ERICSSON

# ENM Network Integration Guideline

## Integration Specification

1/102 72-AOM 901 151 Uen CJ

## Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

## Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document Trademark Information.

# Contents

# 1 ENM Network Integration Guideline

> This document contains the network parameters that have to be configured during the Ericsson Network Manager (ENM) installation.

## Scope

The purpose of this document is to help network engineers to configure the network connectivity between ENM and managed nodes.

This document outlines the configurations required to integrate ENM in Customer Data Communication Network (DCN). The relevant ENM communication flows are towards:

— Supported Network Elements

  For the complete list of supported nodes refer to *ENM Supported Network Elements*,

— Service Network

— External NMS system

— Client hardware for operator access

## Target Audience

The intended target groups for this document are the following:

— System Integration Engineer

— Solution Architect

## Requirements

This document is expected to be used from the ENM deployment planning activity phases onward, and it is assumed that the reader of this document is familiar with the following:

— Network Firewalls configuration practices.

— RHEL™ operating system, JAVA™ web UI/CLI software or concepts.

— Installation, upgrade, configuration or operation of the ENM Deployment.

# 2 IP Network Architecture

> This section contains the Network Architecture for Physical Ericsson Network Manager (ENM) , Small Integrated ENM Multi-Technology and Small Integrated ENM Transport Only

## 2.1 ENM on Physical Network Layout

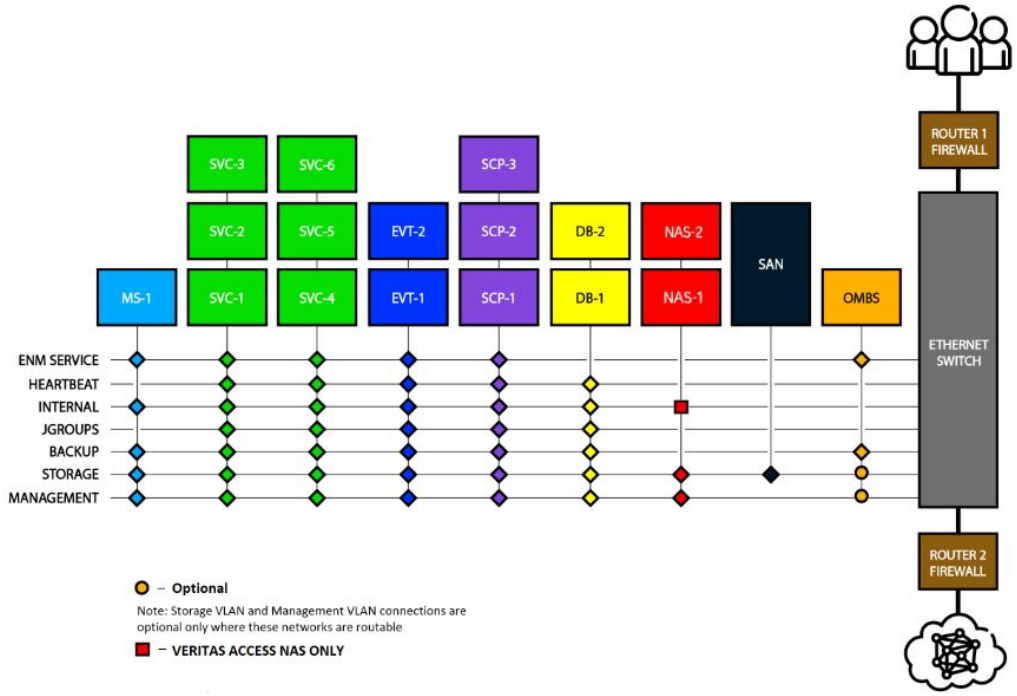
A typical 13-blade layout contains the following blades:

— 6 blades in a Service cluster

— 3 blades in a Scripting cluster

— 2 blades in a Database cluster

— 2 blades in an Event cluster




Router/Firewall 1 (RF1) represents the ENM DCN connectivity point (Northbound) to Users or External Systems.

Router/Firewall 2 (RF2) represents the DCN ENM connectivity point (Southbound) to managed nodes.

DVMS is a temporary client, it is required to perform Upgrade of the Medium, Large and Extra Large ENM.

DVMS requires access to the following VLAN's:

— ENM SERVICE

— INTERNAL

For additional information related to the diagram (such as logical blocks and ENM VLANs definition or Medium and Extra Large deployment layouts), refer to References on page 37 and References on page 37

## 2.2 Small Integrated ENM Multi-Technology Network Layout

A Small Integrated ENM Multi-technology deployment contains three racks in a VMware Integrated Openstack (VIO) cluster.

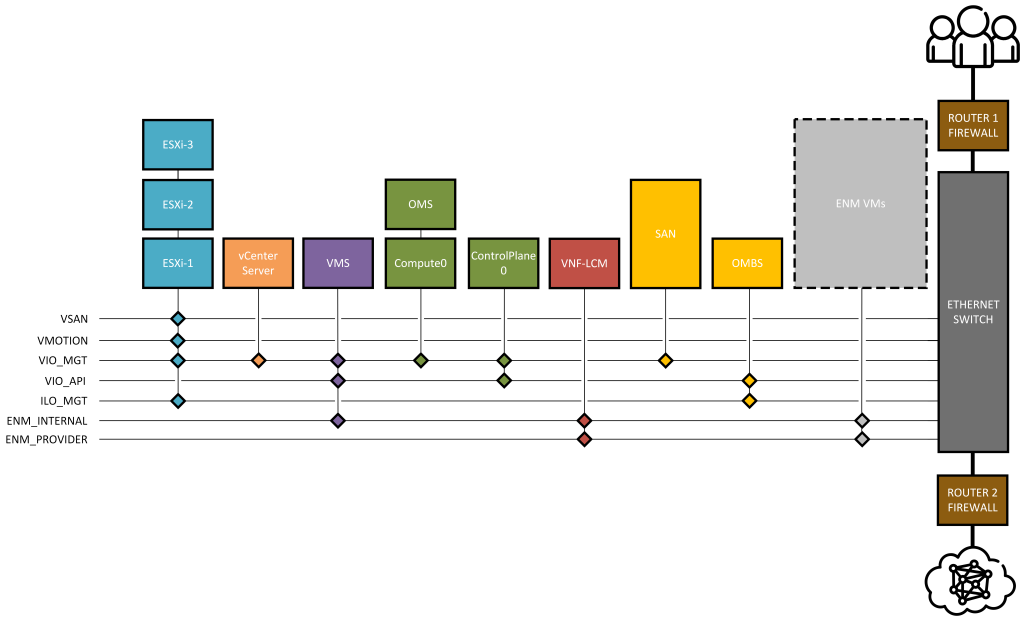
— Router/Firewall 1 (RF1) represents the ENM DCN connectivity point (Northbound) to Users or External Systems.

— Router/Firewall 2 (RF2) represents the DCN ENM connectivity point (Southbound) to managed nodes.

— DVMS is a temporary external client, it is required to perform the Install and Full Restore of the Small Integrated ENM Multi-Technology deployment.

  DVMS requires access to the following VLAN's :

  - VIO_MGT
  - ILO_MGT




## 2.3 Small Integrated ENM Transport Only Network Layout

A Small Integrated ENM Transport Only deployment contains one rack in a VMware Integrated Openstack (VIO) cluster.

— Router/Firewall 1 (RF1) represents the ENM DCN connectivity point (Northbound) to Users or External Systems..

