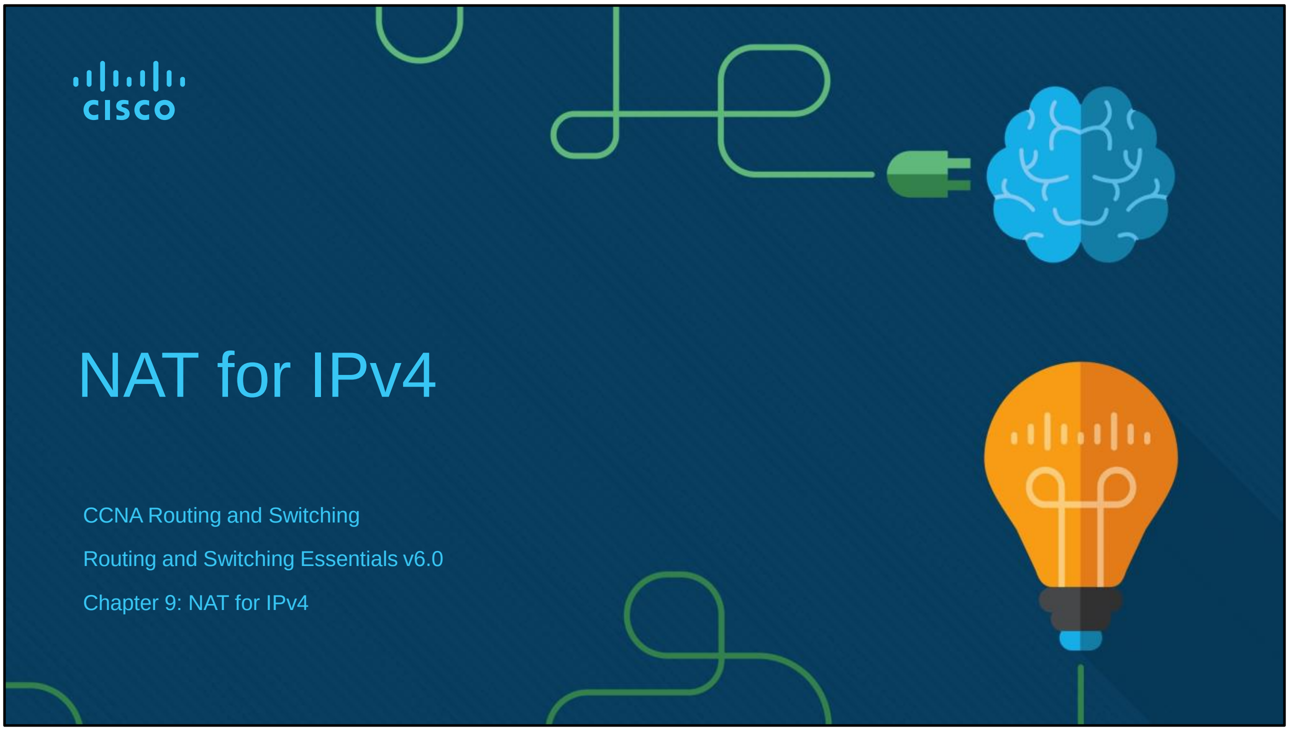


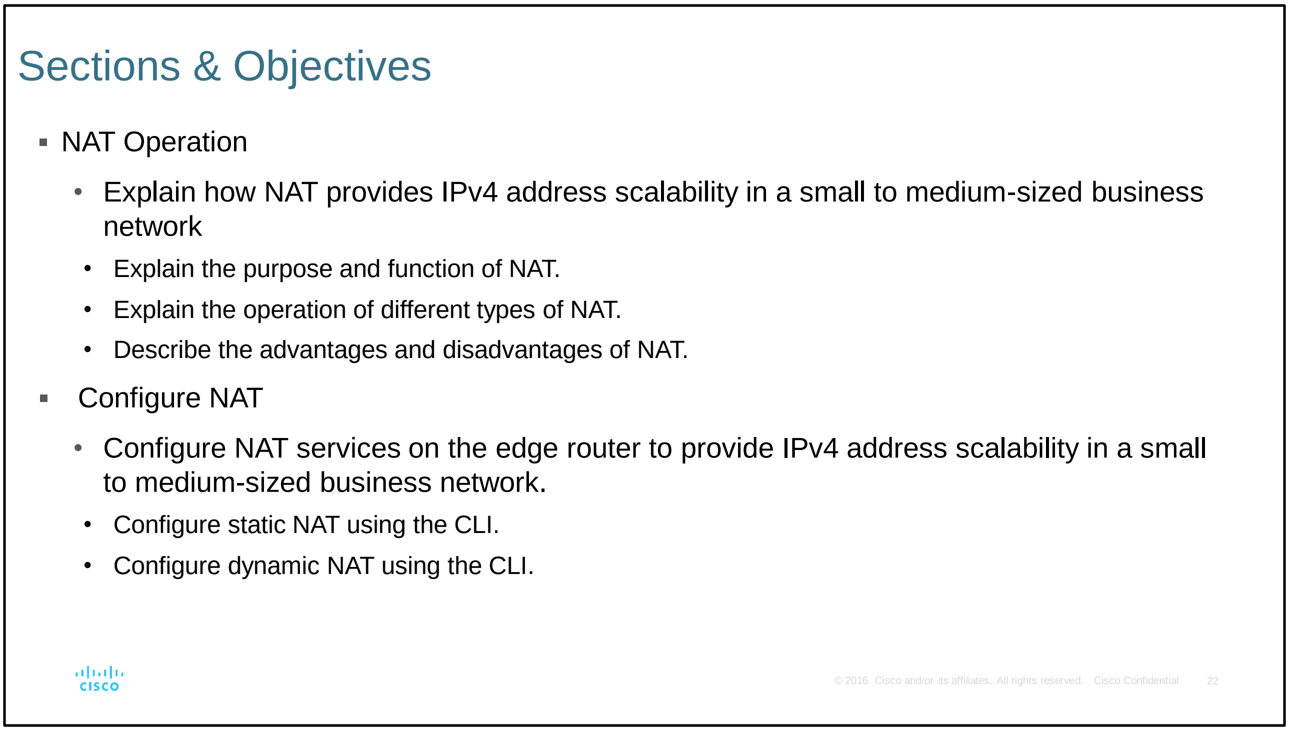
NAT for IPv4

CCNA Routing and Switching

Routing and Switching Essentials v6.0

Chapter 9: NAT for IPv4

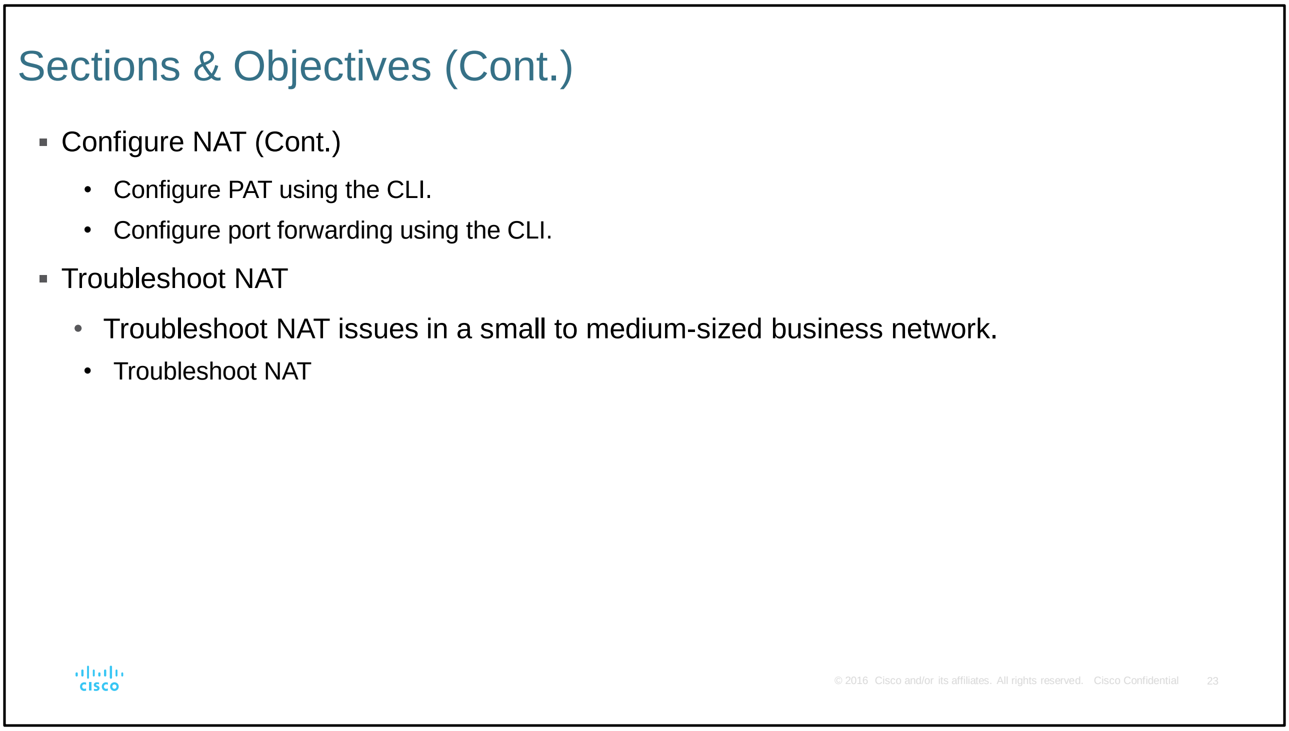
Cisco Networking Academy Program
Routing and Switching Essentials v6.0
Chapter 9: NAT for IPv4



Sections & Objectives

- NAT Operation
  - Explain how NAT provides IPv4 address scalability in a small to medium-sized business network
  - Explain the purpose and function of NAT.
  - Explain the operation of different types of NAT.
  - Describe the advantages and disadvantages of NAT.
- Configure NAT
  - Configure NAT services on the edge router to provide IPv4 address scalability in a small to medium-sized business network.
  - Configure static NAT using the CLI.
  - Configure dynamic NAT using the CLI.

Cisco Networking Academy Program
Routing and Switching Essentials v6.0
Chapter 9: NAT for IPv4



Sections & Objectives (Cont.)

- Configure NAT (Cont.)
  - Configure PAT using the CLI.
  - Configure port forwarding using the CLI.
- Troubleshoot NAT
  - Troubleshoot NAT issues in a small to medium-sized business network.
  - Troubleshoot NAT

Cisco Networking Academy Program
Routing and Switching Essentials v6.0
Chapter 9: NAT for IPv4

NAT Operation

All public IPv4 addresses that transverse the Internet must be registered with a Regional Internet Registry (RIR). Organizations can lease public addresses from an SP, but only the registered holder of a public Internet address can assign that address to a network device. However, with a theoretical maximum of 4.3 billion addresses, IPv4 address space is severely limited. When Bob Kahn and Vint Cerf first developed the suite of TCP/IP protocols including IPv4 in 1981, they never envisioned what the Internet would become. At the time, the personal computer was mostly a curiosity for hobbyists and the World Wide Web was still more than a decade away.

With the proliferation of personal computing and the advent of the World Wide Web, it soon became obvious that 4.3 billion IPv4 addresses would not be enough. The long term solution was IPv6, but more immediate solutions to address exhaustion were required. For the short term, several solutions were implemented by the IETF including Network Address Translation (NAT) and RFC 1918 private IPv4 addresses.

The chapter discusses how NAT, combined with the use of private address space, is used to both conserve and more efficiently use IPv4 addresses to provide networks of all sizes access to the Internet. This chapter covers:

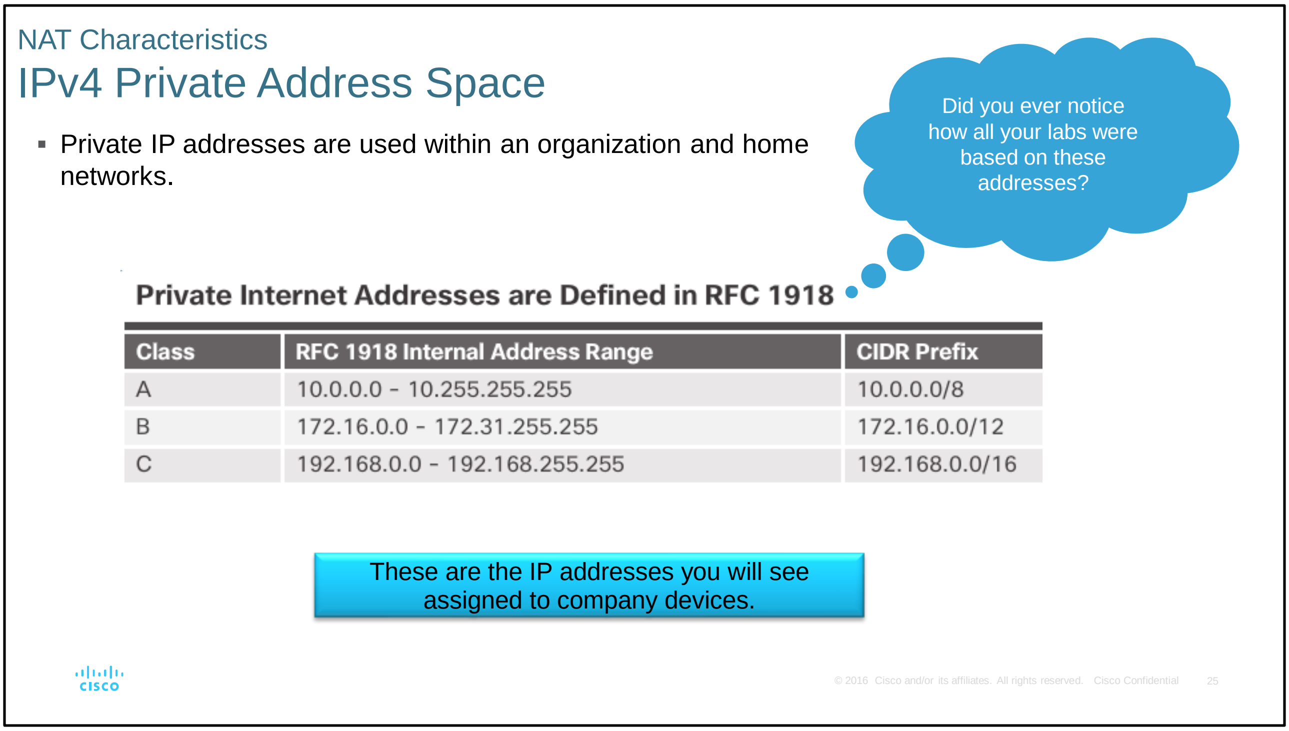
NAT characteristics, terminology, and general operations

The different types of NAT, including static NAT, dynamic NAT, and NAT with overloading

The benefits and disadvantages of NAT

The configuration, verification, and analysis of static NAT, dynamic NAT, and NAT with overloading

How port forwarding can be used to access an internal devices from the Internet
Troubleshooting NAT using **show** and **debug** commands
How NAT for IPv6 is used to translate between IPv6 addresses and IPv4 addresses



NAT Characteristics

IPv4 Private Address Space

- Private IP addresses are used within an organization and home networks.

Did you ever notice how all your labs were based on these addresses?

Private Internet Addresses are Defined in RFC 1918

Class	RFC 1918 Internal Address Range	CIDR Prefix
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

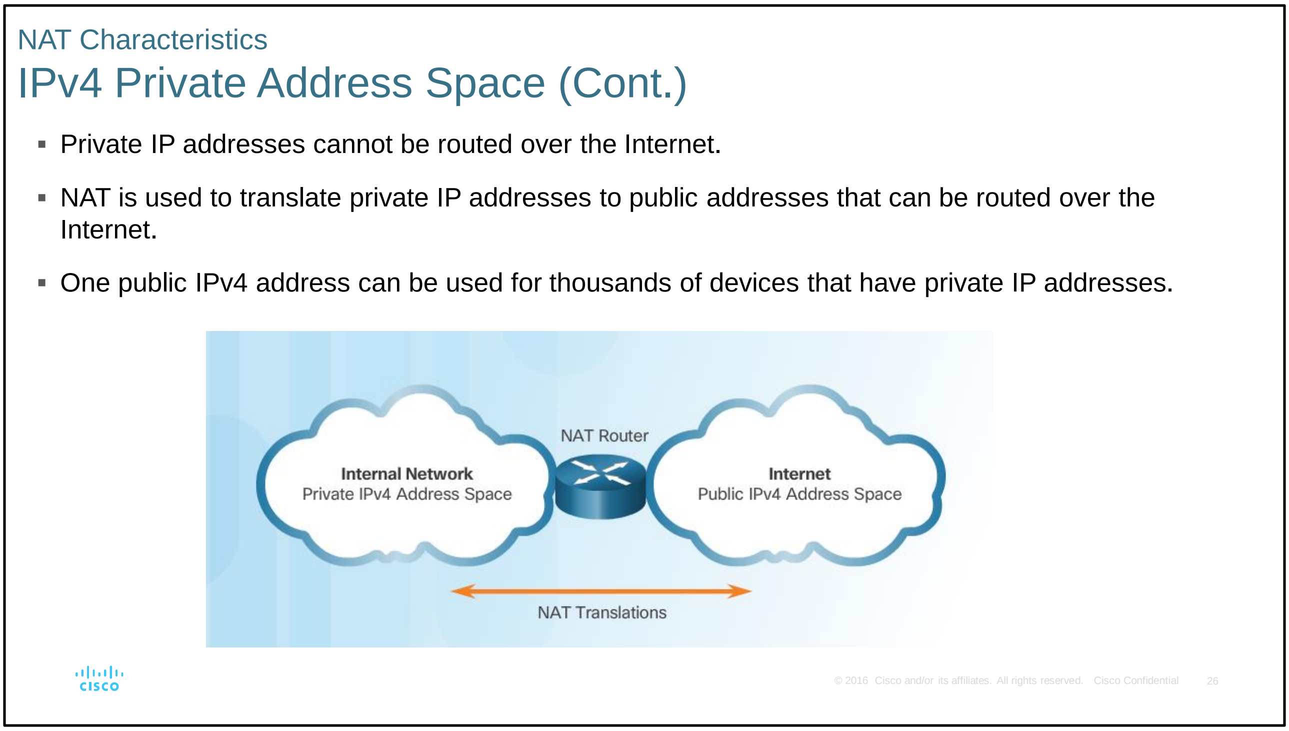
These are the IP addresses you will see assigned to company devices.

There are not enough public IPv4 addresses to assign a unique address to each device connected to the Internet. Networks are commonly implemented using private IPv4 addresses, as defined in RFC 1918.

Figure shows the range of addresses included in RFC 1918. It is very likely that the computer that you use to view this course is assigned a private address.

These private addresses are used within an organization or site to allow devices to communicate locally. However, because these addresses do not identify any single company or organization, private IPv4 addresses cannot be routed over the Internet.

To allow a device with a private IPv4 address to access devices and resources outside of the local network, the private address must first be translated to a public address.



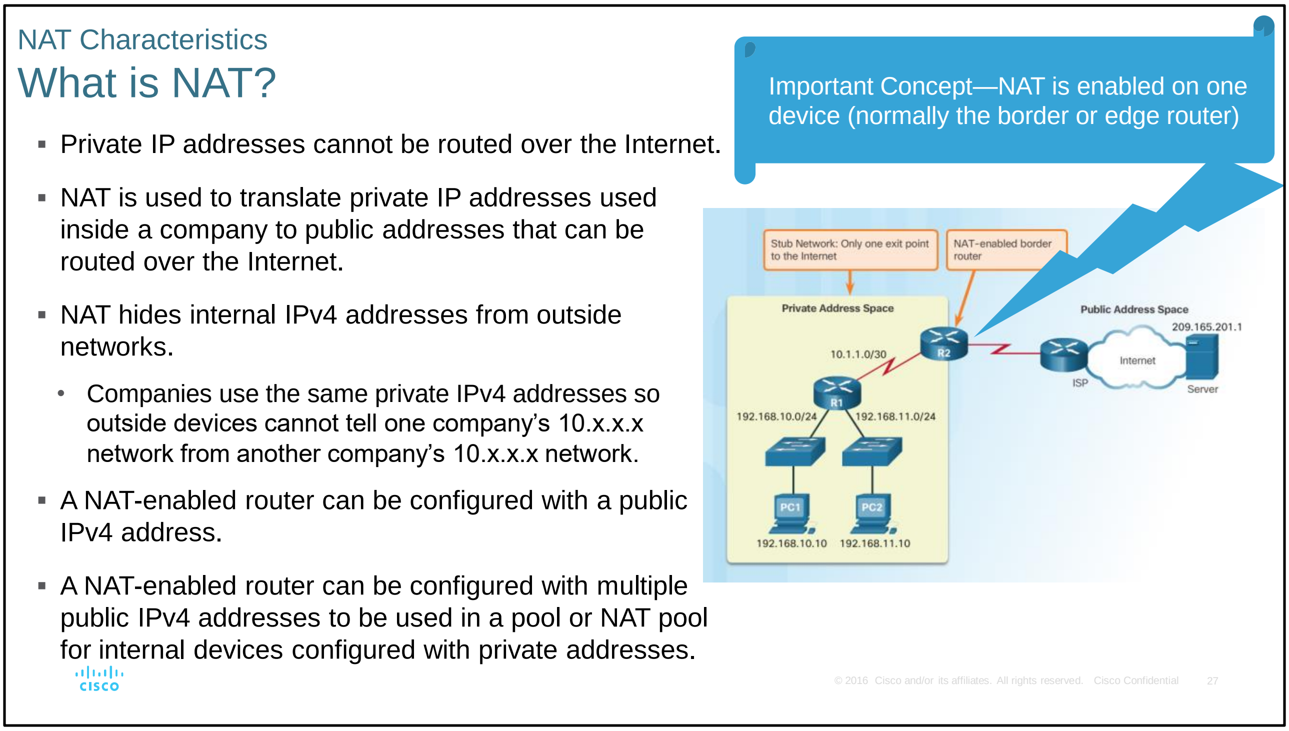
NAT Characteristics

IPv4 Private Address Space (Cont.)

- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses to public addresses that can be routed over the Internet.
- One public IPv4 address can be used for thousands of devices that have private IP addresses.

NAT Router
Internal Network
Private IPv4 Address Space
Internet
Public IPv4 Address Space
NAT Translations

As shown in figure, NAT provides the translation of private addresses to public addresses. This allows a device with a private IPv4 address to access resources outside of their private network, such as those found on the Internet. NAT combined with private IPv4 addresses, has proven to be a useful method of preserving public IPv4 addresses. A single, public IPv4 address can be shared by hundreds, even thousands of devices, each configured with a unique private IPv4 address. Without NAT, the exhaustion of the IPv4 address space would have occurred well before the year 2000. However, NAT has certain limitations, which will be explored later in this chapter. The solution to the exhaustion of IPv4 address space and the limitations of NAT is the eventual transition to IPv6.



NAT Characteristics

What is NAT?

- Private IP addresses cannot be routed over the Internet.
- NAT is used to translate private IP addresses used inside a company to public addresses that can be routed over the Internet.
- NAT hides internal IPv4 addresses from outside networks.
  - Companies use the same private IPv4 addresses so outside devices cannot tell one company’s 10.x.x.x network from another company’s 10.x.x.x network.
- A NAT-enabled router can be configured with a public IPv4 address.
- A NAT-enabled router can be configured with multiple public IPv4 addresses to be used in a pool or NAT pool for internal devices configured with private addresses.

