



HPE Aruba Networking EdgeConnect SD-WAN – Business Intent Overlays and Link Bonding

Technical White Paper

Important Notice

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to [Aruba EULA](#).

Revision B, November 2023

Open Source Code:

Hewlett Packard Enterprise Company
Attn: General Counsel
WW Corporate Headquarters
1701 E Mossy Oaks Rd Spring, TX 77389
United States of America



Contents

1	Overview.....	5
2	Introduction to Business Intent Overlays and Network Segmentation	6
2.1	Business Intent Overlays.....	6
2.2	Network Segmentation with Virtual Routing and Forwarding (VRF)	7
2.3	Traffic Flow: SD-WAN Fabric or Internet.....	8
2.4	Terminology	9
3	Business Intent Overlay Orchestration.....	10
3.1	Traffic Match Criteria	11
3.1.1	Traffic Match – Overlay ACL.....	11
3.1.2	Traffic Match – LAN Port	12
3.1.3	Traffic Match – Appliance ACL	12
3.2	Internal Subnets.....	13
3.2.1	Consider Non-default Routes as Internal Subnets	14
3.3	SD-WAN Traffic to Internal Subnets.....	15
3.3.1	Topologies	16
3.3.2	Link Bonding Policy.....	18
3.3.3	QoS, Security, and Optimization.....	18
3.3.4	Service Level Objectives (Degraded or Down with Thresholds)	21
3.3.5	Build SD-WAN Using These Interfaces (Primary, Secondary, and Backup).....	22
3.4	Breakout Traffic to Internet & Cloud Services	26
3.4.1	Preferred Policy Order	26
3.4.2	Available Policies.....	27
3.4.3	Break Out Locally Using These Interfaces	27
3.4.4	Link Selection.....	27
3.4.5	Branch and Hub Settings.....	27
3.5	Regions.....	28
4	Link Bonding Policy on SD-WAN Fabric	30
4.1	Primary, Secondary vs. Backup and Service Level Objective	30
4.1.1	Add Secondary Underlay Tunnels (UTs).....	30
4.1.2	Add Backup Underlay Tunnels if Primary and Secondary UTs Are Degraded	31
4.2	Link Bonding Policy Attributes	32
4.2.1	Link Selection – Waterfall	32
4.2.2	Link Selection – Balanced	32
4.3	Forward Error Correction.....	33
4.4	Underlay Tunnel Eligibility, Selection, Link Scoring, and Utilization.....	33
4.4.1	Underlay Tunnel Eligibility Based on SLO	33
4.4.2	Degraded Underlay Determination When Exceeding Loss Threshold	34



4.4.3	Underlay Sorting	34
4.4.4	Underlay Selection.....	35
4.5	Underlay Tunnel Bandwidth Negotiation	36
4.6	End-to-End Overlay Mapping for SD-WAN Traffic	36
4.7	High Availability (HA) and High Quality (HQ) Operation	37
4.7.1	High Availability (HA) Link Bonding Policy Attributes	37
4.7.2	HA Operation Over a Single Link.....	37
4.7.3	High Quality (HQ) Link Bonding Policy Attributes.....	38
4.7.4	HA and HQ Example 1 – Payload Fits in Best UT.....	38
4.7.5	HA and HQ Example 2 – Payload “Waterfalls” to Next-best Link; FEC Moves to Third UT.....	39
4.7.6	HA and HQ Example 3 – 2 Underlay Tunnels; Payload + FEC Both Fit	39
4.7.7	HA and HQ Example 4 – 2 Underlay Tunnels; Payload + FEC Do NOT Fit	40
4.7.8	HA and HQ Example 5 – Utilization of a Browned-out Underlay Tunnel (R8.1.9.5+ Behavior)	40
4.8	High Throughput (HT) Operation.....	41
4.8.1	HT Use Case	42
4.8.2	Cross-connected Underlay Tunnels in HT Overlay	43
4.8.3	HT Example	43
4.9	High Efficiency (HE) Operation.....	44
4.9.1	HE Example	45
4.10	Custom Bonding Policy	45
4.10.1	FEC Wait Time (Default: 80ms)	46
4.10.2	Exclude Links (Default: On overlay brownout).....	46
4.10.3	Link Reorder Frequency (Default: Moderate).....	46
4.10.4	Path Conditioning (Default: Min 2% and Max 20%)	47
4.10.5	Packet Reorder Wait Time (Default: 100ms)	47
4.10.6	Link Selection (Default: Waterfall – Overall Quality)	47
5	Link Bonding Policy for Internet & Cloud Services.....	48
5.1	Break Out Locally	49
5.1.1	Break Out Locally Using These Interfaces	50
5.1.2	Passthrough Tunnel Eligibility for Local Breakout	51
5.1.3	Inferred Performance Metrics for Passthrough Tunnels.....	53
5.1.4	Link Selection.....	54
5.1.5	Session Affinity for Break Out Local Traffic	59
5.2	Service Tunnels	60
5.2.1	API-based Orchestrated Tunnels to Secure Web Gateway	61
5.2.2	Service Orchestration–based Orchestrated Tunnels to Secure Web Gateway	61
5.2.3	Path Selection for Orchestrated Service Tunnels.....	62
5.2.4	Manual Passthrough IPSec / GRE Tunnels	64



5.2.5	Path Selection for Manual Passthrough IPSec / GRE Tunnels.....	65
5.3	Backhaul via Overlay	66
5.3.1	LAN to External Flow – Backhaul via Overlay	66
5.3.2	LAN to External – Backhaul Flow: Peer Unavailable Scenario	67
5.3.3	WAN to External – Backhaul via Overlay	68
5.3.4	WAN to WAN Backhaul Flow – LAN-side Drain on the Receiving EdgeConnect	69
5.3.5	WAN to WAN Backhaul Flow – WAN-side Drain on the Receiving EdgeConnect.....	70
5.3.6	Advertising Internet Routes to Attract Internet Traffic.....	71
5.3.7	Bonding Policy and Path Selection for Backhaul Traffic	71
5.4	Hairpinning and Allow WAN-to-WAN Routing	72
6	Underlay Tunnel States, Settings, and State Behavior.....	74
6.1	Orchestrator Tunnel States	74
6.2	Live View	75
6.3	Global Tunnel Settings	76
6.4	Underlay Tunnel Degraded / Down States	77
7	Link Bonding Policy Recommendations	78



1 Overview

The Aruba EdgeConnect SD-WAN edge platform enables distributed enterprises to build a better WAN, securely connecting users to applications while increasing application performance. Aruba EdgeConnect is the premier SD-WAN solution for unifying the cloud, internet, and enterprise WAN into a single fabric. It provides enterprises with visibility and control over the new cloud-driven network while ensuring consistent performance for every enterprise and Software as a Service (SaaS) application.

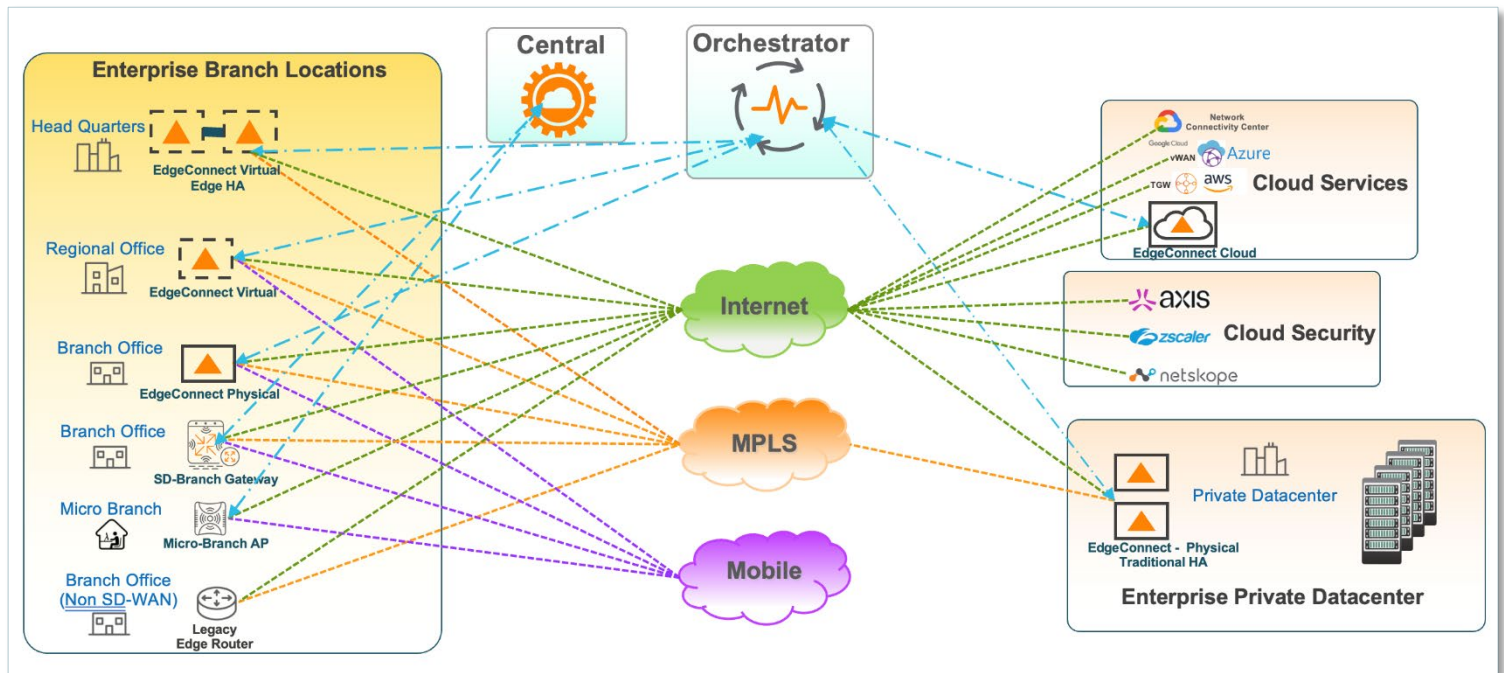


Figure 1 – EdgeConnect SD-WAN Architecture

EdgeConnect seamlessly utilizes various underlay transport options, including (but not limited to) Internet (Broadband, Fiber, Satellite), MPLS, and Wireless (4G/5G) in any desired combination, ensuring a consistent "network fabric" across diverse physical networks.

This document focuses on detailing various aspects of SD-WAN fabric connectivity, topologies, path selection, and error correction.



2 Introduction to Business Intent Overlays and Network Segmentation

The EdgeConnect SD-WAN platform is designed for end-to-end performance. Whether it is a branch connecting to a data center (private and/or public) using a hub-and-spoke topology, or branch-to-branch using a mesh topology, EdgeConnect monitors, evaluates, and acts to ensure the highest possible end-to-end performance.

2.1 Business Intent Overlays

Business Intent Overlays create virtual, end-to-end, network overlays that align application performance to underlying network resources.

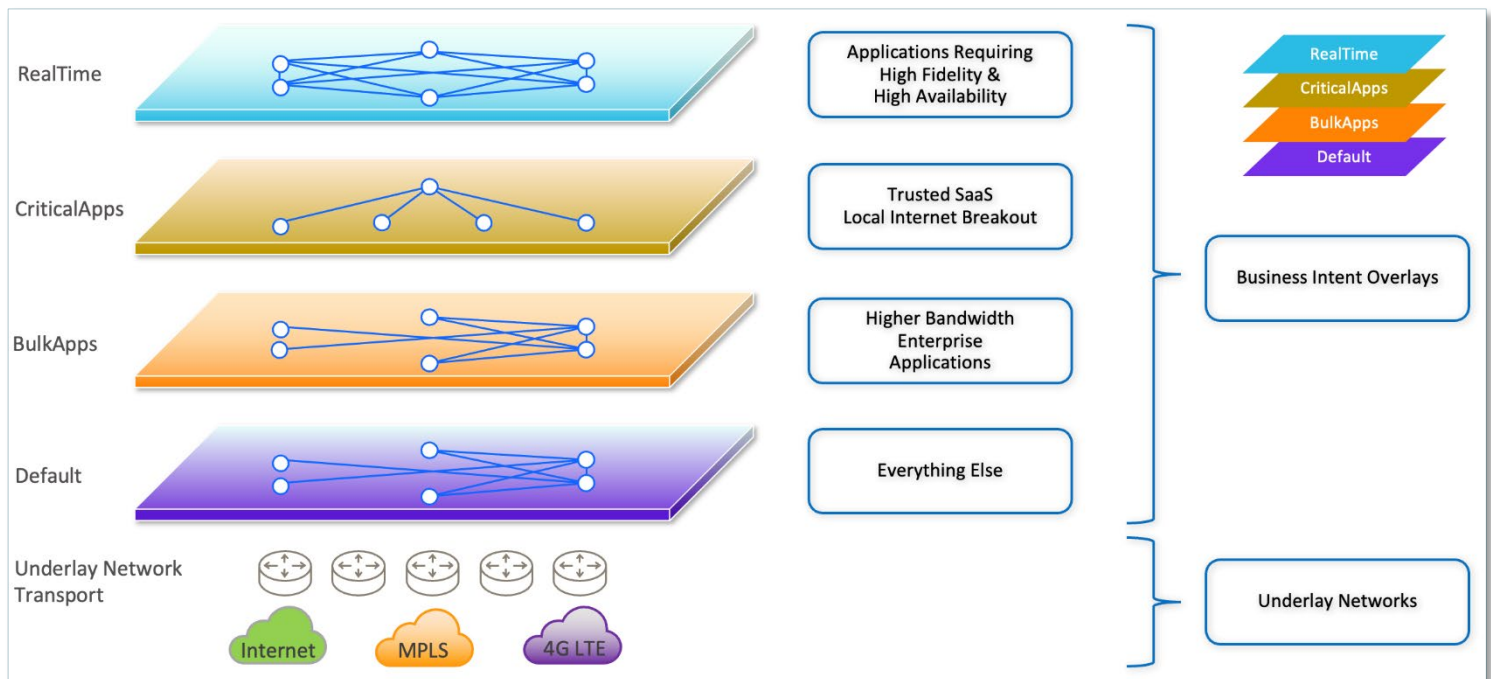


Figure 2 – Application Alignment to Business Intent Overlays

Each Business Intent Overlay can be visualized as mapping a set of applications to a network overlay where each overlay has:

- A specific topology
- Specific policies and network-level service objective attributes for traffic that routes on the SD-WAN fabric
- Specific policies and network-level service objective attributes for traffic that routes external to the SD-WAN fabric (typically known as Internet Breakout)
- Specific policies for cloud-based security



2.2 Network Segmentation with Virtual Routing and Forwarding (VRF)

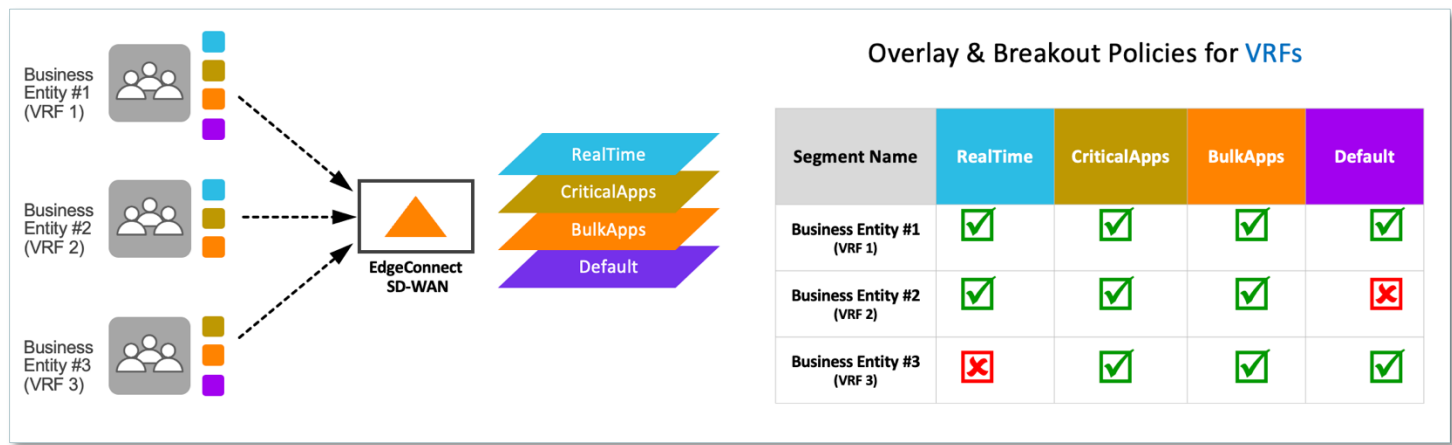


Figure 3 – Network Segmentation with VRFs

Many large enterprises want to use Business Intent Overlays as a “network Service Level Objective”, but still need network partitioning to meet various business objectives, including:

- Business unit segmentation
- Merger and acquisition transition process
- Security policies
- Compliance

The EdgeConnect platform supports advanced network segmentation with Virtual Routing and Forwarding (VRFs). Figure 3 above depicts an enterprise with three business entities that require network isolation. Each business entity has its application requirements that can be mapped to network service levels provided by Business Intent Overlays (BIOs). The figure above shows four BIOs:

- RealTime
- CriticalApps
- BulkApps
- Default

Each business entity maps its applications to some or all the BIOs. Figure 3 shows how EdgeConnect simply and intuitively maps network segments provided by VRFs to network-level service objectives provided by BIOs.



2.3 Traffic Flow: SD-WAN Fabric or Internet

In simplest terms, traffic is either bound for an EdgeConnect peer over the SD-WAN fabric (internal subnets) or external subnets such as internet or cloud services. When traffic matches a BIO's classification, the BIO contains policies for both internal and external traffic. BIO link bonding policy specifies all attributes for the use of both underlay tunnels (UTs) and overlay tunnels (OTs). As shown in the following figure, an overlay tunnel is a logical tunnel that uses the transport services of one or more underlay tunnels. The policies, attributes, and mechanisms for this process are explained in Sections 4 and 5.

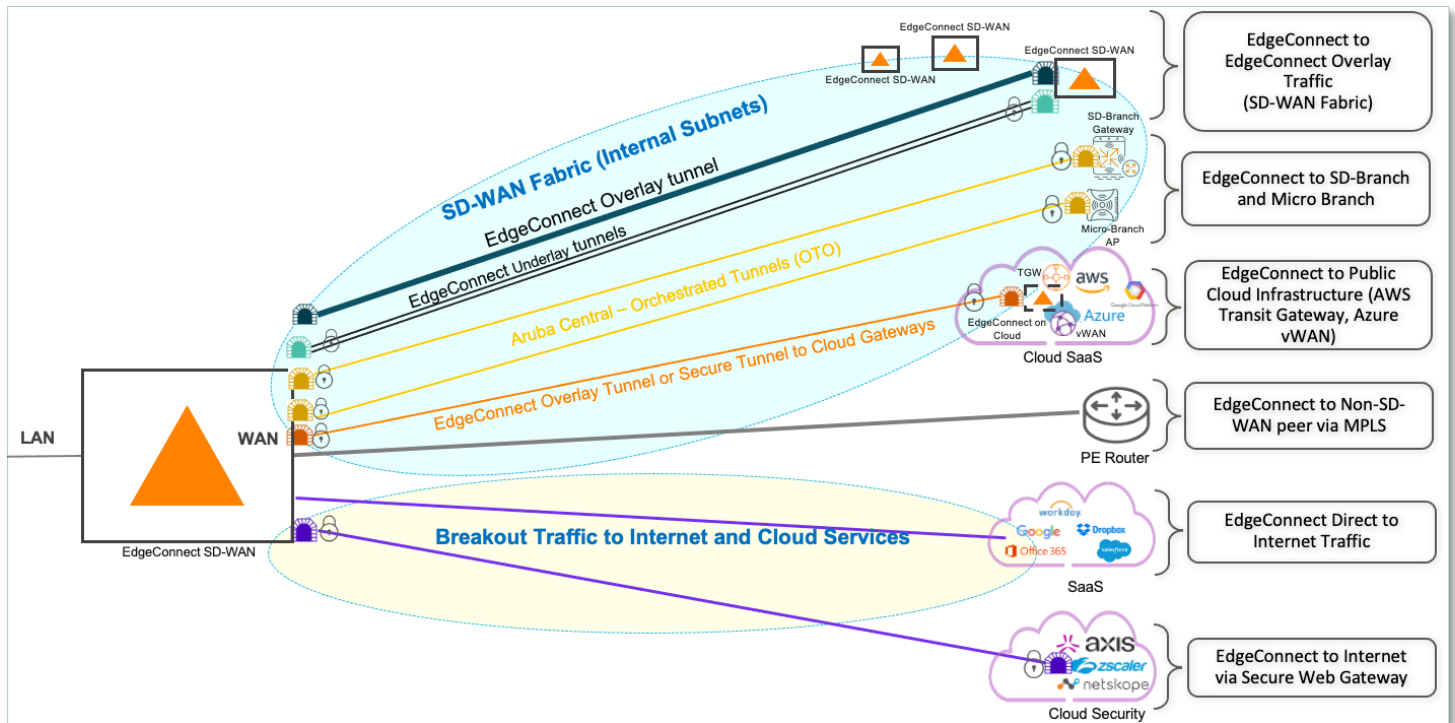


Figure 4 – EdgeConnect Traffic Forwarding

Internal traffic can be forwarded to its final destination based on where the destination is located. For example, internal destination traffic can be sent to:

- An EdgeConnect at the data center (hub) – overlay tunnel
- An EdgeConnect at a remote branch (spoke) – overlay tunnel
- An EdgeConnect in the cloud (EC-V-Cloud on AWS/Azure/Google, or other supported cloud) – overlay tunnel
- A SD-Branch Gateway (OTO tunnels)
- A Micro-Branch Access Point (OTO tunnels)
- A Cloud Gateway (Azure vWAN / AWS Transit Gateway / Google NCC...and so forth) – IPSec/GRE tunnels
- A PE router (legacy WAN sites) that connects via private MPLS/VPLS

External traffic (internet) can be sent to its final destination using the following transport paths:

- Passthrough tunnels using provisioned WAN connections for Local Internet Breakout traffic
- Passthrough tunnels to HPE SSE (Axis) or other third parties such as Zscaler or Netskope for cloud-based security services or to a Firewall or other Network Security Devices
- Backhauling traffic via overlay tunnels to an EdgeConnect (hub)



2.4 Terminology

The following table defines terms used in this document to achieve a consistent understanding.

Term	Definition
Aruba EdgeConnect	EdgeConnect refers to an SD-WAN appliance that can be in the form of a physical appliance or Virtual Network Function (VNF). EdgeConnect software refers to appliance-level software.
Aruba Orchestrator	Provides central management and orchestration of the SD-WAN fabric, which consists of a collection of EdgeConnect appliances.
Port (or Interface)	Bandwidth (Tx/Rx or Out/In) provisioned on EdgeConnect deployment configurations. Typically, these are provisioned to equal the service provider's circuit, but could be provisioned to be less than the advertised link speed.
Interface Label	Interface labels are generic labels associated with EdgeConnect WAN and LAN interfaces. Orchestrator builds tunnels between appliances with matching interface labels that belong to the same Business Intent Overlay. For example, an appliance can have WAN interface labels of Internet, MPLS, and LTE, and LAN interface labels of Data or Voice.
Virtual Tunnel Interface (VTI)	EdgeConnect 8.2.0 supports BGP over IPsec tunnels with Virtual Tunnel Interfaces (VTIs). You can configure VTIs via the Orchestrator "Configuration / VTI", and then add them as interfaces for BGP peers via "Configuration / BGP".
Loopback Interface	Loopback interfaces can be configured and advertised to the fabric to provide appliance reachability over the fabric from remote locations.
Secure Service Edge (SSE)	A cloud-based solution offering Firewall as a Service (FWaaS), Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and Secure Web Gateway (SWG).
Security Web Gateway (SWG)	Cloud-based gateways provide inspection of client traffic to enforce SSE policies.
Underlay Network	Underlay Networks are physical networks that provide Layers 1 through 4 of the OSI reference model. Layers 1 and 2 access methods include copper, fiber, and wireless. Layer 3 addressing can be public (Internet) or private (MPLS), and it can be IPv4 or IPv6.
Underlay Link (UL)	An underlay network construct that provides end-to-end Layer-3 connectivity.
Underlay Tunnel (UT)	An EdgeConnect-to-EdgeConnect IPsec encapsulated tunnel. Underlay tunnels are constructed by Orchestrator between EdgeConnect appliances that have matching provisioned interface labels (e.g., INET1, MPLS1) and belong to one or more of the same Business Intent Overlays (BIOs).
Overlay Tunnel (OT)	An overlay tunnel is constructed for a given EdgeConnect node pair that participate in each BIO. The overlay tunnel selects one or more underlay tunnels based on Link Bonding Policy and the underlay tunnel state (eligible, meeting service level objectives [Degraded], and UT status [up/down]) as described in this document. The overlay tunnel is a logical abstraction of the underlay networks, which greatly simplifies the wide area network and its operations.
Passthrough Tunnel (PT)	Passthrough tunnels are constructed between an EdgeConnect node and a peer service such as internet breakout or cloud-based firewall. For internet breakout, PT is a tunnel between the EdgeConnect appliance and the internet and can be thought of as a single-ended tunnel. For cloud services, a PT can be an IPsec encapsulated tunnel between the EdgeConnect appliance and the peer host in the cloud service such as Azure Virtual WAN or Zscaler cloud security service.



