ERICSSON

Configuring NAT Policies

SYSTEM ADMINISTRATOR GUIDE

28/1543-CRA 119 1170/1-V1 Uen E

Contents

1 Overview

This document provides an overview of the Network Address Translation (NAT) policy features supported by the SmartEdge® router and describes the tasks used to configure, monitor, and administer NAT policy. This document also provides configuration examples of NAT policies.

Global IPv4 addresses from the IANA pool will run out because they are in a short supply. As a result, carriers need to move from IPv4 services to IPv6. However, deploying IPv6 takes a long time. NAT extends IPv4 addresses. ISPs can place NAT devices between end users and the public Internet to suppress global IPv4 address consumption.

Traditional NAT - CPE NAT – appears at the edge of the customer network, where it connects to a service provider and translates between private IPv4 addresses within the customer network and a public address assigned by the provider. Carrier Grade NAT (CGN) appears within the service provider network. Both translate between private and public IPv4 addresses, the private side of the CGN faces the provider's customer. CGN appears as the most acceptable solution to manage both IPv4 exhaustion and Dual stack IP addressing while facing IPv4 exhaustion by sharing one global IPv4 address within multiple users. It will help customers to optimize usage of IPv4 pools, thus potentially delaying and optimizing introduction of IPv6.

Through NAT, hosts using unregistered IP addresses on an internal, private network can connect to hosts on the Internet, and conversely. NAT translates the private (not globally unique) addresses in the internal network into public IP addresses before packets are forwarded onto another network. Network Address and Port Translation (NAPT) translates a private network and its Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port on the internal network into a public address and its TCP/UDP ports. By using port multiplexing, NAPT enables multiple hosts on a private network to simultaneously access remote networks through a single IP address.

NAT policies can contain a combination of static and dynamic translation actions as well as drop and ignore actions, and can be applied to all packets traveling across a circuit, or to a particular class of packets using a policy access control list (ACL).

Note: NAT policies are not supported for subscriber sessions that use the Layer 2 Tunneling Protocol (L2TP) and that are terminated at the SmartEdge router when it is acting as an L2TP network server (LNS). If you inadvertently apply a NAT policy to such a subscriber, the session comes up because the policy has no effect on it.

Figure 1 illustrates how NAT translates private source IP addresses to public addresses.

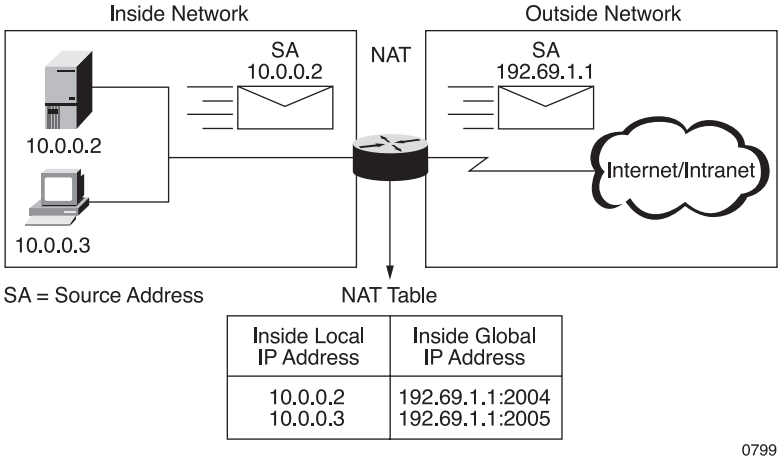

Figure 1 NAT Process (799)

The SmartEdge 800 router supports traditional NAT as well as enhanced NAT. For information about enhanced CGNAT functionality, see Section 1.7 on page 7. In traditional NAT, sessions are unidirectional, outbound from the private network. Sessions in the opposite direction may be allowed on an exception basis, using static address maps for preselected hosts. It is assumed that NAT policies are applied on private interfaces only because applying them on public interfaces would profoundly affect performance.

Note: Traditional NAT is also known as source NAT or SNAT.

Note: In this document, the terms, incoming and outgoing, refer to the direction of the packets passing through the interface. The terms, outbound and inbound, refer to the direction of the packet flow from the private network to the public network, and from the public network to the private network, respectively.

Note: On the SmartEdge router, NAPT does not support fragmented packets. Fragmentation is supported in basic NAT (one-to-one IP address mapping).

The SmartEdge router implementation of NAT is described in the following sections.

1.1 Static Translation

With static translation, the private source IP addresses and TCP or UDP ports and the NAT addresses and the ports to which they are translated are fixed numbers.

Note: When just the IP address is translated, static NAT is referred to as basic static NAT. Static NAT includes both basic static NAT and static NAPT.

Note: Static translations require manual configuration of the static IP routes and the static IP ARP entries for the NAT addresses.

1.2 Dynamic Translation

With dynamic translation, the SmartEdge router translates the private source IP addresses and TCP or UDP ports to the NAT addresses and ports. At runtime, the SmartEdge router selects the NAT addresses and ports from a pool of global IP addresses (referred to as a NAT pool). With dynamic translation, you can also modify the period after which translations time out.

NAPT also supports dynamic translation of subsets of TCP/UDP ports, referred to as port blocks. The port number space of the TCP/UDP ports is divided into 16 port blocks, numbered 0 to 15; each port block consists of 4,096 port numbers. Port block granularity allows the sharing of a single IP address between NAT pools, and thus between NAT policies and traffic cards, with each pool having the IP address with a unique subset of TCP/UDP port blocks assigned to it.

Note: When just the IP address is translated, dynamic NAT is referred to as basic dynamic NAT. Dynamic NAT includes both basic dynamic NAT and dynamic NAPT.

1.3 Policy ACLs

A policy ACL defines classes of packets using classification statements (rules). Each policy ACL supports up to eight unique classes. You can classify a packet according to its IP precedence value, protocol number, IP source and destination address, Internet Control Message Protocol (ICMP) attributes, Internet Group Management Protocol (IGMP) attributes, TCP attributes, or UDP attributes.

When you include the **`destination`**, **`drop`**, **`ignore`**, **`pool`**, **`admission-control`**, and **`timeout`** commands (in NAT policy configuration mode) in a NAT policy, the specified action is applied to all packets traveling across the interface or subscriber circuit or, if an ACL is referenced, to packets that do not belong to the classes specified by the ACL and by the NAT policy. These packets are referred to as belonging to the default class.

NAT policies can contain a combination of static and dynamic translation actions as well as drop and ignore actions, and can be applied to all packets traveling across a circuit, or to a particular class of packets using a policy access control list (ACL). The default NAT policy action is "drop".

When you include the **`destination`**, **`drop`**, **`ignore`**, **`pool`**, **`admission-control`**, and **`timeout`** commands (in class configuration mode) in a policy ACL, the specified action is applied only to packets belonging to the specified class.

Note: The **`pool`** and **`timeout`** commands apply only to dynamic NAT. The **`admission-control`** and **`destination`** commands apply only to dynamic NAPT.

