DANOS-Vyatta Edition (DVe) Cell Site Router (CSR)

Application Note

TABLE OF CONTENTS

Purpose

This document describes UFI Space S9500-30XS switches running Vyatta software as Disaggregated Cell Site Gateways (DCSGs) in a mobile backhaul network. This document also explains the deployment solution to run the mobile services through the access layer of mobile backhaul networks provisioned using this DCSGs.

This document is a deployment guide for operators interested in deploying DCSGs to run their 3G/4G/5G services in their network. The scope of this document is limited to solution design/configurations to provision mobile backhaul networks only.

Disaggregated Cell Site Gateway Overview

A DCSG provides cell site gateway/router functionality. A DCSG is typically deployed at a cell site and capable of aggregating traffic from 3G/4G/5G base stations and providing communication with other NodeB/eNB/gNB or with the operator's mobile packet core through the existing access/aggregation/core transport networks. Figure 1 shows an end-to-end high level network diagram and the location of DCSGs in the network.

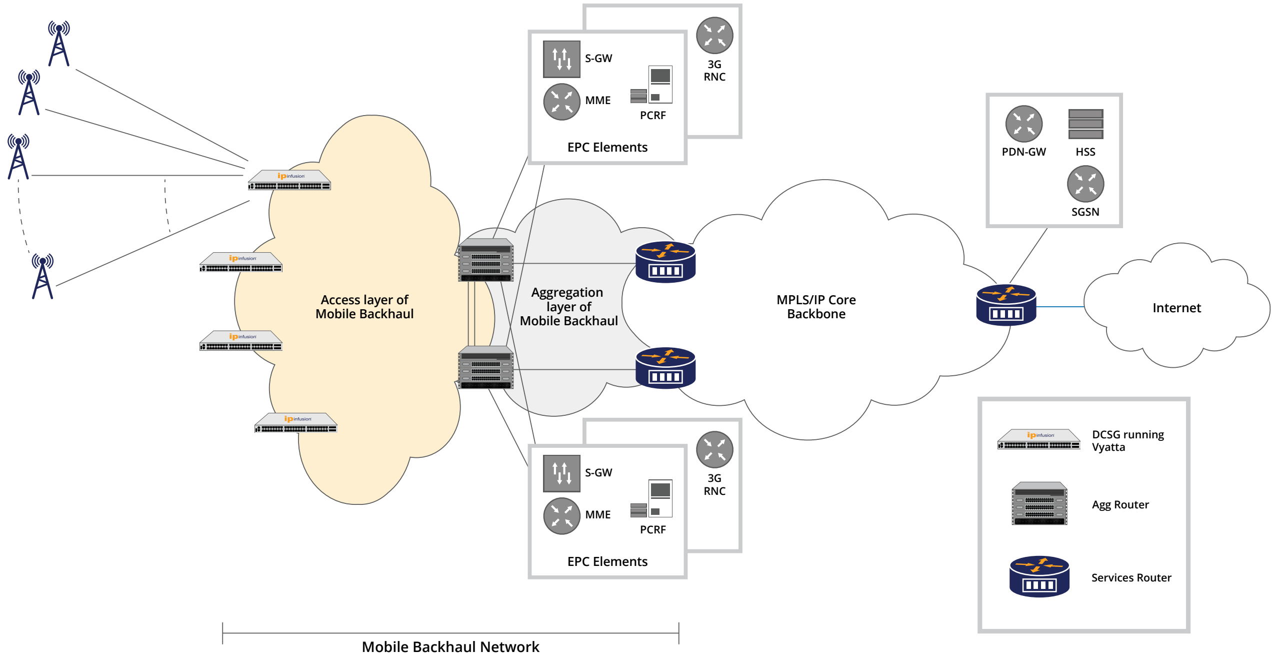


Figure 1: High Level Diagram of Mobile Backhaul Network (DCSGs in Access Network)

Note: This diagram depicts a sample backhaul network. The positioning of EPC/3G elements is not fixed and can vary between different operators' mobile backhaul networks.

Two different topologies are proposed for running Access networks with DCSGs to carry 3G/4G/5G mobile traffic.

- Access network with DCSGs dual-homed to the AGG Router (aggregation network). This can be achieved in two ways:

1. DCSGs physically connected to AGG routers and dual-homed. Access network with DCSG Physically Dual-homed to AGG shows the topology.

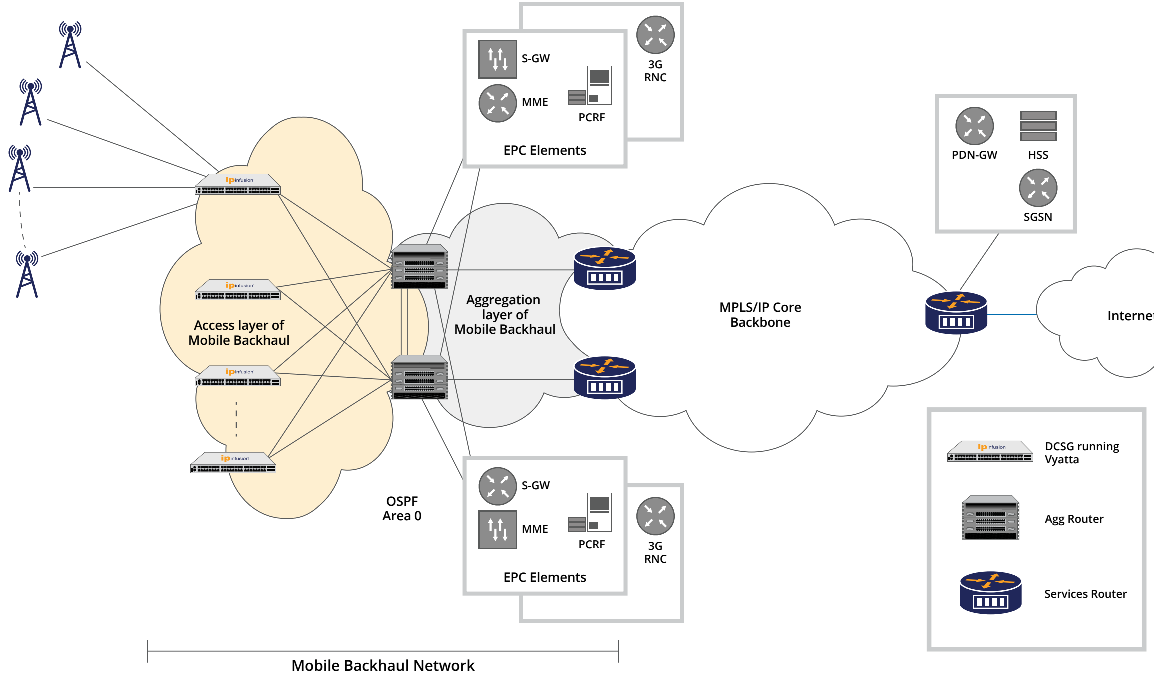


Figure 2: Access network with DCSG Physically Dual-homed to AGG

2. DCSGs logically (via L2 network) connected to AGG routers and dual-homed. Access network with DCSG dual-homed to AGG via L2 network shows the topology.

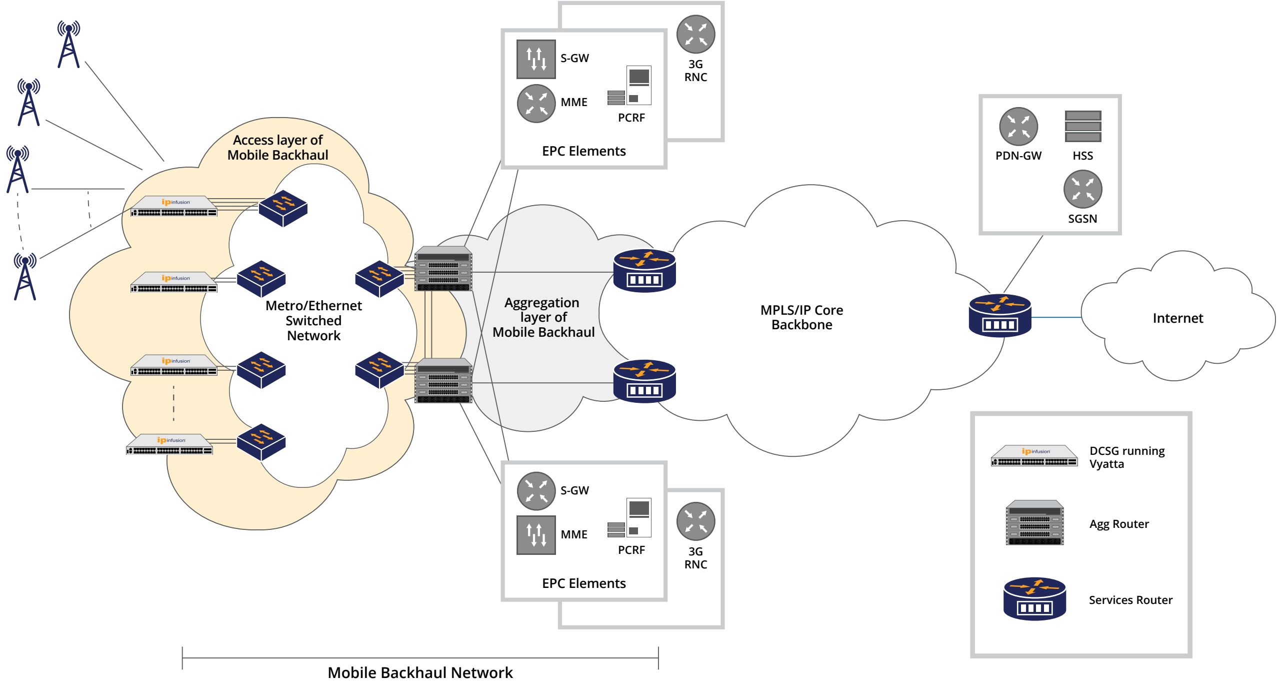
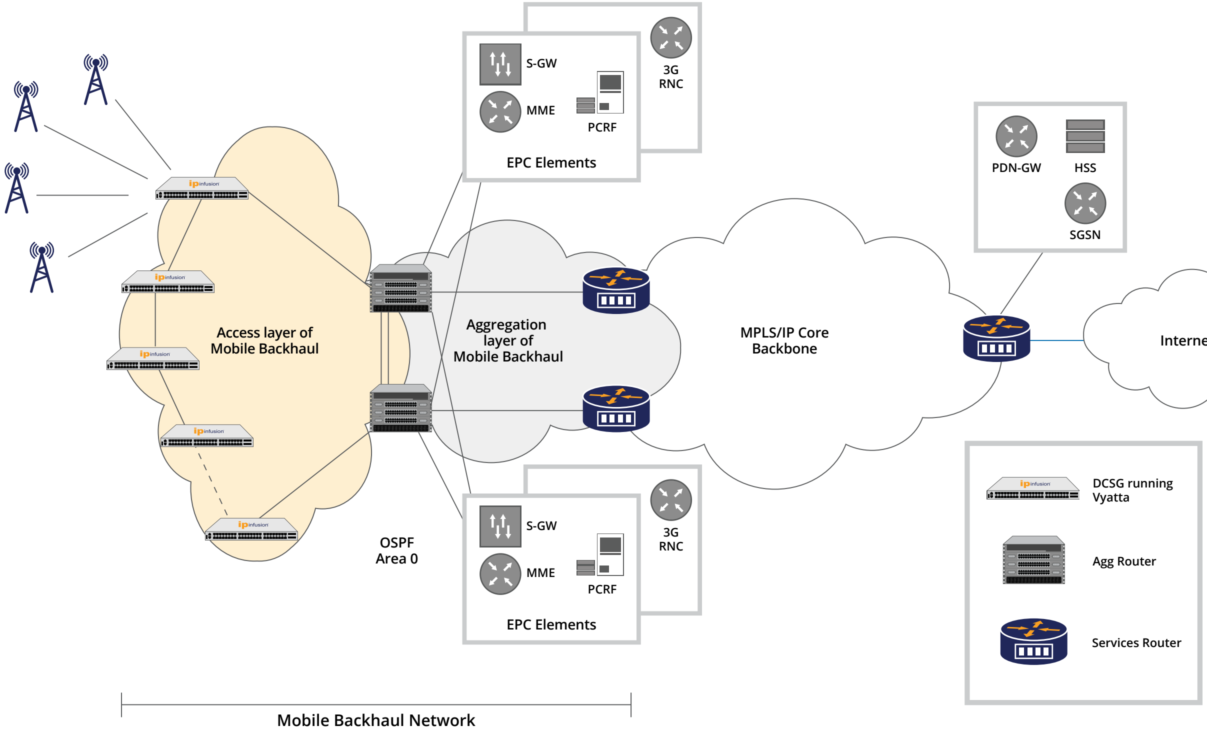


Figure 3: Access network with DCSG dual-homed to AGG via L2 network

- Access network with DCSGs in a ring connected to an AGG router (aggregation network). Access network with DCSG in a Ring shows the topology.



DCSG Deployment Solutions

DCSGs can be deployed in two different physical topologies shown in the above section. Multiple deployment solutions can be used based on the operator's requirements. This document suggests an IP-based deployment solution to provision DCSGs considering the topologies given in the previous section.

Following solutions can be used to deploy DCSGs in the access layer of mobile backhaul network.

IP Transport using IGP in a Dual Homed Environment

This option is used to provision 3G and 4G mobile services in the access network with the help of OSPFv2 and OSPFv3 as IGP. The access network is divided into non-backbone areas connecting to AGG routers which are running area-0. Non-backbone areas are realized as NSSA areas (or any form of stub areas) to limit the routing entries on the DCSGs. AGG routers can then transport the mobile traffic to the EPC elements or to the core backbone where an MPLS service can be implemented to transport this traffic to the destination.

Figure 5 shows the deployment method:

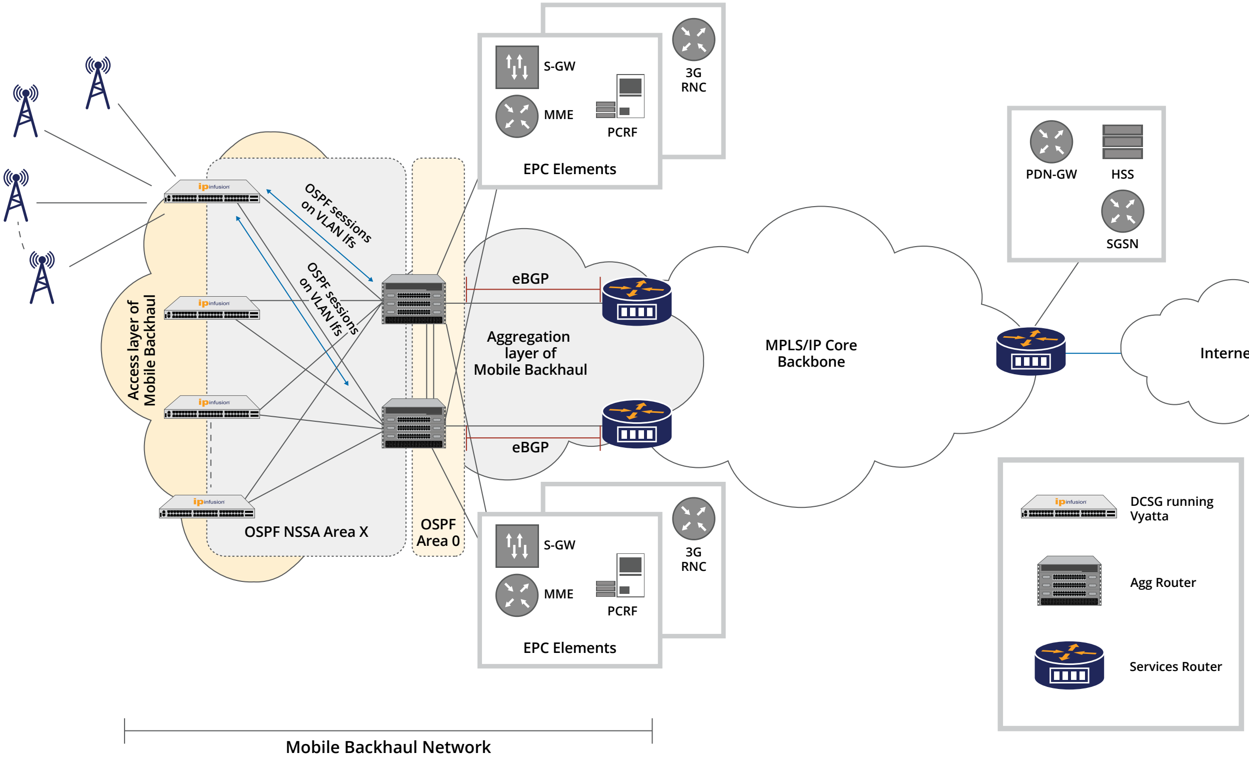


Figure 5: OSPFv2/OSPFv3 Design in dual-homed access network

IP Transport using IGP in a Dual-homed via L2-Network

This option is used to provision 3G and 4G mobile services in the access network with the help of OSPFv2 and OSPFv3 as the IGP. The access network is divided into non-backbone areas connecting to AGG routers which are running area-0. Non-backbone areas are realized as NSSA areas (or any form of stub areas) to limit the routing entries on the DCSGs. AGG routers can then transport the mobile traffic to the EPC elements or to the core backbone where an MPLS service can be used to transport this traffic to the destination. This can be considered as a subset of the above design and from DCSG perspective there is no configuration change required.

