exaware

CONFIGURATION GUIDE

Network Operating System for Disaggregated IP/MPLS Router Solutions

Networking Solution for building FMC networks. Reference HLD.

www.exaware.com

Disclaimer

Exaware Ltd. 5 Hamelacha St Netanya 42505 ISRAEL
Phone: +972-73-212-4500 Fax: +972-73-212-4600
Email: info@exaware.com
Website: http://www.exaware.com

History of Change

Rev.	Date	Change Description	Author
1.0	2024-11-26	Initial edition	Evgenii Melnikov

Table of Contents

1. Preface

1.1. Preliminary Statements

1.1.1. Intended Audience

This document is intended for network engineers responsible for ExaNOS configuration and management. You should be familiar with basic networking technologies knowledge and have extensive experience in network deployment and management.

1.1.2. Product/Feature Overview

ExaNOS is carrier grade Network Operation System based on a cloud architecture, that developed to rollout on White Box hardware of several manufacturers.

1.2. Reference Matrix

The matrix below contains descriptions of all available reference documents at the time this spec was prepared.

1.2.1. Reference documents

1.2.1.1. Reference documents

Reference Document	Document revision	Number/Page/Paragraph
ExaNOS Command Reference Guide	Release 8.X.0 July 2024	

2. Network architecture

2.1. Concept

In today's rapidly evolving digital landscape, telecommunications networks have undergone a significant transformation, driven by technological advancements and changing consumer demands. The concept of a modern network encompasses a convergence of fixed and mobile technologies, enabling seamless connectivity across diverse devices and applications.

Fixed networks, also known as landline networks, have traditionally provided voice and data services to homes and businesses. IP fixed networks typically consist of DSL and FTTx access technologies.

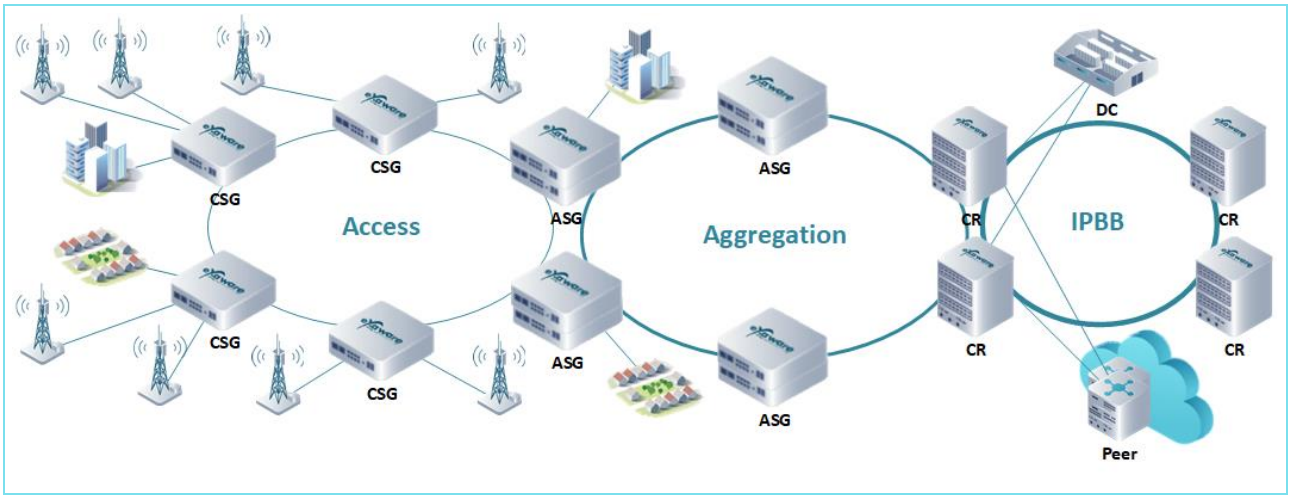
IP Backhaul is a cornerstone of modern networks. This refers to the transport of data traffic between base stations and core network elements using the Internet Protocol (IP). IP backhaul offers several key benefits, including:

Fixed-Mobile Convergence (FMC) is another critical aspect of modern networks. It involves the integration of fixed and mobile networks to provide a unified, seamless user experience. FMC enables subscribers to access services and applications across multiple devices, regardless of their location. Key benefits of FMC include enhanced customer experience, increased efficiency, and new revenue opportunities.

In the following chapters, we will dig deeper into the architecture, functionalities and configuration of modern networks, including IP backhaul and FMC based on ExaNOS enabled devices. (ExaNOS - Exaware Network Operation System).

2.2. Network design

2.2.1.1. FMC networking topology



3. Interfaces

This chapter covers aspects of interface planning, including interface types, IP addressing, and configuration best practices.

Note that in addition to the key fundamental interface features such as media type, speed, MTU, and IP planning, it's crucial to consider interface types based on their placement within the network hierarchy:

- UNI (User Network Interface): Interfaces designed to connect directly to customer devices or services, typically located at the edge of the network.
- NNI (Network-to-Network Interface): Interfaces used to interconnect with other networks or providers, often found at the core or aggregation layers of the network.

3.1. Physical design

In designing the physical IP backhaul for an FMC network, interface speeds are typically selected based on traffic demands and scalability requirements.

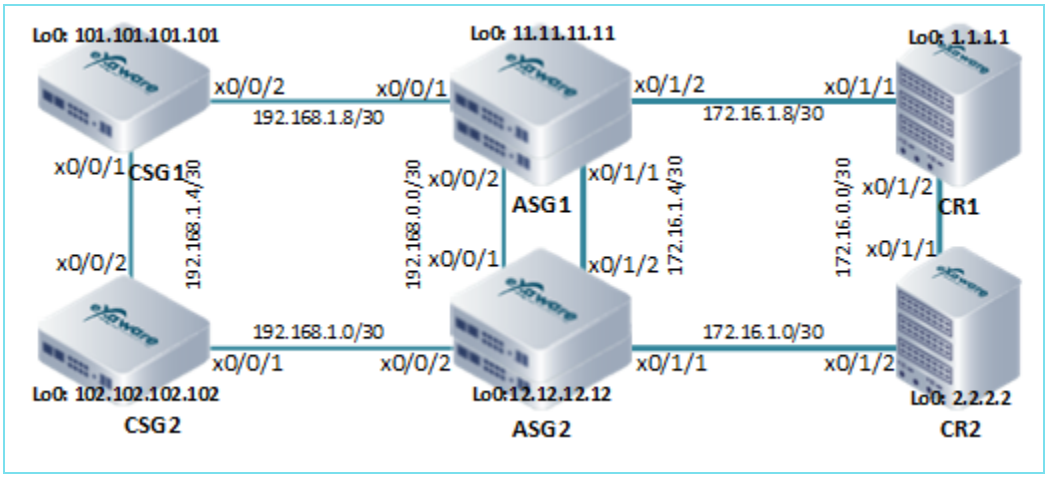
Generally, the network consists of up to ten aggregation rings connected to a pair of core routers, with each aggregation ring supporting two to ten access rings. At the access layer, 1G or 10G interfaces are typically sufficient, depending on endpoint density and projected growth. Moving up to the aggregation layer, 10G or 100G interfaces are usually chosen to handle higher cumulative traffic loads. At the core layer, 100G interfaces are generally required to manage the aggregated

traffic from all rings, ensuring capacity and reliability across the network. This approach enables efficient scaling and high performance from access to core.

3.2. IP design

3.2.1. Interfaces and IP topologies

3.2.1.1. Interfaces and IP topology



3.2.2. IP interfaces

3.2.2.1. IP interface configuration for CSG1

Command	Description
!	
interface x-eth 0/0/1	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface state
description to_CSG2_x0/0/2	Interface description for appropriate labelling
!	
interface x-eth 0/0/1.100	Sub-Interface view
ipv4-address 192.168.1.6/30	Assign IPv4 address to the interface

vlan-id 100	VLAN tag for the sub-interface
description to_CSG2_x0/0/2.100	Interface description for appropriate labelling
!	
interface x-eth 0/0/2	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface state
description to_ASG1_x0/0/1	Interface description for appropriate labelling
!	
interface x-eth 0/0/2.200	Sub-Interface view
ipv4-address 192.168.1.9/30	Assign IPv4 address to the interface
vlan-id 200	VLAN tag for the sub-interface
description to_CSG1_x0/0/1.100	Interface description for appropriate labelling
!	
interface loopback 0	Loopback Interface view
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
description RouterID	Interface description
!	

4. IGP

4.1. IGP Concept

IGP plays a crucial role in enabling efficient communication and data routing within a modern network infrastructure.

Both OSPF and ISIS are suitable choices for IGP due to their scalability, reliability, and support for various network topologies and protocols. The choice between OSPF and ISIS often depends on specific network requirements, such as the size of the network, the supported protocols, and the desired level of hierarchical routing. Also, possible solution of deploying of both protocols the same time with isolation one IGP domain from another.

While OSPF remains a reliable and widely used routing protocol, ISIS consistently demonstrates superior scalability for large-scale networks. Its hierarchical design and efficient routing protocols enable it to handle complex topologies and heavy traffic loads more effectively. However, OSPF

may be a better fit in smaller networks or scenarios where simplicity and ease of configuration are paramount.

4.2. IGP hierarchy

4.2.1. IGP hierarchy concept

Dividing large IGP domains of IP backhauls into independent sub-domains is a critical strategy for improving network scalability, reliability, security, and performance. By carefully designing and managing sub-domains, network operators can ensure that their IP backhaul networks remain efficient and resilient in the face of growth and change. The reasons are:

Scalability: Reduced Routing Table Size: As the size of an IGP domain increases, so does the amount of routing information that each router needs to maintain. Dividing the domain into sub-domains reduces the size of routing tables, improving router performance and reducing memory requirements.

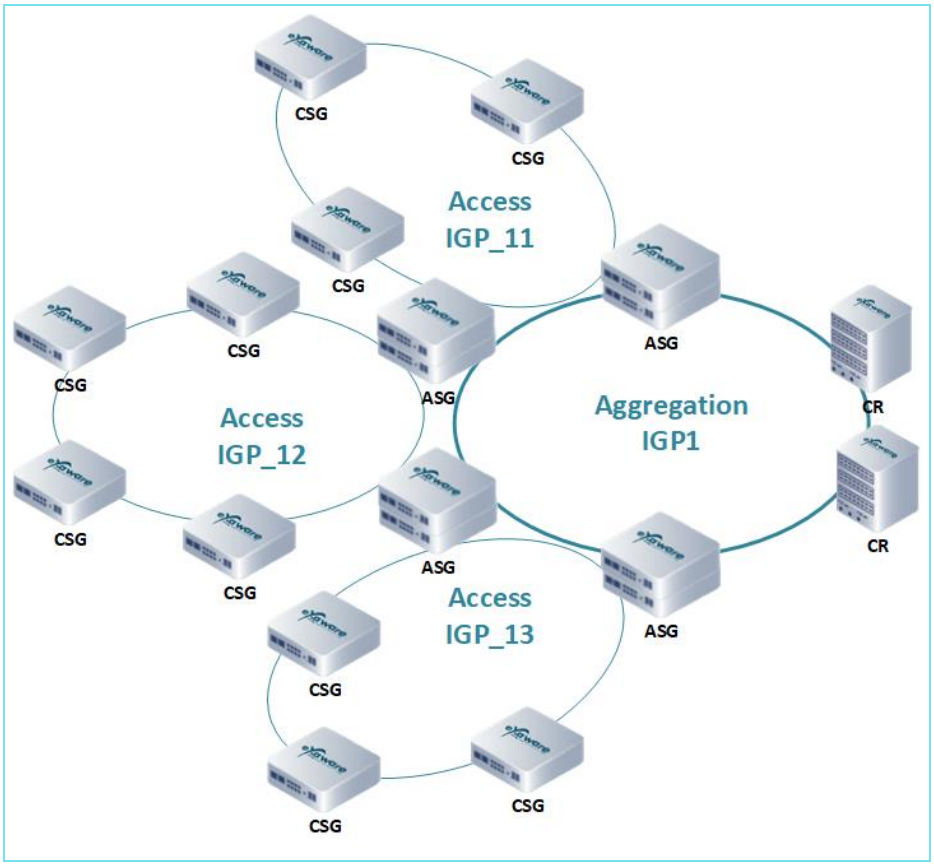
Faster Convergence: When a topology change occurs within a large domain, it can take a considerable amount of time for routing updates to propagate throughout the entire network. Dividing the domain into sub-domains can significantly reduce convergence time, as routing updates only need to propagate within the affected sub-domain.

Fault Isolation: Containment of Routing Disruptions: If a failure occurs within a sub-domain, the impact on the overall network can be minimized by isolating the disruption to that sub-domain. This helps to prevent routing black holes and other widespread network issues.

Simplified Troubleshooting: By dividing the network into smaller, more manageable sub-domains, it becomes easier to identify and troubleshoot problems.

Performance Optimization: Traffic Engineering: Sub-domains can be used to implement traffic engineering techniques, such as load balancing and traffic shaping, to optimize network performance and utilization.

4.2.1.1. IGP instances hierarchy



4.3. OSPF based solution

4.3.1. OSPF Concepts

OSPF hierarchical routing can be achieved by dividing the network into areas, and routers within an area exchange routing information only with other routers in the same area, which can improve scalability and performance in large networks.

When an OSPF network is divided into independent sub-domains, the exchange of Link-State Advertisements (LSAs) is restricted to within each sub-domain. This means that LSAs from one sub-domain do not propagate to other sub-domains. In such a scenario, the overall network connectivity is typically achieved using external routing protocols like Border Gateway Protocol (BGP).

When OSPF is divided into isolated sub-domains, it's essential to ensure that LSAs do not propagate between domains. Isolation can be achieved by one of the following methods: by filtering on ABRs, by splitting OSPF into different processes, by avoiding zero-area.

4.3.2. OSPF Multi-Instance

With **VRF multi-instance**, OSPF instances are tied to Virtual Routing and Forwarding (VRF) tables, allowing for network segmentation in a multi-tenant environment. Each VRF instance maintains its own routing table, isolating routes between different networks, which is particularly useful in scenarios like MPLS VPNs where traffic and routing information need to remain separated between customers or departments.

The **process multi-instance** involves running multiple OSPF processes on the same router, where each instance serves distinct segments of the network. This is beneficial when you need to segment internal routing across different domains or regions, allowing for more granular control of routing policies and avoiding a single OSPF process that would otherwise aggregate all routes into one database. These instances ensure greater flexibility and isolation for scalability and security in complex network designs.

4.3.2.1. OSPF Multi-Instance example

Command	Description
!	
vrf VA1 rd 1:1 af-ipv4 unicast	VRF configuration (one line style)
vrf VA2 rd 1:2 af-ipv4 unicast	VRF configuration (one line style)
!	
interface x-eth 0/0/1	Interface view
description to_PEER_port_x0/0/1	Interface description for appropriate labelling
admin-state up	Interface state
!	
interface x-eth 0/0/1.1 ipv4-address 172.16.1.1/30 vrf VA1 vlan-id 101 description toDev-2_x0/0/1.1	Sub-Interface view and configuration (one line style)
!	
interface x-eth 0/0/1.2 ipv4-address 172.16.2.1/30 vrf VA2 vlan-id 102 description toDev-2_x0/0/1.2	Sub-Interface view and configuration (one line style)
!	

routing ospf 1 vrf VA1 area 0.0.0.1 interface x0/0/1.1 mtu 1500 network point-to-point	Routing OSPF process and configuration (one line style)
!	
routing ospf 2 vrf VA2 area 0.0.0.1 interface x0/0/1.2 mtu 1500 network point-to-point	Routing OSPF process and configuration (one line style)
!	
routing ospf 1 vrf VA1 redistribute connected	Routing OSPF process and additional configuration (one line style)
!	
routing ospf 2 vrf VA2 redistribute connected	Routing OSPF process and additional configuration (one line style)
!	

4.3.3. OSPF fast convergence

4.3.3.1. OSPF fast convergence

Command	Description
!	
routing ospf 1	Routing OSPF process tag "1"
vrf default	GRT view for the protocol
router-id 101.101.101.101	Router ID
fast-reroute enable	Enable IP FRR
ldp-synchronization enable	Enable LDP synchronization
area 0.0.0.1	OSPF AREA view
interface x-eth 0/0/1.100	Interface view in protocol view
!	

4.3.4. OSPF configuration for CSG1

This chapter provides a comprehensive guide to configuring OSPF on ExaNOS enabled network.

4.3.4.1. OSPF configuration for CSG1

Command	Description
!	

routing ospf 1	Routing OSPF process tag "1"
vrf default	GRT view for the protocol
mpls-te enable	Enable MPLS for the section
distance	Configure administrative distance
admin-distance 120	Configure administrative distance
!	
redistribute static policy STATIC_TO_OSPF	Refer to Route policy
router-id 101.101.101.101	Router ID
fast-reroute enable	Enable FRR
ldp-synchronization enable	Enable LDP synchronization
area 0.0.0.1	OSPF AREA view
interface x-eth 0/0/1.100	Interface view in protocol view
network-type point-to-point	Network type
mtu 1500	Set MTU
authentication-key md5 key-id 1	Enable authentication key
password 123456	Set password for the link authentication
!	
interface x-eth 0/0/2.200	Interface view in protocol view
network-type point-to-point	Network type
mtu 1500	Set MTU
authentication-key md5 key-id 1	Enable authentication key
password 123456	Set password for the link authentication
!	
interface loopback 0	Reference to interface
passive enable	Passive for adjacency. Stop sending outgoing hello packets, hence the router cannot form any neighbor relationships via the passive interface. This behavior stops both outgoing and incoming routing updates.
!	
!	
!	
!	
policy route STATIC_TO_OSPF	Route policy
rule permit_77.0.123.1	Set policy rule
if prefix exist-in (77.0.123.1/32)	IF-condition in policy
then permit	Permit routes
end-policy	End Policy view

!	
routing static	Static routing section
vrf default	GRT view for the protocol
af-ipv4 unicast	IPv4 Address Family
route 77.0.123.1/32 gateway 192.168.134.161	Set specific route
route 172.22.80.0/24 gateway 192.168.135.1	Set specific route
route 10.10.0.0/23 gateway 192.168.137.97	Set specific route
!	
!	

4.3.5. OSPF configuration for ASG1

4.3.5.1. OSPF configuration for ASG1

Command	Description
!	
routing ospf 1	Routing OSPF process tag "1"
vrf default	GRT view for the protocol
mpls-te enable	Enable MPLS for the section
distance	Configure administrative distance
admin-distance 120	Configure administrative distance
!	
redistribute connected policy Loopback0_TO_OSPF	Redistribute Loopback0 prefix (it is advertised in another OSPF process)
router-id 11.11.11.11	Router ID
fast-reroute enable	Enable FRR
ldp-synchronization enable	Enable LDP synchronization
area 0.0.0.1	OSPF AREA view
interface x-eth 0/0/1.100	Interface view in protocol view
network-type point-to-point	Network type
mtu 1500	Set MTU
authentication-key md5 key-id 1	Enable authentication key
password 123456	Set password for the link authentication
!	
interface x-eth 0/0/2.300	Interface view in protocol view
network-type point-to-point	Network type

mtu 1500	Set MTU
authentication-key md5 key-id 1	Enable authentication key
password 123456	Set password for the link authentication
!	
!	
!	
routing ospf 2	Routing OSPF process tag "2"
vrf default	GRT view for the protocol
mpls-te enable	Enable MPLS for the section
distance	Configure administrative distance
admin-distance 120	Configure administrative distance
!	
router-id 11.11.11.11	Router ID
fast-reroute enable	Enable FRR
ldp-synchronization enable	Enable LDP synchronization
area 0.0.0.2	OSPF AREA view
interface x-eth 0/1/1.100	Interface view in protocol view
network-type point-to-point	Network type
mtu 1500	Set MTU
authentication-key md5 key-id 1	Enable authentication key
password 123456	Set password for the link authentication
!	
Interf0ace x-eth 0/1/2.200	Interface view in protocol view
network-type point-to-point	Network type
mtu 1500	Set MTU
authentication-key md5 key-id 1	Enable authentication key
password 123456	Set password for the link authentication
!	
interface loopback 0	Reference to interface
passive enable	Passive for adjacency. Stop sending outgoing hello packets, hence the router cannot form any neighbor relationships via the passive interface. This behavior stops both outgoing and incoming routing updates.
!	
!	
!	
policy route Loopback0_TO_OSPF	Route policy

rule permit_Lo0	Set policy rule
if prefix exist-in (11.11.11.11/32)	IF-condition in policy
then permit	Permit routes
end-policy	End Policy view
!	

4.4. ISIS based solution

4.4.1. ISIS concept

While ISIS doesn't explicitly use the term "areas", it achieves hierarchical routing using a similar concept: levels.

- Level 1: This level is used for intra-domain routing.
- Level 2: This level is used for inter-domain routing.

In ISIS, domain isolation is achieved through the system concept. A system is a logical entity that represents a single routing domain. Routers within a system exchange routing information only with other routers in the same system.

ISIS domain isolation can be achieved through:

- Assign unique system IDs to each domain.
- Limit Level 2 advertising to specific interfaces or areas to prevent LSAs from propagating between domains.
- Configure systems as stub systems to prevent them from receiving or originating Level 2 LSAs.
- Divide ISIS processes among domains.