The order in which the conditions in a NAT policy are checked to determine the action for a packet is as follows: T

1 The conditions set by the policy static translations.

2 The conditions set by the policy ACL.

If the conditions in step 1 and step 2 are not satisfied, the action for the packet is determined by the default class action if the policy ACL exists, or by the NAT policy action.

To configure class-based actions for a circuit, you apply a policy ACL to a NAT policy, specify the action for each class that you want the policy to take, and then attach the NAT policy to the circuit. For more information about policy ACLs, see *Configuring ACLs*.

1.3.1 Policy ACL Configuration Example

```
context local
!
 ip nat pool pool1 napt multibind
  address 100.1.1.5/32
!
 policy access-list NAT-ACL
  seq 10 permit ip 10.1.1.0 0.0.0.255 class NAT
!
 nat policy nat-policy
! Default class
  drop
! Named classes
  access-group NAT-ACL
   class NAT
    pool pool1 local
!
 interface if-private
  ip nat nat-policy
!
end
```

1.4 Destination IP Address Translation

The SmartEdge router allows you to configure a NAT policy or its class to use a specified destination IP address instead of the original destination IP address. Using the **destination** command, you can configure Destination NAT (DNAT) to redirect traffic destined for the original address to a different specified address. On the return path, the source address of the incoming traffic is translated to the original destination address of the outgoing packet, so the returning traffic appears to be sent from the original destination address.

You can enable DNAT with or without the SmartEdge router having to perform NAT.

You can use DNAT both with and without NAT in the same configuration.

1.5 NAT DMZ

The SmartEdge router also provides support for the demilitarized zone (DMZ) feature in NAT policies. You can configure a DMZ rule in a NAT policy to translate traffic returning to the SmartEdge router that does not satisfy any of the conditions for static or dynamic NAT that you have specified in that NAT policy. The basic NAT specified by the DMZ rule changes the destination IP address of the packet to a fixed private IP address of a DMZ host server without changing the TCP/UDP port number.

Three types of applications might require a DMZ host server:

- You use your own tools to do extensive logging and analysis of the packets that would be dropped by the NAT policy.
- You do not know the exact TCP/UDP port numbers, or there are too many ports, that need to be opened by static NAPT rules to allow access to applications.
- You need a work around for applications that do not work with NAPT, because they use protocols other than UPD or TCP, or require IP packet fragmentation.

The following differences apply to a private network with a DMZ host server:

- A DMZ rule in a NAT policy does not affect non-DMZ hosts on the internal network that use static or dynamic NAPT, except that returning traffic for dynamic UDP sessions are now subject to source IP address verification.
- Non-DMZ hosts can use basic static or basic dynamic NAT, although such configurations might not seem practical.
- The DMZ host server cannot use basic static NAT, basic dynamic NAT, and dynamic NAPT, but can still use static NAPT.

1.6 Session Limit Control

Session limit control allows you to set session limits independently for TCP, UDP, and ICMP sessions from the subscriber to the network. The SmartEdge 800 router does not limit sessions from the network to the subscriber.

Note: In this document, the terms, session and connection, refer to a request to establish a connection between a subscriber port (that is, an IP address and port tuple) and a host port (represented by an IP address and port tuple). These requests can be initiated from a subscriber or from a host, but you can only enable the SmartEdge router to limit the requests initiated by the subscriber or initiated on another system, sent to the subscriber, and accepted by that subscriber.

When multiple sessions are initiated from the same IP address and port number on the subscriber side, they are counted as a single connection by the operating system.

When the action of a NAT policy or a class in a NAT policy is ignored, you can use the NAT policy only for the purpose of session limit control, without any NAT.

The following restrictions apply to the NAT implementation of session limit control:

- Session limit control is a modification of a NAT policy; it applies to any circuit that has that NAT policy attached.
- Session limit control is supported on Ethernet, Gigabit Ethernet, and ATM OC-3 traffic cards.
- The SmartEdge router applies the session limit at the IP level; it is available for LNS circuits, but not when the SmartEdge router is configured as an L2TP access concentrator (LAC)
- You can set a session limit to support up to 65,535 sessions on a circuit.

  Note: The sum of the configured session limit control numbers for a traffic card can exceed the maximum number of sessions (approximately one million) allowed by the amount of memory on the traffic card. In that case, some circuits might be unable to reach their configured maximum session limit.

1.7 Enhanced NAT Policy with Paired Mode and Logging

The SmartEdge router allows you to configure an enhanced NAT policy that supports logging and paired mode.

Carrier-grade NATs typically have pools containing multiple addresses. NATs can map internal addresses to external addresses either in an arbitrary way or by always mapping an internal IP address to the same external IP address. NATs using the first method have the IP address pooling behavior of “Arbitrary” while the second method is called “Paired” (paired mode).

Arbitrary pooling behavior hides the internal IP address assigned to specific endpoints. However this pool behavior can break applications that use several ports from the same endpoint but do not negotiate IP addresses individually. Typical examples are peer-to-peer applications that are not able to negotiate IP addresses for Real-Time Transport Protocol (RTP) and Real-Time Transport Control Protocol (RTCP) separately. Therefore, it is important for these applications that NAT has an IP address pooling configured to use paired mode.

When all the external IP addresses and ports are used from the pool, there will be complete traffic loss for the newly initiated sessions. As result, you need to carefully design your pools based on number of subscribers, number of line cards, expected traffic, and paired mode. If this happens and NAT ICMP generation is enabled, an IP error message is sent to the user. An incorrectly designed NAT configuration can negatively impact service and even cause a line card crash due to memory exhaustion as the maximum number of allocated translations are not limited.

The configuration must also ensure that the maximum supported number of translations are not exceeded by limiting the following:

- Subscribers allowed to come up on a card
- NAT pools
- Available ports in a NAT pool

With paired mode, you can also limit the maximum number of IP addresses downloaded to a card by correctly configuring the over-subscription ratio and the maximum number of subscribers.

1.7.1 Paired Mode

When paired mode is configured, an internal address (for example, a subscriber) is bound to an external address when the first translation is created. From that point on, outgoing packets are translated to this IP address during the lifetime of the subscriber session are given the same external address, even if this means NAT is not able to allocate more translations, despite having other free IP addresses in the pool.

Assigning a paired mode pool to an enhanced NAT policy ensures that a subscriber with the policy always gets the same external IP address. If the paired mode pool is already assigned to a class, then other pools cannot be assigned to the same policy.

You can apply paired mode settings in a NAT pool with the type "NAPT". You can also assign pools using paired mode behavior to either regular classes or the default class in a policy.

1.7.2 NAT Logging Profile

When you configure a NAT logging profile, an assignment time is logged when a NATed IP address or a port block is assigned to a subscriber or circuit.

When you configure a valid NAT logging profile and assign it to a pool, the logging profile must be valid (all the mandatory fields give in the profile).

Un-assignment time is logged in the following conditions:

- The port block is unassigned by the timer due to idle timeout.
- The subscriber goes down because the circuit is unbound.
- The pool or policy is deleted.
- The pool action is changed for a class under a policy.

Note: You can only configure two logging profiles for each pool.

1.7.3 NAT Logging Suboptions

The following suboptions are available in NAT logging profile configuration mode.

