CCNA 3 v7.0 Curriculum: Module 6 – NAT for IPv4

itexamanswers.net/ccna-3-v7-0-curriculum-module-6-nat-for-ipv4.html

April 10, 2020

Contents

6.0. Introduction

6.0.1. Why should I take this module?

Welcome to NAT for IPv4!

IPv4 addresses are 32-bit numbers. Mathematically, this means that there can be just over 4 billion unique IPv4 addresses. In the 1980s, this seemed like more than enough IPv4 addresses. Then came the development of affordable desktop and laptop computers, smart phones and tablets, many other digital technologies, and of course, the internet. Rather quickly it became apparent that 4 billion IPv4 addresses would not be nearly enough to handle the growing demand. This is why IPv6 was developed. Even with IPv6, most networks today are IPv4-only, or a combination of IPv4 and IPv6. The transition to IPv6-only networks is still ongoing, that is why Network Address Translation (NAT) was developed. NAT is designed to help manage those 4 billion addresses so that we can all use our many devices to access the internet. As you can see, it is important that you understand the purpose of (NAT) and how it works. As a bonus, this module contains multiple Packet Tracer activities where you get to configure different types of NAT. Get going!

6.0.2. What will I learn to do in this module?

Module Title: NAT for IPv4

Module Objective: Configure NAT services on the edge router to provide IPv4 address scalability.

Topic Title	Topic Objective
NAT Characteristics	Explain the purpose and function of NAT.
Types of NAT	Explain the operation of different types of NAT.
NAT Advantages and Disadvantages	Describe the advantages and disadvantages of NAT.
Static NAT	Configure static NAT using the CLI.

Topic Title	Topic Objective
Dynamic NAT	Configure dynamic NAT using the CLI.
PAT	Configure PAT using the CLI.
NAT64	Describe NAT for IPv6.

6.1. NAT Characteristics

6.1.1. IPv4 Private Address Space

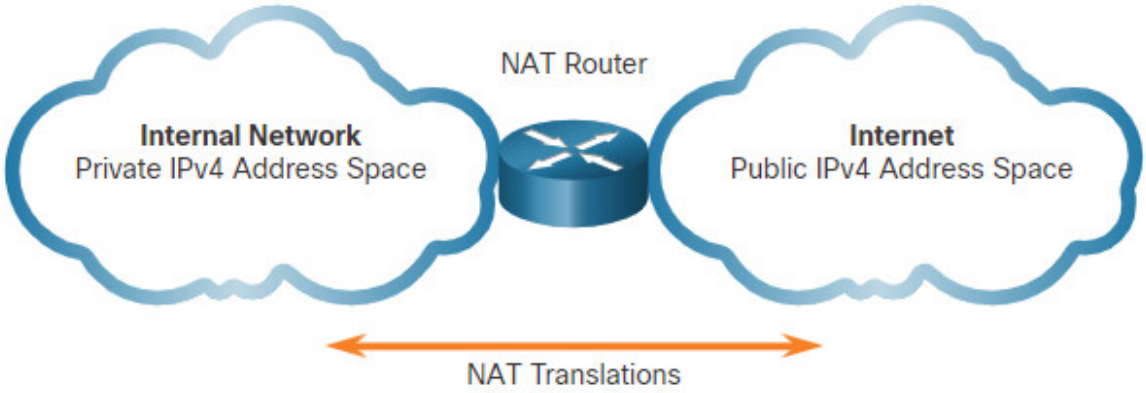
As you know, there are not enough public IPv4 addresses to assign a unique address to each device connected to the internet. Networks are commonly implemented using private IPv4 addresses, as defined in RFC 1918. The range of addresses included in RFC 1918 are included in the following table. It is very likely that the computer that you use to view this course is assigned a private address.

Private Internet Addresses are Defined in RFC 1918

Class	RFC 1918 Internal Address Range	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 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 provides the translation of private addresses to public addresses, as shown in the figure. 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 been the primary 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.



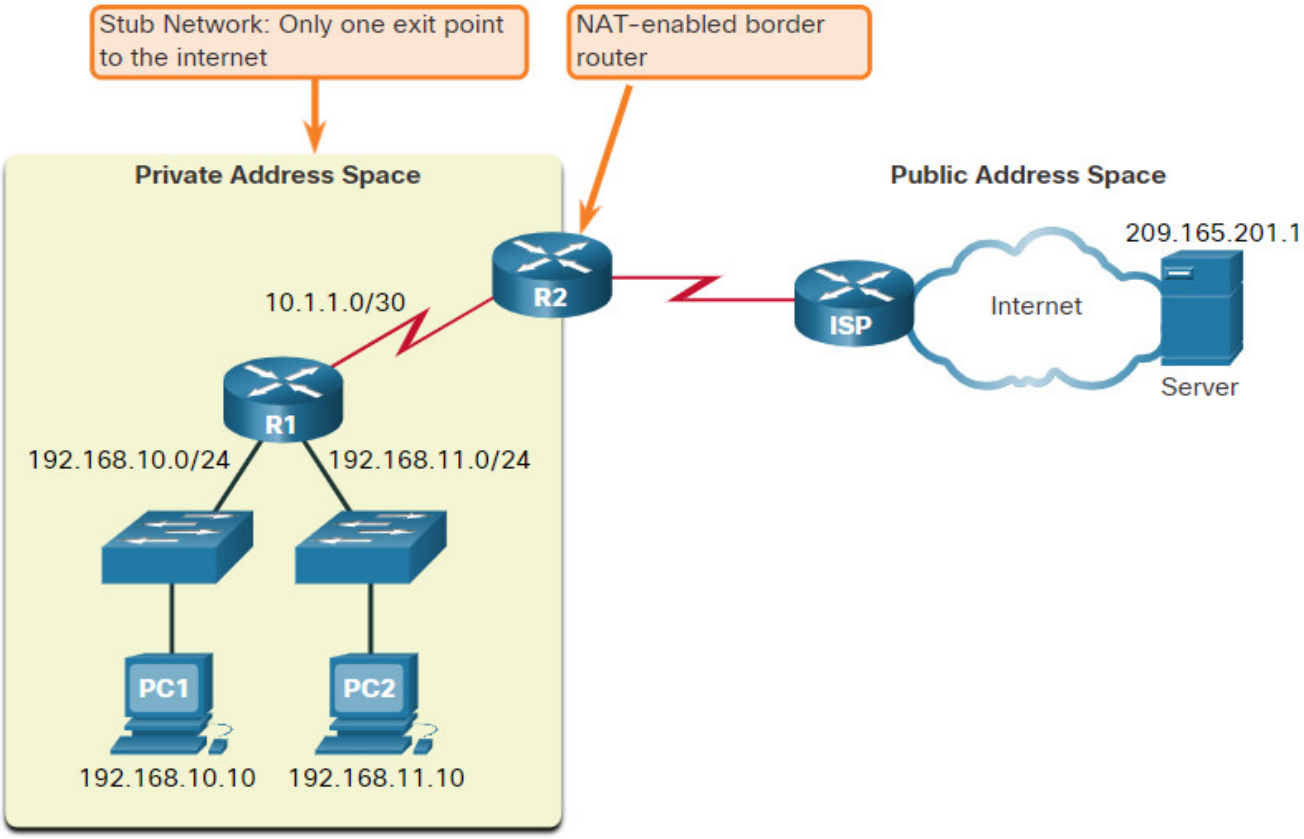
Without NAT, the exhaustion of the IPv4 address space would have occurred well before the year 2000. However, NAT has limitations and disadvantages, which will be explored later in this module. The solution to the exhaustion of IPv4 address space and the limitations of NAT is the eventual transition to IPv6.

6.1.2. What is NAT

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 a perceived 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 one or more networks with 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.

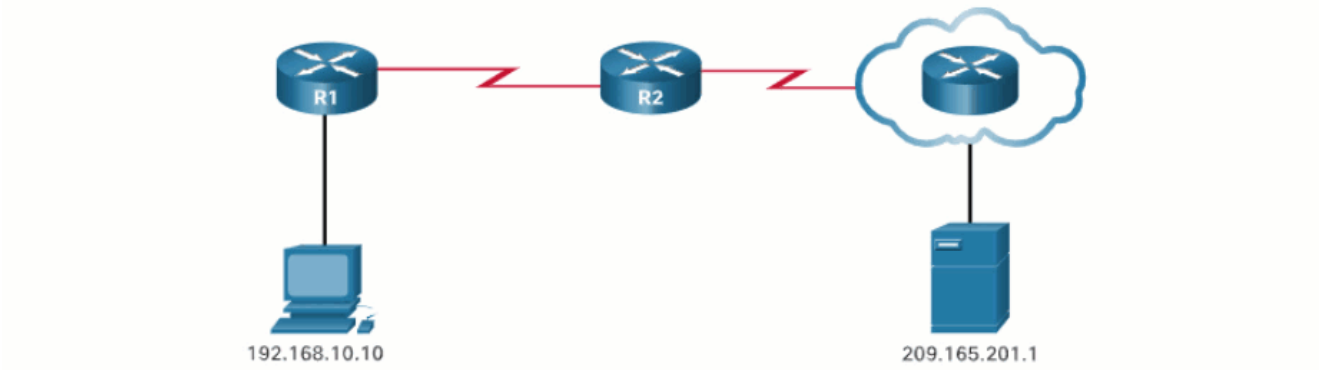


When a device inside the stub network wants to communicate with a device outside of its network, the packet is forwarded to the border router. The border router performs the NAT process, translating the internal private address of the device to a public, outside, routable address.