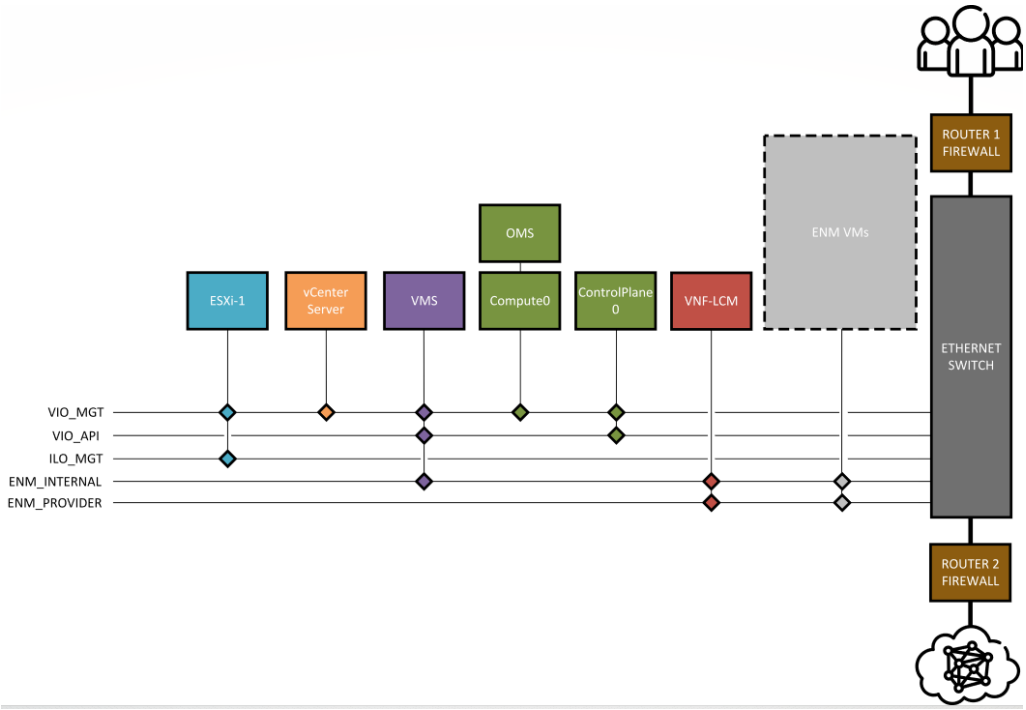
— Router/Firewall 2 (RF2) represents the DCN ENM connectivity point (Southbound) to managed nodes..

— DVMS is an external client, it is required to perform the Install, Upgrade and Full Restore of the Small Integrated ENM Transport Only deployment.

DVMS requires access to the following VLAN's :

VIO_MGT

ILO_MGT




## 2.4 ENM VLANs Description

Only the ENM Services VLAN IP subnet has to be routed externally for remote Clients or external NMS system connectivity (via RF1), and for nodes connectivity (via RF2).

The current ENM release does not natively support deployments in Customer networks where DCN arrives to ENM site with separated VLAN tags for the SBI/NBI connectivity ( SBI towards NEs, NBI towards Clients or external NMS Systems). It is then required for proper ENM deployment to have available at the ENM site a DCN connectivity toward NEs (managed nodes) and Clients/external NMS Systems based on a common (single) ENM Service VLAN.

Additional communications may be required to connect ENM with customer IP network services,such as NTP or DNS.

The Multicast Listener Discovery (MLD) protocol manages multicast groups by establishing, maintaining, and removing groups on a subnet. MLD must be enabled and MLD snooping must be disabled on the Services VLAN and on any externally connected switches for ENM nodes.

### 2.4.1 ENM on Physical VLANs

| VLAN | Description |
|---|---|
| ENM Services | This VLAN uses public routable addresses. The Services VLAN is both switched and routed. All northbound and southbound communication uses |

| VLAN | Description |
|---|---|
| | this VLAN. Each peer within ENM needs an address on the ENM Services VLAN. |
| ENM Internal VLAN | It is recommended that an RFC 1918 compliant private addresses be used for this VLAN. Non RFC 1918 compliant addresses such as reserved IP address ranges are not supported by the ENM application examples 169.254/16 127.0.0.0/8 , 0.0.0.0/8, 224.0.0.0/4,240.0.0.0/4,255.255.255.255/32.<br>Please note that 169.254 range is not a compliant private address as they are used in zero configuration networking when Dynamic Host Configuration Protocol (DHCP) services are not available. Each peer within ENM needs an address on the Internal VLAN. |
| JGroups VLAN | It is recommended that an RFC 1918 compliant private addresses be used for this VLAN. Non RFC 1918 compliant addresses such as reserved IP address ranges are not supported by the ENM application examples 169.254/16 127.0.0.0/8 , 0.0.0.0/8, 224.0.0.0/4,240.0.0.0/4,255.255.255.255/32.<br>Please note that 169.254 range is not a compliant private address as they are used in zero configuration networking when Dynamic Host Configuration Protocol (DHCP) services are not available. Each peer within ENM needs an address on the JGroups VLAN. ** The JGroups VLAN is used for JBoss multicasting. |
| Backup VLAN | It is recommended that an RFC 1918 compliant private addresses be used for this VLAN. Non RFC 1918 compliant addresses such as reserved IP address ranges are not supported by the ENM application examples 169.254/16 127.0.0.0/8 , 0.0.0.0/8, 224.0.0.0/4,240.0.0.0/4,255.255.255.255/32.<br>Please note that 169.254 range is not a compliant private address as they are used in zero configuration networking when Dynamic Host Configuration Protocol (DHCP) services are not available. This VLAN is used for all backup traffic. |
| Storage VLAN | It is recommended that an RFC 1918 compliant private addresses be used for this VLAN. Non RFC 1918 compliant addresses such as reserved IP address ranges are not supported by the ENM application examples 169.254/16 127.0.0.0/8 , 0.0.0.0/8, 224.0.0.0/4,240.0.0.0/4,255.255.255.255/32.<br>Please note that 169.254 range is not a compliant private address as they are used in zero configuration networking when Dynamic Host Configuration Protocol (DHCP) services are not available. All communication towards the SAN and NAS use this VLAN. |
| Heartbeat VLAN | The Heartbeat VLAN is only switched and not routed. VCS uses the Heartbeat VLAN for inter-node traffic to verify the status of services. |
| Management VLAN | This VLAN uses RFC 1918 compliant private addresses. The Management VLAN is only switched and not routed. Each peer within ENM needs an address on the Management VLAN. The dedicated Management VLAN is used to connect the management interface of every machine. This allows the management server to reach every node and use the Integrated Lights Out Manager (ILOM) console for remote management without passing through the firewall. |

