



Configuring Static and Dynamic NAT Translation

This chapter contains the following sections:

- [Network Address Translation Overview, on page 1](#)
- [Information About Static NAT, on page 1](#)
- [Static Twice NAT Overview, on page 3](#)
- [Dynamic NAT Overview, on page 3](#)
- [NAT Inside and Outside Addresses, on page 4](#)
- [Licensing Requirements for Static NAT, on page 4](#)
- [Guidelines and Limitations for Static NAT, on page 5](#)
- [Restrictions for Dynamic NAT, on page 5](#)
- [Configuring Static NAT, on page 6](#)
- [Configuring Dynamic NAT, on page 14](#)

Network Address Translation Overview

Network Address Translation (NAT) enables private IP internetworks that use nonregistered IP addresses to connect to the Internet. NAT operates on a device, usually connecting two networks, and translates private (not globally unique) IP addresses in the internal network into legal IP addresses before packets are forwarded to another network. You can configure NAT to advertise only one IP address for the entire network to the outside world. This ability provides additional security, effectively hiding the entire internal network behind one IP address.

A device configured with NAT has at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit router between a stub domain and a backbone. When a packet leaves the domain, NAT translates the locally significant source IP address into a globally unique IP address. When a packet enters the domain, NAT translates the globally unique destination IP address into a local IP address. If more than one exit point exists, NAT configured at each point must have the same translation table.

NAT is described in RFC 1631.

Information About Static NAT

Static Network Address Translation (NAT) allows the user to configure one-to-one translations of the inside local addresses to the outside global addresses. It allows both IP addresses and port number translations from

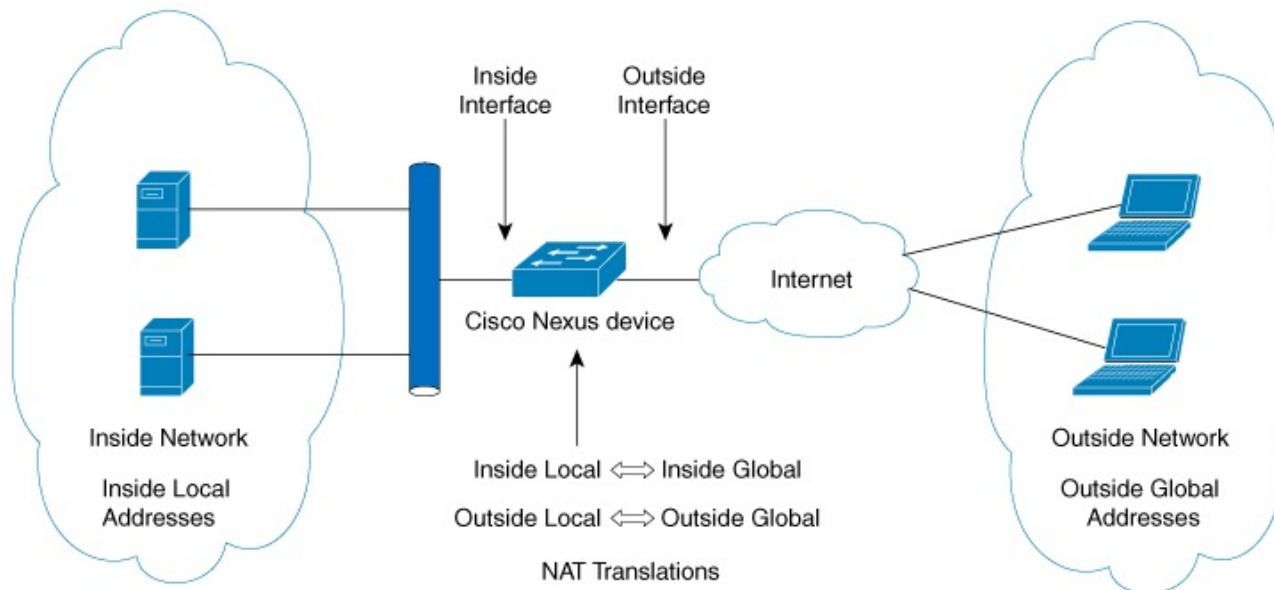
the inside to the outside traffic and the outside to the inside traffic. The Cisco Nexus device supports Hitless NAT, which means that you can add or remove a NAT translation in the NAT configuration without affecting the existing NAT traffic flows.

