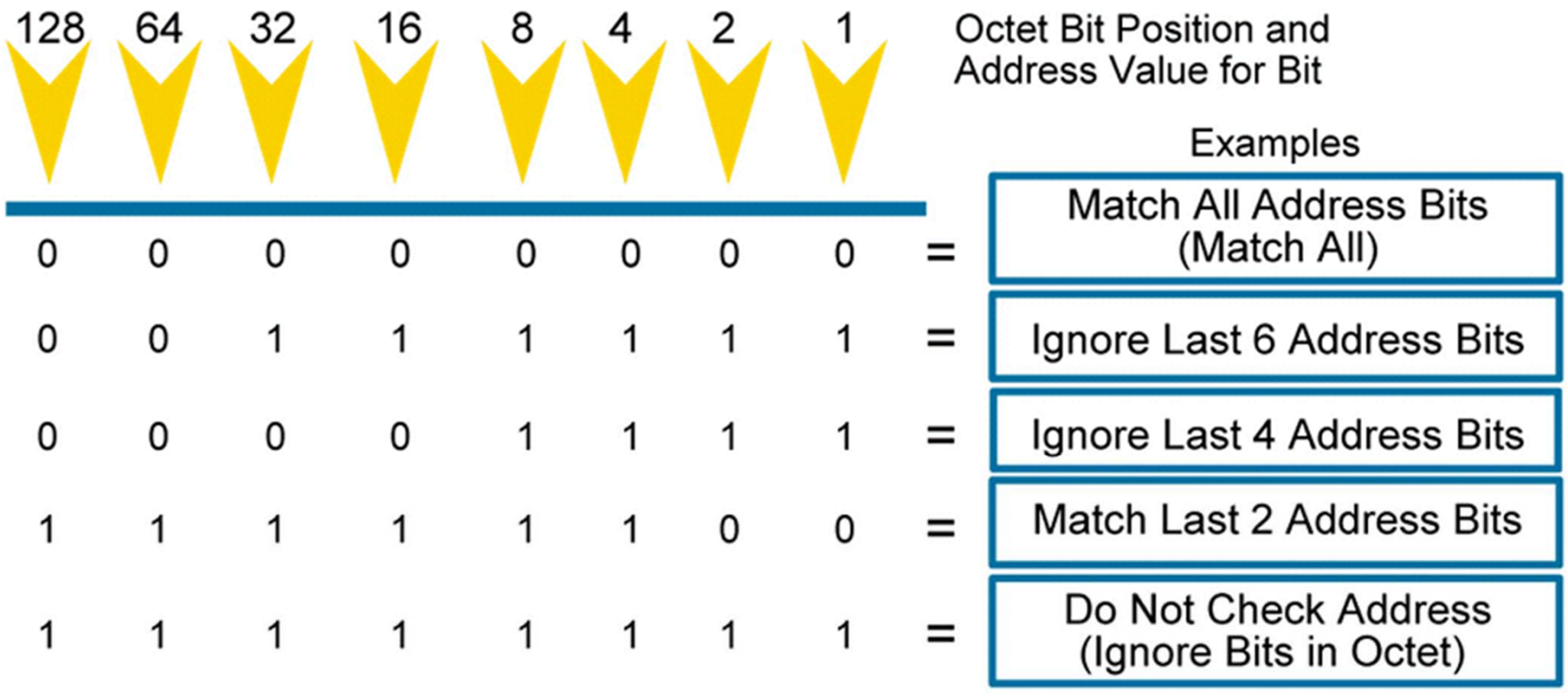
ACL Wildcard Masking

Wildcard bits—how to check the corresponding address bits:

- 0 means to match the value of the corresponding address bit.
- 1 means to ignore the value of the corresponding address bit.



ACL Wildcard Masking (Cont.)

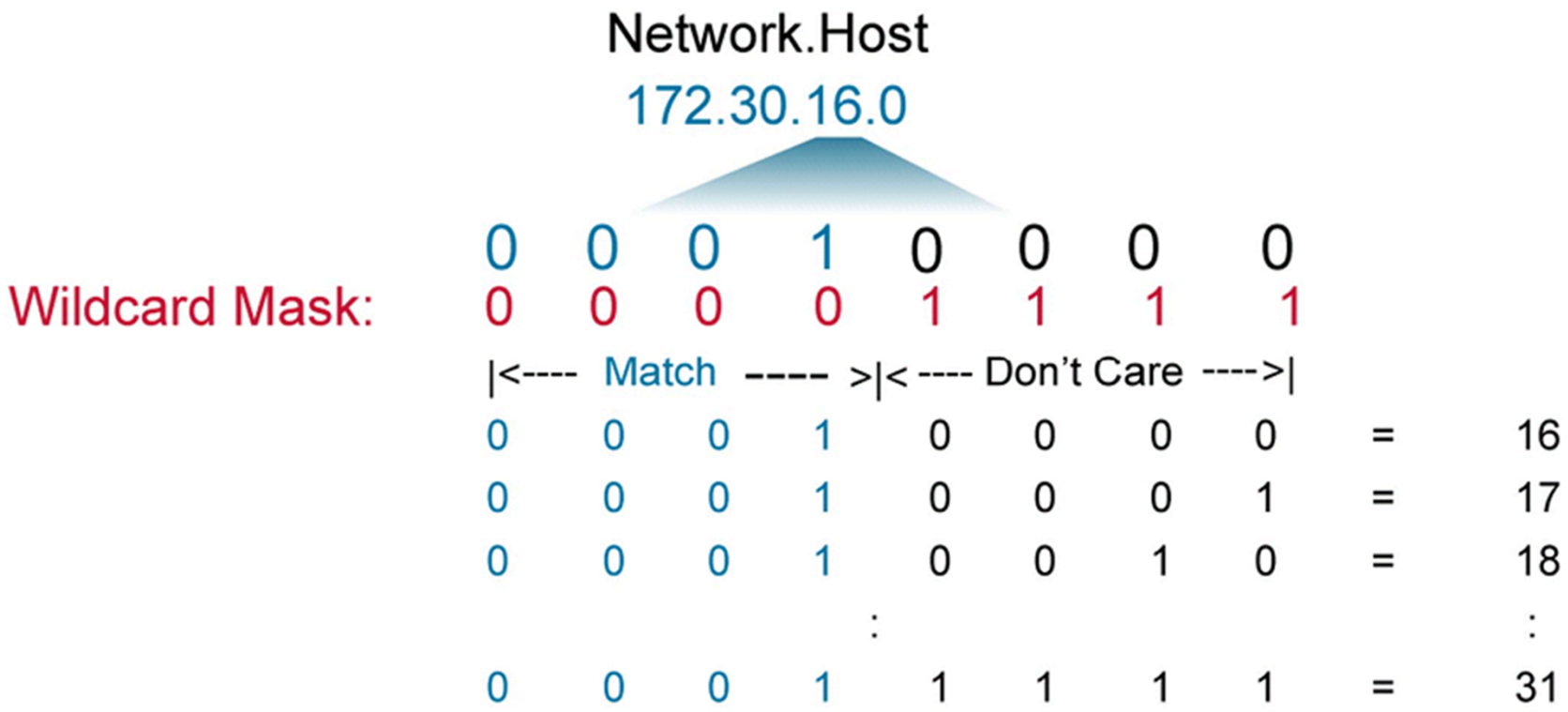
Filter for IP subnets 170.30.**16**.0/24 to 172.30.**31**.0/24.

Address and wildcard mask:

172.30.16.0 0.0.15.255

ACL Wildcard Masking (Cont.)

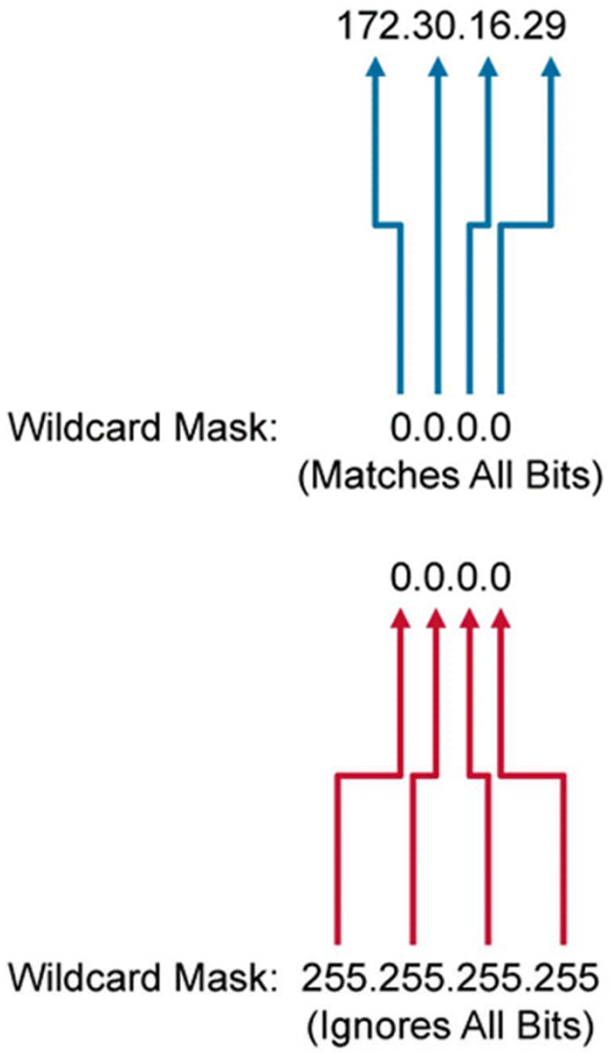
This example shows the wildcard masking process for IP subnets.



