《计算机网络系统》路由交换系列实验-1

IPv4 子网划分与路由器、交换机基础配置

设计编辑：张翔、张超魁（电子科技大学信软学院）

一、实验名称：IPv4 子网划分与路由器、交换机基础配置

二、实验学时：4 学时

三、实验目的

1. 掌握 IP 子网划分基本原则，可根据需求开展 IPv4 子网划分最优设计；
2. 掌握交换机与路由器命令行各种操作模式的区别，能够使用各种帮助信息，以及用命令进行基本的配置；
3. 掌握网络设备 IP、端口的配置，通过对网络设备的相关的安全操作提升安全意识。

四、实验原理

1. IP 地址及子网划分

IP 地址是分配给主机或路由器接口的标识符，接口（Interface）是主机/路由器与物理链路之间的边界，路由器有多个接口，主机可以有多个接口，每个接口有一个 IP 地址。以下为 IP 地址及子网划分的主要说明：

- IP 地址有两种：IPv4 和 IPv6，IPv4 为 32 个二进制位长（4 字节），常用点分十进制表示；IPv6 为 128 个二进制位长（16 字节），常用冒号分隔表示。
- IP 地址包括两部分，高位数 bits 标识网络号，其指明主机所在网络的编号，剩余的地位是主机号，它是主机在网络中的编号。网络号相同的 IP 地址属于同一个网络。而网络还可以划分为若干子网（subnet）。划分子网的方法是从主机号借用若干个比特作为子网号，剩下的主机位为主机号。从 IP 地址的观点看，子网中设备接口的 IP 地址具有同样的网络部分，没有路由器的介入，物理上能够相互到达。
- 子网号字段长度是可变的，为了确定子网地址，IP 协议提供了子网掩码的概念。子网掩码用来确定网络地址（包括网络号和子网号）和主机地

址的长度。子网掩码长为 32 位比特，其中的 1 对应于 IP 地址中的网络号和子网号，而子网掩码中的 0 对应于主机号。

- 目前通常使用 CIDR 进行地址的分配与网络路由。其使用斜线记法，又称为 CIDR 记法，用于区分网络前缀和主机号，即在 IP 地址后面加上一个斜线“/”，斜线后用数字指定网络前缀的长度。CIDR 将网络前缀都相同的连续的 IP 地址组成“CIDR 地址块”。一个 CIDR 地址块可以表示分类 IP 的多个分类地址，这种地址的聚合称为路由聚合，又称为构造超网。
- 子网划分的步骤通常为：

(1) 确定主机总数：必须具有足以支持全部设备的地址块，这些设备包括终端用户设备、服务器、中间设备和路由器接口。

(2) 确定网段数量和大小：对这个网络，考虑网络的总数和每个网络中主机数量，将网络划分为子网，以此解决地点、大小和控制存在的问题。

(3) 执行 IPv4 地址分配：根据计算所知的网段数量和每个网段的主机数量，从整个地址块中分配地址；需要注意每个网段中真正可分配给接口使用的地址都需要减去 2 个地址：网络地址和广播地址。

2. IOS 设备及其接口

IOS（Internetwork Operating System，互联网操作系统）是 Cisco 公司为其网络设备开发的操作维护系统。大多数 Cisco 设备都会使用 Cisco IOS，包括路由器、交换机等。一般对 IOS 设备的配置需要使用命令行界面(CLI)。

一个典型的 Cisco 路由器如图 1 所示（此路由器型号为 Cisco 1841）：

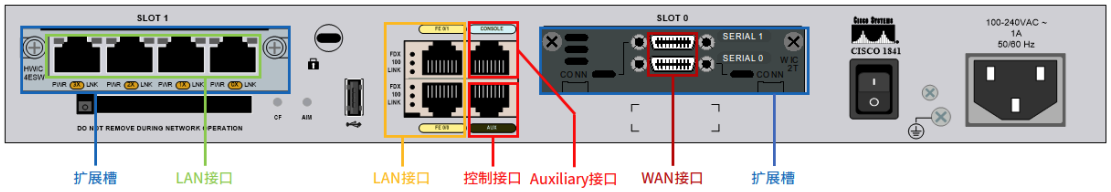


图 1 Cisco 1841 路由器背面接口图

除了电源相关，我们可以找到如下接口：

(1) Console 控制台接口：用作在本地连接到电脑，并用电脑配置设备的接口，在设备上未配置网络或发生故障时也可访问该端口，常用于初次配置网络设备、在远程访问不可行时进行灾难恢复和故障排除、口令恢复规程，一般仅可在能够物理接触网络设备时使用。

