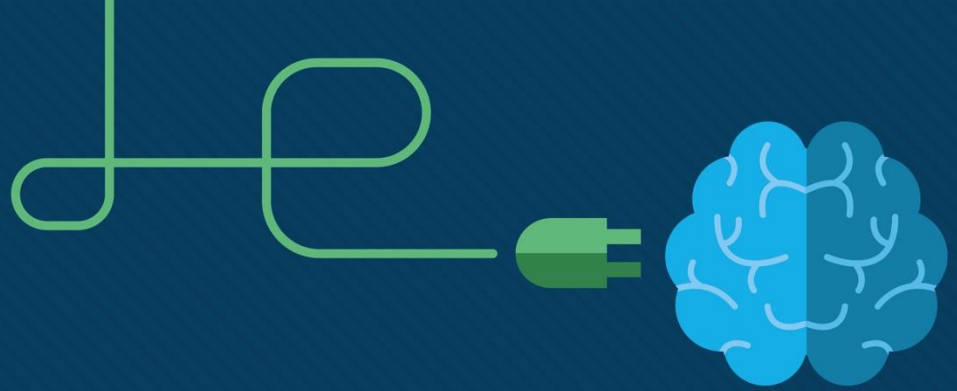


22 IPv4 NAT

单元目标

模块标题： IPv4 NAT

模块目标：在边缘路由器上实施 NAT 服务，以提供 IPv4 地址可扩展性。

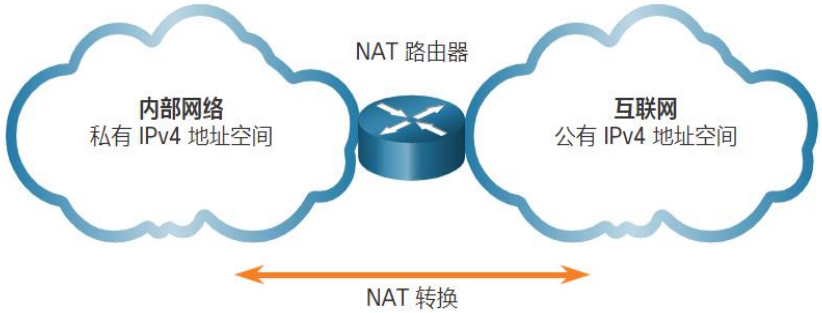
主题标题	主题目标
NAT 的特征	说明 NAT 的用途和功能。
NAT 的类型	说明不同类型的 NAT 的工作方式。
NAT的优点和缺点	阐述 NAT 的优点和缺点。
静态 NAT	使用 CLI 配置静态 NAT。
动态 NAT	使用 CLI 配置动态 NAT。
PAT	使用 CLI 配置 PAT。

22.1 NAT 的特征

IPv4 地址空间

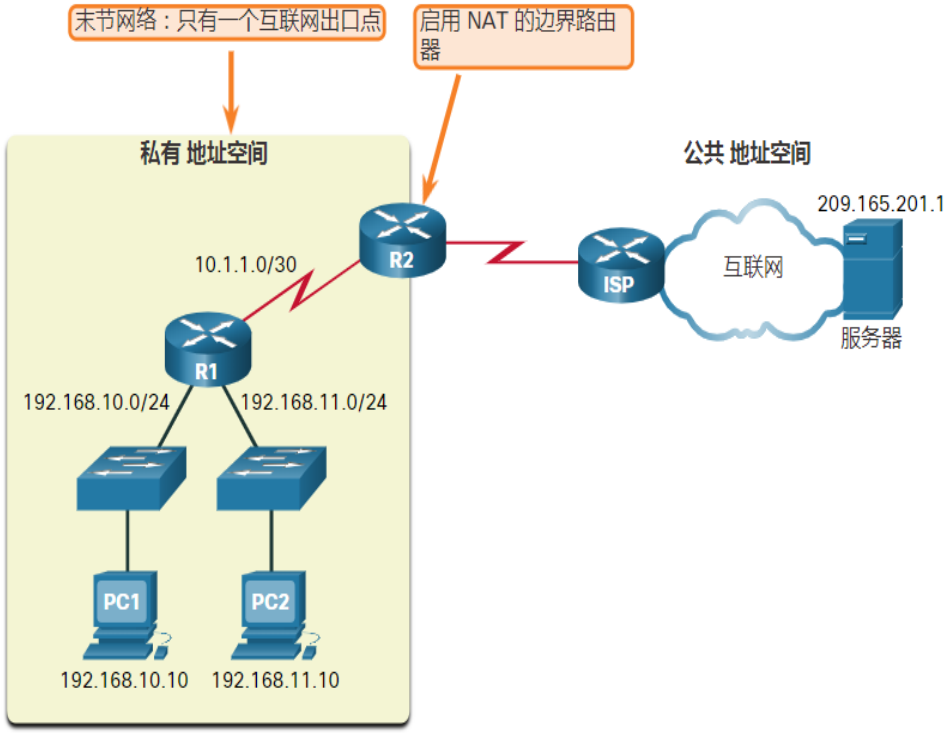
- 通常使用 RFC 1918 中定义的私有 IPv4 地址来实施网络。
- 这些私有地址可在企业或站点内使用，允许设备进行本地通信。
- 为了使具有私有 IPv4 地址的设备能够访问本地网络之外的设备和资源，必须首先将私有地址转换为公有地址。
- NAT 提供了私有地址到公有地址的转换。

分类	练习类型	练习名称
A	10.0.0.0 - 10.255.255.255	10.0.0.0/8
B	172.16.0.0 - 172.31.255.255	172.16.0.0/12
C	192.168.0.0 - 192.168.255.255	192.168.0.0/16

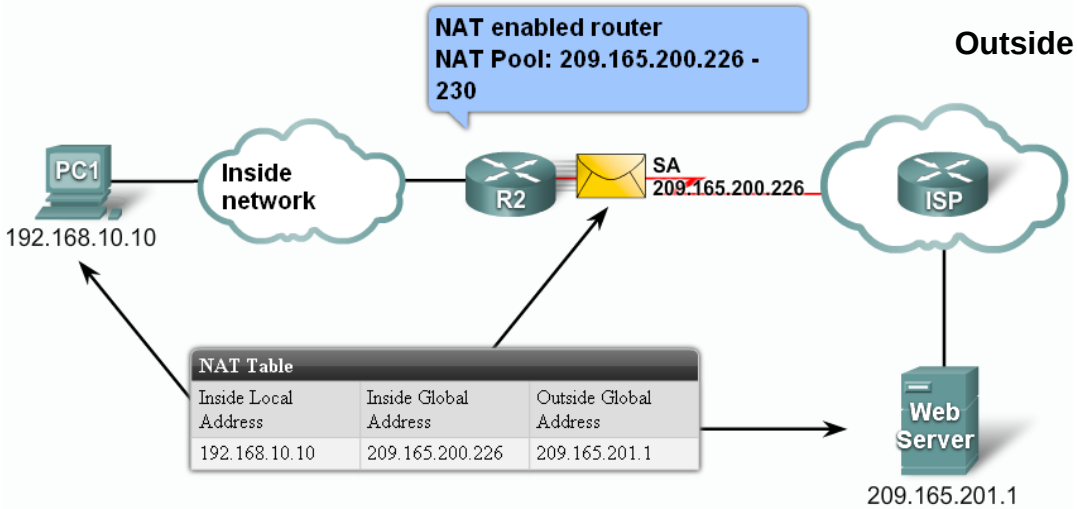


NAT是什么？

- NAT的主要作用是节省了公有IPv4地址。
- 它能够让网络在其内部使用私有IPv4地址并在需要时转换为公有地址。
- NAT 路由器通常工作在末端网络边界。
- 当末节网络中的设备想要与本地网络之外的设备进行通信，数据包会被转发到边缘路由器，并在那里执行NAT转换，把设备的内部私有地址转换为外部的公有可路由地址。



What is NAT?



