《计算机网络系统》路由交换系列实验-3

静态（默认）路由与 DHCP、NAT

设计编辑：张翔、张超魁

一、实验名称：DHCP、NAT 与静态路由及默认路由

二、实验学时：4 学时

三、实验目的

1. 理解动态主机配置协议 DHCP 与网络地址转换协议 NAT 的基本原理，掌握基于 ACL 的 DHCP 与 NAT 配置应用；
2. 理解掌握静态路由以及默认路由的基本原理，且能正确加以配置应用；
3. 具备在大型园区网络中面向需求开展 DHCP、NAT、ACL 配置设计与配置的能力。

四、实验原理

1. 静态（默认）路由

(1) 静态路由

从一个网络路由到短截网络（只能通过单条路由访问的网络），一般使用静态路由。

配置静态路由采用如下命令：

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

- dest_address：要加入路由表的远程网络的目的网络地址；
- mask：要加入路由表的远程网络的子网掩码；
- ip-address：指定可用于到达该网络的下一跳路由器的 IP 地址；
- exit_interface：将数据包转发到目的网络时使用的送出接口；
- administrative_distance：路由优先级，有效范围是 1 – 255，默认值为 1。

这一语句可以理解为：若待转发 IP 报文的目的 IP 符合 dest_address 与 mask

定义的网段，则将该 IP 报文发往下一跳 IP 地址为 ip-address 的邻居路由器，或直接从本地 exit_interface 接口发出。

metric-value 主要用在当一路由器有多条路径到达某一目的网络时，使用路由协议时一般会自动进行计算，对于静态路由可手动指定。

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

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

指定 IPv6 网段时，掩码使用前缀长度表达法。

(2) 默认路由

默认路由是一类特殊的静态路由，默认路由使用零或者没有比特匹配的方法来表示全部路由。换言之，如果没有一条具体路由被匹配，那么默认路由就将被匹配。

配置默认路由的语法类似于配置其他静态路由，但网络地址和子网掩码均为 0.0.0.0：

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

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

IPv6：全零路由地址为 ::/0

(3) 浮动静态路由

前面(1)中提到的静态路由可配置参数 administrative_distance(简称 AD)，用于标识路由的优先级。静态路由的 AD 默认值为 1（本地直连路由 AD 为 0），动态路由 AD 依据协议其默认值不同，但都大于 1。

到达同一目的地有多条路由时，路由器会选择优先级最高的路由(AD 值最低)。通过手动指定 AD 值，可以设置浮动静态路由，即作为当前优先级最高的路由的备份（比如将该静态路由的 AD 设置为高于某动态路由的 AD)，默认不使用（路由表中只会插入优先级最高的路由)。只有当优先级最高的路由失效时，该静态路由才会被插入路由表加以应用。

2. DHCP

每台连接到网络的设备都需要一个 IP 地址。网络管理员给路由器、服务器以及其他物理位置不太可能变化的网络设备手工分配静态 IP 地址。这些静态地址让管理员能够远程管理设备。

然而，组织中的台式机和笔记本电脑的物理位置经常发生变化，如果给这些主机手工分配地址，则每当员工搬到新办公室或隔间时，管理员都必须给它们重新分配地址。

同时，客户端计算机并非一定要使用静态地址。相反，管理员可指定一个地址池，让客户端借用其中的 IP 地址。工作站可使用地址池中的任何地址，因为地址池中的地址通常属于特定子网，且可给工作站分配位于其所属子网中的任何地址。而子网掩码、默认网关和 DNS 服务器可设置为适用于整个子网或网络的值。例如，同一个子网中的所有主机使用不同的主机 IP 地址，但使用的子网掩码和默认网关 IP 地址相同。

DHCP 使得 IP 地址的分配过程几乎是透明的。DHCP 动态地分配 IP 地址和其他重要的网络配置信息。

DHCP 有三种机制分配 IP 地址：

(1) **自动分配方式**：DHCP 服务器为主机指定一个永久性的 IP 地址，一旦 DHCP 客户端第一次成功从 DHCP 服务器端租用到 IP 地址后，就可以永久性的使用该地址。

(2) **动态分配方式**：DHCP 服务器给主机指定一个具有时间限制的 IP 地址，时间到期或主机明确表示放弃该地址时，该地址可以被其他主机使用。

(3) **手工分配方式**：客户端的 IP 地址是由网络管理员指定的，DHCP 服务器只是将指定的 IP 地址告诉客户端主机。

三种地址分配方式中，只有动态分配可以重复使用客户端不再需要的地址。

3. DHCPv4 配置应用

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

下面是将路由器配置成 DHCP 服务器的一般步骤：

(1) 指定待排除的地址

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

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

(2) 建立待分配地址池

下面的命令可以建立地址池并为其命名,执行命令后会进入 DHCP 配置模式。

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

(3) 配置可用网段信息：指定子网号和子网掩码，同时配置默认网关地址。

```
R1(config-config)# network <network_number> [<mask>]：定义可用地址范围
R1(config-config)# default-router <address> [<address2>...<address8>]：定义默认网关（路由器），至少指定一个，最多可指定 8 个
```