### 2.4.2 Small Integrated ENM VLANs

| VLAN | Description |
|---|---|
| ENM Internal VLAN | It is recommended that an RFC 1918 compliant private addresses be used for this VLAN. Non RFC 1918 compliant addresses such as reserved IP address ranges are not supported by the ENM application examples 169.254/16 127.0.0.0/8 , 0.0.0.0/8, 224.0.0.0/4,240.0.0.0/4,255.255.255.255/32. |
| ENM Provider VLAN | This VLAN is equivalent to an ENM Services VLAN in an ENM Physical Deployment. All northbound and southbound communication will use this VLAN. |
| ILO_MGT | This VLAN uses RFC 1918 compliant private addresses. The ILO_MGT VLAN is both switched and routed. All physical infrastructure peers in a Small Integrated ENM deployment need an address on this VLAN to permit management access. |
| VIO_API | This VLAN uses RFC 1918 compliant private addresses. The VIO_API VLAN is both switched and routed. All virtualized infrastructure peers in |

| VLAN | Description |
|---|---|
| | the Small Integrated ENM deployment need an address on this VLAN to permit management access.<br>The VIO_API VLAN should be routable from the corporate network. |
| VIO_MGT | This VLAN uses RFC 1918 compliant private addresses. The VIO_MGT VLAN is both switched and routed. All infrastructure peers in a Small Integrated ENM deployment need an address on this VLAN to permit management access.<br>The VIO_MGT VLAN should be routable from the corporate network so that a user can access Administrative Web GUIs.<br>A route needs to exist between the VIO_MGT network and the ENM Provider VLAN so that the Virtual Management Server (VMS) can log in to LAF and the Backup and Restore workflows can log in to the vCenter Server from LAF. |
| VMOTION | This VLAN is used for vSphere VM migrations.<br>**Note:**<br>This VLAN exist only in Small Integrated ENM Multi-technology deployment |
| VSAN | This is the shared storage network.<br>**Note:**<br>This VLAN exist only in Small Integrated ENM Multi-technology deployment |

## 2.5 Firewall Configuration

> Firewall Routers are present to route and filter communication between ENM and the different communication domains (Security zones), as domain of managed nodes, domain of external NMS systems, domain of application clients, and so on.

**Note:** For Small Integrated ENM deployments, the ENM Services VLAN refers to the ENM Provider VLAN.

The information in the ENM Connectivity Details on page 8 is not based on any predefined firewall from any specific vendor. The following general aspects of a firewall configuration must to be considered:

— NAT (Network Address Translation) is used between the ENM Clients and ENM Services VMs. ENM clients connect a single IP address representing the ENM Application, and NAT/Load Balancing is used by ENM toward VMs running the relevant services. Even if NAT service is always enabled, NAT is not used for Corba-based North Bound Interface communications.

— SNMP(Simple Network Management Protocol) Trap is used for receiving the "Node Up" notification from the node.

  SNMP Trap requires the firewall be configured to allow the UDP reply.

— It is recommended to use a firewall that supports a stateful inspection of the following services or protocols: NTP, DNS, FTP, NFS, LDAP, DHCP and Sun-RPC. This reduces the number of ports that need to be opened explicitly.

— NFS uses Sun Remote Procedure Call (RPC) services and this can be required by ENM (for example, in a brownfield scenario between ENM and ENIQ-S, or

ENIQ-E for PM statistics or events reporting). The RPC service executes at a well-known port 111 but dynamically assigns and opens other TCP/UDP ports for other services defined by Sun program numbers. The NFS service is composed of nfsprog/100003 and mountd/100005. If after verifying its actual configuration, and the firewall appears not RPC aware, then a check is needed at the NFS hosts (with the command `rpcinfo -p`) to determine the actual allocated port numbers, and to open them in the firewall. With an RPC aware firewall, the NFS port are dynamically opened.

If not differently specified, the protocols/ports specified in ENM Connectivity Details are valid for IPv4 and, when applicable, IPv6 communication flows. Refer to ENM Supported Network Elements document for additional information about ENM and nodes IPv6 support.

**Note:** Port 111 must be opened on Storage VLAN only, not on Services VLAN

### 2.5.1 ENM Connectivity Details

> ENM Connectivity Details is a guideline for the Firewall Router configuration to facilitate ENM operations.

All nodes and Clients have a communication link with ENM Services, and the VNF Lifecycle Manager (ENM Cloud) also has a connection with the ENM Cloud Manager.

Information related to ENM communications with ENIQ-S/E cover greenfield scenarios only.

The ENM Connectivity Details only considers communication between ENM and different communication domains. The ENM communication end point at the ENM side is always represented by the IP subnets configured on the ENM Services VLANs, and not by specific IP addresses.

All above Connectivity details are deployed in the next sections of this chapter.

The NE Types connectivity is fully described in the ENM Connection Matrix: 1/102 72-aom 901 151-1 Uen

Filtering of communications within each communication domain is out of the scope, as well as filtering between ENM application components internal to the ENM service VLAN.

#### 2.5.1.1 ENM Clients

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 1 ENM Services to ENM Clients

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| NA | | | | |

Table 2 ENM Clients to ENM Services

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPS | TCP | 443 | ENM | ENM Web Client communication to Apache VM |
| HTTP | TCP | 7080 | ENM | Client connectivity GUI for ENM System Monitoring |
| HTTPS | TCP | 7443 | ENM | Client connectivity GUI for ENM System Monitoring, secure |
| HTTPS | TCP | 443 | EEA application | EEA application connectivity |
| SSH/SFTP | TCP | 22 | ENM | Secure File Transfer, Secure CLI |
| SSH | TCP | 5022 | ENM | Load balanced access for AMOS interactive sessions |
| SSH | TCP | 5023 | ENM | Load balanced access for ENM scripting interactive sessions |
| SSH/SFTP | TCP | 22 | ENIQ-E/S | ENIQ-E/S files fetching |
| SQL | TCP | 2640 | ENIQ-E/S | ENIQ-E/S data fetching |
| SQL | TCP | 2642 | ENIQ-E/S | NetAn Server, BIS and OCS clients connectivity |

Table 3 ENM Clients to ENIQ-S OCS

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPS | TCP | 443 | OCS Citrix | ENM Client to SON OM Port secure |
| HTTP | TCP | 80 | OCS Citrix | ENM Client to OCS Citrix Port |
| Citrix Common Gateway | TCP | 2598 | OCS Citrix | ENM Client to OCS Citrix Port |
| HTTP | TCP | 8080 | ENIQ-S | ENM Client to Business Objects Port |

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPS | TCP | 8443 | ENIQ-S | ENM Client to Business Objects Port secure |
| HTTPS | TCP | 443 | ENIQ-S | ENM Client to Network Analytics Port secure |

Table 4 ENM Clients to SON-OM

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPS | TCP | 443 | SON OM | ENM Client to SON OM Port secure |
| HTTP | TCP | 80 | SON OM | ENM Client to SON OM Port |

#### 2.5.1.2 Customer IP Nw Services (RF1/RF2)

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 5 ENM Services to Customer IP Nw Services

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| DNS | UDP | 53 | Infrastructure DNS Server | Domain Name System |
| NTP | UDP | 123 | Infrastructure NTP Server | Network Time Protocol |
| SMTP | SMTP | 25 | Infrastructure SMTP MTA | ENM uses the service IP address of the LVS router handling the mailx service for SMTP communications. This port is required only if ENM has SMTP relay host function to support ENM application sending emails (for example FMX). |

Table 6 Customer IP Nw Services to ENM Services

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| None | | | | |

### 2.5.1.3 External NMS Servers

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 7 ENM Services to external NMS Servers