- **Inside local** address
- **Inside global** address
- **Outside global** address
- **Outside local** address

NAT 的术语

内部本地地址

网络内部设备看到的源地址。这通常是私有 IPv4 地址。PC1的内部本地地址为192.168.10.10。

内部全局地址

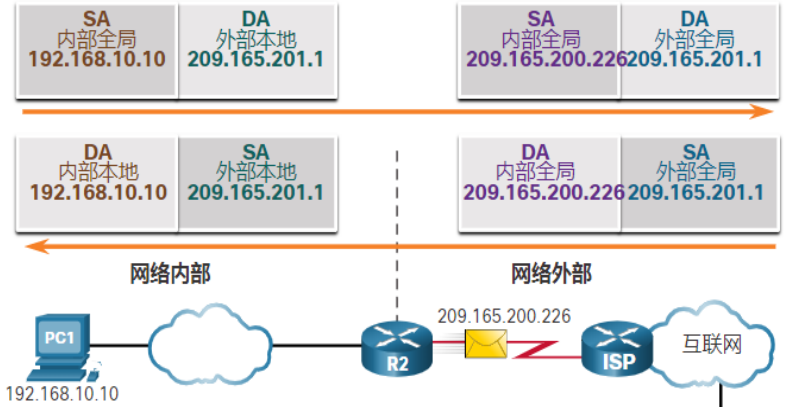
网络外部设备看到的源地址。PC1 的内部全局地址为 209.165.200.226

外部全局地址

网络外部设备看到的目的地址。Web 服务器的外部全局地址为 209.165.201.1

外部本地地址

网络内部设备看到的目的地址。PC1 把流量发送到 IPv4 地址为 209.165.201.1 的 Web 服务器上。虽然不常见，但该地址也可能与目标设备的全局可路由地址不同。



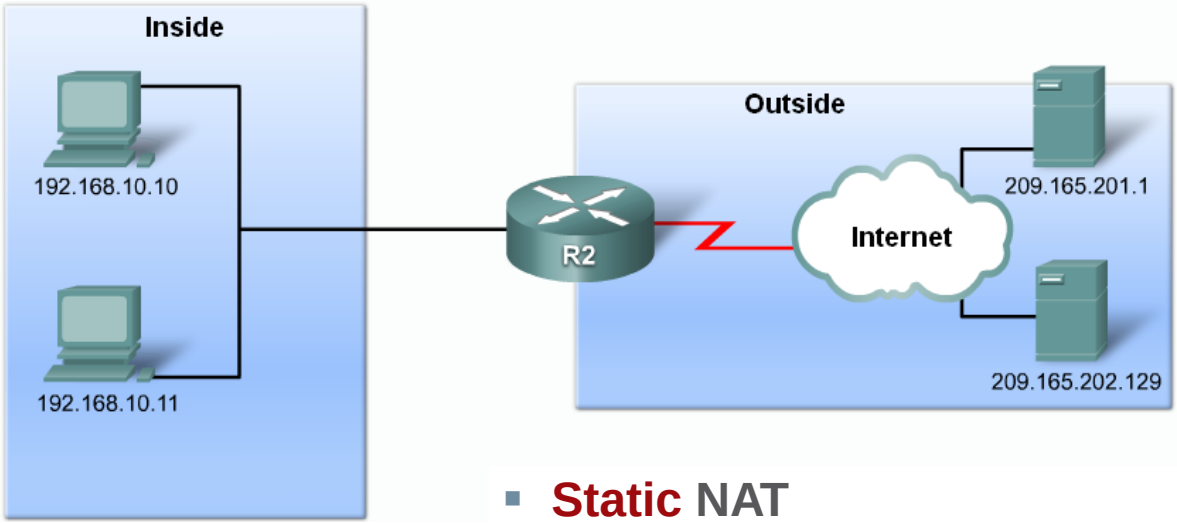
R2 NAT 表

PC1		Web 服务器	
内部全局地址	内部本地地址	外部本地地址	外部全局地址
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

22.2 NAT 的类型

NAT 的类型
NAT类型

- Two types of NAT translation

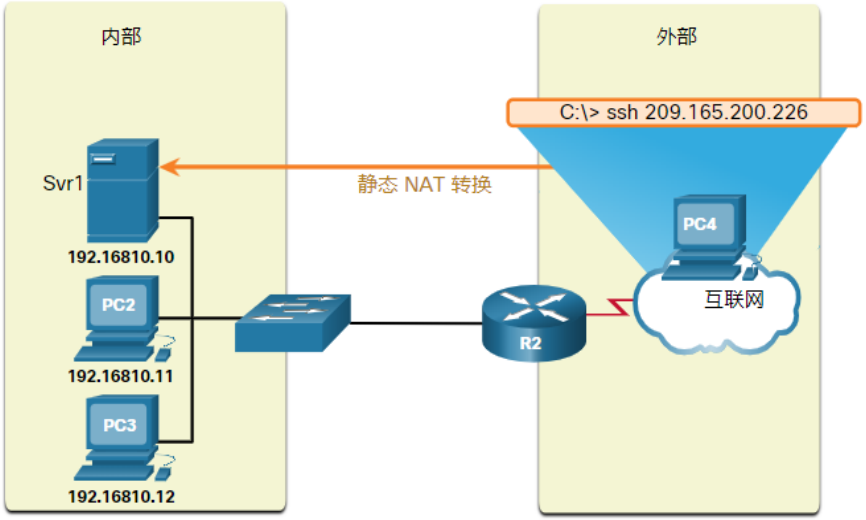


- **Static** NAT
- **Dynamic** NAT
- **PAT** (Port Address Translation)

静态 NAT

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。

- 如果Web服务器或设备必须拥有固定的地址，以便能够让其他设备从互联网发起访问的话（比如公司的Web服务器），静态NAT就尤为有用。
- 静态NAT也适用于这种情况：只有拥有授权的人员才能够从互联网对设备进行访问，发起访问的并不是互联网上一般的公有设备。



静态 NAT 表

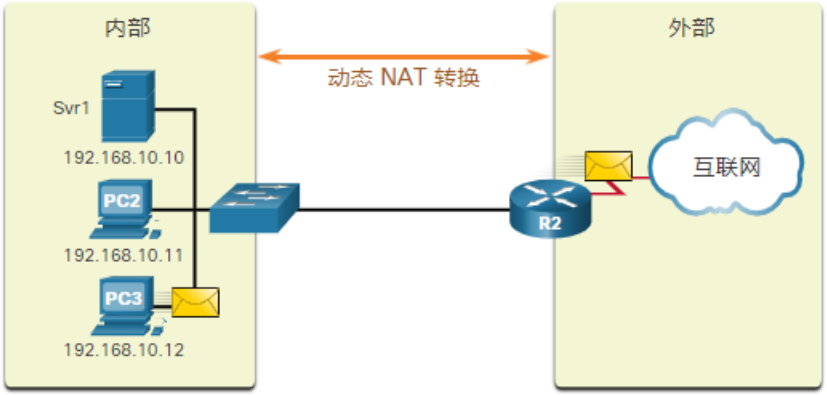
内部本地地址	内部全局地址 - R2 可到达的地址
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

