NAT in Combination with ESM

In This Chapter

This section provides information about Network Address Translation (NAT) in combination with Enhanced Subscriber Management (ESM).

Topics in this section include:

Applicability

This example is applicable to 7750 SR-7 and SR-12 and was tested on release 8.0R6. It is required to have at least one Multi-Service ISA (MS-ISA) card equipped in an IOM3-XP. Chassis mode B or higher is required.

The Alcatel-Lucent 7750 SR-7 and SR-12 supports Source Network Address and Port Translation (SNAPT aka N:1) and Source Network Address Translation (SNAT aka 1:1) to provide continuity of legacy IPv4 services during the migration to native IPv6.

The 7750 SR-7SR-/12 can operate in two different modes known as:

- Large Scale NAT
- Layer 2-Aware NAT = NAT in combination with Enhanced Subscriber Management (ESM)

This configuration note is restricted to the Layer 2-Aware NAT.

Overview

Layer 2-Aware NAT performs source address and port translation as commonly deployed for shared Internet access. The 7750 SR with NAT is used to provide consumer broadband or business Internet customers access to IPv4 internet resources with a shared pool of IPv4 addresses, such as may occur with the IPv4 exhaustion.

TCP/UDP connections use ports for multiplexing, with 65536 ports available for every IP address. Whenever many hosts are trying to share a single public IP address there is a chance of port collision where two different hosts may use the same source port for a connection. The resultant collision is avoided in SNAPT devices by translating the source port and tracking this in a stateful manner. All SNAPT devices are stateful in nature and must monitor connection establishment and traffic to maintain translation mappings.

In most circumstances, SNAPT requires the inside host to establish a connection to the public Internet host or server before a mapping and translation will occur. With the initial outbound IP packet, the SNAPT knows the inside IP, inside port, remote IP, remote port and protocol. L2-Aware NAT will also take into account the subscriber identification string. With this information the SNAPT device can select an IP and port combination (referred to as outside IP and outside port) from its pool of addresses and create a unique mapping for this flow of data.

Any traffic returned from the server will use the outside IP and outside port in the destination IP/port fields matching the unique NAT mapping. The mapping then provides the inside IP and inside port for translation.

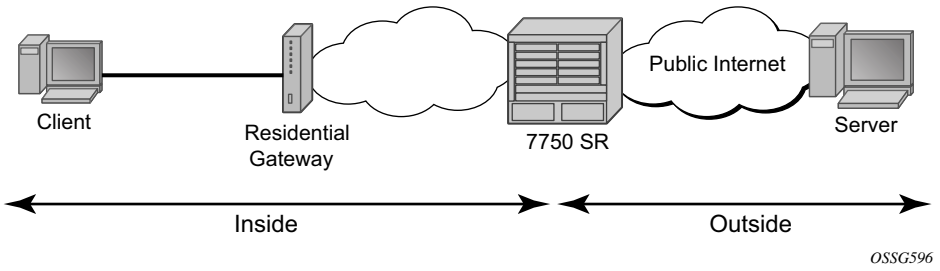

Figure 240: Network Address Translation Overview

L2-Aware NAT supports the following ESM hosts:

- IP over Ethernet (IPoE)
- PPP over Ethernet (PPPoE)
- L2TP Network Server (LNS)

L2-Aware NAT is not supported on static- or arp-hosts.

L2-Aware NAT makes the differentiation between two interfaces. The inside interface, towards the residential gateway and the outside interface, towards the public network, as seen in Figure 1. The outside IP needs to be a public IP address.

NAT is supported in the base and VPRN routing contexts. NAT can originate in a VPRN routing context and exit through a base or VPRN routing context. L2-Aware NAT allows reusing IP address towards residential customers.

A typical flow-session will be recorded using the following fields:

- Subscriber identification string
- Inside IP Outside IP
- Inside port Outside port
- Inside VRFid Outside VRFid

This configuration note will focus on the NAT configuration and functionality. For completeness other configuration will be given, but not explained in detail. Two IPoE clients will be set up with the same IP address inside one VPRN. One PPPoE client will be set up inside a different VPRN as the public VPRN.

Server Functionality Behind NAT

Applications which operate as servers (such as HTTP, SMTP, etc) or Peer-to-Peer (P2P) applications can have difficulty when operating behind an SNAPT because traffic from the Internet can reach the NAT without a mapping in place.

Different methods can be employed to overcome this, including:

- Port forwarding
- STUN support
- Application Layer Gateways (ALG)

The 7750 SR supports all three methods following the best-practice RFC for TCP (RFC 5382, *NAT Behavioral Requirements for TCP*) and UDP (RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*). Port Forwarding setup, supported in this release through SNMP only, allows servers which operate on well-known ports <1024 (such as HTTP and SMTP) to request the appropriate outside port for permanent allocation.

STUN is facilitated by the support of Endpoint-Independent Filtering and Endpoint-Independent Mapping (RFC 4787) in the NAT device, allowing STUN-capable applications to detect the NAT and allow inbound P2P connections for that specific application. Many new voice over IP clients and instant messaging chat applications are STUN capable.