- *dscp*

  This command configures the DSCP value of the IP packet.

- *export-version v9*

  This command configures the external collector to use version 9 formatting when exporting flow records.

- *maximum ip-packet-size*

  This command configures the maximum size of the IP packet in bytes.

- *source*

  This command configures the source IP address and port number to put into the NetFlow packet for a NAT logging profile.

- *transport-protocol udp (NAT)*

  This command configures the transport protocol used to export the flow records.

1.7.4 Enhanced NAT Policy and Pool

The enhanced NAT policy also supports the following options:

- P2MP TCP
- *Inbound refresh settings for UDP*
- *Exclusion of port ranges from a pool*
- *ICMP notification when rejecting outbound flows*

The enhanced NAT policy supports port block configuration for IP ranges and exclusion of port ranges. These options can be also be used by non-enhanced policies. A CGNAT license is required to be able to configure and use these enhancements in pools. For more information about this option, see the *exclude* command.

1.7.5 SmartEdge Router Specific Logging Field Types

The export entity uses Cisco Systems NetFlow export format version 9 (v9) to export flow records. When you use this format, NAT records are made up of a header and a sequence of flow data or template FlowSets. The data template describes the fields that are present in data FlowSets. The data FlowSets might occur later in the same export packet or in subsequent export packets.

To use your own collector, you might need to modify the collector (the NetFlow collector's configuration) to accept the following new SmartEdge router specific field types.

Table 1 SmartEdge Router Specific Logging Field Types

Field Type	Value	Length (bytes)	Description
NAT_LOG_FIELD_IDX_CONTEXT_ID = 0	24628	4	Internal context ID
NAT_LOG_FIELD_IDX_CONTEXT_NAME	24629	64	Zero terminated context Name
NAT_LOG_FIELD_IDX_ASSIGN_TS_SEC	24630	4	Seconds of UNIX timestamp for assign
NAT_LOG_FIELD_IDX_UNASSIGN_TS_SEC	24631	4	Seconds of UNIX timestamp for unassign
NAT_LOG_FIELD_IDX_IPV4_INT_ADDR	24632	4	Internal IPv4 address
NAT_LOG_FIELD_IDX_IPV4_EXT_ADDR	24633	4	External IPv4 address
NAT_LOG_FIELD_IDX_EXT_PORT_FIRST	24634	2	External L4 port start
NAT_LOG_FIELD_IDX_EXT_PORT_LAST	24635	2	External L4 port end

1.7.6 Restrictions and Limitations

1.7.6.1 Licensing

To configure enhanced carrier grade NAT features on the SmartEdge router, you must have enabled the NAT enhanced license with the **`nat enhanced password`** ***`nat_password`*** command. For information about enabling NAT licensed features, see *Enabling Licensed Features*.

1.7.6.2 Pools and Policy Limitations

With an enhanced NAT policy, the SmartEdge router does not support configuration changes to pools and policies that are already bound because doing so will negatively affect service. In some cases the CLI restricts you from making these changes. As a result, you must completely unbound policies and then bind them for the changes to take full effect.

Note: You can only configure two logging profiles for each pool.

1.7.6.3 Circuit Limitations

These features are supported on the following subscriber circuits:

- CLIPS
- DHCP
- Hitless access link aggregation groups (LAG) (only **`maximum-links 1`** is supported)
- Economical access link aggregation groups (LAG)
- LNS
- MLPPP

- PPPoE

The following are not supported:

- Pseudo circuits except MLPPP
- Static circuits

1.7.6.4 Limitations Common to Access LAG (Hitless and Economical) and LNS

Access LAG and LNS will only work for subscriber circuits with enhanced NAT policy applied. Configuration of an enhanced NAT policy requires the presence of the NAT enhanced license. The CLI does not check whether an enhanced NAT policy is configured when bringing up a subscriber. If a non-enhanced NAT policy is applied to a LAG or LNS terminated subscriber, the subscriber will not come up, even if the NAT enhanced license is configured.

When subscribers are re-homed to a new card, for example, because of a card or port failure, paired IP addresses and all existing NAT translations are lost because they are stored only on the home slot and not synchronized across cards. If subscribers are re-homed to the same card, for example, if the active link moves to a different port on the same card, existing NAT translations are not lost. If subscribers are re-homed to a new card for any reason other than a card reload, there is a transient period while new translations are being created on the new home slot and translations on the old home slot are being cleaned up. In this situation, inbound traffic uses the old translations during the transient period.

1.7.6.5 Hitless Access LAG Limitations

Subscriber circuits on hitless access LAG with multiple active links is not supported. Subscriber traffic must be routed through a single slot (the home slot) because NAT translations are not synchronized across line cards. The system must be configured so that outbound traffic from a given subscriber only flows through the subscriber's home slot using the **`maximum-links 1`** command. For more information, see *maximum-links*.

The number of IP addresses required in the NAT pool is greater for subscriber circuits on hitless access LAG than for the general case. At a minimum, the number required for hitless access LAG is the amount required in the general case plus the additional slots involved in the hitless access LAG configuration. In the worst case (paired-mode configuration), the IP addresses required is the amount required for the general case multiplied by the total number of slots used for hitless access LAG. For example, 10 IP addresses are required in a non-hitless access LAG environment. In a hitless access LAG environment on two slots, the minimum number is 11 (10, plus 1 for the additional slot used), and the maximum number is 20 (10 times 2 slots used in total). Because hitless access LAG can only operate on one slot at a time, the additional IP addresses required are not actively used for translations on the standby slots.

Static rules, DNAT, and DMZ are not supported for hitless access LAG subscribers.

1.7.6.6 Economical Access LAG Limitations

The number of IP addresses required in the NAT pool is greater for subscriber circuits on economical access LAG than for the general case. This is due to a situation that can occur during subscriber re-homing. The NAT pool, with its downloaded port blocks, is not deleted from a slot until the last subscriber unbind has occurred. So, for proper operation during subscriber re-homing, at least one more IP address than the number used on the active slot is required to prevent newly re-homed subscriber traffic from being blocked. In the worst case, the number of additional IP addresses required is equal to the number of IP addresses on the most loaded active slot that uses economical LAG.

1.7.6.7 Paired Mode Limitations

- Paired mode and logging is only available for subscriber interfaces.
- You cannot mix paired and non-paired pools in a policy.
- If paired mode is used, adding more IP addresses to the pool and decreasing the over-subscription rate results in more memory usage and less efficient use of available port ranges across subscribers.

1.7.6.8 Logging Limitations

- A single micro block is always assigned to a single subscriber, no matter how many ports are used. When logging is enabled, the sharing of ports across multiple subscribers are more limited because even if only one port is used by a subscriber, multiple ports (the whole microblock) are reserved from the pool.
- Using multiple profiles downloaded to a card can result in performance degradation because packet streams are maintained and assembled for each NAT logging profile.
- Configuring static entries with logging causes less efficient use of ports even if only one static entry is configured, multiple ports (the whole microblock) are reserved from the pool.
- You can only configure two logging profiles for each pool.