3 Business Intent Overlay Orchestration

The following Orchestrator figure illustrates the single-pane-of-glass provisioning model for EdgeConnect Business Intent Overlays (BIOs).

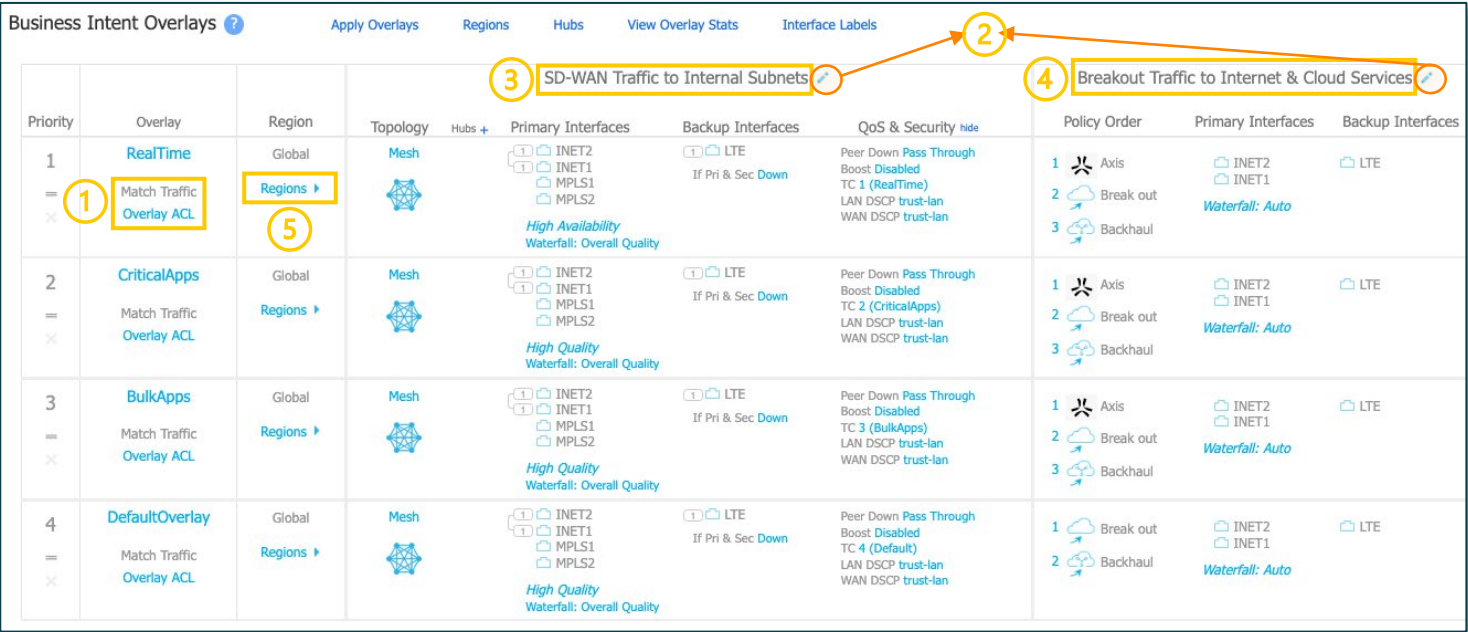


Figure 5 – Business Intent Overlay Orchestration

All overlays are displayed in a single summary panel showing overlay priority, name, and two primary traffic categories: **“SD-WAN Traffic to Internal Subnets”** (SD-WAN traffic to other EdgeConnect appliances) and **“Breakout Traffic to Internet & Cloud Services”** (internet-bound traffic).

The following sections detail the key components of the Business Intent Overlay orchestration page.

- 1. Traffic Match Criteria (see section 3.1)
- 2. Internal Subnets (see section 3.2)
- 3. SD-WAN Traffic to Internal Subnets (see section 3.3)
- 4. Breakout Traffic to Internet & Cloud Services (see section 3.4)
- 5. Regions (see section 3.5)

The second column shows four BIOs for this example network: RealTime, CriticalApps, BulkApps, and DefaultOverlay. These are typical examples.

NOTE: Orchestrator supports up to **seven** BIOs.



3.1 Traffic Match Criteria

The **Match Traffic** section defines selecting which traffic is handled by a given BIO. There are three ways traffic can match an overlay: Overlay ACL (Access List), LAN Port, or Appliance ACL.

It is recommended that you use Overlay ACL to configure traffic match criteria policies because this method orchestrates the policy across SD-WAN fabric appliances.

3.1.1 Traffic Match – Overlay ACL

Overlay ACL defines the criteria for the traffic to match **a particular Business Intent Overlay**. Traffic can be matched by intuitive Application Groups and/or Applications, and can be granularly specified by DSCP, IP, Port, user-role, username, and so forth. If the traffic is matched to a particular BIO, it follows the bonding policies mapped to that BIO. If the traffic is not matched, it moves to the next Overlay ACL for a policy match until it matches one. When no matching overlay is found for a given traffic, that traffic is subjected to default route policy (65535).

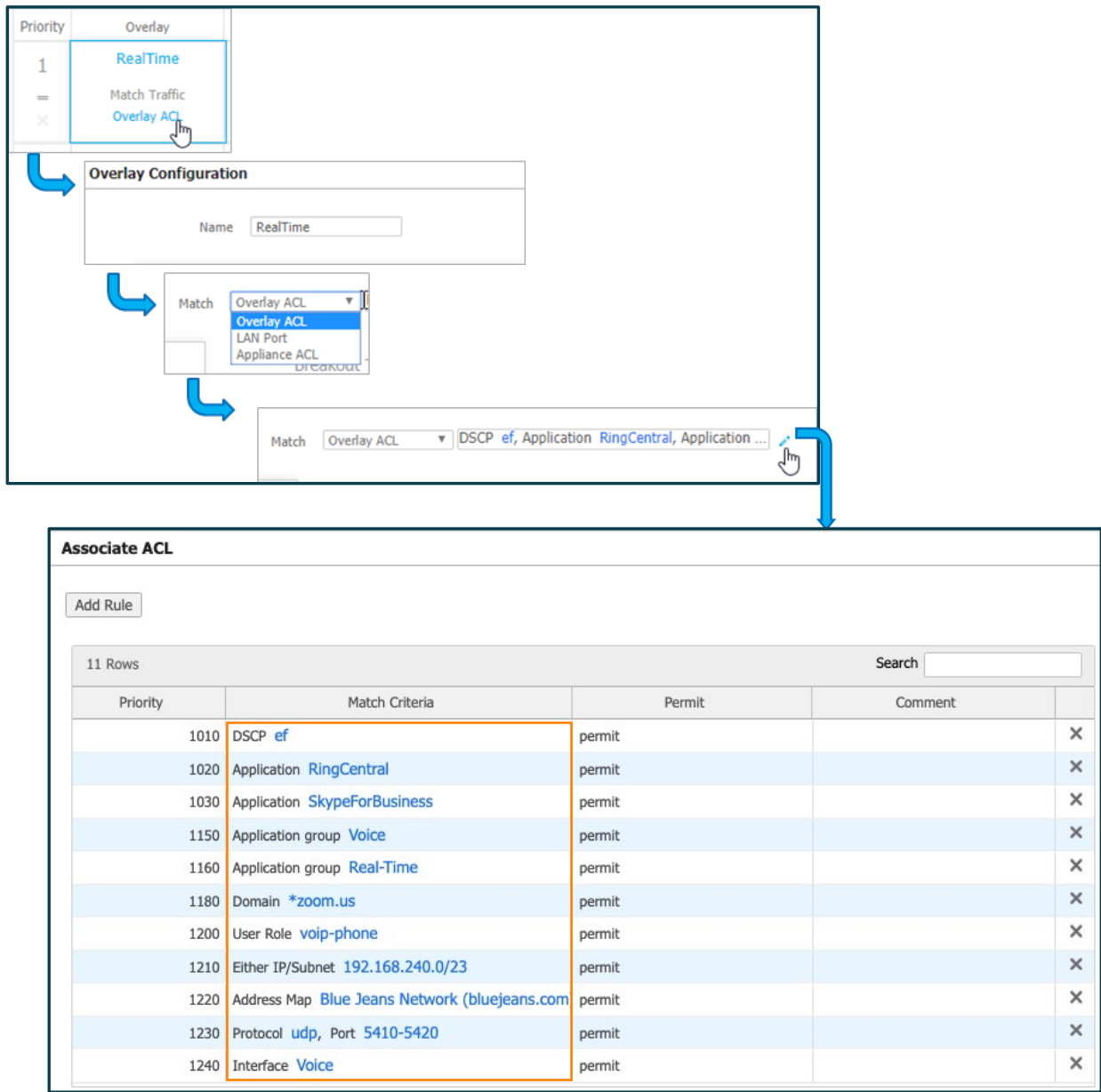


Figure 6 – Traffic Match Using Overlay ACL Policy

3.1.2 Traffic Match – LAN Port

You can configure traffic match using a simple LAN label. Any traffic arriving on the matching source LAN interface (label) will be matched and subjected to the BIO.

NOTE: Only one label can be selected using this method. Therefore, it is recommended that you use “Overlay ACL”, which enables you to enter multiple LAN interface labels.

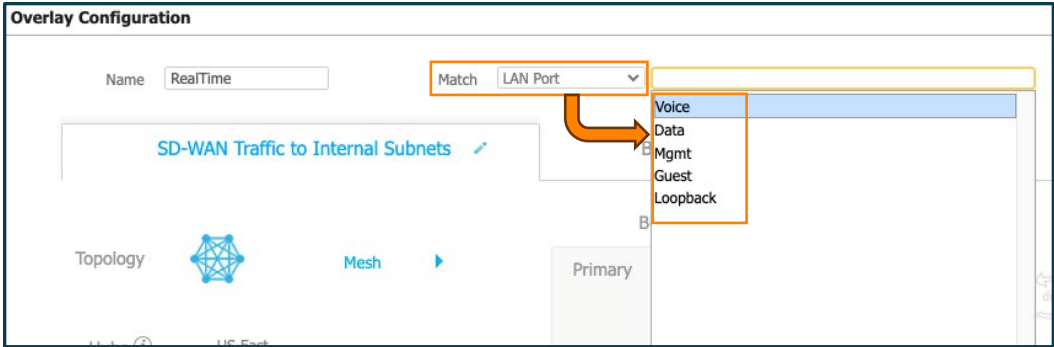


Figure 7 – Traffic Match Using LAN Port Label

3.1.3 Traffic Match – Appliance ACL

Appliance ACL is another method to match traffic criteria. However, to use appliance ACL, you must configure appliance ACL before configuring the BIO. After an appliance ACL is configured, it becomes available on the BIO configuration page for selection.

Using Templates to push Appliance ACL to all the appliances:

- Use an existing Template Group or create a new Template Group
- Select Access List from the available Templates (under Show All)
- Create a new ACL and add ACL entries within the ACL definition
- Save and Apply the Templates to the Appliances

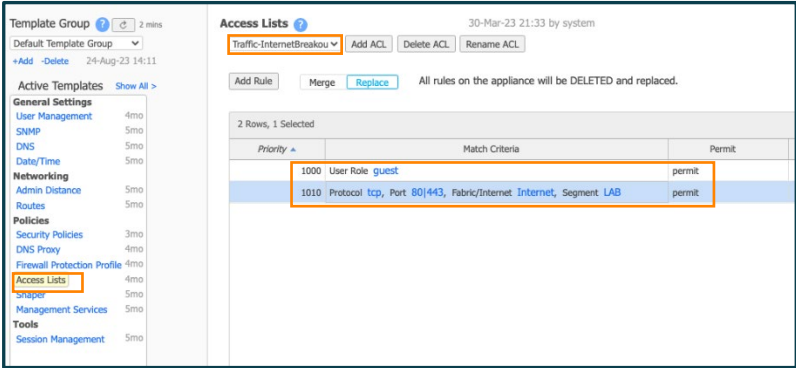


Figure 8 – Configuring Appliance ACL Using Template Group

The BIO Configuration page will list the newly configured Appliance ACL available for selection. Selecting this ACL will match traffic based on the configured ACL entries.

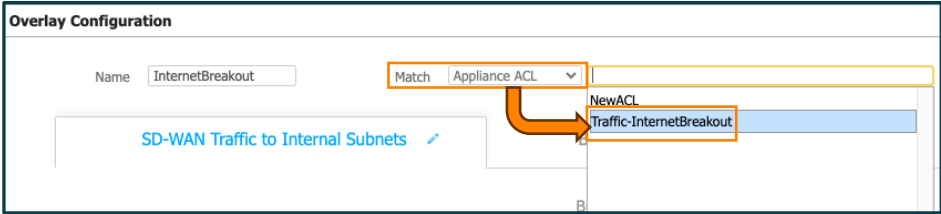


Figure 9 – Traffic Match Using Appliance ACL



3.2 Internal Subnets

The Internal Subnets table is used to inform the EdgeConnect that a given subnet is either internal or external to the SD-WAN fabric. If it is internal, it implies that the traffic is destined within the enterprise and will be sent over one of the configured tunnels to another branch/hub. If it is external, the traffic is considered outside of the enterprise network.

External traffic can be handled as local breakout traffic, backhauled to the hub device via a tunnel, sent over via SSE service tunnel, or dropped. This table is part of the BIO page. It is common across all BIOs. The size of this table is 1024 entries. Separate lists can be configured for IPV4 (512 entries) and IPV6 (512 entries) subnets.

The screenshot shows the 'Business Intent Overlays' interface. A modal window titled 'Internal Subnets' is open, displaying a table of internal subnets. The table has columns for 'Subnet/Mask' and 'Segment'. The following subnets are listed:

Subnet/Mask	Segment
224.0.0.0/4	All
169.254.0.0/16	All
192.168.0.0/16	All
172.16.0.0/12	All
10.0.0.0/8	All

The modal also includes a checkbox for 'Consider Non-default routes as internal subnets' and buttons for 'Add' and 'Bulk Add/Replace'.

Figure 10 – Internal Subnets Table

By default, the following address ranges are treated as internal subnets:

- 224.0.0.0/4
- 169.254.0.0/16
- 192.168.0.0/16
- 172.16.0.0/12
- 10.0.0.0/8

Additional subnets can be added to mark the traffic as internal by using either the Add button or the Bulk Add Replace knob on the Internal Subnets page (Figure 10). Subnets can also be mapped to a specific VRF segment. When a specific subnet is configured in the internal list and marked for VRF-Segment-A, the traffic is treated as internal for that subnet when it is on VRF-Segment-A.

In the following example (Figure 11), 16.143.16.0/24 is considered INTERNAL subnet for CORP VRF segment, but the same subnet is treated as EXTERNAL for other segments. Subnet 16.17.10.0/30 is treated as INTERNAL in ALL segments.

To Bulk Add/Replace, simply add subnets with comma separators. All subnets added using the Bulk Add/Replace knob are marked with ALL segments. You can modify the segment after adding in bulk.

16.17.10.0/24 will be treated as Internal for traffic originating from any segment.

Subnets can also be imported by simply adding texts with comma separated value.

16.143.16.0/24 will be treated as Internal only for traffic originating from **CORP** VRF segment. For all other segment, this subnet will be treated as External.

Internal Subnets

Add Bulk Add/Replace

7 Rows, 1 Selected

Subnet/Mask	Segment	
16.17.10.0/30	All	×
16.143.16.0/24	CORP	×
224.0.0.0/4	All	×

Figure 11 – Internal Subnet Table Options

3.2.1 Consider Non-default Routes as Internal Subnets

The **Consider Non-default routes as internal subnets** feature provides two methods to define internal subnets. Both methods are processed in the following sequence: manually configured internal subnets first, and then consider any non-default route as internal. This feature also helps to overcome the limitation of 1024 entries (512 IPv4 + 512 IPv6) in the Internal Subnets table; the routing table can handle up to 60K (30K IPv4 + 30K IPv6) routes.

This feature helps to augment the internal subnets list by leveraging the destination route information in the routing table. It infers that if a route entry is present in a device for a given destination, it must be internal.

If only a default route matches for the given destination, it must be internet destined. It also ensures that internal traffic does not get “leaked” over to the internet because of a missing specific or summary route in the Internal Subnets table.

The flowchart in Figure 12 shows how a flow (LAN side to the WAN side direction) is determined to be either Internal or External using the internal subnet list and considering non-default route features.

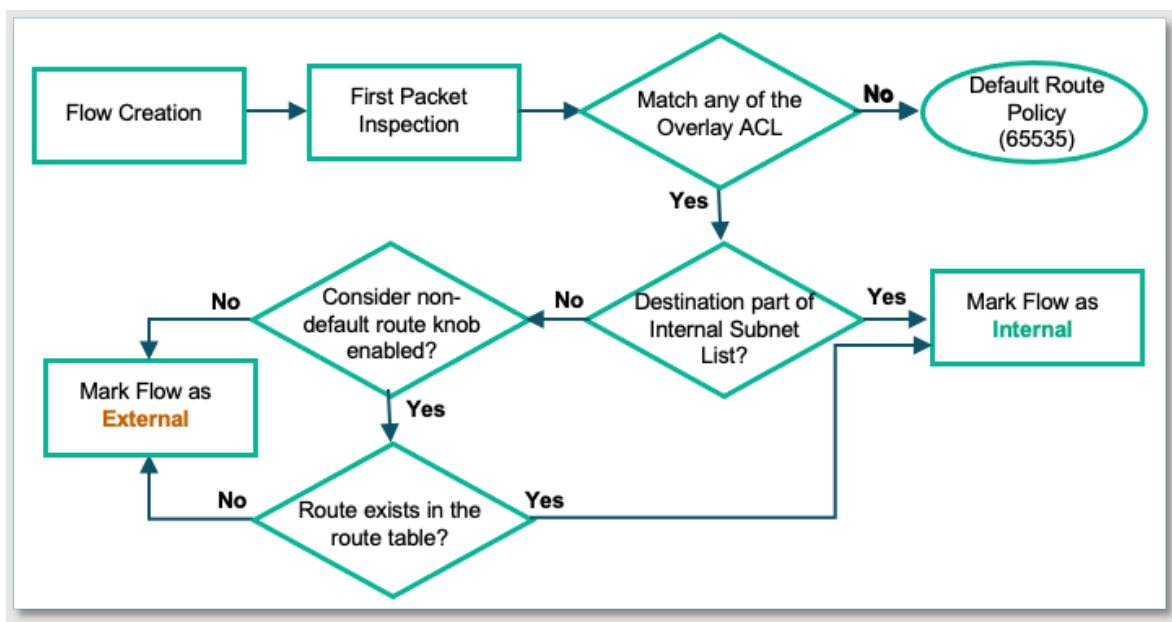


Figure 12 – Determining a Flow Internal or External (LAN to WAN Direction)

3.3 SD-WAN Traffic to Internal Subnets

This document primarily focuses on detailing Link Bonding Policy. This section introduces the topic from the perspective of orchestration. Section 4 expands upon it in the context of operations.

The section of BIO configuration that covers traffic to internal subnets has five subsections:

1. Topology
2. Link Bonding Policy
3. QoS, Security & Optimization
4. Service Level Objectives (Degraded or DOWN with thresholds)
5. Primary / Backup Interface Label (Underlay Network) Selection with Cross-Connects

Overlay Configuration

Name: RealTime Match: Overlay ACL DSCP: ef, Application: RingCentral, Application ... Region: Global (selected), US-East, US-West, US-Central, India, Australia. Use Global Settings

SD-WAN Traffic to Internal Subnets Breakout Traffic to Internet & Cloud Services

1 Topology Mesh Hubs: US-East, Hub-East. Include Hubs in other Regions

5 Build SD-WAN Using These Interfaces

Primary

Interface	Cross Connect
MPLS2	None
INET1	Group1
INET2	Group1
LAB1	None

Secondary

Add Backup if Above Are: Down

Backup

Interface	Group
LTE	Group1

Hide Secondary

4 Service Level Objective

Loss: < 5 %
Latency: < 250 ms
Jitter: < 0 ms

2 Link Bonding Policy

High Availability

- Failover 0sec
- Use Best Quality Path
- Path Conditioning
- BW Efficiency 50%

High Quality

- Failover <1sec
- Use Best Quality Path
- Path Conditioning
- BW Efficiency >80%

High Throughput

- Failover <1sec
- Load Balance Paths
- Path Conditioning
- BW Efficiency >80%

High Efficiency

- Failover <1sec
- Load Balance Paths
- BW Efficiency 100%

Custom

- FEC Wait Time:
- Path Conditioning:
- Link Selection:

3 QoS, Security & Optimization

Boost: Disabled
Peer Unavailable Option: Use Best Route
Traffic Class: 1 (RealTime)
LAN DSCP: trust-lan
WAN DSCP: trust-lan

Show Details

IMPORTANT: By default, BIO configuration is global. It is applied to all nodes associated with this BIO.

If a region-specific BIO modification is made, only appliances belonging to that region will have those specific modifications.

A given EdgeConnect deployment might not have all the WAN underlays. For example, a site could be Internet-only or MPLS-only. It will utilize only the WAN underlays provisioned at that location.

3.3.1 Topologies

When an appliance is deployed and provisioned into Orchestrator, you can use the Hub Site configuration knob to mark the appliance as a hub. Similarly, you can mark the appliance as a hub by using **Orchestrator UI > Configuration > Hubs**. Without this configuration, an appliance is considered as a spoke (non-hub). In the following example (Figure 13), the appliance is configured as a hub site because the knob is checked.

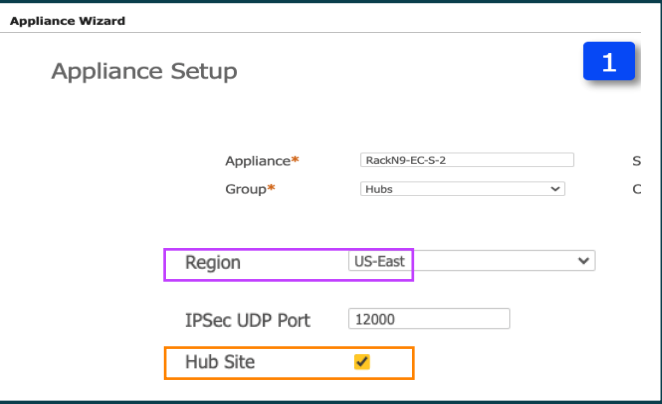


Figure 13 – Provisioning as Hub in Wizard Configuration

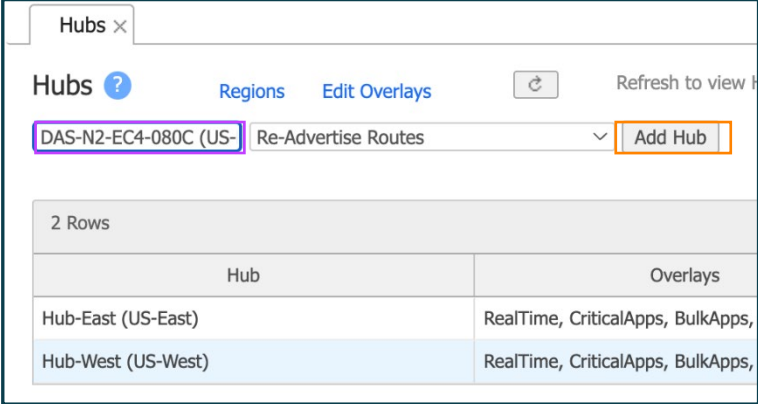


Figure 14 – Provisioning as Hub on Hubs Configuration Tab

Based on the hub and region settings, some of the Business Intent Overlay topologies will establish tunnels between a few remote sites or all remote sites.