Application Layer Gateways (ALG) allow the NAT to monitor the application running over TCP or UDP and make appropriate changes in the NAT translations accordingly. The 7750 SR has an FTP ALG enabled following the recommendation of RFC 5382, *NAT Behavioral Requirements for TCP.*

Configuration

Hardware Configuration

L2-aware NAT is implemented today in the 7750-SR7 and SR12 using the MS-ISA MDA hosted in an IOM3-XP. The MS-ISA card is a multi-purpose MDA which can be used for multiple applications like LNS, video (FCC/RET/VQE), AA (application assurance/DPI), tunneling (GRE/IPSEC), etc. This approach allows re-deploying the same hardware in a different software configuration for other purposes once the IPv4 to IPv6 transition is completed.

For L2-Aware NAT, configure the MS-ISA as an ISA-BB (BroadBand) MDA which allows running L2-aware NAT, LNS and carrier grade-NAT (CG-NAT) simultaneously on the configured MDA. CG-NAT or large scale NAT is set-up independently of ESM subscriber hosts.

```
configure card 1
        card-type iom3-xp
...
        mda 2
            mda-type isa-bb
        exit
exit all
```

An ISA NAT-group needs to be created. A NAT-group can host up to 6 MDA(s) for load-sharing or providing resilience when an MS-ISA fails. Multiple NAT groups can be created to achieve hardware separation between e.g. residential and business customers.

```
configure isa nat-group 1
            description "L2 Aware NAT Group"
            active-mda-limit 1
            mda 1/2
            no shutdown
exit all
```

The active-mda-limit controls the number of MS-ISA MDA’s which can be used as active members of the NAT group. Each active card will be assigned sessions/flows and will process traffic. The backup cards are cold standby; they are used only in case of a failure of one (or more) of the active cards. Load balancing over the active cards is done using the source ip address in the upstream, and the outside destination IP in the downstream direction. Public IP address pools are assigned to a specific card, thus resulting in both upstream and downstream traffic flowing through the same MS-ISA card.

All MS-ISA cards (active + backup) need to be configured under the ISA NAT group.

Service Configuration

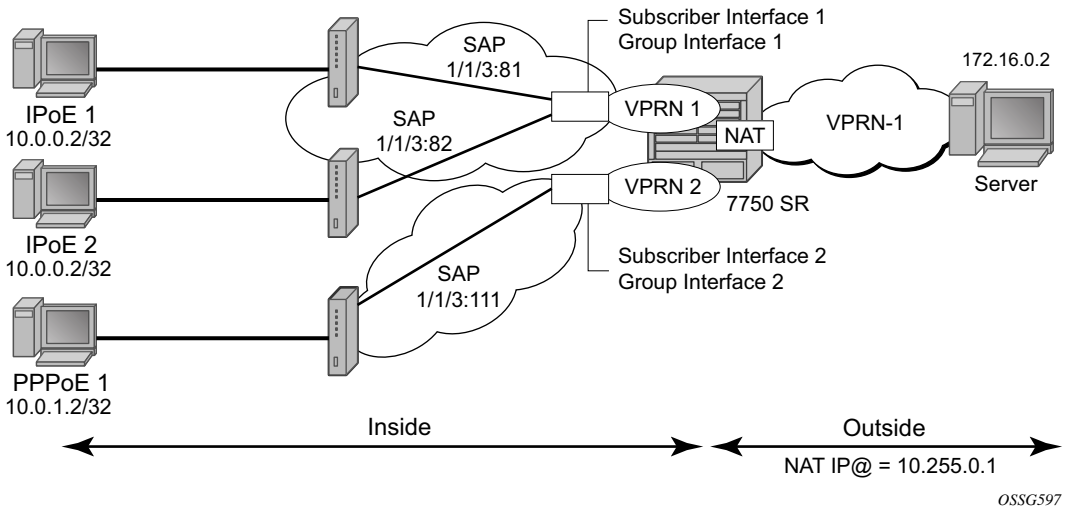

Figure 241: Setup Topology

The setup used for this note is depicted in Figure 241 and Figure 242. There are three clients:

1. IPoE_1 going to SAP 1/1/3:81 in VPRN 1 (NAT to VPRN 1)
2. IPoE_2 going to SAP 1/1/3:82 in VPRN 1 (NAT to VPRN 1)
3. PPPoE_1 going to SAP 1/1/3:111 in VPRN 2 (NAT to VPRN 1)