Important Concept—NAT is enabled on one device (normally the border or edge router)

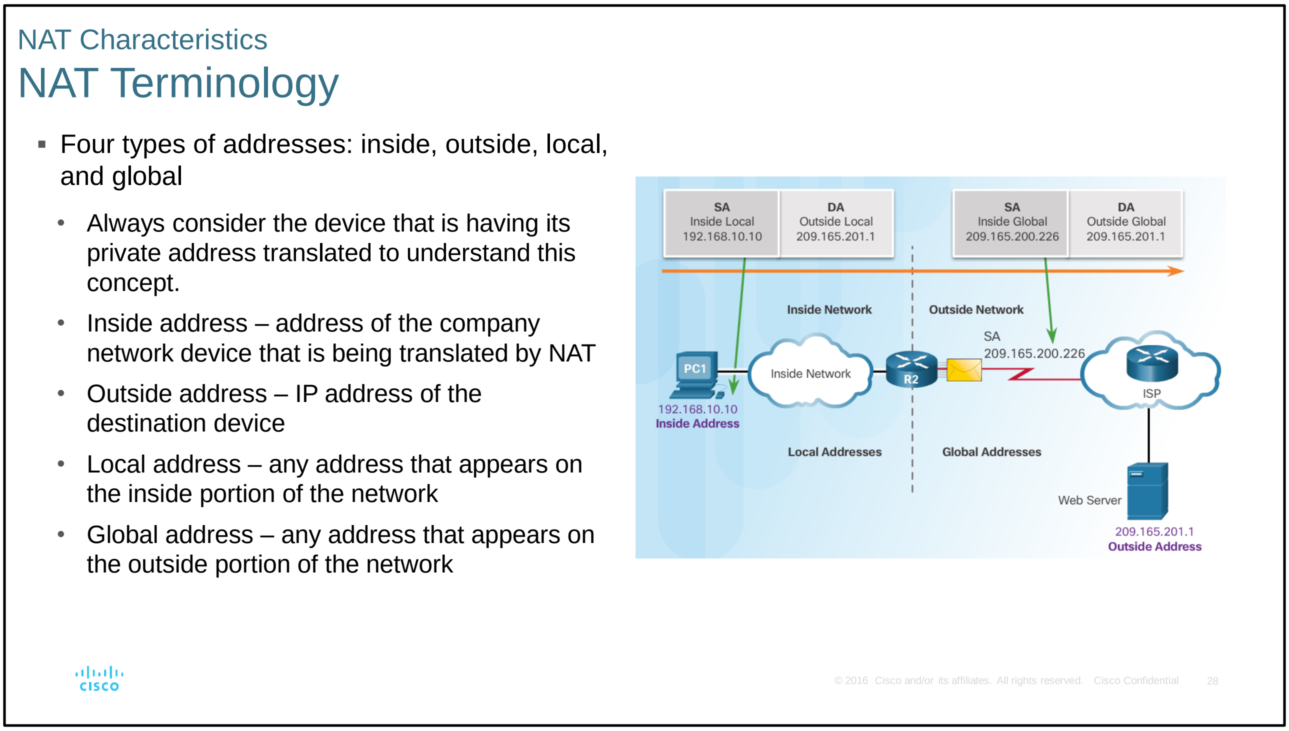
NAT has many uses, but its primary use is to conserve public IPv4 addresses. It does this by allowing networks to use private IPv4 addresses internally and providing translation to a public address only when needed. NAT has an added benefit of adding a degree of privacy and security to a network, because it hides internal IPv4 addresses from outside networks.

NAT-enabled routers can be configured with one or more valid public IPv4 addresses. These public addresses are known as the NAT pool. When an internal device sends traffic out of the network, the NAT-enabled router translates the internal IPv4 address of the device to a public address from the NAT pool. To outside devices, all traffic entering and exiting the network appears to have a public IPv4 address from the provided pool of addresses.

A NAT router typically operates at the border of a stub network. A stub network is a network that has a single connection to its neighboring network, one way in and one way out of the network. In the example in the figure, R2 is a border router. As seen from the ISP, R2 forms a stub network.

When a device inside the stub network wants to communicate with a device outside of its network, the packet is forwarded to the border router. The border router performs the NAT process, translating the internal private address of the device to a public, outside, routable address.

Note: The connection to the ISP may also use a private address or a public address that is shared among customers. For the purposes of this chapter, a public address is shown.



NAT Characteristics

NAT Terminology

- Four types of addresses: inside, outside, local, and global
  - Always consider the device that is having its private address translated to understand this concept.
  - Inside address – address of the company network device that is being translated by NAT
  - Outside address – IP address of the destination device
  - Local address – any address that appears on the inside portion of the network
  - Global address – any address that appears on the outside portion of the network

28

In NAT terminology, the inside network is the set of networks that is subject to translation. The outside network refers to all other networks.

When using NAT, IPv4 addresses have different designations based on whether they are on the private network, or on the public network (Internet), and whether the traffic is incoming or outgoing.

NAT includes four types of addresses:

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

When determining which type of address is used, it is important to remember that NAT terminology is always applied from the perspective of the device with the translated address:

- **Inside address** - The address of the device which is being translated by NAT.
- **Outside address** - The address of the destination device.

NAT also uses the concept of local or global with respect to addresses:

- **Local address** - A local address is any address that appears on the inside portion of the network.
- **Global address** - A global address is any address that appears on the outside portion of the network.

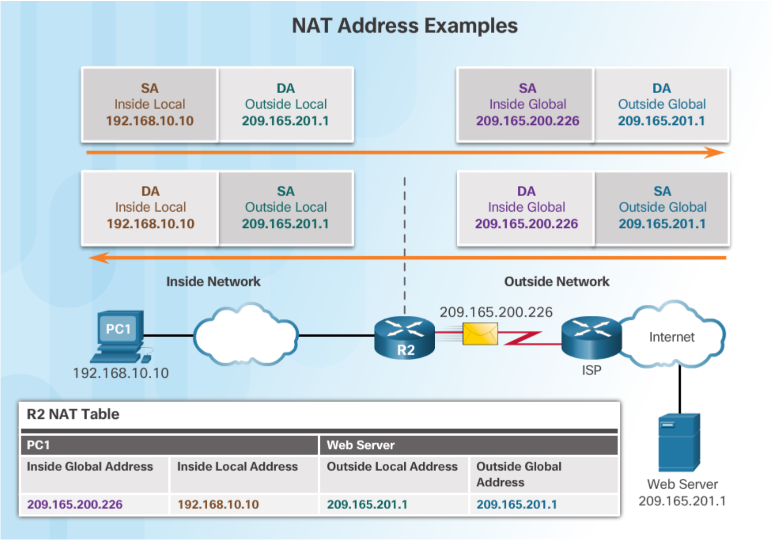
In the figure, PC1 has an inside local address of 192.168.10.10. From the perspective of PC1, the web server has an outside address of 209.165.201.1. When packets are sent from PC1 to the global address of the web server, the inside local address of PC1 is translated to 209.165.200.226 (inside global address). The address of the outside device is not typically translated, because that address is usually a public IPv4 address.

Notice that PC1 has different local and global addresses, whereas the web server has the same public IPv4 address for both. From the perspective of the web server, traffic originating from PC1 appears to have come from 209.165.200.226, the inside global address.

The NAT router, R2 in the figure, is the demarcation point between the inside and outside networks and as between local and global addresses.

NAT Characteristics

NAT Terminology (Cont.)



R2 NAT Table

PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

The terms, inside and outside, are combined with the terms local and global to refer to specific addresses. In the figure, router R2 has been configured to provide NAT. It has a pool of public addresses to assign to inside hosts.

Inside local address - The address of the source as seen from inside the network. In the figure, the IPv4 address 192.168.10.10 is assigned to PC1. This is the inside local address of PC1.

Inside global address - The address of source as seen from the outside network. In the figure, when traffic from PC1 is sent to the web server at 209.165.201.1, R2 translates the inside local address to an inside global address. In this case, R2 changes the IPv4 source address from 192.168.10.10 to 209.165.200.226. In NAT terminology, the inside local address of 192.168.10.10 is translated to the inside global address of 209.165.200.226.

Outside global address - The address of the destination as seen from the outside network. It is a globally routable IPv4 address assigned to a host on the Internet. For example, the web server is reachable at IPv4 address 209.165.201.1. Most often the outside local and outside global addresses are the same.

Outside local address - The address of the destination as seen from the inside network. In this example, PC1 sends traffic to the web server at the IPv4 address 209.165.201.1. While uncommon, this address could be different than the globally routable address of the destination.

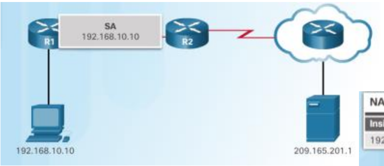
The figure shows how traffic is addressed that is sent from an internal PC to an external web server, across the NAT-enabled router. It also shows how return traffic is initially addressed and translated.

Note: The use of the outside local address is outside the scope of this course.

NAT Characteristics

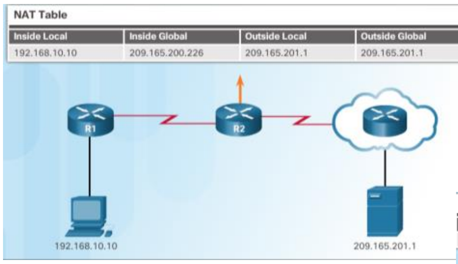
How NAT Works

1. The private (internal) IP address gets translated to a public IP address used to reach the external server.



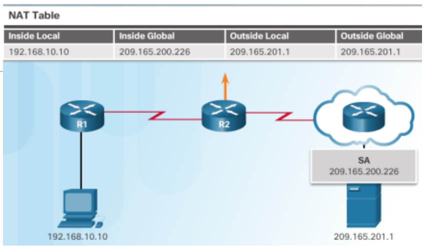
NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

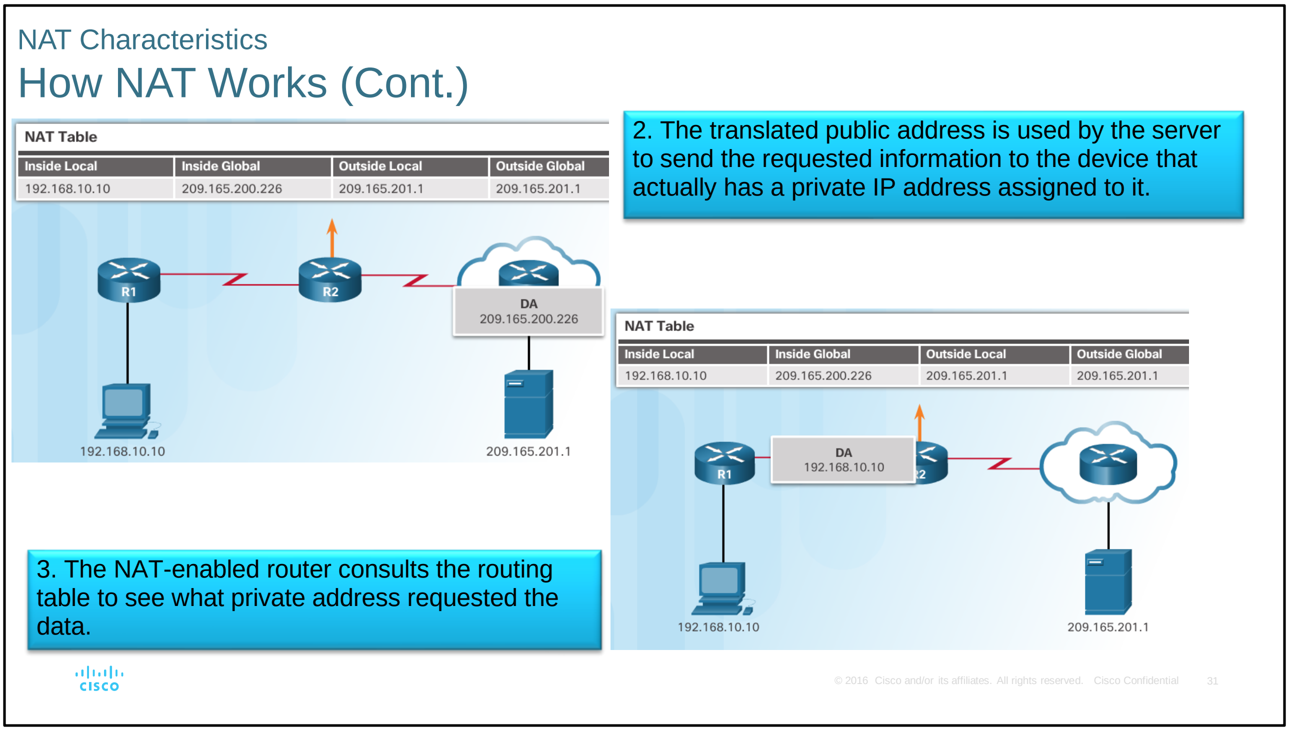


NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



9.1 – NAT Operation
9.1.1 – NAT Characteristics
9.1.1.5 – How NAT Works



NAT Characteristics

How NAT Works (Cont.)

NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

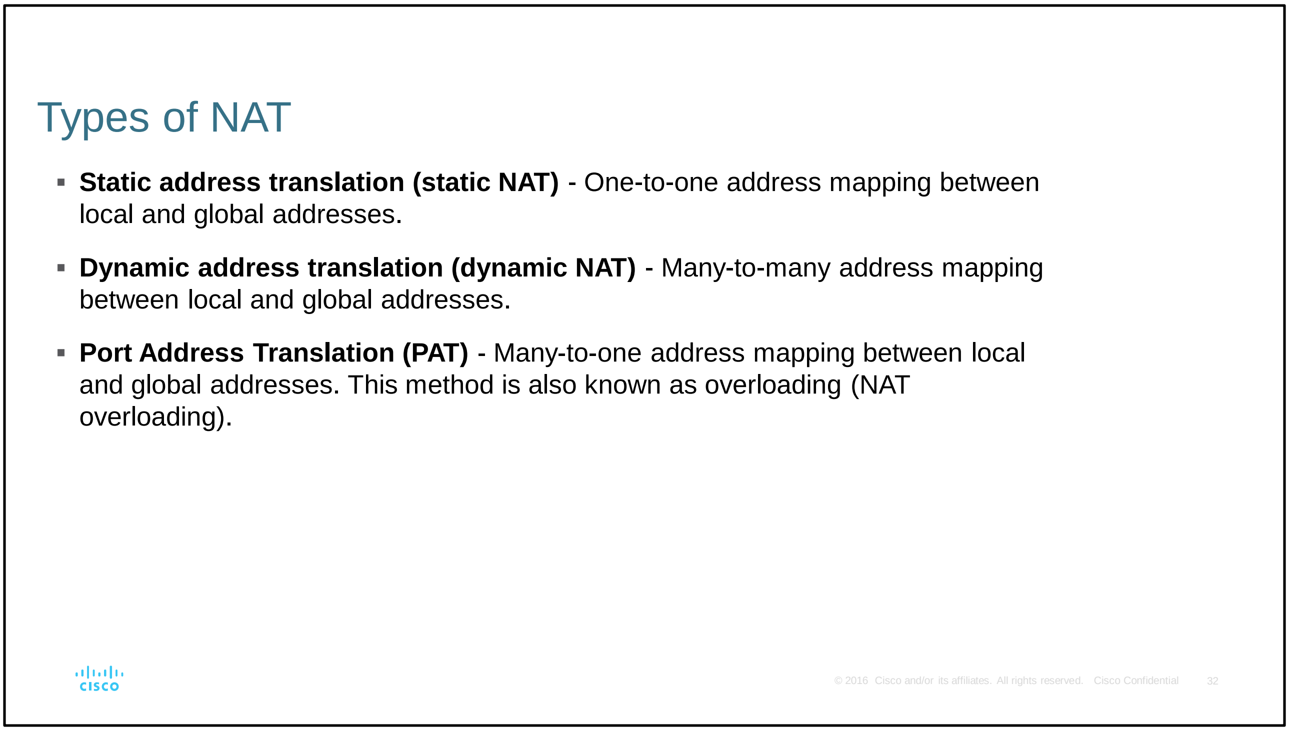
2. The translated public address is used by the server to send the requested information to the device that actually has a private IP address assigned to it.

NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1

3. The NAT-enabled router consults the routing table to see what private address requested the data.

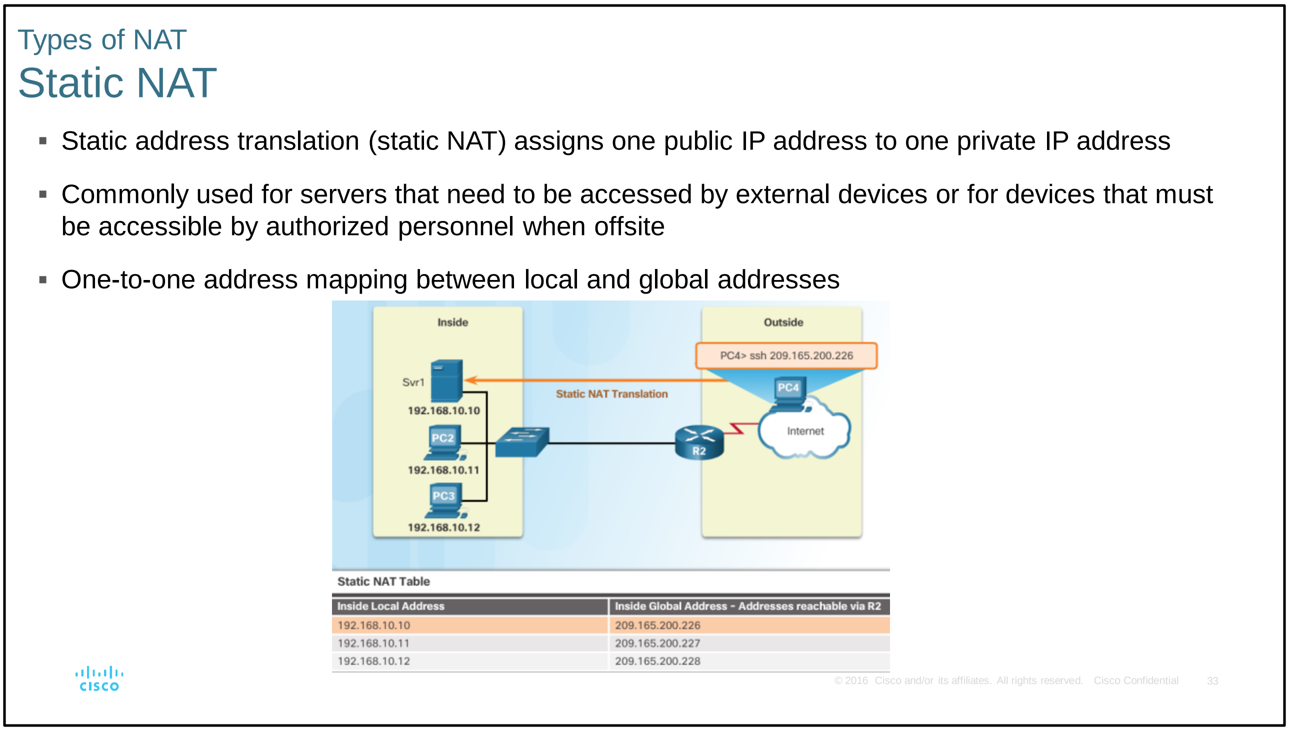
9.1 – NAT Operation
9.1.1 – NAT Characteristics
9.1.1.5 – How NAT Works (Cont.)



Types of NAT

- **Static address translation (static NAT)** - One-to-one address mapping between local and global addresses.
- **Dynamic address translation (dynamic NAT)** - Many-to-many address mapping between local and global addresses.
- **Port Address Translation (PAT)** - Many-to-one address mapping between local and global addresses. This method is also known as overloading (NAT overloading).

There are three types of NAT translation:
Static address translation (static NAT) - One-to-one address mapping between local and global addresses.
Dynamic address translation (dynamic NAT) - Many-to-many address mapping between local and global addresses.
Port Address Translation (PAT) - Many-to-one address mapping between local and global addresses. This method is also known as overloading (NAT overloading).



Types of NAT

Static NAT

- Static address translation (static NAT) assigns one public IP address to one private IP address
- Commonly used for servers that need to be accessed by external devices or for devices that must be accessible by authorized personnel when offsite
- One-to-one address mapping between local and global addresses

Static NAT Table

Inside Local Address	Inside Global Address - Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Static NAT

Static NAT uses a one-to-one mapping of local and global addresses. These mappings are configured by the network administrator and remain constant.

In the figure, R2 is configured with static mappings for the inside local addresses of Svr1, PC2, and PC3. When these devices send traffic to the Internet, their inside local addresses are translated to the configured inside global addresses. To outside networks, these devices have public IPv4 addresses.

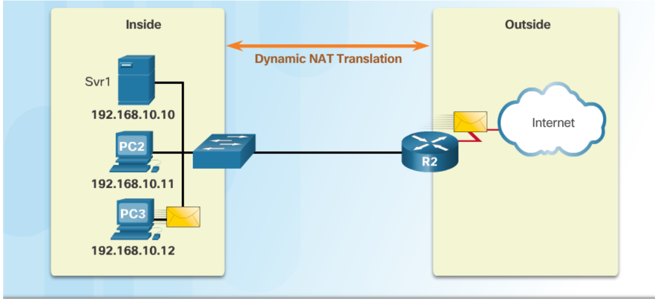
Static NAT is particularly useful for web servers or devices that must have a consistent address that is accessible from the Internet, such as a company web server. It is also useful for devices that must be accessible by authorized personnel when offsite, but not by the general public on the Internet. For example, a network administrator from PC4 can SSH to Svr1’s inside global address (209.165.200.226). R2 translates this inside global address to the inside local address and connects the administrator’s session to Svr1.

Static NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.

Types of NAT

Dynamic NAT

- Dynamic NAT assigns a public IP address from a pool of addresses to each packet that originates from a device that has a private IP address assigned when that packet is destined to a network outside the company.
    - Addresses are assigned on a first-come, first serve basis
    - The number of internal devices that can transmit outside the company is limited to the number of public IP addresses in the pool.

