别外部 IP 地址。因此没有定义 NAT 池。利用 **overload** 关键字可以将端口号添加到转换中。

因为已经配置 ACL 来确定转换哪些内部 IP 地址, 并且已经指定哪些接口是内部接口和外部接口, 所以只需配置以下命令:

```
R2(config)#ip nat inside source list NAT interface S0/0/1 overload
```

### 步骤 3: 检验配置。

从 PC1 和 PC2 ping ISP。然后在 R2 上使用 **show ip nat translations** 命令检验 NAT。

```
R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.225:3  192.168.10.11:3   209.165.200.226:3
209.165.200.226:3
icmp 209.165.200.225:1024 192.168.11.11:3  209.165.200.226:3
209.165.200.226:1024
---  209.165.200.254      192.168.20.254   ---               ---
```

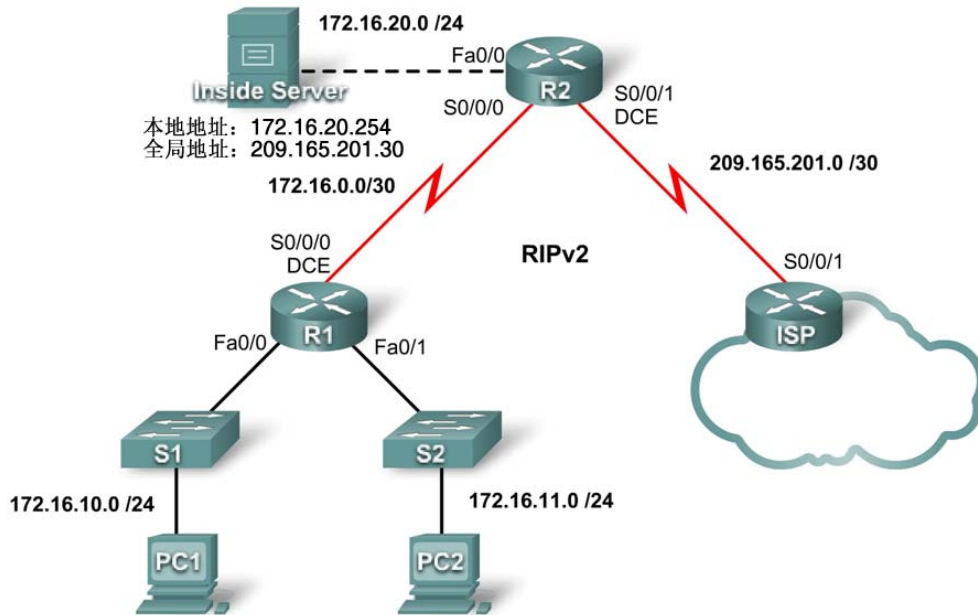
注: 前一任务中, 您可以将关键字 **overload** 添加到 **ip nat inside source list NAT pool MY-NAT-POOL** 命令中, 以允许六位以上的用户同时访问外部。

## 任务 7: 记录网络

在每台路由器上发出 **show run** 命令捕获配置信息。

## 练习 7.4.2: DHCP 与 NAT 配置练习（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	S0/0/0	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	S0/0/0	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	S0/0/1	209.165.201.2	255.255.255.252



## 学习目标

完成本实验后，您将能够：

- 准备网络
- 执行基本路由器配置
- 配置 Cisco IOS DHCP 服务器
- 配置静态路由和默认路由
- 配置静态 NAT
- 利用地址池配置动态 NAT
- 配置 NAT 过载

## 场景

本实验中，请使用拓扑图所示的网络配置 IP 地址服务。如需帮助，请参考前面的基本 DHCP 与 NAT 配置实验。不过，请尽量自己完成练习。

### 任务 1：执行基本路由器配置

根据以下说明配置 R1、R2 和 ISP 路由器：

- 配置设备主机名。
- 禁用 DNS 查找。
- 配置特权执行模式口令。
- 配置当日消息标语。
- 为控制台连接配置口令。
- 为所有 vty 连接配置口令。
- 在所有路由器上配置 IP 地址。本实验中，PC 稍后将从 DHCP 接收 IP 编址信息。
- 在 R1 和 R2 上启用 RIPv2。请勿通告 209.165.200.224/27 网络。

#### 对所有设备：

```
enable
conf t
no ip domain-lookup
enable secret class
banner motd $Authorized Access Only!$
!
line con 0
logging synchronous
password cisco
login
!
line vty 0 4
password cisco
login
end
copy run start
```

### R1:

```
hostname R1
int fa0/0
 ip address 172.16.10.1 255.255.255.0
 no shut
int fa0/1
 ip address 172.16.11.1 255.255.255.0
 no shut
int s0/0/0
 ip address 172.16.0.1 255.255.255.252
 clock rate 125000
 no shut
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

### R2:

```
hostname R2
int fa0/0
 ip address 172.16.20.1 255.255.255.0
 no shut
int s0/0/0
 ip address 172.16.0.2 255.255.255.252
 no shut
int s0/0/1
 ip address 209.165.201.1 255.255.255.252
 clock rate 125000
 no shut
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
```

### ISP:

```
hostname ISP
int s0/0/1
 ip address 209.165.201.2 255.255.255.252
 no shut
!
```

## 任务 2: 配置 Cisco IOS DHCP 服务器

将 R1 配置为这两个直接连接的 LAN 的 DHCP 服务器。

### 步骤 1. 排除静态分配的地址。

排除各地址池中的前三个地址。

```
R1(config)#ip dhcp excluded-address 172.16.10.1 172.16.10.3
R1(config)#ip dhcp excluded-address 172.16.11.1 172.16.11.3
```

## 步骤 2. 配置 DHCP 池。

- 创建两个 DHCP 池。将用于 172.16.10.0/24 网络的 DHCP 池命名为 **R1\_LAN10**，将用于 172.16.11.0/24 网络的 DHCP 池命名为 **R1\_LAN11**。
- 利用默认网关和模拟的 DNS 172.16.20.254 配置各池。

```
R1(config)#ip dhcp pool R1_LAN10
R1(dhcp-config)#network 172.16.10.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.10.1
R1(dhcp-config)#dns-server 172.16.20.254
R1(dhcp-config)#ip dhcp pool R1_LAN11
R1(dhcp-config)#network 172.16.11.0 255.255.255.0
R1(dhcp-config)#default-router 172.16.11.1
R1(dhcp-config)#dns-server 172.16.20.254
```

## 步骤 3. 检验 DHCP 配置。

```
R1#show ip dhcp binding
```

IP address	Client-ID/ Hardware address	Lease expiration	Type
172.16.10.4	00E0.F70C.7E1E	--	Automatic
172.16.11.4	0009.7CB0.39E6	--	Automatic

## 任务 3: 配置静态路由和默认路由

- 对于 209.165.201.0/27 网络，利用静态路由配置 ISP。使用送出接口作为参数。

```
ISP(config)#ip route 209.165.201.0 255.255.255.224 serial 0/0/1
```

- 在 R2 上配置默认路由，并在 OSPF 中传播此路由。使用下一跳 IP 地址作为参数。

```
R2(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.2
R2(config)#router rip
R2(config-router)#default-information originate
```

## 任务 4: 配置静态 NAT

### 步骤 1. 静态映射公有 IP 地址到私有 IP 地址。

将内部服务器 IP 地址静态映射到公有地址 209.165.201.30。

```
R2(config)#ip nat inside source static 172.16.20.254 209.165.201.30
```

### 步骤 2. 指定内部和外部 NAT 接口。

```
R2(config)#interface serial 0/0/1
R2(config-if)#ip nat outside
R2(config-if)#interface fa0/0
R2(config-if)#ip nat inside
```

### 步骤 3. 检验静态 NAT 配置。

```
R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
---  209.165.201.30       172.16.20.254    ---               ---
```

## 任务 5: 利用地址池配置动态 NAT

### 步骤 1. 定义全局地址池。

使用 /29 子网掩码创建名为 **NAT\_POOL** 的地址池，其中包括从 209.165.201.9 到 209.165.201.14 的 IP 地址范围。

```
R2(config)#ip nat pool NAT_POOL 209.165.201.9 209.165.201.14 netmask
255.255.255.248
```

### 步骤 2. 创建标准访问控制列表，以便确定需要转换的内部地址。

将标准访问控制列表命名为 **NAT\_ACL**，并允许对所有与 R1 的两个 LAN 相连的主机进行转换。

注：首先必须配置 .10 LAN，然后配置 .11 LAN。否则，Packet Tracer 不会认为该 ACL 是正确的。

```
R2(config)#ip access-list standard NAT_ACL
R2(config-std-nacl)#permit 172.16.10.0 0.0.0.255
R2(config-std-nacl)#permit 172.16.11.0 0.0.0.255
```

### 步骤 3. 建立动态源转换。

绑定 NAT 池与 ACL 并使用 NAT 过载。

```
R2(config)#ip nat inside source list NAT_ACL pool NAT_POOL overload
```

### 步骤 4. 指定内部和外部 NAT 接口。

确认内部接口和外部接口已正确指定。