注意：为了满足所有同时发生的用户会话需要，静态 NAT 要求有足够的公有地址可用。

动态 NAT

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。

- 内部设备请求访问外部网络时，动态 NAT 分配该池中的可用公共 IPv4 地址。
- 地址池中的其他地址仍可供使用。



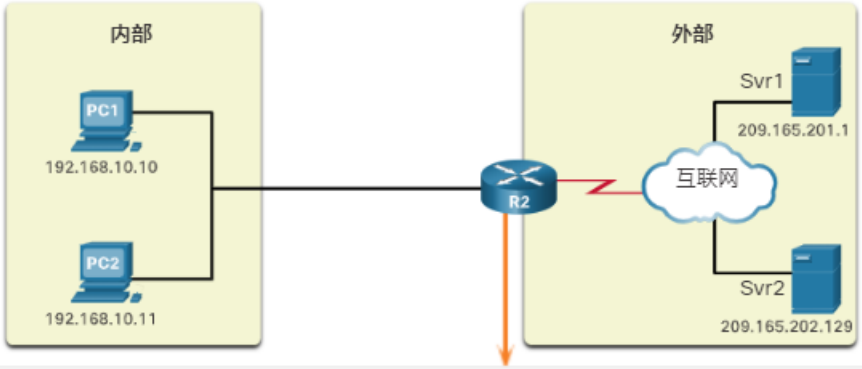
IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool - Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

注意为了满足所有同时发生的用户会话需要，动态 NAT 要求有足够的公有地址可用。。

端口地址转换(PAT)

端口地址转换 (PAT)(也称为 NAT 过载),将多个私有 IPv4 地址映射到单个私有 IPv4 地址或几个地址。

- 在使用PAT时,当 NAT 路由器收到来自客户端的数据包时,将使用其源端口号来唯一确定特定的 NAT 转换。
- PAT 利用互联网上的服务器确保设备对每个会话使用不同的 TCP 端口号。



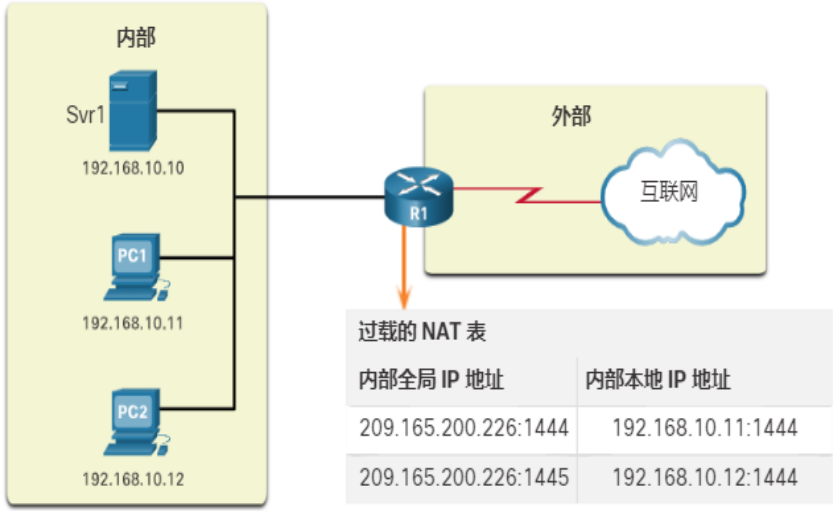
过载的 NAT 表

内部本地 IP 地址	内部全局 IP 地址	外部本地 IP 地址	外部全局 IP 地址
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

下一个可用端口

PAT 会尝试保留原始的源端口。如果原始的源端口已被使用，PAT 就会从相应的端口组（0–511、512–1023 或 1024–65535）中分配第一个可用的端口号。

- 如果没有其他可用端口，而地址池中的外部地址多于一个，则 PAT 会进入下一地址并尝试重新分配原始的源端口。
- 这一过程会一直持续，直到不再有可用端口或外部 IPv4 地址。



每个内部全局地址实际可用的端口号约4000个。

NAT和PAT的比较

下表概述了 NAT 和 PAT 之间的差异。

NAT -仅修改 IPv4 地址

内部全局地址	内部本地地址
209.165.200.226	192.168.10.10

PAT - PAT 会同时修改地址和端口号。

内部全局地址	内部本地地址
209.165.200.226:2031	192.168.10.10:2031

NAT	PAT
内部本地地址与内部全局地址之间的一对一映射。	一个内部全局地址可以映射到多个内部本地地址。
在转换过程中只会使用 IPv4地址。	在转换过程中会使用 IPv4 地址和 TCP 或 UDP 源端口号。
每个内部主机在访问外部网络时都需要唯一的内部全局地址。	内部主机在访问外部网络时，多台内部主机可以共享单个内部全局地址。

不包含第4层分段的数据包

有些数据包不包含第 4 层端口号，例如 ICMPv4 消息。对于每种类型的协议，PAT 会以不同方式进行处理。

例如，ICMPv4 查询消息、响应请求和响应应答会包含一个查询 ID。ICMPv4 使用查询 ID 来识别响应请求及其相应的响应应答。

注意：其他ICMPv4消息不使用查询ID。对于这些消息以及其他不使用 TCP 或 UDP 端口号的协议，情况有所不同，不在本课程的讨论范围之内。

22.3 NAT的优点和缺点

NAT的优点

NAT 有许多优点，其中包括：

- NAT 允许对内联网实行私有编址，从而维护合法注册的公有编址方案。
- NAT 通过应用程序端口级别的多路复用节省了地址。
- NAT 增强了与公有网络连接的灵活性。
- NAT 为内部网络编址方案提供了一致性。
- NAT 允许维持现有的私有 IPv4 地址方案，同时能够很容易地更换为新的公有编址方案。
- NAT可以隐藏用户和其他设备的IPv4地址。

NAT的缺点

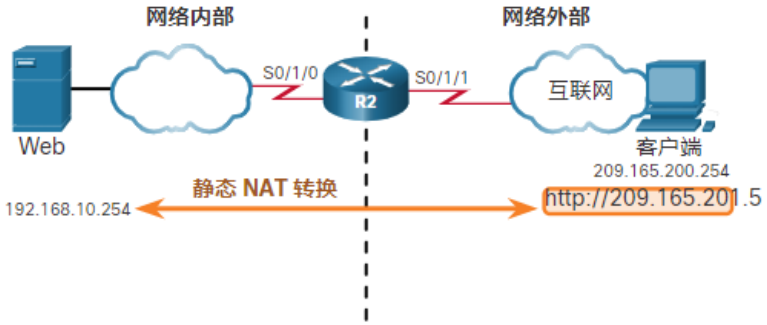
NAT 也有一些缺点：

- NAT 会增加转发延迟。
- 失去端到端寻址功能。
- 端到端 IPv4 可追溯性会丧失。
- NAT 会让隧道协议（如 IPsec）的使用变得复杂。
- 需要外部网络发起 TCP 连接的一些服务，或者无状态协议（诸如使用 UDP 的无状态协议），可能会中断。

