CHAPTER 5

Configuring Network Address Translation

Note The information in this chapter applies to both the ACE module and the ACE appliance unless otherwise noted.

This chapter contains the following major sections which describe how to configure NAT on the Cisco ACE Application Control Engine:

Network Address Translation Overview

When a client attempts to access a server in a data center, the client incorporates its IP address in the IP header when it connects to the server. An ACE placed between the client and the server can either preserve the client IP address or translate that IP address to a routable address in the server network, based on a pool of reserved dynamic NAT addresses or a static NAT address mapping, and pass the request on to the server.

This IP address translation process is called Network Address Translation (NAT) or source NAT (SNAT). The ACE tracks all SNAT mappings to ensure that response packets from the server are routed back to the client. If your application requires that the client IP address be preserved for statistical or accounting purposes, do not implement SNAT.

Destination NAT (DNAT) translates the IP address and port of an inside host so that it appears with a publicly addressable destination IP address to the rest of the world. Typically, you configure DNAT using static NAT and port redirection. You can use port redirection to configure servers that host a service on a custom port (for example, servers hosting HTTP on port 8080).

To provide security for a server, you can map the server private IP address to a global routable IP address that a client can use to connect to the server. In this case, the ACE translates the global IP address to the server private IP address when sending data from the client to the server. Conversely, when a server responds to a client, the ACE translates the local server IP address to a global IP address for security reasons. This process is called DNAT.

You can also configure the ACE to translate TCP and UDP port numbers greater than 1024, and ICMP identifiers. This process is known as Port Address Translation (PAT). The ACE provides 64 K minus 1 K ports for each IP address for PAT. Ports 0 through 1024 are reserved and cannot be used for PAT.

By default, the ACE performs implicit PAT for the FTP/RTSP/SIP data/media channel if you enable Layer 7 load-balancing or inspection. This identifies the real server from the server farm when the client sends data on the data/media channel using VIP and ACE performs real server IP to VIP translation for the data/media channel.

Note (ACE module only) Implicit PAT is also performed for the same source/destination port and port redirection scenarios to ensure that the server response returns to the same network processor.

Note (ACE module only) You can also disable implicit PAT and preserve the source port when the source and destination ports are the same by using the **hw-module cde-same-port-hash** in configuration mode. For details, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

The ACE supports the translation of IPv6 host or VIP addresses to IPv4 server addresses and the opposite for load balancing HTTP and HTTPS. This translation allow you to provide IPv6 functionality while maintaining an IPv4-only or an IPv6-only server farm or a server farm with a combination of the two protocols.

Some of the benefits of NAT are as follows:

- You can use private addresses on your inside networks. Private addresses are not routable on the Internet.
- NAT hides the local addresses from other networks, so attackers cannot learn the real address of a server in the data center.
- You can resolve IP routing problems, such as overlapping addresses, when you have two interfaces connected to overlapping subnets.

The ACE provides the following types of NAT and PAT:

- Interface-based dynamic NAT
- Interface-based dynamic PAT
- Server farm-based dynamic NAT
- Static NAT
- Static port redirection

This section contains the following topics:

- Maximum Number of NAT Commands
- Global Address Guidelines

Dynamic NAT

Dynamic NAT, which is typically used for SNAT, translates a group of local source addresses to a pool of global source addresses that are routable on the destination network. The global pool can include fewer addresses than the local group. When a local host accesses the destination network, the ACE assigns an IP address from the global pool to the host.

Because the translation times out after being idle for a user-configurable period of time, a given user does not keep the same IP address. For this reason, users on the destination network cannot reliably initiate a connection to a host that uses dynamic NAT (even if the connection is allowed by an access control list [ACL]). Not only can you not predict the global IP address of the host, but the ACE does not create a translation unless the local host is the initiator. See the "Configuring Static NAT and Static Port Redirection" section for details about reliable access to hosts.

Note For the duration of the translation, a global host can initiate a connection to the local host if an ACL allows it. Because the address is unpredictable, a connection to the host is unlikely. However, in this case, you can rely on the security of the ACL.

Dynamic NAT has these disadvantages:

- If the global address pool has fewer addresses than the local group, you could run out of addresses if the amount of traffic is greater than expected.

  Use dynamic PAT if this event occurs often, because dynamic PAT provides over 64,000 translations using multiple ports of a single IP address.

- If you need to use a large number of routable addresses in the global pool and the destination network requires registered addresses (for example, the Internet), you may encounter a shortage of usable addresses.

Note The ACE allows you to configure a virtual IP (VIP) address in the NAT pool for dynamic NAT and PAT. This action is useful when you want to source NAT real server originated connections (bound to the client) using the VIP address. This feature is specifically useful when there are a limited number of real world IP addresses on the client-side network. To perform PAT for different real servers that are source-NATed to the same IP address (VIP), you must configure the **pat** keyword in the **nat-pool** command.

The advantage of dynamic NAT is that some protocols cannot use dynamic PAT. Dynamic PAT does not work with some applications that have a data stream on one port and the control path on another, such as some multimedia applications.

Dynamic PAT

Dynamic PAT, which is also used for Source Network Address Translation (SNAT), translates multiple local source addresses and ports to a single global IP address and port that are routable on the destination network from a pool of IP addresses and ports reserved for this purpose. The ACE translates the local address and local port for multiple connections and/or hosts to a single global address and a unique port starting with port numbers greater than 1024.

When a local host connects to the destination network on a given source port, the ACE assigns a global IP address to it and a unique port number. Each host receives the same IP address but, because the source port number is unique, the ACE sends the return traffic, which includes the IP address and port number as the destination, to the correct host.

The ACE supports over 64,000 ports for each unique local IP address. Because the translation is specific to the local address and local port, each connection, which generates a new source port, requires a separate translation. For example, 10.1.1.1:1025 requires a separate translation from 10.1.1.1:1026.

The translation is valid only for the duration of the connection, so a user does not keep the same global IP address and port number. For this reason, users on the destination network cannot reliably initiate a connection to a host that uses dynamic PAT (even if the connection is allowed by an ACL). Not only can you not predict the local or global port number of the host, but the ACE does not create a translation unless the local host is the initiator. See the "Configuring Static NAT and Static Port Redirection" section for details about reliable access to hosts.

Dynamic PAT allows you to use a single global address, which helps to conserve routable addresses. Dynamic PAT does not work with some multimedia applications that have a data stream on a port that is different from the control path port.

Server Farm-Based Dynamic NAT

In addition to the interface-level dynamic NAT, the ACE supports dynamic NAT at the server farm level. Server farm-based dynamic NAT, which is also used for SNAT, is useful in situations where you want to perform NAT on only the IP addresses of the real servers in the primary and/or the backup server farm. Like interface-based dynamic NAT, server farm-based dynamic NAT uses a pool of IP addresses to translate a source address. Unlike interface-based NAT, server farm-based NAT translates the primary server farm IP addresses, the backup server farm IP addresses, or both.

Use this feature in the following cases:

- The ACE is configured in one-arm mode, that is, there is only one VLAN between the ACE and the Cisco Systems 6500 and 7600 Series Catalyst MSFC that is used for both client and server traffic. Both the primary and backup server farms are in the internal customer network (reachable from the same VLAN or from different VLANs), the primary server farm is Layer 2-attached, and the backup server farm is several Layer 3 hops away. In this case, perform NAT only for the backup server farm and never for the primary server farm.
- The ACE is configured in one-arm mode, the primary server farm is local, and the backup server farm is remote and reachable from the public, external network. In this case, use a private pool of IP addresses for SNAT of the primary server farm and a public, externally routable set of IP addresses for the backup server farm.
- You want to perform source NAT based on a Layer 7 rule or the selected server farm.

For details about configuring server farm-based dynamic NAT, see the "Configuring Server Farm-Based Dynamic NAT" section.

Static NAT

Static NAT, which is typically used for Destination NAT (DNAT), translates each local address to a fixed global address. With dynamic NAT and PAT, each host uses a different address or port after the translation times out. Because the global address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the global network to initiate traffic to a local host (if there is an ACL that allows it).

The main differences between dynamic NAT and static NAT are as follows:

- Static NAT uses a one-to-one correspondence between a local IP address and a fixed global IP address, while dynamic NAT assigns a global IP address from a pool of global addresses.
- With static NAT, you need an equal number of global IP addresses and local IP addresses. With dynamic NAT, you can have a pool of fewer global addresses than local addresses.

Static Port Redirection

Static port redirection, also used for DNAT, performs the same function as static NAT and additionally translates TCP or UDP ports or ICMP identifiers for the local and global addresses. With static port redirection, you can use the same global address in multiple static NAT statements, provided that, along with the address, you use different port numbers.

For example, if you want to provide a single address for global users to access FTP, HTTP, and SMTP, but there are different servers for each protocol on the local network, you can specify static port redirection statements for each server that use the same global IP address with different ports.

IPv6 NAT Support

As with IPv4 to IPv4 NAT, the ACE supports IPv6 to IPv6 NAT. The ACE also supports the translation of IPv6 or IPv4 VIPs in packets from clients to IPv4 or IPv6 server addresses for HTTP and HTTPS. This feature allows you to provide IPv6 functionality while maintaining an IPv4-only or an IPv6-only server farm infrastructure or a server farm with a combination of both protocols (mixed mode).

This IPv6 implementation is useful for load balancing packets from an IPv6-only network to a an IPv4-only server farm or an IPv4-only network to an IPv6-only server farm. Be sure to configure the insertion of the X-Forwarded-For HTTP header field with the source address to ensure that the servers of one protocol can log the client addresses of the other protocol. For more information, see the "Configuring NAT for IPv6 to IPv4 Load Balancing" section and the "Configuring NAT for IPv4 to IPv6 Load Balancing" section.

Maximum Number of NAT Commands

The ACE supports the following maximum numbers of **nat**, **nat-pool**, and **nat static** commands divided among all contexts:

- **nat** command—8192
- **nat-pool** command—8192
- **nat static** command—8192

Global Address Guidelines

When you translate the local address to a global address, you can use the following global addresses:

- Addresses on the same network as the global interface—If you use addresses on the same network as the global interface (through which traffic exits the ACE), the ACE uses proxy ARP to answer any requests for translated addresses and thus intercepts traffic destined for a local address. This solution simplifies routing, because the ACE does not need to be the gateway for any additional networks. However, this approach does put a limit on the number of available addresses used for translations.

  Note You cannot use the IP address of the global interface for NAT or PAT.

- Addresses on a unique network—If you need more addresses than are available on the global interface network, you can identify addresses on a different subnet. The ACE uses proxy ARP to answer any requests for translated addresses, so it intercepts traffic destined for a local address. You need to add a static route on the upstream router that sends traffic destined for the translated addresses on the ACE.