```
R2(config)#interface serial 0/0/0
R2(config-if)#ip nat inside
```

### 步骤 5. 从 PC1 和 PC2 ping ISP，检验动态 NAT 配置。

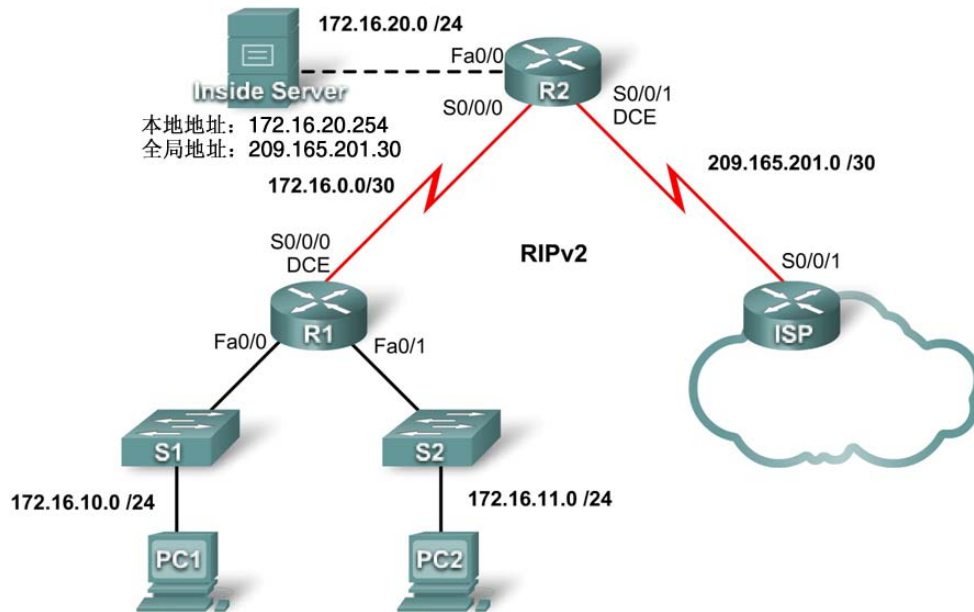
```
R2#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp  209.165.201.9:2     172.16.10.4:2     209.165.201.2:2    209.165.201.2:2
icmp  209.165.201.9:1024 172.16.11.4:2     209.165.201.2:2    209.165.201.2:1024
---  209.165.201.30       172.16.20.254    ---               ---
```

## 任务 6: 记录网络

在每台路由器上发出 **show run** 命令捕获配置信息。

## PT 练习 7.4.3: DHCP 与 NAT 故障排除 (教师版)

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	S0/0/0	172.16.0.1	255.255.255.252
	Fa0/0	172.16.10.1	255.255.255.0
	Fa0/1	172.16.11.1	255.255.255.0
R2	S0/0/0	172.16.0.2	255.255.255.252
	S0/0/1	209.165.201.1	255.255.255.252
	Fa0/0	172.16.20.1	255.255.255.0
ISP	S0/0/1	209.165.201.2	255.255.255.252

### 学习目标

完成本实验后，您将能够：

- 查找并纠正网络错误
- 记录纠正后的网络

## 场景

配置贵公司路由器的网络工程师缺乏经验，因此，若干配置错误导致了连通性问题。上级要求您排除故障并纠正配置错误，然后记录纠正后的网络。请利用您的 DHCP、NAT 知识和标准测试方法，查找并纠正错误。请确保所有客户端均能完全连接。

### 任务 1：查找并纠正网络错误

使用故障排除命令发现错误，然后纠正错误。所有错误都予以纠正后，应当能从 PC1 和 PC2 ping 通 ISP。ISP 应能 ping 通内部 Web 服务器的公有 IP 地址。

本练习中有下列错误：

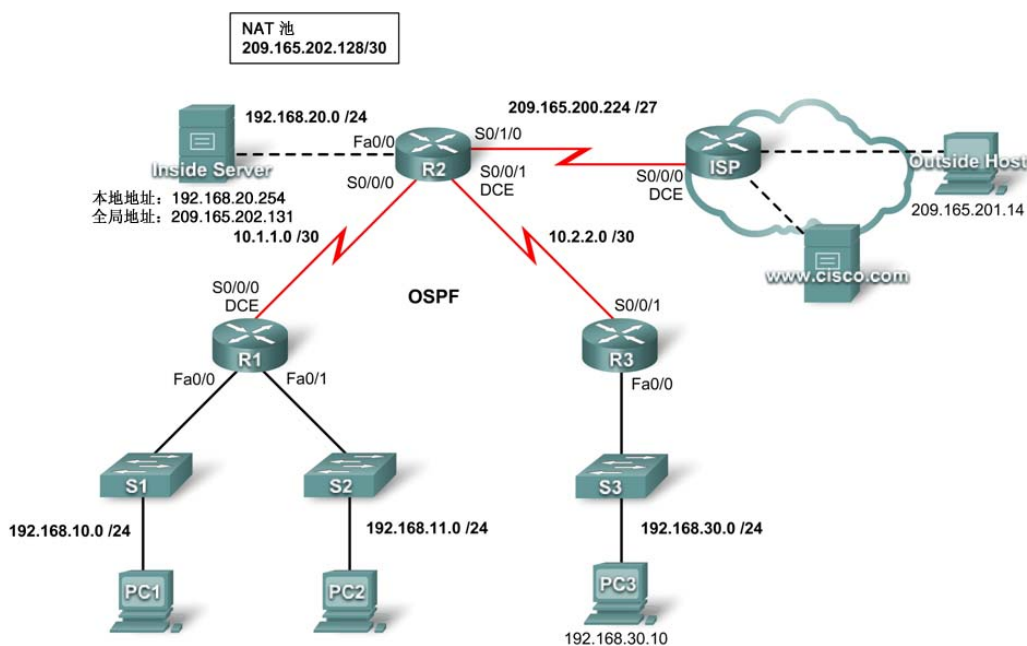
- R1 的 serial 0/0/0 接口缺少 **no shutdown** 命令。
- R2 上的 ACL 缺少允许 .11 网络的语句。
- R2 的 serial 0/0/0 接口缺少 **ip nat inside** 命令。
- R2 的 RIP 配置中缺少 **default-information originate** 命令。

### 任务 2：记录纠正后的网络

在每台路由器上发出 **show run** 命令捕获配置信息。

## PT 练习 7.5.1: Packet Tracer 综合技能练习（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码
R1	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
	S0/0/0	10.1.1.1	255.255.255.252
R2	Fa0/0	192.168.20.1	255.255.255.0
	S0/0/0	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.1	255.255.255.252
	S0/1/0	209.165.200.225	225.255.255.224
R3	Fa0/1	192.168.30.1	255.255.255.0
	S0/0/1	10.2.2.2	255.255.255.252
Inside Server	NIC	本地: 192.168.20.254	255.255.255.0
	NIC	全局: 209.165.202.131	255.255.255.252
Outside Host	NIC	209.165.201.14	255.255.255.240

## 学习目标

- 应用基本配置
- 使用 CHAP 配置 PPP 封装
- 配置动态路由和默认路由
- 使用 Easy IP 配置路由器
- 检验 PC 是否自动配置了编址信息
- 利用 DNS 条目配置 DNS 服务器
- 配置 ACL 以规定可以进行 NAT 的地址
- 配置静态 NAT
- 配置带过载的动态 NAT
- 利用静态路由配置 ISP 路由器
- 测试连通性

## 简介

在此总结练习中，您将配置 PPP、OSPF、DHCP、NAT 和到 ISP 的默认路由。然后您需要检验您的配置。

### 任务 1：应用基本配置

#### 步骤 1. 使用基本全局配置配置 R1、R2 和 R3。

- 主机名见地址表所列
- 控制台线路登录口令：**cisco**
- vty 0–4 登录口令：**cisco**
- 加密口令：**class**
- 标语：AUTHORIZED ACCESS ONLY!（仅限授权访问）

只有主机名和标语将被评分。

#### 步骤 2. 在 R1、R2 和 R3 上配置接口。

使用地址表确定接口地址。使用拓扑图确定哪些接口是 DCE 接口。配置 DCE 接口的时钟频率为 64000。

#### 步骤 3. 检查结果。

完成比例应为 38%。如果不是，请单击 **Check Results**（检查结果），查看哪些需要的组件尚未完成。

### 任务 2：使用 CHAP 配置 PPP 封装

#### 步骤 1. 将 R1 与 R2 之间的链路配置为使用带有 CHAP 身份验证的 PPP 封装。

CHAP 身份验证的口令是 **cisco123**。

#### 步骤 2. 将 R2 与 R3 之间的链路配置为使用带有 CHAP 身份验证的 PPP 封装。

CHAP 身份验证的口令是 **cisco123**。



### 步骤 3. 检查路由器之间是否已恢复连通性。

R2 应能 ping 通 R1 和 R3。接口恢复可能需要几分钟。在 Realtime（实时）模式和 Simulation（模拟）模式之间来回切换可加快此过程。对于 Packet Tracer 的这种行为，另一种可行的临时解决方法是对接口使用 **shutdown** 和 **no shutdown** 命令。

注：由于 Packet Tracer 程序缺陷，接口可能会在练习期间的任何时候随机关闭。如果等待几秒钟，通常接口会自行重新打开。

### 步骤 4. 检查结果。

完成比例应为 51%。如果不是，请单击 **Check Results（检查结果）**，查看哪些需要的组件尚未完成。

## 任务 3: 配置动态路由和默认路由

### 步骤 1. 配置 R1、R2 和 R3 使用 OSPF 路由协议。

- 在路由器上配置 OSPF 时，使用进程 ID 1。
- 通告与 R1 和 R3 相连的所有网络，但请勿将路由更新送出 LAN 接口以外。
- 在 R2 上，请勿通告 209.165.200.224 网络，并请勿将路由更新送出 Fa0/0 或 Serial 0/1/0 接口以外。

### 步骤 2. 在 R2 上配置默认路由。

配置到 ISP 的静态路由，将 R2 上的送出接口指定为下一跳地址。

### 步骤 3. 配置 OSPF 通告默认路由。

在 R2 上，输入命令以通过 OSPF 向 R1 和 R3 通告默认路由。

### 步骤 4. 检查结果。

完成比例应为 66%。如果不是，请单击 **Check Results（检查结果）**，查看哪些需要的组件尚未完成。

## 任务 4: 使用 Easy IP 配置路由器

### 步骤 1. 配置 R1 充当 192.168.10.0 和 192.168.11.0 网络的 DHCP 服务器。

- 将用于 192.168.10.0 网络的 DHCP 池命名为 **R1LAN1**。将用于 192.168.11.0 网络的 DHCP 池命名为 **R1LAN2**。
- 将各网络上的前九个地址排除出去，不用于动态分配。
- 除分配 IP 地址和子网掩码外，还应分配默认网关和 DNS 服务器地址。

### 步骤 2. 配置 R3 充当 192.168.30.0 网络的 DHCP 服务器。

- 将用于 192.168.30.0 网络的 DHCP 池命名为 **R3LAN**。
- 将各网络上的前九个地址排除出去，不用于动态分配。
- 除分配 IP 地址和子网掩码外，还应分配默认网关和 DNS 服务器地址。

### 步骤 3. 检查结果。

完成比例应为 75%。如果不是，请单击 **Check Results（检查结果）**，查看哪些需要的组件尚未完成。

## 任务 5: 检验 PC 是否自动配置了编址信息

**步骤 1. 配置 PC1、PC2 和 PC3，使其可以通过 DHCP 自动配置 IP 信息。**

**步骤 2. 检验各台 PC 是否自动从正确的 DHCP 池获得了地址。**

**步骤 3. 检查结果。**

完成比例应为 88%。如果不是，请单击 **Check Results** (检查结果)，查看哪些需要的组件尚未完成。

## 任务 6: 利用 DNS 条目配置 DNS 服务器

**步骤 1. 配置 DNS 服务器。**

要在 Inside Server 上配置 DNS，请单击 **Config** (配置) 选项卡上的 **DNS** 按钮。

确保 DNS 已启动，输入以下 DNS 条目：

- www.cisco.com            209.165.201.30

**步骤 2. 检查结果。**

目前无法通过域名 ping 通 **www.cisco.com** 服务器，您需要在任务 10 中配置完静态路由后才能 ping 通。  
完成比例应为 90%。如果不是，请单击 **Check Results** (检查结果)，查看哪些需要的组件尚未完成。

## 任务 7: 配置 ACL 以规定可以进行 NAT 的地址

**步骤 1. 创建标准命名 ACL。**

创建标准命名 ACL **R2NAT**，使其允许所有内部网络均可通过 NAT 建立映射。

注：为了让 Packet Tracer 给此任务正确评分，必须按下列顺序输入允许进行 NAT 的网络：

- 192.168.10.0
- 192.168.20.0
- 192.168.30.0
- 192.168.11.0

**步骤 2. 检查结果。**

完成比例应为 91%。如果不是，请单击 **Check Results** (检查结果)，查看哪些需要的组件尚未完成。

## 任务 8: 配置静态 NAT

**步骤 1. 为内部 Web 服务器配置静态 NAT。**

配置静态 NAT 将 Inside Server 的本地 IP 地址与全局 IP 地址建立映射。请使用地址表中列出的地址。

**步骤 2. 检查结果。**

完成比例应为 92%。如果不是，请单击 **Check Results** (检查结果)，查看哪些需要的组件尚未完成。

## 任务 9: 配置带过载的动态 NAT

### 步骤 1. 配置动态 NAT 池。

使用拓扑图中指定的 NAT 池配置动态 NAT 地址池。将该地址池命名为 **R2POOL**。

### 步骤 2. 配置动态 NAT 映射。

将 R2POOL 中的地址映射到以上定义的 R2NAT 中的网络。

### 步骤 3. 将 NAT 应用到 R2 的内部接口和外部接口。

### 步骤 4. 检查结果。

完成比例应为 99%。如果不是，请单击 **Check Results (检查结果)**，查看哪些需要的组件尚未完成。

## 任务 10: 利用静态路由配置 ISP 路由器

### 步骤 1. 配置到 R2 全局 IP 地址的静态路由。

此为 209.165.202.128/27 网络。使用 ISP 的串行接口作为下一跳地址。

### 步骤 2. 检查结果。

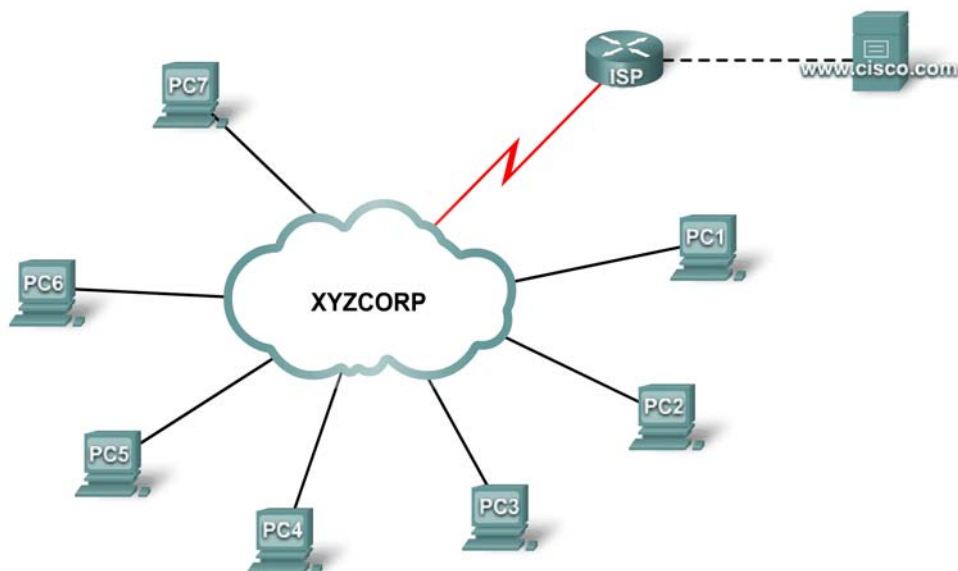
完成比例应为 100%。如果不是，请单击 **Check Results (检查结果)**，查看哪些需要的组件尚未完成。

## 任务 11: 测试连通性

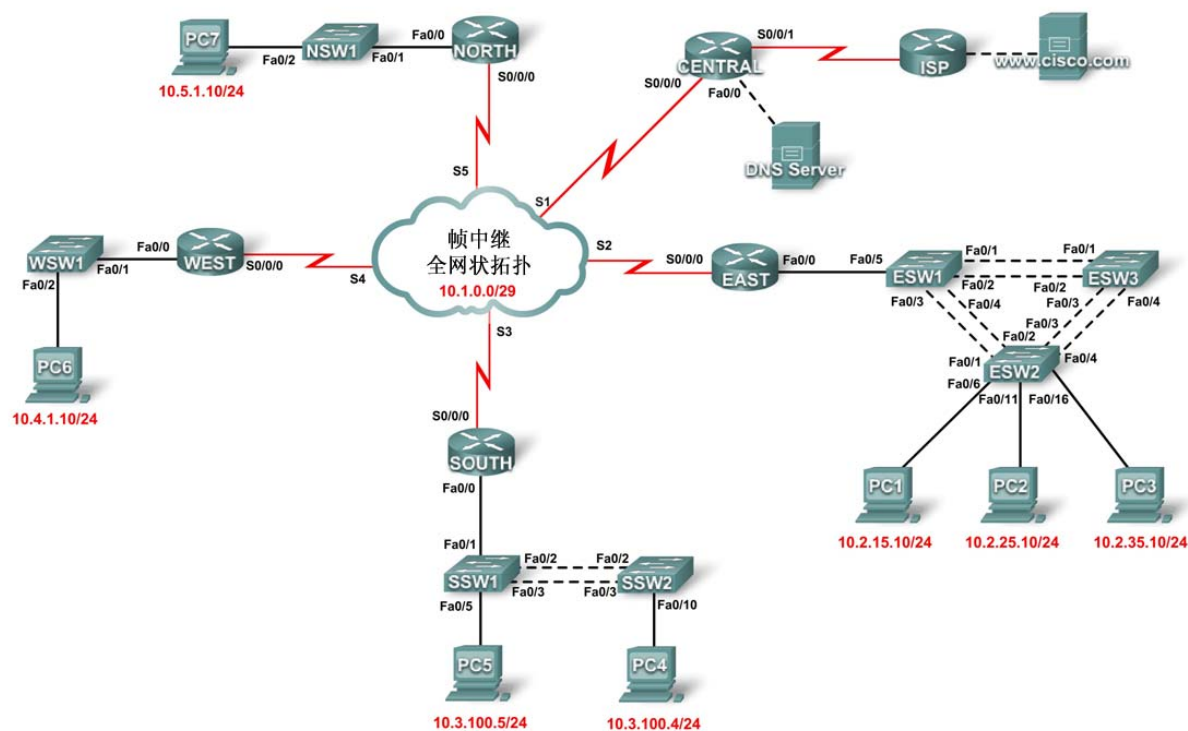
- 内部主机应能 ping 通 Outside Host。
- 内部主机应能 ping 通 www.cisco.com。
- Outside Host 应能 ping 通 Inside Server 的全局 IP 地址。

## PT 练习 8.1.2: 网络的发现与记录 (教师版)

拓扑图



拓扑图 (仅供教师使用)



## 地址表

设备	接口	IP 地址	子网掩码	默认网关
PC1	网卡	10.2.15.10	255.255.255.0	10.2.15.1
PC2	网卡	10.2.25.10	255.255.255.0	10.2.25.1
PC3	网卡	10.2.35.10	255.255.255.0	10.2.35.1
PC4	网卡	10.3.100.4	255.255.255.0	10.3.100.1
PC5	网卡	10.3.100.5	255.255.255.0	10.3.100.1
PC6	网卡	10.4.1.10	255.255.255.0	10.4.1.1
PC7	网卡	10.5.1.10	255.255.255.0	10.5.1.1
DNS Server	网卡	10.1.100.2	255.255.255.0	10.1.100.1
CENTRAL	S0/0/0	10.1.0.1	255.255.255.248	不适用
CENTRAL	S0/0/1	209.165.201.2	255.255.255.252	不适用
CENTRAL	Fa0/0	10.1.100.1	255.255.255.0	不适用
EAST	S0/0/0	10.1.0.2	255.255.255.248	不适用
EAST	Fa0/0.5	10.2.5.1	255.255.255.0	不适用
EAST	Fa0/0.15	10.2.15.1	255.255.255.0	不适用
EAST	Fa0/0.25	10.2.25.1	255.255.255.0	不适用
EAST	Fa0/0.35	10.2.35.1	255.255.255.0	不适用
ESW1	VLAN 5	10.2.5.21	255.255.255.0	10.2.5.1
ESW2	VLAN 5	10.2.5.22	255.255.255.0	10.2.5.1
ESW3	VLAN 5	10.2.5.23	255.255.255.0	10.2.5.1
SOUTH	S0/0/0	10.1.0.3	255.255.255.248	不适用
SOUTH	Fa0/0.100	10.3.100.1	255.255.255.0	不适用
SOUTH	Fa0/0.105	10.3.105.1	255.255.255.0	不适用
SSW1	VLAN 105	10.3.105.21	255.255.255.0	10.3.105.1
SSW2	VLAN 105	10.3.105.22	255.255.255.0	10.3.105.1
WEST	S0/0/0	10.1.0.4	255.255.255.248	不适用
WEST	Fa0/0	10.4.1.1	255.255.255.0	不适用
WSW1	无	无	无	无
NORTH	S0/0/0	10.1.0.5	255.255.255.248	不适用
NORTH	Fa0/0	10.5.1.1	255.255.255.0	不适用
NSW1	无	无	无	无

## 学习目标

- 测试连通性
- 查找 PC 配置信息
- 查找默认网关的配置信息
- 查找网络中的路由和邻居
- 绘制网络拓扑

## 简介

本练习主要包含有关使用 **telnet** 命令、**show cdp neighbors detail** 命令以及 **show ip route** 命令查找网络的步骤。本练习包含两部分，这是第一部分。

您打开 **Packet Tracer** 练习时看到的拓扑并不会显示网络的所有详细信息。详细信息已通过 **Packet Tracer** 的群集功能隐藏起来。网络基础架构已经过折叠，文件中的拓扑仅显示了终端设备。您的任务就是通过掌握的网络连接命令和查找命令来了解整个网络拓扑并将其记录下来。

### 任务 1：测试连通性

#### 步骤 1. 收敛并测试整个网络。

您需要提供一些协助，以便 **Packet Tracer** 收敛网络。在 PC 之间以及 PC 与 **www.cisco.com** 服务器之间执行 **ping** 命令，以加快收敛速度并测试网络。所有 PC 之间应该能彼此 **ping** 通，并且 PC 能 **ping** 通服务器。请记住，可能需要多次执行 **ping** 命令才能成功。

### 任务 2：查找 PC 配置信息

#### 步骤 1. 访问 PC1 命令提示符。

单击 **PC1**，再单击 **Desktop**（桌面）选项卡，然后单击 **Command Prompt**（命令提示符）。

#### 步骤 2. 确定 PC1 的编址信息。

要确定当前的 IP 地址配置，请输入 **ipconfig /all** 命令。

注：在 **Packet Tracer** 中，您必须在 **ipconfig** 和 **/all** 之间输入一个空格。

#### 步骤 3. 将 PC1 的信息记录在地址表中。

#### 步骤 4. 对其它 PC 重复以上步骤。

对 PC2 至 PC7 重复步骤 1-3。

### 任务 3：查找默认网关的配置信息

#### 步骤 1. 测试 PC1 与其默认网关之间的连通性。

从 PC1 **ping** 默认网关，确保它们的连通性。

#### 步骤 2. Telnet 至默认网关。

使用 **telnet ip-address** 命令。此处的 IP 地址是默认网关的 IP 地址。系统提示输入口令时，请键入 **cisco**。

### 步骤 3. 查看当前接口配置。

分别使用 **show ip interface brief** 命令和 **show protocols** 命令来检查当前接口配置。

这两条命令有何差异？

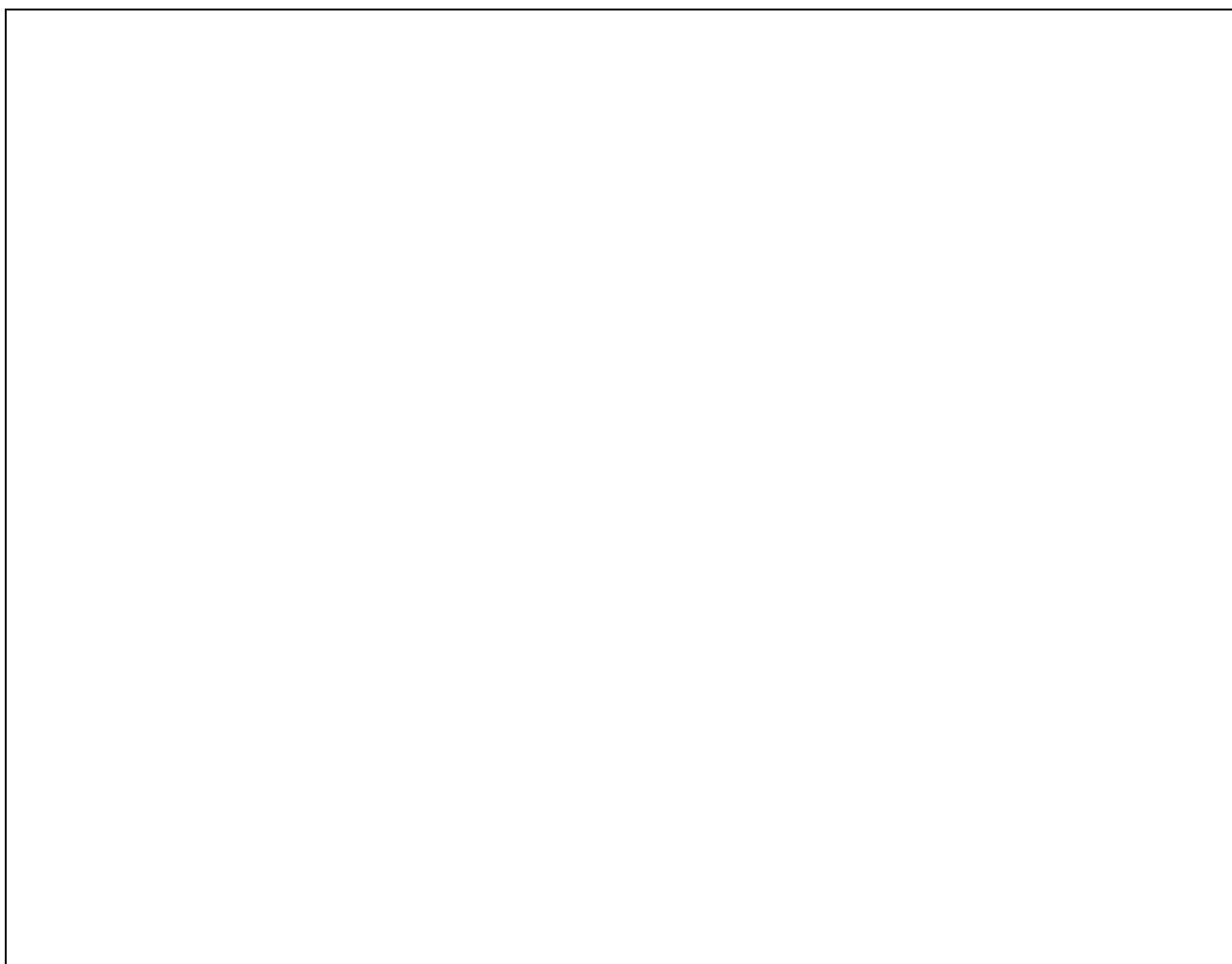
---

**show protocols** 命令会显示子网掩码信息。

### 步骤 4. 将主机名和接口配置记录在地址表中。

在下面的空白处绘制拓扑草图。

### 拓扑草图



## 任务 4：查找网络中的路由和邻居

### 步骤 1. 在同一台路由器上显示路由表。

用 **show ip route** 命令显示路由表。您应该会看到五条已连接的路由和六条通过 RIP 获知的路由，其中一条是默认路由。

除了显示路由，路由表还会显示其它哪些可帮助您进一步发现并记录网络的有用信息？

---

还显示四个 IP 地址，可供您通过 telnet 方式继续发现网络。

### 步骤 2. 查找直接相连的 Cisco 设备。

在同一台路由器上，用 **show cdp neighbors detail** 命令查找其它直接相连的 Cisco 设备。

### 步骤 3. 记录邻居信息并测试连通性。

**show cdp neighbors detail** 命令会列出一个邻居的相关信息，包括它的 IP 地址。请记录该邻居的主机名和 IP 地址。然后 ping 该 IP 地址，以此测试连通性。前几次 ping 操作会失败，直到 ARP 解析出 MAC 地址。

### 步骤 4. Telnet 至邻居，查找直接相连的 Cisco 设备。

Telnet 至邻居，然后用 **show cdp neighbors detail** 命令查找其它直接相连的 Cisco 设备。

此时，您会看到列出了三台设备。为何系统会重复列出路由器？

---

