Cisco ASR 5000 Series Network Address Translation Administration Guide

Version 10.0

Last Updated June 30, 2010

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-22992-01

Cisco ASR 5000 Series Network Address Translation Administration Guide

CONTENTS

About this Guide v
Conventions Used vi
Contacting Customer Support viii
Network Address Translation Overview 9
Supported Platforms and Products 10
Licenses 11
Supported Standards 12
NAT Feature Overview 13
NAT Realms 14
NAT IP Pool Groups 15
NAT IP Address Allocation and Deallocation 16
NAT IP Address Allocation 16
NAT IP Address Deallocation 17
NAT Port-chunk Allocation and Deallocation 17
NAT Port-chunk Allocation 17
NAT Port-chunk Deallocation 17
NAT IP Address/Port Allocation Failure 18
TCP 2MSL Timer 18
NAT Binding Records 19
NAT Binding Updates 19
CoA NAT Query 20
Firewall-and-NAT Policy 21
Disabling NAT Policy 22
Updating Firewall-and-NAT Policy in Mid-session 22
Target-based NAT Configuration 22
NAT Application Level Gateway 23
Supported NAT ALGs 24
EDRs and UDRs 24
EDRs 24
UDRs 24
Bulk Statistics 24
Alarms 25
Session Recovery and ICSR 26
How NAT Works 28
NAT Configuration 33
Before You Begin 34
Configuring the System 35
Configuring NAT 36
Enabling the ECS Subsystem and Creating the ECS Service 37
Configuring Port Maps 37
Configuring Host Pools 38
Configuring IMSI Pools 38
Configuring Access Ruledefs 39
Configuring NAT IP pools/NAT IP Pool Groups 40
Configuring One-to-One NAT IP Pools /NAT IP Pool Groups 40

Configuring Many-to-One NAT IP Pools /NAT IP Pool Groups 41
Configuring Firewall-and-NAT Policies 42
Configuring Action on NAT IP Address/Port Allocation Failure 43
Configuring Action on Packets During NAT IP Allocation 44
Configuring NAT TCP-2msl-timeout Setting 44
Configuring Action on TCP Idle Timeout 44
Configuring Private IP NPU Flow Timeout Setting 45
Configuring Flow Recovery 45
Enabling NAT for APN/Subscribers 45
Enabling NAT for APN 46
Enabling NAT for Subscribers 46
Configuring the Default Firewall-and-NAT Policy 47
Configuring NAT Application Level Gateways/Dynamic Pinholes 47
Creating Routing Ruledefs 47
Configuring Routing Ruledefs in Rulebase 48
Enabling NAT ALG 48
Configuring EDR Format 49
Configuring UDR Format 49
Configuring NAT Binding Record Format 50
Configuring Bulkstats Collection 51
Configuring NAT Thresholds 52
Enabling Thresholds 52
Configuring Threshold Poll Interval 52
Configuring Thresholds Limits 53
Enabling SNMP Notifications 53
Backing Out of NAT 53
Configuring NAT Backout for APN 54
Configuring NAT Backout for Subscribers 54
Changing Firewall-and-NAT Policy in Mid-session 55
Verifying the Configuration 56
Saving the Configuration 57
Gathering NAT Statistics 58
Verifying and Saving Your Configuration 61
Verifying the Configuration 62
Feature Configuration 62
Service Configuration 63
Context Configuration 64
System Configuration 64
Finding Configuration Errors 64
Saving the Configuration 66
Saving the Configuration on the Chassis 67
Sample NAT Configuration 69

About this Guide

This document pertains to features and functionality that run on and/or that are related to the Cisco® ASR 5000 Chassis, formerly the Starent Networks ST40.

Conventions Used

The following tables describe the conventions used throughout this documentation.

Icon	Notice Type	Description
	Information Note	Provides information about important features or instructions.
	Caution	Alerts you of potential damage to a program, device, or system.
	Warning	Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.
	Electro-Static Discharge (ESD)	Alerts you to take proper grounding precautions before handling a product.

Typeface Conventions	Description
Text represented as a `screen display`	This typeface represents displays that appear on your terminal screen, for example: `Login:`
Text represented as **`commands`**	This typeface represents commands that you enter, for example: **`show ip access-list`** This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.
Text represented as a **`command`** *`variable`*	This typeface represents a variable that is part of a command, for example: **`show card`** *`slot_number`* slot_number is a variable representing the desired chassis slot number.
Text represented as menu or sub-menu names	This typeface represents menus and sub-menus that you access within a software application, for example: Click the **File** menu, then click **New**

Command Syntax Conventions	Description
{ **`keyword`** or *`variable`* }	Required keywords and variables are surrounded by grouped brackets. Required keywords and variables are those components that are required to be entered as part of the command syntax.

Command Syntax Conventions	Description
[**keyword** or *variable*]	Optional keywords or variables, or those that a user may or may not choose to use, are surrounded by square brackets.
|	With some commands there may be a group of variables from which the user chooses one. These are called alternative variables and are documented by separating each variable with a vertical bar (also known as a pipe filter). Pipe filters can be used in conjunction with required or optional keywords or variables. For example: **{ nonce | timestamp }** OR [**count** *number_of_packets* | **size** *number_of_bytes*]

Contacting Customer Support

Use the information in this section to contact customer support.

For New Customers: Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

For Existing Customers with support contracts through Starent Networks: Refer to the support area of https://support.starentnetworks.com/ for up-to-date product documentation or to submit a service request. A valid username and password is required to this site. Please contact your local sales or service representative for additional information.

Important: For warranty and repair information, please be sure to include the Return Material Authorization (RMA) tracking number on the outside of the package.

Chapter 1
Network Address Translation Overview

This chapter provides an overview of Network Address Translation (NAT) in-line service feature.

The following topics are covered in this chapter:

- Supported Platforms and Products
- Licenses
- Supported Standards
- NAT Feature Overview
- How NAT Works

Supported Platforms and Products

NAT is an in-line service feature supported on the Cisco ASR 5000 chassis running 3GPP, 3GPP2, and LTE core network services (PDSN, HA, GGSN, and P-GW).

Important: For information on ASR 5000, please refer to the *Product Overview Guide*.

Licenses

NAT is a licensed in-line service feature requiring the following licenses:

- [600-00-7805] *NAT/PAT With DPI*
- Any other in-line service counting license (Enhanced Charging Service, Stateful Firewall, Content Filtering, etc.). For more information, please contact your local sales representative.

Important: For information on license requirements for any customer-specific features, please contact your local sales/service representative.

Important: For information on installing licenses, see the *Managing License Keys* chapter of the *System Administration and Configuration Guide*.

Supported Standards

The NAT feature supports the following RFCs:

- RFC 1631: The IP Network Address Translator (NAT); May 1994
- RFC 1918: Address Allocation for Private Internets; February 1996
- RFC 2663: IP Network Address Translator (NAT) Terminology and Considerations; August 1999
- RFC 3022: Traditional IP Network Address Translator (Traditional NAT); January 2001
- RFC 3027: Protocol Complications with the IP Network Address Translator; January 2001
- RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP; January 2007
- RFC 4966: Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status; July 2007
- RFC draft-nishitani-cgn-00.txt: Carrier Grade Network Address Translator (NAT) Behavioral Requirements for Unicast UDP, TCP and ICMP; July 2, 2008

NAT Feature Overview

This section provides an overview of the NAT in-line service feature.

NAT translates non-routable private IP address(es) to routable public IP address(es) from a pool of public IP addresses that have been designated for NAT. This enables to conserve on the number of public IP addresses required to communicate with external networks, and ensures security as the IP address scheme for the internal network is masked from external hosts, and each outgoing and incoming packet goes through the translation process.

NAT works by inspecting both incoming and outgoing IP datagrams and, as needed, modifying the source IP address and port number in the IP header to reflect the configured NAT address mapping for outgoing datagrams. The reverse NAT translation is applied to incoming datagrams.

NAT can be used to perform address translation for simple IP and mobile IP. NAT can be selectively applied/denied to different flows (5-tuple connections) originating from subscribers based on the flows' L3/L4 characteristics—Source-IP, Source-Port, Destination-IP, Destination-Port, and Protocol.

Important: NAT works only on flows originating internally. Bi-directional NAT is not supported.

Important: NAT is supported only for TCP, UDP, and ICMP flows. For other flows NAT is bypassed. For GRE flows, NAT is supported only if the PPTP ALG is configured. For more information on ALGs, please refer to the NAT Application Level Gateway section.

Important: If a subscriber is assigned with a public IP address, NAT is not applied.

Important: To get NATed, the private IP addresses assigned to subscribers must be from the following ranges: Class A 10.0.0.0 – 10.255.255.255, Class B 172.16.0.0 – 172.31.255.255, and Class C 192.168.0.0 – 192.168.255.255

NAT supports the following mappings:

- One-to-One: In one-to-one NAT each private IP address is mapped to a unique public NAT IP address. The private source ports do not change.

  When a private IP address (IP1:port1) is mapped to a public IP address (IP2:port1), any packets from IP1:port1 will be sent as though via IP2:port1. The external host can only send packets to IP2:port1, which are translated to IP1:port1. The NAT port number will be the same as the source private port.

- Many-to-One: In many-to-one NAT, multiple private IP addresses are mapped to a single public NAT IP address. In order to distinguish between different subscribers and different connections originating from same subscriber, internal private L4 source ports are translated to pre-assigned L4 NAT ports. Ports are allocated in chunks such that each private IP address is reserved a set of ports for future use. This is also known as Network Address Port Translation (NAPT).

Once a flow is marked to use a specific NAT IP address the same NAT IP address is used for all packets originating on that flow. The NAT IP address is released only when all flows and subscribers associated with it are released.

When all NAT IP addresses are in use, and a subscriber with a private IP address fails to get a NAT IP address for a specific flow, that specific flow will not be allowed and will fail.

All downlink—inbound from external networks—IP packets that do not match one of the existing NAT bindings are discarded by the system.

NAT Realms

A NAT realm is a pool of unique public IP addresses available for translation from private source IP addresses. IP addresses in a NAT IP pool are contiguous, and assignable as a subnet or a range that constitutes less than an entire subnet. IP addresses configured in NAT IP pools within a context must not overlap. At any time, within a context, a NAT IP address must be configured in any one NAT IP pool. IP addresses can be added to a NAT IP pool as a range of IP addresses.

Important: The minimum number of public IP addresses that must be allocated to each NAT IP pool must be greater than or equal to the number of Session Managers (SessMgrs) available on the system. On the ASR 5000, it is >= 84 public IP addresses. This can be met by a range of 84 host addresses from a single Class C. The remaining space from the Class C can be used for other allocations. Each address has available its port range ~64K ports.

Up to 2000 unique "IP pools + NAT IP pools" can be configured per context. A maximum of three NAT IP pools/NAT IP pool groups can be configured in a Firewall-and-NAT policy. At any time a subscriber can be associated with a maximum of three different NAT IP pools/NAT IP pool groups and can have NATed flows on three different NAT IP addresses at the same time.

Allocation of NAT IP addresses in NAT IP pools to subscriber traffic is based on the L3/L4 characteristics—IP addresses, ports, and protocol—of the subscriber flows. It is possible to configure the system to perform or not perform NAT based on one or more L3/L4 parameters. This feature is also known as Target-based NAT. For more information, see the Target-based NAT Configuration section.

NAT IP pools have the following configurable parameters. These parameters are applicable to all IP addresses in a NAT IP pool.

- NAT IP Address Allocation Mode: Specifies when to allocate a NAT IP address to a subscriber; either at call setup or during data flow based on the allocation mode.
  - Not-on-demand Allocation Mode: This is the default mode. In this mode, the NAT IP address is allocated to the subscriber at call setup. If there are three NAT IP pools/NAT IP pool groups (maximum possible) configured in the subscriber's Firewall-and-NAT policy, the subscriber is allocated three NAT IP addresses, one from each NAT IP pool/NAT IP pool group based on rule matching.
  - On-demand Allocation Mode: In this mode NAT resources are assigned and allocated dynamically based on subscriber flows. The NAT IP address is allocated to the subscriber when the data traffic flows in and not at call setup.

    In case of on-demand pools, since the NAT IP address is not allocated to the subscriber at call setup, the subscriber may not have a NAT IP address allocated when the first packet is received. Until the successful allocation of a NAT IP address, based on the configuration, the packets can either be buffered or dropped. Once a free NAT IP address is available, it is allocated to the subscriber to be used for flows matching the pool.
- NAT Binding Timer: Specifies the timeout period, in seconds, to deallocate NAT resources that were allocated to subscriber flows. When a subscriber flow stops the timer starts counting down, and on expiry the NAT resources are deallocated to be made available for other subscriber flows.

  - In one-to-one allocation, for a given NAT IP address, the NAT Binding Timer starts counting down when there are no active flows using that NAT IP address. When the NAT Binding Timer expires, the NAT IP address gets deallocated.
  - In many-to-one allocation, wherein subscribers are allocated port-chunks rather than individual ports, as long as a port-chunk is allocated to a subscriber, all ports from that port-chunk are reserved for that subscriber. When all flows using ports from that port-chunk get timed out/cleared, the NAT Binding Timer starts counting down. If any new flows come up before the NAT Binding Timer expires, ports are once again allocated from that port-chunk, and the NAT Binding Timer gets cancelled. As long as there are active flows using the port-chunk it cannot be deallocated. But, if no new flows come and the NAT Binding Timer expires, the port-chunk gets deallocated. In the case of on-demand NAT, if it is the last port-chunk for the NAT IP address, on NAT Binding Timer expiry, the NAT IP address gets deallocated along with the last port-chunk.