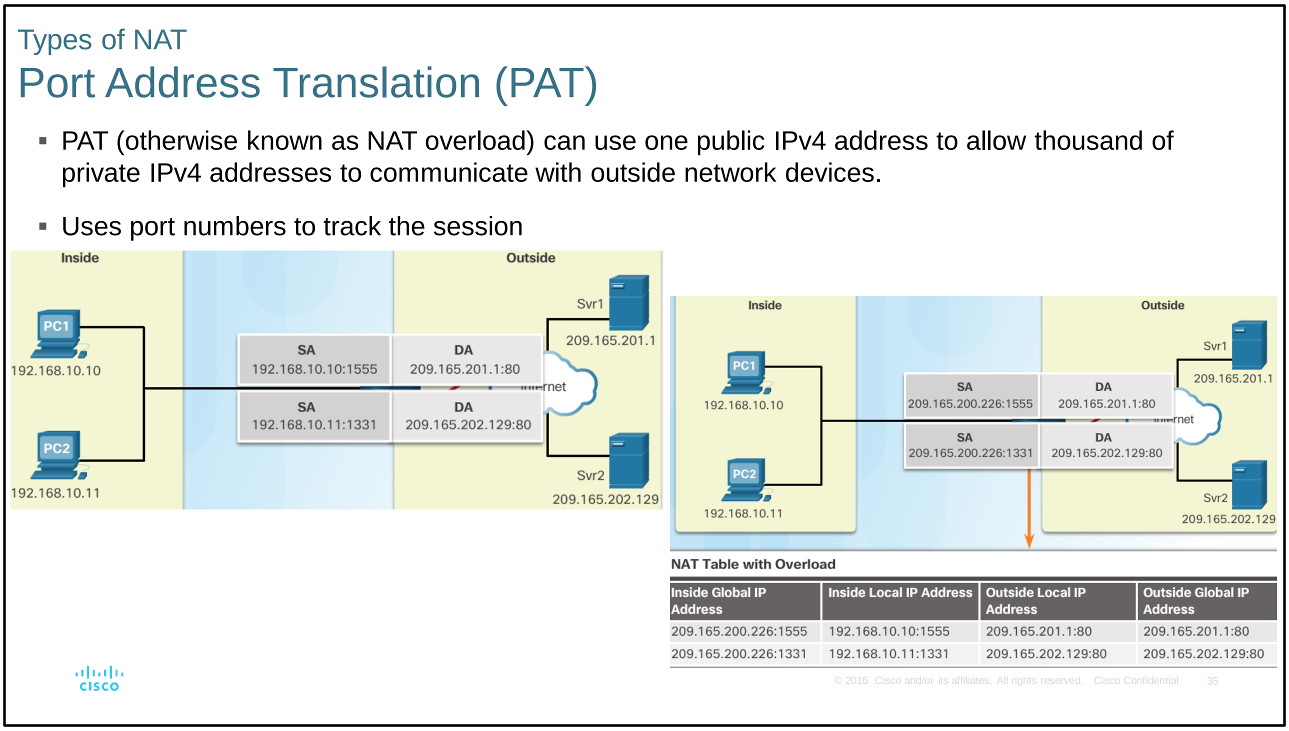


IPv4 NAT Pool

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

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool.

In the figure, PC3 has accessed the Internet using the first available address in the dynamic NAT pool. The other addresses are still available for use. Similar to static NAT, dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions.



Types of NAT

Port Address Translation (PAT)

- PAT (otherwise known as NAT overload) can use one public IPv4 address to allow thousand of private IPv4 addresses to communicate with outside network devices.
- Uses port numbers to track the session

SA	DA
192.168.10.10:1555	209.165.201.1:80
192.168.10.11:1331	209.165.202.129:80

SA	DA
209.165.200.226:1555	209.165.201.1:80
209.165.200.226:1331	209.165.202.129:80

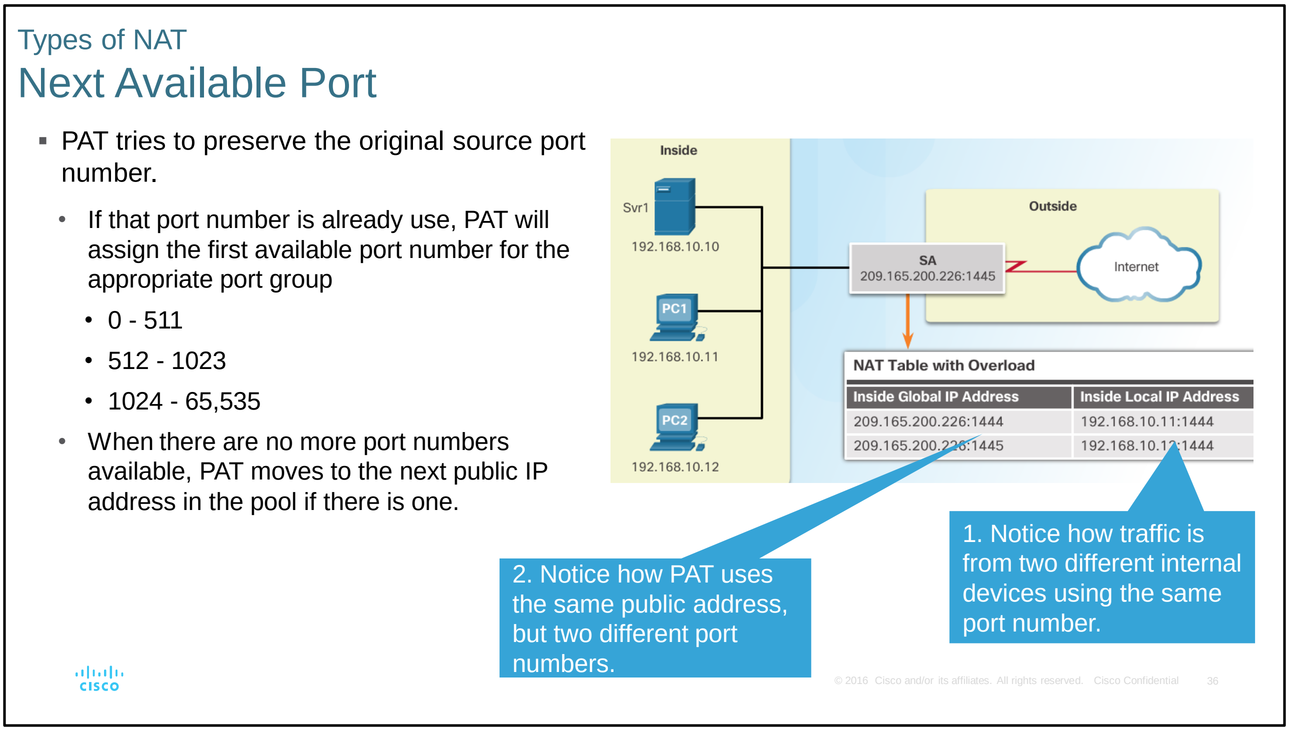
NAT Table with Overload

Inside Global IP Address	Inside Local IP Address	Outside Local IP Address	Outside Global IP Address
209.165.200.226:1555	192.168.10.10:1555	209.165.201.1:80	209.165.201.1:80
209.165.200.226:1331	192.168.10.11:1331	209.165.202.129:80	209.165.202.129:80

Port Address Translation (PAT), also known as NAT overloading, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses. This is what most home routers do. The ISP assigns one address to the router, yet several members of the household can simultaneously access the Internet. This is the most common form of NAT.

With PAT, multiple addresses can be mapped to one or to a few addresses, because each private address is also tracked by a port number. When a device initiates a TCP/IP session, it generates a TCP or UDP source port value to uniquely identify the session. When the NAT router receives a packet from the client, it uses its source port number to uniquely identify the specific NAT translation.
PAT ensures that devices use a different TCP port number for each session with a server on the Internet. When a response comes back from the server, the source port number, which becomes the destination port number on the return trip, determines to which device the router forwards the packets. The PAT process also validates that the incoming packets were requested, thus adding a degree of security to the session.

PAT adds unique source port numbers to the inside global address to distinguish between translations.



Types of NAT

Next Available Port

- PAT tries to preserve the original source port number.
  - If that port number is already use, PAT will assign the first available port number for the appropriate port group
    - 0 - 511
    - 512 - 1023
    - 1024 - 65,535
  - When there are no more port numbers available, PAT moves to the next public IP address in the pool if there is one.

NAT Table with Overload

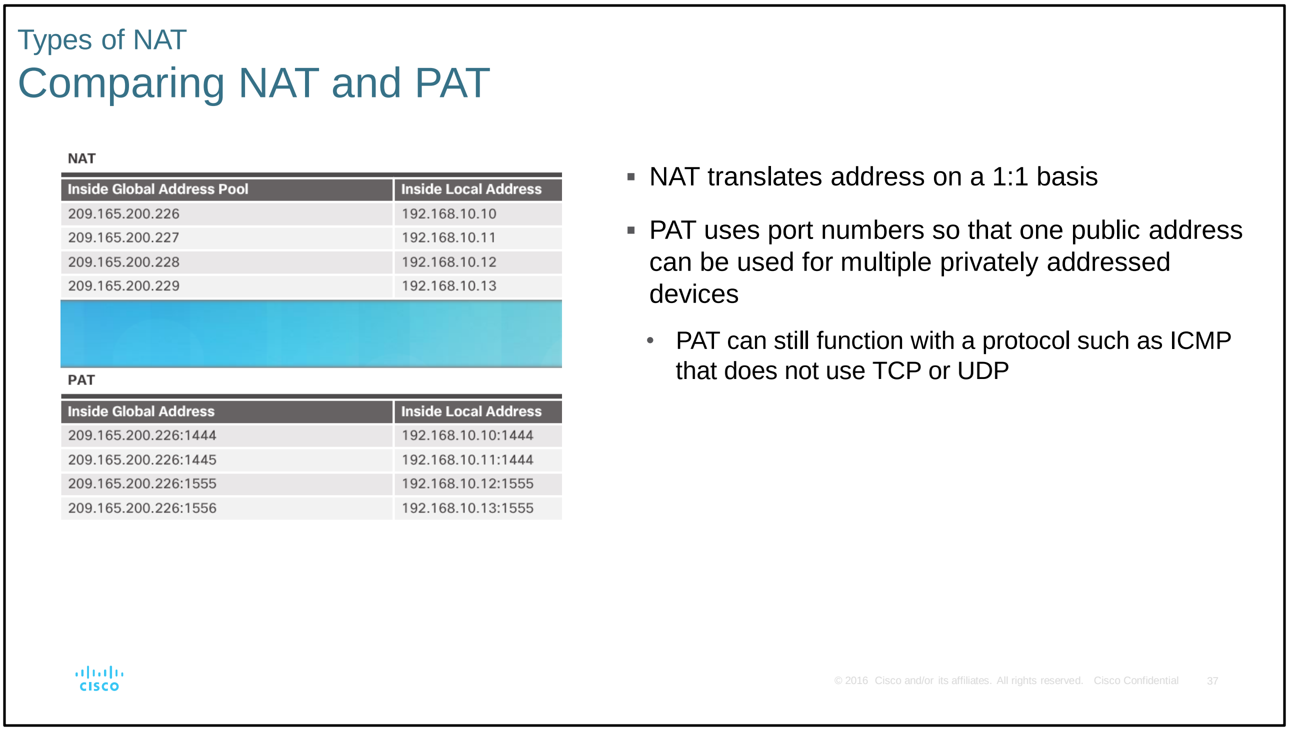
Inside Global IP Address	Inside Local IP Address
209.165.200.226:1444	192.168.10.11:1444
209.165.200.226:1445	192.168.10.12:1444

1. Notice how traffic is from two different internal devices using the same port number.

2. Notice how PAT uses the same public address, but two different port numbers.

PAT attempts to preserve the original source port. However, if the original source port is already used, PAT assigns the first available port number starting from the beginning of the appropriate port group 0–511, 512–1,023, or 1,024–65,535. When there are no more ports available and there is more than one external address in the address pool, PAT moves to the next address to try to allocate the original source port. This process continues until there are no more available ports or external IP addresses.

In figure, the hosts have chosen the same port number 1444. This is acceptable for the inside address, because the hosts have unique private IP addresses. However, at the NAT router, the port numbers must be changed; otherwise, packets from two different hosts would exit R2 with the same source address. In this example, PAT has assigned the next available port (1445) to the second host address.



Types of NAT

Comparing NAT and PAT

NAT

Inside Global Address Pool	Inside Local Address
209.165.200.226	192.168.10.10
209.165.200.227	192.168.10.11
209.165.200.228	192.168.10.12
209.165.200.229	192.168.10.13

PAT

Inside Global Address	Inside Local Address
209.165.200.226:1444	192.168.10.10:1444
209.165.200.226:1445	192.168.10.11:1444
209.165.200.226:1555	192.168.10.12:1555
209.165.200.226:1556	192.168.10.13:1555

- NAT translates address on a 1:1 basis
- PAT uses port numbers so that one public address can be used for multiple privately addressed devices
  - PAT can still function with a protocol such as ICMP that does not use TCP or UDP

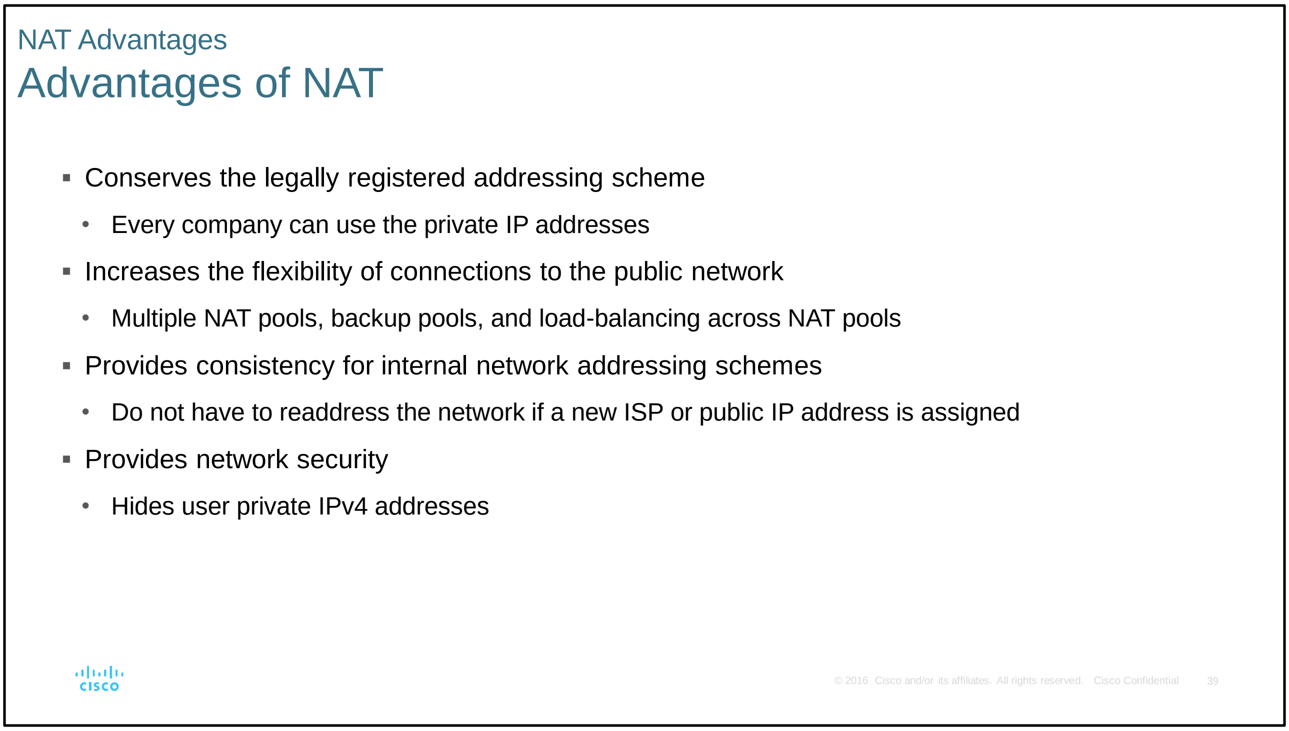
Summarizing the differences between NAT and PAT helps your understanding of each.

- NAT translates IPv4 addresses on a 1:1 basis between private IPv4 addresses and public IPv4 addresses. However, PAT modifies both the address and the port number.
- NAT forwards incoming packets to their inside destination by referring to the incoming source IPv4 address given by the host on the public network. With PAT, there is generally only one or a very few publicly exposed IPv4 addresses. Incoming packets from the public network are routed to their destinations on the private network by referring to a table in the NAT router. This table tracks public and private port pairs. This is called connection tracking.

Packets without a Layer 4 Segment

What about IPv4 packets carrying data other than a TCP or UDP segment? These packets do not contain a Layer 4 port number. PAT translates most common protocols carried by IPv4 that do not use TCP or UDP as a transport layer protocol. The most common of these is ICMPv4. Each of these types of protocols is handled differently by PAT. For example, ICMPv4 query messages, echo requests, and echo replies include a Query ID. ICMPv4 uses the Query ID to identify an echo request with its corresponding echo reply. The Query ID is incremented with each echo request sent. PAT uses the Query ID instead of a Layer 4 port number.

Note: Other ICMPv4 messages do not use the Query ID. These messages and other protocols that do not use TCP or UDP port numbers vary and are beyond the scope of this class.



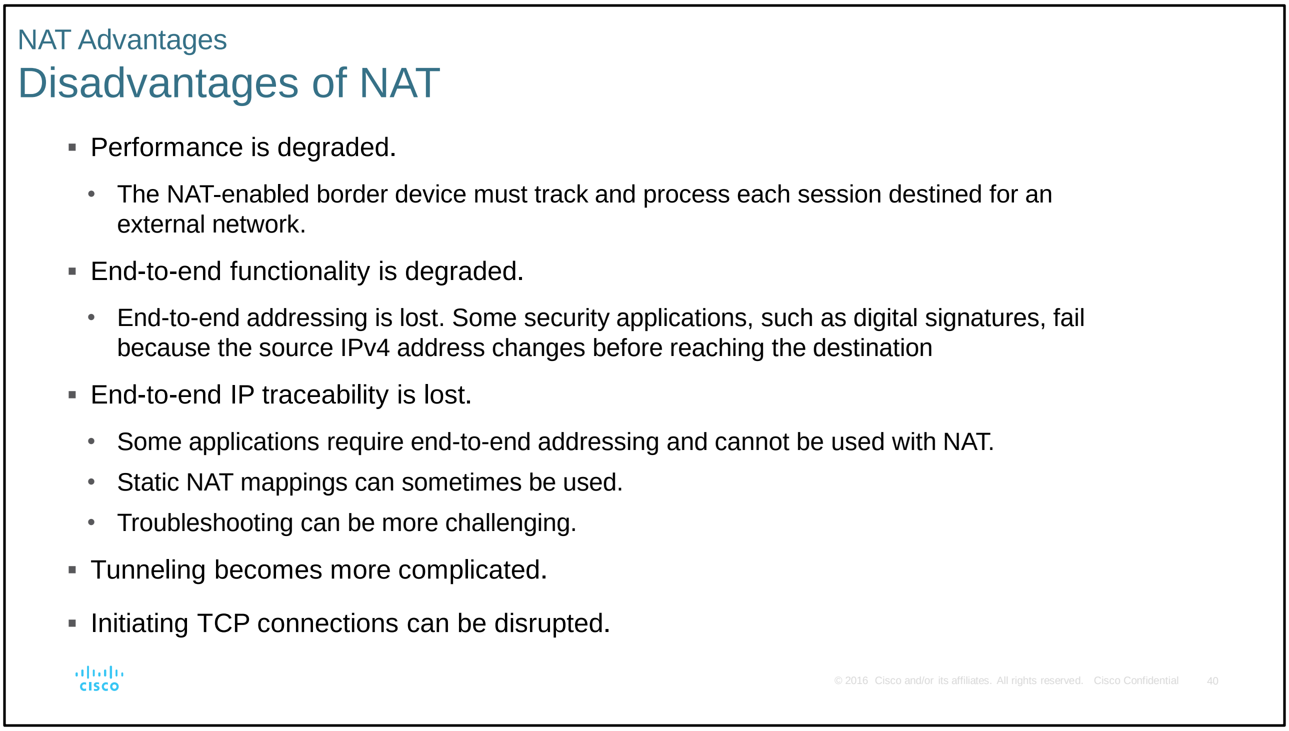
NAT Advantages

Advantages of NAT

- Conserves the legally registered addressing scheme
  - Every company can use the private IP addresses
- Increases the flexibility of connections to the public network
  - Multiple NAT pools, backup pools, and load-balancing across NAT pools
- Provides consistency for internal network addressing schemes
  - Do not have to readdress the network if a new ISP or public IP address is assigned
- Provides network security
  - Hides user private IPv4 addresses

NAT provides many benefits, including:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets. NAT conserves addresses through application port-level multiplexing. With NAT overload, internal hosts can share a single public IPv4 address for all external communications. In this type of configuration, very few external addresses are required to support many internal hosts.
- NAT increases the flexibility of connections to the public network. Multiple pools, backup pools, and load-balancing pools can be implemented to ensure reliable public network connections.
- NAT provides consistency for internal network addressing schemes. On a network not using private IPv4 addresses and NAT, changing the public IPv4 address scheme requires the readdressing of all hosts on the existing network. The costs of readdressing hosts can be significant. NAT allows the existing private IPv4 address scheme to remain while allowing for easy change to a new public addressing scheme. This means an organization could change ISPs and not need to change any of its inside clients.
- NAT provides network security. Because private networks do not advertise their addresses or internal topology, they remain reasonably secure when used in conjunction with NAT to gain controlled external access. However, NAT does not replace firewalls.



NAT Advantages

Disadvantages of NAT

- Performance is degraded.
  - The NAT-enabled border device must track and process each session destined for an external network.
- End-to-end functionality is degraded.
  - End-to-end addressing is lost. Some security applications, such as digital signatures, fail because the source IPv4 address changes before reaching the destination
- End-to-end IP traceability is lost.
  - Some applications require end-to-end addressing and cannot be used with NAT.
  - Static NAT mappings can sometimes be used.
  - Troubleshooting can be more challenging.
- Tunneling becomes more complicated.
- Initiating TCP connections can be disrupted.

NAT does have some drawbacks. The fact that hosts on the Internet appear to communicate directly with the NAT-enabled device, rather than with the actual host inside the private network, creates a number of issues.

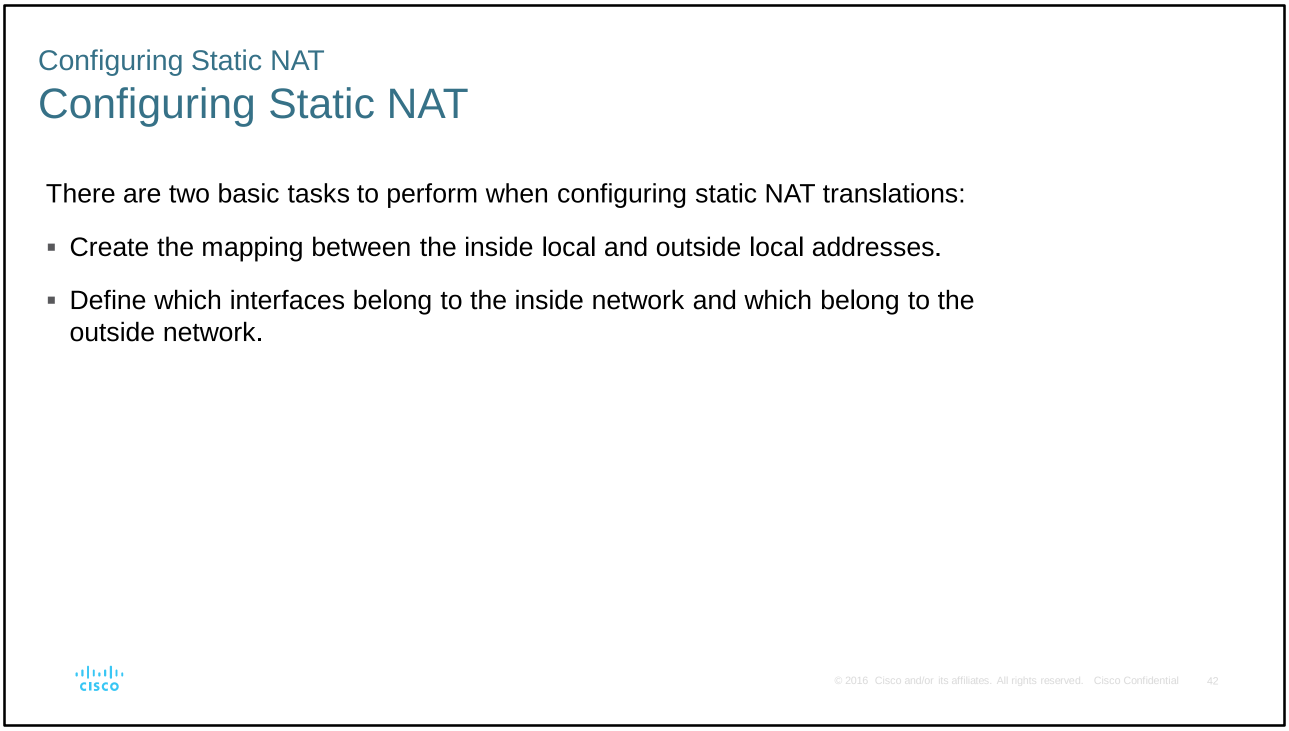
- One disadvantage of using NAT is related to network performance, particularly for real time protocols such as VoIP. NAT increases switching delays because the translation of each IPv4 address within the packet headers takes time. The first packet is process-switched; it always goes through the slower path. The router must look at every packet to decide whether it needs translation. The router must alter the IPv4 header, and possibly alter the TCP or UDP header. The IPv4 header checksum, along with the TCP or UDP checksum must be recalculated each time a translation is made. Remaining packets go through the fast-switched path if a cache entry exists; otherwise, they too are delayed.
- Another disadvantage of using NAT is that end-to-end addressing is lost. Many Internet protocols and applications depend on end-to-end addressing from the source to the destination. Some applications do not work with NAT. For example, some security applications, such as digital signatures, fail because the source IPv4 address changes before reaching the destination. Applications that use physical addresses, instead of a qualified domain name, do not reach destinations that are translated across the NAT router. Sometimes, this problem can be avoided by implementing static NAT mappings.
- End-to-end IPv4 traceability is also lost. It becomes much more difficult to trace packets that undergo numerous packet address changes over multiple NAT hops,

making troubleshooting challenging.