对于每个子接口，都会列出一台 EAST 路由器。

### 步骤 5. 记录邻居的主机名和 IP 地址并测试连通性。

记录并 ping 发现的新邻居。请记住，前几次 ping 操作会失败，直到 ARP 解析出 MAC 地址。

### 步骤 6. Telnet 至每个邻居，查找其它 Cisco 设备。

Telnet 至您发现的每个新邻居，然后用 **show cdp neighbors detail** 命令查找是否还有其它 Cisco 设备。访问口令是 **cisco**。

### 步骤 7. 继续发现并记录网络。

退出 telnet 会话，从而返回 PC1 的默认网关路由器。从该路由器 telnet 至网络中的其它路由器，以便继续发现并记录网络。务必使用 **show ip route** 命令和 **show ip cdp neighbors** 命令查找可用于 Telnet 操作的 IP 地址。



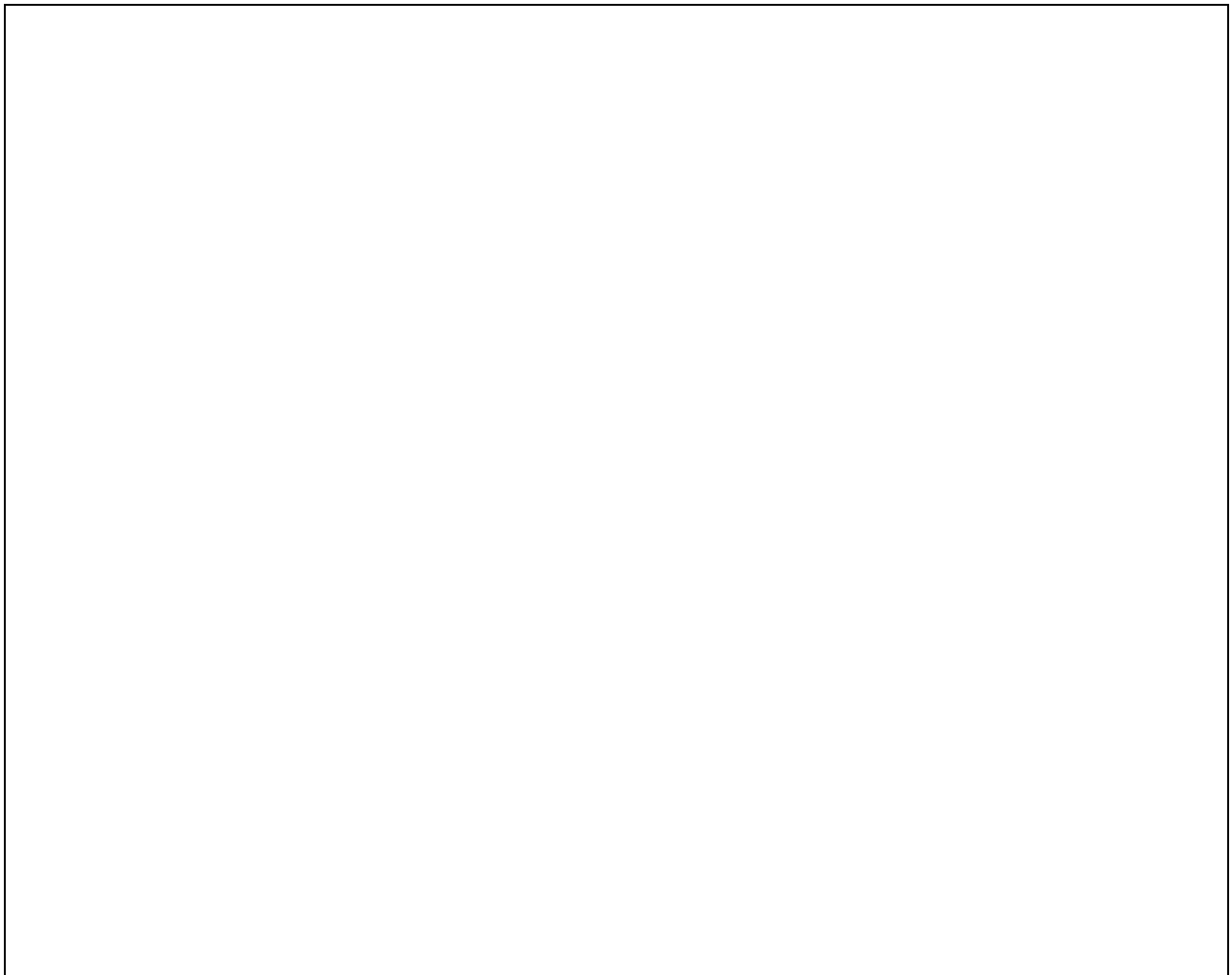
## 任务 5：绘制网络拓扑

### 步骤 1. 绘制拓扑。

您已经找出所有网络设备并记下它们的地址，接下来请用地址表和先前绘制的拓扑草图来绘制最终版的拓扑图。

提示：该网络中间位置有一个帧中继网云。

### 最终拓扑图

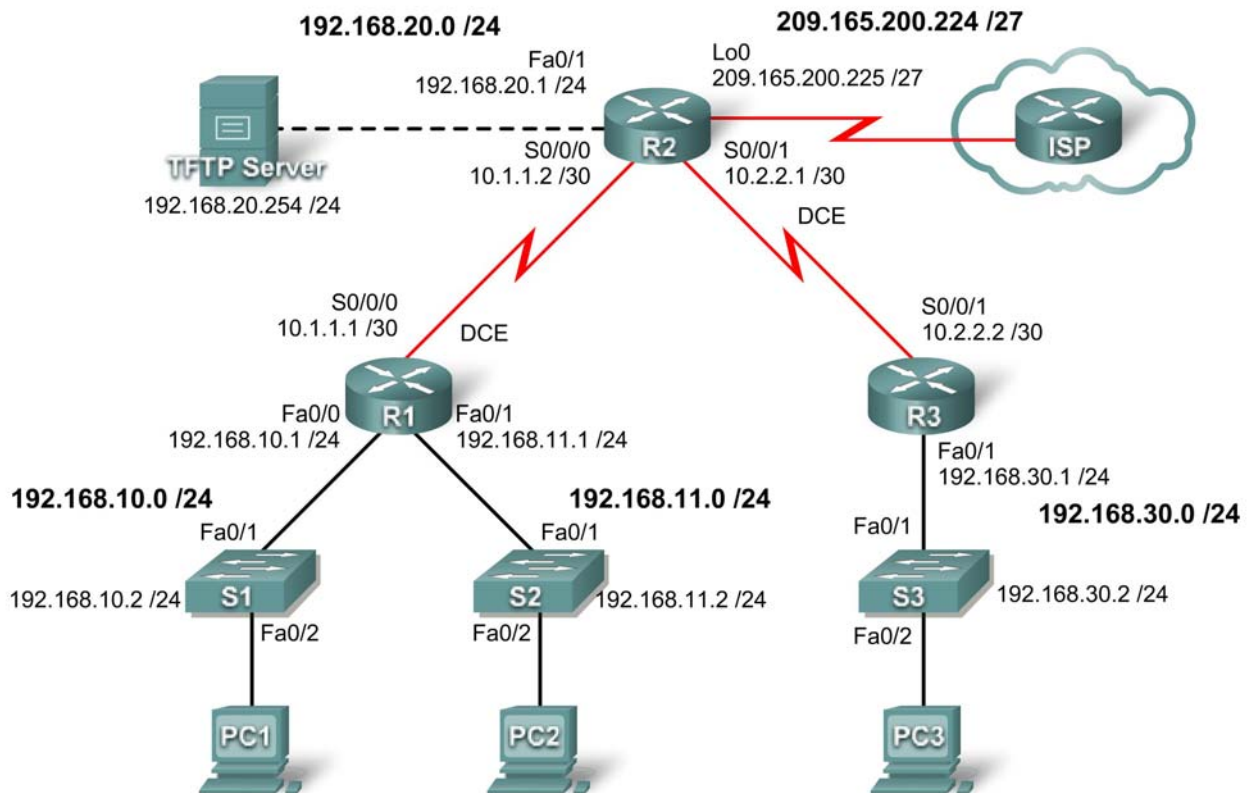


### 步骤 2. 保存该记录文档。

在接下来的练习 8.4.6 “网络故障排除”中将会用到您记录的拓扑图和地址表。

### 练习 8.3.7: 故障排除角色扮演 (教师版)

## 拓扑图



## 学习目标

- 构建网络
- 测试网络
- 破坏网络
- 排查问题
- 收集症状
- 修复问题
- 记录问题和解决方案。

## 场景

在本练习中，您和另外一位学生将构建拓扑图中的网络。您将配置 NAT、DHCP 和 OSPF，然后检验连通性。在网络完全正常工作之后，一个学生将故意制造一些故障。另外一个学生将使用其故障排除技能来隔离并解决问题。学生互换角色，重复此过程。此练习在真实设备或 Packet Tracer 上进行。

## 任务 1：建立网络

步骤 1：根据拓扑图进行网络布线。

步骤 2：配置 NAT、DHCP 和 OSPF

## 任务 2：测试网络

步骤 1：确认端到端连接正常。

步骤 2：检验 DHCP 和 NAT 是否正常工作。

步骤 3：通过使用 **show** 和 **debug** 命令了解每台设备。

## 任务 3：破坏网络

一个学生破坏配置，另一个学生根据需要可离开或留在教室。破坏行为应当仅产生一项问题。整个思路是互助培养故障排除能力。创建多个问题会扩大所需的工作范围，这不是本实验的目的。本实验的目的是让您了解，在网络中，一个问题可能会引起多项变化。

## 任务 4：排查问题

回避的学生回到教室，询问另外一个学生问题的有关症状。提问由一般性问题开始，然后试着将问题的范围缩小。当被提问的学生感觉已经提供了足够的信息时，便可以结束提问过程。

## 任务 5：从可疑设备收集症状

使用各种 **show** 和 **debug** 命令开始收集症状。在不得已时才能使用 **show running-config** 命令。

## 任务 6：纠正问题

纠正配置，测试解决方案。

## 任务 7：记录问题和解决方案。

两个学生都应当在自己的日志中记录问题和解决方案。

## 任务 8：交换角色，重新开始。

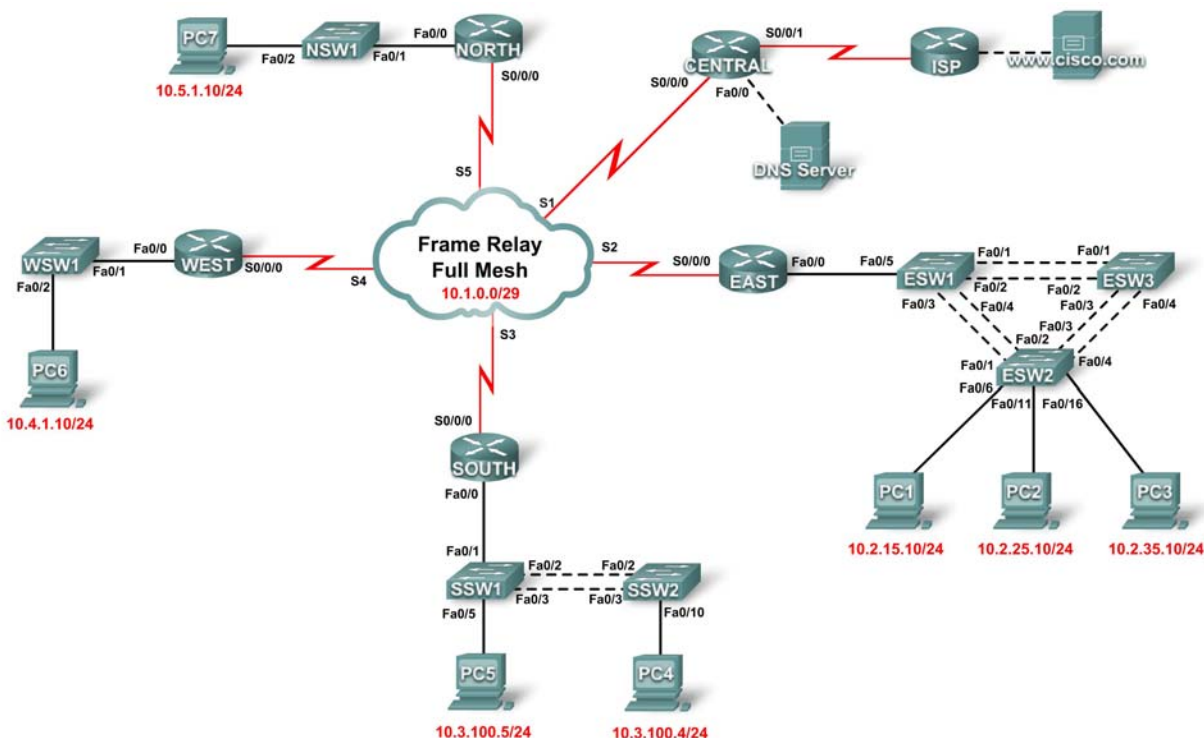
现在学生应当交换角色，重新开始整个过程。

## 任务 9：实验后清理

清除配置，然后重新启动路由器。拆下电缆并放回存放处。对于正常情况下连接到其它网络（例如学校 LAN 或 Internet）的 PC 主机，请重新连接相应的电缆并恢复原有的 TCP/IP 设置。

## PT 练习 8.4.6: 网络故障排除 (教师版)

拓扑图 (仅供教师使用)



地址表 (仅供教师使用)

设备	接口	IP 地址	子网掩码	默认网关
PC1	网卡	10.2.15.10	255.255.255.0	10.2.15.1
PC2	网卡	10.2.25.10	255.255.255.0	10.2.25.1
PC3	网卡	10.2.35.10	255.255.255.0	10.2.35.1
PC4	网卡	10.3.100.4	255.255.255.0	10.3.100.1
PC5	网卡	10.3.100.5	255.255.255.0	10.3.100.1
PC6	网卡	10.4.1.10	255.255.255.0	10.4.1.1
PC7	网卡	10.5.1.10	255.255.255.0	10.5.1.1
DNS Server	网卡	10.1.100.2	255.255.255.0	10.1.100.1
CENTRAL	S0/0/0	10.1.0.1	255.255.255.0	不适用
CENTRAL	S0/0/1	209.165.201.2	255.255.255.252	不适用
CENTRAL	Fa0/0	10.1.100.1	255.255.255.0	不适用

设备	接口	IP 地址	子网掩码	默认网关
EAST	S0/0/0	10.1.0.2	255.255.255.0	不适用
EAST	Fa0/0.5	10.2.5.1	255.255.255.0	不适用
EAST	Fa0/0.15	10.2.15.1	255.255.255.0	不适用
EAST	Fa0/0.25	10.2.25.1	255.255.255.0	不适用
EAST	Fa0/0.35	10.2.35.1	255.255.255.0	不适用
ESW1	VLAN 5	10.2.5.21	255.255.255.0	10.2.5.1
ESW2	VLAN 5	10.2.5.22	255.255.255.0	10.2.5.1
ESW3	VLAN 5	10.2.5.23	255.255.255.0	10.2.5.1
SOUTH	S0/0/0	10.1.0.3	255.255.255.0	不适用
SOUTH	Fa0/0.100	10.3.100.1	255.255.255.0	不适用
SOUTH	Fa0/0.105	10.3.105.1	255.255.255.0	不适用
SSW1	VLAN 105	10.3.105.21	255.255.255.0	10.3.105.1
SSW2	VLAN 105	10.3.105.22	255.255.255.0	10.3.105.1
WEST	S0/0/0	10.1.0.4	255.255.255.0	不适用
WEST	Fa0/0	10.4.1.1	255.255.255.0	不适用
WSW1	无	无	无	无
NORTH	S0/0/0	10.1.0.5	255.255.255.0	不适用
NORTH	Fa0/0	10.5.1.1	255.255.255.0	不适用
NSW1	无	无	无	无

## 学习目标

- 收集网络文档
- 测试连通性
- 收集数据并实施解决方案
- 测试连通性

## 简介

在本练习中，您将解决通过 XYZCORP 路由的 PC 之间的连通性问题。当您的进度达到 100%，而所有 PC 能互相 ping 通且能 ping 通 www.cisco.com 服务器时，本练习即完成。您实施的任何解决方案都必须遵循拓扑图。

## 任务 1：收集网络文档

要成功完成本练习，需要用到在本章前面部分所完成的“PT 练习 8.1.2：网络的发现与记录”的最终文档。该文档中记录了准确的拓扑图和地址表。如果您没有该文档，请向您的教师索取正确版本。

## 任务 2：测试连通性

本练习结束时，所有的 PC 之间以及 PC 与 [www.cisco.com](http://www.cisco.com) 服务器之间都应达到完全连通。连通性故障排除的第一步是在以下设备间执行 ping 命令：

- PC 至 [www.cisco.com](http://www.cisco.com) 服务器
- PC 至 PC
- PC 至默认网关

有成功的 ping 操作吗？哪些失败了？

---

---

---

---

所有 PC 之间均无法彼此 ping 通，PC 也无法 ping 通 [www.cisco.com](http://www.cisco.com) 服务器。只有 PC4、PC5、PC6 和 PC7 可以 ping 通它们各自的默认网关。

## 任务 3：收集数据并实施解决方案

**步骤 1. 选取一台 PC 开始收集数据。**

任意选择一台 PC，然后通过测试该 PC 与默认网关的连通性来收集数据。您还可以使用 **tracert** 找出存在连通性故障的位置。

**步骤 2. Telnet 至默认网关，继续收集数据。**

如果您选择的 PC 无法与其默认网关连通，请另外选择一台 PC，以便从不同的方向找出问题所在。

如果您通过默认网关成功建立连接，请使用 **cisco** 口令登录。

**步骤 3. 使用故障排除工具检验配置。**

在默认网关路由器上，使用故障排除工具检验该配置是否与您记录的信息一致。请记住，除了检查路由器，还应检查交换机。务必要确认以下各项：

- 编址信息
- 接口是否激活
- 封装
- 路由
- VLAN 配置
- 是否存在双工或速率不匹配问题
- VTP 操作

发现 PC 连通性问题的症状后，将这些症状记录在下一步的空白处。

#### 步骤 4. 记录网络问题症状和可行的解决方案。

[illegible]

**教师注意事项：**下面只介绍了一种供学生循序渐进地进行本练习的方式。学生可以从 PC4、PC6 或 PC7 着手。在本参考答案中，我们是从 PC4 着手的。

PC1、PC2、PC3 和 PC5 都无法访问默认网关，因此只能从其它方向着手排查这些 PC 之间的连通性故障。

**问题 1：**从 PC4 可以访问默认网关 SOUTH。Telnet 至 SOUTH，然后检查路由表。您会看到 SOUTH 只有直接相连的路由，因此使用 **show protocols** 命令或 **show ip interface brief** 命令来检验当前的接口配置。仔细检查 IP 地址后发现 S0/0/0 地址出错。该地址应当是 10.1.0.3，但当前却是 10.0.1.3。执行 **show ip protocols** 命令后表明 SOUTH 上的 RIP 配置并无问题。

**解决方案 1：**为 SOUTH 上的 S0/0/0 接口配置正确的 IP 地址。

**问题 2：**待 RIP 在 SOUTH 上收敛后，使用 **show ip route** 命令进一步收集潜在问题的信息。SOUTH 有直接相连的路由，但只有两条 RIP 路由。缺失的路由包括 EAST 对应的四个 VLAN、WEST LAN 以及 NORTH LAN。可以 ping 通 EAST，因此 telnet 至 EAST。由于 SOUTH 不能从 EAST 收到路由，因此用 **show ip protocols** 命令检查一下 EAST 的 RIP 配置。EAST 会收发 RIP 更新信息并通告正确的网络。但是，网络自动总结功能目前是有效的。因此，EAST 在 RIP 定期更新中仅发送有类 10.0.0.0/8 网络。

**解决方案 2：**用 **no auto-summary** 命令配置 EAST。

**问题 3：**在 EAST 上检查 PC1、PC2 和 PC3 之间的连通性问题。用 **show ip interface brief** 命令和 **show protocols** 命令检查 VLAN 子接口的 IP 配置。没有发现任何问题，接下来 ping ESW1，然后 telnet 至 ESW1。由于 ESW1 并非接入层交换机，因此检查一下 VLAN 配置（用 **show vlan brief** 命令）和 VTP 状态（用 **show vtp status** 命令）。所有 VLAN 都正常存在。该交换机也已正确配置为 XYZCORP 域的 VTP 服务器。运行 **show vtp password** 命令表明 ESW1 使用的是正确的口令，即 **eastbranch**。首先 ping ESW2，然后 telnet 至 ESW2。用 **show ip interface brief** 命令检查各接口的第 1 层和第 2 层是否存在任何问题。结果发现，PC1、PC2 和 PC3 连接着的接口，其接口状态和链路协议状态都为“up”。检查 VLAN 配置和 VTP 状态。ESW2 的 VLAN 并非全部正确，VTP 状态表明 ESW2 属于空域。ESW2 使用的 VTP 口令是正确的。

**解决方案 3：**为 ESW2 配置正确的 VTP 域名，即 XYZCORP。待 STP 收敛后，PC1、PC2 和 PC3 应该能彼此 ping 通。

**问题 4：**退回到 EAST，然后检查路由表。WEST LAN 和 NORTH LAN 缺少路由。通过 ping WEST 和 NORTH 路由器的串行接口，检测到达这些路由器的连通性。无法 ping 通 WEST，但能 ping 通 NORTH。Telnet 至 NORTH。在 NORTH 上显示路由表。您将看到 NORTH 没有 RIP 路由，因此使用 **show ip protocols** 命令来检查 RIP 路由。执行该命令后并未产生任何输出，据此可以判定要么是 RIP 根本没有配置，要么就是 RIP 配置错误。使用 **show run** 命令检查 RIP 命令。RIP 缺少 **network** 命令。

**解决方案 4：**用 RIP 命令 **network 10.0.0.0** 配置 NORTH。

**问题 5：**待 RIP 收敛后，检查 NORTH 路由表。WEST LAN 仍然缺失。由于 ping WEST 失败，改从 PC6 访问 WEST。首先，ping 默认网关地址，然后 telnet 至 WEST。显示路由表。您将看到路由表中只有 Fa0/0 网络。使用 **show ip interface brief** 命令检查接口配置。S0/0/0 接口在物理上为“up”状态，但数据链路层为“down”状态。进一步用 **show interface** 命令检查 S0/0/0 接口。您会发现它的封装设置为 HDLC，而不是帧中继。

**解决方案 5：**用 **encapsulation frame-relay** 命令将 S0/0/0 接口的封装从 HDLC 更改为帧中继。现在所有 PC 之间应该能互相 ping 通。

**问题 6：**PC 仍然无法 ping 通 www.cisco.com 服务器。从任意一台设备开始测试连通性，然后 telnet 至 CENTRAL。使用 **show ip interface brief** 命令检查接口状态。S0/0/1 接口状态为 **administratively down**（管理性关闭）。

**解决方案 6：**用 **no shutdown** 命令激活 CENTRAL 上的 S0/0/1 接口。

**问题 7：**PC 仍然无法 ping 通 www.cisco.com 服务器。不过，PC 能 ping 通 DNS 服务器。这可能是由于 CENTRAL 配置或 ISP 配置有问题。由于您无法访问 ISP 路由器，请检查 CENTRAL 上的配置。**show run** 命令表明 CENTRAL 使用的是 NAT。该配置缺少能将 NAT 池绑定到访问列表的 NAT 语句。

**解决方案 7：**用 **ip nat inside source list 1 pool XYZCORP overload** 命令配置 CENTRAL。



**步骤 5.** 根据上一步的解决方案做出修改。

## 任务 4：测试连通性

**步骤 1. 测试 PC 连通性。**

现在所有 PC 之间应该能互相 ping 通，并能从 PC ping 通 [www.cisco.com](http://www.cisco.com) 服务器。如果更改了任何 IP 配置，请重新执行 ping 操作，因为之前的 ping 使用的是旧 IP 地址。

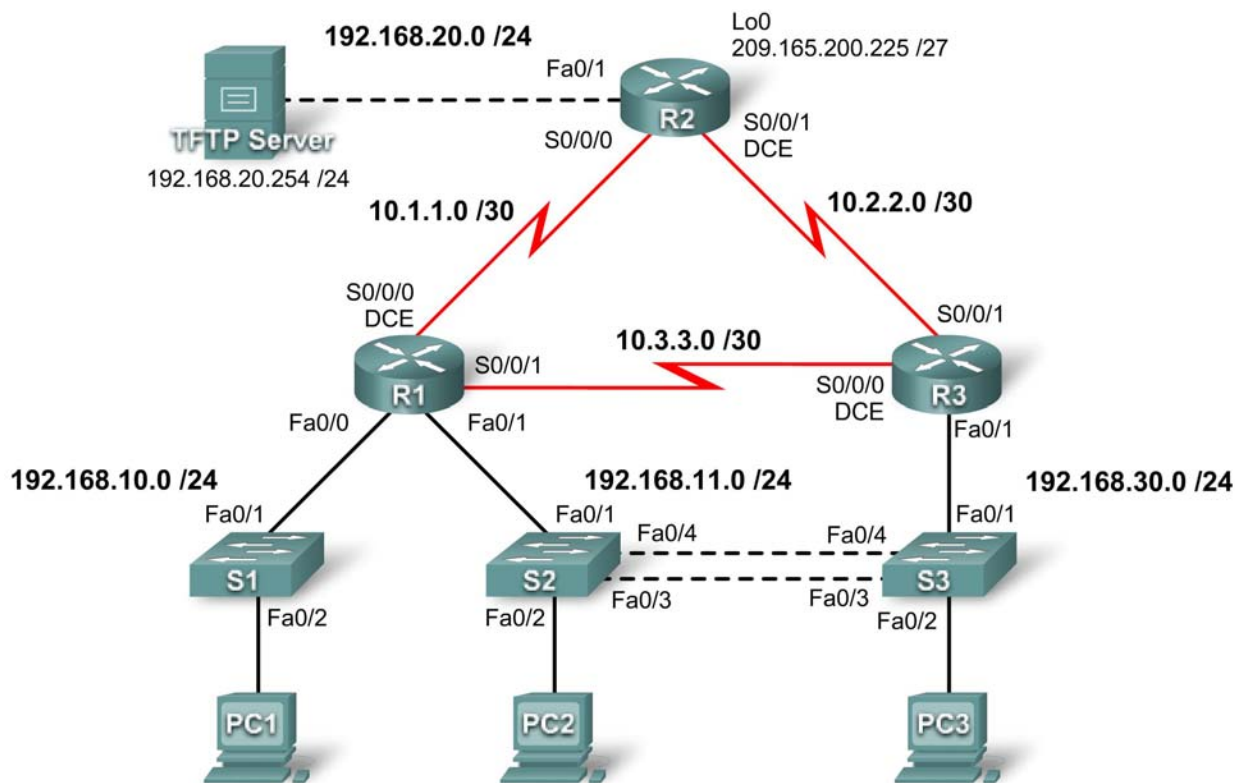
如果各台 PC 之间或 PC 与服务器之间仍存在连通性问题，请返回任务 3 继续执行故障排除。

**步骤 2. 检查结果。**

完成比例应为 100%。如果不是，请返回任务 3 继续执行故障排除并实施您建议的解决方案。您将无法单击 **Check Results**（检查结果），因此也看不到哪些必需组件尚未完成。

## PT 练习 8.5.1：企业网络故障排除 1（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/0	192.168.10.1	255.255.255.0	不适用
	Fa0/1	192.168.11.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
	S0/0/1	10.3.3.1	255.255.255.252	不适用
R2	Fa0/1	192.168.20.1	255.255.255.0	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

地址表接下一页

地址表（续）

<b>R3</b>	<b>Fa0/1</b>	不适用	不适用	不适用
	<b>Fa0/1.11</b>	192.168.11.3	255.255.255.0	不适用
	<b>Fa0/1.30</b>	192.168.30.1	255.255.255.0	不适用
	<b>S0/0/0</b>	10.3.3.2	255.255.255.252	不适用
	<b>S0/0/1</b>	10.2.2.2	255.255.255.252	不适用
<b>S1</b>	<b>VLAN10</b>	DHCP	255.255.255.0	不适用
<b>S2</b>	<b>VLAN11</b>	192.168.11.2	255.255.255.0	不适用
<b>S3</b>	<b>VLAN30</b>	192.168.30.2	255.255.255.0	不适用
<b>PC1</b>	网卡	DHCP	DHCP	DHCP
<b>PC2</b>	网卡	192.168.11.10	255.255.255.0	192.168.11.1
<b>PC3</b>	网卡	192.168.30.10	255.255.255.0	192.168.30.1
<b>TFTP Server</b>	网卡	192.168.20.254	255.255.255.0	192.168.20.1

## 学习目标

- 查找并纠正所有网络错误
- 检查是否完全符合要求
- 记录纠正后的网络

## 场景

前面已要求您纠正公司网络中的配置错误。在本练习中，请不要对任何控制台线路使用登录保护或口令保护功能，以免网络连接意外中断。请在本实验中统一使用 **ciscoccna** 口令。

注：由于本练习是综合性的，您需要使用从前面材料中获得的所有知识和故障排除技术，才能成功完成本练习。

## 要求

- S2 是 VLAN 11 的生成树根，而 S3 是 VLAN 30 的生成树根。
- S3 为 VTP 服务器，并以 S2 作为客户端。
- R1 和 R2 之间的串行链路为帧中继。
- R2 和 R3 之间的串行链路使用 HDLC 封装。
- R1 和 R3 之间的串行链路使用 PPP。
- R1 和 R3 之间的串行链路使用 CHAP 进行身份验证。
- 由于 R2 是 Internet 边缘路由器，因此它必须具有安全的登录过程。
- 所有 vty 线路（属于 R2 的 vty 线路除外）都只允许来自拓扑图所示子网的连接，不包括公有地址。
- 对于所有未连接到其它路由器的链路，应当防止出现源 IP 地址欺骗。
- R3 绝不能通过直接相连的串行链路 telnet 至 R2。
- R3 能通过快速以太网端口 0/0 访问 VLAN 11 和 VLAN 30。
- TFTP 服务器应该不能获得源地址位于子网之外的任何流量。所有设备均能访问 TFTP 服务器。
- 位于 192.168.10.0 子网的所有设备必须能够通过 R1 上的 DHCP 获得自己的 IP 地址。
- 必须能从每台设备访问拓扑图中显示的所有地址。

## 任务 1：查找并纠正所有网络错误