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| Ericsson Proprietary | TCP | 5111 | NMS | TCP NBI Stream |
| REXEC, RSH | TCP | 113 | NMS | Port for REXEC and RSH server Firewall acknowledgment. Based BNSI interface (for backward compatibility) – Required only if such protocol is used |
| REXEC | TCP | 1025 - 65535 | NMS | Port in proposed range can be used to allow the REXEC stderr printouts Based BNSI interface (for backward compatibility) – Required only if such protocol is used |
| RSH | TCP | 514 -1022 | NMS | Port in proposed range can be used to allow the RSH stderr printouts. Based BNSI interface (for backward compatibility) – Required only if such protocol is use |
| CORBA | TCP | 1025 - 65535 | NMS | Depending on NMS Corba configuration, a port in the proposed range is used to send asynch alarms |
| AVRO | TCP | 1025 - 65535 | NMS | NBI access to Analytic Session Record (ASR). Port is configurable independently for ASR-L and ASR-N. |
| SNMP | UDP | 162 | NMS | The port is configurable and the default is 162. The SG that generates traffic on this port is nbfmsnmp |

Table 8 External NMS Servers to ENM Services

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH | TCP | 8345 | ENM (FM IPv4/ IPv6 VIP address) | SSH based BNSI interface – Required only if such protocol is used |
| REXEC | TCP | 512 | ENM (FM IPv4/ IPv6 VIP address) | REXEC based BNSI interface (for backward compatibility) – Required only if such protocol is used |
| RSH | TCP | 514 | ENM (FM IPv4/ IPv6 VIP address) | RSH based BNSI interface (for backward compatibility) – Required only if such protocol is used |
| HTTPs | TCP | 443 | ENM | NBI access to Schema Registry REST inteface |
| HTTPs | TCP | 9200 | ENM | NBI Access to Elasticsearch to query logs |
| SQL | TCP | 2640 | ENIQ-E/S | ENIQ-E/S data fetching |
| Telnet | TCP | 23 | ENIQ-E/S | ENIQ-E/S NBI files fetching. Optional, SSH should be used when available |
| SSH/SFTP | TCP | 22 | ENIQ-E/S | ENIQ-E/S NBI files fetching |
| FTP | TCP | 21 | ENIQ-E/S | ENIQ-E/S NBI files fetching. Optional, SFTP should be used when available |
| CORBA | TCP | 9951 - 9956 | ENM | NBI access to IRP |
| HTTPS | TCP | 443 | ENM | NBI access to Schema Registry REST inteface<br>Retrieve Name Service IOR File (FM Corba NBI) |
| SNMP | UDP | 35161 | ENM (FM IPv4/ IPv6 VIP address | FM SNMP NBI Agent port<br>The SG that exposes the port is nbfmsnmp |

**Note:** Elasticsearch port is for internal use only. Customer unit (CU) can request Ericsson Organization to get the information on Elasticsearch API.

Refer to ENM FM BNSI Northbound Interface Integration Programmers Guide, References [12] for Enabling/Disabling BNSI Interface.

### 2.5.1.4 External PM Servers

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 9 ENM Services to external PM Servers

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SNMP | UDP | 162 | ENIQ-S/E | Sun Management Centre Trap Handler |
| NFS | TCP, UDP | 2049 | ENM | Sun (Network File System). See Firewall Configuration on page 7 about NFS services using RPC and how different firewalls treat this dynamic service. |
| SNMP | UDP | 50720 - 50739 | ENIQ-S/E | Server Layer of the System Monitoring application initiates session towards the Agent Layer of the System Monitoring application |
| SNMP | UDP | 50740 | ENIQ-S/E | Default System Monitoring Application Agent port 161 will be reconfigured to this higher port. Server Layer initiates session towards the Agent Layer. |
| DHCP | UDP | 67,68 | MWS | Used for communication between MWS SERVER and CLIENT<br>**Note:**<br>PM service VLAN (OSS storage), these ports do not communicate outside of the VLAN, both client and server are in same VLAN. |
| TFTP | UDP | 69 | MWS | Used for communication between MWS SERVER and CLIENT<br>**Note:**<br>PM service VLAN (OSS storage), these ports do not communicate |

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| | | | | outside of the VLAN, both client and server are in same VLAN. |

Table 10 External PM Servers to ENM Services

| Application Protocol | Transport Protocol | Dst Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SNMP | UDP | 50600-50719 | ENM | Agent Layer of the System Monitoring application initiates session towards the Server Layer of the System Monitoring application |
| TCP/IP (hdl-srv) | TCP | 2641 | ENIQ statistics standalone/ coordinator node | Port to access ENIQ repository database |

### 2.5.1.5 VNF Lifecycle Manager (VNF-LCM)

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 11 VNF Lifecycle Manager to ENM Services

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | ENM (scp-1-scripting) | |
| IIOP/ GIOP | TCP | 9951 | ENM (LVSRouter) | |
| NTP | UDP | 123 | ENM (scp-1-scripting) | |
| IIOP/ GIOP | TCP | 9954 | ENM (visinamingnb) | |

Table 12 ENM Services to VNF Lifecycle Manager

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| IIOP/GIOP | TCP | 9002 | VNF-LCM (vnflaf-services) | |
| HTTP | TCP | 8080 | VNF-LCM (vnflaf-services) | |
| IIOP/ GIOP | TCP | 9954 | VNF-LCM (vnflaf-services) | |
| HTTP | TCP | 80 | VNF-LCM (vnflaf-services) | |

Table 13 VNF Lifecycle Manager to ECM

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPs | TCP | 8080 | ECM | ECM REST API port contacted by VNF Lifecycle Manager for cloud resource orchestration i.e. instantiation, scaling and termination of VNFs. |

Table 14 VNF Lifecycle Manager to ECEE/Openstack

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPs | TCP | 5000 | ECEE | ECEE Identity Service REST API port contacted by VNF Lifecycle Manager to authenticate with ECEE (default port, exact port numbers should be checked for the specific ECEE deployment) |
| HTTPs | TCP | 8004 | ECEE | ATLAS (Openstack Heat) API port contacted by VNF Lifecycle Manager for cloud resource orchestration i.e. instantiation, scaling and termination of VNFs (default port, exact port numbers should be checked for the specific ECEE deployment) |
| HTTPS | TCP | 8774 | ECEE | ECEE NOVA Compute Service REST API port contacted by workflows to creating virtual machines on ECEE (default port, exact port numbers should be checked for the specific ECEE deployment) |
| HTTPS | TCP | 9292 | ECEE | ECEE Glance Service REST API port contacted by workflows to querying of VM image metadata as well as retrieval of the actual images on ECEE (default port, exact port numbers should be checked for the specific ECEE deployment) |

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPS | TCP | 9696 | ECEE | ECEE Neutron Service REST API port contacted by workflows to install and configure the Networking service on ECEE (default port, exact port numbers should be checked for the specific ECEE deployment) |
| HTTPS | TCP | 8776 | ECEE | ECEE Cinder Service REST API port contacted by workflows to provides block storage devices to guest instances on ECEE (default port, exact port numbers should be checked for the specific ECEE deployment) |
| HTTPs | TCP | 443 | ECEE | |
| HTTPS | TCP | 8082 | ECEE | ECEE Contrail Service REST API port contacted by workflow to install and configure the Contrail service on ECEE (default port, exact port numbers should be checked for the specific ECEE deployment) |

Table 15 VNF Lifecycle Manager (VNF-LCM to VNFs)

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH | TCP | 22 | VNFs | SSH default port. For VNF specific ports refer to respective VNFs section |

Table 16 VIM to VNF Lifecycle Manager

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTP | TCP | 80 | VNF-LCM (vnflaf-services) | vim to access files from Apache |
| HTTPs | TCP | 443 | VNF-LCM (vnflaf-services) | vim to access files from Apache |