- Maximum Users per NAT IP Address: Applicable only to many-to-one NAT IP pools. Specifies the maximum number of subscribers sharing one NAT IP address. A maximum of 2016 subscribers can be configured per NAT IP address.
- Port Chunk Size: Applicable only to many-to-one NAT IP pools. Specifies the block size of contiguous ports to be assigned to a many-to-one NAT subscriber. This number has to be divisible by 32 up to a maximum of 32,256.
- Maximum Port-chunks per User: Applicable only to many-to-one NAT IP pools. Specifies the maximum number of port-chunks allowed for an individual subscriber from the same NAT IP address. This will limit subscribers from dominating all the available ports in a many-to-one NAT IP. A maximum of 2016 port-chunks can be configured per subscriber.

  Consider a case where a single TCP flow is active in a port-chunk. When this connection gets cleared, the TCP NAT port goes to Time Wait state. Since it is the last flow of the port-chunk, the NAT Binding Timer also gets started. Assume NAT Binding Timer >= TCP 2MSL Timer. Once the 2MSL Timer expires, the TCP port would go to Free state. However, the NAT Binding Timer keeps running. On NAT Binding Timer expiry, the port-chunk is deallocated. If this was the last port-chunk for that subscriber, the NAT IP address is also deallocated along with this port-chunk.

  In case NAT Binding Timer < TCP 2MSL Timer, at NAT Binding Timer expiry, the TCP port is forcefully moved to Free state from Time Wait state and the port-chunk deallocated.
- Port Chunk Thresholds: Applicable only to many-to-one NAT IP pools. Specifies threshold in terms of percentage of allocated port-chunks against total port-chunks available. Once the threshold is reached, new subscribers will not be allocated the same NAT IP address.
- AAA Binding Update Message Required: Applicable only to one-to-one NAT IP pools. Enables AAA binding messages for one-to-one NAT IP pools. This is not supported for many-to-one NAT IP pools.
- Alert Thresholds: Threshold limits can be specified to trigger alarms for NAT IP pools for pool-used, pool-free, pool-hold, and pool-release cases.
- SRP-Activate: Applicable to both one-to-one and many-to-one NAT IP pools. When configured, the NAT IP pool will become usable only when the SRP state is active.

NAT IP Pool Groups

Similar NAT IP pools can be grouped into NAT IP pool groups. This enables to bind discontiguous IP address blocks in individual NAT IP pools to a single NAT IP pool group.

When configuring a NAT IP pool group, note that only those NAT IP pools that have similar characteristics can be grouped together. The similarity is determined by the NAT IP pool Type (One-to-One / Many-to-One), users configured per NAT IP address (applicable only to many-to-one NAT IP pools), NAT IP Address Allocation Mode (On-demand/Not-on-demand), and Port Chunk Size (applicable only to many-to-one NAT IP pools) parameters. Dissimilar NAT IP pools cannot be grouped together.

It is recommended that all the NAT IP pools in a NAT IP pool group be configured with the same values for the other parameters, so that the NAT behavior is predictable across all NAT IP pools in that NAT IP pool group.

The NAT IP pool from which a NAT IP address is assigned will determine the actual values to use for all parameters.

It is recommended that in a Firewall-and-NAT policy all the realms configured either be NAT IP pools or NAT IP pool groups. If both NAT IP pool(s) and NAT IP pool group(s) are configured, ensure that none of the NAT IP pool(s) are also included in the NAT IP pool group.

NAT IP Address Allocation and Deallocation

Cisco System's implementation of NAPT is Endpoint-independent Mapping, wherein NAT reuses the same NAT source port mapping for subsequent packets sent from the same private IP address and port, and with the same protocol to any public destination host IP address and port.

That is, all flows coming from the subscriber for the current session with the same protocol and same source IP address and source port (X:x) would get the same NAT IP address and NAT port (X:x) irrespective of the destination IP address and port. NAT will not allow any inbound packets to the NAT IP address and NAT port (X:x) from an external host IP address and host port (Y:y), unless the internal host (MS) had previously sent a packet of the same protocol type to that external IP address and Port (Y:y). However, this behavior changes if NAT ALG is enabled. The ALG creates pin holes / dynamic routes in the NAT and allows downlink packets that match the pin holes / dynamic routes towards the internal host (MS) given that there was already a parent connection from MS towards the external host.

The advantage of endpoint-independent mapping is that applications are unaffected by NAT translations.

Inbound connection to the NAT IP address can be allowed in one-to-one pools based on configuration.

NAT IP Address Allocation

The NAT IP address is allocated based on the following parameters:

- Maximum Users per NAT IP Address: The maximum number of subscribers sharing a NAT IP address. Once the number of active subscribers using a NAT IP address reaches this limit, that NAT IP address will not be allocated to new subscribers.
- Port-chunk Thresholds: The threshold is configured in percentage of total number of port-chunks. If the number of port-chunks already allocated from a given NAT IP address is less than the configured threshold limit of port-chunks, then the NAT IP address can be chosen for a new subscriber provided the "Maximum Users per NAT IP Address" is not reached. But if the number of chunks allocated is greater than or equal to the threshold limit of port-chunks, then the NAT IP address will not be chosen for a new subscriber. The remaining free port-chunks will be used for existing subscribers using the NAT IP address.

NAT IP Address Deallocation

Whenever a NAT IP address is deallocated, all the port-chunks associated with the subscriber are released back to the pool.

In case there is only one port-chunk associated with the subscriber:

- In case of many-to-one not-on-demand NAT IP pools, the last port-chunk is not released back to the pool even after NAT Binding Timer expires. Only when the call gets disconnected, the port-chunk is released along with the NAT IP address.
- In case of many-to-one on-demand NAT IP pools, when the last flow using the port-chunk gets cleared, the NAT Binding Timer is started. When the NAT Binding Timer expires, the port-chunk along with the NAT IP address is released back to the pool.
- In case of one-to-one on-demand NAT IP pools, when there are no active flows using a NAT IP address, the NAT Binding Timer is started. When the NAT Binding Timer expires, the NAT IP address gets deallocated.

NAT Port-chunk Allocation and Deallocation

This section describes the Port-chunk Allocation and Deallocation feature for many-to-one NAT.

NAT Port-chunk Allocation

Subscribers sharing a NAT IP address are allocated NAT ports in chunks. The ports in a port-chunk are always used for the subscriber to whom that port-chunk is allocated irrespective of the protocol.

Whenever a NAT IP address gets allocated to a subscriber, the first port-chunk gets allocated along with the NAT IP address. Thus, for not-on-demand pools, the first port-chunk gets allocated during call setup, and for on-demand pools during data flow.

A subscriber's TCP and UDP data traffic is NATed with ports chosen in a random fashion from the port-chunk allocated to that subscriber. For other protocol traffic, the first available port is allocated. When all the ports in a port-chunk are in use, a free port-chunk is requested for. A new port-chunk is only allocated if the "Maximum Port-chunks Per User" limit is not reached.

NAT Port-chunk Deallocation

A port-chunk gets deallocated in the following cases:

- "NAT Binding Timer" expiry
- Subscriber session disconnect

NAT Binding Timer

When all flows using ports from a particular port-chunk get timed out/cleared, the port-chunk gets freed. When the last port of that port-chunk gets freed, the NAT Binding Timer starts counting. Before the NAT Binding Timer expires, if any new flows come up, ports are reallocated from the port-chunk, and the timer gets cancelled. The port-chunk cannot be deallocated as long as there are active flows using that port-chunk. But, if no new flows come and the NAT Binding Timer expires, the port-chunk gets deallocated.

In case of not-on-demand pools, the additional port-chunks that were allocated on demand will be deallocated based on the NAT binding timeout. However, the last port-chunk will not be deallocated even after the Binding Timer expires. This last port-chunk will only be deallocated when the NAT IP address is deallocated from the subscriber.

In case of on-demand pools, the port-chunks are deallocated based on the NAT binding timeout. When the last port-chunk gets freed, the NAT IP address also gets deallocated from the subscriber.

It is ensured that a port-chunk is associated with the subscriber as long as a valid NAT IP address is allocated to the subscriber.

Subscriber Session Disconnect

When a subscriber disconnects, all port-chunks associated with that subscriber are freed.

If the NAT Binding Timer has not expired, the port-chunks will not be usable immediately, only on NAT Binding Timer expiry will the port-chunks become available for new subscribers.

NAT IP Address/Port Allocation Failure

When a packet cannot be translated, the application can be notified by way of ICMP error messages, if configured. Translation failures may be due to no NAT IP address or port being available for translation.

Important: In the case of P-GW, NAT IP Address/Port Allocation Failure notification is not applicable.

TCP 2MSL Timer

NAT does port management only for many-to-one pools. Hence, The TCP 2MSL timer is only available for many-to-one NAT. It is necessary to ensure that a TCP NAT port in Time Wait state is not reused if there are other free ports available for the subscriber. If such a reuse happens, then there is a possibility that connections might get terminated by the server. To avoid such issues, whenever a many-to-one NAT TCP flow gets cleared, the NAT port goes to Time Wait state (2MSL started for that port). Once 2MSL timer expires, the NAT port becomes usable. The 2MSL timer is started for every TCP NAT port as soon as the TCP connection gets cleared. This ensures that a NAT TCP port gets reused only after expiry of the configured TCP 2MSL timer.

Consider a case where a single TCP flow is active in a port-chunk. When this connection gets cleared, the TCP NAT port goes to Time Wait state. Since this is the last flow of the port-chunk, the NAT Binding Timer also gets started. Assume NAT Binding timer >= TCP 2MSL timer. Once the 2MSL timer expires, the TCP port becomes usable. However, the NAT Binding Timer keeps counting, and on expiry, the port-chunk is released.

In case the NAT Binding Timer < TCP 2MSL Timer, on NAT Binding Timer expiry, the TCP port is forcefully moved to Free State (made usable) from Time Wait state and the port-chunk released.

NAT Binding Records

Whenever a NAT IP address or NAT port-chunk is allocated/deallocated to/from a subscriber, NAT Binding Records (NBR) can be generated. Generation of NBRs is configurable in the Firewall-and-NAT policy configuration.

NBRs are supported for both on-demand and not-on-demand NAT IP pools. For a one-to-one NAT IP pool, an NBR is generated whenever a NAT IP address is allocated/deallocated to/from a subscriber. For a many-to-one NAT IP pool, an NBR is generated when a port-chunk is allocated/deallocated to/from a subscriber for a NAT IP address. It is also possible to configure generation of NBRs only when a port-chunk is allocated, or deallocated, or in both cases.

The following is the list of attributes that can be present in NBRs. You can configure a subset of these attributes or all of them to be logged in NBRs. If an attribute is not available, while logging records that field is populated with NULL.

- ip subscriber-ip-address: The private IP address
- radius-calling-station-id
- radius-fa-nas-identifier
- radius-fa-nas-ip-address
- radius-user-name
- sn-correlation-id: If available
- sn-fa-correlation-id: If available
- sn-nat-binding-timer: Optional
- sn-nat-gmt-offset: Optional, GMT offset of the node generating this record. For example: -5.00, +5.30
- sn-nat-ip
- sn-nat-last-activity-time-gmt
- sn-nat-port-block-end
- sn-nat-port-block-start
- sn-nat-port-chunk-alloc-dealloc-flag: 1: allocate; 0: deallocate
- sn-nat-port-chunk-alloc-time-gmt: Sample time format: 03/11/2009 10:38:35
- sn-nat-port-chunk-dealloc-time-gmt
- sn-nat-realm-name: Optional
- sn-nat-subscribers-per-ip-address: Optional

NAT Binding Updates

Whenever a NAT IP address or NAT port-chunk is allocated/deallocated to/from a subscriber, to update NAT binding information for that subscriber in the AAA, a NAT Binding Update (NBU) can be sent to the AAA server.

Important: In the case of P-GW, NBUs is not applicable since it does not use RADIUS.

Since port-chunk allocation/deallocation happens on a per-call basis, this ensures that AAA messaging is reduced to a great extent. NBUs are sent to the AAA server in accounting-interim messages. To send or not to send NBUs to the AAA server is configurable in the NAT IP pool configuration.

NBUs are supported for both one-to-one and many-to-one NAT IP pools.

An NBU contains the following attributes:

- Alloc-Flag
- Binding-Timer
- Correlation-Id
- Loading-Factor
- NAT-IP-Address
- NAT-Port-Block-End: In the case of one-to-one NAT, the value is 65535
- NAT-Port-Block-Start: In the case of one-to-one NAT, the value is 1

CoA NAT Query

If the NAT binding information is not available at the AAA, the AAA server can query the chassis for the information. This query uses the Change of Authorization (CoA) format, wherein the AAA sends a one-to-one NAT IP address as a query, and in the CoA query response the NBU is obtained if available at the time of query.

Important: In this release, CoA query for NAT binding information is only supported for one-to-one NAT.

The CoA query request must contain the following attributes:

- Event-Timestamp
- NAS-IP-Address
- SN1-NAT-IP-Address

  Important: For SN1-NAT-IP-Address, this release supports VSA-Type values 0 and 1.

For a successful query, the CoA ACK response contains the following attributes:

- Acct-Session-Id
- Correlation-Id
- Framed-IP-Address
- NAT-IP-Address
- NAT-Port-Block-End

- NAT-Port-Block-Start
- User-Name

Important: For information on the AVPs/VSAs, please refer to the *AAA Interface Administration and Reference*.

Firewall-and-NAT Policy

Firewall-and-NAT policies are configured in the CLI Firewall-and-NAT Policy Configuration Mode. Each policy contains a set of access ruledefs with priorities and actions, and the NAT configurations. On a system, multiple such policies can be configured, however at any point of time only one policy is associated to a subscriber.