The following topologies are supported on a per-BIO basis:

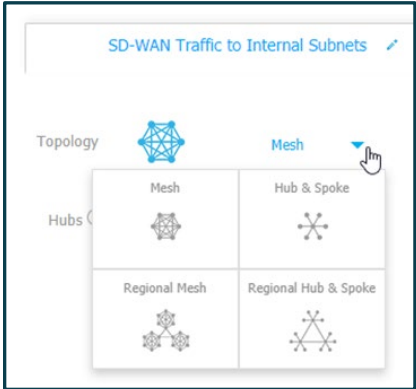


Figure 15 – Business Intent Overlay Topology Selection

Hub and Spoke with One or Multiple Hubs

Overlay tunnels are established between appliances marked as hub and the non-hubs for that specific overlay. For example, if an overlay named “BulkApps” is applied to six appliances with two of them marked as hubs, the BulkApps overlay is built only between the two hubs and the four non-hub appliances. Overlay tunnels are not built between non-hub appliances. This results in eight tunnels overall.

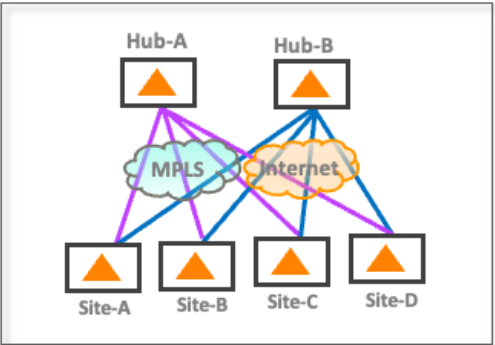


Figure 16 – Hub and Spoke Topology

Mesh (Full Mesh)

Overlay tunnels are established between all appliances in the fabric without any distinction of hub or non-hub for that specific overlay. For example, if an overlay named “RealTime” is applied to six appliances, all six appliances build overlay tunnels between them. This results in 15 tunnels overall.

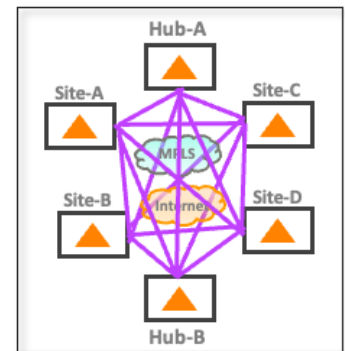
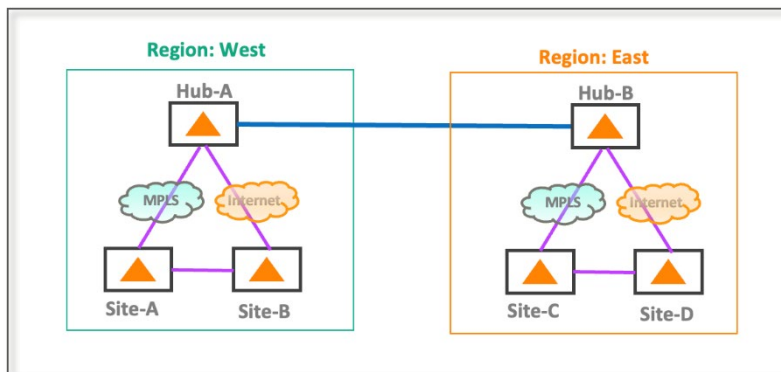


Figure 17 – Mesh (Full Mesh) Topology

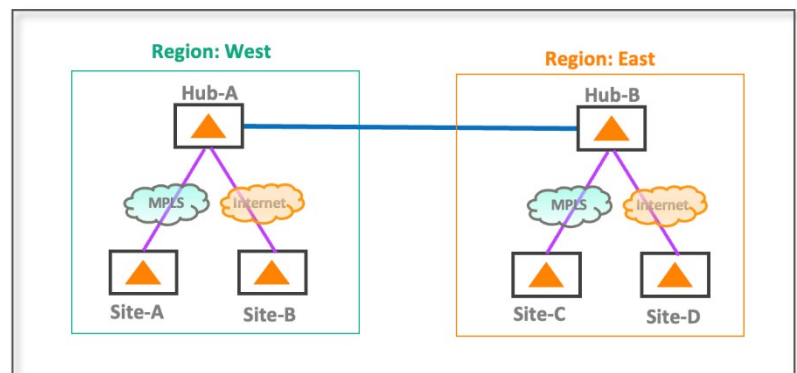
Regional Mesh

In a regional mesh topology, overlay tunnels are established between all appliances within the region without any distinction of hub or non-hub for that specific overlay. For example, each region has three appliances with one marked as a hub. Appliances within the region build overlay tunnels between them. In addition, hubs in the regions build full-mesh tunnels with each other.



Regional Hub & Spoke

In a regional hub & spoke topology, spokes establish overlay tunnels with a hub in the same region. No overlay tunnels are built between the spokes within or outside of the region. However, hubs between the regions build full-mesh overlay tunnels for inter-regional connectivity.



HPE Aruba Networking recommends using Regional Hub & Spoke as the preferred network topology.



3.3.2 Link Bonding Policy

Link bonding policies provide the following four predefined SLA options and one custom bond policy. These bonding policies are detailed in sections 4.7 through 4.10.

- High Availability (HA): Ultra FEC, ultra-fast path switching, highest quality path
- High Quality (HQ): Adaptive FEC, sub-second path switching, highest quality path
- High Throughput (HT): Adaptive FEC, sub-second path switching, load balance across paths
- High Efficiency (HE): No FEC, sub-second path switching, load balance across paths
- Custom: Path selection based on the configured policy

Link Bonding Policy				
High Availability	High Quality	High Throughput	High Efficiency	Custom
<ul style="list-style-type: none">• Failover 0sec• Use Best Quality Path• Path Conditioning• BW Efficiency 50%	<ul style="list-style-type: none">• Failover <1sec• Use Best Quality Path• Path Conditioning• BW Efficiency >80%	<ul style="list-style-type: none">• Failover <1sec• Load Balance Paths• Path Conditioning• BW Efficiency >80%	<ul style="list-style-type: none">• Failover <1sec• Load Balance Paths• BW Efficiency 100%	<ul style="list-style-type: none">• FEC Wait Time:• Path Conditioning:• Link Selection:

Figure 20 – BIO Link Bonding Policy Selection Options

3.3.3 QoS, Security, and Optimization

The Traffic Management section covers:

- Boost – Enable/disable WAN Optimization on this BIO.
- Underlay Routing Options when EdgeConnect peer is unavailable.
- Traffic Class to use in the Shaper for this BIO.
- LAN DSCP – DSCP that will appear on the far-end LAN.
- WAN DSCP – DSCP that will appear on the tunnel encapsulated packets. These can be set to align with the service provider’s MPLS Class of Service.

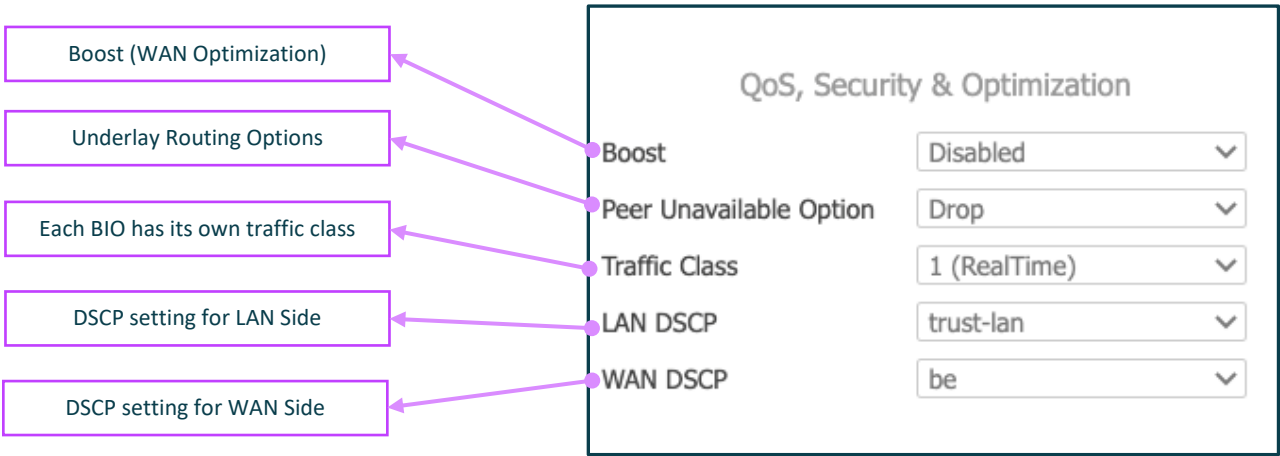


Figure 21 – BIO QoS/Optimization and Traffic Mgmt



Peer Unavailable Option

Enabling one of the Peer Unavailable options (Use Best Route or WAN Label) enables the EdgeConnect to find an alternate path for the internal subnet destinations that is not behind an EdgeConnect appliance. Peer Unavailable means that the remote EdgeConnect is unavailable.

The Peer Unavailable Option provides Underlay Options to redirect internal subnets traffic to SD-Branch/Micro Branch destinations, IaaS Cloud Gateways (e.g., AWS Transit Gateway, Azure vWAN/vHub, Google NCC...and so forth), or destinations that are behind a non-EdgeConnect router (e.g., Core router behind EdgeConnect or Branch connected through a legacy MPLS/Private WAN cloud).

The following flowchart shows the packet flow to determine what happens to an "internal" traffic when either an SD-WAN route or an SD-WAN peer (remote EdgeConnect) is unavailable.

Alternatively, this option can be set to **Drop** to restrict internal subnet traffic to stay only on SD-WAN tunnels and drop if the SD-WAN peer is unavailable.

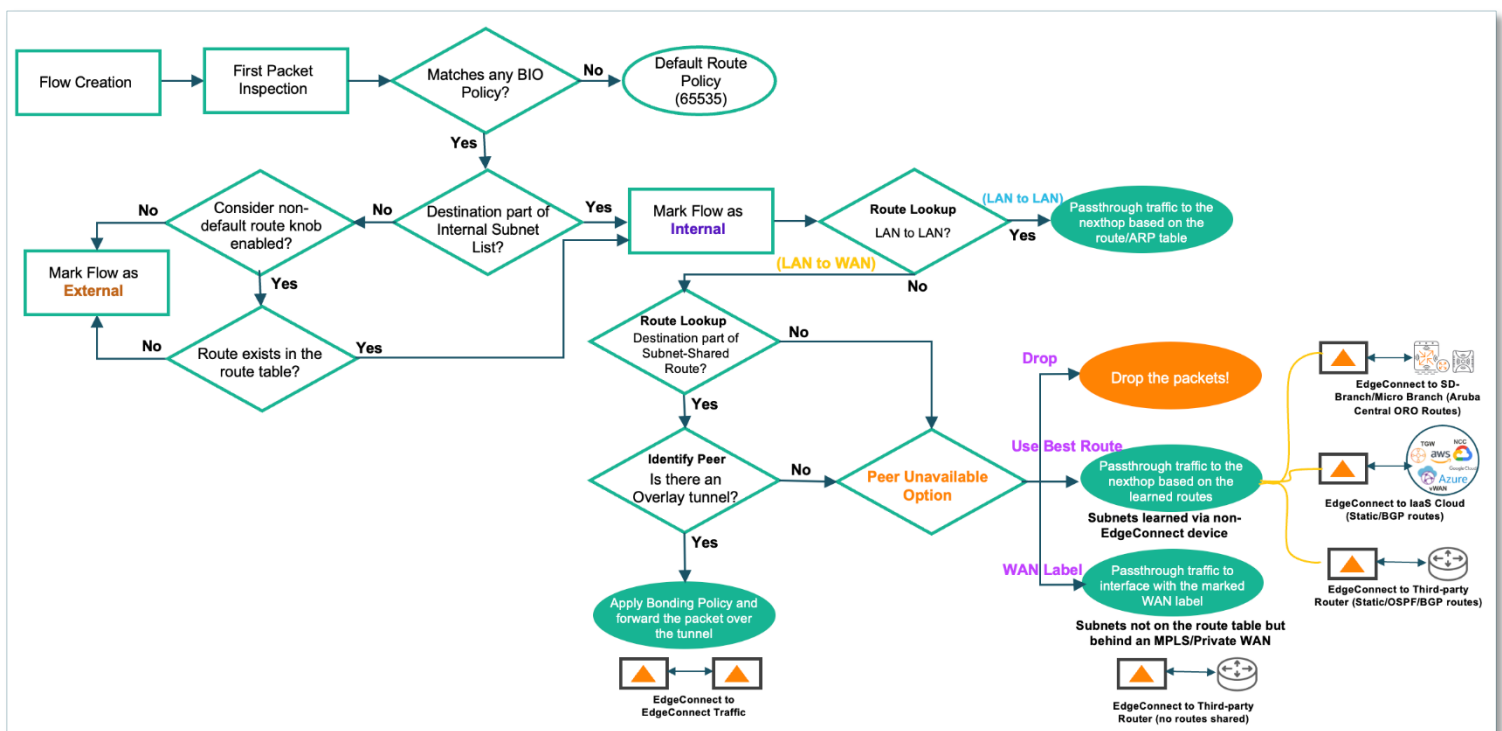


Figure 22 – Peer Unavailable Option - Packet Flow

Drop

This is the default selection. Traffic will be dropped when no route or no peer is available for the matched overlay.

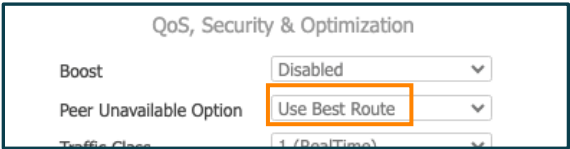
Exception: For LAN-to-LAN traffic or traffic originating from the LAN side to the EdgeConnect itself (ping/ssh to LAN interface IP), the traffic is allowed as passthrough-unshaped even when Peer Unavailable Option is set to Drop.

QoS, Security & Optimization	
Boost	Disabled
Peer Unavailable Option	Drop

Use Best Route

Use Best Route is the most used setting. It provides an alternate path for the internal traffic when the peer or route is unavailable.

Traffic will be sent as a passthrough (i.e., no bonded tunnel treatment and no bonding policy will be applied) based on the simple lookup of the route-table. Routes that will be considered for this route lookup are OSPF/BGP/Static/Default routes. Any subnet-shared routes will NOT be considered for this route lookup.



Use Case: A user behind the LAN side of the EdgeConnect accesses an application behind the WAN side. Both the router and EdgeConnect share the routes through BGP routing protocol.

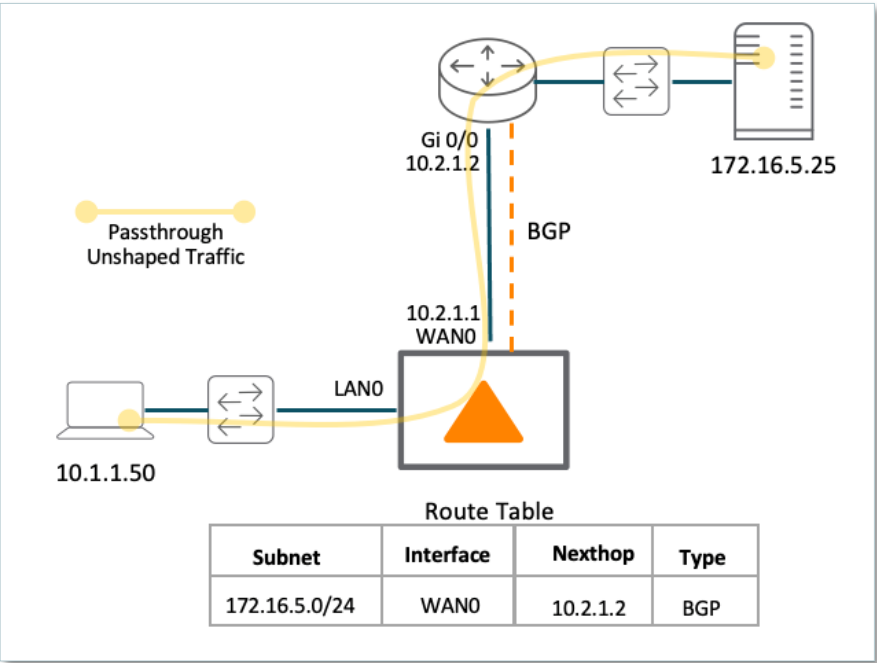


Figure 23 – Use Best Route - When Peer Unavailable

In this example (assumption), the user traffic from 10.1.1.50 will match an internal subnet list and subsequently matches an overlay (e.g., CriticalApps). In following scenario, “Peer Unavailable Option” will be invoked:

- a) When there is no matching subnet-shared route (routes advertised by another EdgeConnect peer) to the destination 172.16.5.25
- b) When the overlay SD-WAN tunnel is unavailable

In this example, Peer Unavailable Option is set to “Use Best Route”. Therefore, the EdgeConnect will look at the routing table to see if there are any routes to the destination 172.16.5.0/24 and sees a BGP route 172.16.5.0/24 via WAN0-nexthop-10.2.1.2.

Traffic will be forwarded through WAN0 interface to the next hop 10.2.1.2 as passthrough traffic.



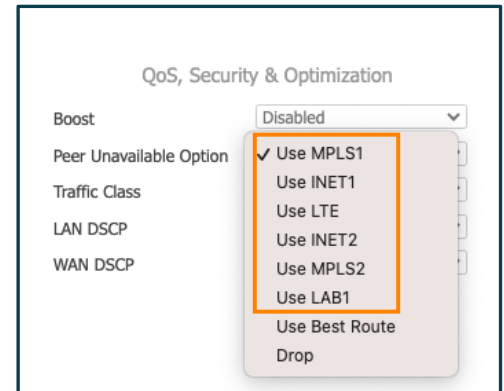
Use WAN Label

This is very similar to “Use Best Route”, but instead of using the route lookup, it simply forwards the traffic (passthrough) to a provisioned WAN label (WAN label to be selected from the available options).

Use Case: A user behind the LAN side of the EdgeConnect accesses an application that is at a non-SD-WAN location but connected through a legacy MPLS network on the WAN side.

In this example (assumption), the user traffic from 10.1.1.50 will match an internal subnet list and subsequently match an overlay (e.g., CriticalApps). In the following scenario, the “Peer Unavailable Option” will be invoked:

- When there is no matching subnet-shared route (routes shared by another EdgeConnect peer) to the destination 172.16.5.25
- When the overlay SD-WAN tunnel is unavailable



In this example, Peer Unavailable Option is set to “**Use MPLS1**”. Therefore, the EdgeConnect will forward the traffic to the WAN interface marked with MPLS1 as a passthrough (Figure 24).

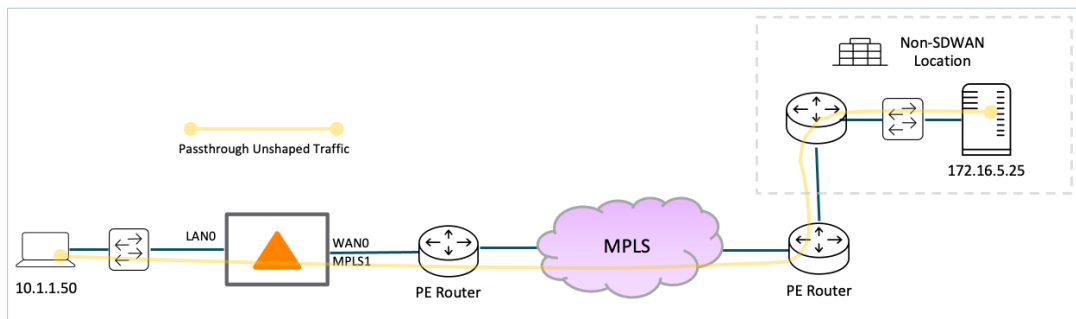


Figure 24 – Peer Unavailable "Use WAN Label"

3.3.4 Service Level Objectives (Degraded or Down with Thresholds)

Fundamental to the architecture of how Business Intent Overlays work is selection and switching between an overlay's associated underlay tunnels on a packet-by-packet basis to achieve a required Service Level Objective. Specific Service Level Objectives can be set for a BIO on a regional basis for packet loss, latency, and/or jitter. When a non-zero value is entered, and a given underlay tunnel meets the configured threshold, it might become disqualified or ineligible to carry packets for the overlay. The WAN interfaces do not need to exceed all three thresholds. If any of the values are set to zero, that parameter is ignored. The specific rules and actions for determining Degraded Link will be described in sections 4.4.1 and 4.4.2.

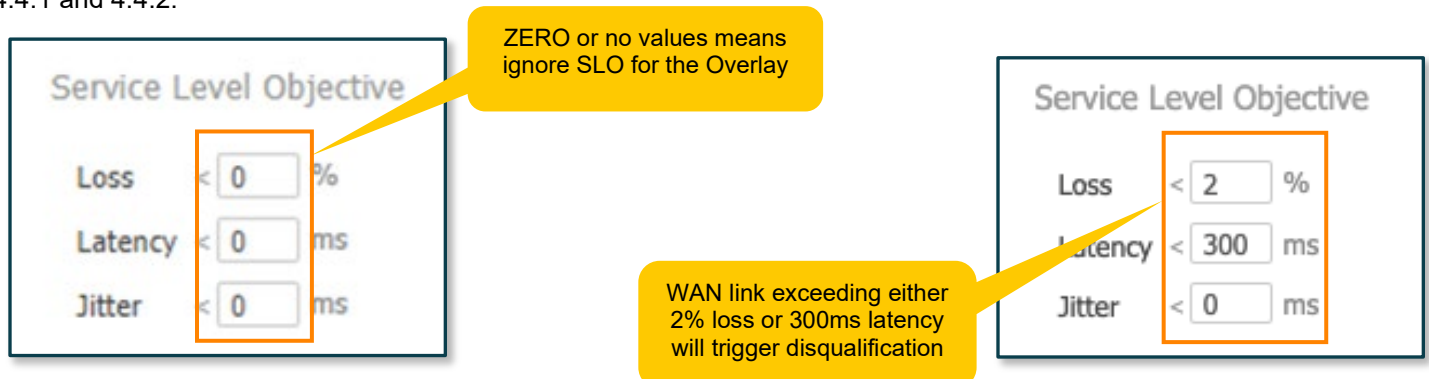


Figure 25 – Service Level Objective for Underlays

3.3.5 Build SD-WAN Using These Interfaces (Primary, Secondary, and Backup)

Orchestrator automatically builds overlay tunnels between EdgeConnect appliances that are members of that given BIO. Stated a different way, a pair of EdgeConnect appliances will have one overlay tunnel to which they are jointly members. As part of this process, Orchestrator also builds underlay tunnels as defined by the BIO policy. Figure 26 shows an example of Orchestrator policies for WAN selection.