(2) AUX 接口：这是一个辅助接口，此接口可以连接调制解调器（modem）并通过电话拨号连接建立会话，此方法不需要在设备上配置或提供任何网络服务，这一点与控制台连接相似。此端口也可以与 Console 口一样本地访问，但应优先使用控制台端口，一般只有在使用控制台端口有问题时（例如，不清楚某些控制台参数），才需要从本地使用辅助端口替代控制台端口。并非所有网络设备都有 AUX 接口。

(3) 网络接口：用于连接其他网络设备或主机。网络接口有 WAN 口与 LAN 口之区别。这里的 WAN 口是串行口，可以连接广域网上的其他路由器。LAN 口分为两种，中间黄色框中是路由器默认具有的，可以配置 IP 地址等作为网关，左面扩展槽中的是交换机中默认具有的，其仅具有交换功能，可以为其配置所属 VLAN。此外常见的网络接口还包括光纤接口等。

(4) 扩展插槽：通过扩展卡可以扩展网络设备的接口，如这一台路由器插入了两张扩展卡，左边的是 HWIC-4ESW，其提供了 4 个交换接口，右边是 WIC-2T，其提供了两个串行口。

3. IOS 执行模式

Cisco IOS 设计为模式化操作系统，其包含多种工作模式，每种模式有各自的工作领域。对于这些模式，CLI 采用了层次结构。从上到下，主要的模式有以下几种：

(1) 用户执行模式：进入设备后得到的第一个操作模式，该模式下可以简单查看设备的软、硬件版本信息，并进行简单的测试。提示符为 Device>。

(2) 特权执行模式：由用户模式进入的下一级模式，该模式下可以对设备的配置文件进行管理，查看设备的配置信息，进行网络的测试和调试等。提示符为 Device#。

(3) 全局配置模式：属于特权模式的下一级模式，该模式下可以配置设备的全局性参数（如主机名、登录信息等）。在该模式下可以进入下一级的配置模式，对交换机具体的功能进行配置。提示符为 Router(config)#

(4) 其他特定配置模式：针对特定服务的配置，例如交换机可以进入端口模式进行参数配置，路由器可以在此制定特定的路由过程。提示符为 Device(config-mode)#

(5) 图 2 显示了模式间切换的命令：

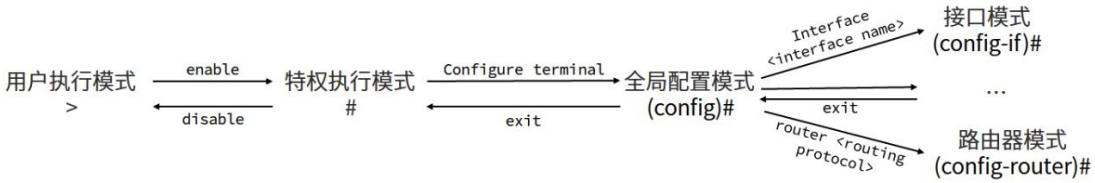


图 2 IOS CLI 中模式切换的命令

4. 基本 IOS 命令与配置

每个 IOS 命令都具有特定的格式或语法，并在相应的提示符下执行。命令大小写不敏感。常规命令语法为命令字后接相应的关键字和参数。下面将分类介绍基本的 IOS 命令。

4.1 检查命令 show

show 是最基本的检查命令，使用 show ?可以获得当前上下文或模式下可以检查的内容。常用的有：

```
//显示设备 ARP 表
show arp
//显示交换机的 MAC 表（只用于交换机）
show mac-address-table
//显示路由器上所有接口的统计信息。
show ip interfaces
//查看某个接口的信息可以使用
show ip interfaces <interfaces name>
//获得接口及其运行状态的摘要信息
show ip interface brief
//显示设备上所有接口的统计信息
show interfaces
//查看某个具体接口的统计信息
show interfaces <interfaces name>
//显示当前加载的软件版本以及硬件和设备相关的信息
show version
```

4.2 命名设备

命名设备需要在全局配置模式模式下进行，如：

```
//修改设备名为 myrout
Router(config)# hostname myrout
myrout(config)#
//删除设备名称
myrout(config)# no hostname
Router(config)#
```