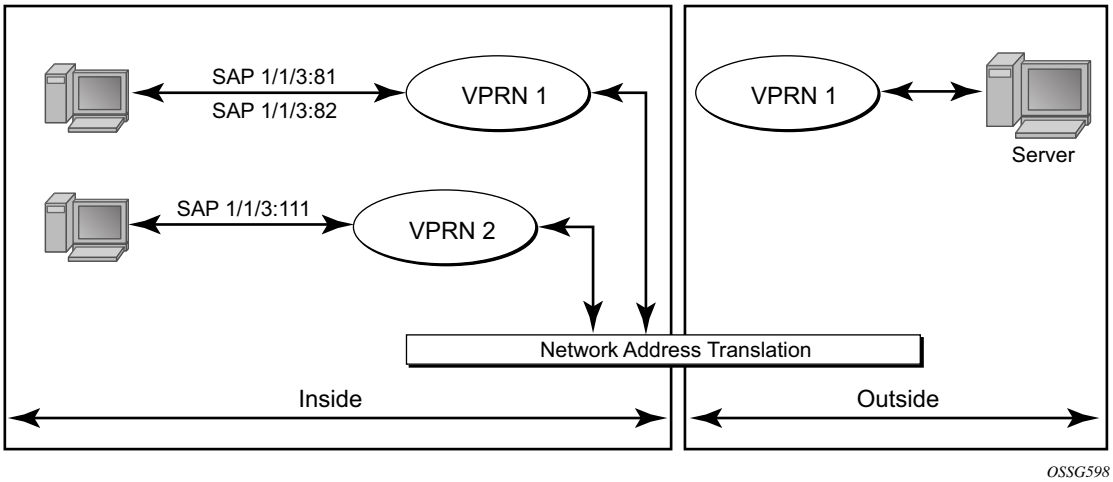

Figure 242: Simplified Routing Topology

Initial Service and Enhanced Subscriber Management Configuration

The initial service and ESM configuration is given below for VPRN 1. This VPRN contains subscriber interface sub-int-1 with group interface group-int-ipoe-cpe, in routed central office (CO). There are two SAPs under the group interface, 1/1/3:81 and 1/1/3:82. The subscribers are IP over Ethernet subscribers. Upon receiving a DHCP request the subscriber will first be authenticated using radius authentication. A DHCP emulation server is configured under the group interface.

```
configure service vprn 1
            route-distinguisher 64500:1
            vrf-target target:64500:1
            interface "int-PE-1-servers"  create
                address 172.16.0.1/30
                sap 1/1/4:110 create
                exit
            exit
            subscriber-interface "sub-int-1" create
                address 10.0.0.254/24
                dhcp
                    gi-address 10.0.0.254 src-ip-addr
                exit
                group-interface "group-int-ipoe-cpe" create
                    arp-populate
                    dhcp
                        proxy-server
                            emulated-server 10.0.0.254
                            lease-time hrs 1
                            no shutdown
                        exit
                        trusted
                        lease-populate 10
                        gi-address 10.0.0.254 src-ip-addr
                        no shutdown
                    exit
                    authentication-policy "radiusAuth"
                    sap 1/1/3:81 create
                        sub-sla-mgmt
                            sub-ident-policy "sub-ident-all"
                            multi-sub-sap 10
                            no shutdown
                        exit
                    exit
                    sap 1/1/3:82 create
                        sub-sla-mgmt
                            sub-ident-policy "sub-ident-all"
                            multi-sub-sap 10
                            no shutdown
                        exit
                    exit
                exit
            exit
            no shutdown
exit all
```

All parameters are returned by the radius server, including all ESM strings as well as IP address, mask, default gateway and session timeout.

The RADIUS user configuration is given below. The users's mac-address is used to authenticate the IPoE of PPPoE sessions.

```
00:0c:29:9d:10:2d     Cleartext-Password := "admin"
                      Alc-Subsc-ID-Str = "ipoe_sub_00:0c:29:9d:10:2d",
                      Alc-SLA-Prof-Str = "sla-profile-nat",
                      Alc-Subsc-Prof-Str = "sub-profile-nat",
                      Framed-IP-Address = 10.0.0.2,
                      Framed-IP-Netmask = 255.255.255.0,
                      Alc-Default-Router = 10.0.0.254,
                      Session-Timeout = 3600
00:0c:29:34:cc:74     Cleartext-Password := "admin"
                      Alc-Subsc-ID-Str = "ipoe_sub_00:0c:29:34:cc:74",
                      Alc-SLA-Prof-Str = "sla-profile-nat",
                      Alc-Subsc-Prof-Str = "sub-profile-nat",
                      Framed-IP-Address = 10.0.0.2,
                      Framed-IP-Netmask = 255.255.255.0,
                      Alc-Default-Router = 10.0.0.254,
                      Session-Timeout = 3600

00:0c:29:1d:44:34 Auth-Type := Local, User-Password == "admin"
                    Alc-Subsc-ID-Str = "pppoe_sub_%{User-Name}",
                    Alc-SLA-Prof-Str = "sla-profile-nat",
                    Alc-Subsc-Prof-Str = "sub-profile-nat",
                    Framed-IP-Address = 10.0.1.2,
                    Framed-IP-Netmask = 255.255.255.0,
                    Alc-Default-Router = 10.0.1.254
```

The subscriber management policies are as follows.

```
configure subscriber-mgmt
        authentication-policy "radiusPPP" create
            password "B7O7GD4VdMqISRo2VWbZqn14IyuUXUDb" hash2
            radius-authentication-server
                router "management"
                server 1 address 172.16.40.108 secret "j3VRf4lH1u1XI/RJOb4LkE" hash2
            exit
        exit
        authentication-policy "radiusAuth" create
            password "2VL2PrE6sZJRQPY6ipW7ifwOFyEsqb/k" hash2
            radius-authentication-server
                router "management"
                server 1 address 172.16.15.58 secret "j3VRf4lH1u./Gx3thvq7Tk" hash2
            exit
        exit
        sla-profile "sla-profile-nat" create
        exit
        sub-profile "sub-profile-nat" create
        exit
        sub-ident-policy "sub-ident-all" create
            sub-profile-map
                use-direct-map-as-default
            exit
```

```
            sla-profile-map
                use-direct-map-as-default
            exit
        exit
exit all
```

