Securing the Mobile Backhaul Infrastructure

Building an LTE Mobile Backhaul Network with the MX Series Integrated Security Gateway

Design Guide

December 2016
Version 1.0

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

The document may contain information relating to Juniper Networks' development plans and plans for future products, features or enhancements ("SOPD"). SOPD information is subject to change at any time, without notice. Except as may be set forth in definitive agreements for the potential transaction, Juniper Networks provides no assurances, and assumes no responsibility, that such future products, features or enhancements will be introduced.

The information in this document is current as of the date on the title page.

Contents

Purpose

The document explains the architecture solution and design used to add the mobile security gateway function to the mobile backhaul (MBH) network. The solution for the secured MBH infrastructure is based on two main components:

- End-to-end seamless Multiprotocol Label Switching (MPLS) network infrastructure used to enable flexibility at service layer; and
- Juniper Networks MX Series router capabilities used as an IPsec gateway located directly on top of the MBH infrastructure.

This design guide defines multiple deployment scenarios, and proposes a different high-level design for each scenario.

Overview

To take advantage of the benefits that a scalable, cost-effective IP or IP/MPLS backhaul network can provide, mobile service providers are moving to an all IP-based MBH network. Migrating a mobile network to an all IP-based MBH network leads to a new set of security challenges.

Generally, all IP networks expose the core network to IP-based threats, attacks, and exploitations. The Long Term Evolution (LTE) standards body, Third-Generation Partnership Project (3GPP), has recommended various guidelines for LTE security—particularly for S1/X2 interface, which is between the eNodeB and the serving gateway [SGW]). Managed services providers should consider these guidelines when planning their LTE network deployment. The most vulnerable location of the MBH network is the cell site, where the eNodeB interconnects to MBH network. This opens the network to exposure for the man in the middle (MitM) attack.

Contrary to the relatively protected MBH network sites such as the pre-aggregation, aggregation, and core segments, potential attackers can easily compromise the physical security of the cell site. This threat becomes more significant as the operator starts to deploy even less protected small-cell sites. To preserve data integrity and prevent MitM attack, vendors of the LTE cell towers started to implement IPsec functionality within its eNodeBs. This enables the eNodeB to send its traffic through an encrypted IPsec tunnel. Traditionally, mobile operators needed to deploy a dedicated IPsec concentrator—Mobile SecGW—to terminate those tunnels, with the SecGW usually located somewhere close to the evolved packet core (EPC). Thus, eNodeB can authenticate itself in the network using an X.509 certificate, and securely deliver traffic to EPC. In most deployment scenarios using the modern 4G LTE network, this solution provides an acceptable level of performance and latency to serve both S1 and X2 traffic.

This solution addresses security problems of the modern 4G LTE Small Cell, Macro Cell, and HetNet networks by introducing a router integrated security gateway on the Juniper Networks MX Series platform in the MBH networks. It shows how to enable security features on top of the end-to- end MBH infrastructure which is built on Juniper Networks routing platforms, such as the MX Series and ACX Series. This solution classifies different deployment scenarios and provides a systematic approach of how to protect elements of the LTE mobile network and provide consistency for the data (S1 and X2 traffic) traversing through the MBH infrastructure.

The solution for the secured MBH addresses the following challenges and security threats:

- Unauthorized access to the network elements of the MBH infrastructure
- Protection against LTE signaling storms towards mobility management entity (MME)
- Data eavesdropping
- Compromising of data integrity transported over the MBH network (using own infrastructure or leased lines from third-party provider) by enabling the IPsec gateway function.
- MitM attacks
- Attacks against elements of the MBH infrastructure itself

To better understand the MX Series router capability, this guide describes the MX platform internal architecture with regards to the IPsec function, and provides an overview of the future direction for development and enhancements in this area.

Audience

This document is targeted for the following audience:

- Networking and Software Engineers–provide a perspective of cross-platform feature dependencies necessary to deliver services over an end-to-end solution, as well as, contribute to future platform development releases to meet these needs.
- Documentation Developers–provide an understanding of how the products involved are designed and implemented as an end-to-end solution.
- Field/Sales Engineers–provide a perspective of the support and deployability aspects of the proposed solution.

Value Proposition

Between 2011-2013, the market for the access and aggregation networks, and metro-area networks was disrupted because many operators started the migration to the packet-based access networks with 4G LTE mobile networks as the main driver. To adapt to the market changes, Juniper Networks introduced a new product that provided an integrated end-to-end solution for the universal access and aggregation network. It is based on a seamless MPLS architecture and supported on a broad range of routing platforms portfolio, including: MX80, MX104, MX240, MX480, MX960, MX2020 Series and ACX Series, based on the single Junos OS operating system. Service Providers can benefit from both network architecture and platform capabilities, by flexibly moving different intelligent functions, such as mobile security gateway, into the MBH network.

The solution adds value to the existing MX Series based access and aggregation network. The existing network is represented by end-to-end access and aggregation network segments built with a mix of Juniper Networks MX Series routers in the aggregation, or service edge, or both segments. In all these situations, operators can benefit by enabling security features (all or just portion of them) on the Juniper Networks routers comprising the network. This enables the protection of the S1/X2 traffic between the eNodeBs and evolved packet core (EPC), and also protects the MBH infrastructure elements.

The value proposition for this solution includes the following:

- Router integrated IPsec Security Gateway (SecGW)
  - Distributed SecGW in the pre-aggregation segment using the MX104 router
  - Centralized SecGW in the aggregation or core segment using an MX240/MX480/MX960 router
- Stream Control Transmission Protocol (SCTP) traffic rate limiting for X2 and S1 interface in distributed or centralized location
- Optimized forwarding path for the X2 traffic with reduced latency
- Protection of the routing nodes control plane from Distributed Denial of Service (DDoS) attack
- Proven integration with existing routing and switching infrastructure of the MBH network
- Reduced OPEX costs resulting from less rack mount space, power, and cooling
- High scalability with distributed architecture
- Hardened hardware to deploy the router integrated SecGW at cell site locations
- Unified management for network and security services across the MBH network

This solution provides operators the freedom deploy security in their network. Operators can use centralized, distributed security architecture, or a combination of both, depending on the network’s current and future needs. This solution focuses on the Small cell and HetNet backhaul networks.

Inter-Solution Interfaces

The solution for the secured MBH infrastructure remains separate from the mobile SecGW solution based on the SRX Series platform. However, some of the security functions defined in both solutions are the same, but the addressable market and positioning are different. There are use cases where both solutions may supplement each other. For example, the SRX Series platform has a more comprehensive portfolio for security features, which may be critical to the evolved packet core (EPC) network or Mobile Packet Backbone Network (MPBN). The service provider may also benefit by placing the router with integrated security into the pre-aggregation segment of the MBH network to protect LTE X2 traffic, and prevent its hair-pinning to the central location.

Chapter 1 - Secured Mobile Backhaul Use Case

The market segment described in this use case is the solution for mobile operators (MO) of the 4G LTE network who own their MBH infrastructure or lease lines to backhaul traffic between its radio access network and mobile core.

Service Architecture for Mobile Operators Who Own the Mobile Backhaul Infrastructure

Figure 1 shows possible scenarios of when a mobile operator owns the MBH infrastructure and it is deployed for a 4G LTE network. Scenarios differ by evolved packet core (EPC) location in the network. There are two possible locations for LTE EPC in the network:

- National point of presence (POP)
- Regional POP

National POP is located within the operator's National IP/MPLS network. LTE EPC is placed in the network to serve multiple regional networks.

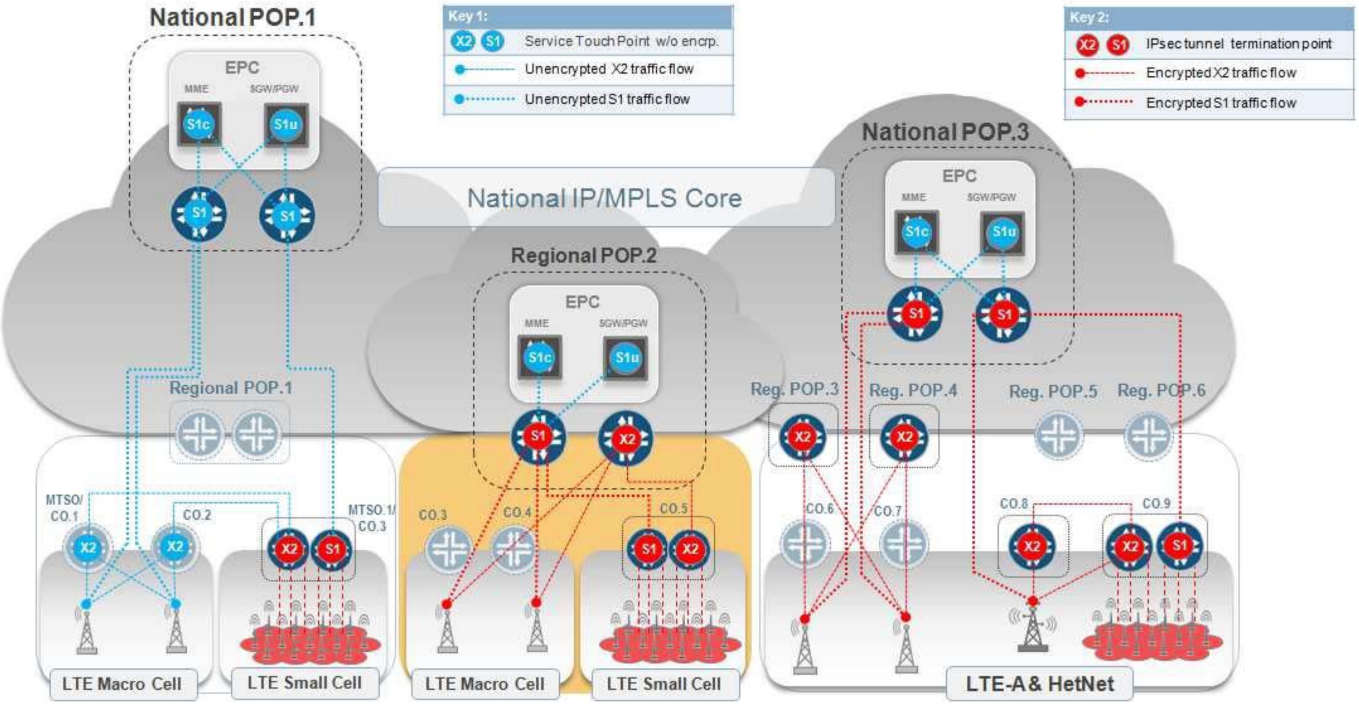


Figure 1 – Use Cases for the MBH with Enabled Security Functionality (own infrastructure)

The distance between the Regional POP and the actual location of the eNodeB varies depending on operator, country, and geography. The distance can range anywhere from 400 to 500 kilometers to a few thousands kilometers. Regional POP is the part of the particular metro-network. Within this use case, we assume that the distance between the Regional POP and eNodeB is less than 400 to 500 kilometers.

In all use cases, eNodeB (which requires protection) starts an IPsec tunnel that terminates at a place located in the mobile operator's network. The location of the terminating point of the IPsec tunnel depends on the type of mobile traffic, and on requirements for mobile traffic encryption established by the mobile operator's internal procedures or local legislation rules.

As mentioned previously, the most vulnerable point in the network is where the eNodeB connects to the MBH network. Protecting this point is the primary goal of enabling security functionality in a MBH network. You can achieve this goal by just adding encryption in the particular network segment. In some situations, the mobile operator's requirements are even stronger and may lead to full end-to-end encryption of traffic for both X2 interface (X2c and X2-AP) and S1 interface (S1-c and S1-u). The maximum allowed value of latency (for X2 traffic delivery between two eNodeBs) determines the location of the SecGW by using the network closer to the access network segment. Juniper Networks recommends that you set latency, for packet forwarding between the eNodeBs for the X2 interface, within 10ms for LTE network, and approximately 5ms for LTE-A (as per NGMN Optimized Backhaul Requirements: *http://www.ngmn.org/uploads/media/NGMN_Optimised_Backhaul_Requirements.pdf*).

An optimal location for the termination point of tunnels, which carry X2 and S1, is different. Use cases depicted in Figure 1 leads to a number of possible locations for the IPsec tunnel termination points within the MBH network (shown as red circles for X2 and S1 traffic flows). Red-dashed and red dotted-lines represent the IPsec traffic flows for X2 and S1 interfaces, respectively. Both red and blue lines represent the traffic flows; not the physical connections.

The deployment scenarios for the IPsec function within the MBH infrastructure are:

- LTE macro cell:
  - Without encryption, with SCTP policing only: CO.1, CO.2, and National POP.1
  - With encryption of S1 and X2 at the aggregation node: Regional POP.2.
  - With encryption of S1 at core segment node: POP.3.
  - With encryption of X2 at pre-aggregation node: CO.8 and CO.9.
- LTE small cell:
  - With encryption of S1 and X2 in access and pre-aggregation segment without end-to- end encryption between small cell and eNodeB: CO.3
  - With full end-to-end encryption of S1 between small cell and EPC, and X2 between any two small or macro eNodeB: CO.8 and CO.9

This secured MBH network use case reuses the network architecture and design principles defined in the *Universal Access and Aggregation Mobile Backhaul Design Guide* (*http://www.juniper.net/us/en/local/pdf/design-guides/8020018-en.pdf*), in particular:

- Topologies
- IP and MPLS transport
- MPLS service layers
- Timing and synchronization
- CoS

Because of the decoupling of transport and service levels in this use case, only some aspects of the MPLS service configuration is described when it relates to the integrated security functionality (IPsec and Firewall filtering) in the MBH infrastructure.

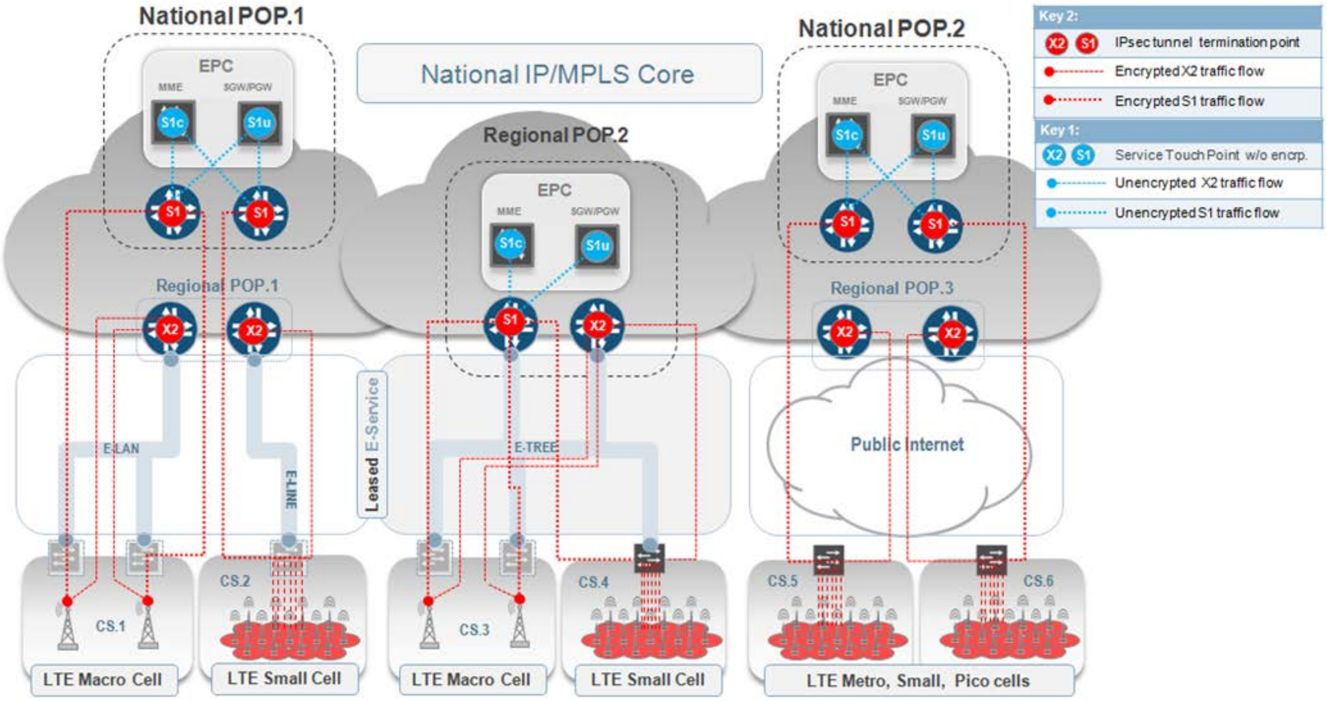
Service Architecture for Wholesale Models

A wholesale MBH network use case example is when the mobile operator (MO) leases lines from a third-party MBH operator. Connectivity between small and macro eNodeBs and an EPC is provided by E-LINE, E-LAN, and E-TREE metro services, or through a public IP network. Figure 2 shows a wholesale MBH network with different options to enable mobile SecGW functionality.

As in Figure 1, eNodeBs originate IPsec tunnels that terminate in the mobile provider network.

In most cases, the cell site router is unaware of IPsec encryption and transparently switches it as regular IP packets. You can also use these tunnels to provide data encryption and integrity for the OAM, and management traffic between the MBH network elements that sit behind the CSR and MO management system. To secure management of the CSR routers, a mobile operator may also decide to establish additional IPsec tunnels from the cell site router.

Note: The case of enabling IPsec functionality at the access node is out of scope of this document.



Key 2:	
X2 S1	IPsec tunnel termination point
●--------	Encrypted X2 traffic flow
●········	Encrypted S1 traffic flow
Key 1:	
X2 S1	Service Touch Point w/o encrp.
●--------	Unencrypted X2 traffic flow
●········	Unencrypted S1 traffic flow

Figure 2 – Enabling IPsec Functionality on top of the Wholesale MBH Network

The deployment scenarios for IPsec functionality for the leased backhaul services use case are:

- Macro eNodeB:
  - With termination of IPsec tunnels for S1 and X2 traffic at the aggregation node connected to leased line services (E-LINE, E-LAN, and E-TREE): Regional POP.2
  - With termination of IPsec tunnels for S1 at PE routers of the core segment: National POP.1 and National POP.3
  - With termination of IPsec tunnels for X2 at the pre-aggregation node connected to leased line services (E-LINE, E-LAN, E-TREE): Regional POP.1
- Small cell eNodeB:
  - With termination of IPsec tunnels for S1 and X2 traffic at the aggregation node connected to leased line services (E-LINE, E-LAN, and E-TREE): Regional POP.2.
  - With termination of IPsec tunnels for S1 at PE routers of the core segment: National POP.1 and National POP.3
  - With termination of IPsec tunnels for X2 at pre-aggregation node connected to leased line services (E-LINE, E-LAN, and E-TREE): Regional POP.1
  - With termination of IPsec tunnels for X2 at pre-aggregation node connected to public IP networks: Regional POP.3

Note: Use cases that lease MBH services from a third-party MAN operator include a number of deployment scenarios which are out of scope of this document.

Chapter 2 - Solution Overview

End-to-End Solution Architecture

To secure mobile network and MBH infrastructure, mobile operators typically needed to deploy a dedicated IPsec concentrator, such as Mobile SecGW, to terminate IPsec tunnels originated at eNodeB. The SecGW is usually placed close to the evolved packet core enabling eNodeB to authenticate itself in the network using X.509 certification; thereby able to deliver traffic securely to the evolved packet core.

The secured MBH infrastructure solution enables maximum flexibility to deploy the SecGW in any part of the transport network using any MX Series platform with add-on IPsec and SCTP firewall functionality. This solution can also solve X2 hair-pinning problems, and handle more stringent requirements for latency that are upcoming in future LTE-A, small cell, and heterogeneous networks. To summarize this proposed solution– encrypt what you need, where you need to, and when you need it.

Figure 3 shows an MBH network with security functions enabled by adding multiservice service cards into an MX Series chassis. You can activate the IPsec GW function or SCTP firewall functionality in any segment. The exact placement of the security features depends on many different factors. This solution describes a few of those use cases in more details.

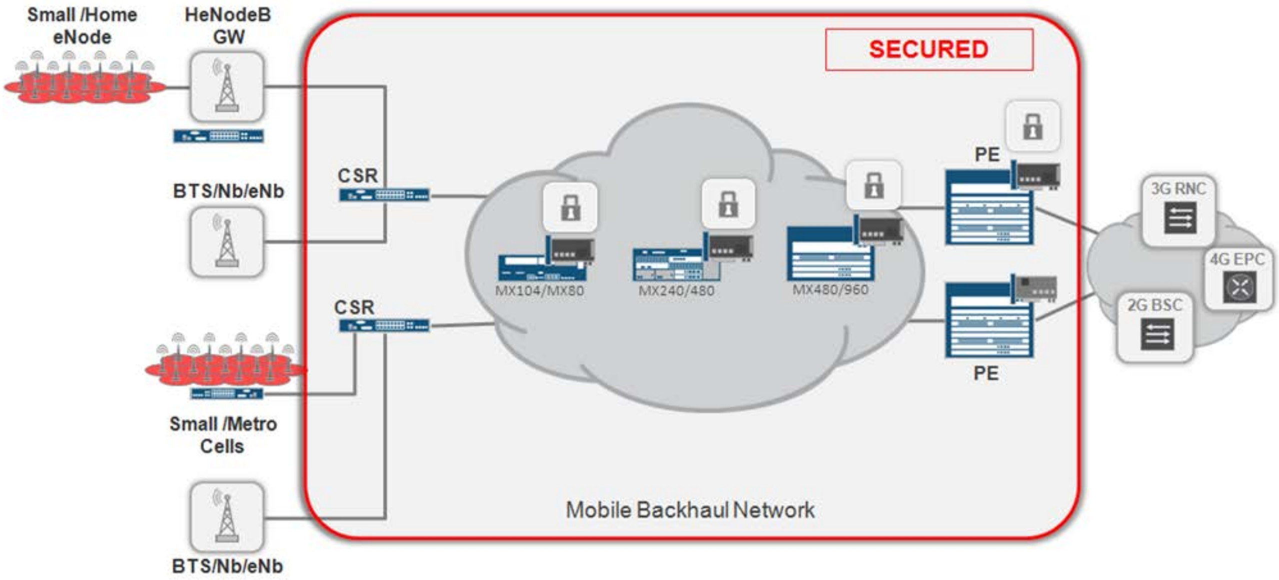


Figure 3 – Secured MBH Network Overview

You can add security functions in any place of the MBH infrastructure based on the following:

- **Solution components:** All MX Series routers are equipped with multiservice cards, such as MS-MIC or MS-DPC, and support the same Junos OS functionality.
- **MBH infrastructure**: Based on seamless MPLS architecture which allows you to seamlessly set any security service as part of the Layer 3 VPN at any place with very low operational costs, and without disrupting other network layers and network elements.

Solution Components

The main solution components are:

- MX Series routers: Including MX5, MX10, MX40, MX80, and MX104, with embedded multiservice module: MS-MIC-16G
- MX Series routers: Including MX240, MX480, MX960, MX2010, and MX2020 with embedded multiservice module: MS-MPC-128G
- The ACX Series routers are an integral part of the end-to-end Juniper Networks solution for MBH infrastructure in the access segment. The design and configuration of this element is similar to what is described in the Design Guide for the MBH Solution 1.0, with special notes added. However, the design for the security infrastructure does not explicitly leverage the ACX Series portfolio. You can use any types of access nodes with similar functionality.

Figure 4 shows the platform positioning across the secured MBH network.