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

6.1.3. How NAT Works

In this example, PC1 with private address 192.168.10.10 wants to communicate with an outside web server with public address 209.165.201.1.



6.1.4. NAT Terminology

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

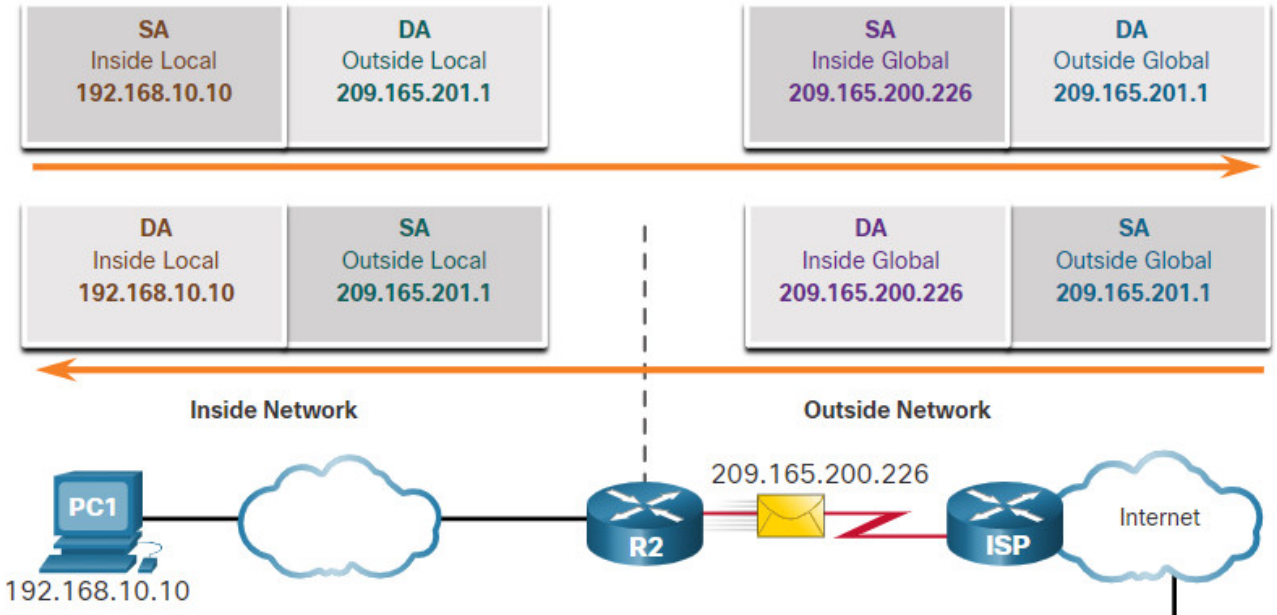
When determining which type of address is used, it is important to remember that NAT terminology is always applied from the perspective of the device with the translated address:

- **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.

The terms, inside and outside, are combined with the terms local and global to refer to specific addresses. The NAT router, R2 in the figure, is the demarcation point between the inside and outside networks. R2 is configured with a pool of public addresses to assign to inside hosts. Refer to the network and NAT table in the figure for the following discussion of each of the NAT address types.



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

Click each button for more information about the different address types.

Inside local address

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

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.

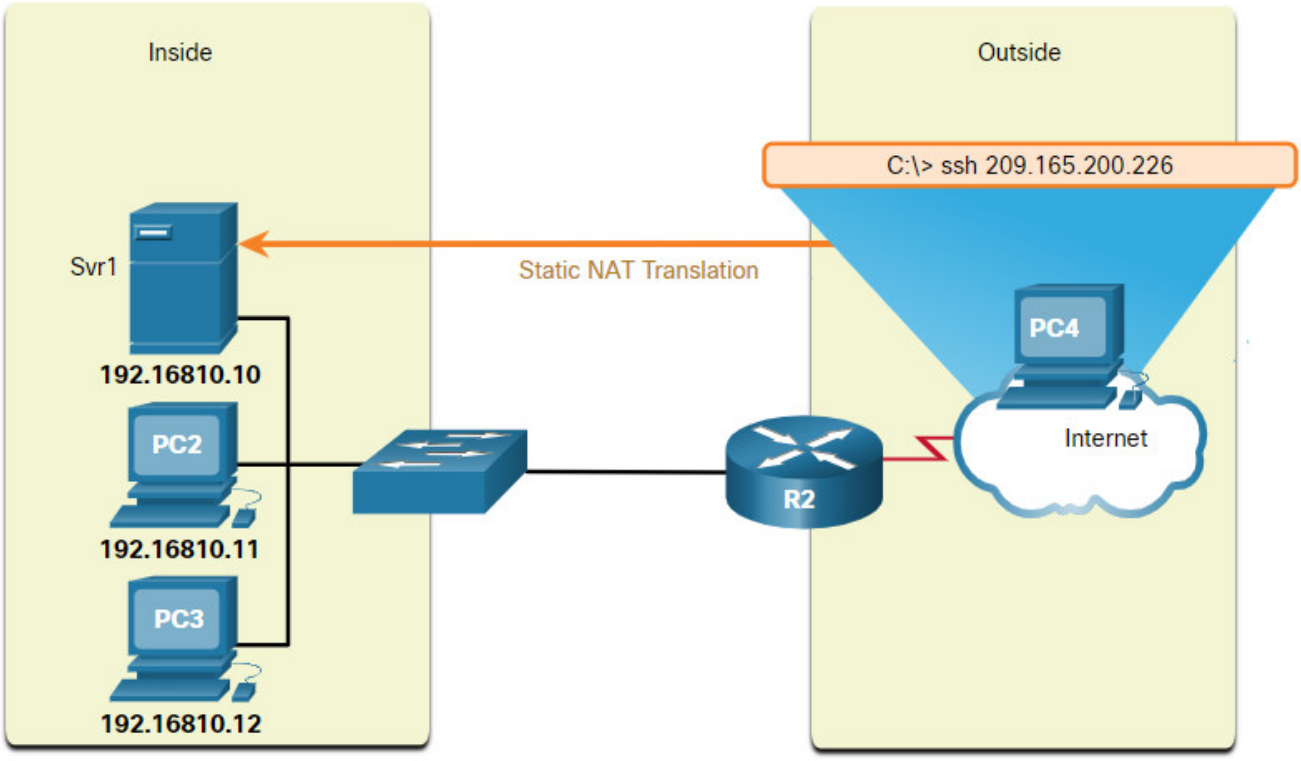
6.2. Types of NAT

6.2.1. Static NAT

Now that you have learned about NAT and how it works, this topic will discuss the many versions of NAT that are available to you.

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 appear to have public IPv4 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

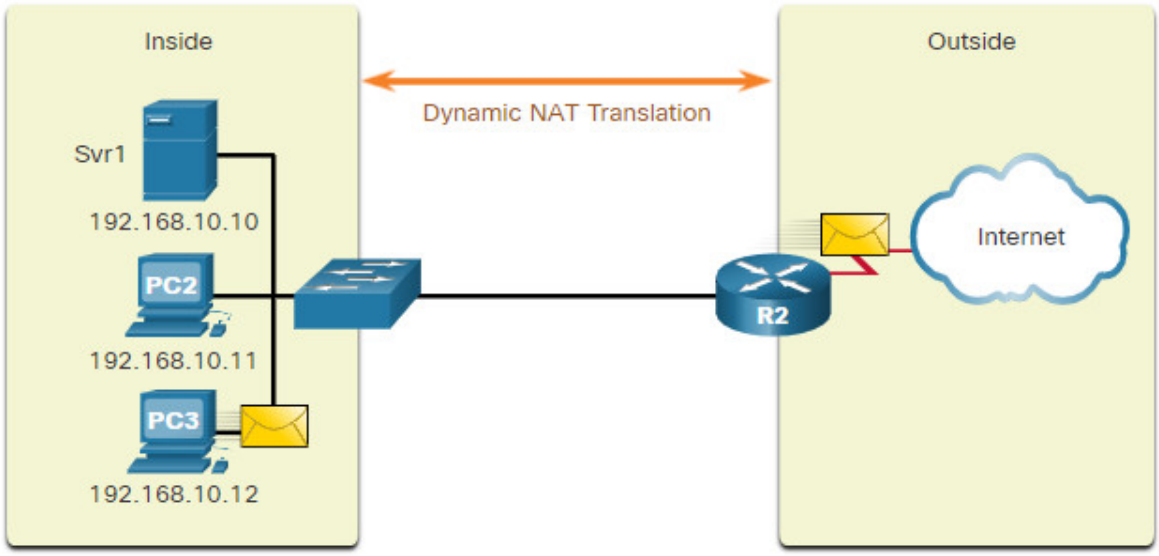
Static NAT is particularly useful for web servers or devices that must have a consistent address that is accessible from the internet, such as a company web server. It is also useful for devices that must be accessible by authorized personnel when offsite, but not by the general public on the internet. For example, a network administrator from PC4 can use SSH to gain access to the inside global address of Svr1 (209.165.200.226). R2 translates this inside global address to the inside local address 192.168.10.10 and connects the session to Svr1.