4.3 限制设备访问

交换机、路由器一般放在机房中上锁机的机柜里，可以限制人员物理接触，但是口令仍是防范未经授权的人员访问网络设备的主要手段。必须从本地为每台设备配置口令以限制访问。

IOS 使用分层模式来提高设备安全性。作为此安全措施的一部分，IOS 可以通过不同的口令来提供不同的设备访问权限。

4.3.1 控制台口令

控制台口令用于限制通过控制台连接的访问。

可在全局配置模式下使用下列命令来为控制台线路设置口令：

//从全局配置模式进入控制台线路配置模式。0 代表设备的第一个（而且在大多数情况下是唯一的一个）控制台接口

```
Router(config)# line  console  0
//指定<password>作为这条线路的口令
Router(config-line)# password  <password>
```

//配置要求用户登录时进行身份验证；当启用登录且设置口令后，设备在用户登录时会提示用户输入口令

```
Router(config-line)# login
```

一旦这三个命令执行完成后，每次用户尝试访问控制台端口时，都会出现要求输入口令的提示。

4.3.2 Enable 口令和 Enable 加密口令

限制访问特权执行模式 enable password(较老版本,不推荐)命令或 enable secret 命令（推荐，设置的口令会被加密）可提供更多的安全性。这两个口令都可用于在用户访问特权执行模式（使能模式）前进行身份验证：

Router(config)# enable secret <password>

4.3.3 VTY 口令

限制通过 Telnet、SSH 的访问 VTY(虚拟终端)线路使用户可通过 Telnet 访问路由器。通过(config)# line vty 0 ？ 可以看到设备最大支持的 VTY 线路数量。所有可用的 VTY 线路均需要设置口令。可为所有连接设置同一个口令。下列命令用于为 VTY 线路设置口令（以最大支持 4 个 VTY 的设备为例）：

Router(config)# line vty 0 4

Router(config-line)# password <password>

Router(config-line)# login

4.3.4 口令显示加密

Router(config)# service password-encryption

可在显示配置文件（show running-config）时防止将口令显示为明文。

4.3.5 配置最短密码长度

Router(config)# security passwords min-length <0-16>

最短密码长度可设为 0-16 中的一个值。

该命令可以影响以后创建的所有用户密码、特权（加密）密码、线路密码，但不会影响现有的路由器密码。

4.3.6 标语消息

标语是用作向试图访问设备的人员声明仅授权人员才可访问设备的。一种常用的标语是当日消息（MOTD），其配置方法如下：

Router(config)# banner motd #<message>#

4.3.7 管理配置文件

//把当前配置拷贝到 TFTP 服务器上

copy running-config tftp:

输入命令后回车,在下面的提示后面输入 tftp server 的 ip 地址

Address or name of remote host []?

//同上

write network

//把当前配置写入 NVRAM 保存，覆盖当前的启动配置

copy running-config startup-config

//同上

write

//把当前配置输出到终端上

write terminal

//同上

show run

4.3.8 设备远程访问的安全性

网络管理员可以使用 Console 端口以本地方式访问到设备，这是最安全的方式，但其工作量很大，每次都本地连接也不现实，远程访问会更方便，但如果实现方式不安全则容易造成信息泄露。

Telnet 远程管理访问很不安全，因为其以明文方式发送网络数据流，攻击者可以对其进行监听窃取信息，因此需要提高远程访问的安全性。增强安全性，首先要保护管理线路（VTY），然后配置网络设备使其加密 SSH 隧道中的数据流。

在设备中配置 SSH 的步骤如下：

1) 配置设备主机名：SSH 要求设备不使用默认主机名。

2) 配置域名：必须有域名才能启用 SSH

Router(config)# ip domain-name <domain_name>

3) 生成 RSA 非对称密钥。

需要创建一个密钥供路由器加密其 SSH 管理数据流，为此可在全局配置模式下使用命令 crypto key generate rsa：

Router(config)# crypto key generate rsa

…

How many bits in the modulus [512]: 1024

% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

在输入第一条命令后会要求指定密钥长度，建议密钥长度不小于 1024。

4) 配置本地身份认证和 VTY：

//进入线路配置模式

Router(config)# line vty 0 4

//清除原有登录协议

Router(config-line)# no transport input

//让 VTY 接收 SSH 连接

Router(config-line)# transport input ssh

//根据本地数据库进行身份验证

Router(config-line)# login local

//退出线路配置模式，回到全局配置模式

Router(config)# exit

5) 配置 SSH 超时（可选）

//设置超时时间（不活动退出时间，这里设置为 15s）

Router(config)# ip ssh time-out 15

//设置重试次数（这里设置为 2 次）

Router(config)# ip ssh authentication-retries 2

4.3.9 创建新用户

Username 命令可以创建新用户，并指定用户权限、密码等，常用的命令为：

username <name> [secret <password> | privilege <level>]