下面是其他一些可选网络信息配置，包括指定 DNS 服务器、指定域名等：

```
R1(config-config)# dns_server <address> [<address2>...<address8>]：指定 DNS 服务器，最多可指定 8 个
R1(config-config)# domain-name <domain>：指定域名
```

(4) 查看 DHCP 配置应用

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

```
R1# show ip dhcp binding
IP
address       Client-ID/ Hardware address    Lease expiration  Type

192.168.1.2   0060.5CB8.010D       --                    Automatic
192.168.1.3   000D.BDE1.D854       --                    Automatic
192.168.1.4   0007.ECEC.8DCB       --                    Automatic
```

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

```
Router#show ip dhcp pool

Pool test :
  Utilization mark (high/low)     : 100 / 0
  Subnet size (first/next)          : 0 / 0
  Total addresses                              : 254
  Leased addresses                           : 3
  Excluded addresses                       : 0
  Pending event                                  : none
```

```
1 subnet is currently in the pool
Current index      IP address range      Leased/Excluded/Total
192.168.1.1          192.168.1.1   - 192.168.1.254      3 / 0 / 254
```

4. NAT

IPv4 地址看上去很多，但互联网发展迅速，现在看来已远远不够用，NAT 技术从某种程度上缓解了这个问题。

- **NAT（Network Address Translation，网络地址转换）**
  - 是一种将私有（保留）地址转化为合法 IP 地址的转换技术，这种技术被普遍使用在有多台主机但只通过一个公有 IP 地址访问互联网的私有网络中；
  - NAT 的主要用途是让网络能够使用私有 IP 地址以节省 IP 地址,因为 NAT 将不可路由的私有内部地址转换为可路由的公有地址；
  - NAT 在一定程度上改善了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；
  - NAT 转换有两种类型：
    (1) **动态 NAT**：使用公有地址池，并以先到先得的原则分配这些地址。当使用私有 IP 地址的主机请求访问 Internet 时，动态 NAT 从地址池中选择一个未被其他主机使用的 IP 地址，这就是前面介绍的映射；
    (2) **静态 NAT**：使用本地地址与全局地址的一对一映射，这些映射保持不变。对必须使用固定地址以便能够从 Internet 访问的 Web 服务器或主机来说，静态 NAT 很有用。这些内部主机可能是企业服务器或网络设备。
- **NAT 重载（通常也成为端口地址转换，PAT）**

无论使用静态 NAT 还是动态 NAT，都必须有足够的公有地址，能够给同时发生的每个用户会话分配一个地址。因此出现 NAT 重载的方法：将多个私有 IP 地址映射到一个或几个公有 IP 地址。大多数家用路由器都具有这种功能。

- 通过使用 NAT 重载，可将多个地址映射到一个或几个地址，即使用端口号跟踪每个私有地址；

- 客户端打开 TCP/IP 会话时，NAT 路由器将为源地址分配一个端口号。NAT 重载确保连接到 Intermet 服务器的每个客户端会话使用不同的 TCP 端口号；
- 服务器返回响应时，路由器将根据源端口号（在回程中为目标端口号）决定将分组转发给哪个客户端；同时路由器还检查收到的是否是响应请求的分组，这在一定程度上提高了会话的安全性。

- **NAT 的固有缺陷**
  - NAT 某种程度上影响了网络性能，进行转换不可避免地回增加时延延；
  - NAT 影响端到端的功能，很多协议和应用程序依赖端到端功能，这要求分组从源转发到目的地的过程中不被修改；
  - NAT 使隧道协议（IPSec）更复杂等；
  - IPv6 避免了 NAT 大部分缺点。

5. NAT 配置应用

(1) 配置静态 NAT

静态 NAT 在内部地址和外部地址之间建立一对一映射。静态 NAT 让外部设备能够连接到内部设备。配置静态 NAT 很简单，只需指定要转换的地址并在合适的接口上配置 NAT 即可。配置的步骤如下：

```
// 指定内部本地地址和外部全局地址之间的静态转换
R1(config)# ip nat inside source static <local_ip> <global_ip>
// 指定内部接口
R1(config)# interface <type> <num>
// 将这个接口标记为连接到内部
R1(config-if)# ip nat inside
// 指定外部接口
R1(config-if)# interface <type> <num>
// 将这个接口标记为连接到外部
R1(config-if)# ip nat outside
```

(2) 配置动态 NAT

静态 NAT 建立内部地址与公有地址之间的永久性映射，而动态 NAT 将私有 IP 地址映射到 NAT 地址池中的公有地址。

动态 NAT 的配置与静态 NAT 不同，但也有些相似之处。与静态 NAT 相似，配置动态 NAT 时也需要将接口指定为内部或外部接口，但不是创建到 IP 地址的