OSPFv2/OSPFv3 Design in dual-homed access via L2-network shows the deployment method:

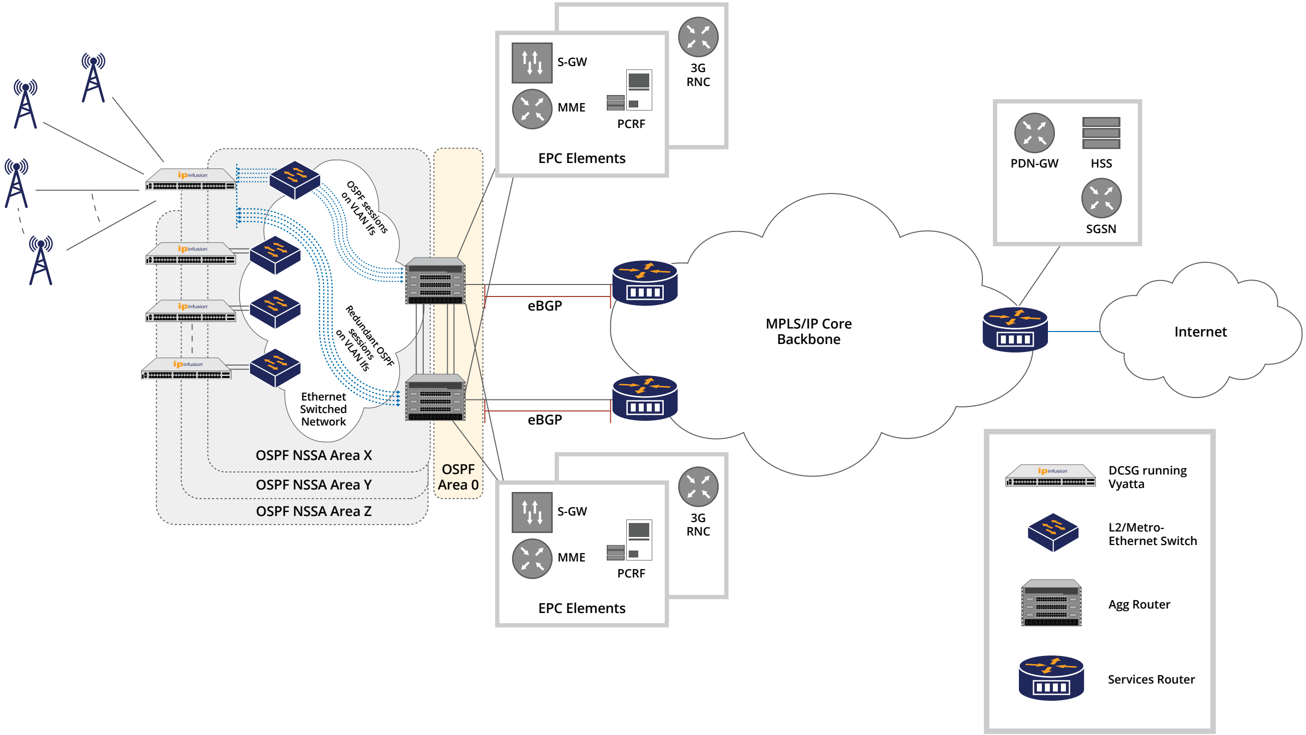


Figure 6: OSPFv2/OSPFv3 Design in dual-homed access via L2-network

IP Transport using BGP in a Dual-homed via L2-Network

This option is used to provision 3G and 4G mobile services in the access network with the help of BGP to advertise both IPv4 and IPv6 addresses of the cells to the backbone. The access network advertises all the IPv6 routes as BGP to the AGG routers, and also advertises the IPv4 addresses to the AGG. AGG routers can then transport the mobile traffic to the EPC elements or to the core backbone where an MPLS service can be used to transport this traffic to the destination.

BGP Design in dual-homed access via L2-network shows the deployment method:

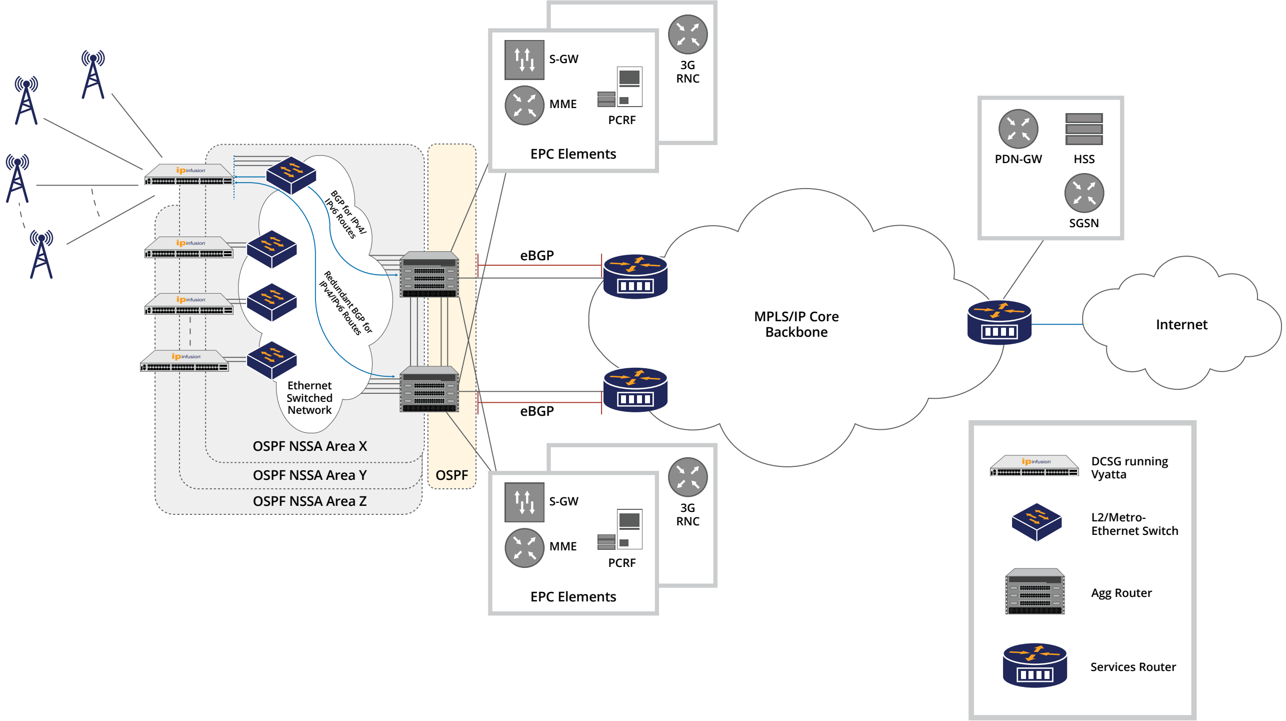


Figure 7: BGP Design in dual-homed access via L2-network

IP Transport using OSPFv2/v3 in a Ring topology

This option is used to provision 3G and 4G mobile services in the access network with the help of OSPFv2/OSPFv3. The access network is divided into non-backbone areas connecting to AGG routers which are running area-0. Non-backbone areas are realized as NSSA areas (or any form of stub areas) to limit the routing entries on the DCSGs. AGG routers can then transport the mobile traffic to the EPC elements or to the core backbone where an MPLS service can be used to transport this traffic to the destination.

OSPFv2/OSPFv3 Design in Ring based Access network shows the deployment method:

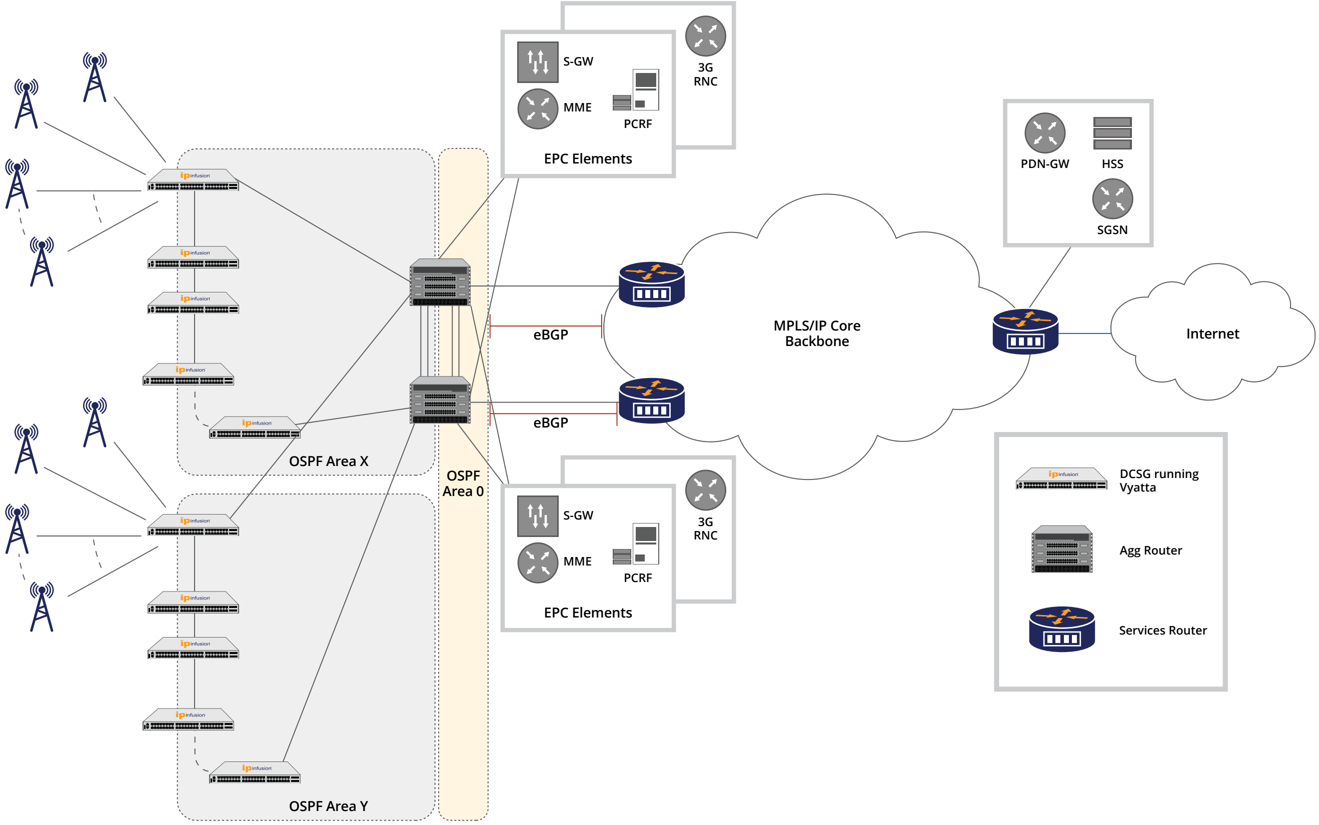


Figure 8: OSPFv2/OSPFv3 Design in Ring based Access network

DCSG Overview

Hardware

This section provides an overview of the DCSG hardware and Vyatta Software. This extract is taken from the system specification of the S9500-30XS and the full specification can be found at:

https://www.opencompute.org/documents/ufispace-csgr-s9500-30xs-system-specification-pdf

This section describes the technical specifications of the S9500-30XS switch designed for telecommunications service applications.

By providing 10GbE, 25GbE, 100GbE high speed Ethernet ports, PTP/1588V2, and SyncE timing synchronization features, the S9500-30XS switch enables service providers to deliver next-generation technologies such as 5G mobile Ethernet network which requires higher data bandwidth and more precise timing synchronization.

With temperature-hardened, high port density, high-throughput, small form factor, low-power-consumption and redundancy (PSU and fan) features, the S9500-30XS delivers high system reliability, Ethernet switching performance, and intelligence to the network edge in a flexible 1U form factor that helps reduce infrastructure and administrative costs.

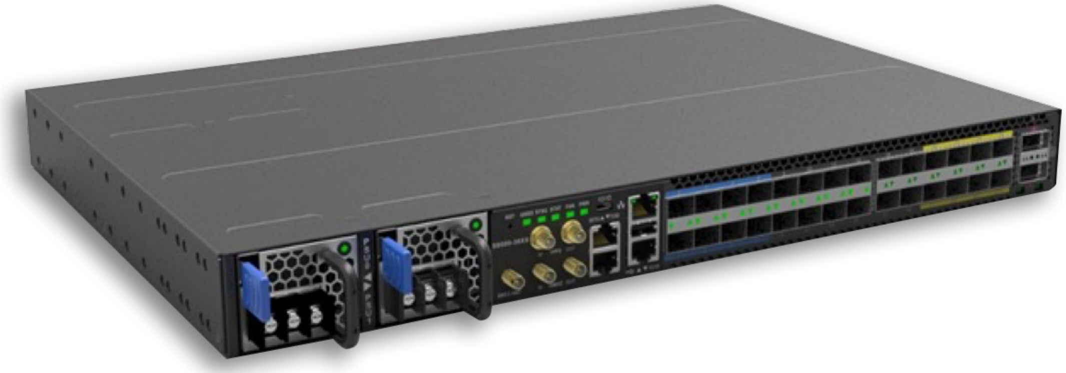


Figure 9: S9500-30XS Front view

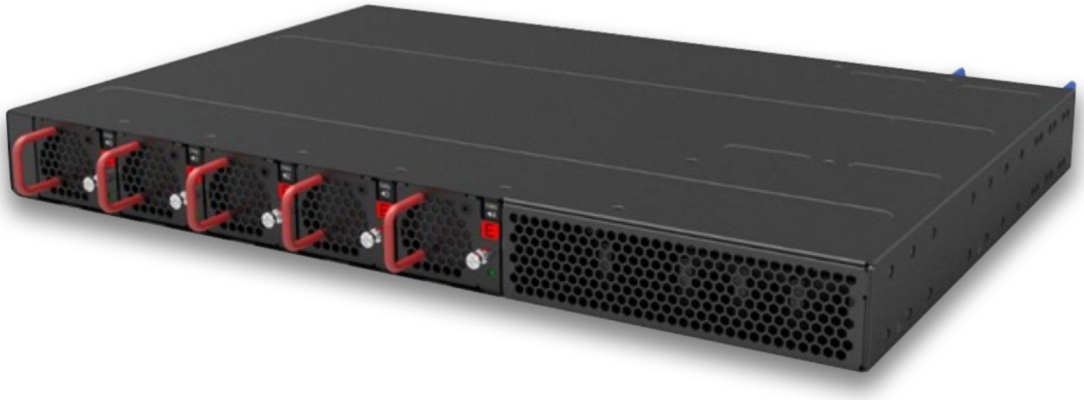


Figure 10: S9500-30XS Rear view

Switch Ports

TABLE 1-1: PORT MAPPING

PORT NUMBER	INTERFACE	MAXIMUM LINK SPEED
1	SFP+	10GbE
2	SFP+	10GbE
3	SFP+	10GbE
4	SFP+	10GbE
5	SFP+	10GbE
6	SFP+	10GbE
7	SFP+	10GbE
8	SFP+	10GbE
9	SFP+	10GbE
10	SFP+	10GbE
11	SFP+	10GbE
12	SFP+	10GbE
13	SFP+	10GbE
14	SFP+	10GbE
15	SFP+	10GbE
16	SFP+	10GbE
17	SFP+	10GbE
18	SFP+	10GbE
19	SFP+	10GbE
20	SFP+	10GbE
21	SFP28	25GbE
22	SFP28	25GbE
23	SFP28	25GbE
24	SFP28	25GbE
25	SFP28	25GbE
26	SFP28	25GbE
27	SFP28	25GbE
28	SFP28	25GbE
29	QSFP28	100GbE
30	QSFP28	100GbE

Management interfaces

- 1 x GbE OOB management port (CPU)
- 1 x USB2.0 Type-A general purpose port
- 1 x RS232 console port in RJ45 form factor
- 1 x USB console port in Micro USB form factor
- 1 x tact switch for system reset/reload default configuration

Clocking and Timing ports

- E1/T1
- ToD
- 1PPS and 10MHz

GPS Antenna

- 1XGNSS/GPS

Key Components

Switch Silicon

- 1 x MAC Qumran-AX BCM88470
- 6 x 512MB DDR4 SDRAM @ 1200MHz
- 1 x Octal port 10GbE PHY BCM82780F
- 1 x Dual port 100GbE PHY BCM82398
- 1 x management CPLD 10M04SAU169I7G
- 1 x PCIe NIC controller I210-IT for CPU
- 1 x SyncE and IEEE 1588 DPLL 82P33831
- 1 x Clock jitter attenuator buffer Si5344D
- 1 x GNSS/GPS module NEO-M8T
- 1 x T1/E1 transceiver 82P2281

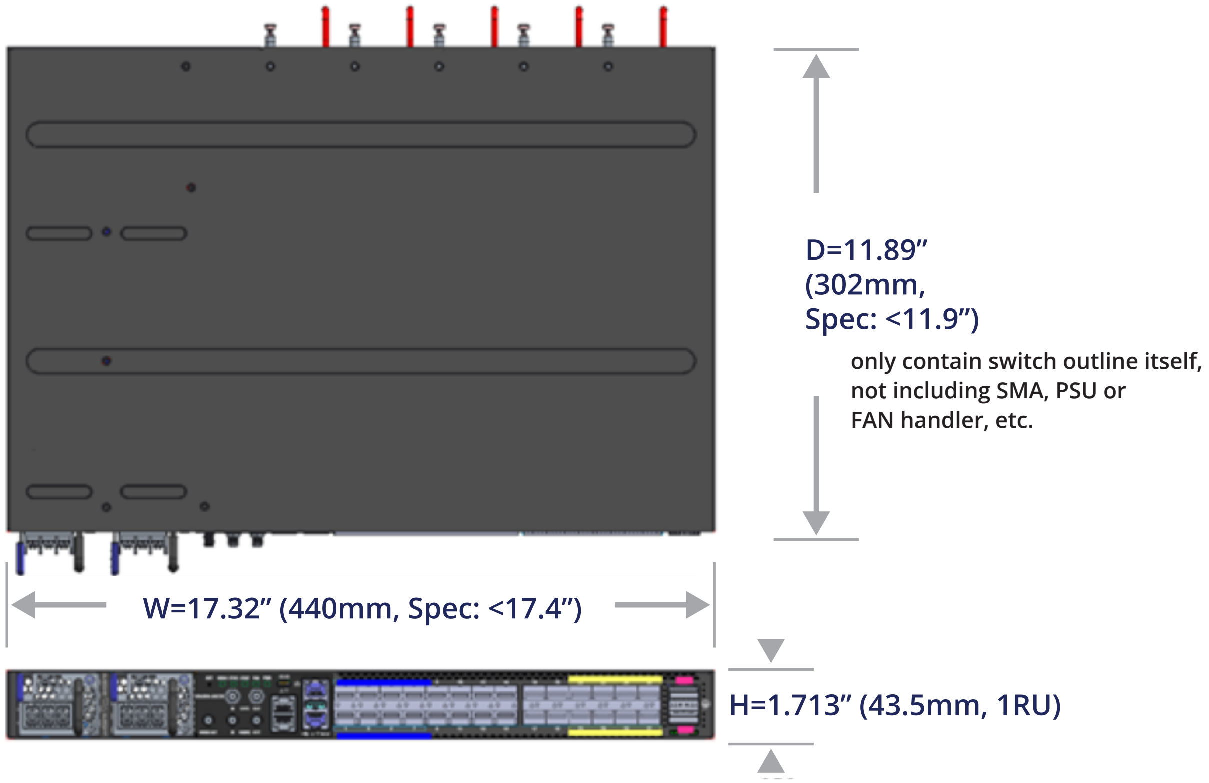
CPU Modules

- 1 x CPU Broadwell-DE D-1519 with quad core @ 1.5GHz
- 2 x 8GB DDR4 SODIMM memory module with ECC support
- 1 x 128GB SATA3 M.2 SSD Memory module

Physical and Environmental

S9500-30XS chassis is designed to meet cabinet with 19" depth installation requirement. This 1 Rack Unit (RU) system mechanical dimension is: 440mm (W) x 302mm (D) x 43.5mm (H).