用户特权等级分为 0-15 级，0 最低，15 最高。

使用 no username <name> 可以删除已创建的用户。

5. 设备接口配置

5.1 启用接口

路由器接口默认被禁用。要启用接口，需要在接口配置模式下输入 no shutdown 命令。如果因维护或故障排除而需要禁用接口，需使用 shutdown 命令。

5.2 配置路由器以太网接口

路由器以太网接口用作局域网中直接连接到路由器的网络中的终端设备的网关。每个以太网接口必须拥有一个 IP 地址和一个子网掩码才能路由 IP 数据包。

//在全局配置模式进入接口配置模式

Router(config)# interface FastEthernet 0/0

//指定接口 IP 地址和子网掩码

Router(config-if)# ip address <ip_address> <netmask>

//启动接口

Router(config-if)# no shutdown

IPv6 地址的配置与之类似，其在端口配置模式下使用 ipv6 address 命令：

Router(config-if)# ipv6 address <ipv6-prefix>/<prefix-length>

请注意前缀长度的使用。

当在一个节点启用 IPV6，启动时节点的每个接口自动生成一个 link-local address。对这个地址的配置可以使用下面的命令：

Router(config-if)# ipv6 address <ipv6-address>/<prefix-length> link-local

也就是在 IPv6 地址配置的后面加上 link-local。

另外需要注意到是，要在路由器上转发 IPv6 流量，需要使用全局配置命令 ipv6 unicast-routing 在路由器上启用 IPv6 单播数据报的转发。

5.3 接口描述

正如主机名可帮助在网络中标识设备一样，接口描述用于说明接口的用途。应该在配置每个接口的过程中描述接口的作用以及接口连接的位置，有助于排除故障。

使用 description 命令可以创建接口描述：

Switch#configure terminal

Switch(config)# interface fa0/0

Switch(config-if)# description <description>

5.4 配置交换机虚拟接口（SVI，Switch Virtual Interface）

要管理交换机，需要为其分配地址。为交换机分配 IP 地址后，它就像主机设备。一旦分配好地址后，就可通过 Telnet、SSH 或 Web 服务访问该交换机。

交换机的地址被分配给称为虚拟局域网接口（VLAN）的虚拟接口。大多数情况下，该接口为 VLAN 1（通常作为交换机远程管理接口）。下面显示了为 VLAN 1 接口分配了一个 IP 地址。此接口与路由器的物理接口相似，需要通过 no shutdown 命令启用此接口。交换机与其他任何主机一样，也需要一个网关地址才能与本地网络之外的设备通信。可以使用 ip default-gateway 命令分配了此网关。