1.7.6.9 Exclude Limitations

The granularity to excluded ports (by using the **`exclude`** command) is based on the micro port block size (the port range assigned to a subscriber in case of logging). For example, when the micro port block size is 32, then excluding port 0 removes all the ports from 0 to 31.

You cannot configure more than four excludes per IP or address range when you use the **`exclude`** command. Specifying a fifth exclude option displays an error message.

1.7.7 Example

This example shows the subscriber configuration. The subscriber pool is created under the interface pppoe-subs. The pool is connected to the default subscriber together with the NAT policy. The PPPoE authentication is then bound to the private (subscriber) facing port and the actual bind happens only when the subscriber is authenticated.

```
configure
!
software license
 nat enhanced password enhanced-nat-password   <--Enable the license for enhanced NAT features
!
context nat-context
!
 nat logging-profile nat-log-profile           <--Create a NAT logging profile
  transport-protocol udp
  export-version v9
  source 10.2.1.1 port 4242
  destination 10.2.1.2 context nat-context port 8989
  dscp ef
  maximum ip-packet-size 1400
!
ip nat pool nat-pool napt paired logging        <--Configure an Enhanced NAT pool


 logging-profile nat-log-profile
 paired-mode subscriber over-subscription 100 port-limit 2000
 address 100.1.1.1 to 100.1.1.20 port-block 0 to 15
  exclude well-known   <-Excludes TCP and UDP ports 0-1023 from the entire pool
  exclude 5888 to 6015 <-Excludes a given port range from the given address or address range of a pool
!
 policy access-list nat-acl
  seq 10 permit udp 192.168.0.0 0.0.255.255 192.168.100.0 0.0.0.255 class voip-class
  seq 20 permit icmp 192.168.0.0 0.0.255.255 any class nat-class
  seq 30 permit udp 192.168.0.0 0.0.255.255 any class nat-class
  seq 40 permit tcp 192.168.0.0 0.0.255.255 any class nat-class
!
 nat policy nat-policy enhanced               <--Create an enhanced NAT policy
! Default class
  drop
! Named classes
  access-group nat-acl                        <--Configure an Access Group and Class
   class voip-class
    ignore
   class nat-class
    pool nat-pool nat-context                 <--Refer to the enhanced NAT pool

    endpoint-independent filtering tcp
    endpoint-independent filtering udp
    inbound-refresh udp
    timeout abandoned 3600
    icmp-notification
!
 interface pppoe-subs multibind
  ip address 192.168.1.1/20
  ip pool 192.168.1.0/20 name pppoe-pool       <--Set up a subscriber pool

!
 interface exporter
  ip address 10.2.1.1/30
!
 interface public
  ip address 10.1.1.1/24
!
 subscriber default                           <--Apply NAT policy to default subscribers
   ip address pool name pppoe-pool
   nat policy-name nat-policy
!
 subscriber name user                         <-- Apply NAT policy to default subscribers
   password password
!
port ethernet 2/5
```

```
 no shutdown
 bind interface exporter nat-context
!
port ethernet 2/6                                <--Bind to the private facing port

 no shutdown
 encapsulation pppoe
   bind authentication chap context nat-context maximum 2000  <--Bind interface to the public facing port

!
port ethernet 4/5
 no shutdown
 bind interface public nat-context
!
end
```

1.8 NAT and Point-to-Multipoint UDP and TCP Traffic

The SmartEdge router supports point-to-multipoint (P2MP) scenarios using Endpoint-Independent Filtering, as described in the following documents:

- RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP, REQ 8*
- RFC 5382, NAT behavioral requirements for TCP

P2MP traffic is common in many applications, such as multimedia communications and online gaming. In these scenarios, an internal host initiates multiple simultaneous sessions from a single endpoint (which are defined by its private IP address, private port, and UDP or TCP port) and sends it to multiple distinct endpoints on the external network.

Enabling endpoint independent filtering allows point to multi-point traffic and disables firewall for the specific transport protocol in the current class.

To enable endpoint-independent filtering on UDP or TCP traffic, issue the **`endpoint-independent filtering udp`** or **`endpoint-independent filtering tcp`** command, respectively, (in NAT policy or NAT policy class configuration mode). Specify either an existing address pool (by using the pool command) or the "ignore" action (using the ignore command).

You can apply endpoint-independent filtering:

- At the class level within a NAT policy, so that P2MP traffic can be enabled for selected UDP or TCP traffic streams.
- To the default class at the policy level.

Note: You must first configure an enhanced NAT policy to configure the **`endpoint-independent filtering tcp`** command.

When P2MP mode is enabled, it is applied to all UDP or TCP traffic in the class respectively. This can make the private host initiating UDP or TCP traffic from a given port susceptible to UDP or TCP traffic from any host through

that port; care should be taken to protect the initiating host from a Denial of Service (DoS) attack.

When you enable endpoint-independent filtering, the change applies only to new NAPT sessions; P2MP functionality is not added to existing sessions.

When you disable endpoint-independent filtering, the change applies only to new NAPT sessions; P2MP functionality is not removed for existing sessions.

When endpoint-independent filtering is used with a DMZ, filtering limits the DMZ functionality. If the P2MP NAT IP addresses configured for the class overlap with those in the DMZ rules, then return traffic to the private host (from which the UDP or TCP traffic initiated) is treated differently. For example, in cases where return NAPT traffic would be dropped because the return source destination does not match the original outgoing destination IP address ("destination address mismatch"), traffic is not dropped as expected, but is translated and sent to the private host from which the UDP or TCP traffic originated. If the return traffic is dropped for other reasons than a destination address mismatch, the traffic is dropped as expected and redirected to the DMZ server.

If the return traffic is dropped for other reasons than a destination address mismatch, the traffic is dropped as expected and redirected to the DMZ server.

- You cannot enable Endpoint-Independent Filtering with an action of "drop"; if you configure an action of "drop" for the class, the system returns a warning. If you do configure an action of "drop" for the class, the system disables Endpoint-Independent Filtering.

- You cannot use Endpoint-Independent Filtering with destination NAT (DNAT). If you try to configure DNAT when Endpoint-Independent Filtering is enabled, or vice versa, the system issues a warning.

The order in which the conditions in a NAT policy are checked to determine the action for a packet is as follows:

1. The conditions set by the policy static translations.

2. The conditions set by the policy ACL.

3. If the conditions in step 1 and step 2 are not satisfied, the action for the packet is determined by the default class action, if the policy ACL exists, or by the NAT policy action.

1.8.1 Parent and Child Session Handling for TCP

P2MP for TCP enables several TCP connections initiated from the same internal endpoint to use the same translation.

The NAT translation:

- Follows the state of the TCP connection.
- Maps a public IP address, public port and protocol table to a private IP address, private, and port table (tuple).
- Stores session information, such as the state and remote address.

NAT does tracks only the state of the parent session, but it does not update the state and refresh age of child sessions in the incoming direction. This means that NAT is not able to determine the state and number of active child sessions.

To comply with REQ-5 of RFC 5382, NAT Behavioral Requirements for TCP, NAT does not immediately delete the NAT translation when it cannot determine whether there are still active TCP connections (active child sessions) from the same local endpoint.