The initial service and ESM configuration is given below for VPRN 2. This VPRN contains subscriber interface sub-int-2 with group interface group-int-pppoe-cpe, in routed CO. There is one SAP under the group interface, 1/1/3:111. The subscribers are PPP over Ethernet, using radius as authentication method.

```
configure service vprn 2
            route-distinguisher 64500:2
            vrf-target target:64500:2
            subscriber-interface "sub-int-2" create
                address 10.0.1.254/24
                group-interface "group-int-pppoe-cpe" create
                    authentication-policy "radiusPPP"
                    sap 1/1/3:111 create
                        sub-sla-mgmt
                            sub-ident-policy "sub-ident-all"
                            multi-sub-sap 10
                            no shutdown
                        exit
                    exit
                    pppoe
                        session-limit 10
                        sap-session-limit 10
                        no shutdown
                    exit
                exit
            exit
            no shutdown
exit all
```

Successful Creation of a NAT Subscriber

When a subscriber-host is created and a NAT-policy is defined, its inside IP address should fall within the L2-Aware range (see next section). If this is not the case the subscriber-host creation will fail. As mentioned before NAT is not supported on static-hosts. The subscriber-host creation is shown in Figure 243. If the subscriber-host does not get an inside or outside IP address, it would not be able to communicate with any servers on the outside.

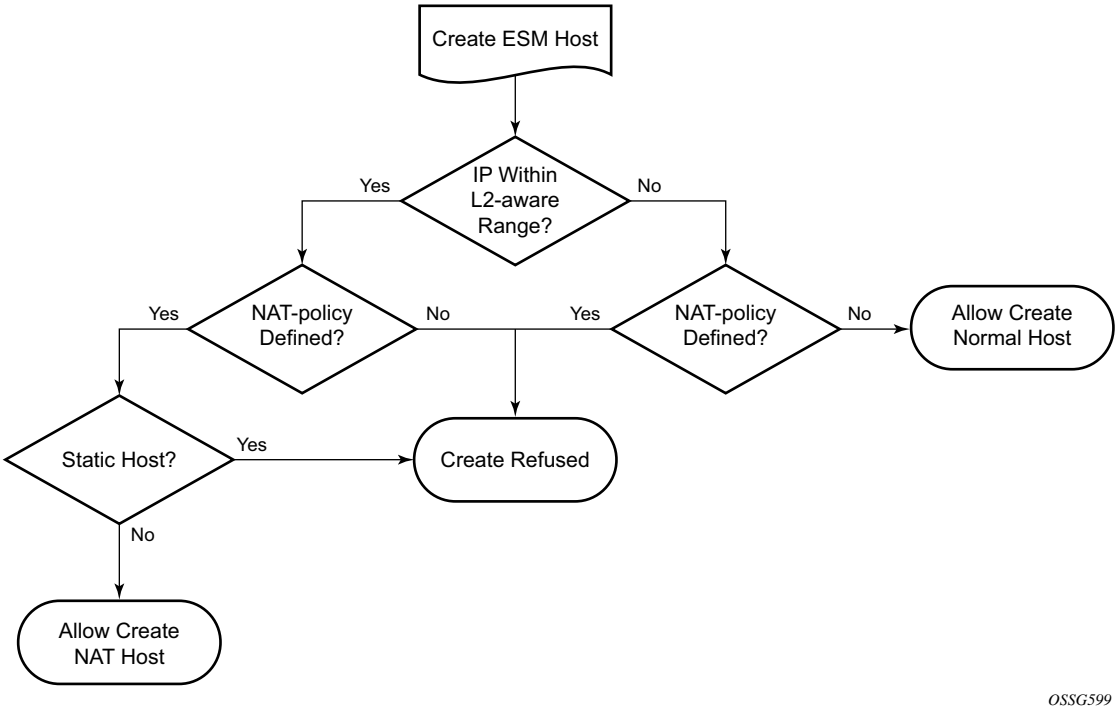

Figure 243: Subscriber-Host Creation Flow

NAT Inside Configuration

The residential gateway subnets which are to be NATed need to be configured under the nat inside L2-Aware context. For this configuration note all subscribers belonging to VPRN 1 will be allocated an address in subnet 10.0.0.0/24. All subscribers belonging to VPRN 2 will be allocated an IP address in subsnet 10.0.1.0/24. Hosts in these services within these subnets will be subject to L2-Aware NAT if they have the correct nat-policy in their subscriber profile.

The actual address configured here will act as the local IP address of the system. Hosts connected to the inside service will be able to ARP for this address. To verify connectivity, a host can also ping the address. This address is typically used as next hop of the default route of a L2-Aware host.

```
configure service vprn 1
            nat
                inside
                    l2-aware
                        address 10.0.0.254/24
                    exit
                exit
            exit
exit all

configure service vprn 2
            nat
                inside
                    l2-aware
                        address 10.0.1.254/24
                    exit
                exit
            exit
exit all
```

NAT Outside Configuration

The NAT outside pool needs to be configured on the VPRN facing the outside world, e.g. the public internet. The NAT outside pool controls the NAT type, which in this case is l2-aware, and the NAT group to send the traffic to.

These addresses will be used to as source addresses for all packets in the upstream direction (toward the public internet) and as destination address for all packets in the downstream direction.

```
configure service vprn 1
            nat
                outside
                    pool "nat-outside-pool-1" nat-group 1 type l2-aware create
                        port-reservation blocks 128
                        address-range 10.255.0.1 10.255.0.10 create
                        exit
                        no shutdown
                    exit
                exit
            exit
exit all
```

The port-reservation command specifies the number of port-blocks (blocks of consecutive usable port numbers) per IP address. In this configuration, each public IP address is subdivided into 128 port blocks which can be used for NAT, that results in 504 public ports per block.