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip address <ip_address> <netmask>
Switch(config-if)# no shutdown
Switch(config-if)# exit
Switch(config)# ip default-gateway <ip_address>
Switch(config)# exit
Switch#
```

五、实验内容

实验拓扑如图 3 所示：

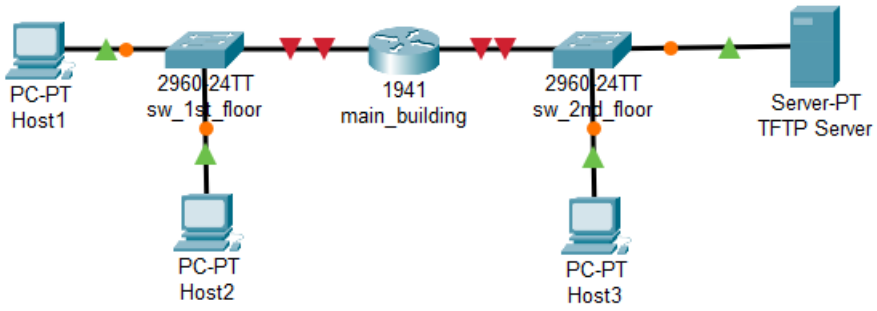


图 3 实验使用的拓扑

实验要求执行 IPv4/IPv6 网络配置，实现全网互联互通，并将设备配置备份到 TFTP 服务器。IPv4 地址与 IPv6 地址需要同时配置，且还需要激活交换机的管理接口。所有 IOS 设备配置应该从终端直接连接到设备控制台完成。

(1) 路由器 main_building：

路由器初始化配置

接口配置以及 IPv4 和 IPv6 地址配置

设备安全性相关配置

SSH 访问配置

将配置文件备份到 TFTP 服务器

(2) 交换机 sw_2nd_floor：

启用基本远程配置，即可以通过 Telnet 连接配置交换机

(3) PC 和服务器主机：

IPv4 与 IPv6 地址配置

全网地址配置表如下：

Device	Interface	IPv4 Address	Subnet Mask	IPv4 Default Gateway
		IPv6 Address		IPv6 Default Gateway
main_building	G0/0			N/A
		2001:DB8:ACAD:A::1/64		N/A
	G0/1			N/A
		2001:DB8:ACAD:B::1/64		N/A
	Link Local	FE80::1		N/A
sw_1st_floor	Vlan 1			
		N/A	N/A	N/A
sw_2nd_floor	Vlan 1			
		N/A	N/A	N/A
Host 1	NIC			
		2001:DB8:ACAD:A::FF		
Host 2	NIC			
		2001:DB8:ACAD:A::15		
Host 3	NIC			
		2001:DB8:ACAD:B::FF		
TFTP Server	NIC			
		2001:DB8:ACAD:B::15		

六、实验器材

Packet Tracer

七、实验步骤

1. 确定 IPv4 编址方案，并完成如下地址表：

Subnet Number	Hosts Available	Network Address	Beginning Address	Ending Address	Mask	Assignment
1	30	192.168.1.0				
2						
3						
4						
5						
6						

(1) 以浪费最少的原则进行 192.168.1.0/24 子网划分，每个子网提供 30 个主机地址。

30 台主机，需要 5 个主机比特位，因此子网的比特位是 3 位，子网掩码；255.255.255.224。11100000=224

第 1 个子网；000 00001-000 11110

第 2 个子网：

(2) 将第四个子网分配给 First Floor LAN。

在表中记录下来，作为后续 ip 地址分配的依据

(3) 将此子网中的最后一个网络主机地址分配给 main_building 上的 G0/0 接口。

(4) 从第五个子网开始，再次对网络进行子网划分，在浪费最少的地址的基础上新子网将为每个子网提供 14 个主机地址。

子网 5;100 0 xxxx 100 0 0001-100 0 1110【129-142】

100 1 xxxx 10010001-10011110【145-158】

192.168.1.145-192.168.1.158

(5) 将这些新的 14 主机子网中的第二个分配给二楼 LAN。

(6) 将第二层 LAN 子网中的最后一个网络主机地址分配给主楼路由器的 G0 / 1 接口。

G0 / 1=192.168.1.158 2552.255.255.224

(7) 将第该子网倒数第二个地址分配给第二层交换机的 VLAN 1 接口。

192.168.1.157

(8) 将所在子网中任意一个其他地址分配给相应主机。

2. 配置主楼 Router

(1)初始化路由器

选择一台 PC，用控制线连接 PC 的 RS232 接口到路由器的 Console 接口，在 PC 的终端对路由器进行配置

①将路由器 hostname 修改为“main_building”；

相关命令参见 4.2

```
Router#configure terminal
Router(config)#hostname main_building
Middle(config)#
```

②使用加密的特权执行模式密码保护设备配置；

相关命令参见 4.3.2，注意:根据要求应使用 enable secret 命令，不要用 enable password 命令

```
Middle(config)#enable secret 123
```

③设置标语，这一项在 PT 在线考试中没有明确要求，但为一个得分点

```
Middle(config)#banner motd    #message-test#
```

④将路由器的所有访问线路加密；

需要加密 console(控制台)和 vty(虚拟终端)线路

控制台线路加密相关命令参见 4.3.1

```
Middle(config)#line console 0
Middle(config-line)#password 123
Middle(config-line)#login
```

虚拟终端线路加密相关命令参见 4.3.3