```
R1
!
router rip
  no passive-interface FastEthernet0/0
  no passive-interface FastEthernet0/1
  no passive-interface Serial0/0/0
  no passive-interface Serial0/0/1
!

R2
!
interface Serial0/0/0
  ip address 10.1.1.2 255.255.255.252
  frame-relay map ip 10.1.1.2 201
!
interface Serial0/0/1
  ip address 10.2.2.1 255.255.255.252

S2
!
vtp mode client
!

S3
!
vtp domain CCNA_Troubleshooting
!
vlan 11
vlan 30
!
interface FastEthernet0/1
  switchport trunk allowed vlan 11,30
!
interface FastEthernet0/2
  switchport access vlan 30
!
```

## 任务 2：检查是否完全符合要求

由于时间有限，无法针对每个主题执行故障排除，因此只针对一部分主题设置了故障。但是，为了巩固和强化故障排除技巧，您应当确保达到每个要求。为此，请提供检验每个要求完成情况的命令示例（例如 **show** 命令或 **debug** 命令）。

此处并未给出全部命令示例，因为有很多种方式可以检验是否符合要求。下面是要求 1 的命令示例。

**S2#show spanning-tree**

```
VLAN0011
  Spanning tree enabled protocol ieee
  Root ID    Priority      24587
             Address      00E0.A380.CD1C
             This bridge is the root
             Hello Time   2 sec   Max Age 20 sec   Forward Delay 15 sec
  Bridge ID  Priority      24587 (priority 24576 sys-id-ext 11)
             Address      00E0.A380.CD1C
             Aging Time   300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/3	Desg	FWD	19	128.3	Shr
Fa0/1	Desg	FWD	19	128.3	Shr
Fa0/4	Desg	FWD	19	128.3	Shr
Fa0/2	Desg	FWD	19	128.3	Shr

### 任务 3：记录纠正后的网络

```
R1
!
hostname R1
!
!
enable secret ciscoccna
!
username R3 password 0 ciscoccna
username ccna password 0 ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no keepalive
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
```

```
network 10.0.0.0
network 192.168.10.0
network 192.168.11.0
no auto-summary
!
ip classless
!
ip access-list standard Anti-spoofing
permit 192.168.10.0 0.0.0.255
deny any
ip access-list standard VTY
permit 10.0.0.0 0.255.255.255
permit 192.168.10.0 0.0.0.255
permit 192.168.11.0 0.0.0.255
permit 192.168.20.0 0.0.0.255
permit 192.168.30.0 0.0.0.255
!
!
ip dhcp pool Access1
network 192.168.10.0 255.255.255.0
default-router 192.168.10.1
!
line con 0
line vty 0 4
access-class VTY in
login
!
!
end
```

```
R2
!
hostname R2
!
!
enable secret ciscocna
!
username ccna password 0 ciscocna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
shutdown
!
interface FastEthernet0/1
ip address 192.168.20.1 255.255.255.0
ip access-group Anti-spoofing in
ip access-group TFTP out
ip nat outside
duplex auto
speed auto
!
```

```
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
 no keepalive
 ip nat inside
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
 ip nat inside
 clock rate 4000000
!
interface Loopback0
 ip address 209.165.200.245 255.255.255.224
 ip access-group private in
!
interface Vlan1
 no ip address
 shutdown
!
router rip
 version 2
 passive-interface default
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.0.0.0
 network 192.168.20.0
 default-information originate
 no auto-summary
!
ip nat inside source list NAT interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard Anti-spoofing
 permit 192.168.20.0 0.0.0.255
 deny any
ip access-list standard NAT
 permit 10.0.0.0 0.255.255.255
 permit 192.168.0.0 0.0.255.255
ip access-list standard private
 deny host 127.0.0.1
 deny 10.0.0.0 0.255.255.255
 deny 172.0.0.0 0.31.255.255
 deny 192.168.0.0 0.0.255.255
 permit any
ip access-list extended R3-telnet
 deny tcp host 10.2.2.2 host 10.2.2.1 eq telnet
 deny tcp host 10.3.3.2 host 10.2.2.1 eq telnet
 deny tcp host 192.168.11.3 host 10.2.2.1 eq telnet
 deny tcp host 192.168.30.1 host 10.2.2.1 eq telnet
 permit ip any any
ip access-list standard TFTP
 permit 192.168.20.0 0.0.0.255
```

```
!  
!  
!  
line con 0  
line vty 0 4  
    login  
!  
!  
end  
  
R3  
!  
hostname R3  
!  
!  
enable secret 5 $1$mERr$NY2X7xBCS5tAN/W1NAs2c1  
!  
username R1 password 0 ciscocna  
username ccna password 0 ciscocna  
!  
no ip domain-lookup  
!  
!  
interface FastEthernet0/0  
    no ip address  
    duplex auto  
    speed auto  
    shutdown  
!  
interface FastEthernet0/1  
    no ip address  
    duplex auto  
    speed auto  
!  
interface FastEthernet0/1.11  
    encapsulation dot1Q 11  
    ip address 192.168.11.3 255.255.255.0  
!  
interface FastEthernet0/1.30  
    encapsulation dot1Q 30  
    ip address 192.168.30.1 255.255.255.0  
    ip access-group Anti-spoofing in  
!  
interface Serial0/0/0  
    ip address 10.3.3.2 255.255.255.252  
    encapsulation ppp  
    ppp authentication chap  
    clock rate 4000000  
!  
interface Serial0/0/1  
    ip address 10.2.2.2 255.255.255.252  
!  
interface Vlan1  
    no ip address  
    shutdown  
!
```



```
router rip
  version 2
  passive-interface default
  no passive-interface Serial0/0/0
  no passive-interface Serial0/0/1
  no passive-interface FastEthernet0/1.11
  no passive-interface FastEthernet0/1.30
  network 10.0.0.0
  network 192.168.11.0
  network 192.168.30.0
  no auto-summary
!
ip classless
!
ip access-list standard Anti-spoofing
  permit 192.168.30.0 0.0.0.255
  deny any
ip access-list standard VTY
  permit 10.0.0.0 0.255.255.255
  permit 192.168.10.0 0.0.0.255
  permit 192.168.11.0 0.0.0.255
  permit 192.168.20.0 0.0.0.255
  permit 192.168.30.0 0.0.0.255
!
!
!
line con 0
line vty 0 4
  login
!
!
end
```

```
S1
!
hostname S1
!
enable secret ciscocna
!
no ip domain-lookup
!
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscocna
!
!
vlan 10
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
```

```
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10
  ip address dhcp
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end
```

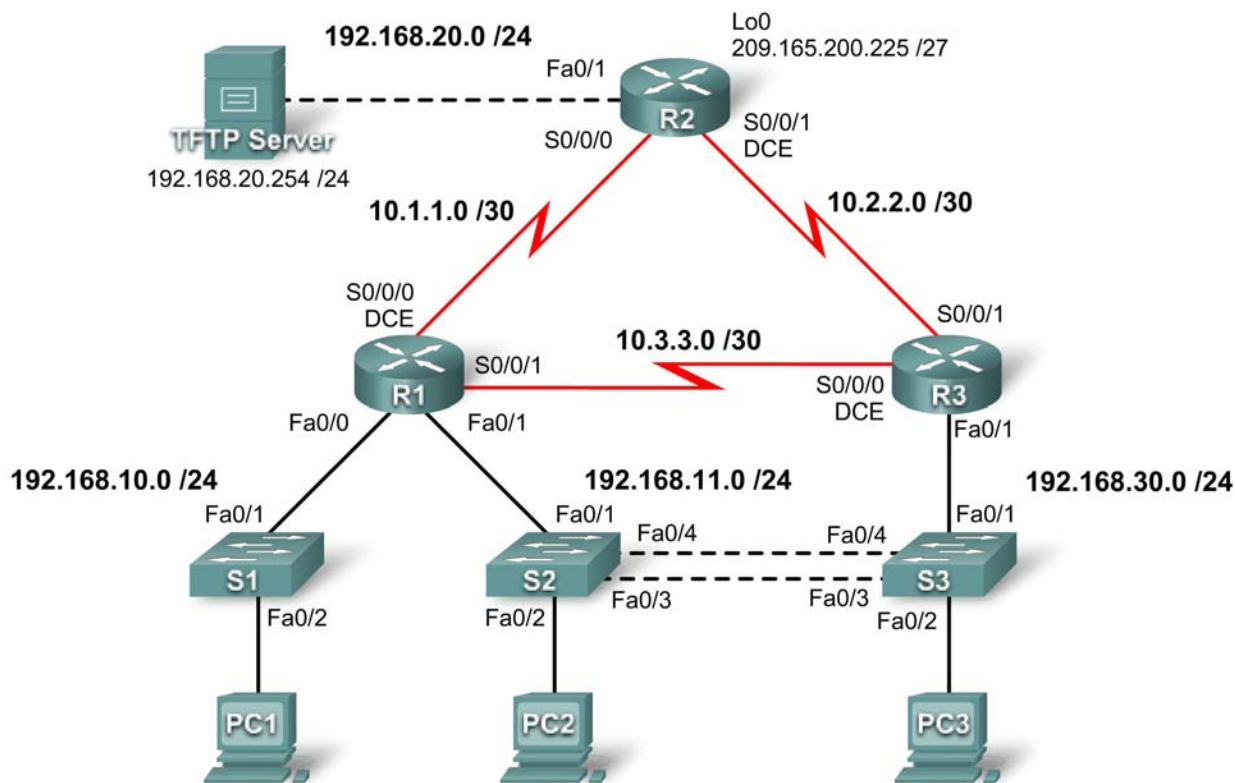
```
S2
!
hostname S2
!
enable secret ciscocna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 24576
spanning-tree vlan 30 priority 28672
!
interface FastEthernet0/1
  switchport access vlan 11
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 11
  switchport mode access
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan11
  ip address 192.168.11.2 255.255.255.0
!
line con 0
!
```

```
line vty 0 4
  login
line vty 5 15
  login
!
!
end

S3
!
hostname S3
!
enable secret ciscocna
!
no ip domain-lookup
!
spanning-tree vlan 11 priority 28672
spanning-tree vlan 30 priority 24576
!
interface FastEthernet0/1
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan30
  ip address 192.168.30.2 255.255.255.0
!
ip default-gateway 192.168.30.1
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end
```

## PT 练习 8.5.2：企业网络故障排除 2（教师版）

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/0	192.168.10.1	255.255.255.0	不适用
	Fa0/1	192.168.11.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
	S0/0/1	10.3.3.1	255.255.255.252	不适用
R2	Fa0/1	192.168.20.1	255.255.255.0	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

地址表接下一页

地址表（续）

<b>R3</b>	<b>Fa0/1</b>	不适用	不适用	不适用
	<b>Fa0/1.11</b>	192.168.11.3	255.255.255.0	不适用
	<b>Fa0/1.30</b>	192.168.30.1	255.255.255.0	不适用
	<b>S0/0/0</b>	10.3.3.2	255.255.255.252	不适用
	<b>S0/0/1</b>	10.2.2.2	255.255.255.252	不适用
<b>S1</b>	<b>VLAN10</b>	DHCP	255.255.255.0	不适用
<b>S2</b>	<b>VLAN11</b>	192.168.11.2	255.255.255.0	不适用
<b>S3</b>	<b>VLAN30</b>	192.168.30.2	255.255.255.0	不适用
<b>PC1</b>	网卡	DHCP	DHCP	DHCP
<b>PC2</b>	网卡	192.168.11.10	255.255.255.0	192.168.11.1
<b>PC3</b>	网卡	192.168.30.10	255.255.255.0	192.168.30.1
<b>TFTP Server</b>	网卡	192.168.20.254	255.255.255.0	192.168.20.1

## 学习目标

- 查找并纠正所有网络错误
- 检查是否完全符合要求
- 记录纠正后的网络

## 场景

在本练习中，请不要对任何控制台线路使用登录保护或口令保护功能，以免网络连接意外中断。请在本练习中统一使用 **ciscocna** 口令。

注：由于本练习是综合性的，您需要使用从前面材料中获得的所有知识和故障排除技术，才能成功完成本练习。

## 要求

- S2 是 VLAN 11 的生成树根，而 S3 是 VLAN 30 的生成树根。
- S3 为 VTP 服务器，并以 S2 作为客户端。
- R1 和 R2 之间的串行链路为帧中继。
- R2 和 R3 之间的串行链路使用 HDLC 封装。
- R1 和 R3 之间的串行链路使用 CHAP 进行身份验证。
- 由于 R2 是 Internet 边缘路由器，因此它必须具有安全的登录过程。
- 所有 vty 线路（属于 R2 的 vty 线路除外）都只允许来自拓扑图所示子网的连接，不包括公有地址。
- 对于所有未连接到其它路由器的链路，应当防止出现源 IP 地址欺骗。
- 必须以安全的方式使用路由协议。在本场景中使用 EIGRP。
- R3 绝不能通过直接相连的串行链路 telnet 至 R2。
- R3 能通过快速以太网端口 0/1 访问 VLAN 11 和 VLAN 30。

- TFTP 服务器应该不能获得源地址位于子网之外的任何流量。所有设备均能访问 TFTP 服务器。
- 位于 192.168.10.0 子网的所有设备必须能够通过 R1 上的 DHCP 获得自己的 IP 地址。其中包括 S1 设备。
- 必须能从每台设备访问拓扑图中显示的所有地址。

### 任务 1：查找并纠正所有网络错误

如需要，请将时钟频率设置为 **4000000**，VLAN 优先级设置为 **24576**。

```
R1
!
no username R2
username R3 password ciscocna
! 用户名输入错误会阻碍 R3 通过 CHAP 完成身份验证。
!
interface FastEthernet0/0
  no ip access-group Anti-spoofing out
  ip access-group Anti-spoofing in
! 应用访问列表的方向出错。这种常见的
! 错误会阻碍所有流量从接口上送出。
!
interface Serial0/0/1
  ip address 10.3.3.1 255.255.255.252
! 此子网配置错误的原因很可能是因为 /24 子网出现得比较多
! （所以此处也顺手误写成了 /24）。
!

R2
!
interface Serial0/0/1
  ip access-group R3-telnet in
! 经常出现的问题是，创建了访问列表但是未应用于接口，
! 这就导致 ACL 无法发挥作用。

R3
!
interface Serial0/0/0
  clock rate 4000000
! 忘记对 DCE 接口设置时钟频率。
  ppp authentication chap
! 错误地配置为 PAP 而不是 CHAP。
!
router eigrp 10
  no passive-interface FastEthernet0/1.11
  no passive-interface FastEthernet0/1.30
  no passive-interface Serial0/0/0
  no passive-interface Serial0/0/1
! 忘记输入这些命令会造成所有接口都发送 EIGRP。
!
ip route 0.0.0.0 0.0.0.0 10.2.2.1
! 忘记输入到达 Internet 网关的默认路由，导致
! 该设备无法到达 Internet 网关。
!
```

```
interface FastEthernet0/1.30
 ip access-group Anti-spoofing in
! 访问列表输入错误。它现在引用不存在的 ACL，
! 所以流量将被丢弃，因为每个 ACL 末尾都有隐式 "deny all" ！ 语句。
!

S3
!
spanning-tree vlan 30 priority 24576
!
```

## 任务 2：检查是否完全符合要求

由于时间有限，无法针对每个主题执行故障排除，因此只针对一部分主题设置了故障。但是，为了巩固和强化故障排除技巧，您应当确保达到每个要求。为此，请提供检验每个要求完成情况的命令示例（例如 **show** 命令或 **debug** 命令）。

此处并未给出全部命令示例，因为有很多种方式可以检验是否符合要求。下面是要求 1 的命令示例。

S2#**show spanning-tree**

```
VLAN0011
  Spanning tree enabled protocol ieee
  Root ID    Priority      24587
             Address      00E0.A380.CD1C
             This bridge is the root
             Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority      24587 (priority 24576 sys-id-ext 11)
             Address      00E0.A380.CD1C
             Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/4	Desg	FWD	19	128.3	Shr
Fa0/1	Desg	FWD	19	128.3	Shr
Fa0/2	Desg	FWD	19	128.3	Shr
Fa0/3	Desg	FWD	19	128.3	Shr

S3#**show spanning-tree**

<省略部分输出>

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority      24606
             Address      0050.0FCE.8E14
             This bridge is the root
             Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority      24606 (priority 24576 sys-id-ext 30)
             Address      0050.0FCE.8E14
             Aging Time 300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/2	Desg	FWD	19	128.3	Shr
Fa0/3	Desg	FWD	19	128.3	Shr
Fa0/1	Desg	FWD	19	128.3	Shr
Fa0/4	Desg	FWD	19	128.3	Shr

### 任务 3：记录纠正后的网络

```
R1
!
hostname R1
!
!
enable secret ciscoccna
!
username R3 password ciscoccna
username ccna password ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip access-group Anti-spoofing in
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no keepalive
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Vlan1
 no ip address
 shutdown
!
router eigrp 10
 passive-interface default
 no passive-interface FastEthernet0/0
 no passive-interface FastEthernet0/1
 no passive-interface Serial0/0/0
 no passive-interface Serial0/0/1
 network 10.1.1.0 0.0.0.255
 network 10.3.3.0 0.0.0.255
 network 192.168.10.0
 network 192.168.11.0
 network 10.1.1.0 0.0.0.3
 network 10.3.3.0 0.0.0.3
 no auto-summary
!
ip classless
```