To address this issue, you can configure the timeout to a lower value (by using the **`timeout abandoned`** command at the class level) to not keep the translation for a longer period of time, thus making the translation available for other sessions. The default timeout value is 2 hours and 4 minutes.

Since the remote port is not stored in the NAT translation table, two TCP sessions could be identified as a parent session. This happens when a new session is initiated towards the same remote IP address as the parent session's remote address, but towards a different port. In this case, both sessions are treated as parent sessions. The system updates refresh timers and states for both sessions. Closing one of the sessions results in closing the other session, even if one session is still in an established state.

1.8.2 Restrictions

This section lists the following restrictions for Endpoint-Independent Filtering.

- Policies that use classification based on the remote endpoint must use the same filtering mode. Using different filtering modes are not supported and can result in unexpected behavior.
- Enabling endpoint-independent filtering for TCP might have a negative impact on performance and scalability, as short lived P2MP sessions are deleted only after 2 hours and 4 minutes. This behavior has no effect when only point to point traffic was initiated from a local endpoint.

  You can configure the timeout to a lower value (by using the **`timeout abandoned`** command at the class level) to not keep the translation for

a longer period of time, thus making the translation available for other sessions. The **`timeout abandoned`** command configures the timeout value for P2MP TCP sessions that have no active parent session.

For more information about NAT, see RFC 3022, *Traditional IP Network Address Translator (NAT)* and RFC 2663, *IP Network Address Translator (NAT) Terminology and Considerations.*

2 Configuration and Operations Tasks

Note: In this section, the command syntax in the task tables displays only the root command; for the complete command syntax, see the *Command List*.

To configure NAT policies, perform the tasks described in the following sections.

2.1 Configure a NAT Policy with Static Translations

To configure a NAT policy with static translations, perform the tasks described in Table 2.

Table 2 Configure a NAT Policy with Traditional Static Translations

Step	Task	Root Command	Notes
1.	Configure a NAT policy name and access NAT policy configuration mode.	*nat policy*	Enter this command in context configuration mode.
2.	Translate the source IP address for incoming packets on the interface or the subscriber circuit to which the NAT policy will be attached in the private network.	*ip static in*	Enter this command in NAT policy configuration mode. The destination IP address of incoming packets is translated in the reverse direction. Use the optional **`tcp`** or **`udp`** keyword to translate the source address and source port number of the TCP/UDP packets.
3.	Translate the source IP address for outgoing packets on the interface or the subscriber circuit to which the NAT policy will be attached in the private network.	*ip static out*	Enter this command in NAT policy configuration mode. The destination IP address of incoming packets is translated in the reverse direction.

Table 2 Configure a NAT Policy with Traditional Static Translations

Step	Task	Root Command	Notes
4.	Translate the destination IP address for those inbound packets (on the interface or subscriber circuit to which the NAT policy will be attached) that do not satisfy any condition for static or dynamic translation in the policy.	*ip dmz*	Enter this command in NAT policy configuration mode. The source IP address is translated in the outbound direction.
5.	Optional. Apply a policy ACL.		See Section 2.4 on page 23.
6.	Attach the policy to an interface or subscriber, using one of the following tasks:		
	To an interface.	*ip nat*	Enter this command in interface configuration mode.
	To a subscriber record, named profile, or default profile.	*nat policy-name*	Enter this command in subscriber configuration mode.

Note: For information about configuring interfaces and subscribers, see and *Configuring Subscribers*.

2.2 Configure a NAT Policy with a DMZ Host Server

To configure a NAT policy with a DMZ host server, perform the tasks described in Table 3.

Table 3 Configure a NAT Policy with a DMZ Host Server

Step	Task	Root Command	Notes
1.	Configure a NAT policy name and access NAT policy configuration mode.	*nat policy*	Enter this command in context configuration mode.

Table 3 Configure a NAT Policy with a DMZ Host Server

Step	Task	Root Command	Notes
2.	Translate the destination IP address for those outgoing packets (on the interface or subscriber circuit to which the NAT policy will be attached) that do not satisfy any of the static or dynamic rules in the policy.	*ip dmz*	Enter this command in NAT policy configuration mode. The destination IP address of incoming packets is translated in the reverse direction.
3.	Attach the policy to an interface or subscriber, using one of the following tasks:		
	To an interface.	*ip nat*	Enter this command in interface configuration mode.
	To a subscriber record, named profile, or default profile.	*nat policy-name*	Enter this command in subscriber configuration mode.

2.3 Configure a NAT Policy with Dynamic Translations

To configure a NAT policy with dynamic translations, perform the tasks described in Table 4; enter all commands in NAT policy configuration mode, unless otherwise noted.

Table 4 Configure a NAT Policy with Dynamic Translations

Step	Task	Root Command	Notes
1.	Create or select a NAT pool and access NAT pool configuration mode.	*ip nat pool*	Enter this command in context configuration mode. Use the **`napt`** keyword to indicate that the addresses associated with the pool will be used for NAPT policies. Use the **`multibind`** keyword to enable the NAT pool to be applied to multibind interfaces.

Table 4 Configure a NAT Policy with Dynamic Translations

Step	Task	Root Command	Notes
2.	Configure the IP address, range of IP addresses, or the IP address with a range of TCP/UDP port blocks for the NAT pool.	*address*	Enter this command in NAT pool configuration mode. Enter this command multiple times to configure several IP addresses, address ranges, and IP addresses with port blocks for the NAT pool.
3.	Create or select a policy and access NAT policy configuration mode.	*nat policy*	Enter this command in context configuration mode.
4.	Optional. Specify the maximum number of sessions allowed for the specified protocol for each circuit.	*connections*	
5.	Specify the action to take on packets not associated with a class with one of the following tasks:		Any of these actions is applied to packets not associated with a class if a policy ACL is applied to this NAT policy.
	Translate the source IP addresses of the packets using the pool of IP addresses (created in step 1).	*pool*	
	Drop packets.	*drop (NAT policy)*	
	Forward packets without translating their source IP addresses.	*ignore*	
6.	Optional. Modify the period after which translations time out.	*timeout (NAT)*	Enter this command only if you have specified the **`pool`** command (in step 5). This timeout is used for packets not associated with a class, if a policy ACL is applied to this NAT policy.
7.	Optional. Enable session limit control for the default class for the specified protocol.	*admission-control*	
8.	Optional. Overwrites the destination IP address.	*destination*	

Table 4 Configure a NAT Policy with Dynamic Translations

Step	Task	Root Command	Notes
9.	Optional. Enable Endpoint-Independent Filtering.	*endpoint-independent filtering udp*	Enter this command only if if you have specified the **`pool`** command (in step 5) and/or the action is **`ignore`**.
10.	Optional. Apply a policy ACL to this policy.		See Section 2.4 on page 23.
11.	Attach the NAT or NATP policy to an interface or subscriber, using one of the following tasks:		
	To an interface.	*ip nat*	Enter this command in interface configuration mode.
	To a subscriber record, named profile, or default profile.	*nat policy-name*	Enter this command in subscriber configuration mode.