Wildcard Bit Mask Abbreviations

Using wildcard bit mask abbreviations:

- 172.30.16.29 0.0.0.0 matches all of the address bits.
- Abbreviate this wildcard mask using the IP address preceded by the keyword **host** (**host 172.30.16.29**).
- 0.0.0.0 255.255.255.255 ignores all address bits.
- Abbreviate *expression* with the keyword **any**.



Types of ACLs

Two main types of ACLs:

- Standard ACL:
  - Checks source IP address
  - Permits or denies entire protocol suite
- Extended ACL:
  - Checks source and destination IP address
  - Generally permits or denies specific protocols and applications

Two methods that you can use to identify standard and extended ACLs:

- Numbered ACLs
- Named ACLs

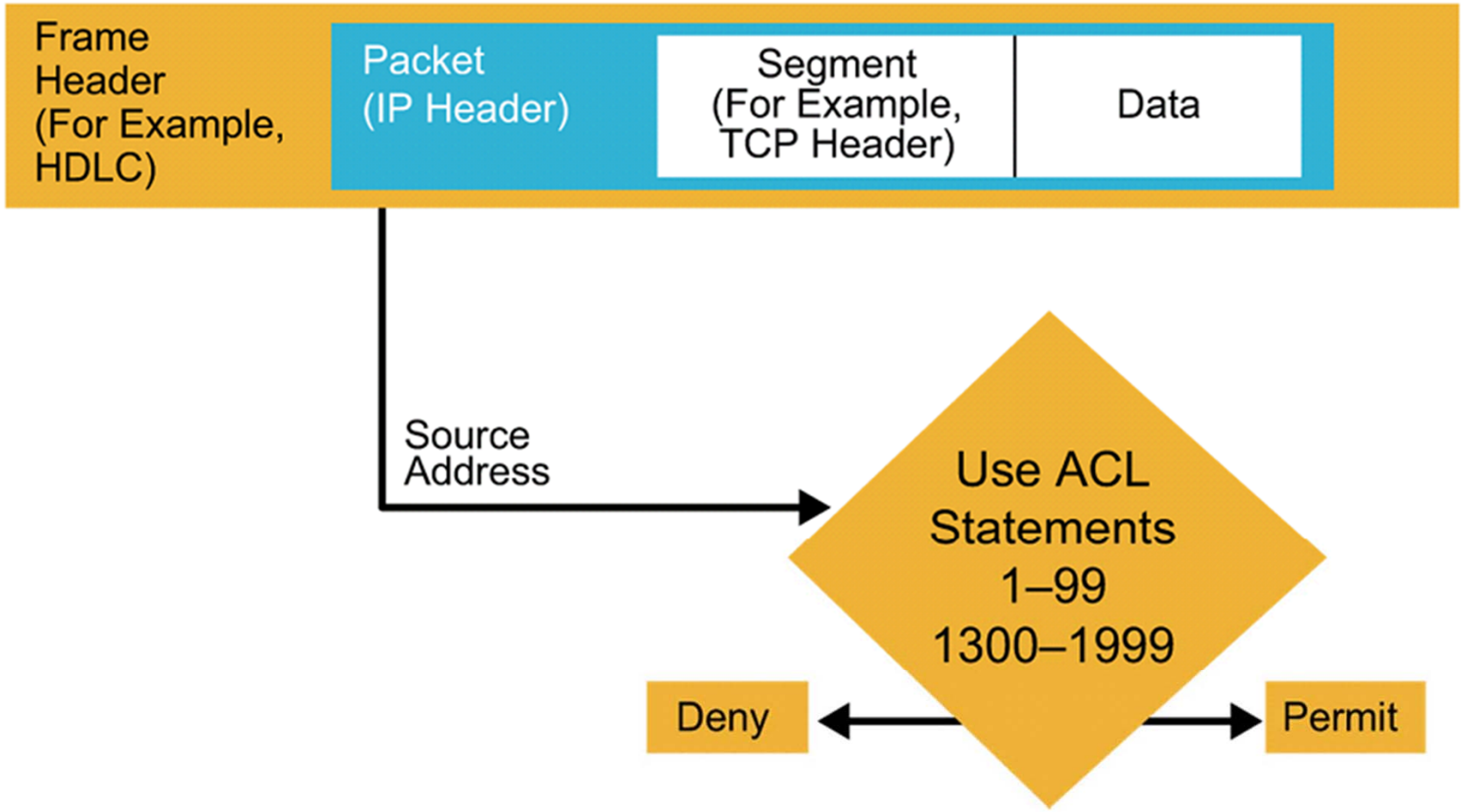
Types of ACLs (Cont.)

How to identify ACLs:

- Numbered standard IPv4 ACLs (1 to 99) test conditions of all IP packets for source addresses. The expanded range is 1300 to 1999.
- Numbered extended IPv4 ACLs (100 to 199) test conditions of source and destination addresses, specific TCP/IP protocols, and destination ports. The expanded range is 2000 to 2699.
- Named ACLs identify IP standard and extended ACLs with an alphanumeric string (name).

IPv4 ACL Type	Number Range or Identifier
Numbered Standard	1–99, 1300–1999
Numbered Extended	100–199, 2000–2699
Named (Standard and Extended)	Name

Testing An IP Packet Against a Numbered Standard Access List



Basic Configuration of Numbered Standard IPv4 ACLs

Configure a numbered standard IPv4 ACL:

- Standard ACL configuration uses 1 to 99, or 1300 to 1999, for the ACL number (1-99 in this example).

```
RouterX(config)#access-list 1 permit 172.16.0.0 0.0.255.255
```

- The default wildcard mask is 0.0.0.0 (only standard ACL).

Display the current ACLs configured on RouterX:

```
RouterX#show access-lists
Standard IP access list 1
     10 permit 172.16.0.0, wildcard bits 0.0.255.255
```

Basic Configuration of Numbered Standard IPv4 ACLs (Cont.)

Delete a numbered standard IPv4 ACL:

```
RouterX(config)#no access-list 1
RouterX(config)#exit
RouterX#show access-lists
RouterX#
```

- Use the **no access-list 1** command to remove the entire ACL 1.

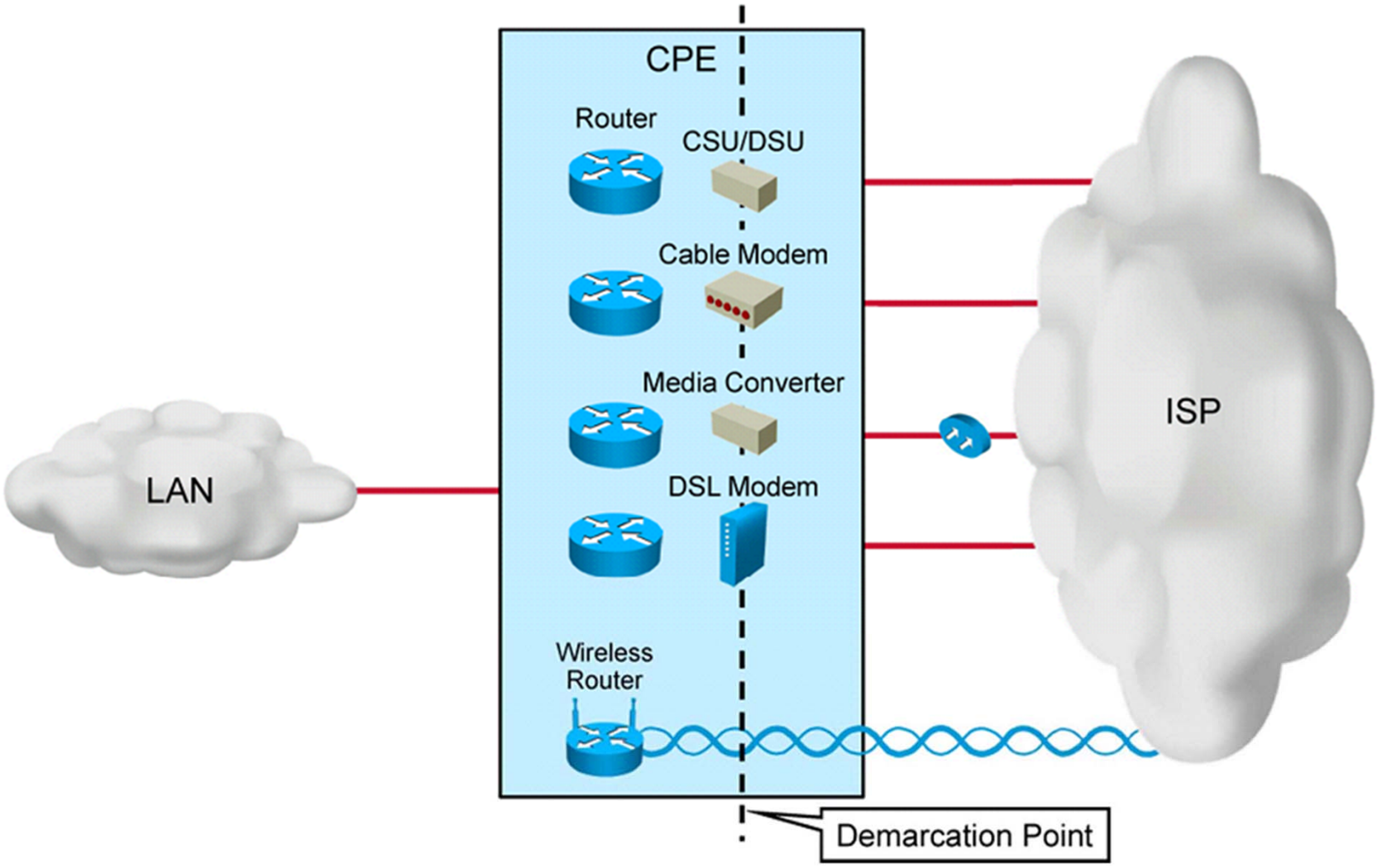
Summary

- An ACL is a tool to identify traffic for special handling.
- ACLs perform top-down processing and can be configured for incoming or outgoing traffic.
- In a wildcard bit mask, a 0 bit means to match the corresponding address bit and a 1 bit means to ignore the corresponding address bit.
- You can create an ACL using a named or numbered ACL. Named or numbered ACLs can be configured as standard or extended ACLs, which determines what they can filter.