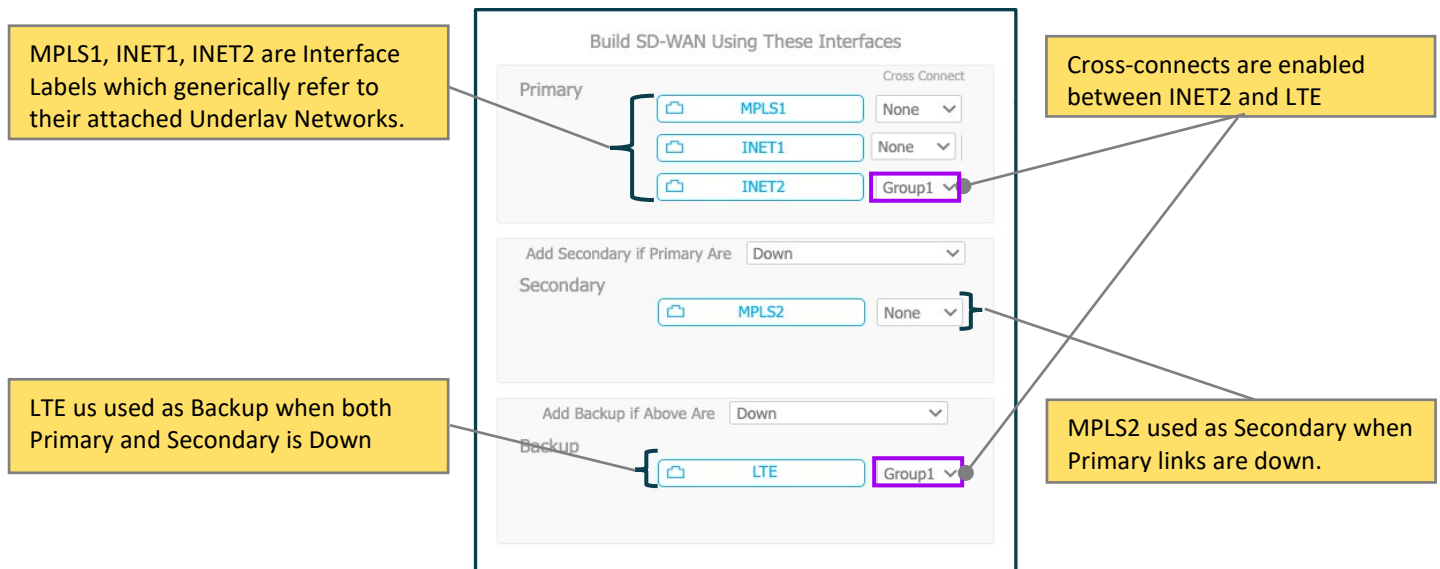


Figure 26 – BIO - Build Tunnels Using WAN Interfaces

When two appliances belong to one or more of the same BIOs, Orchestrator will build underlay tunnels for each interface label they have in common. Figure 27 shows the deployment of two EdgeConnect appliances that both belong to the RealTime, Bulk Apps, and Critical Apps BIOs. Orchestrator builds underlay tunnels between like-labels (MPLS1 to MPLS1 and INET1 to INET1) as well as cross-connected interfaces (LTE to INET2). Notice that the BIO configuration includes the Interface label MPLS2 (Figure 26), which neither node has.

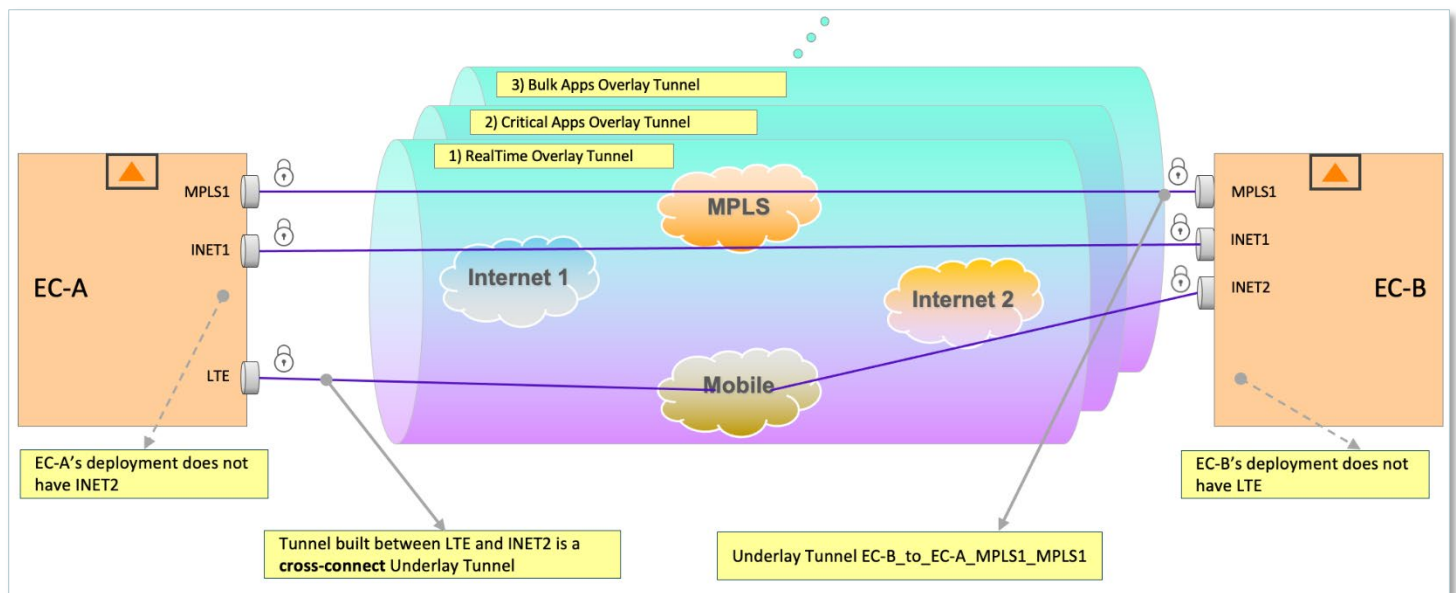


Figure 27 – Overlay and Underlay Tunnel Construction

The three underlay tunnels depicted in the figure above (Figure 27) are shared across all BIOs to which both appliances belong. In this example, they belong to RealTime, Critical Apps, and Bulk Apps.

Underlay Tunnel Limit per Bonded Overlay Tunnel

Each EdgeConnect appliance builds tunnels with the peers based on the applied BIO and the number of WAN labels provisioned per appliance. The BIO configuration page enables you to map multiple WAN labels on a given BIO but depending on what WAN connections (labels) are available on each EdgeConnect, underlay tunnels are built with the peer matching the WAN label. The BIO configuration also allows underlays to “cross connect”. When “cross-connect” is configured for a WAN label, underlay tunnels are created with the cross-connect enabled WAN labels. Cross-connect provides multiple paths to the peers, which increases the underlay tunnels between the peers.

NOTE: Each overlay tunnel can be tied only to a maximum of 16 underlay tunnels. This is the hard system limit and cannot be modified. The following examples review overlay configurations and combinations of WAN labels (with or without cross-connect) so that you understand the impact of the underlay tunnel limit for an overlay.

Example 1: EdgeConnect with five WAN connections having “No Cross-Connect WAN labels”

- In this example (Figure 28), each EdgeConnect has five WAN connections, and the BIO has Cross Connect set to **None** against each WAN label.
- Underlay tunnels will be built only between matching WAN labels. As a result, EC-A will have five underlay tunnels and EC-B will have five underlay tunnels. Therefore, the RealTime overlay (in this example) on each of these appliances will have five underlay tunnels bonded.
- This example does not exceed the maximum underlay tunnel limit of 16 for an overlay tunnel and is acceptable.

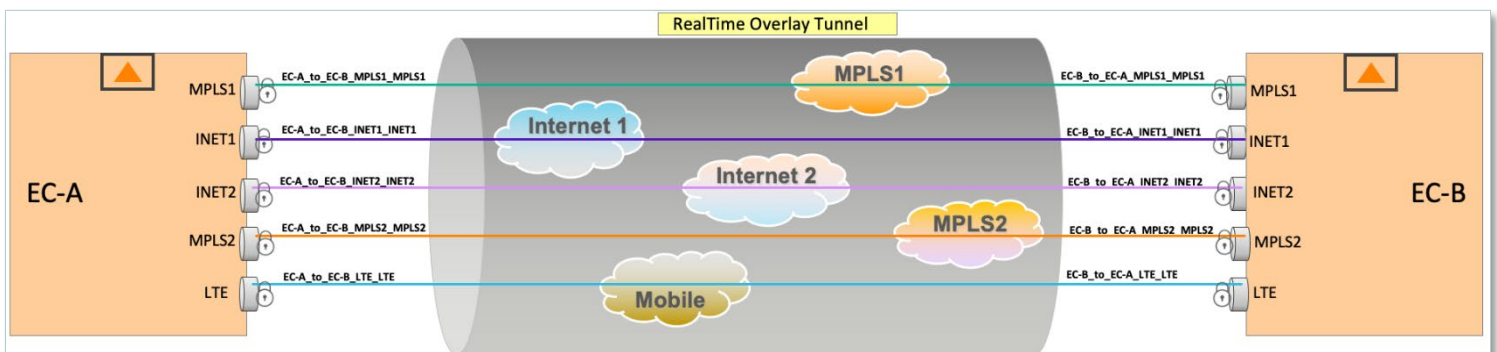


Figure 28 – Multiple WAN connection with No "Cross-Connect"

Example 2: EdgeConnect with four WAN connections having “Cross-Connect”

- In this example (Figure 29), each EdgeConnect has four WAN connections, and the BIO is provisioned with five WAN labels and Cross Connect set to **Group1** against each of the five WAN labels.

NOTE: The BIO has five WAN labels configured, but EC-A and EC-B have only four WAN connections available.

- Underlay tunnels will be built between all matching WAN labels and with Group1 cross-connect enabled WAN labels. Because each EdgeConnect has four WAN connections available and all are tagged with “Group1 – Cross Connect”, they will build a total of 16 underlay tunnels, including the cross connect tunnels.
- 16 is the maximum underlay tunnels supported for a bonded overlay tunnel. Therefore, the RealTime overlay in this case will have the total of 16 underlay tunnels bonded, which is still acceptable.

Build SD-WAN Using These Interfaces

Primary	Cross Connect
MPLS1	Group1
INET2	Group1
INET1	Group1
MPLS2	Group1
LTE	Group1

- Any new WAN connection or cross-connect will result in EdgeConnect triggering an error message based on the max tunnel limit for the overlay. Those additional tunnels will not be included as part of the overlay tunnel.

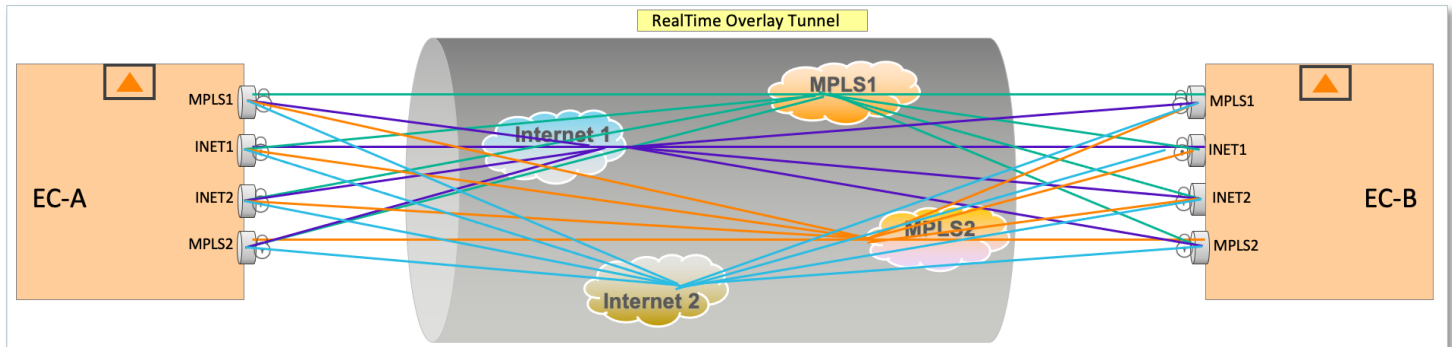


Figure 29 – Max Underlay Tunnel Limit with Cross-connect WAN Labels

Example 3: EdgeConnect with five WAN connections having “Cross-Connect”

- In this example (Figure 30), each EdgeConnect has five WAN connections, and the BIO has Cross Connect set to **Group1** against each WAN label.
- The BIO has five WAN labels configured, and EC-A and EC-B have five WAN connections available.
- EdgeConnect will attempt to build underlay tunnels between all matching WAN labels and with Group1 cross-connect enabled WAN labels. As a result, EC-A will have 25 underlay tunnels and EC-B will have 25 underlay tunnels.
- EdgeConnect will cap the maximum underlay tunnel bonding for the overlay at 16 and will generate an error message that indicates the underlay tunnel count exceeds the tunnel limit for the overlay.

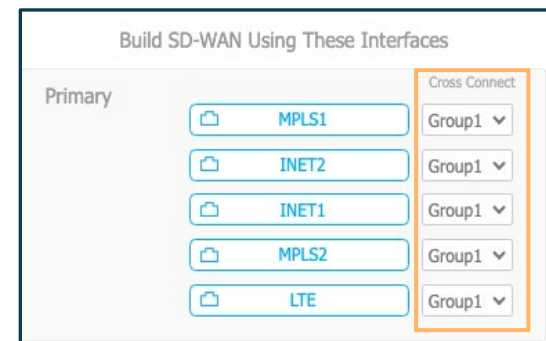
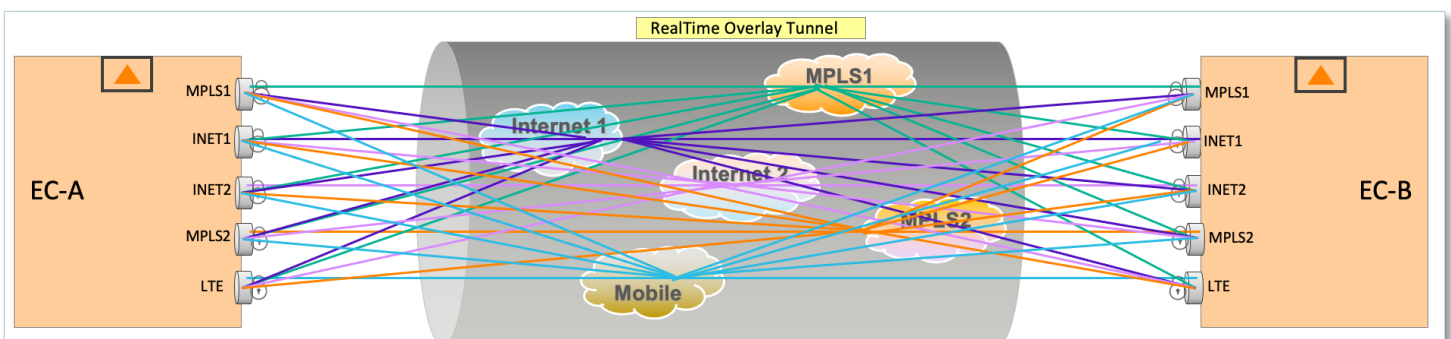


Figure 30 – Multiple WAN with Cross-connect - RealTime Overlay Exceeds Max Bonded Underlay Tunnel Limit of 16

It is recommended that you use cross-connect for path diversity. However, it is important to remember the impact of cross-connect for sites with more WAN connections. This results in reaching the system limit for maximum underlay tunnels for a bonded overlay tunnel.

FAQs Around Underlay Tunnel Limit

1. Will Orchestrator prevent misconfigurations that exceed the maximum underlay tunnel limit?

Yes, for a scenario in which a **new** overlay configuration is configured with multiple WAN labels and any EdgeConnect with as many WAN connections available results in more than 16 underlay tunnels for a single overlay. In this scenario, Orchestrator will not be able to orchestrate overlay configurations to that specific EdgeConnect. It will generate an error.

2. In what scenario might you see the error "The number of bound tunnels for these bonded tunnels exceeds the limit of 16"?

You would see this error when the overlay configuration that is applied initially does not exceed the maximum tunnel count, but additional WAN labels or new cross-connect labels are introduced that cause more tunnels to be created that exceed the limit of 16. In that scenario, EdgeConnect will build those additional tunnels but will not be able to bind those underlay tunnels to the overlay tunnel. As a result, the error related to exceeding the limit of 16 is generated.



3.4 Breakout Traffic to Internet & Cloud Services

Traffic to destinations that are not part of the “Internal Subnet List” are considered external flows (refer to Section 3.2 for an explanation of how internal/external flows are classified). Traffic classified as “External” flows enters the Breakout Traffic to Internet & Cloud Services; the traffic is sent over in the order of preferred policy configuration. This section introduces the topic from the perspective of orchestration. Section 4 expands upon it in the context of operations.

The Breakout Traffic to Internet & Cloud Services section contains the following subsections:

1. Preferred Policy Order
2. Available Policies
3. Break Out Locally Using These Interfaces
4. Link Selection
5. Branch and Hub Settings

The screenshot displays the SD-WAN configuration interface for a branch named 'GUEST'. The 'Match' dropdown is set to 'Overlay ACL' and the 'Application group' is 'SilverPeak, Application Hulu...'. The 'Region' is set to 'Global'. The 'Breakout Traffic to Internet & Cloud Services' section is active, showing a list of hubs and a configuration for breakout traffic. The configuration includes a 'Preferred Policy Order' with three policies: 'HPE-Axis-SSE', 'Backhaul Via Overlay', and 'Break Out Locally'. The 'Available Policies' section lists various cloud services like Perimeter81, Skyhigh, Netskope Cloud, Zscaler Cloud, Akamai, Lookout, and CheckPoint. The 'Break Out Locally Using These Interfaces' section shows a primary interface 'INETA' and a backup interface 'LTEA'. The 'Link Selection' section shows a 'Waterfall' link selection method and performance thresholds for Loss, Latency, Jitter, and Utilization. A 'Threshold-based Failover' checkbox is checked, indicating that the next preferred policy will be used if the current one fails to meet the thresholds.

3.4.1 Preferred Policy Order

Preferred Policy Order of an overlay determines how an EdgeConnect will process the internet-bound (external to SD-WAN subnets) traffic. Policy Order can include one or more policies **up to a maximum of 32**. An EdgeConnect runs these policies similarly to access-list processing (top to down).

The example above shows a preferred policy order of:

1. HPE-Axis-SSE (Secure Web Gateways)
2. Backhaul via Overlay (SD-WAN Fabric)
3. Break Out Locally
4. Drop (Default Action at the end)

The order in which these Breakout policies are placed matters. The policy at the top is preferred first in processing, and then the other listed policies in order.

3.4.2 Available Policies

Available Policies lists all available policies that an internet bound traffic can take. You must drag the available policy into Preferred Policy Order so that the internet traffic can use the policy. By default, two policies are available: 1. Break Out Locally and 2. Backhaul Via Overlay. There are three additional ways that policies can be introduced into the Available Policies section by provisioning:

1. API-based Orchestrated Tunnels to Cloud Security Provider (e.g., Secure Web Gateway – SWG)
2. Service Orchestration-based Orchestrated Tunnels to Cloud Security Provider (e.g., Secure Web Gateway – SWG)
3. Manual passthrough IPsec or GRE tunnels (to SWGs, third-party router, firewall, or VPN Gateways)

3.4.3 Break Out Locally Using These Interfaces

For Break Out Locally, specific WAN underlays can be selected as primary with others designated as backup. The order in which these labels are mapped only matters when the Link Selection is set to “Waterfall” and Rank Links is set to “Fixed Order”. Otherwise, all WAN underlays will be treated the same way.

WAN Underlays under the Primary section will be used if deemed UP (determined by IP-SLA) and eligible (determined by performance threshold). IF all primary links are degraded, backup links will be considered for link selection.

3.4.4 Link Selection

The Link Selection section relates to Break Out Locally internet policy. Primary/Backup WAN underlays will be considered ineligible when exceeding the configured performance threshold.

Threshold-based Failover allows the overlay to find the next-best path based on the configured policy order.

Section 5 provides additional details on path selection and link rankings for internet breakout traffic.

3.4.5 Branch and Hub Settings

Business Intent Overlay configuration for Internet Breakout is global and applicable for all appliances managed by Orchestrator. The BIO page’s Branch Settings enable you to make internet policy modifications for specific hub appliances. This provides unique internet policies for hub appliances while the branches all have common policies.

The screenshot displays the 'Branch Settings' configuration page for a hub appliance. The page is divided into several sections:

- Header:** Includes fields for Name (GUEST), Match (Overlay ACL), Application group (SilverPeak, Application Hulu...), and Region (Global).
- Traffic Selection:** Two tabs are visible: 'SD-WAN Traffic to Internal Subnets' and 'Breakout Traffic to Internet & Cloud Services' (selected).
- Branch Settings:** A table lists various hub appliances. The 'Kennesaw4-Powers' appliance is highlighted with a yellow box. A checkbox labeled 'Use Branch settings' is located to the right of the table.
- Preferred Policy Order:** A list of policies including 'Backhaul Via Overlay' and 'Break Out Locally'.
- Available Policies:** A list of policies including 'Perimeter81', 'Skyhigh', and 'Netskope Cloud'.
- Break Out Locally Using These Interfaces:** A section for selecting primary interfaces, with 'INETA', 'INETB', and 'INETC' listed.
- Available Interfaces:** A list of interfaces including 'LTEB', 'SAT1', and 'MPLS1'.
- Link Selection:** A section for selecting link selection methods, with 'Waterfall' and 'Balance' options.

Annotations with yellow boxes and arrows point to the 'Use Branch settings' checkbox and the 'Kennesaw4-Powers' appliance, with the following text:

- 'Uncheck Use Branch Settings to make changes to the hub'
- 'Select one of the hub appliances from the available list'

This setting is visible only when the BIO is applied to at least one of the hub appliances.

3.5 Regions

An appliance can be associated to a region either during initial setup (Configuration Wizard) or by using the Regions option in the Orchestrator UI. Region configuration, and association of an appliance to a region, is done using the Orchestrator UI: **Configuration > Overlays & Security > Region** (Figure 31).

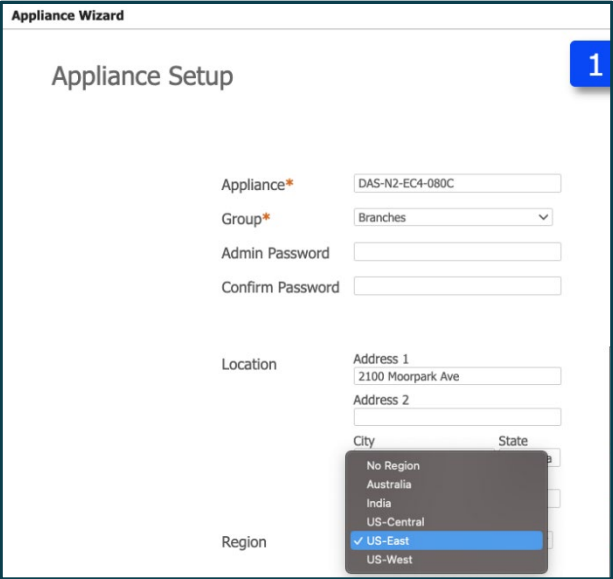


Figure 32 – Region association - Configuration Wizard

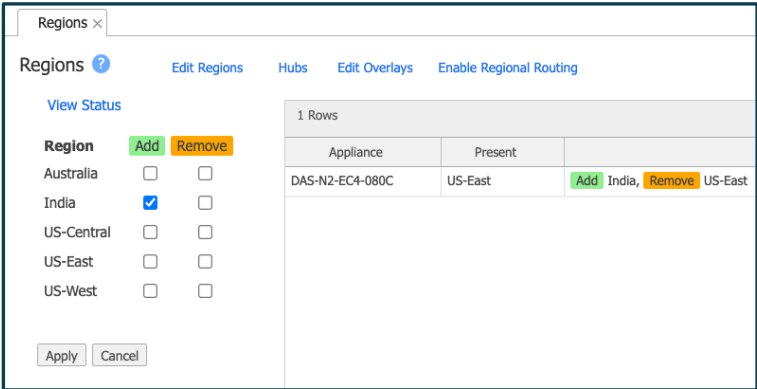


Figure 31 – Region Association Under Regions Configuration

Business Intent Overlay can be customized per region to accommodate respective region-specific variables. For example, some regions might need to use Full-Mesh topology for a given overlay while the remaining regions use Hub and Spoke topology. Based on region association for an appliance, the region-specific BIO configuration will be followed.

In the example shown in the Figure 33, the **entire** configuration (everything under SD-WAN Traffic and Breakout Traffic tabs) for this overlay (RealTime) can be customized, including (but not limited to) Match Criteria (Overlay ACL), Topology, Bonding Policy, WAN Interfaces for SD-WAN/internet, SLO...and so forth. This significantly helps reduce the total number of BIOs and the reuse of existing BIOs with modification based on the regional requirement. Region setting provides diversity for a global enterprise to accommodate region-specific requirements in a single overlay without creating additional tunnels.

NOTE: Any changes made specifically to a region on the overlay configuration is applied to all appliances that have the Region mapped. For example, if a change is made to a BIO that is specific to the US-East region, all appliances that are part of the US-East region will get this configuration update.

