NAT Configuration

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

Important In release 8.x, NAT for CDMA and early UMTS releases used rulebase-based configurations, whereas in later UMTS releases NAT used policy-based configurations. In 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 following topics are covered in this chapter:

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 the required feature 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 your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command save configuration. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and *Command Line Interface Reference*.

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, on page 3 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 allocation of multiple IP addresses for a NAT realm as described in the Configuring IP address allocation for NAT realm, on page 9 section.

Step 7 Configure NAT IP pools/NAT IP pool groups as described in the Configuring NAT IP Pools/NAT IP Pool Groups, on page 4 section.

Step 8 Configure Firewall-and-NAT policies as described in the Configuring Firewall-and-NAT Policies section.

Step 9 Configure Firewall-and-NAT actions as described in the Configuring Firewall-and-NAT Action section.

Step 10 Configure action on NAT IP address/port allocation failure as described in the Configuring Action on NAT IP Address/Port Allocation Failure section.

Step 11 Configure action on packets during NAT IP allocation as described in the Configuring Action on Packets During NAT IP Allocation section.

Step 12 Configure NAT TCP-2msl-timeout setting as described in the Configuring NAT TCP-2msl-timeout Setting section.

Step 13 Configure action on TCP idle timeout as described in the Configuring Action on TCP Idle Timeout section.

Step 14 Configure Private IP NPU Flow Timeout setting as described in the Configuring Private IP NPU Flow Timeout Setting section.

Step 15 Configure NAT reassembly timer as described in the Configuring NAT Reassembly Timer section.

Step 16 Configure Flow Recovery as described in the Configuring Flow Recovery section.

Step 17 Configure NAT Flow Checkpointing as described in the Configuring NAT Flow Checkpointing section.

Step 18 Enable NAT support for APN/subscribers as described in the Enabling NAT for APN/Subscribers section.

Step 19 (Optional) Configure the default Firewall-and-NAT policy as described in the Configuring the Default Firewall-and-NAT Policy section.

Step 20 Configure NAT ALGs as described in the Configuring NAT Application Level Gateways/Dynamic Pinholes section.

Step 21 (Optional) Configure the PCP service as described in the Configuring PCP Service section.

Step 22 Configure the EDR Format for NAT Packet Drops as described in the Configuring EDR Format for NAT Packet Drops, on page 16 section.

Step 23 Configure EDR format as described in the Configuring EDR Format section.

Step 24 Configure UDR format as described in the Configuring UDR Format section.

Step 25 Configure NBR formats as described in the Configuring NAT Binding Record Format section.

Step 26 Configure NAT realm bulk statistics collection as described in the Configuring Bulkstats Collection section.

Step 27 Configure NAT thresholds as described in the Configuring NAT Thresholds section.

Step 28 Configure a secondary IP pool, which is not overwritten by the RADIUS supplied list, as described in the Configuring NAT Backout 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 service
  active-charging service acs_service_name [ -noconfirm ]
  end
```

Important After you configure this command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

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 acs_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 acs_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 acs_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 IMSI pool.

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 IP Pools/NAT IP Pool Groups, on page 4
- Configuring Many-to-One NAT IP Pools/NAT IP Pool Groups, on page 6

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 ] [ include-nw-bcast ] [ on-demand ] [
send-icmp-dest-destunreachable ] [ send-nat-binding-update ] [
skip-nat-subscriber-ip-check ] [ 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.
- The **skip-nat-subscriber-ip-check** keyword is added to skip private IP address check for non-NAT pools. This can be configured only for non-NAT pools during call-setup if NAT is enabled for the subscriber.

  If NAT is disabled, this value is not considered. Default: Disabled (subscriber IP check is done).
- 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.
- Network broadcast is supported for NAT pools and ordinary pools using the **include-nw-bcast** option.

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 ] [ min-port-chunk-per-user chunks ] [
port-chunk-threshold threshold ] [ send-icmp-dest-destunreachable ] [
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 acs_service_name
      fw-and-nat policy fw_nat_policy_name [ -noconfirm ]
         nat policy [ ipv4-and-ipv6 | ipv4-only | ipv6-only ] [
default-nat-realm nat_realm_name [ fw-and-nat-action action_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.
- In 12.1 and earlier releases: The nat policy nat-required command enables NAT44 for all subscribers using the policy. This keyword is supported in release 12.2 for backward compatibility.
- In 12.2 and later releases: The **nat policy [ipv4-and-ipv6 | ipv4-only | ipv6-only]** command enables NAT processing for IPv4/IPv6 or both using the policy.
- Duplicate ruledef names or priorities are not allowed in the same rulebase.
- A maximum of twenty NAT IP pools/NAT IP pool groups can be configured in a Firewall-and-NAT 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 Firewall-and-NAT Action

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