Enabling Internet Connectivity

Establishing Internet Connectivity

The Demarcation Point



Dynamic Host Configuration Protocol

Understanding DHCP:

- DHCP is a client-server model.
- A DHCP server allocates network addresses and delivers configurations.
- A DHCP client is a host that requests an IP address and configuration from a DHCP server.

Dynamic Host Configuration Protocol (Cont.)

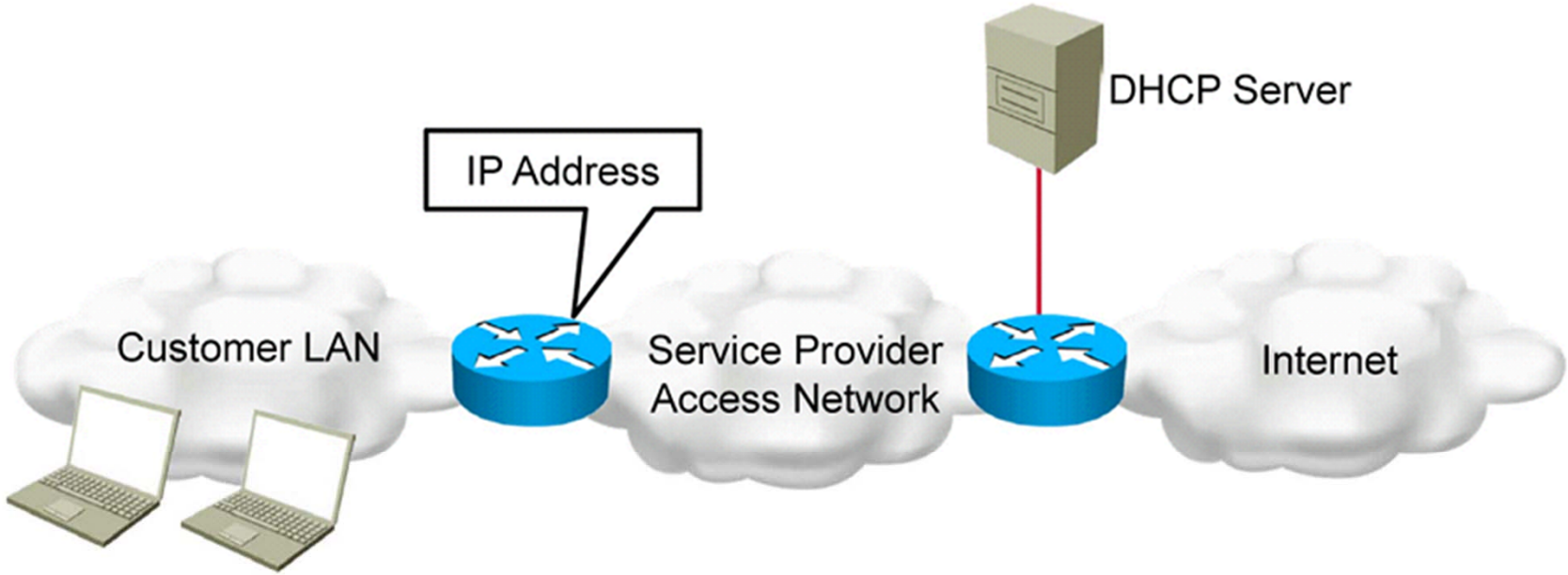
DHCP IP address allocation mechanisms:

- **Automatic allocation:** A permanent IP address is assigned to a client.
- **Dynamic allocation:** A client is assigned an IP address for a limited time.
- **Manual allocation:** A client is assigned an IP address by the network administrator.

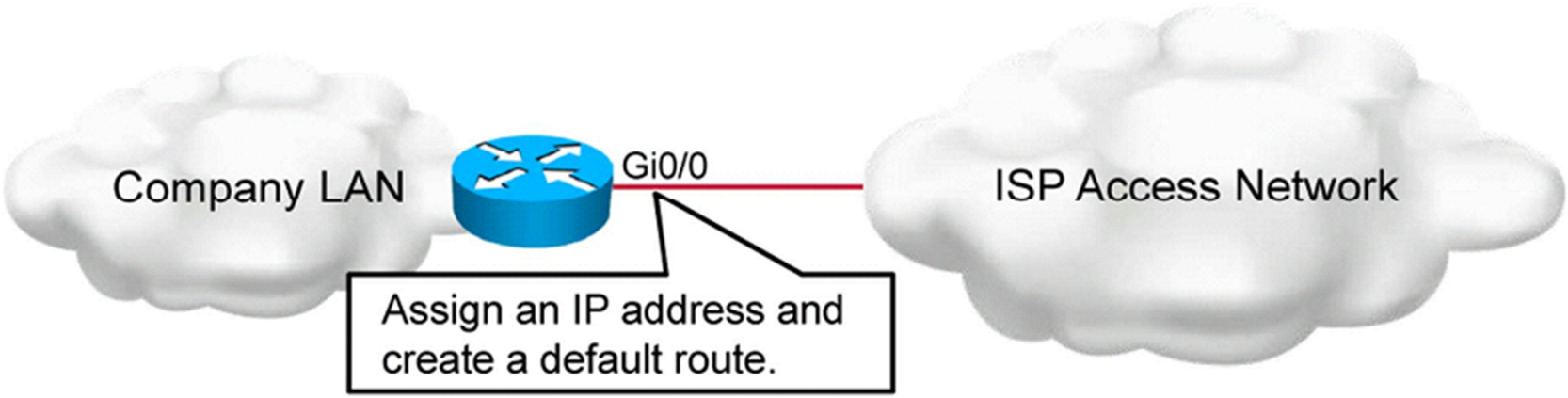
Options for Configuring a Provider-Assigned IP Address

Options for configuring IP addresses:

- Statically assigned
- Dynamically assigned through DHCP



Configuring a Static Provider-Assigned IP Address



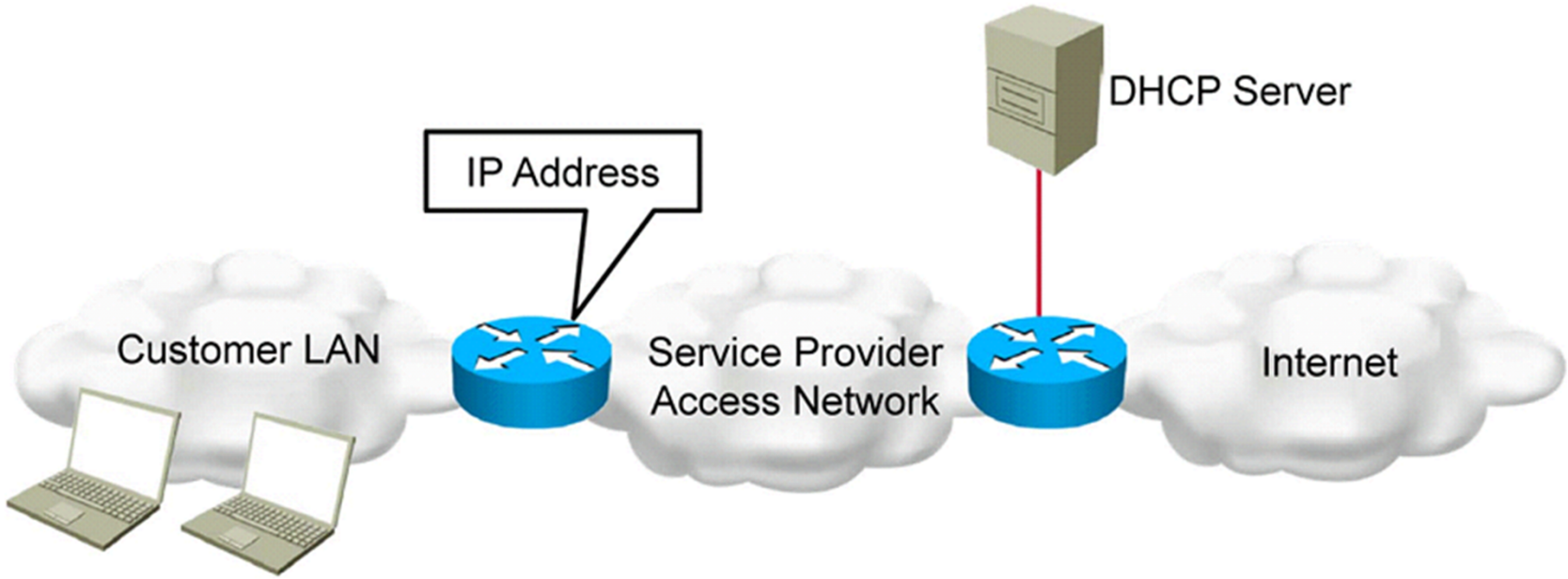

```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 209.165.200.225 255.255.255.224
Router(config-if)#no shutdown
```