22.4 静态 NAT

静态 NAT 的应用场景

- 静态 NAT 是内部地址与外部地址之间的一对一映射。
- 静态 NAT 允许外部设备使用静态分配的公有地址发起与内部设备的连接。
- 例如，可以将内部 Web 服务器映射到特定的内部全局地址，以便从外部网络对其进行访问。

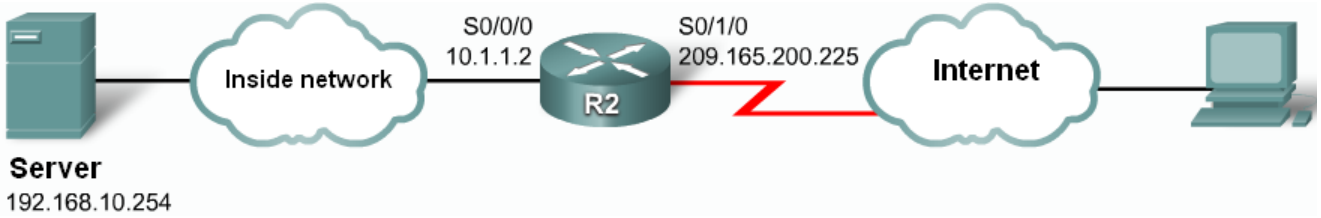


配置静态 NAT

在配置静态NAT转换时，我们需要完成两个基本任务：

- **第1步** - 使用**ip nat inside source static** 命令建立内部本地地址与内部全局地址之间的映射。
- **第2步** - 使用**ip nat inside** 和 **ip nat outside** 命令把参与转换的接口配置为NAT内部或NAT外部接口。

Configuring Static NAT



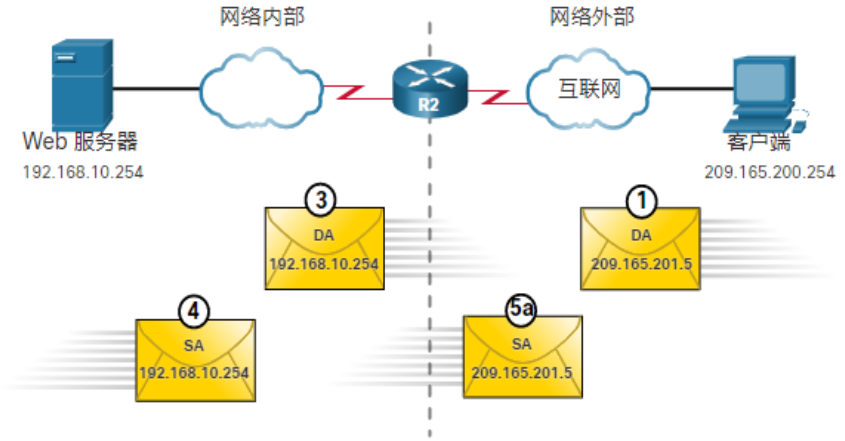

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.200.254
!--Establishes static translation between an inside local address and an inside
!--global address.
R2(config)# interface serial0/0/0
R2(config-if)# ip nat inside
!--Identifies Serial 0/0/0 as an inside NAT interface.
R2(config-if)# interface serial 0/1/0
R2(config-if)# ip nat outside
!--Identifies Serial 0/1/0 as an outside NAT interface.
```

With this configuration, 192.168.10.254 **will always translate to** 209.165.200.254

分析静态 NAT

客户端和 Web 服务器之间的静态 NAT 转换过程如下所示：

1. 客户端向 Web 服务器发送一个数据包。
2. R2从NAT外部接口接收到客户端发来的数据包，并检查自己的NAT表。
3. R2把内部全局地址转换为内部本地地址，然后把数据包转发给Web服务器。
4. Web 服务器接收到数据包，并使用内部本地地址对客户端做出响应。
5. (a) R2从其NAT内部接口接收到Web服务器的数据包，源地址是Web服务器的内部本地地址。(b) 它把这个源地址转换为内部全局地址。



内部本地地址	内部全局地址	外部本地地址	外部全局地址
192.168.10.254	209.165.201.5	209.165.200.254	209.165.200.254

2 5b

验证静态 NAT

要想验证 NAT 操作，我们可以使用 **show ip nat translations** 命令。

- 此命令可用于显示活动的 NAT 转换。
- 由于该示例是静态 NAT 配置，因此不论正在进行的是何种通信，转换都会在 NAT 表中进行。
- 如果在活跃会话进行过程中执行了上述命令，命令输出中就会显示出外部设备的地址。

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.254 192.168.10.254 --- ---
Total number of translations: 1
```

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.254 192.168.10.254 209.165.201.5 209.165.201.5
--- 209.165.200.254 192.168.10.254 --- ---
Total number of translations: 2
```

验证静态 NAT（续）

另一个有用命令是 **show ip nat statistics**。

- 它会显示出活动转换总数、NAT配置参数、地址池中的地址数量，以及已分配出去的地址数量。
- 要想验证NAT转换的工作是否正常，最好先使用 **clear ip nat statistics** 命令清除以前的转换计数统计，然后再执行测试。

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
Serial0/1/1
Inside interfaces:
Serial0/1/0
Hits: 4 Misses: 1
（省略部分输出）
```

验证静态 NAT（续）

```
R2# debug ip nat
IP NAT debugging is on
R2#
*Oct  6 19:55:31.579: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14434]
*Oct  6 19:55:31.595: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6334]
*Oct  6 19:55:31.611: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14435]
*Oct  6 19:55:31.619: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14436]
*Oct  6 19:55:31.627: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14437]
*Oct  6 19:55:31.631: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6335]
*Oct  6 19:55:31.643: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6336]
*Oct  6 19:55:31.647: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14438]
*Oct  6 19:55:31.651: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6337]
*Oct  6 19:55:31.655: NAT*: s=192.168.10.10->209.165.200.225, d=209.165.200.254 [14439]
*Oct  6 19:55:31.659: NAT*: s=209.165.200.254, d=209.165.200.225->192.168.10.10 [6338]

<Output omitted>
```

Packet Tracer - 配置静态 NAT

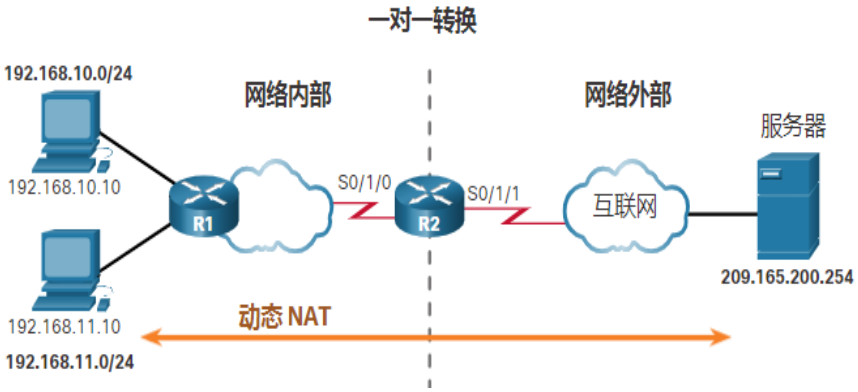
在这个 Packet Tracer 中，您会完成以下目标：

- 测试不使用 NAT 的访问
- 配置静态 NAT
- 测试使用 NAT 的访问

22.5 动态 NAT

动态 NAT 的应用场景

- 动态NAT会自动把内部本地地址映射为内部全局地址。
- 动态 NAT 使用内部全局地址的池。
- 内部网络中的任何设备根据先到先得的原则使用公有 IPv4 地址池（内部全局地址池）。
- 如果地址池中的所有地址都被使用了，其他设备必须等到有可用地址时，才能访问外部网络。