- Using NAT also complicates tunneling protocols, such as IPsec, because NAT modifies values in the headers that interfere with the integrity checks done by IPsec and other tunneling protocols.
- Services that require the initiation of TCP connections from the outside network, or stateless protocols, such as those using UDP, can be disrupted. Unless the NAT router has been configured to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts (passive mode FTP, for example), but fail when both systems are separated from the Internet by NAT.

Configure NAT

9 – NAT for IPv4
9.2 – Configure NAT



Configuring Static NAT

Configuring Static NAT

There are two basic tasks to perform when configuring static NAT translations:

- Create the mapping between the inside local and outside local addresses.
- Define which interfaces belong to the inside network and which belong to the outside network.

Static NAT is a one-to-one mapping between an inside address and an outside address. Static NAT allows external devices to initiate connections to internal devices using the statically assigned public address. For instance, an internal web server may be mapped to a specific inside global address so that it is accessible from outside networks.

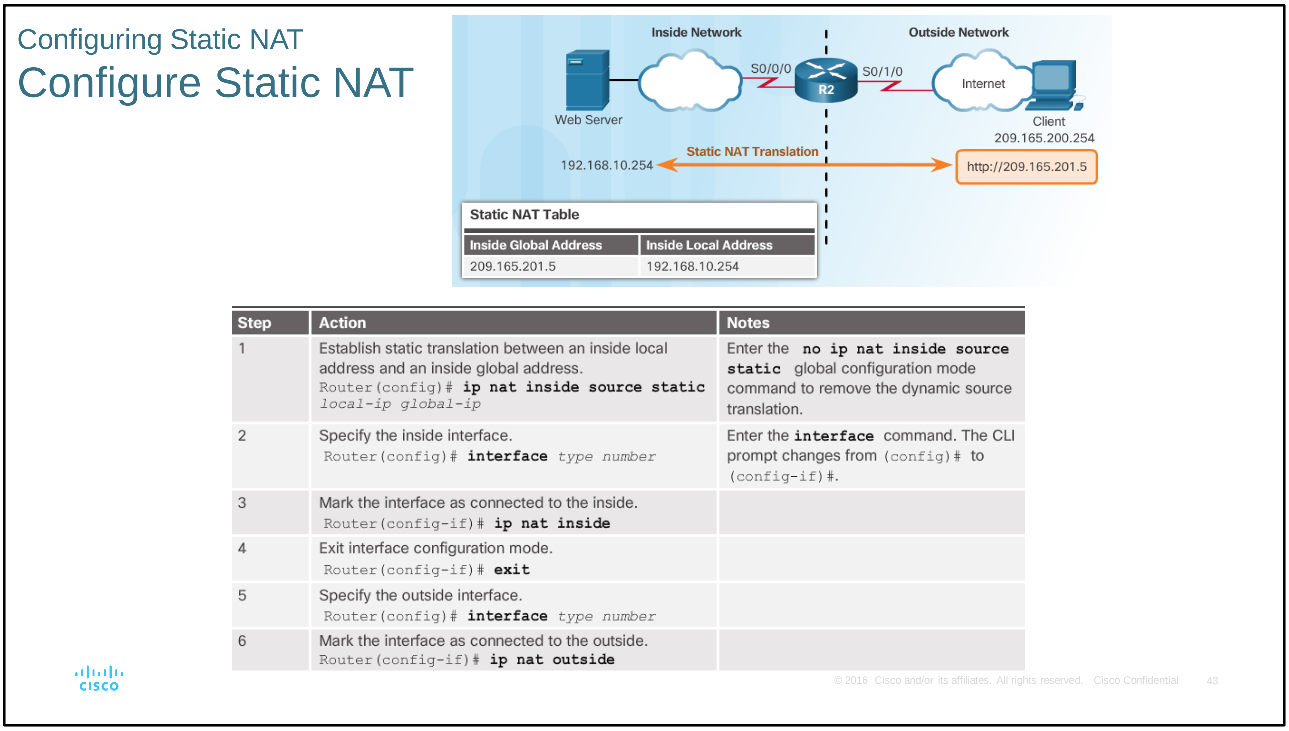
Figure 1 shows an inside network containing a web server with a private IPv4 address. Router R2 is configured with static NAT to allow devices on the outside network (Internet) to access the web server. The client on the outside network accesses the web server using a public IPv4 address. Static NAT translates the public IPv4 address to the private IPv4 address.

There are two basic tasks when configuring static NAT translations.

Step 1. The first task is to create a mapping between the inside local address and the inside global addresses. For example, the 192.168.10.254 inside local address and the 209.165.201.5 inside global address in Figure 1 are configured as a static NAT translation.

Step 2. After the mapping is configured, the interfaces participating in the translation are configured as inside or outside relative to NAT. In the example, the Serial 0/0/0 interface of R2 is an inside interface and Serial 0/1/0 is an outside interface.

Packets arriving on the inside interface of R2 (Serial 0/0/0) from the configured inside local IPv4 address (192.168.10.254) are translated and then forwarded towards the outside network. Packets arriving on the outside interface of R2 (Serial 0/1/0), that are addressed to the configured inside global IPv4 address (209.165.201.5), are translated to the inside local address (192.168.10.254) and then forwarded to the inside network.



Configuring Static NAT

Configure Static NAT

Static NAT Table

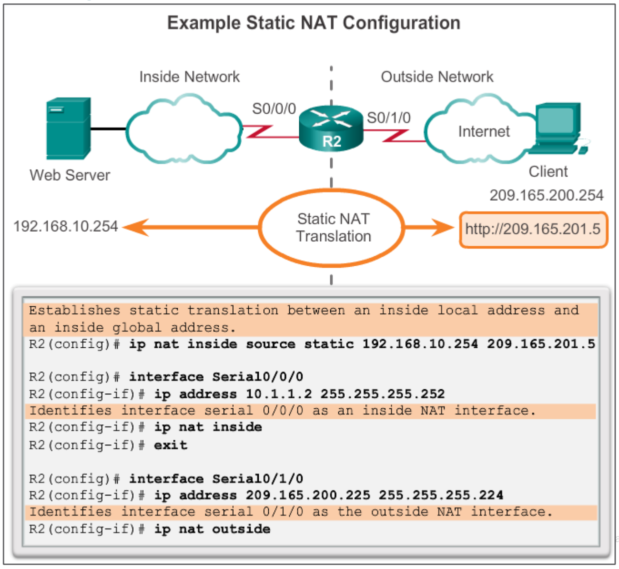
Inside Global Address	Inside Local Address
209.165.201.5	192.168.10.254

Step	Action	Notes
1	Establish static translation between an inside local address and an inside global address. `Router(config)# ip nat inside source static local-ip global-ip`	Enter the `no ip nat inside source static` global configuration mode command to remove the dynamic source translation.
2	Specify the inside interface. `Router(config)# interface type number`	Enter the `interface` command. The CLI prompt changes from `(config)#` to `(config-if)#`.
3	Mark the interface as connected to the inside. `Router(config-if)# ip nat inside`	
4	Exit interface configuration mode. `Router(config-if)# exit`	
5	Specify the outside interface. `Router(config)# interface type number`	
6	Mark the interface as connected to the outside. `Router(config-if)# ip nat outside`	

Figure outlines the commands needed to configure static NAT.

Configuring Static NAT

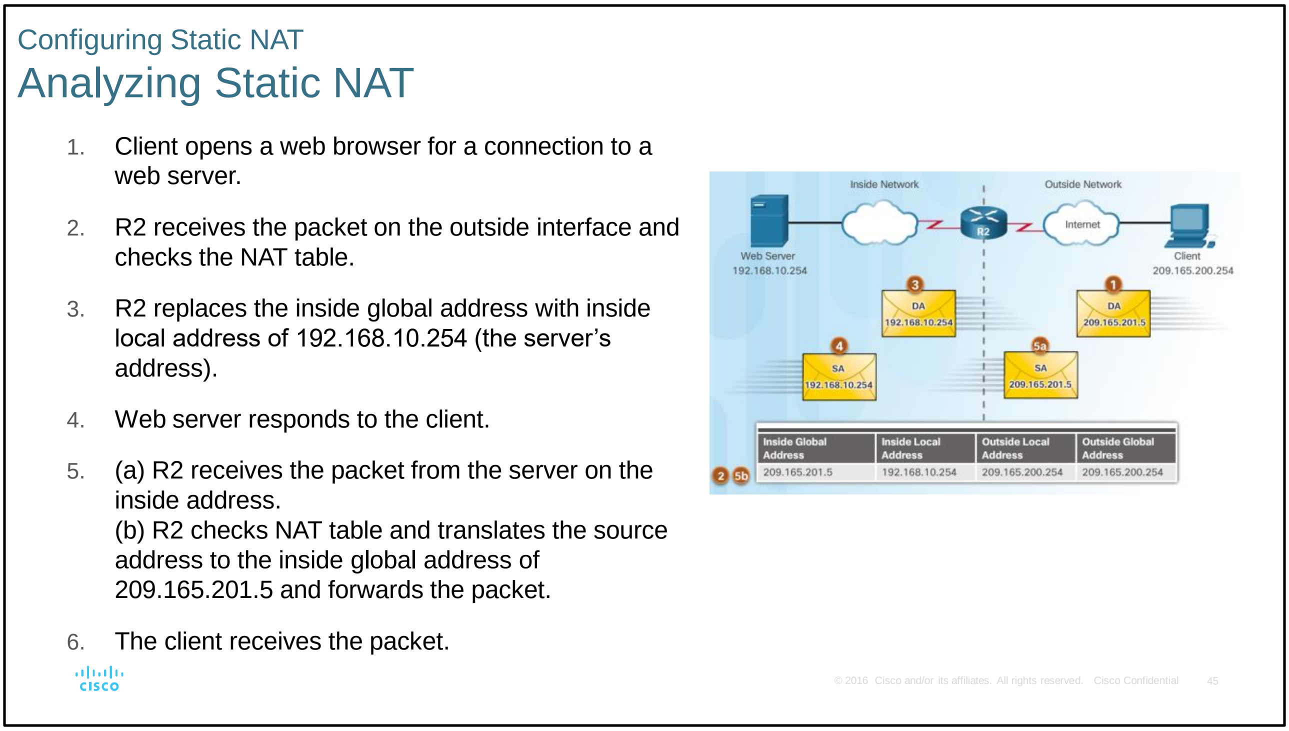
Configuring Static NAT



```
Establishes static translation between an inside local address and
an inside global address.
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5

R2(config)# interface Serial0/0/0
R2(config-if)# ip address 10.1.1.2 255.255.255.252
Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config-if)# ip nat inside
R2(config-if)# exit

R2(config)# interface Serial0/1/0
R2(config-if)# ip address 209.165.200.225 255.255.255.224
Identifies interface serial 0/1/0 as the outside NAT interface.
R2(config-if)# ip nat outside
```

Figure outlines the commands needed to configure static NAT. With the configuration shown, R2 translates packets from the web server with address 192.168.10.254 to public IPv4 address 209.165.201.5. The Internet client directs web requests to the public IPv4 address 209.165.201.5. R2 forwards that traffic to the web server at 192.168.10.254.

Use the Syntax Checker in Figure 4 to configure an additional static NAT entry on R2.



Configuring Static NAT

Analyzing Static NAT

1. Client opens a web browser for a connection to a web server.
2. R2 receives the packet on the outside interface and checks the NAT table.
3. R2 replaces the inside global address with inside local address of 192.168.10.254 (the server's address).
4. Web server responds to the client.
5. (a) R2 receives the packet from the server on the inside address.
   (b) R2 checks NAT table and translates the source address to the inside global address of 209.165.201.5 and forwards the packet.
6. The client receives the packet.

Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.201.5	192.168.10.254	209.165.200.254	209.165.200.254

45

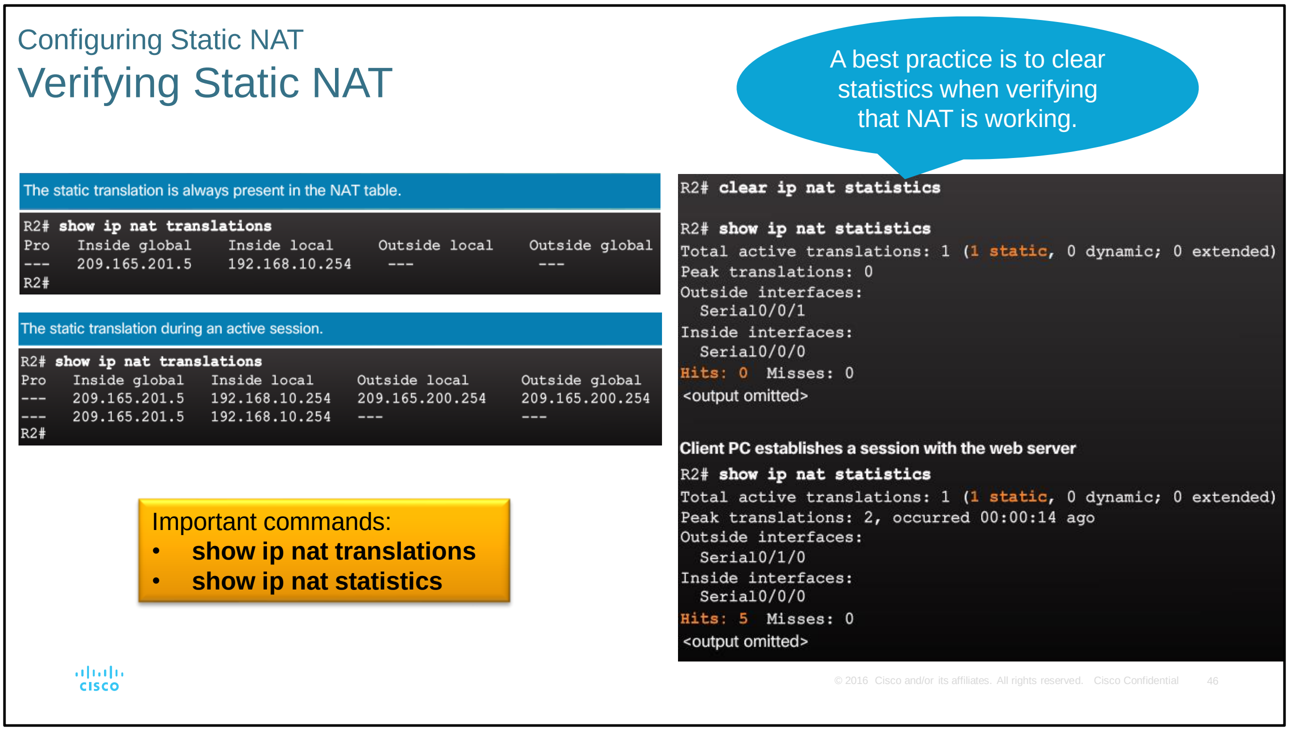
Using the previous configuration, the figure illustrates the static NAT translation process between the client and the web server. Usually static translations are used when clients on the outside network (Internet) need to reach servers on the inside (internal) network.

1. The client wants to open a connection to the web server. The client sends a packet to the web server using the public IPv4 destination address of 209.165.201.5. This is the inside global address of the web server.
2. The first packet that R2 receives from the client on its NAT outside interface causes R2 to check its NAT table. The destination IPv4 address is located in the NAT table and is translated.
3. R2 replaces the inside global address of 209.165.201.5 with the inside local address of 192.168.10.254. R2 then forwards the packet towards the web server.
4. The web server receives the packet and responds to the client using the inside local address, 192.168.10.254.

5a. R2 receives the packet from the web server on its NAT inside interface with source address of the inside local address of the web server, 192.168.10.254.

5b. R2 checks the NAT table for a translation for the inside local address. The address is found in the NAT table. R2 translates the source address to the inside global address of 209.165.201.5 and forwards the packet out of its serial 0/1/0 interface toward the client.

6. The client receives the packet and continues the conversation. The NAT router performs Steps 2 to 5b for each packet. (Step 6 is not shown in the figure.)



Configuring Static NAT

Verifying Static NAT

A best practice is to clear statistics when verifying that NAT is working.

The static translation is always present in the NAT table.

```
R2# show ip nat translations
Pro  Inside global    Inside local     Outside local    Outside global
---  209.165.201.5    192.168.10.254   ---              ---
R2#
```

The static translation during an active session.

```
R2# show ip nat translations
Pro  Inside global   Inside local    Outside local    Outside global
---  209.165.201.5   192.168.10.254  209.165.200.254  209.165.200.254
---  209.165.201.5   192.168.10.254  ---              ---
R2#
```

Important commands:

- **show ip nat translations**
- **show ip nat statistics**

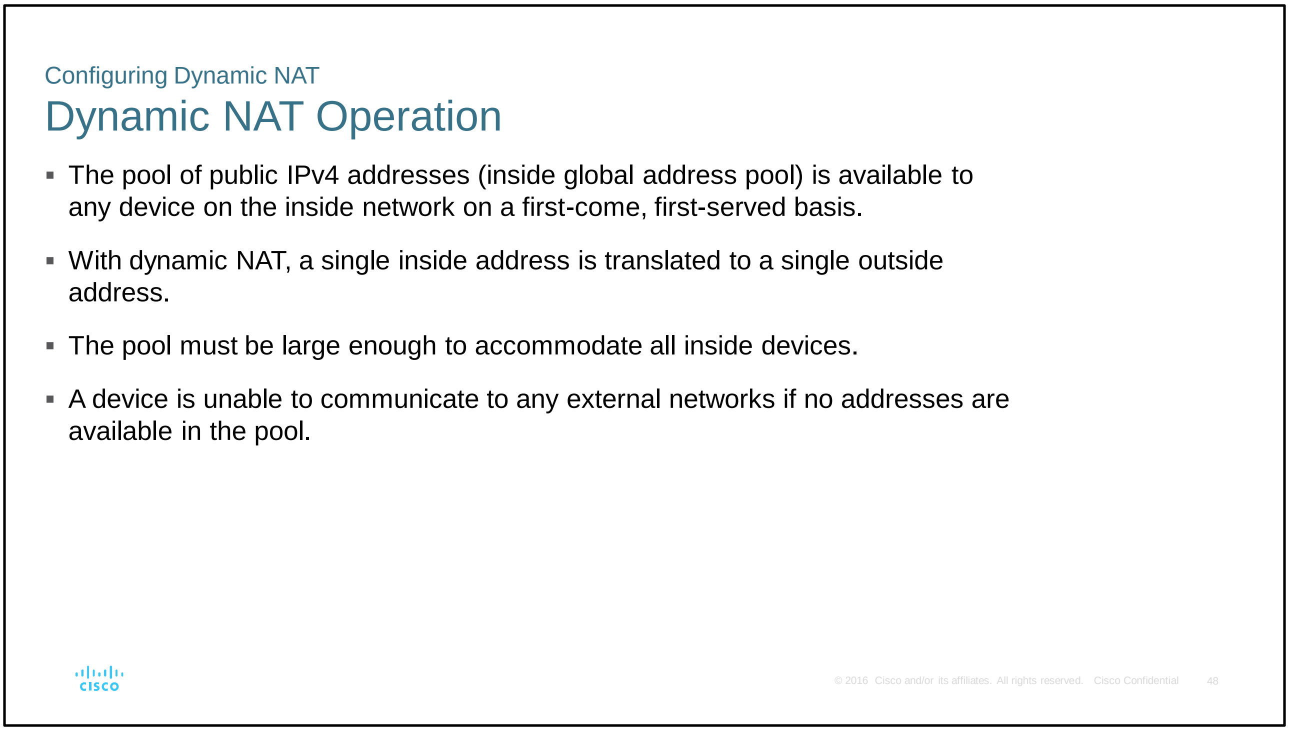
```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 0  Misses: 0
<output omitted>
```