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

6.2.2. Dynamic NAT

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.



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

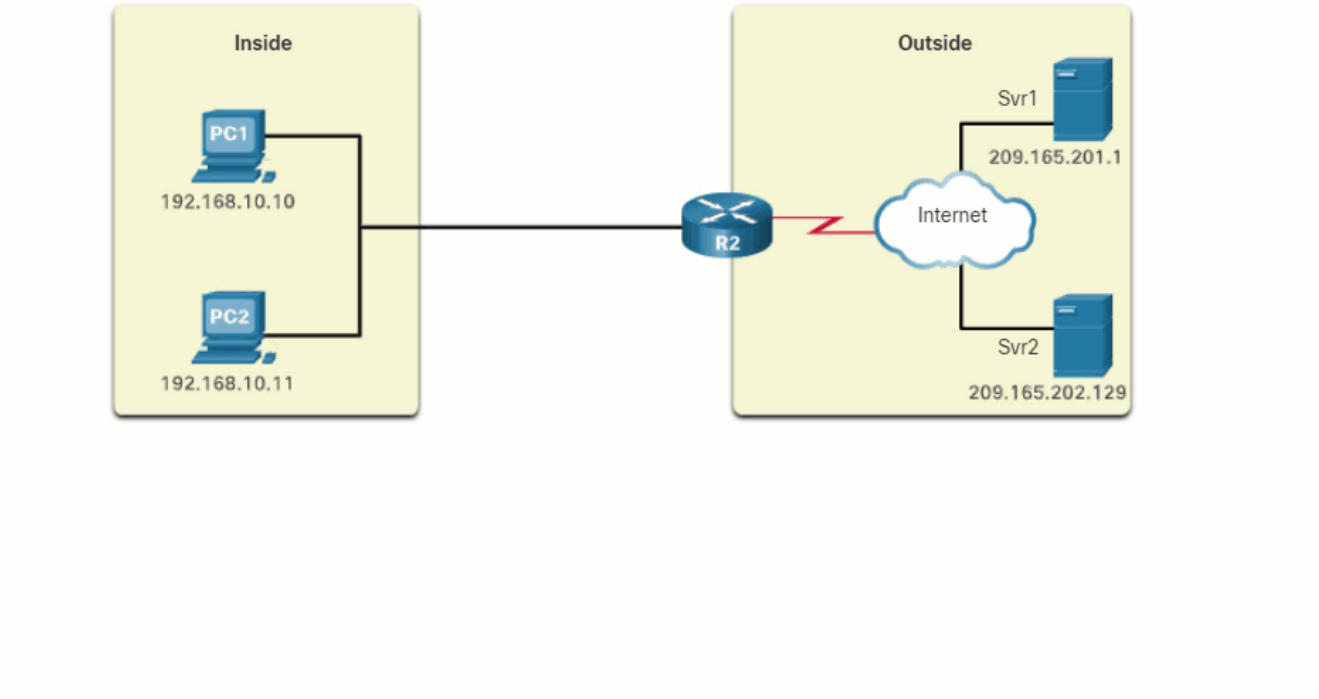
6.2.3. Port Address Translation

Port Address Translation (PAT), also known as NAT overload, 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 for both the home and the enterprise.

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, or a specially assigned query ID for ICMP, 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.

Click Play in the figure to view an animation of the PAT process. PAT adds unique source port numbers to the inside global address to distinguish between translations.



As R2 processes each packet, it uses a port number (1331 and 1555, in this example) to identify the device from which the packet originated. The source address (SA) is the inside local address with the TCP/UDP assigned port number added. The destination address (DA) is the outside global address with the service port number added. In this example, the service port is 80, which is HTTP.

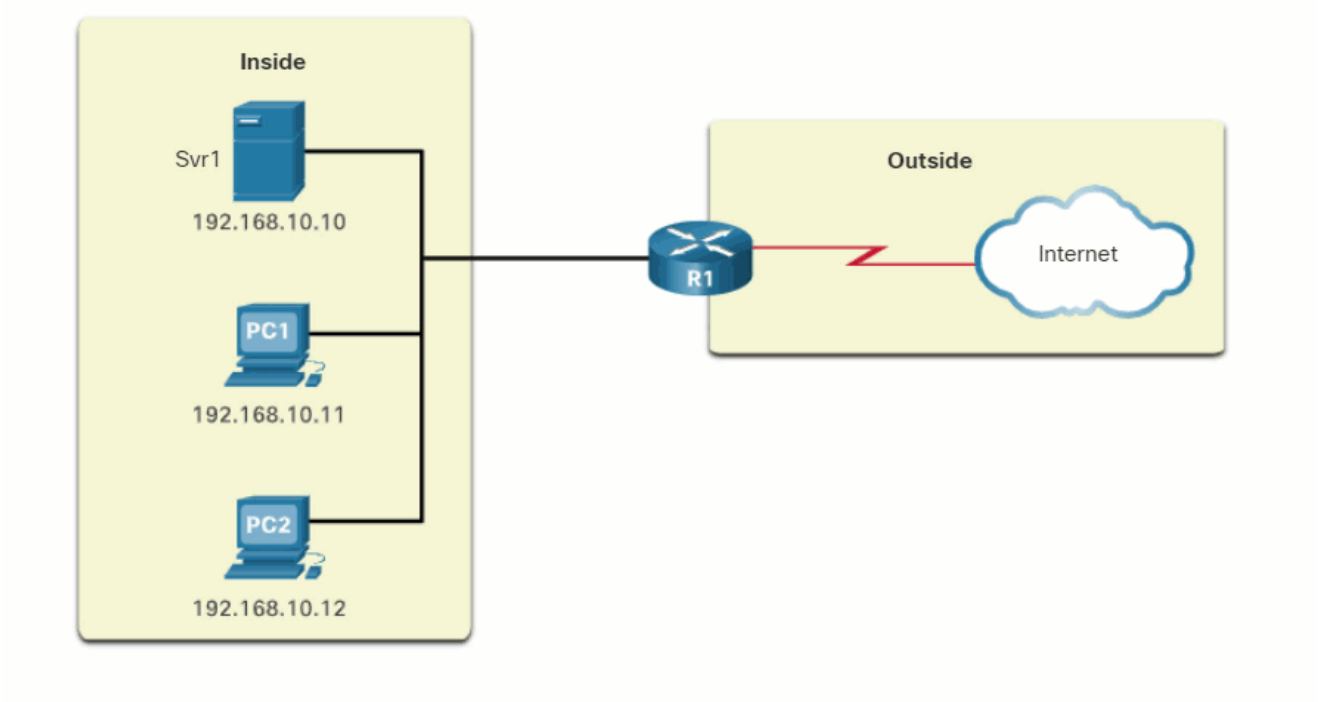
For the source address, R2 translates the inside local address to an inside global address with the port number added. The destination address is not changed but is now referred to as the outside global IPv4 address. When the web server replies, the path is reversed.

6.2.4. Next Available Port

In the previous example, the client port numbers, 1331 and 1555, did not change at the NAT-enabled router. This is not a very likely scenario, because there is a good chance that these port numbers may have already been attached to other active sessions.

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 IPv4 addresses.

Click Play in the figure to view an animation of PAT operation. In this example, PAT has assigned the next available port (1445) to the second host address.



In the animation, the hosts have chosen the same port number of 1444. This is acceptable for the inside address, because the hosts have unique private IPv4 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. This example assumes that the first 420 ports in the range 1,024 – 65,535 are already in use, so the next available port number, 1445, is used.

When packets are returned from outside the network, if the source port number was previously modified by the NAT-enable router, the destination port number will now be changed back to the original port number by the NAT-enabled router.

6.2.5. NAT and PAT Comparison

The table provides a summary of the differences between NAT and PAT.

NAT	PAT
One-to-one mapping between Inside Local and Inside Global addresses.	One Inside Global address can be mapped to many Inside Local addresses.
Uses only IPv4 addresses in translation process.	Uses IPv4 addresses and TCP or UDP source port numbers in translation process.
A unique Inside Global address is required for each inside host accessing the outside network.	A single unique Inside Global address can be shared by many inside hosts accessing the outside network.

Click each button for an example and explanation of the differences between NAT and PAT.

- NAT
- PAT

NAT
The figure shows a simple example of a NAT table. In this example, four hosts on the internal network are communicating to the outside network. The left column lists the addresses in the global address pool that are used by NAT to translate the Inside Local address of each host. Note the one-to-one relationship of Inside Global addresses to Inside Local addresses for each of the four hosts accessing the outside network. With NAT, an Inside Global address is needed for each host that needs to connect to the outside network.