4.4.2. ISIS Multi-Instance

4.4.2.1. ISIS Multi-Instance example

Command	Description
!	
vrf a1	VRF configuration
rd 100:1	Set Route Distinguisher
af-ipv4 unicast	IPv4 Address Family
!	

vrf a2	VRF configuration
rd 100:2	Set Route Distinguisher
af-ipv4 unicast	IPv4 Address Family
!	
interface x-eth 0/0/5.1	Sub-Interface view
ipv4-address 192.168.1.2/30	Assign IPv4 address to the interface
vrf a1	Refers existing VRF name
vlan-id 101	VLAN tag for the sub-interface
!	
interface x-eth 0/0/5.2	Sub-Interface view
ipv4-address 192.168.2.2/30	Assign IPv4 address to the interface
vrf a2	Refers existing VRF name
vlan-id 102	VLAN tag for the sub-interface
!	
interface loopback 1	Loopback Interface view
ipv4-address 96.168.1.1/32	Assign IPv4 address to the interface
vrf a1	Refers existing VRF name
!	
interface loopback 2	Loopback Interface view
ipv4-address 96.168.2.1/32	Assign IPv4 address to the interface
vrf a2	Refers existing VRF name
!	
routing isis 1	Routing ISIS process tag “1”
is-type level-2-only	ISIS level
net 49.0000.0000.0000.1001.00	ISIS NET
vrf a1	Refers existing VRF name
interface x-eth 0/0/5.1	Interface view in protocol view
af-ipv4 unicast	IPv4 Address Family
!	
!	
interface loopback 1	Loopback Interface in ISIS view
passive enable	Passive for adjacency. Stop sending outgoing hello packets, hence the router cannot form any neighbor relationships via the passive interface. This behavior stops both outgoing and incoming routing updates.
af-ipv4 unicast	IPv4 Address Family
!	

!	
routing isis 2	Routing ISIS process tag "2"
is-type level-2-only	ISIS level
net 49.0000.0000.0000.1002.00	ISIS NET
vrf a2	Refers existing VRF name
interface x-eth 0/0/5.2	Interface view in protocol view
af-ipv4 unicast	IPv4 Address Family
!	
!	
interface loopback 2	Interface view in protocol view
passive enable	
af-ipv4 unicast	IPv4 Address Family
!	
!	
!	

4.4.3. ISIS fast convergence

4.4.3.1. ISIS fast convergence

Command	Description
!	
routing isis 1	ISIS section
is-type level-2-only	ISIS level
net 49.0930.1008.2371.0001.00	ISIS NET
fast-reroute enable	Enable IP FRR
af-ipv4 unicast	IPv4 Address Family
router-id 94.94.94.94	Router ID
level 2-only	ISIS level
!	
!	
interface x-eth 0/0/62.10	Interface view in protocol view
network point-to-point	Network type
af-ipv4 unicast	IPv4 Address Family
!	

!	
!	

4.4.4. ISIS configuration for CSG1

This chapter provides a comprehensive guide to configuring ISIS on ExaNOS enabled network

4.4.4.1. ISIS configuration for CSG1

Command	Description
!	
routing isis 1	ISIS section
is-type level-2-only	ISIS level
net 49.0000.0000.0000.0001.00	ISIS NET
fast-reroute enable	Enable FRR
log-adjacency-changes enable	Enable logging of adjacency changes
ldp-synchronization enable	Enable LDP Synchronization
af-ipv4 unicast	IPv4 Address Family
mpls-te	Enable MPLS for the section
router-id 101.101.101.101	Router ID
level 2-only	ISIS levelin MPLS-TE DB
!	
!	
interface x-eth 0/0/62.10	Interface view in protocol view
network point-to-point	Network type
af-ipv4 unicast	IPv4 Address Family
!	
!	
interface loopback 0	Interface view in protocol view
af-ipv4 unicast	IPv4 Address Family
!	
!	
!	

4.4.5. ISIS configuration for ASG1

4.4.5.1. ISIS configuration for ASG1

Command	Description
!	
routing isis 1	ISIS section
is-type level-2-only	ISIS level
net 49.0000.0000.0000.0001.00	ISIS NET
fast-reroute enable	Enable FRR
log-adjacency-changes enable	Enable logging of adjacency changes
ldp-synchronization enable	Enable LDP Synchronization
af-ipv4 unicast	IPv4 Address Family
redistribute connect policy Loopback0_TO_ISIS	Redistribute Loopback0 prefix (it is advertised in another ISIS instance-process)
mpls-te	Enable MPLS for the section
router-id 11.11.11.11	Router ID
level 2-only	ISIS levelin MPLS-TE DB
!	
interface x-eth 0/0/1.100	Interface view in protocol view
network point-to-point	Network type
af-ipv4 unicast	IPv4 Address Family
!	
interface x-eth 0/0/2.200	Interface view in protocol view
network point-to-point	Network type
af-ipv4 unicast	IPv4 Address Family
!	
!	
routing isis 2	ISIS section
is-type level-2-only	ISIS level
net 49.0000.0000.0000.1001.00	ISIS NET
fast-reroute enable	Enable FRR
log-adjacency-changes enable	Enable logging of adjacency changes
ldp-synchronization enable	Enable LDP Synchronization
af-ipv4 unicast	IPv4 Address Family

mpls-te	Enable MPLS for the section
router-id 11.11.11.11	Router ID
level 2-only	ISIS levelin MPLS-TE DB
!	
interface x-eth 0/1/1.100	Interface view in protocol view
network point-to-point	Network type
af-ipv4 unicast	IPv4 Address Family
!	
interface x-eth 0/1/2.200	Interface view in protocol view
network point-to-point	Network type
af-ipv4 unicast	IPv4 Address Family
!	
interface loopback 0	Interface view in protocol view
passive enable	IPv4 Address Family
!	
!	
!	
!	
policy route Loopback0_TO_ISIS	Route policy
rule permit_Lo0	Set policy rule
if prefix exist-in (11.11.11.11/32)	IF-condition in policy
then permit	Permit routes
end-policy	End Policy view
!	

5. BGP

5.1.1. BGP concept

MP-BGP is an extension of BGP that allows for the routing of multiple address families and SAFIs. This is crucial for supporting diverse network environments and protocols on MPLS networks. MP-BGP supports various AFI/SAFI combinations.

By establishing peering relationships between sub-domains, BGP enables seamless communication and data exchange across the entire network. This process, often referred to as network stitching, is

essential for maintaining network connectivity and ensuring that traffic can flow between different parts of the backhaul infrastructure.

5.1.2. BGP configurations

This chapter provides a comprehensive guide to configuring BGP on ExaNOS enabled network

5.1.2.1. BGP configuration for CSG1

Command	Description
!	
routing bgp 65000	BGP routing protocol view
router-id 101.101.101.101	Router ID
vrf default	GRT view for the protocol
neighbor 11.11.11.11	Refers to the neighbor IP
local-address loopback 0	Refers to the local interface
!	
remote-as-number 65000	Set remote AS for neighboring
af-ipv4 unicast	IPv4 Address Family
send-community all	Enable community of all types in messages to send
!	
af-ipv4 vpn	Enter VPNv4 section
send-community standard	Enable community of the type “Standard” in messages to send
!	
!	
!	
!	

5.1.2.2. BGP configuration for ASG1

Command	Description
!	
routing bgp 65000	BGP routing protocol view

router-id 11.11.11.11	Router ID
vrf default	GRT view for the protocol
neighbor 101.101.101.101	Refers to the neighbor IP
local-address loopback 0	Refers to the local interface
!	
remote-as-number 65000	Set remote AS for neighboring
af-ipv4 unicast	IPv4 Address Family
route-reflector-client enable	Enable BGP route reflector function for the neighbor
next-hop-self enable	Enable Next Hop Self function to the neighbor
send-community all	Enable community of all types in messages to send
!	
af-ipv4 vpn	Enter VPNv4 section
route-reflector-client enable	Enable BGP route reflector function for the neighbor
send-community standard	Enable community of the type “Standard” in messages to send
!	
!	
neighbor 1.1.1.1	Refers to the neighbor IP
local-address loopback 0	Refers to the local interface
!	
remote-as-number 65000	Set remote AS for neighboring
af-ipv4 unicast	IPv4 Address Family
next-hop-self enable	Enable Next Hop Self function to the neighbor
send-community all	Enable community of all types in messages to send
!	
af-ipv4 vpn	Enter VPNv4 section
send-community standard	Enable community of the type “Standard” in messages to send
!	
!	
neighbor 2.2.2.2	Refers to the neighbor IP
local-address loopback 0	Refers to the local interface
!	
remote-as-number 65000	Set remote AS for neighboring
af-ipv4 unicast	IPv4 Address Family
next-hop-self enable	Enable Next Hop Self function to the neighbor
send-community all	Enable community of all types in messages to send

!	
af-ipv4 vpn	Enter VPNv4 section
send-community standard	Enable community of the type “Standard” in messages to send
!	
!	
!	
!	

6. MPLS

Multiprotocol Label Switching (MPLS) provides efficient and scalable way to forward packets through a network by using labels, which are short identifiers attached to packets as they traverse the network. These labels are used to make forwarding decisions, bypassing the routing table lookups.

MPLS relies on two essential IP transport technologies: LDP (Label Distribution Protocol) and RSVP-TE (Resource Reservation Protocol - Traffic Engineering). These protocols can be deployed independently or in conjunction with each other, depending on the specific network requirements and desired functionalities.

6.1.1. MPLS deployment

This chapter provides a comprehensive guide to configuring MPLS on ExaNOS enabled network

6.1.1.1. MPLS configuration for CSG1

Command	Description
!	
interface x-eth 0/0/1	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface state
description to_CSG1_x0/0/2	Interface description for appropriate labelling
!	
interface x-eth 0/0/1.100	Sub-Interface view

ipv4-address 122.168.1.6/30	Assign IPv4 address to the interface
mpls enable	Enable MPLS for sub-interface
vlan-id 100	VLAN tag for the sub-interface
description to_CSG1_x0/0/2.100	Interface description for appropriate labelling
!	
interface x-eth 0/0/2	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface state
description to_ASG1_x0/0/1	Interface description for appropriate labelling
!	
interface x-eth 0/0/2.200	Sub-Interface view
ipv4-address 192.168.1.9/30	Assign IPv4 address to the interface
mpls enable	Enable MPLS for sub-interface
vlan-id 200	VLAN tag for the sub-interface
description to_CSG1_x0/0/1.100	Interface description for appropriate labelling
!	
interface loopback 0	Loopback Interface view
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
description RouterID	Interface description
!	

6.2. LDP

6.2.1. LDP concept

LDP is responsible for distributing labels between MPLS routers. Labels are used to identify specific paths through the network, allowing for faster and more efficient packet forwarding. LDP is typically deployed on all MPLS routers within a sub-domain. It establishes peering relationships with neighboring routers and exchanges label information using a flooding mechanism and IGP database. LDP is essential for the basic operation of MPLS networks.

6.2.2. LDP deployment

This chapter provides a comprehensive guide to configuring LDP on ExaNOS enabled network

6.2.2.1. LDP configuration for CSG1

Command	Description
!	
interface x-eth 0/0/1	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_CSG1_x0/0/2	Interface description for appropriate labelling
!	
interface x-eth 0/0/1.100	Sub-interface view
ipv4-address 122.168.1.6/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface
vlan-id 100	VLAN tag for the sub-interface
description to_CSG1_x0/0/2.100	Interface description for appropriate labelling
!	
interface x-eth 0/0/2	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_ASG1_x0/0/1	Interface description for appropriate labelling
!	
interface x-eth 0/0/2.200	Sub-interface view
ipv4-address 192.168.1.9/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface
vlan-id 200	VLAN tag for the sub-interface
description to_CSG1_x0/0/1.100	Interface description for appropriate labelling
!	
interface loopback 0	Interface view (Loopback)
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
description RouterID	Interface description
!	
policy route LDP_LABEL_HOST	Policy route for LDP label distribution rules
rule rule1	Set policy rule
if match-any	IF-condition in policy
prefix exist-in (0.0.0.0/0 matching-len 32)	Match prefix, in this case all /32 host routes
then permit	Permit routes
end-policy	Leave policy route

!	
mpls ldp default	LDP section view
local-address ipv4 101.101.101.101	Source IP for LDP
router-id 101.101.101.101	LDP Router ID
interface x-eth 0/0/1.100	Enable LDP on existing interface
af-ipv4	IPv4 family
!	
interface x-eth 0/0/2.200	Enable LDP on existing interface
af-ipv4	IPv4 family
!	
label-allocation policy LDP_LABEL_HOST	Use existing policy route
!	

6.3. RSVP-TE

6.3.1. RSVP-TE concept

RSVP-TE is used to reserve resources (e.g., bandwidth) for specific traffic flows. This is particularly important for applications that require guaranteed quality of service, such as voice and video. RSVP-TE is then typically deployed on MPLS routers that are part of the desired LSPs. It involves sending signaling messages to reserve resources along the path.

The RSVP-TE process involves two main message types: PATH and RESV. The PATH message initiates the reservation process by containing the sender's address, desired bandwidth, and QoS parameters. This message travels downstream from the sender. In response, the RESV message confirms resource allocation, including requested bandwidth and QoS attributes, and travels upstream from the receiver to the sender.

Key mandatory parameters in RSVP-TE include Affinity, which indicates constraints or preferences for path selection; Bandwidth, specifying the minimum bandwidth required for the flow; End Points, which identify the source and destination addresses; and Traffic Control Parameters, such as Latency and Jitter, which define desired delay characteristics and maximum allowed packet arrival time variation, respectively.

RSVP-TE can be used in conjunction with LDP to create LSPs with guaranteed bandwidth and performance. It is often used for traffic engineering purposes, such as load balancing or congestion avoidance.

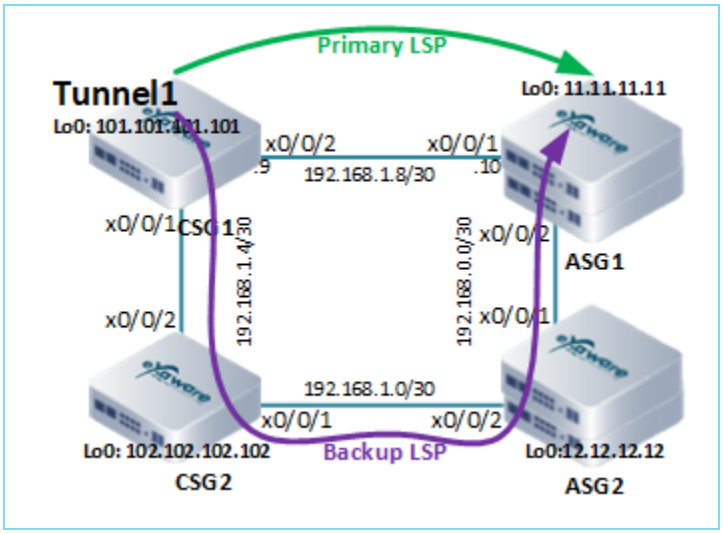
6.3.2. RSVP-TE protection scenarios

In the context of **RSVP-TE (Resource Reservation Protocol - Traffic Engineering)**, both Backup LSPs (Label Switched Paths) and Fast Reroute (FRR) are mechanisms designed to improve network reliability and availability by providing alternative paths in case of failure. However, they function differently in terms of protection, restoration, and the mechanisms involved.

- A **Backup LSP** is a pre-established secondary Label Switched Path that is created in advance and remains in standby mode. It can be utilized if the primary LSP experiences a failure. Backup protection with always up backup LSP is called Hot-Standby (HSB).
- **FRR** is a local protection mechanism where, upon a local link or node failure, the router quickly reroutes traffic to a pre-configured detour path. This reroute happens in milliseconds, minimizing traffic disruption. Legacy FRR uses two methods for protection:
    - **One-to-One Protection**: A separate bypass tunnel is pre-established (Hot Standby) for each protected LSP.
    - **Many-to-One Protection**: A single bypass tunnel can protect multiple LSPs passing through a common link or node. In this case additional label (in label stack) is used for bypass tunnel. Many-to-One LSP provides **Facility** for protection of several RSVP-TE Tunnels.

6.3.3. RSVP-TE One-to-One protection

6.3.3.1. RSVP-TE backup LSP protection (Hot-Standby)



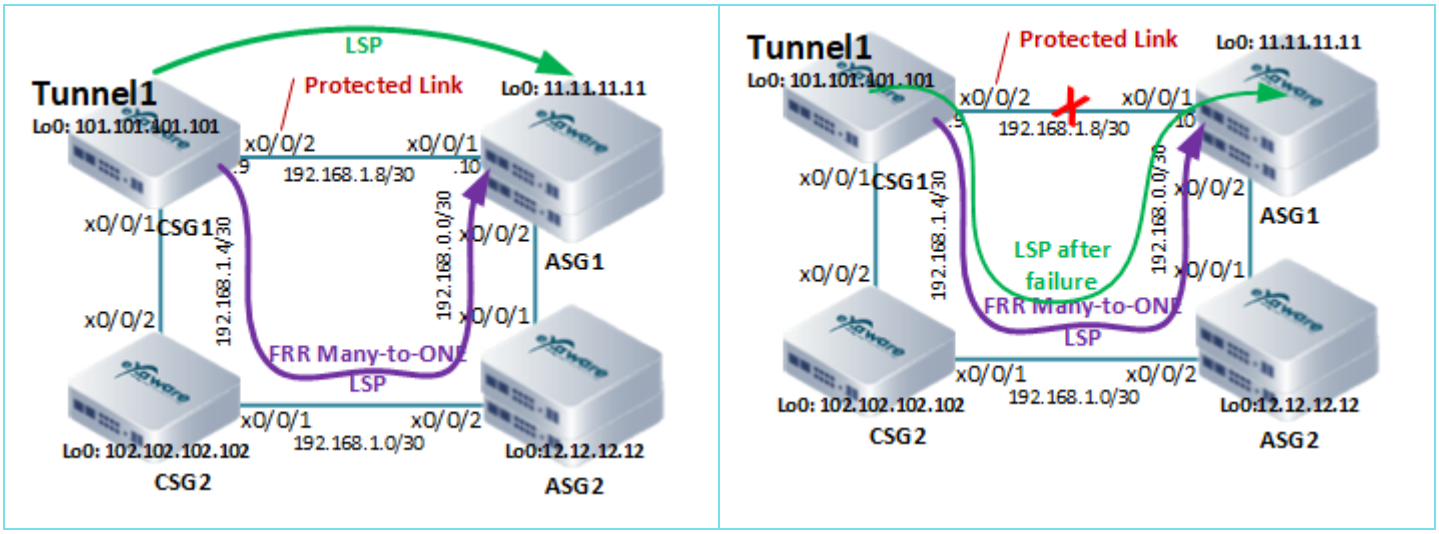
6.3.3.2. Configuration example for RSVP-TE backup LSP protection (Head End only)

Command	Description
!	
interface x-eth 0/0/1	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_CSG1_x0/0/2	Interface description
!	
interface x-eth 0/0/1.100	Sub-interface view
ipv4-address 122.168.1.6/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface
vlan-id 100	VLAN tag for the sub-interface
description to_CSG1_x0/0/2.100	Interface description for appropriate labelling
!	
interface x-eth 0/0/2	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_ASG1_x0/0/1	Interface description for appropriate labelling
!	
interface x-eth 0/0/2.200	Sub-interface view

ipv4-address 192.168.1.9/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface
vlan-id 200	VLAN tag for the sub-interface
description to_CSG1_x0/0/1.100	Interface description for appropriate labelling
!	
interface loopback 0	Interface view (Loopback)
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
description RouterID	Interface description
!	
mpls te rsvp default	RSVP-TE section
ip-source 101.101.101.101	IP source (by default) for RSVP-TE
interface x-eth 0/0/1.100	Enable RSVP-TE on existing interface
interface x-eth 0/0/2.200	Enable RSVP-TE on existing interface
!	
tunnel-te toASG1	Tunnel interface
tunnel-destination 11.11.11.11	Tunnel destination
tunnel-source 101.101.101.101	Tunnel source
secondary default	Enable Backup LSP
cspf enable	Use CSPF for backup LSP
standby enable	Make backup LSP standby
!	
!	
!	

6.3.4. RSVP-TE FRR protection

6.3.4.1. RSVP-TE FRR protection (LSP before and after failure)



6.3.4.2. Configuration example for RSVP-TE FRR protection

Command	Description
!	
interface x-eth 0/0/1	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_CSG1_x0/0/2	Interface description
!	
interface x-eth 0/0/1.100	Sub-interface view
ipv4-address 122.168.1.6/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface
vlan-id 100	VLAN tag for the sub-interface
description to_CSG1_x0/0/2.100	Interface description for appropriate labelling
!	
interface x-eth 0/0/2	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_ASG1_x0/0/1	Interface description for appropriate labelling
!	
interface x-eth 0/0/2.200	Sub-interface view
ipv4-address 192.168.1.9/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface

vlan-id 200	VLAN tag for the sub-interface
description to_CSG1_x0/0/1.100	Interface description for appropriate labelling
local-protection node-link	Specify that LSP going through the specified interface will be protected by a bypass tunnel in node-link mode.
!	
interface loopback 0	Interface view (Loopback)
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
description RouterID	Interface description
!	
mpls te rsvp default	RSVP-TE section
ip-source 101.101.101.101	IP source (by default) for RSVP-TE
interface x-eth 0/0/1.100	Enable RSVP-TE on existing interface
interface x-eth 0/0/2.200	Enable RSVP-TE on existing interface
!	
tunnel-te toASG1	Tunnel interface
tunnel-destination 11.11.11.11	Tunnel destination
tunnel-source 101.101.101.101	Tunnel source
cspf enable	Use CSPF for LSP
local-protection node-link	Specify that a tunnel will request a node-link protection.
!	
!	
!	

6.3.5. RSVP-TE affinity

An affinity is a 128-bit vector that describes the links to be used by a TE tunnel. It is configured and implemented on the tunnel ingress and used together with a link affinity group attribute (on links) to manage link selection. After a tunnel is assigned an affinity, a device compares the affinity with the affinity group attribute during link selection. Based on the comparison result, the device determines whether to select a link with specified attributes.