Table 17 External orchestrator to VNF-LCM

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTP | TCP | 12987 | VNF-LCM (vnflaf-services) | Orchestrator to monitor VNF-LCM health. |

### 2.5.1.6 ENM Services SSO to ENIQ OCS

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 18 ENM Services SSO to ENIQ OCS

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| LDAP | TCP | 636 | Active Directory | ENM Services SSO to OCS AD Port |

Table 19 SBG-IS Services to ENM Services

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | ENM | SSH and SFTP |
| SNMP | UDP | 162 | ENM | SNMP traps |

### 2.5.1.7 SON-OM to ENM Services

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 20 SON-OM to ENM Services

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPS | TCP | 443 | ENM Services | SON-OM to ENM Services Port Secure |
| HTTP | TCP | 80 | ENM Services | SON-OM to ENM Services Port |

Table 21 SBG-IS Services to ENM Services

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | ENM | SSH and SFTP |
| SNMP | UDP | 162 | ENM | SNMP traps |

### 2.5.1.8 External SHM Servers

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 22 ENM Services to external SHM Servers

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | Network Element Software Store (CAS-C) | SFTP only, no SSH connectivity permitted.<br>SFTP default port. |
| HTTPS | TCP | 10010 | Network Element Software Store (CAS-C) | ENM uses CAS-C to make REST API call for submitting instantaneous licensing requests. |

### 2.5.1.9 DVMS

DVMS is a temporary appliance used to orchestrate install and upgrade on Small ENM deployments.

DVMS is also used as an ephemeral VM to orchestrate the Medium, Large and Extra Large ENM Upgrades.

For physical ENM Upgrades the DVMS runs into the LMS as a VM.

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 23 DVMS to Openstack (Small ENM deployments)

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| HTTPs | TCP | 5000 | Openstack | Openstack Identity Service REST API |

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| | | | | port contacted by DVMS to authenticate with Openstack (default port, exact port numbers should be checked for the specific Openstack deployment) |
| HTTPs | TCP | 8004 | Openstack | HEAT (Openstack Heat) API port contacted by DVMSfor cloud resource orchestration i.e. instantiation, scaling and termination of VNFs (default port, exact port numbers should be checked for the specific Openstack deployment) |
| HTTPS | TCP | 8774 | Openstack | Openstack NOVA Compute Service REST API port contacted by workflows to creating virtual machines on Openstack (default port, exact port numbers should be checked for the specific Openstack deployment) |
| HTTPS | TCP | 9292 | Openstack | Openstack Glance Service REST API port contacted by workflows to querying of VM image metadata as well as retrieval of the actual images on Openstack (default port, exact port numbers should be checked for the specific Openstack deployment) |
| HTTPS | TCP | 9696 | Openstack | Openstack Neutron Service REST API port contacted by workflows to install and configure the Networking service on Openstack (default port, exact port numbers should be checked for the specific Openstack deployment) |
| HTTPS | TCP | 8776 | Openstack | Openstack Cinder Service REST API port contacted by workflows to provides block storage devices to guest instances on Openstack (default |

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| | | | | port, exact port numbers should be checked for the specific Openstack deployment) |
| HTTPs | TCP | 443 | Openstack | |
| HTTPS | TCP | 8082 | Openstack | Openstack Contrail Service REST API port contacted by workflow to install and configure the Contrail service on Openstack (default port, exact port numbers should be checked for the specific Openstack deployment) |

Table 24 DVMS to ENM Provider (Small ENM deployments)

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | VNFLCM, ENM | |
| HTTP | TCP | 80 | VNFLCM | |
| HTTPS | TCP | 443 | VNFLCM | |
| NTP | TCP | 123 | ENM | |
| DNS | TCP | 53 | ENM | |
| DNS | UDP | 53 | ENM | |

Table 25 CDD/SWDP Infrastructure to DVMS (Small ENM deployments)

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | DVMS | |
| HTTP | TCP | 80 | DVMS | |
| HTTPS | TCP | 443 | DVMS | |
| HTTP | TCP | 8080 | DVMS | |

Table 26 DVMS to ENM (Medium, Large & Extra Large ENM Upgrades)

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | LMS | Connectivity from DVMS to LMS to run the ENM Upgrade |

Table 27 CDD/SWDP to ENM (Medium, Large & Extra Large ENM Upgrades)

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | LMS | Connectivity from DVMS to LMS to run the ENM Upgrade |

Table 28 Small Integrated ENM to DVMS

| Application Protocol | Transport Protocol | DST Port Number | Destination VLAN | Comment |
|---|---|---|---|---|
| HTTP | TCP | 80 | ilo_management | Administrative access to iLO management console |
| HTTPS | TCP | 443 | ilo_management | Administrative access to iLO management console |
| SSH/SFTP | TCP | 22 | ilo_management | Administrative access to iLO management console |
| HTTPS | TCP | 443 | vio_mgt | Administrative access to ESXi web UI. Administrative access to vCenter web UI. |
| HTTPS | TCP | 5480 | vio_mgt | Administrative access to vCenter web UI - Administrator Mode |
| SSH/SFTP | TCP | 22 | vio_mgt | Administrative access to ESXi console. |
| DNS BIND server | TCP | 53 | vio_mgt | TCP and UDP ports need to be open for the Domain Name Service |
| DNS BIND server | UDP | 53 | vio_mgt | TCP and UDP ports need to be open for the Domain Name Service |
| Remote Console Port | TCP | 17990 | ilo_management | Access to the ILO remote console |
| Virtual Media Port | TCP | 17988 | ilo_management | Access to the ILO virtual media port |

**Note:** Applicable for initial installation of Small Integrated ENM Deployments only.

Table 29 Small Integrated ENM from DVMS

| Application Protocol | Transport Protocol | DST Port Number | Destination VLAN | Comment |
|---|---|---|---|---|
| HTTP | TCP | 80 | ilo_management | Administrative access to iLO management console |
| HTTPS | TCP | 443 | ilo_management | Administrative access to iLO management console |
| SSH/SFTP | TCP | 22 | ilo_management | Administrative access to iLO management console |
| HTTPS | TCP | 443 | vio_mgt | Administrative access to ESXi web UI. Administrative access to vCenter web UI. |
| HTTPS | TCP | 5480 | vio_mgt | Administrative access to vCenter web UI - Administrator Mode |
| SSH/SFTP | TCP | 22 | vio_mgt | Administrative access to ESXi console. |
| DNS BIND server | TCP | 53 | vio_mgt | TCP and UDP ports need to be open for the Domain Name Service |
| DNS BIND server | UDP | 53 | vio_mgt | TCP and UDP ports need to be open for the Domain Name Service |

| Application Protocol | Transport Protocol | DST Port Number | Destination VLAN | Comment |
|---|---|---|---|---|
| Remote Console Port | TCP | 17990 | ilo_management | Access to the ILO remote console |
| Virtual Media Port | TCP | 17988 | ilo_management | Access to the ILO virtual media port |

**Note:** Applicable for initial installation of Small Integrated ENM Deployments only.

### 2.5.1.10 Small Integrated ENM

The communication flows representation in terms of "from/to" refers to the expected initial communication setup (only the documented unidirectional communication initiation flows have to be allowed on relevant firewalls).

Unless otherwise specified, the Source port number is expected to fall in to the ephemeral port range (OS dependent, usually in the 1024-65535 port range).