Static NAT creates a fixed translation of private addresses to public addresses. Because static NAT assigns addresses on a one-to-one basis, you need an equal number of public addresses as private addresses. Because the public address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT enables hosts on the destination network to initiate traffic to a translated host if an access list exists that allows it.

With dynamic NAT and Port Address Translation (PAT), each host uses a different address or port for each subsequent translation. The main difference between dynamic NAT and static NAT is that static NAT allows a remote host to initiate a connection to a translated host if an access list exists that allows it, while dynamic NAT does not.

The figure shows a typical static NAT scenario. The translation is always active so both translated and remote hosts can originate connections, and the mapped address is statically assigned by the **static** command.

Figure 1: Static NAT



These are key terms to help you understand static NAT:

- NAT inside interface—The Layer 3 interface that faces the private network.
- NAT outside interface—The Layer 3 interface that faces the public network.
- Local address—Any address that appears on the inside (private) portion of the network.
- Global address—Any address that appears on the outside (public) portion of the network.
- Legitimate IP address—An address that is assigned by the Network Information Center (NIC) or service provider.
- Inside local address—The IP address assigned to a host on the inside network. This address does not need to be a legitimate IP address.

- Outside local address—The IP address of an outside host as it appears to the inside network. It does not have to be a legitimate address, because it is allocated from an address space that can be routed on the inside network.
- Inside global address—A legitimate IP address that represents one or more inside local IP addresses to the outside world.
- Outside global address—The IP address that the host owner assigns to a host on the outside network. The address is a legitimate address that is allocated from an address or network space that can be routed.

Static Twice NAT Overview

When both the source IP address and the destination IP address are translated as a single packet that goes through a Network Address Translation (NAT) device, it is referred to as twice NAT. Twice NAT is supported only for static translations.

Twice NAT allows you to configure two NAT translations (one inside and one outside) as part of a group of translations. These translations can be applied to a single packet as it flows through a NAT device. When you add two translations as part of a group, both the individual translations and the combined translation take effect.

A NAT inside translation modifies the source IP address and port number when a packet flows from inside to outside. It modifies the destination IP address and port number when the packet returns from outside to inside. NAT outside translation modifies the source IP address and port number when the packet flows from outside to inside, and it modifies the destination IP address and port number when the packet returns from inside to outside.

Without twice NAT, only one of the translation rules is applied on a packet, either the source IP address and port number or the destination IP address and port number.

Static NAT translations that belong to the same group are considered for twice NAT configuration. If a static configuration does not have a configured group ID, the twice NAT configuration will not work. All inside and outside NAT translations that belong to a single group that is identified by the group ID are paired to form twice NAT translations.

Dynamic NAT Overview

Dynamic Network Address Translation (NAT) translates a group of real IP addresses into mapped IP addresses that are routable on a destination network. Dynamic NAT establishes a one-to-one mapping between unregistered and registered IP addresses; however, the mapping can vary depending on the registered IP address that is available at the time of communication.

A dynamic NAT configuration automatically creates a firewall between your internal network and outside networks or the Internet. Dynamic NAT allows only connections that originate inside the stub domain—a device on an external network cannot connect to devices in your network, unless your device has initiated the contact.

Dynamic NAT translations do not exist in the NAT translation table until a device receives traffic that requires translation. Dynamic translations are cleared or timed out when not in use to make space for new entries. Usually, NAT translation entries are cleared when the ternary content addressable memory (TCAM) entries are limited. The default minimum timeout for dynamic NAT translations is 30 minutes.

Dynamic NAT supports Port Address Translation (PAT) and access control lists (ACLs). PAT, also known as overloading, is a form of dynamic NAT that maps multiple unregistered IP addresses to a single registered IP address by using different ports. Your NAT configuration can have multiple dynamic NAT translations with same or different ACLs. However, for a given ACL, only one interface can be specified.

For aging, there are three different options that can be configured:

- 1-Time-out: This is applicable for all type of flows (both TCP and UDP)
- 2-TCP TIME-OUT: This is applicable for only TCP flows
- 3-UDP TIME-OUT: This is applicable for only UDP flows

NAT Inside and Outside Addresses

NAT inside refers to networks owned by an organization that must be translated. When NAT is configured, hosts within this network will have addresses in one space (known as the local address space) that will appear to those outside the network as being in another space (known as the global address space).

Similarly, NAT outside refers to those networks to which the stub network connects. They are not generally under the control of the organization. Hosts in outside networks can be subject to translation and can have local and global addresses.