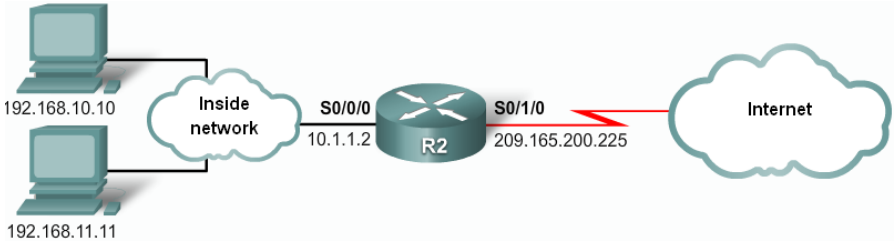


配置动态 NAT

在配置动态NAT转换时，我们需要完成下列五个任务：

- **第1步**- 使用 **ip nat pool** 命令定义用来提供转换的地址池。
- **第2步** - 配置一个标准 ACL，用于仅标识（允许）那些将要进行转换的地址。
- **第3步**- 使用**ip nat inside source list**命令在地址池中绑定ACL。
- **第4步**- 确定哪些是内部接口。
- **第5步** - 确定哪些是外部接口。

Configuring Dynamic NAT

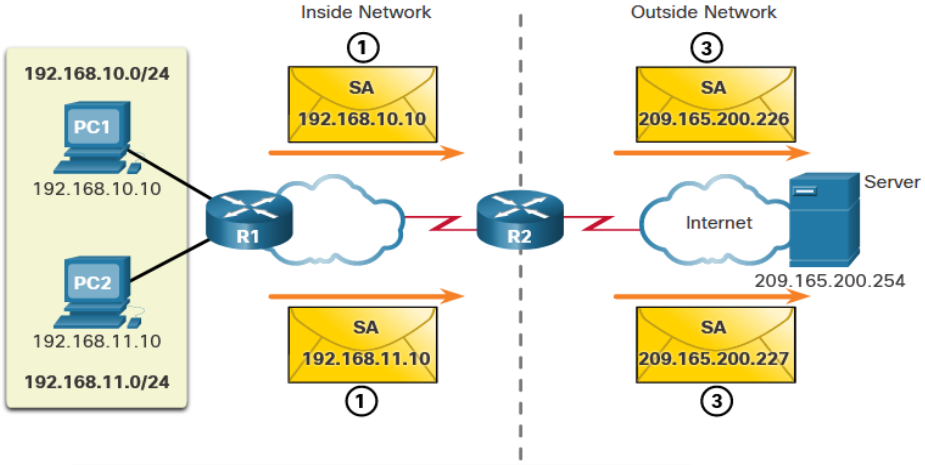



```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask
  255.255.255.224
!--Defines a pool of public IP addresses under the pool name NAT-POOL1
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
!--Defines which addresses are eligible to be translated
R2(config)# ip nat inside source list 1 pool NAT-POOL1
!--Binds the NAT pool with ACL 1
R2(config)# interface serial 0/0/0
R2(config-if)# ip nat inside
!--Identifies interface Serial 0/0/0 as an inside NAT interface
R2(config-if)# interface serial s0/1/0
R2(config-if)# ip nat outside
!--Identifies interface Serial 0/1/0 as the outside NAT interface.
```

分析动态 NAT - 从内部到外部

动态 NAT 转换过程：

1. PC1 和 PC2 发送数据包，请求连接服务器。
2. R2从PC1接收到第一个数据包，它检查ACL来确定是否应该转换这个数据包，然后它选择可用的全局地址，在NAT表中创建转换条目。
3. R2 使用转换后的内部全局地址 209.165.200.226 替换 PC1 的内部本地源地址 192.168.10.10。（R2会使用转换后的地址209.165.200.227为来自PC2的数据包执行相同的操作。）

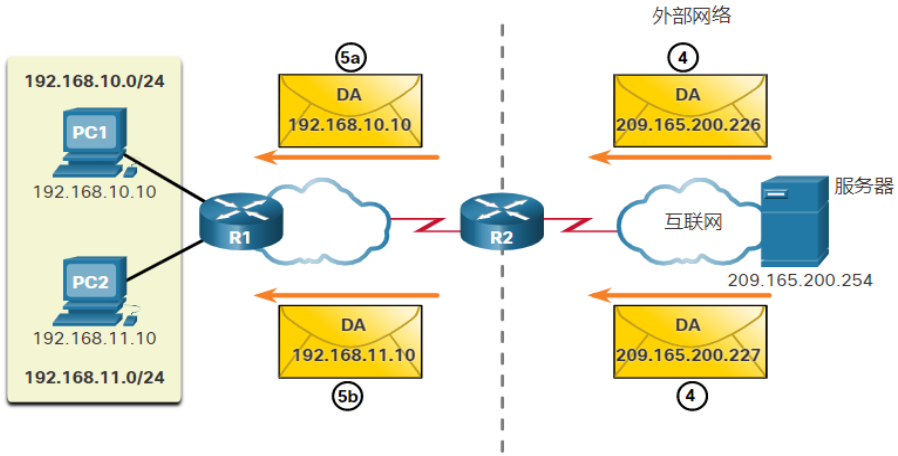


IPv4 NAT Pool	
Inside Local Address Pool	Inside Global Address
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227

分析动态 NAT — 从外部到内部

动态 NAT 转换过程：

4. 服务器收到来自 PC1 的数据包，使用 IPv4 目标地址 209.165.200.226 做出响应。服务器收到来自 PC2 的数据包，使用 IPv4 目标地址 209.165.200.227 做出响应。
5. (a) 当 R2 接收目的地址为 209.165.200.226 的数据包时；它执行 NAT 表查找，把地址转换回内部本地地址，并将数据包转发到 PC1。
(b) 当 R2 收到目的地址为 209.165.200.227 的数据包时，它执行 NAT 表查找，把地址转换回内部本地地址 192.168.11.10，并将数据包转发到 PC2。