6.3.5.1. Configuration example for RSVP-TE Affinity

Command	Description
interface loopback 0	Loopback for Router-ID and LSR ID
ipv4-address 11.11.11.11/32	Assign IPv4 address to the interface

!	
interface x-eth 0/0/3	Physical interface to MPLS backbone with RSVP-TE enabled
ipv4-address 1.34.1.1/30	Assign IPv4 address to the interface
mpls enable	Enable common MPLS
!	
interface x-eth 0/0/4	Physical interface to MPLS backbone with RSVP-TE enabled
ipv4-address 1.50.70.33/30	Assign IPv4 address to the interface
mpls enable	Enable common MPLS
!	
mpls te affinity-map YELLOW 2	Create Affinity map "YELLOW" with RSVP-TE value equal to 2
mpls te affinity-map BLUE 6	Create Affinity map "BLUE" with RSVP-TE value equal to 6
!	
mpls te rsvp default	Enter common RSVP-TE section
ip-source 11.11.11.11	Set IP source that is generally MPLS LSR-ID
interface x-eth 0/0/3	Enable RSVP-TE for the MPLS interface
affinity [BLUE]	Assign Affinity to interface ("color path")
!	
interface x-eth 0/0/4	Enable RSVP-TE for the MPLS interface
affinity [YELLOW]	Assign Affinity to interface ("color path")
!	
tunnel-te to_PARIS_by_BLUE_road	Enter tunnel interface view
tunnel-destination 1.1.1.1	Set tunnel destination IP
tunnel-source 11.11.11.11	Set tunnel source IP
affinity include-any [BLUE]	Enable tunnel establish path only by interfaces with specified affinity ("BLUE road"). Here is used "include-any" keyword.
!	
tunnel-te to_PARIS_by_YELLOW_road	Enter tunnel interface view
tunnel-destination 1.1.1.1	Set tunnel destination IP
tunnel-source 11.11.11.11	Set tunnel source IP
affinity include-any [YELLOW]	Enable tunnel establish path only by interfaces with specified affinity ("YELLOW road"). Here is used "include-any" keyword.
!	
!	

6.3.6. RSVP-TE Bandwidth and Auto-Bandwidth

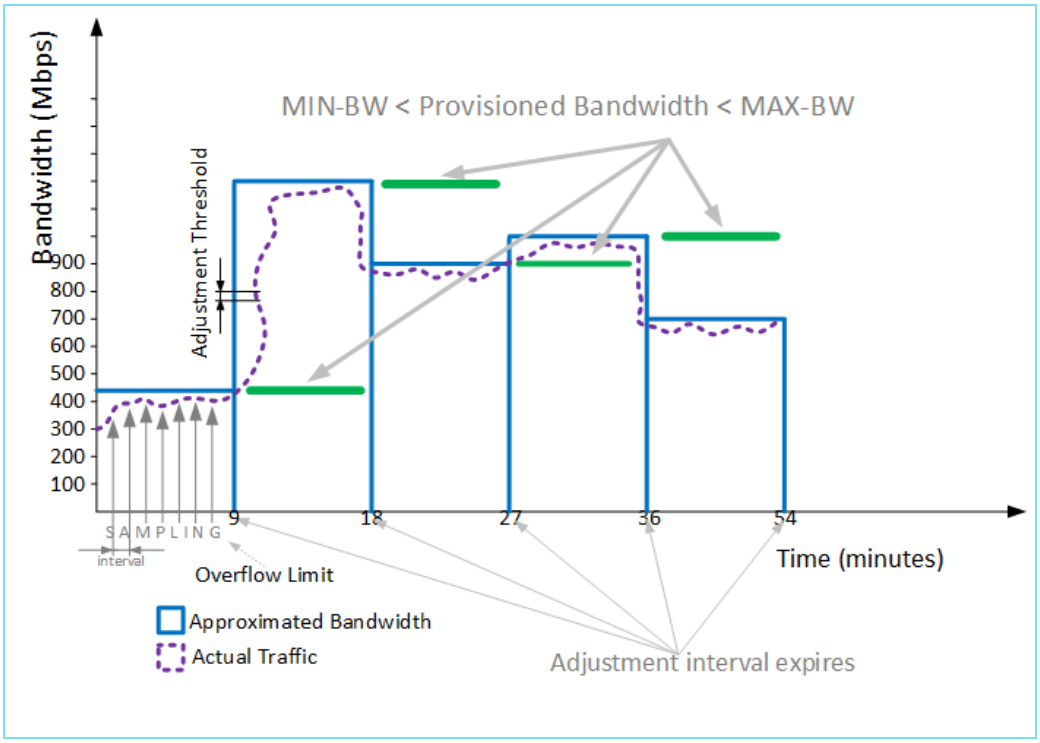
MPLS TE establishes constraint based routed label switched paths (LSPs) and transparently transmits traffic over the LSPs. Based on certain constraints, the LSP path is controllable, and links along the LSP reserve sufficient bandwidth for service traffic. In the case of resource insufficiency, the LSP with a higher priority can preempt the bandwidth of the LSP with a lower priority to meet the requirements of the service with a higher priority. In addition, when an LSP fails or a node on the network is congested, MPLS TE can provide protection through Fast Reroute (FRR) and a backup path.

Auto-bandwidth allows for a very efficient use of network-bandwidth. With the auto-bandwidth feature, the traffic rate through an LSP is sampled and the reserved bandwidth of the LSP is automatically changed through a make-before-break mechanism. This is done in order to keep the reserved bandwidth close to the actual traffic rate. It is beneficial to have an optimum bandwidth reservation for an LSP.

Several parameters are available to tune the automatic adjustment behavior. Some examples of parameters are the adjustment-interval, the sample-interval, the adjustment-threshold, and the overflow-limit. The basic auto-bandwidth functionality is that for every adjustment-interval, the predicted bandwidth is calculated as the maximum sampled traffic-rate in the previous adjustment-interval. For example, the adjustment interval is 10 minutes, and the sample interval is 1 minute. Every adjustment-period contains 10 samples of traffic rate. Out of these 10 samples, the highest sampled rate is selected as the reserved bandwidth for the next adjustment interval.

Use the make-before-break procedure to change the bandwidth of an LSP without affecting the traffic. This procedure involves the exchange of RSVP control messages. The user may sometimes choose to ignore a bandwidth change when the difference in the current bandwidth and the predicted bandwidth is insignificant. For example, if the current bandwidth is 1 Mbps and the predicted bandwidth is 1.01 Mbps, the delta change is insignificant. To avoid a bandwidth adjustment, in this case, the user can set an adjustment-threshold. The user can configure the adjustment-threshold in terms of percentage in the previous releases. If the user sets the adjustment-threshold to be 10%, the bandwidth of an LSP adjusts only if the different between the current bandwidth and the predicted bandwidth is greater than 10% of the current bandwidth.

6.3.6.1. RSVP-TE Auto-Bandwidth algorithm



The actual traffic rate may not be close to the predicted rate always, given the very nature of prediction. In order to adapt to a higher traffic rate, it may be required to increase the reserved bandwidth of the LSP sooner than waiting for the adjustment-interval to expire. To achieve this, there is a parameter called the overflow-limit. If the overflow-limit is set to 3, and 3 consecutive samples of actual traffic-rate are found to exceed the current bandwidth by an amount greater than the configured threshold, a premature adjustment is triggered, setting the bandwidth to the maximum of the samples obtained so far in the adjustment-interval.

6.3.6.2. RSVP-TE Bandwidth configuration example

Command	Description
!	
mpls te rsvp default	Enter common RSVP-TE section
ip-source 11.11.11.11	Set IP source that is generally MPLS LSR-ID
interface x-eth 0/0/14.201	Enable RSVP-TE for the MPLS interface
max-reservable-bw 90 percent	Configures the maximum amount of bandwidth that can be reserved on the interface. Units in which the bandwidth is measured: Bits per second Kilo bps (Default)

	Mega bps Giga bps Percentage of the interface bandwidth
!	
tunnel-te toPE77	Enter tunnel interface view
tunnel-destination 1.1.1.1	Set tunnel destination IP
tunnel-source 11.11.11.11	Set tunnel source IP
bandwidth 100 mbps	Reserves the bandwidth for the current tunnel.
!	
!	

6.3.6.3. RSVP-TE Auto-Bandwidth configuration example

Command	Description
!	
mpls te rsvp default	Enter common RSVP-TE section
ip-source 11.11.11.11	Set IP source that is generally MPLS LSR-ID
auto-bandwidth sample-interval 60 sec	Configures the time interval between sampling bandwidth utilization statistics. The sample interval can be between one minute and one year, expressed in terms of a number of either seconds, minutes, hours, days, or weeks. The sample interval should be at least 3 times lower than any adjust interval.
interface x-eth 0/0/14.201	Enable RSVP-TE for the MPLS interface
max-reservable-bw 1000 mbps	Configures the maximum amount of bandwidth that can be reserved on the interface. Units in which the bandwidth is measured: Bits per second Kilo bps (Default) Mega bps Giga bps Percentage of the interface bandwidth
interface x-eth 0/0/15.701	Enable RSVP-TE for the MPLS interface
max-reservable-bw 100 mbps	Configures the maximum amount of bandwidth that can be reserved on the interface.
!	
tunnel-te toPE77	Enter tunnel interface view
tunnel-destination 1.1.1.1	Set tunnel destination IP
tunnel-source 11.11.11.11	Set tunnel source IP
auto-bandwidth adjust-interval 3 min	The adjust interval can be between one minute and one year, expressed in terms of a number of either seconds, minutes, hours, days, or weeks. The adjust-interval should be at least 3 times higher than the sample-interval.
auto-bandwidth adjust-threshold 2	Configures the threshold at which bandwidth is automatically adjusted. Bandwidth differential percentage at which point adjustment occurs. (Default = 15)

auto-bandwidth minimum-bandwidth 1000	Configures the minimum bandwidth allowed for the LSP.
auto-bandwidth maximum-bandwidth 1 gbps	Configures the maximum bandwidth allowed for the LSP.
auto-bandwidth overflow-limit 10	Configures the number of consecutive bandwidth overflow samples that triggers automatic bandwidth adjustment.
auto-bandwidth monitor enable	Starts bandwidth monitoring. In order for bandwidth monitoring to work 'auto-bandwidth adjust-interval' must be configured.
!	
!	

6.3.7. RSVP-TE Configuration for CSG1

This chapter provides a comprehensive guide to configuring RSVP-TE on ExaNOS enabled network

6.3.7.1. RSVP-TE configuration for CSG1

Command	Description
!	
interface x-eth 0/0/1	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_CSG1_x0/0/2	Interface description
!	
interface x-eth 0/0/1.100	Sub-interface view
ipv4-address 122.168.1.6/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface
vlan-id 100	VLAN tag for the sub-interface
description to_CSG1_x0/0/2.100	Interface description for appropriate labelling
!	
interface x-eth 0/0/2	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface admin state
description to_ASG1_x0/0/1	Interface description for appropriate labelling
!	
interface x-eth 0/0/2.200	Sub-interface view
ipv4-address 192.168.1.9/30	Assign IPv4 address to the interface
mpls enable	MPLS enable on the sub-interface

vlan-id 200	VLAN tag for the sub-interface
description to_CSG1_x0/0/1.100	Interface description for appropriate labelling
!	
interface loopback 0	Interface view (Loopback)
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
description RouterID	Interface description
!	
mpls te rsvp default	RSVP-TE section
ip-source 101.101.101.101	IP source (by default) for RSVP-TE
interface x-eth 0/0/1.100	Enable RSVP-TE on existing interface
interface x-eth 0/0/2.200	Enable RSVP-TE on existing interface
!	
path toASG1_path	Static path view
nexthop 192.168.1.10 strict	Next hop configuration
nexthop 11.11.11.11 strict	Next hop configuration
!	
tunnel-te toASG1	Tunnel interface
tunnel-destination 11.11.11.11	Tunnel destination
tunnel-source 101.101.101.101	Tunnel source
path toASG1_path	Assign static path to primary LSP
secondary default	Enable Backup LSP
cspf enable	Use CSPF for backup LSP
standby enable	Make backup LSP standby
hop-limit 2	Limit RSVP-TE hops for backup LSP
!	
!	
!	

6.4. BGP LSP

6.4.1. BGP LSP concept

BGP Labeled Unicast (BGP-LU) is an extension of the Border Gateway Protocol (BGP) that allows BGP to carry MPLS (Multiprotocol Label Switching) labels in the routing information it distributes. In this mode, BGP is not only responsible for distributing IP routes but also the associated labels, which helps in the setup of MPLS Label Switched Paths (LSPs). This is useful for establishing end-to-end LSPs across different routing domains, whether they are different IGP (Interior Gateway Protocol) domains or across Autonomous Systems (AS). By enabling BGP to carry label information, this mechanism allows for more flexibility in how MPLS forwarding can be orchestrated across complex, multi-domain networks.

BGP-LU is primarily described in RFC 8277, titled "*Using BGP to Bind MPLS Labels to Address Prefixes*". This RFC extends BGP by defining new protocol extensions that allow routers to advertise both a label and a route for a specific IP prefix. The purpose is to allow seamless forwarding across MPLS networks that might span different administrative boundaries or routing domains. By binding labels to prefixes, BGP enables the creation of MPLS LSPs based on reachability information it already distributes.

The main purpose of BGP-LSP based on labeled unicast is to facilitate the stitching of isolated IGP domains and to enable inter-AS LSPs in MPLS networks. Here's how these two concepts work:

- **Stitching Isolated IGP Domains**: In large-scale networks, different IGP domains may exist for administrative or scalability reasons (for example, using OSPF in one part of the network and IS-IS in another). BGP-LU allows for label-switched paths to cross these domain boundaries, as BGP is able to propagate not just the route, but also the associated MPLS label. This ensures that traffic can traverse different IGP domains without needing a common IGP or complex inter-domain routing configurations.
- **Inter-AS LSP**: BGP-LU is also commonly used to build End-to-End MPLS LSPs between different Autonomous Systems (ASs). This is important in scenarios where traffic must cross multiple service provider networks. By carrying labels in BGP updates, it is possible to establish a single end-to-end LSP across multiple AS boundaries without needing to fully distribute internal routing information between them. This enables seamless MPLS-based services, such as VPNs or traffic engineering, across disparate networks.

6.4.2. BGP LSP deployment

This chapter provides a comprehensive guide to configuring BGP LSP on ExaNOS enabled network

6.4.2.1. BGP LSP configuration for CSG1

Command	Description
!	

interface loopback 0	Loopback Interface view
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
!	
routing bgp 65000	BGP routing protocol view
vrf default	GRT view for the protocol
af-ipv4 labeled-unicast	IPv4 Address Family
network 101.101.101.101/32	Network announce
!	
neighbor 11.11.11.11	Refers to the neighbor IP
local-address 101.101.101.101	Refers to the local IP
remote-as-number 65000	Set remote AS for neighboring
af-ipv4 labeled-unicast	IPv4 Address LU Family
!	
!	
!	

6.4.2.2. BGP LSP maintenance

Command	Description
show bgp neighbors	Shoes BGP neighbor basic information
show bgp table	Shows BGP RIB with basic information
show bgp table ipv4 labeled-unicast	Shows BGP RIB with detail information of LU family

7. Services

MPLS services can be categorized into several distinct types, each tailored to meet specific operational requirements:

7.1. Layer 2 VPNs

7.1.1. L2VPN concept

These services allow for the creation of virtual private networks that connect multiple customer sites, enabling them to communicate as if they were on the same local area network (LAN).

- **E-LAN** provides a multipoint-to-multipoint Ethernet service that enables all connected sites to communicate with one another as if they are part of a single broadcast domain. This service allows for the transmission of Ethernet frames between any number of sites without requiring a direct connection between them.
- **E-LINE** is a point-to-point Ethernet service that connects two sites directly, providing a dedicated link that simulates a private Ethernet connection. This service ensures that traffic between the two endpoints is isolated from other users.

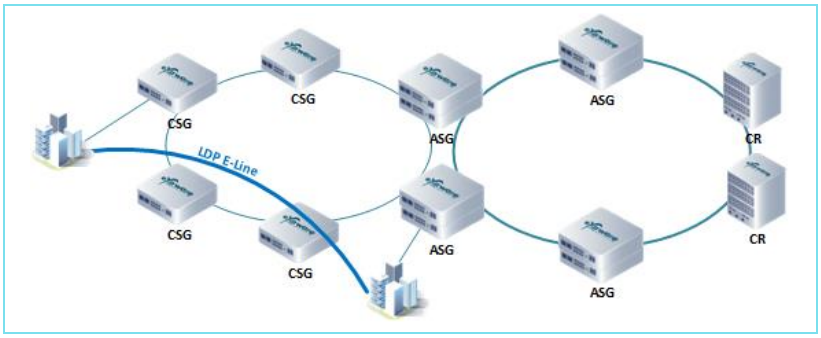
L2VPNs can be implemented using various protocols, primarily based on Label Distribution Protocol (LDP) or Border Gateway Protocol (BGP). Each method has its own strengths and is suited to different network architectures.

- In **LDP-based** L2VPNs, the Label Distribution Protocol is used to distribute labels among routers in the MPLS network. This approach enables the establishment of virtual circuits without requiring a full routing protocol.
- **BGP-based** L2VPNs leverage the Border Gateway Protocol to distribute label information and manage VPN routes. This method provides enhanced scalability and flexibility, making it suitable for larger and more complex networks.

7.1.2. LDP E-Line L2VPN deployment

This chapter provides a comprehensive guide to configuring L2VPN on ExaNOS enabled network.

7.1.2.1. LDP E-Line deployment example



7.1.2.2. LDP E-Line L2VPN configuration commands

Command	Description
!	
interface x-eth 0/0/3	Interface view
description to_L2-cloud	Interface description for appropriate labelling
admin-state up	Interface state
l2-transport enable	Enable interface for L2 services
!	
l2-services	L2 Services section
pw-profile Profile1	Enter PW Profile section
type raw	Type of PW (tag/raw)
mtu 1500	Set MTU
control-word enable	Enable Control Word for the PW
!	
vpws L2vpn1	Enter VPWS section, set name of the VPWS
neighbor 12.12.12.12 pw-id 1001	Set neighbor IP and PW ID
interface x-eth 0/0/3	Refer to L2 enabled interface for L2 services
profile Profile1	Refer to PW Profile
!	

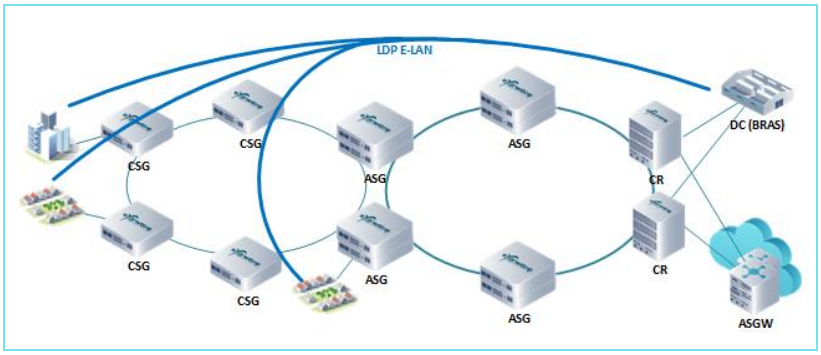
7.1.2.3. LDP E-Line L2VPN maintenance

Command	Description
show configuration l2-services	Show configuration of the L2VPN services
show vpws	Show status of PWs
show fib vpws	Show table of FIB for the VPWS instances

7.1.3. LDP E-LAN L2VPN deployment

This chapter provides a comprehensive guide to configuring LDP E-LAN L2VPN on ExaNOS enabled network

7.1.3.1. E-LAN deployment example



7.1.3.2. LDP E-LAN L2VPN configuration commands

Command	Description
!	
interface x-eth 0/0/2	Interface view
description to_L2_Domain	Interface description for appropriate labelling
admin-state up	Interface state
l2-transport enable	Enable interface for L2 services
!	
l2-services	L2 Services section
pw-profile Profile1	Enter PW Profile section
type raw	Type of PW (tag/raw)
mtu 1500	Set MTU
!control-word enable	Enable Control Word for the PW
!	
vpws Peer1	Enter VPWS section, set name of the VPWS
neighbor 12.12.12.12 pw-id 100	Set neighbor IP and PW ID
profile Profile1	Refer to PW Profile
vpls VPLS1	Enter VPLS section, set name of the VPLS
ve-id 100	Set VPLS ID

interface x-eth 0/0/2	Refer to L2 enabled interface for L2 services
vpws Peer1 mesh	Refer to VPWS with the name specified and type
!	
!	

7.1.3.3. LDP E-LAN L2VPN maintenance

Command	Description
show configuration l2-services	Show configuration of the L2VPN services
show vpws	Show status of PWs
show vpls	Show status of VPLS instances

7.1.4. BGP E-LAN L2VPN deployment

This chapter provides a comprehensive guide to configuring BGP E-LAN L2VPN on ExaNOS enabled network

7.1.4.1. BGP E-LAN L2VPN configuration commands

Command	Description
!	
interface x-eth 0/0/10.101	Interface view
l2-transport enable	Enable interface for L2 services
admin-state up	Interface state
!	
l2-services	L2 Services section
vpls VPLS-AD1	Enter VPLS section, set name of the VPLS
ve-id 100	Set VPLS ID
auto-discovery	VPLS type is BGP AD
rd 1:10	BGP AD Route Distinguisher
import-rt 1:10	BGP AD Import Route Target
export-rt 1:10	BGP AD Export Route Target
!	
interface x-eth 0/0/10.101	Refer to L2 enabled interface for L2 services

!	
!	
!	
!	
routing bgp 65001	BGP routing protocol view
router-id 2.2.2.2	BGP Router-ID
!	
vrf default	VRF “default”, BGP neighboring in GRT
!	
neighbor 1.1.1.1	Refers to the neighbor IP
local-address loopback 0	
remote-as-number 65001	
af-l2vpn vpls	Set peer for the BGP AD family
!	
!	
!	
!	