NAT uses the following definitions:

- Local address—A local IP address that appears on the inside of a network.
- Global address—A global IP address that appears on the outside of a network.
- Inside local address—The IP address that is assigned to a host on the inside network. The address is probably not a legitimate IP address assigned by the Internet Network Information Center (InterNIC) or a service provider.
- Inside global address—A legitimate IP address (assigned by InterNIC or a service provider) that represents one or more inside local IP addresses to the outside world.
- Outside local address—The IP address of an outside host as it appears to the inside network. The address is not necessarily legitimate; it was allocated from the address space that is routable on the inside.
- Outside global address—The IP address that is assigned to a host on the outside network by the owner of the host. The address was allocated from a globally routable address or a network space.

Licensing Requirements for Static NAT

This table shows the licensing requirements for static NAT.

| Product | License Requirement |
|----------------|---------------------|
| Cisco NX-OS | |

Guidelines and Limitations for Static NAT

Static NAT has the following configuration guidelines and limitations:

- NAT supports up to 1024 translations which include both static and dynamic NAT.
- Cisco Nexus 3500 Series switches do not support static and dynamic NAT on vPC topology.
- The Cisco Nexus device supports NAT on the following interface types:
 - Switch Virtual Interfaces (SVIs)
 - Routed ports
- NAT is supported for IPv4 Unicast only.
- The Cisco Nexus device does not support the following:
 - Application layer translation. Layer 4 and other embedded IPs are not translated, including FTP, ICMP failures, IPsec, and HTTPs.
 - NAT and VLAN Access Control Lists (VACLs) that are configured on an interface at the same time.
 - PAT translation of fragmented IP packets.
 - NAT translation on software forwarded packets. For example, packets with IP-options are not NAT translated.
- Egress ACLs are applied to the original packets and not the NAT translated packets.
- HSRP and VRRP are not supported on a NAT interface.
- Warp mode latency performance is not supported on packets coming from the outside to the inside domain.
- If an IP address is used for Static NAT or PAT translations, it cannot be used for any other purpose. For example, it cannot be assigned to an interface.
- For Static NAT, the outside global IP address should be different from the outside interface IP address.
- Twice NAT is not supported. (Twice NAT is a variation of NAT in that both the source and destination addresses are modified by NAT as a datagram crosses address domains (inside to outside or outside to inside.)
- NAT statistics are not available.
- When configuring a large number of translations (more than 100), it is faster to configure the translations before configuring the NAT interfaces.

Restrictions for Dynamic NAT

The following restrictions apply to dynamic Network Address Translation (NAT):

- Fragmented packets are not supported.

- Application layer gateway (ALG) translations are not supported. ALG, also known as application-level gateway, is an application that translates IP address information inside the payload of an application packet.
- NAT and virtual access control lists (ACLs) are not supported together on an interface. You can configure either NAT or virtual ACL on an interface.
- Egress ACLs are not applied to translated packets.
- Nondefault virtual routing and forwarding (VRF) instances are not supported.
- MIBs are not supported.
- Cisco Data Center Network Manager (DCNM) is not supported.
- Multiple global virtual device contexts (VDCs) are not supported on Cisco Nexus devices.
- Dynamic NAT on traffic coming from outside domains is not supported.
- Dynamic NAT translations are not synchronized with active and standby devices.
- Stateful NAT is not supported. However, NAT and Hot Standby Router Protocol (HSRP) can coexist.
- When you configure dynamic NAT on a Layer 3 interface, after a reload or after you have cleared the NAT translations, the existing NAT translations are not learnt. Due to this, there is traffic drop for the access control list (ACL) that matches the NAT configuration. To avoid this, remove the NAT configuration and reconfigure it on the same interfaces so that NAT translations can be learnt.
- The timeout value for take up to the configured time-out + 119 seconds.

Configuring Static NAT

Enabling Static NAT

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# feature nat | Enables the static NAT feature on the device. |
| Step 3 | (Optional) switch(config)# copy running-config startup-config | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

Configuring Static NAT on an Interface

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# interface <i>type slot/port</i> | Specifies an interface to configure, and enters interface configuration mode. |
| Step 3 | switch(config-if)# ip nat {inside outside} | Specifies the interface as inside or outside. Note Only packets that arrive on a marked interface can be translated. |
| Step 4 | (Optional) switch(config)# copy running-config startup-config | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

Example

This example shows how to configure an interface with static NAT from the inside:

```
switch# configure terminal
switch(config)# interface ethernet 1/4
switch(config-if)# ip nat inside
```

Enabling Static NAT for an Inside Source Address

For inside source translation, the traffic flows from inside interface to the outside interface. NAT translates the inside local IP address to the inside global IP address. On the return traffic, the destination inside global IP address gets translated back to the inside local IP address.



