

NAT Support

- Feature Summary and Revision History, on page 1
- Feature Description, on page 1
- Configuring NAT in CUPS, on page 3
- Monitoring and Troubleshooting, on page 5

Feature Summary and Revision History

Revision History

Note Revision history details are not provided for features introduced before release 21.24.

Revision Details	Release
With this release clarification for firewall NAT port release behaviour change in CUPS UP is provided.	21.27.x
First introduced.	Pre 21.24

Feature Description

CUPS supports Network Address Translation (NAT) which allows you to configure network addresses. The system can be configured to automatically forward data packets encapsulating the source IP or Source port address of the UE with NAT IP address and NAT port.

The supported NAT combinations include:

- NAT44 On Demand Many to One
- NAT44 On Demand One to One
- NAT64 On Demand Many to One

- NAT 64 On Demand One to One
- NAT44 Not On Demand Many to One
- NAT44 Not On Demand One to One
- NAT64 Not On Demand Many to One
- NAT64 Not On Demand One to One

For supplemental information about NAT, see StarOS *NAT Administration Guide*.

NOTE: Not all features and/or functionality that are mentioned in StarOS *NAT Administration Guide* are applicable in the CUPS architecture.

Behavior of NAT Port Release

The ICMP NAT port usage is higher in CUPS solutions than legacy due to the following reasons:

- In Legacy, on receiving the ICMP response, the NAT ports are released so that they can be used for the next message. In CUPS, the NAT ports are released only after the 100th ICMP message is received.
- In Legacy, if no ICMP response is received for the requests, then 20 NAT ports are allocated continuously and released starting from the first one. In CUPS, the deletion happens only after the 100th ICMP packet.

Limitations

NAT support has the following limitations:

- Only NAT44 with many-to-one and on-demand mode is supported.
- All NAT pools are configured at respective User Plane on destination context.
- Charging action with CLI action deny in fw-and-nat policy and for flow-any-error charging action in active-charging-service is not supported.
- Access-rules which are configured with "dynamic-only" and "static-and-dynamic" – rules from external servers are not supported.
- Multiple IP support from same realm is not supported with this feature.
- Next hop forwarding in NAT pool is not supported.
- Port range in NAT pool is not supported.
- Skip private IP check CLI is not supported.
- RADIUS and Gy returned Fw-and-nat policy-based applying NAT policy is not supported.
- Bearer specific filters are not supported in access-ruledefs.
- Access-rules do not support trigger open-port port range config in fw-and-nat policy.
- NAT port recovery (fw-and-nat action) is not supported after SR/ICSR.
- NAT Re-assembly Timeout CLI is not supported in active-charging service. The generic context level CLI on UP must be used instead.
- NAT fragmentation re-assembly failure is not supported due to open bugs in basic CUPS re-assembly.

- NAT flow-mapping timer is not supported
- For N:M redundancy, the NAT IP pools to be configured from RCM done as part of interface config for each UP host and the pool name needs to be unique across all the active User Planes. This makes it mandatory to use NAT Groups for all the pools so that the same NAT realm referred in fw-and-nat policy can be applicable for all the User Planes.
- In case of N:M redundancy, the total number of NAT IP pools collectively configured on all UPs via RCM must be as per the maximum limit (2000) of IP pools. The configuration in standby User Plane fails if the cumulative total of all active UPs exceeds the maximum value.

Configuring NAT in CUPS

The relevant configuration of NAT is done at CP and pushed to UP. Only pool-related configuration is present on User Plane.

For information on NAT-related CLI commands, refer to the *StarOS NAT Administration Guide > NAT Configuration* chapter.

NOTE: Not all CLI commands and configurations mentioned in the *StarOS NAT Administration Guide > NAT Configuration* chapter are applicable in CUPS architecture.