Important: In StarOS 8.x, NAT for CDMA and early UMTS releases used rulebase-based configurations, whereas in later UMTS releases NAT used policy-based configurations. In StarOS 9.0 and later releases, NAT for UMTS and CDMA releases both use policy-based configurations. For more information, please contact your local service representative.

Important: In a Firewall-and-NAT policy, a maximum of three NAT IP pools/NAT IP pool groups can be configured. A subscriber can be allocated only one NAT IP address per NAT IP pool/NAT IP pool group, hence at anytime, there can only be a maximum of three NAT IP addresses allocated to a subscriber.

New NAT IP pools/NAT IP pool groups cannot be added to a policy if the maximum allowed is already configured in it. However, a pool/pool group can be removed and then a new one added. When a pool/pool group is removed and a new one added, the pool/pool group that was removed will stay associated with the subscriber as long as the subscriber has active flows using that pool/pool group. If the subscriber is already associated with three NAT IP pools (maximum allowed), any new flows from that subscriber for the newly added pool will be dropped. A deleted pool is disassociated from the subscriber on termination of all flows from that subscriber using that pool. The new pool/pool group is associated with the subscriber only when the subscriber sends a packet to the newly added pool.

In the Firewall-and-NAT policy configuration, the NAT policy must be enabled. Once NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT IP pools/NAT IP pool groups specified in matching access rules configured in the Firewall-and-NAT policy.

The Firewall-and-NAT policy used for a subscriber can be changed either from the command line interface, or through dynamic update of policy name in Diameter and RADIUS messages. In both the cases, NAT status on the active call remains unchanged.

The Firewall-and-NAT policy to be used for a subscriber can be configured in:

- ECS Rulebase: The default Firewall-and-NAT policy configured in the ECS rulebase has the least priority. If there is no policy configured in the APN/subscriber template, and/or no policy to use is received from the AAA/OCS, only then the default policy configured in the ECS rulebase is used.
- APN/Subscriber Template: The Firewall-and-NAT policy configured in the APN/subscriber template overrides the default policy configured in the ECS rulebase. To use the default policy configured in the ECS rulebase, in the APN/subscriber configuration, the command to use the default rulebase policy must be configured.

- AAA/OCS: The Firewall-and-NAT policy to be used can come from the AAA server or the OCS. If the policy comes from the AAA/OCS, it will override the policy configured in the APN/subscriber template and/or the ECS rulebase.

Important: The Firewall-and-NAT policy received from the AAA and OCS have the same priority. Whichever comes latest, either from AAA/OCS, is applied.

The Firewall-and-NAT policy to use can also be received from RADIUS during authentication.

Disabling NAT Policy

Important: By default, NAT processing for subscribers is disabled.

NAT processing for subscribers is disabled in the following cases:

- If the AAA/OCS sends the SN-Firewall-Policy AVP with the string “disable”, the locally configured Firewall-and-NAT policy does not get applied.
- If the SN-Firewall-Policy AVP is received with the string “NULL”, the existing Firewall-and-NAT policy will continue.
- If the SN-Firewall-Policy AVP is received with a name that is not configured locally, the subscriber session is terminated.

Updating Firewall-and-NAT Policy in Mid-session

The Firewall-and-NAT policy can be updated mid-session provided the policy was enabled during call setup.

Important: When the firewall AVP contains “disable” during mid-session firewall policy change, there will be no action taken as the Firewall-and-NAT policy cannot be disabled dynamically. The policy currently applied will continue.

Important: For all NAT-enabled subscribers, when the Firewall-and-NAT policy is deleted, the call is dropped.

In a Firewall-and-NAT policy, you can change the NAT enabled/disabled status at any time. However, the updated NAT status will only be applied to new calls, active calls using that Firewall-and-NAT policy will remain unaffected.

Target-based NAT Configuration

A NAT IP pool can be selected based on the L3/L4 characteristics of a subscriber’s flows. NAT can be configured such that all subscriber traffic coming towards specific public IP address(es) always selects a specific NAT IP pool based on the L3/L4 traffic characteristics.

Important: A subscriber can be allocated only one NAT IP address per NAT IP pool/NAT IP pool group from a maximum of three NAT IP pools/NAT IP pool groups. Hence, at anytime, there can only be a maximum of three NAT IP addresses allocated to a subscriber.

This association is done with the help of access ruledefs configured in the Firewall-and-NAT policy. The NAT IP pool/NAT IP address to be used for a subscriber flow is decided during rule match. When packets match an access ruledef, NAT is applied using the NAT IP address allocated to the subscriber from the NAT IP pool/NAT IP pool group configured in that access ruledef.

If no NAT IP pool/NAT IP pool group name is configured in the access ruledef matching the packet, and if there is a NAT IP pool/NAT IP pool group configured for “no ruledef matches”, a NAT IP address from the NAT IP pool/NAT IP pool group configured for “no ruledef matches” is allocated to the flow.

If no NAT IP pool/NAT IP pool group is configured for “no ruledef matches” and if there is a default NAT IP pool/NAT IP pool group configured in the rulebase, a NAT IP address from this default NAT IP pool/NAT IP pool group is allocated to the flow.

If a NAT IP pool/NAT IP pool group is not configured in any of the above cases, no NAT will be performed for the flow. Or, if bypass NAT is configured in a matched access rule or for “no ruledef matches” then NAT will not be applied even if the default NAT IP pool/NAT IP pool group is configured. The order of priority is:

1. Bypass NAT
2. NAT IP pool/NAT IP pool group in ruledef
3. NAT IP pool/NAT IP pool group for “no-ruledef-matches”
4. Default NAT IP pool/NAT IP pool group

When a new NAT IP pool/NAT IP pool group is added to a Firewall-and-NAT policy, it is associated with the active subscriber (call) only if that call is associated with less than three (maximum limit) NAT IP pools/NAT IP pool groups. If the subscriber is already associated with three NAT IP pools/NAT IP pool groups, any new flows referring to the newly added NAT IP pool/NAT IP pool group will get dropped. The newly added NAT IP pool/NAT IP pool group is associated to a call only when one of the previously associated NAT IP pools/NAT IP pool groups is freed from the call.

NAT Application Level Gateway

Some network applications exchange IP/port information of the host endpoints as part of the packet payload. This information is used to create new flows, by server or client.

As part of NAT ALGs, the IP/port information is extracted from the payload, and the flows are allowed dynamically (through pinholes). IP and port translations are done accordingly. However, the sender application may not be aware of these translations since these are transparent, so they insert the private IP or port in the payload as usual.

For example, FTP NAT ALG interprets “PORT” and “PASV reply” messages, and NAT translates the same in the payload so that FTP happens transparently through NAT. This payload-level translation is handled by the NAT ALG module.

The NAT module will have multiple NAT ALGs for each individual application or protocol.

Supported NAT ALGs

This release supports NAT ALGs only for the following protocols:

- File Transfer Protocol (FTP)
- Point-to-Point Tunneling Protocol (PPTP): If PPTP ALG is enabled, NAT is supported for GRE flows that are generated by PPTP.
- Real Time Streaming Protocol (RTSP)
- Session Initiation Protocol (SIP)
- Trivial File Transfer Protocol (TFTP)

For NAT ALG processing, in the rulebase, routing rules must be configured to route packets to the corresponding analyzers.

EDRs and UDRs

This section describes the NAT-specific attributes supported in EDRs and UDRs.

EDRs

The following NAT-specific attributes are supported in regular EDRs:

- sn-nat-subscribers-per-ip-address: Subscriber(s) per NAT IP address
- sn-subscriber-nat-flow-ip: NAT IP address of NAT-enabled subscribers
- sn-subscriber-nat-flow-port: NAT port number of NAT-enabled subscribers

UDRs

The following NAT-specific attribute is supported in regular UDRs:

sn-subscriber-nat-flow-ip: NAT IP addresses that are being used by NAT-enabled subscribers. The NAT IP addresses assigned from each of the associated pool for the call are logged. A space is used as a separator between individual IP addresses.

Bulk Statistics

NAT bulkstats are per context and per NAT realm. The NAT realms are configured in a context and statistics are stored per context per realm. These statistic variables, both cumulative and snapshot, are available in the nat-realm schema.

Bulkstats are only generated for the first 100 NAT IP pools from an alphabetical list of all NAT IP pools, which is based on the context name and pool name. Therefore, to generate bulkstats for a specific NAT IP pool it must be named such that it gets selected in the first 100 bulkstats.

The following are cumulative statistics that can be part of NAT bulkstats:

- vpnname: Context name
- realmname: Realm name
- nat-bind-updates: Total interim AAA NBU sent
- nat-rlm-bytes-tx: Total number of bytes transferred by realm (uplink + downlink)
- nat-rlm-flows: Total number of flows used by the realm
- nat-rlm-ip-denied: Total number of flows denied NAT IP address
- nat-rlm-port-denied: Total number of flows denied NAT ports
- nat-rlm-max-port-chunk-subs: Total number of subscribers who used maximum number of port chunks
- nat-rlm-max-port-chunk-used: Maximum port chunks used

The following are snapshot statistics that can be part of NAT bulkstats:

- vpnname: Context name
- realmname: Realm name
- nat-rlm-ttl-ips: Total number of NAT public IP addresses, per context per NAT realm. Is a static value.
- nat-rlm-ips-in-use: Total number of NAT IP addresses currently in use, per context per NAT realm.
- nat-rlm-current-users: Total number of subscribers currently using the NAT realm.
- nat-rlm-ttl-port-chunks: Total number port-chunks, per context per NAT realm. Is a static value.
- nat-rlm-chunks-in-use: Total number of port-chunks currently in use, per context per NAT realm.
- nat-rlm-max-cur-port-chunk-subs: Current number of subscribers using maximum number of port chunks.
- nat-rlm-max-cur-port-chunk-used: Maximum port chunks used by active subscribers.
- nat-rlm-port-chunk-size: Size of the port chunk in the NAT realm.
- nat-rlm-port-chunk-average-usage-tcp: Average TCP port usage in the allocated TCP ports, i.e. out of allocated TCP ports how many got used. Not percentage value.
- nat-rlm-port-chunk-average-usage-udp: Average UDP port usage in the allocated UDP ports, i.e. out of allocated UDP ports how many got used. Not percentage value.
- nat-rlm-port-chunk-average-usage-others: Average other (ICMP or GRE) port usage in the allocated other ports, i.e. out of allocated ‘other’ ports how many got used. Not percentage value.

Alarms

Alert threshold values can be specified to generate alarms for NAT IP pools. To specify realm-specific threshold limits (pool-used, pool-free, pool-release, and pool-hold) “alert-threshold” NAT IP pool parameter can be used, or it can also be specified across context. These thresholds can be specified to any number of NAT IP pools.

In case of many-to-one NAT, it is possible to specify port-chunks usage threshold per NAT IP pool. This threshold value is applicable to all many-to-one NAT IP pools across the system. However, note that alarms are only generated for the first 100 many-to-one NAT IP pools from an alphabetical list of all NAT IP pools.

Session Recovery and ICSR

In session recovery, as part of the Private IP assigned to the subscriber:

- The public IP address used for the subscriber is recovered. The NAT IP address being used by the subscriber can be on-demand or not-on-demand. In case of many-to-one NAT, the port-chunks associated with the NAT IP address for the subscriber needs to check-pointed as well.
- In case Bypass NAT feature is used, then the private IP flow needs to be recovered.

To be recovered the NAT IP addresses need to be checkpointed. The checkpointing can be:

- Full Checkpoint
- Micro Checkpoint

To recover the bypass NAT flow, the bypass flow needs to be checkpointed. The checkpointing of Bypass NAT flow can be:

- Full Checkpoint
- Micro Checkpoint

In case of not-on-demand, the NAT IP address being used by the subscriber is known after call setup. This gets checkpointed as part of the normal full checkpoint. In case of on-demand NAT, the NAT IP address being used by the subscriber is known only in the data-path. This will be checkpointed as part of micro checkpoint.

In case of many-to-one NAT, the port-chunks being used will always be checkpointed as part of micro checkpoint.

In case of bypass NAT flow, in most cases the flow gets checkpointed as part of micro checkpoint.

Any information that is checkpointed as part of full checkpoint is always recovered. Data checkpointed through micro checkpoint cannot be guaranteed to be recovered. The timing of switchover plays a role for recovery of data done through micro checkpoint. If failover happens after micro checkpoint is completed, then the micro checkpointed data will get recovered. If failover happens during micro checkpoint, then the data recovered will be the one obtained from full checkpoint.

Once NAT IP/and Port-Chunks/Bypass NAT flow are recovered, the following holds good:

- One-to-one NAT: Since NAT IP address being used for one-to-one NAT is recovered, on-going flows will be recovered as part of Firewall Flow Recovery algorithm as one-to-one NAT does not change the port.
- Many-to-one NAT: On-going flows will not be recovered as the port numbers being used for flows across chassis peers/SessMgr peers are not preserved.
- Bypass NAT Flow: On-going flows will be recovered as part of Firewall Flow Recovery algorithm.

All of the above items is applicable for ICSR as well.

Category	Event		Impacted	Details
One-to-One NAT	Session		No	Session recovered.
	New Traffic		No	NAT will be applied.
	Ongoing Traffic		Yes	Cannot differentiate between ongoing traffic and unsolicited traffic. A rule-match is done and if allowed, NAT will be applied accordingly on the packet.
	Unsolicited Traffic (downlink packets)		Yes	Cannot differentiate between ongoing traffic and unsolicited traffic. Translation will be done and packet action taken based on the rule-match.
Many-to-One NAT	Session		No	Session recovered.
	New Traffic		No	NAT will be applied.
	Ongoing Traffic	TCP	Yes	Packet will be dropped.
		UDP	Yes and No	If it is downlink packet, it will be dropped. If it is uplink packet, NAT will be applied with a new port.
		ICMP	Yes and No	If it is downlink packet, it will be dropped. If it is uplink packet, NAT will be applied with a new port.
	Unsolicited Traffic (downlink packets)		No	Packet will be dropped.
Bypass NAT	Session		No	Session recovered.
	New Traffic		No	Traffic will be NAT bypassed.
	Ongoing Traffic		No	Traffic will be NAT bypassed.
	Unsolicited Traffic (downlink packets)		No	Traffic will be NAT bypassed.