- You cannot configure global IP address ranges across subnets. For example, the following command is not allowed and will generate an Invalid IP address error: **nat-pool 2 10.0.6.1 10.0.7.20 netmask 255.255.255.0**.
- For IPv4, you must configure a netmask when you configure a NAT pool. A netmask of 255.255.255.255 instructs the ACE to use all the IP addresses in the range.
- For IPv6, you must configure a prefix length when you configure a NAT pool. For example, /64.

Configuring an Idle Timeout for NAT

You can configure an idle timeout for NAT by using the **timeout xlate** command in configuration mode. The syntax of this command is as follows:

timeout xlate *seconds*

The *seconds* argument is an integer from 60 to 2147483. The default is 10800 seconds (3 hours). The *seconds* value determines how long the ACE waits to free the Xlate slot after it becomes idle.

For example, to specify an idle timeout of 120 seconds (2 minutes), enter:

```
host1/Admin(config)# timeout xlate 120
```

To reset the NAT idle timeout to the default value of 10800 seconds, enter:

```
host1/Admin(config)# no timeout xlate 120
```

Configuring Dynamic NAT and PAT

This section describes how to configure dynamic NAT and PAT on an ACE for SNAT. For overview information about dynamic NAT and dynamic PAT, see the "Network Address Translation Overview" section. This section contains the following topics:

- Dynamic NAT and PAT Configuration Quick Start
- Configuring an ACL
- Configuring Interfaces for Dynamic NAT and PAT

- Creating a Global IP Address Pool for NAT
- Configuring a Class Map
- Configuring a Policy Map
- Configuring Dynamic NAT and PAT as a Layer 3 and Layer 4 Policy-Map Action
- Applying the Dynamic NAT and PAT Policy Map to an Interface Using a Service Policy

Dynamic NAT and PAT Configuration Quick Start

Table 5-1 provides a quick overview of the steps required to configure dynamic NAT and PAT. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections following Table 5-1.

Table 5-1 Dynamic NAT and PAT Configuration Quick Start

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to the correct context.
`host1/Admin# changeto C1`
`host1/C1#`
The rest of the examples in this table use the C1 user context, unless otherwise specified. For details on creating contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

2. Enter configuration mode.
`host1/C1# config`
`host1/C1(config)#`

3. Configure an ACL to allow traffic that requires NAT.
`host1/C1(config)# access-list NAT_ACCESS extended permit tcp 192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0 eq 80`
`host1/C1(config-acl)# exit`

Table 5-1 Dynamic NAT and PAT Configuration Quick Start (continued)

Task and Command Example

4. Configure a local interface (client interface) to receive traffic that requires NAT. If you are operating the ACE in one-arm mode, omit this step.
 	
`host1/C1(config)# interface vlan 100`
`host1/C1(config-if)# mtu 1500`
`host1/C1(config-if)# ip address 192.168.12.100 255.255.255.0`
`host1/C1(config-if)# no shutdown`
`host1/C1(config-if)# exit`

5. Configure a second interface (server interface) for the global IP address pool.
 	
`host1/C1(config)# interface vlan 200`
`host1/C1(config-if)# mtu 1500`
`host1/C1(config-if)# ip address 172.27.16.2 255.255.255.0`
`host1/C1(config-if)# no shutdown`
`host1/C1(config-if)# exit`

6. Configure a class map and define a match statement for the ACL that you configured in Step 3 for the client source address.
 	
`host1/C1(config)# class-map match-any NAT_CLASS`
`host1/C1(config-cmap)# match access-list NAT_ACCESS`
`host1/C1(config-cmap)# exit`

7. Configure a policy map and associate the class map with the policy map.
 	
`host1/C1(config)# policy-map multi-match NAT_POLICY`
`host1/C1(config-pmap)# class NAT_CLASS`
`host1/C1(config-pmap-c)#`

8. Configure dynamic NAT as a policy-map action.
 	
`host1/C1(config-pmap-c)# nat dynamic 1 vlan 200`
`host1/C1(config-pmap-c)# exit`
`host1/C1(config-pmap)# exit`

9. Activate the policy on the client interface using a service policy. If you are operating the ACE in one-arm mode, configure the **service-policy** command on the interface specified in Step 10.
 	
`host1/C1(config)# interface vlan 100`
`host1/C1(config-if)# service-policy input NAT_POLICY`
`host1/C1(config-if)# ctrl-z`

Table 5-1 Dynamic NAT and PAT Configuration Quick Start (continued)

Task and Command Example

10. Configure the IPv6 or IPv4 NAT pool on the server interface of the ACE. To configure dynamic PAT, include the **pat** keyword in the **nat-pool** command.
`host1/C1(config)# interface vlan 200`
`host1/C1(config-if)# nat-pool 1 2001:DB8:1::10 2001:DB8:1::41 pat`
`host1/C1(config-if)# Ctrl-Z`
 	
`or`
 	
`host1/C1(config)# interface vlan 200`
`host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask 255.255.255.0 pat`
`host1/C1(config-if)# Ctrl-Z`

11. (Optional) Save your configuration changes to flash memory. `host1/Admin# copy running-config startup-config`

12. Display and verify your dynamic NAT and PAT configuration.
`host1/C1# show running-config class-map`
`host1/C1# show running-config policy-map`
`host1/C1# show running-config service-policy`

Configuring an ACL

You can use a security access control list (ACL) to permit the traffic that requires NAT. For details about configuring an ACL, see Chapter 1, Configuring Security Access Control Lists.

IPv6 Syntax and Examples

To configure an ACL for dynamic NAT, use the **access-list** command in configuration mode. The syntax of this command is as follows:

access-list *name* [**line** *number*] **extended** {**deny** | **permit**} {*protocol*} {**anyv6** | **host** *src_ipv6_address* | *src_ipv6_address/prefix_length*} [*operator port1* [*port2*]] {**anyv6** | **host** *dest_ipv6_address* | *dest_ipv6_address/prefix_length*} [*operator port3* [*port4*]]

For example, enter:

```
host1/C1(config)# host1/Admin(config)# access-list NAT_ACCESS line 10
extended permit tcp 2001:DB8:1::/64 2001:DB8:2::/64 eq 80
```

To delete the ACL from the configuration, enter:

```
host1/C1(config)# no access-list NAT_ACCESS
```

IPv4 Syntax and Examples

To configure an ACL for dynamic NAT, use the **access-list** command in configuration mode. The syntax of this command is as follows:

access-list *name* [**line** *number*] **extended** {**deny** | **permit**} {*protocol*} {*src_ip_address netmask* | **any** | **host** *src_ip_address*} [*operator port1* [*port2*]] {*dest_ip_address netmask* | **any** | **host** *dest_ip_address*} [*operator port3* [*port4*]]

For example, enter:

```
host1/C1(config)# access-list NAT_ACCESS extended permit tcp
192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0 eq 80
```

To delete the ACL from the configuration, enter:

```
host1/C1(config)# no access-list NAT_ACCESS
```

Configuring Interfaces for Dynamic NAT and PAT

Configure an interface for clients and an interface for the real servers. If you are operating the ACE in one-arm mode, do not configure an interface for clients. For details, see the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.

Creating a Global IP Address Pool for NAT

Dynamic NAT uses a pool of global IP addresses that you specify. You can define either a single global IP address for a group of servers with PAT to differentiate between them, or a range of global IP addresses when using dynamic NAT only. To use a single IP address or a range of addresses, you assign an identifier to the address pool. You configure the NAT pool on the server VLAN interface.

Note If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

To create a pool of IP addresses for dynamic NAT, use the **nat-pool** command in interface configuration mode.

IPv6 Syntax and Examples

The syntax of this command is as follows:

nat-pool *pool_id* {*ipv6_address1*[*/prefix_length*]} | {*ipv6_address1 ipv6_address2*} [**pat**]

The keywords, arguments, and options are as follows:

- *pool_id*—Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.

  Note If you configure more than one NAT pool with the same ID, the ACE uses the last-configured NAT pool first, and then the other NAT pools.

- *ipv6_address1/prefix_length*—Single IPv6 address and optional prefix length, or if you are also using the *ipv6_address2* argument, the first IPv6 address in a range of global addresses used for NAT.
- *ipv6_address2*—(Optional) Highest IPv6 address in a range of global IPv6 addresses used for NAT. You can configure a maximum of 64 K addresses in a NAT pool.

  If you specify PAT, you can configure a maximum of 32 IP addresses in a NAT pool range. You cannot configure an IP address range across subnets. For example, the following command is not allowed and will generate an Invalid IP address error: **nat-pool 2 2001:DB8:1::1 2001:DB8:2::21**.

Note The ACE allows you to configure a virtual IP (VIP) address in the NAT pool for dynamic NAT and PAT. This action is useful when you want to source NAT real server originated connections (bound to the client) using the VIP address. This feature is specifically useful when there are a limited number of real world IP addresses on the client-side network. To perform PAT for different real servers that are source-NATed to the same IP address (VIP), you must configure the **pat** keyword in the **nat-pool** command.

- **pat**—(Optional) Specifies that the ACE perform Port Address Translation (PAT) in addition to NAT.