Client PC establishes a session with the web server

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Peak translations: 2, occurred 00:00:14 ago
Outside interfaces:
  Serial0/1/0
Inside interfaces:
  Serial0/0/0
Hits: 5  Misses: 0
<output omitted>
```

A useful command to verify NAT operation is the **show ip nat translations** command. This command shows active NAT translations. Static translations, unlike dynamic translations, are always in the NAT table. Figure shows the output from this command using the previous configuration example. Because the example is a static NAT configuration, the translation is always present in the NAT table regardless of any active communications. If the command is issued during an active session, the output also indicates the address of the outside device as shown in figure.
Another useful command is the **show ip nat statistics** command. This command displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and the number of addresses that have been allocated.

To verify that the NAT translation is working, it is best to clear statistics from any past translations using the **clear ip nat statistics** command before testing.
Prior to any communications with the web server, the **show ip nat statistics** command shows no current hits. After the client establishes a session with the web server, the **show ip nat statistics** command has been incremented to five hits. This verifies that the static NAT translation is taking place on R2.



Configuring Dynamic NAT

Dynamic NAT Operation

- The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come, first-served basis.
- With dynamic NAT, a single inside address is translated to a single outside address.
- The pool must be large enough to accommodate all inside devices.
- A device is unable to communicate to any external networks if no addresses are available in the pool.

While static NAT provides a permanent mapping between an inside local address and an inside global address, dynamic NAT allows the automatic mapping of inside local addresses to inside global addresses. These inside global addresses are typically public IPv4 addresses. Dynamic NAT uses a group, or pool of public IPv4 addresses for translation.
Dynamic NAT, like static NAT, requires the configuration of the inside and outside interfaces participating in NAT. However, where static NAT creates a permanent mapping to a single address, dynamic NAT uses a pool of addresses.

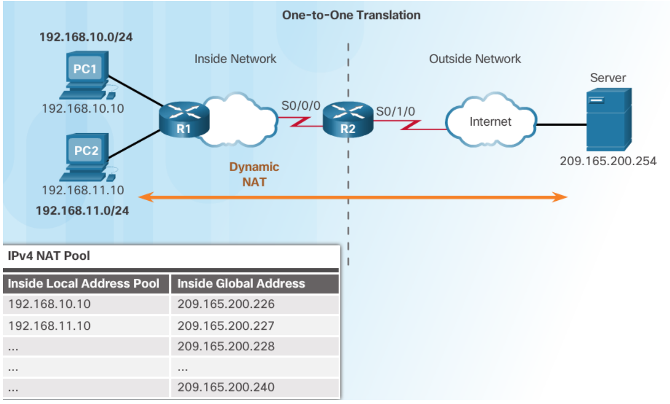
The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come first-served basis. With dynamic NAT, a single inside address is translated to a single outside address. With this type of translation there must be enough addresses in the pool to accommodate all the inside devices needing access to the outside network at the same time. If all of the addresses in the pool have been used, a device must wait for an available address before it can access the outside network.

Note: Translating between public and private IPv4 addresses is by far the most common use of NAT. However, NAT translations can occur between any pair of addresses.

Configure Dynamic NAT

Dynamic NAT Operation

- Remember that dynamic NAT uses a pool of public IPv4 addresses.
- Use the same concepts of inside and outside NAT interfaces as static NAT.



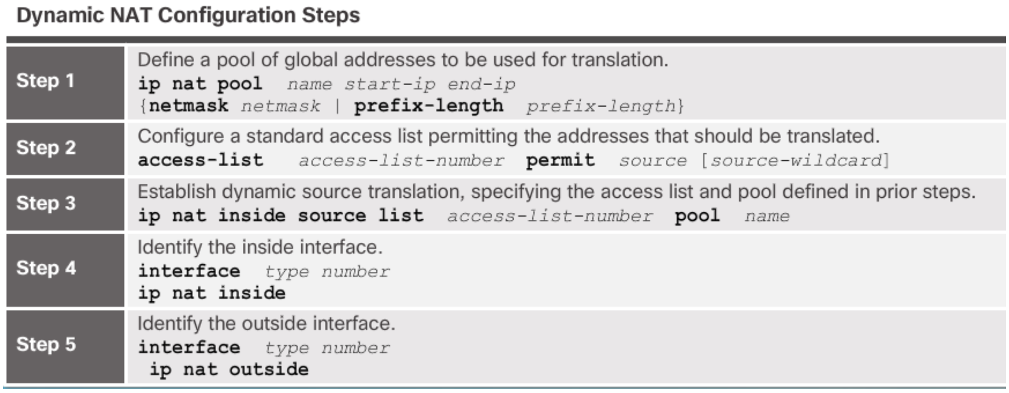
IPv4 NAT Pool

Inside Local Address Pool	Inside Global Address
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227
...	209.165.200.228
...	...
...	209.165.200.240

The example topology shown in the figure has an inside network using addresses from the RFC 1918 private address space. Attached to router R1 are two LANs, 192.168.10.0/24 and 192.168.11.0/24. Router R2, the border router, is configured for dynamic NAT using a pool of public IPv4 addresses 209.165.200.226 through 209.165.200.240.

Configure Dynamic NAT

Configuring Dynamic NAT



Dynamic NAT Configuration Steps

Step 1	Define a pool of global addresses to be used for translation.
	`ip nat pool` *`name start-ip end-ip`*
	`{`**`netmask`** *`netmask`* `|` **`prefix-length`** *`prefix-length`*`}`

Step 2	Configure a standard access list permitting the addresses that should be translated. **`access-list`** *`access-list-number`* **`permit`** *`source`* `[`*`source-wildcard`*`]`
Step 3	Establish dynamic source translation, specifying the access list and pool defined in prior steps. **`ip nat inside source list`** *`access-list-number`* **`pool`** *`name`*

Step 4	Identify the inside interface.
	`interface` *`type number`*
	`ip nat inside`

Step 5	Identify the outside interface.
	`interface` *`type number`*
	`ip nat outside`

Figure shows the steps and the commands used to configure dynamic NAT.

Step 1. Define the pool of addresses that will be used for translation using the **ip nat pool** command. This pool of addresses is typically a group of public addresses. The addresses are defined by indicating the starting IP address and the ending IP address of the pool. The **netmask** or **prefix-length** keyword indicates which address bits belong to the network and which bits belong to the host for the range of addresses.

Step 2. Configure a standard ACL to identify (permit) only those addresses that are to be translated. An ACL that is too permissive can lead to unpredictable results. Remember there is an implicit **deny all** statement at the end of each ACL.

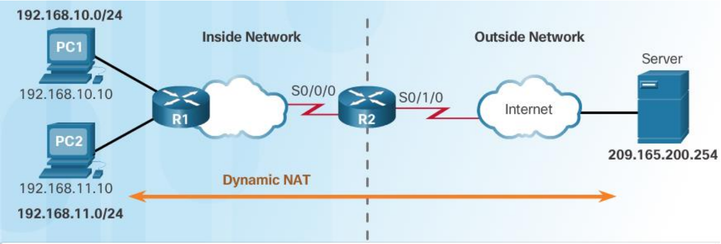
Step 3. Bind the ACL to the pool. The **ip nat inside source list** *access-list-number* **number pool** *pool name* command is used to bind the ACL to the pool. This configuration is used by the router to identify which devices (**list**) receive which addresses (**pool**).

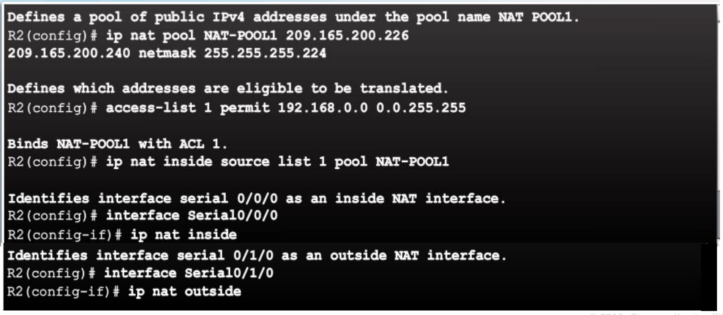
Step 4. Identify which interfaces are inside, in relation to NAT; that is, any interface that connects to the inside network.

Step 5. Identify which interfaces are outside, in relation to NAT; that is, any interface that connects to the outside network.

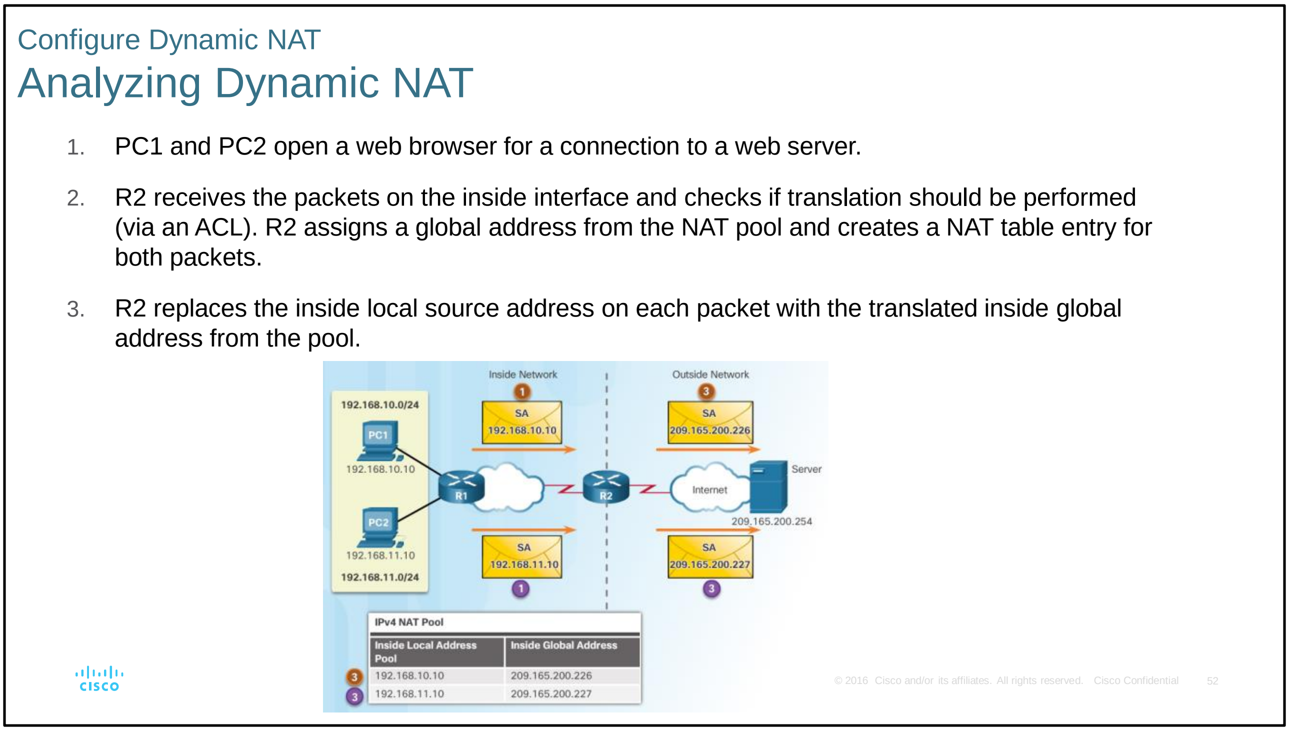
Configure Dynamic NAT

Configuring Dynamic NAT (Cont.)





```
Defines a pool of public IPv4 addresses under the pool name NAT POOL1.
R2(config)# ip nat pool NAT-POOL1 209.165.200.226
209.165.200.240 netmask 255.255.255.224

Defines which addresses are eligible to be translated.
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255

Binds NAT-POOL1 with ACL 1.
R2(config)# ip nat inside source list 1 pool NAT-POOL1

Identifies interface serial 0/0/0 as an inside NAT interface.
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
Identifies interface serial 0/1/0 as an outside NAT interface.
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```



Configure Dynamic NAT

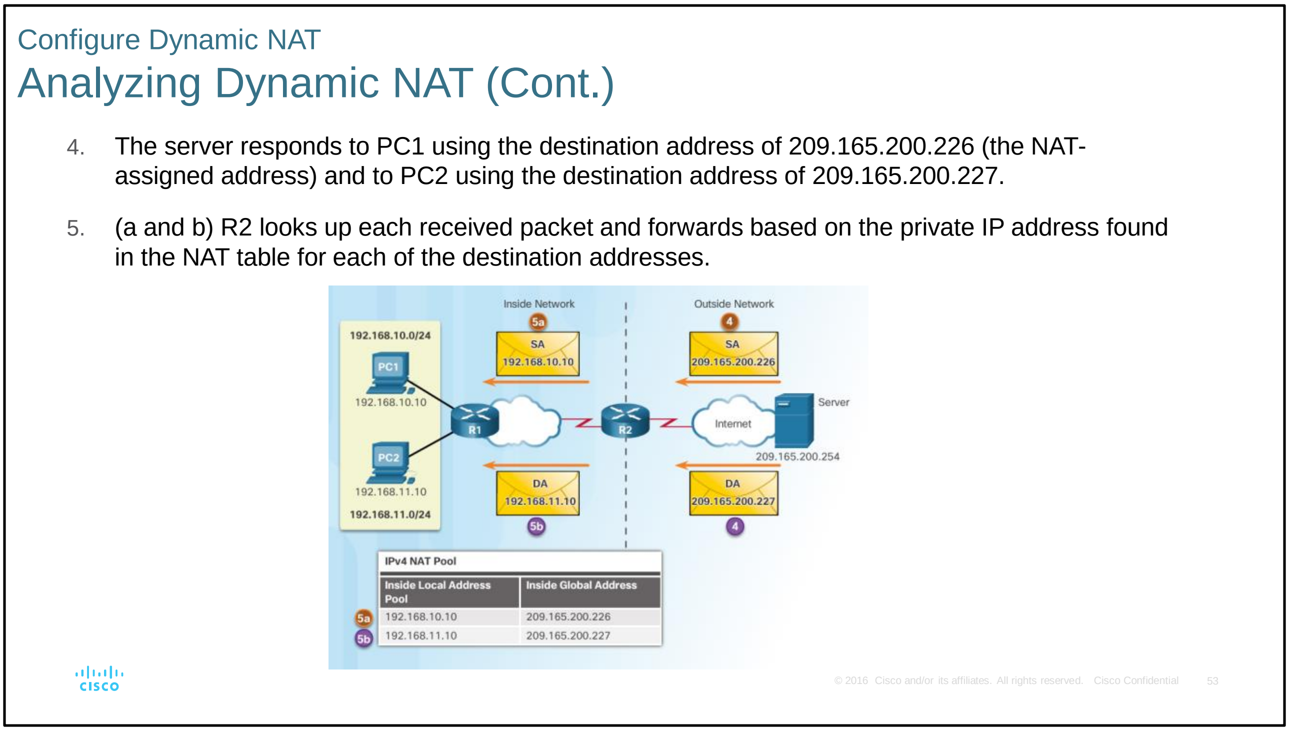
Analyzing Dynamic NAT

1. PC1 and PC2 open a web browser for a connection to a web server.
2. R2 receives the packets on the inside interface and checks if translation should be performed (via an ACL). R2 assigns a global address from the NAT pool and creates a NAT table entry for both packets.
3. R2 replaces the inside local source address on each packet with the translated inside global address from the pool.

IPv4 NAT Pool

	Inside Local Address Pool	Inside Global Address
3	192.168.10.10	209.165.200.226
3	192.168.11.10	209.165.200.227

Using the previous configuration, the figures illustrate the dynamic NAT translation process between two clients and the web server:
In Figure, the traffic flow from inside to outside is shown:
1. The hosts with the source IPv4 addresses (192.168.10.10 (PC1) and 192.168.11.10 (PC2)) send packets requesting a connection to the server at the public IPv4 address (209.165.200.254).
2. R2 receives the first packet from host 192.168.10.10. Because this packet was received on an interface configured as an inside NAT interface, R2 checks the NAT configuration to determine if this packet should be translated. The ACL permits this packet, so R2 will translate the packet. R2 checks its NAT table. Because there is no translation entry for this IP address, R2 determines that the source address 192.168.10.10 must be translated dynamically. R2 selects an available global address from the dynamic address pool and creates a translation entry, 209.165.200.226. The original source IPv4 address (192.168.10.10) is the inside local address and the translated address is the inside global address (209.165.200.226) in the NAT table. For the second host, 192.168.11.10, R2 repeats the procedure, selects the next available global address from the dynamic address pool, and creates a second translation entry, 209.165.200.227.
3. R2 replaces the inside local source address of PC1, 192.168.10.10, with the translated inside global address of 209.165.200.226 and forwards the packet. The same process occurs for the packet from PC2 using the translated address for PC2 (209.165.200.227).



Configure Dynamic NAT

Analyzing Dynamic NAT (Cont.)

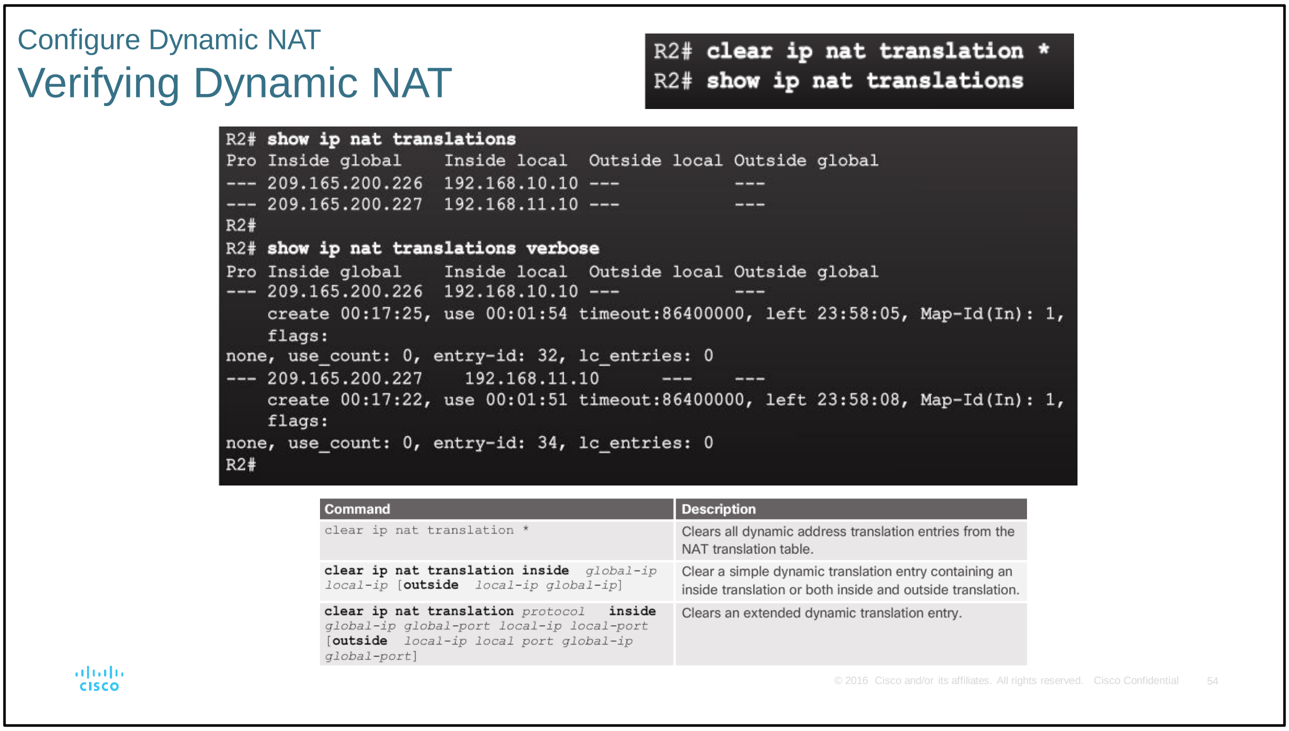
4. The server responds to PC1 using the destination address of 209.165.200.226 (the NAT-assigned address) and to PC2 using the destination address of 209.165.200.227.

5. (a and b) R2 looks up each received packet and forwards based on the private IP address found in the NAT table for each of the destination addresses.

IPv4 NAT Pool

	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

In figure the traffic flow from outside to inside is shown:
4. The server receives the packet from PC1 and responds using the IPv4 destination address of 209.165.200.226. When the server receives the second packet, it responds to PC2 using the IPv4 destination address of 209.165.200.227.
5a. When R2 receives the packet with the destination IPv4 address of 209.165.200.226; it performs a NAT table lookup. Using the mapping from the table, R2 translates the address back to the inside local address (192.168.10.10) and forwards the packet toward PC1.
5b. When R2 receives the packet with the destination IPv4 address of 209.165.200.227; it performs a NAT table lookup. Using the mapping from the table, R2 translates the address back to the inside local address (192.168.11.10) and forwards the packet toward PC2.
6. PC1 at 192.168.10.10 and PC2 at 192.168.11.10 receive the packets and continue the conversation. The router performs Steps 2 to 5 for each packet. (Step 6 is not shown in the figures.)



Configure Dynamic NAT

Verifying Dynamic NAT

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

```
R2# show ip nat translations
Pro Inside global     Inside local   Outside local Outside global
--- 209.165.200.226  192.168.10.10 ---           ---
--- 209.165.200.227  192.168.11.10 ---           ---
R2#
R2# show ip nat translations verbose
Pro Inside global     Inside local   Outside local Outside global
--- 209.165.200.226  192.168.10.10 ---           ---
    create 00:17:25, use 00:01:54 timeout:86400000, left 23:58:05, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 32, lc_entries: 0
--- 209.165.200.227    192.168.11.10      ---    ---
    create 00:17:22, use 00:01:51 timeout:86400000, left 23:58:08, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 34, lc_entries: 0
R2#
```

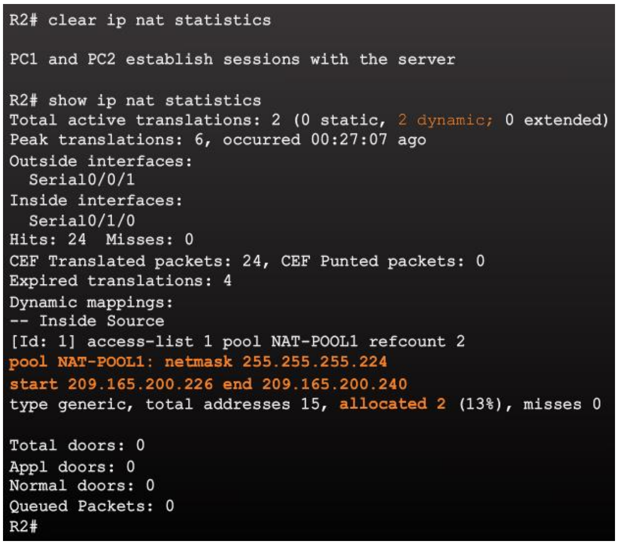
Command	Description
`clear ip nat translation *`	Clears all dynamic address translation entries from the NAT translation table.
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Clear a simple dynamic translation entry containing an inside translation or both inside and outside translation.
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local port global-ip global-port*]	Clears an extended dynamic translation entry.

The output of the **show ip nat translations** command shown in figure displays the details of the two previous NAT assignments. The command displays all static translations that have been configured and any dynamic translations that have been created by traffic.

Adding the **verbose** keyword displays additional information about each translation, including how long ago the entry was created and used.

Configure Dynamic NAT

Verifying Dynamic NAT (Cont.)