- Configures a public IP address

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

- Creates a default route that points toward the next-hop IP address

Configuring a DHCP Client




```
Router(config)#interface GigabitEthernet0/0
Router(config-if)#ip address dhcp
```

- Router automatically injects default route based on optional default gateway parameter received with assigned IP address

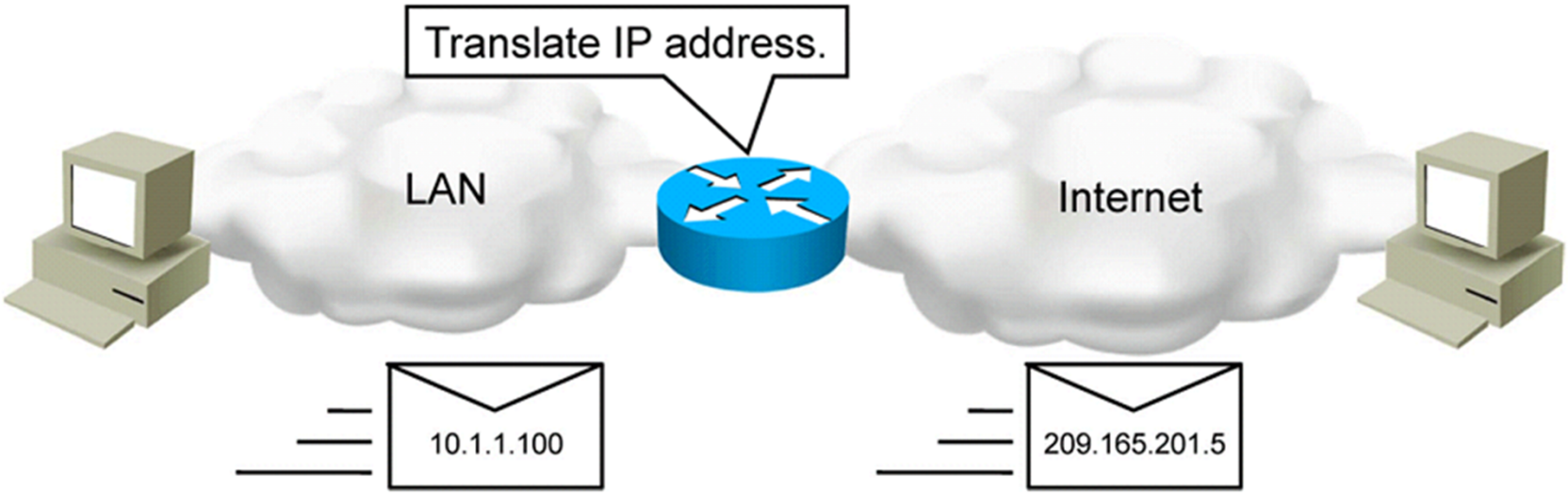
Public vs. Private IPv4 Addresses

Class	Private Address Range
A	10.0.0.0 to 10.255.255.255
B	172.16.0.0 to 172.31.255.255
C	192.168.0.0 to 192.168.255.255

Class	Public Address Range
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 172.15.255.255 172.32.0.0 to 191.255.255.255
C	192.0.0.0 to 192.167.255.255 192.169.0.0 to 223.255.255.255

Introducing NAT

NAT allows private users to access the Internet by sharing one or more public IP addresses.

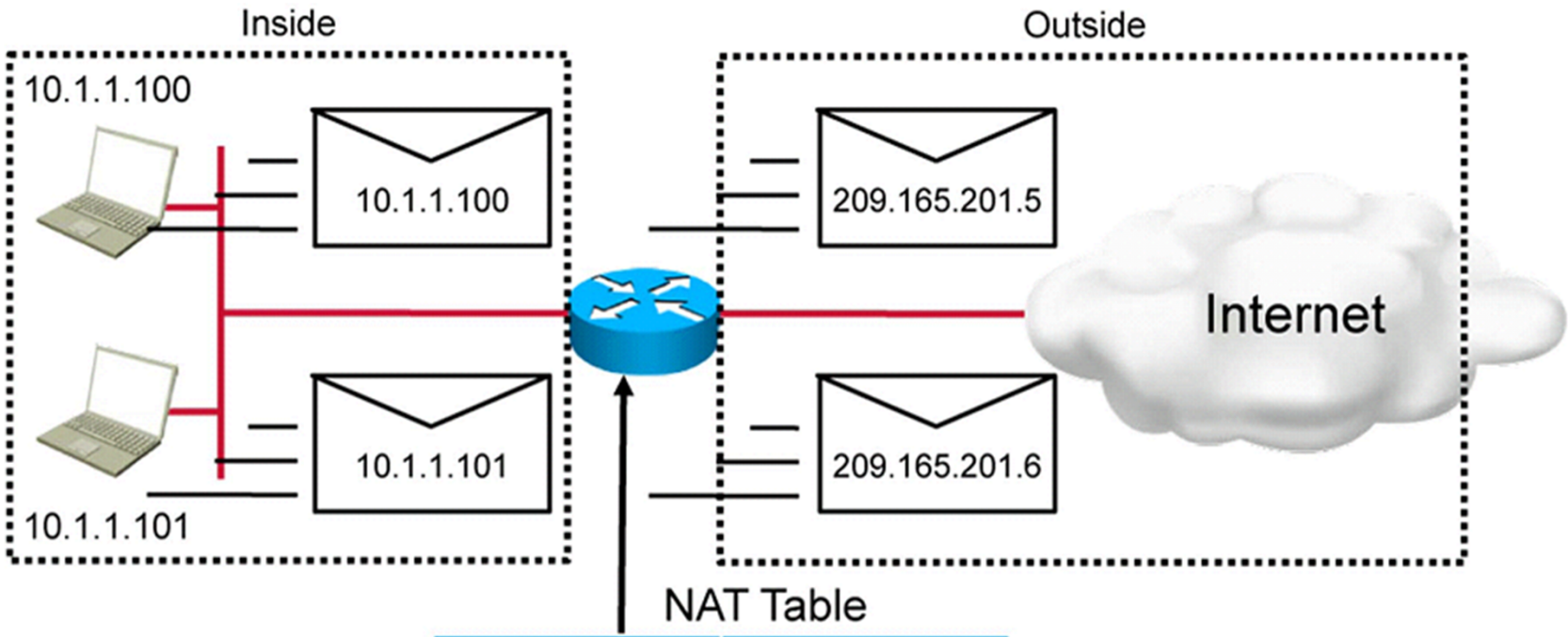


Types of Addresses in NAT

These are the most important types of addresses in NAT:

- **Inside local:** Host on the inside network
- **Inside global:** Usually assigned by an ISP and allows the customer outside access
- **Outside global:** Host on the outside network

Types of Addresses in NAT (Cont.)



NAT Table

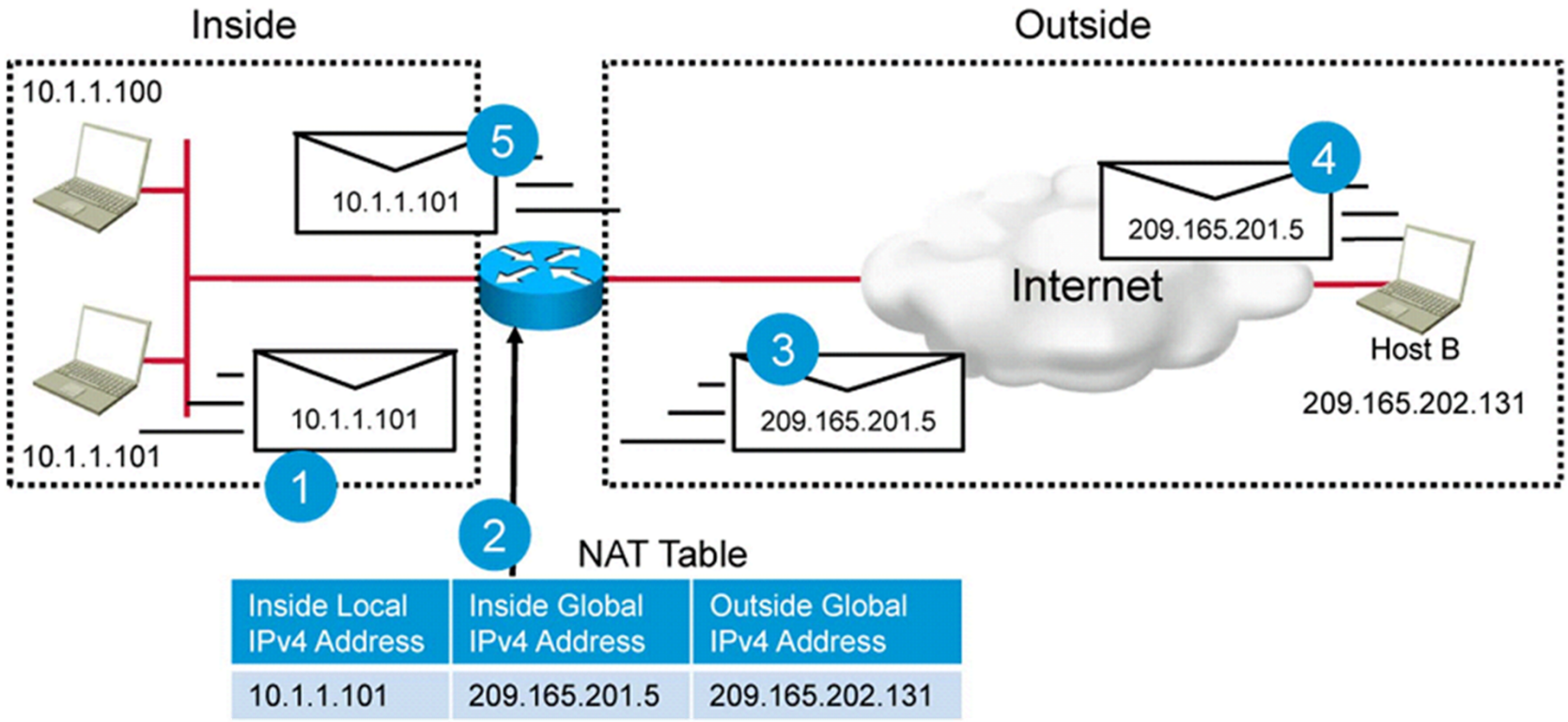
Inside Local IPv4 Address	Outside Global IPv4 Address
10.1.1.100	209.165.201.5
10.1.1.101	209.165.201.6