静态映射，而使用一个内部全局地址池。配置步骤如下：

// 定义一个用于分配地址的全局地址池

R1(config)# ip nat pool <name> <start_ip> <end_ip> [netmask <netmask>]

// 定义一个标准访问列表，它允许那些要转换的地址

R1(config)# access-list <access_list_number> permit <source> [<source-wildcard>]

// 建立动态转换并指定前一步定义的访问列表

R1(config)# ip nat inside source list <access-list-number> pool <name>

// 指定内部接口

R1(config)# interface <type> <number>

// 将接口标记为连接到内部网络

R1(config-if)# ip nat inside

// 指定外部接口

R1(config)# interface <type> <number>

// 将接口标记为连接到外部网络

R1(config-if)# ip nat outside

要配置动态 NAT，需要创建一个 ACL，其只允许那些需要转换的地址。编写 ACL 时，要注意每个 ACL 末尾都隐式 deny all 语句。限制性太低的 ACL 可能导致意外结果。配置供 NAT 命令使用的访问控制列表时，强烈建议不要使用 permit any 命令，否则可能将导致 NAT 消耗过多路由器资源，从而引发性能问题。

(3) 配置仅单个公有 IP 地址的 NAT 重载

只有一个公有 IP 地址时，重载配置通常将该公有地址分配给连接到 ISP 的外部接口。所有内部地址离开外部接口时都将被转换为同一个 IP 地址。

配置与动态 NAT 相似，只是没有使用地址池，而使用关键字 interface 指定外部 IP 地址，因此不需要定义 NAT 地址池。关键字 overload 使在转换中添加端口号。步骤如下：

R1(config)# access-list <access_list_num> permit <source> [<source-wildcard>]:定义一个标准访问列表，它只允许要转换的地址

R1(config)# ip nat inside source list <access_list_num> interface <interface> overdoad：建立动态转换并指定前一步定义的访问列表

R1(config)# interface <type> <number>：指定内部接口

R1(config-if)# ip nat inside：将接口标记为连接到内部网络

R1(config)# interface <type> <number>：指定外部接口

R1(config-if)# ip nat outside：将接口标记为连接到外部网络

(4) 配置使用公有 IP 地址池的 NAT 重载

如果 ISP 提供了多个公有 IP 地址，可将 NAT 重载配置成使用地址池。这种配置与一对一的动态 NAT 配置的主要区别是使用了关键字 overload。关键字 overload 启用端口地址转换。步骤如下：

R1(config)# ip nat pool <name> <start_ip> <end_ip> [netmask <netmask>]：定义一个用于分配地址的全局地址池

R1(config)# access-list <access_list_num> permit <source> [<source-wildcard>]：定义一个标准访问列表，它只允许要转换的地址

R1(config)# ip nat inside source list <access_list_num> pool <name> overdoad：建立重载转换

R1(config)# interface <type> <number>：指定内部接口

R1(config-if)# ip nat inside 将接口标记为连接到内部网络

R1(config)# interface <type> <number>：指定外部接口

R1(config-if)# ip nat outside：将接口标记为连接到外部网络

6. CDP

CDP（Cisco Discovery Protocol，思科发现协议）是功能强大的网络监控与故障排除工具。网络管理员使用 CDP 作为信息收集工具，通过它来收集与直接相连的思科设备有关的信息。CDP 是思科专有的一款工具，可以用它来了解与直接相连的思科设备有关的协议与地址概要信息。

- 默认情况下，每台思科设备会定期向直接相连的思科设备发送消息，这种消息成为 CDP 通告，通告包含特定信息，如连接设备的类型、设备所连接的路由器接口、用于进行连接的接口以及设备型号等。
- 以下命令可以在这台设备上启用 CDP：

R1(config)# cdp run

- CDP 协议收集到的邻居信息，包括设备 ID、本地接口、保持时间（单位秒）、邻居设备功能代码、邻居硬件平台、邻居远程端口 ID，可通过以下命令查看：

R1(config)# show cdp neighbors

- 以下命令会显示邻居设备的 IP 地址（无论是否能 ping 通邻居，CDP 都会显示邻居的 IP 地址），当两台思科路由器无法通过共享的数据链路进行路由时，非常有用；该命令也有助于确定某个 CDP 邻居是否存在 IP 配置错误。