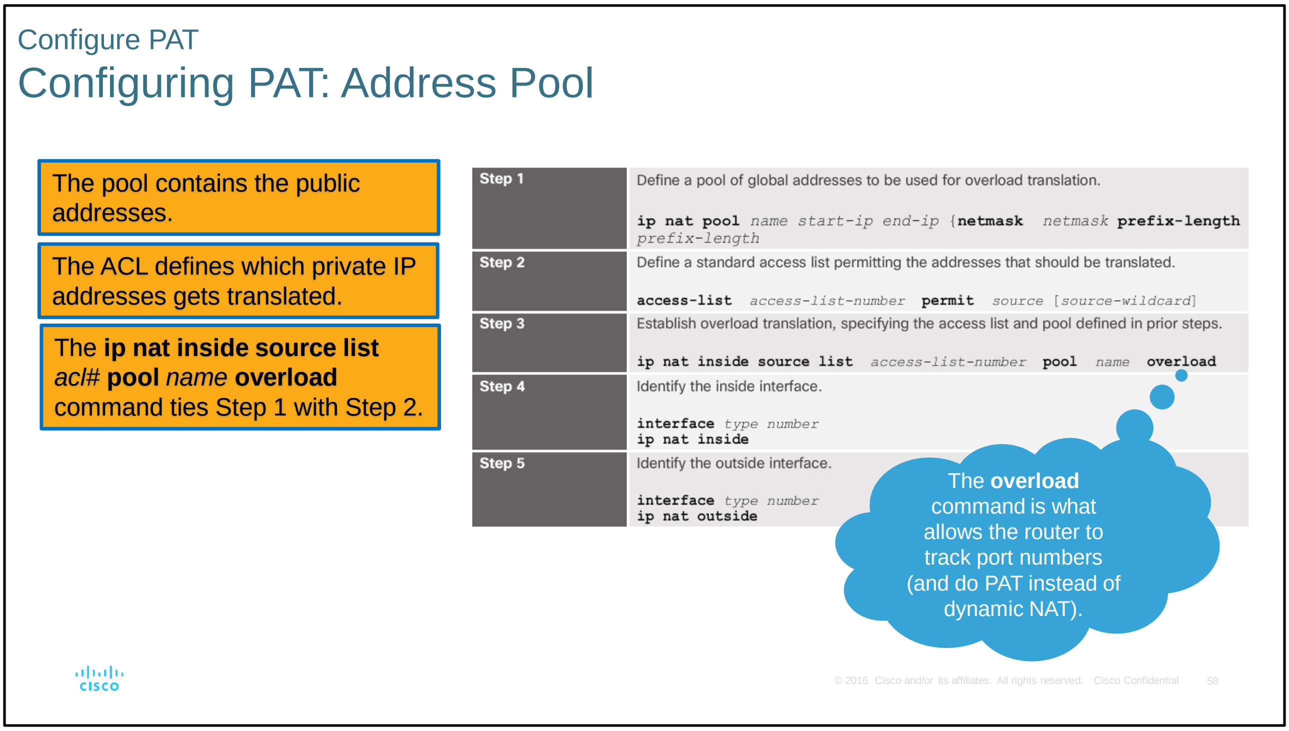


```
R2# clear ip nat statistics

PC1 and PC2 establish sessions with the server

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 0 extended)
Peak translations: 6, occurred 00:27:07 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 24  Misses: 0
CEF Translated packets: 24, CEF Punted packets: 0
Expired translations: 4
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 2
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

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

By default, translation entries time out after 24 hours, unless the timers have been reconfigured with the **ip nat translation timeout** *timeout-seconds* command in global configuration mode.
To clear dynamic entries before the timeout has expired, use the **clear ip nat translation** global configuration mode command. It is useful to clear the dynamic entries when testing the NAT configuration. As shown in the table, this command can be used with keywords and variables to control which entries are cleared. Specific entries can be cleared to avoid disrupting active sessions. Use the **clear ip nat translation *** global configuration command to clear all translations from the table.

Note: Only the dynamic translations are cleared from the table. Static translations cannot be cleared from the translation table.

In figure, the **show ip nat statistics** command displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and how many of the addresses have been allocated.
Alternatively, use the **show running-config** command and look for NAT, ACL, interface, or pool commands with the required values. Examine these carefully and correct any errors discovered.



Configure PAT

Configuring PAT: Address Pool

The pool contains the public addresses.

The ACL defines which private IP addresses gets translated.

The **ip nat inside source list** *acl#* **pool** *name* **overload** command ties Step 1 with Step 2.

Step 1	Define a pool of global addresses to be used for overload translation. `ip nat pool name start-ip end-ip {netmask netmask prefix-length prefix-length`
Step 2	Define a standard access list permitting the addresses that should be translated. `access-list access-list-number permit source [source-wildcard]`
Step 3	Establish overload translation, specifying the access list and pool defined in prior steps. `ip nat inside source list access-list-number pool name overload`

Step 4	Identify the inside interface.
	`interface type number`
	`ip nat inside`

Step 5	Identify the outside interface.
	`interface type number`
	`ip nat outside`

The **overload** command is what allows the router to track port numbers (and do PAT instead of dynamic NAT).

58

PAT (also called NAT overload) conserves addresses in the inside global address pool by allowing the router to use one inside global address for many inside local addresses. In other words, a single public IPv4 address can be used for hundreds, even thousands of internal private IPv4 addresses. When this type of translation is configured, the router maintains enough information from higher-level protocols, TCP or UDP port numbers, for example, to translate the inside global address back into the correct inside local address. When multiple inside local addresses map to one inside global address, the TCP or UDP port numbers of each inside host distinguish between the local addresses.

Note: The total number of internal addresses that can be translated to one external address could theoretically be as high as 65,536 per IP address. However, the number of internal addresses that can be assigned a single IP address is around 4,000.

There are two ways to configure PAT, depending on how the ISP allocates public IPv4 addresses. In the first instance, the ISP allocates more than one public IPv4 address to the organization, and in the other, it allocates a single public IPv4 address that is required for the organization to connect to the ISP.

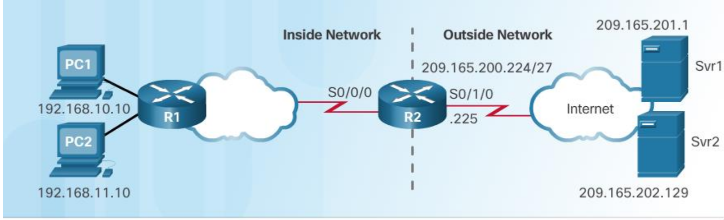
Configuring PAT for a Pool of Public IP Addresses

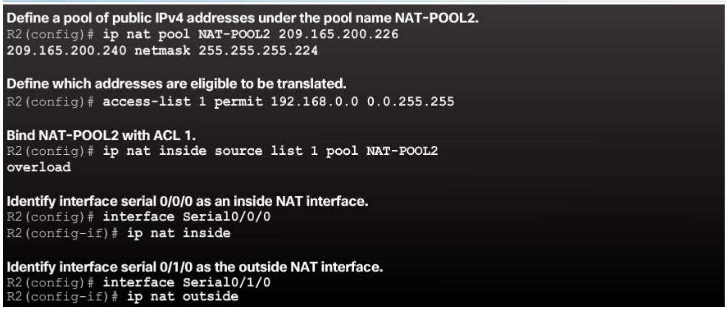
If a site has been issued more than one public IPv4 address, these addresses can be part of a pool that is used by PAT. This is similar to dynamic NAT, except that there are not enough public addresses for a one-to-one mapping of inside to outside addresses. The small pool of addresses is shared among a larger number of devices.

Figure shows the steps to configure PAT to use a pool of addresses. The primary difference between this configuration and the configuration for dynamic, one-to-one NAT is that the **overload** keyword is used. The **overload** keyword enables PAT.

Configure PAT

Configuring PAT: Address Pool (Cont.)





Define a pool of public IPv4 addresses under the pool name NAT-POOL2.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226
209.165.200.240 netmask 255.255.255.224
```

Define which addresses are eligible to be translated.

```
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

Bind NAT-POOL2 with ACL 1.

```
R2(config)# ip nat inside source list 1 pool NAT-POOL2
overload
```

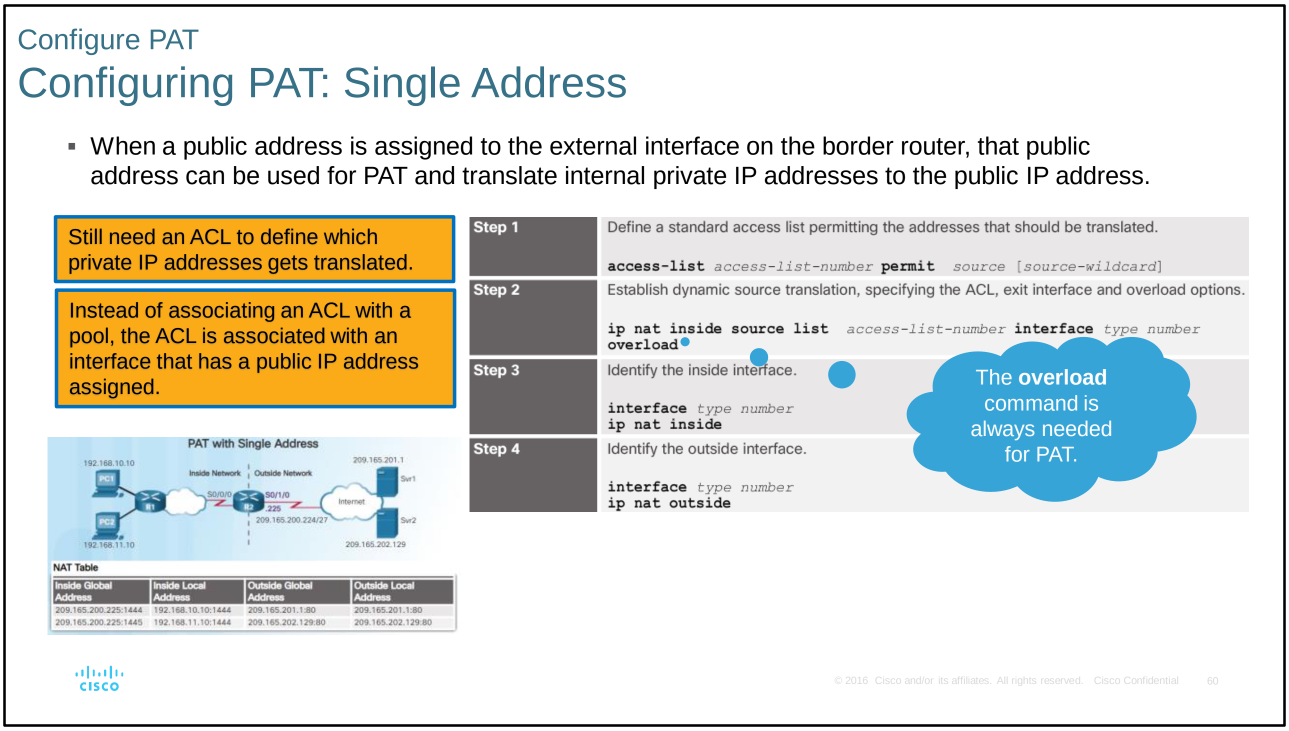
Identify interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identify interface serial 0/1/0 as the outside NAT interface.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

9.2 – Configure NAT
9.2.3 – Configure PAT
9.2.3.1 – Configuring PAT: Address Pool (Cont.)



Configure PAT

Configuring PAT: Single Address

- When a public address is assigned to the external interface on the border router, that public address can be used for PAT and translate internal private IP addresses to the public IP address.

Still need an ACL to define which private IP addresses gets translated.

Instead of associating an ACL with a pool, the ACL is associated with an interface that has a public IP address assigned.

PAT with Single Address

NAT Table

Inside Global Address	Inside Local Address	Outside Global Address	Outside Local Address
209.165.200.225:1444	192.168.10.10:1444	209.165.201.1:80	209.165.201.1:80
209.165.200.225:1445	192.168.11.10:1444	209.165.202.129:80	209.165.202.129:80

Step 1	Define a standard access list permitting the addresses that should be translated. **`access-list`** *`access-list-number`* **`permit`** *`source [source-wildcard]`*
Step 2	Establish dynamic source translation, specifying the ACL, exit interface and overload options. **`ip nat inside source list`** *`access-list-number`* **`interface`** *`type number`* **`overload`**

Step 3	Identify the inside interface.
	`interface` *`type number`*
	`ip nat inside`

Step 4	Identify the outside interface.
	`interface` *`type number`*
	`ip nat outside`

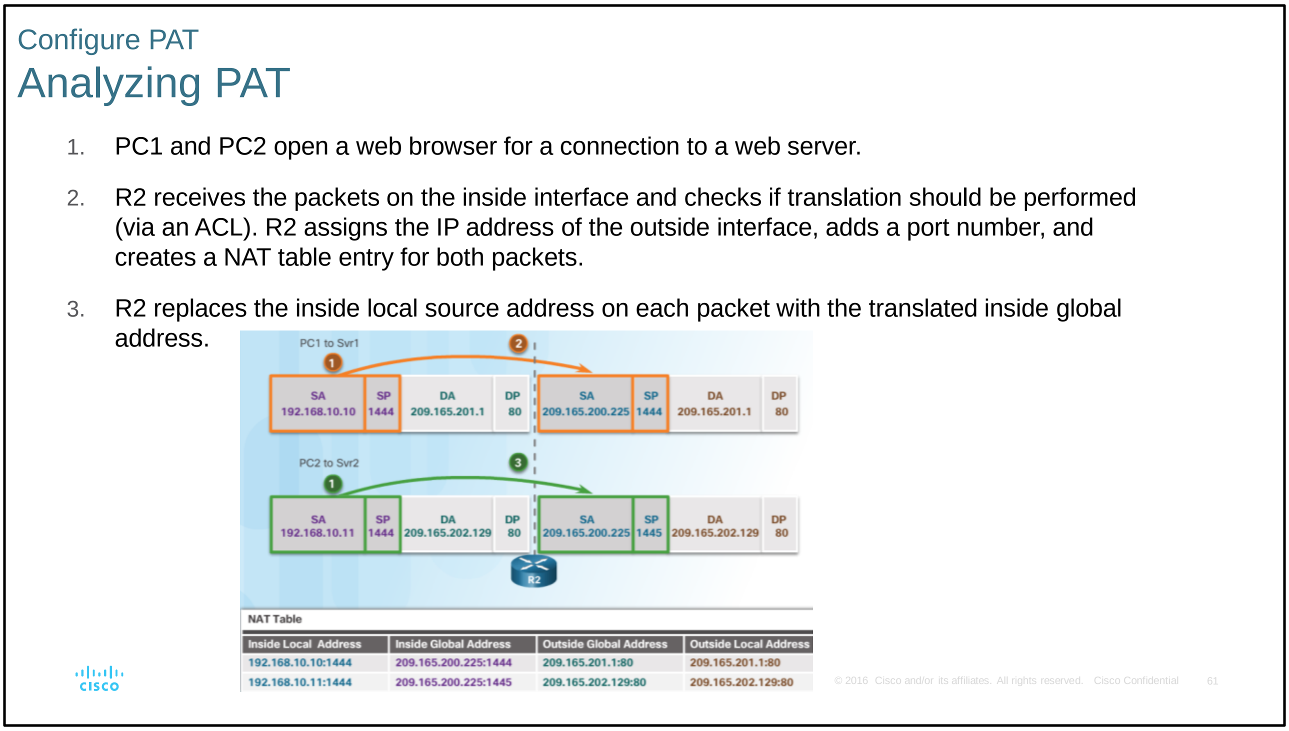
The **overload** command is always needed for PAT.

Configuring PAT for a Single Public IPv4 Address

Figure shows the steps to follow to configure PAT with a single IPv4 address. If only a single public IPv4 address is available, the overload configuration typically assigns the public address to the outside interface that connects to the ISP. All inside addresses are translated to the single IPv4 address when leaving the outside interface.

Step 1. Define an ACL to permit the traffic to be translated.
Step 2. Configure source translation using the **interface** and **overload** keywords.
The **interface** keyword identifies which interface IP address to use when translating inside addresses. The **overload** keyword directs the router to track port numbers with each NAT entry.
Step 3. Identify which interfaces are inside in relation to NAT. That is any interface that connects to the inside network.
Step 4. Identify which interface is outside in relation to NAT. This should be the same interface identified in the source translation statement from Step 2.

Figure shows the topology of a PAT implementation for a single public IPv4 address translation. In the example, all hosts from network 192.168.0.0/16 (matching ACL 1) that send traffic through router R2 to the Internet will be translated to IPv4 address 209.165.200.225 (IPv4 address of interface S0/1/0). The traffic flows will be identified by port numbers in the NAT table, because the **overload** keyword was used.



Configure PAT

Analyzing PAT

1. PC1 and PC2 open a web browser for a connection to a web server.
2. R2 receives the packets on the inside interface and checks if translation should be performed (via an ACL). R2 assigns the IP address of the outside interface, adds a port number, and creates a NAT table entry for both packets.
3. R2 replaces the inside local source address on each packet with the translated inside global address.

NAT Table

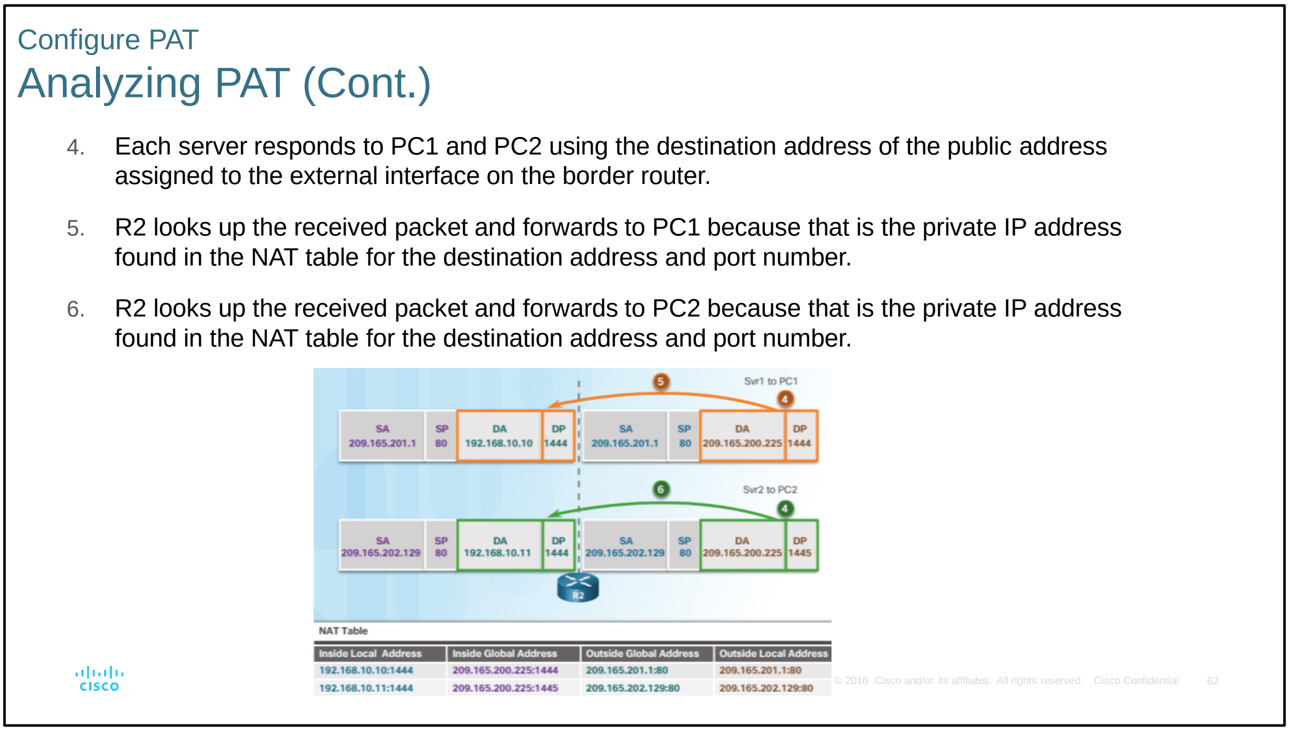
Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

The process of NAT overload is the same whether a pool of addresses is used or a single address is used. Continuing with the previous PAT example, using a single public IPv4 address, PC1 wants to communicate with the web server, Svr1. At the same time another client, PC2, wants to establish a similar session with the web server Svr2. Both PC1 and PC2 are configured with private IPv4 addresses, with R2 enabled for PAT.

PC to Server Process

1. Figure shows both PC1 and PC2 sending packets to Svr1 and Svr2, respectively. PC1 has the source IPv4 address 192.168.10.10 and is using TCP source port 1444. PC2 has the source IPv4 address 192.168.10.11 and is coincidentally assigned the same source port of 1444.
2. The packet from PC1 reaches R2 first. Using PAT, R2 modifies the source IPv4 address to 209.165.200.225 (inside global address). There are no other devices in the NAT table using port 1444, so PAT maintains the same port number. The packet is then forwarded towards Svr1 at 209.165.201.1.
3. Next, the packet from PC2 arrives at R2. PAT is configured to use a single inside global IPv4 address for all translations, 209.165.200.225. Similar to the translation process for PC1, PAT changes PC2's source IPv4 address to the inside global address 209.165.200.225. However, PC2 has the same source port number as a current PAT entry, the translation for PC1. PAT increments the source port number until it is a unique value in its table. In this instance, the source port entry in the NAT table and the packet for PC2 receives 1445.

Although PC1 and PC2 are using the same translated address, the inside global address of 209.165.200.225, and the same source port number of 1444; the modified port number for PC2 (1445) makes each entry in the NAT table unique. This will become evident with the packets sent from the servers back to the clients.



Configure PAT

Analyzing PAT (Cont.)

4. Each server responds to PC1 and PC2 using the destination address of the public address assigned to the external interface on the border router.
5. R2 looks up the received packet and forwards to PC1 because that is the private IP address found in the NAT table for the destination address and port number.
6. R2 looks up the received packet and forwards to PC2 because that is the private IP address found in the NAT table for the destination address and port number.

SA	SP	DA	DP	SA	SP	DA	DP
209.165.201.1	80	192.168.10.10	1444	209.165.201.1	80	209.165.200.225	1444

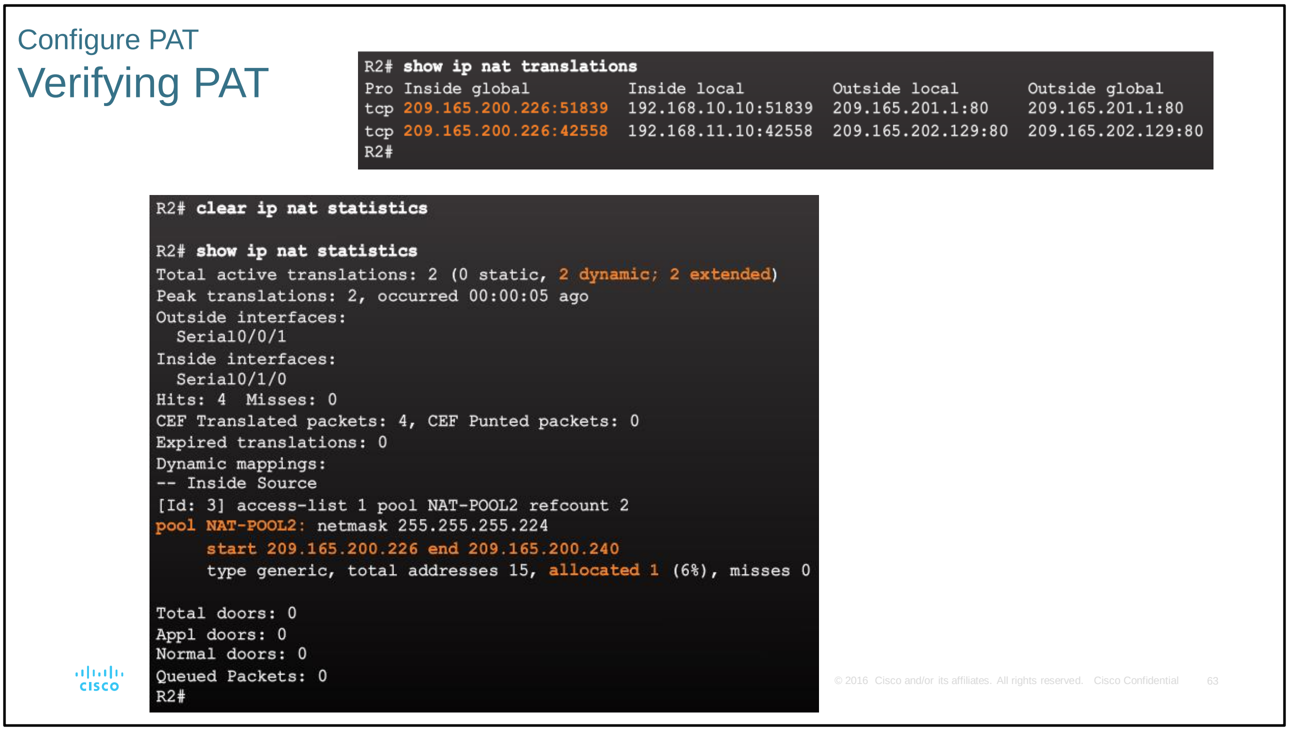
SA	SP	DA	DP	SA	SP	DA	DP
209.165.202.129	80	192.168.10.11	1444	209.165.202.129	80	209.165.200.225	1445

NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
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	209.165.202.129:80	209.165.202.129:80

Server to PC Process

4. As shown in Figure, in a typical client-server exchange, Svr1 and Svr2 respond to the requests received from PC1 and PC2, respectively. The servers use the source port from the received packet as the destination port, and the source address as the destination address for the return traffic. The servers seem as if they are communicating with the same host at 209.165.200.225; however, this is not the case.
5. As the packets arrive, R2 locates the unique entry in its NAT table using the destination address and the destination port of each packet. In the case of the packet from Svr1, the destination IPv4 address of 209.165.200.225 has multiple entries but only one with the destination port 1444. Using the entry in its table, R2 changes the destination IPv4 address of the packet to 192.168.10.10, with no change required for the destination port. The packet is then forwarded toward PC1.
6. When the packet from Svr2 arrives R2 performs a similar translation. The destination IPv4 address of 209.165.200.225 is located, again with multiple entries. However, using the destination port of 1445, R2 is able to uniquely identify the translation entry. The destination IPv4 address is changed to 192.168.10.11. In this case, the destination port must also be modified back to its original value of 1444, which is stored in the NAT table. The packet is then forwarded toward PC2.



Configure PAT

Verifying PAT

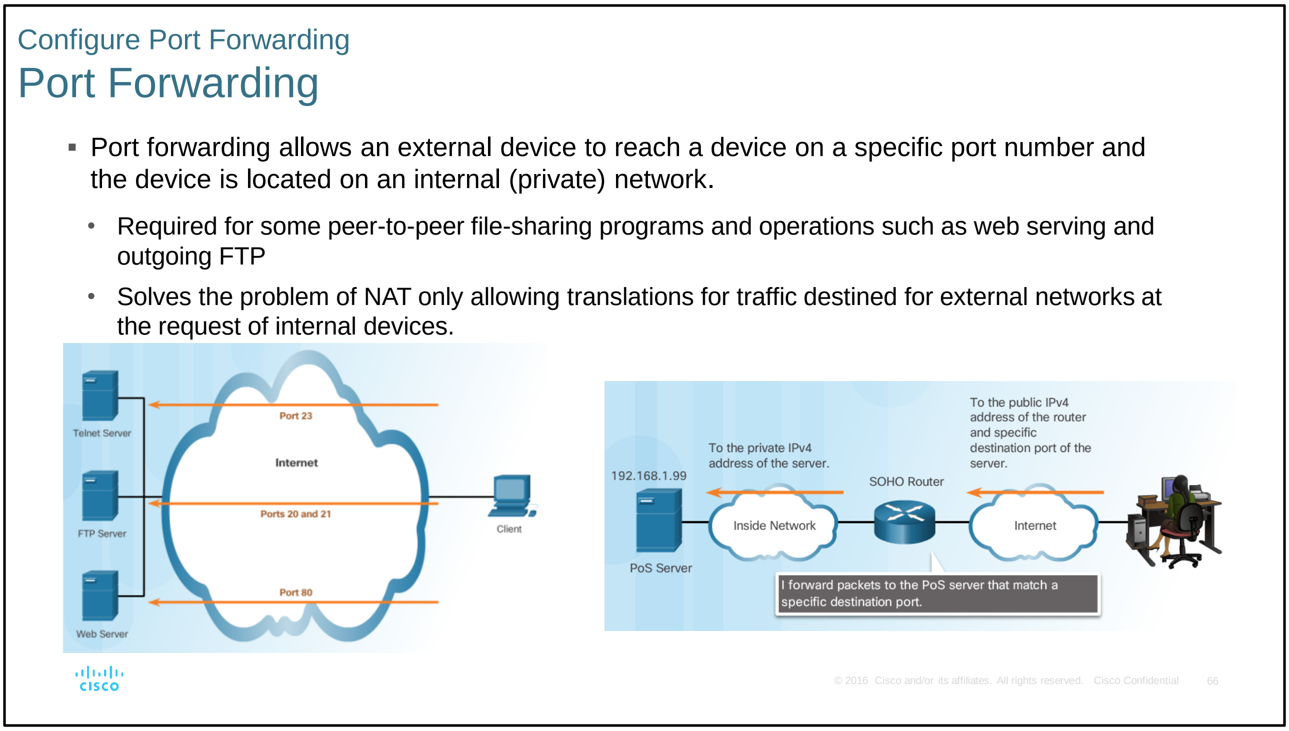
```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local       Outside global
tcp 209.165.200.226:51839  192.168.10.10:51839  209.165.201.1:80    209.165.201.1:80
tcp 209.165.200.226:42558  192.168.11.10:42558  209.165.202.129:80  209.165.202.129:80
R2#
```