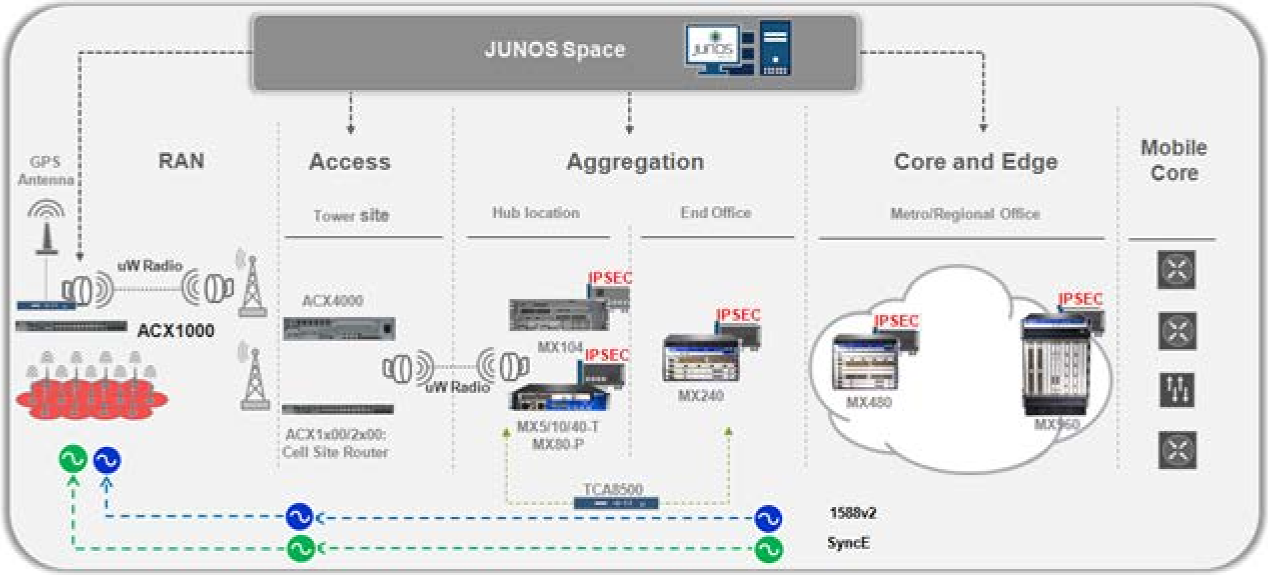


Figure 4 – Juniper Networks Platform Positioning

Table 1 – Juniper Networks Software and Hardware Solution Components

Architectural Role	Hardware	Software Version
Cell Site Router	ACX Series routers	Junos OS Release 12.3S4 or later
Pre-aggregation router (AG1)/Distributed Security GW	MX104/MX80 with MS-MIC-16G	Junos OS Release 14.1R1 or later
Aggregation router (AG2)/Distributed Security GW	MX240/MX480/MX960 with MS-MPC-128G	Junos OS Release 14.1R1 or later
Aggregation router (AG3)/Centralized Security GW	MX480/MX960/MX2010/MX2020 with MS-MPC-128G	Junos OS Release 14.1R1 or later

Seamless MPLS Architecture as the Base of an MBH Infrastructure

Seamless MPLS network architecture serves as a base for the MBH infrastructure solution. Seamless MPLS clearly defines network layers and network element functions for each layer. A seamless MPLS network (shown in Figure 5) forwards packets end-to-end, across multiple networks' segments [IGP areas or autonomous systems (AS)], based on MPLS labels only. This occurs from the time a packet enters the network, until it leaves the network at the next service node. Seamless MPLS introduces a systematic way of enabling MPLS end-to-end across all segments: access, pre-aggregation, aggregation, and core. In a seamless MPLS network, there are no boundaries, which enables very flexible models of service delivery, and a decoupling of network transport from the service layer.

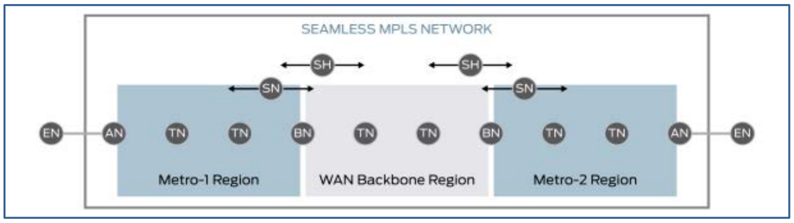


Figure 5 – Seamless MPLS Regions and Network Functions

The following six network functions are defined:

- Access nodes: terminate local loop from subscribers (such as DSLAM and MSAN)
- Transport nodes: represent packet transport within the region (such as Metro LSR and Core LSR)
- Border nodes: enable inter-region packet transport (such as ABR)
- Service nodes: are service delivery points, with flexible topological placement (such as IPVPN PE)
- Service helpers: are service enablement or control plane scale points (such as RADIUS and RR)
- End nodes: represent the network customer, located outside of service provider network

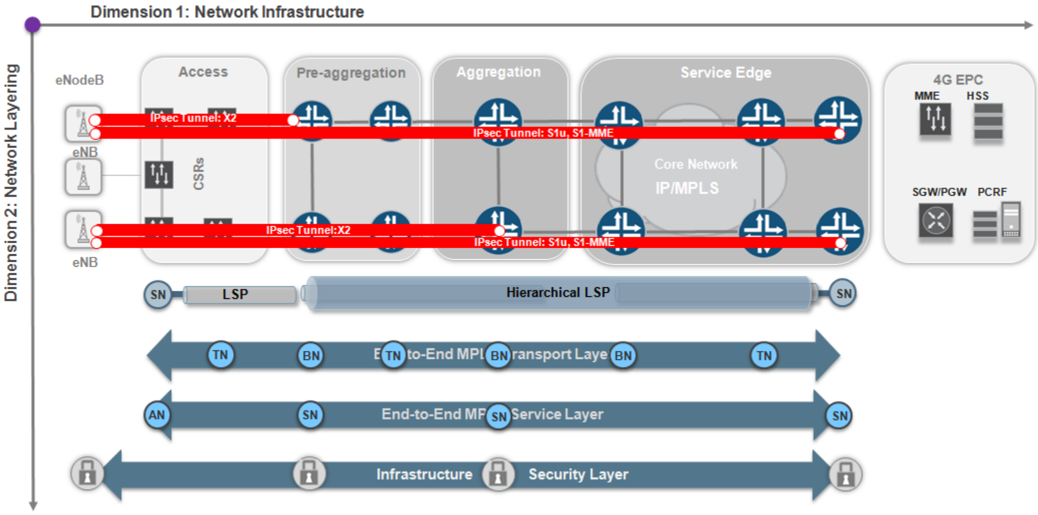
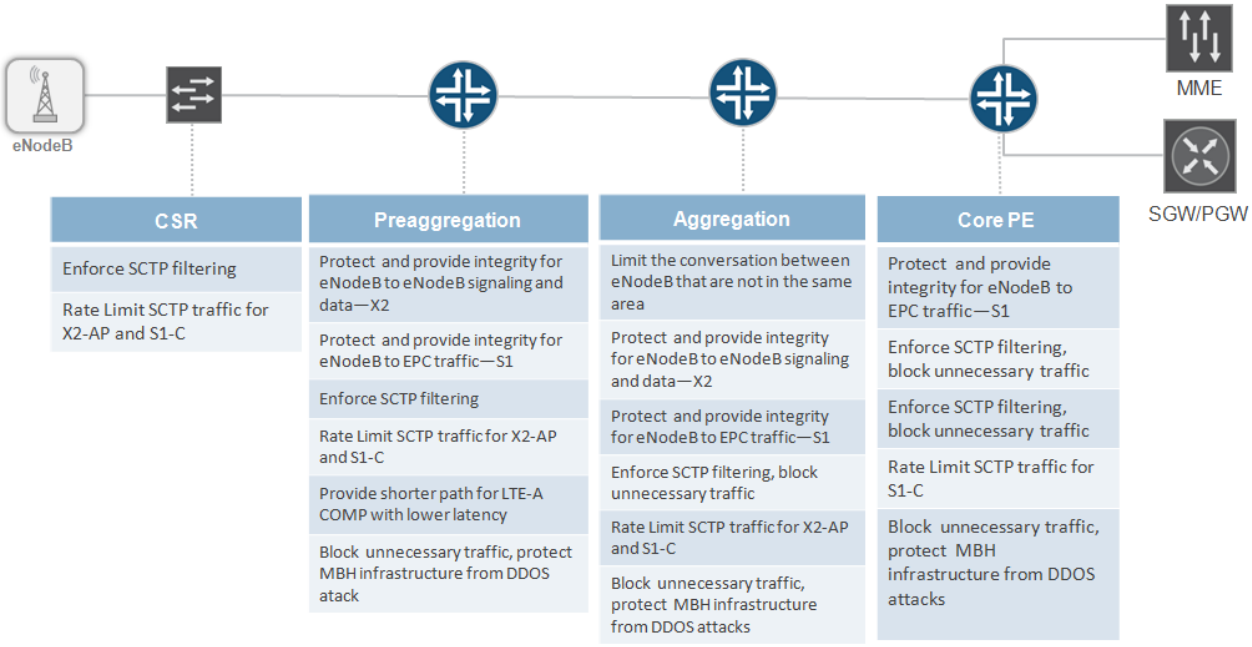


Figure 6 – Infrastructure Security Layer

Figure 6 shows the decoupling principle that enables you to flexibly place the security function within the MBH network. The security function is represented as a dedicated functional layer within the multilayered MBH architecture. Adding SecGW functionality at any node in the network requires adding a new service function, Layer 3 VRF/VPN at pre-aggregation or aggregation segment, and leaves the underlying transport layer unchanged. As soon as you create the Layer 3 VPN and map service interfaces of the embedded SecGW into VPN, it becomes accessible from any place in the network by any eNodeB.

Adding Security Functions on Top of the MBH Infrastructure

Within this solution, Juniper Networks provides recommendations for the design and configuration of the infrastructure security layer, and partially recommends Layer 3 VPN and Layer 2 VPN configuration, when it is required. In some cases, correct configuration of the network IP/MPLS transport and service layers helps assure an optimal service restoration time for encrypted data when the IPsec function fails, or when routing nodes host the IPsec function.



CSR	Preaggregation	Aggregation	Core PE
Enforce SCTP filtering	Protect and provide integrity for eNodeB to eNodeB signaling and data—X2	Limit the conversation between eNodeB that are not in the same area	Protect and provide integrity for eNodeB to EPC traffic—S1
Rate Limit SCTP traffic for X2-AP and S1-C	Protect and provide integrity for eNodeB to EPC traffic—S1	Protect and provide integrity for eNodeB to eNodeB signaling and data—X2	Enforce SCTP filtering, block unnecessary traffic
	Enforce SCTP filtering	Protect and provide integrity for eNodeB to EPC traffic—S1	Enforce SCTP filtering, block unnecessary traffic
	Rate Limit SCTP traffic for X2-AP and S1-C	Enforce SCTP filtering, block unnecessary traffic	Rate Limit SCTP traffic for S1-C
	Provide shorter path for LTE-A COMP with lower latency	Rate Limit SCTP traffic for X2-AP and S1-C	Block unnecessary traffic, protect MBH infrastructure from DDOS attacks
	Block unnecessary traffic, protect MBH infrastructure from DDOS atack	Block unnecessary traffic, protect MBH infrastructure from DDOS attacks	

Figure 7 – Infrastructure Security Layer Functions in the MBH Network

The overall solution for the secured MBH infrastructure includes additional features that you can enable on Juniper Networks routing platforms to protect mobile network and MBH infrastructure from security threats. Figure 7 shows the possible add-ons. Not all functions are enabled on all types of nodes, at the same time. The actual set of functions depends on various deployment factors. While the main focus of this design guide is to describe the router integrated IPsec function, it also provides recommendations for the following: SCTP traffic filtering and policing, protection against spoofing, and DDoS protection of the routing nodes control and management planes.

Chapter 3 - Design Considerations

Mobile SecGW Design Options

Several use cases have been described in this document that differ by type of the MBH network infrastructure and location of the SecGW function. A few more security-related functions are added to the overall solution. Table 2 shows the complete set of the design consideration which one should have in mind when planning Mobile SecGW deployment on top of its MBH infrastructure.

Table 2 – Design Options for Router Integrated Mobile SecGW

IPsec	SecGW Location	MBH Infrastructure	eNodeB HA	SecGW HA
Authentication profile	Distributed	End-to-end L3 VPN	Single IPsec tunnel with DPD	IPsec tunnel with DPD and multihop BFD
Encryption profile	Semi-distributed	L2 VPN to L3 VPN termination	Dual IPsec tunnel with DPD	Junos OS opt scripts
Dynamic or manual end-point provisioning	Centralized	Wholesale MBH	Dual IPsec tunnel with BFD	Intrachassis and Interchassis HA

MBH Infrastructure Introduction

The MBH network design guide provides and classifies a systematic description of most valuable deployment scenarios of the MBH network infrastructure owned by mobile operators. The following scenarios continue to leverage this classification by selecting the ones most suitable by adding security features inside the routing nodes.

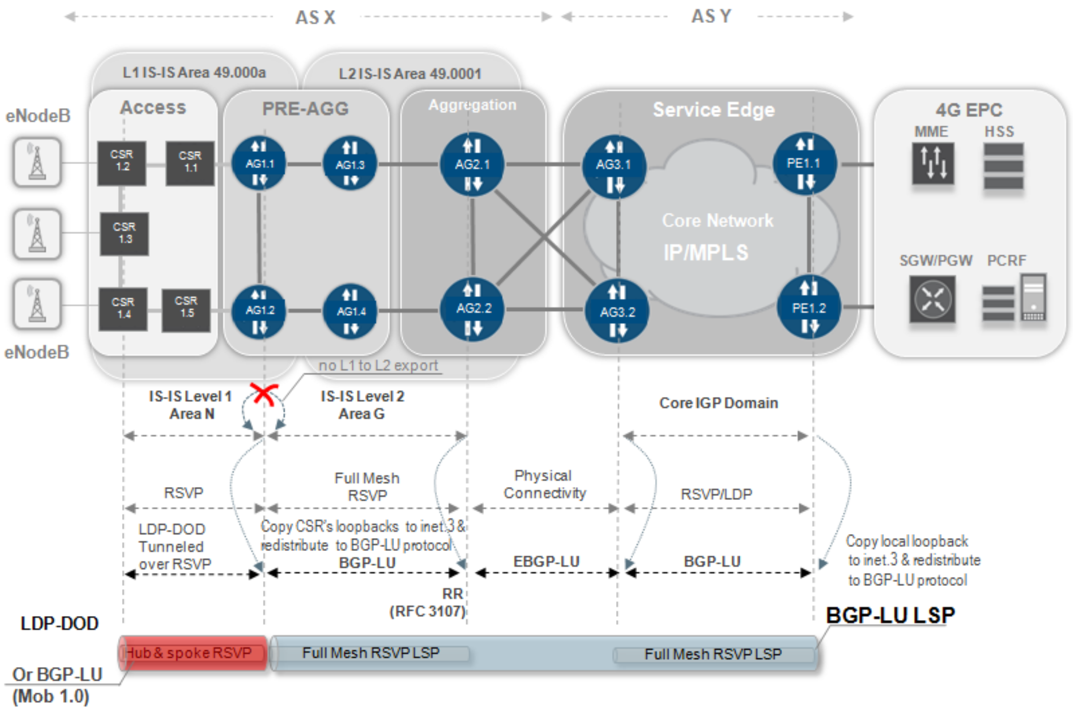


Figure 8 – MBH Network Segments, Topology, and MPLS Transport

By decoupling the service and transport layers, the exact topology of the MBH infrastructure is not important for this example. Figure 8 shows the MBH regions and the underlying IP and MPLS end-to-end transport design.

The MPLS service layer architecture of the MBH network influences the decision about optimal placement of the SecGW function. In some cases, it may also provide the solution for resiliency at the security infrastructure layer. The MPLS service layer architecture is described by the service profile. The service profile defines the following:

- UNI parameters to interconnect cell site router (CSR) and cell tower.
- Traffic delivery method in the access segment of the MBH network.
- Service type to deliver traffic within the aggregation and metro core network segment.
- Seamless service stitching between the access and aggregation segments.

The following four service profiles, or service architectures, defined in the MBH design guide address the needs of the backhaul network for any-G (2G, 3G, HSPA, and 4G LTE) mobile network:

- End to end L3 VPN
- Layer 2 Pseudowire to Layer 3 VPN termination
- Layer 2 Pseudowire to VPLS termination (H-VPLS)
- End-to-end Layer 2 circuit (E-LINE, TDM, and ATM)

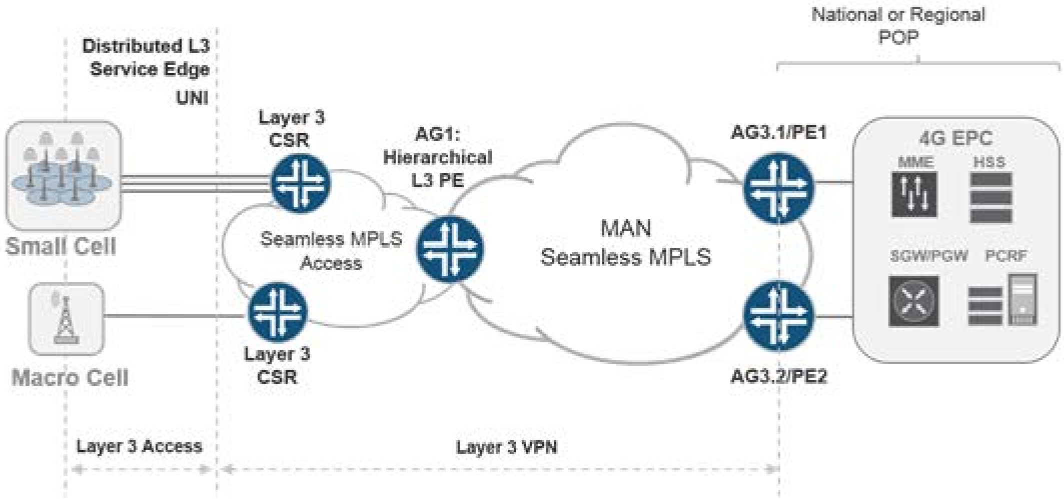


Figure 9 – 4G LTE MBH Service Architecture for End-to-End Layer 3 VPN

The first three architectures are used to backhaul LTE traffic. However, you can enable the IPsec function on the MX Series router only in the context of the Layer 3 routing instance. Only two out of the four service architectures fit this requirement and are considered as feasible foundations for the mobile operator's secured infrastructure within the solution (shown in Figure 9 and Figure 10, respectively). The MBH infrastructure provides a reliable traffic delivery between eNodeB and the evolved packet core. In this use case, the MBH network also provides an IP level connectivity between the eNodeB and SecGW. The underlying MPLS network infrastructure also provides resiliency against any link or node failure between eNodeB and SecGW. To enable resiliency against an SecGW failure, eNodeB can select one of two IPsec GWs used to establish a secured connection.

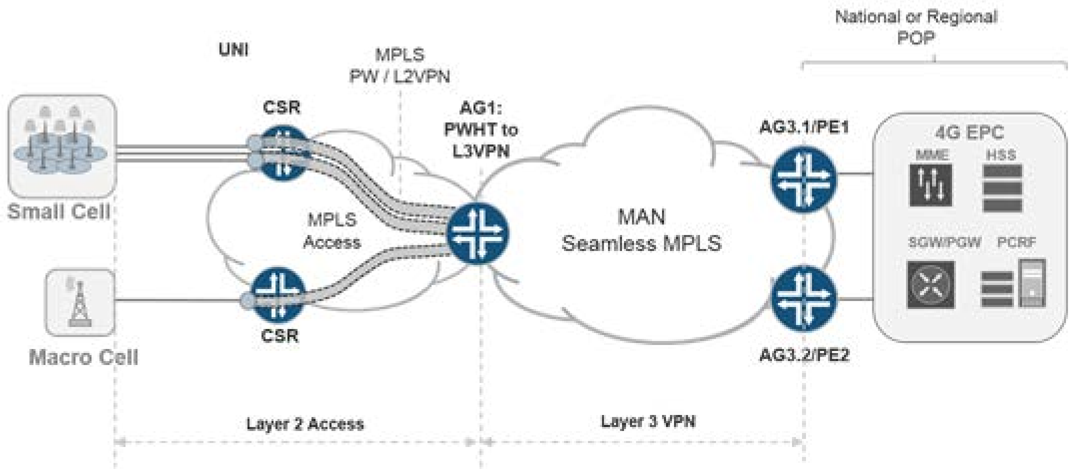


Figure 10 – 4G LTE MBH Service Architecture for Layer 2 PW to Layer 3 VPN Termination

You can use different methods to provide an IPsec tunnel switchover in the event of an active gateway failure (described later in this document).

MBH Wholesale Infrastructure

Metro Ethernet Ethernet Virtual Circuit (EVC) (including E-LINE, E-LAN, or E-TREE) provides connectivity when each cell site router (CSR) is dual-homed to a pair of mobile operator's provider edge (PE) routers. The CSR and PE router (which host the IPsec gateway functions) are considered part of the end-to-end network infrastructure. Three models are used to describe the majority of the wholesale MBH scenarios. All of the following three models assume a sort of redundancy provided at the mobile operator's aggregation or PE routers:

- Redundant pair of E-Line EVC between the CSR and PE
- Single E-Line with dual-homed PE router and multichassis redundancy
- E-LAN EVC with dual-homed PE routers to the MAN (see Figure 11).

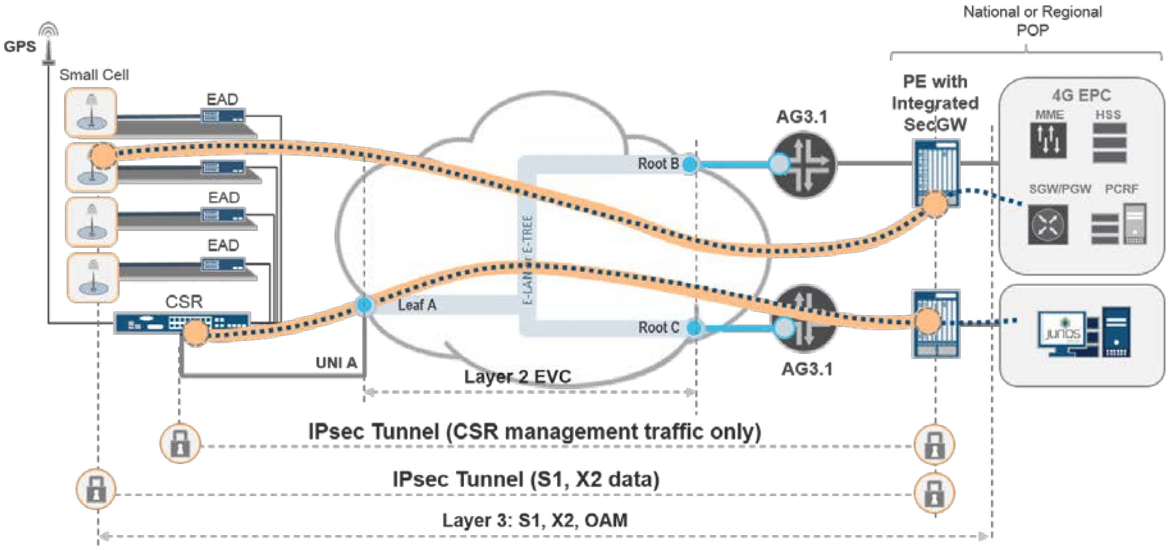


Figure 11 – Wholesale MBH Deployment Scenario with Centralized SecGW

Mobile SecGW Location

Different use cases, such as Macro eNodeB, small cell, and HetNet, have different requirements regarding the optimal location of the Mobile SecGW function in the network. The following three locations for the MBH infrastructure are described:

- Distributed SecGW hosted at the AG1 routing node
- Semi-distributed SecGW hosted at the AG2 routing node
- Centralized SecGW hosted at the AG3 or PE routing nodes

High Availability Capabilities of eNodeB

Typically, there are two IPsec gateways, one active one backup, in the network. They provide resiliency against the mobile SecGW failure. In normal conditions, all traffic flows go through the primary IPsec tunnel to the primary IPsec gateway. In case of the primary gateway failure, the eNodeB should be able to switchover traffic to the secondary gateway. The type of eNodeB is differentiated based on its ability to establish an IPsec tunnel to multiple IPsec gateways:

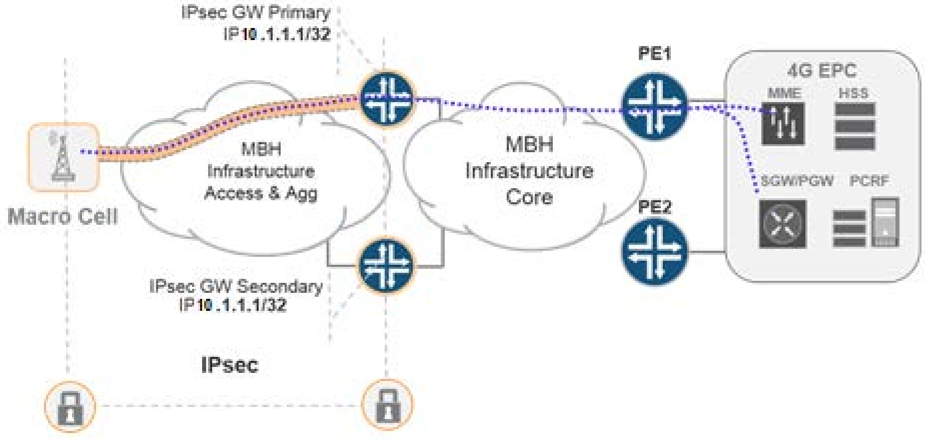


Figure 12 – Single Tunnel Mode

- eNodeB can be configured with a single IP address of the remote SecGW, and can establish a single IPsec tunnel at a time (see Figure 12).
- eNodeB can be configured with two or more IP addresses of the remote SecGW, but can establish one tunnel at a time to only one of two configured gateways (see Figure 13). The DPD mechanism detects an active tunnel failure. As soon as an active tunnel failure is detected, eNodeB initiates a new tunnel to back up the IPsec gateway.
- eNodeB can be configured with two or more IP addresses of the remote SecGW, and can establish two IPsec tunnels at the same time (see Figure 14). Traffic forwarding is arranged in active/active or active/standby mode. Multihop BFD detects one of the forwarding path failures on both sides, eNodeB and IPsec GW. BFD keepalive packets follow the same forwarding path as the data packets, through the IPsec tunnels.