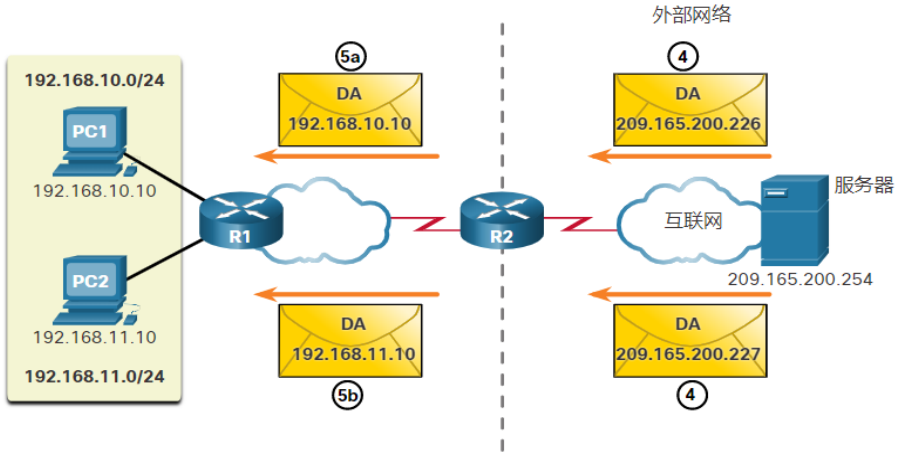
IPv4 NAT 池	
内部本地地址池	内部全局地址
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227

5a
5b

分析动态 NAT - 从外部到内部(续)

动态 NAT 转换过程:

6. PC1 和 PC2 接收数据包并继续会话。路由器对每个数据包执行步骤 2 至步骤 5。



IPv4 NAT 池	
内部本地地址池	内部全局地址
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227

5a
5b

验证动态 NAT

show ip nat translations 命令的输出中显示出已配置的所有静态转换，以及由流量创建的动态转换。

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
--- 209.165.200.228 192.168.10.10 --- ---
--- 209.165.200.229 192.168.11.10 --- ---
R2#
```

验证动态 NAT(续)

增加 verbose 关键字可显示关于每个转换的附加信息，包括创建和使用条目的时间长短。

```
R2# show ip nat translation verbose
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.228 192.168.10.10 --- ---
create 00:02:11, use 00:02:11 timeout:86400000, left 23:57:48, Map-Id(In): 1,
flags:
none, use_count: 0, entry-id: 10, lc_entries: 0
tcp 209.165.200.229 192.168.11.10 --- ---
create 00:02:10, use 00:02:10 timeout:86400000, left 23:57:49, Map-Id(In): 1,
flags:
none, use_count: 0, entry-id: 12, lc_entries: 0
R2#
```

验证动态 NAT(续)

默认情况下，转换条目会在24小时后超时，我们可以使用 **ip nat translation timeout** *timeout-seconds* 全局配置命令来更改计时器设置。要想在计时器超时之前清除动态条目，我们可以使用 **clear ip nat translation** 特权EXEC模式的命令。

```
R2# clear ip nat translation *
R2# show ip nat translation
```

命令	说明
clear ip nat translation *	清除 NAT 转换表中的所有动态地址转换条目。
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	清除包含内部转换或包含内部与外部转换的简单动态转换条目。
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	清除扩展动态转换条目。

验证动态 NAT（续）

show ip nat statistics 命令显示有关总活动转换数、NAT 配置参数、地址池中地址数量和已分配地址数量的信息。

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 0 extended)
Peak translations: 4, occurred 00:31:43 ago
Outside interfaces:
Serial0/1/1
Inside interfaces:
Serial0/1/0
Hits: 47 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 4
pool NAT-POOL1: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 2 (13%), misses 0
（省略部分输出）
R2#
```

验证动态 NAT（续）

使用**show running-config** 命令查看 NAT、ACL、接口或池命令。

```
R2# show running-config | include NAT
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
ip nat inside source list 1 pool NAT-POOL1
```

Packet Tracer – 配置动态 NAT

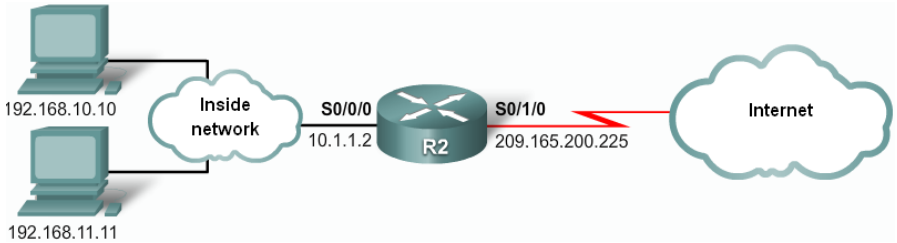
在这个 Packet Tracer 中，您会完成以下目标：

- 配置动态 NAT
- 验证 NAT 实施

22.6 PAT

使用单个IPv4地址配置PAT

要在配置PAT时只使用单个IPv4地址，只需要把关键字 **overload** 添加到 **ip nat inside source** 命令中即可。

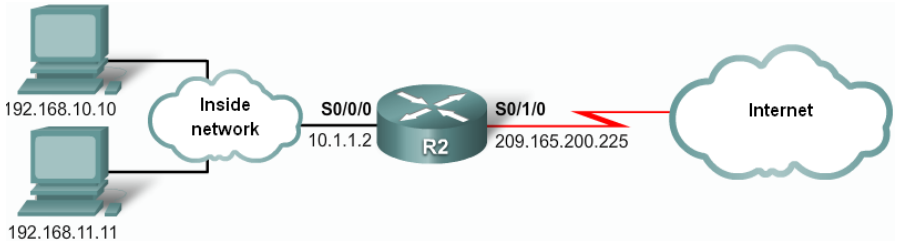



```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
!--Defines which addresses are eligible to be translated
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
!--Identifies the outside interface Serial 0/1/0 as the inside global address to
!--be overloaded
R2(config)# interface serial 0/0/0
R2(config-if)# ip nat inside
!--Identifies interface Serial 0/0/0 as an inside NAT interface
R2(config-if)# interface serial s0/1/0
R2(config-if)# ip nat outside
```

PAT

配置PAT来使用地址池

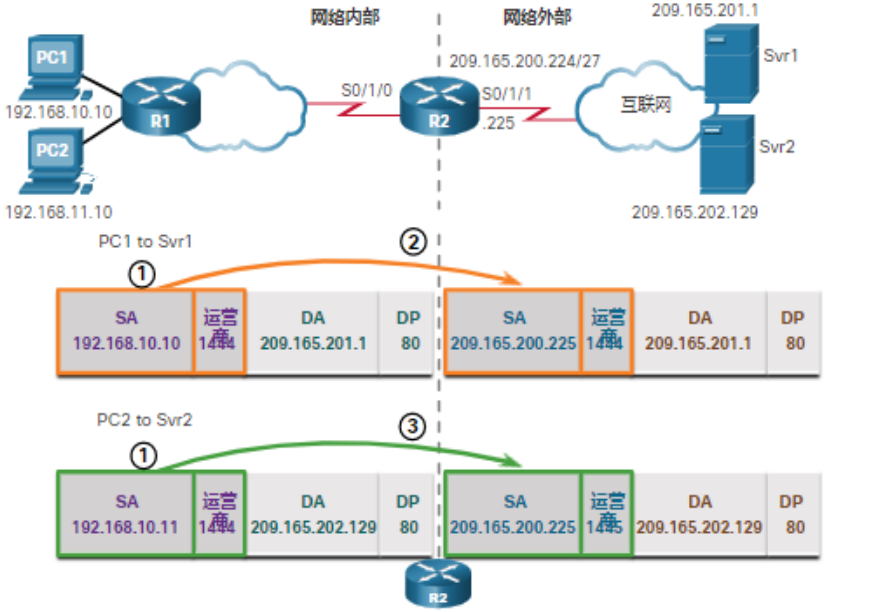
ISP 可以向组织机构分配多个公有 IPv4 地址。在这种场景中，组织机构可以配置PAT来使用一个IPv4公有地址池进行转换。




```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask
  255.255.255.224
!--Defines a pool of addresses named NAT-POOL2 to be used in NAT translation
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
!--Defines which addresses are eligible to be translated
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
!--Bonds the NAT pool with ACL 1 address to be overloaded
R2(config)# interface serial 0/0/0
R2(config-if)# ip nat inside
!--Identifies interface Serial 0/0/0 as an inside NAT interface
R2(config-if)# interface serial s0/1/0
R2(config-if)# ip nat outside
```