TABLE 1-2: DIMENSIONS		
DIMENSION	INCHES	MILLIMETERS
Length	11.89	302
Width	17.32	440
Height	1.73	43.5



only contain switch outline itself, not including SMA, PSU or FAN handler, etc.

Figure 11: S9500-30XS Mechanical Outline

Power and FRUs

- 1+1 redundant power supply unit
- 400W output
- -36~72V DC input
- Field replaceable
- 4+1 redundant fan module
- 25000 RPM
- Front to back air flow
- Field replaceable

System LEDs

- Front/Real panel LED indicators:
- 1 x power status LED
- 1 x FAN status LED
- 1 x system status LED
- 1 x synchronization status LED
- 1 x GNSS\GNSS status LED
- Per port FAN status LED
- Per port PSU status LED
- Per port link status LED

Efficiency

The cell site gateway router adopts x86, BMC, switching and timing 4 subsystems in a compact pizza box, with temperature-hardened, high port density, high-throughput, low packet latency, power and cooling redundancy, full 1588V2 and SyncE synchronization functions, and self hardware management features, the CSGR enables lower infrastructure cost and higher TEER(4Gbps/W) for both indoor and outdoor 5G application.

Scalability

With automatic provisioning and remote management features, the cell site gateway router enables carrier/service providers to deploy large scale disaggregated open network infrastructure for various 5G mobile network access applications. Components with firmware/software inside the box are 100% online programmable, easy to maintain this equipment and upgrade service rapidly.

Software

The access network consists of the DCSGs interconnected in a ring or a Dual-homed topologies. The DCSGs are configured with 1/10GE/25GE.

The DCSG has the following high-level functionalities

IP Based Routing Protocols (Static/OSPFv2/OSPFv3/BGP with multi-protocol extensions)

- BFD support for all Routing protocols. BFD is Software Offloaded.
- Layer-2 Bridging support.
- Layer-3 SVIs support for IP Termination on the box. Both IPv4 and IPv6 support is available.
- Link aggregation or Bonding
- Layer-3 Equal Cost Multiple Path support.
- IP ACLs support (IPv4 and IPv6).
- Quality of Service (classification, marking, scheduling and Egress-shaping)
- IEEE1588 full-timing support profile (phase/time distribution) using Telecom Boundary Clock

- Ring topology and Dual-homed topology support
- 25GE interface speed
- Software upgrade / downgrade
- Zero Touch Provisioning
- NetConf
- TACACS+/RADIUS/Syslog
- SNMP
- TWAMP

Reference Topology

Reference Topology for Vyatta Based DCSG solution for Mobile Transport shows an example backhaul network which is used as a reference throughout this document to describe design and configurations. The network shown below is divided into different logical segments called “access”, “aggregation”, and “core” throughout this document. The access network consists of the DCSGs interconnected in a dual-homed topology with connections to both the AGGs in the aggregation network. The DCSGs are UFI Space S9500-30XS running Vyatta OS and are configured with 1/10GE interfaces towards the base station and 10GE/25GE/100GE towards the aggregation network (Note: The 25GE/100GE ports were not used for preparing this solution). The DCSG are powered by an AC power supply. The aggregation routers in Reference Topology for Vyatta Based DCSG solution for Mobile Transport are running IP Infusion’s OcNOS for creating this solution design. An Ixia traffic tester generates and captures traffic. Calnex Paragon-X is used to run IEEE1588-2008/PTP 1588v2 Master Clock in addition to capturing performance results.

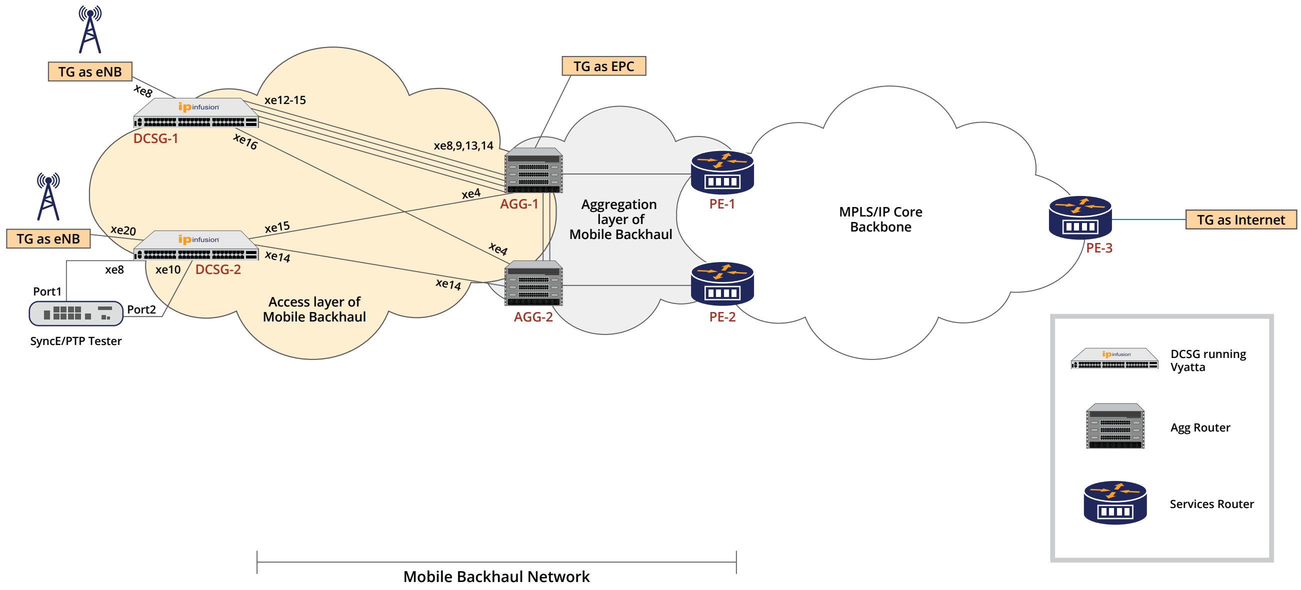


Figure 12: Reference Topology for Vyatta Based DCSG solution for Mobile Transport

Note: This solution guide only presents configurations for DCSGs running Vyatta software and other configurations are not in the scope of this document.

Design and Physical Connectivity

As shown in Reference Topology for Vyatta Based DCSG solution for Mobile Transport, the entire network is divided into an access layer (consisting of the DCSGs), an aggregation layer, and a core layer.

- The access layer consists of DCSGs. The network topology can be either a ring or a dual-homed to the aggregation routers. The access network is running OSPFv2 on DCSGs S9500-30XS running Vyatta software as an NSSA area.
- The aggregation layer consists of AGG aggregating traffic from the access layer. For this network, the AGG routers are running IP Infusion's OcNOS software.
- The core layer is an existing network which connects NodeBs/eNBs/gNBs, RNCs/MME/SGW, and so on to the Internet. For this network, the core network routers (PE-1, PE-2, and PE-3) are running IP Infusion's OcNOS software.

Physical Interface

The physical connectivity in the access network is done with the 10G links dual homed to AGG1 and AGG2. All physical connectivity to the eNB (TG simulating NodeB/eNB/gNB) are 10G links from DCSG.

AGG1 and AGG2 connections to PE-1, PE-2 are 10G physical connections in this design.

A traffic generator is used for traffic and a master clock generator and PTP packet generator are used for frequency/phase/time generation and measurement.

Designing Interconnected Interfaces using L3

Design Guidelines

- The physical interfaces in the access network are an L3 interface bound in the DCSG and on the AGG.

The interfaces are created and IPv4 and IPv6 addresses are assigned to them.

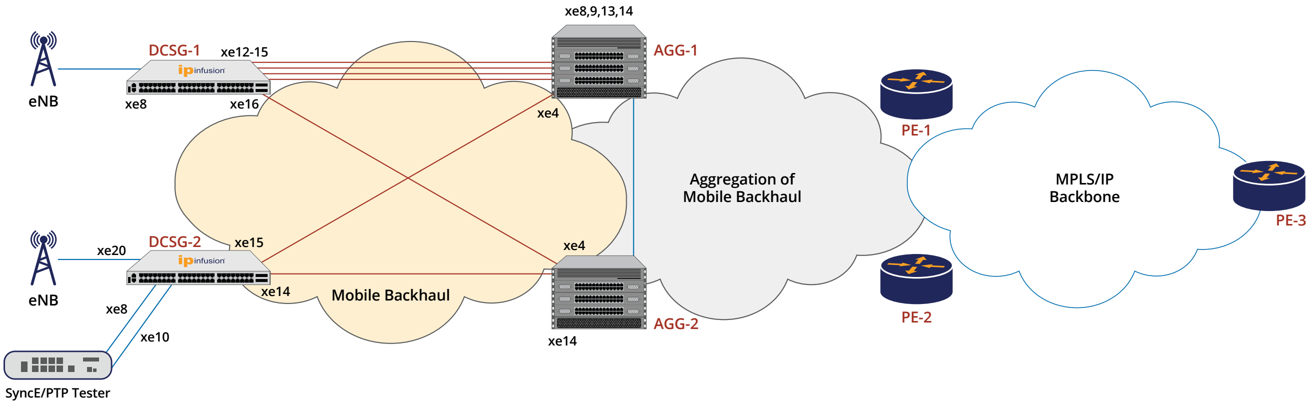


Figure 13: DCSG Configured with L3 interfaces

Design Results

- On DCSG-1 and DCSG-2, physical interfaces connected to AGG devices configured as Layer-3

TABLE 1-3: INTERCONNECTED INTERFACE

LOCAL SITE	PHYSICAL INTERFACE NAME	REMOTE SITE	REMOTE INTERFACE NAME
DCSG-1	dp0xe12	AGG-1	dp0xe8
DCSG-1	dp0xe13	AGG-1	dp0xe9
DCSG-1	dp0xe14	AGG-1	dp0xe13
DCSG-1	dp0xe15	AGG-1	dp0xe14
DCSG-1	dp0xe16	AGG-2	dp0xe4
DCSG-2	dp0xe15	AGG-1	dp0xe4
DCSG-2	dp0xe14	AGG-2	dp0xe14

Configurations and Validations

DCSG-1

```
set system platform type router
set interfaces dataplane dp0xe12 speed 10g
set interfaces dataplane dp0xe13 speed 10g
set interfaces dataplane dp0xe14 speed 10g
set interfaces dataplane dp0xe15 speed 10g
set interfaces dataplane dp0xe16 speed 10g
```

DCSG-2

```
set system platform type router
set interfaces dataplane dp0xe14 speed 10g
set interfaces dataplane dp0xe15 speed 10g
```

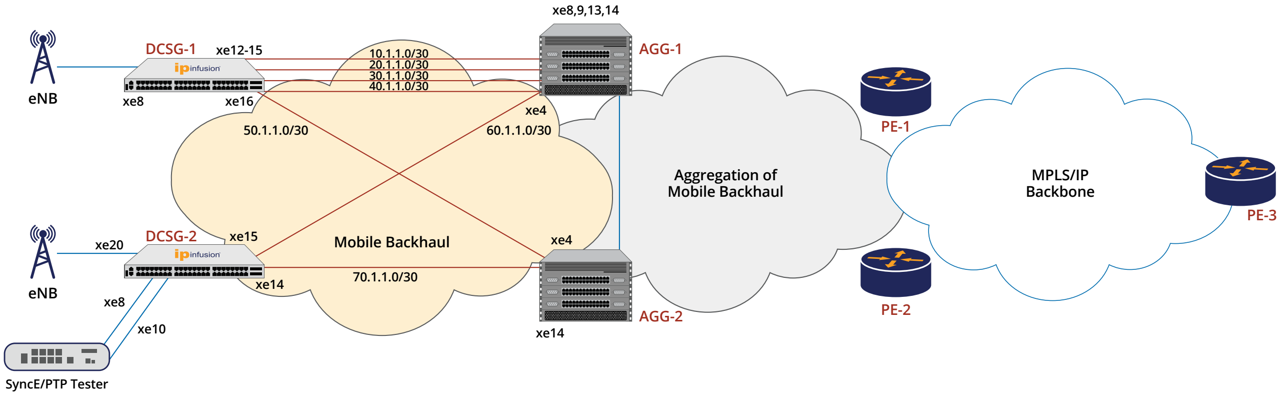


Figure 14: DCSG Configured with IPv4 Addresses

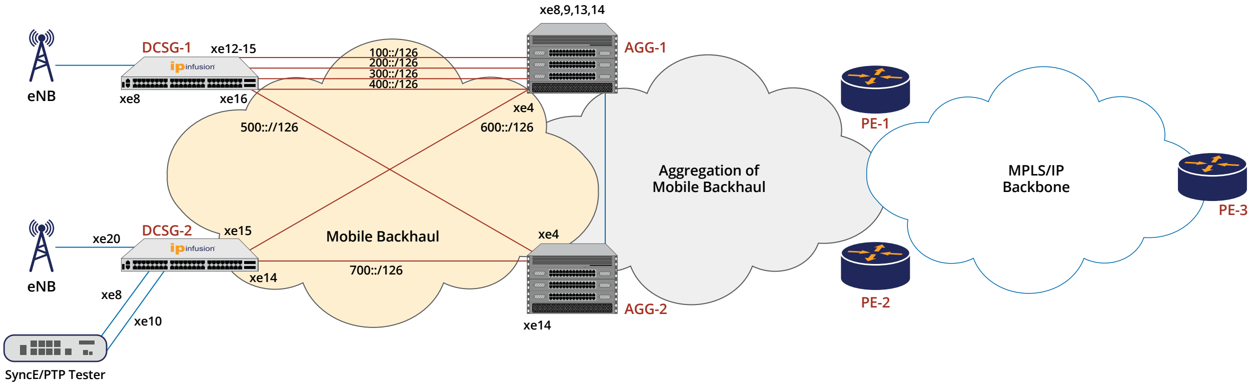


Figure 15: DCSG Configured with IPv6 Addresses

Design Guidelines

- The physical interfaces in the access network are an L3 interface in the DCSG and on the AGG.
- Interfaces are created and IPv4 and IPv6 addresses are assigned to them.
- The address of an interconnected interface uses a 30-bit mask for ipv4 and 126-bit mask for ipv6.
- The addresses of interconnected interfaces are allocated from the core layer (already existing), then the aggregation layer (only links connecting to DCSGs are configured), and finally to the access layer. The values are in ascending order.

Design Results

TABLE 1-4: INTERCONNECTED INTERFACE IPV4 ADDRESSES

LOCAL SITE	PHYSICAL INTERFACE NAME	IP ADDRESS PREFIX	REMOTE SITE	REMOTE INTERFACE NAME	REMOTE IP ADDRESS PREFIX
DCSG-1	dp0xe12	10.1.1.1/30	AGG-1	dp0xe8	10.1.1.2/30
DCSG-1	dp0xe13	20.1.1.1/30	AGG-1	dp0xe9	20.1.1.2/30
DCSG-1	dp0xe14	30.1.1.1/30	AGG-1	dp0xe13	30.1.1.2/30
DCSG-1	dp0xe15	40.1.1.1/30	AGG-1	dp0xe14	40.1.1.2/30
DCSG-1	dp0xe16	50.1.1.1/30	AGG-2	dp0xe4	50.1.1.2/30
DCSG-2	dp0xe15	60.1.1.1/30	AGG-1	dp0xe4	60.1.1.2/30
DCSG-2	dp0xe14	70.1.1.1/30	AGG-2	dp0xe14	70.1.1.2/30

TABLE 1-5: INTERCONNECTED INTERFACE IPV6 ADDRESSES					
LOCAL SITE	PHYSICAL INTERFACE NAME	IP ADDRESS PREFIX	REMOTE SITE	REMOTE INTERFACE NAME	REMOTE IP ADDRESS PREFIX
DCSG-1	dp0xe12	100::1/126	AGG-1	dp0xe8	100::2/126
DCSG-1	dp0xe13	200::1/126	AGG-1	dp0xe9	200::2/126
DCSG-1	dp0xe14	300::1/126	AGG-1	dp0xe13	300::2/126
DCSG-1	dp0xe15	400::1/126	AGG-1	dp0xe14	400::2/126
DCSG-1	dp0xe16	500::1/126	AGG-2	dp0xe4	500::2/126
DCSG-2	dp0xe15	600::1/126	AGG-1	dp0xe4	600::2/126
DCSG-2	dp0xe14	700::1/126	AGG-2	dp0xe14	700::2/126

Configurations and Validations

DCSG-1

```
set interface dataplane dp0xe12 address 10.1.1.1/30
set interface dataplane dp0xe12 address 100::1/26
set interfaces dataplane dp0xe13 address 20.1.1.1/30
set interfaces dataplane dp0xe13 address ‘200::1/126’
set interfaces dataplane dp0xe14 address 30.1.1.1/30
set interfaces dataplane dp0xe14 address ‘300::1/126’
set interfaces dataplane dp0xe15 address 40.1.1.1/30
set interfaces dataplane dp0xe15 address ‘400::1/126’
set interfaces dataplane dp0xe16 address 50.1.1.1/30
set interfaces dataplane dp0xe16 address ‘500::1/126’
```

DCSG-2

```
set interfaces dataplane dp0xe15 address 60.1.1.1/30
set interfaces dataplane dp0xe15 address ‘600::1/126’
set interfaces dataplane dp0xe14 address 70.1.1.1/30
set interfaces dataplane dp0xe14 address ‘700::1/126’
```

Designing Loopback Interface IP Addresses

Design Guidelines

- The address of a loopback interface uses a 32-bit mask.
- Loopback 0 is used as the router ID of OSPF, router ID of BGP, and LSR ID.