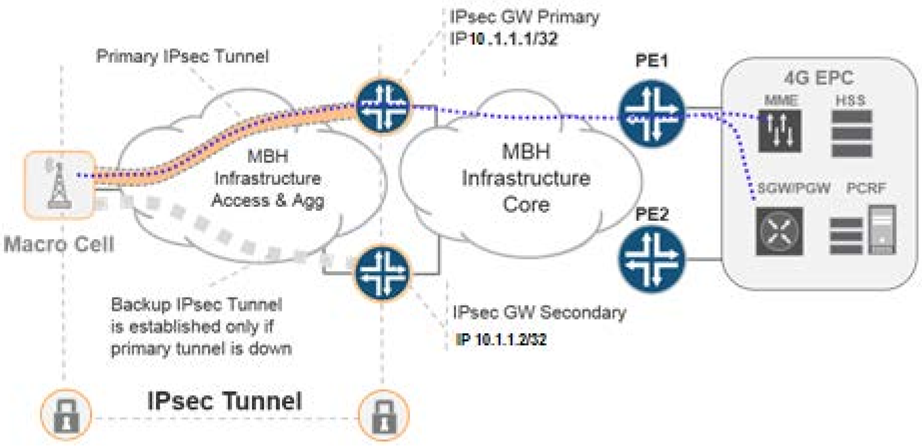


Figure 13 – eNodeB Dual Tunnel Model with PDP

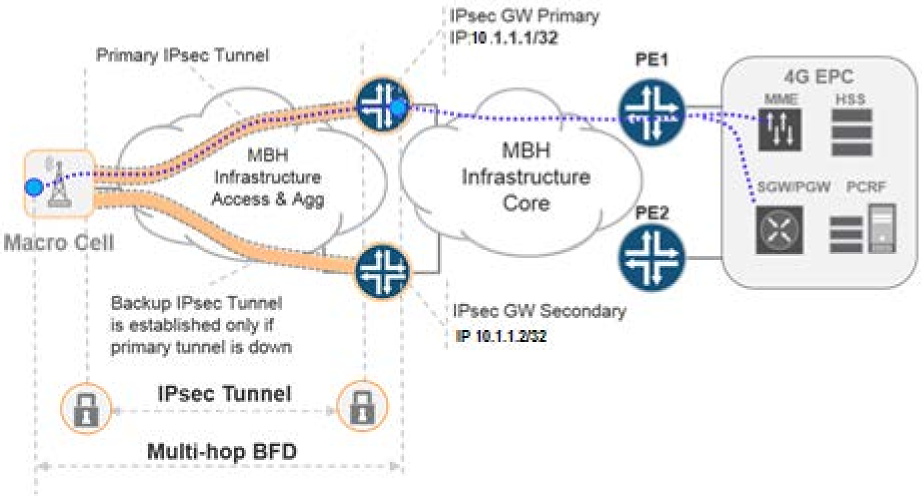


Figure 14 – eNodeB Dual Tunnel Model with PDP with Multihop BFD

SecGW Stateful High Availability Options

With the Junos OS 14.1R1 Release, processes that participate in the IPsec security association (SA) establishment (IPsec control plane), and traffic encrypting/decrypting (IPsec data plane), are distributed among the Routing Engine and a service network processing unit (NPU), respectively. For more details about the MX SecGW hardware architecture, see *Appendix C – MX Series IPsec GW Architecture*.

Intra-chassis high availability (HA) features provide a single system resiliency against the Routing Engine or NPU failure. When failure occurs in any of the described components, it also leads to failure of the IPsec SA associated with the particular HW components. In an MX Series router (except for the MX80) with a redundant pair of Routing Engines, the IPsec control plane HA function is processed by the non-stop routing (NSR) feature. Failure of an active Routing Engine does not lead to an IPsec tunnel reestablishment, or to any traffic loss within the existing IPsec tunnels.

A similar level of HA exists with NPU failure. You can configure each NPU with a redundant processing unit, where both units keep the same forwarding states for the IPsec tunnel. So, if any one of two NPU fails, traffic flow is not affected for the existing tunnels. The existing infrastructure with aggregated multiservice (AMS) interface (available with the Junos OS 14.2R1 release) is used for services, such as NAT and firewall.

Note: A stateful inter-chassis IPsec HA is more complex and not supported natively between two MX Series routers. In the current solution, eNodeB is responsible for the tunnel switchover between two SecGWs.

Deployment Scenarios Inventory

Table 3 summarizes the deployment scenarios considered within the solution. Deployment scenarios of the IPsec gateway for X2 and S1 LTE data are independent. For example, you can combine Scenario 1.1 (distributed SecGW) for X2 traffic with the scenario for semi-distributed SecGW location for S1 traffic. You can also combine different design options for HA within the scenarios.

Table 3 – Inventory of the Router Integrated SecGW Deployment Scenarios

Service/ Scenario #	IPsec GW Location		IPsec Auth, Encryption			MBH Infra profile	SCTP Policing	IPsec Tunnel Switchover provided by		
								eNodeB Dual Tunnel		SecGW Stateful HA
	S1	X2	PSK	PKI Cert	Encrypt.			DPD	BFD	Intra Chas.
Scenario 1.1	AG1	AG1	YES	YES[1]	ANY[2]	L3VPN	YES	YES	YES	Junos OS 16.1R3
Scenario 1.2	AG1	AG1	YES	YES[1]	ANY[2]	PWHT	YES	YES	YES	Junos OS 16.1R3
Scenario 1.3	AG1	AG1	YES	YES[1]	ANY[2]	Both[3]	YES	YES	YES	Junos OS 16.1R3
Scenario 2	AG2	AG2	YES	YES[1]	ANY[2]	Both[3]	YES	YES	YES	Junos OS 16.1R3
Scenario 3	AG2	AG2	YES	YES[1]	ANY[2]	Both[3]	YES	YES	YES	Junos OS 16.1R3
Scenario 4	AG3	AG3	YES	YES[1]	ANY[2]	Both[3]	YES	YES	YES	Junos OS 16.1R3
Scenario 5	AG2	AG2	YES	YES[1]	ANY[2]	E-LAN[4]	YES	YES	YES	Junos OS 16.1R3
Scenario 6	AG2	AG2	YES	YES[1]	ANY[2]	E-LINE[4]	YES	YES	YES	Junos OS 16.1R3
Scenario 7	AG2	AG2	YES	YES[1]	ANY[2]	E-LINE[4]	YES	YES	YES	Junos OS 16.1R3
Scenario 8	AG3	AG3	YES	YES[1]	ANY[2]	E-LAN[4]	YES	YES	YES	Junos OS 16.1R3
Scenario 9	AG3	AG3	YES	YES[1]	ANY[2]	E-LINE[4]	YES	YES	YES	Junos OS 16.1R3
Scenario 10	AG3	AG3	YES	YES[1]	ANY[2]	E-LINE[4]	YES	YES	YES	Junos OS 16.1R3

Notes:

- Authentication mode which relates to the IPsec gateway interacting with Public Key Infrastructure (PKI).
- Term "ANY" relates to any type of the authentication algorithm listed in the Supported Standards and Features section of this document.
- Term "Both" stands for two types of MBH network profiles: End-to-End Layer 3 VPN and Layer 2 Pseudowire Termination into Layer 3 VPN. For more details, see http://www.juniper.net/us/en/local/pdf/design-guides/8020018-en.pdf).
- E-LAN/E-LINE terms used in the network architecture of the wholesale MBH model.

Each deployment scenario considers the following:

- Redundancy and HA
- Setting up IPsec tunnel
- Filter-based forwarding and policing

Within the solution, the design leverages the IGP, BGP, and MPLS protocols recommended within the MBH1.0 Solution (for details, see http://www.juniper.net/us/en/local/pdf/design-guides/8020018-en.pdf).

Table 4 summarizes the list of additional security services and features that you can enable in the MBH network for additional protection of the network elements.

Table 4 – Add-on Security Services to Protect Mobile Backhaul Infrastructure

Security Service	CSR	AG1	AG2	AG3	PE
Protection Against Unauthorized Access	YES	YES	YES	YES	YES
Protection Against Hijacking Threats	YES	YES	YES	YES	YES
Protection Against Spoofing	YES	YES	YES	YES	YES
Protection Against DDoS Attacks (control plane)	YES	YES	YES	YES	YES

Network Sizing

Requirements for scaling and performance of the Mobile SecGW regarding the IPsec function depend on the location of the SecGW within the MBH network. The following two main parameters are considered:

- Maximum number of tunnels
- Maximum throughput of the encrypted/decrypted traffic

To assess these requirements, a network model of a large scale regional metro network was used (see Figure 15). Table 5 lists the number of nodes, of each type in each segment, and the number of access nodes aggregated at the segment. The table also summarizes the number of IPsec tunnels that must be supported if tunnels are terminated at a particular network segment or node.

Table 5 – Sample Network Segment Size

	AG3 Nodes	AG2 Nodes	AG1 Nodes	CSRs	Macro Cells, N_M	Small Cells, N_S	UNIs	IPsec Tunnels X2/S1
Per Region	2	32	1024	10240	10240	51200	61640	61440 / 61440
Per AG3 Node	-	32	1024	10240	10240	51200	61640	61440 / 61440
Per AG2 Ring	-	2	64	640	640	3200	4040	3840 / 3840
Per AG1 Ring	-	-	4	40	40	200	160	240 / 240
Per Pair of AG1 Nodes			2	20	20	100	80	120 / 120

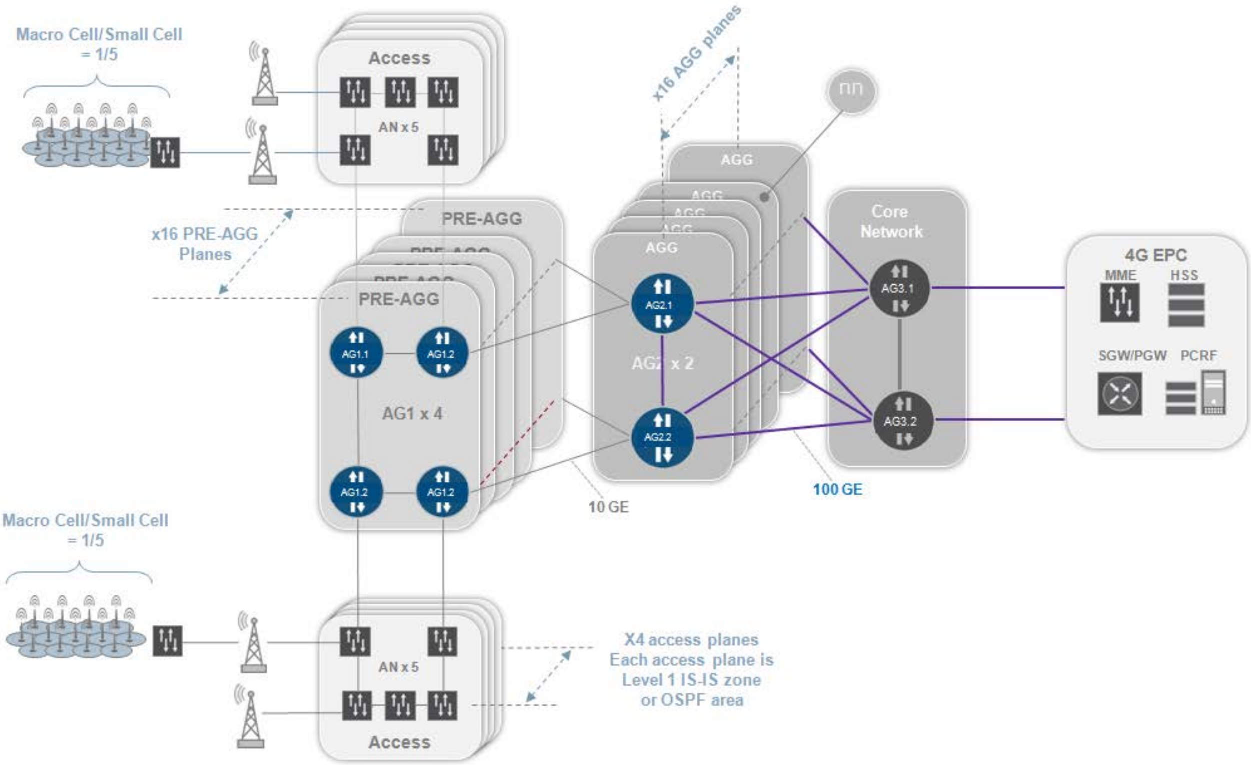


Figure 15 –MBH Network Sizing

In scenarios where the same SecGW provides connectivity for both type of interfaces, the number of tunnels per type of LTE Mobile interface (S1 or X2) can be the same IPsec tunnel that is used to carry both types of traffic.

To assess the traffic throughput generated in such a model, assumptions were made about eNodeB's effective bandwidth and statistical multiplexing of the IP data. The network sizing results are provided in Appendix A of this document.

Timing and Synchronization Considerations

No special consideration is taken into account for timing and synchronization issues that differ from regular (non-IPsec protected) scenarios. You should deploy both SyncE and 1588v2 outside of the IPsec tunnels.

Chapter 4 - Design Examples

The following sections provide network design technical details for some of the SecGW deployment scenarios. You can easily adopt the proposed configuration examples and techniques to other real-life scenarios.

Distributed SecGW Scenario 1.1

The distributed SecGW scenario is one of the most interesting and strongest differentiators of Juniper Networks MBH solution. In this scenario, the IPsec gateway function is placed into the pre-aggregation router of the MBH network. Figure 17 shows two routers, AG1.1 and AG1.2, used as an LTE security gateway which terminates one or two IPsec tunnels from each LTE small cell or macro cell eNodeB. The IPsec gateway function is located nearest to the radio access network location, and provides the shortest possible latency for the X2 traffic between the eNodeBs in the same geographic area.

For this scenario, the MX104 router or MX80-P (or any version of the MX80 Series) router is the best choice as the IPsec gateway. This scenario assumes that each MX Series router is equipped with at least one active multiservice module (MS-MIC) to provide IPsec gateway capabilities. Based on the data presented in Appendix A of this document, the requirements for scaling and performance vary within the following range:

- Number of IPsec tunnels: approximately 40 to 400
- Throughput for IMIX traffic: approximately 1 to 5.5Gbps of encrypted data

Setting Up Routing and IPsec Tunnels

Scenario 1.1 describes an MBH infrastructure service architecture (see Figure 16) with hierarchical end-to-end Layer 3 VPN that provides Layer 3 connectivity across the MBH network. CSR routers act as the service node providing access to the Layer 3 VPN service at the physical Ethernet ports (for more details, see : *http://www.juniper.net/us/en/local/pdf/design-guides/8020018-en.pdf*).

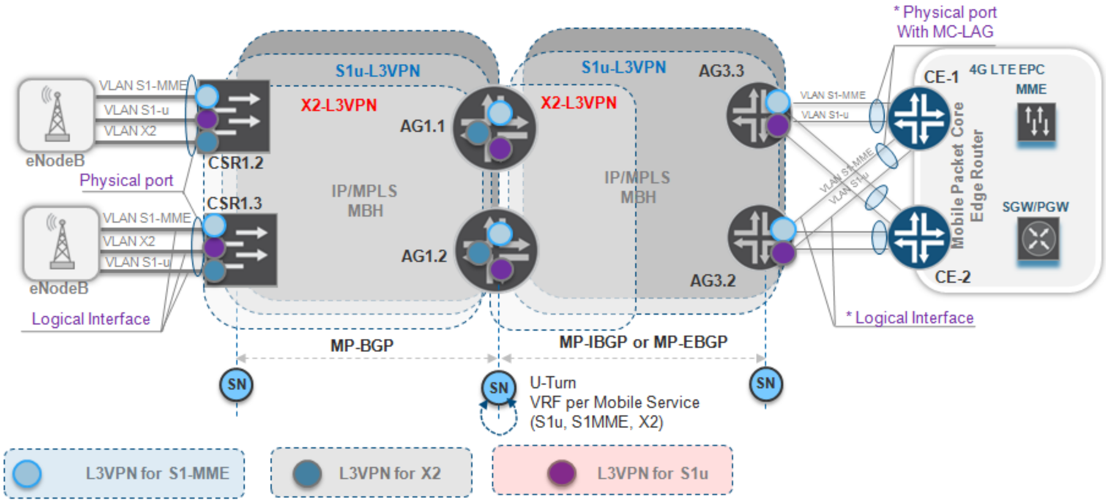


Figure 16 – MBH Service Architecture with End-to-End Layer 3 VPN

Figure 17 shows the case of two groups of small cells connected to the CSR1.2 and CSR1.4.

S1 and X2 traffic is delivered within the IPsec tunnels which are established between each small LTE cell and pre-aggregation node (AG1 router). Depending on the requirements of the RAN, both types of X2 and S1 data can be delivered within the same IPsec tunnel, or within two different tunnels. For this example, only one tunnel carrying the X2 traffic is shown in Figure 17. To provide redundancy, you should configure both AG1.1 and AG1.2 routers as IPsec concentrators. In most deployment scenarios, you should configure redundancy at the IPsec gateway level using active/standby mode only when one router at a time can serve the IPsec traffic for a dedicated eNodeB. In this example, we assume the AG1.2 router serves as an active IPsec concentrator and AG1.1 serves as a backup.

You should configure a pair of multiservice (ms-) interfaces (inside and outside) at the AG routers to serve as the end point of the IPsec tunnel, and place it into the Layer 3 VPN. Configure the inside ms-interface (ms-1/1/0.1) using the IP address that is used as the local IPsec gateway IP address (which is also the remote IPsec gateway address used to configure the eNodeB side) to establish IPsec tunnels for X2 and S1 data. Announce those addresses to the CSR and to the adjacent AG1 router within the Layer 3 VPN using MP-BGP.

Use next-hop style configuration to set up IPsec tunnels on the AG routers. To allow traffic forwarding from the AG1 node to eNodeB prefixes through the tunnel, add a static route for the remote IPsec GW (eNodeB) into the VRF of the Layer 3 VPN with the corresponding inside ms-interface as the next-hop.

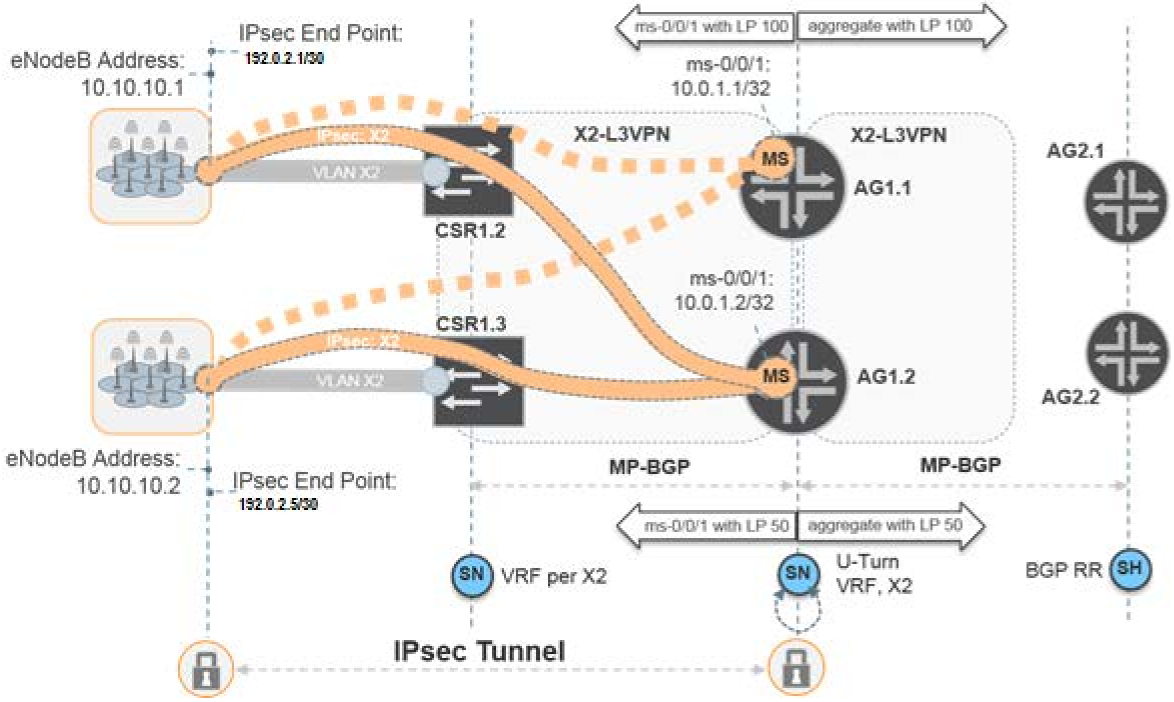
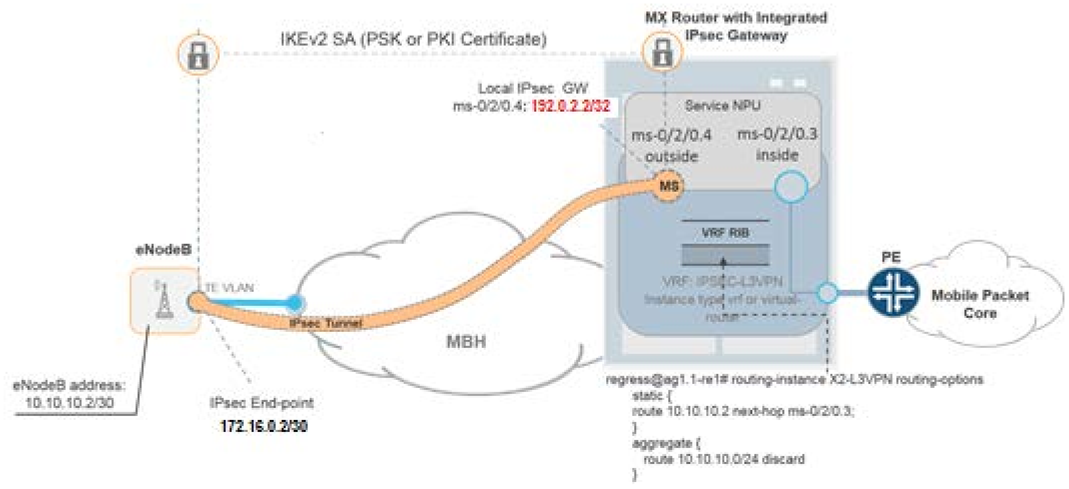


Figure 17 – IPsec Tunnels Termination at MBH Pre-Aggregation Node for X2 Traffic

You can add static routes to the configuration for MX Series routers using the following two options:

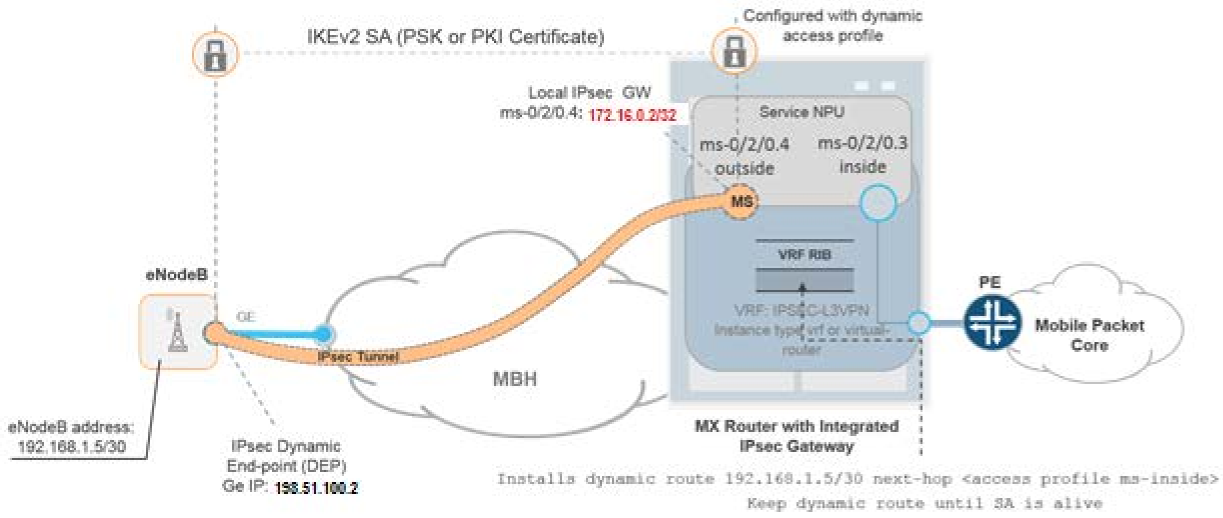
- Manual static routing configuration with static site-to-site IPsec tunnel mode.
- Dynamic static routes installation or Reverse Route Installation (RRI) available with the Dynamic End Point (DEP) mode of the IPsec tunnel establishment (which is the recommended configuration for the Mobile SecGW scenario).