```
ip route 0.0.0.0 0.0.0.0 10.1.1.2
!
ip access-list standard Anti-spoofing
  permit 192.168.10.0 0.0.0.255
  deny any
ip access-list standard VTY
  permit 10.0.0.0 0.255.255.255
  permit 192.168.10.0 0.0.0.255
  permit 192.168.11.0 0.0.0.255
  permit 192.168.20.0 0.0.0.255
  permit 192.168.30.0 0.0.0.255
!
!
ip dhcp pool Access1
  network 192.168.10.0 255.255.255.0
  default-router 192.168.10.1
!
line con 0
line vty 0 4
  access-class VTY in
  login
!
!
end

R2
!
hostname R2
!
!
enable secret ciscoccna
!
username ccna password ciscoccna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
  no ip address
  duplex auto
  speed auto
  shutdown
!
interface FastEthernet0/1
  ip address 192.168.20.1 255.255.255.0
  ip access-group Anti-spoofing in
  ip access-group TFTP out
  ip nat outside
  duplex auto
  speed auto
!
interface Serial0/0/0
  ip address 10.1.1.2 255.255.255.252
  encapsulation frame-relay
  frame-relay map ip 10.1.1.1 201 broadcast
  frame-relay map ip 10.1.1.2 201
  no keepalive
```

```
ip nat inside
!
interface Serial0/0/1
ip address 10.2.2.1 255.255.255.252
ip access-group R3-telnet in
ip nat inside
clock rate 4000000
!
interface Loopback0
ip address 209.165.200.245 255.255.255.224
ip access-group private in
!
interface Vlan1
no ip address
shutdown
!
router eigrp 10
passive-interface default
no passive-interface Serial0/0/0
no passive-interface Serial0/0/1
network 10.1.1.0 0.0.0.3
network 10.2.2.0 0.0.0.3
network 192.168.20.0
no auto-summary
!
ip nat inside source list NAT interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard Anti-spoofing
permit 192.168.20.0 0.0.0.255
deny any
ip access-list standard NAT
permit 10.0.0.0 0.255.255.255
permit 192.168.0.0 0.0.255.255
ip access-list standard private
deny host 127.0.0.1
deny 10.0.0.0 0.255.255.255
deny 172.0.0.0 0.31.255.255
deny 192.168.0.0 0.0.255.255
permit any
ip access-list extended R3-telnet
deny tcp host 10.2.2.2 host 10.2.2.1 eq telnet
deny tcp host 10.3.3.2 host 10.2.2.1 eq telnet
deny tcp host 192.168.11.3 host 10.2.2.1 eq telnet
deny tcp host 192.168.30.1 host 10.2.2.1 eq telnet
permit ip any any
ip access-list standard TFTP
permit 192.168.20.0 0.0.0.255
!
!
!
line con 0
line vty 0 4
login
!
!
```

```
end
```

### R3

```
!  
hostname R3  
!  
!  
enable secret ciscocna  
!  
username R1 password ciscocna  
username ccna password ciscocna  
!  
no ip domain-lookup  
!  
!  
interface FastEthernet0/0  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1.11  
  encapsulation dot1Q 11  
  ip address 192.168.11.3 255.255.255.0  
!  
interface FastEthernet0/1.30  
  encapsulation dot1Q 30  
  ip address 192.168.30.1 255.255.255.0  
  ip access-group Anti-spoofing in  
!  
interface Serial0/0/0  
  ip address 10.3.3.2 255.255.255.252  
  encapsulation ppp  
  ppp authentication chap  
  clock rate 4000000  
!  
interface Serial0/0/1  
  ip address 10.2.2.2 255.255.255.252  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
router eigrp 10  
  network 10.3.3.0 0.0.0.3  
  network 10.2.2.0 0.0.0.3  
  network 192.168.11.0  
  network 192.168.30.0  
  no auto-summary  
!  
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 10.2.2.1
!
ip access-list standard Anti-spoofing
  permit 192.168.30.0 0.0.0.255
  deny any
ip access-list standard VTY
  permit 10.0.0.0 0.255.255.255
  permit 192.168.10.0 0.0.0.255
  permit 192.168.11.0 0.0.0.255
  permit 192.168.20.0 0.0.0.255
  permit 192.168.30.0 0.0.0.255
!
!
!
line con 0
line vty 0 4
  login
!
!
end
```

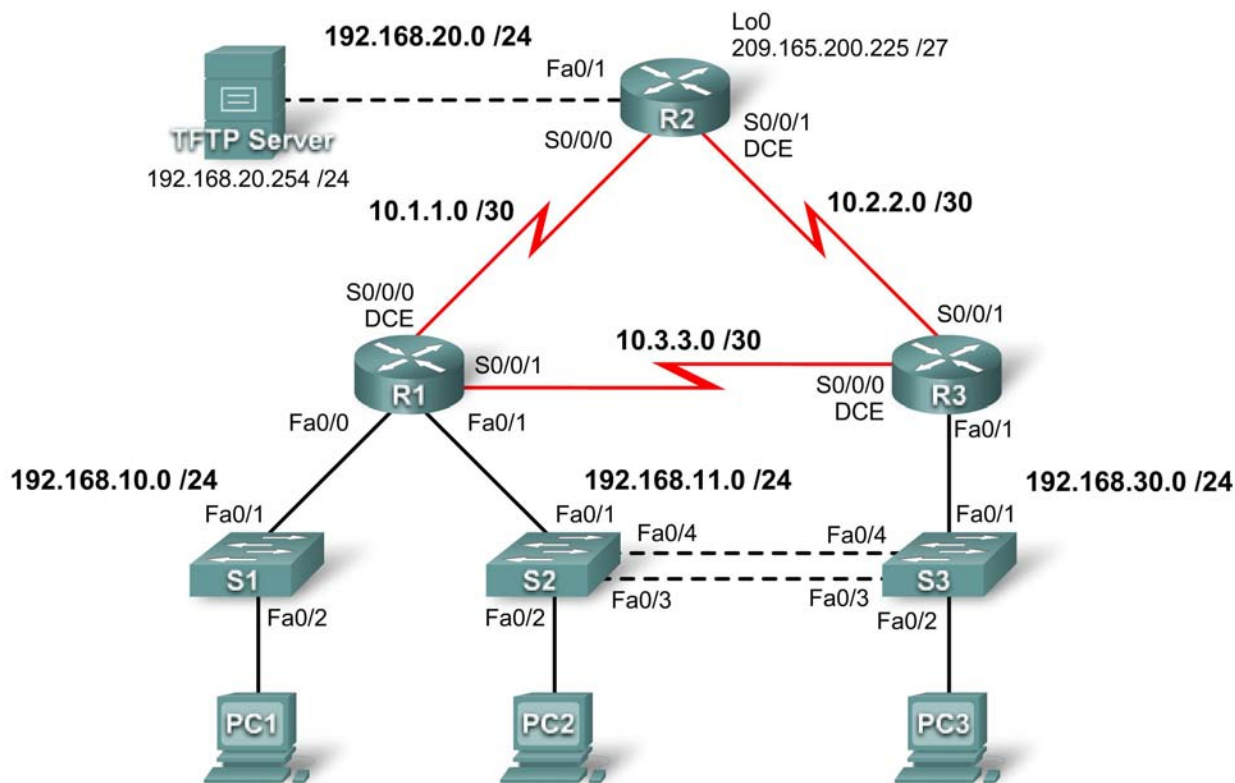
```
S1
!
hostname S1
!
enable secret ciscocna
!
no ip domain-lookup
!
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscocna
!
!
vlan 10
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan10
  ip address dhcp
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
```

```
!  
!  
end  
  
S2  
!  
hostname S2  
!  
enable secret ciscocna  
!  
no ip domain-lookup  
!  
spanning-tree vlan 11 priority 24576  
spanning-tree vlan 30 priority 28672  
!  
interface FastEthernet0/1  
    switchport access vlan 11  
    switchport mode access  
!  
interface FastEthernet0/2  
    switchport access vlan 11  
    switchport mode access  
!  
interface FastEthernet0/3  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface FastEthernet0/4  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface Vlan1  
    no ip address  
    shutdown  
!  
interface Vlan11  
    ip address 192.168.11.2 255.255.255.0  
!  
line con 0  
!  
line vty 0 4  
    login  
line vty 5 15  
    login  
!  
!  
end  
  
S3  
!  
hostname S3  
!  
enable secret ciscocna
```

```
!  
no ip domain-lookup  
!  
spanning-tree vlan 11 priority 28672  
spanning-tree vlan 30 priority 24576  
!  
interface FastEthernet0/1  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface FastEthernet0/2  
    switchport access vlan 30  
    switchport mode access  
!  
interface FastEthernet0/3  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface FastEthernet0/4  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface Vlan1  
    no ip address  
    shutdown  
!  
interface Vlan30  
    ip address 192.168.30.2 255.255.255.0  
!  
ip default-gateway 192.168.30.1  
!  
line con 0  
!  
line vty 0 4  
    login  
line vty 5 15  
    login  
!  
!  
end
```

## PT 练习 8.5.3: 企业网络故障排除 3 (教师版)

### 拓扑图



### 地址表

设备	接口	IP 地址	子网掩码	默认网关
R1	Fa0/0	192.168.10.1	255.255.255.0	不适用
	Fa0/1	192.168.11.1	255.255.255.0	不适用
	S0/0/0	10.1.1.1	255.255.255.252	不适用
	S0/0/1	10.3.3.1	255.255.255.252	不适用
R2	Fa0/1	192.168.20.1	255.255.255.0	不适用
	S0/0/0	10.1.1.2	255.255.255.252	不适用
	S0/0/1	10.2.2.1	255.255.255.252	不适用
	Lo0	209.165.200.225	255.255.255.224	209.165.200.226

地址表接下一页

地址表（续）

<b>R3</b>	<b>Fa0/1</b>	不适用	不适用	不适用
	<b>Fa0/1.11</b>	192.168.11.3	255.255.255.0	不适用
	<b>Fa0/1.30</b>	192.168.30.1	255.255.255.0	不适用
	<b>S0/0/0</b>	10.3.3.2	255.255.255.252	不适用
	<b>S0/0/1</b>	10.2.2.2	255.255.255.252	不适用
<b>S1</b>	<b>VLAN10</b>	DHCP	255.255.255.0	不适用
<b>S2</b>	<b>VLAN11</b>	192.168.11.2	255.255.255.0	不适用
<b>S3</b>	<b>VLAN30</b>	192.168.30.2	255.255.255.0	不适用
<b>PC1</b>	网卡	DHCP	DHCP	DHCP
<b>PC2</b>	网卡	192.168.11.10	255.255.255.0	192.168.11.1
<b>PC3</b>	网卡	192.168.30.10	255.255.255.0	192.168.30.1
<b>TFTP Server</b>	网卡	192.168.20.254	255.255.255.0	192.168.20.1

## 学习目标

- 查找并纠正所有网络错误
- 检查是否完全符合要求
- 记录纠正后的网络

## 场景

在本练习中，请不要对任何控制台线路使用登录保护或口令保护功能，以免意外注销。请在本练习中统一使用 **ciscocccna** 口令。

注：由于本练习是综合性的，您需要使用从前面材料中获得的所有知识和故障排除技术，才能成功完成本练习。

## 要求

- S2 是 VLAN 11 的生成树根，而 S3 是 VLAN 30 的生成树根。
- S3 为 VTP 服务器，并以 S2 作为客户端。
- R1 和 R2 之间的串行链路为帧中继。
- R2 和 R3 之间的串行链路使用 HDLC 封装。
- R1 和 R3 之间的串行链路使用 CHAP 进行身份验证。
- 由于 R2 是 Internet 边缘路由器，因此它必须具有安全的登录过程。
- 所有 vty 线路（属于 R2 的 vty 线路除外）都只允许来自拓扑图所示子网的连接，不包括公有地址。
- 对于所有未连接到其它路由器的链路，应当防止出现源 IP 地址欺骗。
- 必须以安全的方式使用路由协议。在本场景中使用 OSPF。
- R3 绝不能通过直接相连的串行链路 telnet 至 R2。
- R3 能通过快速以太网端口 0/1 访问 VLAN 11 和 VLAN 30。



- TFTP 服务器应该不能获得源地址位于子网之外的任何流量。所有设备均能访问 TFTP 服务器。
- 位于 192.168.10.0 子网的所有设备必须能够通过 R1 上的 DHCP 获得自己的 IP 地址。其中包括 S1 设备。
- 必须能从每台设备访问拓扑图中显示的所有地址。

### 任务 1：查找并纠正所有网络错误

如需要，请将时钟频率设置为 **4000000**，VLAN 优先级设置为 **24576**。

#### R1

```
!  
router ospf 1  
 network 10.3.3.0 0.0.0.3 area 0  
!
```

#### R2

```
interface FastEthernet0/1  
 ip nat outside  
 no shutdown  
!  
interface Serial0/0/0  
 ip nat inside  
 no shutdown  
!  
interface Serial0/0/1  
 clock rate 4000000  
 ip nat inside  
 no shutdown  
!  
router ospf 1  
 network 192.168.20.0 0.0.0.255 area 0  
 default-information originate  
!  
ip nat inside source list NAT interface FastEthernet0/1 overload  
!
```

#### R3

```
!  
interface FastEthernet0/1.11  
 encapsulation dot1Q 11  
! 输入的 VLAN 错误，致使子网位于错误的 VLAN 中。
```

#### S2

```
!  
interface FastEthernet0/3  
 switchport trunk native vlan 99  
interface FastEthernet0/4  
 switchport trunk native vlan 99  
! 本征 VLAN 在 S3 上已修改，但是后来忘记了此操作。此类本征  
! VLAN 不匹配的问题会在中继时造成错误。
```

#### S3

```
!  
vlan 11  
! 必须存在 VLAN 11 此设备才能位于活动的管理域中，  
! 而且这样流量才能从设备通过。
```

## 任务 2：检查是否完全符合要求

由于时间有限，无法针对每个主题执行故障排除，因此只针对一部分主题设置了故障。但是，为了巩固和强化故障排除技巧，您应当确保达到每个要求。为此，请提供检验每个要求完成情况的命令示例（例如 **show** 命令或 **debug** 命令）。

此处并未给出全部命令示例，因为有很多种方式可以检验是否符合要求。下面是要求 1 的命令示例。

S2#**show spanning-tree**

```
VLAN0011
  Spanning tree enabled protocol ieee
  Root ID    Priority      24587
             Address      00E0.A380.CD1C
             This bridge is the root
             Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority      24587 (priority 24576 sys-id-ext 11)
             Address      00E0.A380.CD1C
             Aging Time    300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/4	Desg	FWD	19	128.3	Shr
Fa0/3	Desg	FWD	19	128.3	Shr
Fa0/2	Desg	FWD	19	128.3	Shr
Fa0/1	Desg	FWD	19	128.3	Shr

S3#**show spanning-tree**

<省略部分输出>

```
VLAN0030
  Spanning tree enabled protocol ieee
  Root ID    Priority      24606
             Address      0050.0FCE.8E14
             This bridge is the root
             Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority      24606 (priority 24576 sys-id-ext 30)
             Address      0050.0FCE.8E14
             Aging Time    300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/4	Desg	FWD	19	128.3	Shr
Fa0/3	Desg	FWD	19	128.3	Shr
Fa0/2	Desg	FWD	19	128.3	Shr
Fa0/1	Desg	FWD	19	128.3	Shr

### 任务 3：记录纠正后的网络

```
R1
!
hostname R1
!
!
enable secret ciscocna
!
username R3 password ciscocna
username ccna password ciscocna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.11.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201
 frame-relay map ip 10.1.1.2 201 broadcast
 no keepalive
 clock rate 4000000
!
interface Serial0/0/1
 ip address 10.3.3.1 255.255.255.252
 encapsulation ppp
 ppp authentication chap
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 log-adjacency-changes
 passive-interface FastEthernet0/0
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.11.0 0.0.0.255 area 0
 network 10.3.3.0 0.0.0.3 area 0
 default-information originate
!
ip classless
!
ip access-list standard Anti-spoofing
 permit 192.168.10.0 0.0.0.255
 deny any
```

```
ip access-list standard VTY
 permit 10.0.0.0 0.255.255.255
 permit 192.168.10.0 0.0.0.255
 permit 192.168.11.0 0.0.0.255
 permit 192.168.20.0 0.0.0.255
 permit 192.168.30.0 0.0.0.255
!
!
ip dhcp pool Access1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
!
line con 0
line vty 0 4
 access-class VTY in
 login
!
!
end

R2
!
hostname R2
!
!
enable secret ciscocna
!
username ccna password ciscocna
!
no ip domain-lookup
!
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 shutdown
!
interface FastEthernet0/1
 ip address 192.168.20.1 255.255.255.0
 ip access-group Anti-spoofing in
 ip access-group TFTP out
 ip nat outside
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 10.1.1.2 255.255.255.252
 encapsulation frame-relay
 frame-relay map ip 10.1.1.1 201 broadcast
 frame-relay map ip 10.1.1.2 201
 no keepalive
 ip nat inside
!
interface Serial0/0/1
 ip address 10.2.2.1 255.255.255.252
 ip access-group R3-telnet in
```

```
ip nat inside
clock rate 4000000
!
interface Loopback0
ip address 209.165.200.245 255.255.255.224
ip access-group private in
!
interface Vlan1
no ip address
shutdown
!
router ospf 1
log-adjacency-changes
passive-interface FastEthernet0/1
network 10.1.1.0 0.0.0.3 area 0
network 10.2.2.0 0.0.0.3 area 0
network 192.168.20.0 0.0.0.255 area 0
default-information originate
!
ip nat inside source list NAT interface FastEthernet0/1 overload
ip nat inside source list nat interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 209.165.200.226
!
ip access-list standard Anti-spoofing
permit 192.168.20.0 0.0.0.255
deny any
ip access-list standard NAT
permit 10.0.0.0 0.255.255.255
permit 192.168.0.0 0.0.255.255
ip access-list standard private
deny host 127.0.0.1
deny 10.0.0.0 0.255.255.255
deny 172.0.0.0 0.31.255.255
deny 192.168.0.0 0.0.255.255
permit any
ip access-list extended R3-telnet
deny tcp host 10.2.2.2 host 10.2.2.1 eq telnet
deny tcp host 10.3.3.2 host 10.2.2.1 eq telnet
deny tcp host 192.168.11.3 host 10.2.2.1 eq telnet
deny tcp host 192.168.30.1 host 10.2.2.1 eq telnet
permit ip any any
ip access-list standard TFTP
permit 192.168.20.0 0.0.0.255
!
!
!
line con 0
line vty 0 4
login
!
!
end
```

### R3

```
!  
hostname R3  
!  
!  
enable secret 5 $1$mERr$NY2X7xBCS5tAN/W1NAs2c1  
!  
username R1 password 0 ciscocna  
username ccna password 0 ciscocna  
!  
no ip domain-lookup  
!  
!  
interface FastEthernet0/0  
  no ip address  
  duplex auto  
  speed auto  
  shutdown  
!  
interface FastEthernet0/1  
  no ip address  
  duplex auto  
  speed auto  
!  
interface FastEthernet0/1.11  
  encapsulation dot1Q 11  
  no ip address  
!  
interface FastEthernet0/1.30  
  encapsulation dot1Q 30  
  ip address 192.168.30.1 255.255.255.0  
  ip access-group Anti-spoofing in  
!  
interface Serial0/0/0  
  ip address 10.3.3.2 255.255.255.252  
  encapsulation ppp  
  ppp authentication chap  
  clock rate 4000000  
!  
interface Serial0/0/1  
  ip address 10.2.2.2 255.255.255.252  
!  
interface Vlan1  
  no ip address  
  shutdown  
!  
router ospf 1  
  log-adjacency-changes  
  passive-interface FastEthernet0/1.30  
  network 10.2.2.0 0.0.0.3 area 0  
  network 10.3.3.0 0.0.0.3 area 0  
  network 192.168.11.0 0.0.0.255 area 0  
  network 192.168.30.0 0.0.0.255 area 0  
!  
ip classless  
!  
ip access-list standard Anti-spoofing
```

```
    permit 192.168.30.0 0.0.0.255
    deny any
ip access-list standard VTY
    permit 10.0.0.0 0.255.255.255
    permit 192.168.10.0 0.0.0.255
    permit 192.168.11.0 0.0.0.255
    permit 192.168.20.0 0.0.0.255
    permit 192.168.30.0 0.0.0.255
!
!
!
line con 0
line vty 0 4
    login
!
!
end

S1
!
hostname S1
!
enable secret ciscocna
!
no ip domain-lookup
!
vtp domain CCNA_Troubleshooting
vtp mode transparent
vtp password ciscocna
!
!
vlan 10
!
interface FastEthernet0/1
    switchport access vlan 10
    switchport mode access
!
interface FastEthernet0/2
    switchport access vlan 10
    switchport mode access
!
interface Vlan1
    no ip address
    shutdown
!
interface Vlan10
    ip address dhcp
!
line con 0
!
line vty 0 4
    login
line vty 5 15
    login
!
!
end
```

## S2