Sample Configurations

Control Plane

The following is a sample configuration required at Control Plane for enabling NAT in CUPS. This configuration is pushed to User Plane during User Plane registration through PFD mechanism.

```
configure
active-charging service ACS
     access-ruledef all
       ip any-match = TRUE
     #exit
     access-ruledef udp
       udp any-match = TRUE
     #exit
     access-ruledef tcp
       tcp any-match = TRUE
     #exit
     access-ruledef icmp
       icmp any-match = TRUE
     #exit
     fw-and-nat policy NatPolicy1
        access-rule priority 1 access-ruledef tcp permit nat-realm NAT44_GRP1
        access-rule priority 2 access-ruledef icmp permit nat-realm NAT44_GRP1
        #access-rule priority 2 access-ruledef r2 permit bypass-nat
        nat policy ipv4-only default-nat-realm NAT44_PUBLIC5
        nat binding-record edr-format NBR port-chunk-allocation port-chunk-release
     #exit

     fw-and-nat policy NatPolicy2
        access-rule priority 1 access-ruledef all permit nat-realm NAT44_PUBLIC1
        #access-rule priority 2 access-ruledef r2 permit bypass-nat
        nat policy ipv4-only
```

```
        nat binding-record edr-format NBR port-chunk-allocation port-chunk-release
     #exit

     rulebase cisco
     fw-and-nat default-policy NatPolicy1
     flow end-condition normal-end-signaling session-end timeout edr NBR
     #exit
#exit
end
```

User Plane

The following pool-related configuration is required at User Plane in ISP context.

```
configure
   context ISP1-UP
      ip pool NAT44_PUBLIC1 209.165.200.225 255.255.255.224 napt-users-per-ip-address 2
on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC2 209.165.200.226 255.255.255.224 napt-users-per-ip-address 2
on-demand port-chunk-size 16 max-chunks-per-user 4 group-name NAT44_GRP1
      ip pool NAT44_PUBLIC3 209.165.200.227 255.255.255.224 napt-users-per-ip-address 2
on-demand port-chunk-size 8 max-chunks-per-user 1 group-name NAT44_GRP2
      ip pool NAT44_PUBLIC4 209.165.200.228 255.255.255.224 napt-users-per-ip-address 4
on-demand port-chunk-size 32256 max-chunks-per-user 4 group-name NAT44_GRP2
      ip pool NAT44_PUBLIC5 209.165.200.229 255.255.255.224 napt-users-per-ip-address 8064
 on-demand port-chunk-size 8 max-chunks-per-user 2
      end
```

Sample NAT Pool Related Configuration for Different NAT Pool Types

```
1-1 on-demand:
----------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_1_1 209.165.200.230 255.255.255.224 nat-one-to-one on-demand
nat-binding-timer 60
end

N-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_N_1 209.165.200.231 255.255.255.224 napt-users-per-ip-address 2
max-chunks-per-user 2 port-chunk-size 8
end

1-1 Not-on-demand:
------------------------
config
context ISP1-UP
ip pool NAT44_ipv4_NOD_1_1 209.165.200.232 255.255.255.224 nat-one-to-one
end
```

Note Add the Control Plane configuration and map one or more access rule definitions to any required NAT Pool or Group configured in the User Plane.

Monitoring and Troubleshooting

Gathering NAT Statistics

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

The first column lists the statistics to gather and the second column lists the command to use.

Statistics/Information	Show Command
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 user-plane-only full all**
Information on NAT subsystem statistics.	**show user-plane-service statistics all**
All NAT-related statistics.	**show user-plane-service statistics nat all**
All NAT Realm-related statistics.	**show user-plane-service statistics nat nat-realm all**
Statistics of all NAT IP pools in a NAT IP pool group.	**show user-plane-service statistics nat nat-realm** *pool_name*
Information on NAT bind records generated.	**show user-plane-service edr-format statistics all**
Verifying association of fw-and-nat policy in APN on UP.	**show user-plane-service pdn-instance name** *name*
Verifying cofiguration of fw-an-nat policy on UP.	**show user-plane-service fw-and-nat policy all**
Information on NAT bind records generated for port chunk allocation and release.	**show user-plane-service rulebase name** *name*
Information on access ruledef.	**show user-plane-service ruledef all**
Verifying association of fw-and-nat policy in rulebase on UP.	**show user-plane-service rulebase name** *name*

Clear Commands

The following clear CLI commands are available in support of this feature:

- **clear user-plane-service statistics nat nat-realm all**
- **clear user-plane-service statistics nat all**

SNMP Traps for NAT Parameter Thresholds

The following SNMP traps for NAT parameter thresholds are supported.