Table 30 ENM Clients to Small Integrated ENM

| Application Protocol | Transport Protocol | DST Port Number | Destination VLAN | Comment |
|---|---|---|---|---|
| SSH/SFTP | TCP | 22 | vio_mgt | Administrative access to ESXi console. |
| HTTPS | TCP | 443 | vio_mgt | Administrative access to ESXi web UI.<br>Administrative access to vCenter web UI. |
| HTTPS | TCP | 5480 | vio_mgt | Administrative access to vCenter web UI - Administrator Mode |
| SSH/SFTP | TCP | 22 | vio_api | Administrative access to Openstack API & management console.I |
| HTTPS | TCP | 443 | vio_api | Administrative access to Openstack API & management console. |
| SSH/SFTP | TCP | 22 | enm_provider | Administrative access to ESXi console. |
| HTTP | TCP | 80 | enm_provider | Administrative access to ESXi web UI. |

| Application Protocol | Transport Protocol | DST Port Number | Destination VLAN | Comment |
|---|---|---|---|---|
| | | | | Administrative access to vCenter web UI. |
| SSH/SFTP | TCP | 22 | ilo_management | Administrative access to iLO management console. |
| HTTP | TCP | 80 | ilo_management | Administrative access to iLO management console. |
| HTTPS | TCP | 443 | ilo_management | Administrative access to iLO management console. |

Table 31 External Syslog Server to Small Integrated ENM

| Application Protocol | Transport Protocol | DST Port Number | Destination VLAN | Comment |
|---|---|---|---|---|
| SYSLOG | UDP | 514 | vio_mgt | ESXi and vCenter access to External Syslog Server to forward the vSphere Logs to External Syslog Server. |

**Note:** Configuring an external `syslog` server to collect `vSphere` logs is not a mandatory requirement but it is highly recommended for debugging purposes.

### 2.5.2 Configure DHCP Relay

> Ensure the availability of the DHCP relays.

ENM provides a DHCP service and it is deployed on the services VM on the SVC cluster. The DHCP service has a primary and secondary configuration with two separate IP addresses. The DHCP service may change between hosts at failover, upgrade or rollback.

#### Steps

1. Configure the relay agents in the Network Elements to forward DHCP requests to the primary DHCP server.

2. To find the primary DHCP server, log in to the itservices VMs and check the status of the dhcpd/dhcpd6 service to see if it is running.

   For more information, refer to the DHCP Configuration for Autointegration section in the References on page 37

### 2.5.3 Configure TCP Connection Timeout

Some of the TCP connections passing through the firewall are long-lived. Without traffic, long delays may occur and as a result, the firewall may mistakenly consider these connections abandoned (for example, for CORBA connections to the network elements).

#### Steps

1. Set the TCP idle timeout parameter in the firewall to 65 minutes.

   Usually, the TCP connections for node management are configured on respective peers TCP/IP stacks to have a maximum TCP idle time of 60 minutes.

2. Configure the firewalls in the DCN networks not to drop idle connections.

### 2.5.4 ENM Backup and Restore Configuration

#### Firewall configuration

NetBackup proprietary protocol is used for backup transfer between:

— the OMBS server and the ENM MS,

— the OMBS server and the ENM peer servers and the NAS.

NetBackup needs the TCP/IP ports 1556, 2821, 4032, 13724 and 13782 to be open in the ENM firewall for backup operations that use NetBackup proprietary protocol functionalities.

#### DNS

If DNS is used for the ENM deployment the UDP port 53 must be open for DNS queries in the ENM firewall configuration. NetBackup requires name resolution for the host names, therefore the site DNS must be configured with:

1. OMBS server IP address on backup VLAN.
2. ENM peer servers IP addresses on backup and ENM service/internal VLAN.
3. NAS servers physical and virtual IP addresses on storage VLAN and console IP/VIP.

### Routing and additional switch configuration

- If the DNS is not available, routing must be provided between the OMBS server backup VLAN and the NAS storage VLAN, because the backup VLAN does not exist on the NAS. If no routing is provided, the OMBS server must be manually configured with the storage VLAN.
- Link Aggregation Control Protocol (LACP) must be configured on the network switches with the bonding method LACP L3+L4. The configuration on the network switches and the OMBS server must match. For more information and details about ENM deployement LACP and VLANs configuration refer to the ENM Installation Instructions in the References.
- For MS restore, the PXE booting of the MS from the OMBS server and the ENM Services VLAN must be configured on the OMBS server in a default configuration. Alternatively, the MS PXE boots the backup VLAN. This requires network switch configuration of the DHCP relay between the ENM Services VLAN on the MS and the backup VLAN on the OMBS.
- PXE booting, operating on the backup VLAN, requires that a route is configured between the OMBS backup VLAN IP and the ENM MS management VLAN.

For more information refer to the References on page 37

## 2.5.5 WAN-SDN Controller Integration

WAN-SDN controller is playing the role of Domain SDN Controller in an IP/MPLS network domain. Using standard IETF protocols, WAN-SDN controller supports the collection of logical network topology data from managed Network Elements, centralized path computation, and provisioning across the managed domain.

Following ports must be open at client firewall.

Table 32 WAN-SDN Controller Connectivity

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| Cassandra | TCP | 17000 | Northstar App Server | Cassandra database cluster |
| HTTPS | TCP | 9300 | Analytics Server | Elasticsearch cluster. Elasticsearch port is for internal use only. Customer unit (CU) can request Ericsson Organization to get the information on Elasticsearch API. |
| HTTPS | TCP | 9201 | Analytics Server | Elasticsearch cluster. Elasticsearch port is for internal use only. Customer unit (CU) can |

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| | | | | request Ericsson Organization to get the information on Elasticsearch API. |
| Netflow | UDP | 9000 | Analytics Server | Netflow |
| HTTPS | TCP | 8443 | Northstar App Server | Web:Web client/REST to secure web server (https) |
| HTTP | TCP | 8091 | Northstar App Server | Web:Web client/REST to web server (http) |
| Cassandra | TCP | 7001 | Northstar App Server | Cassandra database cluster |
| Planner | TCP | 7000 | Northstar App Server | Communications port to NorthStar Planner |
| Redis | TCP | 6379 | Northstar App Server | Redis |
| RabbitMQ | TCP | 5672 | Northstar App Server | RabbitMQ |
| PCEP | TCP | 4189 | Northstar App Server | PCEP: PCC (router) to NorthStar PCE server |
| Zookeeper | TCP | 3888 | Northstar App Server | Zookeeper cluster |
| Zookeeper | TCP | 2888 | Northstar App Server | Zookeeper cluster |
| JTI | UDP | 2002 | Analytics Server | JTI: Default Junos Telemetry Interface reports for LSP (supports Analytics) |
| JTI | UDP | 2001 | Analytics Server | JTI: Default Junos Telemetry Interface reports for IFL (supports Analytics) |
| JTI | UDP | 2000 | Analytics Server | JTI: Default Junos Telemetry Interface reports for IFD (supports Analytics) |
| SYSLOG | UDP | 1514 | Analytics Server | Syslog: Default Junos Telemetry Interface reports for RPM probe statistics (supports Analytics) |
| NETCONF | TCP | 830 | Router Network | NETCONF communication between NorthStar Controller and routers |
| NTAD | TCP | 450 | Junos VM | NTAD |

| Application Protocol | Transport Protocol | DST Port Number | Destination Node | Comment |
|---|---|---|---|---|
| BGP | TCP | 179 | Northstar App Server, Junos VM | BGP: JunosVM for router BGP-LS —not needed if IGP is used for topology acquisition |
| SNMP | UDP | 161 | Router Network | SNMP |
| PCEP | TCP | 21111 | Northstar App Server | Source port number of exported packets |
| PCEP | TCP | 30000 | Northstar App Server | Destination port number for the exported packets |
| NA | NA | 8124 | Northstar App Server | Health Monitor |
| JTI | UDP | 3000 | Analytics Server | JTI: In previous NorthStar releases, three JTI ports were required (2000, 2001, 2002).<br>Starting with Release 4.3.0, this single port can be used instead. |
| MDT | UDP | 3001 | Analytics Server | Model Driven Telemetry (MDT) |
| MDT | TCP | 3002 | Analytics Server | Model Driven Telemetry (MDT) |
| BMP | TCP | 10001 | Northstar App Server | BMP passive mode: By default, the monitor listens on this port for incoming connections from the network. |
| PRPD | TCP | 50051 | Router Network | PRPD: NorthStar application to router network |