Note When the Cisco Nexus device is configured to translate an inside source IP address (Src:ip1) to an outside source IP address (newSrc:ip2), the Cisco Nexus device implicitly adds a translation for an outside destination IP address (Dst: ip2) to an inside destination IP address (newDst: ip1).

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# ip nat inside source static <i>local-ip-address global-ip-address</i> | Configures static NAT to translate the inside global address to the inside local address or to translate the opposite (the inside local traffic to the inside global traffic). |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 3 | (Optional) switch(config)# copy running-config startup-config | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

Example

This example shows how to configure static NAT for an inside source address:

```
switch# configure terminal
switch(config)# ip nat inside source static 1.1.1.1 5.5.5.5
switch(config)# copy running-config startup-config
```

Enabling Static NAT for an Outside Source Address

For outside source translation, the traffic flows from the outside interface to the inside interface. NAT translates the outside global IP address to the outside local IP address. On the return traffic, the destination outside local IP address gets translated back to outside global IP address.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# ip nat outside source static <i>global-ip-address local-ip-address</i> [add-route] | Configures static NAT to translate the outside global address to the outside local address or to translate the opposite (the outside local traffic to the outside global traffic). When an inside translation without ports is configured, an implicit add route is performed. The original add route functionality is an option while configuring an outside translation. |
| Step 3 | (Optional) switch(config)# copy running-config startup-config | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

Example

This example show how to configure static NAT for an outside source address:

```
switch# configure terminal
switch(config)# ip nat outside source static 2.2.2.2 6.6.6.6
switch(config)# copy running-config startup-config
```

Configuring Static PAT for an Inside Source Address

You can map services to specific inside hosts using Port Address Translation (PAT).

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# ip nat inside source static <i>{inside-local-address outside-local-address {tcp udp} inside-local-address {local-tcp-port local-udp-port} inside-global-address {global-tcp-port global-udp-port}}</i> | Maps static NAT to an inside local port to an inside global port. |
| Step 3 | (Optional) switch(config)# copy running-config startup-config | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

Example

This example shows how to map UDP services to a specific inside source address and UDP port:

```
switch# configure terminal
switch(config)# ip nat inside source static udp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

Configuring Static PAT for an Outside Source Address

You can map services to specific outside hosts using Port Address Translation (PAT).

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# ip nat outside source static <i>{outside-global-address outside-local-address {tcp udp} outside-global-address {global-tcp-port global-udp-port} outside-local-address {global-tcp-port global-udp-port}}</i> | Maps static NAT to an outside global port to an outside local port. |
| Step 3 | (Optional) switch(config)# copy running-config startup-config | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

Example

This example shows how to map TCP services to a specific outside source address and TCP port:

```
switch# configure terminal
switch(config)# ip nat outside source static tcp 20.1.9.2 63 35.48.35.48 130
switch(config)# copy running-config startup-config
```

Configuring Static Twice NAT

All translations within the same group are considered for creating static twice Network Address Translation (NAT) rules.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: <code>Switch> enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: <code>Switch# configure terminal</code> | Enters privileged EXEC mode. |
| Step 3 | ip nat inside source static <i>inside-local-ip-address</i> <i>outside-global-ip-address</i> [group <i>group-id</i>] Example: <code>Switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4</code> | Configures static twice NAT to translate an inside global address to an inside local address or to translate inside local traffic to inside global traffic. <ul style="list-style-type: none">• The group keyword determines the group to which a translation belongs. |
| Step 4 | ip nat outside source static <i>inside-local-ip-address</i> <i>outside-global-ip-address</i> [group <i>group-id</i>] [add-route] Example: <code>Switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4 add-route</code> | Configures static twice NAT to translate an outside global address to an inside local address or to translate inside local traffic to inside global traffic. <ul style="list-style-type: none">• The group keyword determines the group to which a translation belongs. |
| Step 5 | interface type number Example: <code>Switch(config)# interface ethernet 1/2</code> | Configures an interface and enters interface configuration mode. |
| Step 6 | ip address ip-address mask Example: <code>Switch(config-if)# ip address 10.2.4.1 255.255.255.0</code> | Sets a primary IP address for an interface. |
| Step 7 | ip nat {inside outside} Example: <code>Switch(config-if)# ip nat inside</code> | Connects the interface to an inside network, which is subject to NAT. |
| Step 8 | end Example: | Exits interface configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|--|--------------------------------------|---------|
| | <code>Switch(config-if) # end</code> | |

Configuring Static Twice NAT for an Outside Source Address

All translations within the same group are considered for creating the static Twice Network Address Translation (NAT) rules. You can use all combinations for inside and outside NAT translation as Twice NAT rules.

Procedure

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <code>switch> enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <code>switch# configure terminal</code> | Enters privileged EXEC mode. |
| Step 3 | ip nat outside source static <i>local-ip-address</i> <i>global-ip-address</i> [group <i>group-id</i>] Example: <code>switch(config) # ip nat outside source static 10.1.1.1 192.168.34.4 group 4</code> | Configures static twice NAT to translate the inside global address to the inside local address or to translate the outside local traffic to the outside global traffic. <ul style="list-style-type: none"> • The group keyword determines the group to which a translation belongs. |
| Step 4 | interface <i>type number</i> Example: <code>switch(config) # interface ethernet 1/2</code> | Configures an interface and enters interface configuration mode. |
| Step 5 | ip address <i>ip-address mask</i> Example: <code>switch(config-if) # ip address 10.2.4.1 255.255.255.0</code> | Sets a primary IP address for the interface. |
| Step 6 | ip nat {inside outside} Example: <code>switch(config-if) # ip nat outside</code> | Connects the interface to the inside network, which is subject to NAT. |
| Step 7 | end Example: <code>switch(config-if) # end</code> | Exits interface configuration mode and returns to privileged EXEC mode. |

Configuring the NAT Limit

To configure the NAT limit to a specific value, the VACL region of the TCAMs in all of the ASICs cannot have any VACLs configured below that value. For example, to configure the NAT limit to 400 the VACL region of the TCAMs in all of the ASICs cannot have any VACL configured below offset 400. If there are any VACLs below the NAT limit, the command checks if all current VACLs can be accommodated with the NAT limit upon switch reload. If the command completes, you are asked to reload the switch.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | switch# configure terminal | Enters global configuration mode. |
| Step 2 | switch(config)# hardware profile tcam feature nat limit <i>tcam-size</i> | Configures the NAT TCAM limit. The valid range of <i>tcam-size</i> is from 2 to 2048. |
| Step 3 | switch(config)# show hardware profile tcam feature nat limit | Displays the NAT limit. |
| Step 4 | (Optional) switch(config)# copy running-config startup-config | Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration. |

Example

The following example shows how to configure the NAT limit to 400.

```
switch# configure terminal
switch(config)# hardware profile tcam feature nat limit 400
switch(config)# show hardware profile tcam feature nat limit
switch(config)# copy running-config startup-config
```

Configuration Example for Static NAT and PAT

This example shows the configuration for static NAT:

```
ip nat inside source static 103.1.1.1 11.3.1.1
ip nat inside source static 139.1.1.1 11.39.1.1
ip nat inside source static 141.1.1.1 11.41.1.1
ip nat inside source static 149.1.1.1 95.1.1.1
ip nat inside source static 149.2.1.1 96.1.1.1
ip nat outside source static 95.3.1.1 95.4.1.1
ip nat outside source static 96.3.1.1 96.4.1.1
ip nat outside source static 102.1.2.1 51.1.2.1
ip nat outside source static 104.1.1.1 51.3.1.1
ip nat outside source static 140.1.1.1 51.40.1.1
```

This example shows the configuration for static PAT:

```
ip nat inside source static tcp 10.11.1.1 1 210.11.1.1 101
ip nat inside source static tcp 10.11.1.1 2 210.11.1.1 201
ip nat inside source static tcp 10.11.1.1 3 210.11.1.1 301
ip nat inside source static tcp 10.11.1.1 4 210.11.1.1 401
```

```
ip nat inside source static tcp 10.11.1.1 5 210.11.1.1 501
ip nat inside source static tcp 10.11.1.1 6 210.11.1.1 601
ip nat inside source static tcp 10.11.1.1 7 210.11.1.1 701
ip nat inside source static tcp 10.11.1.1 8 210.11.1.1 801
ip nat inside source static tcp 10.11.1.1 9 210.11.1.1 901
ip nat inside source static tcp 10.11.1.1 10 210.11.1.1 1001
ip nat inside source static tcp 10.11.1.1 11 210.11.1.1 1101
ip nat inside source static tcp 10.11.1.1 12 210.11.1.1 1201
```

Example: Configuring Static Twice NAT

The following example shows how to configure the inside source and outside source static twice NAT configurations:

```
Switch> enable
Switch# configure terminal
Switch(config)# ip nat inside source static 10.1.1.1 192.168.34.4 group 4
Switch(config)# ip nat outside source static 209.165.201.1 10.3.2.42 group 4
Switch(config)# interface ethernet 1/2
Switch(config-if)# ip address 10.2.4.1 255.255.255.0
Switch(config-if)# ip nat inside
Switch(config-if)# end
```

Example: Configuring Static Twice NAT for an Outside Source Address

This example shows how to configure static twice NAT for outside local IP address 10.1.1.2 and outside global IP address 192.168.34.4:

```
switch> enable
switch# configure terminal
switch(config)# ip nat outside source static 10.1.1.2 192.168.34.4 group 4
switch(config)# interface ethernet 1/2
switch(config-if)# ip address 10.2.4.1 255.255.255.0
switch(config-if)# ip nat outside
switch(config-if)# end
```

Verifying the Static NAT Configuration

To display the static NAT configuration, perform this task:

Procedure

| | Command or Action | Purpose |
|---------------|----------------------------------|---|
| Step 1 | switch# show ip nat translations | Shows the translations for the inside global, inside local, outside local, and outside global IP addresses. |

Example

This example shows how to display the static NAT configuration:

```

switch# sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- ---
--- ---                ---                51.3.1.1           104.1.1.1
--- ---                ---                95.4.1.1           95.3.1.1
--- ---                ---                96.4.1.1           96.3.1.1
--- ---                ---                51.40.1.1          140.1.1.1
--- ---                ---                51.42.1.1          142.1.2.1
--- ---                ---                51.1.2.1           102.1.2.1
--- 11.1.1.1           101.1.1.1         ---                ---
--- 11.3.1.1           103.1.1.1         ---                ---
--- 11.39.1.1          139.1.1.1         ---                ---
--- 11.41.1.1          141.1.1.1         ---                ---
--- 95.1.1.1           149.1.1.1         ---                ---
--- 96.1.1.1           149.2.1.1         ---                ---
    130.1.1.1:590      30.1.1.100:5000    ---                ---
    130.2.1.1:590      30.2.1.100:5000    ---                ---
    130.3.1.1:590      30.3.1.100:5000    ---                ---
    130.4.1.1:590      30.4.1.100:5000    ---                ---
    130.1.1.1:591      30.1.1.101:5000    ---                ---

```

Configuring Dynamic NAT

Configuring Dynamic Translation and Translation Timeouts

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Switch> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Switch# configure terminal | Enters global configuration mode. |
| Step 3 | ip access-list <i>access-list-name</i> Example: Switch(config)# ip access-list acl1 | Defines an access list and enters access-list configuration mode. |
| Step 4 | permit <i>protocol source source-wildcard any</i> Example: Switch(config-acl)# permit ip 10.111.11.0/24 any | Sets conditions in an IP access list that permit traffic matching the conditions. |
| Step 5 | deny <i>protocol source source-wildcard any</i> Example: | Sets conditions in an IP access list that deny packets from entering a network. |

| | Command or Action | Purpose |
|----------------|---|---|
| | Switch(config-acl)# deny udp 10.111.11.100/32 any | |
| Step 6 | exit Example: Switch(config-acl)# exit | Exits access-list configuration mode and returns to global configuration mode. |
| Step 7 | ip nat inside source list <i>access-list-name</i> interface <i>type number</i> overload Example: Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload | Establishes dynamic source translation by specifying the access list defined in Step 3. |
| Step 8 | interface <i>type number</i> Example: Switch(config)# interface ethernet 1/4 | Configures an interface and enters interface configuration mode. |
| Step 9 | ip address <i>ip-address mask</i> Example: Switch(config-if)# ip address 10.111.11.39 255.255.255.0 | Sets a primary IP address for the interface. |
| Step 10 | ip nat inside Example: Switch(config-if)# ip nat inside | Connects the interface to an inside network, which is subject to NAT. |
| Step 11 | exit Example: Switch(config-if)# exit | Exits interface configuration mode and returns to global configuration mode. |
| Step 12 | interface <i>type number</i> Example: Switch(config)# interface ethernet 1/1 | Configures an interface and enters interface configuration mode. |
| Step 13 | ip address <i>ip-address mask</i> Example: Switch(config-if)# ip address 172.16.232.182 255.255.255.240 | Sets a primary IP address for an interface. |
| Step 14 | ip nat outside Example: Switch(config-if)# ip nat outside | Connects the interface to an outside network. |
| Step 15 | exit Example: | Exits interface configuration mode and returns to global configuration mode. |

| | Command or Action | Purpose |
|----------------|--|---|
| | Switch(config-if)# exit | |
| Step 16 | ip nat translation tcp-timeout <i>seconds</i> Example: <pre>Switch(config)# ip nat translation tcp-timeout 50000</pre> | Specifies the timeout value for TCP-based dynamic NAT entries. <ul style="list-style-type: none"> • Dynamically created NAT translations are cleared when the configured timeout limit is reached. |
| Step 17 | ip nat translation max-entries <i>number-of-entries</i> Example: <pre>Switch(config)# ip nat translation max-entries 300</pre> | Specifies the maximum number of dynamic NAT translations. The number of entries can be between 1 and 1023. |
| Step 18 | ip nat translation udp-timeout <i>seconds</i> Example: <pre>Switch(config)# ip nat translation udp-timeout 45000</pre> | Specifies the timeout value for UDP-based dynamic NAT entries. <ul style="list-style-type: none"> • Dynamically created NAT translations are cleared when the configured timeout limit is reached. |
| Step 19 | ip nat translation timeout <i>seconds</i> Example: <pre>switch(config)# ip nat translation timeout 13000</pre> | Specifies the timeout value for dynamic NAT translations. <ul style="list-style-type: none"> • NAT uses this timeout value only if the tcp-timeout or udp-timeout keywords are not configured. |
| Step 20 | end Example: <pre>Switch(config)# end</pre> | Exits global configuration mode and returns to privileged EXEC mode. |

Verifying Dynamic and Static Twice NAT Configurations

Procedure

-
- Step 1** **enable**
Example:

```
Switch> enable
```

 Enables privileged EXEC mode.
 - Enter your password if prompted.
- Step 2** **show ip nat translations**
Example:


```
Switch# show ip nat translations
```

Displays active Network Address Translation (NAT) translations.

- Displays additional information for each translation table entry, including when an entry was created and used.

Example

The following is sample output from the **show ip nat translations** command:

```
switch# show ip nat translations
```

| Pro | Inside global | Inside local | Outside local | Outside global |
|-----|------------------|---------------|-----------------|----------------|
| any | --- | --- | 10.4.4.40 | 203.2.133.20 |
| tcp | --- | --- | 10.24.1.133:333 | 198.5.133:555 |
| any | 192.168.1.140 | 10.1.1.40 | --- | --- |
| any | 192.168.1.140 | 10.1.1.40 | 10.4.4.40 | 203.2.133.20 |
| tcp | 172.16.9.142:777 | 10.2.2.42:444 | --- | --- |
| tcp | 172.16.9.142:777 | 10.2.2.42:444 | 10.24.1.133:333 | 198.5.133:555 |

Example: Configuring Dynamic Translation and Translation Timeouts

The following example shows how to configure dynamic overload Network Address Translation (NAT) by specifying an access list:

```
Switch> enable
Switch# configure terminal
Switch(config)# ip access-list acl1
Switch(config-acl)# permit ip 10.111.11.0/24 any
Switch(config-acl)# deny udp 10.111.11.100/32 any
Switch(config-acl)# exit
Switch(config)# ip nat inside source list acl1 interface ethernet 1/1 overload
Switch(config)# interface ethernet 1/4
Switch(config-if)# ip address 10.111.11.39 255.255.255.0
Switch(config-if)# ip nat inside
Switch(config-if)# exit
Switch(config)# interface ethernet 1/1
Switch(config-if)# ip address 172.16.232.182 255.255.255.240
Switch(config-if)# ip nat outside
Switch(config-if)# exit
Switch(config)# ip nat translation tcp-timeout 50000
Switch(config)# ip nat translation max-entries 300
Switch(config)# ip nat translation udp-timeout 45000
Switch(config)# ip nat translation timeout 13000
Switch(config)# end
```

Example: Configuring Dynamic Translation and Translation Timeouts