Note: NAT forwards the incoming return packets to the original inside host by referring to the table and translating the Inside Global address back to the corresponding Inside Local address of the host.

Inside Global Address	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

6.2.6. 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 curriculum.

6.2.7. Packet Tracer – Investigate NAT Operations

You know that as a frame travels across a network, the MAC addresses change. But IPv4 addresses can also change when a packet is forwarded by a device configure with NAT. In this activity we will see what happens to IPv4 addresses during the NAT process.

In this Packet Tracer activity, you will:

- Investigate NAT operation across the intranet
- Investigate NAT operation across the internet
- Conduct further investigations

6.2.7 Packet Tracer – Investigate NAT Operation

6.3. NAT Advantages and Disadvantages

6.3.1. Advantages of NAT

NAT solves our problem of not having enough IPv4 addresses, but it can also create other problems. This topic addresses the advantages and disadvantage of NAT.

NAT provides many benefits, including the following:

- NAT conserves the legally registered addressing scheme by allowing the privatization of intranets. NAT conserves addresses through application port-level multiplexing. With NAT overload (PAT), 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.
- Using RFC 1918 IPv4 addresses, NAT hides the IPv4 addresses of users and other devices. Some people consider this a security feature; however, most experts agree that NAT does not provide security. A stateful firewall is what provides security on the edge of the network.

6.3.2. Disadvantages of NAT

NAT does have 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 forwarding delays because the translation of each IPv4 address within the packet headers takes time. The first packet is always process-switched going 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.

This becomes more of an issue as the pools of public IPv4 addresses for ISPs become depleted. Many ISPs are having to assign customers a private IPv4 address instead of a public IPv4 address. This means the customer's router translates the packet from its private IPv4 address to the private IPv4 address of the ISP. Before forwarding the packet to another provider, the ISP will then perform NAT again, translating its private IPv4 addresses to one of its limited number of public IPv4 addresses. This process of two layers of NAT translation is known as Carrier Grade NAT (CGN).

Another disadvantage of using NAT is that end-to-end addressing is lost. This is known as the end-to-end principle. 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 the use of tunneling protocols, such as IPsec, because NAT modifies values in the headers, causing integrity checks to fail.

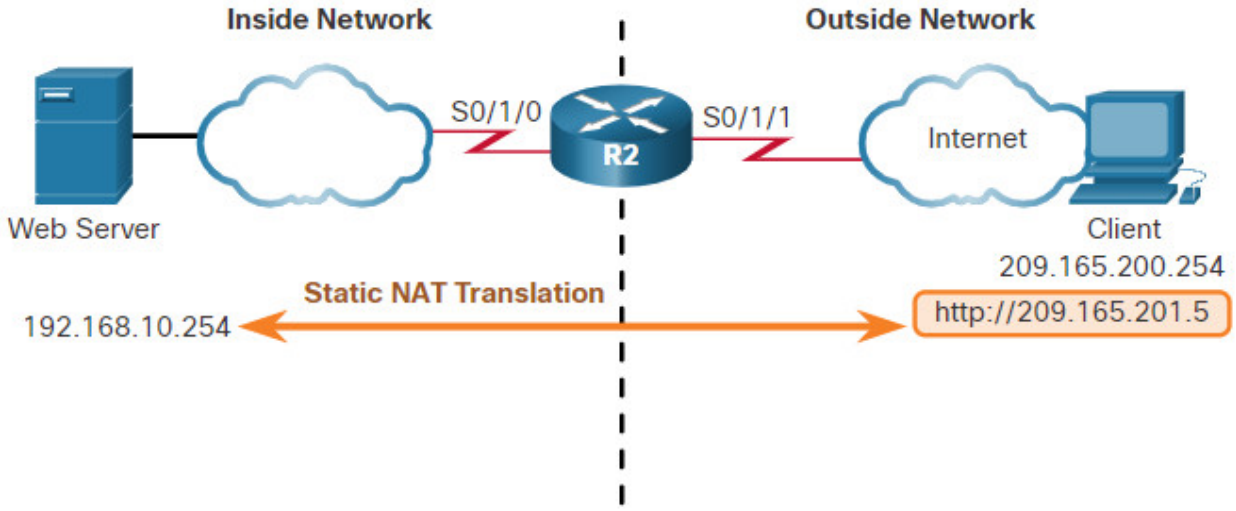
Services that require the initiation of TCP connections from the outside network, or stateless protocols, such as those using UDP, can be disrupted. Unless the NAT router has been configured to support such protocols, incoming packets cannot reach their destination. Some protocols can accommodate one instance of NAT between participating hosts (passive mode FTP, for example), but fail when both systems are separated from the internet by NAT.

6.4. Static NAT

6.4.1. Static NAT Scenario

In this topic, you will learn how to configure and verify static NAT. It includes a Packet Tracer activity to test your skills and knowledge. 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.

The figure 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.



6.4.2. Configure Static NAT

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 the figure are configured as a static NAT translation.

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
```

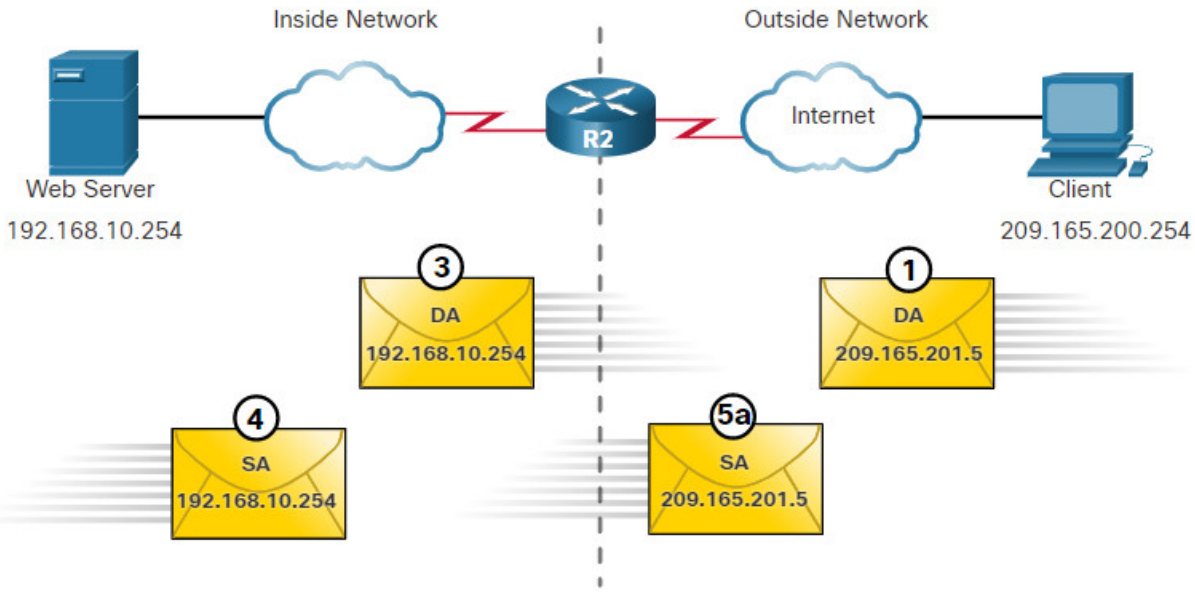
Step 2. After the mapping is configured, the interfaces participating in the translation are configured as inside or outside relative to NAT. In the example, the R2 Serial 0/1/0 interface is an inside interface and Serial 0/1/1 is an outside interface.

```
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

With this configuration in place, packets arriving on the inside interface of R2 (Serial 0/1/0) 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 0/1/1), 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.

6.4.3. Analyze Static NAT

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.



	Inside Local Address	Inside Global Address	Outside Local Address	Outside Global Address
2 5b	192.168.10.254	209.165.201.5	209.165.200.254	209.165.200.254

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 of 209.165.201.5 is located in the NAT table and is translated to 192.168.10.254.
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 as the source address of the response packet.
5. (a) 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.
   (b) 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 192.168.10.254 to the inside global address of 209.165.201.5 and forwards the packet toward the client.
6. (Not shown) The client receives the packet and continues the conversation. The NAT router performs Steps 2 to 5b for each packet.

6.4.4. Verify Static NAT

To verify NAT operation, issue the **show ip nat translations** command. This command shows active NAT translations. Because the example is a static NAT configuration, the translation is always present in the NAT table regardless of any active communications.

```
R2# show ip nat translations
Pro  Inside global       Inside local       Outside local     Outside global
---  209.165.201.5       192.168.10.254     ---               ---
Total number of translations: 1
```

If the command is issued during an active session, the output also indicates the address of the outside device as shown in the following example.

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

Another useful command is **show ip nat statistics,** which 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.

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

After the client establishes a session with the web server, the **show ip nat statistics** displays an increase to four hits on the inside (Serial0/1/0) interface. This verifies that the static NAT translation is taking place on R2.