Design Results

TABLE 1-6: LOOPBACK INTERFACE ADDRESSES			
ROUTER	INTERFACE NAME	IP ADDRESS PREFIX	IPV6 ADDRESS PREFIX
DCSG-1	Lo	1.1.1.1	::1:1:1:1/128
DCSG-2	Lo	2.2.2.2	::2:2:2:2/128

Configuration and Validations

DCSG-1

```
set interfaces loopback lo address 1.1.1.1/32
set interfaces loopback lo address '::1:1:1:1/128'
```

DCSG-2

```
set interfaces loopback lo address 2.2.2.2/32
set interfaces loopback lo address '::2:2:2:2/128'
```

Designing Service VLANs

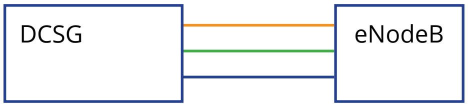
Design Guidelines

- Access-layer VLANs indicate service types. To facilitate daily maintenance, the services of the same type from different base stations are configured with the same VLAN ID. That is, each service carries a unique VLAN ID.

Access Layer

One interface (VLAN interface, colored as below) for eNodeB.

Note: Below example is shown on two DCSGs (DCSG-1 and DCSG-2 in this case). The same can be implemented on all DCSGs. Make IP addresses unique while designing BTS/eNB-side design because everything is under the default VRF.



Design results of access VLANs

TABLE 1-7: DCSG-1

NB/ENB	VLANS	IPV4 ADDRESS	IPV6 ADDRESS	SERVICE TYPE
NB	1000	150.1.1.1/30	1000::1/126	Iub
eNB	1001	151.1.1.1/30	1001::1/126	S1
eNB	1002	152.1.1.1/30	1002::1/126	X2

TABLE 1-8: DCSG-2

NB/ENB	VLANS	IPV4 ADDRESS	IPV6 ADDRESS	SERVICE TYPE
NB	1000	160.1.1.1/30	2000::1/126	Iub
eNB	1001	161.1.1.1/30	2001::1/126	S1
eNB	1002	162.1.1.1/30	2002::1/126	X2

Configuration and Validation

Service VLAN DCSG-1

```
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1000
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1001
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1002
set interfaces dataplane dp0xe8 speed 10g
set interfaces dataplane dp0xe8 switch-group port-parameters mode trunk
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1000
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1001
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1002
set interfaces dataplane dp0xe8 switch-group switch sw0
set interfaces switch sw0 vif 1000 address 150.1.1.1/30
set interfaces switch sw0 vif 1000 address ‘1000::1/126’
set interfaces switch sw0 vif 1000 description 3G-Iub
set interfaces switch sw0 vif 1001 address 151.1.1.1/30
set interfaces switch sw0 vif 1001 address ‘1001::1/126’
set interfaces switch sw0 vif 1001 description 4G-S1
set interfaces switch sw0 vif 1002 address 152.1.1.1/30
set interfaces switch sw0 vif 1002 address ‘1002::1/126’
set interfaces switch sw0 vif 1002 description 4G-X2
```

Service VLAN DCSG-2

```
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1000
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1001
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1002
set interfaces dataplane dp0xe20 speed 10g
set interfaces dataplane dp0xe20 switch-group port-parameters mode trunk
set interfaces dataplane dp0xe20 switch-group port-parameters vlan-parameters vlans 1000
set interfaces dataplane dp0xe20 switch-group port-parameters vlan-parameters vlans 1001
set interfaces dataplane dp0xe20 switch-group port-parameters vlan-parameters vlans 1002
set interfaces dataplane dp0xe20 switch-group switch sw0
set interfaces switch sw0 vif 1000 address 160.1.1.1/30
set interfaces switch sw0 vif 1000 address ‘2000::1/126’
set interfaces switch sw0 vif 1000 description 3G-Iub
set interfaces switch sw0 vif 1001 address 161.1.1.1/30
set interfaces switch sw0 vif 1001 address ‘2001::1/126’
set interfaces switch sw0 vif 1001 description 4G-S1
set interfaces switch sw0 vif 1002 address 162.1.1.1/30
set interfaces switch sw0 vif 1002 address ‘2002::1/126’
set interfaces switch sw0 vif 1002 description 4G-X2
```

Designing Transport OSPFv2 and OSPFv3

Overview

- OSPFv2 and OSPFv3 have two areas of which the backbone area (area 0) consists of an aggregation domain and the non-backbone area consists of all access domains.
- Non-backbone area is an NSSA area to reduce the number of routing entries in the FIB on DCSGs. Thus, only a default route is advertised by the ABR (AGG-1 or AGG-2) to all the DCSGs in the NSSA area.
- A pair of AGG routers in the backbone area can connect to multiple non-backbone NSSA areas or access domains.
- OSPF authentication is configured with key-chain and crypto-algorithm as md5.
- BFD runs on the interface between the DCSGs and the AGG routers with timers of 150x3 (this can be changed based on the requirement).
- All AGG routers have specific routes of BTS/eNB/gNBs and DCSGs installed using OSPFv2 and OSPFv3.

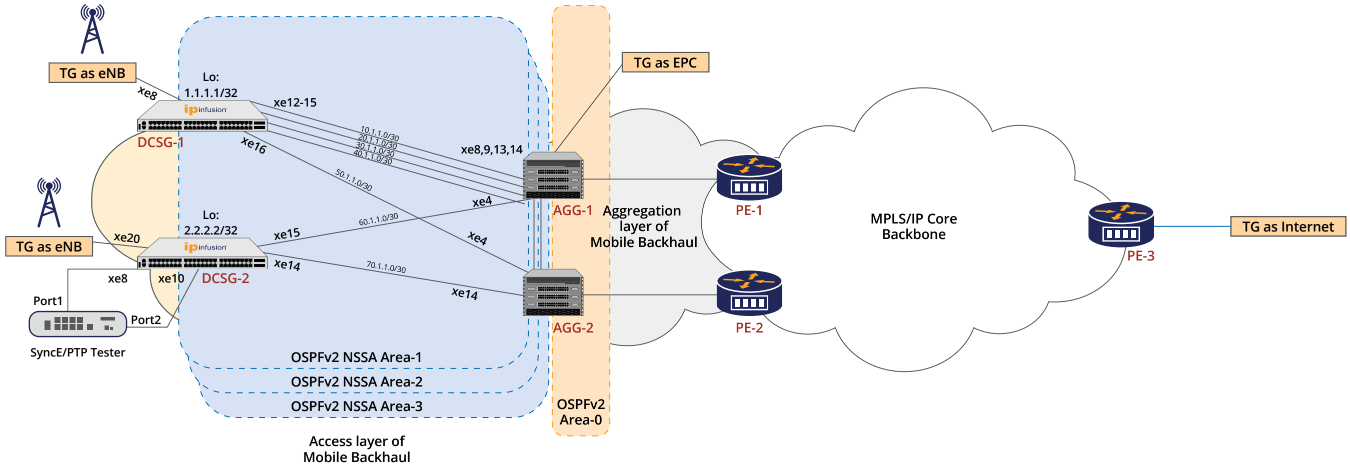


Figure 16: OSPFv2 Logical Topology

Note: MD5 cryptographic-algorithm for key-chain is not supported for OSPFv3.

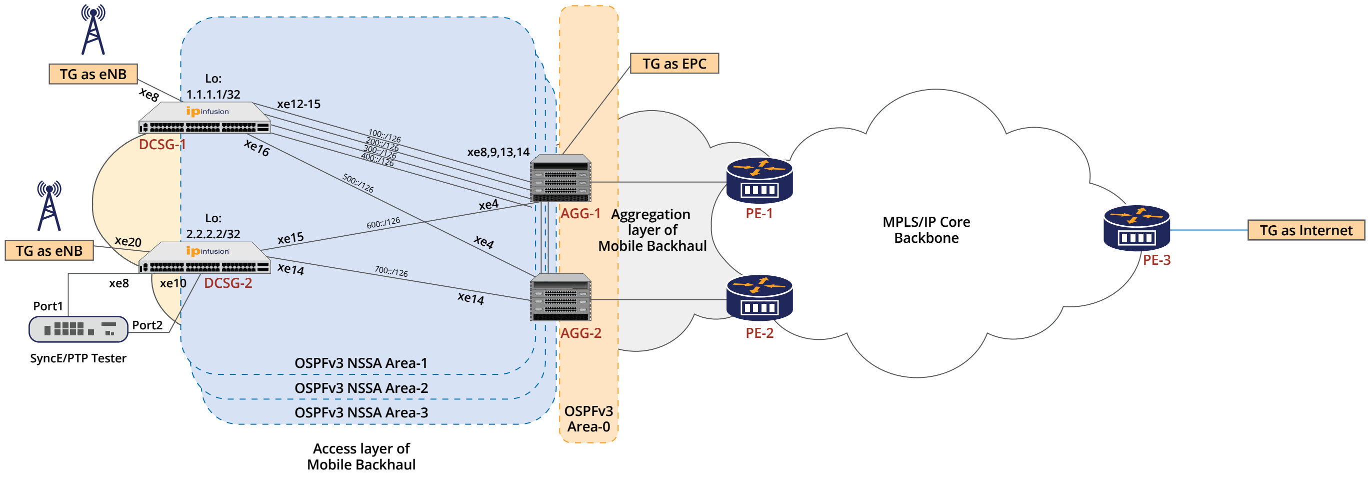


Figure 17: OSPFv3 Logical Topology

Designing Basic Functions

TABLE 1-9: OSPFV2 AND OSPFV3 BASIC FUNCTIONS	
PARAMETER	**DESIGN GUIDELINES**
OSPF process ID/Routing instance	Default process
Router ID	Loopback interface address
OSPF area ID	Non-backbone
Area type	NSSA
Route mask of the network segment included in an area	For IPv4 /30 for connected interfaces /32 for loopback interfaces For IPv6 /126 for connected interfaces /128 for loopback interfaces
Route redistribute	From non OSPF routing domain (if required)
BFD	Enable BFD with 20X3 on all interfaces

Designing Basic Functions for ECMP

Design Guidelines

- All the connected interfaces are enabled for OSPFv2 and OSPFv3.
- Loopback interfaces are configured as passive-interfaces for OSPFv2 and OSPFv3.
- All interfaces are configured as point-to-point.
- This gives multiple next-hops for IPv4 and IPv6 prefixes and all traffic would be load-balanced based on the configured algorithm.

Configuration and Validation

DCSG-1 Configuration for OSPFv2

```
set security key-chains key-chain dcsg key 1 crypto-algorithm md5
set security key-chains key-chain dcsg key 1 key-string keystring dcsg
set protocols ospf area 1 area-type nssa
set protocols ospf area 1 network 1.1.1.1/32
set protocols ospf area 1 network 10.1.1.0/30
set protocols ospf area 1 network 20.1.1.0/30
set protocols ospf area 1 network 30.1.1.0/30
set protocols ospf area 1 network 40.1.1.0/30
set protocols ospf area 1 network 50.1.1.0/30
set protocols ospf parameters router-id 1.1.1.1
set protocols ospf passive-interface lo
set interfaces dataplane dp0xe12 ip ospf network point-to-point
set interfaces dataplane dp0xe12 ip ospf authentication key-chain dcsg
set interfaces dataplane dp0xe13 ip ospf network point-to-point
set interfaces dataplane dp0xe13 ip ospf authentication key-chain dcsg
set interfaces dataplane dp0xe14 ip ospf network point-to-point
set interfaces dataplane dp0xe14 ip ospf authentication key-chain dcsg
set interfaces dataplane dp0xe15 ip ospf network point-to-point
set interfaces dataplane dp0xe15 ip ospf authentication key-chain dcsg
set interfaces dataplane dp0xe16 ip ospf network point-to-point
set interfaces dataplane dp0xe16 ip ospf authentication key-chain dcsg

set interfaces dataplane dp0xe12 ip ospf fall-over bfd
set interfaces dataplane dp0xe13 ip ospf fall-over bfd
set interfaces dataplane dp0xe14 ip ospf fall-over bfd
set interfaces dataplane dp0xe15 ip ospf fall-over bfd
set interfaces dataplane dp0xe16 ip ospf fall-over bfd
```

DCSG-2 Configuration for OSPFv2

```
set security key-chains key-chain dcsg key 1 crypto-algorithm md5
set security key-chains key-chain dcsg key 1 key-string keystring dcsg
set protocols ospf area 1 area-type nssa
set protocols ospf area 1 network 2.2.2.2/32
set protocols ospf area 1 network 60.1.1.0/30
set protocols ospf area 1 network 70.1.1.0/30
set protocols ospf parameters router-id 2.2.2.2
set protocols ospf passive-interface lo
set interfaces dataplane dp0xe15 ip ospf network point-to-point
set interfaces dataplane dp0xe15 ip ospf authentication key-chain dcsg
set interfaces dataplane dp0xe14 ip ospf network point-to-point
set interfaces dataplane dp0xe14 ip ospf authentication key-chain dcsg
set interfaces dataplane dp0xe15 ip ospf fall-over bfd
set interfaces dataplane dp0xe14 ip ospf fall-over bfd
```

DCSG-1 Configuration for OSPFv3

```
set protocols ospfv3 area 1 nssa
set protocols ospfv3 router-id 1.1.1.1
set interfaces dataplane dp0xe12 ipv6 ospfv3 area 1
set interfaces dataplane dp0xe13 ipv6 ospfv3 area 1
set interfaces dataplane dp0xe14 ipv6 ospfv3 area 1
set interfaces dataplane dp0xe15 ipv6 ospfv3 area 1
set interfaces dataplane dp0xe16 ipv6 ospfv3 area 1

set interfaces loopback lo ipv6 ospfv3 area 1
set protocols ospfv3 passive-interface lo
set interfaces dataplane dp0xe12 ipv6 ospfv3 network point-to-point
set interfaces dataplane dp0xe13 ipv6 ospfv3 network point-to-point
set interfaces dataplane dp0xe14 ipv6 ospfv3 network point-to-point
set interfaces dataplane dp0xe14 ipv6 ospfv3 network point-to-point
set interfaces dataplane dp0xe15 ipv6 ospfv3 network point-to-point

set interfaces dataplane dp0xe12 ipv6 ospfv3 fall-over bfd
set interfaces dataplane dp0xe13 ipv6 ospfv3 fall-over bfd
set interfaces dataplane dp0xe14 ipv6 ospfv3 fall-over bfd
set interfaces dataplane dp0xe15 ipv6 ospfv3 fall-over bfd
set interfaces dataplane dp0xe16 ipv6 ospfv3 fall-over bfd
```

DCSG-2 Configuration for OSPFv3

```
set protocols ospfv3 area 1 nssa
set protocols ospfv3 router-id 1.1.1.1
set interfaces dataplane dp0xe15 ipv6 ospfv3 area 1
set interfaces dataplane dp0xe14 ipv6 ospfv3 area 1
set interfaces loopback lo ipv6 ospfv3 area 1
set protocols ospfv3 passive-interface lo
set interfaces dataplane dp0xe15 ipv6 ospfv3 network point-to-point
set interfaces dataplane dp0xe14 ipv6 ospfv3 network point-to-point
set interfaces dataplane dp0xe15 ipv6 ospfv3 fall-over bfd
set interfaces dataplane dp0xe14 ipv6 ospfv3 fall-over bfd
```

DCSG-1 Configuration for BFD

```
set protocols bfd template vyatta minimum-rx 20
set protocols bfd template vyatta minimum-tx 20
set protocols bfd template vyatta multiplier 3
set interfaces dataplane dp0xe12 bfd template vyatta
set interfaces dataplane dp0xe13 bfd template vyatta
set interfaces dataplane dp0xe14 bfd template vyatta
set interfaces dataplane dp0xe15 bfd template vyatta
set interfaces dataplane dp0xe16 bfd template vyatta
```

DCSG-2 Configuration for BFD

```
set protocols bfd template vyatta minimum-rx 20
set protocols bfd template vyatta minimum-tx 20
set protocols bfd template vyatta multiplier 3
set interfaces dataplane dp0xe14 bfd template vyatta
set interfaces dataplane dp0xe15 bfd template vyatta
```

Designing transport using BGP

Overview of BGP for IPv4 and IPv6

BGP IPv4 and IPv6 route advertisement in the access layer:

- iBGP can learn IPv4 and IPv6 BTS/eNB/gNB routes in the core and have DCSGs learn a default route from the AGG
- To achieve ECMP, the same route is learned by BGP from different sessions and max-paths are configured to control the number of ECMP paths.
- BFD is used for fast failover detection and therefore better convergence.
- The AGG can be configured to only send default route towards the DCSG. This also helps minimize the routing table in DCSG and facilitate the X2 connection for a 4G service.

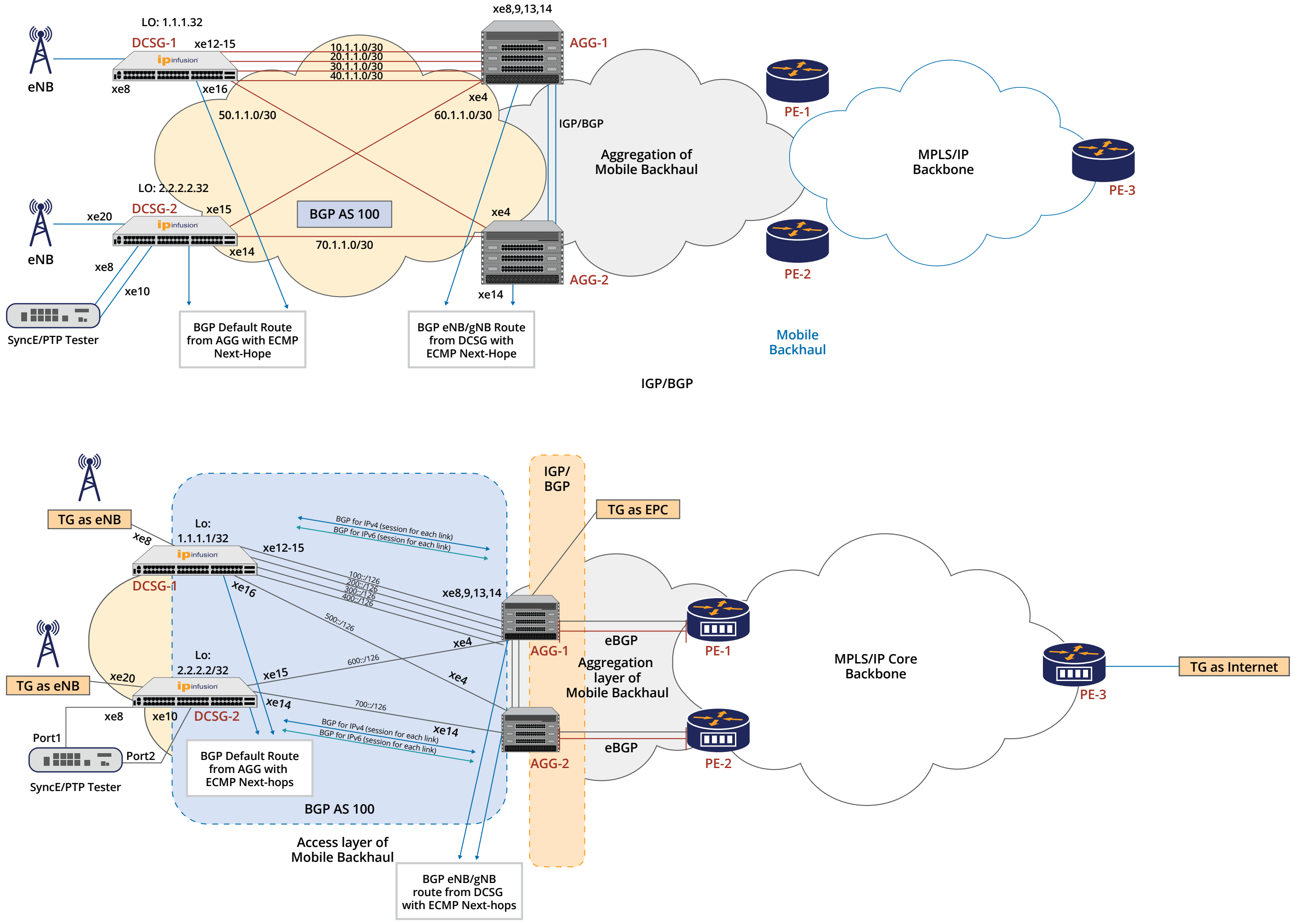


Figure 18: BGP Logical Topology

Note: Peer groups can also be used to reduce the configuration lines. This document demonstrates configurations without peer groups.