It is always recommended that you configure and associate devices to the respective region if you are managing a large SD-WAN fabric. It is also possible that an appliance might not have any region association mapped. In this case, those appliances will use the BIO configuration relevant to **Region: Global**.



Overlay Configuration

NameRealTime

MatchOverlay ACL

DSCPef, ApplicationRingCentral, Application ...

Region

Global

US-East

US-West

US-Central

India

Australia

Use Global Settings

SD-WAN Traffic to Internal Subnets

Breakout Traffic to Internet & Cloud Services

Topology

Mesh

Hubs

US-East

Hub-East

Include Hubs in other Regions

Build SD-WAN Using These Interfaces

Primary

MPLS2

INET1

INET2

LAB1

Cross Connect

None

Group1

Group1

None

Secondary

Add Backup if Above Are

Down

Backup

LTE

Group1

Hide Secondary

Available Interfaces

MPLS1

Service Level Objective

Loss

< 5

%

Latency

< 250

ms

Jitter

< 0

ms

Link Bonding Policy

High Availability

Failover 0sec

Use Best Quality Path

Path Conditioning

BW Efficiency 50%

High Quality

Failover <1sec

Use Best Quality Path

Path Conditioning

BW Efficiency >80%

High Throughput

Failover <1sec

Load Balance Paths

Path Conditioning

BW Efficiency >80%

High Efficiency

Failover <1sec

Load Balance Paths

BW Efficiency 100%

Custom

FEC Wait Time:

Path Conditioning:

Link Selection:

Show Details

QoS, Security & Optimization

Boost

Disabled

Peer Unavailable Option

Use Best Route

Traffic Class

1 (RealTime)

LAN DSCP

trust-lan

WAN DSCP

trust-lan

Figure 33 - Region Specific BIO Configuration

4 Link Bonding Policy on SD-WAN Fabric

4.1 Primary, Secondary vs. Backup and Service Level Objective

In general, underlay tunnels (UTs) are selected for use by the overlay (those primary links marked as “eligible”) unless a given failure/degraded condition exists whereby UT is either marked DOWN (Unavailable) or is not meeting Service Level Objectives (Degraded). EdgeConnect will build underlay tunnels using WAN labels configured under the Primary, Secondary and Backup section.

A given overlay’s operation uses secondary and backup links based on customizable parameters. Underlay tunnels using the secondary and backup WAN labels are effective only when ALL primary underlay tunnels are either down or exceed the configured service level objective (SLO).

4.1.1 Add Secondary Underlay Tunnels (UTs)

If “**Add Secondary if Primary Are Down**” (Figure 34) is selected, start using Secondary link(s) if **ALL** primary underlay tunnels are unavailable (underlay tunnels are down).

Build SD-WAN Using These Interfaces

Primary

INET1

INET2

MPLS1

MPLS2

Cross Connect

Group1

Group1

Group2

Group2

Add Secondary if Primary Are

Down

Secondary

EXT1

EXT2

Group1

Group1

Add Backup if Above Are

Down

Backup

LTE

None

Figure 34 – Secondary Link Selection When Primary Down

If “**Add Secondary if Primary Are Not Meeting Service Levels**” (Figure 35) is selected, start using secondary link(s) if **ALL** primary underlay tunnels exceed the configured “Service Level Objective”.

Build SD-WAN Using These Interfaces

Primary

INET1

INET2

MPLS1

MPLS2

Cross Connect

Group1

Group1

Group2

Group2

Add Secondary if Primary Are

Not Meeting Service Levels

Secondary

EXT1

EXT2

Group1

Group1

Add Backup if Above Are

Down

Backup

LTE

None

Available Interfaces

LAB2

EXT3

INET3

LAB1

Service Level Objective

Loss

< 20

%

Latency

< 0

ms

Jitter

< 0

ms

Figure 35 – Secondary Link Selection When Primary Links Degraded



4.1.2 Add Backup Underlay Tunnels if Primary and Secondary UTs Are Degraded

If “**Add Backup if Above Are Down**” (Figure 36) is selected, start using Backup link(s) if both primary & secondary underlay tunnels are unavailable (underlay tunnels are down).

Build SD-WAN Using These Interfaces

Primary

Cross Connect

INET1Group1

INET2Group1

MPLS1Group2

MPLS2Group2

Add Secondary if Primary Are

Down

Secondary

EXT1Group1

EXT2Group1

Add Backup if Above Are

Down

Backup

LTENone

Figure 36 – Backup Link Selection When Primary and Secondary Down

If “**Add Backup if Above Are Not Meeting Service Levels**” (Figure 37) is selected, start using secondary link(s) if both primary & secondary underlay tunnels exceed the configured “Service Level Objective”.

Build SD-WAN Using These Interfaces

Primary

Cross Connect

INET1Group1

INET2Group1

MPLS1Group2

MPLS2Group2

Add Secondary if Primary Are

Down

Secondary

EXT1Group1

EXT2Group1

Add Backup if Above Are

Not Meeting Service Levels

Backup

LTENone

Available Interfaces

LAB2

EXT3

INET3

LAB1

Service Level Objective

Loss

< 20

%

Latency

< 300

ms

Jitter

< 20

ms

Figure 37 – Backup Link Selection When Primary and Secondary Degraded

NOTE: SD-WAN tunnels (underlay tunnels) are built using all the provisioned WAN labels (Primary, Secondary, and Backup) and are in a state of “ready-to-use”. The UT that will be used is determined on a packet-by-packet basis.



4.2 Link Bonding Policy Attributes

Each Link Bonding Policy includes the following attributes:

Link Bonding Policy				
High Availability <ul style="list-style-type: none"> Failover 0sec Use Best Quality Path Path Conditioning BW Efficiency 50% 	High Quality <ul style="list-style-type: none"> Failover <1sec Use Best Quality Path Path Conditioning BW Efficiency >80% 	High Throughput <ul style="list-style-type: none"> Failover <1sec Load Balance Paths Path Conditioning BW Efficiency >80% 	High Efficiency <ul style="list-style-type: none"> Failover <1sec Load Balance Paths BW Efficiency 100% 	Custom <ul style="list-style-type: none"> FEC Wait Time: 80 ms Path Conditioning: 2%... Link Selection: Waterfa...
Hide Details				
1 FEC Wait Time 2 Exclude Links 3 Link Reorder Frequency 4 Path Conditioning 5 Packet Reorder Wait time	2ms On overlay brownout Moderate 100%-100% 5ms-100ms			6 Link Selection Waterfall: Overall Quality

- FEC Wait Time** is a transmit-side attribute. It indicates how long the sender should integrate data (payload) packets before sending the computed FEC packets. This results in a design trade-off between latency (wait longer to send FEC packet) and overhead (wait less time but send more FEC packets). This is less of a factor for busy links in which a lot of data is being sent.
- Exclude Links** specifies when an underlay tunnel is declared as "not meeting service level objectives" (degraded). If you choose **On overlay brownout**, a tunnel is excluded only when both underlay and overlay exceed the service level objectives. Otherwise (**On underlay brownout**), the tunnel is removed as soon as the underlay tunnel crosses the threshold(s).
- Link Reorder Frequency** controls how aggressively the underlays and switch traffic from one link to another are evaluated. Moderate mode of reorder frequency is applied in all four pre-configured bonding policies.
- Path Conditioning (FEC Overhead)** specifies the ratio of FEC packets to data (payload) packets. When adaptive FEC is employed, this will be a range specifying minimum and maximum FEC ratios.
- Packet Reorder Wait Time** is a receive-side attribute. It indicates how long the receiver should wait (and keep packets in a buffer) for an out-of-order packet. This results in a design trade-off between latency through EdgeConnect while waiting for packets and potentially dropping packets if received after the window. **NOTE:** Packet sequencing is on an overlay-tunnel basis.
- Link Selection (Waterfall or Balanced)** specifies whether the Overlay Tunnel Link Bonding policy queues packets into the "best Underlay Tunnel" or queues packets according to a path-loading scheme without regard to "best" ranking.

4.2.1 Link Selection – Waterfall

The waterfall method of link selection uses a rank-ordered list of eligible underlay tunnels (UTs) to determine where to send overlay payload and FEC packets. The ranking orders UTs by a default quality metric that is a weighted average of packet loss and latency measured on each UT.

Another metric is bandwidth availability on the UT as inferred or derived from the UT's outbound queue length. Traffic (payload) packets for an overlay tunnel will be placed in the best UT (as defined by the quality metric). FEC packets will be placed in the next-best UT that has available capacity. HA and HQ bonding policy uses the waterfall method of link selection. Specific examples are covered in the HA and HQ bonding policies explained later in this document.

4.2.2 Link Selection – Balanced

The balanced method of link selection does not use a rank-ordering of available tunnels but loads balance packets across available UTs. It will either aim to balance available capacity or purely load balance in proportion to UT bandwidth. HT and HE bonding policy uses the balanced method of link selection. Specific examples are covered in the HT and HE bonding policies explained later in this document.



4.3 Forward Error Correction

Forward Error Correction (FEC) has been used in telecommunications and transmission systems for many years wherein extra coded information is sent along with the payload traffic. The receiver uses the extra information to correct for errors introduced in the communications channel. In modern systems, errors result in packet loss, which are typically the result of network congestion. With all forward-acting, error-correcting codes, there is a trade-off in the amount of bandwidth added with FEC codes and the amount of error recovery by the receiver at the far end. EdgeConnect offers the choice of four bonding policies to best align end-user application performance requirements with underlying network resources.

FEC ratio relative to payload traffic is based on the Link Bonding Policy as follows:

- HA with greater than one primary link: FEC ratio is fixed at 1:1 (bandwidth efficiency of 50%).
- HA with single primary link: FEC is adaptive, and FEC ratio is from no FEC to 1:5. **NOTE:** HA operation with one underlay link is the same whether the given instance is configured with only one link or is operating with only one link as the result of other primary link(s) in a failed/degraded state.
- HQ FEC ratio is adaptive from a minimum of 1:40 to a maximum of 1:5 (bandwidth efficiency greater than 80%).
- HT FEC ratio is adaptive from no FEC to a maximum of 1:5 (bandwidth efficiency greater than 80%).
- HE has no FEC.

4.4 Underlay Tunnel Eligibility, Selection, Link Scoring, and Utilization

Traffic to destinations within the SD-WAN fabric typically use an overlay tunnel (OT) for transport. A given overlay has one or more associated underlay tunnels (UTs). When placing a packet into an underlay tunnel, three factors are considered:

1. Is the UT eligible (i.e., not in Down or Degraded state due to high latency or jitter or loss)?
2. What is its ranking as “best link”?
3. Does it have available capacity?

4.4.1 Underlay Tunnel Eligibility Based on SLO

Tunnel Degraded (Brownout) state is determined by the Service Level Objective (SLO) as defined in the Business Intent Overlay section. This setting can be configured as a Global setting or modified on a Regional basis. If regional settings are provisioned, EdgeConnect in that region use that specific SLO to determine UT Brownout state.

Overlay Configuration

Name: RealTime Match: Overlay ACL DSCP ef, Application RingCentral, Application ...

Region: Global

SD-WAN Traffic to Internal Subnets Breakout Traffic to Internet & Cloud Services

Topology: Regional Hub & Spoke

Hubs: US-East Hub-East, US-West Hub-West, US-Central, India, Australia

Build SD-WAN Using These Interfaces

Primary: MPLS2, INET1, INET2, LAB1

Cross Connect: None, Group1, Group1, None

Add Backup If Above Are: Down

Backup: LTE

Available Int: MPLS1

Service Level Objective: Loss < 5%, Latency < 200 ms, Jitter < 0 ms

Show Secondary

4.4.2 Degraded Underlay Determination When Exceeding Loss Threshold

An **underlay tunnel** that exceeds its **loss** threshold (provisioned under SLO of the BIO) will still be marked as eligible and will continue to be used for HA, HQ link bonding policies. If an associated **overlay tunnel** exceeds its loss threshold, the offending underlay tunnel will be disqualified and marked as ineligible. The reasons will be clearly explained in subsequent sections. Actions are summarized as follows:

- If a given underlay tunnel (UT) is not meeting service levels (Brownout) due to loss and the overlay tunnel (OT) is still meeting service levels, the UT remains marked as eligible. This only applies to High Availability (HA) and High Quality (HQ) link bonding policies.
- If a given underlay tunnel (UT) is not meeting service levels (Brownout) due to loss with the High Efficiency (HE) or High Throughput (HT) link bonding policy, the UT is marked as ineligible.
- If a given underlay tunnel (UT) is not meeting service levels (Brownout) due to latency or jitter, the UT is marked as ineligible.
- If **all** primary underlay tunnels are not meeting service levels (Brownout), backup links are added to the eligible list.
- If at least one primary link comes out of degraded state, all backup links are removed from the eligible list.

4.4.3 Underlay Sorting

Figure 38 shows an EdgeConnect appliance that has five underlay tunnels. UT1 and UT2 are both good (therefore, eligible for consideration). UT3 is in Degraded condition due to packet loss. It is still in contention to be eligible pending the status of its associated overlay tunnels.

The inclusion of a UT that is in Brownout state due to packet loss is determined independently for each overlay that uses that specific UT.

UT4 is degraded due to exceeding the overlay's latency or jitter threshold (therefore, marked as ineligible).

UT5 is down as driven by either the Path Fail mechanism or Tunnel Health mechanism (therefore, marked as ineligible).

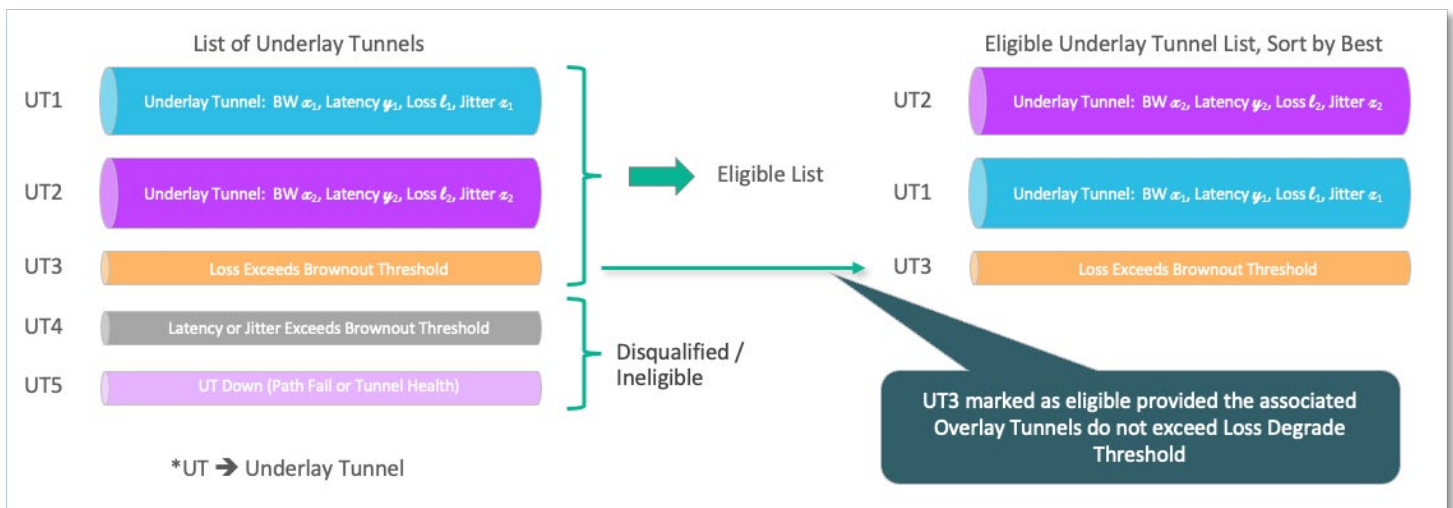


Figure 38 – Underlay Tunnel Eligibility and Selection Ranking

4.4.4 Underlay Selection

Tunnel selection differs based on bonding policy.

High Availability (HA) and High Quality (HQ)

- Uses underlay tunnel quality metric whereby payload traffic is sent over the “best link”. Underlay tunnel quality is determined as a function of latency and packet loss over an integration interval of five seconds. In the figure above (Figure 38), UT2 is considered better than UT1.
- Another important concept is the notion of “waterfall”. Assume all link conditions are stable (no degradation). If the overlay queue back pressure (wait time) is greater than the threshold, waterfall to next-best link (Figure 39). The rationale is to place a given flow on the best possible link that has available bandwidth. HA and HQ link bonding policies will use the Waterfall method to transport payload and FEC packets.

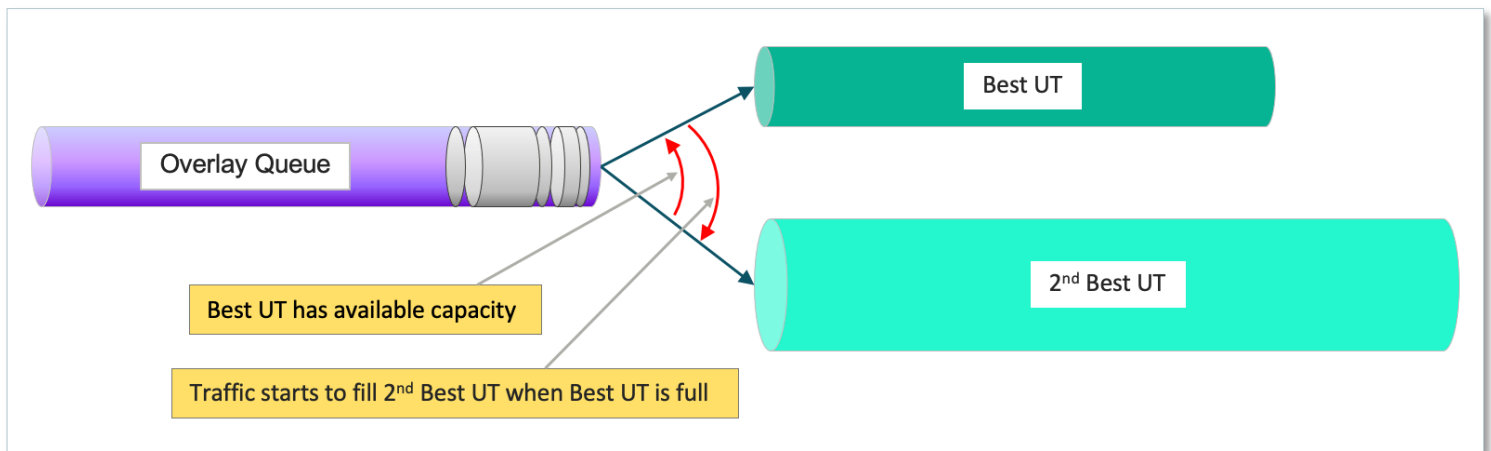


Figure 39 – Underlay Tunnel Waterfall for HA & HQ Bonding Policies

High Throughput (HT)

- Load balances across UTs without regard to best-link scoring
- Load balances traffic based on link capacity

High Efficiency (HE)

- Fills traffic on a round-robin basis without regard to best-link scoring
- UTs are filled on a round-robin basis proportional to available bandwidth

NOTE: These decisions are on a packet-by-packet basis. If a flow is long lasting, the link bonding policy will place it on the best link with available capacity for each packet.



4.5 Underlay Tunnel Bandwidth Negotiation

Underlay tunnel bandwidth is negotiated with the remote EdgeConnect based on the configured bandwidth of the port. Bandwidth is the minimum of [local, remote] for each direction as the following figure shows.

In this scenario, EC-A has a 20 Mbps uplink speed and a 50 Mbps downlink speed. EC-B has a 100 Mbps uplink spend and a 75 Mbps downlink speed. The underlay tunnel will be negotiated between the two appliances in each direction and the lowest possible capacity will be determined as the underlay bandwidth. In this example, the underlay will have 20 Mbps uplink bandwidth and 50 Mbps downlink bandwidth.

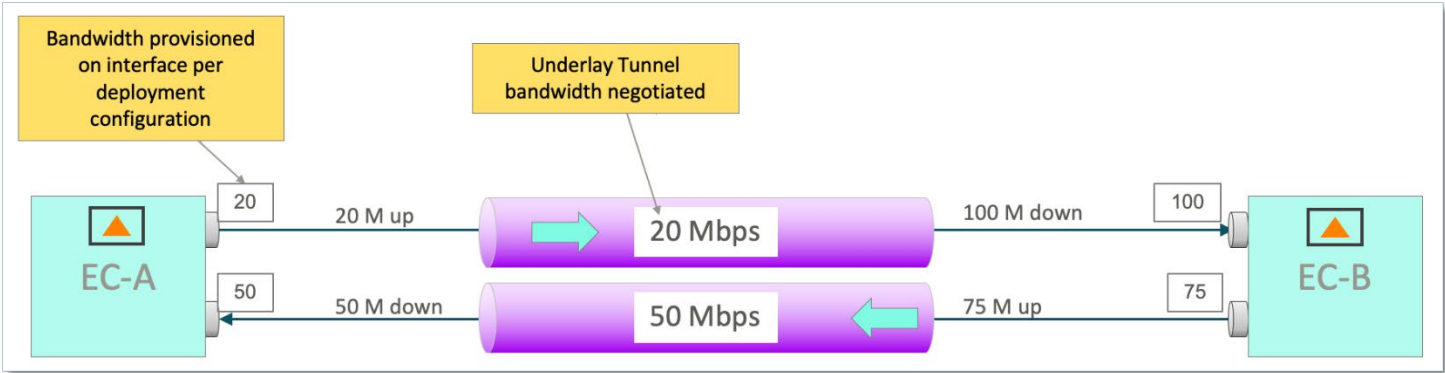


Figure 40 – Underlay Tunnel Bandwidth Negotiation

4.6 End-to-End Overlay Mapping for SD-WAN Traffic

Underlay tunnels within an overlay have no flow stickiness. Flows are switched packet-by-packet based on constantly changing underlay conditions. Therefore, EdgeConnects do not maintain flows on the same underlay tunnel (no session affinity). However, the EdgeConnect has a “Maintain end-to-end overlay mapping” behavior, which ensures that flows are always kept on the same overlay tunnel (e.g., RealTime overlay) when traffic is forwarded on multiple nodes.

The following figure shows the **System Setting** page on which the **Maintain end-to-end Overlay mapping** is configured.

System Information - Torrance-Liptzin

System Summary

System Settings

General

Model

EC-V 208003003003 Rev 86005

Serial

001BBC1CFE81

Site Name

Torrance-Liptzin

Hub Site?

No

Contact Name

Russell Liptzin

Contact Email

russell.liptzin@hpe.com

Location

1616 W 221st Street, Wilmington, Calif

Region

WEST

Optimization

IP Id auto optimization

☐

TCP auto optimization

☐

Flows and tunnel failure

fail-stick

Network Memory

Encrypt data on disk

☒

Configured Media Type

ram and disk

Media Type

ram and disk

Shell Access

Shell Access Status

Open Shell Access

Excess Flow Handling

Excess flow policy

drop

Miscellaneous

SSL optimization for non-IPSec tunnels

☒

Bridge Loop Test

☒

Enable IGMP snooping

☐

Auto Flow Re-Classify

5

(0..65535) seconds

Always send pass-through traffic to original sender

☐

IPSec UDP Port

11121

Enable default DNS lookup

☒

Enable HTTP/HTTPS snooping

☒

Quiescent tunnel keep alive time

25

(1..65535) seconds

UDP flow timeout

90

(1..65535) seconds

Non-accelerated TCP Flow Timeout

3600

(1..65535) secs

Maximum TCP MSS

1200

(500..9000) bytes

NAT-T keep alive time

60

(0..65535) seconds

Tunnel Alarm Aggregation Threshold

No Aggregat

Tunnel Alarms

Raise only 1 alarm above this threshold

Maintain end-to-end overlay mapping

☒

IP Directed Broadcast

☐

Allow WAN to WAN routing

☒



4.7 High Availability (HA) and High Quality (HQ) Operation

HA and HQ operations with respect to UT selection are the same. The only difference is with FEC ratio. With HA and HQ, underlay tunnels (UTs) are sorted based on the “best” quality metric.