R1(config)# show cdp neighbors detail

- CDP 也会带来一些安全风险，如需彻底禁用 CDP，可使用以下命令：

R1(config)# no cdp run

- 如需使用 CDP 但针对特定接口停止 CDP 通告，可在端口配置模式下使用以下命令：

R1(config-if)# no cdp enable

五、实验内容

实验拓扑如图 1 所示：

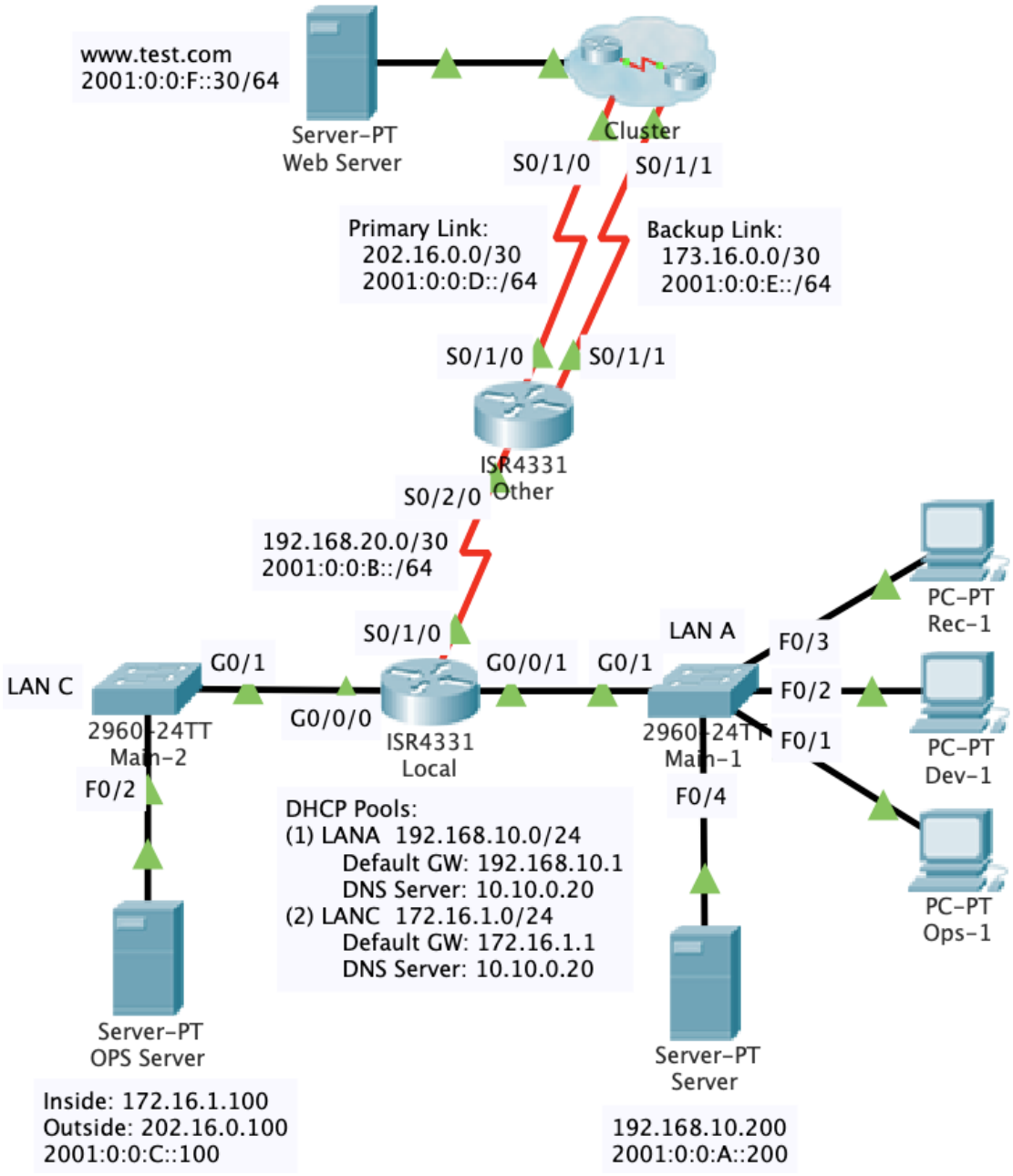


图 1 实验使用的拓扑

在此实践技能评估中，您将配置科学院网络，并通过在路由器接口上配置 IPv4 和 IPv6 地址来建立网络连接。您将配置 DHCPv4 和 NAT 寻址服务，并通过在 IPv4 和 IPv6 中配置默认和静态路由来建立网络之间的通信。**请注意，路由器相关端口 IP 地址已配置完成，无需自行进行配置。**

需要从终端连接到设备控制台来完成所有 IOS 设备配置。

需要配置的内容包括：

Local：

接口激活与编址

两个 DHCPv4 池

IPv4 和 IPv6 中的静态路由

Other：

IPv4 和 IPv6 中的接口激活与编址

静态 NAT

单地址上的 NAT Overload（PAT）

IPv4 和 IPv6 网络的静态路由、静态主机路由、默认路由和浮动静态默认路由

标准编号 ACL 配置

CDP 配置

LAN A 中主机：

激活 DHCP 寻址

手动配置 IPv6 地址

地址表

Device	Interface	Network/Address
Local	G0/0/0	172.16.1.1/24
		2001:0:0:C::1/64 FE80::2
	G0/0/1	192.168.10.1/24
		2001:0:0:A::1/64 FE80::2
	S0/1/0	192.168.20.1/30
		2001:0:0:B::1/64
Other	S0/1/0	202.16.0.1/30
		2001:0:0:D::1/64
	S0/1/1	173.16.0.1/30