分析 PAT — 从 PC 到服务器

1. PC1 和 PC2 向 Svr1 和 Svr2 发送数据包。
2. 来自 PC1 的数据包先到达 R2。R2 把源 IPv4 地址转换 209.165.200.225（内部全局地址）。然后把数据包转发到 Svr1。
3. 来自 PC2 的数据包到达 R2。PAT把PC2的IPv4地址转换为内部全局地址 209.165.200.225。PC2 的源端口号与 PC1 相同。PAT 将增大源端口号，直到源端口号在其表中为唯一值。在本例中是 1445。

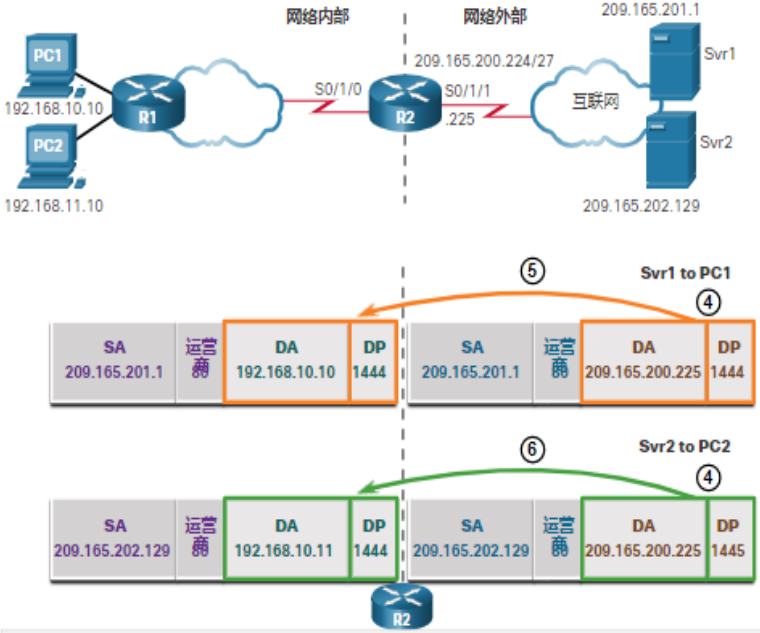


NAT 表

内部本地地址	内部全局地址	外部全局地址	外部本地地址
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.10:1444	209.165.200.225:1445	209.165.201.129:80	209.165.201.129:80

分析 PAT — 从服务器到 PC

4. 服务器将来自已接收数据包的源端口用作目标端口，而将源地址用作返回流量的目标地址。服务器看起来像和位于209.165.200.225中的同一主机通信；但事实并非如此。
5. 数据包到达时，R2 使用每个数据包的目标地址和目标端口在NAT 表中查找唯一条目。对于来自 Svr1 的数据包，目标 地址 209.165.200.225 具有多个条目，只有一个条目具有目标端口 1444。
6. 来自 Svr2 的数据包到达 R2 时，对其执行类似转换。找到209.165.200.225，仍具有多个条目。但目标端口 1445。



NAT 表

内部本地地址	内部全局地址	外部全局地址	外部本地地址
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

验证 PAT

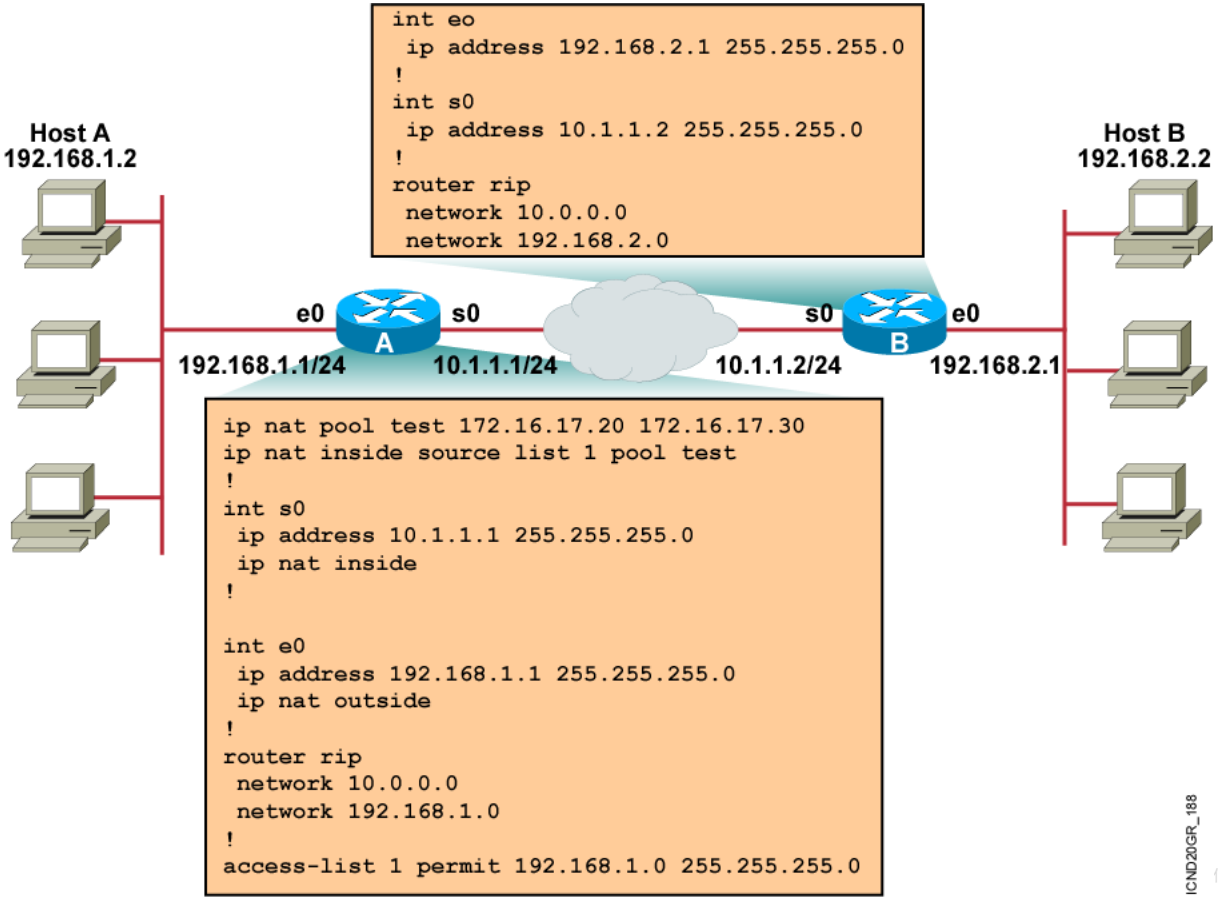
```
R2# show ip nat translations

Pro Inside global          Inside local         Outside local
tcp 209.165.200.225:16642  192.168.10.10:16642  209.165.200.254:80
tcp 209.165.200.225:62452  192.168.11.10:62452  209.165.200.254:80
 Outside global
 209.165.200.254:80
 209.165.200.254:80

R2# show ip nat translations verbose

Pro Inside global          Inside local          Outside local
tcp 209.165.200.225:16642  192.168.10.10:16642   209.165.200.254:80
Outside global
  209.165.200.254:80
    create 00:01:45, use 00:01:43 timeout:86400000, left 23:58:16, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 4, lc_entries: 0
tcp 209.165.200.225:62452  192.168.11.10:62452   209.165.200.254:80
  209.165.200.254:80
    create 00:00:37, use 00:00:35 timeout:86400000, left 23:59:24, Map-Id(In): 1,
    flags:
extended, use_count: 0, entry-id: 5, lc_entries: 0
R2#
```