If the ACE runs out of IP addresses in a NAT pool, it can switch over to a PAT rule, if configured. For example, you can configure the following:

```
host1/Admin(config-if)# nat-pool 1 2001:DB8:1::10/64 2001:DB8:1::99/64
host1/Admin(config-if)# nat-pool 1 2001:DB8:1::100/64
2001:DB8:1::100/64 pat
```

If your network configuration has the following conditions, you should configure multiple PAT pools with a single IP address in each pool:

- Traffic coming from the same source IP address
- Source ports varying from 1 to 64000
- The same destination port going to different destination addresses
- All ports in one PAT pool are used

So instead of configuring:

```
host1/Admin(config-if)# nat-pool 1 2001:DB8:1::3 2001:DB8:1::5 pat
```

configure:

```
host1/Admin(config-if)# nat-pool 1 2001:DB8:1::3/64 pat

host1/Admin(config-if)# nat-pool 1 2001:DB8:1::4/64 pat

host1/Admin(config-if)# nat-pool 1 2001:DB8:1::5/64 pat
```

To configure a NAT pool consisting of a range of 32 (the maximum number of IP addresses per PAT pool) global IP addresses with PAT, enter:

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 2001:DB8:1::A/64 2001:DB8:1::29/64 pat
```

Note Before you can remove a NAT pool from an interface, you must remove the service policy and the policy map associated with the NAT pool.

To remove a NAT pool from the configuration, enter:

```
host1/C1(config-if)# no nat-pool 1
```

IPv4 Syntax and Examples

The syntax of this command is as follows:

nat-pool *pool_id ip_address1* [*ip_address2*] **netmask** *mask* [**pat**]

The keywords, arguments, and options are as follows:

- *pool_id*—Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.

  Note If you configure more than one NAT pool with the same ID, the ACE uses the last-configured NAT pool first, and then the other NAT pools.

- *ip_address1*—Single IP address, or if also using the *ip_address2* argument, the first IP address in a range of global addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
- *ip_address2*—(Optional) Highest IP address in a range of global IP addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.109). You can configure a maximum of 64 K addresses in a NAT pool.

  If you specify PAT, you can configure a maximum of 32 IP addresses in a NAT pool range. You cannot configure an IP address range across subnets. For example, the following command is not allowed and will generate an Invalid IP address error: **nat-pool 2 10.0.6.1 10.0.7.20 netmask 255.255.255.0**.

Note The ACE allows you to configure a virtual IP (VIP) address in the NAT pool for dynamic NAT and PAT. This action is useful when you want to source NAT real server originated connections (bound to the client) using the VIP address. This feature is specifically useful when there are a limited number of real world IP addresses on the client-side network. To perform PAT for different real servers that are source-NATed to the same IP address (VIP), you must configure the **pat** keyword in the **nat-pool** command.

- **netmask** *mask*—Specifies the subnet mask for the IP address pool. Enter a mask in dotted-decimal notation (for example, 255.255.255.255). A network mask of 255.255.255.255 instructs the ACE to use all the IP addresses in the specified range.
- **pat**—(Optional) Specifies that the ACE perform Port Address Translation (PAT) in addition to NAT.

If the ACE runs out of IP addresses in a NAT pool, it can switch over to a PAT rule, if configured. For example, you can configure the following:

```
host1/Admin(config-if)# nat-pool 1 10.1.100.10 10.1.100.99 netmask
255.255.255.255
host1/Admin(config-if)# nat-pool 1 10.1.100.100 10.1.100.100 netmask
255.255.255.255 pat
```

If your network configuration has the following conditions, you should configure multiple PAT pools with a single IP address in each pool:

- Traffic coming from the same source IP address
- Source ports varying from 1 to 64000
- The same destination port going to different destination addresses
- All ports in one PAT pool are used

So instead of configuring:

```
host1/Admin(config-if)# nat-pool 1 3.3.3.3 3.3.3.5 netmask
255.255.255.255 pat
```

configure:

```
host1/Admin(config-if)# nat-pool 1 192.161.12.3 netmask
255.255.255.255 pat
```

```
host1/Admin(config-if)# nat-pool 1 192.161.12.4 netmask
255.255.255.255 pat

host1/Admin(config-if)# nat-pool 1 192.161.12.5 netmask
255.255.255.255 pat
```

To configure a NAT pool consisting of a range of 32 (the maximum number of IP addresses per PAT pool) global IP addresses with PAT, enter:

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask
255.255.255.255 pat
```

Note Before you can remove a NAT pool from an interface, you must remove the service policy and the policy map associated with the NAT pool.

To remove a NAT pool from the configuration, enter:

```
host1/C1(config-if)# no nat-pool 1
```

Configuring a Class Map

You can configure a traffic class for dynamic NAT and PAT by using the **class-map** command in configuration mode. For more information about class maps, see the *Administration Guide, Cisco ACE Application Control Engine*.

The syntax of this command is as follows:

class-map match-any *name*

The *name* argument is a unique identifier for the class map, specified as an unquoted text string with a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)#
```

To remove a class-map from the configuration, enter:

```
host1/C1(config)# no class-map match-any NAT_CLASS
```

Enter match criteria for the ACL or the client source address using the **match** command in class-map configuration mode. For example, to set the match criteria to an existing ACL, enter the following command:

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

or

For IPv6, enter:

```
host1/C1(config-cmap)# match source-address 2001:DB8:1::10/64
```

For IPv4, enter:

```
host1/C1(config-cmap)# match source-address 192.168.12.15
255.255.255.0
```

To remove a match statement from a class map, enter:

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

Configuring a Class Map for Passive FTP

If you are using passive FTP with source NAT, you must configure an additional class map to source NAT the passive data connection. You then associate this class map with the Layer 4 multimatch policy and configure the **nat dynamic** command as an action in the policy map under this class map. To configure a class map for passive FTP, enter the commands in the following examples.

For IPv6, enter:

```
host1/C1(config)# class-map match-any FTP_NAT_CLASS
host1/C1(config-cmap)# match virtual address 2001:DB8:1::10 any
```

For Ipv4, enter:

```
host1/C1(config)# class-map match-any FTP_NAT_CLASS
host1/C1(config-cmap)# match virtual address 172.16.35.37 any
```

Configuring a Policy Map

You can configure a traffic policy for dynamic NAT and PAT by using the **policy-map** command in configuration mode. For more information about policy maps, see the *Administration Guide, Cisco ACE Application Control Engine*.

The syntax of this command is as follows:

policy-map multi-match *name*

The *name* argument is the name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

To remove a policy map from the configuration, enter:

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

Associate the previously created class map with the policy map. For example, enter:

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

To dissociate a class map from a policy map, enter:

```
host1/C1(config-pmap)# no class NAT_CLASS
```

Configure policy-map actions as required. For example, configure:

```
host1/C1(config-pmap-c)# loadbalance policy L7_POLICY
host1/C1(config-pmap-c)# loadbalance vip inservice
```

Note The **loadbalance vip inservice** command is not valid with a **match access-list** or a **match source-address** class map.

For passive FTP, associate the FTP_NAT_CLASS class map (see the Configuring a Class Map for Passive FTP section) with the Layer 4 policy map. For example, enter the following commands in policy map configuration mode:

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)# class FTP_NAT_CLASS
```

If you are using passive FTP, proceed with the following section and configure the **nat dynamic** command as a policy action under the FTP class map. Otherwise, configure the **nat dynamic** command as a policy action under the NAT_CLASS class map.

Configuring Dynamic NAT and PAT as a Layer 3 and Layer 4 Policy-Map Action

You can configure dynamic NAT and PAT (SNAT) as an action in a Layer 3 and Layer 4 policy map by using the **nat dynamic** command in policy-map class configuration mode. The ACE applies dynamic NAT from the interface to which the traffic policy is attached (through the **service-policy** interface configuration command) to the interface specified in the **nat** command. If you are operating in one-arm mode, there is only one VLAN interface.

The syntax of this command is as follows:

nat dynamic *pool_id* **vlan** *number*

The keywords, arguments, and options are as follows:

- **dynamic** *pool_id*—Refers to the identifier of a global pool of IP addresses that was configured using the **nat-pool** command on the specified VLAN (see the "Creating a Global IP Address Pool for NAT" section). Dynamic NAT translates a group of local source IP addresses to a pool of global IP addresses that are routable on the destination network. All packets egressing the interface attached to the traffic policy have their source address translated to one of the available addresses in the global pool. Enter an integer from 1 to 2147483647.
- **vlan** *number*—Specifies the server interface for the global IP address. This interface must be different from the interface that the ACE uses to filter and receive traffic that requires NAT, unless the network design operates in one-arm mode. In that case, the VLAN number is the same.

Note If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

The following example specifies the **nat** command as an action for a dynamic NAT Layer 3 and Layer 4 policy map:

```
host1/C1(config)# policy-map multi-action NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)# nat dynamic 1 vlan 200
```

To remove a dynamic NAT action from a policy map, enter:

```
host1/C1(config-pmap-c)# no nat dynamic 1 vlan 200
```

Applying the Dynamic NAT and PAT Policy Map to an Interface Using a Service Policy

Activate the dynamic NAT and PAT policy map and associate it with an interface by using the **service-policy** command in interface configuration mode. For details about the **service-policy** command, see the *Administration Guide, Cisco ACE Application Control Engine*.

Note You can configure dynamic NAT as an input service policy only, not as an output service policy. You cannot apply the same NAT policy both locally and globally.

The syntax of this command is as follows:

service-policy input *policy_name*

The keywords and arguments are as follows:

- **input**—Specifies that the traffic policy is to be attached to the input direction of a VLAN interface. The traffic policy evaluates all traffic received by that interface.
- *policy_name*—Name of a previously defined policy map. The name can have a maximum of 64 alphanumeric characters.

IPv6 Example

To apply a service policy to a specific interface for IPv6, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1700
host1/C1(config-if)# ip address 2001:DB8:1::2/64
host1/C1(config-if)# service-policy input NAT_POLICY
```

To apply a service policy globally to all interfaces in a context, enter:

```
host1/C1(config)# service-policy input NAT_POLICY
```

To remove a service policy from an interface, enter:

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```

To remove a service policy globally from all interfaces in a context, enter:

```
host1/C1(config)# no service-policy input NAT_POLICY
```

IPv4 Example

To apply a service policy to a specific interface for IPv6, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1700
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0
host1/C1(config-if)# service-policy input NAT_POLICY
```

To apply a service policy globally to all interfaces in a context, enter:

```
host1/C1(config)# service-policy input NAT_POLICY
```

To remove a service policy from an interface, enter:

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```

To remove a service policy globally from all interfaces in a context, enter:

```
host1/C1(config)# no service-policy input NAT_POLICY
```

Note When you detach a traffic policy either individually from the last VLAN interface on which you applied the service policy or globally from all VLAN interfaces in the same context, the ACE automatically resets the associated service-policy statistics. The ACE performs this action to provide a new starting point for the service-policy statistics the next time that you attach a traffic policy to a specific VLAN interface or globally to all VLAN interfaces in the same context.