For more information, in the *System Enhanced Feature Configuration Guide*, see the *Session Recovery* and *Interchassis Session Recovery* chapters.

How NAT Works

The following steps describe how NAT works:

Step 1 In the subscriber profile received from the AAA Manager, the SessMgr checks for the following:

- Enhanced Charging Service subsystem must be enabled
- In the Firewall-and-NAT policy, NAT must be enabled
- The Firewall-and-NAT policy must be valid
- For Many-to-One NAT, at least one valid NAT IP pool must be configured in the Firewall-and-NAT policy, and that NAT IP pool must be configured in the context

Step 2 If all of the above is true, once a private IP address is allocated to the subscriber, the NAT resource to be used for the subscriber is determined. This is only applicable for not-on-demand allocation mode.

Important: The private IP addresses assigned to subscribers must be from the following ranges for them to get translated: Class A 10.0.0.0 – 10.255.255.255, Class B 172.16.0.0 – 172.31.255.255, and Class C 192.168.0.0 – 192.168.255.255

Important: A subscriber can be allocated only one NAT IP address per NAT IP pool/NAT IP pool group from a maximum of three pools/pool groups. Hence, at any point, there can be a maximum of three NAT IP addresses allocated to a subscriber.

Step 3 Flow setup is based on the NAT mapping configured for the subscriber:

- In case of one-to-one NAT mapping, the subscriber IP address is mapped to a public IP address. The private source ports do not change. The SessMgr installs a flow using the NAT IP address and a fixed port range (1–65535).
- In case of many-to-one NAT mapping, a NAT IP address and a port from a port-chunk, are allocated for each connection originating from the subscriber. In order to identify a particular subscriber call line, the SessMgr installs a flow using NAT (public) IP address + NAT ports allocated for the subscriber.

The following figures illustrate the flow of packets in NAT processing.

Figure 1. NAT Processing Flow

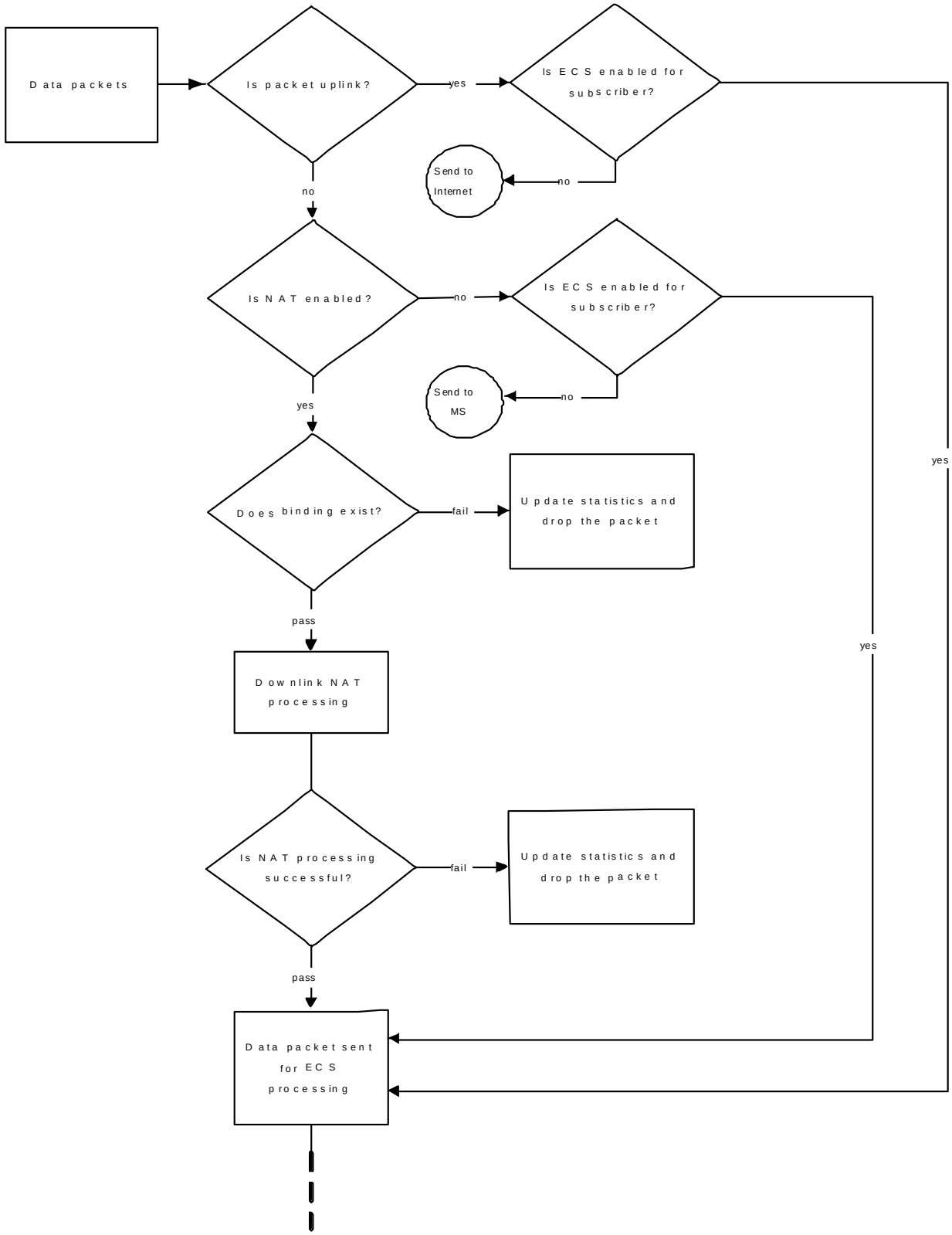


Figure 2. ... NAT Processing Flow

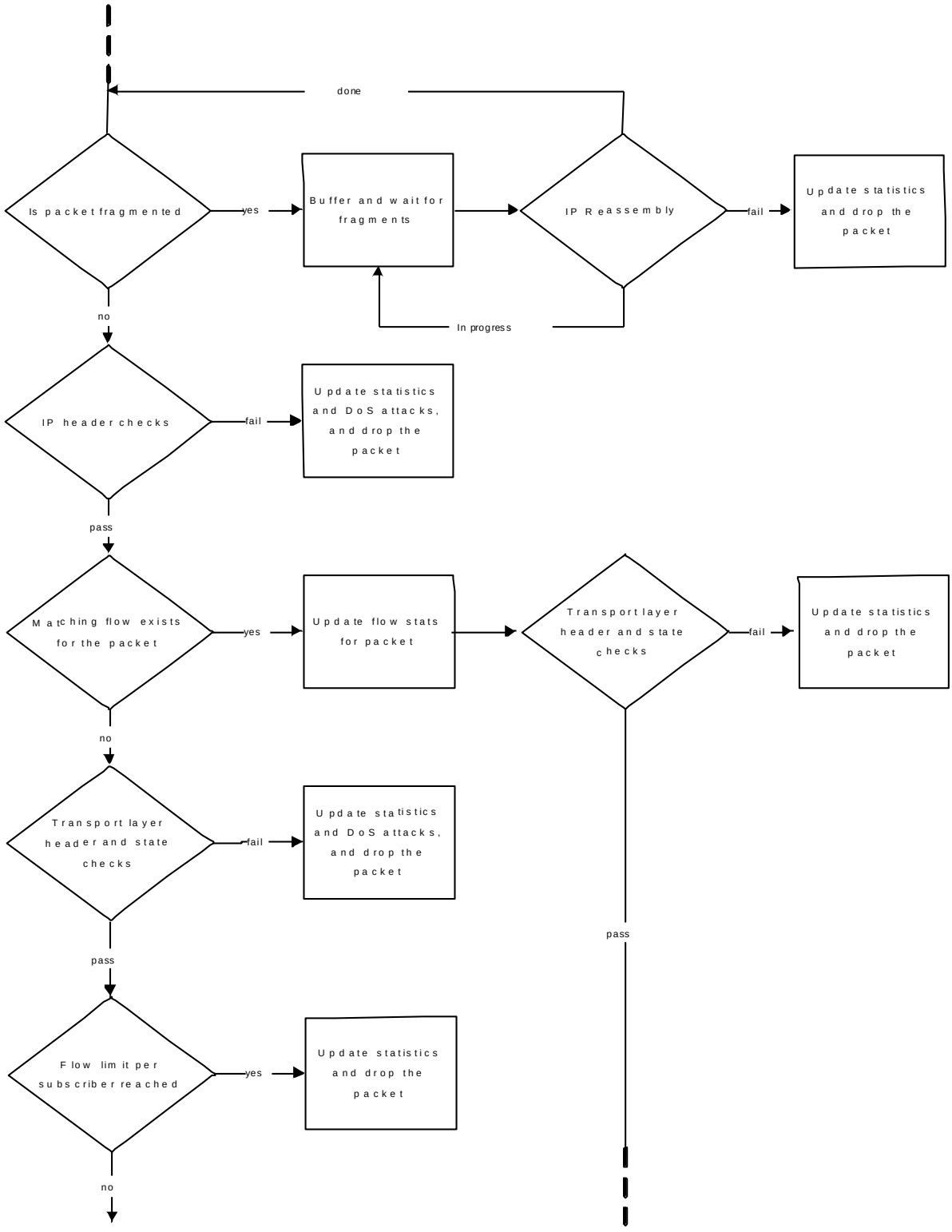


Figure 3. ... NAT Processing Flow

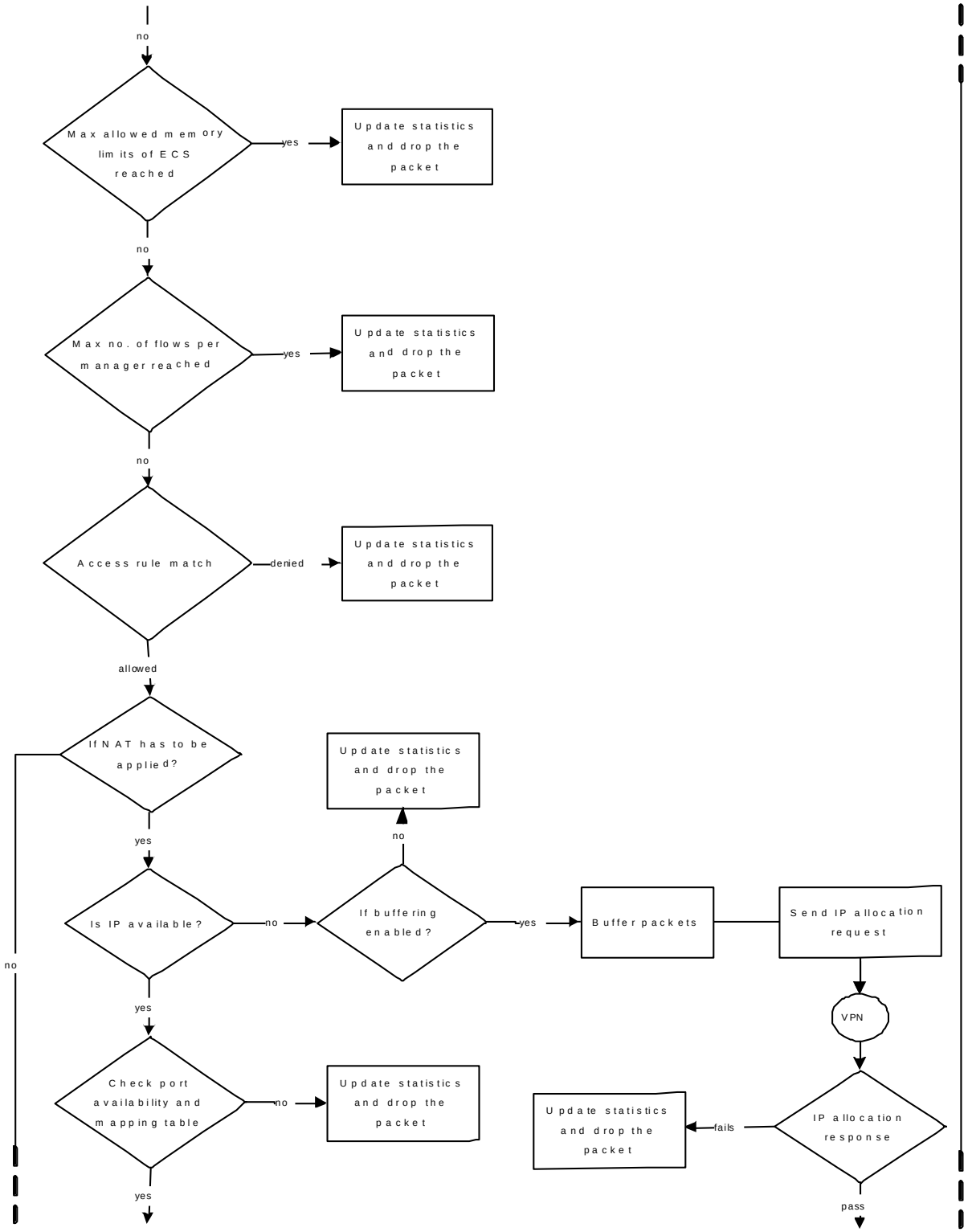
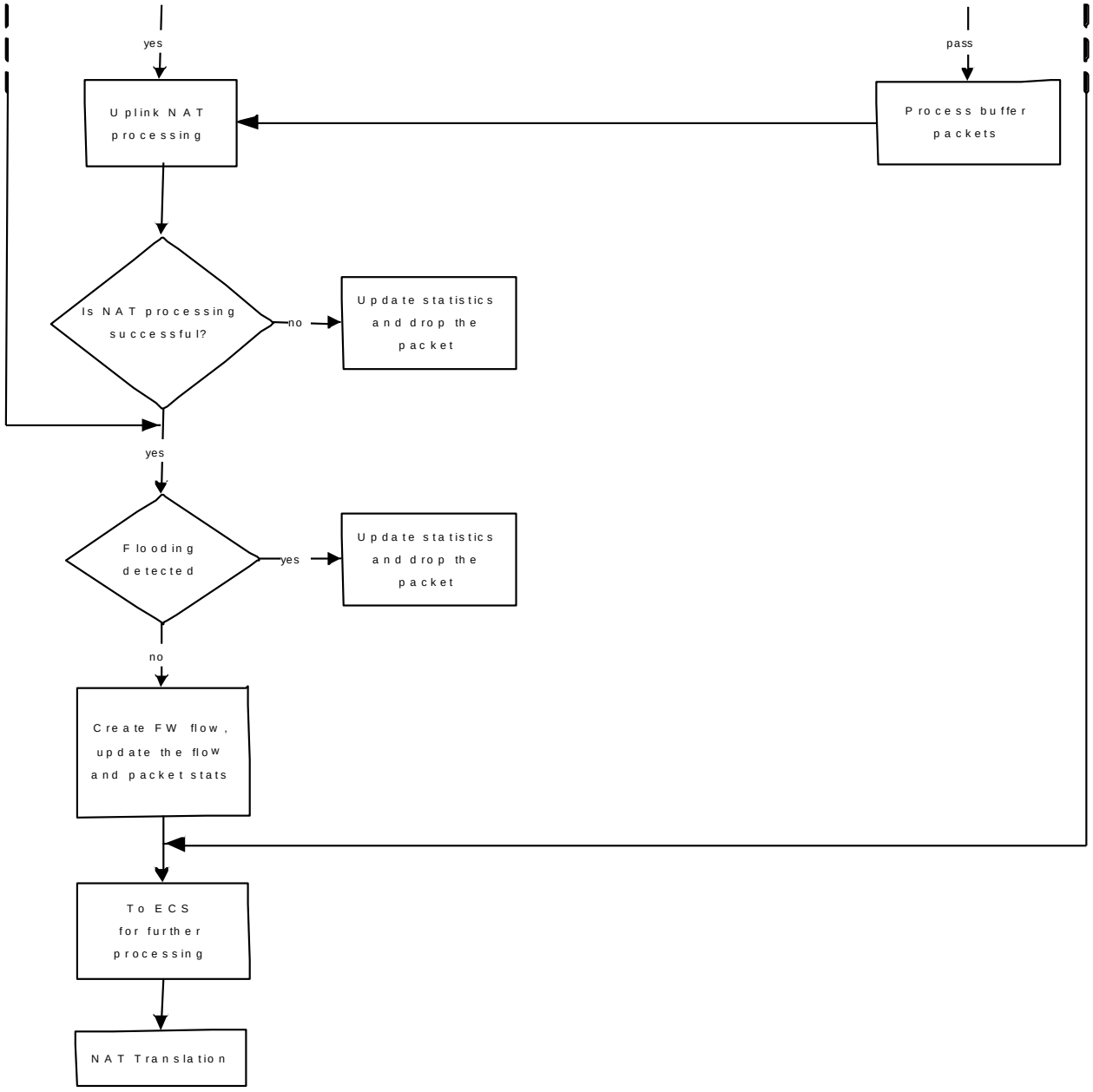