7.2. Layer 3 VPNs

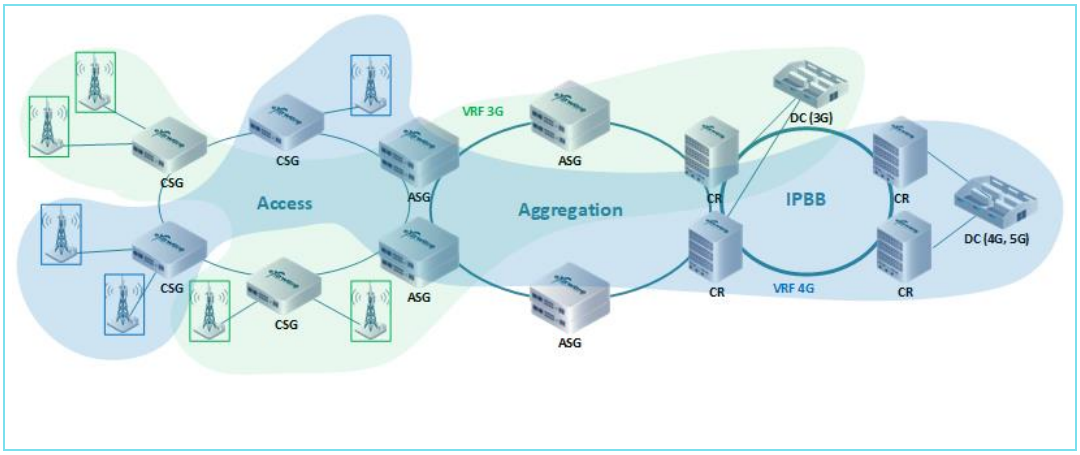
7.2.1. L3VPN concept

This service type facilitates the routing of IP packets between different customer sites over a shared MPLS infrastructure, providing robust connectivity while maintaining data privacy and security.

In the following sections, will be explored the implementation considerations, operational best practices, and future trends associated with MPLS services, equipping stakeholders with the knowledge needed to leverage this powerful technology effectively.

Layer 2 VPNs (L2VPNs) provide a robust solution for connecting multiple sites at the data link layer (Layer 2) of the OSI model. They facilitate seamless communication between geographically dispersed locations, allowing enterprises to create virtualized networks that behave like a single LAN.

7.2.1.1. L3VPN deployment example



7.2.2. L3VPN deployment

This chapter provides a comprehensive guide to configuring L3VPN on ExaNOS enabled network

7.2.2.1. L3VPN configuration example

Command	Description
!	
vrf 3G	Enter VRF section and set VRF name
rd 1:1	Set Route Distinguisher
af-ipv4 unicast	IPv4 Address Family
!	
!	
interface x-eth 0/0/3	Interface view
description to_IPv4-cloud	Interface description for appropriate labelling
admin-state up	Interface state
ipv4-address 172.16.1.1/30	Assign IPv4 address to the interface
vrf 3G	Refer VRF
!	
routing bgp 65001	BGP routing protocol view
router-id 101.101.101.101	Router ID
vrf 3G	Refers existing VRF name

af-ipv4 unicast	IPv4 Address Family
redistribute connected	
export-rt 1:1	Set VRF Route Target for export
import-rt 1:1	Set VRF Route Target for import
!	
vrf default	GRT view for the protocol
af-ipv4 unicast	IPv4 Address Family
!	
af-ipv4 vpn	Enter VPNv4 section
!	
af-ipv4 unicast	IPv4 Address Family
!	
neighbor 11.11.11.11	Refers to the neighbor IP
local-address loopback 0	
!	
remote-as-number 65001	
af-ipv4 unicast	IPv4 Address Family
inbound-soft-reconfiguration enable	
!	
af-ipv4 vpn	Enter VPNv4 section
!	
!	
!	
!	

7.2.2.2. L3VPN maintenance commands

Command	Description
show route vrf <VRF_NAME>	Show routing table of the VRF
show interface ip vrf <VRF_NAME>	Show IP table of the interfaces bound to the VRF
show bgp table ipv4 vpn rd <x:x>	Show BGP VPNv4 routing table for the VRF of specified RD

8. QoS

Using QoS and HQoS under a DiffServ model within White Box networks thus enables high performance and scalability for IP backhaul, ensuring reliable delivery for a range of services and aligning with the demands of both mobile and fixed-network convergence. Thus, packets are classified into multiple classes based on traffic types, allowing prioritized and differentiated handling. This is achieved by marking packets with a Differentiated Services Code Point (DSCP) in the IP header, enabling routers and switches to identify and treat traffic according to predefined policies.

8.1. QoS elements

QoS marking is the initial step in establishing a robust QoS model, where the network assigns priority to packets by marking them according to the desired service class. In a DiffServ-based IP backhaul, this is primarily done through DSCP values, which categorize traffic into classes based on performance requirements (e.g., low latency for voice, high bandwidth for video). Within an MPLS domain, packet priority is often indicated by the MPLS EXP bits in the MPLS header, which allows for efficient traffic handling and prioritization within MPLS tunnels. The 802.1p field within the VLAN header can be utilized for marking, which assigns priority levels at Layer 2. Designing an effective marking model involves mapping application-specific traffic types to DSCP classes. A consistent marking scheme must be established across all network elements to ensure end-to-end QoS. In a White Box environment, the NOS should support flexible traffic classification and marking policies that can adapt as new applications are introduced or existing applications evolve.

QoS queuing mechanisms are essential for managing traffic flows according to priority, typically through a combination of queuing disciplines like Weighted Fair Queuing (WFQ), Priority Queuing (PQ), or Class-Based Queuing (CBQ). The specific queuing model can vary based on the hardware capabilities of White Box platforms, as each NOS and hardware vendor may support different queuing algorithms and buffer depths. Effective queuing design is crucial to prevent congestion and packet loss, especially in mobile backhaul, where traffic patterns are highly variable. The NOS should be capable of implementing and adjusting queues dynamically, based on real-time network conditions and service requirements.

Prioritization is central to QoS, ensuring that critical services like voice and real-time video receive precedence over less time-sensitive traffic like bulk data transfers. In a DiffServ model, prioritized traffic is handled through the DSCP markings, where higher-priority traffic classes are placed into higher-priority queues. For White Box networks, this requires the NOS to support fine-grained prioritization policies and dynamic reordering of traffic. Additionally, in FMC scenarios, prioritization

rules may need to extend across mobile and fixed networks, ensuring that service levels are consistent across the entire network path, from core to access.

Traffic limitation, or rate limiting, is used to control the bandwidth allocated to specific applications, users, or service classes. In a mobile backhaul environment, traffic limitation can prevent resource exhaustion, ensuring fair access across multiple users and services. The NOS supports granular rate limiting at various levels (e.g., per-service, per-user, per-port) and enforce these limits with minimal impact on overall performance. Rate limiting can also be beneficial for enforcing policies during peak usage periods or when certain applications need throttling to maintain network stability.

8.2. QoS architecture

8.2.1. QoS architecture on White Box

The functional operation of the queueing is as follows:

- EF1 – there is one queue per core toward the destination port. This serves packets from CPU and packets classified to TC=7 (EF1 in CLI) by the PMF.
- EF1 packets are strict priority over all other traffic and is not subject to the VLAN shaper. If the operator wants HP traffic to be counted against the VLAN shaper it should use the EF2 class.

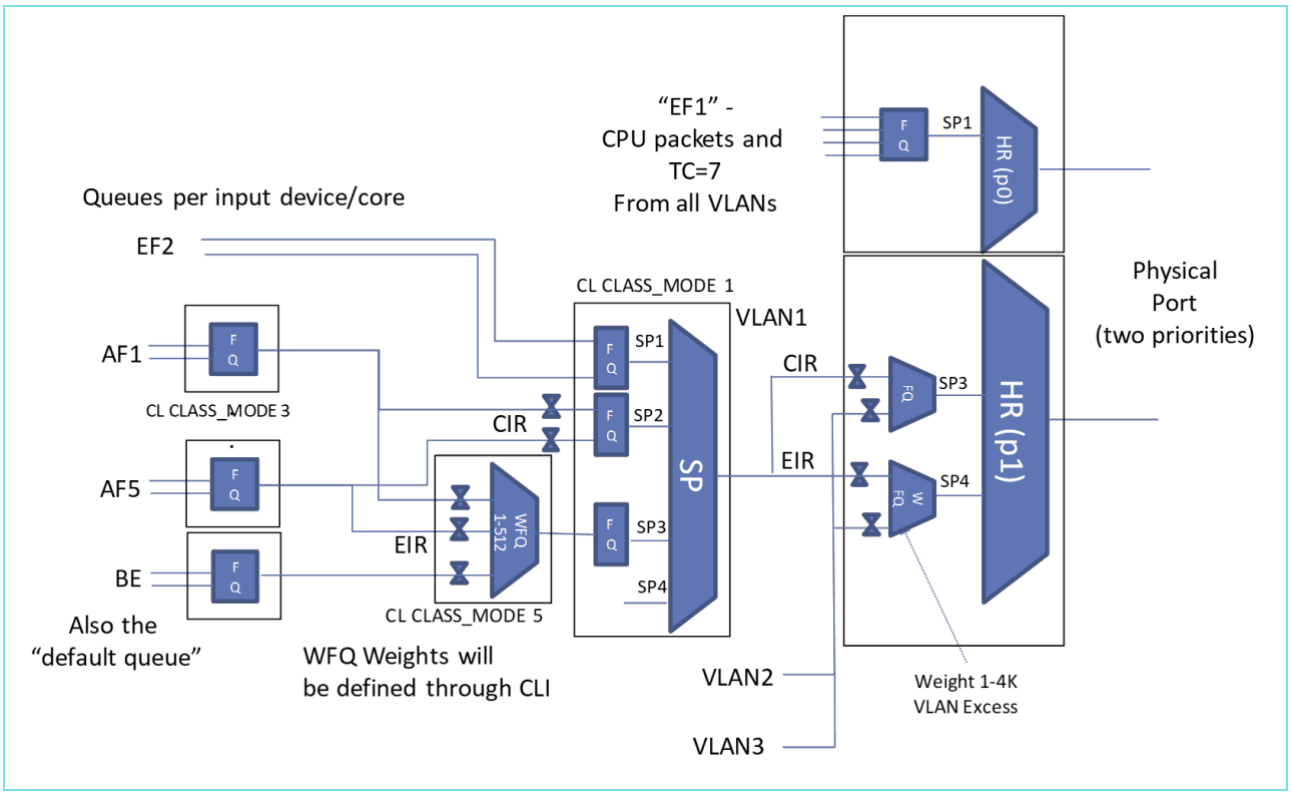
All non-EF1 traffic use the HR scheduler connected to p1 at the port level. The HR uses only the SP4 WFQ structure that handles the fairness between VLANs. In this release all VLANs has the same weight.

Each VLAN construct uses a main scheduler that includes an embedded scheduler. The combined scheduler properties:

- SP1 - EF2 traffic is handled as highest priority.
- SP2 of main scheduler - Serves the AFx classes and BE traffic.
- Embedded scheduler:
    - SP1 – Serves the guaranteed traffic of the AFx classes.
    - SP2 – Serves the excess traffic of the AFx classes and the BE traffic based on weights.

The main scheduler SPx order is working in strict priority, which mean that the next priority is only served if the higher priorities has no traffic or if the scheduler on the connector to the next level is exhausted. The verification of each priority is reexamined for each credit to send traffic which is available from the previous hierarchy (in this case the VLAN shaper and the HR WFQ).

The AFx classes are using a composite connector, which allows the AF scheduler to map the traffic for CIR and EIR portion, each uses a separate connector to the SP1 (CIR) and SP2 (EIR) of the embedded scheduler. In practice it means that each AF class is served up to the CIR by SP1 and only after all CIRs of other AF classes are exhausted (or if there are no packets in the queues) than EIR portion will be served together with the BE traffic based on the relative weights.



8.3. QoS configuration for UNI

8.3.1. HQoS Policy UNI IN

8.3.1.1. Policy UNI IN configuration example

Command	Description
!	
interface x-eth 0/0/32.100	
policy qos in-port-classification Policy1-UNI-IN-Pr	Apply hierarchical policy to interface
!	
policy qos Policy1-UNI-IN-Pr	Create hierarchical policies by nesting one policy within another. To do this, define the child policy and then create a parent policy that uses the exec-policy command to call the child policy.
rule rule-default	Set policy rule
exec-policy Policy1-UNI-IN-Ch	Execute child policy
end-policy	End Policy view
!	
policy qos Policy1-UNI-IN-Ch	Create child policy for the hierarchical QoS.
rule r0	Set policy rule
if dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)	IF-condition in policy
then	Enter Then set
set qos-tag 0	Set QoS parameters according to conditions
set dscp 0	Set QoS parameters according to conditions
set queue be	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r11	Set policy rule
if dscp exist-in (8, af11)	IF-condition in policy
then	Enter Then set
set qos-tag 11	Set QoS parameters according to conditions
set queue af5	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r12	Set policy rule
if dscp exist-in (af12, af13)	IF-condition in policy
then	Enter Then set
set qos-tag 12	Set QoS parameters according to conditions
set queue af5	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r21	Set policy rule
if dscp exist-in (16, af21)	IF-condition in policy
then	Enter Then set
set qos-tag 21	Set QoS parameters according to conditions

set queue af4	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r22	Set policy rule
if dscp exist-in (af22, af23)	IF-condition in policy
then	Enter Then set
set qos-tag 22	Set QoS parameters according to conditions
set queue af4	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r31	Set policy rule
if dscp exist-in (24, af31)	IF-condition in policy
then	Enter Then set
set qos-tag 31	Set QoS parameters according to conditions
set queue af3	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r32	Set policy rule
if dscp exist-in (af32, af33)	IF-condition in policy
then	Enter Then set
set qos-tag 32	Set QoS parameters according to conditions
set queue af3	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r41	Set policy rule
if dscp exist-in (32, af41)	IF-condition in policy
then	Enter Then set
set qos-tag 41	Set QoS parameters according to conditions
set queue af2	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r42	Set policy rule
if dscp exist-in (af42, af43)	IF-condition in policy
then	Enter Then set
set qos-tag 42	Set QoS parameters according to conditions
set queue af2	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r51	Set policy rule
if dscp exist-in (40, 46)	IF-condition in policy
then	Enter Then set

set qos-tag 46	Set QoS parameters according to conditions
set queue ef2	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r7	Set policy rule
if dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)	IF-condition in policy
then	Enter Then set
set qos-tag 56	Set QoS parameters according to conditions
set queue ef1	Set QoS parameters according to conditions
rule rule-default	Set policy rule (default)
end-policy	End Policy view
!	

8.3.2. HQoS Policy UNI OUT

8.3.2.1. Policy UNI OUT configuration example

Command	Description
!	
interface x-eth 0/0/32.100	
policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr	Apply hierarchical policy to interface
!	
policy qos Policy4-UNI-OUT-Pr	Create hierarchical policies by nesting one policy within another. To do this, define the child policy and then create a parent policy that uses the exec-policy command to call the child policy.
rule rule-default	Set policy rule (default)
exec-policy Policy4-UNI-OUT-Ch	Execute child policy
end-policy	End Policy view
!	
policy qos Policy4-UNI-OUT-Ch	Create child policy for the hierarchical QoS.
rule r7	Set policy rule
if qos-tag eq 56	IF-condition in policy
then	Enter Then set
set ieee-802.1p 7	Set QoS parameters according to conditions
set dscp XXX	Set QoS parameters according to conditions
rule r5	Set policy rule

if qos-tag eq 46	IF-condition in policy
then	Enter Then set
set ieee-802.1p 5	Set QoS parameters according to conditions
! set dscp XXX	Set QoS parameters according to conditions
rule r4	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 41	IF-condition in policy in “if” view
qos-tag eq 42	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 4	Set QoS parameters according to conditions
! set dscp XXX	Set QoS parameters according to conditions
rule r3	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 31	IF-condition in policy in “if” view
qos-tag eq 32	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 3	Set QoS parameters according to conditions
! set dscp XXX	Set QoS parameters according to conditions
rule r2	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 21	IF-condition in policy in “if” view
qos-tag eq 22	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 2	Set QoS parameters according to conditions
! set dscp XXX	Set QoS parameters according to conditions
rule r1	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 11	IF-condition in policy in “if” view
qos-tag eq 12	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 1	Set QoS parameters according to conditions
! set dscp XXX	Set QoS parameters according to conditions
rule r0	Set policy rule
if qos-tag eq 0	IF-condition in policy
then	Enter Then set

set ieee-802.1p 0	Set QoS parameters according to conditions
! set dscp XXX	Set QoS parameters according to conditions
rule rule-default	Set policy rule (default)
end-policy	End Policy view
!	

8.4. QoS configuration for NNI

8.4.1. HQoS Policy NNI IN

8.4.1.1. Policy NNI IN configuration example

Command	Description
!	
interface x-eth 0/0/62.10	
policy qos in-port-classification Policy3-NNI-IN-Pr	Apply hierarchical policy to interface
!	
policy qos Policy3-NNI-IN-Pr	Create hierarchical policies by nesting one policy within another. To do this, define the child policy and then create a parent policy that uses the exec-policy command to call the child policy.
rule rule-default	Set policy rule (default)
exec-policy Policy3-NNI-IN-Ch	Execute child policy
end-policy	End Policy view
!	
policy qos Policy3-NNI-IN-Ch	Create child policy for the hierarchical QoS.
rule r0	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 0	IF-condition in policy in “if” view
dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 0	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
set queue be	Set QoS parameters according to conditions
rule r11	Set policy rule
if match-any	IF-condition in policy

mpls-exp topmost eq 1	IF-condition in policy in “if” view
dscp exist-in (8, af11)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 11	Set QoS parameters according to conditions
set queue af5	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r12	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 1	IF-condition in policy in “if” view
dscp exist-in (af12, af13)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 12	Set QoS parameters according to conditions
set queue af5	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r21	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 2	IF-condition in policy in “if” view
dscp exist-in (16, af21)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 21	Set QoS parameters according to conditions
set queue af4	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r22	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 2	IF-condition in policy in “if” view
dscp exist-in (af22, af23)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 22	Set QoS parameters according to conditions
set queue af4	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r31	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 3	IF-condition in policy in “if” view
dscp exist-in (24, af31)	IF-condition in policy in “if” view
then	Enter Then set

set qos-tag 31	Set QoS parameters according to conditions
set queue af3	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r32	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 3	IF-condition in policy in “if” view
dscp exist-in (af32, af33)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 32	Set QoS parameters according to conditions
set queue af3	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r41	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 4	IF-condition in policy in “if” view
dscp exist-in (32, af41)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 41	Set QoS parameters according to conditions
set queue af2	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions
rule r42	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 4	IF-condition in policy in “if” view
dscp exist-in (af42, af43)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 42	Set QoS parameters according to conditions
set queue af2	Set QoS parameters according to conditions
set color yellow	Set QoS parameters according to conditions
rule r51	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 5	IF-condition in policy in “if” view
dscp exist-in (40, 46)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 46	Set QoS parameters according to conditions
set queue ef2	Set QoS parameters according to conditions
set color green	Set QoS parameters according to conditions

rule r7	Set policy rule
if match-any	IF-condition in policy
mpls-exp topmost eq 6	IF-condition in policy in “if” view
mpls-exp topmost eq 7	IF-condition in policy in “if” view
dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)	IF-condition in policy in “if” view
then	Enter Then set
set qos-tag 56	Set QoS parameters according to conditions
set queue ef1	Set QoS parameters according to conditions
rule rule-default	Set policy rule (default)
end-policy	End Policy view
!	

8.4.2. HQoS Policy NNI OUT

8.4.2.1. Policy NNI OUT configuration example

Command	Description
!	
interface x-eth 0/0/62.10	
policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr	Apply hierarchical policy to interface
!	
policy qos Policy2-NNI-OUT-Pr	Create hierarchical policies by nesting one policy within another. To do this, define the child policy and then create a parent policy that uses the exec-policy command to call the child policy.
rule rule-default	Set policy rule (default)
exec-policy Policy2-NNI-OUT-Ch	Execute child policy
end-policy	End Policy view
!	
policy qos Policy2-NNI-OUT-Ch	Create child policy for the hierarchical QoS.
rule r7	Set policy rule
if qos-tag eq 56	IF-condition in policy
then	Enter Then set
set ieee-802.1p 7	Set QoS parameters according to conditions
set mpls-exp topmost 7	Set QoS parameters according to conditions
rule r5	Set policy rule

if qos-tag eq 46	IF-condition in policy
then	Enter Then set
set ieee-802.1p 5	Set QoS parameters according to conditions
set mpls-exp topmost 5	Set QoS parameters according to conditions
rule r4	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 41	IF-condition in policy in “if” view
qos-tag eq 42	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 4	Set QoS parameters according to conditions
set mpls-exp topmost 4	Set QoS parameters according to conditions
rule r3	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 31	IF-condition in policy in “if” view
qos-tag eq 32	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 3	Set QoS parameters according to conditions
set mpls-exp topmost 3	Set QoS parameters according to conditions
rule r2	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 21	IF-condition in policy in “if” view
qos-tag eq 22	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 2	Set QoS parameters according to conditions
set mpls-exp topmost 2	Set QoS parameters according to conditions
rule r1	Set policy rule
if match-any	IF-condition in policy
qos-tag eq 11	IF-condition in policy in “if” view
qos-tag eq 12	IF-condition in policy in “if” view
then	Enter Then set
set ieee-802.1p 1	Set QoS parameters according to conditions
set mpls-exp topmost 1	Set QoS parameters according to conditions
rule r0	Set policy rule
if qos-tag eq 0	IF-condition in policy
then	Enter Then set

set ieee-802.1p 0	Set QoS parameters according to conditions
set mpls-exp topmost 0	Set QoS parameters according to conditions
rule rule-default	Set policy rule (default)
end-policy	End Policy view
!	

9. O&M

The O&M chapter covers key aspects of managing white box routers. These components ensure effective control, monitoring, and security of the network infrastructure.

- SSH provides secure remote CLI access for administrators, while local users serve as backups when centralized systems fail.
- RADIUS and TACACS+ offer centralized access control.
- SNMP is used for monitoring router performance and health, sending data to centralized managers for real-time analysis.
- SYSLOG handles logging, capturing critical events like configuration changes and errors for auditing and troubleshooting.