		2001:0:0:E::1/64
	S0/2/0	192.168.20.2/30
		2001:0:0:B::2/64
Rec-1	NIC	DHCP Assigned
		2001:0:0:A::5/64
Dev-1	NIC	DHCP Assigned
		2001:0:0:A::10/64
Ops-1	NIC	DHCP Assigned
		2001:0:0:A::15/64
Server	NIC	192.168.10.200/24
		2001:0:0:A::200/64
OPS Server	NIC	172.16.1.100/24
		2001:0:0:C::100
Web Server	NIC	10.10.0.30/24
		2001:0:0:F::30/64
DNS Server	NIC	10.10.0.20/24
		2001:0:0:F::20/64
Cloud Network	S0/1/0	202.16.0.2/30
		2001:0:0:D::2/64
	S0/1/1	173.16.0.2/30
		2001:0:0:E::2/64

六、实验器材

Packet Tracer

七、实验步骤

1. 激活 CDP：

CDP 仅应在 Local 路由器与 Other 路由器之间的串行接口上激活，在任何其他接口上，CDP 不应发送消息。

2. 配置静态和默认路由，如下所示：

网络中的所有路由都将静态配置。所有网络上的主机都应该能够通过 IPv4

和 IPv6 相互访问并能够访问 Internet。

应该使用下一跳接口地址作为参数配置路由。

- Local：
  - IPv6 和 IPv4 默认路由。
- Other：
  - IPv6 和 IPv4 默认路由；
  - IPv6 和 IPv4 浮动静态默认路由。路由开销设置为 5；
  - 到 LANA 网络的 IPv6 和 IPv4 静态路由；
  - 到服务器 OPS Server 的 IPv6 和 IPv4 主机路由。

3. 配置 DHCPv4

LAN A 和 LAN C 上的主机应从 DHCP Server 接收地址信息。OPS Server 与 Server 已预先指定了静态地址。有以下要求：

(1) 使用 LANC 作为连接 Local 中 G0/0/0 接口的网络的 DHCP 池的名称；

(2) 使用 LANA 作为连接 Local 中 G0/0/1 接口的网络的 DHCP 池的名称；

(3) 使用 10.10.0.20 作为 DNS 服务器地址；

(4) 根据网络拓扑中当前的设备与状态，避免分配保留的的地址；

(5) LAN A 和 LAN C 上所有主机相互可达，并且可以访问 Web Server 服务器。

4. 配置 NAT：

在 Other 上，按如下要求配置内部与外部网络之间的 NAT：

(1) 在 LAN C 的 OPS Server 服务器与内部全局地址 202.16.0.100 之间创建静态 NAT 映射；

(2) 将 PAT 配置为仅使用接口 S0/1/0 来转换 LAN A 和 LAN C 上 PC 主机的地址，配置中应仅引用接口而不要引用接口 IP 地址；

(3) 允许 LAN A 和 LAN C 网络上的所有主机地址通过以进行由 NAT 转换；

(4) 使用的 ACL 编号应为 1，使用 permit 语句，ACL 应该只有两个语句。

5. 配置主机地址

按如下要求配置 LAN A 上的主机：

(1) 所有主机都应从 DHCP 动态获取其 IPv4 地址；

(2) 根据地址表中的信息为所有主机静态配置完整的 IPv6 地址（将路由器 link-local 接口地址作为所有主机的 IPv6 默认网关）

设计编辑：张翔、张超魁（助教）
电子科技大学信息与软件工程学院

七、实验步骤

1. 激活 CDP：

CDP 仅应在 Local 路由器与 Other 路由器之间的串行接口上激活，在任何其他接口上，CDP 不应发送消息。

!路由器 Local 配置

! 由于路由器 Local 使用了 3 个接口，而题目要求仅应在 Local 路由器与 Other 路由器之间的串行接口上激活 CDP,因此在激活 CDP 后,需要把 gigabitEthernet 0/0/0－0/0/ 1 这两个接口的 CDP 功能禁用。

```
Local(config)#cdp run
```

! 使用 cdp run 命令在这台设备上启用 CDP。

```
Local(config)#interface gigabitEthernet 0/0/0
```

! 进入接口 gigabitEthernet 0/0/0 的配置模式

```
Local(config-if)#no cdp enable
```

! 使用 no cdp enable 命令禁用该接口的 CDP 功能。

```
Local(config-if)#exit
Local(config)#interface gigabitEthernet 0/0/1
Local(config-if)#no cdp enable
Local(config-if)#exit
```