Figure 4. ... NAT Processing Flow



Chapter 2
NAT Configuration

This chapter describes how to configure the Network Address Translation (NAT) in-line service feature.

The following topics are covered in this chapter:

- Before You Begin
- Configuring the System
- Configuring NAT
- Verifying the Configuration
- Gathering NAT Statistics
- Saving the Configuration

Before You Begin

This section lists the steps to perform before you can start configuring NAT support on a system:

Step 1 Configure the required core network service on the system as described in the *System Administration Guide*.

Step 2 Obtain and install required licenses for the required number of subscriber sessions.

Step 3 Proceed to the Configuring the System section.

Configuring the System

This section lists the high-level steps to configure the NAT feature.

Step 1 Configure the NAT feature as described in the Configuring NAT section.

Step 2 Verify your configuration as described in the Verifying the Configuration section.

Step 3 Save the configuration as described in the Saving the Configuration section.

Configuring NAT

This section describes how to configure the NAT in-line service feature.

Step 1 Enable the Enhanced Charging Service (ECS) subsystem and create the enhanced charging service as described in the Enabling the ECS Subsystem and Creating the ECS Service section.

Step 2 *Optional:* Configure port maps as described in the Configuring Port Maps section.

Step 3 *Optional:* Configure host pools as described in the Configuring Host Pools section.

Step 4 *Optional:* Configure IMSI pools as described in the Configuring IMSI Pools section.

Step 5 Configure access ruledefs as described in the Configuring Access Ruledefs section.

Step 6 Configure NAT IP pools/NAT IP pool groups as described in the Configuring NAT Realms section.

Step 7 Configure Firewall-and-NAT policies as described in the Configuring Firewall-and-NAT Policy section.

Step 8 Configure action on NAT IP address/port allocation failure as described in the Configuring Action on NAT IP AddressPort Allocation Failure section.

Step 9 Configure action on packets during NAT IP allocation as described in the Configuring Action on Packets During NAT IP Allocation section.

Step 10 Configure NAT TCP-2msl-timeout setting as described in the Configuring NAT TCP-2msl-timeout Setting section.

Step 11 Configure action on TCP idle timeout as described in the Configuring Action on TCP Idle Timeout section.

Step 12 Configure Private IP NPU Flow Timeout setting as described in the Configuring Private IP NPU Flow Timeout Setting section.

Step 13 Configure Flow Recovery as described in the Configuring Flow Recovery section.

Step 14 Enable NAT support for APN/subscribers as described in the Enabling NAT for APNSubscribers section.

Step 15 *Optional:* Configure the default Firewall-and-NAT policy as described in the Configuring the Default Firewall-and-NAT Policy section.

Step 16 Configure NAT ALGs as described in the Configuring Dynamic PinholesApplication Level Gateways section.

Step 17 Configure EDR format as described in the Configuring EDR Format section.

Step 18 Configure UDR format as described in the Configuring UDR Format section.

Step 19 Configure NBR formats as described in the Configuring NAT Binding Record Format section.

Step 20 Configure NAT realm bulk statistics collection as described in the Configuring Bulkstats Collection section.

Step 21 Configure NAT thresholds as described in the Configuring NAT Thresholds section.

Step 22 Configure a secondary IP pool, which is not overwritten by the RADIUS supplied list, as described in the Backing Out of NAT section.

Important: Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Enabling the ECS Subsystem and Creating the ECS Service

To enable the ECS subsystem and create the enhanced charging service, use the following configuration:

```
configure
   require active-charging
   active-charging service <ecs_service_name> [ -noconfirm ]
   end
```

Configuring Port Maps

This is an optional configuration. To create and configure an application-port map for TCP and UDP protocols, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      port-map <port_map_name> [ -noconfirm ]
         port { <port_number> | range <start_port> to <end_port> }
         end
```

Notes:

- A maximum of 256 host pools, IMSI pools, and port maps each, and a combined maximum of 4096 rules (host pools + IMSI pools + port maps + charging ruledefs + access ruledefs + routing ruledefs) can be created in a system.
- Port maps, host pools, IMSI pools, and charging, access, and routing ruledefs must each have unique names.
- A maximum of 10 entries can be configured in each port map.

Configuring Host Pools

This is an optional configuration. To create and configure a host pool, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      host-pool <host_pool_name> [ -noconfirm ]
         ip { <ip_address> | <ip_address/mask> | range <start_ip_address> to
<end_ip_address> }
         end
```

Notes:

- A maximum of 256 host pools, IMSI pools, and port maps each, and a combined maximum of 4096 rules (host pools + IMSI pools + port maps + charging ruledefs + access ruledefs + routing ruledefs) can be created in a system.
- Port maps, host pools, IMSI pools, and charging, access, and routing ruledefs must each have unique names.
- A maximum of 10 entries can be configured in each host pool.

Configuring IMSI Pools

This is an optional configuration. To create and configure an IMSI pool, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      imsi-pool <imsi_pool_name> [ -noconfirm ]
         imsi { <imsi_number> | range <start_imsi> to <end_imsi> }
         end
```

Notes:

- A maximum of 256 host pools, IMSI pools, and port maps each, and a combined maximum of 4096 rules (host pools + IMSI pools + port maps + charging ruledefs + access ruledefs + routing ruledefs) can be created in a system.
- Port maps, host pools, IMSI pools, and charging, access, and routing ruledefs must each have unique names.
- A maximum of 10 entries can be configured in each port map.

Configuring Access Ruledefs

To create and configure an access rule definition, use the following configuration:

```
configure

   active-charging service <ecs_service_name>

      access-ruledef <access_ruledef_name> [ -noconfirm ]

         bearer 3gpp apn [ case-sensitive ] <operator> <value>

         bearer 3gpp imsi { <operator> <msid> | { !range | range } imsi-pool
<imsi_pool> }

         bearer username [ case-sensitive ] <operator> <user_name>

         icmp { any-match <operator> <condition> | code <operator> <code> | type
<operator> <type> }

         ip { { { any-match | downlink | uplink } <operator> <condition> } | { {
dst-address | src-address } { { <operator> { <ip_address> | <ip_address/mask> }
} | { !range | range } host-pool <host_pool_name> } | protocol { { <operator> {
<protocol> | <protocol_assignment> } } | { <operator> <protocol_assignment> } }

         tcp { any-match <operator> <condition> | { { dst-port | either-port |
src-port } { { <operator> <port_number> } | { !range | range } { <start_range>
to <end_range> | port-map <port_map_name> } } }

         udp { any-match <operator> <condition> | { dst-port | either-port |
src-port } { <operator> <port_number> | { !range | range } { <start_range> to
<end_range> | port-map <port_map_name> } } }

         create-log-record

         end
```

Notes:

- If the source IP address is not configured, then it is treated as any source IP.
- If the destination IP address is not configured, then it is treated as any destination IP.
- If the source port is not configured, then it is treated as any source port.
- If the destination port is not configured, then it is treated as any destination port.
- If no protocol is specified then it is treated as any protocol.
- If both uplink and downlink fields are not configured, then the rule will be treated as either direction, i.e. packets from any direction will match that rule.

- Access ruledefs are different from enhanced charging service ruledefs. A combined maximum of 4096 rules (host pools, IMSI pools, port maps, and access, charging, and routing ruledefs) can be created in a system. A combined maximum of 2048 access and charging ruledefs can be created in a system.
- Configuring access ruledefs involves the creation of several ruledefs with different sets of rules and parameters. For more information, see the *Firewall Ruledef Configuration Mode Commands* chapter of the *Command Line Interface Reference*.

Configuring NAT IP pools/NAT IP Pool Groups

This section describes how to create and configure NAT IP pools/NAT IP pool groups.

The following topics are covered in this section:

- Configuring One-to-One NAT Realm
- Configuring Many-to-One NAT Realm

Configuring One-to-One NAT IP Pools /NAT IP Pool Groups

To create and configure a one-to-one NAT IP pool/NAT IP pool group, use the following configuration:

```
configure

   context <context_name> [ -noconfirm ]

      ip pool <nat_pool_name> { <ip_address> <subnet_mask> | <ip_address/mask> |
range <start_ip_address> <end_ip_address> } nat-one-to-one [ alert-threshold { {
pool-free | pool-hold | pool-release | pool-used } <low_thresh> [ clear
<high_thresh> ] } + ] [ group-name <nat_pool_group_name> ] [ nat-binding-timer
<binding_timer> ] [ nexthop-forwarding-address <ip_address> ] [ on-demand ] [
send-icmp-dest-unreachable ] [ send-nat-binding-update ] [ srp-activate ] + ]

      ip pool <pool_name> { <ip_address> <subnet_mask> | <ip_address/mask> |
range <start_ip_address> <end_ip_address> } public <priority>

      end
```

Notes:

- Within a context, all IP pool and NAT IP pool and NAT IP pool group names must be unique.
- IP pool and NAT IP pool and NAT IP pool group names are case sensitive.
- The IP addresses configured in the NAT IP pools within a context must not overlap. At any time, within a context, a NAT IP address must be configured in any one NAT IP pool.
- The IP addresses in a NAT IP pool may be contiguous, and must be assignable as a subnet or a range that constitutes less than an entire subnet.

- For many-to-one NAT IP pools, the default NAT Binding Timer value is 60 seconds. For one-to-one NAT IP pools, by default the feature is disabled—the IP addresses/ port-chunks once allocated will never be freed.
- Thresholds configured using the **alert-threshold** keyword are specific to the pool that they are configured in. Thresholds configured using the **threshold ip-pool-*** commands in the Context Configuration Mode apply to all IP pools in the context, and override the threshold configurations set within individual pools.
- Not-on-demand allocation mode is the default NAT IP Address Allocation mode.
- To add a NAT IP pool to a NAT IP pool group, use the **group-name** *<nat_pool_group_name>* option.

  NAT IP pool and NAT IP pool group names must be unique.

  When configuring a NAT IP pool group, note that only those NAT IP pools that have similar characteristics can be grouped together. The similarity is determined by the "nat-one-to-one" and "on-demand" parameters. Dissimilar NAT IP pools cannot be grouped together.

  It is recommended that for each NAT IP pool in a NAT IP pool group the other parameters ("nat-binding-timer", "send-nat-binding-update", "nexthop-forwarding-address", "send-icmp-dest-unreachable", and "srp-activate") also be configured with the same values, so that the NAT behavior is predictable across all NAT IP pools in that NAT IP pool group.

  The NAT IP pool from which a NAT IP address is assigned will determine the actual values to use for all parameters.
- It is recommended that in a Firewall-and-NAT policy all the realms configured either be NAT IP pools or NAT IP pool groups. If both NAT IP pool(s) and NAT IP pool group(s) are configured, ensure that none of the NAT IP pool(s) are also included in the NAT IP pool group.

Configuring Many-to-One NAT IP Pools /NAT IP Pool Groups

To create and configure a Many-to-One NAT IP pool/NAT IP pool group, use the following configuration:

```
configure

   context <context_name> [ -noconfirm ]

      ip pool <nat_pool_name> { <ip_address> <subnet_mask> | <ip_address/mask> |
range <start_ip_address> <end_ip_address> } napt-users-per-ip-address <users> [
alert-threshold { { pool-free | pool-hold | pool-release | pool-used }
<low_thresh> [ clear <high_thresh> ] } + ] [ group-name <nat_pool_group_name> ]
[ max-chunks-per-user <chunks> ] [ nat-binding-timer <binding_timer> ] [
nexthop-forwarding-address <ip_address> ] [ on-demand ] [ port-chunk-size <size>
] [ port-chunk-threshold <threshold> ] [ send-icmp-dest-unreachable ] [ send-
nat-binding-update ] [ srp-activate ] + ]

      ip pool <pool_name> { <ip_address> <subnet_mask> | <ip_address/mask> |
range <start_ip_address> <end_ip_address> } public <priority>

      end
```

Notes:

- Within a context, all IP pool and NAT IP pool and NAT IP pool group names must be unique.

- IP pool and NAT IP pool and NAT IP pool group names are case sensitive.
- The IP addresses configured in the NAT IP pools within a context must not overlap. At any time, within a context, a NAT IP address must be configured in any one NAT IP pool.
- The IP addresses in a NAT IP pool may be contiguous, and must be assignable as a subnet or a range that constitutes less than an entire subnet.
- For many-to-one NAT IP pools, the default NAT Binding Timer value is 60 seconds. For one-to-one NAT IP pools, by default the feature is disabled—the IP addresses/ port-chunks once allocated will never be freed.
- Thresholds configured using the **alert-threshold** keyword are specific to the pool that they are configured in. Thresholds configured using the **threshold ip-pool-*** commands in the Context Configuration Mode apply to all IP pools in the context, and override the threshold configurations set within individual pools.
- Not-on-demand allocation mode is the default NAT IP Address Allocation mode.
- To add a NAT IP pool to a NAT IP pool group, use the **group-name** *<nat_pool_group_name>* option.

  NAT IP pool and NAT IP pool group names must be unique.

  When configuring a NAT IP pool group, note that only those NAT IP pools that have similar characteristics can be grouped together. The similarity is determined by the “napt-users-per-ip-address”, “napt-users-per-ip-address <users>”, “on-demand”, and “port-chunk-size” parameters. Dissimilar NAT IP pools cannot be grouped together.

  It is recommended that for each NAT IP pool in a NAT IP pool group the other parameters (“nat-binding-timer”, “send-nat-binding-update”, “nexthop-forwarding-address”, “send-icmp-dest-unreachable”, “srp-activate”, and “port-chunk-threshold”) also be configured with the same values, so that the NAT behavior is predictable across all NAT IP pools in that NAT IP pool group.

  The NAT IP pool from which a NAT IP address is assigned will determine the actual values to use for all parameters.
- It is recommended that in a Firewall-and-NAT policy all the realms configured either be NAT IP pools or NAT IP pool groups. If both NAT IP pool(s) and NAT IP pool group(s) are configured, ensure that none of the NAT IP pool(s) are also included in the NAT IP pool group.

Configuring Firewall-and-NAT Policies

To create and configure a Firewall-and-NAT Policy, use the following configuration:

```
configure

   active-charging service <ecs_service_name>

      fw-and-nat policy <fw_nat_policy_name> [ -noconfirm ]

         nat policy nat-required default-nat-realm <nat_pool_name /
nat_pool_group_name>

         access-rule priority <priority> { [ dynamic-only | static-and-dynamic ]
access-ruledef <access_ruledef_name> { deny [ charging-action
<charging_action_name> ] | permit [ nat-realm
<nat_pool_name/nat_pool_group_name> | [ bypass-nat ] ] }
```

```
        access-rule no-ruledef-matches { downlink | uplink } action { deny [
charging-action <charging_action_name> ] | permit [ bypass-nat | nat-realm
<nat_pool_name/nat_pool_group_name> ] }

        end
```

Notes:

- In StarOS 8.x, NAT for CDMA and early UMTS releases used rulebase-based configurations, whereas in later UMTS releases NAT used policy-based configurations. In StarOS 9.0 and later releases, NAT for UMTS and CDMA releases both use policy-based configurations. For more information, please contact your local service representative.
- The **nat policy nat-required** command enables NAT for all subscribers using the policy.
- Duplicate ruledef names or priorities are not allowed in the same rulebase
- A maximum of three NAT IP pools/NAT IP pool groups can be configured in a policy. A subscriber can be allocated only one NAT IP address per NAT IP pool/NAT IP pool group from a maximum of three pools/pool groups. Hence, at anytime, there can only be a maximum of three NAT IP addresses allocated to a subscriber.
- It is recommended that in a Firewall-and-NAT policy all the realms configured either be NAT IP pools or NAT IP pool groups. If both NAT IP pool(s) and NAT IP pool group(s) are configured, ensure that a NAT IP pool is not a part of a NAT IP pool group.
- NAT is applied only to packets in the uplink direction.
- Rule matching is done for the first packet for a flow. Only when no rules match, the **no-ruledef-matches** configuration is considered. The default settings for uplink direction is “permit”, and for downlink direction “deny”.
- If there are no rules matching a packet, then the NAT IP pool/NAT IP pool group to be used for the flow is taken from the following configuration:

  access-rule no-ruledef-matches uplink action permit nat-realm *<nat_pool_name/nat_pool_group_name>*
- If there is no NAT IP pool/NAT IP pool group name configured in the matching access ruledef, NAT will be bypassed, i.e., NAT will not be applied to the flow.

Configuring Action on NAT IP Address/Port Allocation Failure

To configure sending ICMP error messages in the event of NAT IP address/port allocation failure, use the following configuration:

```
configure

   active-charging service <ecs_service_name>

      nat allocation-failure send-icmp-dest-unreachable

      end
```

Configuring Action on Packets During NAT IP Allocation

To configure action to take on packets when NAT IP/NPU allocation is in progress, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      nat allocation-in-progress { buffer | drop }
      end
```

Notes:

- In On-demand NAT IP allocation (wherein a NAT IP address is allocated to the subscriber when a packet is being sent), if no free NAT IP address is available, a NAT-IP Alloc Request is sent to the VPNMgr to get a NAT IP. During that time packets are dropped. This command enables to either buffer or drop the packets received when IP Alloc Request is sent to VPNMgr.

Configuring NAT TCP-2msl-timeout Setting

To configure NAT TCP 2msl Timeout setting, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      nat tcp-2msl-timeout <timeout>
      end
```

Configuring Action on TCP Idle Timeout

To configure action to take on TCP idle timeout expiry for NAT flows, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      fw-and-nat policy <fw_nat_policy_name>
         firewall tcp-idle-timeout-action { drop | reset }
         end
```

Configuring Private IP NPU Flow Timeout Setting

To configure Private IP NPU Flow Timeout setting, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      fw-and-nat policy <fw_nat_policy_name>
         nat private-ip-flow-timeout <timeout>
         end
```

Notes:

- By default, for NAT-enabled calls the downlink private IP NPU flow will not be installed at call setup for a subscriber session. The flow will only be installed for uplink traffic on demand. When there is no traffic on the private flow, the private IP flow will be removed after the configurable timeout period.
- Downlink traffic will be dropped after flow is deleted after the configurable timeout period.

Configuring Flow Recovery

To configure Flow Recovery parameters for NAT flows, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      firewall flow-recovery { downlink | uplink } [ [ no-flow-creation ] [
timeout <timeout> ] + ]
      end
```

Notes:

- The **no-flow-creation** keyword specifies not to create data session/flow-related information for downlink-initiated packets (from the Internet to the subscriber) while the downlink flow-recovery timer is running, but send to subscriber.

Enabling NAT for APN/Subscribers

This section describes how to enable NAT support for APN/subscribers.

The following topics are covered in this section:

- Enabling NAT for APN
- Enabling NAT for Subscribers

Enabling NAT for APN

To configure the Firewall-and-NAT Policy within an APN, use the following configuration:

Important: This configuration is only applicable to UMTS networks.

```
configure
   context <context_name>
      apn <apn_name>
         fw-and-nat policy <fw_nat_policy_name>
         end
```

Notes:

- *<fw_nat_policy_name>* must be a valid Firewall-and-NAT policy in which NAT policy is enabled as described in the Configuring Firewall-and-NAT Policy section.
- To specify that the default Firewall-and-NAT policy configured in the rulebase be used for subscribers who use this APN, in the APN Configuration Mode, apply the following command: **default fw-and-nat policy**

Enabling NAT for Subscribers

To configure the Firewall-and-NAT Policy in a subscriber template, use the following configuration:

```
configure
   context <context_name>
      subscriber default
         fw-and-nat policy <fw_nat_policy_name>
         end
```

Notes:

- *<fw_nat_policy_name>* must be a valid Firewall-and-NAT policy in which NAT policy is enabled as described in the Configuring Firewall-and-NAT Policy section.

- To specify that the default Firewall-and-NAT policy configured in the rulebase be used for subscribers, in the Subscriber Configuration Mode, apply the following command: **`default fw-and-nat policy`**

Configuring the Default Firewall-and-NAT Policy

This is an optional configuration to specify a default Firewall-and-NAT policy to use if in the APN/subscriber configurations the following command is configured:

`default fw-and-nat policy`

To create a rulebase and configure a default Firewall-and-NAT policy in it, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      rulebase <rulebase_name> [ -noconfirm ]
         fw-and-nat default-policy <fw_nat_policy_name>
         end
```

Configuring NAT Application Level Gateways/Dynamic Pinholes

This section describes how to configure routing rules to open up dynamic pinholes for Application Level Gateways (ALG) functionality.

The following topics are covered in this section:

- Creating Routing Ruledefs
- Configuring Routing Ruledefs in Rulebase
- Enabling NAT ALG

Creating Routing Ruledefs

To configure ECS routing rules for FTP and RTSP protocols, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      ruledef <ruledef_name>
         tcp either-port <operator> <value>
         rule-application routing
```

```
end
```

Notes:

- Create a separate routing ruledef for each protocol.

Configuring Routing Ruledefs in Rulebase

To configure the routing ruledefs in the rulebase, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      rulebase <rulebase_name>
         route priority <priority> ruledef <ruledef_name> analyzer { ftp-control
| pptp | rtsp | sip advanced | tftp }
         rtp dynamic-flow-detection
         end
```

Notes:

- Add each routing ruledef as a separate route priority.
- If PPTP ALG is enabled, NAT is supported for GREv1 flows that are generated by PPTP.
- For RTSP ALG processing, in the rulebase, the **rtp dynamic-flow-detection** command must be configured.
- For SIP ALG processing, the **advanced** option must be configured to ensure that packets matching the routing rule will be routed to the SIP ALG for processing and not to the ECS SIP analyzer.

Enabling NAT ALG

To enable NAT ALGs, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      firewall nat-alg { all | ftp | pptp | rtsp | sip }
      idle-timeout alg-media <idle_timeout>
      end
```

Notes:

- If enabled, in the rulebase, a routing rule for the protocol must be configured. For example:

  route priority 1 ruledef ftp analyzer ftp-control

  route priority 2 ruledef rtsp analyzer rtsp

- For RTSP NAT ALG processing, in the rulebase, the following command must be configured:

  rtp dynamic-flow-detection

- The **idle-timeout alg-media** *idle_timeout* CLI command configures the Media Inactivity Timeout setting. The timeout gets applied on RTP and RTCP media flows that are created for SIP calls. The timeout is applied only on those flows that actually match the RTP and RTCP media pinholes that are created by the SIP ALG.
- Configuration changes are only applied to new flows.

Configuring EDR Format

To configure EDR format for NAT-specific attributes, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      edr-format <edr_format_name>
         attribute sn-nat-subscribers-per-ip-address priority <priority>
         attribute sn-subscriber-nat-flow-ip priority <priority>
         attribute sn-subscriber-nat-flow-port priority <priority>
         end
```

Configuring UDR Format

To configure UDR format for NAT-specific attributes, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      udr-format <udr_format_name>
         attribute sn-subscriber-nat-flow-ip priority <priority>
         end
```

Configuring NAT Binding Record Format

To configure NBR format, use the following configuration:

```
configure
   active-charging service <ecs_service_name>
      edr-format <nbr_format_name>
         attribute sn-correlation-id priority <priority>
         rule-variable ip subscriber-ip-address priority <priority>
         attribute sn-fa-correlation-id priority <priority>
         attribute radius-fa-nas-ip-address priority <priority>
         attribute radius-fa-nas-identifier priority <priority>
         attribute radius-user-name priority <priority>
         attribute radius-calling-station-id priority <priority>
         attribute sn-nat-ip priority <priority>
         attribute sn-nat-port-block-start priority <priority>
         attribute sn-nat-port-block-end priority <priority>
         attribute sn-nat-binding-timer priority <priority>
         attribute sn-nat-subscribers-per-ip-address priority <priority>
         attribute sn-nat-realm-name priority <priority>
         attribute sn-nat-gmt-offset priority <priority>
         attribute sn-nat-port-chunk-alloc-dealloc-flag priority <priority>
         attribute sn-nat-port-chunk-alloc-time-gmt priority <priority>
         attribute sn-nat-port-chunk-dealloc-time-gmt priority <priority>
         attribute sn-nat-last-activity-time-gmt priority <priority>
         exit
      fw-and-nat policy <fw_nat_policy_name>
         nat binding-record edr-format <nbr_format_name>  port-chunk-allocation
port-chunk-release
         end
```

Notes:

- The NBR format name configured in the **edr-format** *<nbr_format_name>* and the **nat binding-record edr-format** *<nbr_format_name>* commands must be the same.