Designing Basic Functions and ECMP

TABLE 1-10: BGP BASIC FUNCTIONS	
PARAMETER	**DESIGN GUIDELINES**
BGP process ID	AS number
Router ID	Loopback IPv4 address of DCSGs
Update-source	IPv4/IPv6 addresses
AFI/SAFI Capability	IPv4 session with IPv4-unicast IPv6 session with IPv6-unicast
Convergence	BFD over each session for fast failover detection

Configurations and Validations

DCSG-1 ECMP

```
set protocols bgp 100 parameters maximum-paths ibgp 5
set protocols bgp 100 neighbor 10.1.1.2 remote-as 100
set protocols bgp 100 neighbor 10.1.1.2 address-family ipv4-unicast
set protocols bgp 100 neighbor 10.1.1.2 fall-over bfd
set protocols bgp 100 neighbor 20.1.1.2 remote-as 100
set protocols bgp 100 neighbor 20.1.1.2 address-family ipv4-unicast
set protocols bgp 100 neighbor 20.1.1.2 fall-over bfd
set protocols bgp 100 neighbor 30.1.1.2 remote-as 100
set protocols bgp 100 neighbor 30.1.1.2 address-family ipv4-unicast
set protocols bgp 100 neighbor 30.1.1.2 fall-over bfd
set protocols bgp 100 neighbor 40.1.1.2 remote-as 100
set protocols bgp 100 neighbor 40.1.1.2 address-family ipv4-unicast
set protocols bgp 100 neighbor 40.1.1.2 fall-over bfd
set protocols bgp 100 neighbor 50.1.1.2 remote-as 100
set protocols bgp 100 neighbor 50.1.1.2 address-family ipv4-unicast
set protocols bgp 100 neighbor 50.1.1.2 fall-over bfd
set protocols bgp 100 neighbor ‘100::2’ remote-as 100
set protocols bgp 100 neighbor ‘100::2’ address-family ipv6-unicast
set protocols bgp 100 neighbor ‘100::2’ fall-over bfd
set protocols bgp 100 neighbor ‘200::2’ remote-as 100
set protocols bgp 100 neighbor ‘200::2’ address-family ipv6-unicast

set protocols bgp 100 neighbor ‘200::2’ fall-over bfd
set protocols bgp 100 neighbor ‘300::2’ remote-as 100
set protocols bgp 100 neighbor ‘300::2’ address-family ipv6-unicast
set protocols bgp 100 neighbor ‘300::2’ fall-over bfd
set protocols bgp 100 neighbor ‘400::2’ remote-as 100
set protocols bgp 100 neighbor ‘400::2’ address-family ipv6-unicast
set protocols bgp 100 neighbor ‘400::2’ fall-over bfd
set protocols bgp 100 neighbor ‘500::2’ remote-as 100
set protocols bgp 100 neighbor ‘500::2’ address-family ipv6-unicast
set protocols bgp 100 neighbor ‘500::2’ fall-over bfd
set protocols bgp 100 address-family ipv4-unicast redistribute connected
set protocols bgp 100 address-family ipv6-unicast redistribute connected
```

DCSG-2 ECMP

```
set protocols bgp 100 parameters maximum-paths ibgp 5
set protocols bgp 100 neighbor 60.1.1.2 remote-as 100
set protocols bgp 100 neighbor 60.1.1.2 address-family ipv4-unicast
set protocols bgp 100 neighbor 60.1.1.2 fall-over bfd
set protocols bgp 100 neighbor 70.1.1.2 remote-as 100
set protocols bgp 100 neighbor 70.1.1.2 address-family ipv4-unicast
set protocols bgp 100 neighbor 70.1.1.2 fall-over bfd
set protocols bgp 100 neighbor ‘600::2’ remote-as 100
set protocols bgp 100 neighbor ‘600::2’ address-family ipv6-unicast
set protocols bgp 100 neighbor ‘600::2’ fall-over bfd
set protocols bgp 100 neighbor ‘700::2’ remote-as 100
set protocols bgp 100 neighbor ‘700::2’ address-family ipv6-unicast
set protocols bgp 100 neighbor ‘700::2’ fall-over bfd
set protocols bgp 100 address-family ipv4-unicast redistribute connected
set protocols bgp 100 address-family ipv6-unicast redistribute connected
```

Service Design

3G Services Overview

- 3G Iub service deployment is mainly for communication between the NodeB and the RNCs (“Iub” is internal interface connecting an RNC to Node B).
- VLAN is configured for the service, that is, the Iub is configured as VLANs (SVIs) on the DCSGs.
- This guide demonstrates the 3G implementation with OSPFv2/OSPFv3 as transport protocol. The real implementation can use an alternate IGP as a transport mechanism in the access network of the backhaul.
- DCSGs redistribute only connected routes of NodeBs in the OSPFv2/OSPFv3 protocol to reduce the number of routing entries on the aggregation nodes.

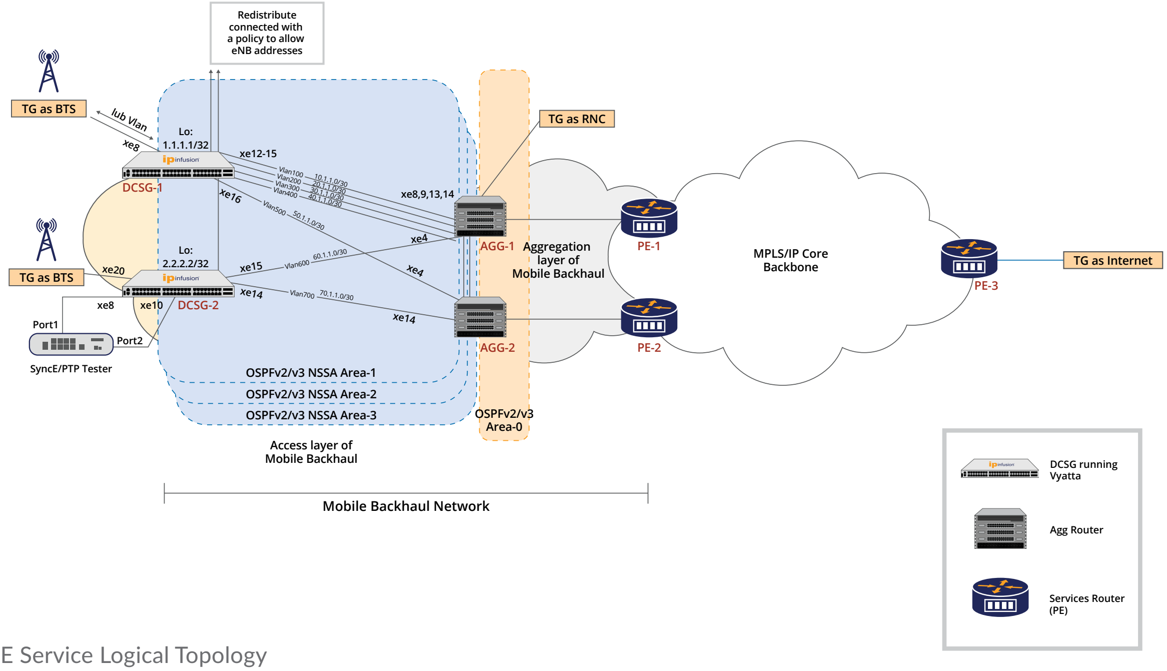


Figure 19: LTE Service Logical Topology

Basic Design

TABLE 1-11: DESIGN RESULTS

NODE	SERVICE NAME	VLAN	IPV4 ADDRESS	IPV6 ADDRESS
DCSG-1	3G Iub	1100	155.1.1.1/30	1100::1/126
DCSG-2	3G Iub	1100	165.1.1.1/30	2100::1/126

Configurations and Validations

DCSG-1 3G Services

```
#3G service
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1100
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1100
set interfaces switch sw0 vif 1100 address 155.1.1.1/30
set interfaces switch sw0 vif 1100 address ‘1100::1/126’

#Creating policy and redistributing restricted routes in ospf/ospfv3
set policy route prefix-list eNBv4 rule 10 action permit
set policy route prefix-list eNBv4 rule 10 prefix 155.1.1.0/30
set policy route prefix-list eNBv4 rule 1000 action deny
set policy route prefix-list eNBv4 rule 1000 prefix 0.0.0.0/0

set policy route route-map eNBv4 rule 1 action permit
set policy route route-map eNBv4 rule 1 match ip address prefix-list eNBv4
set protocols ospf redistribute connected route-map eNBv4

set policy route prefix-list6 eNBv6 rule 10 action permit
set policy route prefix-list6 eNBv6 rule 10 prefix ‘1100::/126’
set policy route prefix-list6 eNBv6 rule 1000 action deny
set policy route prefix-list6 eNBv6 rule 1000 prefix ::0/0

set policy route route-map eNBv6 rule 1 action permit
set policy route route-map eNBv6 rule 1 match ipv6 address prefix-list eNBv6
set protocols ospfv3 redistribute connected route-map eNBv6
```

DCSG-2 3G Services

```
#3G service
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1100
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1100
set interfaces switch sw0 vif 1100 address 165.1.1.1/30
set interfaces switch sw0 vif 1100 address ‘2100::1/126’

#Creating policy and redistributing restricted routes in ospf/ospfv3
set policy route prefix-list eNBv4 rule 10 action permit
set policy route prefix-list eNBv4 rule 10 prefix 165.1.1.0/30
set policy route prefix-list eNBv4 rule 1000 action deny
set policy route prefix-list eNBv4 rule 1000 prefix 0.0.0.0/0
set policy route route-map eNBv4 rule 1 action permit
set policy route route-map eNBv4 rule 1 match ip address prefix-list eNBv4
set protocols ospf redistribute connected route-map eNBv4

set policy route prefix-list6 eNBv6 rule 10 action permit
set policy route prefix-list6 eNBv6 rule 10 prefix ‘2100::/126’
set policy route prefix-list6 eNBv6 rule 1000 action deny
set policy route prefix-list6 eNBv6 rule 1000 prefix ::0/0

set policy route route-map eNBv6 rule 1 action permit
set policy route route-map eNBv6 rule 1 match ipv6 address prefix-list eNBv6
set protocols ospfv3 redistribute connected route-map eNBv6
```

4G/LTE Services

Overview

- LTE S1 service deployment is mainly for the S1-MME bearer and S1-U bearer establishment for control plane and data plane communication between the UE and the MME/SGW.
- LTE X2 services are mainly deployed to implement communication between DCSGs.
- S1 Service is E2E service that from DCSG router to MME/SGW that located in mobile packet core or aggregation.
- Each VLAN is configured per service, that is, S1-MME, S1-U and X2 is configured as different VLANs (SVIs) on the DCSGs.
- This guide demonstrates the 4G implementation with OSPF/OSPFv3 as transport protocol. The real implementation can use any alternate IGP protocol as a transport mechanism in the Access network of the backhaul.
- DCSGs redistribute only connected routes of eNBs in the OSPF/OSPFv3 protocol to reduce the number of routing entries on the aggregation nodes.

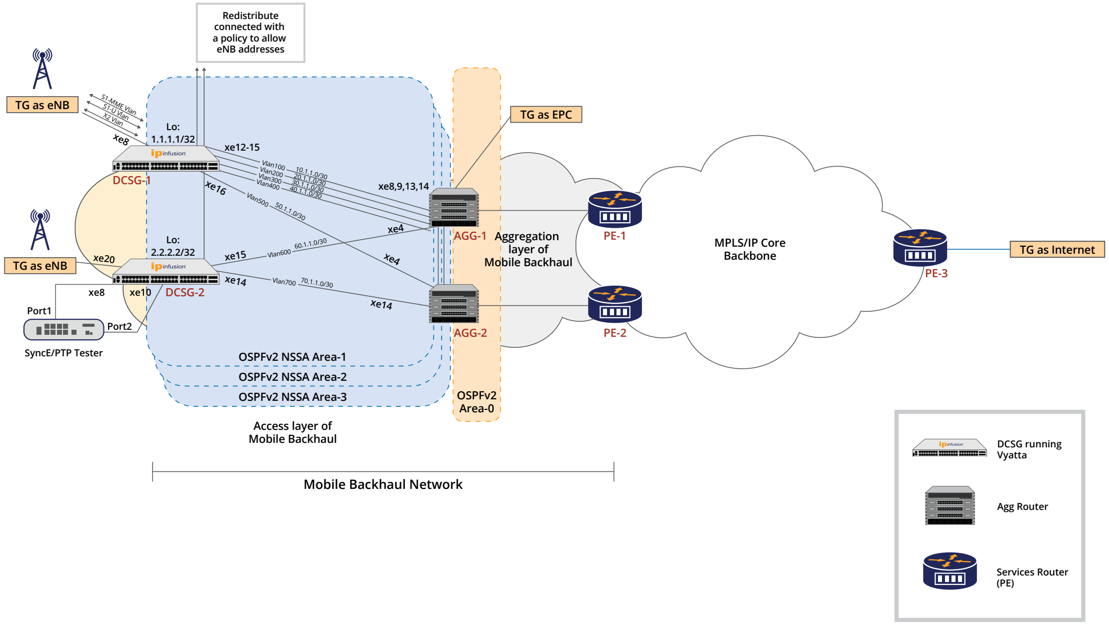


Figure 20: LTE Service Logical Topology

Basic Design

The DCSGs eNB facing interfaces are configured with VLANs per S1, X2 connection. S1-MME, S1-U and X2 each have a unique VLAN and SVI configured on the DCSGs.

These SVIs are configured with IPv4/IPv6 addresses and are redistributed by the routing protocol (OSPFv2/OSPFv3 in this case).

Note: DCSGs are configured with a policy to restrict what is redistributed by the routing protocol. We can also advertise the NodeB/eNodeB networks in the OSPF process and configure them as passive interfaces.

TABLE 1-12: DESIGN RESULTS

NODE	SERVICE TYPE	VLAN	IPV4 ADDRESS	IPV6 ADDRESS
DCSG-1	4G S1-MME	1000	150.1.1.1/30	1000::1/126
	4G S1-U	1001	151.1.1.1/30	1001::/126
	4G X2	1002	152.1.1.1/30	1002::/126
DCSG-2	4G S1-MME	1000	160.1.1.1/30	2000::1/126
	4G S1-U	1001	161.1.1.1/30	2001::1/126
	4G X2	1002	162.1.1.1/30	2002::1/126

Configurations and Validations

DCSG-1 4G/LTE Services

```
#4G Service
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1000
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1000
set interfaces switch sw0 vif 1000 address 150.1.1.1/30
set interfaces switch sw0 vif 1000 address ‘1000::1/126’
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1001
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1001
set interfaces switch sw0 vif 1001 address 151.1.1.1/30
set interfaces switch sw0 vif 1001 address ‘1001::1/126’
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1002
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1002
set interfaces switch sw0 vif 1002 address 152.1.1.1/30
set interfaces switch sw0 vif 1002 address ‘1002::1/126’

#Creating policy and redistributing only NodeB/eNB routes in ospf/ospfv3
set policy route prefix-list eNBv4 rule 1 action permit
set policy route prefix-list eNBv4 rule 1 prefix 150.1.1.0/30
set policy route prefix-list eNBv4 rule 2 action permit
set policy route prefix-list eNBv4 rule 2 prefix 151.1.1.0/30
set policy route prefix-list eNBv4 rule 3 action permit
set policy route prefix-list eNBv4 rule 3 prefix 152.1.1.0/30
set policy route prefix-list eNBv4 rule 1000 action deny
set policy route prefix-list eNBv4 rule 1000 prefix 0.0.0.0/0
set policy route route-map eNBv4 rule 1 action permit
set policy route route-map eNBv4 rule 1 match ip address prefix-list eNBv4
set protocols ospf redistribute connected route-map eNBv4
set policy route prefix-list6 eNBv6 rule 1 action permit
set policy route prefix-list6 eNBv6 rule 1 prefix '1000::/126'
set policy route prefix-list6 eNBv6 rule 2 action permit
set policy route prefix-list6 eNBv6 rule 2 prefix  '1001::/126'
set policy route prefix-list6 eNBv6 rule 3 action permit
set policy route prefix-list6 eNBv6 rule 3 prefix  '1002::/126'
set policy route prefix-list6 eNBv6 rule 1000 action deny
set policy route prefix-list6 eNBv6 rule 1000 prefix '::/0'

set policy route route-map eNBv6 rule 1 action permit
set policy route route-map eNBv6 rule 1 match ipv6 address prefix-list eNBv6
set protocols ospfv3 redistribute connected route-map eNBv6
```

DCSG-2 4G/LTE Services

```
#4G Service
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1000
set interfaces dataplane dp0xe20 switch-group port-parameters vlan-parameters vlans 1000
set interfaces switch sw0 vif 1000 address 160.1.1.1/30
set interfaces switch sw0 vif 1000 address '2000::1/126'
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1001
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1001
set interfaces switch sw0 vif 1001 address 161.1.1.1/30
set interfaces switch sw0 vif 1001 address '2001::1/126'
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1002
set interfaces dataplane dp0xe8 switch-group port-parameters vlan-parameters vlans 1002
set interfaces switch sw0 vif 1002 address 162.1.1.1/30
set interfaces switch sw0 vif 1002 address '2002::1/126'

#Creating policy and redistributing restricted routes in ospf/ospfv3
set policy route prefix-list eNBv4 rule 1 action permit
set policy route prefix-list eNBv4 rule 1 prefix 160.1.1.0/30
set policy route prefix-list eNBv4 rule 2 action permit
set policy route prefix-list eNBv4 rule 2 prefix 161.1.1.0/30
set policy route prefix-list eNBv4 rule 3 action permit
set policy route prefix-list eNBv4 rule 3 prefix 162.1.1.0/30
set policy route prefix-list eNBv4 rule 1000 action deny
set policy route prefix-list eNBv4 rule 1000 prefix 0.0.0.0/0

set policy route route-map eNBv4 rule 1 action permit
set policy route route-map eNBv4 rule 1 match ip address prefix-list eNBv4
set protocols ospf redistribute connected route-map eNBv4

set policy route prefix-list6 eNBv6 rule 1 action permit
set policy route prefix-list6 eNBv6 rule 1 prefix '2000::/126'
set policy route prefix-list6 eNBv6 rule 2 action permit
set policy route prefix-list6 eNBv6 rule 2 prefix  '2001::/126'
set policy route prefix-list6 eNBv6 rule 3 action permit
set policy route prefix-list6 eNBv6 rule 3 prefix  '2002::/126'
set policy route prefix-list6 eNBv6 rule 1000 action deny
set policy route prefix-list6 eNBv6 rule 1000 prefix '::/0'

set policy route route-map eNBv6 rule 1 action permit
set policy route route-map eNBv6 rule 1 match ipv6 address prefix-list eNBv6
set protocols ospfv3 redistribute connected route-map eNBv6
```

Synchronization

The DCSG supports time and phase synchronization.