```
configure
  active-charging service acs_service_name
    fw-and-nat action fw_nat_action_name [ -noconfirm ]
      flow check-point [ data-usage data_usage [ and | or ] | time-duration
duration [ and | or ] ]
      end
```

Configuring Access Ruledefs

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

```
configure
  active-charging service acs_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 | server-ipv6-network-prefix
 operator ipv6_prefix/prefix_length } } }
      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.
- The **server-ipv6-network-prefix** *operator ipv6_prefix/prefix_length* rule is matched against the Destination IPv6 address of the incoming packet to decide whether NAT64 has to be applied or not.
- 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 Server IP Address

To configure an access rule definition to analyze user traffic based on server IP address, use the following configuration:

```
configure
   active-charging service acs_service_name
      access-ruledef access_ruledef_name
         [ no ] ip server-ip-address { operator { ipv4/ipv6_address |
ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }
         end
```

Notes:

The **ip server-ip-address** command is added in access rule definitions to avoid configuring multiple rule options as part of Firewall rules. If any address or host-pool range is specified as the server IP address, this address in the uplink direction will be treated as the destination address, and in downlink direction will be treated as the source address.

Configuring IP address allocation for NAT realm

To enable or disable the allocation of multiple NAT IP addresses for the same many-to-one (N:1) NAT realm for a subscriber, use the following configuration:

```
configure
   active-charging service service_name
      fw-and-nat policy policy_name
         nat max-chunk-per-realm { multiple-ip | single-ip }
         { default | no } nat max-chunk-per-realm
         end
```

Notes:

- The **nat max-chunk-per-realm multiple-ip** command enables the feature, that is, allows allocation of more than one IP address for a NAT realm if required.

- The **nat max-chunk-per-realm single-ip** command disables the feature, allows allocation of only one IP address for NAT realm. If the port chunks get exhausted, packets will be dropped. This is the default behavior.
- The **no nat max-chunk-per-realm** command disables the allocation of multiple IP addresses for the same NAT realm for a subscriber. This command when configured, allows only one IP address to be allocated for a NAT realm.
- This enhancement is applicable only for N:1 NAT realms and not for 1:1 NAT realms.

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 acs_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 acs_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 Forcible NAT IP Release

To forcibly clear NAT IP addresses from SessMgr to VPNMgr, use the following configuration:

```
clear nat-ip { ip_address | pool pool_name } context context_name [ -noconfirm ]
```

Configuring NAT TCP-2msl-timeout Setting

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

```
configure
  active-charging service acs_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 acs_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 acs_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.
- Downlink traffic will be dropped after flow is deleted after the configurable timeout period.

Configuring NAT Reassembly Timer

To configure the maximum duration for which IP packet fragments can be retained, use the following configuration:

```
configure
  active-charging service acs_service_name
    [ default ] nat ip downlink reassembly-timeout timeout
    end
```

Configuring Flow Recovery

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

```
configure
  active-charging service acs_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.

NAT64 flow binding recovery is not supported in Release 21.2.

Configuring NAT Flow Checkpointing

To enable/disable checkpointing of basic NAT, SIP and H323 ALG recovery, enable/disable ICSR recovery for basic NAT and SIP flows, and configure the maximum basic flows that can be checkpointed, use the following configuration:

```
configure
   active-charging service acs_service_name
      fw-and-nat policy fw_nat_policy_name
        [ default | no ] nat check-point-info { basic [ icsr-also | limit-flows
 limit ] h323-alg | sip-alg [ icsr-also ] }
        end
```

Configuring Flow-mapping Timeout

To configure flow-mapping timeout, use the following configuration in either of the two modes: Active Charging Service Configuration mode and ACS Charging Action Configuration mode.

In ACS Configuration mode:

```
configure
   active-charging service acs_service_name
      idle-timeout flow-mapping { tcp | udp } timeout
      end
```

In ACS Charging Action Configuration mode:

```
configure
   active-charging service acs_service_name
      charging-action charging_action_name
         flow idle-timeout flow-mapping flow_timeout
         end
```

Notes:

- The value configured in charging action takes precedence to the value configured in the ACS service mode. In global mode (ACS Configuration mode), the default values are different for TCP and UDP.
- Even if the flow-mapping timeout is configured inside a charging action, and if the flow that matched the charging action was not a TCP or a UDP flow, then the Mapping timer will not be triggered for the flow.