Configuring NAT for IPv6 to IPv4 Load Balancing

You can configure the ACE to act as a proxy and translate VIP addresses in packets from clients in an IPv6 network to IPv4 real server addresses. This configuration allows you to implement IPv6 in your network while maintaining your current IPv4 real servers. When a client sends an IPv6 packet to an ACE IPv6 VIP, the ACE translates the VIP address to a server IPv4 private address and sends the packet to the server. In the absence of a specific configuration, the IPv6 address of the client would be lost and the IPv4 server would not be able to log the client IPv6 address. To ensure that the IPv4 server can log the client IPv6

address, you must configure the X-Forwarded-For: HTTP header on the ACE. For example, the following configuration shows how to implement NAT IPv6 to IPv4 load balancing:

```
access-list ALL line 8 extended permit ip any any
access-list V6-ANY line 8 extended permit ip anyv6 anyv6

rserver host RS1
  ip address 10.1.1.21
  inservice
rserver host RS2
  ip address 10.1.1.22
  inservice

serverfarm host sf1
  rserver rs1
    inservice
  rserver rs2
    inservice

class-map match-any L4_V6_HTTP-1
  2 match virtual-address 2001:2001:2001:2001::2011/64 tcp eq www
class-map type management match-all V6-MGMT
  2 match protocol icmpv6 anyv6
class-map type management match-any MANAGEMENT
  2 match protocol ssh any
  3 match protocol https any
  4 match protocol icmp any
  5 match protocol http any
  6 match protocol telnet any
  8 match protocol snmp any

policy-map type management first-match MGMT
  class management
    permit
  class V6-MGMT
    permit

policy-map type loadbalance first-match L4_HTTP
  class class-default
    serverfarm sf1
    insert-http x-forward-for header-value "%is"

policy-map multi-match V6_Policy1
  class L4_V6_HTTP-1
    loadbalance vip inservice
    loadbalance policy L4_V6_HTTP
    loadbalance vip icmp-reply
```

```
    nat dynamic 1 vlan 3001

interface vlan 2001
  ipv6 enable
  ip address 2001:DB8:1::2002/96
  access-group input all
  access-group input v6-any
  service-policy input V6_Policy1
  service-policy input MGMT
  no shutdown

interface vlan 3001
  ip address 10.1.1.1
  nat-pool 1 10.1.1.100 10.1.1.110 netmask 255.255.255.0 pat
  no shutdown
```

Configuring NAT for IPv4 to IPv6 Load Balancing

You can configure the ACE to act as a proxy and translate VIP addresses in packets from clients in an IPv4 network to IPv6 real server addresses. This configuration allows you to implement IPv6 in your network and connect to IPv4 networks. When a client sends an IPv4 packet to an ACE IPv4 VIP, the ACE translates the VIP address to a server IPv6 unique local address and sends the packet to the server. In the absence of a specific configuration, the IPv4 address of the client would be lost and the IPv6 server would not be able to log the client address. To ensure that the IPv6 server can log the client IPv4 address, you must configure the X-Forwarded-For: HTTP header on the ACE. For example, the following configuration shows how to implement NAT for IPv4 to IPv6 load balancing. The NAT-specific commands are shown in bold.

```
access-list all line 8 extended permit ip any any
access-list v6-any line 8 extended permit ip anyv6 anyv6

rserver host v6_rs1
  ip address 2001:DB6:1::10
  inservice
rserver host v6_rs2
  ip address 2001:DB6:1::11
  inservice

serverfarm host v6_sf1
  rserver v6_rs1
    inservice
```

```
  rserver v6_rs2
    inservice

class-map match-any L4_HTTP-1
  2 match virtual-address 192.168.12.20 tcp eq www
class-map type management match-any management
  2 match protocol ssh any
  3 match protocol https any
  4 match protocol icmp any
  5 match protocol http any
  6 match protocol telnet any
  8 match protocol snmp any

policy-map type management first-match MGMT
  class management
    permit

policy-map type loadbalance first-match L4_HTTP
  class class-default
    serverfarm v6_sf1
    insert-http x-forward-for header-value "%is"

policy-map multi-match Policy1
  class L4_HTTP-1
    loadbalance vip inservice
    loadbalance policy L4_HTTP
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 3001

interface vlan 2001
  ipv6 enable
  ip address 192.168.12.1 255.255.255.0
  access-group input all
  access-group input v6-any
  service-policy input Policy1
  service-policy input MGMT
  no shutdown

interface vlan 3001
  ip address 2001:DB8:1::/64
  nat-pool 1 2001:DB8:1::100 2001:DB8:2::110 pat
  no shutdown
```

Configuring Server Farm-Based Dynamic NAT

This section describes how to configure server farm-based dynamic NAT on an ACE for SNAT. For overview information about server farm-based dynamic NAT, see the "Network Address Translation Overview" section. This section contains the following topics:

- Server Farm-Based Dynamic NAT Configuration Quick Start
- Configuring an ACL for Server Farm-Based Dynamic NAT
- Configuring Interfaces for Server Farm-Based Dynamic NAT
- Creating a Global IP Address Pool for Dynamic NAT
- Configuring Real Servers and a Server Farm
- Configuring a Layer 7 Load-Balancing Class Map for Server Farm-Based Dynamic NAT
- Configuring a Layer 7 Load-Balancing Policy Map for Server Farm-Based Dynamic NAT
- Configuring Server Farm-Based Dynamic NAT as a Layer 7 Policy Action
- Configuring a Layer 3 and Layer 4 Class Map for Server Farm-Based Dynamic NAT
- Configuring a Layer 3 and Layer 4 Policy Map for Server Farm-Based Dynamic NAT
- Applying the Layer 3 and Layer 4 Policy Map to an Interface Using a Service Policy
- Configuring a Mixed Mode (IPv6 and IPv4) Server Farm

Server Farm-Based Dynamic NAT Configuration Quick Start

Table 5-2 provides a quick overview of the steps required to configure server farm-based dynamic NAT. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections following Table 5-2.

Table 5-2 Sever Farm-Based Dynamic NAT Configuration Quick Start

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to the correct context.
`host1/Admin# changeto C1`
`host1/C1#`
The rest of the examples in this table use the C1 user context, unless otherwise specified. For details on creating contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

2. Enter configuration mode.
`host1/C1# config`
`host1/C1(config)#`

3. Configure an IPv6 or an IPv4 ACL to allow traffic that requires NAT.
`host1/C1(config)# access-list ACL1 line 10 extended permit tcp 2001:DB8:1::/64 eq 8080 anyv6`
or
`host1/C1(config)# access-list ACL1 line 10 extended permit tcp 10.0.0.0 255.0.0.0 eq 8080 any`
`host1/C1(config-acl)# exit`

Table 5-2 Sever Farm-Based Dynamic NAT Configuration Quick Start (continued)

Task and Command Example

4. Configure real servers with an IPv4 or an IPv6 address and a server farm for load balancing. The **nat dynamic** command in Step 9 references this server farm.
 	
`host1/C1(config)# rserver SERVER1`
`host1/C1(config-rserver-host)# ip address 2001:DB8:2::201/64`
 	
`or`
 	
`host1/C1(config-rserver-host)# ip address 172.27.16.201/64`
`host1/C1(config-rserver-host)# inservice`
`host1/C1(config-rserver-host)# exit`
`host1/C1(config)# rserver SERVER2`
`host1/C1(config-rserver-host)# ip address 2001:DB8:2::202/64`
 	
`or`
 	
`host1/C1(config-rserver-host)# ip address 172.27.16.202`
`host1/C1(config-rserver-host)# inservice`
`host1/C1(config-rserver-host)# exit`
`host1/C1(config)# serverfarm SF1`
`host1/C1(config-sfarm-host)# rserver SERVER1 3000`
`host1/C1(config-sfarm-host-rs)# inservice`
`host1/C1(config-sfarm-host-rs)# exit`
`host1/C1(config-sfarm-host)# rserver SERVER2 3001`
`host1/C1(config-sfarm-host-rs)# inservice`
`host1/C1(config-sfarm-host-rs)# exit`
`host1/C1(config-sfarm-host)# exit`

5. Configure a local interface (client VLAN) to filter and receive client traffic. If you are operating the ACE in one-arm mode, omit this step.
 	
`host1/C1(config)# interface vlan 100`
`host1/C1(config-if)# mtu 1500`
`host1/C1(config-if)# ip address 2001:DB8:3::100/64`
 	
`or`
 	
`host1/C1(config-if)# ip address 192.168.12.100 255.255.255.0`
`host1/C1(config-if)# no shutdown`
`host1/C1(config-if)# exit`

Table 5-2 Sever Farm-Based Dynamic NAT Configuration Quick Start (continued)

Task and Command Example

6. Configure a second interface (server VLAN) for the NAT pool.
`host1/C1(config)# interface vlan 200`
`host1/C1(config-if)# mtu 1500`
`host1/C1(config-if)# ip address 2001:DB8:2::200/64`
 	
`or`
 	
`host1/C1(config-if)# ip address 172.27.16.200 255.255.255.0`
`host1/C1(config-if)# no shutdown`
`host1/C1(config-if)# exit`

7. Configure a Layer 7 load-balancing class map and define match criteria.
`host1/C1(config)# class-map type http loadbalance match-any L7_CLASS`
`host1/C1(config-cmap-http-lb)# match http content .*cisco.com`

8. Configure a Layer 7 load-balancing policy map and associate the class map with the policy map.
`host1/C1(config)# policy-map type loadbalance http first-match L7_POLICY`
`host1/C1(config-pmap-lb)# class L7_CLASS`
`host1/C1(config-pmap-lb-c)#`

9. Configure server farm-based dynamic NAT as a policy-map action in the Layer 7 load-balancing policy. You can configure multiple instances of this command for each primary and backup server farm and each outgoing server VLAN.
`host1/C1(config-pmap-lb-c)# nat dynamic 1 vlan 200 serverfarm primary`
`host1/C1(config-pmap-lb-c)# exit`
`host1/C1(config-pmap-lb)# exit`
`host1/C1(config)#`

10. Configure a Layer 3 and Layer 4 class map and define match criteria.
`host1/C1(config)# class-map match-any SLB_CLASS`
`host1/C1(config-cmap)# match virtual-address 2001:DB8:2::/64 tcp eq http`
`host1/C1(config-cmap)# exit`

Table 5-2 Sever Farm-Based Dynamic NAT Configuration Quick Start (continued)

Task and Command Example

11. Configure a Layer 3 and Layer 4 policy map and associate the class map with the policy map.
`host1/C1(config)# policy-map multi-match SLB_POLICY`
`host1/C1(config-pmap)# class SLB_CLASS`
`host1/C1(config-pmap-c)#`

12. Configure Layer 3 and Layer 4 policy map actions.
`host1/C1(config-pmap-c)# loadbalance policy L7_POLICY`
`host1/C1(config-pmap-c)# loadbalance vip inservice`
`host1/C1(config-pmap-c)# exit`
`host1/C1(config-pmap)# exit`
`host1/C1(config)#`

13. Activate the policy on the client interface using a service policy. If you are operating the ACE in one-arm mode, configure the **service-policy** command on the interface specified in Step 14.
`host1/C1(config)# interface vlan 100`
`host1/C1(config-if)# service-policy input SLB_POLICY`
`host1/C1(config-if)# exit`

14. Configure the NAT pool on the server interface.
`host1/C1(config)# interface vlan 200`
`host1/C1(config-if)# nat-pool 1 2001:DB8:2::A 2001:DB8:2::29/64`
 	
`or`
 	
`host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.26.49 255.255.255.0`
`host1/C1(config-if)# Ctrl-Z`

15. (Optional) Save your configuration changes to flash memory. `host1/Admin# copy running-config startup-config`

16. Display and verify your server farm-based dynamic NAT configuration.
`host1/C1# show running-config class-map`
`host1/C1# show running-config policy-map`
`host1/C1# show running-config service-policy`

Configuring an ACL for Server Farm-Based Dynamic NAT

Use an access control list (ACL) to permit the traffic that requires NAT. See the "Configuring an ACL" section. For details about configuring an ACL, see Chapter 1, Configuring Security Access Control Lists.