Configuring Bulkstats Collection

To configure NAT realm bulk statistics collection, use the following configuration:

```
configure
   bulkstats collection
   bulkstats historical collection
   bulkstats mode
      sample-interval <sample_interval>
      transfer-interval <transfer_interval>
      file <file_number>
         remotefile format <format>
         receiver <ip_address> primary mechanism { tftp | { ftp | sftp } login
<login> encrypted password <password> }
         exit
      nat-realm schema <schema_name> format <format_string>
      end
```

The following is a sample configuration for cumulative bulkstats collection:

```
nat-realm schema cumulativenatschema format "NAT-REALM Schema:
cumulativenatschema\nVPN Name: %vpnname%\nRealm Name: %realmname%\n Total
binding updates sent to AAA: %nat-bind-updates%\nTotal bytes transferred
by realm: %nat-rlm-bytes-tx%\nTotal flows used by realm: %nat-rlm-
flows%\nTotal flows denied IP: %nat-rlm-ip-denied%\nTotal flows denied
ports: %nat-rlm-port-denied%\n----------------------\n"
```

The following is a sample configuration for snapshot bulkstats collection:

```
nat-realm schema snapshotnatschema format "NAT-REALM Schema:
snapshotnatschema\nVPN Name: %vpnname%\nRealm Name: %realmname%\nTotal
NAT public IP address: %nat-rlm-ttl-ips%\nCurrent NAT public IP address
in use: %nat-rlm-ips-in-use%\nCurrent subscribers using realm: %nat-rlm-
current-users%\nTotal port chunks: %nat-rlm-ttl-port-chunks%\nCurrent
port chunks in use: %nat-rlm-chunks-in-use%\n----------------------\n"
```

Configuring NAT Thresholds

This section describes how to configure NAT thresholds.

The following topics are covered in this section:

- Enabling Thresholds
- Configuring Threshold Poll Interval
- Configuring Thresholds Limits
- Enabling SNMP Notifications

Enabling Thresholds

To enable thresholds, use the following configuration:

```
configure
   threshold monitoring firewall
   context <context_name>
      threshold monitoring available-ip-pool-group
      end
```

Notes:

- The **threshold monitoring available-ip-pool-group** command is required only if you are configuring IP pool thresholds. It is not required if you are only configuring NAT port chunks usage threshold.

Configuring Threshold Poll Interval

To configure threshold polling interval, use the following configuration:

```
configure
   threshold poll ip-pool-used interval <interval>
   threshold poll nat-port-chunks-usage interval <interval>
   end
```

Configuring Thresholds Limits

To configure threshold limits, use the following configuration:

```
configure
   context <context_name>
      threshold ip-pool-free <high_threshold> clear <low_threshold>
      threshold ip-pool-hold <high_threshold> clear <low_threshold>
      threshold ip-pool-release <high_threshold> clear <low_threshold>
      threshold ip-pool-used <high_threshold> clear <low_threshold>
      exit
   threshold nat-port-chunks-usage <high_threshold> clear <low_threshold>
   end
```

Notes:

- Thresholds configured using the **`threshold ip-pool-*`** commands in the Context Configuration Mode apply to all IP pools in the context.
- The thresholds configured for an individual NAT IP pool using the **`alert-threshold`** keyword will take priority, i.e it will override the above context-wide configuration.

Enabling SNMP Notifications

To enable SNMP notifications, use the following configuration:

```
configure
   snmp trap { enable | suppress } { ThreshNATPortChunksUsage |
ThreshClearNATPortChunksUsage }
   snmp trap { enable | suppress } { ThreshIPPoolUsed | ThreshIPPoolFree |
ThreshIPPoolRelease | ThreshIPPoolHold | ThreshClearIPPoolUsed }
   end
```

Backing Out of NAT

This is a licensed feature requiring the [600-00-7871] *NAT Bypass* license. For more information please contact your local sales representative.

Configuring NAT Backout for APN

To configure a secondary IP pool that is not overwritten by the RADIUS supplied list, use the following configuration. The secondary pool configured will be appended to the RADIUS supplied IP pool list / APN provided IP pool list whichever is applicable during call setup.

 ***Important:*** This configuration is only applicable to UMTS networks.

```
configure
   context <context_name>
      apn <apn_name>
         secondary ip pool <pool_name>
         exit
      busyout ip pool name <private_pool_name>
      end
```

Notes:

- The **secondary ip pool** *<pool_name>* command is license dependent.
- The **busyout ip pool name** *<private_pool_name>* command must be configured in the destination context. This command makes addresses from the specified IP pool in the current context unavailable once they are free.

Configuring NAT Backout for Subscribers

To configure a secondary IP pool that is not overwritten by the RADIUS supplied list, use the following configuration. The secondary pool configured will be appended to the RADIUS supplied IP pool list/subscriber template provided IP pool list whichever is applicable during call setup.

```
configure
   context <context_name>
      subscriber default
         secondary ip pool <pool_name>
         exit
      busyout ip pool name <private_pool_name>
      end
```

Notes:

- The **secondary ip pool** *<pool_name>* command is license dependent.
- The **busyout ip pool name** *<private_pool_name>* command must be configured in the destination context. This command makes addresses from the specified IP pool in the current context unavailable once they are free.

Changing Firewall-and-NAT Policy in Mid-session

To change Firewall-and-NAT policy in mid-session, use the following configuration:

```
update active-charging { switch-to-fw-and-nat-policy <fw_nat_policy_name> |
switch-to-rulebase <rulebase_name> } { all | callid <call_id> | fw-and-nat-
policy <fw_nat_policy_name> | imsi <imsi> | ip-address <ipv4_address> | msid
<msid> | rulebase <rulebase_name> | username <user_name> } [ -noconfirm ]
```

Notes:

- To be able to change the Firewall-and-NAT policy in mid session, firewall-and-NAT must have been enabled for the subscriber in the APN/Subscriber template configuration, or in the rulebase (the default policy) during call setup.
- The above command takes effect only for current calls. For new calls, the RADIUS returned/APN/subscriber template/rulebase configured policy is used.

Verifying the Configuration

To verify your configurations:

Step 1 To view subscriber configuration, in the Exec mode, enter the following command:

```
show subscriber full
```

The output displays subscriber information. Verify the NAT IP pools associated with subscriber and the NAT IP addresses allocated from each pool.

If a pool type is not-on-demand, the pool's type is indicated explicitly.

Step 2 To view enhanced charging flow information, in the Exec mode, enter the following command:

```
show active-charging flows full
```

The output displays enhanced charging flow information.

For many-to-one NAT, verify the NAT IP address and NAT port used for the subscriber flow.

For one-to-one NAT, verify the NAT IP address.

For ICMP, the NAT IP address is displayed only if an active ICMP record is available.

Saving the Configuration

To save changes to the configuration, see the *Verifying and Saving Your Configuration* chapter.

Gathering NAT Statistics

The following table lists the commands that can be used to gather NAT statistics.

In the following table, the first column lists what statistics to gather and the second column lists the command to use.

Table 1. Gathering NAT Statistics

Statistics/Information	Action to perform
NAT statistics	**show active-charging nat statistics**
Statistics of a specific NAT IP pool	**show active-charging nat statistics nat-realm** *<nat_pool_name>*
Statistics of all NAT IP pools in a NAT IP pool group	**show active-charging nat statistics nat-realm** *<pool_group_name>*
Summary statistics of all NAT IP pools in a NAT IP pool group	**show active-charging nat statistics nat-realm** *<pool_group_name>***summary**
Firewall-and-NAT Policy statistics.	**show active-charging fw-and-nat policy statistics all** **show active-charging fw-and-nat policy statistics name** *<fw_nat_policy_name>*
Information on NAT bind records generated for port chunk allocation and release.	**show active-charging rulebase statistics name** *<rulebase_name>*
Information on NAT bind records generated.	**show active-charging edr-format statistics**
Information for subscriber flows with NAT disabled.	**show active-charging flows nat not-required**
Information for subscriber flows with NAT enabled.	**show active-charging flows nat required**
Information for subscriber flows with NAT enabled, and using specific NAT IP address.	**show active-charging flows nat required nat-ip** *<nat_ip_address>*
Information for subscriber flows with NAT enabled, and using specific NAT IP address and NAT port number.	**show active-charging flows nat required nat-ip** *<nat_ip_address>* **nat-port** *<nat_port>*
NAT session details.	**show active-charging sessions nat { not-required | required }**
Information for all current subscribers who have either active or dormant sessions. Check IP address associated with subscriber.	**show subscribers full all**
Information for subscribers with NAT processing not required.	**show subscribers nat not-required**
Information for subscribers with NAT processing enabled and using the specified NAT IP address.	**show subscribers nat required nat-ip** *<nat_ip_address>*
Information for subscribers with NAT processing enabled and using the specified NAT realm.	**show subscribers nat required nat-realm** *<nat_pool_name>*
NAT realm IP address pool information.	**show ip pool nat-realm wide**

Statistics/Information	Action to perform
Call drop reason due to invalid NAT configuration.	`show session disconnect-reasons`

Chapter 3
Verifying and Saving Your Configuration

This chapter describes how to save the system configuration.

Verifying the Configuration

You can use a number of command to verify the configuration of your feature, service, or system. Many are hierarchical in their implementation and some are specific to portions of or specific lines in the configuration file.

Feature Configuration

In many configurations, specific features are set and need to be verified. Examples include APN and IP address pool configuration. Using these examples, enter the following commands to verify proper feature configuration:

show apn all

The output displays the complete configuration for the APN. In this example, an APN called apn1 is configured.

```
access point name (APN): apn1

authentication context: test

pdp type: ipv4

Selection Mode: subscribed

ip source violation: Checked drop limit: 10

accounting mode: gtpp No early PDUs: Disabled

max-primary-pdp-contexts: 1000000 total-pdp-contexts: 1000000

primary contexts: not available total contexts: not available

local ip: 0.0.0.0

primary dns: 0.0.0.0 secondary dns: 0.0.0.0

ppp keep alive period : 0 ppp mtu : 1500

absolute timeout : 0 idle timeout : 0

long duration timeout: 0 long duration action: Detection

ip header compression: vj

data compression: stac mppc deflate compression mode: normal

min compression size: 128

ip output access-group: ip input access-group:

ppp authentication:

allow noauthentication: Enabled imsi
```

```
 authentication:Disabled
```

Enter the following command to display the IP address pool configuration:

show ip pool

The output from this command should look similar to the sample shown below. In this example, all IP pools were configured in the *isp1* context.

```
context : isp1:

+-----Type: (P) - Public (R) - Private

 | (S) - Static (E) - Resource

 |

 |+----State: (G) - Good (D) - Pending Delete (R)-Resizing

 ||

 ||++--Priority: 0..10 (Highest (0) .. Lowest (10))

 ||||

 ||||+-Busyout: (B) - Busyout configured

 |||| |||||| vvvvv Pool Name Start Address Mask/End Address Used Avail

 ----- --------- --------------- --------------- -------- --------

PG00 ipsec 12.12.12.0 255.255.255.0 0 254 PG00

pool1 10.10.0.0 255.255.0.0 0 65534 SG00

vpnpool 192.168.1.250 192.168.1.254 0 5 Total Pool Count: 5
```

Important: Many features can be configured on the system. There are show commands specifically for these features. Refer to the *Command Line Interface Reference* for more information.

Service Configuration

Verify that your service was created and configured properly by entering the following command:

show *<service_type> <service_name>*

The output is a concise listing of the service parameter settings similar to the sample displayed below. In this example, a P-GW service called pgw is configured.

```
Service name : pgw1

Service-Id : 1
```

```
Context : test1

Status : STARTED

Restart Counter : 8

EGTP Service : egtp1

LMA Service : Not defined

Session-Delete-Delay Timer : Enabled

Session-Delete-Delay timeout : 10000(msecs)

PLMN ID List : MCC: 100, MNC: 99

Newcall Policy : None
```

Context Configuration

Verify that your context was created and configured properly by entering the following command:

show context name *<name>*

The output shows the active context. Its ID is similar to the sample displayed below. In this example, a context named *test1* is configured.

```
Context Name     ContextID     State

------------     ---------     -----

test1            2          Active
```

System Configuration

Verify that your entire configuration file was created and configured properly by entering the following command:

show configuration

This command displays the entire configuration including the context and service configurations defined above.

Finding Configuration Errors

Identify errors in your configuration file by entering the following command:

show configuration errors

This command displays errors it finds within the configuration. For example, if you have created a service named "service1", but entered it as "srv1" in another part of the configuration, the system displays this error.

You must refine this command to specify particular sections of the configuration. Add the **section** keyword and choose a section from the help menu:

show configuration errors section ggsn-service

or

show configuration errors section aaa-config

If the configuration contains no errors, an output similar to the following is displayed:

```
##################################################################################

Displaying Global
AAA-configuration errors
##################################################################################

Total 0 error(s) in this section !
```

Saving the Configuration

Save system configuration information to a file locally or to a remote node on the network. You can use this configuration file on any other systems that require the same configuration.