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

6.4.5. Packet Tracer – Configure Static NAT

In IPv4 configured networks, clients and servers use private addressing. Before packets with private addressing can cross the internet, they need to be translated to public addressing. Servers that are accessed from outside the organization are usually assigned both a public and a private static IPv4 address. In this activity, you will configure static NAT so that outside devices can access an inside server at its public address.

In this Packet Tracer activity, you will:

- Test Access without NAT
- Configure Static NAT
- Test Access with NAT

6.4.5 Packet Tracer – Configure Static NAT

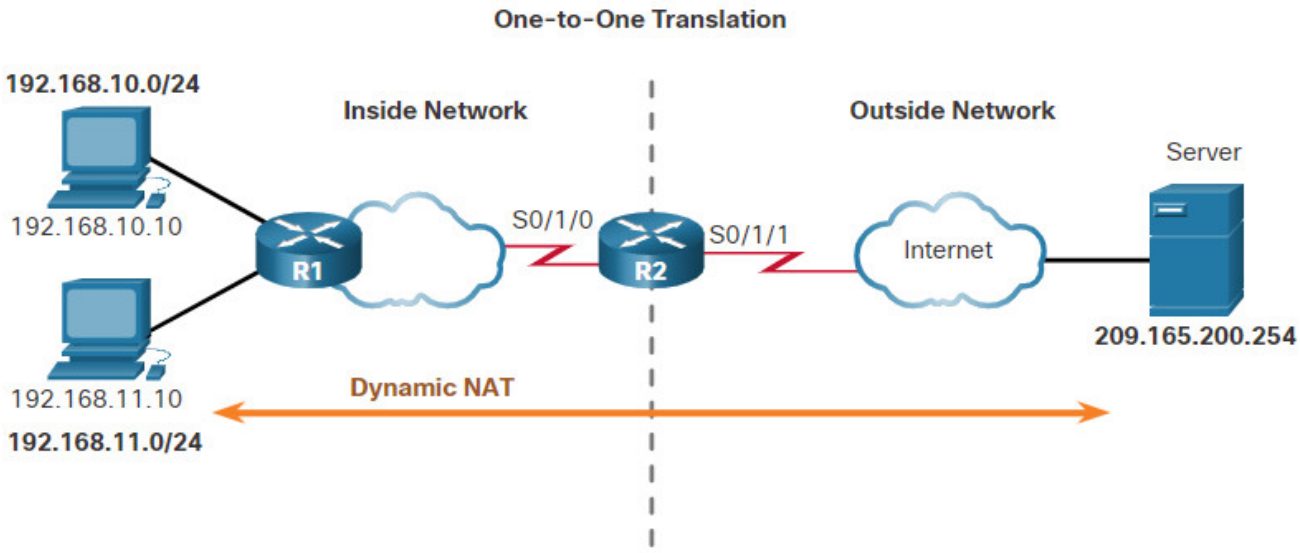
6.5. Dynamic NAT

6.5.1. Dynamic NAT Scenario

In this topic, you will learn how to configure and verify dynamic NAT. It includes a Packet Tracer activity to test your skills and knowledge. Although static NAT provides a permanent mapping between an inside local address and an inside global address, dynamic NAT automatically maps inside local addresses to inside global addresses. These inside global addresses are typically public IPv4 addresses. Dynamic NAT, like static NAT, requires the

configuration of the inside and outside interfaces participating in NAT with the **ip nat inside** and **ip nat outside** interface configuration commands. However, where static NAT creates a permanent mapping to a single address, dynamic NAT uses a pool of addresses.

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.

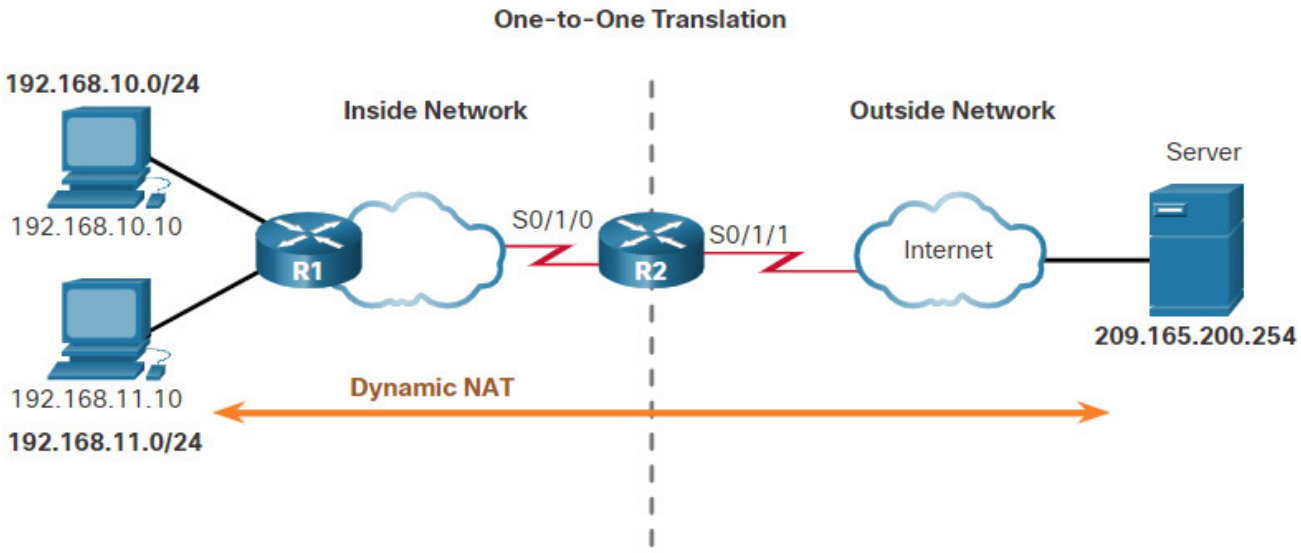


The pool of public IPv4 addresses (inside global address pool) is available to any device on the inside network on a first-come first-served basis. With dynamic NAT, a single inside address is translated to a single outside address. With this type of translation there must be enough addresses in the pool to accommodate all the inside devices needing concurrent access to the outside network. If all addresses in the pool are in use, 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 pair of IPv4 addresses.

6.5.2. Configure Dynamic NAT

The figure shows an example topology where the NAT configuration allows translation for all hosts on the 192.168.0.0/16 network. This includes the 192.168.10.0 and 192.168.11.0 LANs when the hosts generate traffic that enters interface S0/1/0 and exits S0/1/1. The host inside local addresses are translated to an available pool address in the range of 209.165.200.226 to209.165.200.240.



Click each button for a description and example of each step to configure static NAT.

- Step 1
- Step 2
- Step 3
- Step 4
- Step 5

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 IPv4 address and the ending IPv4 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 that range of addresses.