Binding Inside NAT, Outside NAT and ESM Host

In order to bind the inside part of the NAT with the outside part a nat-policy needs to be created, under the service nat level. The outside nat-pool, which is associated with the VPRN instance in this example, and outside IP addresses, is configured under the nat-policy.

```
configure service nat
       nat-policy "nat-l2aware-vprn1" create
            pool "nat-outside-pool-1" router 1
       exit
```

This nat-policy is then associated to the different subscribers by means of the subscriber profile. The ESM host traffic will be diverted to the NAT device.

```
configure subscriber-mgmt sub-profile "sub-profile-nat"
            nat-policy "nat-l2aware-vprn1"
exit all
```

The nat-policy also controls the following parameters:

Filtering — Two filtering modes are available, endpoint-independent (default configuration) and address-and-port dependent filtering. The filtering behavior will control which upstream packets are transmitted (based on the existing sessions). If endpoint-independent filtering is configured, any outside host/port can use mappings the NAT has created to send traffic to the inside. If address-and-port-dependent filtering is selected, only packets from the same destination and port which created the mapping will be processed.

Port limits — A number of ports can be reserved for prioritized sessions. A session is considered as a priority-session depending on its forwarding class. High and low watermarks can be configured to trigger alarms based on the port usage.

The reserved resources mean that if the resources get down to the level that there is only the reserved amount left, this leftover can only be used by priority sessions, not taking into account the amount of priority sessions already set up at that point.

Example: By default each host is assigned 504 outside ports. 100 of these ports can be reserved for the EF and H1 forwarding classes. As soon as any given host reaches 404 utilized outside ports, the remaining 100 will only be used for EF or H1 sessions.

Priority sessions — The forwarding classes for which the sessions should be prioritized in terms of port or session assignment can be configured here. Multiple forwarding classes can be configured.

Session limits — A maximum number of sessions can be configured for each subscriber associated with this nat-policy. A number of sessions can be reserved for prioritized sessions. Sessions are prioritized based on forwarding class. High and low watermarks can be configured to trigger alarms based on the session usage.

Notes:

- The reserved sessions and reserved ports are not the same. A user can have many applications contacting the same destination. Many different source ports will be used, therefore many different outside ports. A user can have one application contacting many different destinations. The same source port, but many different destination IP addresses will be used. Only one outside port is consumed, but many sessions exist.
- It is possible to configure a reserved ports session-limit on the nat-group as well. In case both per Layer 2 aware host and per nat-group limits are configured the most restrictive will be enforced.

Timeouts — Several timeouts can be configured.

→ icmp-query: Timeout applied to an ICMP query session.

→ tcp-established: The idle timeout applied to a TCP session in the established state.

→ tcp-syn: The timeout applied to a TCP session in the SYN state.

→ tcp-time-wait: Time-wait assassination is enabled by default to quickly remove TCP mappings in the time-wait state.

→ tcp-transitory: The idle timeout applied to a TCP session in a transitory state. TCP transition between SYN and Open.

→ udp: All udp streams (with exceptions of udp-initial and udp-dns).

→ udp-initial: UDP mapping timeout applied to new sessions. Applicable when only 1 UDP packet is sent.

→ udp-dns: Only traffic to destination UDP port 53

Advanced Topics

RADIUS Accounting

RADIUS accounting is extended with a new attribute, nat-port-range, reporting the NAT port range in use by the subscriber. In order to configure RADIUS accounting, first the RADIUS accounting policy must be created.

```
configure subscriber-mgmt radius-accounting-policy "nat-accounting" create
            update-interval 5
            include-radius-attribute
                mac-address
                nat-port-range
                subscriber-id
            exit
            radius-accounting-server
                router "management"
                server 1 address 172.16.15.58 secret "j3VRf4lH1u./Gx3thvq7Tk" hash2
            exit
exit all
```

The configuration specifies which attributes to include in the radius accounting messages towards the configured server. The update interval is specified in minutes. Every 5 minutes an update will be sent to the radius accounting server.

Then this RADIUS accounting policy must be attached to the subscriber profile.

```
configure subscriber-mgmt sub-profile "sub-profile-nat"
            nat-policy "nat-l2aware-vprn1"
            radius-accounting-policy "nat-accounting"
```

Hardware Resource Monitoring

It is possible to define watermarks to monitor the actual usage of sessions and/or ports. For each watermark, a high and a low value have to be set (as a percentage). Once the high value is reached, a notification will be sent. As soon as the usage drops below the low watermark, another notification (trap) will be sent.

Watermarks can be defined on nat-group, pool and policy level.

- Nat-group — Watermarks can be configured to monitor the total number of sessions on an MDA

```
configure isa nat-group 1
            session-limits
                watermarks high 90 low 80
            exit
exit all
```

- Pool — Watermarks can be configured to monitor the total number of blocks in use in a pool

```
configure service vprn 1 nat outside pool "nat-outside-pool-1"
                        watermarks high 90 low 80
exit all
```

- Policy — In the policy it is possible to define watermarks on session and port usage. The usage per subscriber will be monitored.

```
configure service nat nat-policy "nat-l2aware-vprn1"
                port-limits
                    watermarks high 90 low 80
                exit
                session-limits
                    watermarks high 90 low 80
                exit
exit all
```

Outside IP Address Range Management

From an operational point of view it may be required to unprovision an outside IP address range. To that end, the **drain** has been introduced. If configured, no new sessions will be set up using this address-range. Existing mappings will cease to exist only when the session ends (tcp fin, fin ack, ack) or other timeout mechanism.

```
configure service vprn 1
            nat
                outside
                    pool "nat-outside-pool-1" nat-group 1 type l2-aware create
                        port-reservation blocks 128
                        address-range 10.255.0.1 10.255.0.10 create
                            drain
                        exit
                        no shutdown
                    exit
                exit
            exit
exit all
```

When all sessions have drained the address-range can be unprovisioned.