**Note:** Elasticsearch port is for internal use only. Customer unit (CU) can request Ericsson Organization to get the information on Elasticsearch API.

### 2.5.6 Connectivity to External Identity Provider

ENM provides the possibility to interact with External Customer Identity Provider using LDAPS protocol.

The connectivity is over TCP and it occurs on a specific TCP Port provided by the Customer.

Below table provides the Source IP address's used by ENM applications on different Virtual Machines and different ENM Deployment Types:

Table 33 Source IP address's used by ENM applications to establish tcp connection to External Identity Provider

| Phy ENM | | | | vENM | |
|---|---|---|---|---|---|
| **Feature** | **VMs** | **Source IP-Addr in case of IPv4** | **Source IP-Addr in case of IPv6** | **Source IP-Addr in case of IPv4** | **Source IP-Addr in case of IPv6** |
| **Remote User Authentication with Ext IdP** | **SSO** | svc_CM_vip_ipaddress | sso_service_IPv6_IPs | svc_PM_vip_ipaddress | svc_PM_vip_ipv6address |
| | **secserv** | svc_CM_vip_ipaddress | secserv_service_IPv6_IPs | svc_CM_vip_ipaddress | svc_FM_vip_ipv6address |
| **Federated Identity Management** | **idmserv** | svc_CM_vip_ipaddress | N/A<br>See Note(1) | N/A<br>(1) | N/A<br>(1) |

(1) Federated Identity Management is restricted to IPv4 and on Phy ENM deployment type ONLY

# 3 DCN Dimensioning for Transport Nodes

In previous sections we already mentioned the DCN (also known as O&M Network) classification from an ENM perspective as:.

— Northbound DCN: network infrastructure (e.g. a set of interconnected switches/routers implementing the Customer IT service) connecting Northbound ENM network interfaces with Users or External Systems

— Southbound DCN: network infrastructure (e.g. a set of interconnected switches/routers plus dedicated data connections between managed nodes) connecting Southbound ENM network interfaces with managed nodes

If not differently specified, in this section the DCN term is used to refer to the Southbound DCN part.

From a design and provisioning perspective, Transport Networks can be considered as composed by multiple networks carrying different type of data (for example Traffic plane, Control plane, Management plane, Synch plane The network providing the management service is usually indicated as Data Communication Network (DCN). Traffic Networks handle data plane services (for example the transmission of the users data between radio base stations in the mobile access network, or between a MSAN and a Core router) while DCN Networks handle O&M data between nodes and Management System (for example ENM).

DCN in Transport networks is generally composed by:

— An Access Network Infrastructure (for example a set of interconnected switches/routers) part, that connects the Management System to the Gateway Network Elements (GNE). A Gateway Network Element is a managed node that is connected to both the Access Network Infrastructure (for example via dedicated node ethernet port) and to a set of nodes behind it (for example via in-band DCN channels)

— A GNE/NE interconnection part, that can be based either on in-band or out-of-band communication channels, where:

  • A DCN communication channel is defined "in-band" if it transports the network management across a network shared with data plane traffic, using bandwidth that would otherwise be available for data plane traffic

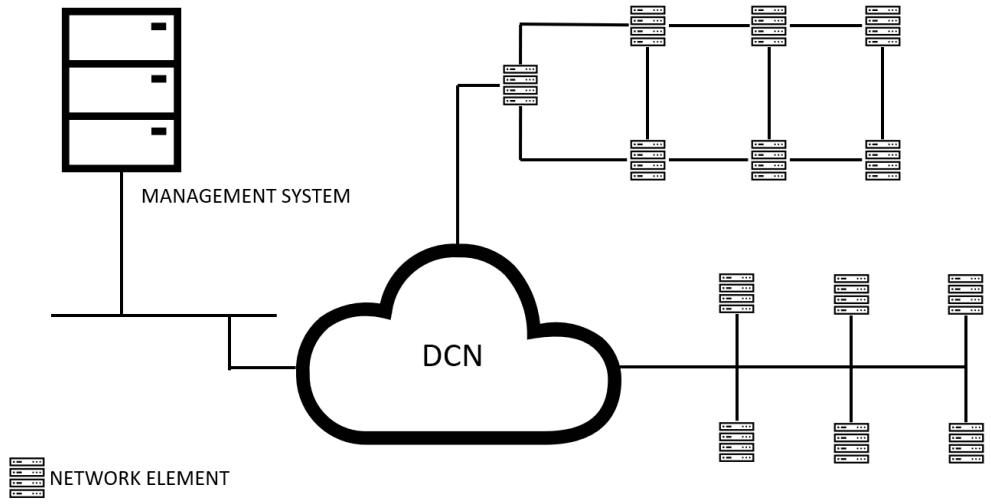
  • A DCN communication channel is defined "out-of-band" if it transports traffic travels on different paths respect the data plane, so these paths are dedicated to management traffic

Depending on the way the Access Network is connected to the GNEs, and on the way GNE are connected to NEs, DCN can be structured as

— A set of L2 networks, where subset of nodes are connected to each other sharing the same VLAN ID and behave as IP hosts. This means that all nodes in an L2 network share the same Ethernet broadcast domain

— A set of L3 IP routed networks (in a common IP routing domain), where nodes are inter-connected via both in-band or out-of-band DCN channels, and where the connected nodes behave as IP routers, having their own IP subnet in which they configure their own management IP address

— A generic mix of previous solutions (most common design)




MINI-LINKs and Router 6000 node families, as well as third parties products (Cisco, Juniper), support IP based DCN and can be integrated as IP hosts only or with IP router (for example OSPF) additional functionality.

When supported by the specific node type DCN functionality, the DCN can be carried over the entire network through embedded DCN channels (in-band DCN) and/or through an external IP network infrastructure (out-of-band DCN, composed by routers, switches, etc.).

Most of the Transport node families have embedded IP routers for handling of DCN traffic between the NEs, which reduces the amount of external routers and switches required to implement e2e IP connectivity with management system

Transport Nodes and related variants are listed in the following table:

Table 34 Transport Nodes

| Node Family | Node Variant |
|---|---|
| MINI-LINK | TN/LH/CN |
| | 66xx |
| | 63xx |

| Node Family | Node Variant |
|---|---|
| Router 6000 | 6x71 |
| | 6672 |
| | 6675 |
| | 6274 |
| Juniper | PTX |
| | MX |
| | SRX |
| FH6000 | 6080 |
| | 6020 |
| ESC | ESC |
| | ERS Support Node |
| SIU/TCU02 | N/A |
| RadioTNode | N/A |
| SSR/BNG | N/A |
| Cisco ASR | N/A |
| ECI | N/A |

## 3.1 DCN For MINI-LINK Nodes

MINI-LINK nodes can be integrated in DCN as pure IP hosts or enabling their IP router (for example. OSPF) additional functionality.