Files saved locally can be stored in the SPC's/SMC's CompactFlash or on an installed PCMCIA memory card on the SPC/SMC. Files that are saved to a remote network node can be transmitted using either FTP, or TFTP.

Saving the Configuration on the Chassis

These instructions assume that you are at the root prompt for the Exec mode:

```
[local]host_name#
```

To save your current configuration, enter the following command:

```
save configuration url [-redundant] [-noconfirm] [showsecrets] [verbose]
```

Keyword/Variable	Description
url	Specifies the path and name to which the configuration file is to be stored. *url* may refer to a local or a remote file. *url* must be entered using one of the following formats: • **{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **file:/{ /flash | /pcmcia1 | /pcmcia2 }** *[/dir] /file_name* • **tftp://**{ *ipaddress*|*host_name*[*:port#*]} [*/directory*] */file_name* • **ftp://**[*username*[*:pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* • **sftp://**[*username*[:*pwd*] *@*] { *ipaddress*|*host_name*} [*:port#*] [*/directory*] */file_name* **/flash** corresponds to the CompactFlash on the SPC/SMC. **/pcmcia1** corresponds to PCMCIA slot 1. **/pcmcia2** corresponds to PCMCIA slot 2. *ipaddress* is the IP address of the network server. *host_name* is the network server's *hostname*. *port#* is the network server's logical port number. Defaults are: • tftp: 69 - data • ftp: 20 - data, 21 - control • sftp: 115 - data Note: *host_name* can only be used if the **networkconfig** parameter is configured for DHCP and the DHCP server returns a valid nameserv er.dx *username* is the username required to gain access to the server if necessary. *password* is the password for the specified username if required. */directory* specifies the directory where the file is located if one exists. */file_name* specifies the name of the configuration file to be saved. Note: Configuration files should be named with a .cfg extension.
-redundant	Optional: This keyword directs the system to save the CLI configuration file to the local device, defined by the url variable, and then automatically copy that same file to the like device on the Standby SPC/SMC, if available. Note: This keyword will only work for like local devices that are located on both the active and standby SPCs/SMCs. For example, if you save the file to the /pcmcia1 device on the active SPC/SMC, that same type of device (a PC-Card in Slot 1 of the standby SPC/SMC) must be available. Otherwise, a failure message is displayed. Note: If saving the file to an external network (non-local) device, the system disregards this keyword.

Keyword/Variable	Description
-noconfirm	Optional: Indicates that no confirmation is to be given prior to saving the configuration information to the specified filename (if one was specified) or to the currently active configuration file (if none was specified).
showsecrets	Optional: This keyword causes the CLI configuration file to be saved with all passwords in plain text, rather than their default encrypted format.
verbose	Optional: Specifies that every parameter that is being saved to the new configuration file should be displayed.

Important: The **`-redundant`** keyword is only applicable when saving a configuration file to local devices.This command does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active SPC/SMC, then you must synchronize the local file system on both SPCs/SMCs.

To save a configuration file called system.cfg to a directory that was previously created called cfgfiles on the SPC's/SMC's CompactFlash, enter the following command:

```
save configuration /flash/cfgfiles/system.cfg
```

To save a configuration file called simple_ip.cfg to a directory called host_name_configs using an FTP server with an IP address of 192.168.34.156 on which you have an account with a username of administrator and a password of secure, use the following command:

```
save configuration
ftp://administrator:secure@192.168.34.156/host_name_configs/
simple_ip.cfg
```

To save a configuration file called init_config.cfg to the root directory of a TFTP server with a hostname of config_server, enter the following command:

`save configuration` *`tftp://config_server/init_config.cfg`*

Appendix A
Sample NAT Configuration

The following is a sample NAT configuration.

```
configure
   license key "\
VER=1|C1M=SanDiskSDCFJ-4096|C1S=116904I0207E3107|DOI=1258470708|DOE=12\
HG=100000|FHE=Y|SIG=MC4CFQCf9f7bAibGKJWq69JaJMd5XowxVwIVALDFfUHAEUTokw"
   aaa default-domain subscriber radius
   aaa last-resort context subscriber radius
   gtpp single-source
   system hostname ABC123DEF456
   autoconfirm
   clock timezone asia-calcutta
   crash enable encrypted url abc123def456ghi789
   card 1
      mode active psc
      exit
   card 2
      mode active psc
      exit
   card 4
      mode active psc
      exit
   require session recovery
   require active-charging
```

```
context local
   interface SPIO1
      ip address 1.2.3.4 255.255.255.0
      exit
   server ftpd
      exit
   ssh key abc123def456ghi789abc123def456ghi789 len 777 type v2-dsa
   server sshd
      subsystem sftp
      exit
   server telnetd
      exit
   subscriber default
      exit
   administrator admin encrypted password abc123def456ghi789 ftp
   aaa group default
      exit
   gtpp group default
      exit
   ip route 0.0.0.0 0.0.0.0 2.3.4.5 SPIO1
   exit
port ethernet 24/1
   no shutdown
   bind interface SPIO1 local
   exit
ntp
   enable
   server 10.6.1.1
   exit
```

```
snmp engine-id local 123007e123275a8c123ff07ca49
active-charging service service_name
   nat allocation-failure send-icmp-dest-unreachable
   host-pool host1
      ip range 3.4.5.6 to 4.5.6.7
      exit
   host-pool host2
      ip range 5.6.7.8 to 6.7.8.9
      exit
   host-pool host3
      ip range 7.8.9.0 to 8.9.0.1
      exit
   ruledef ip_any
      ip any-match = TRUE
      exit
   ruledef rt_ftp
      tcp either-port = 21
      rule-application routing
      exit
   ruledef rt_ftp_data
      tcp either-port = 20
      rule-application routing
      exit
   ruledef rt_http
      tcp either-port = 80
      rule-application routing
      exit
   ruledef rt_rtp
      rtp any-match = TRUE
```

```
    rule-application routing
    exit
ruledef rt_rtsp
    tcp either-port = 554
    rule-application routing
    exit
access-ruledef fw_icmp
    icmp any-match = TRUE
    exit
access-ruledef fw_tcp
    tcp any-match = TRUE
    exit
access-ruledef fw_udp
    udp any-match = TRUE
    exit
edr-format nbr_format1
    attribute sn-correlation-id priority 1
    rule-variable ip subscriber-ip-address priority 2
    attribute sn-fa-correlation-id priority 3
    attribute radius-fa-nas-ip-address priority 4
    attribute radius-fa-nas-identifier priority 5
    attribute radius-user-name priority 6
    attribute radius-calling-station-id priority 7
    attribute sn-nat-ip priority 8
    attribute sn-nat-port-block-start priority 9
    attribute sn-nat-port-block-end priority 10
    attribute sn-nat-binding-timer priority 11
    attribute sn-nat-subscribers-per-ip-address priority 12
    attribute sn-nat-realm-name priority 13
```

```
            attribute sn-nat-gmt-offset priority 14
            attribute sn-nat-port-chunk-alloc-dealloc-flag priority 15
            attribute sn-nat-port-chunk-alloc-time-gmt priority 16
            attribute sn-nat-port-chunk-dealloc-time-gmt priority 17
            attribute sn-nat-last-activity-time-gmt priority 18
            exit
         udr-format udr_format
            attribute sn-start-time format MM/DD/YYYY-HH:MM:SS localtime
priority 1
            attribute sn-end-time format MM/DD/YYYY-HH:MM:SS localtime
priority 2
            attribute sn-correlation-id priority 4
            attribute sn-content-vol bytes uplink priority 6
            attribute sn-content-vol bytes downlink priority 7
            attribute sn-fa-correlation-id priority 8
            attribute radius-fa-nas-ip-address priority 9
            attribute radius-fa-nas-identifier priority 10
            attribute radius-user-name priority 11
            attribute sn-content-vol pkts uplink priority 12
            attribute sn-content-vol pkts downlink priority 13
            attribute sn-group-id priority 14
            attribute sn-content-id priority 15
            exit
         charging-action ca_nothing
            content-id 20
            exit
         bandwidth-policy bw1
            exit
         bandwidth-policy bw2
            exit
```

```
      rulebase base_1
         tcp packets-out-of-order timeout 30000
         billing-records udr udr-format udr_format
         action priority 1 ruledef ip_any charging-action ca_nothing
         route priority 1 ruledef rt_ftp analyzer ftp-control
         route priority 10 ruledef rt_ftp_data analyzer ftp-data
         route priority 20 ruledef rt_rtsp analyzer rtsp
         route priority 30 ruledef rt_rtp analyzer rtp
         route priority 40 ruledef rt_http analyzer http
         rtp dynamic-flow-detection
         bandwidth default-policy bw1
         fw-and-nat default-policy base_1
         exit
      rulebase base_2
         action priority 1 ruledef ip_any charging-action ca_nothing
         route priority 1 ruledef rt_ftp analyzer ftp-control
         route priority 10 ruledef rt_ftp_data analyzer ftp-data
         route priority 40 ruledef rt_http analyzer http
         bandwidth default-policy bw2
         fw-and-nat default-policy base_2
         exit
      rulebase default
         exit
      fw-and-nat policy base_1
         access-rule priority 1 access-ruledef fw_tcp permit nat-realm
nat_pool1
         access-rule priority 2 access-ruledef fw_udp permit nat-realm
nat_pool2
         firewall tcp-first-packet-non-syn reset
         nat policy nat-required default-nat-realm nat_pool3
```

```
         firewall policy firewall-required
         nat binding-record edr-format nbr_format1 port-chunk-allocation
port-chunk-release
         exit
      fw-and-nat policy base_2
         access-rule priority 10 access-ruledef fw_tcp permit nat-realm
nat_pool2
         access-rule priority 20 access-ruledef fw_udp permit nat-realm
nat_pool1
         access-rule priority 25 access-ruledef fw_icmp permit bypass-nat
         nat policy nat-required default-nat-realm nat_pool3
         firewall policy firewall-required
         exit
      nat tcp-2msl-timeout 120
      exit
   context pdsn
      interface pdsn
         ip address 9.0.1.2 255.255.255.0
         exit
      ssh key abc123def456ghi789abc123def456ghi789 len 461
      server sshd
         subsystem sftp
         exit
      subscriber default
         ip access-group css-1 in
         ip access-group css-1 out
         ip context-name isp
         mobile-ip send accounting-correlation-info
         active-charging rulebase base_1
         exit
```

```
      aaa group default

         exit

      gtpp group default

         exit

      pdsn-service pdsn

         spi remote-address 9.0.1.2 spi-number 256 encrypted secret
abc123def456ghi789 timestamp-tolerance 0

         spi remote-address 9.0.1.2 spi-number 256 encrypted secret
abc123def456ghi789 timestamp-tolerance 0

         spi remote-address 9.0.1.2 spi-number 9999 encrypted secret
abc123def456ghi789 timestamp-tolerance 0

         authentication pap 1 chap 2 allow-noauth

         bind address 0.1.2.3

         exit

      edr-module active-charging-service

         file name NBR_nat current-prefix Record rotation time 45 headers
edr-format-name

         exit

      exit

   context isp

      ip access-list css

         redirect css service service_name

         ip any any

         exit

      ip pool nat_pool1 range 20.20.20.0 20.20.20.99 napt-users-per-ip-
address 10 max-chunks-per-user 5 port-chunk-size 128 send-nat-binding-
update

      ip pool nat_pool2 range 30.30.30.0 30.30.30.99 nat-one-to-one on-
demand nat-binding-timer 60 send-nat-binding-update

      ip pool nat_pool3 40.40.40.0 255.255.255.0 napt-users-per-ip-
address 5 max-chunks-per-user 5 port-chunk-size 64 send-nat-binding-
update

      ip pool pool1 11.22.33.44 255.255.0.0 public 0
```

```
   interface isp
      ip address 22.33.44.55 255.255.255.0
      exit
   subscriber default
      exit
   aaa group default
      exit
   gtpp group default
      exit
   ip route 0.0.0.0 0.0.0.0 33.44.55.66 isp
   exit
context radius
   interface radius
      ip address 44.55.66.77 255.255.255.0
      exit
   subscriber default
      exit
   subscriber name test7-sub
      ip access-group css in
      ip access-group css out
      ip context-name isp
      active-charging rulebase base_1
      exit
   subscriber name test9-sub
      ip access-group css in
      ip access-group css out
      ip context-name isp1
      active-charging rulebase base_2
      exit
```

```
      domain test7.com default subscriber test7-sub
      domain test9.com default subscriber test9-sub
      radius change-authorize-nas-ip 44.55.66.77 encrypted key
abc123def456ghi789 port 4000
      aaa group default
         radius attribute nas-ip-address address 44.55.66.77
         radius dictionary custom9
         radius server 55.66.77.88 encrypted key abc123def456ghi port
1645
         radius accounting server 55.66.77.88 encrypted key abc12 port
1646
         exit
      gtpp group default
         exit
      diameter endpoint abc.star.com
         origin host abc.star.com address 44.55.66.77
         peer minid realm star.com address 55.66.77.88
         exit
      exit
   bulkstats collection
   bulkstats mode
      sample-interval 1
      transfer-interval 15
      file 1
         remotefile format /localdisk/ABC.bulkstat
         receiver 66.77.88.99 primary mechanism ftp login root encrypted
password 34dab256a700e2a8
         exit
      exit
   port ethernet 17/1
```

```
    no shutdown
    bind interface pdsn pdsn
    exit
port ethernet 17/2
    no shutdown
    bind interface isp isp
    exit
port ethernet 17/3
    no shutdown
    bind interface radius radius
    exit
port ethernet 17/4
    no shutdown
    exit
port ethernet 17/5
    no shutdown
    exit
end
```