Configuring NAT Unsolicited Packets

To configure NAT unsolicited packets, use the following configuration:

```
configure
   active-charging service acs_service_name
      nat unsolicited-pkts { icmp-host-unreachable { max-rate packets_num } |
server-list { max-limit servers_num } }
      end
```

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

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 Policies, on page 7 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 Policies, on page 7 section.
- To specify that the default Firewall-and-NAT policy configured in the rulebase be used for subscribers who use this APN, 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 acs_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, on page 14
- Configuring Routing Ruledefs in Rulebase, on page 14
- Enabling NAT ALG, on page 15
- Configuring SIP ALG Parameters, on page 15

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 |
h323 | 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 NAT44/NAT64 ALGs, use the following configuration:

```
configure
  active-charging service ecs_service_name
    firewall nat-alg { all | ftp | h323 | pptp | rtsp | sip } [ ipv4-and-ipv6
 | ipv4-only | ipv6-only ]
     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.
- The **ipv4-and-ipv6** | **ipv4-only** | **ipv6-only** keyword enables or disables NAT44/NAT64 ALG or both.
- NAT64 supports only the FTP, PPTP, RTSP and TFTP ALGs.

Configuring SIP ALG Parameters

To enable SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests, use the following configuration:

```
configure
  active-charging service acs_name
     sip advanced out-of-dialog-request retain-tag
     end
```

Configuring PCP Service

This section describes how to configure PCP service for the PCP Server feature.

Important The PCP Server feature is customer specific. Contact your Cisco account representative for more information.

The following topics are covered in this section:

- Configuring PCP Service and PCP Policy Control, on page 16
- Enable/Disable PCP Service in Rulebase, on page 16

Configuring PCP Service and PCP Policy Control

To create and configure a PCP Service, and configure PCP Policy Control related parameters, use the following configuration:

```
configure
  active-charging service acs_service_name
    pcp-service pcp_svc_name [ -noconfirm ]
      policy-control
        request-opcode [ announce | map [ filter | prefer-failure ] | peer
 ]
         response-opcode { map | peer } [ error { long life-time life_time
| short life-time life_time } | success life-time life_time ]
      server ipv4-address ipv4_address [ port port_num ]
      end
```

Notes:

- A maximum of 5 PCP services can be configured in the ACS.

Enable/Disable PCP Service in Rulebase

To configure the PCP service to associate subscribers with in the rulebase, use the following configuration:

```
configure
  active-charging service ecs_service_name
    rulebase rulebase_name
      pcp service pcp_service_name
      end
```

Configuring EDR Format for NAT Packet Drops

To configure EDR format in which records for dropped NAT packets will be saved, use the following configuration:

```
configure
  active-charging service ecs_service_name
    fw-and-nat policy policy_name
      nat pkts-drop { edr-format edr_format_name | timeout timeout_value
      { default | no } nat pkts-drop { edr-format | timeout }
      end
```

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-no-port-packet-dropped priority priority
      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
```

Notes:

- The **sn-nat-no-port-packet-dropped** attribute reports the number of packets dropped because of no NAT IP/port.

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
      attribute subscriber-ipv4-address priority priority
      attribute subscriber-ipv6-address priority priority
      rule-variable ip subscriber-ip-address priority priority
      rule-variable bearer 3gpp charging-id priority priority
      rule-variable bearer 3gpp sgsn-address priority priority
      rule-variable bearer ggsn-address priority priority
      rule-variable bearer 3gpp imsi 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

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-pkt-drop 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-kt-drop high_threshold clear low_threshold
   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
```

Configuring NAT Backout

NAT backout is a licensed feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

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. Busyout feature is now supported for both NAT and ordinary pools.

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-torulebase 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 subscribers 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.

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: 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** *nat_pool_name*
Summary statistics of all NAT IP pools in a NAT IP pool group	**show active-charging nat statistics nat-realm** *nat_pool_name* **summary**
Statistics for a specific ACS/Session Manager instance	**show active-charging nat statistics instance** *instance_number*
Statistics of NAT unsolicited packets for a specific ACS/Session Manager instance	**show active-charging nat statistics unsolicited-pkts-server-list instance** *instance_number*
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*
Stateful Firewall statistics	**show active-charging firewall statistics verbose**

Statistics/Information	Action to perform
PCP service statistics	**show active-charging pcp-service all** **show active-charging pcp-service name** *pcp_service_name* **show active-charging pcp-service statistics**
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** }
SIP ALG Advanced session statistics.	**show active-charging analyzer statistics name sip**
Information for all the active flow-mappings based on the applied filters.	**show active-charging flow-mappings all**
Information for the number of NATed and Bypass NATed packets.	**show active-charging subsystem all**
Information for all current subscribers who have either active or dormant sessions. Checks IP address associated with subscriber. Also displays all the IP addresses that are in use in a NAT realm.	**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-ip** *nat_ip_address*
Information of all subscribers using more than one IP address per NAT realm at any given time.	**show subscribers nat required multiple-ips-per-nat-realm**
Information for subscribers to find out how long (in seconds) the subscriber has been using NAT-IP.	**show active-charging sessions nat required usage-time** [< | > | **greater-than** | **less-than**] *value*

Statistics/Information	Action to perform
NAT realm IP address pool information.	**show ip pool nat-realm wide**
Call drop reason due to invalid NAT configuration.	**show session disconnect-reasons**