Configuring Interfaces for Server Farm-Based Dynamic NAT

Configure an interface for clients and an interface for the real servers. If you are operating the ACE in one-arm mode, omit the client interface. For details about configuring interfaces, see the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.

Creating a Global IP Address Pool for Dynamic NAT

Dynamic NAT uses a pool of global IP addresses that you specify. You can define a range of global IP addresses when using dynamic NAT. To use a range of addresses, you assign an identifier to the address pool. You then associate the NAT pool with the server VLAN interface.

Note If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

To create a pool of IPv6 addresses for dynamic NAT, use the **nat-pool** command in interface configuration mode.

Note If you plan to apply both IPv6 and IPv4 addresses under the same NAT pool because your configuration includes a mixed mode server farm (a mixture of IPv6 and IPv4 servers), also refer to the "Configuring a Mixed Mode (IPv6 and IPv4) Server Farm" section for additional configuration information.

IPv6 Syntax and Examples

The syntax of this command is as follows:

nat-pool *pool_id ipv6_address1*[*/prefix_length*]
ipv6_address2[*/prefix_length*]

The keywords, arguments, and options are as follows:

- *pool_id*—Identifier of the NAT pool of global IPv6 addresses. Enter an integer from 1 to 2147483647.

  Note If you configure more than one NAT pool with the same ID, the ACE uses the last-configured NAT pool first, and then the other NAT pools.

- *ipv6_address1*[*/prefix_length*]—Single IPv6 address, or if also using the *ip_address2* argument, the first IP address in a range of global addresses used for NAT.
- *ipv6_address2*[*/prefix_length*]—Highest IPv6 address in a range of global IPv6 addresses used for NAT. You can configure a maximum of 64 K addresses in a NAT pool.

  You cannot configure an IPv6 address range across subnets. For example, the following command is not allowed and will generate an Invalid IP address error:

  ```
  host1/Admin(config-if)# nat-pool 2 2001:DB8:1::/64
  2001:DB8:2::20/64
  ```

  Note The ACE allows you to configure a virtual IP (VIP) address in the NAT pool for dynamic NAT. This action is useful when you want to source NAT real server originated connections (bound to the client) using the VIP address. This feature is specifically useful when there are a limited number of real world IPv6 addresses on the client-side network.

To configure a NAT pool consisting of a range of 32 global IP addresses, enter:

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 2001:DB8:1::10/64 2001:DB8:1::41/64
```

Note Before you can remove a NAT pool from an interface, you must remove the service policy and the policy map associated with the NAT pool.

To remove a NAT pool from the configuration, enter:

```
host1/C1(config-if)# no nat-pool 1
```

IPv4 Syntax and Examples

To create a pool of IP addresses for dynamic NAT, use the **nat-pool** command in interface configuration mode. The syntax of this command is as follows:

nat-pool *pool_id ip_address1 ip_address2* **netmask** *mask*

The keywords, arguments, and options are as follows:

- *pool_id*—Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.

  Note If you configure more than one NAT pool with the same ID, the ACE uses the last-configured NAT pool first, and then the other NAT pools.

- *ip_address1*—Single IP address and prefix length, or if also using the *ip_address2* argument, the first IP address in a range of global addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.10).
- *ip_address2*—Highest IP address and prefix length in a range of global IP addresses used for NAT. Enter an IP address in dotted-decimal notation (for example, 172.27.16.26). You can configure a maximum of 64 K addresses in a NAT pool.

  You cannot configure an IP address range across subnets. For example, the following command is not allowed and will generate an Invalid IP address error:

  ```
  host1/Admin(config-if)# nat-pool 2 10.0.6.1 10.0.7.20 netmask
  255.255.255.0
  ```

Note The ACE allows you to configure a virtual IP (VIP) address in the NAT pool for dynamic NAT. This action is useful when you want to source NAT real server originated connections (bound to the client) using the VIP address. This feature is specifically useful when there are a limited number of real world IP addresses on the client-side network.

- **netmask** *mask*—Specifies the subnet mask for the IP address pool. Enter a mask in dotted-decimal notation (for example, 255.255.255.255). A network mask of 255.255.255.255 instructs the ACE to use all the IP addresses in the specified range.

To configure a NAT pool consisting of a range of 32 global IP addresses, enter:

```
host1/C1(config)# interface vlan 200
host1/C1(config-if)# nat-pool 1 172.27.16.10 172.27.16.41 netmask
255.255.255.255
```

Note Before you can remove a NAT pool from an interface, you must remove the service policy and the policy map associated with the NAT pool.

To remove a NAT pool from the configuration, enter:

```
host1/C1(config-if)# no nat-pool 1
```

Configuring Real Servers and a Server Farm

For details about configuring real servers and server farms, see the *Server Load-Balancing Guide, Cisco ACE Application Control Engine*.

Configuring a Layer 7 Load-Balancing Class Map for Server Farm-Based Dynamic NAT

Configure a Layer 7 traffic class for server farm-based dynamic NAT by using the **class-map** command in configuration mode. The syntax of this command is as follows:

class-map type http loadbalance match-any *name*

The *name* argument is a unique identifier for the class map, specified as an unquoted text string with a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# class-map type http loadbalance match-any L7_CLASS
host1/C1(config-cmap-http-lb)#
```

To remove a class-map from the configuration, enter:

```
host1/C1(config)# no class-map type http loadbalance match-any
L7_CLASS
```

Enter match criteria as required using the **match** command in class-map load balancing configuration mode. For example, enter:

```
host1/C1(config-cmap-http-lb)# match http content .*cisco.com
```

To remove a match statement from a class map, enter:

```
host1/C1(config-cmap-http-lb)# no match http content .*cisco.com
```

Configuring a Layer 7 Load-Balancing Policy Map for Server Farm-Based Dynamic NAT

Configure a Layer 7 load-balancing policy map by using the policy-map command in configuration mode. The syntax of this command is:

policy-map type loadbalance http first-match *name*

The *name* argument is a unique identifier for the policy map, specified as an unquoted text string with a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# policy-map type loadbalance http first-match
L7_POLICY
host1/C1(config-pmap-lb)#
```

To remove a policy map from the configuration, enter:

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

To associate the previously created class map with the policy map. For example, enter:

```
host1/C1(config-pmap-lb)# class L7_CLASS
host1/C1(config-pmap-lb-c)#
```

To disassociate a class map from a policy map, enter:

```
host1/C1(config-pmap-lb)# no class L7_CLASS
```

Configuring Server Farm-Based Dynamic NAT as a Layer 7 Policy Action

Configure server farm-based dynamic NAT as an action in a Layer 7 load-balancing policy map by using the **nat** command in policy-map load-balancing class configuration mode. Typically, you use dynamic NAT for SNAT. Dynamic NAT allows you to identify local traffic for address translation by specifying the source and destination addresses in an extended ACL, which is referenced as part of the class map traffic classification. The ACE applies dynamic NAT from the interface to which the traffic policy is attached (through the **service-policy** interface configuration command) to the interface specified in the **nat dynamic** command.

The syntax of this command is as follows:

nat dynamic *pool_id* **vlan** *number* **serverfarm** {**primary** | **backup**}

The keywords and arguments are as follows:

- *pool_id*—Identifier of the NAT pool of global IP addresses. Enter an integer from 1 to 2147483647.

Note If you configure more than one NAT pool with the same ID, the ACE uses the last-configured NAT pool first, and then the other NAT pools.

- **vlan** *number*—Specifies the server interface for the global IP address. This interface must be different from the interface that the ACE uses to filter and receive traffic that requires NAT, unless the network design operates in one-arm mode. In that case, the VLAN number is the same.
- **serverfarm**—Specifies server farm-based dynamic NAT.
- **primary | backup**—Specifies that the dynamic NAT applies to either the primary server farm or the backup server farm.

Note If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

The following SNAT server farm-based dynamic NAT example specifies the **nat** command as an action for a Layer 7 policy map:

```
host1/C1(config)# policy-map type loadbalance http first-match
L7_POLICY
host1/C1(config-pmap-lb)# class L7_CLASS
host1/C1(config-pmap-lb-c)# nat dynamic serverfarm primary 1 vlan 200
```

To remove a server farm-based dynamic NAT action from a policy map, enter:

```
host1/C1(config-pmap-lb-c) no nat dynamic serverfarm primary 1
vlan 200
```

Configuring a Layer 3 and Layer 4 Class Map for Server Farm-Based Dynamic NAT

Configure a Layer 3 and Layer 4 traffic class for server farm-based dynamic NAT by using the **class-map** command in configuration mode. For more information about class maps, see the *Administration Guide, Cisco ACE Application Control Engine*.

The syntax of this command is as follows:

class-map match-any *name*

The *name* argument is a unique identifier for the class map, specified as an unquoted text string with a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)#
```

To remove a class map from the configuration, enter:

```
host1/C1(config)# no class-map match-any NAT_CLASS
```

Enter match criteria as required using the **match** command in class-map configuration mode. For example, enter:

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

or

For IPv6, enter:

```
host1/C1(config-cmap)# match source-address 2001:DB8:1::10/64
```

For IPv4, enter:

```
host1/C1(config-cmap)# match source-address 192.168.12.15
255.255.255.0
```

To remove a match statement from a class map, enter:

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

Configuring a Layer 3 and Layer 4 Policy Map for Server Farm-Based Dynamic NAT

Configure a Layer 3 and Layer 4 traffic policy for NAT by using the **policy-map** command in configuration mode. For more information about policy maps, see the *Administration Guide, Cisco ACE Application Control Engine*.

The syntax of this command is as follows:

policy-map multi-match *name*

The *name* argument is the name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

To remove a policy map from the configuration, enter:

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

To associate the previously created class map with the policy map. For example, enter:

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

To dissociate a class map from a policy map, enter:

```
host1/C1(config-pmap)# no class NAT_CLASS
```

Configure policy-map actions as required. For example, configure:

```
host1/C1(config-pmap-c)# loadbalance policy L7_POLICY
host1/C1(config-pmap-c)# loadbalance VIP inservice
```

Applying the Layer 3 and Layer 4 Policy Map to an Interface Using a Service Policy

You can activate the server farm-based dynamic NAT policy and assign it to an interface by using the **service-policy** command in interface configuration mode. For details about the **service-policy** command, see the *Administration Guide, Cisco ACE Application Control Engine*.