Common attributes of HA and HQ bonding policy attributes follow:

- Sends user’s payload data packets on best UT.
- Sends FEC on next-best UT.
- Excludes link from selection when only overlay is in brownout condition.
 - If a given underlay tunnel (UT) is not meeting service levels (Brownout) due to loss, and the overlay tunnel (OT) is still meeting service levels, the UT remains marked as eligible.
- Links are ranked and sorted based on Overall Quality. The Overall Quality is a metric that uses a combination of latency and loss.
- If best UT is full, “waterfall” payload to next-best UT.
 - UT full is determined by measuring queue wait time (back pressure).
 - When the queue wait time exceeds 5 ms, UT full is determined and waterfall starts.
 - FEC moves to next UT down the list.

4.7.1 High Availability (HA) Link Bonding Policy Attributes

HA bonding policy is most suitable for RealTime traffic (e.g., voice) because it offers 1:1 FEC to ensure a seamless user experience. Due to FEC (Path Conditioning) being set at 100%, the effective throughput is reduced to 50%. It does not use per-packet load balancing. Sends the payload over the best underlay tunnel and sends FEC packets on the second-best underlay tunnel.

Link Bonding Policy

High Availability

- Failover Osec
- Use Best Quality Path
- Path Conditioning
- BW Efficiency 50%

High Quality

- Failover <1sec
- Use Best Quality Path
- Path Conditioning
- BW Efficiency >80%

High Throughput

- Failover <1sec
- Load Balance Paths
- Path Conditioning
- BW Efficiency >80%

High Efficiency

- Failover <1sec
- Load Balance Paths
- BW Efficiency 100%

Custom

- FEC Wait Time:
- Path Conditioning:
- Link Selection:

Hide Details

FEC Wait Time

2ms

Exclude Links

On overlay brownout

Link Reorder Frequency

Moderate

Path Conditioning

100%-100%

Packet Reorder Wait time

5ms-100ms

Link Selection

Waterfall: Overall Quality

Link Bonding Attribute	High Availability
Packet Reorder Time	5ms-100 ms
Exclude Links	On overlay brownout (exclude a tunnel when both underlay and overlay exceeds SLO)
FEC Wait Time	2 ms
Path Conditioning (FEC overhead)	100%
Link Selection	Best Link based on Overall Quality Waterfall to next best when link is full

4.7.2 HA Operation Over a Single Link

Business Intent Overlay policies are applied globally to all EdgeConnect instances that are members of that overlay. However, some nodal attributes are unique to a given site or instance (namely, the number of WAN underlays and the provisioned bandwidth of those Underlay Links). As mentioned above, when a node has multiple Underlay Links, HA operates with 100% FEC (normally with payload on one link and FEC on a different link). When an EdgeConnect instance has only one primary link, FEC is adaptive with the FEC ratio operating from no FEC to 1:5 (i.e., 20%). **NOTE:** HA operation with one underlay link is the same whether the given instance is configured with only one link or is operating with only one link as the result of other primary link(s) in a failed/degraded state.



Figure 41 – HA Operation Over Single UT



4.7.3 High Quality (HQ) Link Bonding Policy Attributes

HQ bonding policy should be used as a default selection for all traffic classes except RealTime traffic. It differs from High Availability only in terms of FEC. HQ uses adaptive FEC where the overhead is anywhere between 2% to 20%. It provides the best possible user experience in real-time as network conditions change. It offers the best use of available circuit capacities.

Link Bonding Policy					Link Bonding Attribute	High Quality
High Availability	High Quality	High Throughput	High Efficiency	Custom	Packet Reorder Time	5ms-100ms
<ul style="list-style-type: none">Failover <1secUse Best Quality PathPath ConditioningBW Efficiency 50%	<ul style="list-style-type: none">Failover <1secUse Best Quality PathPath ConditioningBW Efficiency >80%	<ul style="list-style-type: none">Failover <1secLoad Balance PathsPath ConditioningBW Efficiency >80%	<ul style="list-style-type: none">Failover <1secLoad Balance PathsBW Efficiency 100%	<ul style="list-style-type: none">FEC Wait Time:Path Conditioning;Link Selection:	Exclude Links	On overlay brownout (exclude a tunnel when both underlay and overlay exceeds SLO)
Hide Details					FEC Wait Time	80ms
Link Selection					Path Conditioning (FEC overhead)	2% - 20% (adaptive)
FEC Wait Time	80ms				Link Selection	Best Link based on Overall Quality Waterfall to next best when link is full
Exclude Links	On overlay brownout					
Link Reorder Frequency	Moderate					
Path Conditioning	2%-20%					
Packet Reorder Wait time	5ms-100ms					

4.7.4 HA and HQ Example 1 – Payload Fits in Best UT

In example 1, the offered payload traffic bandwidth (P) is less than the available capacity in the best UT.

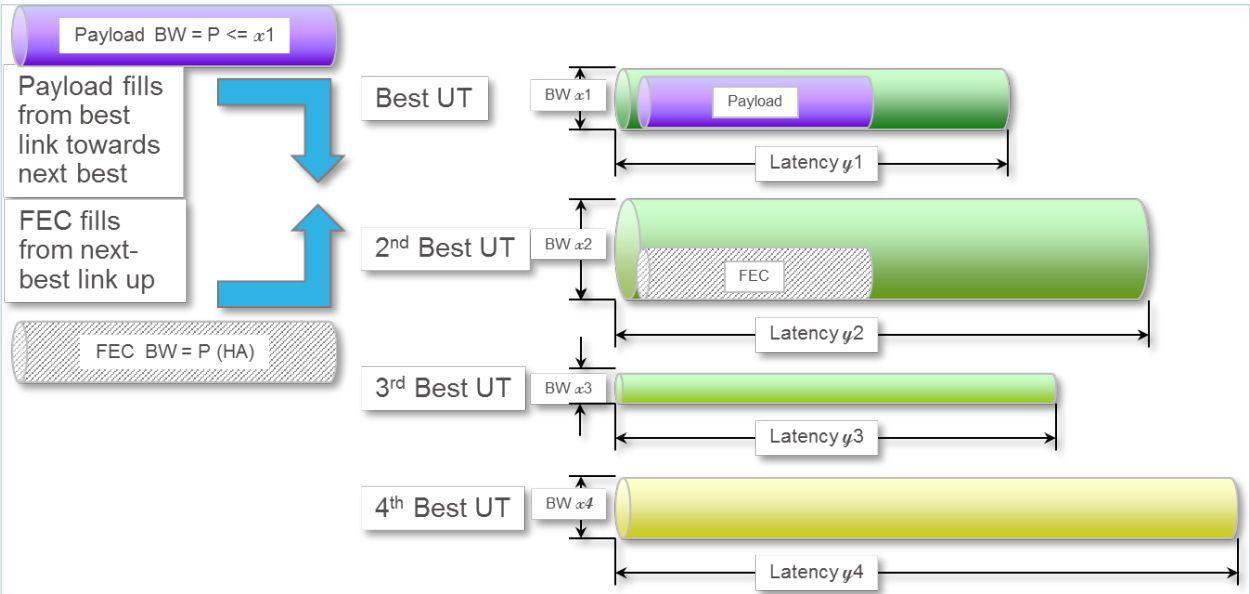


Figure 42 – HA, HQ Example 1; Payload on Best UT

In the example shown above, there are a total of four eligible UTs. The payload fits in the best UT, and all FEC packets go in the second-best UT.



4.7.5 HA and HQ Example 2 – Payload “Waterfalls” to Next-best Link; FEC Moves to Third UT

For example 2, the offered payload traffic bandwidth (P) is greater than the available capacity in the best UT (UT1). Therefore, the payload traffic must waterfall to the next-best UT (UT2). In general, it is preferable to not send FEC and payload on the same link unless necessary. In the same fashion, FEC does not fit on the third-best UT (UT3) (therefore “waterfalls up to UT2”). A simpler way to think about this is that for a given packet, if payload is on UT1, FEC is on UT2. When payload waterfalls to UT2, FEC moves to UT3.

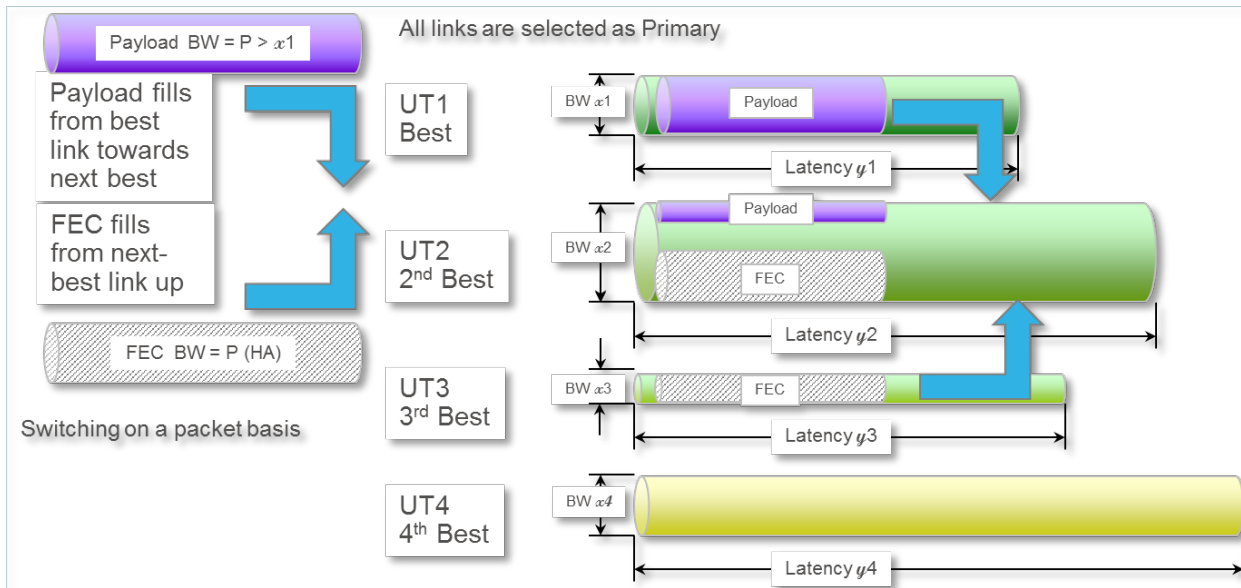


Figure 43 – HA, HQ Example 2; Payload Waterfalls to Next-best UT

4.7.6 HA and HQ Example 3 – 2 Underlay Tunnels; Payload + FEC Both Fit

For example 3, there are two underlay tunnels, and payload + FEC is less than available UT Bandwidth. In this case, the best UT has less bandwidth than the second-best UTb, which carries both payload and FEC.

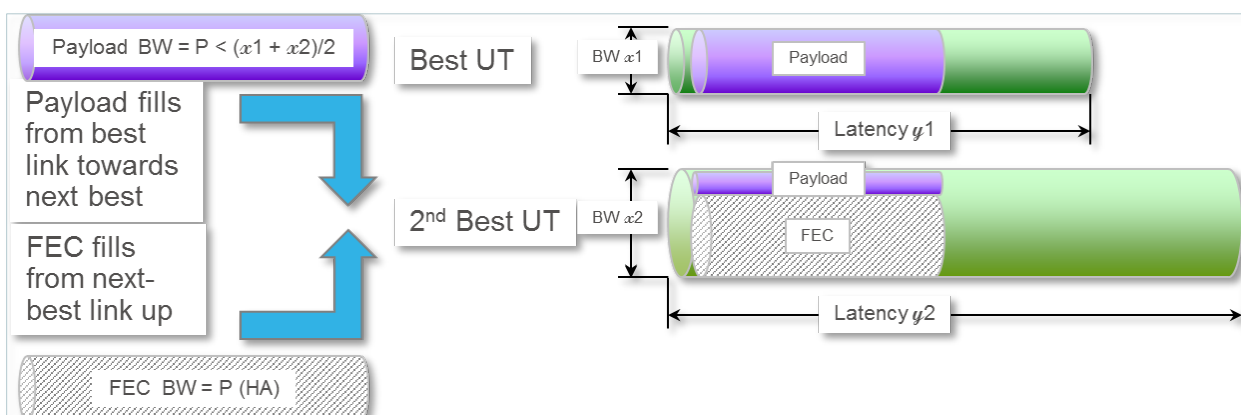


Figure 44 - HA, HQ Example 3; Payload and FEC Share Second Best UT

4.7.7 HA and HQ Example 4 – 2 Underlay Tunnels; Payload + FEC Do NOT Fit

For example 4, there are two underlay tunnels, and payload + FEC is greater than available UT bandwidth. In this case, there is not enough available bandwidth for both payload and FEC. The excess payload is dropped after waiting in the shaper queue up to the configured Max Wait Time interval for that shaper.

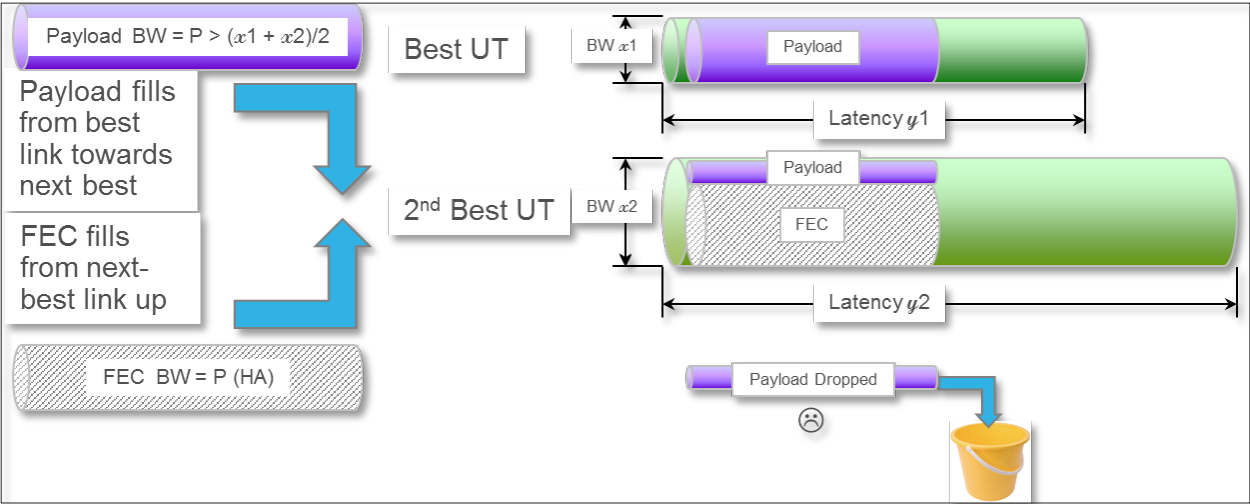


Figure 45 – HA, HQ Example 4; Payload and FEC Exceeds UT Capacity

For example, if the above payload is matched to a “RealTime” BIO, corresponding shaper “Traffic Class – Real Time” will play a role in determining when the packet is dropped.

In the following example (Figure 46), the packet will be dropped after a maximum wait time of 250 ms in the shaper queue.

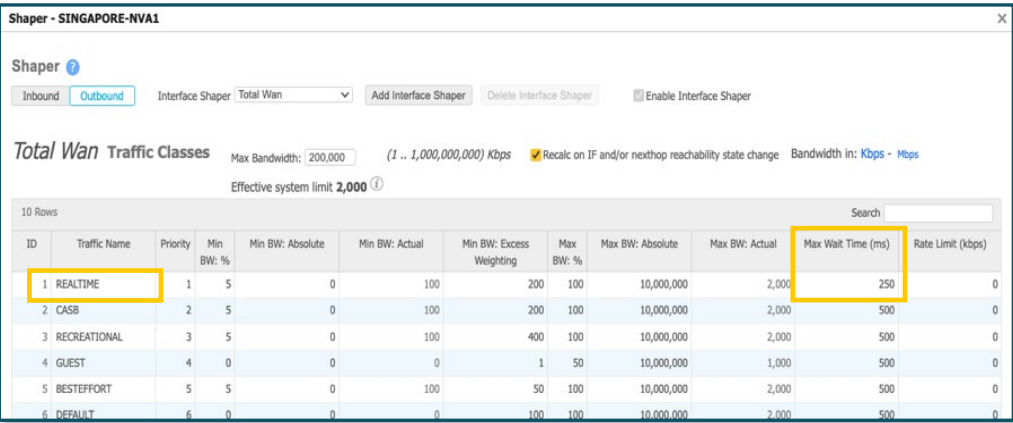


Figure 46 – Max Wait Time Setting on Shaper Config

4.7.8 HA and HQ Example 5 – Utilization of a Browned-out Underlay Tunnel (R8.1.9.5+ Behavior)

Figure 47 illustrates the benefit of keeping a UT marked as eligible even though it might be degraded for loss past the threshold. In this case, the payload P (see Figure 47) can fully utilize the best UT. FEC packets are placed in the second UT. This allows FEC packets to utilize the degraded tunnel while giving the payload packets the best tunnels full bandwidth.

NOTE: The use of a degraded UT only applies to loss conditions (given that the overlay tunnel is still meeting the loss SLA). If UTs are browned-out due to latency or jitter, they will be disqualified because latency or jitter cannot be fixed with FEC.

HA, HQ EXAMPLE 5; PAYLOAD FITS IN BEST UT;
2ND BEST UT IS IN BROWNOUT AND STILL USED

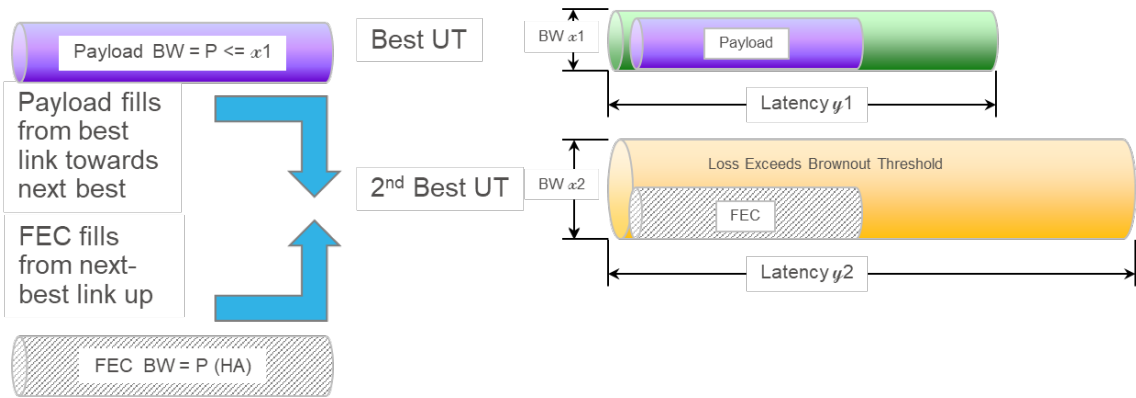


Figure 47 – HQ, HQ Payload on Best UT and Degraded UT in Use

4.8 High Throughput (HT) Operation

HT operation sends user’s payload data packets + FEC across all eligible UTs.

- There is no differentiation between payload and FEC
- Uses adaptive FEC – Ranges from 0% to 20%
- UTs are not scored by “best”
- Load balances across all paths based on the Link Capacity
- Packet order correction is performed
- Excludes links when the underlay crosses the configured Service Level Objective thresholds (setting on BIO)

Link Bonding Policy					Link Bonding Attribute	High Throughput
High Availability	High Quality	High Throughput	High Efficiency	Custom	Packet Reorder Time	5ms-100ms
<ul style="list-style-type: none">• Failover 0sec• Use Best Quality Path• Path Conditioning• BW Efficiency 50%	<ul style="list-style-type: none">• Failover <1sec• Use Best Quality Path• Path Conditioning• BW Efficiency >80%	<ul style="list-style-type: none">• Failover <1sec• Load Balance Paths• Path Conditioning• BW Efficiency >80%	<ul style="list-style-type: none">• Failover <1sec• Load Balance Paths• BW Efficiency 100%	<ul style="list-style-type: none">• FEC Wait Time:• Path Conditioning:• Link Selection:	Exclude Links	On underlay brownout (exclude a tunnel when the underlay exceeds SLO)
Hide Details					FEC Wait Time	80ms
Link Selection					Path Conditioning (FEC overhead)	0% - 20% (adaptive)
Balanced: Link Capacity (Local)					Link Selection	Balance available link capacity
FEC Wait Time	80ms					
Exclude Links	On underlay brownout					
Link Reorder Frequency	Moderate					
Path Conditioning	0%-20%					
Packet Reorder Wait time	5ms-100ms					

Assuming UTs have different available bandwidths, the UT with the higher available bandwidth is filled until its available bandwidth is equal to the available bandwidth on the other UT. **NOTE:** The UT with highest available bandwidth is not necessarily the largest provisioned/configured UT because the instantaneous assessment is based on available bandwidth. When both UTs have the same available bandwidth, they are filled with packets in a round-robin fashion. As in the previous modes, overlays have no flow stickiness with respect to underlay tunnels.



4.8.1 HT Use Case

HT bonding policy should only be used when all underlay WAN characteristics are the same (Loss/Latency/Jitter). HT bonding policy is ideal for scenarios with payloads that have a low number of data replication flows and multiple WAN uplinks with identical bandwidth and latency.

Figure 48 one good underlay (low latency – 125 ms) and a bad underlay (high latency – 250 ms) used with HT mode. This would invariably impact the throughput because the packet arrives out of order due to the nature of HT mode using per packet load balancing. When traffic is load balanced with these asymmetric underlay characteristics (high latency or bandwidth), it results in the packet arriving out of order. This causes TCP to back off and sometimes causes TCP-Resets, which lead to user performance issues.

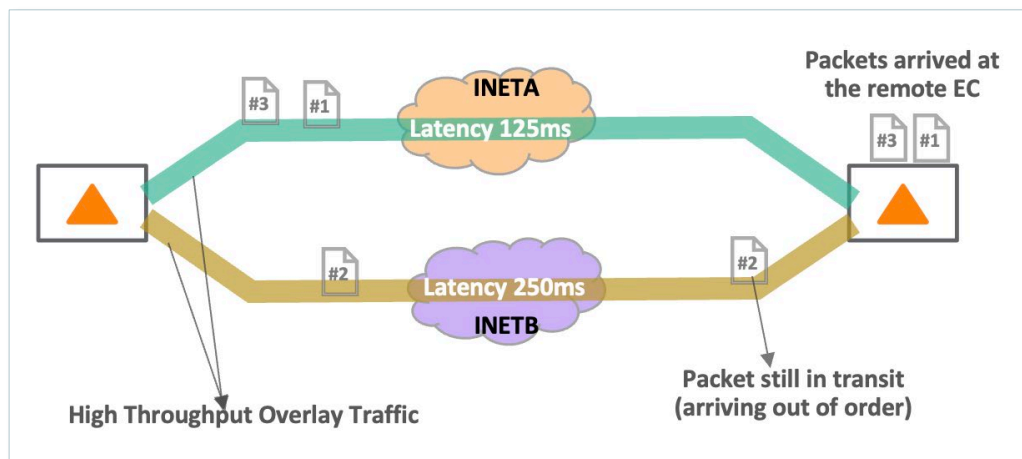


Figure 48 – HT Mode with Asymmetric Underlay Characteristic Causing Packet to Arrive Out of Order

In Figure 49, we can see similar WAN characteristics are in play. Using HT link bonding policy is beneficial in this case because both links are utilized equally.

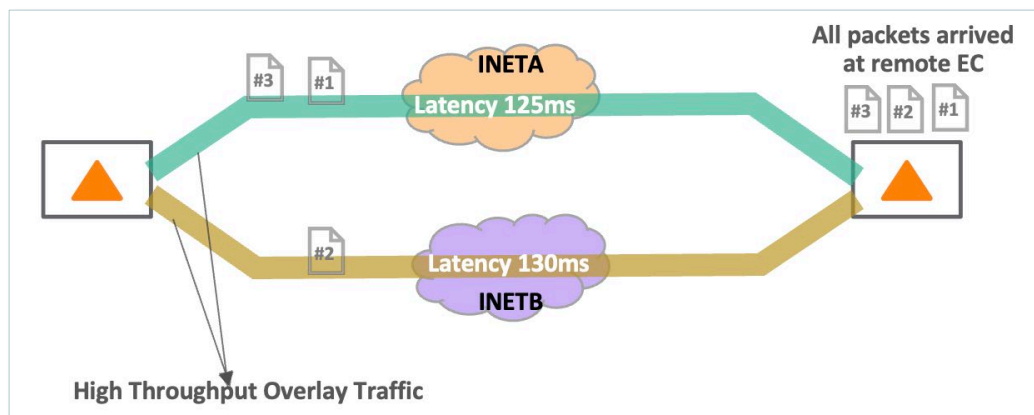


Figure 49 – HT Mode with Symmetric Underlay WAN Characteristics - All Packets Arriving Sequentially



4.8.2 Cross-connected Underlay Tunnels in HT Overlay

In the case of an HT BIO running over cross-connected tunnels on the same interface, the bonding policy behaves the same as HE. Traffic is distributed across both UTs in proportion to available UT bandwidth. The following figure illustrates where EC-A as an “MPLS-only” site connecting to EC-B, which is an MPLS & Internet site. Of course, Layer-3 reachability is required between the two underlays for cross-connect tunnels to function, so the notion of “MPLS” and “Internet” in the example is for illustration purposes only.