Types of NAT

These are the types of NAT:

- **Static NAT:** One-to-one address mapping
- **Dynamic NAT:** Many-to-many address mapping
- **PAT:** Many-to-one address mapping

Understanding Static NAT

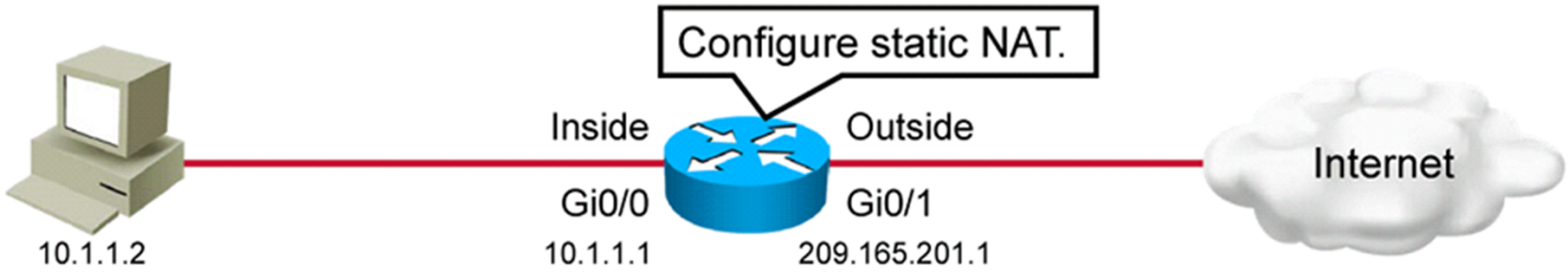


NAT Table

Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.1.1.101	209.165.201.5	209.165.202.131

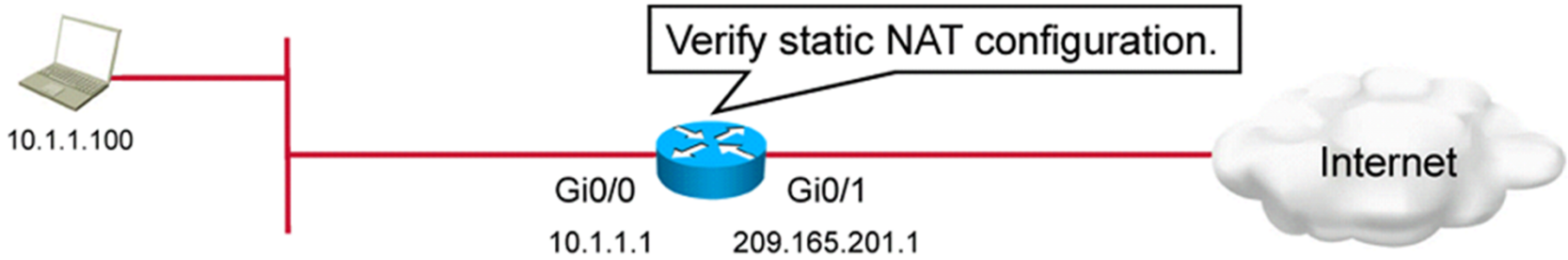
Configuring Static NAT

Example: Configuring static NAT



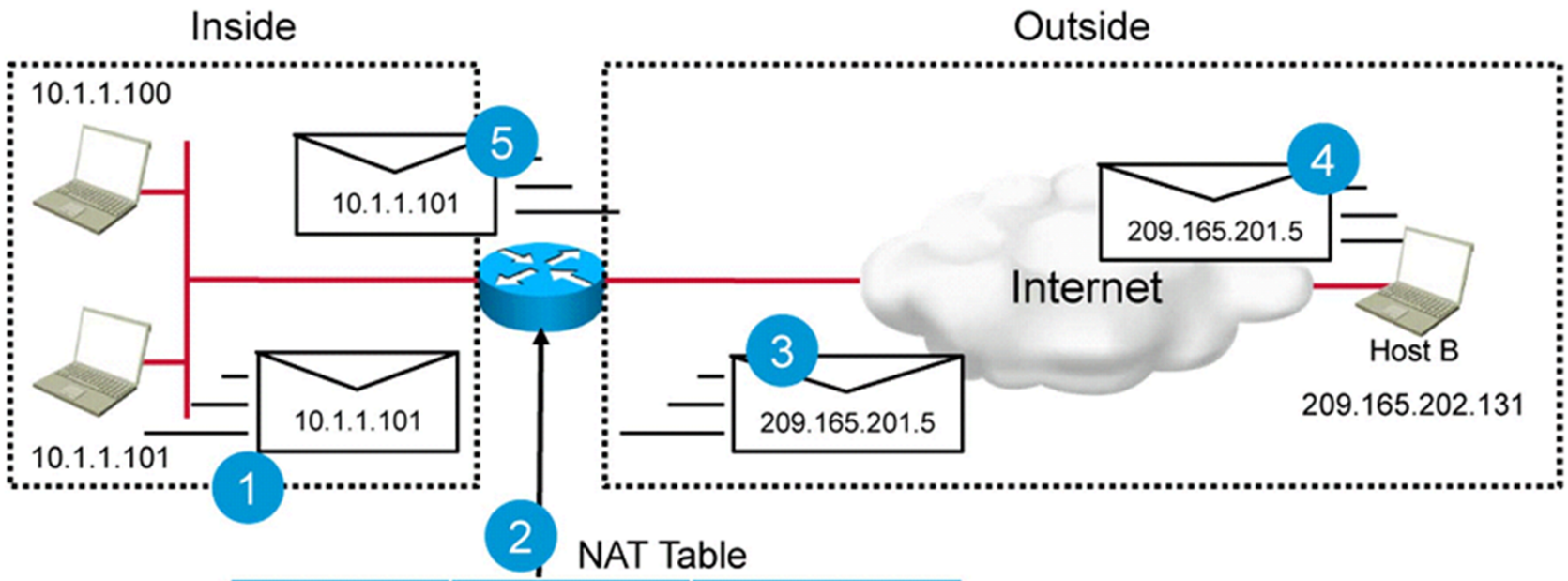

```
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip address 209.165.201.1 255.255.255.240
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#exit

Router(config)#ip nat inside source static 10.1.1.2 209.165.201.5
```

Verifying Static NAT Configuration




```
Router#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 209.165.201.5:1031 10.1.1.100:1031  209.165.202.155:23
209.165.202.155:23
--- 209.165.201.5      10.1.1.100        ---                ---
```