```
R2# clear ip nat statistics

R2# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 4  Misses: 0
CEF Translated packets: 4, 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 209.165.200.226 end 209.165.200.240
     type generic, total addresses 15, allocated 1 (6%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
R2#
```

Router R2 has been configured to provide PAT to the 192.168.0.0/16 clients. When the internal hosts exit router R2 to the Internet, they are translated to an IPv4 address from the PAT pool with a unique source port number.

The same commands used to verify static and dynamic NAT are used to verify PAT, as shown in Figure.
The **show ip nat translations** command displays the translations from two different hosts to different web servers. Notice that two different inside hosts are allocated the same IPv4 address of 209.165.200.226 (inside global address). The source port numbers in the NAT table differentiate the two transactions.

The **show ip nat statistics** command verifies that NAT-POOL2 has allocated a single address for both translations. Included in the output is information about the number and type of active translations, NAT configuration parameters, the number of addresses in the pool, and how many have been allocated.



Configure Port Forwarding

Port Forwarding

- Port forwarding allows an external device to reach a device on a specific port number and the device is located on an internal (private) network.
  - Required for some peer-to-peer file-sharing programs and operations such as web serving and outgoing FTP
  - Solves the problem of NAT only allowing translations for traffic destined for external networks at the request of internal devices.

I forward packets to the PoS server that match a specific destination port.

Port forwarding (sometimes referred to as tunneling) is the act of forwarding a network port from one network node to another. This technique allows an external user to reach a port on a private IPv4 address (inside a LAN) from the outside, through a NAT-enabled router.

Typically, peer-to-peer file-sharing programs and operations, such as web serving and outgoing FTP, require that router ports be forwarded or opened to allow these applications to work. Because NAT hides internal addresses, peer-to-peer only works from the inside out where NAT can map outgoing requests against incoming replies.

The problem is that NAT does not allow requests initiated from the outside. This situation can be resolved with manual intervention. Port forwarding can be configured to identify specific ports that can be forwarded to inside hosts.

Recall that Internet software applications interact with user ports that need to be open or available to those applications. Different applications use different ports. This makes it predictable for applications and routers to identify network services. For example, HTTP operates through the well-known port 80. When someone enters the**http://cisco.com** address, the browser displays the Cisco Systems, Inc. website. Notice that they do not have to specify the HTTP port number for the page request, because the application assumes port 80.

If a different port number is required, it can be appended to the URL separated by a colon (:). For example, if the web server is listening on port 8080, the user would

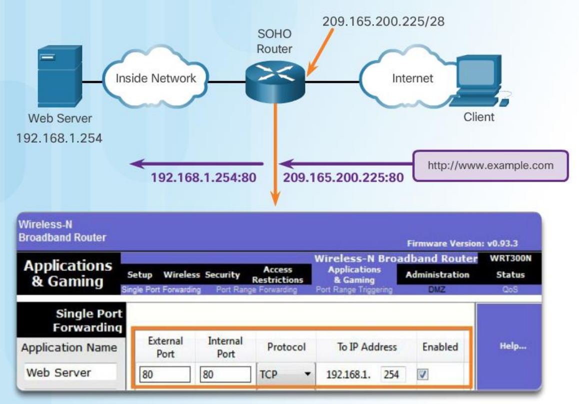
type**http://www.example.com:8080**.
Port forwarding allows users on the Internet to access internal servers by using the WAN port address of the router and the matched external port number. The internal servers are typically configured with RFC 1918 private IPv4 addresses. When a request is sent to the IPv4 address of the WAN port via the Internet, the router forwards the request to the appropriate server on the LAN. For security reasons, broadband routers do not by default permit any external network request to be forwarded to an inside host.

Figure shows a small business owner using a point of sale (PoS) server to track sales and inventories at the store. The server can be accessed within the store but, because it has a private IPv4 address, it is not publically accessible from the Internet. Enabling the local router for port forwarding allows the owner to access the point of sale server from anywhere on the Internet. Port forwarding on the router is configured using the destination port number and the private IPv4 address of the point of sale server. To access the server, the client software would use the public IPv4 address of the router and the destination port of the server.

Configure Port Forwarding

Wireless Router Example

- Port forwarding can be enabled for specific applications
  - Must specify the inside local address that requests should be forwarded to



Single Port Forwarding

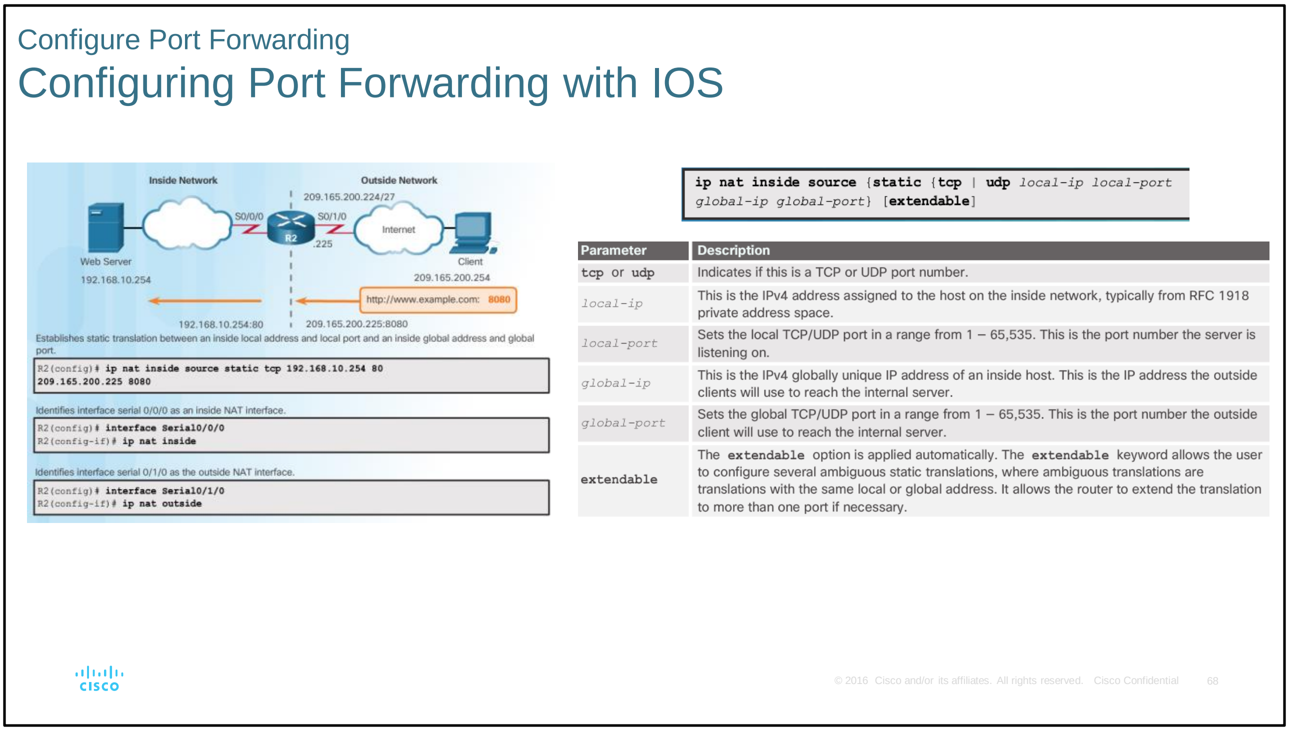
Application Name	External Port	Internal Port	Protocol	To IP Address	Enabled
Web Server	80	80	TCP	192.168.1. 254	☑

The figure shows the Single Port Forwarding configuration window of a Linksys EA6500 SOHO router. By default, port forwarding is not enabled on the router.

Port forwarding can be enabled for applications by specifying the inside local address that requests should be forwarded to. In the figure, HTTP service requests, coming into this Linksys router, are forwarded to the web server with the inside local address of 192.168.1.254. If the external WAN IPv4 address of the SOHO router is 209.165.200.225, the external user can enter **http://www.example.com** and the Linksys router redirects the HTTP request to the internal web server at IPv4 address 192.168.1.254, using the default port number 80.

A port other than the default port 80 can be specified. However, the external user would have to know the specific port number to use. To specify a different port, the value of the External Port in the Single Port Forwarding window would be modified.

The approach taken to configure port forwarding depends on the brand and model of the broadband router in the network. However, there are some generic steps to follow. If the instructions supplied by the ISP, or those that came with the router, do not provide adequate guidance, the websitehttp://www.portforward.com provides guides for several broadband routers. You can follow the instructions to add or delete ports as required to meet the needs of any applications you want to allow or deny.



Configure Port Forwarding

Configuring Port Forwarding with IOS

Establishes static translation between an inside local address and local port and an inside global address and global port.

```
R2(config)# ip nat inside source static tcp 192.168.10.254 80
209.165.200.225 8080
```

Identifies interface serial 0/0/0 as an inside NAT interface.

```
R2(config)# interface Serial0/0/0
R2(config-if)# ip nat inside
```

Identifies interface serial 0/1/0 as the outside NAT interface.

```
R2(config)# interface Serial0/1/0
R2(config-if)# ip nat outside
```

```
ip nat inside source {static {tcp | udp local-ip local-port
global-ip global-port} [extendable]
```

Parameter	Description
`tcp` or `udp`	Indicates if this is a TCP or UDP port number.
local-ip	This is the IPv4 address assigned to the host on the inside network, typically from RFC 1918 private address space.
local-port	Sets the local TCP/UDP port in a range from 1 – 65,535. This is the port number the server is listening on.
global-ip	This is the IPv4 globally unique IP address of an inside host. This is the IP address the outside clients will use to reach the internal server.
global-port	Sets the global TCP/UDP port in a range from 1 – 65,535. This is the port number the outside client will use to reach the internal server.
extendable	The **extendable** option is applied automatically. The **extendable** keyword allows the user to configure several ambiguous static translations, where ambiguous translations are translations with the same local or global address. It allows the router to extend the translation to more than one port if necessary.

Implementing port forwarding with IOS commands is similar to the commands used to configure static NAT. Port forwarding is essentially a static NAT translation with a specified TCP or UDP port number.

Figure shows an example of configuring port forwarding using IOS commands on router R2. 192.168.10.254 is the inside local IPv4 address of the web server listening on port 80. Users will access this internal web server using the global IP address 209.165.200.225, a globally unique public IPv4 address. In this case, it is the address of the Serial 0/1/0 interface of R2. The global port is configured as 8080. This will be the destination port used, along with the global IPv4 address of 209.165.200.225 to access the internal web server. Notice within the NAT configuration, the following command parameters:

- *local-ip* = 192.168.10.254
- *local-port* = 80
- *global-ip* = 209.165.200.225
- *global-port* = 8080

When a well-known port number is not being used, the client must specify the port number in the application.

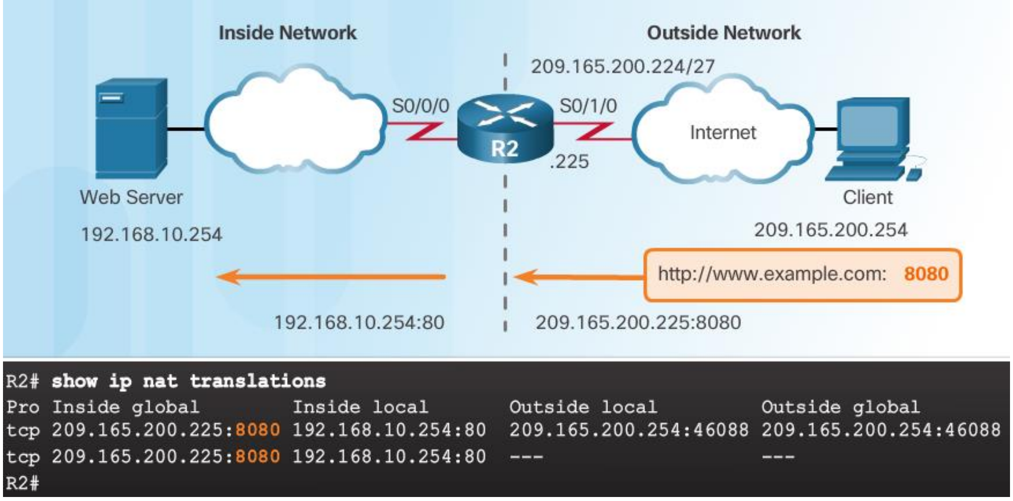
Like other types of NAT, port forwarding requires the configuration of both the inside and outside NAT interfaces.

Similar to static NAT, the **show ip nat translations** command can be used to verify the port forwarding.

In the example, when the router receives the packet with the inside global IPv4 address of 209.165.200.225 and a TCP destination port 8080, the router performs a NAT table lookup using the destination IPv4 address and destination port as the key. The router then translates the address to the inside local address of host 192.168.10.254 and destination port 80. R2 then forwards the packet to the web server. For return packets from the web server back to the client, this process is reversed.

Configure Port Forwarding

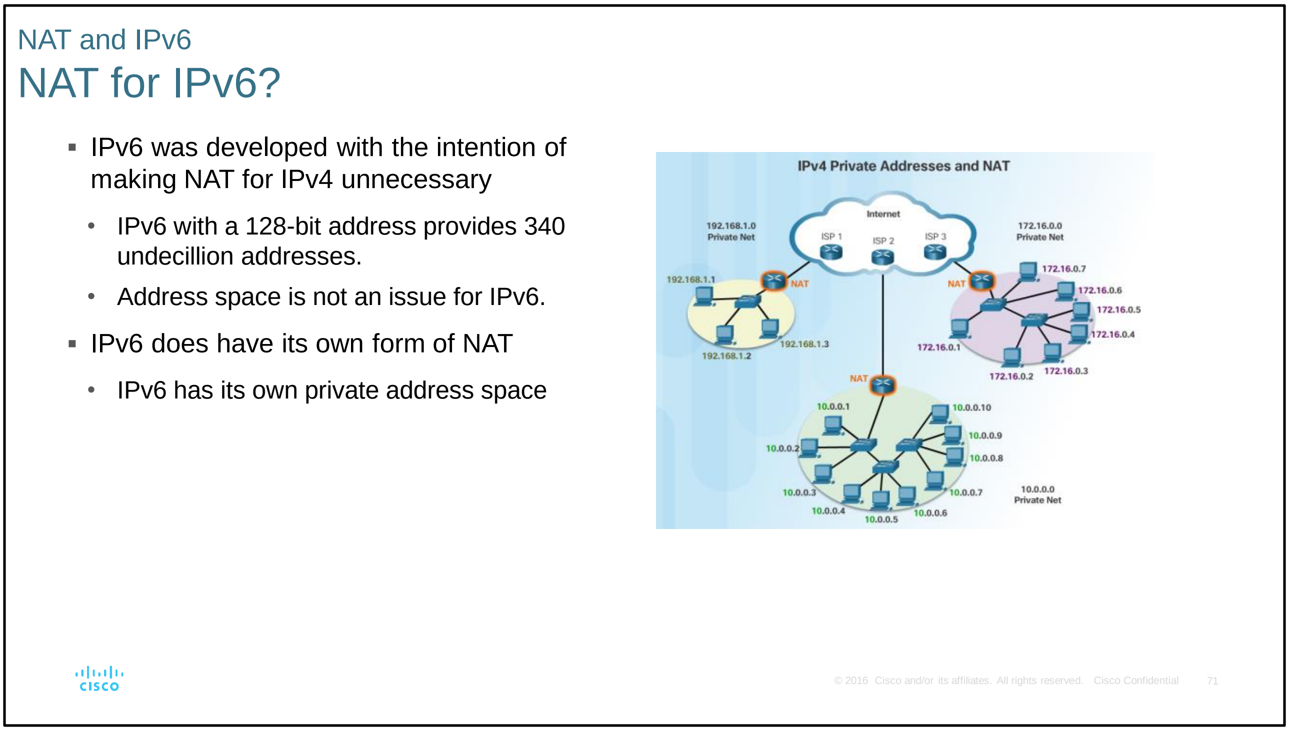
Configuring Port Forwarding with IOS (Cont.)