Quality of Service

NAT is fully transparent in terms of quality of service. The quality of service is determined on ingress into the service router. A forwarding class is assigned to each packet and is retained throughout the whole router.

For L2-aware NAT a virtual port exists on the carrier IOM, nat-in-l2. This port is modelled as a network port with per FC queues both on ingress and egress. On network-ingress per destination queues are implemented, making sure head of line blocking cannot happen.

Operation

The MS-ISA card should be in operational up state.

```
A:PE-1# show mda
===============================================================================
MDA Summary
===============================================================================
Slot  Mda   Provisioned           Equipped              Admin     Operational
            Mda-type              Mda-type              State     State
-------------------------------------------------------------------------------
1     1     m20-1gb-xp-sfp        m20-1gb-xp-sfp        up        up
      2     isa-bb                isa-ms                up        up
===============================================================================
A:PE-1#
```

The NAT group should be configured, with at least one pool of outside IP addresses associated with it.

```
A:PE-1# show isa nat-group 1
===============================================================================
ISA NAT Group 1
===============================================================================
L2 Aware NAT Group

Admin state       : inService           Operational state : inService
Active MDA limit  : 1                   Reserved sessions : 0
High Watermark (%): (Not Specified)     Low Watermark (%) : (Not Specified)
Last Mgmt Change  : 01/18/2011 13:27:40
===============================================================================
===============================================================================
ISA NAT Group 1 members
===============================================================================
Group Member     State          Mda  Addresses  Blocks     Se-% Hi Se-Prio
-------------------------------------------------------------------------------
1     1          active         1/2  1          3          < 1  N  0
-------------------------------------------------------------------------------
No. of members: 1
===============================================================================
```

The following table describes the **show isa nat-group** output fields.

Field	Description
Group	This is the group-id
Member	All members will be listed with associated parameters
State	The operational state of each member
MDA	The MDA position of the member
Addresses	The number of outside ip addresses assigned to the member
Blocks	The number of allocated port-blocks
Se-%	The actual session usage in percentage
Hi	High watermark reached (Y/N)
Se-Prio	The configured number of priority sessions

```
A:PE-1# show isa nat-group 1 associations
===============================================================================
ISA NAT Group 1 pool associations
===============================================================================
Pool                                    Router
-------------------------------------------------------------------------------
nat-outside-pool-1                      vprn1
-------------------------------------------------------------------------------
No. of pools: 1
===============================================================================
```

The subscriber-hosts should be created correctly.

```
A:PE-1# show service id 1 subscriber-hosts
============================================================
Subscriber Host table
============================================================
Sap                    Subscriber
  IP Address
    MAC Address          PPPoE-SID Origin       Fwding State
------------------------------------------------------------
1/1/3:81               ipoe_sub_00:0c:29:9d:10:2d
  10.0.0.2
    00:0c:29:9d:10:2d    N/A       DHCP         Fwding
1/1/3:82               ipoe_sub_00:0c:29:34:cc:74
  10.0.0.2
    00:0c:29:34:cc:74    N/A       DHCP         Fwding
------------------------------------------------------------
Number of subscriber hosts : 2
============================================================
```

```
A:PE-1# show service id 2 subscriber-hosts
===============================================================
Subscriber Host table
===============================================================
Sap                    Subscriber
  IP Address
    MAC Address          PPPoE-SID Origin       Fwding State
---------------------------------------------------------------
1/1/3:111              pppoe_sub_00:0c:29:1d:44:34
  10.0.1.2
    00:0c:29:1d:44:34    1         IPCP         Fwding
---------------------------------------------------------------
Number of subscriber hosts : 1
===============================================================
```