9.1. Local user management

9.1.1.1. Local user configuration for CSG1

Command	Description
!	
aaa user admin	Built-in user
password 1U4$uyksWEZhyup0h5Jj5126H0	Set password
role super_admin	Specify either one of the pre-defined roles or a user-defined role.
!	
aaa user tester	Create new user
password 1LdnPOOER$S4DyvsAPDTKmnixw2r6Vx/	Set password
role super_admin	Specify either one of the pre-defined roles or a user-defined role.
!	
aaa user private	Built-in role. Adds a role to the list of roles that can be defined for a user.
password 1kijc$dKzH4A8ID1SApxXcT2O1o1	Set password

role super_admin	Specify either one of the pre-defined roles or a user-defined role.
!	
aaa user public	Built-in role. Adds a role to the list of roles that can be defined for a user.
password 1kijc$dKzH4A8ID1SApxXcT2O1o1	Set password
role snmp	Specify either one of the pre-defined roles or a user-defined role.
!	
aaa role priv_admin	Built-in role. Adds a role to the list of roles that can be defined for a user.
privilege all	Select from the predefined privileges. The command level the role is permitted to access, for example, routing or view.
exception 1	Exception index will determine the order that the rules are applied. The first match will be executed.
command os-shell	Exception "Command" specifies whether the exception is a command at the operational level or under the configuration menu.
action reject	The action to perform if there is a match on the command.
!	
!	
aaa role snmp	Built-in role. Adds a role to the list of roles that can be defined for a user.
privilege all	Select from the predefined privileges. The command level the role is permitted to access, for example, routing or view.
exception 1	Exception index will determine the order that the rules are applied. The first match will be executed.
command os-shell	Exception "Command" specifies whether the exception is a command at the operational level or under the configuration menu.
action reject	The action to perform if there is a match on the command.
!	
!	
aaa role super_admin	Built-in role (default for admin user). Adds a role to the list of roles that can be defined for a user.
privilege all	Maximum privilege. Select from the predefined privileges. The command level the role is permitted to access, for example, routing or view.
!	

9.2. RADIUS/TACACS+

RADIUS and TACACS+ are both used to control access to white box routers.

9.2.1. RADIUS assumptions

- RADIUS operates over UDP, which prioritizes speed but offers less reliability due to its lack of delivery guarantees.
- RADIUS only encrypts the user's password, leaving other details such as usernames and commands exposed, which makes it less secure in certain environments.
- RADIUS combines authentication and authorization into a single process, making it straightforward but less flexible.
- RADIUS is limited in its ability to provide granular control, as it can only grant or deny access based on predefined roles. Once a user is authenticated, they have broad access to the router's functions.
- In terms of accounting, RADIUS tracks basic session information, such as start and stop times and resource usage.

9.2.2. RADIUS deployment

This chapter provides a comprehensive guide to configuring RADIUS on ExaNOS enabled network

9.2.2.1. RADIUS configuration for CSG1

Command	Description
!	
vrf VRF3150	Enter VRF section and set VRF name
!	
interface x-eth 0/0/30	Interface view
admin-state up	Interface state
!	
interface x-eth 0/0/30.3150	Sub-Interface view
description to_Radius_Servers_VRF3150	Interface description for appropriate labelling
vrf VRF3150	Refers existing VRF name
vlan-id 3150	VLAN tag for the sub-interface
ipv4-address 10.50.1.50/24	Assign IPv4 address to the interface
!	
interface x-eth 0/0/30.3250	Sub-Interface view
description to_Radius_Servers_GRT	Interface description for appropriate labelling
vlan-id 3250	VLAN tag for the sub-interface
ipv4-address 10.50.2.50/24	Assign IPv4 address to the interface
!	
aaa authentication-order 1	Configures the order in which different types of authentication or different servers with the same type of authentication are to be

	performed. Local authentication is the default until this command is executed.
authentication-type radius	Type of authentication to perform: local, tacacs, radius
server-ip 10.50.1.16	
!	
aaa authentication-order 2	Configures the order in which different types of authentication or different servers with the same type of authentication are to be performed. Local authentication is the default until this command is executed.
authentication-type radius	Type of authentication to perform: local, tacacs, radius
server-ip 10.50.2.16	
!	
aaa authentication-order 3	Configures the order in which different types of authentication or different servers with the same type of authentication are to be performed. Local authentication is the default until this command is executed.
authentication-type local	Type of authentication to perform: local, tacacs, radius
!	
aaa authorization-order 1	Sets the authorization fall back order.
authorization-type radius	Type of authorization to perform: local, tacacs, radius
!	
aaa authorization-order 2	Sets the authorization fall back order.
authorization-type radius	Type of authorization to perform: local, tacacs, radius
!	
aaa authorization-order 3	Sets the authorization fall back order.
authorization-type local	Type of authorization to perform: local, tacacs, radius
!	
aaa radius-retry 3	Configures the number of retries when a RADIUS response is not received within the given timeout interval.
!	
aaa radius 10.50.1.16	Configures a RADIUS server, including IP address and related parameters.
authentication-key qwe123	
timeout 10	The length of time in seconds that the local router waits to receive a response from the RADIUS server. (Default = 5)
vrf VRF3150	VRF VRF3150
source ip 10.50.1.50	Valid IP address on one of the router interfaces for all outgoing RADIUS packets. This address is used as long as the interface or sub-interface is in the UP state.
reconnect-interval 31	Reconnect-interval value in seconds in which accounting requests to the Radius server will not be sent since the previous unsuccessful attempt. (Default = 30)
account-port 1813	Refer L4 port

auth-port 1812	Refer L4 port
!	
aaa radius 10.50.2.16	Configures a RADIUS server, including IP address and related parameters.
authentication-key qwe123	
timeout 10	The length of time in seconds that the local router waits to receive a response from the RADIUS server. (Default = 5)
	no VRF, assuming VRF "default" (GRT)
source ip 10.50.2.50	Valid IP address on one of the router interfaces for all outgoing RADIUS packets. This address is used as long as the interface or sub-interface is in the UP state.
reconnect-interval 31	Reconnect-interval value in seconds in which accounting requests to the Radius server will not be sent since the previous unsuccessful attempt. (Default = 30)
account-port 1813	Refer L4 port
auth-port 1812	Refer L4 port
!	

9.2.3. TACACS+ assumptions

- TACACS+ uses TCP, providing more reliable, ordered packet delivery, which is critical for managing complex administrative tasks on routers.
- TACACS+ fully encrypts the entire session, including commands and responses, ensuring a much higher level of protection during sensitive router operations.
- TACACS+ separates functions of authentication and authorization, enabling command-level authorization. This allows administrators to define specific user actions after login, offering greater control over router operations.
- TACACS+, offers much more detailed control, allowing administrators to authorize individual commands, ensuring that users can only execute actions that align with their assigned privileges.
- In terms of accounting, TACACS+ goes further by logging each command issued during a session, making it easier to audit specific actions taken by users on the router.

9.2.4. TACACS+ deployment

This chapter provides a comprehensive guide to configuring TACACS+ on ExaNOS enabled network

9.2.4.1. TACACS+ configuration for CSG1

Command	Description
!	
interface x-eth 0/0/30	Interface view
admin-state up	Interface state
!	
interface x-eth 0/0/30.3150	Sub-Interface view
description to_TACACS_Servers_VRF3150	Interface description for appropriate labelling
vrf VRF3150	Refers existing VRF name
vlan-id 3150	VLAN tag for the sub-interface
ipv4-address 10.50.1.50/24	Assign IPv4 address to the interface
!	
interface x-eth 0/0/30.3250	Sub-Interface view
description to_TACACS_Servers_GRT	Interface description for appropriate labelling
vlan-id 3250	VLAN tag for the sub-interface
ipv4-address 10.50.2.50/24	Assign IPv4 address to the interface
!	
aaa authentication-order 1	Configures the order in which different types of authentication or different servers with the same type of authentication are to be performed. Local authentication is the default until this command is executed.
authentication-type tacacs	Type of authentication to perform: local, tacacs, radius
server-ip 10.50.1.15	tacacs – remote server IP address which should be configured
!	
aaa authentication-order 2	Configures the order in which different types of authentication or different servers with the same type of authentication are to be performed. Local authentication is the default until this command is executed.
authentication-type tacacs	Type of authentication to perform: local, tacacs, radius
server-ip 10.50.2.15	tacacs – remote server IP address which should be configured
!	
aaa authentication-order 3	Configures the order in which different types of authentication or different servers with the same type of authentication are to be performed. Local authentication is the default until this command is executed.
authentication-type local	Type of authentication to perform: local, tacacs, radius
!	
aaa authorization-order 1	Sets the authorization fall back order.
authorization-type tacacs	Type of authorization to perform: local, tacacs, radius

!	
aaa authorization-order 2	Sets the authorization fall back order.
authorization-type tacacs	Type of authorization to perform: local, tacacs, radius
!	
aaa authorization-order 3	Sets the authorization fall back order.
authorization-type local	Type of authorization to perform: local, tacacs, radius
!	
aaa tacacs 10.50.1.15	Configures a TACACS+ server, including IP address and related parameters.
authentication-key qwer12345	
timeout 10	The length of time in seconds that the local router waits to receive a response from a TACACS+ server.
source ip 10.50.1.50	
vrf VRF3150	Refers existing VRF name for IP interconnection
reconnect-interval 31	Time to wait before retrying to connect to the server after a connection failure. (Default = 30)
!	
aaa tacacs 10.50.2.15	Configures a TACACS+ server, including IP address and related parameters.
authentication-key qwer12345	
timeout 10	The length of time in seconds that the local router waits to receive a response from a TACACS+ server.
source ip 10.50.2.50	
vrf default	IP interconnection in GRT
reconnect-interval 31	Time to wait before retrying to connect to the server after a connection failure. (Default = 30)
!	

9.3. SNMP

SNMP is integrated into the white box routers to enable centralized monitoring of device health, traffic, and performance metrics. By leveraging SNMP, the network management system collects real-time data, allowing for proactive detection of issues, performance tuning, and automated alerts. The routers are configured with SNMP agents that provide detailed information on interface utilization, system uptime, and critical alerts, which are essential for maintaining operational efficiency and quick troubleshooting in the network infrastructure. This ensures continuous visibility into the routers' status and performance across the entire deployment.

SNMP is deployed in the white box router environment using SNMPv2c and SNMPv3 protocols. SNMPv2c is employed for basic monitoring and reporting, offering simplicity and efficiency, while SNMPv3 provides enhanced security features like authentication and encryption, which are essential for sensitive environments.

The SNMP data model relies on the Structure of Management Information (SMI) version 2, which defines how data is organized and accessed within the Management Information Base (MIB). The MIBs contain critical information about network elements, such as interface statistics, system health, and resource utilization, which are accessed using object identifiers (OIDs). This structure enables the network management system (NMS) to query the white box routers for detailed performance metrics and device status.

In deployment, an NMS communicates with SNMP agents on the routers to collect and analyze data in real time. The NMS integrates with IT systems such as service management tools, performance dashboards, and alerting mechanisms. These systems process SNMP data to provide network operators with actionable insights, such as capacity planning, fault detection, and performance optimization.

9.3.1. SNMP deployment

This chapter provides a comprehensive guide to configuring SNMP on ExaNOS enabled network

9.3.1.1. SNMP v2 configuration for CSG1

Command	Description
!	
vrf VRF3150	Enter VRF section and set VRF name
!	
interface x-eth 0/0/4.3150	Sub-Interface view
description to_SNMP_managing	Interface description for appropriate labelling
admin-state up	Interface state
ipv4-address 10.50.1.5/24	Assign IPv4 address to the interface
vrf VRF3150	Refers existing VRF name
vlan-id 3150	VLAN tag for the sub-interface
!	
snmp	Enters SNMP configuration mode
status enable	
agent	Enters SNMP agent configuration mode
network	Enters SNMP Network section

ip-address 10.50.1.5	
vrf VRF3150	Refers existing VRF name
version v2c	SNMP version
community-name salsa	SNMP Community
!	
platform	Enters SNMP platform configuration mode
ip-address 10.50.1.5	
vrf VRF3150	Refers existing VRF name
version v2c	SNMP version
community-name salsa	SNMP Community
!	
!	
!	
traps	Enters SNMP traps configuration mode
target-id 1	SNMP Trap Instance ID
target-address 10.50.1.77	Trap server IP
udp-port 162	Refer L4 port
vrf VRF3150	Refers existing VRF name
version v2c	SNMP version
community-name salsa	SNMP Community for Traps
!	
!	
!	
!	

9.3.1.2. SNMP v3 configuration for CSG1

Command	Description
!	
vrf VRF3150	Enter VRF section and set VRF name
!	
interface x-eth 0/0/30	Interface view
admin-state up	Interface state
!	

interface x-eth 0/0/30.3150	Sub-Interface view
vrf VRF3150	Refers existing VRF name
vlan-id 3150	VLAN tag for the sub-interface
ipv4-address 10.50.1.50/24	Assign IPv4 address to the interface
!	
snmp	Enters SNMP configuration mode
status enable	
agent	Enters SNMP agent configuration mode
network	Enters SNMP Network section
ip-address 10.50.1.50	
vrf VRF3150	Refers existing VRF name
version v3usm	SNMP version
username Pluto	SNMPv3 parameters
authentication-key wergfdsa12345hjk	SNMPv3 parameters
authentication-protocol md5	SNMPv3 parameters
privilege-key wergfdsa12345hjk	SNMPv3 parameters
privilege-key-protocol aes128	SNMPv3 parameters
security-level AuthPriv	SNMPv3 parameters
engine-id free-text	SNMPv3 parameters
free-text-input wergfdsa12345hjk	SNMPv3 parameters
!	
!	
!	
!	
traps	Enters SNMP traps configuration mode
target-id 1	SNMP Trap Instance ID
target-address 10.50.1.77	Trap server IP
udp-port 162	Refer L4 port
vrf VRF3150	Refers existing VRF name
version v3usm	SNMP version
username Pluto	SNMPv3 parameters
authentication-key wergfdsa12345hjk	SNMPv3 parameters
authentication-protocol md5	SNMPv3 parameters
privilege-key wergfdsa12345hjk	SNMPv3 parameters
privilege-key-protocol aes128	SNMPv3 parameters

security-level AuthPriv	SNMPv3 parameters
engine-id free-text	SNMPv3 parameters
free-text-input wergfdsa12345hjk	SNMPv3 parameters
!	
!	
!	
!	
!	

9.4. SYSLOG

Syslog is a standardized protocol used for logging system messages across different network devices and systems. It operates over UDP (default port 514) or TCP, and is widely adopted for collecting, processing, and storing logs from various sources such as servers, routers, and firewalls. Syslog serves as a central log collection mechanism, allowing devices to send event messages to a syslog server, which then parses, stores, and potentially forwards them to a Security Information and Event Management (SIEM) system for analysis. The syslog protocol defines a message format containing information like facility, severity, and message content, which helps in identifying and categorizing system events for monitoring, troubleshooting, and auditing purposes.

9.4.1. SYSLOG deployment

This chapter provides a comprehensive guide to configuring SYSLOG on ExaNOS enabled network

9.4.1.1. SYSLOG configuration for CSG1

Command	Description
!	
log output file syslog	Directs log messages to one or more output devices. The following output devices are possible: Console, File, User, Remote server This command also enters configuration mode for the specified device.
filter facility any	Filters the log output by either: facility and severity of the message including / excluding given strings • Include: Send only messages containing the indicated string or strings.

	• Exclude: Do not send messages containing the indicated string or strings.
`severity any`	0-emergency 1-alert 2-critical 3-error 4-warning 5-notice 6-info 7-debug any none (default)
`!`	
`filter facility kernel`	Filters the log output by either: facility and severity of the message including / excluding given strings • Include: Send only messages containing the indicated string or strings. • Exclude: Do not send messages containing the indicated string or strings.
`severity none`	0-emergency 1-alert 2-critical 3-error 4-warning 5-notice 6-info 7-debug any none (default)
`!`	
`filter facility infra`	Filters the log output by either: facility and severity of the message including / excluding given strings • Include: Send only messages containing the indicated string or strings. • Exclude: Do not send messages containing the indicated string or strings.
`severity 5-notice`	0-emergency 1-alert 2-critical 3-error 4-warning 5-notice 6-info 7-debug any none (default)
`!`	
`filter facility infra-utils`	Filters the log output by either: facility and severity of the message

	including / excluding given strings • Include: Send only messages containing the indicated string or strings. • Exclude: Do not send messages containing the indicated string or strings.
severity none	0-emergency 1-alert 2-critical 3-error 4-warning 5-notice 6-info 7-debug any none (default)
!	
!	
log output remote-server 1.1.1.1	Directs log messages to the specified output remote server. Also enters configuration mode to configure the following server parameters: • filter • transport type • port • facility override • log prefix • source interface
vrf management	Refers existing VRF name
source 10.169.22.100	Source IP for SYSLOG messages
transport udp	Transport protocol
port 10514	L4 port number
!	
log output remote-server 2.2.2.2	Directs log messages to the specified output remote server. Also enters configuration mode to configure the following server parameters: • filter • transport type • port • facility override • log prefix • source interface
vrf management	Refers existing VRF name
source 10.169.22.100	Source IP for SYSLOG messages
transport udp	Transport protocol
port 514	L4 port number
!	

Basic log maintenance commands are below. More detailed syslog maintenance is out of this document scope.

9.4.1.2. SYSLOG maintenance commands

Command	Description
`show log syslog`	Output of syslog file content (from the beginning to the end with paging)
`log monitor start syslog`	Start of Real-time log file monitoring (syslog to the current terminal)
`log monitor stop syslog`	Stop displaying log file to the current terminal
`log delete syslog`	Delete syslog file

10. Synchronization and Timing

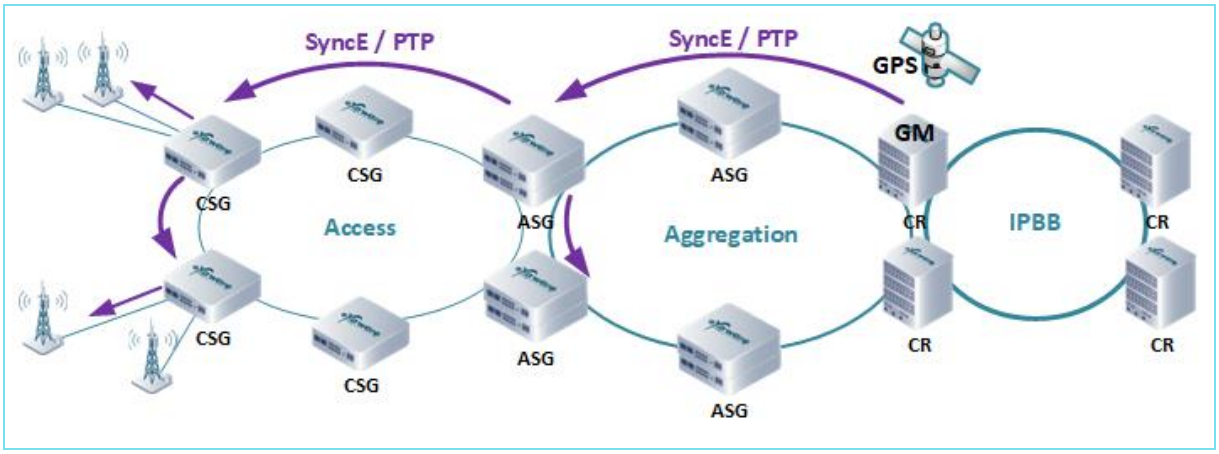
Accurate timing synchronization is crucial for the reliable operation of modern telecom networks, particularly in environments that support time-sensitive services like LTE and 5G.

- NTP is primarily used for synchronizing time within the network infrastructure, such as servers, routers, and switches, where precise timing is less critical.
- In contrast, SyncE and PTP are deployed for more stringent synchronization requirements, such as in base stations, where both frequency (via SyncE) and precise time/phase alignment (via PTP) are essential for supporting services like LTE and 5G, ensuring seamless communication and coordination across the mobile network.

10.1.1.1. Synchronization requirements of different mobile network standards:

Mobile Network Standard	Frequency Synchronization	Time/Phase Synchronization	Synchronization Precision
2G (GSM)	Required	Not required	± 50 ppb (parts per billion)
3G (UMTS)	Required	Not required	± 50 ppb
4G (LTE)	Required	Required (TDD & some FDD modes)	± 1.5 µs (microseconds)
5G (NR)	Required	Required (both TDD & FDD)	± 100 ns (nanoseconds)

10.1.1.2. Sync/Timing concept



10.2. NTP

Network Time Protocol (NTP) is crucial for synchronizing the system time across network devices, ensuring accurate timestamps for logs, events, and other time-sensitive operations. NTP is used to keep the local system time in sync with a reliable external time source, such as a GPS or a public NTP server. Accurate time synchronization is essential for syslog servers, as it ensures consistent and precise timestamps across logs, which are critical for troubleshooting, event correlation, and auditing. By leveraging NTP, the white-box router maintains time consistency across the network, preventing time drifts that could cause issues in log accuracy, security certificates, and operational monitoring.

10.2.1. NTP deployment

This chapter provides a comprehensive guide to configuring NTP on ExaNOS enabled network

10.2.1.1. NTP configuration commands

Command	Description
!	
ntp	Configures NTP options including: Add/Remove NTP servers to/from the list of available time source servers. Specify the source interface/IP address from which NTP requests will be sent.
vrf default	GRT view for the protocol
server 10.1.1.2	

source loopback 0	
!	

10.2.1.2. NTP maintenance commands

Command	Description
show system date	Show current date and time
show ntp associations	Show the NTP server associations
show configuration ntp	NTP related configuration

10.3. SyncE

Synchronous Ethernet (SyncE) is a physical layer protocol used for frequency synchronization across network devices, ensuring that all nodes in a network maintain accurate and stable timing. SyncE is critical for synchronizing routers to a common clock source, enabling precise timing distribution across the network. This is especially important in telecom networks where base stations rely on accurate timing for services like LTE and 5G, which require synchronized frequencies for signal transmission. SyncE allows white-box routers to transmit synchronization information through the Ethernet physical layer, maintaining highly accurate frequency alignment without relying solely on packet-based timing protocols like PTP (Precision Time Protocol). This setup ensures that base stations receive stable and reliable synchronization messages, supporting seamless network operation and preventing timing drifts that could degrade service quality.

Synchronous Ethernet (SyncE) operates by extending traditional Ethernet with the ability to transfer frequency synchronization over the physical layer. This is achieved by embedding clock signals into the Ethernet data stream, enabling network devices like white-box routers to synchronize their local clocks with a master clock in the network. The synchronization is realized through dedicated hardware, such as phase-locked loops (PLLs), that extract the frequency from the received signal, ensuring precise timing alignment.