Note You can configure dynamic NAT as an input service policy only, not as an output service policy. You cannot apply the same NAT policy both locally and globally.

The syntax of this command is as follows:

service-policy input *policy_name*

The keywords and arguments are as follows:

- **input**—Specifies that the traffic policy is to be attached to the input direction of a VLAN interface. The traffic policy evaluates all traffic received by that interface.
- *policy_name*—Name of a previously defined policy map. The name can have a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1700
host1/C1(config-if)# ip address 192.168.12.100 255.255.255.0
host1/C1(config-if)# service-policy input NAT_POLICY
```

To remove a service policy from an interface, enter:

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```

Note When you remove a traffic policy from the last VLAN interface on which you applied the service policy, the ACE automatically resets the associated service-policy statistics. The ACE performs this action to provide a new starting point for the service-policy statistics the next time that you attach a traffic policy to a specific VLAN interface.

Configuring a Mixed Mode (IPv6 and IPv4) Server Farm

To configure a combination of IPv6 and IPv4 servers in a server farm (mixed mode), keep the following considerations in mind:

- If using an IPv4 VIP and you associate a mixed mode server farm with this VIP under a load-balancing policy map, create a NAT pool that converts IPv4 addresses to IPv6 addresses in case the ACE selects the IPv6 real server as part of the load-balancing process (see "Creating a Global IP Address Pool for Dynamic NAT").
- For packets being sent to IPv4 real servers, you may want to optionally apply a NAT policy. In this case:
  a. Create an IPv4 NAT pool.
  b. Configure both the IPv4 and IPv6 NAT pools under the interface that is associated with the NAT pool identifier.
  c. Configure this NAT pool identifier under the Layer 7 policy map.

Included below is a sample configuration for a mixed mode server farm. It builds on the procedures outlined in this section to configure server farm-based dynamic NAT.

```
rserver host v6
  ip address 2001:500:407::25
  inservice
rserver host v6_1
  ip address 2001:500:407::26
  inservice
rserver host v6_2
  ip address 2001:500:407::27
  inservice
rserver host v4
  ip address 40.0.7.25
  inservice
rserver host v4_1
  ip address 40.0.7.26
  inservice
rserver host v4_2
  ip address 40.0.7.27
  inservice
rserver host v4_3
  ip address 40.0.7.28
  inservice

serverfarm host v4v6
  rserver v6
    inservice
  rserver v6_1
    inservice
  rserver v6_2
    inservice
  rserver v4
    inservice
  rserver v4_1
    inservice
  rserver v4_2
    inservice

class-map match-any vip
  2 match virtual-address 40.0.6.20 any

policy-map type loadbalance http first-match l7
  class cmap
    serverfarm v4v6

policy-map multi-match slb
```

```
  class vip
    loadbalance vip inservice
    loadbalance policy l7
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 407

interface vlan 406
description "client interface"
  ipv6 enable
  ip address 2001:500:406::11/64
  ip address 40.0.6.11 255.255.255.0
  service-policy input slb
  no shutdown

interface vlan 407
description "server side interface"
  ipv6 enable
  ip address 2001:500:407::11/64
  ipv6 nd prefix 2111::/64 at 5 January 2013 10:10 31 January 2012
10:10
  ip address 40.0.7.11 255.255.255.0
  nat-pool 1 2001:500:407::abb 2001:500:407::acc/128
  nat-pool 1 40.0.7.100 40.0.7.110 netmask 255.255.255.255
  no shutdown
```

Configuring Static NAT and Static Port Redirection

This section describes how to configure static NAT and static port redirection on an ACE for DNAT. For overview information about static NAT and static port redirection, see the "Network Address Translation Overview" section. This section contains the following topics:

- Static NAT Configuration Quick Start
- Configuring an ACL for Static NAT and Static Port Redirection
- Configuring a Class Map
- Configuring a Policy Map
- Configuring Static NAT and Static Port Redirection as a Policy Action
- Applying the Static NAT and Static Port Redirection Policy Map to an Interface Using a Service Policy

Static NAT Configuration Quick Start

Table 5-3 provides a quick overview of the steps required to configure static NAT and static port redirection. Each step includes the CLI command or a reference to the procedure required to complete the task. For a complete description of each feature and all the options associated with the CLI commands, see the sections following Table 5-3.

Note The ACE supports static NAT only for IPv6 to IPv6 and IPv4 to IPv4 translations. Mixed mode is not supported.

Table 5-3 Static NAT Configuration Quick Start

Task and Command Example

1. If you are operating in multiple contexts, observe the CLI prompt to verify that you are operating in the desired context. If necessary, change to the correct context.
`host1/Admin# changeto C1`
`host1/C1#`
The rest of the examples in this table use the C1 user context, unless otherwise specified. For details on creating contexts, see the *Virtualization Guide, Cisco ACE Application Control Engine*.

2. Enter configuration mode.
`host1/C1# config`
`host1/C1(config)#`

3. Configure an ACL to allow traffic that requires NAT.
`host1/C1(config)# access-list ACL1 line 10 extended permit tcp 2001:DB8:1::/64 eq 8080 any`
or
`host1/C1(config)# access-list ACL1 line 10 extended permit tcp 10.0.0.0 255.0.0.0 eq 8080 any`
`host1/C1(config-acl)# exit`

Table 5-3 Static NAT Configuration Quick Start (continued)

Task and Command Example

4. Configure a local interface to filter and receive traffic that requires NAT.
`host1/C1(config)# interface vlan 100`
`host1/C1(config-if)# mtu 1500`
`host1/C1(config-if)# ip address 2001:DB8:3::100/64`
 	
or
 	
`host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0`
`host1/C1(config-if)# no shutdown`
`host1/C1(config-if)# exit`

5. Configure a second interface (global interface) for performing NAT.
`host1/C1(config)# interface vlan 101`
`host1/C1(config-if)# mtu 1500`
`host1/C1(config-if)# ip address 2001:DB8:2::101/64`
 	
or
 	
`host1/C1(config-if)# ip address 172.27.16.101 255.255.255.0`
`host1/C1(config-if)# no shutdown`
`host1/C1(config-if)# exit`

6. Configure a class map and define match criteria.
`host1/C1(config)# class-map match-any NAT_CLASS`
`host1/C1(config-cmap)# match access-list ACL1`
`host1/C1(config-cmap)# exit`

7. Configure a policy map and associate the class map with the policy map.
`host1/C1(config)# policy-map multi-match NAT_POLICY`
`host1/C1(config-pmap)# class NAT_CLASS`
`host1/C1(config-pmap-c)#`

Table 5-3 Static NAT Configuration Quick Start (continued)

Task and Command Example

8. Configure static NAT as a policy-map action.
`host1/C1(config-pmap-c)# nat static 2001:DB8::1/64 vlan 101`
 	
`or`
 	
`host1/C1(config-pmap-c)# nat static 192.0.0.0 netmask 255.0.0.0 vlan 101`
`host1/C1(config-pmap-c)# exit`
`host1/C1(config-pmap)# exit`
`host1/C1(config)#`

9. Activate the policy on an interface using a service policy.
`host1/C1(config)# interface vlan 100`
`host1/C1(config-if)# service-policy input NAT_POLICY`
`host1/C1(config-if)# Ctrl-Z`

10. (Optional) Save your configuration changes to flash memory. `host1/Admin# copy running-config startup-config`

11. Display and verify your static NAT and static port redirection configuration.
`host1/C1# show running-config class-map`
`host1/C1# show running-config policy-map`

Configuring an ACL for Static NAT and Static Port Redirection

Use an access control list (ACL) to permit the traffic that requires NAT. See the "Configuring an ACL" section. For details about configuring an ACL, see Chapter 1, Configuring Security Access Control Lists.

Configuring Interfaces for Static NAT and Static Port Redirection

Configure an interface for clients and an interface for the real servers. For details, see the *Routing and Bridging Guide, Cisco ACE Application Control Engine*.

Configuring a Class Map

You can configure a traffic class for static NAT and port redirection by using the **class-map** command in configuration mode. For more information about class maps, see the *Administration Guide, Cisco ACE Application Control Engine*.

The syntax of this command is as follows:

class-map match-any *name*

The *name* argument is a unique identifier for the class map, specified as an unquoted text string with a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# class-map match-any NAT_CLASS
host1/C1(config-cmap)#
```

To remove a class-map from the configuration, enter:

```
host1/C1(config)# no class-map match-any NAT_CLASS
```

Enter match criteria as required using the **match** command in class-map configuration mode. For example, enter:

```
host1/C1(config-cmap)# match access-list NAT_ACCESS
```

or

```
host1/C1(config-cmap)# match source address 192.168.12.15
```

To remove a match statement from a class map, enter:

```
host1/C1(config-cmap)# no match access-list NAT_ACCESS
```

Configuring a Policy Map

You can configure a traffic policy for NAT by using the **policy-map** command in configuration mode. For more information about policy maps, see the *Administration Guide, Cisco ACE Application Control Engine*.