2.4 Apply a Policy ACL to a NAT Policy

To apply a policy ACL to packets associated with a dynamic NAT policy and complete the configuration of the policy, perform the tasks described in Table 5; enter all commands in policy group class configuration mode, unless otherwise noted.

Table 5 Apply a Policy ACL to a NAT Policy

Step	Task	Root Command	Notes
1.	Apply a policy ACL to a dynamic NAT policy and access policy group configuration mode.	*access-group*	Enter this command in NAT policy configuration mode.
2.	Specify a class and access class configuration mode.	*class*	Enter this command in policy group configuration mode. For a class-based action to occur, the class name must match one of the class names defined in the policy ACL.
3.	Specify the action to take on packets associated with the class with one of the following tasks:		Enter any of these commands in policy group class configuration mode.

Table 5 Apply a Policy ACL to a NAT Policy

Step	Task	Root Command	Notes
	Translate the source IP addresses of the packets using the pool of IP addresses.	*pool*	
	Drop packets associated with the class.	*drop (NAT policy)*	
	Forward packets associated with the class without translating their source IP addresses.	*ignore*	
4.	Optional. Modify the period after which translations time out.	*timeout (NAT)*	Enter this command only if you have specified the **`pool`** command (in step 3). Enter this command in policy group class configuration mode.
5.	Optional. Enable Endpoint-Independent Filtering.	*endpoint-independent filtering udp*	Enter this command only if if you have specified the **`pool`** command (in step 5) and/or the action is **`ignore`**.
6.	Optional. Enable session limit control for this class for the specified protocol.	*admission-control*	
7.	Optional. Overwrites the destination IP address.	*destination*	

2.5 Configure an Enhanced NAT Policy with Logging and Paired Mode

To configure an enhanced NAT policy on the SmartEdge router, you must enable the enhanced NAT license with the **`software license`** command. You must also configure an enhanced NAT policy to use the enhanced CGNAT functionality.

1 Enable software licensing and access software license configuration mode by using the root command *software license*.

Enter this command in global configuration mode.

2 Enable the license for enhanced NAT features and its functions by using the *nat enhanced password* command; enter this command in software license configuration mode.

3 Create a context for NAT. Enter this command in context configuration mode.

4 Create a NAT logging profile by using the *nat logging-profile* command.

   Enter this command in context configuration mode.

5 Create or select a NAT pool and access NAT pool configuration mode by using the *ip nat pool* command.

   Enter this command in context configuration mode.

   Use the **`napt`** keyword to indicate that the addresses associated with the pool will be used for NAPT policies.

   Use the **`paired-mode`** and **`logging`** keywords to enable paired behavior and logging.

6 Create a NAT policy ACL that uses rules to control access by using the *policy access-list* command.

7 Configure an enhanced NAT policy by using the *nat policy name enhanced* command. Enter this command in context configuration mode. Apply the NAT policy ACL to the enhanced policy.

8 Configure the logging and paired-mode pool under the desired classes under the enhanced NAT policy.

9 Apply NAT policy to the default subscribers by using the *subscriber default* command or *subscriber name* command. Enter this command in context configuration mode.

For information about using enhanced carrier NAT features using logging and paired mode, see Section 1.7 on page 7. For a sample CGNAT configuration, see Section 1.7.7 on page 14. For an example that shows you how to configure enhanced carrier grade NAT features with logging and paired mode, see Section 3.10 on page 35.

2.6 Operations Tasks

To monitor, troubleshoot, and administer NAT policies, perform the NAT operations tasks described in Table 6. Enter the **`clear`** and **`debug`** commands in exec mode; enter the **`show`** commands in any mode.

Table 6 NAT Policy Operations Tasks

Task	Command	Notes
Clear counters for the policy ACL that are associated with the NAT policy attached to the specified interface.	*clear access-group nat*	

Table 6 NAT Policy Operations Tasks

Task	Command	Notes
Enable the generation of NAT debug messages.	*debug nat*	
Display information about ACLs applied to NAT policies and the ports, channels, or circuits to which the ACLs are applied.	*show access-group nat*	
Display the current NAT configuration.	*show configuration nat*	
Display NAT route information.	*show ip route*	Specify the **`nat`** keyword.
Display information for configured NAT policies in the current context.	*show nat policy*	
Display information for configured NAT pools in the current context.	*show nat pool*	

3 Configuration Examples

This section provides NAT configuration examples.

3.1 NAT Policy with Static Translation

The following example configures a NAT policy with static translations:

```
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip static in source 10.1.1.3 100.1.1.3
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos2
[local]Redback(config-if)#ip nat p2
```

3.2 NAT Policy with Static NAPT

The following example configures a static NAPT policy:

```
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip static in tcp source 10.1.1.3 80 100.1.1.3 8080
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface pos2
[local]Redback(config-if)#ip nat p2
```

3.3 NAT Policy with Static Translation and a DMZ Host Server

The following example configures a NAT policy with static translation, two internal hosts, and a DMZ host server:

```
!Configure context, NAT policy, and interface for private network
[local]Redback(config)#context local
[local]Redback(config-ctx)#nat policy p2
[local]Redback(config-policy-nat)#ip dmz source 10.1.1.1 100.1.1.1 context local
[local]Redback(config-policy-nat)#ip static in source 10.1.1.2 100.1.1.2
[local]Redback(config-policy-nat)#ip static in source 10.1.1.3 100.1.1.3
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#interface if-private
[local]Redback(config-if)#ip address 10.1.1.1/24
[local]Redback(config-if)#ip nat p2
[local]Redback(config-if)#exit
[local]Redback(config-ctx)#exit
!Configure context, NAT policy, and interface for public network
[local]Redback(config)#context public
[local]Redback(config-ctx)#interface if-public
[local]Redback(config-if)#ip address 100.1.1.1/24
!Configure an Ethernet port for the private network
[local]Redback(config)#port ethernet 3/1
[local]Redback(config-port)#bind interface if-private local
[local]Redback(config-port)#no shutdown
!Configure an Ethernet port for the public network
[local]Redback(config)#port ethernet 5/1
[local]Redback(config-port)#bind interface if-public public
[local]Redback(config-port)#no shutdown
[local]Redback(config-port)#exit
```

Figure 2 illustrates the network configuration for the example.