IKEv2 SA (PSK or PKI Certificate)
MX Router with Integrated IPsec Gateway
Local IPsec GW
ms-0/2/0.4: 192.0.2.2/32
Service NPU
ms-0/2/0.4 outside
ms-0/2/0.3 inside
MS
VRF RIB
VRF: IPSEC-L3VPN
Instance type vrf or virtual-router
eNodeB
LTE VLAN
IPsec Tunnel
MBH
PE
Mobile Packet Core
eNodeB address: 10.10.10.2/30
IPsec End-point 172.16.0.2/30

```
regress@ag1.1-re1# routing-instance X2-L3VPN routing-options
    static {
    route 10.10.10.2 next-hop ms-0/2/0.3;
    }
    aggregate {
      route 10.10.10.0/24 discard
    }
```

Figure 18 – Static Point-to-Point Tunnel to IPsec GW with MX Series Router

Figure 18 shows static routes that you need to manually add to the configuration for each remote IPsec end point (eNodeB). You must also create a dedicated pair of ms-interfaces (inside and outside) per end point. The second option provides significantly simplified provisioning on the AG router side. With DEP mode, the AG router does not require explicit provisioning when you add a new small, or macro LTE cell, to the RAN.


IKEv2 SA (PSK or PKI Certificate)
Configured with dynamic access profile
Local IPsec GW
ms-0/2/0.4: 172.16.0.2/32
Service NPU
ms-0/2/0.4 outside
ms-0/2/0.3 inside
MS
VRF RIB
VRF: IPSEC-L3VPN
Instance type vrf or virtual-router
eNodeB
GE
IPsec Tunnel
MBH
PE
Mobile Packet Core
MX Router with Integrated IPsec Gateway
eNodeB address: 192.168.1.5/30
IPsec Dynamic End-point (DEP)
Ge IP: 198.51.100.2

```
Installs dynamic route 192.168.1.5/30 next-hop <access profile ms-inside>
                  Keep dynamic route until SA is alive
```

Figure 19 – Reverse Route Installation for DEP Scenarios

To optimize the amount of routing information that AG1 routers announce to the rest of the network, you can use route summarization. Within the Layer 3 VPN at the AG1 routers, you configure aggregate route(s) for the eNodeBs' IP prefixes. Announce those aggregated routes using BGP to the route reflectors (AG2.1 and AG2.2, in the examples) with the local preference set to 50 and 100, for the primary and backup SecGW, respectively. Using different local precedence (LP) allows the remote AG or PE to choose the primary IPsec gateway as the next-hop for the Layer 3 VPN traffic. You can use the same configuration for the S1 traffic.

For more details and configuration examples, see the Junos Service Interfaces Configuration Guide.

Network Resiliency with Single Tunnel Mode

With a single tunnel mode, an LTE small or macro cell establishes one IPsec tunnel per service, S1 or X2, to a single designated IPsec gateway IP address. In this case, no backup option is available at the eNodeB configuration. However, it is still possible to deploy a pair of SecGW, primary and backup. In case of a primary mobile SecGW failure, to enable IPsec tunnel switch over to back up SecGW (without manual intervention), you slightly modify the configuration of the security gateways. Specifically, you use the same IP-address for both IPsec gateways (also referenced as any-cast scenarios). You assign those IP addresses to the outside logical unit of the multiservice interface so the eNodeB can use it as a remote IPsec gateway address. You assign a lower BGP local preference (LP) value for the primary SecGW which enforces CSR to use the primary SecGW's loopback IP address as the next-hop for any IPsec packet destined to the SecGW IP address within the X2-Layer 3 VPN.

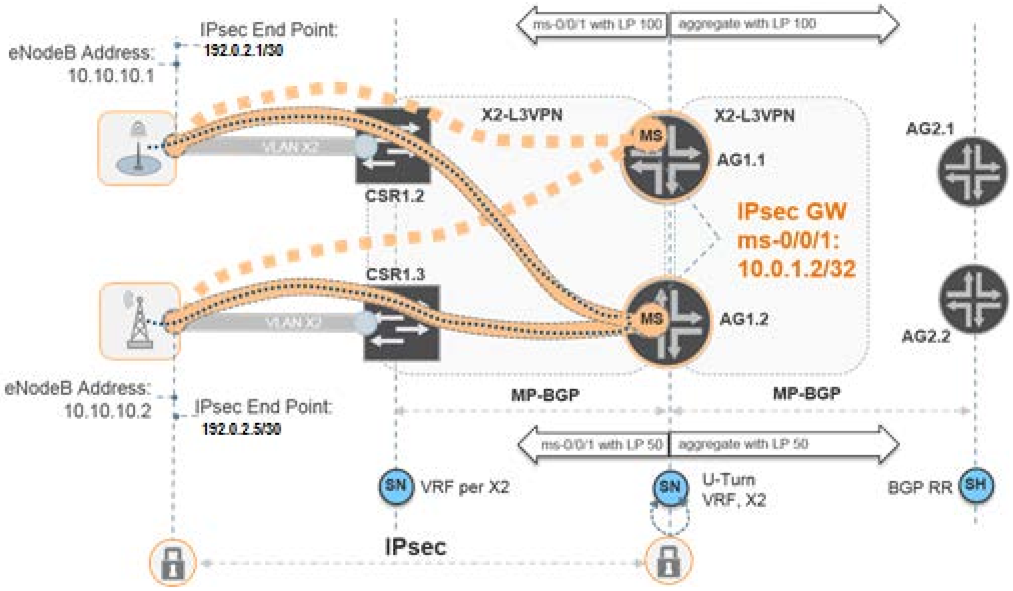


Figure 20 – Terminating X2 IPsec Tunnels at MBH Pre-Aggregation Node

When both security gateways are up, the CSR forwards all of the IPsec packets based on the routing information of the VRF table to the primary IPsec gateway because of a better LP.

In case of a primary SecGW failure or service NPU failure, the eNodeB continues to send packets to the remote IPsec GW IP-address. The CSR switches over the traffic to the backup router based on BGP routing information enabling the eNodeB to reestablish a new IPsec tunnel with the backup IPsec GW. BGP also provides a consistent forwarding path in the aggregation and core segments from EPC to the eNodeB.

For this solution, it is imperative that you tie the IPsec GW IP address into the corresponding ms-interface. Until the service NPU is operational, the status of the ms-interface is up, and its IP address is announced to CSRs using BGP. The service NPU failure triggers re-routing of the traffic flow in the access segment.

To apply stricter control over the switchover, you can implement a Junos opt-script on the SecGW side. An opt-script provides a broader control of the IPsec processes and service NPU events. If necessary, it also triggers the status of the ms-interface, and avoids preemption as soon as the primary SecGW comes back online.

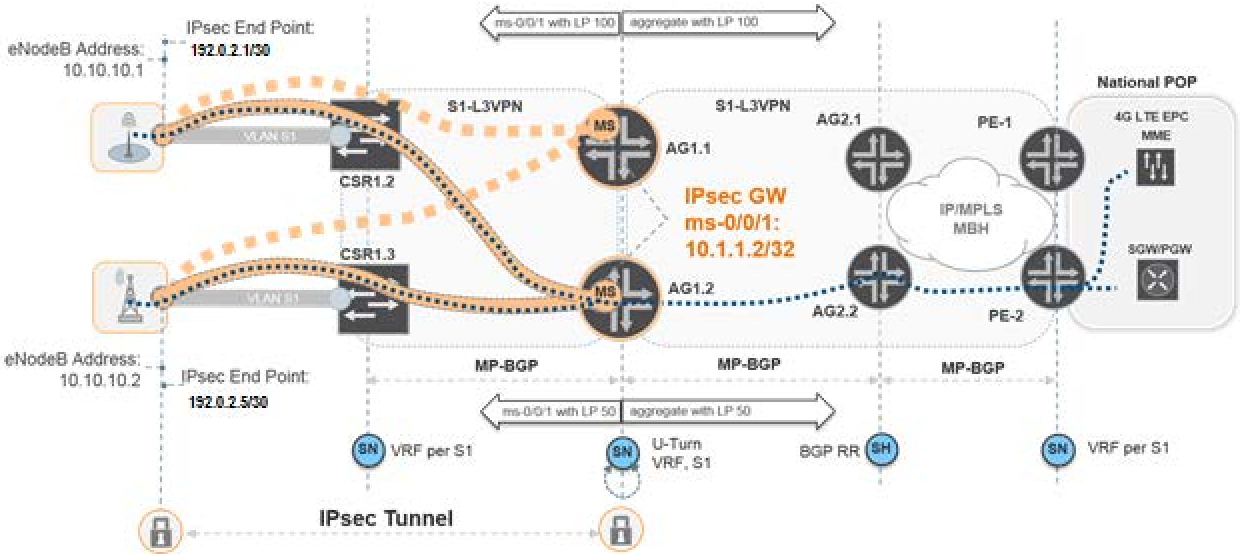


Figure 21 – Terminating S1 IPsec Tunnels at MBH Pre-Aggregation Node

Restoration time is defined by the failure detection time on the eNodeB side (performed by the dead peer detection [DPD]) and the tunnel set up rate on the backup IPsec gateway. For MX Series routers running the latest Junos OS release, the tunnel set up rate range is between 30-60 tunnels per second. The exact value depends on IPsec authentication methods used, PSK or PKI, and Routing Engine load.

Generally, MX Series routers can function as an initiator or responder for the DPD keep-alive messages. Within this solution, Juniper Networks recommends that you configure the Dynamic End Point (DEP) when eNodeB initiates IPsec SA negotiation. In this mode, the MX Series router functions as a DPD responder only.

The DPD function works on Routing Engine of the node. To avoid overloading the Routing Engine with DPD messages, Juniper Networks recommends that you do not configure aggressive timers at the eNodeB side. Dead peer detection leads the tunnel to re-establish with a secondary IPsec GW. Time to re-establish all tunnels depends on the SecGW tunnel setup rate. For example, if there are 900 tunnels terminated at the IPsec GW, it takes approximately 30 seconds to re-establish all tunnels with an average tunnel setup rate of 30 cps. To be consistent with the SecGW tunnel setup rate in this example, set 15 seconds for the DPD timeout, and 30 seconds for the DPD delay values.

Restrictions

If PKI methods are used, some restrictions for this high availability scenario may occur because of the IPsec authentication profile. For the connected eNodeB, two independent IPsec gateways might attempt to retrieve the same certificate from the server which could lead to problems. As an alternative method, you should use PSK.

Network Resiliency with Dual Tunnel Model and DPD

For this scenario, you can configure each eNodeB with a primary and a backup gateway. However, you can establish only one active IPsec tunnel at time. DPD is used to detect failure of the IPsec gateway. In case of a primary gateway failure, eNodeB reestablishes the IPsec tunnel as the secondary gateway. No additional configuration is required on the IPsec gateway side. Restoration time is defined by the failure detection time on the eNodeB side (performed by DPD) and the tunnel set up rate on the backup IPsec gateway. For MX Series routers running the latest Junos OS release, the tunnel set up rate range is between 30-60 tunnels per second with PSK as an authentication method. The exact value depends on IPsec authentication methods used, PSK or PKI, and Routing Engine load.

Similar considerations for the values of the DPD timers (as was described in the previous section) apply to this scenario.

Network Resiliency with Dual Tunnel Model and BFD

For this scenario, you can configure each eNodeB with a primary and secondary IPsec gateway. You can establish two active IPsec tunnels at time with both IPsec gateways. IPsec tunnels overlay the MBH infrastructure. From the eNodeB perspective, the tunnels are valued as an equal cost forwarding path to the EPC or to the other eNodeB. The DPD mechanism tracks the status of the IPsec tunnels, while the status of the forwarding path is controlled by the multihop BFD on both sides, the eNodeB and the IPsec GW. In case of the IPsec tunnels going down, this allows fast failure detection and traffic is re-routed to an alternate path over a second IPsec tunnel.

The advantage of this scenario is that it provides a short restoration time in case of an IPsec gateway, or a single service NPU failure (mainly defined by BFD timers). You can deploy BFD on an MX Series routing using the following two approaches:

- Distributed to the Packet Forwarding Engine level
- Centralized on the Routing Engine

Both methods have advantages and disadvantages, depending on the particular situation.

In a distributed mode, you can set up BFD timers as small as 10 ms and still provide support for a significant amount of simultaneous BFD sessions without affecting the router's performance. However, keep in mind that the distributed BFD session being mapped to a particular Packet Forwarding Engine, fails if the Packet Forwarding Engine fails. Using the multihop BFD approach may lead to an erroneous traffic switchover. For example, if a Packet Forwarding Engine failure of the high-end MX Series router does not cause the IPsec tunnel failure, an alternate valid forwarding path may still exist through the other Packet Forwarding Engine. To switch the BFD back to centralized mode, all BFD sessions are mapped to the Routing Engine. The Routing Engine is protected from failure with NSR mechanisms. Routing Engine performance is the tradeoff for this example. The shortest BFD timer is restricted with a value of 100 ms. Depending on the number of BFD sessions (number of small and macro cells connected to the given IPsec gateway) and the type of Routing Engine, and other protocols using centralized BFD, the value for BFD timer may still require corrections.

Note: For BFD performance information for particular hardware configurations, please see the MX Series scaling data. A single MX Series chassis can support up to 5000 BFD sessions with BFD keep-alive timers of 1 second. Juniper Networks recommends that you tune timers in each case individually because other processes use the Routing Engine resources.

In designs where routing platforms with a single Packet Forwarding Engine per system (such as MX80 or MX104 platforms) are used at the pre-aggregation segment, the distributed mode is the only recommended method for a multihop BFD session.

Distributed SecGW Scenario 1.2

The majority of the IPsec part of the design in deployment scenario 1.2 follows the same recommendations as previously provided in scenario 1.1. To add IPsec on top of the MBH profile with pseudowire head-end termination, you must modify the configuration of the IP and MPLS layers slightly.

For this scenario, the MX104 router or MX80-P (or any version of the MX80 Series) router is the best choice as the IPsec gateway. This scenario assumes that each MX Series router is equipped with at least one active multiservice module (MS-MIC) to provide IPsec gateway capabilities. Based on the data presented in Appendix A of this document, the requirements for scaling and performance vary within the following range:

- Number of IPsec tunnels: approximately 40 to 400
- Throughput for IMIX traffic: approximately 1 to 5.5Gbps of encrypted data

Setting Up Routing and IPsec Tunneling

Figure 22 shows an example of two groups of small cells connected to the CSR1.2 and CSR1.3. IPsec packets are delivered transparently from the CSR routers to the pre-aggregation routers within the Layer 2 MPLS pseudowire (PW). CSR establishes the PW with the pre-aggregation router noted in Figure 22 with the blue solid line for the active PW. You can establish a backup or standby pseudowire towards the second AG router, noted in Figure 23 with dashed lines.

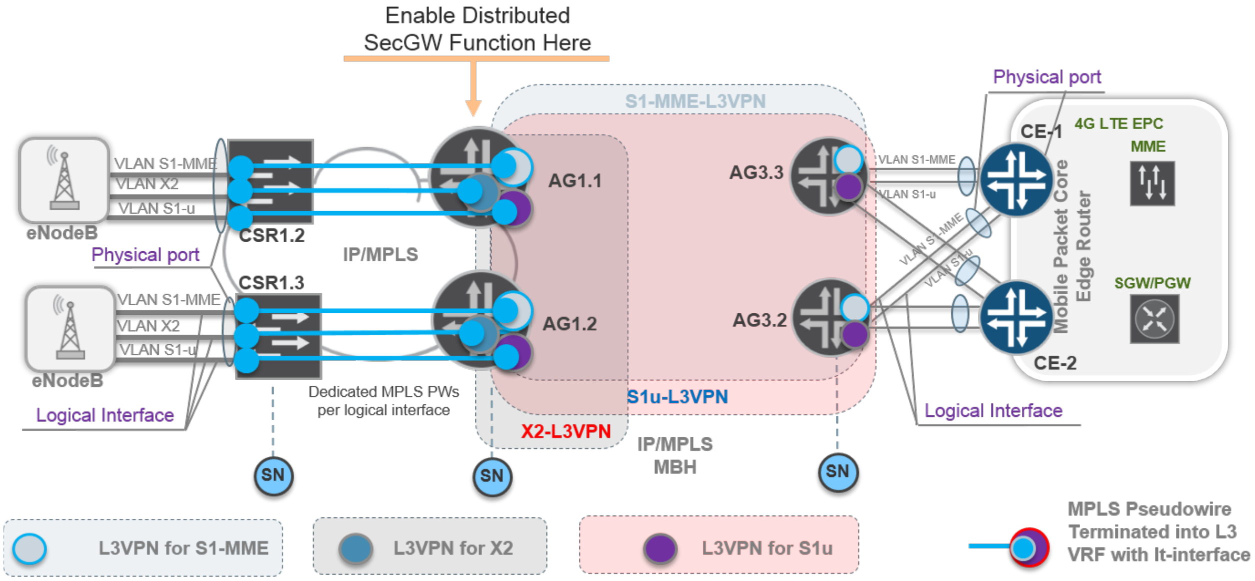


Figure 22 – MBH Deployment Scenario with Pseudowire to Layer 3 VPN Termination

Pseudowires terminate at pre-aggregation routers directly into the dedicated Layer 3 VPN (X2-Layer 3 VPN for X2 traffic) using logical tunnel (lt-) interfaces. You can also apply this same concept to using the ps-interface as the pseudowire termination point. From Figure 22, it appears that each individual small and macro cell is dual-homed to a pair of AG routers with a direct link to the Layer 3 VPN through the individual logical IP interface (lt-interface logical unit).

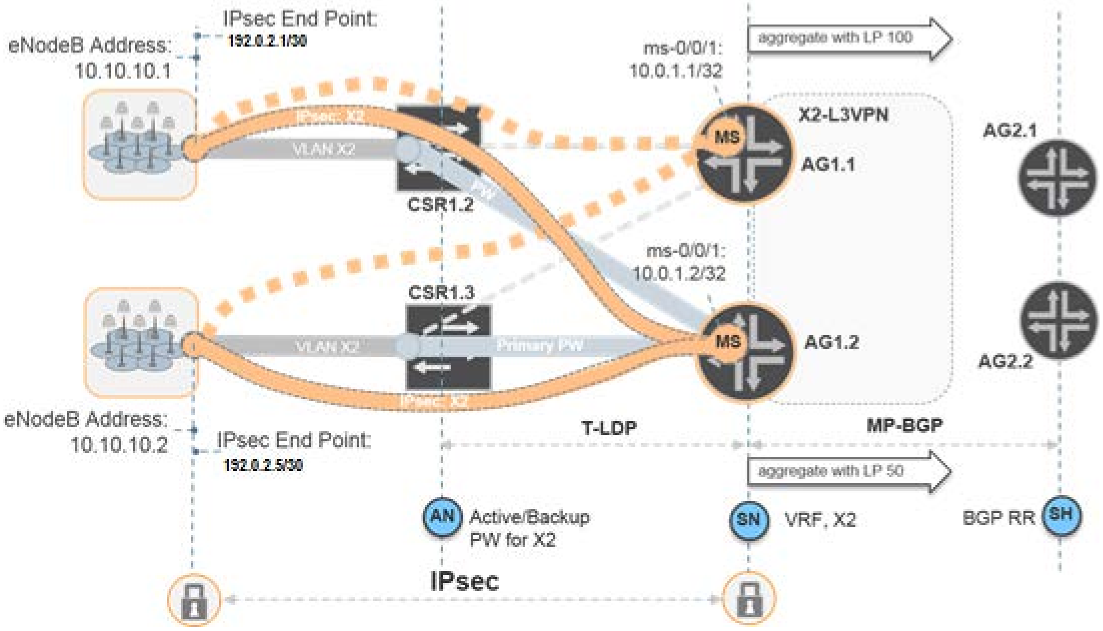


Figure 23 – Terminating X2 IPsec Tunnels at the MBH Pre-Aggregation Node

In case the primary AG1 router fails, to guarantee no traffic loss from eNodeB to the network, you configure each adjacent pair of lt-interfaces on both routers AG1.1 and AG1.2 with a VRRP group and virtual IP address. In a steady situation within the access segment, traffic from eNodeB towards routers AG1.1 and AG1.2 is forwarded to the virtual destination MAC address (which is the same for both AG1.1 and AG1.2). If the primary AG1 routers (AG1.2) goes down, then the following occurs:

1. CSR switches over pseudowire to the secondary AG1 router (AG1.1).
2. eNodeB continues to forward traffic to the same virtual IP MAC without requiring ARP re-learning.

The IPsec tunnel delivers S1 and X2 traffic which is established between the small LTE cell and AG1 routers. For simplicity, only one tunnel is shown in the Figure 23. To provide redundancy, you should configure both routers (AG1.1 and AG1.2) as IPsec concentrators. In most deployment scenarios with redundancy at the IPsec gateway level, you configure one IPsec gateway as primary, and the other as secondary or backup SecGW. Only one router at a time can serve IPsec traffic for a dedicated eNodeB. In this scenario, the AG1.2 router serves as the primary IPsec concentrator and AG1.1 as the backup.

You should configure a pair of multiservice (ms-) interfaces (inside and outside) at the AG routers to serve as the end point of the IPsec tunnel, and place it into the Layer 3 VPN. Configure the inside ms-interface (ms-1/1/0.1) using the IP address that is used as the local IPsec gateway IP address (which is also the remote IPsec gateway address used to configure the eNodeB) to establish IPsec tunnels for X2 and S1 data. Announce those addresses to the CSR and to the adjacent AG1 router within the Layer 3 VPN using MP-BGP.

Use next-hop style configuration to set up IPsec tunnels on the AG routers. To allow traffic forwarding from the AG1 node to eNodeB prefixes through the tunnel, add a static route for the remote IPsec GW (eNodeB) into the VRF of the Layer 3 VPN with the corresponding inside ms-interface as the next-hop.

You can add static routes to the configuration for MX Series routers using the following two options:

- Manual static routing configuration with static site-to-site IPsec tunnel mode.
- Dynamic static routes installation or Reverse Route Installation (RRI) available with the Dynamic End Point (DEP) mode of the IPsec tunnel establishment (which is the recommended configuration for the Mobile SecGW scenario).

The second option provides significantly simplified provisioning on the AG router side. With DEP mode, the AG router does not require explicit provisioning when you add a new small, or macro LTE cell, to the RAN.

To optimize the amount of routing information that AG1 routers announce to the rest of the network, you can:

- Use route summarization. Within the Layer 3 VPN at the AG1 routers, you configure aggregate route(s) for the eNodeBs' IP prefixes. Announce those aggregated routes using BGP to the route reflectors (AG2.1 and AG2.2, in the examples) with the local preference set to 50 and 100, for the primary and backup SecGW, respectively. Using different local precedence (LP) allows the remote AG or PE to choose the primary IPsec gateway as the next-hop for the Layer 3 VPN traffic. You can use the same configuration for the S1 traffic.
- Exclude prefixes assigned to lt-interfaces from being distributed into MP-BGP as in the current deployment. The have a local meaning for the access segment only.