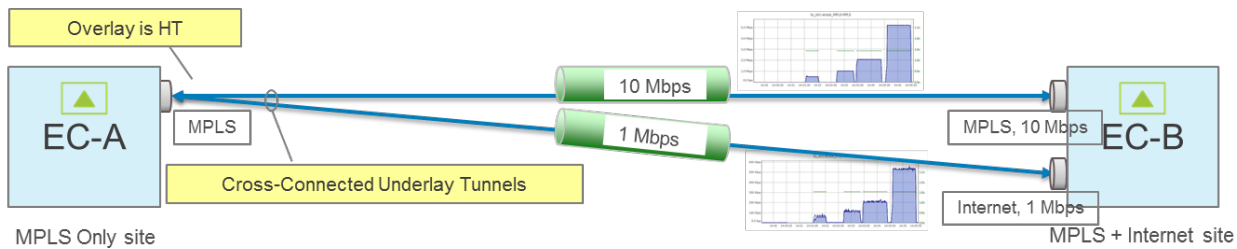


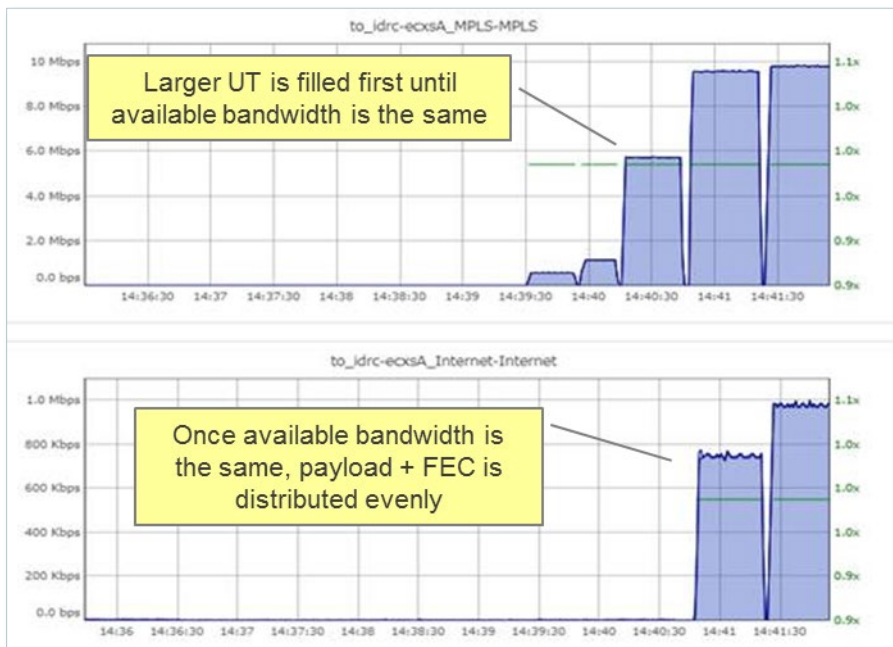
Figure 50 – HT Operation Over Cross-connected UTs

4.8.3 HT Example

An HT example follows. Two UTs are used:

- MPLS (x_1) = 10 Mbps
- Internet (x_2) = 1 Mbps

As illustrated in the following figure, traffic stays on UT with greater available bandwidth (MPLS) while payload is gradually increased up to 9 Mbps ($x_1 - x_2$). When the MPLS UT reaches the 9 Mbps mark, traffic starts to load balance between MPLS and Internet link.



NOTE: For cross-connected underlay tunnels, HT mode is the same as HE mode, as explained below.

Figure 51 – High Throughput Example

4.9 High Efficiency (HE) Operation

HE operation sends user’s payload data packets across all eligible UTs.

- There is no FEC, only payload
- Packet Order Correction is performed
- UTs are not scored by “best”
- UTs are filled on a round-robin basis proportional to available bandwidth
- Excludes links when the underlay crosses the configured Service Level Objective thresholds (setting on BIO)

Link Bonding Policy					Link Bonding Attribute	High Efficiency
High Availability	High Quality	High Throughput	High Efficiency	Custom	Packet Reorder Time	5ms-100ms
<ul style="list-style-type: none">• Failover 0sec• Use Best Quality Path• Path Conditioning• BW Efficiency 50%	<ul style="list-style-type: none">• Failover <1sec• Use Best Quality Path• Path Conditioning• BW Efficiency >80%	<ul style="list-style-type: none">• Failover <1sec• Load Balance Paths• Path Conditioning• BW Efficiency >80%	<ul style="list-style-type: none">• Failover <1sec• Load Balance Paths• BW Efficiency 100%	<ul style="list-style-type: none">• FEC Wait Time:• Path Conditioning:• Link Selection:	Exclude Links	On underlay brownout (exclude a tunnel when the underlay exceeds SLO)
Hide Details					FEC Wait Time	0ms
					Path Conditioning (FEC overhead)	NA
					Link Selection	Balance based on link utilization
Link Selection						
Balanced: Link Utilization (Local)						
FEC Wait Time	0ms					
Exclude Links	On underlay brownout					
Link Reorder Frequency	Moderate					
Path Conditioning	0%-0%					
Packet Reorder Wait time	5ms-100ms					

HE bonding policy should be used only when all underlays have equal WAN characteristics. More importantly, HE bonding policy is preferred when no loss is expected on the UT. Because no FEC packets are sent when HE bonding policy is used, any loss on the underlay would result in loss of payload.

HT and HE bonding policy do not guarantee the best user experience. Therefore, they should be avoided for most use cases. Preferably, you should use HQ for any non-RealTime traffic class.



4.9.1 HE Example

An HE example follows. Two UTs are used:

- MPLS (x1) = 10 Mbps
- Internet (x2) = 1 Mbps

Traffic is distributed equally between the two UTs in proportion to their bandwidth.



Figure 52 – High Efficiency Example

4.10 Custom Bonding Policy

The pre-defined HA, HQ, HT, and HE bonding policies should cover most of use cases in a typical enterprise network. Custom Bonding policy provides the ability to customize the link prioritization and traffic steering policies based on multiple criteria, including physical performance characteristics, link economics, link resiliency characteristics, and customer-definable attributes. It is recommended that you use one of the predefined bonding policies and only use the custom bonding policy when necessary.

Link Bonding Policy

High Availability

- Failover 0sec
- Use Best Quality Path
- Path Conditioning
- BW Efficiency 50%

High Quality

- Failover <1sec
- Use Best Quality Path
- Path Conditioning
- BW Efficiency >80%

High Throughput

- Failover <1sec
- Load Balance Paths
- Path Conditioning
- BW Efficiency >80%

High Efficiency

- Failover <1sec
- Load Balance Paths
- BW Efficiency 100%

Custom

- FEC Wait Time: 80 ms
- Path Conditioning: 2%...
- Link Selection: Waterfa...

Hide Details

FEC Wait Time

80 ms

Exclude Links

On overlay brownout

Link Reorder Frequency

Moderate

Link Selection

Waterfall

Overall Quality

Path Conditioning

Min 2 %

Max 20 %

Packet Reorder Wait Time

Min 5 ms

Max 100 ms

Link Bonding Attribute	Default Value (all the values customizable)
Packet Reorder Time	5ms - 100ms
Exclude Links	On overlay brownout (exclude a tunnel only when overlay exceeds SLO)
FEC Wait Time	80ms
Path Conditioning (FEC overhead)	2%-20%
Link Selection	Waterfall - Overall Quality



Custom bonding policy enables you to customize the following values depending on environmental needs:

4.10.1 FEC Wait Time (Default: 80ms)

Maximum time EdgeConnect waits to construct an FEC frame. EdgeConnect builds an FEC frame for a group of packets. Configuring this wait time determines how long the EdgeConnect should wait before sending the FEC frame out. A longer wait time reduces FEC overheads on the link, but it also increases the time it needs to reconstruct the packet. So, there is a trade-off between latency and overheads that will influence your decision. If the traffic is sensitive to latency, configure a lower value. If the link has lower bandwidth or expensive link, you might want to consider a larger FEC wait time.

4.10.2 Exclude Links (Default: On overlay brownout)

Determines when an EdgeConnect declares an underlay tunnel as “not meeting service level objective” (Degraded). There are two selections available:

- On overlay brownout – Only exclude a tunnel when both underlay and overlay exceed the service level objective thresholds.
- On underlay brownout – Exclude a tunnel as soon as the underlay tunnel crosses the service level objective thresholds.

4.10.3 Link Reorder Frequency (Default: Moderate)

Determines how quickly EdgeConnect reorders the links (underlay tunnels). There are three modes:

- Aggressive
- Moderate
- Conservative

EdgeConnect applies an algorithm using various available statistics to determine the threshold for each of the above modes.

Example: Two tunnels with the following initial values:

- Tunnel 1 – Loss 0% and Latency 0 ms
- Tunnel 2 – Loss 0% and Latency 10 ms

Loss and latency occur on the best tunnel (Tunnel 1). The following table shows (given some assumed increase on the loss/latency metrics) how quickly the EdgeConnect moves to the next tunnel (Failover Time) and how quickly recovery occurs when the latency/loss are recovered (Recover Time) on the tunnel.

	Loss 1% and Latency 20ms		Loss 5%, Latency 20ms		Loss 10%, Latency 20ms	
	Fail over time	Recover Time	Fail over time	Recover Time	Fail over time	Recover Time
Aggressive	7 seconds	19 seconds	5 seconds	21 seconds	4.5 seconds	23 seconds
Moderate	9.5 seconds	30 seconds	5.5 seconds	39.5 seconds	3.5 seconds	42 seconds
Conservative	12 seconds	23 seconds	6.5 seconds	35 seconds	6 seconds	41 seconds

Table 1 – Link Reorder Mode - Sample Failover/Recover Time



4.10.4 Path Conditioning (Default: Min 2% and Max 20%)

Minimum and maximum FEC percentage to the total data traffic. Using the slider for the Path Conditioning value, you can set the Min and Max FEC percentage. When the minimum and maximum values are set to the same value, it will be a fixed rate. Otherwise, the rate would be auto between the minimum and maximum range.

NOTE: When the overlay tunnel has only one eligible tunnel to use, the percentage (both minimum and maximum) will be capped to 20% if they are set higher, which preserves the bandwidth on the lone available link by avoiding overhead (FEC packets).

4.10.5 Packet Reorder Wait Time (Default: 100ms)

Maximum time EdgeConnect waits for a missed packet. EdgeConnect waits until the configured time for the out-of-sequence packet to arrive (to be considered for packet re-assembly). When the wait time expires, all missed packets are declared as lost packets.

4.10.6 Link Selection (Default: Waterfall – Overall Quality)

Determines how EdgeConnect distributes the payload on the underlay tunnels. There are two kinds of load balance policies available: Waterfall and Balanced.

Waterfall

The overlay's underlay tunnels will be sorted according to their metric (as selected below). The traffic will try to fill the best link first, and then waterfall to the next-best links. There are five metrics:

- **Overall Quality** – Best link is determined based on the overall quality metric. EdgeConnect uses an algorithm using latency, loss, and weight to determine the overall quality metric.
- **Latency** – Best link is selected based on the latency.
- **Loss** – Best link is selected based on the loss.
- **Jitter** – Best link is selected based on the jitter.
- **Link Order** – Best link is selected based on the order in which the links are configured on the BIO page (Figure 53).

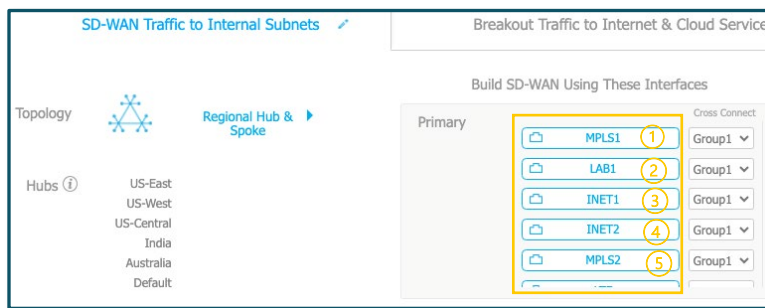


Figure 53 – Link Order on BIO Configuration

Balanced

The traffic will be load-balanced into all eligible tunnels by:

- **Link Capacity (Local)** – Traffic is sent on the underlay with the highest capacity.
- **Link Utilization (Local)** – Traffic is placed on the underlay based on the local interface utilization.
- **Link Utilization (Local & Remote)** – The best underlay is determined by using a combination of the local interface utilization value and the remote site's interface bandwidth utilization.

5 Link Bonding Policy for Internet & Cloud Services

EdgeConnect offers flexibility for granular breakout of internet traffic. Path selection for internet traffic can vary based on the preferred policy configured for Breakout Traffic to Internet & Cloud Services.

Under Business Intent Overlay, the **Preferred Policy Order** section indicates how a non-SD-WAN traffic finds its way to the destination. There are three types of internet policies that can be mapped to a preferred policy order:

1. Break Out Locally (also known as passthrough tunnels)
2. Backhaul Via Overlay (SD-WAN tunnel)
3. Service Tunnels (e.g., IPsec or GRE Tunnels to HPE-Axis-SSE, Zscaler, or Firewall...and so forth)

These policy methods will be detailed in sections 5.1 through 5.3.

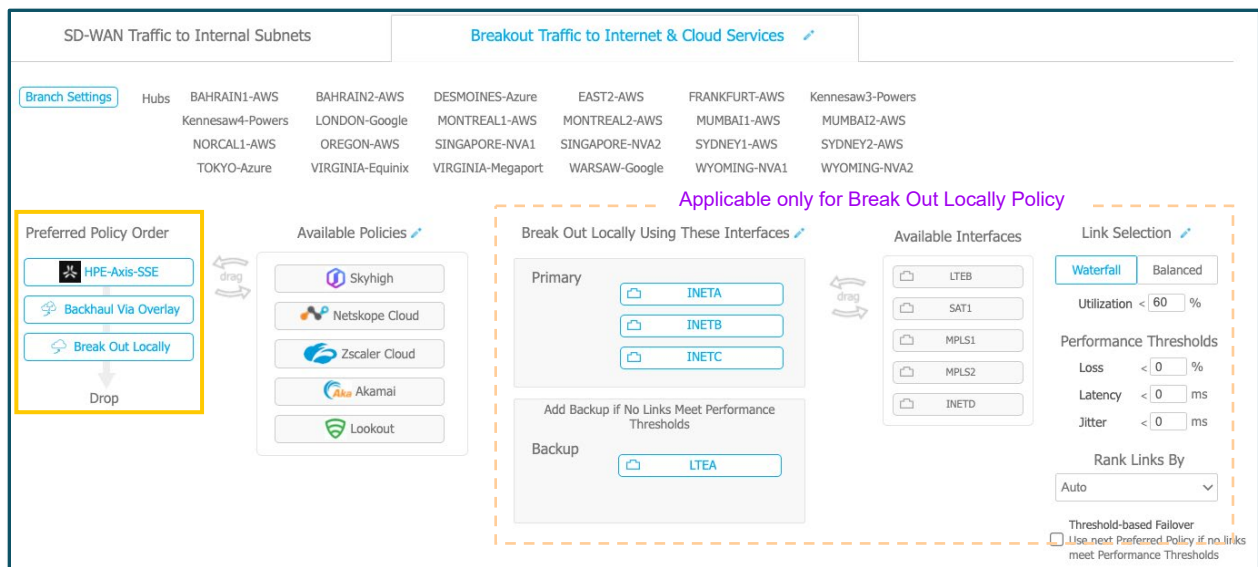


Figure 54 – Preferred Policy Order for a Business Intent Overlay

The order in which policies are placed matters in determining which path the “external” traffic takes. In the figure above (Figure 54), there are three preferred policies configured on the BIO. In this example, internet traffic will be sent over HPE-Axis-SSE Tunnel if the tunnel is available. If it is not available, traffic will be sent over an overlay tunnel to another EdgeConnect appliance or will break out locally when both SSE tunnel and overlay tunnel are unavailable. If no Preferred Policies are configured, the traffic will be dropped by default.

The other three columns on the BIO page (namely, “Break Out Locally Using These Interfaces”, “Available Interfaces”, and “Link Selection”) are relevant only when the Preferred Policy is set to “Break Out Locally”.

Preferred Policy Order can contain one or more policies (up to a maximum of 32).

5.1 Break Out Locally

Break Out Locally policy uses the WAN labels provisioned under the Primary and Backup sections on the BIO page. Traffic is sent on Best PT (passthrough tunnel), which is ranked by the metric (configurable) and spills over to the next-best PT when the link selection is set to “Waterfall”. Traffic can also be load balanced on all available/eligible PTs when link selection is set to “Balanced”.

The following flowchart (Figure 55) provides a walkthrough of an external traffic entering from the LAN side of an EdgeConnect. The Break Out Locally method maintains session affinity (i.e., traffic is always kept on the same WAN label for a given Internal_External IP pair per flow).

Break Out Locally policy can also use performance thresholds (latency/loss/jitter) and bandwidth utilization thresholds to exclude links from the path selection. The performance metrics are inferred values from the SD-WAN probe measurement. The following subsections (5.1.1 through 5.1.4) detail more characteristics of Break Out Locally policy.

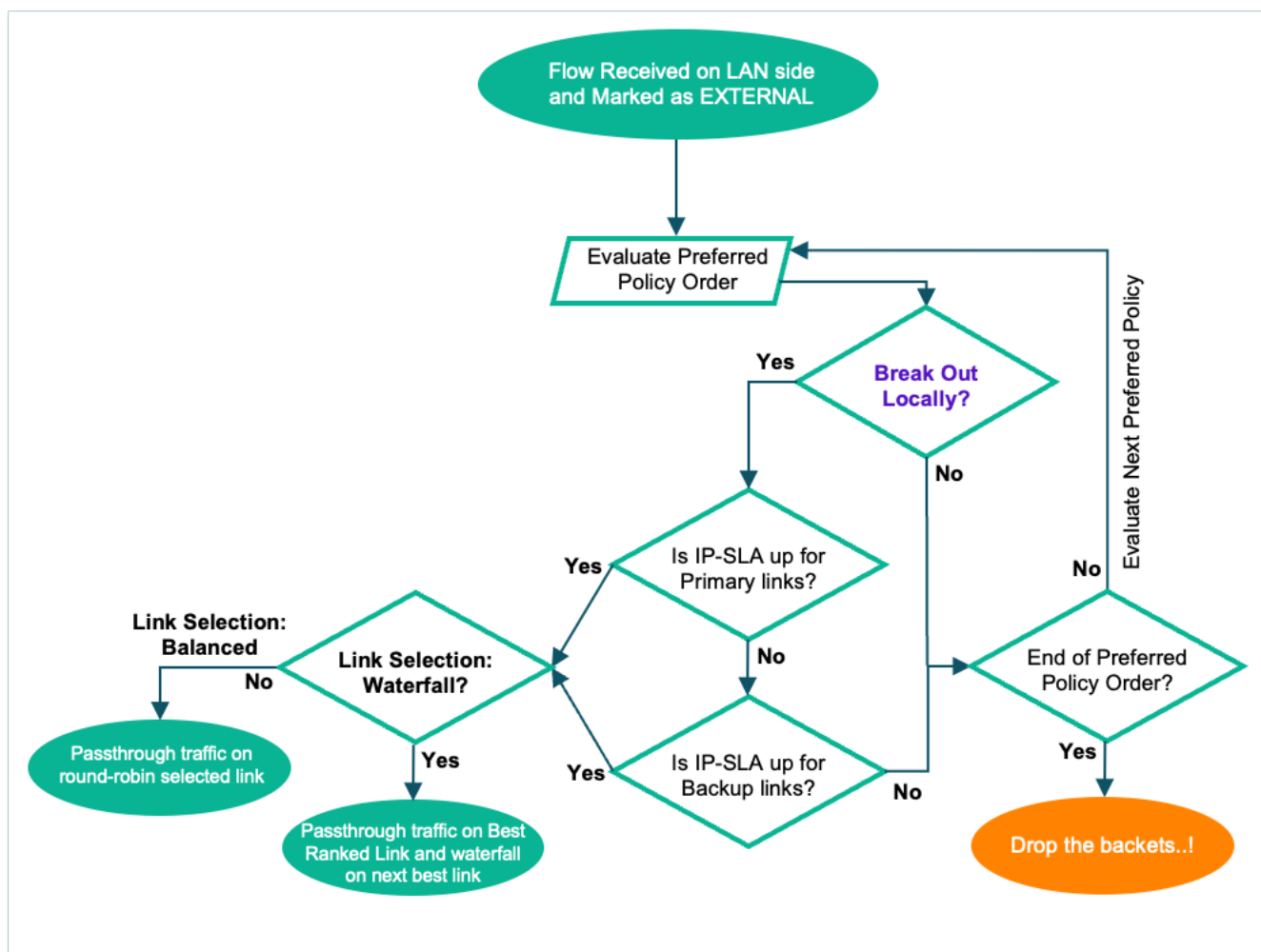


Figure 55 – Local Break Out (LAN to WAN Traffic Flow)



5.1.1 Break Out Locally Using These Interfaces

When the preferred policy order is provisioned with “Break Out Locally” policy, local breakout occurs using the WAN labels configured under the Primary and Backup sections of the “Break Out Locally Using These Interfaces” area.

SD-WAN Traffic to Internal Subnets

Breakout Traffic to Internet & Cloud Services

Branch Settings

Hubs

BAHRAIN1-AWS

BAHRAIN2-AWS

DESMOINES-Azure

EAST2-AWS

FRANKFURT-AWS

Kennesaw3-Powers

Kennesaw4-Powers

LONDON-Google

MONTREAL1-AWS

MONTREAL2-AWS

MUMBAI1-AWS

MUMBAI2-AWS

NORCAL1-AWS

OREGON-AWS

SINGAPORE-NVA1

SINGAPORE-NVA2

SYDNEY1-AWS

SYDNEY2-AWS

TOKYO-Azure

VIRGINIA-Equinix

VIRGINIA-Megaport

WARSAW-Google

WYOMING-NVA1

WYOMING-NVA2

Preferred Policy Order

HPE-Axis-SSE

Backhaul Via Overlay

Break Out Locally

Drop

Available Policies

Skyhigh

Netskope Cloud

Zscaler Cloud

Akamai

Lookout

Break Out Locally Using These Interfaces

Primary

INETA

INETB

INETC

Add Backup if No Links Meet Performance Thresholds

Backup

LTEA

Available Interfaces

LTEB

SAT1

MPLS1

MPLS2

INETD

Link Selection

Waterfall

Balanced

Utilization < 60 %

Performance Thresholds

Loss < 0 %

Latency < 0 ms

Jitter < 0 ms

Rank Links By

Auto

Threshold-based Failover

Use next Preferred Policy if no links meet Performance Thresholds

Starting with ECOS 9.3.1, a maximum of up to 32 WAN labels (primary and backup combined) can be provisioned per EdgeConnect appliance for local breakout traffic. Earlier releases have a maximum limit of 16 WAN labels.

EdgeConnect builds passthrough tunnels (PT) for each overlay per WAN label. If EdgeConnect has 4 x overlay (BIO) applied and has 2 x WAN labels provisioned, it builds eight PTs (Figure 56) in total that will be used to break out internet traffic.