The syntax of this command is as follows:

policy-map multi-match *name*

The *name* argument is the name assigned to the policy map. Enter an unquoted text string with no spaces and a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# policy-map multi-match NAT_POLICY
host1/C1(config-pmap)#
```

To remove a policy map from the configuration, enter:

```
host1/C1(config)# no policy-map multi-match NAT_POLICY
```

To associate the previously created class map with the policy map. For example, enter:

```
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)#
```

To dissociate a class map from a policy map, enter:

```
host1/C1(config-pmap)# no class NAT_CLASS
```

Configuring Static NAT and Static Port Redirection as a Policy Action

You can configure static NAT and static port redirection as an action in a policy map by using the **nat static** command in policy-map class configuration mode. Typically, you use static NAT and port redirection for DNAT. Static NAT allows you to identify local traffic for address translation by specifying the source and destination addresses in an extended ACL, which is referenced as part of the class map traffic classification. The ACE applies static NAT from the interface to which the traffic policy is attached (through the **service-policy** interface configuration command) to the interface specified in the **nat static** command.

The syntax of this command is as follows:

nat static *ip_address* **netmask** *mask* {*port1* | **tcp eq** *port2* | **udp eq** *port3*} **vlan** *number*

The keywords and arguments are as follows:

- **static** *ip_address*—Sets up a single static translation. The *ip_address* argument establishes the globally unique IP address of a host as it appears to the outside world. The policy map performs the global IP address translation for the source IP address specified in the ACL (as part of the class-map traffic classification).

Note The ACE supports static NAT only for IPv6 to IPv6 and IPv4 to IPv4 translations. Mixed mode is not supported.

- **netmask** *mask*—Specifies the subnet mask for the static IP address. Enter a subnet mask in dotted-decimal notation (for example, 255.255.255.0).
- *port1*—Global TCP or UDP port for static port redirection. Enter an integer from 0 to 65535.
- **tcp eq** *port2*—Specifies a TCP port name or number. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to match any port. Alternatively, you can enter a protocol keyword that corresponds to a TCP port number. See Table 5-4 for a list of supported well-known TCP port names and numbers.

Table 5-4 Well-Known TCP Port Numbers and Keywords

Keyword	Port Number	Description
ftp	21	File Transfer Protocol
http	80	Hypertext Transfer Protocol
https	443	HTTP over TLS/SSL
irc	194	Internet Relay Chat
matip-a	350	Mapping of Airline Traffic over Internet Protocol (MATIP) Type A
nntp	119	Network News Transport Protocol
pop2	109	Post Office Protocol v2
pop3	110	Post Office Protocol v3
rtsp	554	Real Time Streaming Protocol
smtp	25	Simple Mail Transfer Protocol
telnet	23	Telnet

- **udp eq** *port3*—Specifies a UDP port name or number. Enter an integer from 0 to 65535. A value of 0 instructs the ACE to match any port. Alternatively, you can enter a protocol keyword that corresponds to a UDP port number. See Table 5-5 for a list of supported well-known UDP port names and numbers.

Table 5-5 Well-Known UDP Port Numbers and Keywords

Keyword	Port Number	Description
dns	53	Domain Name System
wsp	9200	Connectionless Wireless Session Protocol (WSP)
wsp-wtls	9202	Secure Connectionless WSP
wsp-wtp	9201	Connection-based WSP
wsp-wtp-wtls	9203	Secure Connection-based WSP

- **vlan** *number*—Specifies the interface for the global IP address.

Note If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.

The following DNAT static port redirection example specifies the **nat static** command as an action for a static NAT policy map:

```
host1/C1(config)# policy-map multi-action NAT_POLICY
host1/C1(config-pmap)# class NAT_CLASS
host1/C1(config-pmap-c)# nat static 2001:DB8:1::/64 80 vlan 101

or

host1/C1(config-pmap-c)# nat static 192.168.12.0 255.255.255.0 80
vlan 101
```

To remove a NAT action from a policy map, enter:

```
host1/C1(config-pmap-c)# no nat static 2001:DB8:1::/64 80 vlan 101

or

host1/C1(config-pmap-c) no nat static 192.168.12.15 255.255.255.0
vlan 200
```

Applying the Static NAT and Static Port Redirection Policy Map to an Interface Using a Service Policy

You can activate the static NAT and port redirection policy and assign it to an interface by using the **service-policy** command in interface configuration mode. For details about the **service-policy** command, see the *Administration Guide, Cisco ACE Application Control Engine*.

Note You can configure static NAT as an input service policy only; you cannot configure it as an output service policy.

The syntax of this command is as follows:

service-policy input *policy_name*

The keywords and arguments are as follows:

- **input**—Specifies that the traffic policy is to be attached to the input direction of a VLAN interface. The traffic policy evaluates all traffic received by that interface.
- *policy_name*—Name of a previously defined policy map. The name can have a maximum of 64 alphanumeric characters.

For example, enter:

```
host1/C1(config)# interface vlan 100
host1/C1(config-if)# mtu 1700
host1/C1(config-if)# ip address 2001:DB8:1::/64
or
host1/C1(config-if)# ip address 192.168.1.100 255.255.255.0
host1/C1(config-if)# service-policy input NAT_POLICY
```

To remove a service policy from an interface, enter:

```
host1/C1(config-if)# no service-policy input NAT_POLICY
```

Note When you remove a traffic policy from the last VLAN interface on which you applied the service policy, the ACE automatically resets the associated service-policy statistics. The ACE performs this action to provide a new starting point for the service-policy statistics the next time that you attach a traffic policy to a specific VLAN interface.

Displaying NAT Configurations and Statistics

The following sections describe the commands used to display dynamic and static NAT and PAT configurations and statistics:

- Displaying NAT and PAT Configurations
- Displaying IP Address and Port Translations

Displaying NAT and PAT Configurations

You can display NAT and PAT configurations by using the **show running-config class-map** and **show running-config policy-map** commands in Exec mode.

For example, enter:

```
host1/C1# show running-config class-map
host1/C1# show running-config policy-map
```

Displaying IP Address and Port Translations

You can display IP address and port translation (Xlate) information by using the **show xlate** command in Exec mode.

IPv6 Syntax and Examples

The syntax of this command is as follows:

show xlate [**global** {*ipv6_address1* [*ipv6_address2/prefix_length*]}] [**local** {*ipv6_address3* [*ipv6_address4/prefix_length*]}] [**gport** *port1* [*port2*]] [**lport** *port1* [*port2*]]

The keywords, arguments, and options are as follows:

- **global** *ipv6_address1* [*ipv6_address2/prefix_length*]—(Optional) Displays information for a global IPv6 address or range of global IPv6 addresses to which the ACE translates source addresses for static and dynamic NAT. For a single global IPv6 address, enter the IPv6 address. To specify a range of IPv6 addresses, enter a second IPv6 address.

- **local** *ipv6_address3* [*ipv6_address4*/*prefix_length*]—(Optional) Displays information for a local IPv6 address or range of local IPv6 addresses. For a single local IPv6 address, enter the IPv6 address. To specify a range of local IPv6 addresses, enter a second IPv6 address.
- **gport** *port1 port2*—(Optional) Displays information for a global port or a range of global ports to which the ACE translates source ports for static port redirection and dynamic PAT, respectively. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.
- **lport** *port3 port4*—(Optional) Displays information for a local port or a range of local ports. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.

For example, enter:

```
host1/Admin# show xlate global 2001:DB8:1::3 2001:DB8:1::10/64 gport
100 200
```

IPv4 Syntax and Examples

The syntax of this command is as follows:

show xlate [**global** {*ip_address1* [*ip_address2* [**netmask** *mask1*]]}] [**local** {*ip_address3* [*ip_address4* [**netmask** *mask2*]]}] [**gport** *port1* [*port2*]] [**lport** *port1* [*port2*]]

The keywords, arguments, and options are as follows:

- **global** *ip_address1 ip_address2*—(Optional) Displays information for a global IP address or range of global IP addresses to which the ACE translates source addresses for static and dynamic NAT. For a single global IP address, enter the address in dotted-decimal notation (for example, 192.168.12.15). To specify a range of IP addresses, enter a second IP address.
- **netmask** *mask*—(Optional) Displays the subnet mask for the specified IP addresses.
- **local** *ip_address3 ip_address4*—(Optional) Displays the local IP address or range of local IP addresses. For a single local IP address, enter the address in dotted-decimal notation (for example, 192.168.12.15). To specify a range of local IP addresses, enter a second IP address.

- **gport** *port1 port2*—(Optional) Displays information for a global port or a range of global ports to which the ACE translates source ports for static port redirection and dynamic PAT, respectively. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.
- **lport** *port3 port4*—(Optional) Displays information for a local port or a range of local ports. Enter a port number as an integer from 0 to 65535. To specify a range of port numbers, enter a second port number.

For example, enter:

```
host1/Admin# show xlate global 172.27.16.3 172.27.16.10 netmask
255.255.255.0 gport 100 200
```

You can also use the **show conn** command to display NAT information. See the examples in the following sections.

This section contains the following topics:

Dynamic NAT Example

The following example output of the **show xlate** command shows dynamic NAT (SNAT in this example).

IPv6 Example

When you use Telnet from 2001:DB8:1::5 in VLAN 2020, the ACE translates it to 2001:DB8:2::1 in VLAN 2021.

```
host1/Admin# show xlate global 2001:DB8:1::1 2001:DB8:1::10
NAT from vlan2020:2001:DB8:1::5 to vlan2021:2001:DB8:2::1 count:1
```

IPv4 Example

When you use Telnet from 172.27.16.5 in VLAN 2020, the ACE translates it to 192.168.100.1 in VLAN 2021.

```
host1/Admin# show xlate global 192.168.100.1 192.168.100.10
```

```
NAT from vlan2020:172.27.16.5 to vlan2021:192.168.100.1 count:1
```

Dynamic PAT Example

The following example shows dynamic PAT.

IPv6 Example

When you use Telnet from 2001:DB8:1::5 in VLAN 2020, the ACE translates it to 2001:DB8:2::1 in VLAN 2021.

```
host1/Admin# show xlate
TCP PAT from vlan2020:2001:DB8:1::5/38097 to
vlan2021:2001:DB8:2::1/1025
```

IPv4 Example

When you use Telnet from 172.27.16.5 in VLAN 2020, the ACE translates it to 192.168.201.1 in VLAN 2021.

```
host1/Admin# show xlate
TCP PAT from vlan2020:172.27.16.5/38097 to vlan2021:192.168.201.1/1025
```

Static NAT Example

The following example shows static NAT.

IPv6 Example

The ACE maps real IP address 2001:DB8:1::5 to 2001:DB8:2::1.

```
host1/Admin# show xlate
NAT from vlan2020:2001:DB8:1::5 to vlan2021:2001:DB8:2::1 count:1

host1/Admin# show conn

conn-id    np dir proto source                              sport state
                  vlan  destination                         dport
----------+--+---+-----+--------------------------------+------+-----+
7          1  in  TCP   2001:DB8:1::5                     32748  ESTAB
                  2020  2001:DB8:2::1                      5000
6          1  out TCP   2001:DB8:2::1                      5000  ESTAB
                  2021  2001:DB8:1::5                     32748
```

IPv4 Example

The ACE maps a real IP address (172.27.16.5) to 192.168.210.1.

```
host1/Admin# show xlate
NAT from vlan2020:172.27.16.5 to vlan2021:192.168.210.1 count:1

host1/Admin# show conn

total current connections : 2

conn-id    dir prot vlan source           destination      state
----------+---+----+----+----------------+----------------+----------+
7          in  TCP  2020 172.27.16.5      192.168.100.1    ESTAB
6          out TCP  2021 192.168.100.1    192.168.210.1    ESTAB
```

Static Port Redirection (Static PAT) Example

The following example shows static port redirection (DNAT in this example).

IPv6 Example

A host at 2001:DB8:2::3/37766 uses Telnet to connect to 2001:DB8:5::12/3030 on VLAN 2021 on the ACE. The ACE maps 2001:DB8:1::5/23 on VLAN 2020 to 2001:DB8:5::12/3030 on VLAN 2021.