Network Resiliency

As previously described in deployment scenario 1.1, there are three possible ways to arrange the IPsec tunnel switchover depending on the eNodeB capabilities:

- Single tunnel mode
- Dual tunnel mode with DPD
- Dual tunnel mode with DFD

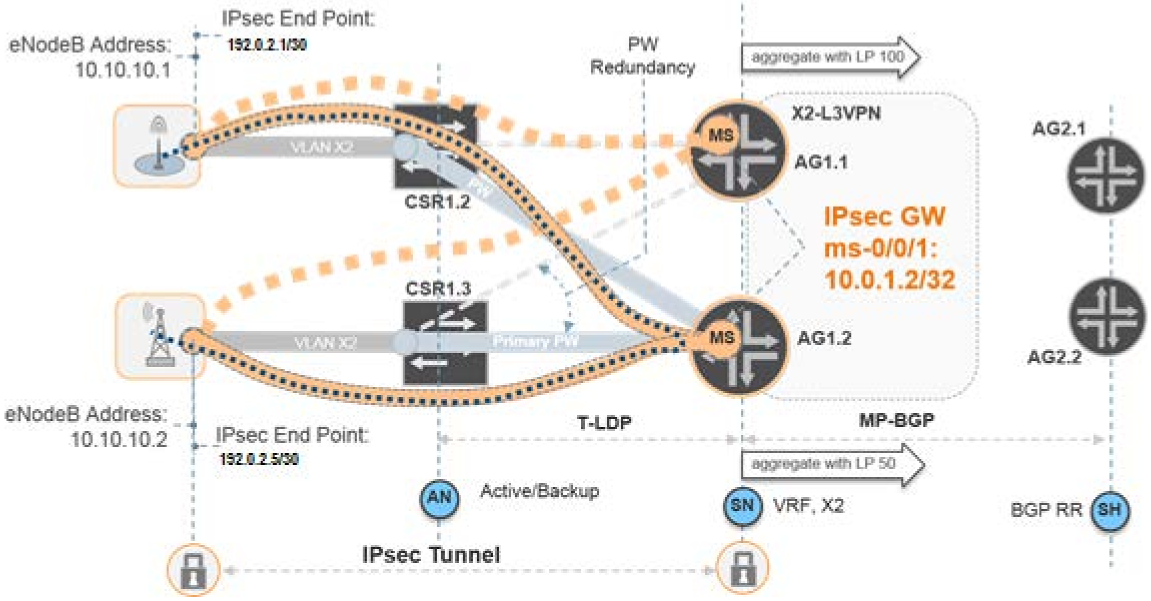


Figure 24 – Terminating X2 IPsec Tunnels at the MBH Pre-Aggregation Node (Scenario 1.2)

Note: All previous design considerations and recommended configurations apply to the deployment scenarios with pseudowires in the access segment.

The only difference is how the forwarding path is managed in the access segment when the service NPU fails. In the previous scenario, the status of the inside ms-interface logical unit is signaled to CSR through MP-BGP. As soon as the ms-interface on the primary IPsec gateway goes down, CSR selects the secondary gateway's (AG1.1) loopback as a next-hop to deliver IPsec packets destined to the IPsec gateway address. In these scenarios, the MPLS PW transport/service layer in the access segment is completely separate from the IPsec layer.

If a service NPU fails at the primary gateway, no pseudowire switchover occurs. CSR nodes continue to forward IPsec packets to the primary AG1.2 through the Layer 2 pseudowire. In response, AG1.2 then forwards packets to the backup AG1 router (AG1.1) through Layer 3 VPN. Finally, new IPsec tunnels are established to the secondary IPsec gateway using a slightly non-optimal forwarding path at the IP/MPLS level. This is minor drawback that you should factor in when planning your topology. The topology must provide enough bandwidth to address additional traffic flow between the adjacent pair of the AG1 routers.

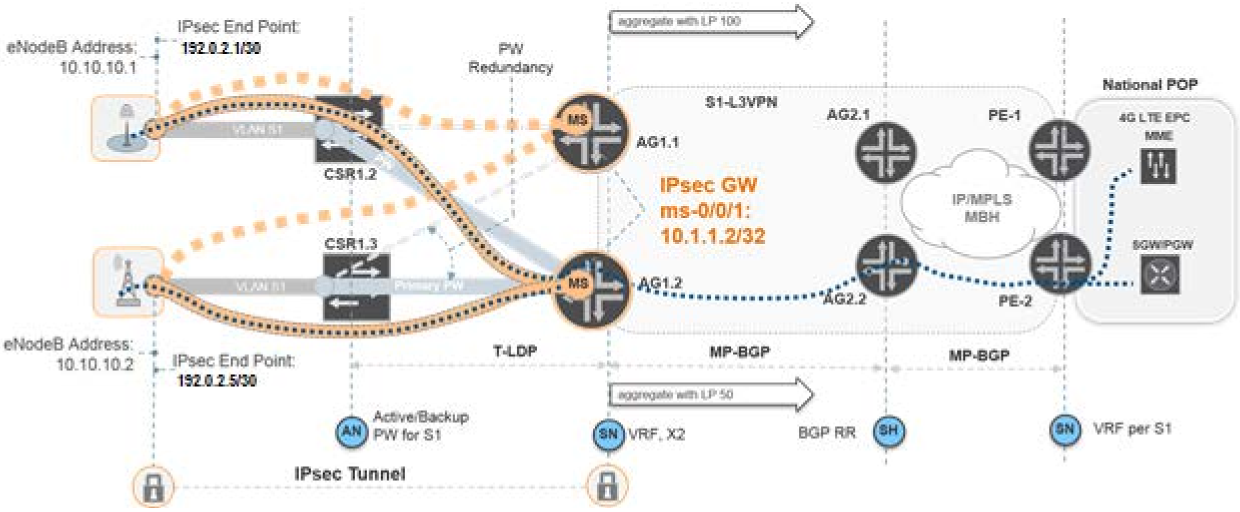


Figure 25 – Terminating S1 IPsec Tunnels at the MBH Pre-Aggregation Node (Scenario 1.2)

You should consider one more additional failure event in the deployment scenarios, lt-interface failure. The lt-interface is anchored to one of the Packet Forwarding Engines of the MX Series router. If the Packet Forwarding Engine or a line-card goes down, the lt-interface also goes down. This event leads to a pseudowire switchover from the primary to the backup AG1 router. For the single tunnel model where both IPsec gateways are assigned the same IP address, this event forces the IPsec session to re-establish to the backup IPsec gateway. To avoid this situation, Juniper Networks highly recommends that you enable lt-interface redundancy (available on MX-Series routers starting with Junos OS Release 13.2).

Small Cell SecGW Scenario 1.3

You may need a solution for small and pico cells (provided by some RAN vendors) that includes components such as: a small cell home gateway (which acts as an aggregator of OAM), mobile signaling, and data traffic from a group of small cells (orange dotted lines in Figure 26). This example assumes that all communication between the small cell and home gateway occurs over the IP protocol.

The home gateway hides the small cell infrastructure from the EPC and enables better scale for the LTE mobile network. These small cell deployment scenarios leverage the existing infrastructure of the MBH network for the Macro eNodeBs with a small cell home gateway located at one of the eNodeB’s cell site. The point where a small cell interconnects with a small cell MBH segment is frequently exposed to potential threats of unauthorized intrusions or MitM attacks.

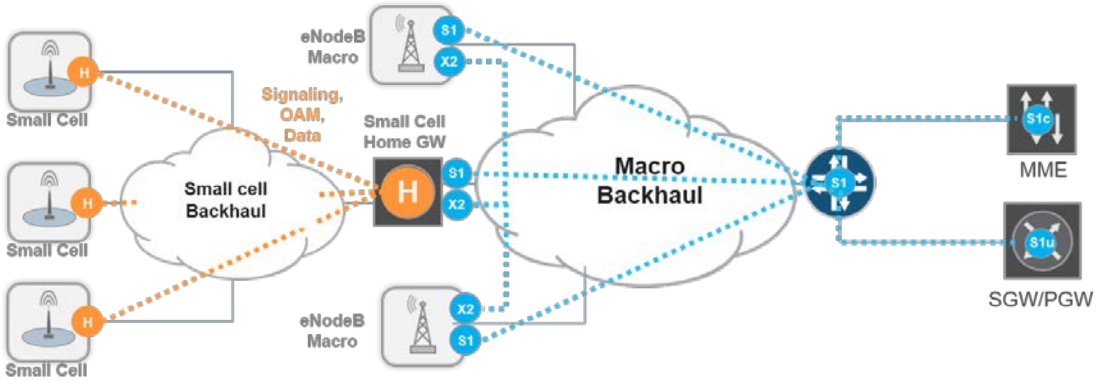


Figure 26 – Small Cell with Home Gateway Use Case

To provide secure communications between the small/pico LTE cell and the home gateway controller (eNodeB GW), this deployment scenario leverages deployment scenario 1.1 for the distributed SecGW.

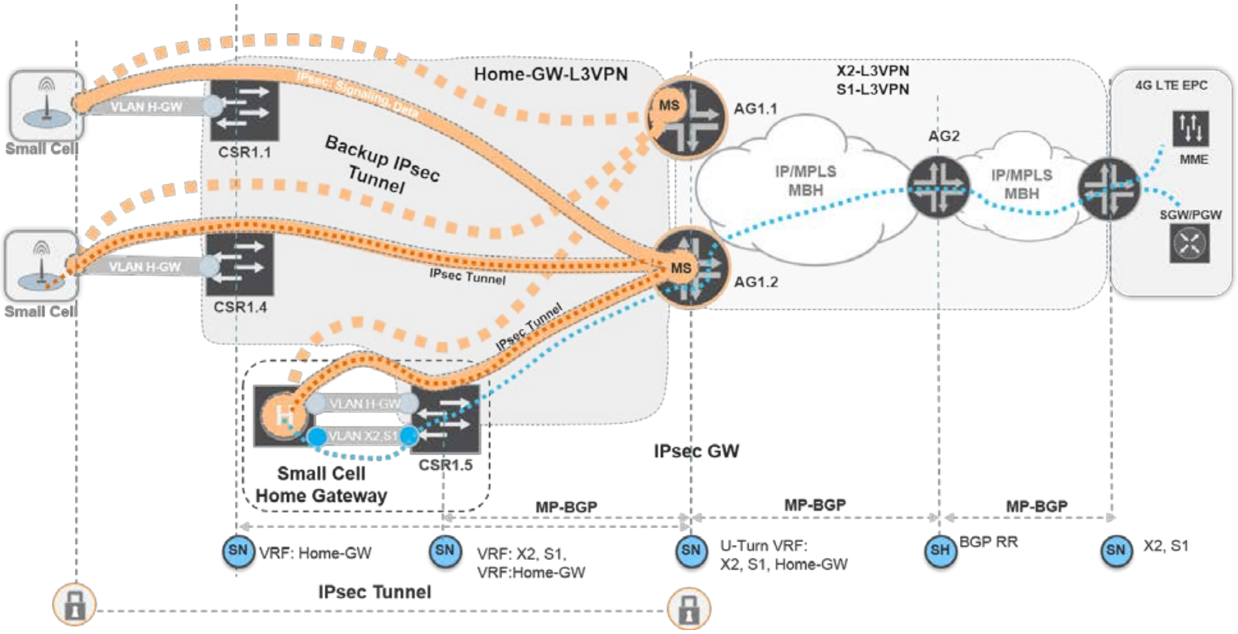


Figure 27 – Small Cell Home Gateway Deployment Scenario Without Encryption

Figure 27 shows a small cell home gateway deployment scenario using the MBH network. To provide connectivity between eNodeBs, the home gateway and the 4G LTE EPC, an end-to-end hierarchical Layer 3 VPN is used in the access and aggregation network segments. A group of CSRs (CSR1.1 and CSR1.4) extends the macro cell backhaul and provides connectivity for the LTE small cells. A dedicated Layer 3 VPN (Home-GW-L3VPN) is used in the access segment to deliver all traffic from the small LTE cell to the small cell home gateway. The home gateway is connected to the macro eNodeB's cell site router CSR1.5.

The IPsec GW function is located at the pre-aggregation routers and terminates IPsec tunnels from the small cell and home gateway, respectively. If you change the Layer 3 VPN to Layer 2 PW, it then describes scenario 1.2. The dotted blue line in Figure 27 shows the actual traffic path from the small LTE cell to the 4G LTE core.

Semi-Distributed and Centralized SecGW Scenarios

The following deployment scenarios use the MX240/MX480/MX960 routing platforms for the IPsec gateway at the regional or national POP. These platforms correspond to PE routers AG2 and AG3 (see Figure 8) within the MBH network infrastructure. The IPsec gateway is directly connected to either the EPC, the mobile core backbone, or through Layer 3 VPN. This scenario assumes that each AG2 router is equipped with at least one active multiservice module (MS-MPC) to provide IPsec gateway capabilities. With Junos OS Release 14.1R1, you can install up to four multiservice modules in one aggregation chassis to provide throughput for IPsec traffic and redundancy.

This scenario assumes that the IPsec gateways are part of the network model previously shown in Figure 15. Based on data and assumptions from Appendix A of this design guide, scaling and performance requirements for each deployment scenario fall within the ranges listed in Table 6.

Table 6 – Scaling and Performance Requirements for IPsec Gateway at POP Locations

Service/Scenario #		Requirements		
		Tunnels	Performance	
Scenario 2 (AG2)		640 – 3840	13.44 – 67.2	Direct connection EPC Regional POP
Scenario 3 (AG2)		640 – 3840	13.44 – 67.2	Connection over L3VPN to EPC at National POP
Scenario 4 (AG3)	Total	10240 - 61640	1.05 Gbps	Direct connection EPC at National POP
	Per IPsec GW	1000-8000	100 Gbps	

The lower limit of the scaling numbers corresponds to the deployment scenarios with macro cell only. Higher numbers correspond to when both the LTE macro and the small cell are connected to the MBH network. Scenarios 2 and 3 represent semi-distributed designs, and Scenario 4 represents a centralized mobile SecGW design.

Two rows in Table 6 show the centralized location of the IPsec gateway:

- The first row shows the total amount of IPsec tunnel and encrypted data throughput that is aggregated based on the assumption it occurs at the regional or national POP. The requirements extend beyond what the scaling figures require (which can be provided by a single MX Series router). With Junos OS Release 14.1, the maximum performance of a single MX Series device with 4 multiservice MPCs is qualified for approximately at 100 Gbps of IMIX traffic per system.
- The second row shows requirements for per single system normalized to its maximum possible performance. For a given network and its needs for LTE data encryption, at least 10 routing systems are required, plus additional routing systems for redundancy. Under this condition, the solution for the “semi-distributed” mobile SecGW function at the regional POPs (AG2) seems more reasonable. For deployments with macro cell only, a design model with a centralized location of the SecGW would be a valuable fit.

Figure 28 and Figure 29 show deployment scenarios with the mobile SecGW function located at the aggregation router of the MBH network at the regional or national POP. Layer 3 VPN is still used to backhaul traffic to and from the LTE EPC. Because of the decoupling of transport and service layers, the routing nodes configuration for Layer 3 VPN and the configuration that enables the IPsec function are the same (described for scenario 1.1), so it is not described in this scenario. The BGP protocol helps to establish consistent end-to-end traffic forwarding in case the primary SecGW fails, or one of its service NPU fails.

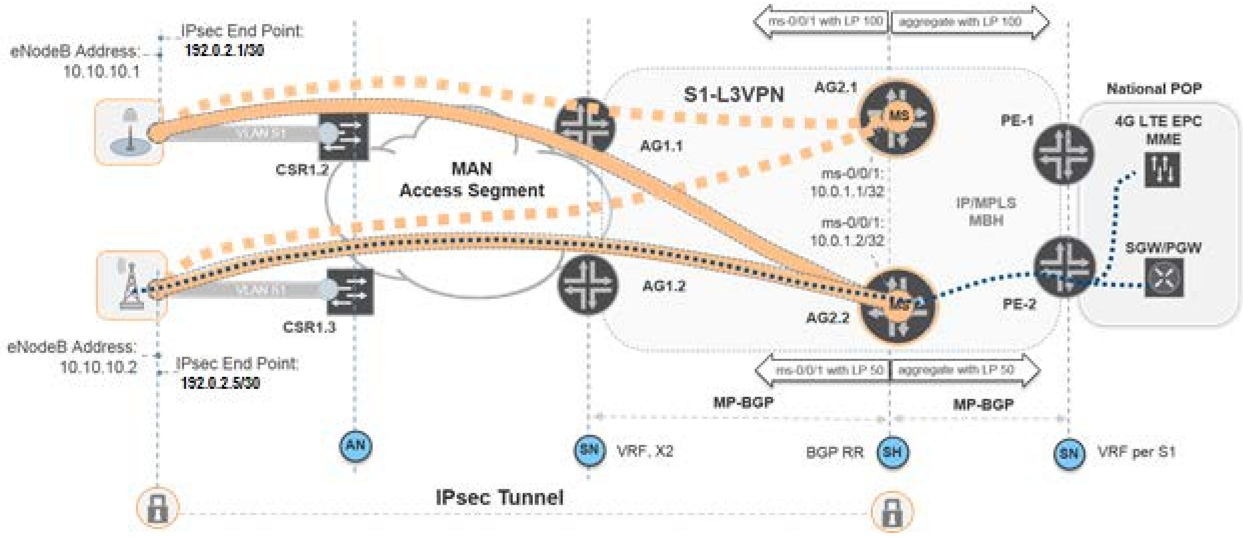


Figure 28 – Semi-Distributed SecGW Scenario

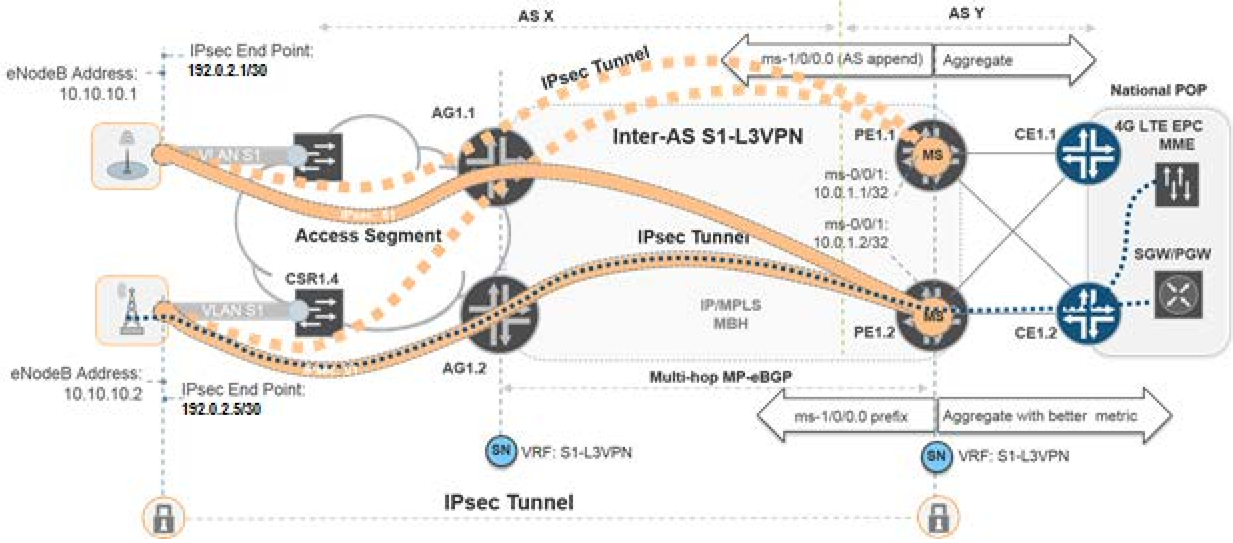


Figure 29 – Centralized SecGW Scenario

When AG2 and AG3 routers host the IPsec gateway function and have a direct connection to the EPC segment, you many need to configure a dynamic routing protocol to enable the EPC border router to recognize the eNodeB prefixes. To accomplish this, redistribute the static routes installed by the RRI feature of the IPsec gateway to the corresponding routing protocols, and announce it to the EPC border router. You can use different values of IGP metrics for the eNodeB prefixes at the primary and secondary gateways to set up optimal routing for the traffic flows from the EPC towards the IPsec gateways.

SecGW Deployment with a Wholesale Model

In a wholesale model, the metro Ethernet network (which belongs to the third-party MBH operator) provides connectivity between an IPsec gateway and a cell site router. Scenarios differ by the type of the EVC (such as E-LINE, E-LAN, and E-TREE) used to deliver traffic flows within a customer VLAN between two or more user-to-network interfaces (UNI). Scenarios also differ by configuring the aggregation router used to provide the correct demultiplexing of the customer VLANs, and by mapping them to Layer 3 logical interfaces.

The following four deployment scenarios described below include when the IPsec function is located at the aggregation router and is directly connected to the wholesale MBH network:

- Dual E-Line EVC with Layer 2 CE: cell site access node
- Dual E-Line EVC with Layer 3 CE: cell site router (CSR)
- Single E-Line EVC with Multichassis LAG at SecGW
- Single E-LAN/E-Tree EVC

High-end MX480/MX960/MX2020 routing platforms are used in the scenarios to host the IPsec gateway function with at least one active multiservice module (MS-MPC) installed. You can install up to four multiservice modules in one aggregation chassis to provide throughput for IPsec traffic and redundancy. The performance requirements are the same as listed in Table 6. The configuration for the IPsec function itself is the same for all of the four scenarios. Some configuration variations are possible because of the different resiliency model implemented in each of the particular scenarios.

Accessing IPsec Gateway with E-Line EVC

Figure 30 and Figure 31 show high-level architecture deployment scenarios with a redundant pair of E-Line EVCs. Each small or macro eNodeB is connected to the access node which can act as Layer 2 or Layer 3 CE node, as shown in Figure 30 and Figure 31, respectively. Each is CSR dual-homed to the MAN network with UNI A1 and UNI A2.

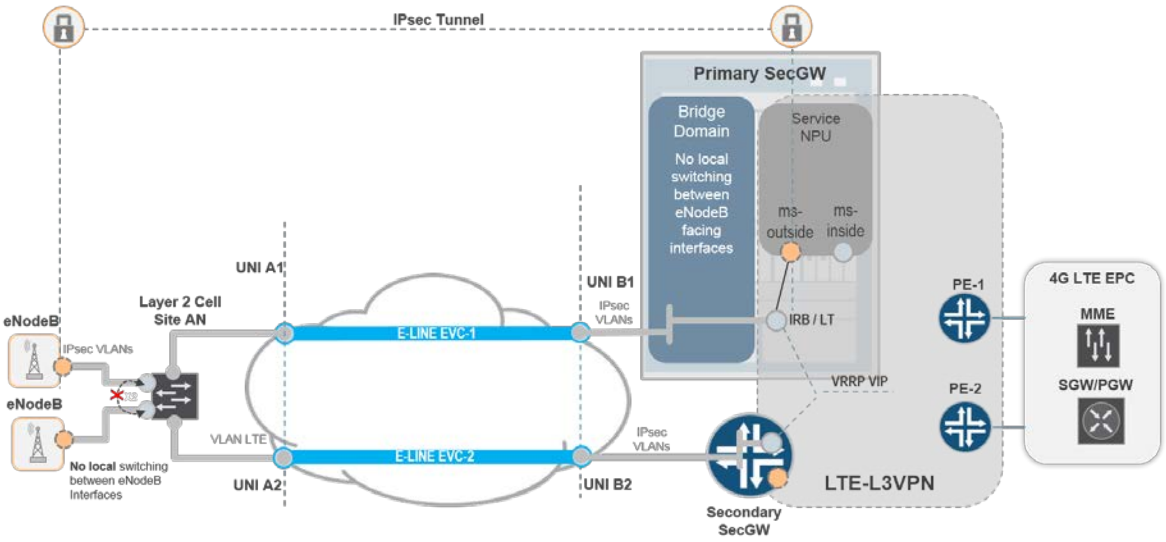


Figure 30 – Wholesale MBH with Dual E-Line EVCs and Layer 2 Access Node

A unique VLAN tag (or few VLAN tags, one per eNodeB) is used at UNI A1 and UNI A2 to identify each site. Within the scenarios, this tag is referenced as IPsec VLAN. Aggregation routers (primary and secondary SecGW) are connected to the MAN at UNI B1 and UNI B2 with multiple EVCs bundled at the physical port.

You can configure the aggregation router to demultiplex traffic flows from an individual cell site and deliver flows to a Layer 3 VPN with the IPsec function configured using two methods.

With the first method, the aggregation router performs VLAN demultiplexing and maps each IPsec VLAN from the individual site to the Layer 3 IFL (interface logical units). The IFL sits on top of the physical Gigabit Ethernet or 10 Gigabit Ethernet UNI port of the MX Series router. One IFL is created per eNodeB and placed into the Layer 3 VPN. Use this method to configure an aggregation router when no encryption is required. The key difference in this scenario is that you do not need to provide Layer 3 direct connectivity between eNodeBs for X2 traffic. Instead, you need to provide connectivity for each eNodeB to the IPsec gateway IP address establish an IPsec tunnel. X2 traffic flows are then allowed between different IPsec tunnels. Because the configuration of the aggregation router is slightly simplified, Juniper Networks recommends the second method shown in Figure 30 and Figure 31.