In the scenario, define 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
```

Step 5

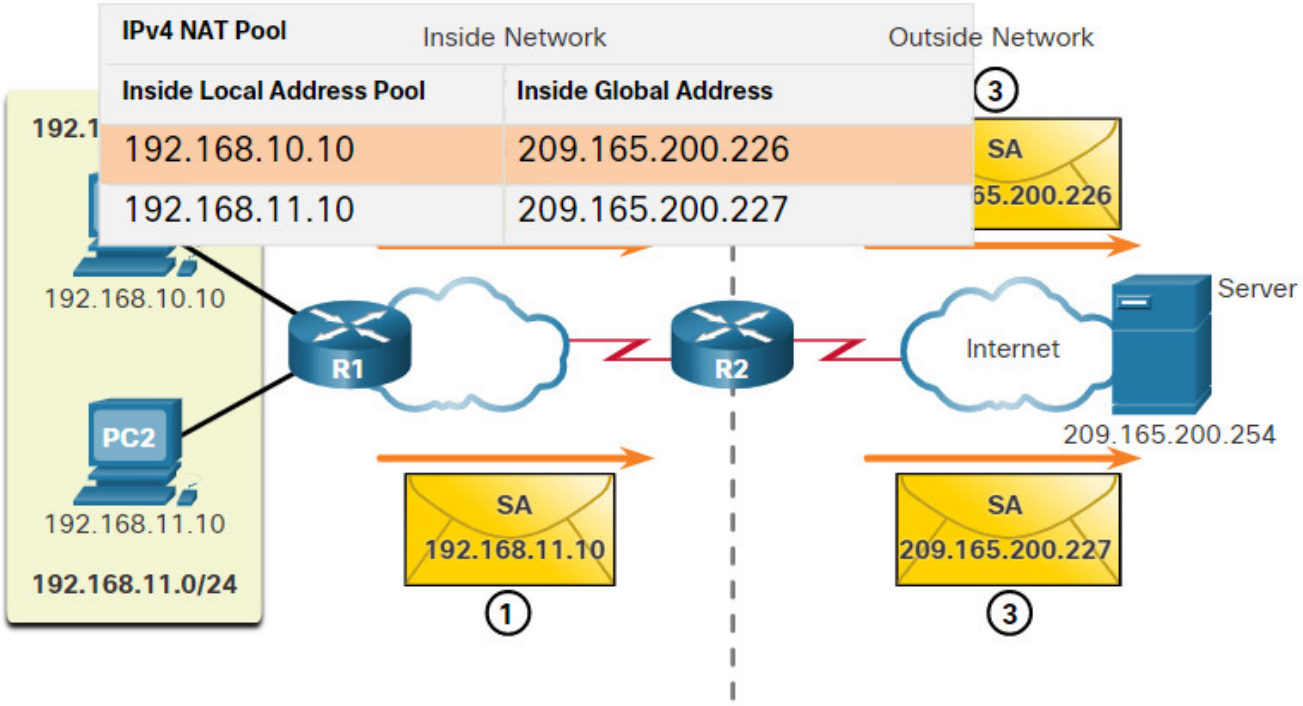
Identify which interfaces are outside, in relation to NAT; this will be any interface that connects to the outside network.

In the scenario, identify interface serial 0/1/1 as the outside NAT interface.

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

6.5.3. Analyze Dynamic NAT – Inside to Outside

Using the previous configuration, the next two figures illustrate the dynamic NAT translation process between two clients and the web server.



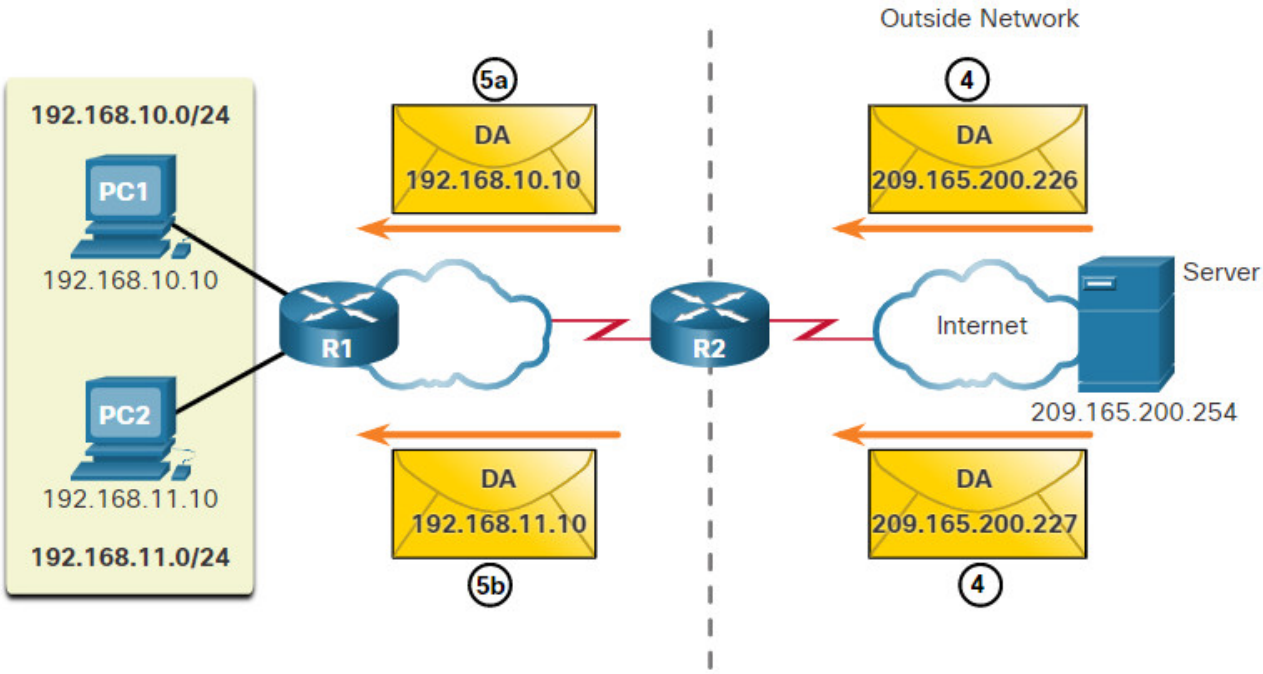
The figure below is used to illustrate the traffic flow from the inside network to the outside.

1. The hosts with the source IPv4 addresses of 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 current translation entry for this IPv4 address, R2 determines that the source address 192.168.10.10 must be translated. 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 of 209.165.200.227.

6.5.4. Analyze Dynamic NAT – Outside to Inside

The figure below illustrates the remainder of the traffic flow between the clients and the server from the outside to the inside direction.



	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

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.
5. (a) 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.
   (b) 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.)

6.5.5. Verify Dynamic NAT

The output of the **show ip nat translations** command displays all static translations that have been configured and any dynamic translations that have been created by traffic.

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

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

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

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** privileged EXEC mode command as shown.

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

It is useful to clear the dynamic entries when testing the NAT configuration. The **clear ip nat translation** command can be used with keywords and variables to control which entries are cleared, as shown in the table. Specific entries can be cleared to avoid disrupting active sessions. Use the **clear ip nat translation** * privileged EXEC command to clear all translations from the table.

Command	Description

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]`	Clears 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.

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

Another useful command, **show ip nat statistics**, 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.

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

Alternatively, you can 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. The example shows the NAT pool configuration.

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

6.5.6. Packet Tracer – Configure Dynamic NAT

In this Packet Tracer, you will complete the following objectives:

- Configure Dynamic NAT
- Verify NAT Implementation

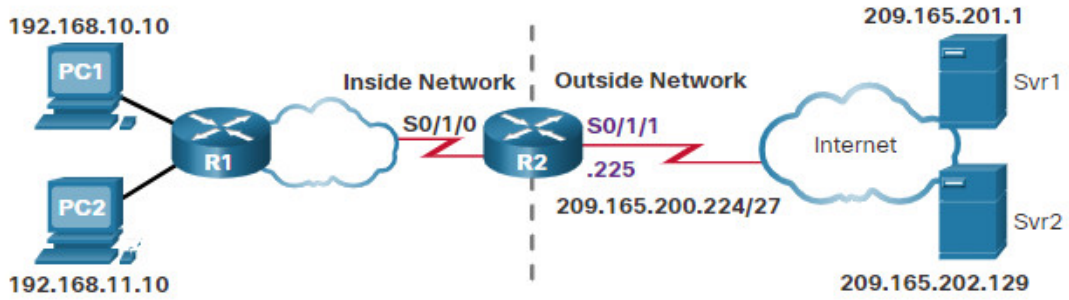
6.5.6 Packet Tracer – Configure Dynamic NAT

6.6. PAT

6.6.1. PAT Scenario

In this topic, you will learn how to configure and verify PAT. It includes a Packet Tracer activity to test your skills and knowledge. There are two ways to configure PAT, depending on how the ISP allocates public IPv4 addresses. In the first instance, the ISP allocates a single public IPv4 address that is required for the organization to connect to the ISP and in the other, it allocates more than one public IPv4 address to the organization.

Both methods will be demonstrated using the scenario shown in the figure.



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
192.168.11.10:1444	209.165.200.225:1445	209.165.202.129:80	209.165.202.129:80

6.6.2. Configure PAT to Use a Single IPv4 Address

To configure PAT to use a single IPv4 address, simply add the keyword **overload** to the **ip nat inside source** command. The rest of the configuration is the similar to static and dynamic NAT configuration except that with PAT, multiple hosts can use the same public IPv4 address to access the internet.

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 S0/1/1). The traffic flows will be identified by port numbers in the NAT table because the **overload** keyword is configured.

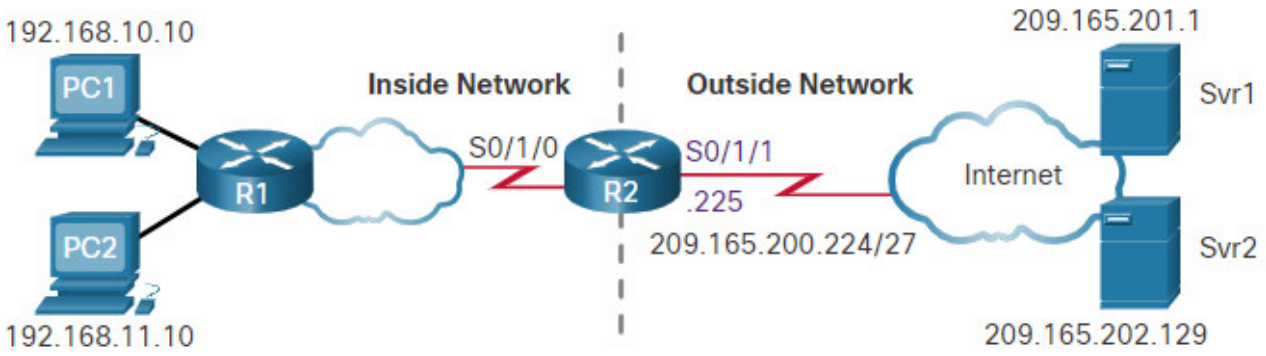
```
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface Serial0/1/1
R2(config-if)# ip nat outside
```

6.6.3. Configure PAT to Use an Address Pool

An ISP may allocate more than one public IPv4 address to an organization. In this scenario the organization can configure PAT to use a pool of IPv4 public addresses for translation.

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. The small pool of addresses is shared among a larger number of devices, with multiple hosts using the same public IPv4 address to access the internet. To configure PAT for a dynamic NAT address pool, simply add the keyword **overload** to the **ip nat inside source** command.

The topology for this scenario is repeated in the figure for your convenience.

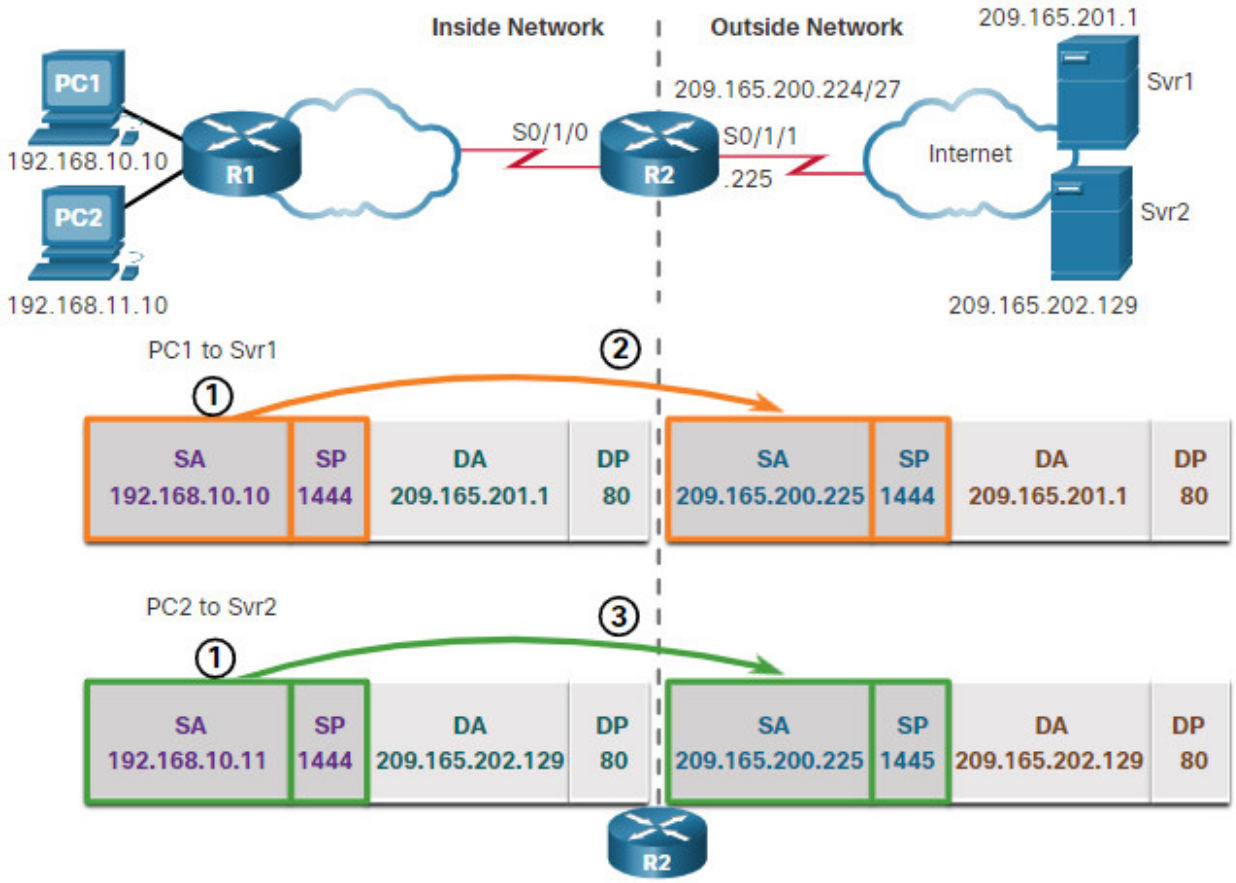


In the example, NAT-POOL2 is bound to an ACL to permit 192.168.0.0/16 to be translated. These hosts can share an IPv4 address from the pool because PAT is enabled with the keyword **overload**.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask
255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)# interface serial0/1/0
R2(config-if)# ip nat inside
R2(config)# interface serial0/1/0
R2(config-if)# ip nat outside
```

