

This article describes ACE network address translation (NAT), how to configure it, and how to troubleshoot issues with NAT that you may encounter.

Guide Contents
<u>Main Article</u>
<u>Overview of ACE Troubleshooting</u>
<u>Understanding the ACE Module Architecture and Traffic Flow</u>
<u>Preliminary ACE Troubleshooting</u>
<u>Troubleshooting ACE Boot Issues</u>
<u>Troubleshooting with ACE Logging</u>
<u>Troubleshooting Connectivity</u>
<u>Troubleshooting ACE Appliance Ethernet Ports</u>
<u>Troubleshooting Remote Access</u>
<u>Troubleshooting Access Control Lists</u>
<u>Troubleshooting Network Address Translation</u>
<u>Troubleshooting ACE Health Monitoring</u>
<u>Troubleshooting Layer 4 Load Balancing</u>
<u>Troubleshooting Layer 7 Load Balancing</u>
<u>Troubleshooting Redundancy</u>
<u>Troubleshooting SSL</u>
<u>Troubleshooting Compression</u>
<u>Troubleshooting Performance Issues</u>
<u>ACE Resource Limits</u>
<u>Managing ACE Resources</u>
<u>Show Counter Reference</u>

Contents

- [1 Overview of ACE Network Address Translation](#)
- [2 NAT Configuration Guidelines and Restrictions](#)
- [3 Configuring Dynamic NAT and PAT](#)
- [4 Configuring Server-Farm Based Dynamic NAT](#)
- [5 Configuring Static NAT and Port Redirection](#)
- [6 Configuring SNAT with Cookie and Load Balancing](#)
- [7 Troubleshooting ACE NAT and PAT](#)

Overview of ACE Network Address Translation

You can configure the ACE to translate a client source IP address to a routable address in the server's network. This process is called source NAT (SNAT). If you want to preserve the client source IP address, do not configure SNAT.

You can also configure the ACE to translate the private address of a server to a global IP address that is accessible to clients. This process is called destination NAT (DNAT) and protects the server by hiding its real IP address from the Internet.

Besides translating IP addresses, you can configure the ACE to translate TCP and UDP ports. This process is called port address translation (PAT).

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

NAT Configuration Guidelines and Restrictions


When you configure NAT and PAT on your ACE, keep in mind the following NAT and PAT guidelines and restrictions:

- If a packet egresses an interface that you have not configured for NAT, the ACE transmits the packet untranslated.
- You can configure dynamic NAT or static NAT as an input service policy only; you cannot configure it as an output service policy.
- 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 Dynamic NAT and PAT

Dynamic NAT is typically used for SNAT. When you configure dynamic NAT and PAT, be sure to configure an interface for the client-side VLAN and an interface for the server-side VLAN.

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.

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

```
access-list NAT_ACCESS line 10 extended permit tcp 192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0

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
```

Configuring Server-Farm Based Dynamic NAT

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 server 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.

 **Note:** 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 192.168.12.0 255.255.255.0 172.27.16.0 255.255.255.0

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

```

Configuring Static NAT and Port Redirection

The following DNAT configuration example shows those sections of the running configuration that are related to the commands necessary to configure static NAT and 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 ingress 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

```

Configuring SNAT with Cookie and Load Balancing

The following configuration example shows those 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 L7SLB Cookie 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 L7SLB_Cookie
  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 L7SLB_Cookie
  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

```

Troubleshooting ACE NAT and PAT

To verify your NAT and PAT configurations and make any necessary corrections, follow these steps:

1. Display your NAT and PAT configurations by entering the following commands:

```
ACE_module5/Admin# show running-config class-map
```

```
class-map match-any L4_CLASS
  2 match access-list ACL1
```

```
ACE_module5/Admin# show running-config policy-map
```

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

```
ACE_module5/Admin# show service-policy NAT_POLICY
```

```
Status      : ACTIVE
```

```
-----
Interface:  vlan 100
  service-policy: NAT_POLICY
    class: NAT_CLASS
      nat:
        nat dynamic 1 vlan 200
        curr conns      : 0           , hit count      : 0
        dropped conns   : 0
        client pkt count : 0           , client byte count: 0
        server pkt count : 0           , server byte count: 0
        conn-rate-limit  : 0           , drop-count     : 0
        bandwidth-rate-limit : 0       , drop-count     : 0
```

```
ACE_module5/Admin# show running-config interface
```

```

interface vlan 100
 ip Address 192.168.12.2
 mtu 1500
 service-policy input NAT_POLICY
 no shutdown
interface vlan 200
 ip address 172.27.16.2 255.255.255.0
 mtu 1500
 access-group input acl1
 nat-pool 1 172.27.16.15 172.27.16.24 netmask 255.255.255.0 pat
 no shutdown

```

2. Use the **show xlate** command to verify that dynamic NAT and PAT, and static NAT and port redirection, are taking place properly.

Dynamic NAT Example

The following example output of the **show xlate** command shows dynamic NAT (SNAT in this example). When you use Telnet from IP address 172.27.16.5 in VLAN 2020, the ACE translates it to IP address 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. When you use Telnet from IP address 172.27.16.5 port 38097 in VLAN 2020, the ACE translates it to IP address 192.168.201.1 port 1025 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. The ACE maps real IP address 172.27.16.5 to IP address 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). A host at IP address 192.168.0.10:37766 uses Telnet to connect to IP address 192.168.211.1:3030 on VLAN 2021 on the ACE. The ACE maps IP address 172.27.0.5:23 on VLAN 2020 to IP address 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

3. To display the NAT policy and pool information for the current context, enter the **show nat-fabric** command. The syntax of this command is as follows:

```
show nat-fabric { policies | src-nat policy_id mapped_if | dst-nat static_xlate_id | nat-pools | implicit-pat | global-static }
```

policies -- Displays the NAT policies.

src-nat *policy_id mapped_if* -- Displays the specified source NAT policy information. To obtain the values for the *policy_id* and *mapped_if* arguments, view the *policy_id* and *mapped_if* fields displayed by the **show nat-fabric policies** command.

dst-nat *static_xlate_id* -- Displays the static address translation for the specified static XLATE ID. To obtain the value for the *static_xlate_id* argument, view the *static_xlate_id* field displayed by the **show nat-fabric policies** command.

nat-pools -- Displays NAT pool information for a dynamic NAT policy.

implicit-pat -- Displays the implicit PAT policies.

global-static -- Displays global static NAT information when the **static** command in global configuration mode is configured.

```
ACE_module5/Admin# show nat-fabric policies
```

```
Nat objects:
```

```
NAT object Hash Bucket: 9
```

```
  NAT object ID:2 mapped_if:8 policy_id:1 type:DYNAMIC nat_pool_id:4
    Pool ID:4 PAT:1 pool_id:1 mapped_if:8 Ref_count:1 ixp_binding:in all IXPs
    lower:172.27.16.15 upper:172.27.16.24 Bitmap-ID:40
    List of NAT object IDs: 2
```