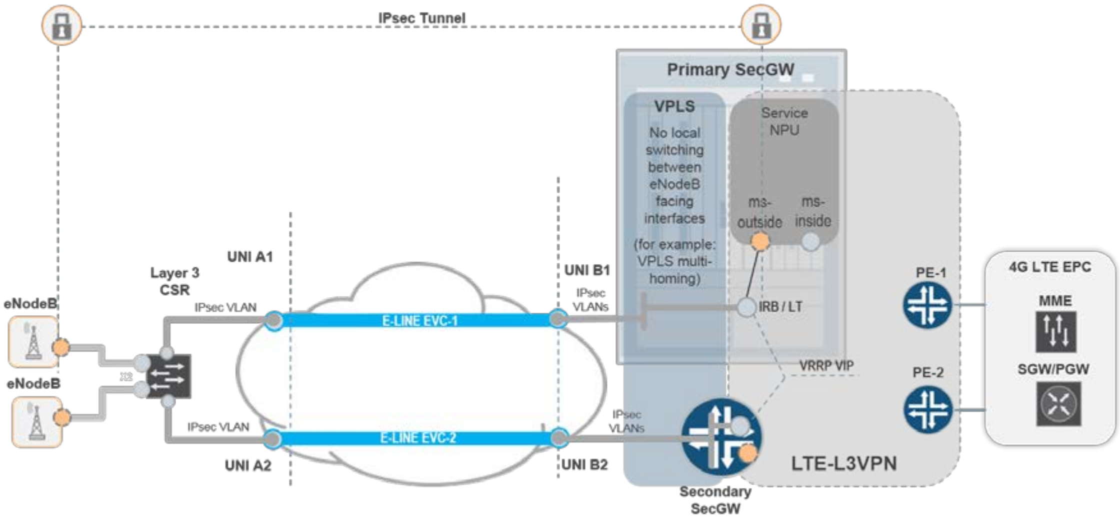


Figure 31 – Wholesale MBH with Dual E-Line EVCs and Layer 3 Access Node

The aggregation router performs VLAN demultiplexing and maps each IPsec VLAN from the individual site to the Layer 2 bridge domain, or to the VPLS logical unit of the physical port. Depending on the type of CSR, configure the bridge domain or VPLS instance with the following items:

- Configure the `vlan-id` none statement for the bridge domain or VPLS instance. This statement causes the MX Series device to use an unqualified learning bridge domain.
- Restrict local switching within the bridge domain between the CE interfaces facing the access segment.
- Create an IRB or lt-interface to allow traffic from the bridge domain to pass to and from the Layer 3 VPN with the IPsec gateway function configured.
- Create a single VRRP group for adjacent pairs of IRB/lt-interfaces on the primary and secondary SecGW.

To enable VRRP peering, allow Layer 2 bridging between UNI A1 and UNI A2 through the Layer 2 cell site AN. If Layer 3 CSR is used, replace the bridge domain with the VPLS instance.

The IPsec gateway function is located in the Laver 3 VPN of the AG routers. Juniper Networks recommends using a configuration for the IPsec gateways similar to what was described earlier in the IPsec gateway distributed scenarios with pseudowires in the access segment. Configure the primary SecGW as a VRRP master. If using the lt-interface instead of the IRB, configure lt-interface redundancy to avoid having the IPsec tunnels switchover when the anchor Packet Forwarding Engine of the lt-interface fails.

Accessing the IPsec Gateway with E-Line EVC and MC-LAG

Figure 32 shows an alternative scenario with E-Line EVC using a single UNI-A to interconnect the CSR to the MAN. Two physical interfaces are used on the other side of the network for a dual-home connectivity between the mobile operator's aggregation routers and MAN. Two physical links are bundled into one logical link using the link aggregation protocol. This scenario leverages the multichassis LAG capability of the MX Series router. As in the previous example, C-VLAN tags are mapped to the logical IFL which is located at the top of the multichassis aggregated interface (mc-ae) of the AG router.

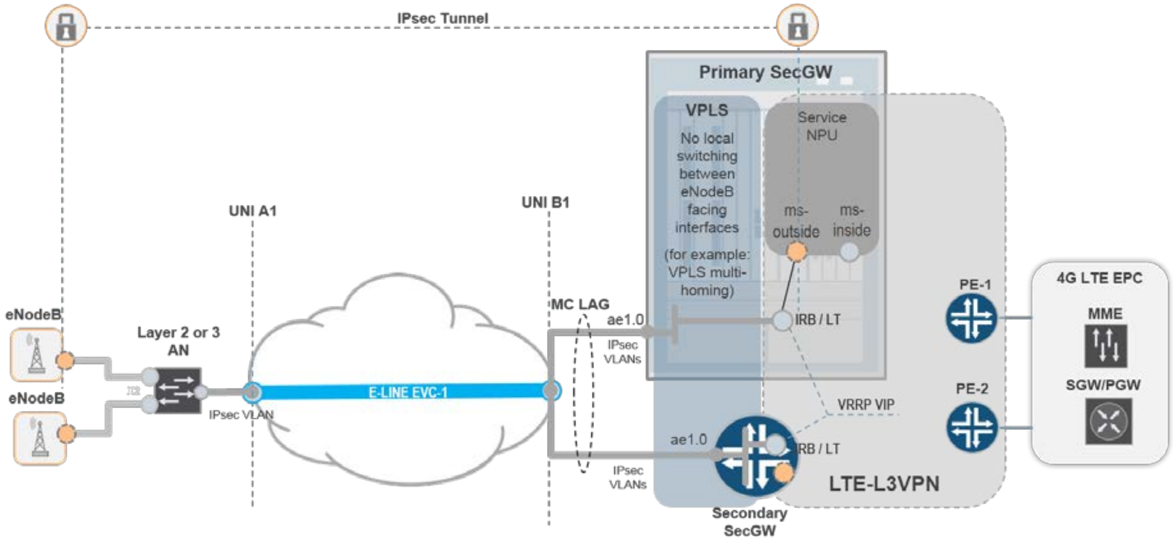


Figure 32 – Wholesale MBH with E-Line E EVC and Multichassis LAG at the SecGW

IFLs are first terminated into the VPLS instance. At this point, VLAN normalization is performed by removing the C-VLAN tag. The easiest way to remove the C-VLAN tag is to configure the `vlan-id none` statement under the `routing-instance` hierarchy level of the MX Series router configuration.

To permit traffic from eNodeB to reach the Layer 3 VPN, configure an integrated routing and bridging (IRB) interface on both AG routers. (For more details, click http://www.juniper.net/techpubs/en_US/junos14.1/topics/task/configuration/interfaces-active-active-bridging-vrrp-over-irb-mx-series.html.)

To restrict direct traffic from switching between eNodeBs within VPLS instances, configure `the use no-local-switching` statement under the `routing-instance` hierarchy level of the MX Series router configuration. In this example, configuration of the per eNodeB Layer 3 interface was avoided while still permitting enough Layer 3 connectivity to establish an IPsec tunnel per eNodeB.

The IPsec function configuration is identical to what described earlier in this document for the MBH with pseudowire head end termination scenario.

Accessing the IPsec Gateway with E-LAN/E-Tree EVC

Figure 33 shows a high-level architecture of deployment scenarios using E-LAN/E-Tree EVCs. Each small or macro eNodeB is connected to the CSR. The CSR can act as a Layer 3 or Layer 2 node. A single VLAN tag is shared across all UNIs between the CSR nodes and MAN (at UNI A). For this example, the UNI A tag is referenced as the IPsec VLAN.

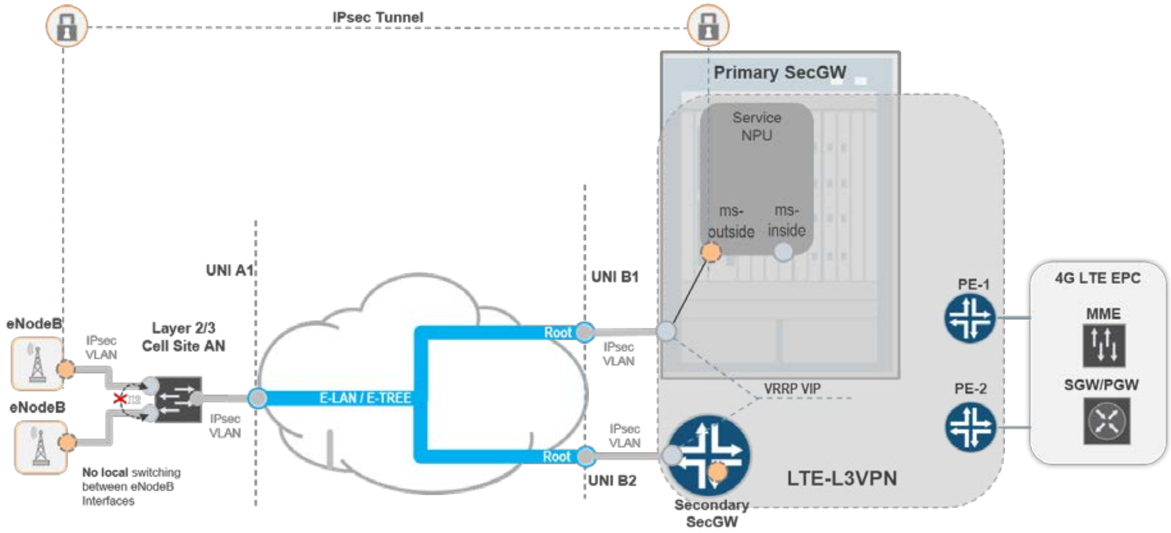


Figure 33 – Aggregating eNodeB IPsec Tunnels Over Leased E-LAN EVCs

Aggregation routers are connected to the MAN at UNI B1 and UNI B2, with one EVC or multiple EVCs bundled at physical port. The aggregation router performs VLAN demultiplexing and maps the IPsec VLAN to the Layer 3 IFL (interface logical units). The IFL is located on top of the physical Gigabit Ethernet or 10 Gigabit Ethernet UNI port of the MX Series router.

In case the primary SecGW fails, and to provide resiliency for the traffic flows from eNodeB, you should include adjacent pairs of IFLs on both of the aggregation routers into the dedicated VRRP group. Layer 2 bridging over E-LAN/E-Tree EVC allows VRRP adjacency to be established for each group.

Locate the IPsec gateway function into the Layer 3 VPN of the AG routers. The recommended configuration for the IPsec gateway in this scenario is similar to what was previously described in the IPsec gateway distributed scenarios with pseudowires in access mode with following noted differences:

- Pseudowires are replaced with E-Line EVC.
- The lt-interface is replaced with logical IFLs on top of physical port.

IPsec GW Resiliency with Wholesale MBH

Previous scenarios in this document described three examples of how you can arrange the IPsec tunnel switchover in the MBH network depending on the eNodeB capabilities:

- Single tunnel model
- Dual tunnel model with DPD
- Dual tunnel model with DFD

Note: All design considerations and recommended configurations provided in the previous scenarios apply to the wholesale deployment scenarios.

The single tunnel model includes two configured security gateways, which uses the same IP address for the IPsec gateway function. Without additional configuration, each gateway considers itself as the primary gateway, and attempts to serve IPsec packets destined to the IP address as soon as packets are received within the Layer 3 VPN. If the physical UNI interface between the primary AG router and the metro area network (MAN) (UNI-B in Figures 30, 31, 32, and 33) fails, or if the UNI-A (in Figure 30) fails, IPsec tunnels may need to be reestablished to the backup SecGW. The central location SecGW may terminate a few thousand tunnels at one physical UNI port causing the complete restoration of all tunnels to take a significant amount of time. Additionally, any flapping events of the interface may cause a serious service disaster.

To avoid this situation, select one of the following suggested workarounds:

- Workaround 1 **–** Move the IPsec gateway function from the aggregation routers directly connected to the MAN to the service edge router. Using this design, you deploy the IPsec gateway using the same method as described in Scenario 1.1 with no restrictions regarding UNI failure scenarios.
- Workaround 2 **–** Deploy a Junos opt script at the primary and backup IPsec gateways for additional control of the IPsec gateway function:
  - Primary IPsec gateway: Controls the status of its own service NPU. If the corresponding NPU goes down, then the IP level configuration for the ms-interface is deactivated.
  - Backup IPsec gateway: Controls the availability of the interfaces on the primary IPsec GW. If the primary SecGW is unavailable, then the configuration for the local ms-interface is activated.

To control the status of the forwarding plane between UNI-A and UNI-B1/UNI-B2, you can use the Ethernet OAM (CFM) or BFD protocols.

Note: Configuration for these protocols is out of scope for this document.

SCTP Policing in a MBH Network

In a 4G LTE mobile network, the S1 control plane interface (S1-MME) is defined between the eNodeB and MME and uses the S1 application layer protocol (S1-AP) to communicate between them. The application layer protocol is located on top of the Stream Control Transmission Protocol (SCTP) which functions the same way as the TCP or UDP protocols. (see Figure 34).

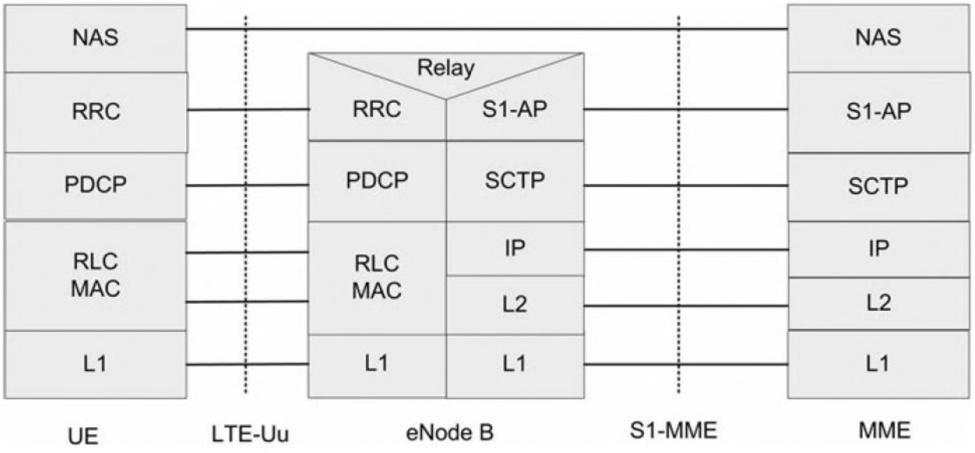


Figure 34 – Protocol Stack for the S1-MME Interface

The 4G LTE network's security provides protection for the MME node from DDoS attacks initiated by malware running on a subscriber's mobile terminal caused by an extensive S1-AP signaling between the eNodeB and MME node.

When placed into a mobile backhaul network, the MX Series platform can simply and effectively control the amount of SCTP traffic traveling between a single eNodeB and MME, or between groups of eNodeBs and MMEs. The solution uses standard, stateless `family inet` filters on the MX Series router. You can create a simple filter with a match condition for the SCTP protocol and destination IP prefix list to filter the SCTP traffic towards the MME node. The filter action is a single-rate color unaware policer with CIR and burst-size. (The values used for the CIR and maximum size in the CLI code snippet are examples; the actual values are described later.) You apply the filter to the forwarding table of the S1 routing-instance. You can use this configuration for both cases: with or without the IPsec gateway configured at the pre-aggregation or aggregation node.

CLI Code Snippet 1: Setting Up SCTP Policing on the IPsec GW

```
user@device02# show firewall
family inet {
    filter FW_SCTP_MME {
        term 1 {
            from {
                destination-prefix-list {
                    MME-LIST;
                }
                protocol sctp;
            }
            then {
                policer 10M;
                count SCTP_Counter;
                accept;
            }
        }
    }
}
```

```
policer 10M {
    if-exceeding {
        bandwidth-limit 10m;
        burst-size-limit 15k;
    }
    then discard;
}
```

```
user@device02# show routing-instances 4G-S1-L3VPN
instance-type vrf;
interface lt-0/0/10.15;
interface lo0.3;
route-distinguisher 192.0.2.2:103;
vrf-import PL-VPN-4G-MNG-IMP;
vrf-export PL-VPN-4G-MNG-EXP;
vrf-table-label;
routing-options {
    aggregate {
        route 198.51.100.1/24 discard;
        route 203.0.113.1/24 discard;
    }
    multipath {
        vpn-unequal-cost equal-external-internal;
    }
}
forwarding-options {
    family inet {
        filter {
            output FW_SCTP_MME;
        }
    }
}
```

Note: You may want to optimize how to filter traffic towards the MME by configuring the source/destination class usage (SCU/DCU) on the MX Series router. This may be more complex when you use zero time provisioning. However, if you add a new MME into the operator network, it eliminates the need for any extra provisioning of the security gateway firewall filters. This is useful for a distributed security gateway model that has multiple gateway configured across the aggregation and core network. This solution involves using a standard BGP community for the EPC and MME prefixes announced in the network.

Addressing Other Network Security Threats

Protecting the MBH Infrastructure from DDoS Attack

By deploying IPsec encryption for the S1, X2, and Mobile Network OAM traffic with SCTP filtering, you can protect elements of the mobile network from different types of attacks. However, the mobile backhaul networks infrastructure itself is vulnerable to attacks from various malicious sources. These attacks can be passive, where a network intruder intercepts data traveling through the network (such as, wiretapping); or active, where an intruder initiates commands to disrupt the normal operation of the network (such as, denial of service attacks or address spoofing). This solution for the secured MBH network includes preventing and monitoring of: unauthorized access, network misuse, unauthorized network modification, and attacks that result in the denial of network services, or network-accessible resources.

It is crucial that you implement measures to protect infrastructure elements. The design elements described here are not service-specific; but rather apply to all MBH services.

The following threats apply to the infrastructure elements:

- Unauthorized access to the routing and switching nodes of the MBH infrastructure. If you do not protect a network correctly, the integrity of the network is at risk of being accessed by unauthorized outsiders.
- Various software and hardware security flaws (such as, vulnerabilities in the TCP stack implementation that enable an attacker to terminate arbitrary BGP sessions).
- IP hijacking (injecting routes). Even if you assign or allocate IP addresses, it does not mean that the devices to which you have assigned the addresses, are actually using the addresses. In some cases, hackers can hijack the addresses and use them to inappropriately route traffic, spam, or implement distributed denial-of-service (DDoS) attacks.
- Distributed Denial of Service (DDoS). Within this design guide’s context, a DDoS attack is any attempt to compromise the control plane of the routing nodes of the MBH infrastructure, including: SCR, AG1, AG2, AG3, or PE-routers. Distributed DDoS attacks involve an attack from multiple sources which enables a larger amount of traffic to attack the network. The attacks typically use network protocol control packets to trigger a large number of exceptions to the router’s control plane resulting in excessive processing loads that disrupt normal network operations.

Protecting Against Unauthorized Access

You can mitigate unauthorized access, and other software and hardware security flaws by implementing the following:

- Limit management access to various network elements. These limitations include physical access and network access, such as: loopback filter configuration, TACACS+/RADIUS authorization, and allow/deny expressions for certain user groups.
- Disable all control protocols that are not used by implementing secure communication for management access. You can use the following forms of secure communication:
  - Secure shell (SSH)—Devices in this solution support the SSH protocol as a secure alternative to telnet for system administration.
  - Secure Copy (SCP)—Based on the SSH protocol, SCP file transfer securely and reliably transfers files between a local host and a remote host, or between two remote hosts (available only for Canada and U.S. versions of Junos OS software).
- Hide infrastructure elements from the end user. For example, at the PE router level, you can hide provider routers by disabling time to live (TTL) propagation from the IP packet header into the MPLS shim header.

Protecting Against Hijacking Threats

To mitigate hijacking threats, you can configure authentication for most control protocols used in the network, such as: LDP, ISIS, OSPF, BGP, or RSVP-TE.

Protecting Against Spoofing

You can use unicast reverse path forwarding (uRPF) to limit IP address spoofing on a network. When you configure uRPF on an interface, the router checks the source address of incoming packets against the routing table. If the router can reach the source address of the incoming packet using the same interface on which it was received, the router allows the packet. However, if the router cannot reach the source address of the incoming packet using the same interface, the router drops the packet. Configuring uRPF on an interface provides protection again spoofed packets that contain unverifiable source addresses.

Protecting Against DoS Attacks

A denial of service attack that targets the control plane of a network element is one of the most complex security threats to manage. For VPN services, the provider edge (PE)-to-customer edge (CE) interface connection (for example, eNodeB to SCR, or EPC to AG3, or PE router. in case of the MBH network) is the most vulnerable location for these attacks. For example, an excessive rate of legitimate host-bound packets coming from a user can affect the processing of other user requests, and eventually result in the tearing down of control, or routing protocol sessions that ultimately lead to traffic loss.

MX Series routers have a hierarchy of built-in (and sometimes non-configurable) control plane protection mechanisms that operate at different levels. These protection mechanisms are contained in the Routing Engine, the line card host processor, and the network processor.

ACX Series routers offer less protection mechanisms. As a result, Juniper Networks recommends, that in addition to configuring the embedded DDOS protection, you also configure loopback filters on both ACX Series and MX Series routing nodes across the MBH network.

You configure loopback filters to block control protocol traffic from unknown sources, or from unauthorized traffic to the Routing Engine, limit eligible traffic to avoid DoS attacks at the control plane.

Appendix A – Supported Standards and Features

IPsec Functions Supported on the MX Series

- Internet Key Exchange (IKE and IKEv2)
- Quick/Main/Aggressive modes for SA setup
- Public Key Infrastructure (PKI)
  - Automatic certificate enrollment using SCEP
  - Manual certificate import
  - Per-service set trusted Certificate Authorities
  - Supports Certificate Revocation Lists (CRLs)
- DPD based tunnel redundancy
- IPv6 Support (starting with Junos OS Release 13.3)
- Service sets style
  - Policy based IPSec
  - Route and link-based IPsec
- Encryption Algorithms (RFC 2405, RFC 2410)
  - AES (128, 192, and 256 bits)
  - 3DES
  - DES
  - Null
- Authentication Hash Algorithms (RFC 2403, RFC 2404)
  - Message Digest 5 (MD5)
  - SHA-1
  - SHA-2 256 (HMAC versions)
  - Fully-qualified domain name (FQDN)

IPsec Supported RFCs

- RFC 2085 - HMAC-MD5 IP Authentication with Replay Prevention
- RFC 2403 - The Use of HMAC-MD5-96 within ESP and AH
- RFC 2405 - The ESP DES-CBC Cipher Algorithm with Explicit IV
- RFC 2410 - The NULL Encryption Algorithm and Its Use with IPSec
- RFC 2451 - The ESP CBC-Mode Cipher Algorithms
- RFC 2460 - Internet Protocol, Version 6 (IPv6)
- RFC 3193 - Securing L2TP using IPsec
- RFC 3602 - The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3947 - Negotiation of NAT-Traversal in the IKE
- RFC 3948 - UDP Encapsulation of IPsec Packets
- RFC 4301 - Security Architecture for the Internet Protocol (Obsolete 2401)
- RFC 4302 - IP Authentication Header (Obsolete 2402)
- RFC 4303 - IP Encapsulating Security Payload (ESP) (Obsolete 2406)
- RFC 4305 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) (Obsolete 2406 and 2404)
- RFC 4306 - Internet Key Exchange (IKEv2) Protocol (Obsolete 2407, 2408, and 2409)
- RFC 4307 - Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308 - Cryptographic Suites for IPsec Suite B (supported with Junos OS Release 14.1)
- RFC 4835 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)"
- RFC 5996 - Internet Key Exchange Protocol Version 2 (IKEv2)

Partially Compliant

- RFC 3526 - More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 5114 - Additional Diffie-Hellman Groups for Use with IETF Standards
- RFC 5903 - Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2

Appendix B – Network Sizing

Mobile Backhaul Network Sizing

Each regional metro network connects to the national IP and MPLS core through an AG3 edge router. Each regional network with 10,000 access nodes may or may not have its own directly connected EPC. If an EPC is not installed in a particular geographical region, then an EPC at the remote provider edge at the national point of presence (POP) is used for that region (see Figure 1).

Figure 35 and Table 7 represent the number of access nodes across a regional network segment: access, pre-aggregation, aggregation, or core.

Table 7 – Sample Network Segment Size

	AG3-Nodes	AG2-Nodes	AG1-Nodes	CSRs	Macro Cells, N_M	Small Cells, N_S	UNIs	IPsec Tunnels
Per Region	2	32	1024	10240	10240	51200	61640	X2: 61440 S1: 61440
Per AG3	-	32	1024	10240	10240	51200	61640	X2: 61440 S1: 61440
Per AG2 Ring	-	2	64	640	640	3200	4040	X2: 3840 S1: 3840
Per AG1 Ring	-	-	4	40	40	200	160	X2: 240 S1: 240
Per Adjacent Pair of AG1 Routers			2	20	20	100	80	X2: 120 S1: 120

Figure 35 shows sixteen pairs of AG2 aggregation routers interconnected with edge routers AG3.1 and AG3.2 using direct 10 GB Ethernet links. On the other side, each aggregation router pair (AG2.1 with AG2.2, and AG2.3 with AG2.4, and so on) interconnects sixteen pre-aggregation rings. Each pre-aggregation semi-ring consists of four pre-aggregation (PRE-AGG) routers (AG1.1, AG1.2, AG1.3, AG1.4, and so on) interconnected with 10 GB Ethernet links. Finally, each pair of pre-aggregation AG1 routers interconnects four access rings with five CSRs in each access ring. To estimate the number of small cells, this example assumes the ratio of macro and small cells to be 1:5. A group of small cells connects to the MBH network through the dedicated CSR router. Table 7 shows the number of nodes of each type in each segment, and the number of access nodes aggregated at each aggregation and pre-aggregation level. Table 7 also summarizes the number of IPsec tunnels to support if tunnels terminate at particular network segment or node.