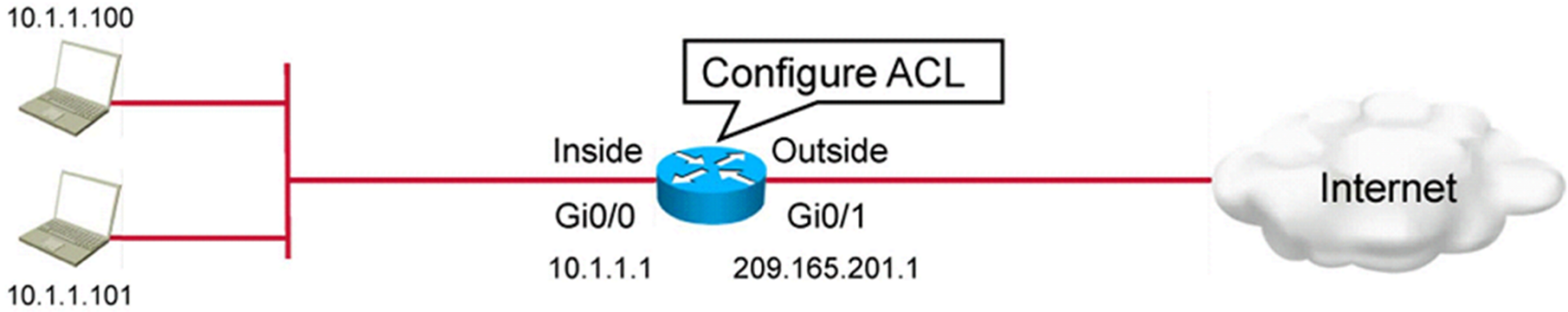
Understanding Dynamic NAT



NAT Table

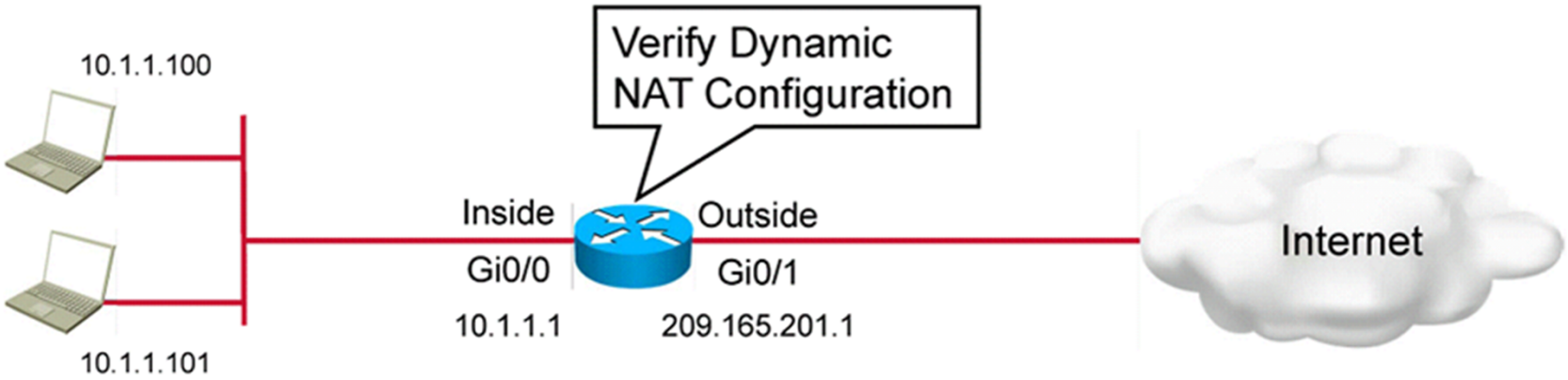
Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
10.1.1.101	209.165.201.5	209.165.202.131
10.1.1.100	209.165.201.6	209.165.202.131

Configuring Dynamic NAT



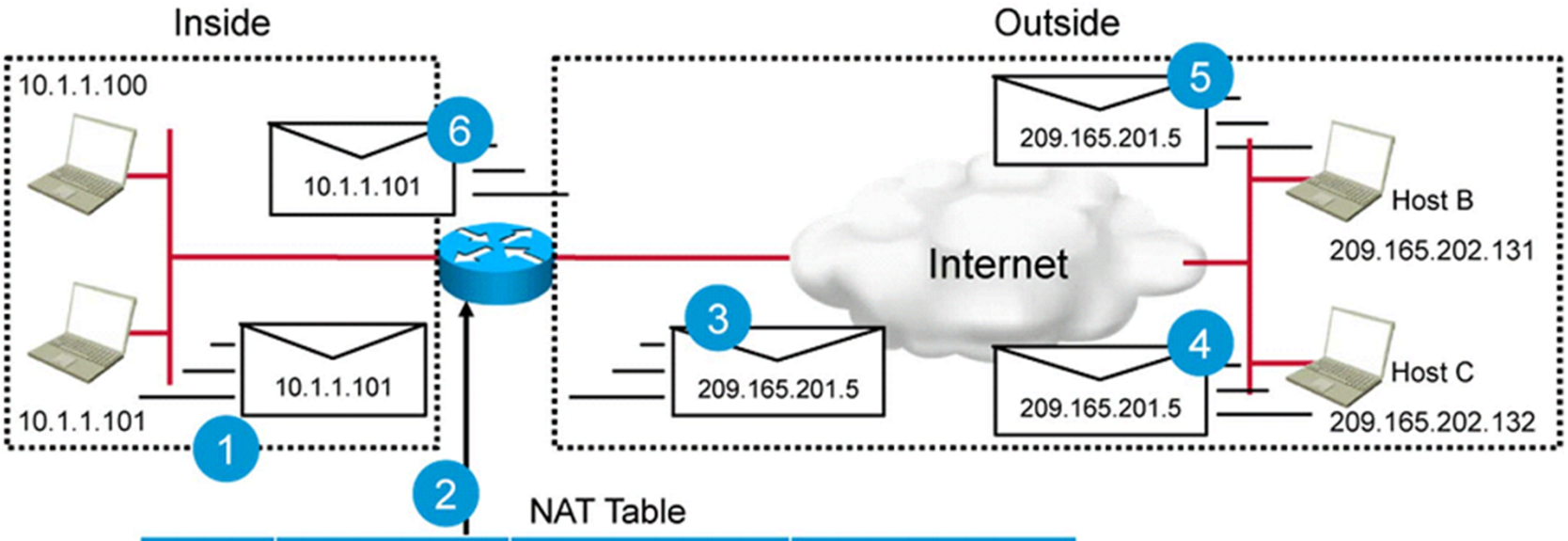

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#ip nat pool NAT-POOL 209.165.201.5 209.165.201.10 netmask
255.255.255.240

Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip address 209.165.201.1 255.255.255.240
Router(config-if)#ip nat outside
Router(config-if)#exit

Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip nat inside
Router(config-if)#exit

Router(config)#ip nat inside source list 1 pool NAT-POOL
```

Verifying Dynamic NAT Configuration