```
!  
hostname S2  
!  
enable secret ciscocna  
!  
no ip domain-lookup  
!  
spanning-tree vlan 11 priority 24576  
spanning-tree vlan 30 priority 28672  
!  
interface FastEthernet0/1  
    switchport access vlan 11  
    switchport mode access  
!  
interface FastEthernet0/2  
    switchport access vlan 11  
    switchport mode access  
!  
interface FastEthernet0/3  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface FastEthernet0/4  
    switchport trunk native vlan 99  
    switchport trunk allowed vlan 11,30  
    switchport mode trunk  
!  
interface Vlan1  
    no ip address  
    shutdown  
!  
interface Vlan11  
    ip address 192.168.11.2 255.255.255.0  
!  
line con 0  
!  
line vty 0 4  
    login  
line vty 5 15  
    login  
!  
!  
end
```

## S3

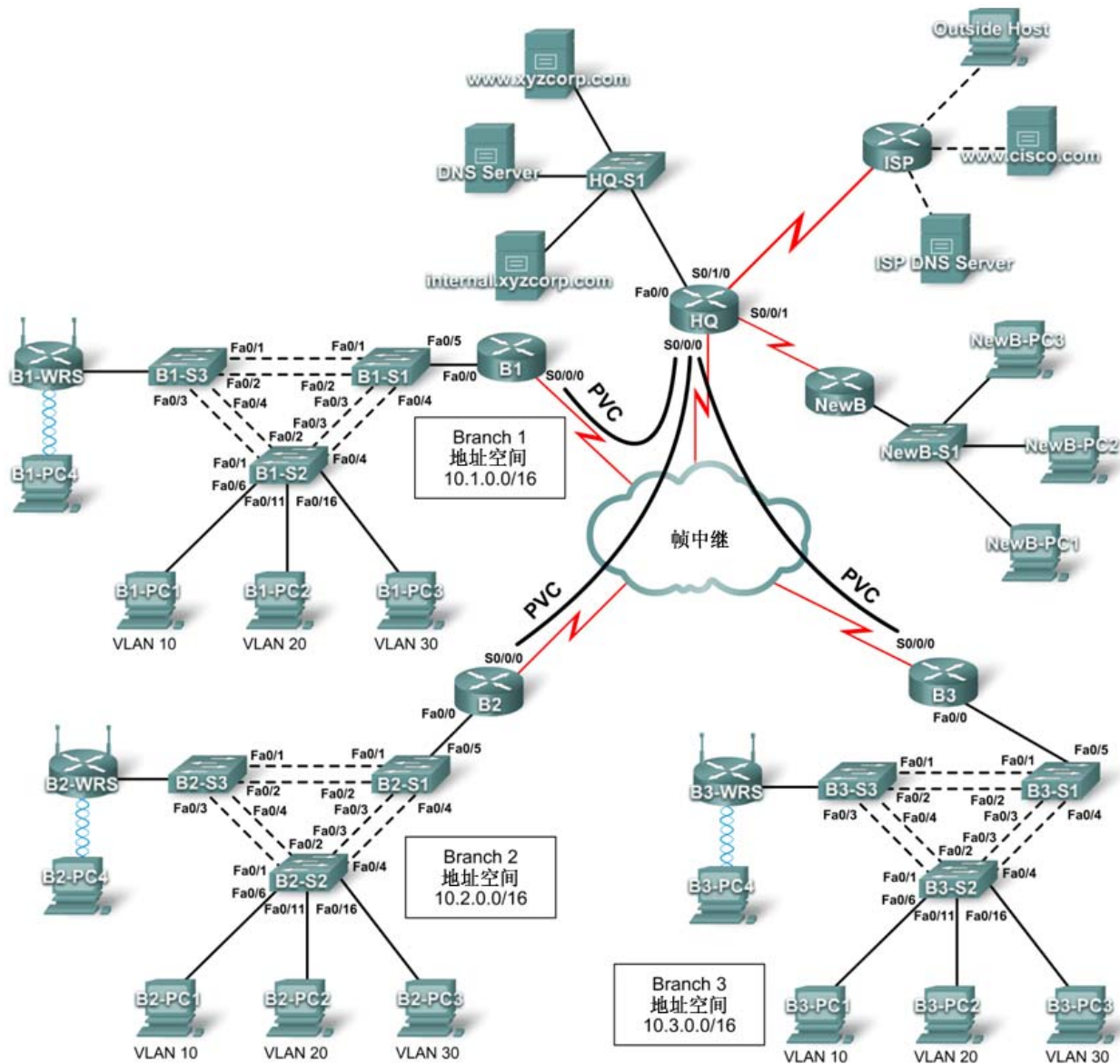
```
!  
hostname S3  
!  
enable secret ciscocna  
!  
no ip domain-lookup  
!  
spanning-tree vlan 11 priority 28672  
spanning-tree vlan 30 priority 24576  
!
```



```
interface FastEthernet0/1
  switchport mode trunk
!
interface FastEthernet0/2
  switchport access vlan 30
  switchport mode access
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport trunk allowed vlan 11,30
  switchport mode trunk
!
interface Vlan1
  no ip address
  shutdown
!
interface Vlan30
  ip address 192.168.30.2 255.255.255.0
!
ip default-gateway 192.168.30.1
!
line con 0
!
line vty 0 4
  login
line vty 5 15
  login
!
!
end
```

## PT 练习 8.6.1: CCNA 综合技能练习 (教师版)

拓扑图



## HQ 地址表

设备	接口	IP 地址	子网掩码	DLCI 映射
HQ	Fa0/0	10.0.1.1	255.255.255.0	不适用
	S0/0/0.41	10.255.255.1	255.255.255.252	DLCI 41 到 B1
	S0/0/0.42	10.255.255.5	255.255.255.252	DLCI 42 到 B2
	S0/0/0.43	10.255.255.9	255.255.255.252	DLCI 43 到 B3
	S0/0/1	10.255.255.253	255.255.255.252	不适用
	S0/1/0	209.165.201.1	255.255.255.252	不适用

## 分支路由器的地址表

设备	接口	IP 地址	子网掩码
BX	Fa0/0.10	10.X.10.1	255.255.255.0
	Fa0/0.20	10.X.20.1	255.255.255.0
	Fa0/0.30	10.X.30.1	255.255.255.0
	Fa0/0.88	10.X.88.1	255.255.255.0
	Fa0/0.99	10.X.99.1	255.255.255.0
	S0/0/0	第二个地址	255.255.255.252
BX-S1	VLAN 99	10.X.99.21	255.255.255.0
BX-S2	VLAN 99	10.X.99.22	255.255.255.0
BX-S3	VLAN 99	10.X.99.23	255.255.255.0
BX-WRS	VLAN 1	10.X.40.1	255.255.255.0

- 以分支路由器 B1、B2 或 B3 的编号代替“X”。
- HQ 的点对点 PVC 使用子网中的第二个地址。HQ 使用第一个地址。
- WRT300N 路由器通过 DHCP 从分支路由器获得 Internet 地址。

## VLAN 配置和端口映射

VLAN 编号	网络地址	VLAN 名称	端口映射
10	10.X.10.0/24	Admin	BX-S2, Fa0/6
20	10.X.20.0/24	Sales	BX-S2, Fa0/11
30	10.X.30.0/24	Production	BX-S2, Fa0/16
88	10.X.88.0/24	Wireless	BX-S3, Fa0/7
99	10.X.99.0/24	Mgmt&Native	所有中继

## 学习目标

- 在集中星型拓扑中配置帧中继
- 将 PPP 的身份验证方式配置为 CHAP 和 PAP
- 配置静态 NAT 和动态 NAT
- 配置静态路由和默认路由

## 简介

在本次综合性 CCNA 技巧练习中，XYZ 公司在 WAN 连接中混合使用帧中继与 PPP。HQ 路由器通过 NAT 提供对服务器群和 Internet 的访问。另外 HQ 还使用基本的防火墙 ACL 来过滤入站流量。每台分支路由器都配置为支持 VLAN 间路由和 DHCP。路由过程通过 EIGRP 以及静态路由和默认路由完成。每个交换网络上都配置了 VLAN、VTP 和 STP。本练习已启用端口安全功能并提供无线接入。在本次综合练习中，您的任务是充分利用您在四门 Exploration 课程中所学的知识，成功运用所有技术。

您要负责配置 HQ 路由器以及分支路由器 B1、B2 和 B3。此外，您还要负责配置每一台通过分支路由器连接到网络的设备。NewB 路由器代表一台小型公司经合并后作为新分支机构的分支路由器。您不具有 NewB 路由器的访问权。但是，您要在 HQ 和 NewB 之间建立一条链路，使这家新的分支机构能够访问内部网络和 Internet。

您管理的路由器和交换机都还没有经过配置。Packet Tracer 不会对基本配置（如主机名、口令、标语和其它常规维护命令）进行评分，这些基本配置也不属于规定的任务。但是，您需要执行这些配置，您的教师可能会选择对这些命令进行评分。

由于本练习所使用的网络相当庞大，试题中有将近 500 个必需的组件，您不必在每次输入命令后查看增加的完成比例。另外，本练习不会说明每个任务结束后应当完成的特定百分比。您需要通过测试连通性来检验每个任务的配置。不过，您随时都可以单击 **Check Results（检查结果）** 查看系统是否对特定的组件评分以及您的配置是否正确。

由于分支路由器（B1、B2 和 B3）和交换机在设计时考虑了可扩展性，因此您可以重复利用配置脚本。例如，适用于 B1、B1-S1、B1-S2 和 B1-S3 的配置只需稍作调整即可直接应用于 B2。

注：本 CCNA 综合技巧练习还有一种开放型版本，这种版本中您可以选择想实施的编址方案和技术。您需要通过测试端到端的连通性来检验配置。

## 任务 1：在集中星型拓扑中配置帧中继

### 步骤 1. 配置帧中继核心。

请使用地址表并遵循下列要求。

HQ 为中心路由器。B1、B2 和 B3 为分支路由器。

- HQ 对每台分支路由器使用点对点接口。
- 必须手动配置 B3 使其使用 IETF 封装。
- 对于 HQ、B1 和 B2，LMI 类型必须手动配置为 q933a。B3 使用 ANSI。

```
!-----  
!HQ  
!-----  
enable  
configure terminal  
host HQ  
enable secret class
```

```
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
  no ip address
  encapsulation frame-relay
  frame-relay lmi-type q933a
  no shutdown
!
interface Serial0/0/0.41 point-to-point
  ip address 10.255.255.1 255.255.255.252
  frame-relay interface-dlci 41
!
interface Serial0/0/0.42 point-to-point
  ip address 10.255.255.5 255.255.255.252
  frame-relay interface-dlci 42
!
interface Serial0/0/0.43 point-to-point
  ip address 10.255.255.9 255.255.255.252
  frame-relay interface-dlci 43
end
wr

!-----
!B1
!-----
enable
configure terminal
host B1
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
  ip address 10.255.255.2 255.255.255.252
  encapsulation frame-relay
  frame-relay lmi-type q933a
  no shutdown
end
wr

!-----
!B2
!-----
enable
```

```
configure terminal
host B2
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
 ip address 10.255.255.6 255.255.255.252
 encapsulation frame-relay
 frame-relay lmi-type q933a
 no shutdown
end
wr

!-----
!B3
!-----
enable
configure terminal
host B3
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
interface Serial0/0/0
 ip address 10.255.255.10 255.255.255.252
 encapsulation frame-relay ietf
 frame-relay lmi-type ansi
 no shutdown
end
wr
```

**步骤 2. 在 HQ 上配置 LAN 接口。**

```
!
interface FastEthernet0/0
 description Server Farm
 ip address 10.0.1.1 255.255.255.0
 no shutdown
!
```

### 步骤 3. 检验 HQ 能否 ping 通每台分支路由器。

```
HQ#ping 10.255.255.2
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.255.255.2, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/71/89 ms
```

```
HQ#ping 10.255.255.6
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.255.255.6, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 35/60/69 ms
```

```
HQ#ping 10.255.255.10
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.255.255.10, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 23/58/87 ms
```

## 任务 2：将 PPP 的身份验证方式配置为 CHAP 和 PAP

### 步骤 1. 使用 PPP 封装和 CHAP 身份验证配置从 HQ 到 ISP 的 WAN 链路。

CHAP 口令是 **ciscochap**。

```
username ISP password ciscochap  
interface Serial0/1/0  
  description Link to ISP  
  ip address 209.165.201.1 255.255.255.252  
  encapsulation ppp  
  ppp authentication chap  
  no shutdown
```

### 步骤 2. 使用 PPP 封装和 PAP 身份验证配置从 HQ 到 NewB 的 WAN 链路。

您需要将电缆连接到正确的接口。HQ 是链路的 DCE 端。您需要选择时钟频率。PAP 口令是 **ciscopap**。

```
username NewB password ciscopap  
interface Serial0/0/1  
  description Link to B4  
  ip address 10.255.255.253 255.255.255.252  
  encapsulation ppp  
  ppp authentication pap  
  ppp pap sent-username HQ password 0 ciscopap  
  clock rate 64000  
  no shutdown  
HQ#ping 209.165.201.2
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.165.201.2, timeout is 2 seconds:  
!!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 17/30/38 ms
```

```
HQ#ping 10.255.255.254
```

```
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 10.255.255.254, timeout is 2 seconds:  
!!!!  
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/29/47 ms
```

### 任务 3：在 HQ 上配置静态 NAT 和动态 NAT

#### 步骤 1. 配置 NAT。

请遵循下列要求：

- 允许转换 10.0.0.0/8 中的所有地址。
- XYZ 公司拥有 209.165.200.240/29 地址空间。XYZCORP 池使用从 .241 到 .245 范围内的地址，子网掩码为 /29。
- 位于 10.0.1.2 的 www.xyzcorp.com 网站注册于 IP 地址为 209.165.200.246 的公共 DNS 系统。

```
ip access-list standard NAT_LIST  
  permit 10.0.0.0 0.255.255.255  
!  
ip nat pool XYZCORP 209.165.200.241 209.165.200.245 netmask 255.255.255.248  
ip nat inside source list NAT_LIST pool XYZCORP overload  
ip nat inside source static 10.0.1.2 209.165.200.246  
!  
interface fa0/0  
  ip nat inside  
interface s0/0/0.41 point-to-point  
  ip nat inside  
interface s0/0/0.42 point-to-point  
  ip nat inside  
interface s0/0/0.43 point-to-point  
  ip nat inside  
interface s0/0/1  
  ip nat inside  
interface s0/1/0  
  ip nat outside
```

#### 步骤 2. 使用扩展 ping 命令检验 NAT 是否在运作。

使用 HQ LAN 接口作为源地址，从 HQ ping ISP 上的 serial 0/0/0 接口。此 ping 命令应该成功。

```
HQ#ping  
Protocol [ip]:  
Target IP address: 209.165.201.2  
Repeat count [5]:  
Datagram size [100]:  
Timeout in seconds [2]:  
Extended commands [n]: y  
Source address or interface: 10.0.1.1  
Type of service [0]:  
Set DF bit in IP header? [no]:  
Validate reply data? [no]:  
Data pattern [0xABCD]:  
Loose, Strict, Record, Timestamp, Verbose[none]:  
Sweep range of sizes [n]:  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 209.165.201.2, timeout is 2 seconds:
```



```
Packet sent with a source address of 10.0.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 18/34/42 ms
```

使用 **show ip nat translations** 命令检验 NAT 是否已将 ping 命令使用的内部地址进行了转换。

```
HQ#show ip nat translations
Pro  Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.241:35 10.0.1.1:35      209.165.201.2:35 209.165.201.2:35
icmp 209.165.200.241:36 10.0.1.1:36      209.165.201.2:36 209.165.201.2:36
icmp 209.165.200.241:37 10.0.1.1:37      209.165.201.2:37 209.165.201.2:37
icmp 209.165.200.241:38 10.0.1.1:38      209.165.201.2:38 209.165.201.2:38
icmp 209.165.200.241:39 10.0.1.1:39      209.165.201.2:39 209.165.201.2:39
--- 209.165.200.246    10.0.1.2        ---              ---
```

#### 任务 4：配置静态路由和默认路由

步骤 1. 配置 HQ 到达 ISP 的默认路由和到达 NewB LAN 的静态路由。

请使用送出接口作为参数。

```
ip route 0.0.0.0 0.0.0.0 Serial0/1/0
ip route 10.4.5.0 255.255.255.0 Serial0/0/1
```

步骤 2. 配置分支路由器到达 HQ 的默认路由。

请使用下一跳 IP 地址作为参数。

```
!B1
ip route 0.0.0.0 0.0.0.0 10.255.255.1

!B2
ip route 0.0.0.0 0.0.0.0 10.255.255.5

!B3
ip route 0.0.0.0 0.0.0.0 10.255.255.9
```

步骤 3. 检验 ISP 范围外的连通性。

所有三台 NewB PC 以及 NetAdmin PC 都应该能 ping 通 www.cisco.com Web 服务器。

!在 NewB-PC1 上

```
Packet Tracer PC Command Line 1.0
PC>ping www.cisco.com
```

```
Pinging 209.165.202.134 with 32 bytes of data:
```

```
Request timed out.
Reply from 209.165.202.134: bytes=32 time=10ms TTL=125
Reply from 209.165.202.134: bytes=32 time=10ms TTL=125
Reply from 209.165.202.134: bytes=32 time=10ms TTL=125
```

```
Ping statistics for 209.165.202.134:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

```
PC>
```

!在 NetAdmin 上

Packet Tracer PC Command Line 1.0  
PC>ping www.cisco.com

Pinging 209.165.202.134 with 32 bytes of data:

Reply from 209.165.202.134: bytes=32 time=12ms TTL=126  
Reply from 209.165.202.134: bytes=32 time=188ms TTL=126  
Reply from 209.165.202.134: bytes=32 time=8ms TTL=126  
Reply from 209.165.202.134: bytes=32 time=8ms TTL=126

Ping statistics for 209.165.202.134:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 8ms, Maximum = 188ms, Average = 54ms

PC>

## 任务 5：配置 VLAN 间路由

**步骤 1. 配置每台分支路由器使其支持 VLAN 间路由。**

使用分支路由器的地址表配置并激活 VLAN 间路由的 LAN 接口。VLAN 99 为本征 VLAN。

!-----  
!分支路由器  
!-----  
!以路由器编号代替 x。

```
interface FastEthernet0/0
  no shutdown
!
interface FastEthernet0/0.10
  description Admin VLAN 10
  encapsulation dot1Q 10
  ip address 10.X.10.1 255.255.255.0
!
interface FastEthernet0/0.20
  description Sales VLAN 20
  encapsulation dot1Q 20
  ip address 10.X.20.1 255.255.255.0
!
interface FastEthernet0/0.30
  description Production VLAN 30
  encapsulation dot1Q 30
  ip address 10.X.30.1 255.255.255.0
!
interface FastEthernet0/0.88
  description Wireless VLAN 88
  encapsulation dot1Q 88
  ip address 10.X.88.1 255.255.255.0
!
interface FastEthernet0/0.99
  description Mgmt&Native VLAN 99
```

```
encapsulation dot1Q 99 native
ip address 10.X.99.1 255.255.255.0
!
```

## 步骤 2. 检查路由表。

每台分支路由器现在都应该有六个直接相连的网络和一条静态默认路由。

```
B1#show ip route
<省略部分输出>
```

```
Gateway of last resort is 10.255.255.1 to network 0.0.0.0

    10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.1.10.0/24 is directly connected, FastEthernet0/0.10
C       10.1.20.0/24 is directly connected, FastEthernet0/0.20
C       10.1.30.0/24 is directly connected, FastEthernet0/0.30
C       10.1.88.0/24 is directly connected, FastEthernet0/0.88
C       10.1.99.0/24 is directly connected, FastEthernet0/0.99
C       10.255.255.0/30 is directly connected, Serial0/0/0
S*    0.0.0.0/0 [1/0] via 10.255.255.1
```

## 任务 6：配置和优化 EIGRP 路由

### 步骤 1. 配置 HQ、B1、B2 和 B3 的 EIGRP。

- 使用 AS 100。
- 在适当的接口上禁用 EIGRP 更新。
- 手动总结 EIGRP 路由，使每台分支路由器只向 HQ 通告 10.X.0.0/16 地址空间。

注：Packet Tracer 无法准确地模拟 EIGRP 总结路由的优势。路由表仍将显示所有的子网，即使您已正确配置手动总结。

```
!-----
!HQ 路由器
!-----

router eigrp 100
  passive-interface FastEthernet0/0
  passive-interface Serial0/0/1
  passive-interface Serial0/1/0
  network 10.0.0.0
  no auto-summary
!

!-----
!分支路由器
!-----

!
router eigrp 100
  passive-interface FastEthernet0/0.10
  passive-interface FastEthernet0/0.20
  passive-interface FastEthernet0/0.30
  passive-interface FastEthernet0/0.99
  network 10.0.0.0
  no auto-summary
```

```
!  
!  
!以路由器编号代替 x  
!  
interface serial 0/0/0  
ip summary-address eigrp 100 10.X.0.0 255.255.0.0
```