6.6.4. Analyze PAT – PC to Server

The process of NAT overload is the same whether a pool of addresses is used, or a single address is used. In this figure, PAT is configured to use a single public IPv4 address, instead of a pool of addresses. 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.



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
192.168.10.10:1444	209.165.200.225:1445	209.165.201.129:80	209.165.201.129:80

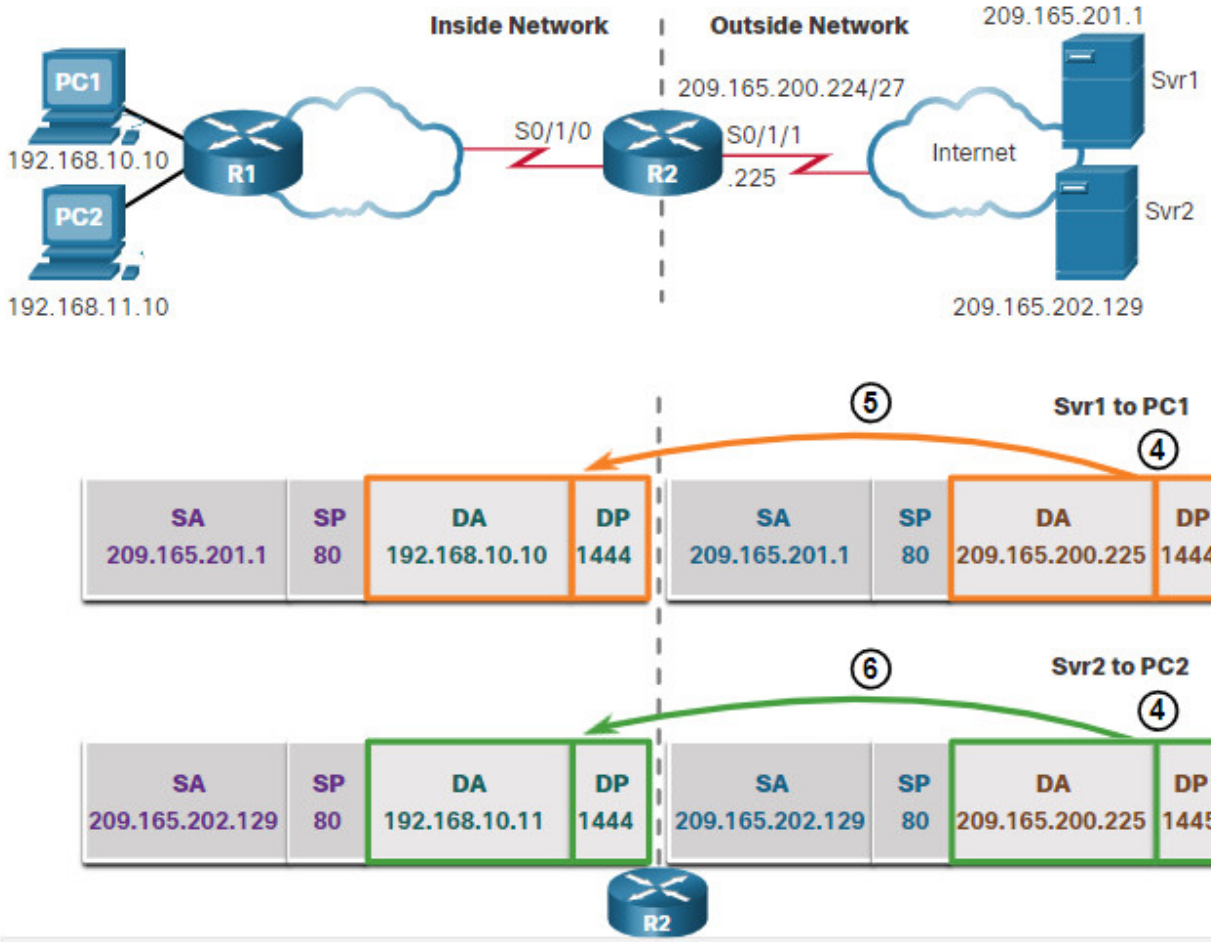
In the figure, the following steps are shown:

1. Both PC1 and PC2 are 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 coincidentally uses the same TCP 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 the source IPv4 address of PC2 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.

6.6.5. Analyze PAT – Server to PC

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, as shown in the figure.



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	209.165.201.129:80	209.165.202.129:80

In this second figure, the steps from the servers to the PCs are as follows:

4. 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.

6.6.6. Verify PAT

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 the example output. 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.

```
R2# show ip nat translations
Pro Inside global          Inside local         Outside local      Outside global
tcp 209.165.200.225:1444  192.168.10.10:1444  209.165.201.1:80   209.165.201.1:80
tcp 209.165.200.225:1445  192.168.11.10:1444  209.165.202.129:80 209.165.202.129:80
R2#
```

In the next example, 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.