```
Router#show ip nat translations
Pro Inside global      Inside local     Outside local      Outside global
icmp 209.165.201.5:3   10.1.1.100:3     209.165.202.155:3  209.165.202.155:3
--- 209.165.201.5      10.1.1.100       ---                ---
icmp 209.165.201.6:1   10.1.1.101:1     209.165.201.125:1  209.165.201.125:1
tcp 209.165.201.6:1030 10.1.1.101:1030 209.165.201.125:23
209.165.201.125:23
--- 209.165.201.6      10.1.1.101       ---                ---
```

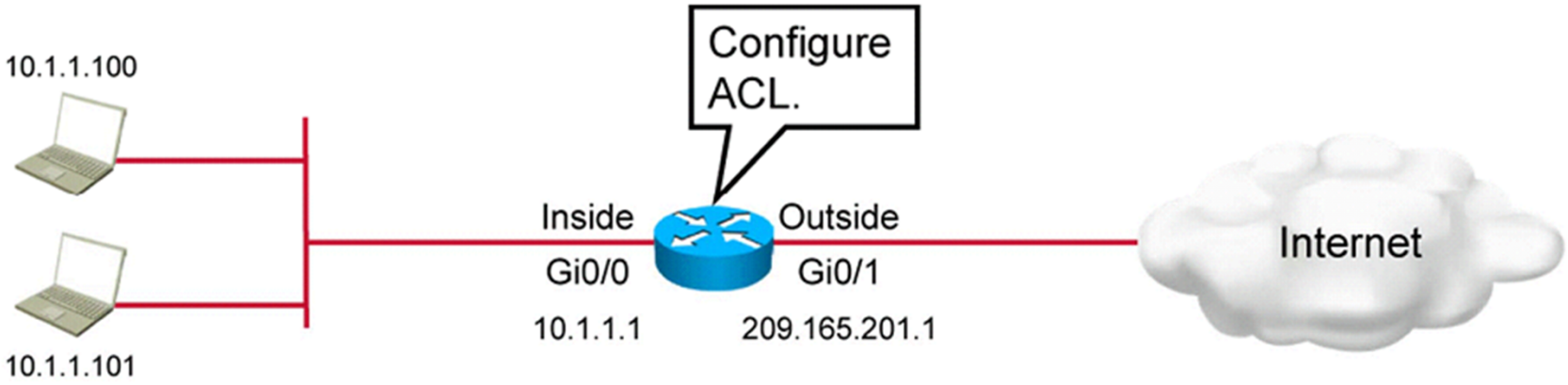
Understanding PAT



NAT Table

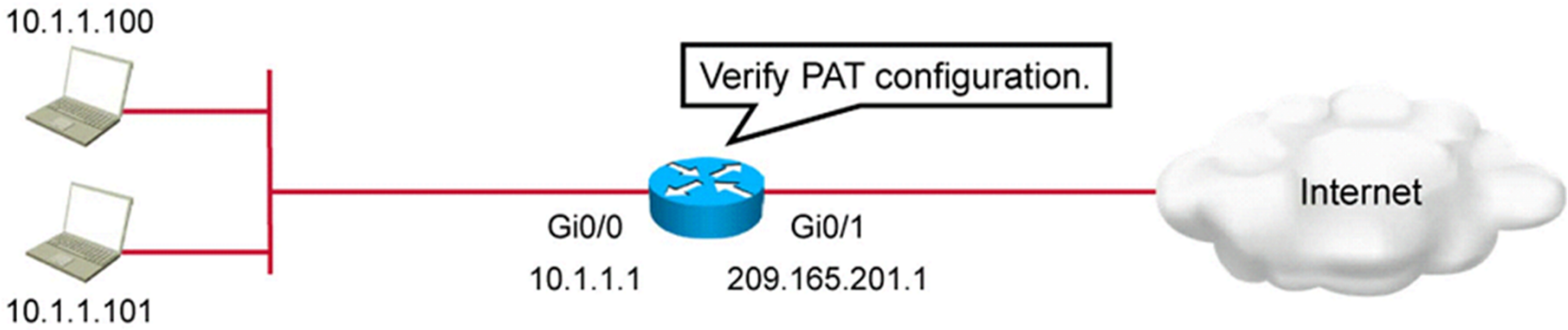
Protocol	Inside Local IPv4 Address	Inside Global IPv4 Address	Outside Global IPv4 Address
TCP	10.1.1.100:1723	209.165.201.5:1723	209.165.202.131:23
TCP	10.1.1.101:1927	209.165.201.5:1927	209.165.202.132:23
TCP	10.1.1.101:1723	209.165.201.5:1724	209.165.202.131:23

Configuring PAT



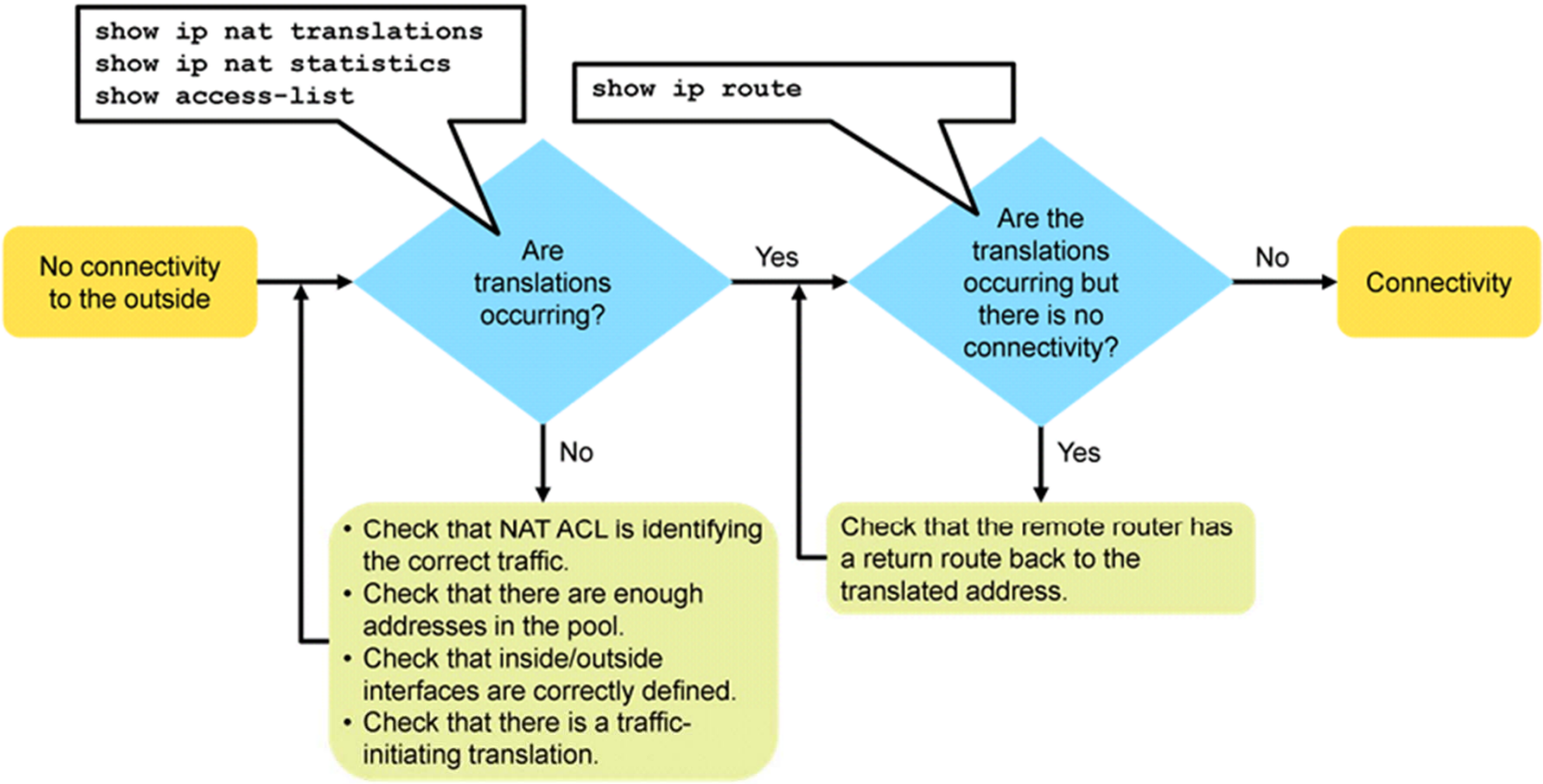

```
Router(config)#access-list 1 permit 10.1.1.0 0.0.0.255
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip address 10.1.1.1 255.255.255.0
Router(config-if)#ip nat inside

Router(config-if)#interface GigabitEthernet 0/1
Router(config-if)#ip address 209.165.201.1 255.255.255.240
Router(config#ip nat outside

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

Verifying PAT Configuration




```
Router#show ip nat translations
Pro Inside global        Inside local      Outside local       Outside global
tcp 209.165.201.5:27497 10.1.1.100:27497 209.165.202.155:80
209.165.202.155:80
tcp 209.165.201.5:2597  10.1.1.100:2597  209.165.201.125:443
209.165.201.125:443
```

Troubleshooting NAT



Troubleshooting NAT (Cont.)

Are Addresses Being Translated?

```
Router#show ip nat statistics
Total translations: 5 (0 static, 5 dynamic, 5 extended)
Outside Interfaces: Serial0
Inside Interfaces: Ethernet0 , Ethernet1
Hits: 42 Misses: 44
<output omitted>
```

- Monitors NAT statistics

```
Router#show access-list
access-list 1 permit 10.1.1.100 0.0.0.255
```

- Verifies that the NAT ACL is permitting all necessary networks

Troubleshooting NAT (Cont.)

- To display detailed dynamic data and events, you can use **debug** commands.
  - A **debug** command can intensively use device resources. Use carefully on production equipment.
  - Always turn off **debug** after troubleshooting with the **no debug all** command.

```
Router#debug ip nat
NAT*: s=10.1.1.100->209.165.201.1, d=172.16.1.100 [103]
NAT*: s=172.16.1.100, d=209.165.201.1->10.1.1.100 [103]
NAT*: s=10.1.1.100->209.165.201.1, d=172.16.1.100 [104]
NAT*: s=172.16.1.100, d=209.165.201.1->10.1.1.100 [104]
<output omitted>
```

- Displays information about every packet that is translated by the router

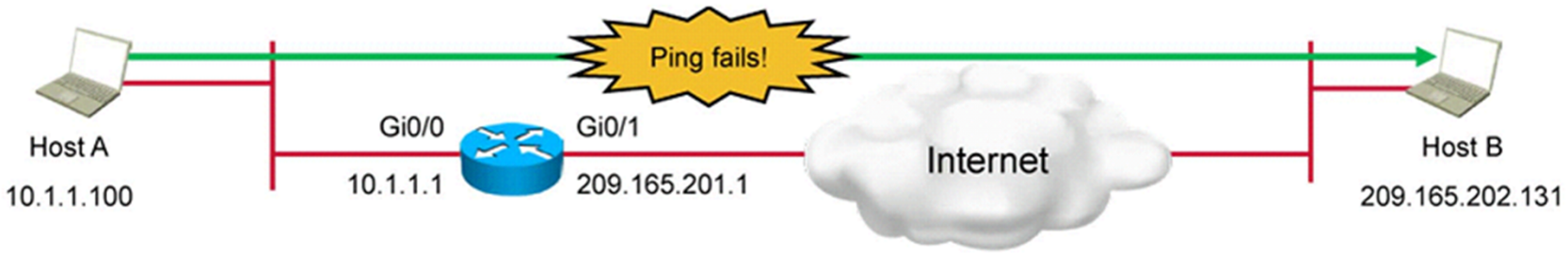
Troubleshooting NAT (Cont.)

If translations are occurring, but there is no connectivity, verify that the remote router has a route to the translated address.


```
Branch#show ip route
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
   i - IS-IS, su - IS-IS summary, 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, + - replicated route
Gateway of last resort is 209.165.201.1 to network 0.0.0.0
C 10.1.1.0/24 is directly connected, GigabitEthernet0/0
L 10.1.1.2/32 is directly connected, GigabitEthernet0/0
C 209.165.201.0/27 is directly connected, GigabitEthernet0/1
S* 0.0.0.0/0 [1/0] via 209.165.201.1
```

Troubleshooting NAT Case Study

Host A and host B are unable to ping after a new NAT configuration is put in place.