IEEE1588/PTP Profile Configuration

PTP follows the specification defined in ITU-T Default Profile, G.8275.1, G.8271.1, and G.8273.2. Ports of the DCSG can be configured to enable default PTP profile(G.8275.2).

The DCSG can be configured as a T-BC (Telecom Boundary Clock).

PTP Default Profile Configuration

```
# Set the ptp clock default profile for single instance #
set service ptp instance 0 clock-profile vyatta-g.8275.2-v1:g.8275.2-profile

# Configure first interface connecting to the PTP tester#
set service ptp instance 0 port-ds-list 1 log-announce-interval 0
set service ptp instance 0 port-ds-list 1 log-min-delay-req-interval -7
set service ptp instance 0 port-ds-list 1 log-sync-interval -7
# Set the master interface IP address of the PTP tester #
set service ptp instance 0 port-ds-list 1 master 100.1.1.2
set service ptp instance 0 port-ds-list 1 underlying-interface dp0xe8
set service ptp instance 0 port-ds-list 1 vlan 1002

# Configure the second interface connecting to the PTP tester#
set service ptp instance 0 port-ds-list 2 log-announce-interval 0
set service ptp instance 0 port-ds-list 2 log-min-delay-req-interval -7
set service ptp instance 0 port-ds-list 2 log-sync-interval -7
set service ptp instance 0 port-ds-list 2 underlying-interface dp0xe10
set service ptp instance 0 port-ds-list 2 vlan 1003

# Configure global priority and source interface#
set service ptp instance 0 priority1 100
set service ptp instance 0 source-interface lo100

set interfaces dataplane dp0xe20 switch-group port-parameters vlan-parameters vlans 1002
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1002
set interfaces switch sw0 vif 1002 address 200.1.1.2/2

set interfaces loopback lo100 address 2.2.2.2/32

set interfaces dataplane dp0xe21 switch-group port-parameters vlan-parameters vlans 1003
set interfaces switch sw0 default-port-parameters vlan-parameters vlans 1003
set interfaces switch sw0 vif 1003 address 203.1.1.2/24
set service ptp instance 0 port-ds-list 2 vlan 1003
#Set a static route to reach the PTP tester #
set protocols static route 100.1.1.0/24 next-hop 200.1.1.1
set protocols static route 100.2.2.0/24 next-hop 203.1.1.1

vyatta@vyatta:~$ show ptp clock
Clock  Servo State  Locked State
    0  time-locked  phase-locked
vyatta@vyatta:~$     show ptp servo
Clock 0 servo statistics
        Servo state: time-locked
        Servo lock state: phase-locked
        State duration: 84 seconds
        Frequency correction: -158.244 ppb
        Phase correction: 0.216816468000 seconds
        Servo history:
                Time                     Freq. (ppb)     Phase (secs)
                2020-06-15T12:37:37Z        -158.198      0.216816468
                2020-06-15T12:35:37Z        -158.127      0.000105419
                2020-06-15T12:33:37Z        -158.127      0.000105419
                2020-06-15T12:31:37Z        -160.217      0.000105419
                2020-06-15T12:29:36Z           0.000      0.000000000
                2020-06-15T12:27:36Z           0.000      0.000000000
                2020-06-15T12:25:36Z           0.000      0.000000000

vyatta@Vyatta:~$ show ptp counters
Clock 0 packet counters
        Transmitted Packets: 33101
        Received Packets: 61100
        Discarded Packets: 330

        Port 1 packet counters
                Transmitted Packets: 30024
                Received Packets: 59650
                Discarded Packets: 300

                Peer: 100.1.1.2
                Clock Identity: 00:00:00:00:00:00:00:01
                        Transmitted Packets: 21221
                        Received Packets: 42614
                        Discarded Packets: 0
                                Received ANNOUNCE messages: 168
                                Received DELAYREQ messages: 0
                                Received DELAYRESP messages: 21152
                                Received FOLLOWUP messages: 0
                                Received Management messages: 0
                                Received Signaling messages: 12
                                Received SYNC messages: 21282
                                Reject messages: 0
                                Transmitted ANNOUNCE messages: 0
                                Transmitted DELAYREQ messages: 21152
                                Transmitted DELAYRESP messages: 0
                                Transmitted FOLLOWUP messages: 0
                                Transmitted Management messages: 0
                                Transmitted Signaling messages: 69
                                Transmitted SYNC messages: 0

Port 2 packet counters
                Transmitted Packets: 3005
                Received Packets: 1405
                Discarded Packets: 0

                Peer: 100.2.2.2
                Clock Identity: 00:00:00:00:00:00:00:02
                        Transmitted Packets: 3008
                        Received Packets: 1408
                        Discarded Packets: 0
                                Received ANNOUNCE messages: 0
                                Received DELAYREQ messages: 1405
                                Received DELAYRESP messages: 0
                                Received FOLLOWUP messages: 0
                                Received Management messages: 0
                                Received Signaling messages: 3
                                Received SYNC messages: 0
                                Reject messages: 0
                                Transmitted ANNOUNCE messages: 177
                                Transmitted DELAYREQ messages: 0
                                Transmitted DELAYRESP messages: 1405
                                Transmitted FOLLOWUP messages: 0
                                Transmitted Management messages: 0
                                Transmitted Signaling messages: 3
                                Transmitted SYNC messages: 1423

vyatta@vyatta:~$  show ptp clock detail
Clock 0 data sets
        Default data set:
                Two Step flag: False
                Clock Identity: e8:c5:7a:ff:ff:02:a0:3b
                Number Ports: 2
                Clock Quality:
                        Clock Class: 248
                        Clock Accuracy: 254
                        Offset Scaled Log Variance: 65535
                Priority1: 100
                Priority2: 128
                Domain Number: 44
                Slave Only: False
```

```
       Current data set:
                Steps Removed: 1
                Offset from Master: -14209082294272 (-216813389.500 ns)
                Mean Path Delay: 216816456

        Parent data set:
                Parent Port Identity:
                        Clock Identity: 00:00:00:00:00:00:00:01
                        Port Number: 1
                Parent Stats: False
                Grandmaster Identity: 00:00:00:00:00:00:00:01
                Observed Parent Offset Scaled Log Variance: 0
                Observed Parent Clock Phase Change Rate: 0
                Grandmaster Clock Quality:
                        Clock Class: 6
                        Clock Accuracy: 33
                        Offset Scaled Log Variance: 20061
                Grandmaster Priority1: 128
                Grandmaster Priority2: 128

Time Properties data set:
                Current UTC Offset: 37
                Leap59: False
                Leap61: False
                Time Traceable: True
                Frequency Traceable: True
                Time Source: 0x20
                PTP Timescale: True

        Clock Port 1 data set:
                Port State: slave
                logMinDelayReqInterval: -7
                peerMeanPathDelay: 0
                logAnnounceInterval: 0
                announceReceiptTimeout: 3
                logSyncInterval: -7
                Delay Mechanism: e2e
                logMinPDelayReqInterval: -4
                Version Number: 2
                Peers:
                        Address: 100.1.1.2
                        Clock Identity: 00:00:00:00:00:00:00:01
        Clock Port 2 data set:
                Port State: master
                logMinDelayReqInterval: -7
                peerMeanPathDelay: 0
                logAnnounceInterval: 0
                announceReceiptTimeout: 3
                logSyncInterval: -7
                Delay Mechanism: e2e
                logMinPDelayReqInterval: -4
                Version Number: 2
                Peers:
                        Address: 100.2.2.2
                        Clock Identity: 00:00:00:00:00:00:00:02
```

Security

ACLs Overview

- Access control lists have many applications some of which include traffic filtering at ingress or egress, classifying traffic in QoS based on L3/L4 headers, and using as a route-map attach point to filter routing updates/advertisements for IGP/BGP.
- This guide demonstrates the use of ACLs on the access facing port as a traffic filter in the ingress/egress in L3 interface direction as an example.

Basic Design

ACLs filter certain sources/destinations IP address for incoming/outgoing traffic and originate traffic for IP protocol type filter.

Configurations and Validations

DCSG-1

```
set security ip-packet-filter group ipv4 ip-version ipv4
set security ip-packet-filter group ipv4 rule 1 action drop
set security ip-packet-filter group ipv4 rule 1 match destination ipv4 prefix 150.1.1.0/24
set security ip-packet-filter group ipv4 rule 1 match source ipv4 prefix 160.1.1.0/24
set security ip-packet-filter group ipv4 rule 2 action accept
set security ip-packet-filter group ipv4 rule 2 match source ipv4 host 150.1.1.2
set security ip-packet-filter interface dp0xe17 out ipv4

set security ip-packet-filter group ipv4 counters count packets
set security ip-packet-filter group ipv4 counters sharing per-interface
set security ip-packet-filter group ipv4 counters type auto-per-rule


show security ip-packet-filter statistics
```

```
Interface       Dir           Group Rule Action      HW packets      SW packets        HW
bytes        SW bytes
---------       ---           ----- ---- ------      ----------      ----------        ---
-----        ---------
dp0xe17         out            ipv4    1   drop               0               3
-               -
dp0xe17         out            ipv4    2 accept               0               4
-               -

create match criteria to IP Protocol type with Rule 3.
set security ip-packet-filter group ipv4 rule 3 action accept
set security ip-packet-filter group ipv4 rule 3 match protocol base name tcp
set security ip-packet-filter interface dp0xe17 in ipv4

show security ip-packet-filter statistics

Interface       Dir           Group Rule Action      HW packets      SW packets        HW
bytes        SW bytes
---------       ---           ----- ---- ------      ----------      ----------        ---
-----        ---------
dp0xe17         in            ipv4    3 accept               0          887726
-               -
```

ACL filter can be applied using SRC and DEST TCP/UDP port with ingress direction rule.

User Management (TACACS+)

Overview

- TACACS+ is used to demonstrate remote authentication/authorization/accounting and RADIUS is used in a similar manner.
- TACACS+ provides a method to manage multiple network access points from a single management service.
- TACACS+ provides separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently.
- Management port is used for connecting to TACACS+ in this solution, but in-band management can also be used in the same manner to connect to TACACS+ servers.
- Users connecting via the management network or via the console are authenticated using TACACS+ and then via local authentication as a fallback method.
- The AT&T Vyatta vRouter supports two user roles:
  - Administrator users
  - Operator users

- Administrator users have full access to the Vyatta CLI. Administrator users can view, configure, and delete information and execute all operational commands. Administrator users can also execute all operating system shell commands and constructs.
- Operator users have read-only access to configuration plus the ability to execute AT&T Vyatta vRouter operational commands. Operator users can view in operational mode (by using show commands), configure their terminal settings (by using the set terminal command), and exit from the Vyatta CLI (by using the exit command). Operator users cannot enter configuration mode; however, they can display configuration by entering the show configuration command in operational mode
- When editing the TACACS+ server configuration file, be sure to set the right privilege level for the users.

Basic Design

- Out-of-band management interface is configured with an IP address (or configured to receive IP address via DHCP).
- A separate routing instance (named "management") is created and the management port is made part of this routing instance.
- A default static route is created to reach devices in the management routing instance.
- The TACACS+ service with a server IPv4 address (10.12.47.72 in this case) is configured in the management routing instance after which it is used for authentication/authorization and accounting.

Configurations and Validations

DCSG-1 (TACACS+)

```
set interfaces dataplane dp0p7s0 address dhcp
set routing-instance management interface dp0p7s0
set routing-instance management protocols static route 0.0.0.0/0 next-hop 10.12.87.1
set routing-instance management system login tacplus-server 10.12.47.72 secret '********'
set routing-instance management system login tacplus-server 10.12.47.72 source-interface
dp0p7s0
```

Control Plane Policing

Overview

- Control Plane Protection (CoPP) is a method of protecting the processor unit and running services on your network device against excessive flooding. Excessive flooding of traffic aimed towards your router/firewall processor, whether valid or malicious, is always undesirable and can also be dangerous.
- Some of the most common control traffic generating services are routing protocols with different update packets such as ARP, ICMP, and NTP and different management traffic services such as SSH, SNMP, RADIUS, and so on.
- This section gives a snapshot of CoPP configuration for Vyatta for SNMP and ICMP as a sample configuration. There is also a last rule of drop all set to drop all which is not allowed as part of the CoPP.

Basic Design

- The configuration below shows two protocol’s packets allowed to the CPU; SNMP and ICMP.
- A last rule of drop all is also configured to make sure all the traffic which is not allowed in the CoPP is dropped and not let through to the CPU.

Note: The configuration below is just a sample and for real implementations all required protocols such as routing protocols, management protocols (SSH, Telnet, SNMP, TACACS+, RADIUS), and ICMP must be configured based on the below syntax.

Configurations and Validations

DCSG-1 Policing

```
#Apply the rule to filter packets going to the local CPU of this Router
set interfaces loopback lo firewall local CoPP

#Example to show SNMP allowed for CPU Processing
set security firewall name CoPP rule 10 action accept
set security firewall name CoPP rule 10 description SNMP
set security firewall name CoPP rule 10 destination port 161
set security firewall name CoPP rule 10 protocol udp

#Example to show ICMP allowed with certain rate-limit
set security firewall name CoPP rule 20 action accept
set security firewall name CoPP rule 20 description ICMP
set security firewall name CoPP rule 20 icmp name echo-request
set security firewall name CoPP rule 20 police ratelimit 500pps
set security firewall name CoPP rule 20 police then action drop

#Example to show a last rule in the filter to drop everything else
set security firewall name CoPP rule 9999 action drop
set security firewall name CoPP rule 9999 description ‘Discard All’
```

Quality of Service (QoS)

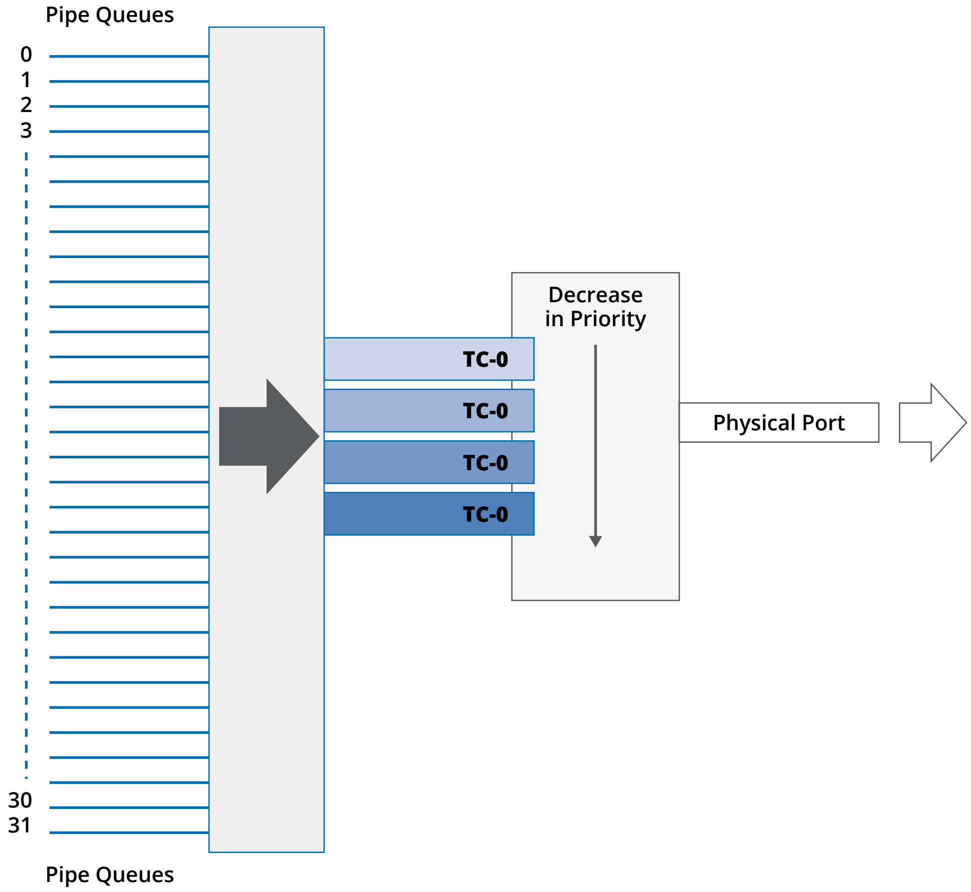


Figure 21: QoS Egress Shaping

The QoS design is configured to match the strict performance key performance indicators needed from the 3G/4G IP interfaces of the transmission architecture. In 3G UMTS architecture, there are four traffic classes: conversational, streaming, interactive, and background. The transmission QOS architecture should guarantee provided bounded maximum permissible delay and maximum allowed errors (BER).