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

6.6.7. Packet Tracer – Configure PAT

In this Packet Tracer, you will complete the following objectives:

- Part 1: Configure Dynamic NAT with Overload
- Part 2: Verify Dynamic NAT with Overload Implementation
- Part 3: Configure PAT using an Interface
- Part 4: Verify PAT Interface Implementation

6.6.7 Packet Tracer – Configure PAT

6.7. NAT64

6.7.1. NAT for IPv6?

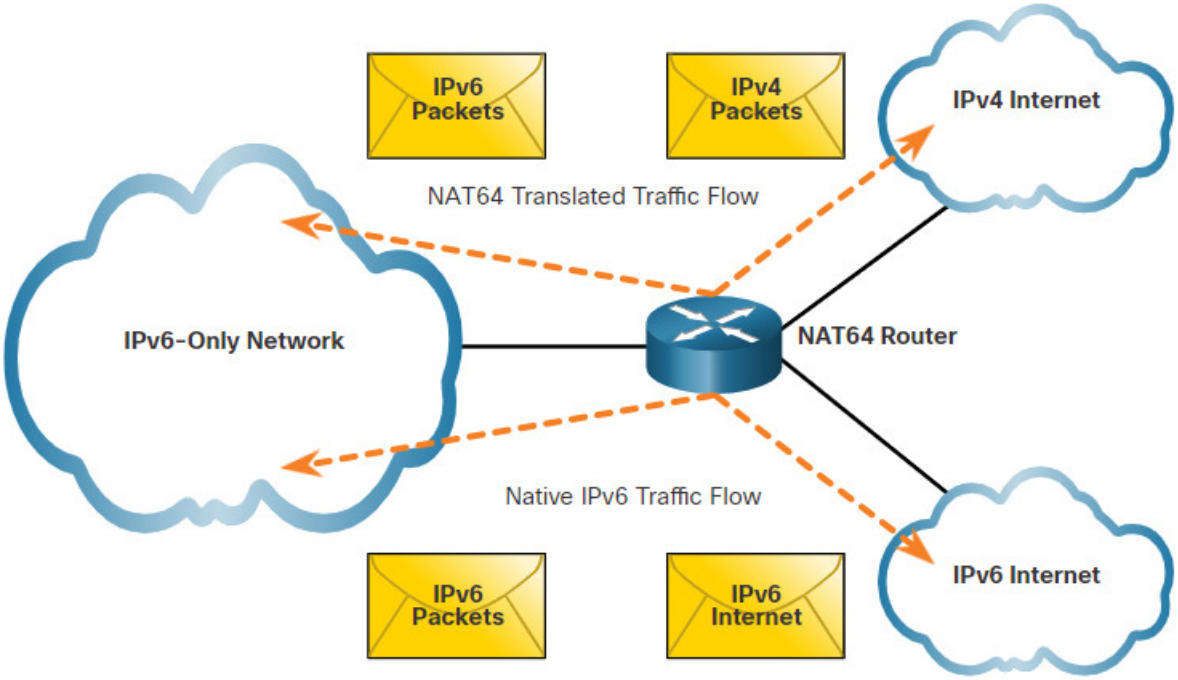
Because many networks use both IPv4 and IPv6, there needs to be a way to use IPv6 with NAT. This topic discusses how IPv6 can be integrated with NAT. IPv6, with a 128-bit address, provides 340 undecillion addresses. Therefore, address space is not an issue. IPv6 was developed with the intention of making NAT for IPv4 with translation between public and private IPv4 addresses unnecessary. However, IPv6 does include its own IPv6 private address space, unique local addresses (ULAs).

IPv6 unique local addresses (ULA) are similar to RFC 1918 private addresses in IPv4 but have a different purpose. ULA addresses are meant for only local communications within a site. ULA addresses are not meant to provide additional IPv6 address space, nor to provide a level of security.

IPv6 does provide for protocol translation between IPv4 and IPv6 known as NAT64.

6.7.2. 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, as shown in the figure. 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 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.

6.8. Module Practice and Quiz

6.8.1. Packet Tracer – Configure NAT for IPv4

In this Packet Tracer, you will complete the following objectives:

- Configure Dynamic NAT with PAT
- Configure Static NAT

6.8.1 Packet Tracer – Configure NAT for IPv4

6.8.2. Lab – Configure NAT for IPv4

In this lab, you will complete the following objectives:

- Part 1: Build the Network and Configure Basic Device Settings
- Part 2: Configure and verify NAT for IPv4
- Part 3: Configure and verify PAT for IPv4
- Part 4: Configure and verify Static NAT for IPv4

6.8.2 Lab – Configure NAT for IPv4

6.8.3. What did I learn in this module?

NAT Characteristics

There are not enough public IPv4 addresses to assign a unique address to each device connected to the internet. 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 provides the translation of private addresses to public addresses. The primary use of NAT is to conserve public IPv4 addresses. It allows networks to use private IPv4 addresses internally and provides translation to a public address only when needed. 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. 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 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.

Types of 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. 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. Static NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions. 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. Similar to static NAT, dynamic NAT requires that enough public addresses are available to satisfy the total number of simultaneous user sessions. Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses. This is the most common form of NAT for both the home and the enterprise. PAT ensures that devices use a different TCP port number for each session with a server on the internet. 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. 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.

NAT	PAT
One-to-one mapping between Inside Local and Inside Global addresses.	One Inside Global address can be mapped to many Inside Local address.
Uses only IPv4 addresses in translation process.	Uses IPv4 addresses and TCP or UDP source port numbers in translation process.
A unique Inside Global address is required for each inside host accessing the outside network.	A single unique Inside Global address can be shared by many inside hosts accessing the outside network.

NAT Advantages and Disadvantages

Advantages: NAT conserves the legally registered addressing scheme by allowing the privatization of intranets. NAT increases the flexibility of connections to the public network. NAT provides consistency for internal network addressing schemes. NAT hides user IPv4 addresses.

Disadvantages: NAT increases forwarding delays because the translation of each IPv4 address within the packet headers takes time. The process of two layers of NAT translation is known as Carrier Grade NAT (CGN). End-to-end addressing is lost. Many internet protocols and applications depend on end-to-end addressing from the source to the destination. End-to-end IPv4 traceability is also lost. Using NAT also complicates the use of tunneling protocols, such as IPsec, because NAT modifies values in the headers, causing integrity checks to fail.

Static NAT

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. The first task is to create a mapping between the inside local address

and the inside global addresses using the **ip nat inside source static** command. After the mapping is configured, the interfaces participating in the translation are configured as inside or outside relative to NAT using the **ip nat inside** and **ip nat outside** commands. To verify NAT operation use the **show ip nat translations** command. 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.

Dynamic NAT

Dynamic NAT automatically maps the inside local addresses to inside global addresses. Dynamic NAT, like static NAT, requires the configuration of the inside and outside interfaces participating in NAT. Dynamic NAT uses a pool of addresses translating a single inside address to a single outside address. 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 this type of translation there must be enough addresses in the pool to accommodate all the inside devices needing concurrent access to the outside network. If all addresses in the pool are in use, a device must wait for an available address before it can access the outside network.

To configure dynamic NAT, first define the pool of addresses that will be used for translation using the **ip nat pool** command. The addresses are defined by indicating the starting IPv4 address and the ending IPv4 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. Configure a standard ACL to identify (permit) only those addresses that are to be translated. Bind the ACL to the pool, using the following command syntax: Router(config)# **ip nat inside source list** {*access-list-number* | *access-list-name*} **pool** *pool-name*. Identify which interfaces are inside, in relation to NAT. Identify which interfaces are outside, in relation to NAT.

To verify dynamic NAT configurations, The output of the **show ip nat translations** command shown 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. 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** privileged EXEC mode command.

PAT

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

IPv4 address to the organization. To configure PAT to use a single IPv4 address, simply add the keyword **overload** to the **ip nat inside source** command. The rest of the configuration is the similar to static and dynamic NAT configuration except that with PAT, multiple hosts can use the same public IPv4 address to access the internet. To configure PAT for a dynamic NAT address pool, simply add the keyword **overload** to the **ip nat inside source** command. Multiple hosts can share an IPv4 address from the pool because PAT is enabled with the keyword **overload**.

To verify PAT configurations us the **show ip nat translations** command. The source port numbers in the NAT table differentiate the transactions. The **show ip nat statistics** command verifies that the NAT-POOL has allocated a single address for multiple 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.

NAT64

IPv6 was developed with the intention of making NAT for IPv4 with translation between public and private IPv4 addresses unnecessary. However, IPv6 does include its own IPv6 private address space, unique local addresses (ULAs). IPv6 unique local addresses (ULA) are similar to RFC 1918 private addresses in IPv4 but have a different purpose. ULA addresses are meant for only local communications within a site. ULA addresses are not meant to provide additional IPv6 address space, nor to provide a level of security; however, IPv6 does provide for protocol translation between IPv4 and IPv6 known as 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. 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.

6.8.4 Module Quiz – NAT for IPv4

Download Slide Powerpoint (PPT)

CCNA 3 v7.0 Curriculum: Module 6 - NAT for IPv4.pptx

1 file(s) 1.89 MB

Download

Tags:ccna 3 v7 modules