!路由器 Other 配置

! 由于路由器 Other 使用了 3 个接口，而题目要求仅应在 Local 路由器与 Other

路由器之间的串行接口上激活 CDP，因此在激活 CDP 后，需要把 serial 0/1/0 和 0/1/1 这两个接口的 CDP 功能禁用。

```
Other(config)#cdp run
Other(config)#interface serial 0/1/0
Other(config-if)#no cdp enable
Other(config-if)#exit
Other(config)#interface serial 0/1/1
Other(config-if)#no cdp enable
Other(config-if)#exit
```

2. 配置静态和默认路由，如下所示：

网络中的所有路由都将静态配置。所有网络上的主机都应该能够通过 IPv4 和 IPv6 相互访问并能够访问 Internet。

应该使用下一跳接口地址作为参数配置路由。

- Local：
  - IPv6 和 IPv4 默认路由。

对于路由器 Local，有三个端口连接三个子网，分别是：172.16.1.0/24、192.168.10.0/24、192.168.20.0/30，对于直连子网，其路由信息将直接进入路由表，不用手动配置，可以使用 show ip rout 命令查看当前的路由状态。比如下图，设置了端口的 I P 地址后，没有配置其他路由信息，其直连子网的路由信息就自动进入的路由表中：

```
Local#show ip rout
Codes: L - local, C - connected, S - static, 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
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, GigabitEthernet0/0/0
L       172.16.1.1/32 is directly connected, GigabitEthernet0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0/1
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0/1
     192.168.20.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.20.0/30 is directly connected, Serial0/1/0
L       192.168.20.1/32 is directly connected, Serial0/1/0
```

因此只需要设置设置默认路由，使得所有目的地是其他子网的数据，都同通过默认路由器转发就可以了，也就是都通过 s0/1/0 转发。而通过该端口转发的数据的下一跳 IP 地址是与之连接的 Other 路由器的端口 S0/2/0 的 IP 地址，是

192.168.20.2（IPV6：2001:0:0:B::2）。配置过程如下：

Local(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.2

！设置默认路由的下一跳地址为：192.168.20.2。即默认路由是下一跳 IP 地址为 192.168.20.2 的邻居路由器。

Local(config)#ipv6 route ::/0 2001:0:0:B::2

！设置 IPv6 的默认路由的下一跳地址为：2001:0:0:B::2。

Local(config)#ipv6 unicast-routing

！启动 IPv6 的数据包转发功能

- Other：
  - **IPv6 和 IPv4 默认路由；**
  - **IPv6 和 IPv4 浮动静态默认路由。路由开销设置为 5；**

Other 路由器通过 Primary Link 和 Backup Link 两条链路连接到外部网络，因此对于 Other 路由器，其默认路由的下一跳就是 Primary Link 连接的另一端的路由器的接口地址，是：202.16.0.2（IPV4）、2001:0:0:D::2（IPV6）（由上面地址表中的 Cloud Network 表项中给出）。而 Backup Link 链路是备份链路，用于设置浮动静态默认路由，在 Primary Link 失效时，启用该备份链路。具体配置如下：

Other(config)#ip route 0.0.0.0 0.0.0.0 202.16.0.2

！设置默认路由的下一跳地址为：202.16.0.2

Other(config)#ip route 0.0.0.0 0.0.0.0 173.16.0.2 5

！设置浮动静态默认路由的下一跳地址为：173.16.0.2，路由开销设置为 5.

Other(config)#ipv6 route ::/0 2001:0:0:D::2

！设置 IPv6 的默认路由的下一跳地址为：2001:0:0:D::2。

Other(config)#ipv6 route ::/0 2001:0:0:E::2 5

！设置 IPv6 的浮动静态默认路由的下一跳地址为：2001:0:0:E::2，路由开销设置为 5。

Other(config)#ipv6 unicast-routing

！启动 IPv6 的数据包转发功能

- **到 LANA 网络的 IPv6 和 IPv4 静态路由；**

到 LANA 网络需要通过路由器 Local 进行转发，其对应的下一条地址为：192.168.20.1（2001:0:0:B::1），相关配置如下：

Other(config)#ip route 192.168.10.0 255.255.255.0 192.168.20.1

！若待转发 IP 报文的目的为 92.168.10.0 255.255.255.0 网段，则将该 IP 报文发往下一跳 IP 地址为 192.168.20.1 的邻居路由器。

Other(config)#ipv6 route 2001:0:0:A::/64 2001:0:0:B::1

！若待转发 IPV6 报文的目的为 2001:0:0:A::/64 网段，则将该 IP 报文发往下一跳 IPV6 地址为 64 2001:0:0:B::1 的邻居路由器。