```
Middle(config)#line vty 0 4
Middle(config-line)#password 123
Middle(config-line)#login
```

⑤要求新输入的密码的最小长度必须为 10 个字符；

配置最短密码长度，相关命令参见 4.3.5

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

⑥防止在设备配置文件中以明文形式查看所有密码；

口令显示加密，参见 4.3.4

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

⑦将路由器配置为仅接受比 Telnet 更安全的协议上的带内管理连接（SSH），使用值 1024 作为加密密钥强度；

即配置 SSH，相关命令参见 4.3.8

```
Middle (config)# ip domain-name smurfs
Middle (config)# crypto key generate rsa
…
How many bits in the modulus [512]: 1024 #题目要求 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
Middle (config)# line vty 0 4
//清除原有登录协议
Middle (config-if)# no transport input
//让 VTY 接收 SSH 连接
Middle (config-if)# transport input ssh
//根据本地数据库进行身份验证
```

```
Middle (config-if)# login local
//退出线路配置模式，回到全局配置模式
Middle (config)# exit
```

⑧为带内管理连接配置本地用户身份验证，创建一个名称为 netadmin 且密码为 Cisco_CCNA5 的用户，为该用户提供最高的管理特权；

即创建新用户，相关命令参见 4.3.9

```
Middle(config)#username netadmin privilege 15 secret Cisco_CCNA5
```

(2)使用计算的 IPv4 地址值和地址表中提供的 IPv6 值配置两个千兆以太网接口。

①将 link-local 地址重新配置为表中所示的值；

Link-local 地址的配置命令参见 5.2

②在配置文件中记录接口

配置接口描述,相关命令参见 5.3

G0/0 配置命令如下，G0/1 同理:

```
//进入 g0/0
Router(config)#interface g0/0
//配置 IPV4 地址及子网掩码
Router(config-if)#ip address 192.168.1.126 255.255.255.224
//配置 IPV6 地址
Router(config-if)#ipv6 address 2001:DB8:ACAD:A::1/64
//配置 link local
Router(config-if)#ipv6 address FE80::1 link-local
//激活接口
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed state to up
//配置接口描述
Router(config-if)#description connect to First Floor
```

3. 配置第二层交换机

配置第二层交换机以通过 Telnet 进行远程管理。

选择一台 PC，用控制线连接 PC 的 RS232 接口到交换机的 Console 接口，在 PC 的终端对交换机进行配置

需要进行的配置包括:

1.交换机 vlan 1 接口的 ipv4 地址，子网掩码，以及默认网关，相关命令参见 5.4

```
Switch_2(config)#int vlan1
Switch_2(config-if)#no shut
Switch_2(config-if)#
%LINK-5-CHANGED: Interface Vlan1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
Switch_2(config-if)#ip add 192.168.1.157 255.255.255.240
Switch_2(config-if)#exit
//交换机默认网关配置，要在全局配置模式下进行
Switch_2(config)#ip default-gateway 192.168.1.158
```

2.配置 vty 口令

```
Switch_2(config)#line vty 0 4
Switch_2(config-line)#password 123
Switch_2(config-line)#login
```

4. 配置验证主机地址

(1) 使用步骤 1 中的 IPv4 地址和地址表中的 IPv6 地址值，为所有 PC 配置正确的寻址；

(2) 使用路由器接口 link-local 地址作为主机上的 IPv6 默认网关。

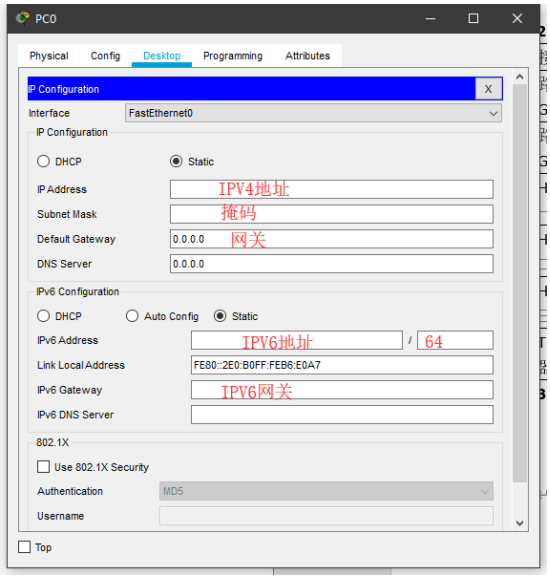
注意事项:

1.避免同一 LAN 内设备 IP 地址冲突

2.ip 地址配置界面进入方式: 点击设备，Desktop→IP Configuration

3.主机需要配置的内容包括: ipv4 地址，子网掩码(注意修改为正确值)，ipv4 默认网关(即主机所属 LAN 连接的路由器接口的 ipv4 地址)，ipv6 地址(注意/后面

需要填写网络前缀长度，本例中为 64，否则无法完成配置)，ipv6 默认网关



5. 将主楼路由器的配置备份到 TFTP

(1) 使用步骤 1 中的 IPv4 地址和地址表中的 IPv6 地址值来完成 TFTP 服务器的配置；

将 TFTP 服务看作一台 PC，ip 地址配置要求同上面的主机地址配置

(2) 将主楼的运行配置备份到 TFTP Server，使用默认文件名。

相关命令参见 4.3.7 第一条命令