## 步骤 2. 检查路由表和连通性。

HQ 路由器和分支路由器现在应该有完整的路由表。

```
HQ#sh ip route  
<省略部分输出>
```

```
Gateway of last resort is 0.0.0.0 to network 0.0.0.0  
  
10.0.0.0/8 is variably subnetted, 21 subnets, 2 masks  
C    10.0.1.0/24 is directly connected, FastEthernet0/0  
D    10.1.10.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41  
D    10.1.20.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41  
D    10.1.30.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41  
D    10.1.88.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41  
D    10.1.99.0/24 [90/2172416] via 10.255.255.2, 00:00:14, Serial0/0/0.41  
D    10.2.10.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42  
D    10.2.20.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42  
D    10.2.30.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42  
D    10.2.88.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42  
D    10.2.99.0/24 [90/2172416] via 10.255.255.6, 00:00:07, Serial0/0/0.42  
D    10.3.10.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43  
D    10.3.20.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43  
D    10.3.30.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43  
D    10.3.88.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43  
D    10.3.99.0/24 [90/2172416] via 10.255.255.10, 00:00:04, Serial0/0/0.43  
S    10.4.5.0/24 is directly connected, Serial0/0/1  
C    10.255.255.0/30 is directly connected, Serial0/0/0.41  
C    10.255.255.4/30 is directly connected, Serial0/0/0.42  
C    10.255.255.8/30 is directly connected, Serial0/0/0.43  
C    10.255.255.252/30 is directly connected, Serial0/0/1  
    209.165.201.0/30 is subnetted, 1 subnets  
C    209.165.201.0 is directly connected, Serial0/1/0  
S*   0.0.0.0/0 is directly connected, Serial0/1/0
```

NetAdmin PC 现在应该能 ping 通每台分支路由器上的每个 VLAN 子接口。

!在 NetAdmin PC 上

```
Packet Tracer PC Command Line 1.0  
PC>ping 10.1.10.1
```

Pinging 10.1.10.1 with 32 bytes of data:

```
Reply from 10.1.10.1: bytes=32 time=104ms TTL=254  
Reply from 10.1.10.1: bytes=32 time=104ms TTL=254  
Reply from 10.1.10.1: bytes=32 time=100ms TTL=254  
Reply from 10.1.10.1: bytes=32 time=132ms TTL=254
```

```
Ping statistics for 10.1.10.1:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
  Minimum = 100ms, Maximum = 132ms, Average = 110ms
```

```
PC>ping 10.2.20.1
```

```
Pinging 10.2.20.1 with 32 bytes of data:
```

```
Reply from 10.2.20.1: bytes=32 time=83ms TTL=254
Reply from 10.2.20.1: bytes=32 time=152ms TTL=254
Reply from 10.2.20.1: bytes=32 time=118ms TTL=254
Reply from 10.2.20.1: bytes=32 time=103ms TTL=254
```

```
Ping statistics for 10.2.20.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 83ms, Maximum = 152ms, Average = 114ms
```

```
PC>ping 10.3.30.1
```

```
Pinging 10.3.30.1 with 32 bytes of data:
```

```
Reply from 10.3.30.1: bytes=32 time=114ms TTL=254
Reply from 10.3.30.1: bytes=32 time=99ms TTL=254
Reply from 10.3.30.1: bytes=32 time=108ms TTL=254
Reply from 10.3.30.1: bytes=32 time=153ms TTL=254
```

```
Ping statistics for 10.3.30.1:
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 99ms, Maximum = 153ms, Average = 118ms
```

## 任务 7：配置 VTP、中继、VLAN 接口和 VLAN

下列要求适用于所有三个分支。配置三台交换机中的一台。然后将这些交换机的脚本应用于其它两台交换机。

### 步骤 1. 配置分支交换机的 VTP。

- BX-S1 为 VTP 服务器。BX-S2 和 BX-S3 为 VTP 客户端。
- 域名为 **XYZCORP**。
- 口令为 **xyzvtp**。

### 步骤 2. 在 BX-S1、BX-S2 和 BX-S3 上配置中继。

将适当的接口配置为中继模式并指定 VLAN 99 为本征 VLAN。

### 步骤 3. 在 BX-S1、BX-S2 和 BX-S3 上配置 VLAN 接口和默认网关。

#### 步骤 4. 在 BX-S1 上创建 VLAN。

只在 BX-S1 上创建并命名“VLAN 配置和端口映射”表中列出的 VLAN。VTP 会向 BX-S1 和 BX-S2 通告新的 VLAN。

```
!  
!Replace the "X" in the following scripts with the Branch number  
!  
!-----  
!S1  
!-----  
enable  
configure terminal  
host BX-S1  
enable secret class  
banner motd $AUTHORIZED ACCESS ONLY!$  
line con 0  
pass cisco  
login  
line vty 0 4  
pass cisco  
login  
service password-encryption  
!  
vtp mode server  
vtp domain xyzcorp  
vtp password xyzvtp  
!  
interface FastEthernet0/1  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/2  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/3  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/4  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface FastEthernet0/5  
    switchport trunk native vlan 99  
    switchport mode trunk  
!  
interface vlan 99  
    ip address 10.X.99.21 255.255.255.0  
    no shut  
ip default-gateway 10.X.99.1  
!  
vlan 10  
    name Admin  
vlan 20  
    name Sales
```

```
vlan 30
  name Production
vlan 88
  name Wireless
vlan 99
  name Mgmt&Native
end
wr

!-----
!S2
!-----
enable
configure terminal
host BX-S2
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
vtp mode client
vtp domain xyzcorp
vtp password xyzvtp
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
!
interface vlan 99
  ip address 10.X.99.22 255.255.255.0
  no shut
ip default-gateway 10.X.99.1
!
end
wr

!-----
!S3
!-----
enable
```

```
configure terminal
host BX-S3
enable secret class
banner motd $AUTHORIZED ACCESS ONLY!$
line con 0
pass cisco
login
line vty 0 4
pass cisco
login
service password-encryption
!
vtp mode client
vtp domain xyzcorp
vtp password xyzvtp
!
interface FastEthernet0/1
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/2
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/3
  switchport trunk native vlan 99
  switchport mode trunk
!
interface FastEthernet0/4
  switchport trunk native vlan 99
  switchport mode trunk
!
interface vlan 99
  ip address 10.X.99.23 255.255.255.0
  no shut
ip default-gateway 10.X.99.1
!
end
wr
```

#### 步骤 5. 检查这些 VLAN 是否已发送到 BX-S2 和 BX-S3。

使用适当的命令检查 S2 和 S3 是否已具有您在 S1 上创建的 VLAN。Packet Tracer 模拟 VTP 通告可能需要花费数分钟的时间。一种强制发送 VTP 通告的快速方法是，将其中一台客户端交换机更改为透明模式然后再改回客户端模式。

!所有交换机将拥有相似的输出。 所有 BX-S1 交换机的 VTP  
!工作模式都是服务器模式。

```
B2-S2#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 10
VTP Operating Mode          : Client
VTP Domain Name              : xyzcorp
VTP Pruning Mode             : Disabled
```



```
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0xCD 0xBF 0xDE 0x4E 0x0F 0x79 0x7D 0x3E
Configuration last modified by 10.2.99.21 at 3-1-93 00:43:41
```

```
B2-S2#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	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 Gig1/1, Gig1/2
10	Admin	active	
20	Sales	active	
30	Production	active	
88	Wireless	active	
99	Mgmt&Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

## 任务 8：分配 VLAN 并配置端口安全性

### 步骤 1. 为接入端口分配 VLAN。

根据“VLAN 配置和端口映射”表完成下列要求：

- 配置接入端口
- 为接入端口分配 VLAN

### 步骤 2. 配置端口安全性。

使用下列策略在 BX-S2 接入端口上建立端口安全性：

- 仅允许一个 MAC 地址
- 将第一个学习到的 MAC 地址配置为“粘滞”在配置中
- 设置端口，使其在出现安全违规时关闭

```
!-----
!BX-S3
!-----
!
interface FastEthernet0/7
 switchport access vlan 88
 switchport mode access

!-----
!BX-S2
!-----

!
interface FastEthernet0/6
 switchport access vlan 10
```

```

switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
!
interface FastEthernet0/11
switchport access vlan 20
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
!
interface FastEthernet0/16
switchport access vlan 30
switchport mode access
switchport port-security
switchport port-security maximum 1
switchport port-security mac-address sticky
switchport port-security violation shutdown
!

```

### 步骤 3. 检查 VLAN 分配和端口安全性。

使用适当的命令检查是否已正确分配接入 VLAN，以及是否已启用端口安全策略。

B1-S2#show vlan brief

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/12, Fa0/13, Fa0/14 Fa0/15, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig1/1, Gig1/2
10	Admin	active	Fa0/6
20	Sales	active	Fa0/11
30	Production	active	Fa0/16
88	Wireless	active	
99	Mgmt&Native	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```

B1-S2#show port-security interface fa0/6
Port Security           : Enabled
Port Status             : Secure-up
Violation Mode          : Shutdown
Aging Time              : 0 mins
Aging Type               : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses    : 1
Total MAC Addresses      : 0
Configured MAC Addresses : 0
Sticky MAC Addresses     : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0

```

## 任务 9：配置 STP

### 步骤 1. 将 BX-S1 配置为根桥。

将 BX-S1 的优先级设置为 4096，使这些交换机始终成为所有 VLAN 的根桥。

```
!-----  
!BX-S1  
!-----  
!  
spanning-tree vlan 1 priority 4096  
spanning-tree vlan 10 priority 4096  
spanning-tree vlan 20 priority 4096  
spanning-tree vlan 30 priority 4096  
spanning-tree vlan 88 priority 4096  
spanning-tree vlan 99 priority 4096  
!
```

### 步骤 2. 将 BX-S3 配置为备用根桥。

将 BX-S3 的优先级设置为 8192，使这些交换机始终成为所有 VLAN 的备用根桥。

```
!-----  
!BX-S3  
!-----  
!  
spanning-tree vlan 1 priority 8192  
spanning-tree vlan 10 priority 8192  
spanning-tree vlan 20 priority 8192  
spanning-tree vlan 30 priority 8192  
spanning-tree vlan 88 priority 8192  
spanning-tree vlan 99 priority 8192  
!
```

### 步骤 3. 检验 BX-S1 是否成为根桥。

!对于所有交换机上的所有 VLAN，输出都应当是类似的。

!

B1-S1#show spanning-tree vlan 10

```
VLAN0010  
  Spanning tree enabled protocol ieee  
  Root ID    Priority      4106  
            Address      00D0.BA3D.2C94  
            This bridge is the root  
            Hello Time    2 sec  Max Age 20 sec  Forward Delay 15 sec  
  Bridge ID  Priority      4106 (priority 4116 sys-id-ext 10)  
            Address      00D0.BA3D.2C94  
            Aging Time    300
```

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/3	Desg	FWD	19	128.3	Shr
Fa0/1	Desg	FWD	19	128.3	Shr
Fa0/2	Desg	FWD	19	128.3	Shr
Fa0/5	Desg	FWD	19	128.3	Shr
Fa0/4	Desg	FWD	19	128.3	Shr

## 任务 10：配置 DHCP

### 步骤 1. 为每个 VLAN 配置 DHCP 池。

在每台分支路由器上，依据下列要求为每个 VLAN 配置 DHCP 池：

- 对于 LAN，在每个池中排除前 10 个 IP 地址。
- 对于无线 LAN，在每个池中排除前 24 个 IP 地址。
- 池的名称为 **BX\_VLAN##**，其中 **X** 是路由器编号，**##** 是 VLAN 编号。
- 将连接到 HQ 服务器群的 DNS 服务器包含在内作为 DHCP 配置的组成部分。

```
!-----
!B1
!-----
!
ip dhcp excluded-address 10.1.10.1 10.1.10.10
ip dhcp excluded-address 10.1.20.1 10.1.20.10
ip dhcp excluded-address 10.1.30.1 10.1.30.10
ip dhcp excluded-address 10.1.88.1 10.1.88.24
!
ip dhcp pool B1_VLAN10
 network 10.1.10.0 255.255.255.0
 default-router 10.1.10.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN20
 network 10.1.20.0 255.255.255.0
 default-router 10.1.20.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN30
 network 10.1.30.0 255.255.255.0
 default-router 10.1.30.1
 dns-server 10.0.1.4
ip dhcp pool B1_VLAN88
 network 10.1.88.0 255.255.255.0
 default-router 10.1.88.1
 dns-server 10.0.1.4

!-----
!B2
!-----
!
ip dhcp excluded-address 10.2.10.1 10.2.10.10
ip dhcp excluded-address 10.2.20.1 10.2.20.10
ip dhcp excluded-address 10.2.30.1 10.2.30.10
ip dhcp excluded-address 10.2.88.1 10.2.88.24
!
ip dhcp pool B2_VLAN10
 network 10.2.10.0 255.255.255.0
 default-router 10.2.10.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN20
 network 10.2.20.0 255.255.255.0
 default-router 10.2.20.1
 dns-server 10.0.1.4
ip dhcp pool B2_VLAN30
 network 10.2.30.0 255.255.255.0
 default-router 10.2.30.1
```

```
    dns-server 10.0.1.4
ip dhcp pool B2_VLAN88
  network 10.2.88.0 255.255.255.0
  default-router 10.2.88.1
  dns-server 10.0.1.4

!-----
!B3
!-----
!
ip dhcp excluded-address 10.3.10.1 10.3.10.10
ip dhcp excluded-address 10.3.20.1 10.3.20.10
ip dhcp excluded-address 10.3.30.1 10.3.30.10
ip dhcp excluded-address 10.3.88.1 10.3.88.24
!
ip dhcp pool B3_VLAN10
  network 10.3.10.0 255.255.255.0
  default-router 10.3.10.1
  dns-server 10.0.1.4
ip dhcp pool B3_VLAN20
  network 10.3.20.0 255.255.255.0
  default-router 10.3.20.1
  dns-server 10.0.1.4
ip dhcp pool B3_VLAN30
  network 10.3.30.0 255.255.255.0
  default-router 10.3.30.1
  dns-server 10.0.1.4
ip dhcp pool B3_VLAN88
  network 10.3.88.0 255.255.255.0
  default-router 10.3.88.1
  dns-server 10.0.1.4
```

## 步骤 2. 配置 PC 使用 DHCP。

目前，这些 PC 配置为使用静态 IP 地址。请将此配置更改为 DHCP。

## 步骤 3. 检验 PC 和无线路由器是否有 IP 地址。

## 步骤 4. 检验连通性。

所有通过物理方式连接到网络中的 PC 都应该能 ping 通 [www.cisco.com](http://www.cisco.com) Web 服务器。

!在 B1-PC1 上

```
Packet Tracer PC Command Line 1.0
PC>ping www.cisco.com
```

```
Pinging 209.165.202.134 with 32 bytes of data:
```

```
Reply from 209.165.202.134: bytes=32 time=234ms TTL=125
Reply from 209.165.202.134: bytes=32 time=184ms TTL=125
Reply from 209.165.202.134: bytes=32 time=230ms TTL=125
Reply from 209.165.202.134: bytes=32 time=228ms TTL=125
```

```
Ping statistics for 209.165.202.134:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 184ms, Maximum = 234ms, Average = 219ms
```

```
PC>
```

## 任务 11：配置防火墙 ACL

### 步骤 1. 检验 Outside Host 的连通性。

Outside Host PC 应该能 ping 通位于 www.xyzcorp.com 的服务器。

```
!-----  
!Outside Host  
!-----  
!  
Packet Tracer PC Command Line 1.0  
PC>ping www.xyzcorp.com  
  
Pinging 209.165.200.246 with 32 bytes of data:  
  
Reply from 209.165.200.246: bytes=32 time=45ms TTL=126  
Reply from 209.165.200.246: bytes=32 time=115ms TTL=126  
Reply from 209.165.200.246: bytes=32 time=124ms TTL=126  
Reply from 209.165.200.246: bytes=32 time=101ms TTL=126  
  
Ping statistics for 209.165.200.246:  
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
    Minimum = 45ms, Maximum = 124ms, Average = 96ms  
  
PC>
```

### 步骤 2. 实施基本的防火墙 ACL。

由于 ISP 提供通往 Internet 的连接，因此请按照下列顺序配置名为 **FIREWALL** 的命名 ACL：

1. 允许发送至 www.xyzcorp.com 服务器的入站 HTTP 请求。
2. 仅允许来自 ISP 和来自 ISP 之外任何源地址的已建立 TCP 会话。
3. 仅允许来自 ISP 和来自 ISP 之外任何源地址的入站 ping 应答。
4. 明确阻止来自 ISP 和来自 ISP 之外任何源地址的所有其它入站访问。

```
!-----  
!HQ  
!-----  
  
ip access-list extended FIREWALL  
  permit tcp any host 209.165.200.244 eq www  
  permit tcp any any established  
  permit icmp any any echo-reply  
  deny ip any any  
!  
interface Serial0/1/0  
  ip access-group FIREWALL in
```

### 步骤 3. 检验 Outside Host 的连通性。

Outside Host PC 应该无法 ping 通位于 www.xyzcorp.com 的服务器。但是 Outside Host PC 应该能请求网页。

```
!-----  
!Outside Host  
!-----  
!
```

```
PC>ping www.xyzcorp.com
```

```
Pinging 209.165.200.246 with 32 bytes of data:
```

```
Request timed out.  
Request timed out.  
Request timed out.  
Request timed out.
```

```
Ping statistics for 209.165.200.246:
```

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

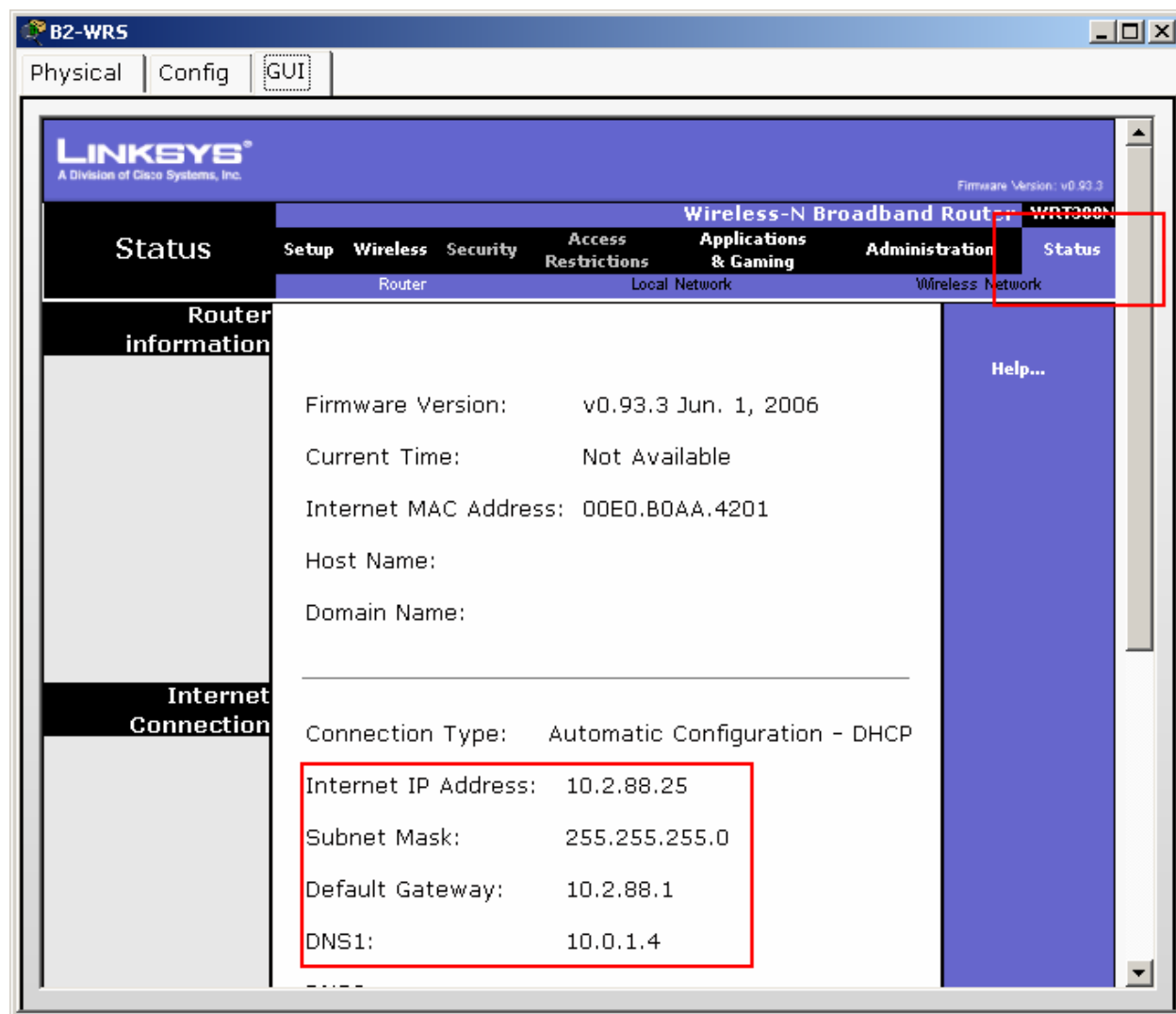
```
PC>
```

## 任务 12：配置无线连接

### 步骤 1. 检验 DHCP 配置。

每台 BX-WRS 路由器都应该已经通过 BX 路由器的 DHCP 获得 VLAN 88 中的 IP 地址。

本任务中的图片仅对教师版提供



## 步骤 2. 配置网络设置/LAN 设置。

GUI 选项卡中 **Status**（状态）页面上的“Router IP”（路由器 IP）应该是 10.X.40.0 /24 子网的第一个 IP。  
请将所有其它设置保留默认值。

The screenshot shows the Linksys WRT300N router configuration interface. The 'Setup' tab is selected, and the 'Network Setup' section is active. A red box highlights the following settings:

- IP Address:** 10 . 2 . 40 . 1
- Subnet Mask:** 255.255.255.0
- DHCP Server:** ☒ Enabled ☐ Disabled
- Start IP Address:** 10.2.40. 100
- Maximum number of Users:** 50
- IP Address Range:** 10.2.40. 100 - 149

Other visible settings include:

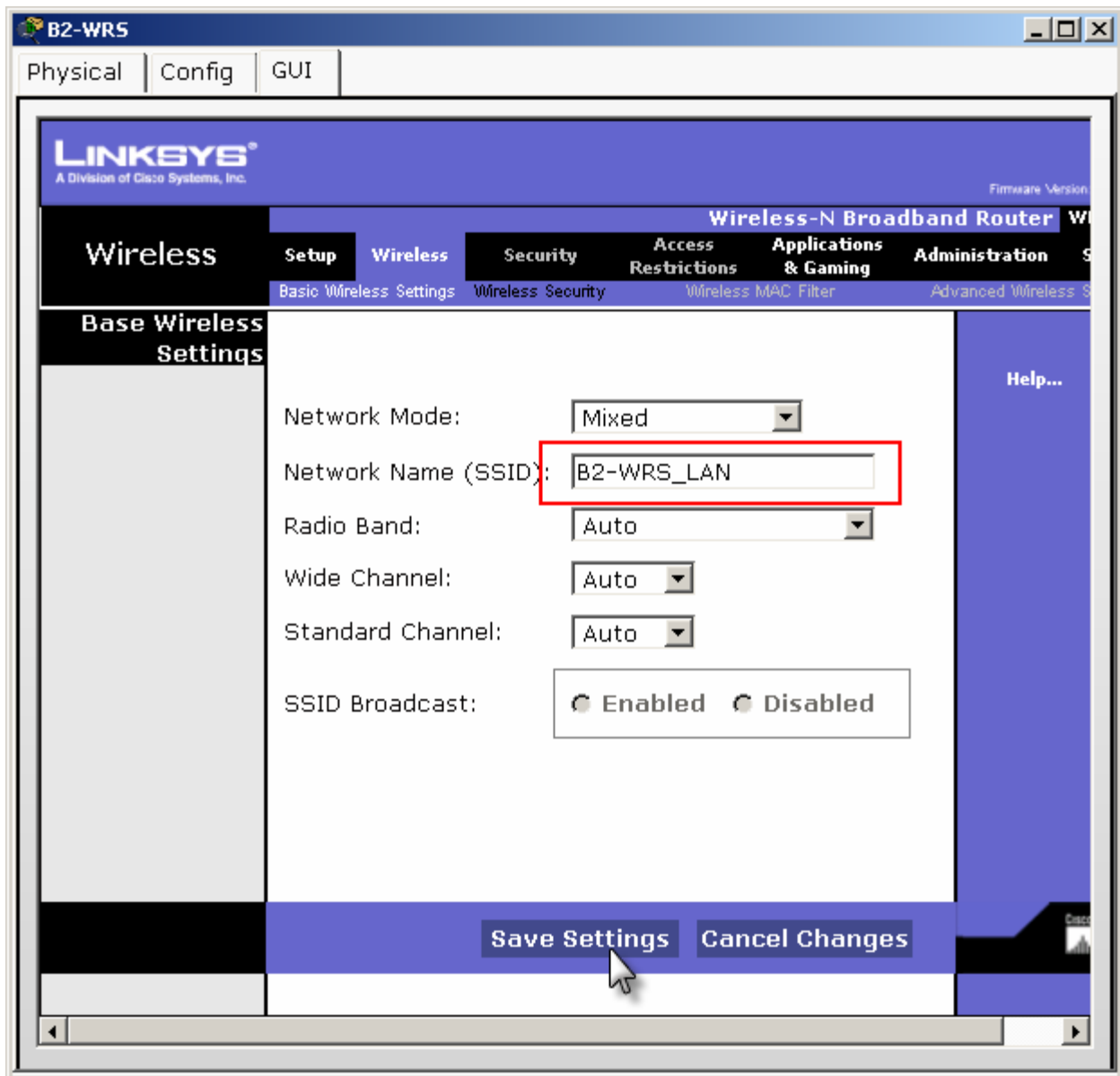
- Internet Setup:** Automatic Configuration - DHCP
- Host Name:** (empty)
- Domain Name:** (empty)
- MTU:** (empty) Size: 1500
- DHCP Reservation:** (button)

At the bottom, there are buttons for 'Save Settings' and 'Cancel Changes'.



**步骤 3. 配置无线网络设置。**

路由器的 SSID 为 **BX-WRS\_LAN**，其中 **X** 是分支路由器编号。



WEP 密钥为 12345ABCDE

The screenshot shows the configuration interface for a Linksys B2-WRS Wireless-N Broadband Router. The 'Wireless Security' tab is selected, and the 'Security Mode' is set to 'WEP'. The 'Encryption' is set to '40/64-Bit(10 Hex digit)'. The 'Passphrase' field is empty, and the 'Generate' button is visible. The 'Key1' field contains the value '12345ABCDE'. The 'Key2', 'Key3', and 'Key4' fields are empty. The 'TX Key' is set to '1'. The 'Save Settings' button is highlighted with a mouse cursor.

Physical | Config | GUI

LINKSYS®  
A Division of Cisco Systems, Inc.

Wireless-N Broadband Router

Wireless | Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Wireless Settings | Wireless Security | Wireless MAC Filter | Advanced Wireless Settings

Wireless Security

Security Mode: WEP

Encryption: 40/64-Bit(10 Hex digit)

Passphrase:  Generate

Key1: 12345ABCDE

Key2:

Key3:

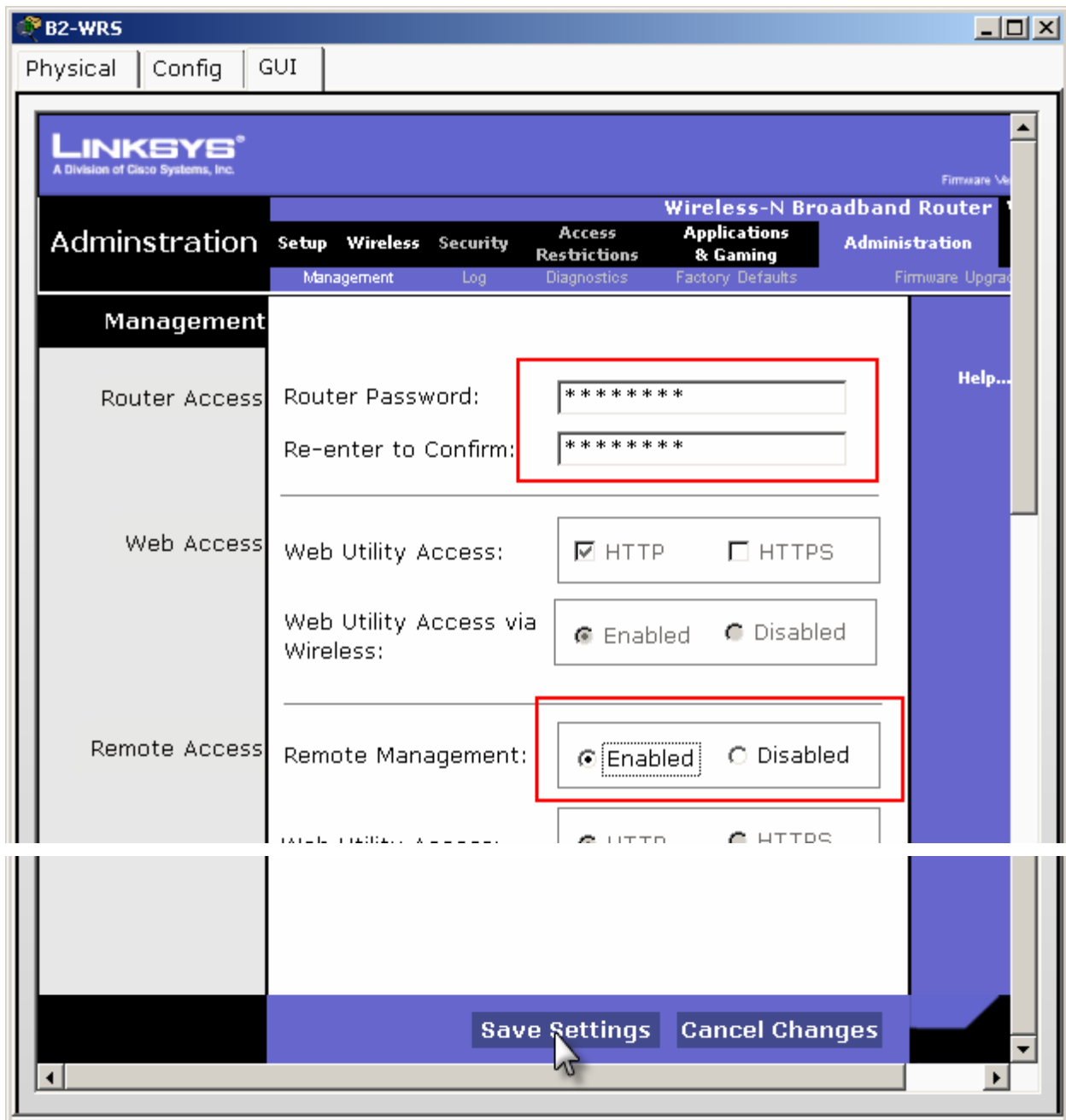
Key4:

TX Key: 1

Save Settings Cancel Changes

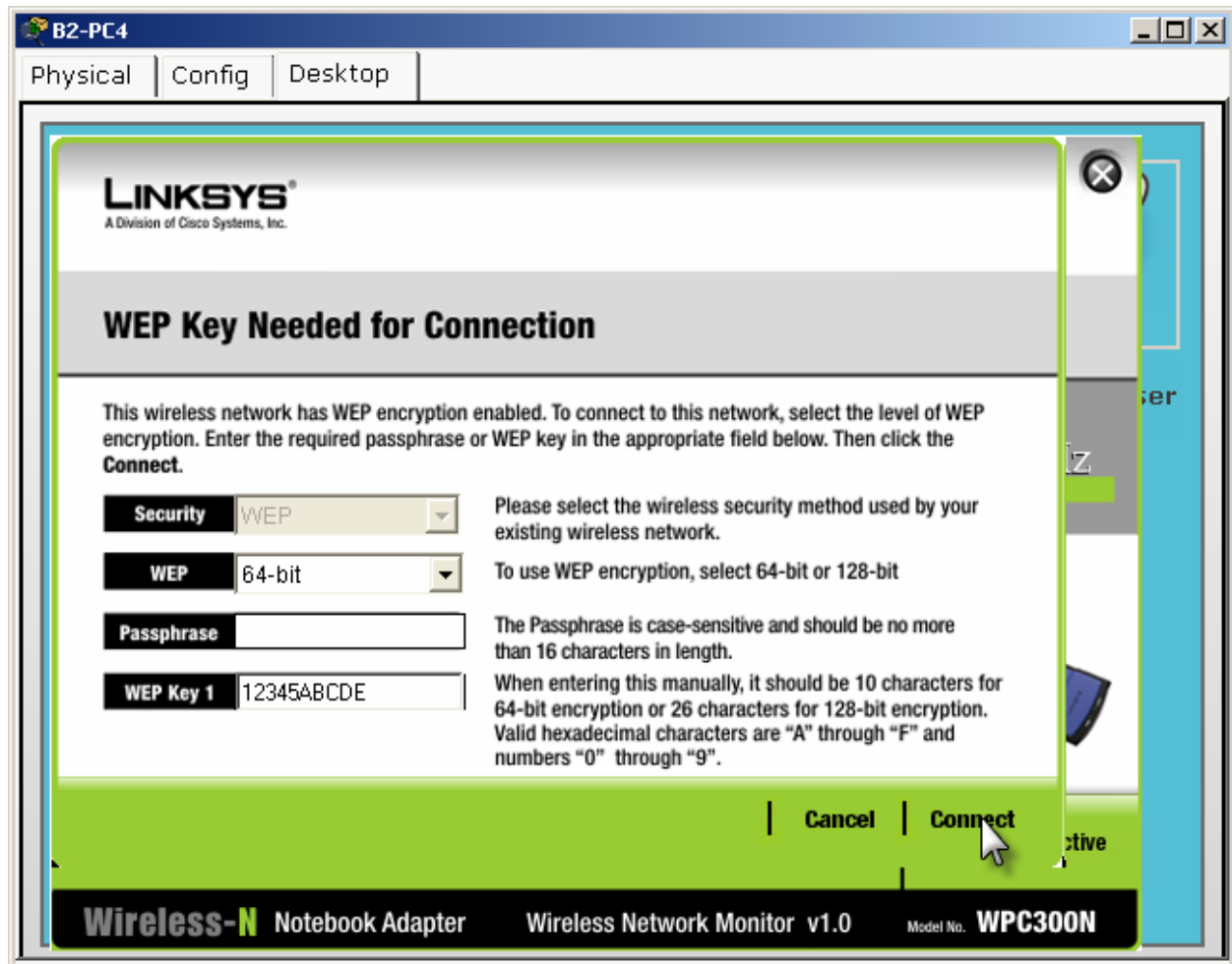
**步骤 4. 配置无线路由器允许远程访问。**

将管理口令配置为 **cisco123** 并启用远程管理。



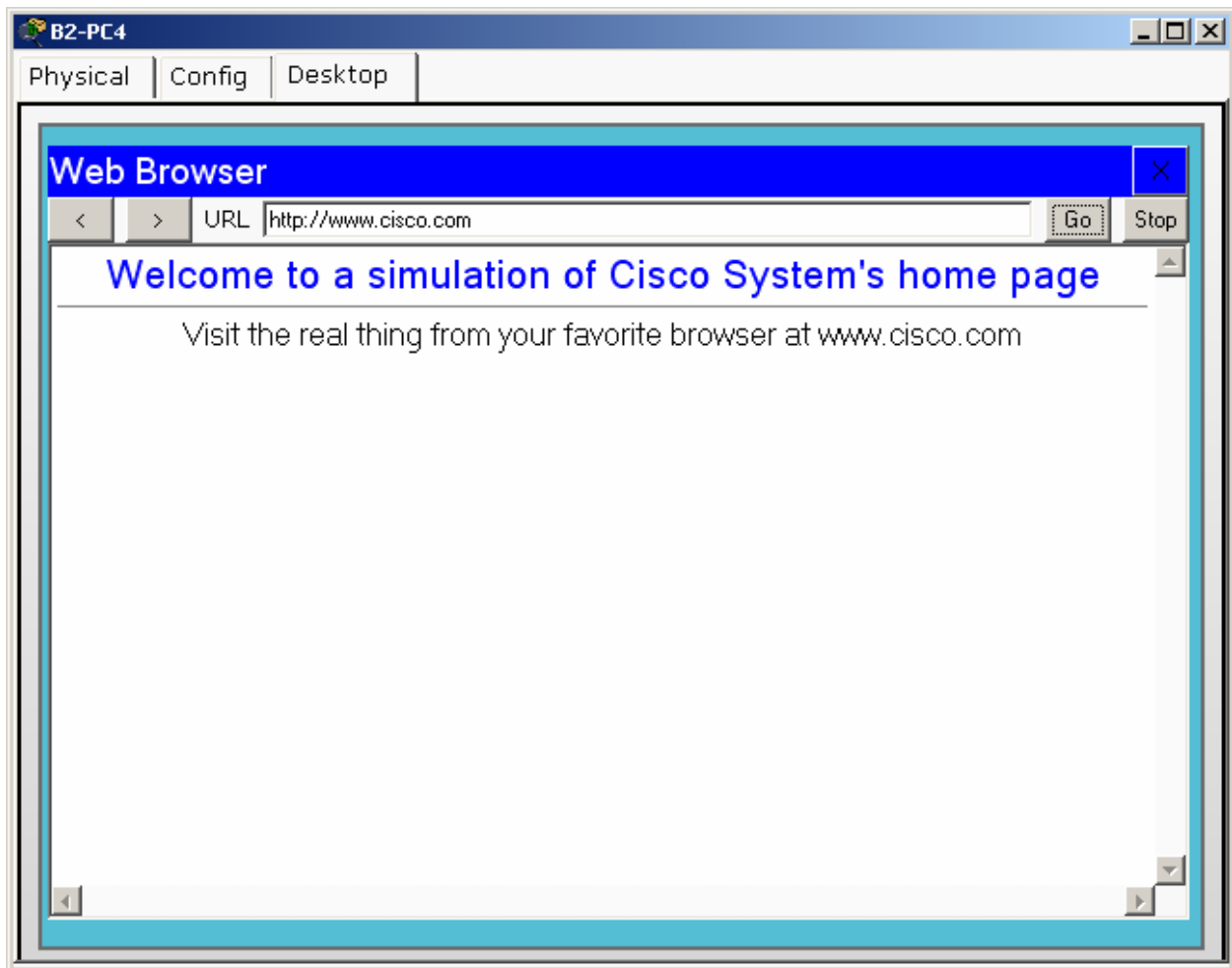
步骤 5. 配置 BX-PC4 PC，使这些 PC 能用 DHCP 访问无线网络。



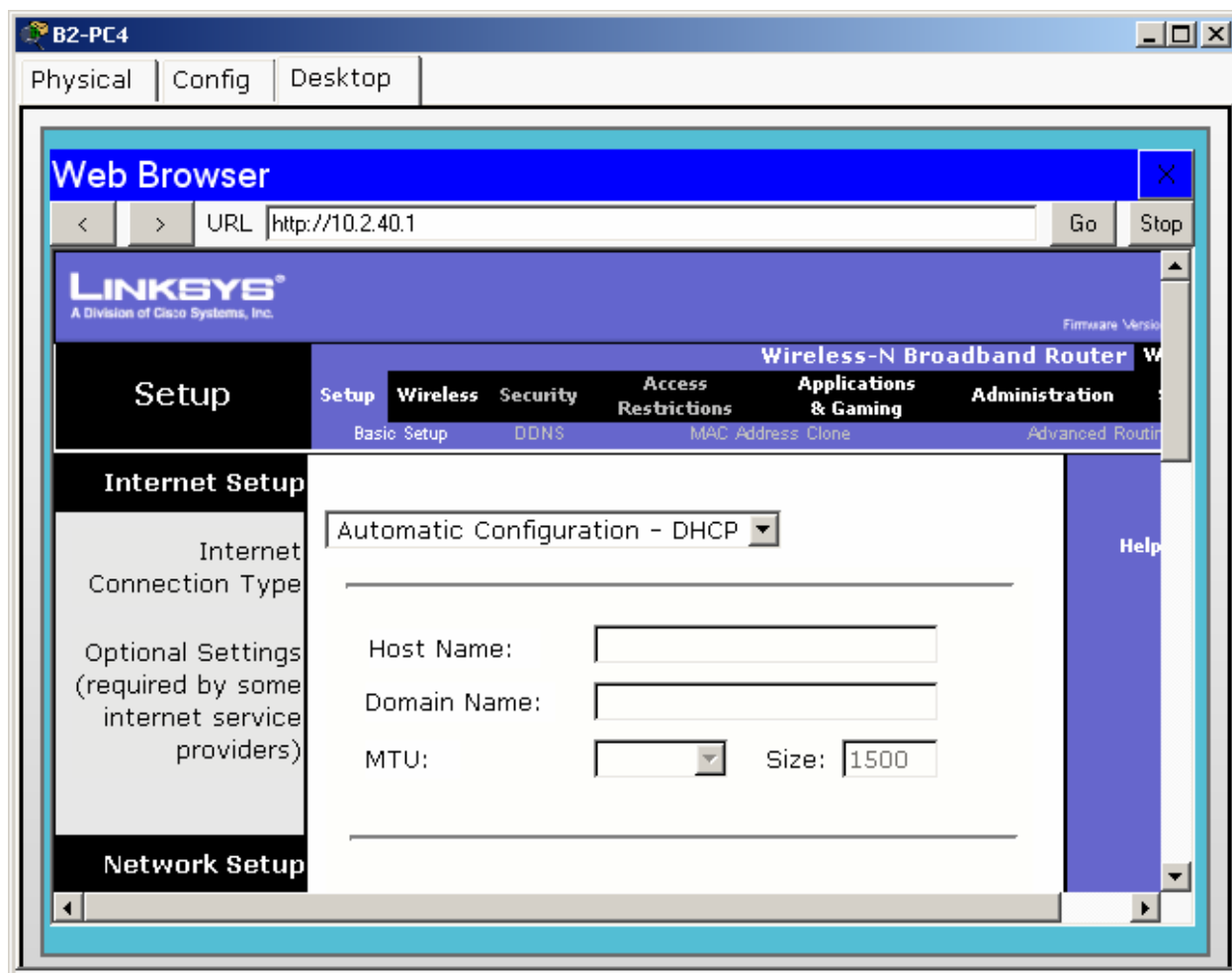


**步骤 6. 检验连通性以及远程管理功能。**

每台无线 PC 应该能够访问 [www.cisco.com](http://www.cisco.com) Web 服务器。



请通过 Web 浏览器访问无线路由器，以此检验远程管理功能。



### 任务 13：网络故障排除

#### 步骤 1. 中断网络。

一名学生离开实验室（如有必要），同时另一名学生破坏配置。

#### 步骤 2. 排查问题。

先前离开学生返回实验室，然后使用故障排除技术排查并解决问题。

#### 步骤 3. 再次中断网络。

两名学生互换角色，并重复步骤 1 和 2。