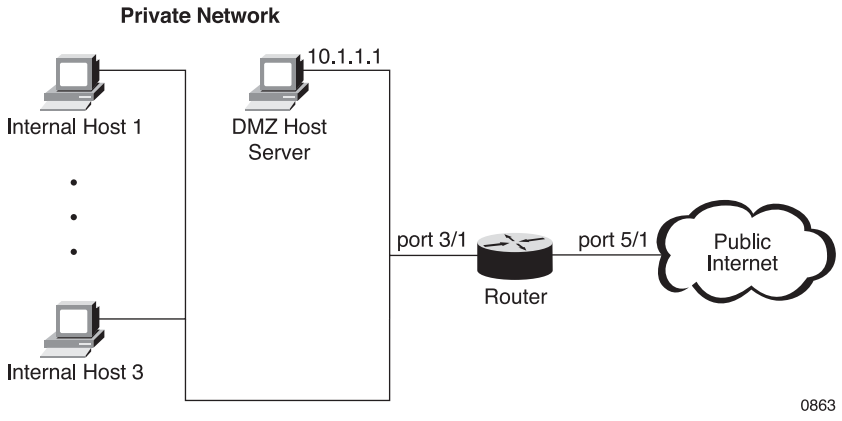

Figure 2 Private Network with NAT DMZ Host Server (863)

3.4 NAT Policy with Dynamic Translation and an Ignore Action

The following example creates a policy ACL and applies it to a NAT policy with dynamic translations in which all packets except those classified as **CLASS3** are ignored (that is, the NAT policy is not applied to them). All source IP addresses for incoming packets classified as **CLASS3** are translated using IP addresses from the **pool_dyn** pool:

```
!Create the NAT pool
[local]Redback(config-ctx)#ip nat pool pool_dyn
[local]Redback(config-nat-pool)#address 11.11.11.0/24
[local]Redback(config-nat-pool)#exit
!Create the policy ACL
[local]Redback(config-ctx)#policy access-list NAT-ACL
[local]Redback(config-access-list)#seq 10 permit ip 10.10.10.0 0.0.0.255 class CLASS3
[local]Redback(config-access-list)#exit
!Create the NAT policy and apply the policy ACL
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-nat-pool)#ignore
[local]Redback(config-nat-pool)#access-group NAT-ACL
[local]Redback(config-policy-group)#class CLASS3
[local]Redback(config-policy-group-class)#pool pool_dyn local
```

3.5 NAT Policy with Dynamic NAPT and a Drop Action

The following example configures a NAPT policy with dynamic translations in which all packets, except those classified as **CLASS3**, are dropped. Source IP addresses and their TCP/UDP ports for packets classified as **CLASS3** are translated using the IP address and its TCP/UDP port blocks **1** to **15** from the **pool_dyn_napt** pool:

```
[local]Redback(config-ctx)#ip nat pool pool_dyn_napt napt
[local]Redback(config-nat-pool)#address 11.11.11.1/32 port-block 1 to 15
[local]Redback(config-nat-pool)#exit
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-policy-nat)#drop
[local]Redback(config-policy-nat)#access-group NAT_ACL
[local]Redback(config-policy-group)#class CLASS3
[local]Redback(config-policy-group-class)#pool pool_dyn_napt local
```

3.6 NAT Policy with Static and Dynamic Translations

The following example configures a NAT policy that uses a combination of static and dynamic, basic NAT and NAPT, and applies a policy ACL:

```
[local]Redback(config-ctx)#ip nat pool pool_dyn
[local]Redback(config-nat-pool)#address 100.1.2.0/24
[local]Redback(config-nat-pool)#exit
[local]Redback(config-ctx)#ip nat pool pool_dyn_napt napt
[local]Redback(config-nat-pool)#address 100.1.1.2/32 port-block 1
[local]Redback(config-nat-pool)#exit
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-policy-nat)#pool pool_dyn local
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-group)#class CLASS3
[local]Redback(config-policy-group-class)#pool pool_dyn_napt local
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-nat)#ip static in tcp source 10.1.1.2 80 100.1.1.2 8080
[local]Redback(config-policy-nat)#ip static in source 10.1.1.3 100.1.1.3
```

3.7 NAT Policy with DNAT

The following example configures a NAT policy that uses DNAT, both with and without NAT, within a single NAT policy. A predefined destination address is configured for the **NAT-CLASS1** and **NAT-CLASS2** classes within the NAT policy **NAT-POLICY** . For all packets from class **NAT-CLASS1**, the destination address of each packet is replaced by **64.233.267.100** so that all packets from class **NAT-CLASS1** are forwarded to that address. On the return path, a reverse translation from **64.233.267.100** to the original destination address is performed so that the returning traffic appears to be sent from the original destination address. For the **NAT-CLASS2** class, the destination address of each packet is translated exactly the same way as for class **NAT-CLASS1**, but the source address is not translated:

```
[local]Redback(config-ctx)#nat policy NAT-POLICY
!Default class
[local]Redback(config-policy-nat)#pool NAT-POOL-DEFAULT local
!Named classes
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-acl)#class NAT-CLASS1
[local]Redback(config-policy-acl-class)#pool NAT-POOL1 local
[local]Redback(config-policy-acl-class)#destination 64.233.167.100
[local]Redback(config-policy-acl)#class NAT-CLASS2
[local]Redback(config-policy-acl-class)#ignore
[local]Redback(config-policy-acl-class)#destination 64.233.167.100
```

3.8 NAT Policy with Session Limit Control

The following example configures a NAT policy that uses session limit control for both the default class and a subset of named classes. Assuming that packets are not satisfied by both static rules (those are of higher priority), the following processing takes place:

- Packets classified into **CLASS2** are NAT-translated with the use of **pool2** addresses and no session limit control is applied (the default state).
- Packets classified into **CLASS3** are unchanged and session limit control is applied to TCP sessions with a maximum number of TCP sessions set to **100**.
- All other packets (that is, those of the default class) are translated with the use of **pool1** addresses and session limit control is applied to TCP sessions with a maximum number of TCP sessions set to **100**.

  Note: Specify the `connections` command (in NAT policy configuration mode) for the policy; then specify the `admission-control` command for each class (including the default one) for which you want the session limit to be enforced.

```
[local]Redback(config)#context local
[local]Redback(config-ctx)#nat policy pol1
[local]Redback(config-policy-nat)#ip static in tcp source 10.1.3.3 80 100.1.3.3 8080
[local]Redback(config-policy-nat)#ip static in tcp source 10.1.4.3 80 100.1.3.4 8080
[local]Redback(config-policy-nat)#connections tcp 100

! Default class
[local]Redback(config-policy-nat)#pool pool1 local
[local]Redback(config-policy-nat)#timeout tcp
[local]Redback(config-policy-nat)#admission-control tcp
! Named classes
[local]Redback(config-policy-nat)#access-group NAT-ACL
[local]Redback(config-policy-group)#class CLASS2
[local]Redback(config-policy-group-class)#pool pool2
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class CLASS3
[local]Redback(config-policy-group-class)#ignore
[local]Redback(config-policy-group-class)#admission-control tcp
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#exit
[local]Redback(config-policy-nat)#exit
[local]Redback(config-ctx)#exit
```

3.9 NAT Policy for Point-to-Multipoint UDP Traffic

The following example enables P2MP mode for all UDP traffic in the class **yes_p2mp**:

```
[local]Redback(config)#context nat_context
[local]Redback(config-ctx)#nat policy basic_nat
[local]Redback(config-policy-nat)#drop
[local]Redback(config-policy-nat)#access group basic_nat_rules
[local]Redback(config-policy-group)#class yes_p2mp
[local]Redback(config-policy-group-class)#pool NAPT_POOL local
[local]Redback(config-policy-group-class)#endpoint-independent filtering udp
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class firewall
[local]Redback(config-policy-group-class)#pool NAPT_POOL local
[local]Redback(config-policy-group-class)#exit
[local]Redback(config-policy-group)#class no_NAT
[local]Redback(config-policy-group-class)#ignore
```

The following example enables P2MP mode for UDP traffic in the default class without employing an access group in the policy:

```
[local]Redback(config)#context nat_context
[local]Redback(config-ctx)#nat policy basic_nat
[local]Redback(config-policy-nat)#pool NAPT_POOL local
[local]Redback(config-policy-nat)#endpoint-independent filtering udp
```

3.10 Enhanced CGNAT with Logging and Paired Mode

This section provides examples for configuring enhanced carrier grade NAT features with logging and paired mode in the **nat-context** context. The sample configuration is separated in a step-by-step procedure.