```
Middle#copy running-config tftp:
Address or name of remote host []? 192.168.1.146
```

八、在线考试得分点

Performance Component: IP Addressing Design

Work Product Feature	Reason for Incorrect
IP Addressing Design	
IPv4 LAN 1 Subnet Mask Calculation	
Network:[[PC1Name]]:Ports:FastEthernet0:Subnet Mask	*PC1 子网掩码错误*
Network:[[PC2Name]]:Ports:FastEthernet0:Subnet Mask	*PC2 子网掩码错误*
IPv4 LAN 2 Subnet Mask Calculation	

Network:[[PC3Name]]:Ports:FastEthernet0:Subnet Mask	*PC3 子网掩码错误*
Network:TFTP Server:Ports:FastEthernet0:Subnet Mask	*TFTP Server 子网掩码错误*
LAN 1 IPv4 Host Addressing Design and Implementation	
Network:[[PC1Name]]:Ports:FastEthernet0:IP Address	*PC1 Ipv4 地址错误*
Network:[[PC2Name]]:Ports:FastEthernet0:IP Address	*PC1 Ipv4 地址错误*
LAN 2 IPv4 Host Addressing Design and Implementation	
Network:[[PC3Name]]:Ports:FastEthernet0:IP Address	*PC3 Ipv4 地址错误*
Network:TFTP Server:Ports:FastEthernet0:IP Address	*TFTP Server Ipv4 地址错误*

Performance Component: IPv6 Host Address Configuration

Work Product Feature	Reason for Incorrect
IPv6 Host Address Configuration	
LAN 1 IPv6 Host Address Configuration	
Network:[[PC1Name]]:Ports:FastEthernet0:Ipv6 Address:2001\:DB8\:ACAD\:A\:\:FF:IP Address	*PC1 IPV6 地址错误*
Network:[[PC2Name]]:Ports:FastEthernet0:Ipv6 Address:2001\:DB8\:ACAD\:A\:\:15:IP Address	*PC1 IPV6 地址错误*
LAN 2 IPv6 Host Address Configuration	
Network:[[PC3Name]]:Ports:FastEthernet0:Ipv6 Address:2001\:DB8\:ACAD\:B\:\:FF:IP Address	*PC3 IPV6 地址错误*
Network:TFTP Server:Ports:FastEthernet0:Ipv6 Address:2001\:DB8\:ACAD\:B\:\:15:IP Address	*TFTP Server IPV6 地址错误*

Performance Component: Router Interface Configuration and Addressing

Work Product Feature	Reason for Incorrect
Router Interface Configuration and Addressing	
Router Interface Activation	
Network:[[Router0Name]]:Ports:GigabitEthernet0/0:Power	*配置路由器 G0/0 接口时，没有用 no shutdown 命令激活接口*
Network:[[Router0Name]]:Ports:GigabitEthernet0/0:Description	*没有配置 G0/0 接口的描述信息*
Network:[[Router0Name]]:Ports:GigabitEthernet0/1:Power	*配置路由器 G0/1 接口时，没有用 no shutdown 命令激活接口*
Network:[[Router0Name]]:Ports:GigabitEthernet0/1:Description	*没有配置 G0/0 接口的描述信息*
Router Interface G0/0 IPv4 Addressing	
Network:[[Router0Name]]:Ports:GigabitEthernet0/0:IP Address	*G0/0 接口 ipv4 地址错误*

Network:[[Router0Name]]:Ports:GigabitEthernet0/0:Subnet Mask	*G0/0 接口子网掩码错误*
Router Interface G0/1 IPv4 Addressing	
Network:[[Router0Name]]: Ports:GigabitEthernet0/1:IP Address	*G0/1 接口 ipv4 地址错误*
Network:[[Router0Name]]:Ports:GigabitEthernet0/1:Subnet Mask	*G0/1 接口子网掩码错误*
Router Interface G0/0 IPv6 Addressing	
Network:[[Router0Name]]:Ports:GigabitEthernet0/0:Ipv6 Address:2001\:DB8\:ACAD\:A\:\:1:IP Address	*G0/0 接口 ipv6 地址错误*