The CSRs within a ring are connected by optical Gigabit Ethernet or 10 Gigabit Ethernet links, or by microwave lines.

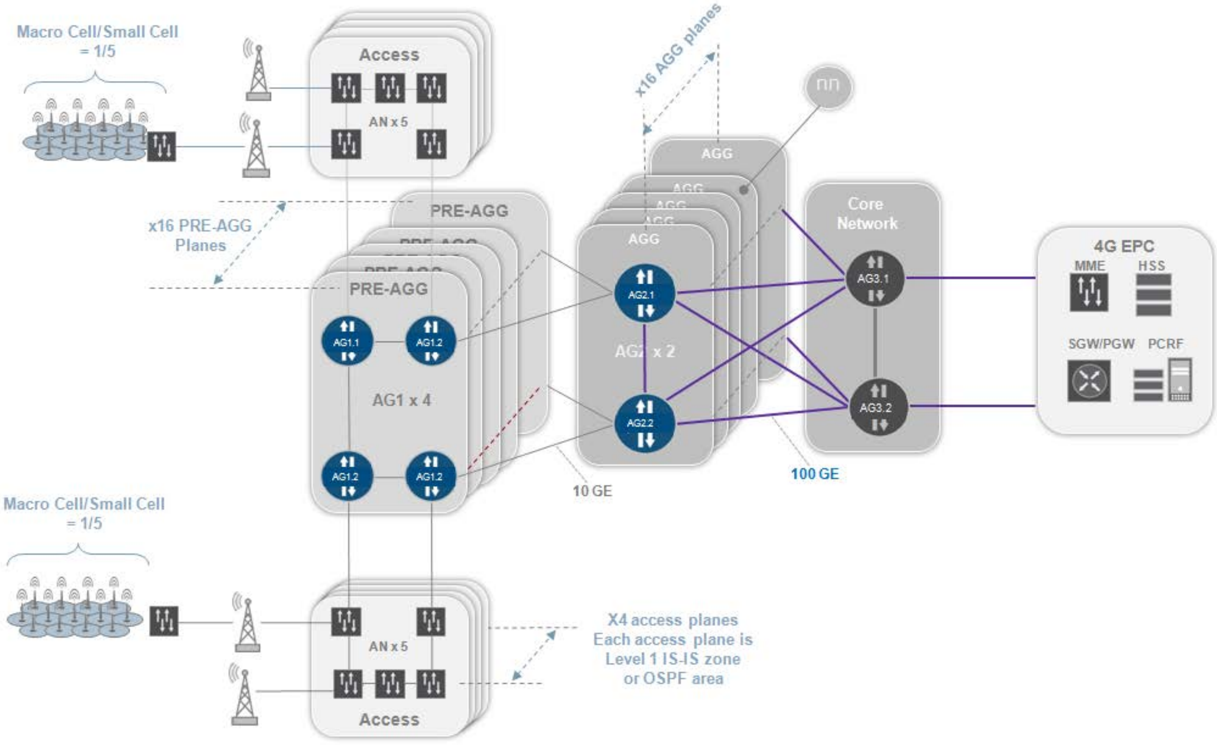


Figure 35 – Mobile Backhaul Network Sizing

Estimates of the traffic amount generated by the small and macro eNodeBs in wireline, and traffic aggregated in the access, aggregation, and core segments are based on the assumptions and methodology proposed in: https://www.ngmn.org/uploads/media/NGMN_Whitepaper_Small_Cell_Backhaul_Requirements.pdf and http://www.ngmn.org/uploads/media/NGMN_Whitepaper_Guideline_for_LTE_Backhaul_Traffic_Estimation.pdf.

Two characteristics of the eNodeB are defined regarding throughput: maximum available bandwidth $(\mathrm{BW}_{\mathrm{MAX}})$ and efficient throughput per eNodeB (BW). See Table 8.

Table 8 – Assumptions About Small and Macro Cell Traffic

Type of Cell	BW_{MAX}, MaxTput per Cell, Up/Down, Mbps	BW_U//BW_D, Efficient Tput per Cell at Pick Hour, Up/Down, Mbps	I_{STAT}, Index of Statistical Multiplexing		
			Pre-Agg Segment	Agg Segment	Core Segment
Macro Cell-1	50/150	20/20	1	0.5	0.3
Small Cell-1	50/150	30/30	0.5	0.25	0.2
Macro Cell-2	150/400	30/30	1	0.5	0.3
Small Cell-2	150/400	50/50	0.5	0.25	0.2

Two types of small cell and macro cell are considered regarding throughput characteristics: cell-1 and cell-2.

The maximum throughput for the single eNodeB is essential for the last mile planning and is not part of this this solution. This solution assumes that the last mile bandwidth is large enough to meet the requirements of the bandwidth table 8. To avoid overestimating the aggregated traffic, this solution adds a coefficient of the statistical multiplexing per network segment and different type of cells. The X2-U traffic requires about 5% of the S1 traffic bandwidth.

The total bandwidth of the IP traffic aggregated by one SecGW equals:

- S1 bandwidth: $S1\_BW_{SecGW} = N * I_{STAT} * (BW_U + BW_D)$
- X2 Bandwidth: $X2\_BW_{SecGW} = 0.05 * S1\_BW_{SecGW}$

This solution assumes that management and OAM bandwidth is negligible. The final requirements for the SecGW's total throughput depends on its locations. Tables 9, 10, and 11 provide summaries of, and given indexes of the statistical multiplexing in the packet MBH network.

Table 9 – Aggregated Traffic at AG1 Level

Scenario	Number of IPsec tunnels	BW_{S1}, per tunnel, Mbps	BW_{X2}, per tunnel, Mbps	BW_{S1}, Total, Mbps	BW_{X2}, Total, Mbps	BW, Total, Mbps
Macro Cell-1	20	40	2	800	40	840
Small Cell-1	100	30	1.5	3000	150	3150
Macro Cell-2	20	60	3	1200	60	1260
Small Cell-2	100	40	2	4000	200	4200

Table 10 – Aggregated Traffic at AG2 Level

Scenario	Number of IPsec tunnels	BW_{S1}, per tunnel, Mbps	BW_{X2}, per tunnel, Mbps	BW_{S1}, Total, Mbps	BW_{X2}, Total, Mbps	BW, Total, Mbps
Macro Cell-1	640	20	1	12800	640	13440
Small Cell-1	3200	15	0.75	48000	2400	50400
Macro Cell-2	640	30	1.5	19200	960	20160
Small Cell-2	3200	20	1	64000	3200	67200

Table 11 – Aggregated Traffic at AG3 Level

Scenario	Number of IPsec tunnels	BW_{S1}, per tunnel, Mbps	BW_{X2}, per tunnel, Mbps	BW_{S1}, Total, Mbps	BW_{X2}, Total, Mbps	BW, Total, Mbps
Macro Cell-1	10240	12	0.6	122880	6144	129024
Small Cell-1	51200	12	0.6	614400	30720	645120
Macro Cell-2	10240	18	0.9	184320	9216	193536
Small Cell-2	51200	16	0.8	819200	40960	860160

The bandwidth throughput provided is for the IMIX traffic for the pick load hours.

As of Junos OS Release 13.3, a single MX Series chassis or a single pair of the redundant MX Series routers cannot provide the requirements listed in Table 11. The data listed in Table 11 exceeds the current system's maximum values for maximum allowed number of IPsec tunnels and maximum IPsec throughput per chassis with multiple MS-MPC cards installed on the MX Series. Assuming the existing model and current level of performance of a single MS-MPC card, the system reaches its limit at the performance side before limitations of the tunnel scale become consequential. To meet the requirements for the IPsec GW at the national POP location with about 10,000 IPsec tunnels, you should use multiple chassis at the location.

Note: Combining multiple chassis within one virtual chassis does not add scale to the current model of the IPsec implementation on MX Series platform.

Performance and Scaling Parameters of the Solution

Tables 12, 13, and 14 contain performance, scaling, and network restoration time parameters expected in different deployment scenarios regarding the router integrated IPsec function.

- Table 12 - Distributed SecGW deployment scenarios apply to: Distributed SecGW Scenario 1.1; Distributed SecGW Scenario 1.2, and Small Cell SecGW Scenario 1.3.
- Table 13 - Semi-distributed SecGW deployment scenarios
- Table 14 - Centralized SecGW scenarios

Table 12 – Performance and Scaling Parameters for Distributed SecGW Scenarios

	IPsec tunnels S1/X2	Total IMIX BW, Gbps	Time to repair in case of different failures events			Recommended Platform
			IPsec GW	MS-MIC/ MS-MPC	Line Card	
Macro Cell-1	20/20	0.84	TBD*	TBD*	TBD*	MX80/ MX104/ MX240/MX480
Macro Cell-2	20/20	1.26	TBD*	TBD*	TBD*	
Small Cell-1	100/100	3.15	TBD*	TBD*	TBD*	MX104/ MX240/MX480
Small Cell-2	100/100	4.2	TBD*	TBD*	TBD*	
Macro Cell X2 only	0/20	0.04	TBD*	TBD*	TBD*	MX80/ MX104/ MX240/MX480
Small Cell X2 only	0/100	0.06	TBD*	TBD*	TBD*	

*Note 1: The expected value for time to repair depends on the availability of the HA feature set for the IPsec GW.

Table 13 – Performance and Scaling Parameters for Semi-Distributed SecGW Scenarios

	IPsec tunnels S1/X2	Total IMIX BW, Gbps	Time to repair in case of different failures events			Recommended Platform
			IPsec GW	MS-MIC/ MS-MPC	Line Card	
Macro Cell-1	640	13.44	TBD*	TBD*	TBD*	MX240/ MX480/ MX960
Macro Cell-2	640	20.160	TBD*	TBD*	TBD*	
Small Cell-1	3200	50.4	TBD*	TBD*	N/A	MX480/ MX960
Small Cell-2	3200	67.2	TBD*	TBD*	N/A	
Macro Cell X2 only	640	0.96	TBD*	TBD*	TBD*	MX240/ MX480/ MX960
Small Cell X2 only	3200	3.2	TBD*	TBD*	TBD*	

* Note 1: The expected value for time to repair depends on the availability of the HA feature set for the IPsec GW.

S1 and X2 traffic is not split into different IPsec tunnels in these scenarios until the S1 and X2 tunnels terminate on different IPsec gateways.

Table 14 – Performance and Scaling Parameters for Centralized SecGW Scenarios

	IPsec tunnels S1/X2	Total IMIX BW, Gbps	Time to repair in case of different failures events			Recommended Platform
			IPsec GW	MS-MIC/ MS-MPC	Line Card	
Macro Cell 1	1323	100	TBD*	TBD*	TBD*	MX480/ MX960/ MX1010/2020
Small Cell 1	6615		TBD*	TBD*	TBD*	
Macro Cell 2	972	100	TBD*	TBD*	TBD*	MX480/ MX960/ MX1010/2020
Small Cell 2	4860		TBD*	TBD*	TBD*	

* Note 1: The expected value for time to repair depends on the availability of the HA feature set for the IPsec GW.

Appendix C – MX Series IPsec GW Architecture

This appendix provides an overview of the internal architecture of the MX Series router regarding the IPsec gateway function. This overview describes the basic processes and hardware components used on the MX Series to establish IPsec tunnels, and how to scale the system. It also provides information about how different software functions on the MX Series router may affect each other when deploying a router integrated SecGW on top of the MBH network.

Router Integrated SecGW Architecture

A modern IP/MPLS network is usually built with a layered approach where the service plane is decoupled from the transport plane. This approach is widely used to establish an end-to-end seamless MPLS network. As soon as you establish the IP/MPLS transport and service infrastructure, you can build an additional IPsec tunnel infrastructure on top of the network.

The security layer, and transport and service infrastructure layers are largely independent of each other. Routing systems are built using a similar approach. A dedicated software process and hardware components within the routing system are responsible for each of the layers. The main components of the MX Series routing system are:

- Routing Engine
- Packet Forwarding Engine (PFE)
- Network Processing Unit (NPU)

The Routing Engine contains multiple processes that control and manage the IP/MPLS layers. The central component is the routing processing daemon (rpd) which builds the routing table, and the sends the table into the Packet Forwarding Engine of the router. In Junos OS Release 14.1, the Routing Engine also hosts the key management process (kmd) daemon which establishes an IPsec security association (SA) with the remote IPsec gateways. kmd negotiates the IPsec phases with the remote gateway and sends the forwarding states into the service NPU.

The Packet Forwarding Engine establishes a packet forwarding data plane within the system. Any network service (such as: VLAN, MPLS LSP, Layer 2 VPN, Layer 3 VPN, VPLS, PWE, traffic filtering and policing) and operations with those forwarding states, are served in silicon by the Packet Forwarding Engine.

The NPU processes packets and traffic flows for the following services *only*: stateful firewall, IPsec, NAT, ALG, and Jflow. Juniper Networks routing systems have used NPU for a long time with increasing performance levels. Relatively simple functions, such as one-to-one NAT, and Jflow (IPFix), have been ported into the Trio Packet Forwarding Engine of the MX Series router so NPUs are no longer required.

The Packet Forwarding Engine is physically located on multiple router line cards. Many different types of line cards can provide non-blocking performance for a single MX Series routing system with up to 1 Tbps per slot. The NPU is represented by three types of service cards on the MX Series router:

- MS-DPC
- MS-MIC
- MS-MPC

Only the MS-MICs and MS-MPCs are qualified for the router integrated SecGW solution. Figure 36 shows the available deployment options for MS-MIC and MS-MPC with different MX Series platforms.

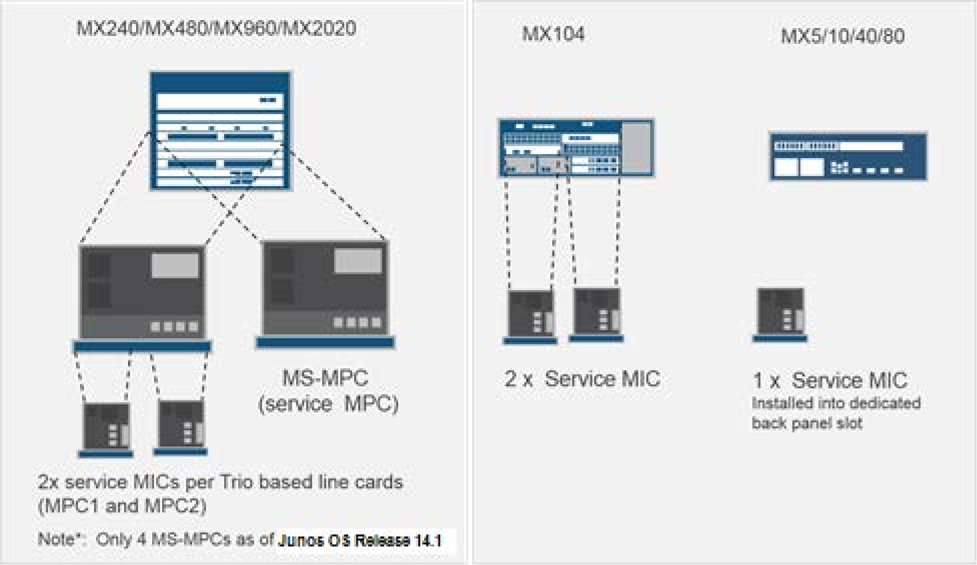


Figure 36 – MS-MPC and MS-MIC Deployment Options with Different MX Series Platforms

Each MS-MPC hosts four independent NPUs that provide up to 26 Gbps of encrypted data throughput for each line card (6 Gbps per NPU) of the IMIX traffic. The MS-MIC has only one NPU and provides throughput of approximately 4.5 Gbps of encrypted data.

Note: For more detailed performance data for different traffic patterns, contact your local Juniper Networks representative teams.

The multiservice (ms-) interface forwards traffic within a Junos OS-based router. Each NPU in the Junos OS-based router is recognized as a physical ms-interface that you can configure with multiple logical interfaces similar to how you would configure regular media interfaces. You can assign a logical interface to particular service rules or policies, such as NAT, firewalls, IPsec, and so on. You then apply the logical interface to any packet arriving at a given ms-interface. For more details, click https://www.juniper.net/techpubs/en_US/junos14.1/information-products/pathway-pages/services-interfaces/index.html

When traffic is forwarded to and from the IPsec tunnel that terminates on a router integrated IPsec gateway on an MX Series router, Figure 37 shows how packet forwarding is arranged within the routing system.

For clear text data arriving from the EPC on the inbound interface of the SecGW:

1. Packets arrive on the inbound interface.
2. The ingress Packet Forwarding Engine classifies packets to the appropriate forwarding class based on the Behavior Aggregate (BA) classifier that you configure using the `class-of-service` hierarchy.
3. Layer 2 through Layer 4 stateless firewall filters (if any) and policers are applied as traffic enters a logical interface (IFL) at the Packet Forwarding Engine level. For example, you can apply SCTP protocol policing at this point.

4. The following two options of how to process packets are available:

   - **Service-set style forwarding** (not depicted in Figure 37)**:** A service filter is applied to the traffic at the Packet Forwarding IFL. If traffic matches the filter conditions, then traffic is forwarded to the service NPU (a particular logical unit of the ms-interface). The NPU applies the service policy to the packets based on the service-set configuration, which is part of the service filter.

   - **Next-hop style forwarding:** This option is shown in Figure 37 and is recommended for Mobile SecGW scenarios. If no service-filters are applied at the IFL, then the Packet Forwarding Engine does a route lookup in the VRF table. Packets are processed based on the information from the forwarding table of the Packet Forwarding Engine. An appropriate VRF is selected based on the routing instance to which the ingress interface belongs, or based on the vrf-table-label for MPLS packets. The table may contain routing records showing the inside ms-interface unit as a next-hop. All qualified traffic is forwarded to an NPU and processed according to the service-set attached to the logical unit (IFL) of the ms-interface.

5. The NPU encrypts traffic, adds the IPsec header, and sends it back to the Packet Forwarding Engine.
6. The Packet Forwarding Engine performs an IP address destination lookup in its forwarding information base, and then forwards the packet to the egress Packet Forwarding Engine.
7. Packets are processed according to the output Layer 2 through Layer 4 stateless firewall filters (if any), and CoS shaping and queuing rules at the outbound interface.

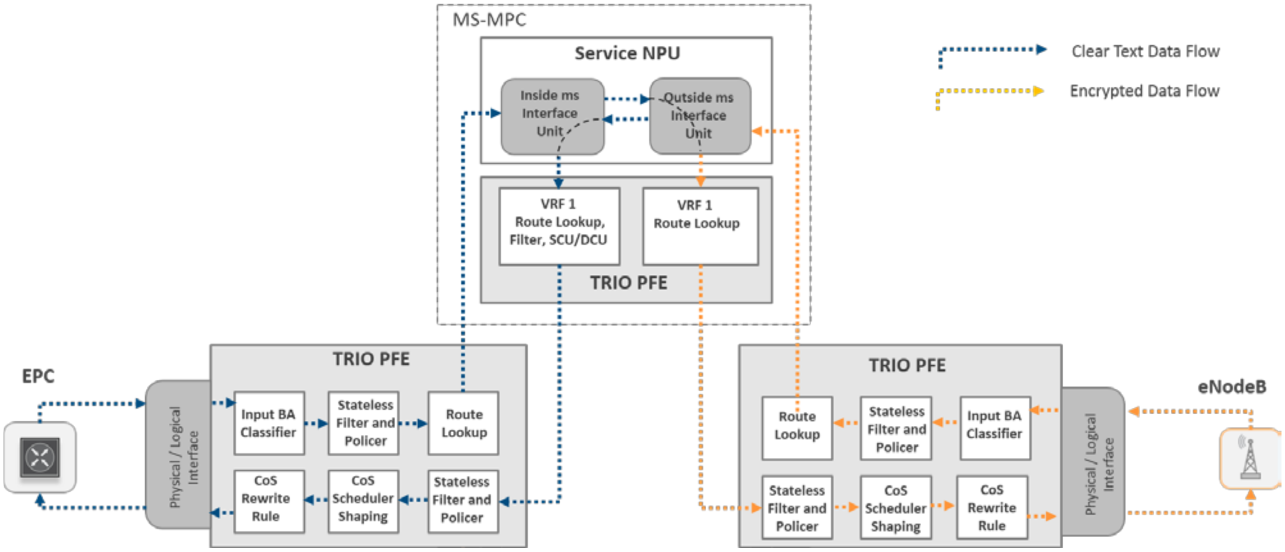


Figure 37 – Router Integrated IPsec Gateway Architecture and Traffic Flows Passing Through

For encrypted traffic coming on from eNodeB:

1. Packets arrive on the physical interface of the ingress Packet Forwarding Engine.
2. The ingress Packet Forwarding Engine classifies packets to the appropriate forwarding class based on the Behavior Aggregate (BA) classifier that you configure using the `class-of-service` hierarchy.
3. Layer 2 through Layer 4 stateless firewall filters (if any) and policers are applied as traffic enters a logical interface (IFL) at the Packet Forwarding Engine level. For example, you can apply SCTP protocol policing at this point.

4. The Packet Forwarding Engine performs a destination IP address lookup in the VRF table, and qualifies packets destined to the IPsec gateway function based on the destination IP address in the IPsec header. An appropriate VRF is selected based on the routing instance to which the ingress interface belongs, or based on the vrf-table-label for MPLS packets. Packets are then sent to the particular NPU (the outside logical unit of the ms-interface).
5. The NPU decrypts the traffic and then sends clear text traffic back to Packet Forwarding Engine.
6. The Packet Forwarding Engine performs a destination IP address lookup and then forwards packets to the egress interface based on forwarding information base data. You can apply additional stateless filters at the forwarding information base level (such as, SCTP filtering). At this point, the filter may contain lookup information for the class usage (SCU/DCU). This provides a powerful and simple mechanism that enables you to apply filter rules to a dedicated type of traffic, such as to all S1-MME traffic destined to the MME.
7. At the egress IFL, packets are processed according to the output Layer 2 through Layer 4 stateless firewall filters (if any), and CoS shaping and queuing rules at the outbound interface.

Figure 38 shows at high-level a control plane process for establishing an IPsec tunnel between eNodeB and an IPsec gateway on a MX Series router.

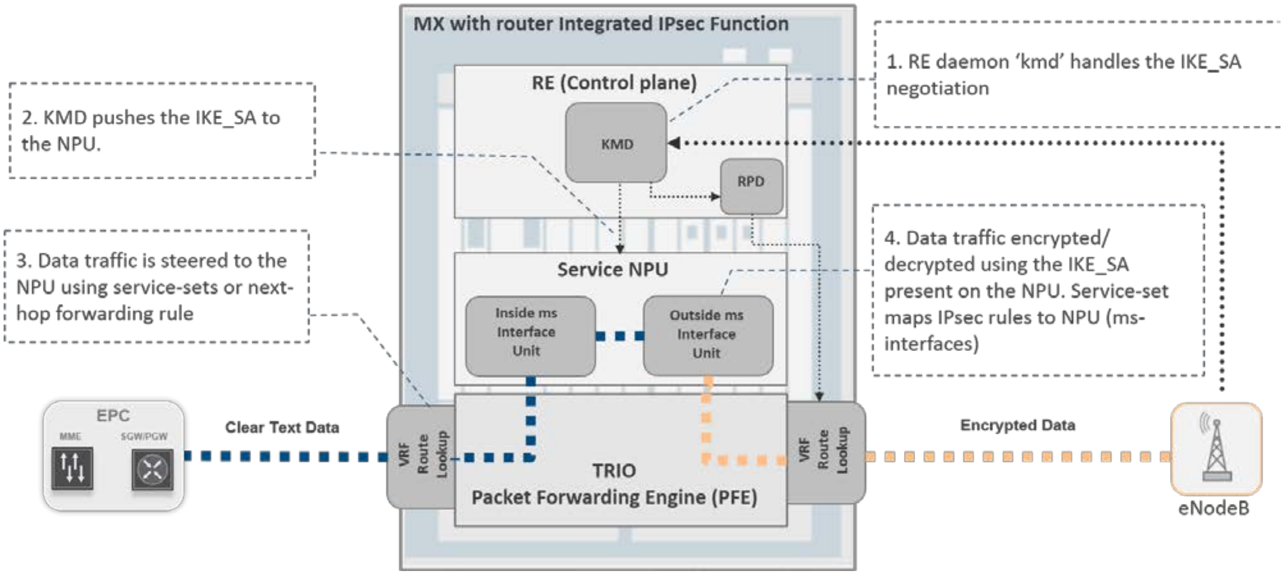

MX with router Integrated IPsec Function
RE (Control plane)
KMD
RPD
Service NPU
Inside ms Interface Unit
Outside ms Interface Unit
TRIO
Packet Forwarding Engine (PFE)
VRF Route Lookup
VRF Route Lookup
1. RE daemon 'kmd' handles the IKE_SA negotiation
2. KMD pushes the IKE_SA to the NPU.
3. Data traffic is steered to the NPU using service-sets or next-hop forwarding rule
4. Data traffic encrypted/ decrypted using the IKE_SA present on the NPU. Service-set maps IPsec rules to NPU (ms-interfaces)
EPC
MME
SGW/PGW
Clear Text Data
Encrypted Data
eNodeB

Figure 38 – Setting Up an IPsec Tunnel Between an IPsec Gateway and eNodeB

Quality of Service (QoS)

This secured MBH infrastructure solution follows the same guidelines for CoS planning as described in the *Mobile Backhaul Solution 1.0 Design Guide*.