The following example shows how to configure enhanced NAT licensing.

```
[local]rock1200#configuration
Enter configuration commands, one per line, 'end' to exit
[local]rock1200(config)#software license
[local]rock1200(config-license)#nat
[password  Enter password
[local]rock1200(config-license)#nat enhanced password
```

Example 1 Configure NAT Enhanced License

The following example shows how to configure context for NAT called `nat-context`.

```
[local]Redback#configuration     <-
Enter configuration commands, one per line, 'end' to exit
[local]Redback(config)#context nat-context
[local]Redback(config-ctx)#nat
[local]Redback(config-ctx)#nat ?
  logging-profile  Configure NAT logging profile
  policy           Configure NAT policy
[local]Redback(config-ctx)#nat logging-profile nat-log-profile
[local]Redback(config-nat-profile)#export-version v9
[local]Redback(config-nat-profile)#source 10.10.10.1 port 4242
[local]Redback(config-nat-profile)#destination 100.1.1.1 context local port 8989
[local]Redback(config-nat-profile)#dscp ef
[local]Redback(config-nat-profile)#maximum ip-packet-size 1400
```

Example 2 Configure NAT Logging Profile

The following example configures an enhanced NAT pool, `nat-pool-1` with NAPT paired-mode and logging enabled. It also configures the logging profile to be associated with the pool, and the address and port range for the pool (which excludes well-known port numbers and port numbers 5000 to 6000):

```
[local]Redback(config-ctx)#ip nat pool nat-pool-1 napt paired-mode logging
[local]Redback(config-nat-pool)#logging-profile nat-log-profile context nat-context
[local]Redback(config-nat-pool)#paired-mode subscriber over-subscription 32 port-limit 4096
[local]Redback(config-nat-pool)#address 100.1.1.1 to 100.1.1.2 port-block 0 to 15
[local]Redback(config-nat-pool-record)#exclude well-known
[local]Redback(config-nat-pool-record)#exclude 5000 to 6000
```

Example 3 Configure an Enhanced NAT Pool

```
[local]rock1200(config)#context nat-context
  logging-profile  Configure NAT logging profile
  policy           Configure NAT policy
 [local]rock1200(config-ctx)#nat policy nat-policy enhanced
[local]rock1200(config-policy-nat)#pool nat-pool local
 [local]rock1200(config-policy-nat)#inbound-refresh udp
 [local]rock1200(config-policy-nat)#icmp-notification
```

Example 4 Configure Inbound Refresh and ICMP Notification

```
[local]rock1200(config-ctx)#context nat-context
[local]rock1200(config-ctx)#class
[local]rock1200(config-ctx)#nat policy nat-policy-1 enhanced
[local]rock1200(config-policy-nat)#access-group nat-acl
[local]rock1200(config-policy-acl)#class nat-class
[local]rock1200(config-policy-acl-class)#pool nat-pool-1 nat
[local]rock1200(config-policy-acl-class)#pool nat-pool-1 nat-context
[local]rock1200(config-policy-acl-class)#timeout abandoned 3600
[local]rock1200(config-policy-acl-class)#endpoint-independent filtering tcp
[local]rock1200(config-policy-acl-class)#endpoint-independent filtering udp
[local]rock1200(config-policy-acl-class)#inbound-refresh udp
local]rock1200(config-policy-acl-class)#
```

Example 5 Configure an Access Group and Class

3.11 Verify and Monitor Logging and Paired Mode

Run the **show nat policy** and **show nat pool** commands to verify the logging and paired mode configuration.

For the given policy and contained classes, the **show nat policy** command will show the following additional parameters:

- Whether inbound refresh is enabled for each class
- Whether endpoint-independent filtering is enabled

```
Policy name          :  enh-pol
Policy grid          :  0x1
Number of rules      :  2
Slot mask            :  0x0
Number of binds      :  0

Reference counters (in circuits * classes):
Slot     1     2     3     4
         0     0     0     0

Static NAT Rules:
In/Out  Protocol  Src-Addr         Port   NAT-Src-Addr     Port   NAT-Ctx-Id
in      tcp/ip    10.1.1.2         80     100.1.1.2        8080   0x40080001
in      ip        10.1.1.3         0      100.1.1.3        0      0x40080001

Class-Name          Action/ Pool-Grid/  Dest-IP-Addr/   Timeout(sec)  Admit-Ctrl
                    Flags   Context-Id  Context-Id

default             drop
Class1              ignore                              tcp    86400
                                                        udp    120
                                                        finrst 240
                                                        icmp   60
                                                        syn    128
                                                        basic  3600
                                                        abndn  7440
Class2              na[p]t  0x1                         tcp    86400
                    mp tcp  0x40080001                  udp    120
                    mp udp                              finrst 240
                    icmpgen                             icmp   60
                    in-refr                             syn    128
                                                        basic  3600
                                                        abndn  7440
```

For the given pool, the **`show nat pool`** command shows the following additional parameters:

- Whether paired mode is enabled
- The subscriber limit for each address range in the pool
- Excluded port ranges
- Logging server IP and port, or disabled if logging is not configured for the pool

The follow configuration maps to the following examples.

```
ip nat pool enh-pool napt paired-mode logging
 paired-mode subscriber over-subscription 64
 logging-profile nat-log-profile context local
 address 100.100.100.1 to 100.100.100.10 port-block 0 to 7
  exclude well-known
  exclude 5000 to 6000
 address 100.100.100.1 to 100.100.100.10 port-block 8 to 10
```

When the over subscription or port limit is not configured, the **`show nat pool`** command displays these parameters as 'Not defined'. Logging profile 1 and 2 shows the profile grid of the configured profiles. Zero (0x00000000) means that there is no (second) profile.

```
[local]Redback#show nat pool detail
Pool name          :  enh-pool
Pool context id    :  0x40080001
Pool grid          :  0x7
Pool type          :  napt, paired logging
Number of records :  2
Slot mask          :  0x0
Oversub. ratio     :  64
Port limit         :  Not defined
Logging profile 1 :  0x00000003
Logging profile 2 :  0x00000000

Reference counters (in circuits * classes):
Slot      1      2      3      4
          0      0      0      0

NAT Address Ranges / Excluded port ranges:
Start-IP-Addr      End-IP-Addr      Start-Port  End-Port
100.100.100.1      100.100.100.10   32768       45055
100.100.100.1      100.100.100.10   00000       32767
Excluded ports: 0-1023; 5000-6000;
```