In the 4G architecture, different QCI (QoS Class Identifiers) applicable to different EPS channels have separate requirements for GBR (Guaranteed bit rate), non-GBR, MBR (Maximum Bit Rate), Priority, permissible delay, and maximum allowed errors.

QoS design for ingress classification

- The incoming packet/frame is classified based on:
  - Ingress DSCP/ToS from the incoming IP packets
  - The 802.1p field is also be remarked based on the DSCP fields

- For classification of the incoming traffic;
  - Using DSCP match groups, DSCP fields are matched and assigned to a particular dscp-group ID
  - Using a qos policy map, a 802.1p remark map is created and bound to different dscp-groups. This results in remarking of the 802.1p field as per DSCP priority.

QoS design for egress shaping and scheduling basic steps:

- The classified traffic is assigned to one of the 32 pipe-queues
- More than one classified traffic can be assigned to the same pipe-queue
  - If there is more than one classified traffic to the same pipe-queue, the one configured first is first used for scheduling and thus has less chance of queue drop.
- There are four traffic classes, TC-0 to 3, where scheduling is enabled from zero to three in SP order.
- The traffic class (TC) queue limit bytes are set as per the expected traffic, to avoid tail drops.
  - Each of the traffic classes are set to queue limit bytes to hold traffic for a certain duration of the shaped rate.
- Pipe-queues are mapped to traffic classes
- Traffic classes are assigned the upper maximum bandwidth if required.
  - Traffic class 0 and 1 are given a upper bandwidth limit to avoid other queues from starvation.
- Configure WRR low, high watermark, and drop probability for the traffic classes separately for the different categories of traffic groups falling into it.

Designing Ingress Service Mapping for All Services

A generic broad classification group for the possible traffic would be to group them as:

a. Real-time

b. Priority - P0 - high

c. Priority - P1 - low

d. Default - P0 - high

e. Default - P1 - low

f. Sync-ptp-traffic

Therefore, selected 3G/4G services and their possible classification can be defined as shown in 3G/4G Services and their Possible Classification:

TABLE 1-13: 3G/4G SERVICES AND THEIR POSSIBLE CLASSIFICATION

SERVICE TYPE	DSCP/COS	802.1P	GROUP CLASSIFICATION
3G (Voice Data, Signaling)	EF/CS5	5	Real-time
3G Management	CS3/CS4	2	Priority-P0-high
4G Real Time Voice	EF/CS5	5	Real-time
4G Real Time Data	EF/CS5	5	Real-time
Other Signaling Management	CS6	2	Priority-P1-low
Control and Management Traffic	CS3/CS4	2	Priority-P0-high
Best Effort	BE/CS0	1	Default-P1-low
Sync-PTP Traffic	"Custom" (See table below)	7	Sync-ptp-traffc

It makes sense to remark the classified traffic with different 802.1p fields, so that at the next hop the traffic gets better treatment.

Thus, a possible remarking scheme would be:

a. Real-time - Remark 802.1p to 5

b. Priority - P0 - high - Remark 802.1p to 4

c. Priority - P1 - low - Remark 802.1p to 3

d. Default - P0 - high - Remark 802.1p to 2

e. Default - P1 - low - Remark 802.1p to 1

f. Sync-ptp-traffic - Remark 802.1p to 7

TABLE 1-14: SERVICE MAPPING

TRAFFIC GROUP'S CLASSIFICATION	EXAMPLE TRAFFIC GROUPS	DSCP MARKINGS	802.1P MARKING
Real-time	• 3G (Voice, Data Signaling) • 4G (Real time Voice) • 4G (Real time data)	Standard: a) EF b) CS5 Custom: a) Match it with traffic QOS markings which is real-time	5
Priority-P0-High	• 3G Management • Control and Management Traffic	Standard: a) CS3 b) CS4 Custom: a) Match it with traffic QOS which needs high priority treatment. Example, Group other High priority groups; a) CS6 b) CS7 c) AF41 d) AF42 e) AF43 f) AF31 g) AF32 h) AF33	4
Priority-P1-Low	Other Signaling management	Custom: a) Match Low AF PHB a) AF21 b) AF22 c) AF23	3
Default-P0-High	Priority messages like Alert, Notifications	Standard: a) CS1	2
Default-P1-Low	Best Effort	Custom: a) Match all remaining dscp markings to this group	1
Sync-Ptp-traffic	Sync, PTP control traffic	Match this with the SyncE and PTP traffic QOS markings. Example: a) CS2	7

Designing Service Scheduling

Services are scheduled on the egress and corresponding pipe-queue and traffic-class mapping is defined as shown in Service Scheduling:

TABLE 1-15: SERVICE SCHEDULING

TRAFFIC-GROUPS	LATENCY TOLERANCE	PACKET DROP TOLERANCE	RECOMMENDED SCHEDULING REQUIREMENT	TRAFFIC-CLASS MAPPING	SAMPLE PIPE-QUEUE IDS MAPPING	RECOMMENDED SP SCHEDULE BANDWIDTH LIMIT & WFQ RATIO
Real-time	Low (<5ms)	Low	SP	TC-1	1	20% of QoS policy
Priority- P0-High	Medium	Average	WFQ - Group A	TC-3	4	WFQ Weight- 70
Priority- P1-Low	Average	Average	WFQ - Group A	TC-3	4	
Default-P0-High	Average	High	WFQ - Group B	TC-3	5	WFQ Weight - 30
Default-P1-Low	Average	High	WFQ - Group B	TC-3	5	
Sync-Ptp-traffic	Low (<5ms)	Low	SP	TC-2	2	20% of QOS policy
Locally generated control traffic	Medium (<20ms)	Medium	SP	TC-1		20% of QOS policy

Note: The above values are only sample recommendations and should be modified to use the deployment scenario.

Configurations and Validations

These configurations are shown for DCSG2 (from Reference Topology), xe14.

Classification

Step 1: Create dscp-group matching incoming traffic service classes

```
#Define six different dscp-group resources #

set resources group dscp-group default-p0-high dscp cs1

set resources group dscp-group default-p1-low dscp af11
set resources group dscp-group default-p1-low dscp af12
set resources group dscp-group default-p1-low dscp af13

set resources group dscp-group priority-p0-high dscp af31
set resources group dscp-group priority-p0-high dscp af32
set resources group dscp-group priority-p0-high dscp af33
set resources group dscp-group priority-p0-high dscp af41

set resources group dscp-group priority-p0-high dscp af42
set resources group dscp-group priority-p0-high dscp af43
set resources group dscp-group priority-p0-high dscp cs3
set resources group dscp-group priority-p0-high dscp cs4
set resources group dscp-group priority-p0-high dscp cs6
set resources group dscp-group priority-p0-high dscp cs7
set resources group dscp-group priority-p1-low dscp af21
set resources group dscp-group priority-p1-low dscp af22
set resources group dscp-group priority-p1-low dscp af23

set resources group dscp-group real-time dscp cs5
set resources group dscp-group real-time dscp ef

set resources group dscp-group sync-ptp-traffic dscp cs2
```

Step 2: Create a qos policy and profile and also set the default profile

```
#Create a qos policy and a qos profile, profile-1 #
#Set the default profile under the policy also as profile-1 #
set policy qos name policy-1
set policy qos name policy-1 shaper profile profile-1
set policy qos name policy-1 shaper default profile-1
```

Step 3: Set the bandwidth at shaper level to be 2G

```
#Recomended to configure shaper to 95% of required value #
#For 2Gbps, 95% is 1.9Gbps #
set policy qos name policy-1 shaper profile profile-1 bandwidth 1.9Gbps
```

Step 4: Set maximum queue length bytes for each of the traffic classes

```
# Traffic class 0 carries low latency traffic holding 5ms of traffic at 2G #
# in bytes 1250000 bytes #
set policy qos name policy-1 shaper traffic-class 0 queue-limit-bytes 1250000

# Traffic class 1 carries low latency traffic holding 5ms of traffic at 2G #
# in bytes 1250000 bytes #
set policy qos name policy-1 shaper traffic-class 1 queue-limit-bytes 1250000

# Traffic class 2 carries medium latency traffic holding 10ms of traffic at 2G #
# in bytes 2500000 bytes #
set policy qos name policy-1 shaper traffic-class 2 queue-limit-bytes 2500000

# Traffic class 3 carries average latency traffic holding 50ms of traffic at 2G #
# in bytes 12500000 #
set policy qos name policy-1 shaper traffic-class 3 queue-limit-bytes 12500000
```

Step 5: Map the dscp-groups to pipe-queues

```
set policy qos name policy-1 shaper profile profile-1 map dscp-group sync-ptp-traffic to 2
set policy qos name policy-1 shaper profile profile-1 map dscp-group real-time to 1
#Assigning two classification to pipe-queue 4 #
#Note to configure high priority earlier for low precedence #
set policy qos name policy-1 shaper profile profile-1 map dscp-group priority-p0-high to 4
set policy qos name policy-1 shaper profile profile-1 map dscp-group priority-p1-low to 4
#Assigning two classifications to pipe-queue 5 #
# Note to configure high priority earlier for low precedence #
set policy qos name policy-1 shaper profile profile-1 map dscp-group default-p0-high to 5
set policy qos name policy-1 shaper profile profile-1 map dscp-group default-p1-low to 5
```

Step 6: Assign the pipe-queues to planned traffic classes

```
# Configure SP scheduling treatment #
set policy qos name policy-1 shaper profile profile-1 queue 0 traffic-class 0
set policy qos name policy-1 shaper profile profile-1 queue 1 traffic-class 1
set policy qos name policy-1 shaper profile profile-1 queue 2 priority-local
set policy qos name policy-1 shaper profile profile-1 queue 2 traffic-class 2

# Configure WFQ scheduling treatment #
set policy qos name policy-1 shaper profile profile-1 queue 4 traffic-class 3
set policy qos name policy-1 shaper profile profile-1 queue 5 traffic-class 3
```

Step 7: Limit the overall bandwidth percentage higher priority traffic classes can take

```
set policy qos name policy-1 shaper profile profile-1 traffic-class 0 bandwidth 20%
set policy qos name policy-1 shaper profile profile-1 traffic-class 1 bandwidth 20%
set policy qos name policy-1 shaper profile profile-1 traffic-class 2 bandwidth 20%

#The remaining 40% is utilized by traffic class 3#
```

Step 8: For pipe-queues sharing the same traffic-class define the sharing ratio of traffic

```
set policy qos name policy-1 shaper profile profile-1 queue 4 weight 70
set policy qos name policy-1 shaper profile profile-1 queue 5 weight 30
```

Step 9: Set the WRR levels for the pipe-queues

```
#pipe-queues 4 and 5 need the WRR configurations for the different traffic #
#classes #

set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
Priority-p0-high mark-probability 10
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
Priority-p0-high max-threshold 12500000
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
Priority-p0-high min-threshold 10000000

set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
Priority-p1-low mark-probability 10
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
Priority-p1-low max-threshold 10000000
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
Priority-p1-low min-threshold 5000000

set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
default-p0-high mark-probability 10
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
default-p0-high max-threshold 12500000
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
default-p0-high min-threshold 10000000

set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
default-p1-low mark-probability 10
```

```
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
default-p1-low max-threshold 10000000
set policy qos name policy-1 shaper profile profile-1 queue 4 wred-map-bytes dscp-group
default-p1-low min-threshold 5000000

Step 10: Bind the policy to the incoming traffic interface
set interfaces dataplane dp0xe14 switch-group port-parameters policy qos policy-1
```

Step 11: Set the default policy as policy-1

```
set policy qos name policy-1 shaper default profile-1
set policy qos name policy-1 shaper frame-overhead 0
```

Step 12: Verify the policy configurations

```
Show policy qos
Interface          TC             Counters
-----------------------------------------------------
dp0xe8             0                    0 Bytes
                                         0 Packets
                                         0 Tail-drop
                                         0 RED-drop
                    1                    0 Bytes
                                         0 Packets
                                         0 Tail-drop
                                         0 RED-drop
                    2                  552 Bytes
                                         8 Packets
                                         0 Tail-drop
                                         0 RED-drop
                    3                   92 Bytes
                                         2 Packets
                                         0 Tail-drop
                                         0 RED-drop


Show policy qos dp0xe14

Class      TC  WRR   Qlength         PLQ             Counters
------------------------------------------------------------------------
0           0    0         0 packets                312423050 bytes
                                                       206357 packets
                                                           51 Tail-drop
                                                            0 RED-drop
                 1         0 packets                        0 bytes
                                                            0 packets
                                                            0 Tail-drop
                                                            0 RED-drop
                 2         0 packets                        0 bytes
                                                            0 packets
                                                            0 Tail-drop
```

```
                                               0 RED-drop
     3         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     4         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     5         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     6         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     7         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
1    0         0 packets               2131220082 bytes
                                          1407677 packets
                                               83 Tail-drop
                                                0 RED-drop
     1         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     2         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     3         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     4         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     5         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     6         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     7         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
2    0         0 packets               1718817632 bytes
                                          1135352 packets
                                              161 Tail-drop
                                                0 RED-drop
     1         0 packets               1192545226 bytes
                                           787851 packets
                                              145 Tail-drop
                                                0 RED-drop
     2         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     3         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     4         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     5         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     6         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     7         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
3    0         0 packets                      168 bytes
                                                3 packets
                                                0 Tail-drop
                                                0 RED-drop
     1         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     2         0 packets                        0 bytes
                                                0 packets
                                                0 Tail-drop
                                                0 RED-drop
     3         0 packets                        0 bytes
                                                0 packets
```

```
                                                            0 Tail-drop
                                                            0 RED-drop
                 4         0 packets                        0 bytes
                                                            0 packets
                                                            0 Tail-drop
                                                            0 RED-drop
                 5         0 packets                        0 bytes
                                                            0 packets
                                                            0 Tail-drop
                                                            0 RED-drop
                 6         0 packets                        0 bytes
                                                            0 packets
                                                            0 Tail-drop
                                                            0 RED-drop
                 7         0 packets                        0 bytes
                                                            0 packets
                                                            0 Tail-drop
                                                            0 RED-drop
                                                            0 RED-drop
```

QoS Marking for self generated control plane traffic (BGP, OSPF)

In order to support End to End QoS packet processing DiffServ domain according to RFC https://tools.ietf.org/html/rfc2475 for control, operation and management protocols originated on Vyatta Router we need to implement egress DS node classifier.

The function of DS classifier is to mark (write DSCP field in IP header) packets based on the content of packet headers according to defined rules or configuration which represent class of service.

This is necessary to correctly map those packets to internal priority and treat them according to configured class of service in all intermediate routers along the path from Vyatta Router to destination router. This allows for example to reduce a chance of dropping control plane packets like OSPF or BGP in intermediate routers in case of path is overload with other traffic like HTTP.

Configuration and Validation

Step 1: Create firewall rule to match BGP traffic and attach the rule to loopback interface using originate.

```
security firewall name cop rule 110 description bgp
set security firewall name cop rule 110 destination port 179
set security firewall name cop rule 110 mark dscp cs7
set security firewall name cop rule 110 protocol tcp
set security firewall name cop rule 120 action accept
set security firewall name cop rule 120 description bgp
set security firewall name cop rule 120 mark dscp cs7
set security firewall name cop rule 120 protocol tcp
set security firewall name cop rule 120 source port 179
```

Step 2: Create dscp resource groups to match all the dscp traffic from 0 to 63.

```
set resources group dscp-group group-0-to-7 dscp 0
set resources group dscp-group group-0-to-7 dscp 1
set resources group dscp-group group-0-to-7 dscp 2
set resources group dscp-group group-0-to-7 dscp 3
set resources group dscp-group group-0-to-7 dscp 4
set resources group dscp-group group-0-to-7 dscp 5
set resources group dscp-group group-0-to-7 dscp 6
set resources group dscp-group group-0-to-7 dscp 7
set resources group dscp-group group-8-to-15 dscp 8
set resources group dscp-group group-8-to-15 dscp 9
set resources group dscp-group group-8-to-15 dscp 10
set resources group dscp-group group-8-to-15 dscp 11
set resources group dscp-group group-8-to-15 dscp 12
set resources group dscp-group group-8-to-15 dscp 13
set resources group dscp-group group-8-to-15 dscp 14
set resources group dscp-group group-8-to-15 dscp 15
set resources group dscp-group group-16-to-23 dscp 16
set resources group dscp-group group-16-to-23 dscp 17
set resources group dscp-group group-16-to-23 dscp 18
set resources group dscp-group group-16-to-23 dscp 19
set resources group dscp-group group-16-to-23 dscp 20
set resources group dscp-group group-16-to-23 dscp 21
set resources group dscp-group group-16-to-23 dscp 22
set resources group dscp-group group-16-to-23 dscp 23
set resources group dscp-group group-24-to-31 dscp 24
set resources group dscp-group group-24-to-31 dscp 25
set resources group dscp-group group-24-to-31 dscp 26
set resources group dscp-group group-24-to-31 dscp 27
set resources group dscp-group group-24-to-31 dscp 28
set resources group dscp-group group-24-to-31 dscp 29
set resources group dscp-group group-24-to-31 dscp 30
set resources group dscp-group group-24-to-31 dscp 31
set resources group dscp-group group-32-to-39 dscp 32
set resources group dscp-group group-32-to-39 dscp 33
set resources group dscp-group group-32-to-39 dscp 34
set resources group dscp-group group-32-to-39 dscp 35
set resources group dscp-group group-32-to-39 dscp 36
set resources group dscp-group group-32-to-39 dscp 37
set resources group dscp-group group-32-to-39 dscp 38
set resources group dscp-group group-32-to-39 dscp 39
set resources group dscp-group group-40-to-47 dscp 40
set resources group dscp-group group-40-to-47 dscp 41
set resources group dscp-group group-40-to-47 dscp 42
set resources group dscp-group group-40-to-47 dscp 43
set resources group dscp-group group-40-to-47 dscp 44
set resources group dscp-group group-40-to-47 dscp 45
set resources group dscp-group group-40-to-47 dscp 46
set resources group dscp-group group-40-to-47 dscp 47
set resources group dscp-group group-48-to-55 dscp 48
set resources group dscp-group group-48-to-55 dscp 49
set resources group dscp-group group-48-to-55 dscp 50
set resources group dscp-group group-48-to-55 dscp 51
set resources group dscp-group group-48-to-55 dscp 52
set resources group dscp-group group-48-to-55 dscp 53
set resources group dscp-group group-48-to-55 dscp 54
set resources group dscp-group group-48-to-55 dscp 55
set resources group dscp-group group-56-to-63 dscp 56
set resources group dscp-group group-56-to-63 dscp 57
set resources group dscp-group group-56-to-63 dscp 58
set resources group dscp-group group-56-to-63 dscp 59
set resources group dscp-group group-56-to-63 dscp 60
set resources group dscp-group group-56-to-63 dscp 61
set resources group dscp-group group-56-to-63 dscp 62
set resources group dscp-group group-56-to-63 dscp 63
```