- **到服务器 OPS Server 的 IPv6 和 IPv4 主机路由。**

到 OPS Server 需要通过路由器 Local 进行转发，其对应的下一条地址为：192.168.20.1（2001:0:0:B::1），相关配置如下：

Other(config)#ip route 172.16.1.100 255.255.255.255 192.168.20.1

Other(config)#ipv6 route 2001:0:0:C::100/128 2001:0:0:B::1

3. 配置 DHCPv4

LAN A 和 LAN C 上的主机应从 DHCP Server 接收地址信息。OPS Server 与 Server 已预先指定了静态地址。有以下要求：

(1) 使用 LANC 作为连接 Local 中 G0/0/0 接口的网络的 DHCP 池的名称；

G0/0/0 接口连接的是 172.16.1.0/24 子网。

```
Local(config)#ip dhcp pool LANC
！建立名字为 LANC 的地址池，然后进入该地址池的 DHCP 配置模式。
Local(dhcp-config)#network 172.16.1.0 255.255.255.0
！指定该地址池可用于分配的网络号和子网掩码。
```

(2) 使用 LANA 作为连接 Local 中 G0/0/1 接口的网络的 DHCP 池的名称；

G0/0/1 接口连接的是 192.168.10.0/24 子网。

```
Local(config)#ip dhcp pool LANA
！建立名字为 LANA 的地址池，然后进入该地址池的 DHCP 配置模式。
Local(dhcp-config)#network 192.168.10.0 255.255.255.0
```

(3) 使用 10.10.0.20 作为 DNS 服务器地址；

```
Local(config)#ip dhcp pool LANA
！进入名为 LANA 的地址池的 DHCP 配置模式。
Local(dhcp-config)#dns-server 10.10.0.20
！配置该地址池的 DNS 服务器地址为 10.10.0.20
Local(config)#ip dhcp pool LANC
！进入名为 LANC 的地址池的 DHCP 配置模式。
Local(dhcp-config)#dns-server 10.10.0.20
！配置该地址池的 DNS 服务器地址为 10.10.0.20
```

(4) 根据网络拓扑中当前的设备与状态，避免分配保留的的地址；

对于 LANA，服务器 server 的 IP 为 192.168.10.200，需要避免。

对于 LANC，服务器 OPS server 的 IP 为 172.16.1.100，需要避免。

```
Local(config)#ip dhcp excluded-address 172.16.1.100
！设置地址 172.16.1.100 为排除地址，不参与分配
Local(config)#ip dhcp excluded-address 192.168.10.200
！设置地址 192.168.10.200 为排除地址，不参与分配
```

(5) LAN A 和 LAN C 上所有主机相互可达，并且可以访问 Web Server 服务器。

要实现这个目的，就需要正确设置网关地址，当发送目的地址不属于本子网

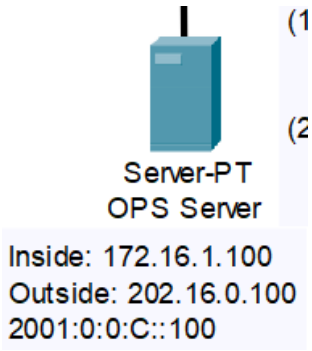
的数据报时，就通过网关转发。网关配置正确后，就可以相互访问。

```
Local(config)#ip dhcp pool LANA
！进入名为 LANA 的地址池的 DHCP 配置模式。
Local(dhcp-config)#default-router 192.168.10.1
！定义默认网关（路由器）为 192.168.10.1
Local(config)#ip dhcp pool LANC
！进入名为 LANC 的地址池的 DHCP 配置模式。
Local(dhcp-config)#default-router 172.16.1.1
！定义默认网关（路由器）为 172.16.1.1
```

4. 配置 NAT：

在 Other 上，按如下要求配置内部与外部网络之间的 NAT：

(1) 在 LAN C 的 OPS Server 服务器与内部全局地址 202.16.0.100 之间创建静态 NAT 映射；



内部地址是 172.116.1.100，映射后的外部地址是 202.16.0.100。其中内部地址是 172.116.1.100 是位于路由器 Other 接口 serial 0/2/0 这一侧，而外部地址是 202.16.0.100 是位于路由器 Other 接口 serial 0/1/0 这一侧

```
Other(config)#ip nat inside source static 172.16.1.100 202.16.0.100
！指定内部本地地址 172.16.1.100 和内部全局地址 202.16.0.100 之间的静态转换。
Other(config)#interface serial 0/1/0
！进入进口 serial 0/1/0 的配置模式
Other(config-if)#ip nat outside
！将这个接口标记为连接到外部
Other(config-if)#exit
Other(config)#interface serial 0/2/0
```

！进入进口 serial 0/2/0 的配置模式

Other(config-if)#ip nat inside

！将这个接口标记为连接到内部

Other(config-if)#exit

(2) 将 PAT（端口地址转换 或 NAT 重载）配置为仅使用接口 S0/1/0 来转换 LAN A 和 LAN C 上 PC 主机的地址，配置中应仅引用接口而不要引用接口 IP 地址；