A key element of SyncE is the use of the Synchronization Status Message (SSM), which is embedded within Ethernet frames. The SSM indicates the quality level of the clock signal being received, allowing network devices to select the most accurate and stable clock source for synchronization. SyncE typically works alongside protocols like PTP (Precision Time Protocol) to enhance overall time and

phase synchronization in environments where both frequency and time alignment are critical, such as telecom networks for base stations.

10.3.1. SyncE deployment

This chapter provides a comprehensive guide to configuring SyncE on ExaNOS enabled network

10.3.1.1. SyncE configuration commands

Command	Description
!	
interface x-eth 0/0/1	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface state
description to_CSG1_x0/0/2	Interface description for appropriate labelling
!	
interface x-eth 0/0/1.100	Sub-Interface view
ipv4-address 122.168.1.6/30	Assign IPv4 address to the interface
vlan-id 100	VLAN tag for the sub-interface
description to_CSG1_x0/0/2.100	Interface description for appropriate labelling
!	
interface x-eth 0/0/2	Interface view
speed 10000	Interface speed according to port and module ability
admin-state up	Interface state
description to_ASG1_x0/0/1	Interface description for appropriate labelling
!	
interface x-eth 0/0/2.200	Sub-Interface view
ipv4-address 192.168.1.9/30	Assign IPv4 address to the interface
vlan-id 200	VLAN tag for the sub-interface
description to_CSG1_x0/0/1.100	Interface description for appropriate labelling
!	
interface loopback 0	Loopback Interface view
ipv4-address 101.101.101.101/32	Assign IPv4 address to the interface
description RouterID	Interface description
!	
!	

timing synchronization	Enter Timing Synchronization section
ql-mode enabled	Set QL mode
ssm-option option1	Set SSM option
!	
interface x-eth 0/0/1	Interface view in protocol view
quality-level ql-ssu-a	Set Quality level
priority 1	Set interface priority
source-id 1	
! wait-to-restore 1	
!	
interface x-eth 0/0/2	Interface view in protocol view
priority 2	Set interface priority
output-source enable	To use the SyncE interface as a timing output source
! wait-to-restore 1	
!	

10.3.1.2. SyncE maintenance commands

Command	Description
show synchronization summary	Show the details of the clock.
show synchronization interfaces detail	Display status and configuration of all synchronization interfaces.
show synchronization interfaces input	Display status and configuration of all synchronization interfaces.
show synchronization interfaces output	Display status and configuration of all synchronization interfaces.
show synchronization statistics esmc	Display Ethernet Synchronization statistics.
!	
clear interface wait-to-restore <x-eth 0/0/2>	
clear synchronization statistics esmc	Clear synchronization statistics

10.4. PTP

Precision Time Protocol (PTP), defined in IEEE 1588, is a highly accurate protocol for synchronizing clocks across network devices. PTP enables sub-microsecond synchronization by using timestamped messages to measure and correct the delay between master and slave clocks. PTP ensures precise time synchronization, which is crucial for applications like mobile base stations in 5G networks, where both time and phase alignment are required for accurate signal transmission and coordination.

IEEE 1588v2 (also known as PTPv2) is the second version of the standard and is widely used in telecom and industrial networks. It provides enhancements over the first version by introducing features like unicast communication, improved security, and better handling of packet delay variation. On the other hand, the ITU-T G.826x/G.827x series adds telecom-specific profiles for PTP, tailoring the protocol for high-precision synchronization in packet-based mobile networks. ITU-T G.8265.1 focuses on frequency synchronization, while G.8275.1 and G.8275.2 focus on both time and phase synchronization. The ITU-T profiles also optimize for asymmetry correction and network topologies typical of telecom networks, ensuring that PTP can meet the stringent timing requirements of applications like LTE and 5G.

The key difference between SyncE and PTP lies in their method of synchronization: SyncE provides frequency synchronization at the physical layer by embedding clock information directly in the Ethernet signal, ensuring that all devices on the network maintain a common frequency. PTP, on the other hand, operates at the packet layer and provides both time and phase synchronization, using timestamped messages to measure and correct network delays for precise timing alignment between devices.

Deploying SyncE and PTP together creates a "hybrid synchronization" model, where SyncE ensures that all devices are aligned to the same frequency, while PTP adds accurate time and phase synchronization. This hybrid approach leverages the strengths of both protocols: SyncE offers a stable, hardware-based frequency sync with low jitter, while PTP refines timing precision over packet networks, compensating for network delays and asymmetries. In telecom networks, this combination is essential for delivering high-quality synchronization to services like LTE and 5G, which require both stable frequency (from SyncE) and precise time/phase alignment (from PTP) to function optimally.

Aspect	IEEE 1588v2 (PTP)	ITU-T G.8xx
Purpose	General-purpose time and frequency synchronization	Telecom-specific synchronization requirements
Clock Types	Grandmaster (GM), Boundary Clock (BC), Transparent Clock (TC)	Similar clock types with additional emphasis on telecom needs
Synchronization Precision	Sub-microsecond precision, typically in the nanoseconds	Higher precision requirements, down to sub-nanoseconds for 5G

Frequency Synchronization	Provides frequency synchronization through PTP messages	Specifies frequency synchronization requirements using PTP and SyncE
Time Synchronization	Time and phase synchronization is a core function	Emphasizes time and phase synchronization, particularly for TDD and FDD modes
Message Types	Sync, Follow_Up, Delay_Request, Delay_Response	Uses similar message types but with additional constraints for telecom applications
SSM (Synchronization Status Messages)	Not part of the standard	Defines SSM to convey clock quality and selection criteria
Use Cases	Suitable for a wide range of applications including industrial and telecommunications	Tailored specifically for mobile networks, including LTE and 5G
Implementation Complexity	Relatively straightforward, with various profiles for complexity	More complex due to telecom-specific requirements and standards

10.4.1. PTP deployment

This chapter provides a comprehensive guide to configuring PTP on ExaNOS enabled network

10.4.1.1. PTP configuration commands

Command	Description
!	
timing ptp	Enter Timing PTP section
clock g8275.1	Set ptp clock configuration mode
! clock-identity <01:02:03:04:05:06:07:08>	Default clock identity is by the following the below steps: 1. Take the first 3 bytes of the chassis' base MAC address (OUI). 2. Follow with the 0xFFFE. 3. Append the last 3 bytes of the MAC address.
clock-type boundary-clock	Set the type of PTP clock
domain <24-43>	Set the current synchronization domain
! local-priority <1-255>	Specify the local attribute of the local clock
! max-steps-removed <1-255>	N/A
! priority2 <1-255>	Set the Priority2 attribute of the local clock
clock-step two-step	Set clock timestamping mode

servo-alg full-on-path	Configure the ptp clock servo algorithm
! holdover 130	Set clock holdover duration
! squelch enable	Configure the ptp clock output squelch mode
interface x-eth 0/0/1	Interface section in protocol view. Creates a new clock interface if it is not created already.
!	
interface x-eth 0/0/2	Interface section in protocol view. Creates a new clock interface if it is not created already.
master-only enable	Set the interface to a master-only port
!	
!	

10.4.1.2. PTP maintenance commands

Command	Description
show ptp clock dataset parent	Show the data set of the master clock this clock is synchronized to.
show ptp clock summary	Show the info of the PTP clock.
show ptp interface summary	Show the info of the PTP clock interface.
show ptp servo	Show the info of the PTP servo.
show ptp statistics brief	Show PTP statistics per PTP clock.
show ptp interface statistics detail	Show PTP statistics per PTP interface.
!	
clear ptp statistics	Clear the PTP statistics.

11. Configuration scripts example

11.1. CSG

11.1.1. CSG1

11.1.1.1. CSG1

```
! CSG1
!
vrf 3G
```

```
 rd 65000:3
 af-ipv4 unicast
 !
!
vrf 4G
 rd 900:104
 af-ipv4 unicast
 !
!
vrf 5G
 rd 900:105
 af-ipv4 unicast
 !
!
vrf default
!
vrf management
!
policy route LDP_LABEL_HOST
 rule rule1
  if prefix exist-in (0.0.0.0/0 matching-len 32)
  then permit
end-policy
!
policy qos Policy1-UNI-IN-Ch
 rule r0
  if dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
  then
   set qos-tag 0
   set color green
   set dscp 0
   set queue be
 rule r11
  if dscp exist-in (8, af11)
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if dscp exist-in (af12, af13)
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
```

```
 if dscp exist-in (16, af21)
 then
  set qos-tag 21
  set color green
  set queue af4
rule r22
 if dscp exist-in (af22, af23)
 then
  set qos-tag 22
  set color yellow
  set queue af4
rule r31
 if dscp exist-in (24, af31)
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if dscp exist-in (af32, af33)
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if dscp exist-in (32, af41)
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if dscp exist-in (af42, af43)
 then
  set qos-tag 42
  set color yellow
  set queue af2
rule r51
 if dscp exist-in (40, 46)
 then
  set qos-tag 46
  set color green
  set queue ef2
rule r7
 if dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
 then
  set qos-tag 56
```

```
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy1-UNI-IN-Pr
 rule rule-default
  exec-policy Policy1-UNI-IN-Ch
end-policy
!
policy qos Policy2-NNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then
   set ieee-802.1p 7
   set mpls-exp topmost 7
 rule r5
  if qos-tag eq 46
  then
   set ieee-802.1p 5
   set mpls-exp topmost 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then
   set ieee-802.1p 4
   set mpls-exp topmost 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then
   set ieee-802.1p 3
   set mpls-exp topmost 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then
   set ieee-802.1p 2
   set mpls-exp topmost 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
```

```
  then
   set ieee-802.1p 1
   set mpls-exp topmost 1
 rule r0
  if qos-tag eq 0
  then
   set ieee-802.1p 0
   set mpls-exp topmost 0
 rule rule-default
end-policy
!
policy qos Policy2-NNI-OUT-Pr
 rule rule-default
  exec-policy Policy2-NNI-OUT-Ch
end-policy
!
policy qos Policy3-NNI-IN-Ch
 rule r0
  if match-any
   dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
   mpls-exp topmost eq 0
  then
   set qos-tag 0
   set color green
   set queue be
 rule r11
  if match-any
   dscp exist-in (8, af11)
   mpls-exp topmost eq 1
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if match-any
   dscp exist-in (af12, af13)
   mpls-exp topmost eq 1
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if match-any
   dscp exist-in (16, af21)
   mpls-exp topmost eq 2
```

```
 then
  set qos-tag 21
  set color green
  set queue af4
rule r22
 if match-any
  dscp exist-in (af22, af23)
  mpls-exp topmost eq 2
 then
  set qos-tag 22
  set color yellow
  set queue af4
rule r31
 if match-any
  dscp exist-in (24, af31)
  mpls-exp topmost eq 3
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if match-any
  dscp exist-in (af32, af33)
  mpls-exp topmost eq 3
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if match-any
  dscp exist-in (32, af41)
  mpls-exp topmost eq 4
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if match-any
  dscp exist-in (af42, af43)
  mpls-exp topmost eq 4
 then
  set qos-tag 42
  set color yellow
  set queue af2
rule r51
```

```
  if match-any
   dscp exist-in (40, 46)
   mpls-exp topmost eq 5
  then
   set qos-tag 46
   set color green
   set queue ef2
 rule r7
  if match-any
   dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
   mpls-exp topmost eq 6
   mpls-exp topmost eq 7
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy3-NNI-IN-Pr
 rule rule-default
  exec-policy Policy3-NNI-IN-Ch
end-policy
!
policy qos Policy4-UNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then set ieee-802.1p 7
 rule r5
  if qos-tag eq 46
  then set ieee-802.1p 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then set ieee-802.1p 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then set ieee-802.1p 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then set ieee-802.1p 2
```

```
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then set ieee-802.1p 1
 rule r0
  if qos-tag eq 0
  then set ieee-802.1p 0
 rule rule-default
end-policy
!
policy qos Policy4-UNI-OUT-Pr
 rule rule-default
  exec-policy Policy4-UNI-OUT-Ch
end-policy
!
interface mgmt 0/0/0
 admin-state  up
 ipv4-address 10.3.51.1/24
!
!
interface x-eth 0/1/7
 l2-transport enable
 speed        10000
 admin-state  up
 description  to_L2-cloud
!
!
interface x-eth 0/1/10
 speed       10000
 admin-state up
 description to_BS_CE3051
!
interface x-eth 0/1/10.103
 description  to_BS_CE3051_VPN3G
 ipv4-address 10.0.31.9/30
 vrf          3G
 vlan-id      103
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr
!
interface x-eth 0/1/10.104
 description  to_BS_CE3051_VPN4G
 ipv4-address 10.90.90.1/30
 vrf          4G
```

```
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr
!
interface x-eth 0/1/10.105
 description  to_BS_CE3051_VPN5G
 ipv4-address 10.1.11.1/30
 vrf          5G
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr

!
interface x-eth 0/0/1
 speed       10000
 admin-state up
 description to_CSG2_x0/0/2
 mpls        enable
!
interface x-eth 0/0/1.100
 description  to_CSG2_x0/0/2.100
 ipv4-address 122.168.1.6/30
 mpls         enable
 vlan-id      100
!
interface x-eth 0/0/2
 speed       10000
 admin-state up
 description to_ASG1_x0/0/1
 mpls        enable
!
interface x-eth 0/0/2.200
 description  to_ASG1_x0/0/1.100
 ipv4-address 192.168.1.9/30
 mpls         enable
 vlan-id      200
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
!
!
interface loopback 0
 description  RouterID
 ipv4-address 101.101.101.101/32
!
mpls ldp default
 explicit-null enable
 local-address ipv4 101.101.101.101
```

```
 router-id     101.101.101.101
 interface x-eth 0/0/1.100
  af-ipv4
 !
 interface x-eth 0/0/2.200
  af-ipv4
 !
 label-allocation policy LDP_LABEL_HOST
!
mpls te rsvp default
 explicit-null enable
 ip-source     101.101.101.101
 interface x-eth 0/0/1.100
 !
 interface x-eth 0/0/2.200
 !
 path toASG1_path
  nexthop 192.168.1.10 strict
  nexthop 11.11.11.11 strict
 !
 tunnel-te toASG1
  tunnel-destination 11.11.11.11
  tunnel-source      101.101.101.101
  admin-state        down
  path               toASG1_path
  igp-metric         9999
  secondary default
   cspf    enable
   standby enable
  !
 !
!
l2-services
 pw-profile Profile1
  type raw
  mtu  1500
 !
 vpws L2vpn1
  neighbor 12.12.12.12 pw-id 1001
  interface x-eth 0/1/7
  profile Profile1
 !
!
system
 hostname 3051CSG1
```

```
!
routing static
 vrf management
  af-ipv4 unicast
   route 0.0.0.0/0 gateway 10.3.51.254
  !
 !
!
routing ospf 1
 vrf default
  mpls-te   enable
  router-id 101.101.101.101
  area 0.0.0.1
   interface x-eth 0/0/1.100
    network-type point-to-point
    mtu          1500
   !
   interface x-eth 0/0/2.200
    network-type point-to-point
    mtu          1500
   !
   interface loopback 0
    passive enable
   !
  !
 !
!
routing bgp 65000
 router-id 101.101.101.101
 vrf 3G
  af-ipv4 unicast
   redistribute connected
   export-rt 65000:3
   import-rt 65000:3
  !
 !
 vrf 4G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:104
   import-rt 900:104
  !
 !
 vrf 5G
  af-ipv4 unicast
```

```
   redistribute connected
   export-rt 900:105
   import-rt 900:105
  !
 !
 vrf default
  af-ipv4 unicast
   network 101.101.101.101/32
  !
  neighbor 11.11.11.11
   local-address 101.101.101.101
   remote-as-number 65000
   af-ipv4 unicast
    send-community all
   !
   af-ipv4 vpn
    send-community all
   !
   af-ipv4 labeled-unicast
   !
  !
  neighbor 12.12.12.12
   local-address 101.101.101.101
   remote-as-number 65000
   af-ipv4 unicast
    send-community all
   !
   af-ipv4 vpn
    send-community all
   !
   af-ipv4 labeled-unicast
   !
  !
 !
!
aaa user admin
 password $1$U4$uyksWEZhyup0h5Jj5126H0
 role super_admin
!
aaa user private
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role super_admin
!
aaa user public
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
```

```
 role snmp
!
aaa role priv_admin
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role snmp
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role super_admin
 privilege all
!
log output file syslog
 filter facility any
  severity 4-warning
 !
 filter facility kernel
  severity none
 !
 filter facility infra
  severity 5-notice
 !
 filter facility infra-utils
  severity none
 !
!
log output remote-server 192.168.0.2
 vrf  default
 port 514
 filter facility any
  severity any
 !
!
snmp
 status enable
 agent
  network
   ip-address 0.0.0.0
```

```
   vrf        management
   version v2c
    community-name dfa98JGhd78s45868$^(()DGFJsscd
   !
  !
  platform
   ip-address 0.0.0.0
   vrf        management
   version v2c
    community-name dfa98JGhd78s45868$^(()DGFJsscd
   !
  !
 !
 traps
  target-id 1
   target-address 192.168.0.100
   udp-port       162
   vrf            management
   version v2c
    community-name dfa98JGhd78s45868$^(()DGFJsscd
   !
  !
 !
!
mib2
 location "Exaware Labs"
 name     Exaros
!
telnet-server disable
!end-of-config
```