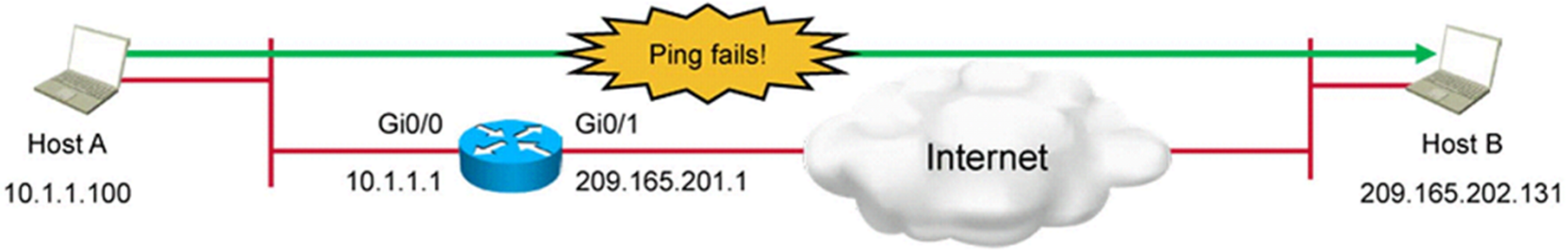


Troubleshooting NAT Case Study (Cont.)

```
Router#show running-config
<output omitted>
ip route 0.0.0.0 0.0.0.0 209.165.201.2
!
access-list 20 permit 0.0.0.0 255.255.255.0
!
interface GigabitEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat outside
!
interface GigabitEthernet0/1
 ip address 209.165.200.1 255.255.255.254
 ip nat inside
!
ip nat inside source list 20 interface GigabitEthernet0/1 overload
```

Troubleshooting NAT Case Study (Cont.)

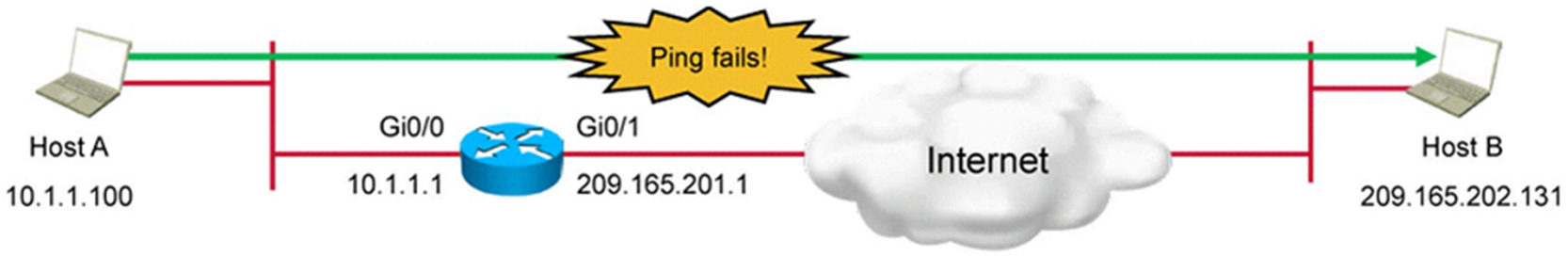
Translations are not occurring.




```
Router#show ip nat translations
   Pro Inside global    Inside local    Outside local    Outside global
```

Troubleshooting NAT Case Study (Cont.)

The router interfaces are incorrectly defined as NAT inside and NAT outside.




```
Router#show ip nat statistics
      Total active translations: 0 (0 static, 0 dynamic; 0 extended)
      Outside interfaces:
      GigabitEthernet0/0
      Inside interfaces:
      GigabitEthernet0/1
<output omitted>
```

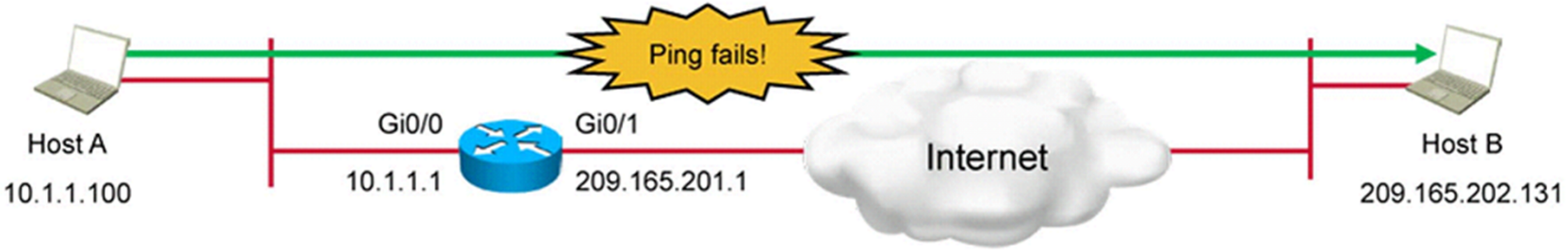
Troubleshooting NAT Case Study (Cont.)

How to fix configuration:

```
Router#configure terminal
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip nat inside
Router(config-if)#interface GigabitEthernet 0/1
Router(config-if)#ip nat outside
```

Troubleshooting NAT Case Study (Cont.)

Verify that the access list is correct.



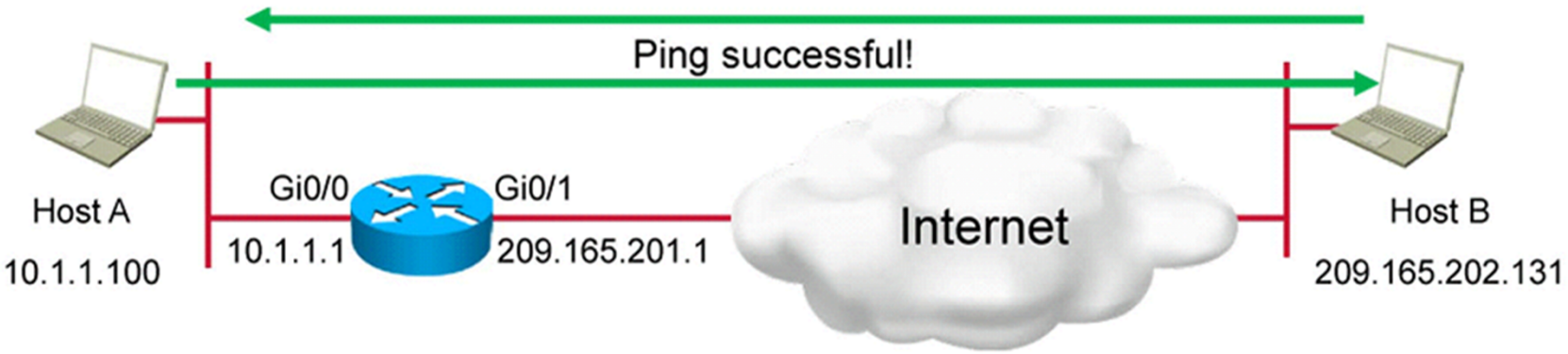

```
RouterA#show access-list

Standard IP access list 20
   10 permit 0.0.0.0, wildcard bits 255.255.255.0
```

How to fix access list:

```
Router#config terminal
Router(config)#no access-list 20
Router(config)#access-list 20 permit 10.1.1.0 0.0.0.255
```

Troubleshooting NAT Case Study (Cont.)

Verify that translations are occurring and you have connectivity to the remote network.




```
C:\>ping 209.165.202.131
Pinging 209.165.202.131 with 32 bytes of data:
Reply from 209.165.202.131: bytes=32 time=107ms TTL=127
Reply from 209.165.202.131: bytes=32 time=70ms TTL=127
<output omitted>
```

```
Router#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.201.1:1  10.1.1.100:1    209.165.202.131:1  209.165.202.131:1
```

Summary

- Provider-assigned IP addresses can be configured on a router statically or can be dynamically assigned through DHCP.
- A DHCP client is a host that requests an IP address and configuration from a DHCP server.
- A DHCP server allocates network addresses and delivers configurations.

Summary (Cont.)

- NAT enables private IP internetworks that use private IP addresses to connect to the Internet. PAT, or NAT overload, a feature of NAT, enables several internal addresses to be translated to only one or a few external addresses.
- Static NAT is one-to-one address mapping. Dynamic NAT addresses are picked from a pool.
- PAT allows you to map many inside addresses to one outside address.
- Use the **show ip nat translations** command to display the translation table and verify that translation has occurred.
- To determine whether a current translation entry is being used, use the **show ip nat statistics** command to check the hits counter.

Module Summary

- IP is a Layer 3 media-independent connectionless protocol that uses hierarchical logical addressing and provides best-effort service.
- Internet hosts require a unique public IP address. Hosts in private networks can have any valid private IP address that is unique locally in each network.
- Networks, particularly large networks, are often divided into smaller subnetworks, or subnets. Subnets can improve network performance and control.
- TCP is a connection-oriented protocol that provides reliable transport. UDP is a connectionless transport protocol that provides best-effort transport.

Module Summary (Cont.)

- The main function of a router is to relay packets from one network device to another. To do this, you must define the characteristics of the interfaces through which packets are received and sent. Interface characteristics, such as the IP address, are configured in interface configuration mode.
- Cisco Discovery Protocol is an information-gathering tool that is used by network administrators to obtain information about directly connected devices.
- Static routers use a route that a network administrator manually enters into the router. Dynamic routers use a route that a network routing protocol adjusts automatically for topology or traffic changes.

Module Summary (Cont.)

- ACLs can be used as a Cisco IOS tool to identify traffic that receives special handling.
- NAT enables private IP internetworks that use private IP addresses to connect to the Internet. PAT, a feature of NAT, enables several internal addresses to be translated to one external address or a few external addresses.