验证 PAT(续)

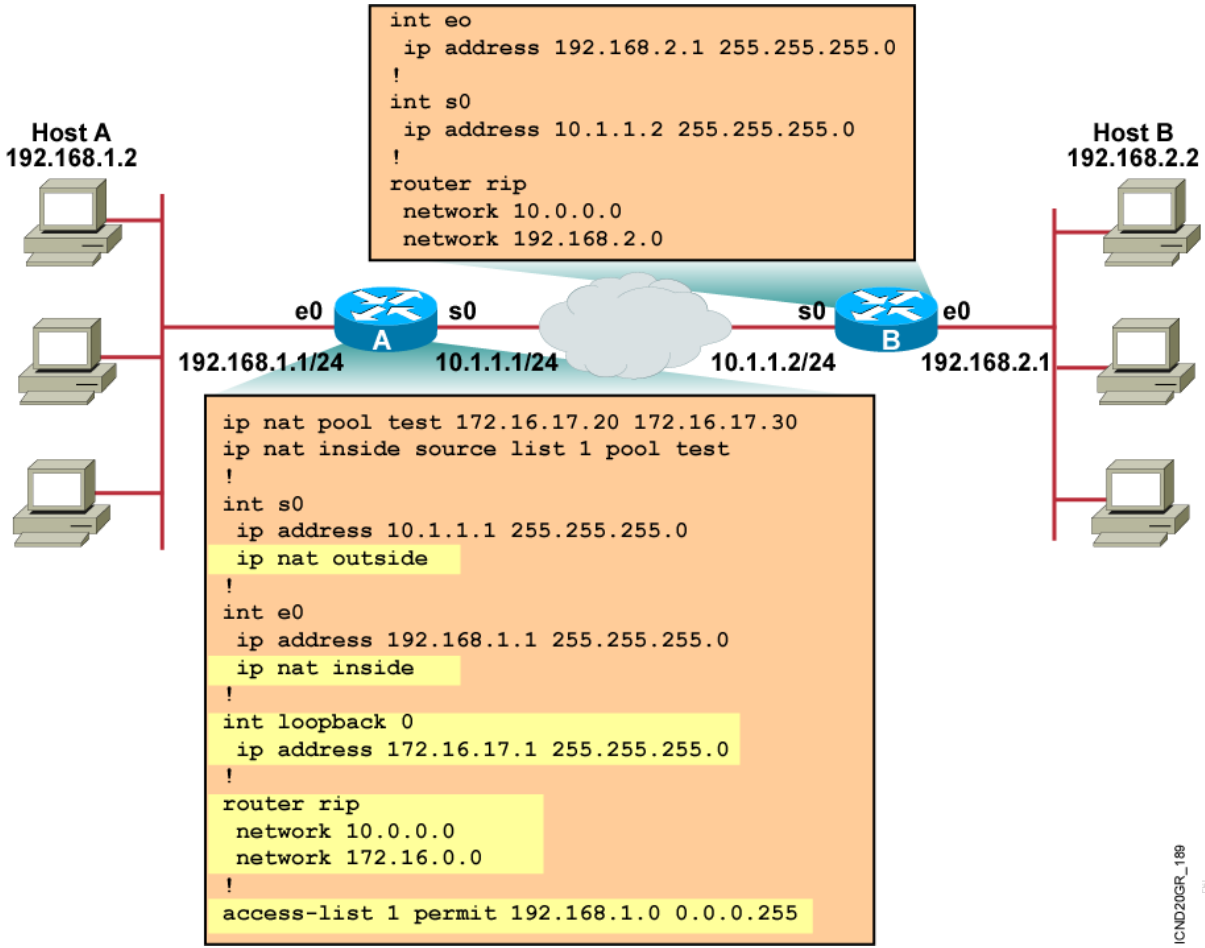
show ip nat statistics命令用于验证 NAT-POOL2 是否为两个转换分配了单个地址。输出中所包含的是有关活动转换的数量和类型、NAT 配置参数、地址池中的地址数量以及已分配的地址数量的信息。

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:31:43 ago
Outside interfaces:
Serial0/1/1
Inside interfaces:
Serial0/1/0
Hits: 4 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.225 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0
(省略部分输出)
R2#
```

Sample Problem: Cannot Ping Remote Host



Solution: New Configuration



22.7 单元练习与测验

Packet Tracer-配置IPv4 NAT

在这个 Packet Tracer 中，您会完成以下目标：

- 利用 PAT 配置动态 NAT
- 配置静态 NAT

Packet Tracer-配置IPv4 NAT

在本实验中，您将完成以下目标：

- 建立网络并配置设备的基本设置
- 配置并验证 IPv4 NAT
- 配置并验证 IPv4 PAT
- 配置并验证静态 IPv4 NAT

我在这个模块中学到了什么？

- 我们没有足够的公有IPv4，让所有设备都能使用唯一的地址来访问互联网。
- NAT的主要作用是节省了公有IPv4地址。
- 在 NAT 术语中，内部网络是指需要经过转换的网络地址集。外部网络指所有其他网络。
- NAT术语始终是从使用转换地址的设备角度出发的：
- 内部地址是经过了NAT转换的设备IP地址。
- 外部地址是目的设备的IP地址。
- 本地地址是在网络内部出现的任何地址。
- 全局地址是在网络外部出现的任何地址。
- 静态 NAT 使用本地地址和全局地址的一对一映射。
- 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。

在这个模块中我学到了什么？（续）

- 端口地址转换 (PAT)（也称为 NAT 过载），将多个私有 IPv4 地址映射到单个私有 IPv4 地址或几个地址。
- 转换数据包报头内的每个 IPv4 地址需要时间，因此 NAT 会增加转发延迟。
- 使用 NAT 也会使隧道协议（例如 IPsec）更加复杂，因为 NAT 会修改报头中的值。
- **show ip nat translations** 命令的输出中显示出已配置的所有静态转换，以及由流量创建的动态转换。
- 要想在计时器超时之前清除动态条目，我们可以使用 **clear ip nat translation** 特权EXEC模式的命令。
- IPv6的开发初衷，就是为了免除公有和私有IPv4地址之间的IPv4 NAT转换。
- IPv6中的唯一本地地址（ULA）与RFC 1918规范中的IPv4私有地址类似，但它们的用途不同。
- IPv6在IPv4和IPv6之间提供的协议转换称为NAT64。


CISCO