11.1.2. CSG2

11.1.2.1. CSG2

```
! CSG2
!
vrf 3G
 rd 65000:3
 af-ipv4 unicast
 !
!
vrf 4G
```

```
 rd 900:104
 af-ipv4 unicast
 !
!
vrf 5G
 rd 900:105
 af-ipv4 unicast
 !
!
vrf default
!
vrf management
!
policy route LDP_LABEL_HOST
 rule rule1
  if prefix exist-in (0.0.0.0/0 matching-len 32)
  then permit
end-policy
!
policy qos Policy1-UNI-IN-Ch
 rule r0
  if dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
  then
   set qos-tag 0
   set color green
   set dscp 0
   set queue be
 rule r11
  if dscp exist-in (8, af11)
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if dscp exist-in (af12, af13)
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if dscp exist-in (16, af21)
  then
   set qos-tag 21
   set color green
   set queue af4
```

```
 rule r22
  if dscp exist-in (af22, af23)
  then
   set qos-tag 22
   set color yellow
   set queue af4
 rule r31
  if dscp exist-in (24, af31)
  then
   set qos-tag 31
   set color green
   set queue af3
 rule r32
  if dscp exist-in (af32, af33)
  then
   set qos-tag 32
   set color yellow
   set queue af3
 rule r41
  if dscp exist-in (32, af41)
  then
   set qos-tag 41
   set color green
   set queue af2
 rule r42
  if dscp exist-in (af42, af43)
  then
   set qos-tag 42
   set color yellow
   set queue af2
 rule r51
  if dscp exist-in (40, 46)
  then
   set qos-tag 46
   set color green
   set queue ef2
 rule r7
  if dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy1-UNI-IN-Pr
```

```
 rule rule-default
  exec-policy Policy1-UNI-IN-Ch
end-policy
!
policy qos Policy2-NNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then
   set ieee-802.1p 7
   set mpls-exp topmost 7
 rule r5
  if qos-tag eq 46
  then
   set ieee-802.1p 5
   set mpls-exp topmost 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then
   set ieee-802.1p 4
   set mpls-exp topmost 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then
   set ieee-802.1p 3
   set mpls-exp topmost 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then
   set ieee-802.1p 2
   set mpls-exp topmost 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then
   set ieee-802.1p 1
   set mpls-exp topmost 1
 rule r0
  if qos-tag eq 0
```

```
  then
   set ieee-802.1p 0
   set mpls-exp topmost 0
 rule rule-default
end-policy
!
policy qos Policy2-NNI-OUT-Pr
 rule rule-default
  exec-policy Policy2-NNI-OUT-Ch
end-policy
!
policy qos Policy3-NNI-IN-Ch
 rule r0
  if match-any
   dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
   mpls-exp topmost eq 0
  then
   set qos-tag 0
   set color green
   set queue be
 rule r11
  if match-any
   dscp exist-in (8, af11)
   mpls-exp topmost eq 1
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if match-any
   dscp exist-in (af12, af13)
   mpls-exp topmost eq 1
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if match-any
   dscp exist-in (16, af21)
   mpls-exp topmost eq 2
  then
   set qos-tag 21
   set color green
   set queue af4
 rule r22
```

```
 if match-any
  dscp exist-in (af22, af23)
  mpls-exp topmost eq 2
 then
  set qos-tag 22
  set color yellow
  set queue af4
rule r31
 if match-any
  dscp exist-in (24, af31)
  mpls-exp topmost eq 3
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if match-any
  dscp exist-in (af32, af33)
  mpls-exp topmost eq 3
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if match-any
  dscp exist-in (32, af41)
  mpls-exp topmost eq 4
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if match-any
  dscp exist-in (af42, af43)
  mpls-exp topmost eq 4
 then
  set qos-tag 42
  set color yellow
  set queue af2
rule r51
 if match-any
  dscp exist-in (40, 46)
  mpls-exp topmost eq 5
 then
  set qos-tag 46
```

```
   set color green
   set queue ef2
 rule r7
  if match-any
   dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
   mpls-exp topmost eq 6
   mpls-exp topmost eq 7
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy3-NNI-IN-Pr
 rule rule-default
  exec-policy Policy3-NNI-IN-Ch
end-policy
!
policy qos Policy4-UNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then set ieee-802.1p 7
 rule r5
  if qos-tag eq 46
  then set ieee-802.1p 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then set ieee-802.1p 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then set ieee-802.1p 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then set ieee-802.1p 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then set ieee-802.1p 1
```

```
 rule r0
  if qos-tag eq 0
  then set ieee-802.1p 0
 rule rule-default
end-policy
!
policy qos Policy4-UNI-OUT-Pr
 rule rule-default
  exec-policy Policy4-UNI-OUT-Ch
end-policy
!
interface mgmt 0/0/0
 admin-state  up
 ipv4-address 10.3.51.2/24
!
!
!
interface x-eth 0/1/10
 speed       10000
 admin-state up
 description to_BS_CE3051
!
interface x-eth 0/1/10.103
 description  to_BS_CE3052_VPN3G
 ipv4-address 10.0.32.9/30
 vrf          3G
 vlan-id      103
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr
!
interface x-eth 0/1/10.104
 description  to_BS_CE3052_VPN4G
 ipv4-address 10.90.92.1/30
 vrf          4G
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr
!
interface x-eth 0/1/10.105
 description  to_BS_CE3052_VPN5G
 ipv4-address 10.1.12.1/30
 vrf          5G
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr

!
```

```
interface x-eth 0/0/2
 speed       10000
 admin-state up
 description to_CSG2_x0/0/1
 mpls        enable
!
interface x-eth 0/0/2.100
 description  to_CSG1_x0/0/1.100
 ipv4-address 122.168.1.5/30
 mpls         enable
 vlan-id      100
!
interface x-eth 0/0/1
 speed       10000
 admin-state up
 description to_ASG2_x0/0/2
 mpls        enable
!
interface x-eth 0/0/1.200
 description  to_ASG2_x0/0/2.100
 ipv4-address 192.168.1.1/30
 mpls         enable
 vlan-id      200
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
!


interface loopback 0
 description  RouterID
 ipv4-address 102.102.102.102/32
!
interface loopback 100
 ipv4-address 100.1.1.51/32
 vrf          a1
!
mpls ldp default
 explicit-null enable
 local-address ipv4 102.102.102.102
 router-id     102.102.102.102
 interface x-eth 0/0/2.100
  af-ipv4
 !
 interface x-eth 0/0/1.200
  af-ipv4
```

```
 !
 label-allocation policy LDP_LABEL_HOST
!
mpls te rsvp default
 explicit-null enable
 ip-source     102.102.102.102
 interface x-eth 0/0/2.100
 !
 interface x-eth 0/0/1.200
 !
 path toASG1_path
  nexthop 192.168.1.10 strict
  nexthop 11.11.11.11 strict
 !
 tunnel-te toASG1
  tunnel-destination 11.11.11.11
  tunnel-source      102.102.102.102
  admin-state        down
  path               toASG1_path
  igp-metric         9999
  secondary default
   cspf    enable
   standby enable
  !
 !
!
system
 hostname 3051CSG2
!
routing static
 vrf management
  af-ipv4 unicast
   route 0.0.0.0/0 gateway 10.3.51.254
  !
 !
!
routing ospf 1
 vrf default
  mpls-te   enable
  router-id 102.102.102.102
  area 0.0.0.1
   interface x-eth 0/0/2.100
    network-type point-to-point
    mtu          1500
   !
```

```
   interface x-eth 0/0/1.200
    network-type point-to-point
    mtu          1500
   !
   interface loopback 0
    passive enable
   !
  !
 !
!
routing bgp 65000
 router-id 102.102.102.102
 vrf 3G
  af-ipv4 unicast
   redistribute connected
   export-rt 65000:3
   import-rt 65000:3
  !
 !
 vrf 4G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:104
   import-rt 900:104
  !
 !
 vrf 5G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:105
   import-rt 900:105
  !
 !
 vrf default
  af-ipv4 unicast
   network 102.102.102.102/32
  !
  neighbor 11.11.11.11
   local-address 102.102.102.102
   remote-as-number 65000
   af-ipv4 unicast
    send-community all
   !
   af-ipv4 vpn
    send-community all
```

```
   !
   af-ipv4 labeled-unicast
   !
  !
  neighbor 12.12.12.12
   local-address 102.102.102.102
   remote-as-number 65000
   af-ipv4 unicast
    send-community all
   !
   af-ipv4 vpn
    send-community all
   !
   af-ipv4 labeled-unicast
   !
  !
 !
!
aaa user admin
 password $1$U4$uyksWEZhyup0h5Jj5126H0
 role super_admin
!
aaa user private
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role super_admin
!
aaa user public
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role snmp
!
aaa role priv_admin
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role snmp
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role super_admin
```

```
 privilege all
!
log output file syslog
 filter facility any
  severity 4-warning
 !
 filter facility kernel
  severity none
 !
 filter facility infra
  severity 5-notice
 !
 filter facility infra-utils
  severity none
 !
!
log output remote-server 192.168.0.2
 vrf  default
 port 514
 filter facility any
  severity any
 !
!
snmp
 status enable
 agent
  network
   ip-address 0.0.0.0
   vrf        management
   version v2c
    community-name dfa98JGh$^(()DGFJsscdd78s45868
   !
  !
  platform
   ip-address 0.0.0.0
   vrf        management
   version v2c
    community-name dfa98JGh$^(()DGFJsscdd78s45868
   !
  !
 !
 traps
  target-id 1
   target-address 192.168.0.100
   udp-port       162
```

```
   vrf            management
   version v2c
    community-name dfa98JGh$^(()DGFJsscdd78s45868
   !
  !
 !
!
mib2
 location "Exaware Labs"
 name     Exaros
!
telnet-server disable
!end-of-config
```

11.2. ASG

11.2.1. ASG1

11.2.1.1. ASG1

```
! ASG1
!
vrf 3G
 rd 65000:3
 af-ipv4 unicast
 !
!
vrf 4G
 rd 900:104
 af-ipv4 unicast
 !
!
vrf 5G
 rd 900:105
 af-ipv4 unicast
 !
!
 af-ipv4 unicast
 !
```

```
!
vrf default
!
vrf management
!
policy route LDP_LABEL_HOST
 rule rule1
  if prefix exist-in (0.0.0.0/0 matching-len 32)
  then permit
end-policy
!
policy route NHS
 rule rule1
  next-hop set self
end-policy
!
policy qos Policy1-UNI-IN-Ch
 rule r0
  if dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
  then
   set qos-tag 0
   set color green
   set dscp 0
   set queue be
 rule r11
  if dscp exist-in (8, af11)
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if dscp exist-in (af12, af13)
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if dscp exist-in (16, af21)
  then
   set qos-tag 21
   set color green
   set queue af4
 rule r22
  if dscp exist-in (af22, af23)
  then
```

```
   set qos-tag 22
   set color yellow
   set queue af4
 rule r31
  if dscp exist-in (24, af31)
  then
   set qos-tag 31
   set color green
   set queue af3
 rule r32
  if dscp exist-in (af32, af33)
  then
   set qos-tag 32
   set color yellow
   set queue af3
 rule r41
  if dscp exist-in (32, af41)
  then
   set qos-tag 41
   set color green
   set queue af2
 rule r42
  if dscp exist-in (af42, af43)
  then
   set qos-tag 42
   set color yellow
   set queue af2
 rule r51
  if dscp exist-in (40, 46)
  then
   set qos-tag 46
   set color green
   set queue ef2
 rule r7
  if dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy1-UNI-IN-Pr
 rule rule-default
  exec-policy Policy1-UNI-IN-Ch
end-policy
```

```
!
policy qos Policy2-NNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then
   set ieee-802.1p 7
   set mpls-exp topmost 7
 rule r5
  if qos-tag eq 46
  then
   set ieee-802.1p 5
   set mpls-exp topmost 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then
   set ieee-802.1p 4
   set mpls-exp topmost 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then
   set ieee-802.1p 3
   set mpls-exp topmost 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then
   set ieee-802.1p 2
   set mpls-exp topmost 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then
   set ieee-802.1p 1
   set mpls-exp topmost 1
 rule r0
  if qos-tag eq 0
  then
   set ieee-802.1p 0
   set mpls-exp topmost 0
```

```
 rule rule-default
end-policy
!
policy qos Policy2-NNI-OUT-Pr
 rule rule-default
  exec-policy Policy2-NNI-OUT-Ch
end-policy
!
policy qos Policy3-NNI-IN-Ch
 rule r0
  if match-any
   dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
   mpls-exp topmost eq 0
  then
   set qos-tag 0
   set color green
   set queue be
 rule r11
  if match-any
   dscp exist-in (8, af11)
   mpls-exp topmost eq 1
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if match-any
   dscp exist-in (af12, af13)
   mpls-exp topmost eq 1
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if match-any
   dscp exist-in (16, af21)
   mpls-exp topmost eq 2
  then
   set qos-tag 21
   set color green
   set queue af4
 rule r22
  if match-any
   dscp exist-in (af22, af23)
   mpls-exp topmost eq 2
```

```
 then
  set qos-tag 22
  set color yellow
  set queue af4
rule r31
 if match-any
  dscp exist-in (24, af31)
  mpls-exp topmost eq 3
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if match-any
  dscp exist-in (af32, af33)
  mpls-exp topmost eq 3
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if match-any
  dscp exist-in (32, af41)
  mpls-exp topmost eq 4
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if match-any
  dscp exist-in (af42, af43)
  mpls-exp topmost eq 4
 then
  set qos-tag 42
  set color yellow
  set queue af2
rule r51
 if match-any
  dscp exist-in (40, 46)
  mpls-exp topmost eq 5
 then
  set qos-tag 46
  set color green
  set queue ef2
rule r7
```

```
  if match-any
   dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
   mpls-exp topmost eq 6
   mpls-exp topmost eq 7
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy3-NNI-IN-Pr
 rule rule-default
  exec-policy Policy3-NNI-IN-Ch
end-policy
!
policy qos Policy4-UNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then set ieee-802.1p 7
 rule r5
  if qos-tag eq 46
  then set ieee-802.1p 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then set ieee-802.1p 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then set ieee-802.1p 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then set ieee-802.1p 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then set ieee-802.1p 1
 rule r0
  if qos-tag eq 0
  then set ieee-802.1p 0
```

```
 rule rule-default
end-policy
!
policy qos Policy4-UNI-OUT-Pr
 rule rule-default
  exec-policy Policy4-UNI-OUT-Ch
end-policy
!
interface mgmt 0/0/0
 admin-state down
!
!
interface x-eth 0/1/2

 speed       10000
 admin-state up
 description toCR1_x0/1/1
!
interface x-eth 0/1/2.20
 description  toCR1_x0/1/1.20
 ipv4-address 172.16.1.9/30
 mpls         enable
 vlan-id      20
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
!
!
interface x-eth 0/1/1
 speed       10000
 admin-state up
 description toASG2_x0/1/2
!
interface x-eth 0/1/1.60
 description  toASG2_x0/1/2.60
 ipv4-address 172.16.1.5/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      60
!
!
interface x-eth 0/0/2
 speed       10000
 admin-state up
 description to_ASG2_x0/0/1
```

```
!
interface x-eth 0/0/2.50
 description  to_ASG2_x0/0/1.50
 ipv4-address 192.168.0.1/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      50
!
!
interface x-eth 0/0/1
 speed       10000
 admin-state up
 description to_CSG1_x0/0/2
 mpls        enable
!
interface x-eth 0/0/1.200
 description  to_CSG1_x0/0/2.200
 ipv4-address 192.168.1.10/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      200
!
!
!
interface loopback 0
 description  RouterID
 ipv4-address 11.11.11.11/32
!
interface loopback 100
 ipv4-address 100.1.1.88/32
 vrf          a1
!
mpls ldp default
 explicit-null enable
 local-address ipv4 11.11.11.11
 router-id     11.11.11.11
 interface x-eth 0/1/2.20
  af-ipv4
 !
 interface x-eth 0/0/14.200
  af-ipv4
  !
 interface x-eth 0/1/1.60
```

```
  af-ipv4
  !
 interface x-eth 0/0/2.50
  af-ipv4
 !
 label-allocation policy LDP_LABEL_HOST
!
mpls te rsvp default
 explicit-null enable
 ip-source     11.11.11.11

interface x-eth 0/0/14.200
 !
interface x-eth 0/1/1.60
 !
interface x-eth 0/0/2.50
 !
 path toCSG1_path
  nexthop 192.168.1.9 strict
  nexthop 101.101.101.101 strict
 !
 tunnel-te toCSG1
  tunnel-destination 101.101.101.101
  tunnel-source      11.11.11.11
  admin-state        down
  path               toCSG1_path
  secondary default
   cspf    enable
   standby enable
  !
 !
!
system
 hostname 3088ASG1
!
routing ospf 1
 vrf default
  mpls-te   enable
  router-id 11.11.11.11
  area 0.0.0.1
   interface x-eth 0/1/2.20
    network-type point-to-point
    mtu          1500
   !
   interface x-eth 0/0/14.200
```

```
    network-type point-to-point
    mtu          1500
   !
  interface x-eth 0/1/1.60
    network-type point-to-point
    mtu          1500
   !
  interface x-eth 0/0/2.50
    network-type point-to-point
    mtu          1500
!
   interface loopback 0
    passive enable
   !
  !
 !
!
routing bgp 65000
 router-id 11.11.11.11
vrf 3G
  af-ipv4 unicast
   redistribute connected
   export-rt 65000:3
   import-rt 65000:3
  !
 !
 vrf 4G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:104
   import-rt 900:104
  !
 !
 vrf 5G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:105
   import-rt 900:105
  !
  !
 !
vrf default
  af-ipv4 unicast
   network 11.11.11.11/32
  !
```

```
neighbor 1.1.1.1
 local-address loopback 0
 !
 remote-as-number 65000
 af-ipv4 unicast
  next-hop-self  enable
  send-community all
 !
 af-ipv4 vpn
  send-community all
 !
 af-ipv4 labeled-unicast
 !
!
neighbor 2.2.2.2
 local-address loopback 0
 !
 remote-as-number 65000
 af-ipv4 unicast
  next-hop-self  enable
  send-community all
 !
 af-ipv4 vpn
  send-community all
 !
!
neighbor 101.101.101.101
 local-address loopback 0
 !
 remote-as-number 65000
 af-ipv4 unicast
  policy out NHS
  route-reflector-client enable
  next-hop-self          enable
  send-community         all
 !
 af-ipv4 vpn
  route-reflector-client enable
  next-hop-self          enable
  send-community         all
 !
 af-ipv4 labeled-unicast
 !
!
  neighbor 102.102.102.102
```

```
   local-address loopback 0
   !
   remote-as-number 65000
   af-ipv4 unicast
    policy out NHS
    route-reflector-client enable
    next-hop-self          enable
    send-community         all
   !
   af-ipv4 vpn
    route-reflector-client enable
    next-hop-self          enable
    send-community         all
   !
   af-ipv4 labeled-unicast
   !
  !
 !
!
aaa user admin
 password $1$U4$uyksWEZhyup0h5Jj5126H0
 role super_admin
!
aaa user private
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role super_admin
!
aaa user public
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role snmp
!
aaa role priv_admin
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role snmp
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
```

```
aaa role super_admin
 privilege all
!
log output file syslog
 filter facility any
  severity 4-warning
 !
 filter facility kernel
  severity none
 !
 filter facility infra
  severity 5-notice
 !
 filter facility infra-utils
  severity none
 !
!
mib2
 location "Exaware Labs"
 name     Exaros
!
telnet-server disable
!end-of-config
```

11.2.2. ASG2

11.2.2.1. ASG2

```
! ASG2
!
vrf 3G
 rd 65000:3
 af-ipv4 unicast
 !
!
vrf 4G
 rd 900:104
 af-ipv4 unicast
 !
!
vrf 5G
 rd 900:105
 af-ipv4 unicast
```

```
 !
!
 af-ipv4 unicast
 !
!
vrf default
!
vrf management
!
policy route LDP_LABEL_HOST
 rule rule1
  if prefix exist-in (0.0.0.0/0 matching-len 32)
  then permit
end-policy
!
policy route NHS
 rule rule1
  next-hop set self
end-policy
!
policy qos Policy1-UNI-IN-Ch
 rule r0
  if dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
  then
   set qos-tag 0
   set color green
   set dscp 0
   set queue be
 rule r11
  if dscp exist-in (8, af11)
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if dscp exist-in (af12, af13)
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if dscp exist-in (16, af21)
  then
   set qos-tag 21
   set color green
```

```
   set queue af4
 rule r22
  if dscp exist-in (af22, af23)
  then
   set qos-tag 22
   set color yellow
   set queue af4
 rule r31
  if dscp exist-in (24, af31)
  then
   set qos-tag 31
   set color green
   set queue af3
 rule r32
  if dscp exist-in (af32, af33)
  then
   set qos-tag 32
   set color yellow
   set queue af3
 rule r41
  if dscp exist-in (32, af41)
  then
   set qos-tag 41
   set color green
   set queue af2
 rule r42
  if dscp exist-in (af42, af43)
  then
   set qos-tag 42
   set color yellow
   set queue af2
 rule r51
  if dscp exist-in (40, 46)
  then
   set qos-tag 46
   set color green
   set queue ef2
 rule r7
  if dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
```

```
policy qos Policy1-UNI-IN-Pr
 rule rule-default
  exec-policy Policy1-UNI-IN-Ch
end-policy
!
policy qos Policy2-NNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then
   set ieee-802.1p 7
   set mpls-exp topmost 7
 rule r5
  if qos-tag eq 46
  then
   set ieee-802.1p 5
   set mpls-exp topmost 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then
   set ieee-802.1p 4
   set mpls-exp topmost 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then
   set ieee-802.1p 3
   set mpls-exp topmost 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then
   set ieee-802.1p 2
   set mpls-exp topmost 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then
   set ieee-802.1p 1
   set mpls-exp topmost 1
 rule r0
```

```
  if qos-tag eq 0
  then
   set ieee-802.1p 0
   set mpls-exp topmost 0
 rule rule-default
end-policy
!
policy qos Policy2-NNI-OUT-Pr
 rule rule-default
  exec-policy Policy2-NNI-OUT-Ch
end-policy
!
policy qos Policy3-NNI-IN-Ch
 rule r0
  if match-any
   dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
   mpls-exp topmost eq 0
  then
   set qos-tag 0
   set color green
   set queue be
 rule r11
  if match-any
   dscp exist-in (8, af11)
   mpls-exp topmost eq 1
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if match-any
   dscp exist-in (af12, af13)
   mpls-exp topmost eq 1
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if match-any
   dscp exist-in (16, af21)
   mpls-exp topmost eq 2
  then
   set qos-tag 21
   set color green
   set queue af4
```

```
rule r22
 if match-any
  dscp exist-in (af22, af23)
  mpls-exp topmost eq 2
 then
  set qos-tag 22
  set color yellow
  set queue af4
rule r31
 if match-any
  dscp exist-in (24, af31)
  mpls-exp topmost eq 3
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if match-any
  dscp exist-in (af32, af33)
  mpls-exp topmost eq 3
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if match-any
  dscp exist-in (32, af41)
  mpls-exp topmost eq 4
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if match-any
  dscp exist-in (af42, af43)
  mpls-exp topmost eq 4
 then
  set qos-tag 42
  set color yellow
  set queue af2
rule r51
 if match-any
  dscp exist-in (40, 46)
  mpls-exp topmost eq 5
 then
```

```
   set qos-tag 46
   set color green
   set queue ef2
 rule r7
  if match-any
   dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
   mpls-exp topmost eq 6
   mpls-exp topmost eq 7
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy3-NNI-IN-Pr
 rule rule-default
  exec-policy Policy3-NNI-IN-Ch
end-policy
!
policy qos Policy4-UNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then set ieee-802.1p 7
 rule r5
  if qos-tag eq 46
  then set ieee-802.1p 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then set ieee-802.1p 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then set ieee-802.1p 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then set ieee-802.1p 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
```

```
  then set ieee-802.1p 1
 rule r0
  if qos-tag eq 0
  then set ieee-802.1p 0
 rule rule-default
end-policy
!
policy qos Policy4-UNI-OUT-Pr
 rule rule-default
  exec-policy Policy4-UNI-OUT-Ch
end-policy
!
interface mgmt 0/0/0
 admin-state down
!
interface x-eth 0/1/1
 speed       10000
 admin-state up
 description toCR2_x0/1/2
!
interface x-eth 0/1/1.20
 description  toCR2_x0/1/2.20
 ipv4-address 172.16.1.1/30
 mpls         enable
 vlan-id      20
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
!
!
interface x-eth 0/1/2
 speed       10000
 admin-state up
 description toASG1_x0/1/1
!
interface x-eth 0/1/2.60
 description  toASG1_x0/1/1.60
 ipv4-address 172.16.1.6/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      60
!
!
!
interface x-eth 0/0/1
```

```
 speed       10000
 admin-state up
 description to_ASG1_x0/0/2
!
interface x-eth 0/0/1.50
 description  to_ASG1_x0/0/2.50
 ipv4-address 192.168.0.2/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      50
!
!
!
interface x-eth 0/0/7
 l2-transport enable
 speed        10000
 admin-state  up
 description  to_L2-cloud
!
!
interface x-eth 0/0/2
 speed       10000
 admin-state up
 description to_CSG2_x0/0/1
 mpls        enable
!
interface x-eth 0/0/2.200
 description  to_CSG2_x0/0/1.200
 ipv4-address 192.168.1.2/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      200
!
!
interface loopback 0
 description  RouterID
 ipv4-address 12.12.12.12/32
!
mpls ldp default
 explicit-null enable
 local-address ipv4 12.12.12.12
 router-id     12.12.12.12
 interface x-eth 0/1/1.20
```

```
  af-ipv4
 !
 interface x-eth 0/0/14.200
  af-ipv4
 !
 interface x-eth 0/1/2.60
   af-ipv4
 !
 interface x-eth 0/0/1.50
   af-ipv4

 !
 label-allocation policy LDP_LABEL_HOST
!
mpls te rsvp default
 explicit-null enable
 ip-source     12.12.12.12
  !
  interface x-eth 0/0/5.20
  !
 interface x-eth 0/0/14.200
  !
 interface x-eth 0/1/2.60
  !
 interface x-eth 0/0/1.50
 !
 !
 tunnel-te toCSG1
  tunnel-destination 101.101.101.101
  tunnel-source      12.12.12.12
  admin-state        down

  secondary default
   cspf    enable
   standby enable
  !
 !
 path toCSG2_path
  nexthop 192.168.1.2 strict
  nexthop 102.102.102.102 strict
 !
 tunnel-te toCSG1
  tunnel-destination 102.102.102.102
  tunnel-source      12.12.12.12
  admin-state        down
```

```
  path               toCSG2_path
  secondary default
   cspf    enable
   standby enable
  !
 !
!
l2-services
 pw-profile Profile1
  type raw
  mtu  1500
 !
 vpws L2vpn1
  neighbor 101.101.101.101 pw-id 1001
  interface x-eth 0/0/7
  profile Profile1
 !
!
system
 hostname 3051CSG1
!
routing static
 vrf management
  af-ipv4 unicast
   route 0.0.0.0/0 gateway 10.3.51.254
  !
 !
!
system
 hostname 3088ASG2
!
routing ospf 1
 vrf default
  mpls-te   enable
  router-id 12.12.12.12
  area 0.0.0.1
   interface x-eth 0/1/1.20
    network-type point-to-point
    mtu          1500
   !
   interface x-eth 0/0/14.200
    network-type point-to-point
    mtu          1500
   interface x-eth 0/1/2.60
    network-type point-to-point
```

```
    mtu          1500
   interface x-eth 0/0/1.50
    network-type point-to-point
    mtu          1500
   !
   interface loopback 0
    passive enable
   !
  !
 !
!
routing bgp 65000
 router-id 12.12.12.12
vrf 3G
  af-ipv4 unicast
   redistribute connected
   export-rt 65000:3
   import-rt 65000:3
  !
 !
 vrf 4G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:104
   import-rt 900:104
  !
 !
 vrf 5G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:105
   import-rt 900:105
  !
!
vrf default
  af-ipv4 unicast
   network 12.12.12.12/32
  !
  neighbor 1.1.1.1
   local-address loopback 0
   !
   remote-as-number 65000
   af-ipv4 unicast
    next-hop-self  enable
    send-community all
```

```
 !
 af-ipv4 vpn
  send-community all
 !
 af-ipv4 labeled-unicast
 !
!
neighbor 2.2.2.2
 local-address loopback 0
 !
 remote-as-number 65000
 af-ipv4 unicast
  next-hop-self  enable
  send-community all
 !
 af-ipv4 vpn
  send-community all
 !
!
neighbor 101.101.101.101
 local-address loopback 0
 !
 remote-as-number 65000
 af-ipv4 unicast
  policy out NHS
  route-reflector-client enable
  next-hop-self          enable
  send-community         all
 !
 af-ipv4 vpn
  route-reflector-client enable
  next-hop-self          enable
  send-community         all
 !
 af-ipv4 labeled-unicast
 !
!
  neighbor 102.102.102.102
 local-address loopback 0
 !
 remote-as-number 65000
 af-ipv4 unicast
  policy out NHS
  route-reflector-client enable
  next-hop-self          enable
```

```
    send-community         all
   !
   af-ipv4 vpn
    route-reflector-client enable
    next-hop-self          enable
    send-community         all
   !
   af-ipv4 labeled-unicast
   !
  !
 !
!
aaa user admin
 password $1$U4$uyksWEZhyup0h5Jj5126H0
 role super_admin
!
aaa user private
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role super_admin
!
aaa user public
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role snmp
!
aaa role priv_admin
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role snmp
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role super_admin
 privilege all
!
log output file syslog
 filter facility any
  severity 4-warning
 !
```

```
 filter facility kernel
  severity none
 !
 filter facility infra
  severity 5-notice
 !
 filter facility infra-utils
  severity none
 !
!
mib2
 location "Exaware Labs"
 name     Exaros
!
telnet-server disable
!end-of-config
```