Step 3: Create policy ingress-map and assign designation to each dscp group and make it system-default.

```
set policy ingress-map in-map1 dscp-group group-0-to-7 designation 0
set policy ingress-map in-map1 dscp-group group-8-to-15 designation 1
set policy ingress-map in-map1 dscp-group group-16-to-23 designation 2
set policy ingress-map in-map1 dscp-group group-24-to-31 designation 3
set policy ingress-map in-map1 dscp-group group-32-to-39 designation 4
set policy ingress-map in-map1 dscp-group group-40-to-47 designation 5
set policy ingress-map in-map1 dscp-group group-48-to-55 designation 6
set policy ingress-map in-map1 dscp-group group-56-to-63 designation 7
set policy ingress-map in-map1 system-default
```

Step 4: Create shaper profile and map designation to queue for local traffic and assign priority-local to that queue as shown below.

```
set policy qos name def shaper default profile
set policy qos name def shaper profile profile bandwidth 5Gbit
set policy qos name def shaper profile profile map designation 7 to 0
set policy qos name def shaper profile profile queue 0 priority-local
set policy qos name def shaper profile profile queue 0 traffic-class 0
```

Step 5: attach the qos policy and ingress-map to the physical interface.

```
set interfaces dataplane dp0xe16 policy qos def
set interfaces dataplane dp0xe16 policy ingress-map in-map1
```

Step 5: attach the qos policy and ingress-map to the physical interface.

```
Verify if the BGP originate traffic flows in Priority Local Queue(PLQ).

      show policy qos dp0xe16 brief
      Class TC WRR Pipe-QID  Qlength         PLQ             Counters
      --------------------------------------------------------------------------
      0      0   0                 0 bytes                          0 bytes
                                                                    0 packets
                                                                    0 Tail-drop
                                                                    0 RED-drop
                 1        0        0 bytes     *                10368 bytes
                                                                  122 packets
                                                                    0 Tail-drop
                                                                    0 RED-drop
             1   0                 0 bytes                          0 bytes
                                                                    0 packets
                                                                    0 Tail-drop
                                                                    0 RED-drop
             2   0                 0 bytes                          0 bytes
                                                                    0 packets
                                                                    0 Tail-drop
                                                                    0 RED-drop
             3   0                 0 bytes                          0 bytes
                                                                    0 packets
                                                                    0 Tail-drop
                                                                    0 RED-drop
```

Zero Touch Provisioning (ZTP)

DSCG devices supported by Vyatta are preloaded with Open Network Install Environment (ONIE). ONIE is the combination of a boot loader and a small operating system for network switches that provides an environment for automated NOS installation and provisioning.

When an ONIE device first boots, it tries to find an installer file. The first step is to get an IP address and the way to do this is to use a DHCP server. Aside from providing the network device with an IP address, the DHCP server can also determine where to find an installer on the network, such as on a FTP,TFTP or HTTP server.

There are few configurations to do on the DHCP server for the device to pick the right installer file. Below is a sample DHCP configuration.

Configurations of DHCP Server

```
option configuration-file code 251 = text;
option licensing-file code 252 = text;
#option licensing-path code 253 = text;
```

```
class “vendor-class” {
      match option vendor-class-identifier;
}
subnet 192.168.2.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
    option routers 192.168.2.1;
    default-lease-time 40;
    max-lease-time 100;
    authoritative;
    option domain-name “Domain1.com”;
    option domain-name-servers 23.32.23.32,1.1.1.1,10.12.3.30;
    option ntp-servers 10.12.28.22;
    option log-servers 54.45.54.45,0.0.0.0,12.1.1.1,13.1.1.1,76.1.1.1;
    subclass “vendor-class” “onie_vendor:x86_64-ufispace_s9500_30xs-r0” {
         option vendor-class-identifier “onie_vendor:x86_64-ufispace_s9500_30xs-r0”;
         option default-url “ftp://192.168.2.1/dve-2009-base_20200921T0513-amd64-Build32.2.hybrid.iso-ONIE.bin”;
    }
    range 192.168.2.1 192.168.2.10;
    option licensing-file “ftp://192.168.2.1/IPI-E8C57A186F1B.bin”;
    option configuration-file “ftp://192.168.2.1/ztp_base.xml”;
    #option licensing-path “http://192.168.2.1/server/”;
}
```

With the above configuration, ONIE picks an IP address and from the pool defined by the range parameter and uses the URL provided by “default-url” parameter to download and install the NOS. Once NOS is installed, the switch reboots to Vyatta network operating system.

Once the device boots to the Vyatta network operating system, a NetConf agent starts listening on default port 830. An SDN controller can be used to push the initial configuration on the device using NetConf as the south bound protocol.

The below figure shows the interactions between the different components of the system to achieve ZTP.

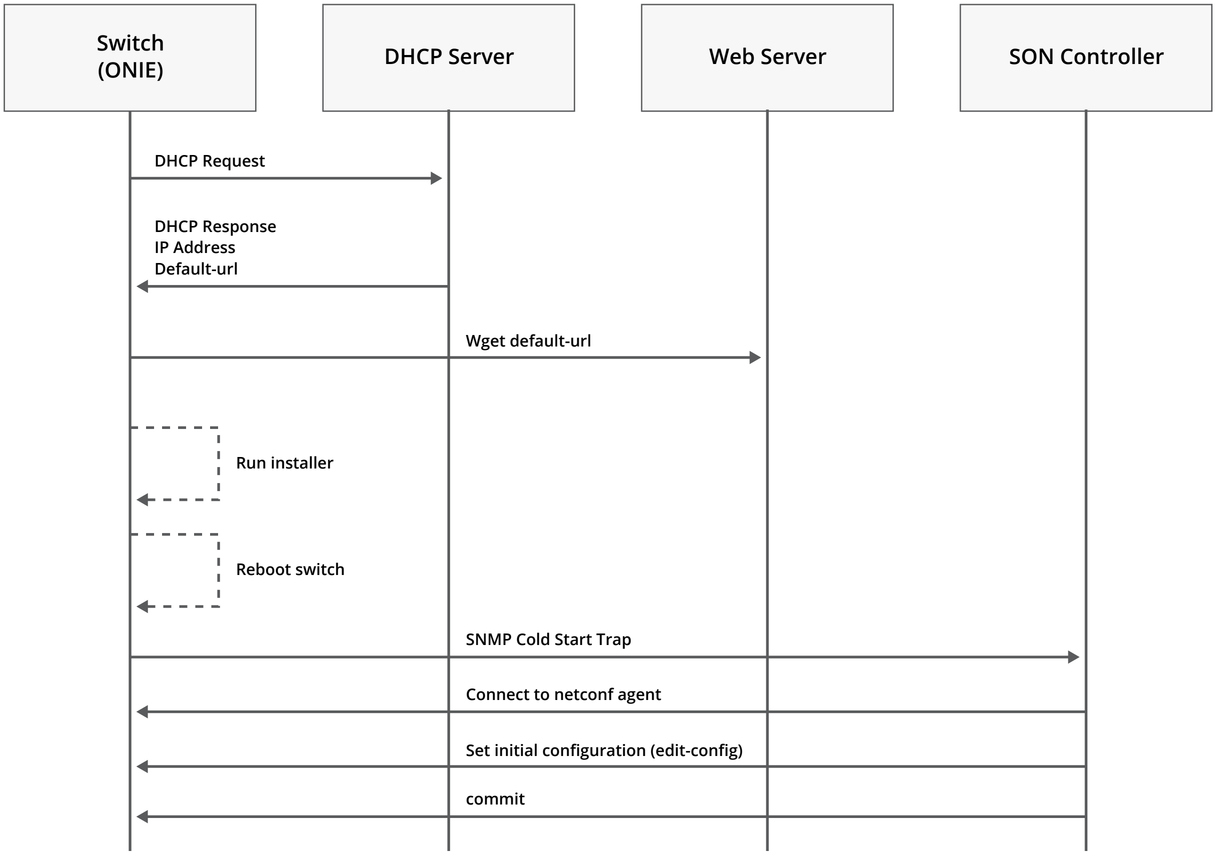


Figure 22: Different Components of the System to Achieve ZTP

Operations and Management

Out-of-band management is configured as a separate routing instance (named "management") on which all management protocols are enabled. A default static route is created in this routing-instance to reach the management stations and ssh/telnet clients in the management network.

This design is used because the default routing instance has a default route installed by OSPF/OSPFv3 so that the DCSG can reach the RNCs/EPCs and Internet.

Configurations for Management Routing-instance

DCSG-1

```
set routing routing-instance management description management
set routing routing-instance management interface dp0p7s0
set routing routing-instance management protocols static route 0.0.0.0/0 next-hop
10.12.87.1
set routing routing-instance management service ssh
set routing routing-instance management service telnet
```

SNMP

Overview

The DCSG Vyatta supports standard SNMP v2c and v3.

Basic Design

The configuration below are for SNMPv2c.

Configurations and Validations

```
# Create snmpv2c community string #
set service snmp community comm-1
#List the snmp clients allowed #
set service snmp community comm-1 client 192.168.1.1
set service snmp community comm-1 client 172.168.1.1
#Set the authorization level for the community string , here it is set to read -write#
set service snmp community comm-1 authorization rw

# Create a view for the community #
set service snmp view commview oid 1.3.6.1.2.1.4
#Bind the view with community string #
set service snmp community comm-1 view commview

# Enabling the Traps and setting a destination for them #
set service snmp notification all

set service snmp trap-target 192.168.1.1
set service snmp trap-target 172.168.1.1

# Set snmp routing context, here done with management #

set service snmp routing-instance management
```

NetConf

Overview

NetConf is a protocol that provides mechanism for installing, manipulating, and deleting the configuration of network devices. In Vyatta, NetConf is used within an SSH session. This mapping allows NetConf to be run from an SSH session by a user or an application. The Vyatta NetConf agent implementation is compliant with RFC 6241 and RFC 6242.

Basic Design

Configuration and monitoring of the network devices involves establishing the NetConf session with the device, getting the schema supported by the device, and get and set operation on various yang models supported by the device. Sample configurations for each of these steps has been provided below.

Configurations and Validations

```
# Enable NetConf service on the device
vyatta@CSR-1# set service netconf
vyatta@CSR-1# commit

# Connect to NetConf agent using SSH
ssh vyatta@10.12.47.77 -s netconf

# Send NetConf hello message to the server
<hello xmlns=”urn:ietf:params:xml:ns:netconf:base:1.0”>
      <capabilities>
            <capability>urn:ietf:params:netconf:base:1.0</capability>
            <capability>urn:ietf:params:netconf:capability:writable-running:1.0</
capability>
            <capability>urn:ietf:params:netconf:capability:candidate:1.0</capability>
            <capability>urn:ietf:params:netconf:capability:startup:1.0</capability>
            <capability>urn:ietf:params:netconf:capability:rollback-on-error:1.0</
capability>
      </capabilities>
</hello>
]]>]]>

# Get the running configuration of the device
<rpc message-id=”102” xmlns=”urn:ietf:params:xml:ns:netconf:base:1.0”>
      <get-config xmlns=”urn:ietf:params:xml:ns:netconf:base:1.0”>
            <source>
                  <running/>
            </source>
      </get-config>
</rpc>]]>]]>

# Set IP address of a loopback interface
<rpc message-id=”101” xmlns=”urn:ietf:params:xml:ns:netconf:base:1.0”>
      <edit-config>
            <target>
                  <candidate/>
            </target>
            <config xmlns=”urn:ietf:params:xml:ns:netconf:base:1.0”>
                  <interfaces xmlns=”urn:vyatta.com:mgmt:vyatta-interfaces:1”>
                        <loopback xmlns=”urn:vyatta.com:mgmt:vyatta-interfaces-
loopback:1”>
                              <tagnode>lo</tagnode>
                              <address>5.5.5.5/32</address>
                        </loopback>
                  </interfaces>
            </config>
      </edit-config>
</rpc>]]>]]>
```

```
<rpc message-id="101" xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
      <commit/>
</rpc>]]>]]>
```

Syslog

Overview

- Significant system events are captured in log messages (also called syslog messages), which you can view on the console, save to a file, forward to an external server such as a syslog server, or direct to the terminal session of one or more specific users.
- Depending on the level of message severity you choose to log, system log messages include notices of ordinary and routine operations as well as warnings, failure, and error messages.
- By default, local logging is enabled and sends messages to the /var/log/messages file.
- Log messages generated by the AT&T Vyatta vRouter are associated with one of the levels of severity in Syslog levels.

Note: Out-Of-Band (OOB) management is enabled as part of this solution guide using the management port (dp0p7s0) for configuring all the management protocols.

TABLE 1-16: SYSLOG LEVELS

SEVERITY	MEANING
emerg	Emergency. A general system failure or other serious failure has occurred, such that the system is unusable.
alert	Alert. Immediate action is required to prevent the system from becoming unstable, for example because a network link has failed or the database has become corrupt.
crit	Critical. A critical condition exists, such as a resource exhaustion- for example the system is out of memory, CPU processing thresholds are being exceeded, or a hardware failure has occurred.
err	Error. An error condition has occurred, such as a failed system call. However the system is still functioning.
Warning	Warning. An event has occurred that has the potential to cause an error, such as invalid parameters being passed to a function. This situation should be monitored.
notice	Notice. A normal but significant event has occurred such as an unexpected event. It is not an error but potentially requires attention.
info	Informational. Normal events of occurring are being reported as they occur.
debug	Debugging Level. Trace Level information is being provided.

A logging server is configured to receive syslogs from the device as per the configuration below.

Configurations and Validations

DCSG-1

```
set routing routing-instance management system syslog host 10.12.47.72 facility all level
warning
set routing routing-instance management system syslog source-interface dp0p7s0
set system syslog console facility all level notice
set system syslog file logfile facility all level notice
set system syslog user vyatta facility auth level notice
set system syslog user vyatta facility dataplane level notice
set system syslog user vyatta facility local5 level notice
```

Baseboard Management Controller (BMC)

Overview

In the S9500-30XS switch, the baseboard management controller (BMC) autonomously monitors system's health including temperature, voltage, fan speed, and so on.

Configurations and Validations

```
set system bmc health-check
set system bmc sel mode circular
set system bmc sel syslog
```

Border Gateway Protocol (BGP) Next Hop Tracking

Overview

BGP maintains a nexthop cache which is refreshed every minute with the current RIB state, where a change in state is applied to the BGP RIB. BGP Nexthop Tracking allows BGP to register the BGP nexthops with the RIB, where any change in the reachability or meta data related to the nexthop is notified to BGP. BGP is then able to apply the event change without having to poll the RIB, improving BGP convergence.

Configurations and Validations

```
set protocols bgp 100 parameters nexthop-tracking delay 5

show protocol bgp nexthop-tracking


Nexthop Tracking is enabled with delay interval 5

Nexthop updates received from RIB: 0


show pro bgp nexthop-cache


Nexthop Tracking is Enabled

Address Family IPv4:

 Nexthop: 10.1.1.2/32 (Single-hop)

   IPv4 Unicast

   Used by: 5 routes

   Reachability: Reachable

   Resolved by: 10.1.1.0/30, Type: connected

   IGP Metric: 0

   Tracking: Enabled
```

```
Nexthop: 20.1.1.2/32 (Single-hop)
   IPv4 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 20.1.1.0/30, Type: connected
   IGP Metric: 0
   Tracking: Enabled
 Nexthop: 30.1.1.2/32 (Single-hop)
   IPv4 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 30.1.1.0/30, Type: connected
   IGP Metric: 0
   Tracking: Enabled
 Nexthop: 40.1.1.2/32 (Single-hop)
   IPv4 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 40.1.1.0/30, Type: connected
   IGP Metric: 0
   Tracking: Enabled
Nexthop: 50.1.1.2/32 (Single-hop)
   IPv4 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 50.1.1.0/30, Type: connected
   IGP Metric: 0
   Tracking: Enabled
Nexthop count : 5
```

```
Address Family IPv6:
 Nexthop: 100::2/128 (Single-hop)
   IPv6 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 100::/126, Type: connected
IGP Metric: 0
   Tracking: Enabled
 Nexthop: 200::2/128 (Single-hop)
   IPv6 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 200::/126, Type: connected
   IGP Metric: 0
   Tracking: Enabled
 Nexthop: 300::2/128 (Single-hop)
   IPv6 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 300::/126, Type: connected
   IGP Metric: 0
   Tracking: Enabled
 Nexthop: 400::2/128 (Single-hop)
   IPv6 Unicast
   Used by: 5 routes
   Reachability: Reachable
   Resolved by: 400::/126, Type: connected
   IGP Metric: 0
   Tracking: Enabled
```

```
Nexthop: 500::2/128 (Single-hop)
  IPv6 Unicast
  Used by: 5 routes
  Reachability: Reachable
  Resolved by: 500::/126, Type: connected
  IGP Metric: 0
  Tracking: Enabled
Nexthop count : 5
```

ABOUT IP INFUSION

IP Infusion, a leader in disaggregated networking solutions, delivers enterprise and carrier-grade software solutions allowing network operators to reduce network costs, increase flexibility, and to deploy new features and services quickly. IP Infusion is headquartered in Santa Clara, Calif., and is a wholly owned and independently operated subsidiary of ACCESS CO., LTD. Additional information can be found at **http://www.ipinfusion.com**

Phone | +1 877-MYZEBOS
Email | sales@ipinfusion.com
Web | www.ipinfusion.com

U.S. (Santa Clara) | +1 408-400-1912
Japan (Tokyo) | +81 03-5259-3771
Korea (Seoul) | +82 10 2733 3016

India (Bangalore) | +91 (80) 6728 7000
China (Shanghai) | +86-186 1658 6466
EMEA | +49 (208) 8290 6464