```
host1/Admin# show xlate
TCP PAT from vlan2020:2001:DB8:1::5/23 to vlan2021:2001:DB8:5::12/3030
Mar 24 2006 20:05:41 : %ACE-7-111009: User 'admin' executed cmd: show
xlate

host1/Admin# show conn

conn-id    np dir proto source                              sport state
                  vlan  destination                         dport
----------+--+---+-----+--------------------------------+------+-----+
7          1  in  TCP   2001:DB8:2::3                     37766  ESTAB
                  2021  2001:DB8:5::12                     3030
6          1  out TCP   2001:DB8:1::5                       23  ESTAB
                  2020  2001:DB8:2::3                      1025
```

IPv4 Example

A host at 192.168.0.10:37766 uses Telnet to connect to 192.168.211.1:3030 on VLAN 2021 on the ACE. The ACE maps 172.27.0.5:23 on VLAN 2020 to 192.168.211.1:3030 on VLAN 2021.

```
host1/Admin# show xlate
TCP PAT from vlan2020:172.27.0.5/23 to vlan2021:192.168.211.1/3030
Mar 24 2006 20:05:41 : %ACE-7-111009: User 'admin' executed cmd: show
xlate

host1/Admin# show conn

total current connections : 2

conn-id    dir prot vlan source           destination        state
----------+---+----+----+-----------------+-----------------+------+
6          in  TCP  2021 192.168.0.10:37766 192.168.211.1:3030 ESTAB
7          out TCP  2020 172.27.0.5:23      192.168.0.10:1025  ESTAB
```

Clearing Xlates

You can clear the global address-to-local address mapping information based on the global address, the global port, the local address, the local port, the interface address as the global address, and the NAT type by using the **clear xlate** command in Exec mode. When you enter this command, the ACE releases sessions that are using the translations (Xlates).

IPv6 Syntax and Examples

The syntax of this command is as follows:

clear xlate [{**global** | **local**} *start_ipv6_address* [*end_ipv6_address* [*/prefix_length*]]] [{**gport** | **lport**} *start_port* [*end_port*]] [**interface vlan** *number*] [**state static**] [**portmap**]

The keyword, arguments, and options are as follows:

- **global**—(Optional) Clears the active translation by the global IPv6 address.
- **local**—(Optional) Clears the active translation by the local IPv6 address.
- *start_ipv6_address*—Single IPv6 address or the starting global or local IPv6 address in a range of IPv6 addresses.
- *end_ipV6_address*—(Optional) Last IPv6 address in a global or local range of IPv6 addresses.
- ***/prefix_length***—(Optional) Specifies the prefix length for global or local IPv6 addresses.

- **gport**—(Optional) Clears active translations by the global port.
- **lport**—(Optional) Clears active translations by the local port.
- *start_port*—A single global port number or the starting global or local port number in a range of ports.
- *end_port*—(Optional) Last port number in a global or local range of ports.
- **interface vlan** *number*—(Optional) Clears active translations by the VLAN number.
- **state static**—(Optional) Clears active translations by the state.
- **portmap**—(Optional) Clears active translations by the port map.

Note If you configured redundancy, then you need to explicitly clear Xlates on both the active and the standby ACEs. Clearing Xlates on the active ACE alone will leave the standby ACE's Xlates at the old mappings.

For example, to clear all static translations, enter:

```
host1/Admin# clear xlate state static
```

IPv4 Syntax and Examples

The syntax of this command is as follows:

clear xlate [{**global** | **local**} *start_ipv4_address* [*end_ipv4_addres* [**netmask** *netmask*]]] [{**gport** | **lport**} *start_port* [*end_port*]] [**interface vlan** *number*] [**state static**] [**portmap**]

The keyword, arguments, and options are as follows:

- **global**—(Optional) Clears the active translation by the global IPv4 address.
- **local**—(Optional) Clears the active translation by the local IPv4 address.
- *start_ipv4_address*—A single global or local IPv4 address or the starting global or local IPv4 address in a range of IPv4 addresses. Enter an IPv4 address in dotted-decimal notation (for example, 172.27.16.10).
- *end_ipv4_address*—(Optional) Last IPv4 address in a global or local range of IPv4 addresses. Enter an IPv4 address in dotted-decimal notation (for example, 172.27.16.20).

- **netmask** *netmask*—(Optional) Specifies the network mask for global or local IPv4 addresses. Enter a mask in dotted-decimal notation (for example, 255.255.255.0).
- **gport**—(Optional) Clears active translations by the global port.
- **lport**—(Optional) Clears active translations by the local port.
- *start_port*—A single global or local port number or the starting port number in a range of global or local port numbers.
- *end_port*—(Optional) Last port number in a global or local range of ports.
- **interface vlan** *number*—(Optional) Clears active translations by the VLAN number.
- **state static**—(Optional) Clears active translations by the state.
- **portmap**—(Optional) Clears active translations by the port map.

Note If you configured redundancy, then you need to explicitly clear Xlates on both the active and the standby ACEs. Clearing Xlates on the active ACE alone will leave the standby ACE's Xlates at the old mappings.

For example, to clear all static translations, enter:

```
host1/Admin# clear xlate state static
```

NAT Configuration Examples

The following sections show typical scenarios that use dynamic and static NAT solutions:

- Dynamic NAT and PAT (SNAT) Configuration Example
- Server Farm-Based Dynamic NAT (SNAT) Configuration Example
- Static Port Redirection (DNAT) Configuration Example
- SNAT with Cookie Load Balancing Example

Dynamic NAT and PAT (SNAT) Configuration Example

The following SNAT configuration example shows the commands that you use to configure dynamic NAT and PAT on your ACE. In this SNAT example, packets that ingress the ACE from the 192.168.12.0 network are translated to one of the IP addresses in the NAT pool defined on VLAN 200 by the **nat-pool** command. The **pat** keyword indicates that ports higher than 1024 are also translated.

If you are operating the ACE in one-arm mode, omit interface VLAN 100 and configure the service policy on interface VLAN 200.

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0
255.255.255.0 1 72.27.16.0 255.255.255.0 eq http

class-map match-any NAT_CLASS
  match access-list NAT_ACCESS

policy-map multi-match NAT_POLICY
  class NAT_CLASS
    nat dynamic 1 vlan 200

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 200
  mtu 1500
  ip address 172.27.16.2 255.255.255.0
  nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0 pat
  no shutdown
```

Server Farm-Based Dynamic NAT (SNAT) Configuration Example

The following SNAT configuration example shows the commands that you use to configure server farm-based dynamic NAT on your ACE. In this SNAT example, real servers addresses on the 172.27.16.0 network are translated to one of the IP addresses in the NAT pool defined on VLAN 200 by the **nat-pool** command.

If you are operating the ACE in one-arm mode, omit interface VLAN 100 and configure the service policy on interface VLAN 200.

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0
255.255.255.0 1 72.27.16.0 255.255.255.0 eq http
```

```
rserver SERVER1
  ip address 172.27.16.3
  inservice
rserver SERVER2
  ip address 172.27.16.4
  inservice

serverfarm SFARM1
  rserver SERVER1
    inservice
  rserver SERVER2
    inservice
class-map type http loadbalance match-any L7_CLASS
  match http content .*cisco.com
class-map match-any NAT_CLASS
  match access-list NAT_ACCESS

policy-map type loadbalance http first-match L7_POLICY
  class L7_CLASS
    serverfarm SFARM1
    nat dynamic 1 vlan 200 serverfarm primary
policy-map multi-match NAT_POLICY
  class NAT_CLASS
    loadbalance policy L7_POLICY
    loadbalance vip inservice

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 200
  mtu 1500
  ip address 172.27.16.2 255.255.255.0
  nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0
  no shutdown
```

Static Port Redirection (DNAT) Configuration Example

The following DNAT configuration example shows those sections of the running configuration related to the commands necessary to configure static port redirection on your ACE. Typically, this configuration is used for DNAT, where

HTTP packets that are destined to 192.0.0.0/8 and ingressing the ACE on VLAN 101 are translated to 10.0.0.0/8 and port 8080. In this example, the servers are hosting HTTP on custom port 8080.

```
access-list acl1 line 10 extended permit tcp 10.0.0.0 255.0.0.0
eq 8080 any

class-map match-any NAT_CLASS
  match access-list acl1

policy-map multi-match NAT_POLICY
  class NAT_CLASS
    nat static 192.0.0.0 255.0.0.0 80 vlan 101

interface vlan 100
  mtu 1500
  ip address 192.168.1.100 255.255.255.0
  service-policy input NAT_POLICY
  no shutdown

interface vlan 101
  mtu 1500
  ip address 172.27.16.100 255.255.255.0
  no shutdown
```

SNAT with Cookie Load Balancing Example

The following configuration example shows those sections of the running configuration related to the commands necessary to configure SNAT (dynamic NAT) with cookie load balancing. Any source host that sends traffic to the VIP 20.11.0.100 is translated to one of the free addresses in the NAT pool in the range 30.11.100.1 to 30.11.200.1, inclusive. If you want to use PAT instead of NAT, replace “nat dynamic 1 vlan 2021” with “nat dynamic 2 vlan 2021” in the L7SLBCookie policy map.

```
server host http
  ip address 30.11.0.10
  inservice
serverfarm host httpsf
  rserver http
    inservice

class-map match-any vip4
  2 match virtual-address 20.11.0.100 tcp eq www
```

```
class-map type http loadbalance match-any L7SLB_Cookie
  3 match http cookie JG cookie-value ".*"

policy-map type loadbalance first-match L7SLB_Cookie
  class L7SLB_Cookie
    serverfarm httpsf
policy-map multi-match L7SLBCookie
  class vip4
    loadbalance vip inservice
    loadbalance L7SLB_Cookie
    nat dynamic 1 vlan 2021  <<<<<<<<<<

interface vlan 2020
  ip address 20.11.0.2 255.255.0.0
  alias 20.11.0.1 255.255.0.0
  peer ip address 20.11.0.3 255.255.0.0
  service-policy input L7SLBCookie <<<<<<<<<<<<<<<<
   no shutdown
interface vlan 2021
  ip address 30.11.0.2 255.255.0.0
  alias 30.11.0.1 255.255.0.0
  peer ip address 30.11.0.3 255.255.0.0
  fragment min-mtu 68
  nat-pool 2 30.11.201.1 30.11.201.1 netmask 255.255.255.255 pat
  nat-pool 3 30.11.202.1 30.11.202.3 netmask 255.255.255.255
  nat-pool 1 30.11.100.1 30.11.200.1 netmask 255.255.255.255 <<<<<<<<<
  no shutdown
```