The MINI-LINK node type is the most critical in terms of the DCN requirement to DCN. For example, the MINI-LINK TN version 20P is one of the ENM managed node impacting the most for DCN load aspects (e.g. PM file size, SW image file size, alarm rate, CM data model size), and DCN configuration complexity (for example. up to 20 PPP DCN interfaces).

From a DCN dimensioning perspective, the possibility to configure DCN trees of subtended MINI-LINKs behind a node acting as a ML acting as GNE (as reported as an example in the figure above), introduces the need of proper bandwidth provisioning on access DCN network connecting ENM to GNE nodes serving the subtended trees.

Even if from a MINI-LINK node DCN functionality perspective, it is possible to configure nodes connected with a single DCN channel of 64 kb/s (for example in case of PPP over TDM transported over low speed radio links), this is not considered as defining the minimal node DCN connectivity requirement for ENM, as referring to a very unlikely scenario (for example. applicable only to very low speed and TDM only MW links with old HW deployments (for example MMU2)).

For additional information on MINI-LINK nodes supported DCN configurations refer to *MINI-LINK - Planning and Dimensioning DCN -1/1551-HSD 101 16/1* .

For MINI-LINK node family, the recommendation is to reserve a DCN bandwidth for ENM O&M traffic at NE side of at least 128 Kb/s per single NE.

## 3.2 DCN For Router 6000 Nodes

Router 6000 nodes can be integrated in DCN as pure IP hosts or enabling their node IP router (e.g. OSPF) additional functionality.

Router 6000 nodes are usually installed with DCN traffic carried over an Ethernet network.

Refer to *Router 6000 - Initial System Configuration - 3/1543-AXI 101 09/1-V1*, fro more details on the Node configured as in-band or out-band traffic.

In typical Router 6000 nodes network deployment, requirements or constraints to support very low speed DCN channels for O&M traffic (e.g. order of few Kb/s) are not expected.

For Router 6000 node family, the recommendation is to reserve a DCN bandwidth for ENM O&M traffic at NE side of at least 1 Mb/s.

Previous indication is valid also when nodes are directly connected to DCN through the out-of-band management port, and it applies for all types of Router 6000 node family variants.

## 3.3 DCN For Optical Fronthaul (Fronthaul 6080) Nodes

Fronthaul (FH) nodes can be integrated in DCN as pure IP hosts only. FH nodes are connected to the DCN network via Ethernet local interface, and Management VLAN can be used as DCN extension. For additional information on FH nodes DCN configuration refer to *Fronthaul - Initial Network Configuration - 14/1543-CRA 119 1832/1*.

For FH node family, the recommendation is to reserve a DCN bandwidth for ENM O&M traffic at NE side of at least 1Mb/s.

## 3.4 DCN For Juniper 3PPs Nodes

ENM supports Juniper 3PP nodes.

Juniper nodes can be integrated in DCN as pure IP hosts or enabling their IP router (e.g. OSPF) additional functionality.

All considerations done for Router 6000 nodes are also valid for Juniper node types. Refer to Juniper nodes specific 3PP technical documentation for additional details on their DCN configuration options.

For supported Juniper node families, the recommendation is to reserve for ENM O&M traffic at least a DCN bandwidth of at least 1Mb/s.

## 3.5 DCN For Cisco 3PPs Nodes

ENM supports Cisco 3PP nodes.

Cisco nodes can be integrated in DCN as pure IP hosts or enabling their IP router (for example OSPF) additional functionality.

All considerations done for Router 6000 nodes are also valid for 3PPs Cisco node types.

Refer to node Cisco nodes specific 3PP technical documentation for additional details on their DCN configuration options.

For supported Cisco and Juniper node families, the recommendation is to reserve for ENM O&M traffic at least a DCN bandwidth of at least 1Mb/s.

## 3.6 ENM DCN Requirements

Following table summarizes the ENM requirements on DCN Southbound connectivity for greenfield network deployments, in terms of recommended minimal bandwidth and maximum IP latency between ENM and managed nodes:

Table 35 ENM DCN Requirements

| Node Type | Supported DCN node integration modes | DCN minumum recommended Bandwidth per node | DCN max recommended ENM Roundtrip IP latency |
|---|---|---|---|
| Router 6000 | IP host/router | 1024 Kb/s | 30 msecs |
| MINI-LINK | IP host/router | 128 Kb/s | 30 msecs |
| Juniper | IP host/router | 1024 Kb/s | 30 msecs |
| FrontHaul | IP host only | 1024 Kb/s | 30 msecs |
| Cisco | IP host/router | 1024 Kb/s | 30 msecs |

**Note:** Above table also considers the bandwidth required when **Telemetry/JTI** is enabled for **WAN-SDN Controller**.

At the ENM side, the ENM platform/hosting cloud DCN connectivity must be sized to support the overall communication channels provisioned on both Southbound and Northbound DCN connectivity.

ENM DCN Bandwidth Capacity Requirements toward External NBI Systems are summarized in the following table:

Table 36 ENM DCN Bandwidth Capacity Requirements

| Component Interaction | Protocol Used | Minimum Recommended Transmission Rate |
|---|---|---|
| ENM CM NBI and External System | TCP/IP | 128 Kb/s, per concurrent NBI client |
| ENM nbfmsnmp and External System | SNMP | 512 Kb/s (5 Mb/s in storm condition), per concurrent NBI client |
| ENM PM NBI and External System | TCP/IP | 1024 Kb/s , per concurrent NBI client |

A not complaint DCN network can affect ENM Performance KPI.

In case ENM is connected to a DCN that was previously in use with any OSS Legacy product, it is recommended to preliminary proceed with validation of the ENM target KPIs under that specific DCN scenario.

# 4 Upgrade Impacts

This section aims to provide general consideration about possible impacts on current firewalling rules related to new or updated ENM functionalities introduced by the ENM release in scope.

# References

| Doc Name | Doc Number |
|---|---|
| *ENM NIG Connectivity Matrix* | 1/102 72-aom 901 151-1 |
| *ENM Operators Guide* | 1/1553-AOM 901 151 |
| *ENM Backup and Restore System Administrator Guide* | 3/1543-aom 901 151 |
| *ENM Supported Network Elements* | 3/1029-AOM 901 151 |
| *ENM Glossary of Terms* | 1/0033-AOM 901 151 |
| *ENM System Description* | 1/1551-AOM 901 151 |
| *ENM Library Typographic Conventions* | 3/1551-FCK 101 05 |
| *ENM Security System Administrator Guide* | 2/1543-AOM 901 151 |
| *ENM Identity and Access Management System Administrator Guide* | 2/1543-aom 901 151-1 |
| *ENM Network Security Configuration System Administrator Guide* | 2/1543-aom 901 151-2 |
| *ENM Public Key Infrastructure System Administrator Guide* | 2/1543-aom 901 151-3 Uen |
| *ENM FM BNSI Northbound Interface Integration Programmers Guide* | 4/198 17-aom 901 151 Uen |