SNMP Traps	Description
ThreshNATPortChunks	Generated when NAT port chunk usage reaches configured threshold limit
ThreshClearNATPortChunks	Generated when NAT port chunk usage reaches configured clear threshold limit.
ThreshNATPktDrop	Generated when NAT packet drop reaches configured threshold limit.
ThreshClearNATPktDrop	Generated when NAT packet drop reaches configured clear threshold limit.
ThreshIPPoolUsed	Generated when the number of IPs used in the IP Pool reaches configured threshold limit.
ThreshClearIPPoolUsed	Generated when the number of IPs used in the IP Pool reaches configured clear threshold limit.
ThreshIPPoolFree	Generated when IP pool is free and threshold limit reached.
ThreshClearIPPoolFree	Generated when IP pool is used, and clear threshold limit reached.
ThreshIPPoolAvail	Generated when IP pool is available for next flow and configured threshold reached.
ThreshClearIPPoolAvail	Generated when IP pool is used, and configured threshold is reached.

NOTE: The respective CLIs must be configured in the User Plane to enable these traps.

Bulk Statistics

Context Schema

Table 1: Context Schema

Variable Name	Data Type	Counter Type	Description
nat-total-flows	Int64	Counter	Total number of NAT44 and NAT64 flows
nat44-total-flows	Int64	Counter	Total number of NAT44 flows
nat64-total-flows	Int64	Counter	Total number of NAT64 flows
bypass-nat-total-flows	Int64	Counter	Total number of NAT44 and NAT64 Bypass NAT flows
bypass-nat-ipv4-total-flows	Int64	Counter	Total number of NAT44 Bypass NAT flows
bypass-nat-ipv6-total-flows	Int64	Counter	Total number of NAT64 Bypass NAT flows
nat-current-flows	Int64	Gauge	Current number of NAT44 and NAT64 flows

Variable Name	Data Type	Counter Type	Description
nat44-current-flows	Int64	Gauge	Current number of NAT44 flows
nat64-current-flows	Int64	Gauge	Current number of NAT64 flows
bypass-nat-current-flows	Int64	Gauge	Current number of NAT44 and NAT64 Bypass NAT flows
bypass-nat-ipv4-current-flows	Int64	Gauge	Current number of NAT44 Bypass NAT flows
bypass-nat-ipv6-current-flows	Int64	Gauge	Current number of NAT64 Bypass NAT flows
sfw-total-rxpackets	Int64	Counter	Total number of packets received by the Service
sfw-total-rxbytes	Int64	Counter	Total number of bytes received by the Service
sfw-total-txpackets	Int64	Counter	Total number of packets transferred by the Service
sfw-total-txbytes	Int64	Counter	Total number of bytes transferred by the Service
sfw-total-injectedpkts	Int64	Counter	Total number of packets injected by the Service
sfw-total-injectedbytes	Int64	Counter	Total number of bytes injected by the Service
sfw-dnlnk-droppkts	Int64	Counter	Total number of downlink packets dropped by the Service
sfw-dnlnk-dropbytes	Int64	Counter	Total number of downlink bytes dropped by the Service
sfw-uplnk-droppkts	Int64	Counter	Total number of uplink packets dropped by the Service
sfw-uplnk-dropbytes	Int64	Counter	Total number of uplink bytes dropped by the Service

Note Schema is supported in User Plane for CUPS.