In the IPsec gateway, when traffic flows through the network processing unit of the MS-MIC/MS-MPS module, it preserves the original value of the DSCP in the IP header. It also performs additional classification of the traffic based of the behavior aggregate classifier when the packet travels from the NPU to the Trio Packet Forwarding Engine of the line card.

Intrachassis Redundancy and Load Balancing

Intrachassis Redundancy

As previously described in this document, you can equip MX Series routers with multiple service NPUs to add more performance throughput for encrypted data, and provide resiliency. With current deployment model, the MX Series does not support intrachassis stateful high availability between different NPUs. Failure of any NPU within the routing node leads to the IPsec tunnel reestablishing with a different NPU, or more likely, with a secondary IPsec GW.

Figure 39 shows how kmd sends the IPsec SA state to a pair of redundant NPUs during the negotiation phase. Both NPUs are mapped to the same AMS group. Additionally, change the configuration of the IPsec gateway by replacing the ms interface with an ams-interface using the `service-set` and `routing-instance` configuration hierarchy levels.

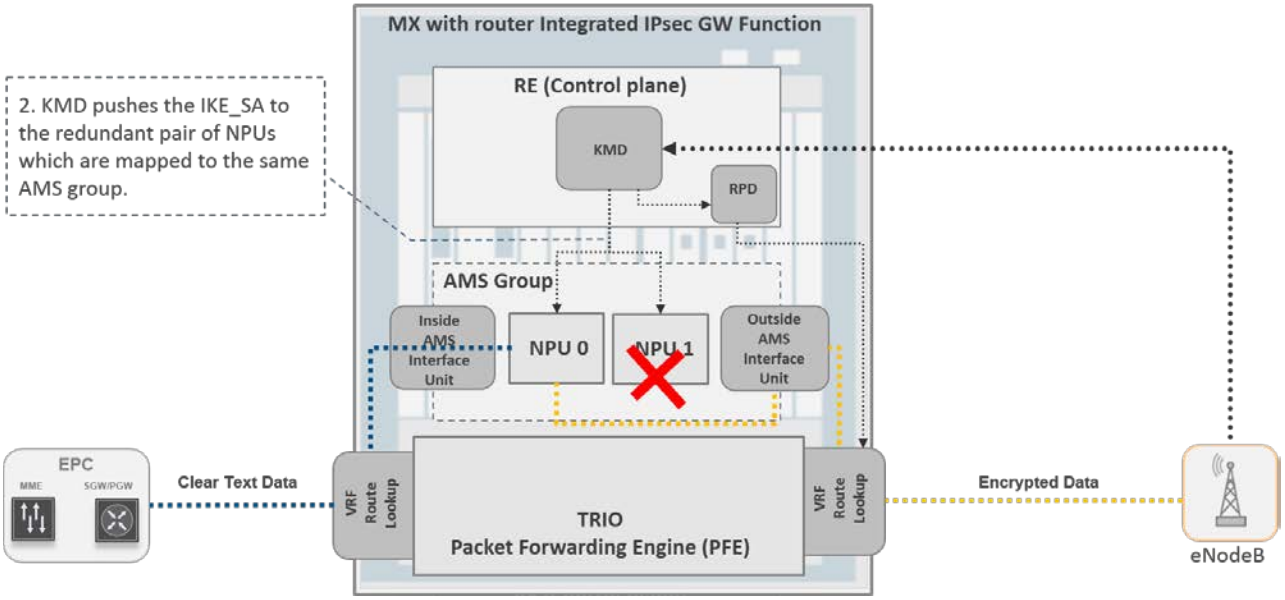

MX with router Integrated IPsec GW Function
2. KMD pushes the IKE_SA to the redundant pair of NPUs which are mapped to the same AMS group.
RE (Control plane)
KMD
RPD
AMS Group
Inside AMS Interface Unit
NPU 0
NPU 1
Outside AMS Interface Unit
EPC
MME
SGW/PGW
Clear Text Data
VRF Route Lookup
TRIO
Packet Forwarding Engine (PFE)
VRF Route Lookup
Encrypted Data
eNodeB

Figure 39 – Intrachassis IPsec Function Stateful HA

Intrachassis IPsec Tunnels Load Balancing

With the Junos OS Release 14.1 deployment model, you plan and configure manually the IPsec tunnel distribution between different NPUs. To achieve load balancing, you configure multiple IPsec gateways (one per NPU, or one per redundant pair of NPUs, in future release) inside the MX Series router. Each IPsec gateway has its own dedicated IP address and a qualified DN name. You configure end points (eNodeB) with an appropriate remote IPsec gateway IP address to terminate its tunnel on a given NPU.

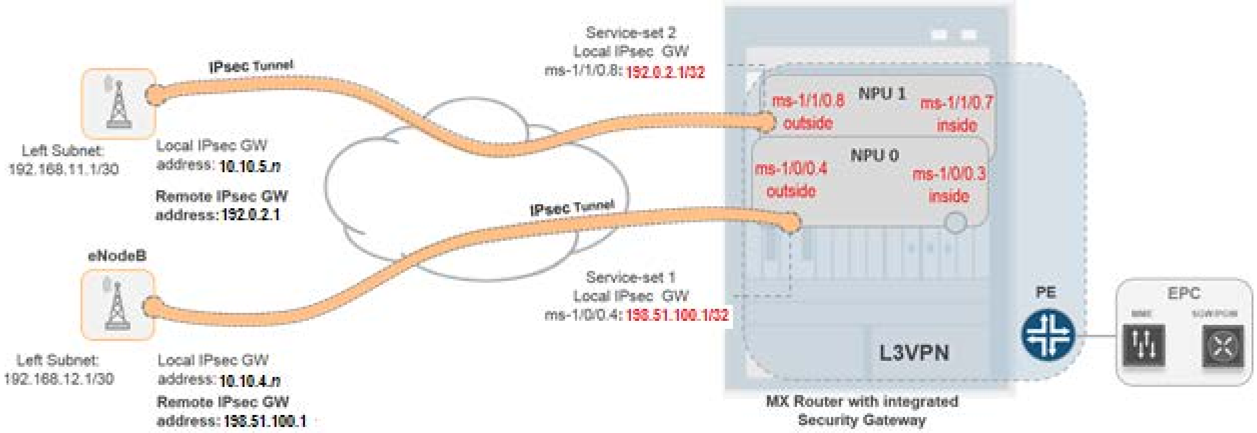
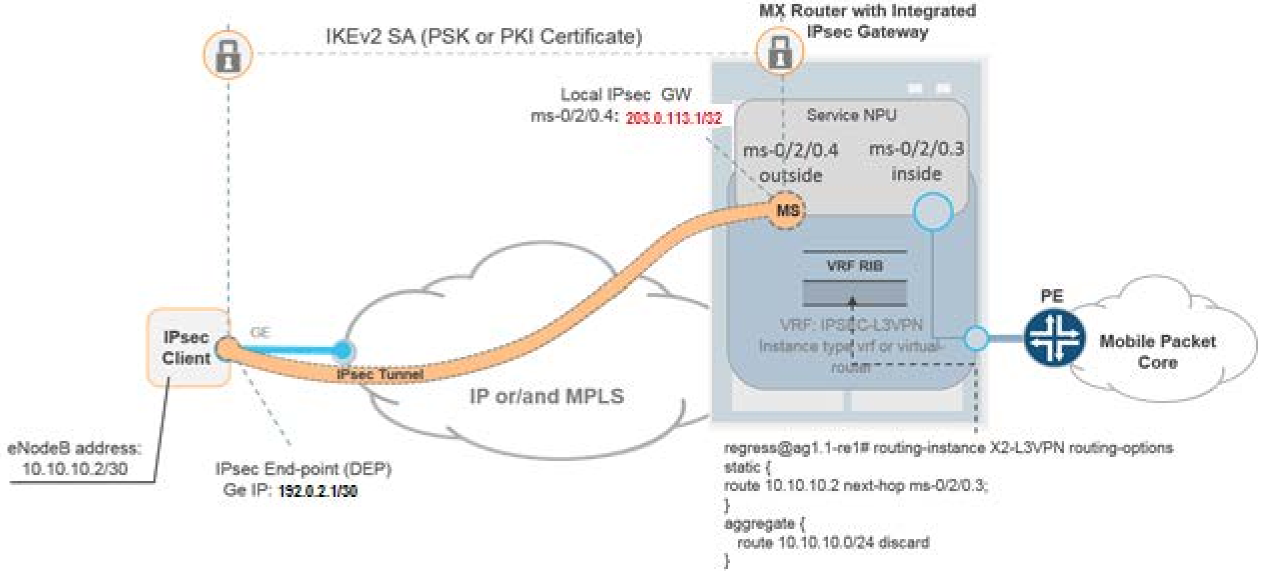


Figure 40 – Load Balancing IPsec Tunnels Across NPU (with Junos OS 14.1 Release)

This solution is applicable for distributed SecGW scenarios when the routing node is equipped with a few NPUs. However, for a semi-distributed or centralized deployment model, this approach may lead to extra provisioning costs. Future development may address this issue by providing an automated load balancing mechanism for the MX Series.

Appendix D – Configuration Examples

Point-to-Point IPsec Gateway Tunnel Configuration Example



```
regress@ag1.1-re1# routing-instance X2-L3VPN routing-options
static {
route 10.10.10.2 next-hop ms-0/2/0.3;
}
aggregate {
  route 10.10.10.0/24 discard
}
```

Figure 41 – MX Series Router with Point-to-Point Static IPsec Tunnel

CLI Code Snippet 2: IPsec Protocol Configuration on MX Series Router: AG1.1

```
user1@ag1.1# show services ipsec-vpn
rule IKE-HW-SECGW {
    term SECGW {
        from {
            source-address {
                0.0.0.0/0;
            }
            destination-address {
                10.10.10.0/30;
            }
        }
        then {
            remote-gateway 192.0.2.1;
            dynamic {
                ike-policy IKE-HW-SECGW-POLICY;
                ipsec-policy IPSEC-HW-SECGW-POLICY;
            }
            no-anti-replay;
            tunnel-mtu 2000;
            inactive: initiate-dead-peer-detection;
            inactive: dead-peer-detection {
                interval 5;
                threshold 5;
            }
        }
    }
    match-direction input;
}
ipsec {
    proposal IPSEC-HW-SECGW-PROPOSAL {
        protocol esp;
        authentication-algorithm hmac-sha1-96;
        encryption-algorithm aes-128-cbc;
        lifetime-seconds 3600;
    }
    policy IPSEC-HW-SECGW-POLICY {
        proposals IPSEC-HW-SECGW-PROPOSAL;
    }
}
ike {
    proposal IKE-HW-SECGW-PROPOSAL {
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm sha1;
        encryption-algorithm aes-128-cbc;
        lifetime-seconds 86400;
    }
    policy IKE-HW-SECGW-POLICY {
        version 2;
        remote-id fqdn IKE;
        proposals IKE-HW-SECGW-PROPOSAL;
        local-id ipv4_addr 203.0.113.1;
        pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
    }
}
inactive: traceoptions {
    file IPsec size 100m;
    level all;
    flag ike;
    flag all;
}
establish-tunnels on-traffic;
clear-ike-sas-on-pic-restart;
clear-ipsec-sas-on-pic-restart;


[edit]
user1@AG1.1-re1# show services service-set HW-SECGW-SSET
next-hop-service {
    inside-service-interface ms-0/2/0.3;
    outside-service-interface ms-0/2/0.4;
}
ipsec-vpn-options {
    local-gateway 203.0.113.1 routing-instance X2-L3VPN;
    no-anti-replay;
}
```

Dynamic End Point (DEP) Configuration Example

DEP is a recommended method for a Mobile SecGW deployment because it significantly decreases the amount of provisioning efforts required to configure an IPsec tunnel for the dedicated eNodeB. In particular, when a new eNodeB is added into the Mobile network, no new configuration is required at the SecGW. The following configuration example shows how a SecGW provides an established IPsec tunnel with DEP.

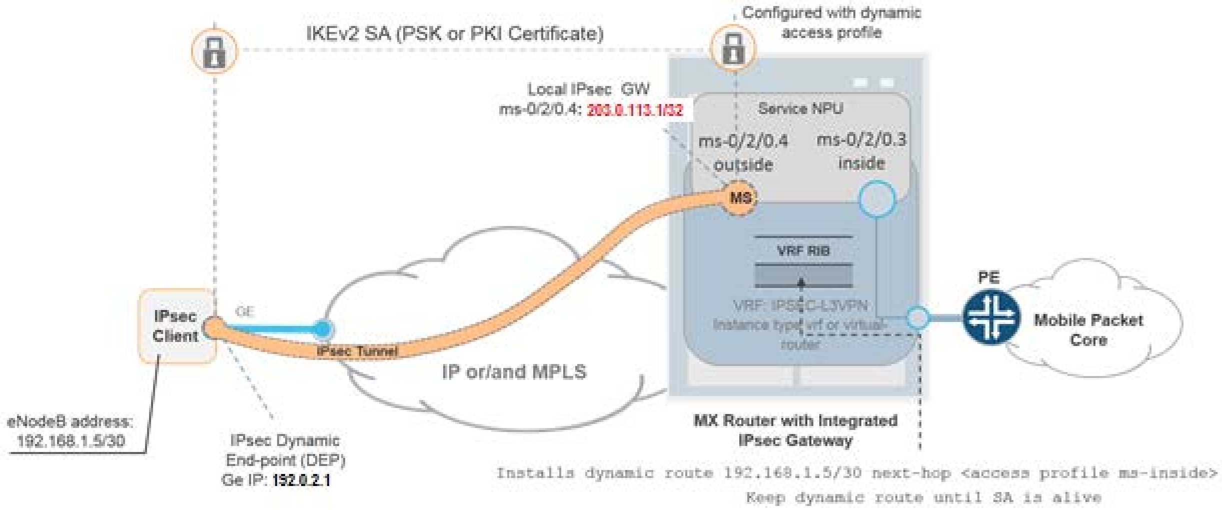

IKEv2 SA (PSK or PKI Certificate)
Configured with dynamic access profile
Local IPsec GW
ms-0/2/0.4: 203.0.113.1/32
Service NPU
ms-0/2/0.4
outside
ms-0/2/0.3
inside
MS
VRF RIB
VRF: IPSEC-L3VPN
Instance type vrf or virtual-router
PE
Mobile Packet Core
IPsec Client
GE
IPsec Tunnel
IP or/and MPLS
eNodeB address: 192.168.1.5/30
IPsec Dynamic End-point (DEP)
Ge IP: 192.0.2.1
MX Router with Integrated IPsec Gateway
Installs dynamic route 192.168.1.5/30 next-hop <access profile ms-inside>
Keep dynamic route until SA is alive

Figure 42 – IPsec GW with a DEP Model

CLI Code Snippet 3: IPsec Protocol Configuration on MX Series Router: AG1.1

```
user1@ag1.1# show interfaces ms-0/2/0
unit 3 {
    dial-options {
        ipsec-interface-id DYNAMIC-INTERFACE;
        shared;
    }
    family inet;
    service-domain inside;
}
unit 4 {
    family inet {
        address 203.0.113.1/32;
    }
    service-domain outside;
}
```

```
user1@ag1.1# show services
ipsec-vpn {
    ipsec {
        proposal AES128-SHA1-ESP {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
        }
        policy IPSEC-HW-SECGW-POLICY {
            proposals AES128-SHA1-ESP;
        }
    }
    ike {
        proposal RSA-G2-AES128-SHA1 {
            authentication-method pre-shared-keys;
            dh-group group2;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
            lifetime-seconds 86400;
        }
        policy IKE-HW-SECGW-POLICY {
            version 2;
            proposals RSA-G2-AES128-SHA1;
            local-id ipv4_addr 203.0.113.1;
            remote-id any-remote-id;
            pre-shared-key ascii-text "$ABC123"; ## SECRET-DATA
        }
    }
    traceoptions {
        file ike.log size 100m;
        level all;
        flag ike;
        flag all;
    }
    clear-ike-sas-on-pic-restart;
    clear-ipsec-sas-on-pic-restart;
}
service-set HW-SECGW-SSET-DEP {
    next-hop-service {
        inside-service-interface ms-0/2/0.3;
        outside-service-interface ms-0/2/0.4;
    }
    ipsec-vpn-options {
        local-gateway 203.0.113.1 routing-instance IPSEC-L3VPN;
        ike-access-profile DYNAMIC-VPN;
    }
}
```

```
user1@ag1.1# show access
profile DYNAMIC-VPN {
    client * {
        ike {
            ike-policy IKE-HW-SECGW-POLICY;
            ipsec-policy IPSEC-HW-SECGW-POLICY;
            interface-id DYNAMIC-INTERFACE;
        }
    }
}
```

```
user1@ag1.1# show routing-instances IPSEC-L3VPN
instance-type vrf;
interface ms-0/2/0.3;
interface ms-0/2/0.4;
interface lt-1/2/10.20;
interface lo0.4;
route-distinguisher 10.10.10.1:120;
vrf-target target:65001:120;
vrf-table-label;
routing-options {
    aggregate {
        route 203.0.113.0/24 discard;
    }
}
```

Multihop BFD for Static Route Configuration Example

CLI Code Snippet 4: IPsec Protocol Configuration on MX Series Router: AG1.1

```
user1@ag1.1# show routing-instances IPSEC-L3VPN
instance-type vrf;
interface ms-0/2/0.3;
interface ms-0/2/0.4;
interface xe-1/1/0.30;
route-distinguisher 10.10.10.1:120;
vrf-target target:65001:120;
vrf-table-label;
routing-options {
    static {
        route 192.168.12.1/32 next-hop ms-0/2/0.3;
        route 192.168.12.0/27 {
            next-hop 192.168.12.1;
            bfd-liveness-detection {
                minimum-interval 1000;
                no-adaptation;
                neighbor 192.168.12.1;
                local-address 192.168.13.5;
            }
            resolve;
        }
    }
    aggregate {
        route 203.0.113.0/24 discard;
    }
}
```

```
user1@ag1.1# show interfaces xe-1/1/0.30
description "Dummy Interface for IPsec bfd OAM";
vlan-id 30;
family inet {
    address 192.168.13.5/30;
}
```

Appendix E - References

The following references are provided:

- [1] NGMN Small Cell Backhaul requirements https://www.ngmn.org/uploads/media/NGMN_Whitepaper_Small_Cell_Backhaul_Requirements.pdf
- [2] Guidelines for LTE Backhaul Traffic Estimation http://www.ngmn.org/uploads/media/NGMN_Whitepaper_Guideline_for_LTE_Backhaul_Traffic_Estimation.pdf
- [3] Universal Access and Aggregation Mobile Backhaul Design Guide: http://www.juniper.net/us/en/local/pdf/design-guides/8020018-en.pdf
- [4] NGMN Optimized Backhaul Requirements
- http://www.ngmn.org/uploads/media/NGMN_Optimised_Backhaul_Requirements.pdf

Glossary

Table 15 lists the acronyms and definitions used within this document.

Table 15 – Acronyms and Definitions

Term	Description
2G	second generation
3G	third generation
3GPP	Third-Generation Partnership Project
4G LTE	fourth-generation Long Term Evolution (refers to 4G wireless broadband technology)
Abis	interface between the BTS and the BSC
ABR	area border router
AN	access node
ARP	Address Resolution Protocol
AS	autonomous system
ATM	Asynchronous Transfer Mode
BA	behavior aggregate (classifiers)
BBF	Broadband Forum
BCD	binary-coded decimal
BFD	Bidirectional Forwarding Detection (protocol)
BGP	Border Gateway Protocol
BGP-LU	BGP-labeled unicast
BN	border node
BS	base station
BSC	base station controller
BTS	base transceiver station
CapEx	capital expenditure
CE	customer entity or customer edge, depending on the context
CES	Carrier Ethernet Services
CESoPSN	Circuit Emulation Service over Packet-Switched Network
CET	Carrier Ethernet Transport
CFM	connectivity fault management
CIR	committed information rate
CLI	command-line interface
CO	central office

Term	Description
CoS	class of service
CSG	cell site gateway
CSR	cell site router
DCU	Destination Class Usage
DDOS	Distributed Denial of Service
DEP	Dynamic Endpoint
DSCP	Differentiated Services code point
EBGP	external BGP
eNodeB	Enhanced NodeB
EPC	evolved packet core
EVC	Ethernet Virtual Circuit
EXP bit	MPLS code point
FIB	forwarding information base
FRR	fast reroute (MPLS)
Gbps	Gigabits per second
GPS	Global Positioning System
GM	grandmaster
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSPA	high-speed packet access
H-VPLS	hierarchical VPLS
IBGP	internal BGP
IEEE	Institute of Electrical and Electronics Engineers
IGP	interior gateway protocol
IP	Internet Protocol
IPsec	Internet Protocol Security
IRB	Integrated Routing and Bridging
IS-IS	Intermediate system-to-Intermediate system
ISSU	in-service software upgrade
ITU	International Telecommunication Union
Iub	Interface UMTS branch—Interface between the RNC and the Node B
LAN	local area network

Term	Description
LDP	Label Distribution Protocol
LDP-DOD	LDP downstream on demand
LFM	link fault management
LSA	link-state advertisement
LSI	label-switched interface
LSP	label-switched path (MPLS)
LSR	label-switched router
LT	Logical Tunnel
LTE	Long Term Evolution
LTE-TDD	Long Term Evolution – Time Division Duplex
MBH	mobile backhaul
MC-LAG	multichassis link aggregation group
MEF	Metro Ethernet Forum
MF	multifield (classifiers)
MME	mobility management entity
MitM	man in the middle
MP-BGP	multiprotocol-BGP
MPLS	Multiprotocol Label Switching
MSC	Mobile Switching Center
MSP	managed services provider
NMS	network management system
NNI	network-to-network interface
NSR	nonstop routing
NTP	Network Time Protocol
OAM	Operation, Administration, and Management
OpEx	operational expenditure
OS	operating system
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PCU	Packet Control Unit
PE	provider edge
PGW	Packet Data Network Gateway
POP	point of presence

Term	Description
pps	packets per second
PSN	packet-switched network
PSTN	public switched telephone network (or telecom network)
PTP	Precision Timing Protocol
PWE3	IETF Pseudowire Emulation Edge to Edge
QoE	quality of experience
QoS	quality of service
RAN	Radio Access Network
RE	Routing Engine
RIB	routing information base, also known as routing table
RNC	radio network controller
RSVP	Resource Reservation Protocol
S1	Interface between the eNodeB and the SGW
SAFI	subsequent address family identifier
SAToP	Structure-Agnostic Time Division Multiplexing (TDM) over Packet
SCTP	Stream Control Transmission Protocol
SCU	Source Class Usage
SGSN	Serving GPRS Support Node
SGW	Serving Gateway
SH	service helper
SLA	service-level agreement
SMS	short message service
SN	service node
TD-CDMA	time division-code-division multiple access
TDD	time division duplex
TDM	time-division multiplexing
TD-SCDMA	time-division–synchronous code-division multiple access
T-LDP	targeted-LDP
TN	transport node
UMTS	universal mobile telecommunications system
UNI	user-to-network interface
UTRAN	UMTS Terrestrial Radio Access Network
VCI	virtual circuit identifier

Term	Description
VIP	Virtual IP
VLAN	virtual LAN
VoD	video on demand
VPI	virtual path identifier
VPLS	virtual private LAN service
VPN	virtual private network
VRF	VPN routing and forwarding (table)
VRRP	Virtual Router Redundancy Protocol
WCDMA	Wideband Code Division Multiple Access
X2	Interface between eNodeBs, or between eNodeB and the MME