Network:[[Router0Name]]:Ports:GigabitEthernet0/0:Link Local	*G0/0 接口 ipv6 link-local 地址错误或没有配置*
Router Interface G0/1 IPv6 Addressing	
Network:[[Router0Name]]:Ports:GigabitEthernet0/1:Ipv6 Address:2001\:DB8\:ACAD\:B\:\:1:IP Address	*G0/1 接口 ipv6 地址错误*
Network:[[Router0Name]]:Ports:GigabitEthernet0/1:Link Local	*G0/1 接口 ipv6 link-local 地址错误或没有配置*

Performance Component: Host Default Gateway Configuration

Work Product Feature	**Reason for Incorrect**
Host Default Gateway Configuration	
LAN 1 Hosts Default Gateway Configuration	
Network:[[PC1Name]]:Default Gateway	*PC1ipv4 默认网关错误*
Network:[[PC1Name]]:Default Gateway IPv6	*PC1 IPV6 默认网关错误*
Network:[[PC2Name]]:Default Gateway	*PC2ipv4 默认网关错误*
Network:[[PC2Name]]:Default Gateway IPv6	*PC2 IPV6 默认网关错误*
LAN 2 Hosts Default Gateway Configuration	
Network:[[PC3Name]]:Default Gateway	*PC3 ipv4 默认网关错误*
Network:[[PC3Name]]:Default Gateway IPv6	*PC3 IPV6 默认网关错误*
Network:TFTP Server:Default Gateway	*TTFP Server ipv4 默认网关错误*
Network:TFTP Server:Default Gateway IPv6	*TFTP Server 默认网关错误*

Performance Component: Switch Management Interface

Work Product Feature	**Reason for Incorrect**
Switch Management Interface	
Switch Management Interface	
Network:[[Switch2Name]]:Ports:Vlan1:Power	*Switch2 vlan1 接口没有用 no shutdown 命令激活*
Network:[[Switch2Name]]:Ports:Vlan1:IP Address	*Switch2 vlan1 接口 ipv4 地址错误*
Network:[[Switch2Name]]:Ports:Vlan1:Subnet Mask	*Switch2 vlan1 接口子网掩码错误*

Network:[[Switch2Name]]:Default Gateway	*Switch2 默认网关错误或没有配置*
Network:[[Switch2Name]]:VTY Lines:0:Password	*Switch2 没有配置 vty 加密*

Performance Component: Initial Device Configuration

Work Product Feature	Reason for Incorrect
Initial Device Configuration	
Basic Router Configuration	
Network:[[Router0Name]]:Host Name	*对路由器，没有配置正确的主机名*
Network:[[Router0Name]]:Enable Secret	*没有配置特权模式访问加密*
Network:[[Router0Name]]:Banner motd	*没有配置标语*
Secure Router Communication Lines	
Network:[[Router0Name]]:Console Line:Login	*没有用 login 命令开启登陆验证*
Network:[[Router0Name]]:Console Line:Password	*没有配置控制台线路密码*

Performance Component: Device Hardening

Work Product Feature	Reason for Incorrect
Device Hardening	
Enhance Router Password Security	
Network:[[Router0Name]]:Service Password Encryption	*路由器没有配置口令显示加密*
Network:[[Router0Name]]:Security Password Min-Length	*没有配置最短密码长度*
Router SSH Configuration	
Network:[[Router0Name]]:VTY Lines:0:Transport Input	*没有清除原有登录协议并接收 ssh 连接*
Network:[[Router0Name]]:VTY Lines:0:Login	*没有用 login 命令开启登陆验证*
Network:[[Router0Name]]:IP Domain Name	*没有配置域名*
Network:[[Router0Name]]:User Names:Username	*创建用户时使用的用户名错误*
Network:[[Router0Name]]:Security:Modulus Bits	*未配置正确的密钥大小*