ECS Schema

Table 2: ECS Schema

Variable Name	Data Type	Counter Type	Description
nat-current-ipv4-pdn-subscribers	Int32	Gauge	Current number of NAT IPv4 PDN Subscribers
nat-current-ipv6-pdn-subscribers	Int32	Gauge	Current number of NAT IPv6 PDN Subscribers
nat-current-ipv4v6-pdn-subscribers	Int32	Gauge	Current number of NAT IPv4v6 PDN Subscribers
nat-total-ipv4-pdn-subscribers	Int64	Counter	Total number of NAT IPv4 PDN Subscribers

Variable Name	Data Type	Counter Type	Description
nat-total-ipv6-pdn-subscribers	Int64	Counter	Total number of NAT IPv6 PDN Subscribers
nat-total-ipv4v6-pdn-subscribers	Int64	Counter	Total number of NAT IPv4v6 PDN Subscribers
nat-current-ipv4-pdn-subscribers-with-nat-ip	Int32	Gauge	Current number of NAT IPv4 PDN Subscribers with NAT IP
nat-current-ipv6-pdn-subscribers-with-nat-ip	Int32	Gauge	Current number of NAT IPv6 PDN Subscribers with NAT IP
nat-current-ipv4v6-pdn-subscribers-with-nat-ip	Int32	Gauge	Current number of NAT IPv4v6 PDN Subscribers with NAT IP
nat-total-ipv4-pdn-subscribers-with-nat-ip	Int64	Counter	Total number of NAT IPv4 PDN Subscribers with NAT IP
nat-total-ipv6-pdn-subscribers-with-nat-ip	Int64	Counter	Total number of NAT IPv6 PDN Subscribers with NAT IP
nat-total-ipv4v6-pdn-subscribers-with-nat-ip	Int64	Counter	Total number of NAT IPv4v6 PDN Subscribers with NAT IP
nat-total-unsolicited-dwnlnk-pkts	Int64	Counter	Total number of unslolicited downlink packets received
nat-total-icmp-hu-sent-for-dwnlnk-pkts	Int64	Counter	Total number of ICMP host unreachable sent for downlink packets

Note Schema is supported in User Plane for CUPS.

NAT-realm Schema

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

Table 3: NAT-realm Schema

Variable Name	Data Type	Counter Type	Description
Vpnname	String	Info	Context name.
Realmname	String	Info	Realm name.
nat-rlm-bind-updates	Int64	Counter	Total interim AAA NBU sent.
nat-rlm-bytes-txferred	Int64	Counter	Total number of NAT44 and NAT64 bytes transferred by realm (uplink + downlink).

Variable Name	Data Type	Counter Type	Description
nat-rlm-bytes-nat44-tx	Int64	Counter	Total number of NAT44 bytes transferred by realm.
nat-rlm-bytes-nat64-tx	Int64	Counter	Total number of NAT64 bytes transferred by realm.
nat-rlm-ip-flows	Int64	Counter	Total number of NAT44 and NAT64 flows used by the realm.
nat-rlm-nat44-flows	Int64	Counter	Total number of NAT44 flows processed by realm.
nat-rlm-nat64-flows	Int64	Counter	Total number of NAT64 flows processed by realm.
nat-rlm-ip-denied	Int32	Counter	Total number of NAT44 and NAT64 flows denied NAT IP address.
nat-rlm-ip-denied-nat44	Int64	Counter	Total number of NAT44 flows denied IP.
nat-rlm-ip-denied-nat64	Int64	Counter	Total number of NAT64 flows denied IP.
nat-rlm-port-denied	Int32	Counter	Total number of NAT44 and NAT64 flows denied ports.
nat-rlm-port-denied-nat44	Int64	Counter	Total number of NAT44 flows denied ports.
nat-rlm-port-denied-nat64	Int64	Counter	Total number of NAT64 flows denied ports.
nat-rlm-memory-denied	Int64	Counter	Total number of NAT44 and NAT64 flows denied memory.
nat-rlm-memory-denied-nat44	Int64	Counter	Total number of NAT44 flows denied memory.
nat-rlm-memory-denied-nat64	Int64	Counter	Total number of NAT64 flows denied memory.
nat-rlm-ttl-ips	Int32	Gauge	Total number of NAT public IP addresses, per context per NAT realm. Is a static value.
nat-rlm-ips-in-use	Int32	Gauge	Total number of NAT IP addresses currently in use, per context per NAT realm.
nat-rlm-current-users	Int32	Gauge	Total number of subscribers currently using the NAT realm.
nat-rlm-ttl-port-chunks	Int32	Gauge	Total number port-chunks, per context per NAT realm. Is a static value.
nat-rlm-chunks-in-use	Int32	Gauge	Total number of port-chunks currently in use, per context per NAT realm.