(3) 允许 LAN A 和 LAN C 网络上的所有主机地址通过以进行由 NAT 转换；

(4) 使用的 ACL 编号应为 1，使用 permit 语句，ACL 应该只有两个语句。

Router(config)#access-list 1 permit 192.168.10.0 0.0.0.255

！定义一个标准访问列表 1，它只允许要转换的 192.168.10.0/24 的地址通过。

Router(config)#access-list 1 permit 172.16.1.0 0.0.0.255

！定义一个标准访问列表 1，它只允许要转换的 172.16.1.0/24 的地址通过。

Router(config)#ip nat inside source list 1 interface s0/1/0 overload

！使用访问列表 1 定制的规则，建立动态转换。将内部局部地址转换为内部全局地址;数据方向 inside->outside,在 outside 上执行转换;

5. 配置主机地址

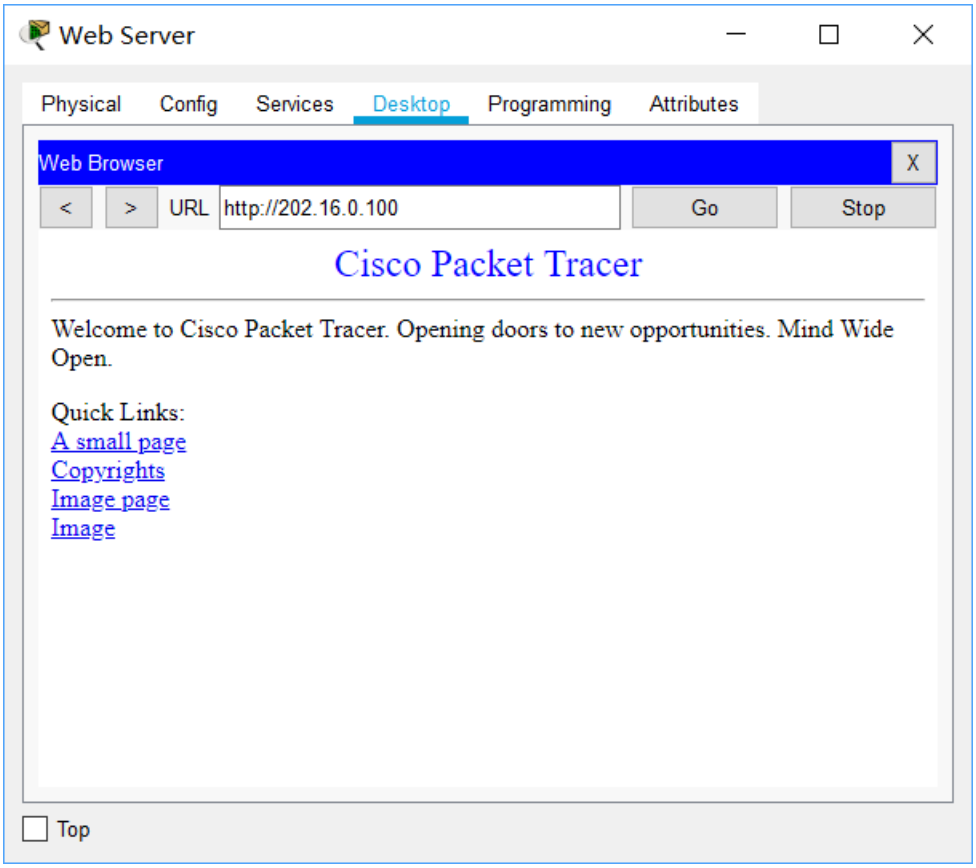
按如下要求配置 LAN A 上的主机：

(3) 所有主机都应从 DHCP 动态获取其 IPv4 地址；

(4) 根据地址表中的信息为所有主机静态配置完整的 IPv6 地址（将路由器 link-local 接口地址作为所有主机的 IPv6 默认网关）

6. 测试示例

下图是从 web server 服务器上，测试访问 OPS server 的 web 页面，它访问的地址是 NAT 转换后的外网的全局地址：202.16.0.100



使用 show ip nat translations 命令查看传输过程 nat 的转换

```
Other#show ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 202.16.0.100:1    172.16.1.100:1     10.10.0.30:1       10.10.0.30:1
icmp 202.16.0.100:2    172.16.1.100:2     10.10.0.30:2       10.10.0.30:2
icmp 202.16.0.100:3    172.16.1.100:3     10.10.0.30:3       10.10.0.30:3
icmp 202.16.0.100:4    172.16.1.100:4     10.10.0.30:4       10.10.0.30:4
---  202.16.0.100      172.16.1.100       ---                ---
tcp 202.16.0.100:80    172.16.1.100:80    10.10.0.30:1025    10.10.0.30:1025
```

上图的 ICMP 是执行了 ping 172.16.1.100 命令后，产生的。