11.3. CR

11.3.1. CR1

11.3.1.1. CR1

```
! CR1
!
vrf 3G
 rd 65000:3
 af-ipv4 unicast
 !
!
vrf 4G
 rd 900:104
 af-ipv4 unicast
 !
!
vrf 5G
 rd 900:105
 af-ipv4 unicast
 !
!
vrf a1
 rd 1:1
```

```
 af-ipv4 unicast
 !
!
vrf default
!
vrf management
!
policy route LDP_LABEL_HOST
 rule rule1
  if prefix exist-in (0.0.0.0/0 matching-len 32)
  then permit
end-policy
!
policy qos Policy1-UNI-IN-Ch
 rule r0
  if dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
  then
   set qos-tag 0
   set color green
   set dscp 0
   set queue be
 rule r11
  if dscp exist-in (8, af11)
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if dscp exist-in (af12, af13)
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if dscp exist-in (16, af21)
  then
   set qos-tag 21
   set color green
   set queue af4
 rule r22
  if dscp exist-in (af22, af23)
  then
   set qos-tag 22
   set color yellow
   set queue af4
```

```
 rule r31
  if dscp exist-in (24, af31)
  then
   set qos-tag 31
   set color green
   set queue af3
 rule r32
  if dscp exist-in (af32, af33)
  then
   set qos-tag 32
   set color yellow
   set queue af3
 rule r41
  if dscp exist-in (32, af41)
  then
   set qos-tag 41
   set color green
   set queue af2
 rule r42
  if dscp exist-in (af42, af43)
  then
   set qos-tag 42
   set color yellow
   set queue af2
 rule r51
  if dscp exist-in (40, 46)
  then
   set qos-tag 46
   set color green
   set queue ef2
 rule r7
  if dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy1-UNI-IN-Pr
 rule rule-default
  exec-policy Policy1-UNI-IN-Ch
end-policy
!
policy qos Policy2-NNI-OUT-Ch
 rule r7
```

```
  if qos-tag eq 56
  then
   set ieee-802.1p 7
   set mpls-exp topmost 7
 rule r5
  if qos-tag eq 46
  then
   set ieee-802.1p 5
   set mpls-exp topmost 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then
   set ieee-802.1p 4
   set mpls-exp topmost 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then
   set ieee-802.1p 3
   set mpls-exp topmost 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then
   set ieee-802.1p 2
   set mpls-exp topmost 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then
   set ieee-802.1p 1
   set mpls-exp topmost 1
 rule r0
  if qos-tag eq 0
  then
   set ieee-802.1p 0
   set mpls-exp topmost 0
 rule rule-default
end-policy
!
```

```
policy qos Policy2-NNI-OUT-Pr
 rule rule-default
  exec-policy Policy2-NNI-OUT-Ch
end-policy
!
policy qos Policy3-NNI-IN-Ch
 rule r0
  if match-any
   dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
   mpls-exp topmost eq 0
  then
   set qos-tag 0
   set color green
   set queue be
 rule r11
  if match-any
   dscp exist-in (8, af11)
   mpls-exp topmost eq 1
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if match-any
   dscp exist-in (af12, af13)
   mpls-exp topmost eq 1
  then
   set qos-tag 12
   set color yellow
   set queue af5
 rule r21
  if match-any
   dscp exist-in (16, af21)
   mpls-exp topmost eq 2
  then
   set qos-tag 21
   set color green
   set queue af4
 rule r22
  if match-any
   dscp exist-in (af22, af23)
   mpls-exp topmost eq 2
  then
   set qos-tag 22
   set color yellow
```

```
  set queue af4
rule r31
 if match-any
  dscp exist-in (24, af31)
  mpls-exp topmost eq 3
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if match-any
  dscp exist-in (af32, af33)
  mpls-exp topmost eq 3
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if match-any
  dscp exist-in (32, af41)
  mpls-exp topmost eq 4
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if match-any
  dscp exist-in (af42, af43)
  mpls-exp topmost eq 4
 then
  set qos-tag 42
  set color yellow
  set queue af2
rule r51
 if match-any
  dscp exist-in (40, 46)
  mpls-exp topmost eq 5
 then
  set qos-tag 46
  set color green
  set queue ef2
rule r7
 if match-any
  dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
  mpls-exp topmost eq 6
```

```
   mpls-exp topmost eq 7
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy3-NNI-IN-Pr
 rule rule-default
  exec-policy Policy3-NNI-IN-Ch
end-policy
!
policy qos Policy4-UNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then set ieee-802.1p 7
 rule r5
  if qos-tag eq 46
  then set ieee-802.1p 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then set ieee-802.1p 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then set ieee-802.1p 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then set ieee-802.1p 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then set ieee-802.1p 1
 rule r0
  if qos-tag eq 0
  then set ieee-802.1p 0
 rule rule-default
end-policy
!
```

```
policy qos Policy4-UNI-OUT-Pr
 rule rule-default
  exec-policy Policy4-UNI-OUT-Ch
end-policy
!
interface mgmt 0/0/0
 admin-state down
!
!
interface x-eth 0/1/1
 speed       10000
 admin-state up
 description toASG1_x0/1/2
!
interface x-eth 0/1/1.20
 ipv4-address 172.16.1.10/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      20
  description  to_ASG1
!
!
interface x-eth 0/1/2
 speed       10000
 admin-state up
 description toCR2_x0/1/1
!
!
interface x-eth 0/0/11
 speed       10000
 admin-state up
 description to_BSC_CE3096
!
interface x-eth 0/0/11.103
 description  to_BSC_CE3096_VPN3G
 ipv4-address 10.0.21.9/30
 vrf          3G
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr
 vlan-id      103
!
!
interface loopback 0
 ipv4-address 1.1.1.1/32
```

```
!
interface loopback 100
 ipv4-address 100.1.1.96/32
 vrf          a1
!
interface agg-eth 1
 l2-transport enable
 admin-state  up
!
mpls ldp default
 explicit-null enable
 local-address ipv4 1.1.1.1
 router-id     1.1.1.1
 interface x-eth 0/1/1.20
  af-ipv4
 !
 label-allocation policy LDP_LABEL_HOST
!
l2-services
 pw-profile NEXTLINK
  type raw
  mtu  1580
 !
 vpws vpws5196
  neighbor 51.51.51.51 pw-id 5196
  profile NEXTLINK
 !
 vpws vpws8896
  neighbor 88.88.88.88 pw-id 8896
  profile NEXTLINK
 !
 vpws vpws9496
  neighbor 94.94.94.94 pw-id 9496
  profile NEXTLINK
 !
 vpls VPLS2
  ve-id 8894
  interface x-eth 0/0/27
  !
  vpws vpws5196
  !
 !
!
system
 hostname 3096RSG1
```

```
!
routing static
 vrf default
  af-ipv4 unicast
   route 6.7.0.0/16 interface x-eth 0/0/21 distance 15 tag 2 description QQQ
  !
 !
!
routing ospf 1
 vrf default
  mpls-te             enable
  router-id           1.1.1.1
  fast-reroute        enable
  ldp-synchronization enable
  area 0.0.0.1
   interface x-eth 0/1/1.20
    network-type point-to-point
    mtu          1500
   !
   interface loopback 0
    passive enable
   !
  !
 !
!
routing bgp 65000
 router-id 1.1.1.1
 vrf 3G
  af-ipv4 unicast
   redistribute connected
   export-rt 65000:3
   import-rt 65000:3
  !
 !
 vrf 4G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:104
   import-rt 900:104
  !
 !
 vrf 5G
  af-ipv4 unicast
   redistribute connected
   export-rt 900:105
```

```
   import-rt 900:105
  !
 !
 vrf a1
  af-ipv4 unicast
   redistribute connected
   export-rt 1:1
   import-rt 1:1
  !
 !
 vrf default
  af-ipv4 unicast
   network 1.1.1.1/32
  !
  neighbor 11.11.11.11
   local-address loopback 0
   !
   remote-as-number 65000
   af-ipv4 unicast
    route-reflector-client enable
    next-hop-self          enable
    send-community         all
   !
   af-ipv4 vpn
    route-reflector-client enable
    send-community         all
   !
   af-ipv4 labeled-unicast
   !
  !
 !
!
aaa user admin
 password $1$U4$uyksWEZhyup0h5Jj5126H0
 role super_admin
!
aaa user private
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role super_admin
!
aaa user public
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role snmp
!
aaa role priv_admin
```

```
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role snmp
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role super_admin
 privilege all
!
log output file syslog
 filter facility any
  severity 4-warning
 !
 filter facility kernel
  severity none
 !
 filter facility infra
  severity 5-notice
 !
 filter facility infra-utils
  severity none
 !
!
mib2
 location "Exaware Labs"
 name     Exaros
!
telnet-server disable
!end-of-config
```

11.3.2. CR2

11.3.2.1. CR2

```
! CR2
!
```

```
vrf 3G
 rd 65000:3
 af-ipv4 unicast
 !
!
vrf 4G
 rd 900:104
 af-ipv4 unicast
 !
!
vrf 5G
 rd 900:105
 af-ipv4 unicast
 !
!
vrf a1
 rd 1:1
 af-ipv4 unicast
 !
!
vrf default
!
vrf management
!
policy route LDP_LABEL_HOST
 rule rule1
  if prefix exist-in (0.0.0.0/0 matching-len 32)
  then permit
end-policy
!
policy qos Policy1-UNI-IN-Ch
 rule r0
  if dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
  then
   set qos-tag 0
   set color green
   set dscp 0
   set queue be
 rule r11
  if dscp exist-in (8, af11)
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
```

```
 if dscp exist-in (af12, af13)
 then
  set qos-tag 12
  set color yellow
  set queue af5
rule r21
 if dscp exist-in (16, af21)
 then
  set qos-tag 21
  set color green
  set queue af4
rule r22
 if dscp exist-in (af22, af23)
 then
  set qos-tag 22
  set color yellow
  set queue af4
rule r31
 if dscp exist-in (24, af31)
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if dscp exist-in (af32, af33)
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if dscp exist-in (32, af41)
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if dscp exist-in (af42, af43)
 then
  set qos-tag 42
  set color yellow
  set queue af2
rule r51
 if dscp exist-in (40, 46)
 then
  set qos-tag 46
```

```
   set color green
   set queue ef2
 rule r7
  if dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy1-UNI-IN-Pr
 rule rule-default
  exec-policy Policy1-UNI-IN-Ch
end-policy
!
policy qos Policy2-NNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then
   set ieee-802.1p 7
   set mpls-exp topmost 7
 rule r5
  if qos-tag eq 46
  then
   set ieee-802.1p 5
   set mpls-exp topmost 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then
   set ieee-802.1p 4
   set mpls-exp topmost 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
  then
   set ieee-802.1p 3
   set mpls-exp topmost 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then
```

```
   set ieee-802.1p 2
   set mpls-exp topmost 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then
   set ieee-802.1p 1
   set mpls-exp topmost 1
 rule r0
  if qos-tag eq 0
  then
   set ieee-802.1p 0
   set mpls-exp topmost 0
 rule rule-default
end-policy
!
policy qos Policy2-NNI-OUT-Pr
 rule rule-default
  exec-policy Policy2-NNI-OUT-Ch
end-policy
!
policy qos Policy3-NNI-IN-Ch
 rule r0
  if match-any
   dscp exist-in (0, 1, 2, 3, 4, 5, 6, 7)
   mpls-exp topmost eq 0
  then
   set qos-tag 0
   set color green
   set queue be
 rule r11
  if match-any
   dscp exist-in (8, af11)
   mpls-exp topmost eq 1
  then
   set qos-tag 11
   set color green
   set queue af5
 rule r12
  if match-any
   dscp exist-in (af12, af13)
   mpls-exp topmost eq 1
  then
   set qos-tag 12
```

```
  set color yellow
  set queue af5
rule r21
 if match-any
  dscp exist-in (16, af21)
  mpls-exp topmost eq 2
 then
  set qos-tag 21
  set color green
  set queue af4
rule r22
 if match-any
  dscp exist-in (af22, af23)
  mpls-exp topmost eq 2
 then
  set qos-tag 22
  set color yellow
  set queue af4
rule r31
 if match-any
  dscp exist-in (24, af31)
  mpls-exp topmost eq 3
 then
  set qos-tag 31
  set color green
  set queue af3
rule r32
 if match-any
  dscp exist-in (af32, af33)
  mpls-exp topmost eq 3
 then
  set qos-tag 32
  set color yellow
  set queue af3
rule r41
 if match-any
  dscp exist-in (32, af41)
  mpls-exp topmost eq 4
 then
  set qos-tag 41
  set color green
  set queue af2
rule r42
 if match-any
  dscp exist-in (af42, af43)
```

```
   mpls-exp topmost eq 4
  then
   set qos-tag 42
   set color yellow
   set queue af2
 rule r51
  if match-any
   dscp exist-in (40, 46)
   mpls-exp topmost eq 5
  then
   set qos-tag 46
   set color green
   set queue ef2
 rule r7
  if match-any
   dscp exist-in (48, 56, 57, 58, 59, 60, 61, 62, 63)
   mpls-exp topmost eq 6
   mpls-exp topmost eq 7
  then
   set qos-tag 56
   set queue ef1
 rule rule-default
end-policy
!
policy qos Policy3-NNI-IN-Pr
 rule rule-default
  exec-policy Policy3-NNI-IN-Ch
end-policy
!
policy qos Policy4-UNI-OUT-Ch
 rule r7
  if qos-tag eq 56
  then set ieee-802.1p 7
 rule r5
  if qos-tag eq 46
  then set ieee-802.1p 5
 rule r4
  if match-any
   qos-tag eq 41
   qos-tag eq 42
  then set ieee-802.1p 4
 rule r3
  if match-any
   qos-tag eq 31
   qos-tag eq 32
```

```
  then set ieee-802.1p 3
 rule r2
  if match-any
   qos-tag eq 21
   qos-tag eq 22
  then set ieee-802.1p 2
 rule r1
  if match-any
   qos-tag eq 11
   qos-tag eq 12
  then set ieee-802.1p 1
 rule r0
  if qos-tag eq 0
  then set ieee-802.1p 0
 rule rule-default
end-policy
!
policy qos Policy4-UNI-OUT-Pr
 rule rule-default
  exec-policy Policy4-UNI-OUT-Ch
end-policy
!
interface mgmt 0/0/0
 admin-state down
!
!
interface x-eth 0/1/2
 speed       10000
 admin-state up
 description toASG1_x0/1/2
 mpls        enable
!
interface x-eth 0/1/2.20
 ipv4-address 172.16.1.1/30
 mpls         enable
 policy qos in-port-classification Policy3-NNI-IN-Pr
 policy qos out-port-pcp-marking Policy2-NNI-OUT-Pr
 vlan-id      20
 description  to_ASG2
!
!
interface x-eth 0/1/1
 speed       10000
 admin-state up
 description toCR1_x0/1/2
```

```
!
!
interface x-eth 0/0/11
 speed       10000
 admin-state up
 description to_BSC_CE3096
!
interface x-eth 0/0/11.103
 description  to_BSC_CE3097_VPN3G
 ipv4-address 10.0.21.1/30
 vrf          3G
 policy qos in-port-classification Policy1-UNI-IN-Pr
 policy qos out-port-pcp-marking Policy4-UNI-OUT-Pr
 vlan-id      103
!

!
interface loopback 0
 ipv4-address 1.1.1.1/32
!
interface loopback 100
 ipv4-address 100.1.1.96/32
 vrf          a1
!
interface agg-eth 1
 l2-transport enable
 admin-state  up
!
mpls ldp default
 explicit-null enable
 local-address ipv4 2.2.2.2
 router-id     2.2.2.2
 interface x-eth 0/1/2.20
  af-ipv4
 !
 label-allocation policy LDP_LABEL_HOST
!
l2-services
 pw-profile NEXTLINK
  type raw
  mtu  1580
 !
 vpws vpws5196
  neighbor 51.51.51.51 pw-id 5196
  profile NEXTLINK
```

```
 !
 vpws vpws8896
  neighbor 88.88.88.88 pw-id 8896
  profile NEXTLINK
 !
 vpws vpws9496
  neighbor 94.94.94.94 pw-id 9496
  profile NEXTLINK
 !
 vpls VPLS2
  ve-id 8894
  interface x-eth 0/0/27
  !
  vpws vpws5196
  !
 !
!
system
 hostname 3096RSG1
!
routing static
 vrf default
  af-ipv4 unicast
   route 6.7.0.0/16 interface x-eth 0/0/21 distance 15 tag 2 description QQQ
  !
 !
!
routing ospf 1
 vrf default
  mpls-te             enable
  router-id           2.2.2.2
  fast-reroute        enable
  ldp-synchronization enable
  area 0.0.0.1
   interface x-eth 0/1/2.20
    network-type point-to-point
    mtu          1500
   !
   interface loopback 0
    passive enable
   !
  !
 !
!
routing bgp 65000
```

```
router-id 2.2.2.2
vrf 3G
 af-ipv4 unicast
  redistribute connected
  export-rt 65000:3
  import-rt 65000:3
 !
!
vrf 4G
 af-ipv4 unicast
  redistribute connected
  export-rt 900:104
  import-rt 900:104
 !
!
vrf 5G
 af-ipv4 unicast
  redistribute connected
  export-rt 900:105
  import-rt 900:105
 !
!
vrf a1
 af-ipv4 unicast
  redistribute connected
  export-rt 1:1
  import-rt 1:1
 !
!
vrf default
 af-ipv4 unicast
  network 2.2.2.2/32
 !
 neighbor 11.11.11.11
  local-address loopback 0
  !
  remote-as-number 65000
  af-ipv4 unicast
   route-reflector-client enable
   next-hop-self          enable
   send-community         all
  !
  af-ipv4 vpn
   route-reflector-client enable
   send-community         all
```

```
   !
   af-ipv4 labeled-unicast
   !
  !
 !
  neighbor 12.12.12.12
   local-address loopback 0
   !
   remote-as-number 65000
   af-ipv4 unicast
    route-reflector-client enable
    next-hop-self          enable
    send-community         all
   !
   af-ipv4 vpn
    route-reflector-client enable
    send-community         all
   !
   af-ipv4 labeled-unicast
   !
!
aaa user admin
 password $1$U4$uyksWEZhyup0h5Jj5126H0
 role super_admin
!
aaa user private
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role super_admin
!
aaa user public
 password $1$kijc$dKzH4A8ID1SApxXcT2O1o1
 role snmp
!
aaa role priv_admin
 privilege all
 exception 1
  command os-shell
  action  reject
 !
!
aaa role snmp
 privilege all
 exception 1
  command os-shell
  action  reject
```

```
 !
!
aaa role super_admin
 privilege all
!
log output file syslog
 filter facility any
  severity 4-warning
 !
 filter facility kernel
  severity none
 !
 filter facility infra
  severity 5-notice
 !
 filter facility infra-utils
  severity none
 !
!
mib2
 location "Exaware Labs"
 name     Exaros
!
telnet-server disable
!end-of-config
```