The associated L2-Aware NAT subscriber-hosts are visible from CLI. The associated group, member and ports can be viewed using this command.

```
A:PE-1# show service nat l2-aware-subscribers
===============================================================================
Layer-2-Aware NAT subscribers
===============================================================================
Subscriber                       Policy                         Group/Member
  Outside IP                              Router                 Ports
-------------------------------------------------------------------------------
ipoe_sub_00:0c:29:34:cc:74       nat-l2aware-vprn1              1/1
  10.255.0.1                              1                      1024-1527
ipoe_sub_00:0c:29:9d:10:2d       nat-l2aware-vprn1              1/1
  10.255.0.1                              1                      1528-2031
pppoe_sub_00:0c:29:1d:44:34      nat-l2aware-vprn1              1/1
  10.255.0.1                              1                      2032-2535
-------------------------------------------------------------------------------
No. of subscribers: 3
===============================================================================


A:PE-1# show service active-subscribers
===============================================================================
Active Subscribers
===============================================================================
-------------------------------------------------------------------------------
Subscriber ipoe_sub_00:0c:29:34:cc:74 (sub-profile-nat)
-------------------------------------------------------------------------------
NAT Policy: nat-l2aware-vprn1
Outside IP: 10.255.0.1 (vprn1)
Ports     : 1024-1527
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
(1) SLA Profile Instance sap:1/1/3:82 - sla:sla-profile-nat
-------------------------------------------------------------------------------
IP Address
                MAC Address       PPPoE-SID Origin
-------------------------------------------------------
10.0.0.2
                00:0c:29:34:cc:74 N/A       DHCP
```

```
-------------------------------------------------------------------------------
Subscriber ipoe_sub_00:0c:29:9d:10:2d (sub-profile-nat)
-------------------------------------------------------------------------------
NAT Policy: nat-l2aware-vprn1
Outside IP: 10.255.0.1 (vprn1)
Ports     : 1528-2031
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
(1) SLA Profile Instance sap:1/1/3:81 - sla:sla-profile-nat
-------------------------------------------------------------------------------
IP Address
                MAC Address       PPPoE-SID Origin
-------------------------------------------------------
10.0.0.2
                00:0c:29:9d:10:2d N/A       DHCP

-------------------------------------------------------------------------------
Subscriber pppoe_sub_00:0c:29:1d:44:34 (sub-profile-nat)
-------------------------------------------------------------------------------
NAT Policy: nat-l2aware-vprn1
Outside IP: 10.255.0.1 (vprn1)
Ports     : 2032-2535
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
(1) SLA Profile Instance sap:1/1/3:111 - sla:sla-profile-nat
-------------------------------------------------------------------------------
IP Address
                MAC Address       PPPoE-SID Origin
-------------------------------------------------------
10.0.1.2
                00:0c:29:1d:44:34 1         IPCP

-------------------------------------------------------------------------------
Number of active subscribers : 3
===============================================================================
```

Traffic arriving on the 7750 SR from the outside should be routed to the correct MS-ISA card (=NAT device).

The route table of VPRN 1 indicates that all traffic towards publicly visible IP addresses are routed to the NAT device, group 1 member 1. In other words all packets coming from the outside towards the 10.255.0.1 to 10.255.0.10 IP addresses are sent to the NAT device.

```
A:PE-1# show router 1 route-table
===============================================================================
Route Table (Service: 1)
===============================================================================
Dest Prefix                                     Type    Proto    Age         Pref
       Next Hop[Interface Name]                                       Metric
-------------------------------------------------------------------------------
10.0.0.0/24                                     Local   Local    04d18h09m   0
       sub-int-1                                                      0
10.255.0.1/32                                   Remote  Static   04d23h15m   5
       NAT outside: group 1 member 1                                  1
10.255.0.2/31                                   Remote  Static   04d23h15m   5
       NAT outside: group 1 member 1                                  1
```

```
10.255.0.4/30                                  Remote  Static   04d23h15m   5
       NAT outside: group 1 member 1                                 1
10.255.0.8/31                                  Remote  Static   04d23h15m   5
       NAT outside: group 1 member 1                                 1
10.255.0.10/32                                 Remote  Static   04d23h15m   5
       NAT outside: group 1 member 1                                 1
172.16.0.0/30                                  Local   Local    04d22h44m   0
       int-PE-1-servers                                              0
-------------------------------------------------------------------------------
No. of Routes: 7
===============================================================================


A:PE-1# show router 2 route-table
===============================================================================
Route Table (Service: 2)
===============================================================================
Dest Prefix                                    Type    Proto    Age         Pref
       Next Hop[Interface Name]                                      Metric
-------------------------------------------------------------------------------
10.0.1.0/24                                    Local   Local    03d20h14m   0
       sub-int-2                                                     0
-------------------------------------------------------------------------------
No. of Routes: 1
===============================================================================
```

Individual sessions are viewed through a tools dump command.

```
*A:PE-1# tools dump nat sessions
===============================================================================
Matched 6 sessions on Slot #1 MDA #2
===============================================================================
Owner               : L2-aware Subscr pppoe_sub_00:0c:29:1d:44:34
Router              : 2
Flow Type           : TCP               Timeout (sec)       : 7408
Inside IP Addr      : 10.0.1.2          Inside Port         : 1065
Outside IP Addr     : 10.255.0.1        Outside Port        : 2037
Foreign IP Addr     : 172.16.0.2        Foreign Port        : 21
-------------------------------------------------------------------------------
Owner               : L2-aware Subscr pppoe_sub_00:0c:29:1d:44:34
Router              : 2
Flow Type           : ICMP              Timeout (sec)       : 59
Inside IP Addr      : 10.0.1.2          Inside Identifier   : 512
Outside IP Addr     : 10.255.0.1        Outside Identifier  : 2034
Foreign IP Addr     : 172.16.0.2
-------------------------------------------------------------------------------
Owner               : L2-aware Subscr ipoe_sub_00:0c:29:9d:10:2d
Router              : 3
Flow Type           : ICMP              Timeout (sec)       : 59
Inside IP Addr      : 10.0.0.2          Inside Identifier   : 1024
Outside IP Addr     : 10.255.0.1        Outside Identifier  : 1536
Foreign IP Addr     : 172.16.0.2
-------------------------------------------------------------------------------
Owner               : L2-aware Subscr ipoe_sub_00:0c:29:9d:10:2d
Router              : 3
Flow Type           : TCP               Timeout (sec)       : 7369
Inside IP Addr      : 10.0.0.2          Inside Port         : 1070
Outside IP Addr     : 10.255.0.1        Outside Port        : 1538
```

```
Foreign IP Addr     : 172.16.0.2        Foreign Port        : 21
-------------------------------------------------------------------------------
Owner               : L2-aware Subscr ipoe_sub_00:0c:29:34:cc:74
Router              : Base
Flow Type           : TCP               Timeout (sec)       : 7439
Inside IP Addr      : 10.0.0.2          Inside Port         : 1035
Outside IP Addr     : 10.255.0.1        Outside Port        : 1043
Foreign IP Addr     : 172.16.0.2        Foreign Port        : 80
-------------------------------------------------------------------------------
Owner               : L2-aware Subscr ipoe_sub_00:0c:29:34:cc:74
Router              : Base
Flow Type           : ICMP              Timeout (sec)       : 59
Inside IP Addr      : 10.0.0.2          Inside Identifier   : 512
Outside IP Addr     : 10.255.0.1        Outside Identifier  : 1034
Foreign IP Addr     : 172.16.0.2
-------------------------------------------------------------------------------
===============================================================================
```