```
R2# show ip nat translations
Pro Inside global          Inside local        Outside local          Outside global
tcp 209.165.200.225:8080 192.168.10.254:80  209.165.200.254:46088 209.165.200.254:46088
tcp 209.165.200.225:8080 192.168.10.254:80  ---                    ---
R2#
```

Similar to static NAT, the **show ip nat translations** command can be used to verify the port forwarding.

In the example, when the router receives the packet with the inside global IPv4 address of 209.165.200.225 and a TCP destination port 8080, the router performs a NAT table lookup using the destination IPv4 address and destination port as the key. The router then translates the address to the inside local address of host 192.168.10.254 and destination port 80. R2 then forwards the packet to the web server. For return packets from the web server back to the client, this process is reversed.



NAT and IPv6

NAT for IPv6?

- IPv6 was developed with the intention of making NAT for IPv4 unnecessary
  - IPv6 with a 128-bit address provides 340 undecillion addresses.
  - Address space is not an issue for IPv6.
- IPv6 does have its own form of NAT
  - IPv6 has its own private address space

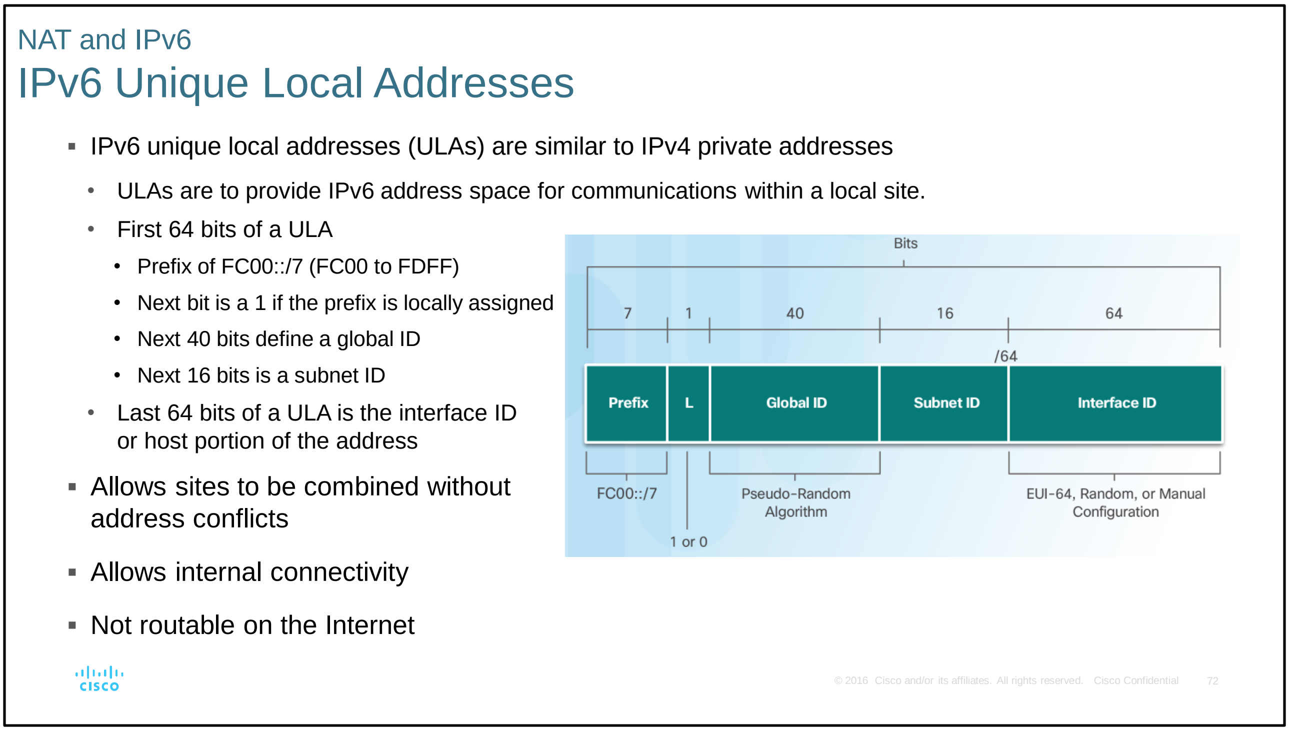
Since the early 1990s, the concern about the depletion of IPv4 address space has been a priority of the IETF. The combination of RFC 1918 private IPv4 addresses and NAT has been instrumental in slowing this depletion. NAT has significant disadvantages, and in January of 2011, IANA allocated the last of its IPv4 addresses to RIRs.

One of the unintentional benefits of NAT for IPv4 is that it hides the private network from the public Internet. NAT has the advantage of providing a perceived level of security by denying computers in the public Internet from accessing internal hosts. However, it should not be considered a substitute for proper network security, such as that provided by a firewall.

In RFC 5902, the Internet Architecture Board (IAB) included the following quote concerning IPv6 network address translation:

“It is commonly perceived that a NAT box provides one level of protection because external hosts cannot directly initiate communication with hosts behind a NAT. However, one should not confuse NAT boxes with firewalls. As discussed in [RFC4864], Section 2.2, the act of translation does not provide security in itself. The stateful filtering function can provide the same level of protection without requiring a translation function.”

IPv6 with a 128-bit address provides 340 undecillion addresses. Therefore, address space is not an issue. IPv6 was developed with the intention of making NAT for IPv4 with its translation between public and private IPv4 addresses unnecessary. However, IPv6 does implement a form of NAT. IPv6 includes both its own IPv6 private address space and NAT, which are implemented differently than they are for IPv4.



NAT and IPv6

IPv6 Unique Local Addresses

- IPv6 unique local addresses (ULAs) are similar to IPv4 private addresses
  - ULAs are to provide IPv6 address space for communications within a local site.
  - First 64 bits of a ULA
    - Prefix of FC00::/7 (FC00 to FDFF)
    - Next bit is a 1 if the prefix is locally assigned
    - Next 40 bits define a global ID
    - Next 16 bits is a subnet ID
  - Last 64 bits of a ULA is the interface ID or host portion of the address
- Allows sites to be combined without address conflicts
- Allows internal connectivity
- Not routable on the Internet

IPv6 unique local addresses (ULA) are similar to RFC 1918 private addresses in IPv4, but there are significant differences as well. The intent of ULA is to provide IPv6 address space for communications within a local site; it is not meant to provide additional IPv6 address space, nor is it meant to provide a level of security.

As shown in the figure, ULA have the prefix FC00::/7, which results in a first hextet range of FC00 to FDFF. The next 1 bit is set to 1 if the prefix is locally assigned. Set to 0 may be defined in the future. The next 40 bits is a global ID followed by a 16-bit Subnet ID. These first 64 bits combine to make the ULA prefix. This leaves the remaining 64 bits for the interface ID, or in IPv4 terms, the host portion of the address.

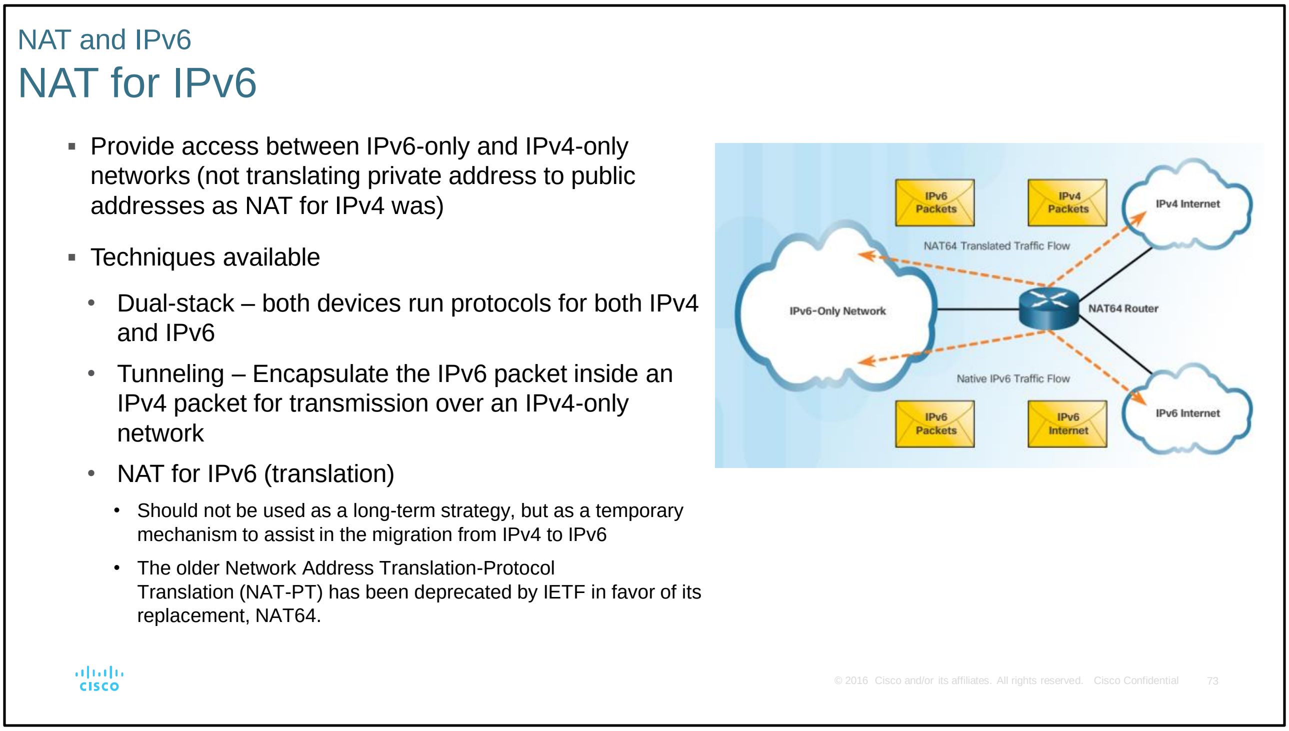
Unique local addresses are defined in RFC 4193. ULAs are also known as local IPv6 addresses (not to be confused with IPv6 link-local addresses) and have several characteristics including:

- Allows sites to be combined or privately interconnected, without creating any address conflicts or requiring renumbering of interfaces that use these prefixes.
- Independent of any ISP and can be used for communications within a site without having any Internet connectivity.
- Not routable across the Internet, however, if accidentally leaked by routing or DNS, there is not conflict with other addresses.

ULA is not quite as straight-forward as RFC 1918 addresses. Unlike private IPv4 addresses, it has not been the intention of the IETF to use a form of NAT to translate between unique local addresses and IPv6 global unicast addresses.

The implementation and potential uses for IPv6 unique local addresses are still being examined by the Internet community. For example, the IETF is considering allowing the option to have the ULA prefix created locally using FC00::/8, or to have it assigned automatically by a third-party beginning with FD00::/8.

Note: The original IPv6 specification allocated address space for site-local addresses, defined in RFC 3513. Site-local addresses have since been deprecated by the IETF in RFC 3879 because the term “site” was somewhat ambiguous. Site-local addresses had the prefix range of FEC0::/10 and may still be found in some older IPv6 documentation.



NAT and IPv6

NAT for IPv6

- Provide access between IPv6-only and IPv4-only networks (not translating private address to public addresses as NAT for IPv4 was)
- Techniques available
  - Dual-stack – both devices run protocols for both IPv4 and IPv6
  - Tunneling – Encapsulate the IPv6 packet inside an IPv4 packet for transmission over an IPv4-only network
  - NAT for IPv6 (translation)
    - Should not be used as a long-term strategy, but as a temporary mechanism to assist in the migration from IPv4 to IPv6
    - The older Network Address Translation-Protocol Translation (NAT-PT) has been deprecated by IETF in favor of its replacement, NAT64.

NAT for IPv6 is used in a much different context than NAT for IPv4. The varieties of NAT for IPv6 are used to transparently provide access between IPv6-only and IPv4-only networks. It is not used as a form of private IPv6 to global IPv6 translation.

Ideally, IPv6 should be run natively wherever possible. This means IPv6 devices communicating with each other over IPv6 networks. However, to aid in the move from IPv4 to IPv6, the IETF has developed several transition techniques to accommodate a variety of IPv4-to-IPv6 scenarios, including dual-stack, tunneling, and translation.
Dual-stack is when the devices are running protocols associated with both the IPv4 and IPv6. Tunneling for IPV6 is the process of encapsulating an IPv6 packet inside an IPv4 packet. This allows the IPv6 packet to be transmitted over an IPv4-only network.
NAT for IPv6 should not be used as a long term strategy, but as a temporary mechanism to assist in the migration from IPv4 to IPv6. Over the years, there have been several types of NAT for IPv6 including Network Address Translation-Protocol Translation (NAT-PT). NAT-PT has been deprecated by IETF in favor of its replacement, NAT64. NAT64 is beyond the scope of this curriculum.

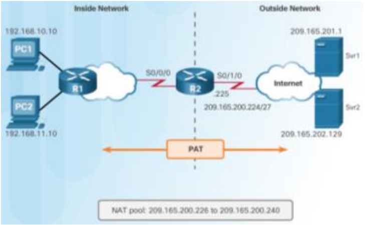
Troubleshoot NAT

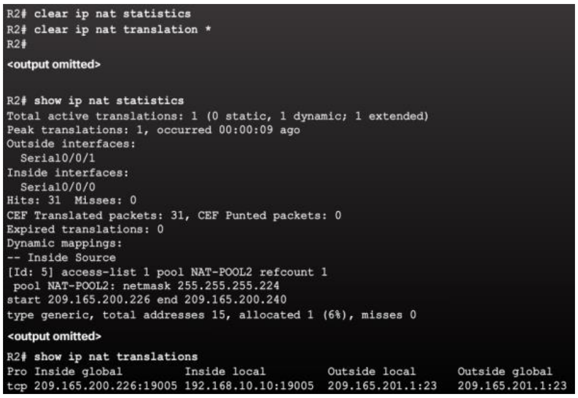
9 – NAT for IPv4
9.3 – Troubleshoot NAT

NAT Troubleshooting Commands

The show ip nat Commands

1. Determine what NAT is supposed to achieve and compare with configuration. This may reveal a problem with the configuration.
2. Verify translations using the **show ip nat translations** command.
3. Use the **clear** and **debug** commands to verify NAT.
4. Review what is happening to the packet and verify routing.





```
R2# clear ip nat statistics
R2# clear ip nat translation *
R2#
<output omitted>

R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:00:09 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/0/0
Hits: 31  Misses: 0
CEF Translated packets: 31, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
 pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0
<output omitted>
R2# show ip nat translations
Pro Inside global         Inside local         Outside local       Outside global
tcp 209.165.200.226:19005 192.168.10.10:19005  209.165.201.1:23    209.165.201.1:23
```

Figure shows R2 enabled for PAT, using the range of addresses 209.165.200.226 to 209.165.200.240.

When there are IPv4 connectivity problems in a NAT environment, it is often difficult to determine the cause of the problem. The first step in solving the problem is to rule out NAT as the cause. Follow these steps to verify that NAT is operating as expected:

Step 1. Based on the configuration, clearly define what NAT is supposed to achieve. This may reveal a problem with the configuration.

Step 2. Verify that correct translations exist in the translation table using the **show ip nat translations** command.

Step 3. Use the **clear** and **debug** commands to verify that NAT is operating as expected. Check to see if dynamic entries are recreated after they are cleared.

Step 4. Review in detail what is happening to the packet, and verify that routers have the correct routing information to move the packet.

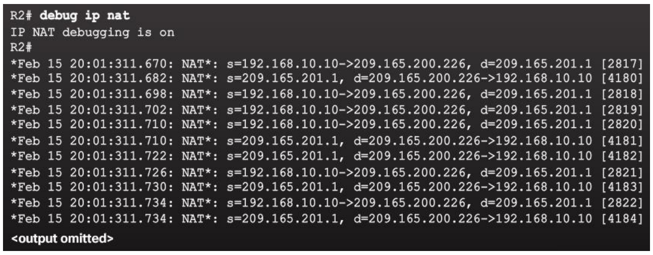
Figure shows the output of the **show ip nat statistics** and **show ip nat translations** commands. Prior to using the **show** commands, the NAT statistics and entries in the NAT table are cleared with the **clear ip nat statistics**and **clear ip nat translation ***commands. After the host at 192.168.10.10 Telnets to the server at 209.165.201.1, the NAT statistics and NAT table are displayed to verify NAT is working as expected.

In a simple network environment, it is useful to monitor NAT statistics with the**show ip nat statistics** command. The **show ip nat statistics**command displays information about the total number of active translations, NAT configuration parameters, the number of addresses in the pool, and the number that have been allocated. However, in a more complex NAT environment, with several translations taking place, this command may not clearly identify the issue. It may be necessary to run **debug** commands on the router.

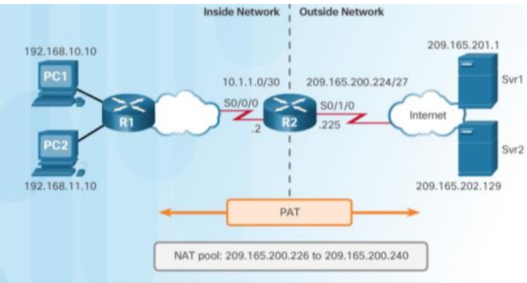
NAT Troubleshooting Commands

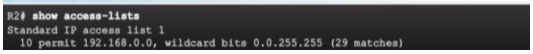
The debug ip nat Commands

- Common commands
  - **debug ip nat**
  - **debug ip nat detailed**
- Output symbols and values
  - * - The translation is occurring in the fast-switched path
  - **s=** - Source IPv4 address
  - **a.b.c.d**--->**w.x.y.z** – Source a.b.c.d is translated to w.x.y.z.
  - **d=** - Destination IPv4 address
  - **[xxxx]** - IPv4 identification number
- Check the ACL to ensure the correct private addresses are designated.



```
R2# debug ip nat
IP NAT debugging is on
R2#
*Feb 15 20:01:311.670: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2817]
*Feb 15 20:01:311.682: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4180]
*Feb 15 20:01:311.698: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2818]
*Feb 15 20:01:311.702: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2819]
*Feb 15 20:01:311.710: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2820]
*Feb 15 20:01:311.710: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4181]
*Feb 15 20:01:311.722: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4182]
*Feb 15 20:01:311.726: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2821]
*Feb 15 20:01:311.730: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4183]
*Feb 15 20:01:311.734: NAT*: s=192.168.10.10->209.165.200.226, d=209.165.201.1 [2822]
*Feb 15 20:01:311.734: NAT*: s=209.165.201.1, d=209.165.200.226->192.168.10.10 [4184]
<output omitted>
```





```
R2# show access-lists
Standard IP access list 1
  10 permit 192.168.0.0, wildcard bits 0.0.255.255 (29 matches)
```

Use the **debug ip nat** command to verify the operation of the NAT feature by displaying information about every packet that is translated by the router. The **debug ip nat detailed** command generates a description of each packet considered for translation. This command also provides information about certain errors or exception conditions, such as the failure to allocate a global address. The **debug ip nat detailed** command generates more overhead than the **debug ip nat**command, but it can provide the detail that may be needed to troubleshoot the NAT problem. Always turn off debugging when finished.

Figure shows a sample **debug ip nat** output. The output shows that the inside host (192.168.10.10) initiated traffic to the outside host (209.165.201.1) and the source address was translated to address 209.165.200.226.

When decoding the debug output, note what the following symbols and values indicate:

*** (asterisk)** - The asterisk next to NAT indicates that the translation is occurring in the fast-switched path. The first packet in a conversation is always process-switched, which is slower. The remaining packets go through the fast-switched path if a cache entry exists.

s= - This symbol refers to the source IP address.

a.b.c.d--->**w.x.y.z** - This value indicates that source address a.b.c.d is translated to w.x.y.z.

d= - This symbol refers to the destination IP address.

[xxxx] - The value in brackets is the IP identification number. This information may be useful for debugging in that it enables correlation with other packet traces from protocol analyzers.

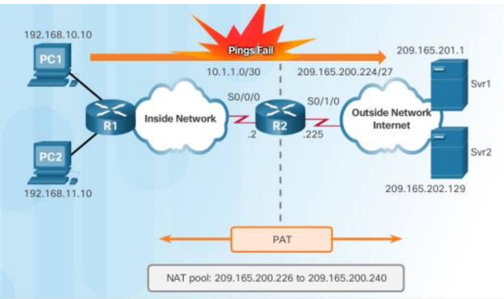
Verify that the ACL referenced in the NAT command reference is permitting all of the necessary networks. In figure, only 192.168.0.0/16 addresses are eligible to be translated. Packets from the inside network destined for the Internet with source addresses that are not explicitly permitted by ACL 1 are not translated by R2.

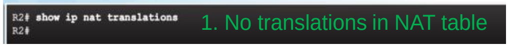
Note: Verify that the ACL referenced in the NAT command reference is permitting all of the necessary networks. In Figure 2, only 192.168.0.0/16 addresses are eligible to be translated. Packets from the inside network destined for the Internet with source addresses that are not explicitly permitted by ACL 1 are not translated by R2.

NAT Troubleshooting Commands

NAT Troubleshooting Scenario

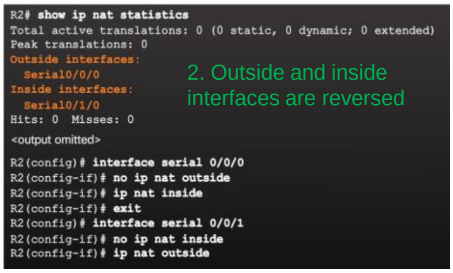
- Internal hosts cannot contact external servers.





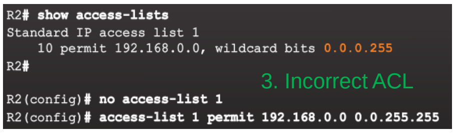
```
R2# show ip nat translations
R2#
```

1. No translations in NAT table



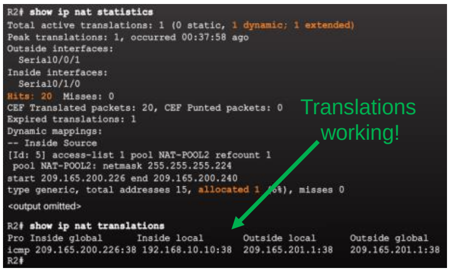
```
R2# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/0
Inside interfaces:
  Serial0/1/0
Hits: 0  Misses: 0
<output omitted>
R2(config)# interface serial 0/0/0
R2(config-if)# no ip nat outside
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/0/1
R2(config-if)# no ip nat inside
R2(config-if)# ip nat outside
```

2. Outside and inside interfaces are reversed



```
R2# show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
R2#

R2(config)# no access-list 1
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
```

3. Incorrect ACL

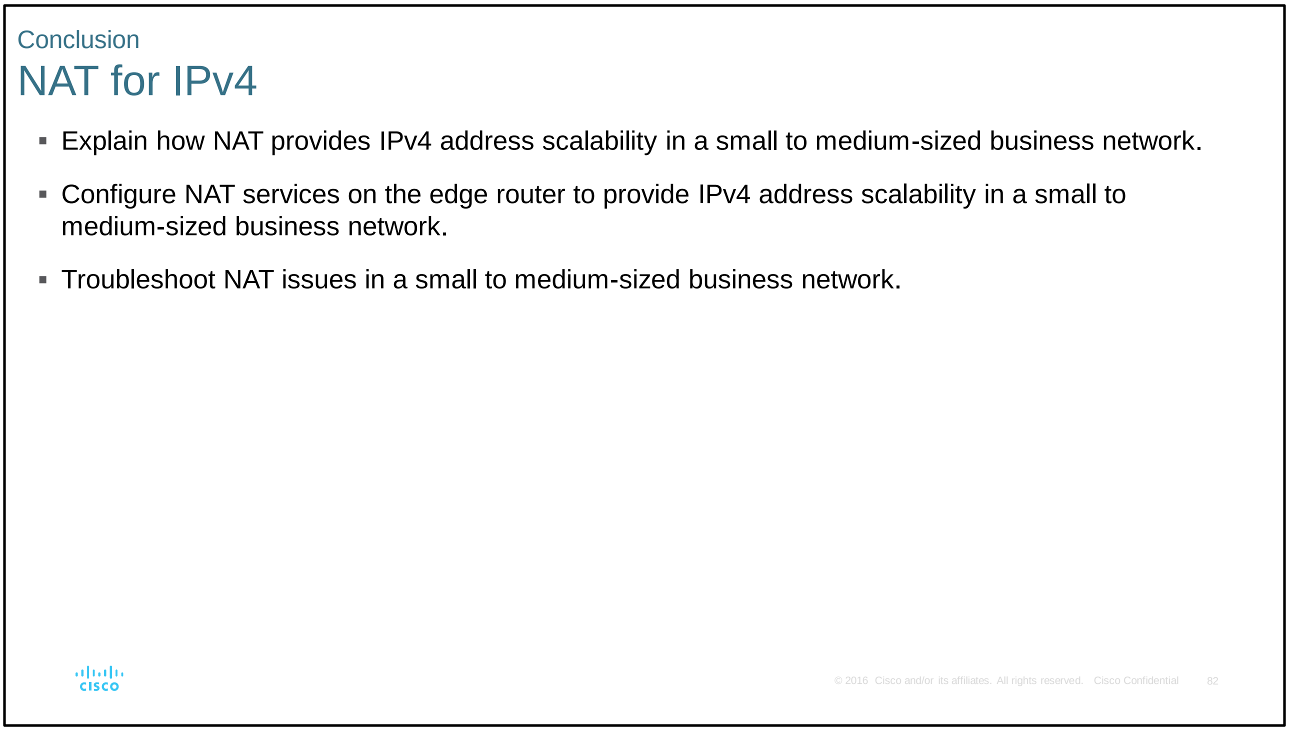


```
R2# show ip nat statistics
Total active translations: 1 (0 static, 1 dynamic; 1 extended)
Peak translations: 1, occurred 00:37:58 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Serial0/1/0
Hits: 20  Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 1
Dynamic mappings:
-- Inside Source
[Id: 5] access-list 1 pool NAT-POOL2 refcount 1
 pool NAT-POOL2: netmask 255.255.255.224
start 209.165.200.226 end 209.165.200.240
type generic, total addresses 15, allocated 1 (6%), misses 0
<output omitted>
R2# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.226:38 192.168.10.10:38  209.165.201.1:38   209.165.201.1:38
R2#
```

Translations working!

Chapter Summary

9 – NAT for IPv4
9.4 – Summary



Conclusion

NAT for IPv4

- Explain how NAT provides IPv4 address scalability in a small to medium-sized business network.
- Configure NAT services on the edge router to provide IPv4 address scalability in a small to medium-sized business network.
- Troubleshoot NAT issues in a small to medium-sized business network.

9.4 – Summary

9.4.1 – Conclusion
9.4.1.3 – NAT for IPv4

cisco