Variable Name	Data Type	Counter Type	Description
nat-rlm-port-chunk-size	Int32	Gauge	Size of the port chunk in the NAT realm.
nat-rlm-port-chunk-average-usage-tcp	Int32	Gauge	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	Int32	Gauge	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	Int32	Gauge	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.
nat-rlm-max-port-chunk-subs	Int64	Counter	Total number of subscribers who used maximum number of port chunks.
nat-rlm-max-port-chunk-used	Int32	Counter	Maximum port chunks used.
nat-rlm-max-cur-port-chunk-subs	Int64	Gauge	Current number of subscribers using maximum number of port chunks.
nat-rlm-max-cur-port-chunk-used	Int32	Gauge	Maximum port chunks used by active subscribers.

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

Sample EDR

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,sn-server-port,
sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,sn-nat-realm-name,
sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,sn-nat-port-chunk-alloc-time-gmt,
sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
02/18/2020 12:11:11:630,02/18/2020
12:11:11:632,1,209.165.200.225,209.165.201.1,0,0,,,,209.165.200.230,1024,,2,,,,,,0,0
02/18/2020 12:11:08:672,02/18/2020
12:11:09:671,6,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.230,1034,,2,,,,,,0,0
02/18/2020 12:11:14:499,02/18/2020
12:11:14:499,17,209.165.200.225,209.165.201.1,1001,3000,,,,209.165.200.240,1025,,8064,,,,,,0,0
```

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.

Sample NBR

```
#sn-start-time,sn-end-time,ip-protocol,ip-subscriber-ip-address,ip-server-ip-address,sn-subscriber-port,
sn-server-port,sn-nat-ip,sn-nat-port-block-start,sn-nat-port-block-end,sn-subscriber-nat-flow-ip,sn-subscriber-nat-flow-port,
sn-nat-realm-name,sn-nat-subscribers-per-ip-address,sn-nat-binding-timer,sn-nat-gmt-offset,sn-nat-port-chunk-alloc-dealloc-flag,
sn-nat-port-chunk-alloc-time-gmt,sn-nat-port-chunk-dealloc-time-gmt,sn-nat-no-port-packet-dropped,sn-closure-reason
,,,209.165.200.225,,,,209.165.201.1,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,1,02/18/2020
06:41:08,,,
,,,209.165.200.225,,,,209.165.201.2,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,1,02/18/2020
06:41:14,,,
,,,209.165.200.225,,,,209.165.201.3,1024,1039,,,NAT44_PUBLIC2,2,60,+0530,0,02/18/2020
06:41:08,02/18/2020 06:42:12,,
,,,209.165.200.225,,,,209.165.201.14,1024,1031,,,NAT44_PUBLIC5,8064,60,+0530,0,02/18/2020
06:41:14,02/18/2020 06:44:24,,
```

Packet Drop EDR

Sample Packet Drop EDR

```
#sn-nat-no-port-packet-dropped,sn-start-time,sn-end-time,sn-subscriber-imsi
2,03/13/2020 08:28:24,03/13/2020 08:28:54,123456789012345
```