The resources on the MS-ISA can also be viewed through a **tools dump** command.

```
A:PE-1# tools dump nat isa resources mda 1/2
Resource Usage for Slot #1 Mda #2:

                               | Total      | Allocated  | Free
 ------------------------------+------------+------------+------------
                         Flows |    4194304 |          0 |    4194304
                      Policies |        256 |          1 |        255
                   Port-ranges |     262144 |          3 |     262144
                         Ports |  201326592 |          0 |  201326592
                  IP-addresses |       1024 |          1 |       1024
             Large-scale hosts |     131072 |          0 |     131072
          L2-aware subscribers |      65536 |          3 |      65536
                L2-aware hosts |      65536 |          3 |      65536
                Delayed ICMP's |        200 |          0 |        200
              FTP ALG session  |      65536 |          0 |      65536
```

The alarm configuration can be verified for the NAT related traps.

```
A:PE-1# show log event-control "nat"
===============================================================================
Log Events
===============================================================================
Application
 ID#    Event Name                          P   g/s     Logged     Dropped
-------------------------------------------------------------------------------
   2001 tmnxNatPlL2AwBlockUsageHigh         WA  gen          1           0
   2002 tmnxNatIsaMemberSessionUsageHigh    WA  gen          0           0
   2003 tmnxNatPlLsnMemberBlockUsageHigh    WA  gen          0           0
   2004 tmnxNatLsnSubIcmpPortUsageHigh      WA  gen          0           0
   2005 tmnxNatLsnSubUdpPortUsageHigh       WA  gen          0           0
   2006 tmnxNatLsnSubTcpPortUsageHigh       WA  gen          0           0
   2007 tmnxNatL2AwSubIcmpPortUsageHigh     WA  gen          0           0
   2008 tmnxNatL2AwSubUdpPortUsageHigh      WA  gen          0           0
   2009 tmnxNatL2AwSubTcpPortUsageHigh      WA  gen          0           0
   2010 tmnxNatL2AwSubSessionUsageHigh      WA  gen          0           0
   2011 tmnxNatLsnSubSessionUsageHigh       WA  gen          0           0
```

```
   2012 tmnxNatPlBlockAllocationLsn      MI  sup          0           0
   2013 tmnxNatPlBlockAllocationL2Aw     MI  sup          0           9
   2014 tmnxNatResourceProblemDetected   MI  gen          0           0
   2015 tmnxNatResourceProblemCause      MI  gen          0           0
===============================================================================
```

RADIUS accounting information can be verified using the **debug router radius detail** command.

```
1 2011/01/19 18:35:22.25 CAT MINOR: DEBUG #2001 management RADIUS
"RADIUS: Accounting Request
  policy nat-accounting"

2 2011/01/19 18:35:22.25 CAT MINOR: DEBUG #2001 management RADIUS
"RADIUS: Transmit
  Accounting-Request(4) 172.16.15.58:1813 id 5  len 295
    STATUS TYPE [40] 4 Interim-Update(3)
    NAS IP ADDRESS [4] 4 172.16.15.96
    SESSION ID [44] 71 ipoe_sub_00:0c:29:9d:10:2d@1/1/3:81@sla-profile-nat_2011/
01/18 14:10:09
    SESSION TIME [46] 4 95113
    EVENT TIMESTAMP [55] 4 1295454922
    VSA [26] 172 Alcatel(6527)
      SUBSC ID STR [11] 26 ipoe_sub_00:0c:29:9d:10:2d
      SUBSC NAT PORT RANGE [121] 27 10.255.0.1 1528-2031 router 1
      CHADDR [27] 17 00:0c:29:9d:10:2d
      INPUT_INPROF_OCTETS_64 [19] 10 0x0001000000000000000
      INPUT_OUTPROF_OCTETS_64 [20] 10 0x0001000000000076e86e
      INPUT_INPROF_PACKETS_64 [23] 10 0x0001000000000000000
      INPUT_OUTPROF_PACKETS_64 [24] 10 0x0001000000000001733c
      OUTPUT_INPROF_OCTETS_64 [21] 10 0x0001000000000076ea5c
      OUTPUT_OUTPROF_OCTETS_64 [22] 10 0x0001000000000000000
      OUTPUT_INPROF_PACKETS_64 [25] 10 0x0001000000000001733d
      OUTPUT_OUTPROF_PACKETS_64 [26] 10 0x0001000000000000000
```

Conclusion

L2-Aware NAT allows the delivery of an IPv4 NAT service to ESM subscribers.

This chapter shows the configuration of L2-Aware NAT together with the associated show outputs which can be used verify and troubleshoot it.