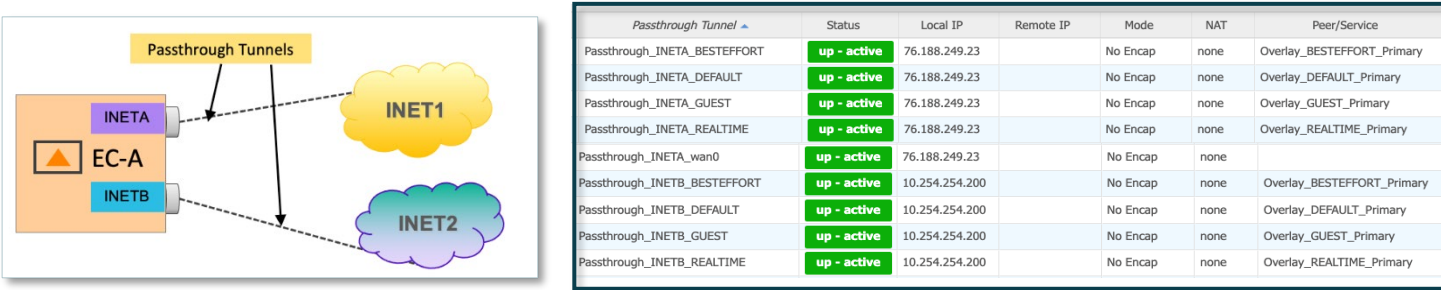


Figure 56 – Passthrough Tunnels on EdgeConnect

When next hop reachability and IP-SLA for the passthrough tunnels is UP, those PTs are considered for path selection. Which PT gets picked up for sending the internet traffic out is determined by the Link Selection section of the BIO. Link Selection determines when a link is marked ineligible and when the waterfall effect is triggered (refer to section 5.1.4 for more detail).



5.1.2 Passthrough Tunnel Eligibility for Local Breakout

When an EdgeConnect appliance has a Business Intent Overlay with Local Break Out policy, Orchestrator automatically pushes an IP-SLA rule for the passthrough tunnels for that overlay. For example, if an EdgeConnect has four Business Intent Overlays and two available WAN connections, it would have a total of eight IP-SLA probes monitoring the passthrough tunnels for the provisioned WAN labels.

EdgeConnect constantly checks the passthrough tunnels eligibility using IP-SLA probes (by default, it sends probes to 8.8.8.8,8.8.4.4 and sp-ipsla.silverpeak.cloud using ICMP every one second). A passthrough tunnel is deemed ineligible or marked down when the system detects no response for 30 probes to ALL destinations (8.8.8.8 and sp-ipsla.silverpeak.cloud). PTs become eligible/marked up after the system receives three responses. Stated otherwise, passthrough tunnel is still eligible when at least one of the probe destinations is actively responding to the probes.

The default IP-SLA Rule for passthrough tunnels can be modified under BIO (Breakout Traffic to Internet & Cloud Services → Pencil icon next to Break Out Locally Using These Interfaces).



The IP-SLA rule definition on the BIO page is a global setting. Modifying the rule in this very specific section would instantly push the configuration changes to all EdgeConnect appliances.

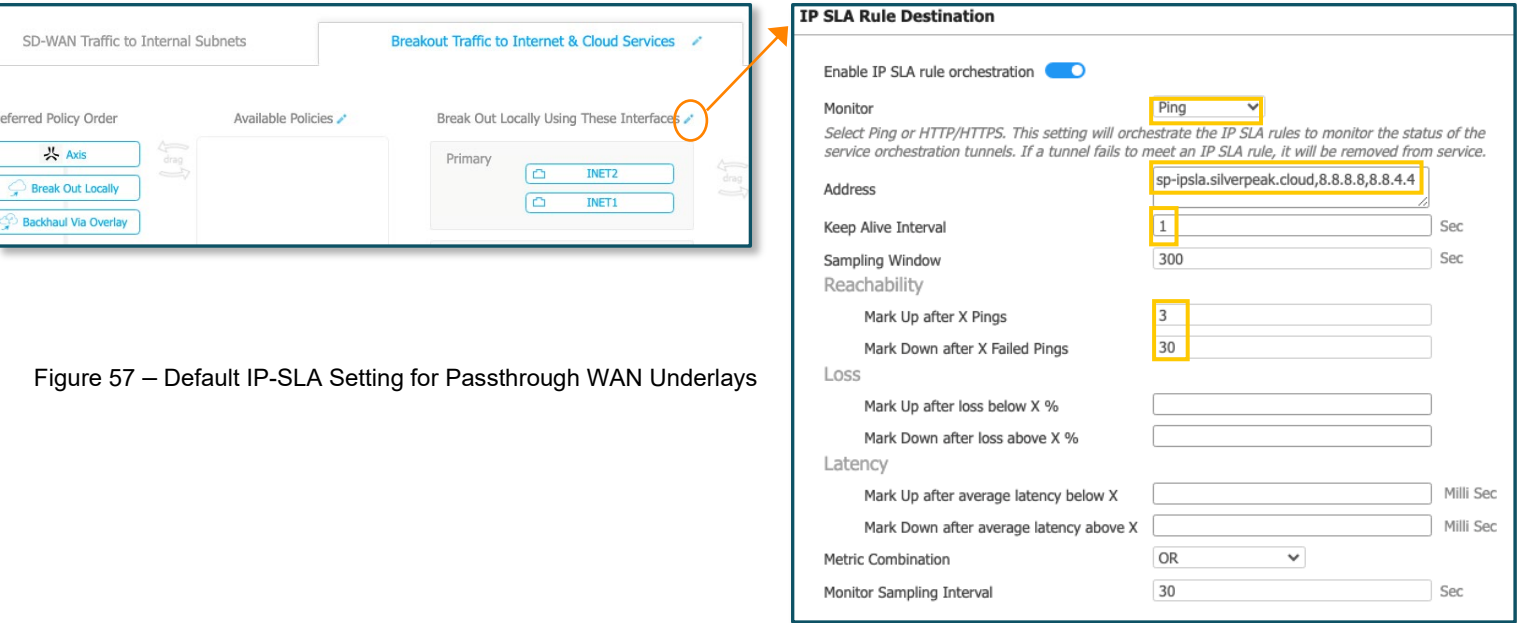


Figure 57 – Default IP-SLA Setting for Passthrough WAN Underlays

IP-SLA Trends for Loss and Latency for a given passthrough tunnel can be viewed under the Monitoring section of the Orchestrator UI (Monitoring → Performance → IP SLA Summary or Configuration → Templates & Policies → TCAs → IPSLA). Click the chart icon for a passthrough tunnel IP SLA (see Figure 58).

The following charts provide an understanding of how each passthrough tunnel has performed over a period of time. They can help you troubleshoot why one PT is preferred over the other available PTs.



IP SLA ?

8/12 Rows

Edit	Appliance	Active	State	Monitor	Down Action	Up Action	Charts
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET1_DefaultOverlay	Tunnel Up: Tunnel = Passthrough_INET1_DefaultOverlay	
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET2_BulkApps	Tunnel Up: Tunnel = Passthrough_INET2_BulkApps	
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET2_DefaultOverlay	Tunnel Up: Tunnel = Passthrough_INET2_DefaultOverlay	
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET1_RealTime	Tunnel Up: Tunnel = Passthrough_INET1_RealTime	
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET1_CriticalApps	Tunnel Up: Tunnel = Passthrough_INET1_CriticalApps	
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET1_BulkApps	Tunnel Up: Tunnel = Passthrough_INET1_BulkApps	
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET2_RealTime	Tunnel Up: Tunnel = Passthrough_INET2_RealTime	
	Branch-East	Yes	Up	Ping: Keep Alive Time = 1, IP = S	Tunnel Down: Tunnel = Passthrough_INET2_CriticalApps	Tunnel Up: Tunnel = Passthrough_INET2_CriticalApps	

Figure 58 – IP SLA Summary Page



Figure 59 – IP SLA Trends for Passthrough Tunnels

5.1.3 Inferred Performance Metrics for Passthrough Tunnels

Local breakout uses passthrough tunnels (PTs), which are single-ended tunnels (i.e., EdgeConnect on one end and “internet” on the other end). Because EdgeConnect cannot exchange performance information with the non-EC at other end, and because SD-WAN fabric tunnels traverse the same underlay networks as the internet breakout passthrough tunnels, EdgeConnect can infer internet passthrough tunnel performance based on detailed statistics of EdgeConnect-to-EdgeConnect, SD-WAN fabric tunnels.

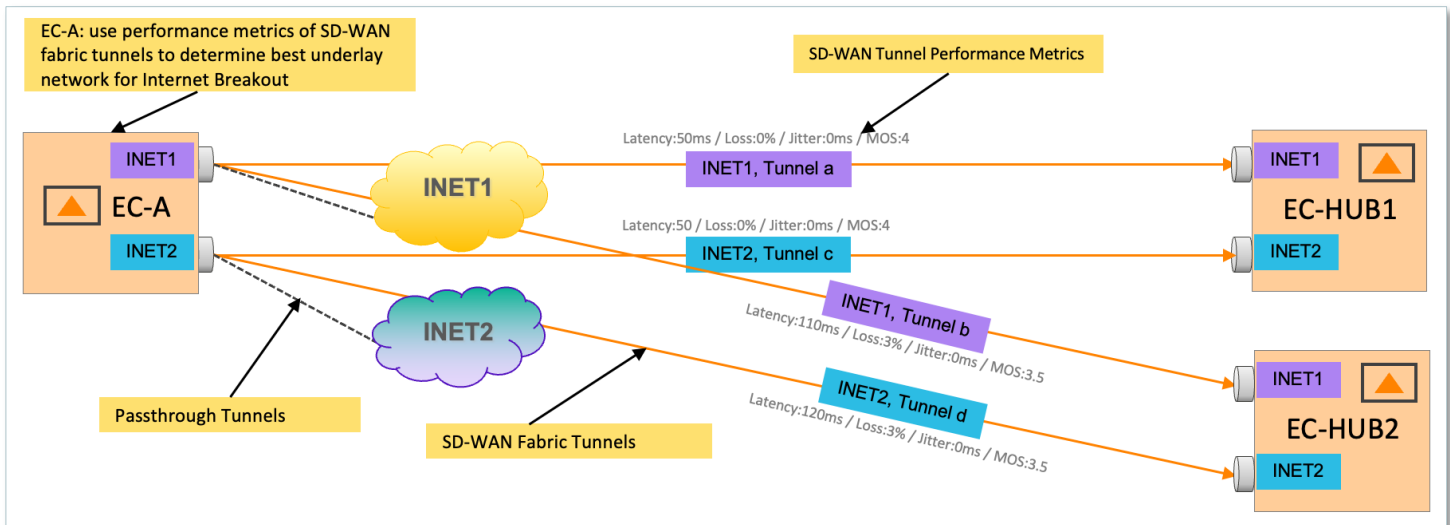


Figure 60 – Inferred Performance Metrics for Local Break Out

In the diagram above (Figure 60), EC-A and HUB-1 gather statistics on SD-WAN tunnel performance for INET1 Tunnel-a and INET2 Tunnel-c. Similarly, EC-A and HUB-2 gather statistics associated with INET1 and INET2. By performing this process across all network adjacencies, EC-A can derive a relative average performance spec for Underlay Networks INET1 and INET2. This relative performance spec can now be associated with the passthrough tunnels for INET1 and INET2.

Local Break Out policy will use the combination of performance metrics and utilization thresholds (both derived from SD-WAN tunnel health probes) to waterfall or load balance the traffic based on the Link Selection on the BIO policy.

NOTE: These inferred performance metrics from SD-WAN tunnels apply only to Break Out Locally policy. These metrics do not apply to traffic sent via service tunnels.

5.1.4 Link Selection

The following figure shows BIO provisioning for Breakout Traffic to Internet & Cloud Services. The Link Selection section indicates how a PT is selected for local breakout traffic.

The screenshot displays the 'Breakout Traffic to Internet & Cloud Services' configuration page. Key sections include:

- Branch Settings:** Lists various hubs and their associated cloud services (e.g., BAHRAIN1-AWS, LONDON-Google).
- Preferred Policy Order:** Shows a stack of policies: HPE-Axis-SSE, Backhaul Via Overlay, and Break Out Locally.
- Available Policies:** Lists external services like Skyhigh, Netskope Cloud, Zscaler Cloud, Akamai, and Lookout.
- Break Out Locally Using These Interfaces:** Configures primary (INETA, INETB, INETC) and backup (LTEA) interfaces.
- Available Interfaces:** Lists local network interfaces like LTEB, SAT1, MPLS1, MPLS2, and INETD.
- Link Selection (highlighted):**
 - Tabs: Waterfall (selected), Balanced.
 - Utilization: < 80 %
 - Performance Thresholds: Loss < 0 %, Latency < 0 ms, Jitter < 0 ms.
 - Rank Links By: Auto (dropdown).
 - Threshold-based Failover: ☐ Use next Preferred Policy if no links meet Performance Thresholds.

Figure 61 – BIO Provisioning Page - Breakout Traffic to Internet & Cloud Services

Link Selection for passthrough tunnels is equivalent to internal SD-WAN fabric as described in section 4.2. The primary difference compared to internal, fabric link bonding is that with external internet addresses, switching between links is done on a flow basis. There are two Link Selection methods available:

1. Waterfall
2. Balanced

5.1.4.1 Waterfall

Waterfall Link Selection uses the following metrics to rank passthrough tunnels:

1. **Auto** (weighted average of Loss and Latency over last two-minute period)
2. **Loss** (average over last two-minute period)
3. **Latency** (average over last two-minute period)
4. **Mean Opinion Score (MOS)** (average over last two-minute period)
5. **Fixed Order** (static order of LABEL placement)

With waterfall link selection, PT ranking is refreshed once per minute. If fixed order (manual) link ranking is selected, the ranking is fixed/static.

This detailed view of the Link Selection section shows:

- Waterfall** tab is active.
- Rank Links By** dropdown is set to **Fixed Order**.
- Other settings like Utilization (80%) and Performance Thresholds remain visible.

The order of configured interface labels matters when the Rank Links By is set to **Fixed Order**. Link selection will occur from top to bottom as shown in Figure 62.

Figure 62 – Waterfall Link Selection - Rank by Fixed Order



Performance Threshold for Loss/Latency and Jitter, along with Utilization percentage, will be considered in determining the eligibility of the PT for path selection. Figure 63 shows that the link has been sorted based on a ranking (for example, Latency), and the best-ranked PT is selected for sending flows out. The second-best PT is used for waterfalling the flows when the best PT exceeds the utilization threshold (default 80%).

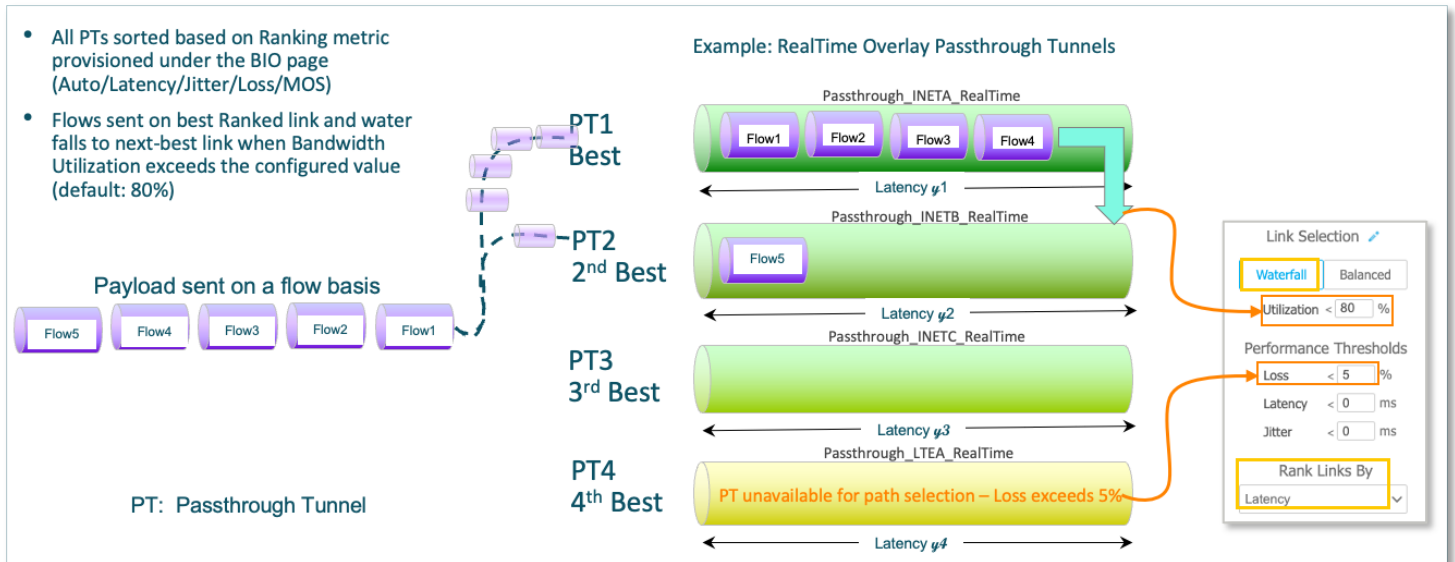


Figure 63 – Local Break Out - Waterfall Link Selection

The following algorithm is used for Waterfall link selection:

1. PTs are ranked based on the configured Ranking metric (Auto / Latency / Loss / MOS / Fixed Order). This ranking is refreshed every minute. The default Ranking is Auto.
2. If performance thresholds are provisioned, and if a PT reaches or exceeds any one or more thresholds, new flows will not be placed on that link for that minute.
3. If a link has exceeded its bandwidth utilization threshold (default utilization is 80%), the traffic will be sent on the next-best BT.
4. Using this rank-ordered list of eligible PTs, traffic is sent over the best link until it reaches the utilization threshold. Traffic spills over to the next-best link after the best link reaches the utilization threshold.
5. If no other primary PTs are available, or if EdgeConnect has only a single PT, the utilization threshold is ignored. Traffic will continue to flow on the same link.
6. If all PTs exceed a performance threshold, backup PTs will be considered for path selection.
7. If all primary and backup PTs exceed the performance thresholds, and Threshold Based failover is enabled, the next policy in the preferred policy order will be evaluated.
8. If all primary and backup PTs exceed the performance thresholds, and Threshold Based failover is NOT enabled, traffic will continue on the originally selected PT as a best effort.

Utilization threshold is hardcoded at 80% on any release earlier than ECOS 9.3.1. Starting with the ECOS 9.3.1 release, utilization threshold can be set on the BIO page of Internet Break Out.

5.1.4.2 Balanced

The Balanced Link Selection method uses links ranked by MOS. Ranking is refreshed every minute. Traffic is load balanced on a round-robin basis starting from the best link to the next-best links. With Balanced Link Selection, performance thresholds can be provisioned for Loss, Latency, and Jitter, which will be considered for determining whether links are eligible for use.

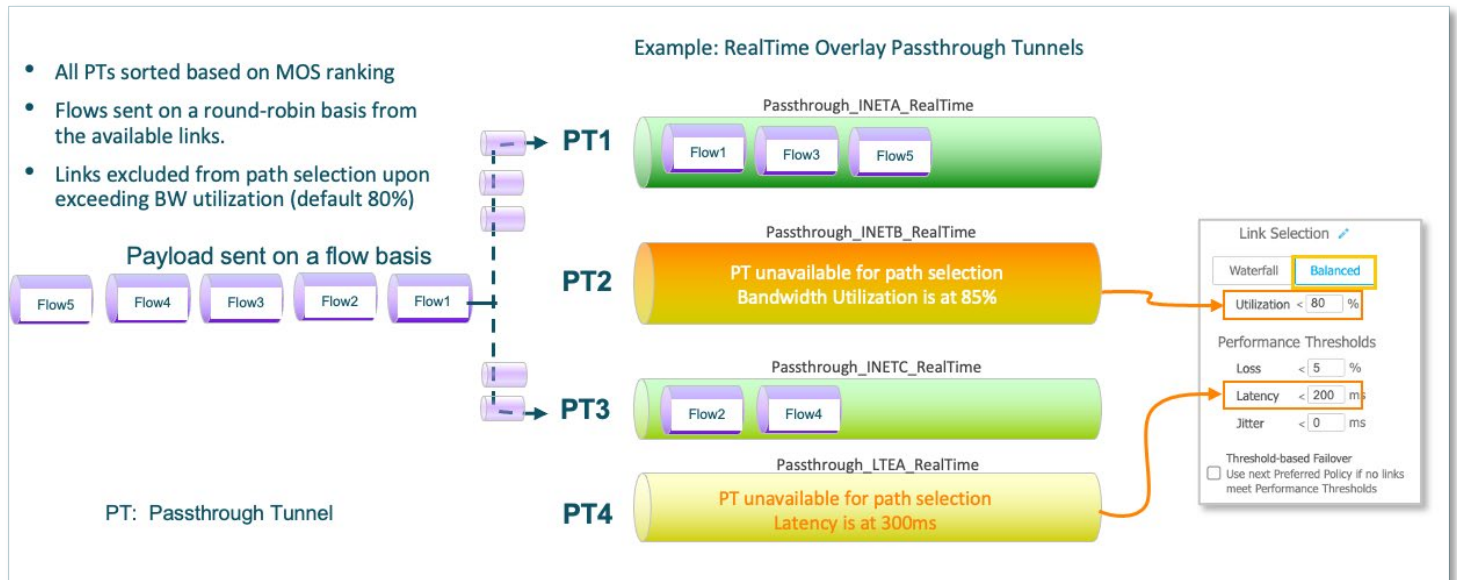


Figure 64 – Local Break Out - Balanced Link Selection

The following algorithm is used for Balanced link selection:

1. PTs are always ranked based on MOS. This ranking is refreshed every minute.
2. If performance thresholds are provisioned, and if a PT exceeds any one or more thresholds, the PT will be disqualified/ineligible for path selection.
3. If a link has exceeded its bandwidth threshold (Default Utilization is 80%), it will be disqualified/ineligible for path selection.
4. With this rank-ordered list of eligible PTs, link selection is based on round-robin starting from top to bottom. Traffic is sent over the selected link.
5. If there are no other PTs available, or if EdgeConnect only has a single PT, the utilization threshold is ignored. Traffic will continue to flow on the same link.
6. If all PTs exceed a performance threshold, backup PTs will be considered for path selection.
7. If all primary and backup PTs exceed the performance thresholds, and Threshold Based failover is enabled, the next policy in the preferred policy order will be evaluated.
8. If all primary and backup PTs exceed the performance thresholds, and Threshold Based failover is NOT enabled, traffic will continue on the originally selected PT as a best effort.

Utilization threshold is hardcoded at 80% on any release earlier than ECOS 9.3.1. Starting with the ECOS 9.3.1 release, utilization threshold can be set on the BIO page of Internet Break Out.

5.1.4.3 Performance Thresholds

When **Performance Thresholds** are configured, PTs must adhere to those thresholds. Any PT that exceeds at least one of the configured performance thresholds (Loss/Latency/Jitter) is excluded from link selection.

- When all primary links exceed thresholds, backup links will be used as a best-effort path.
- If both primary and backup exceed thresholds, OR primary exceeds threshold and no backup links are available, the “Threshold-based failover” knob will be considered to use the next preferred policy.
- If all thresholds are set to 0, the performance threshold is not considered for link selection.

Figure 65 – Performance Thresholds Settings

In this example (Figure 65), Loss of 5% and Latency of 300 ms are set as performance thresholds. If a PT experiences **either** 5% loss **or** 300 ms latency, it would be excluded from the link selection.

5.1.4.4 Utilization Threshold

The **Utilization** threshold on Link Selection determines when to trigger the selection of next-best PT for either Waterfall or Load Balance action. The Utilization threshold value is measured as an average utilization over a one-minute period per WAN label.

For Waterfall mode, traffic is sent over the best-ranked PT. It starts to spill over (waterfall) to the next-best PT when the utilization for the PT crosses the threshold (Default: 80%).

For Balanced mode, traffic is sent over a round-robin selected PT. If the utilization threshold is exceeded for that PT, the next PT is selected (on a round-robin basis) to send the traffic.

Figure 66 – Utilization Thresholds Setting

If all available PTs exceed 80% utilization, OR an EdgeConnect is deployed with a single WAN uplink, the utilization threshold is ignored. The system will continue to use the current PT based on the provisioned link selection.

5.1.4.5 Threshold-based Failover

When PTs are marked ineligible for link selection due to exceeding performance thresholds, the “**Threshold-based Failover**” knob is considered in determining when to process the next Preferred Policy.

- If the knob is enabled, and if all primary and backup PTs exceed the provisioned performance thresholds, or no backup PTs are available, the next policy in the Preferred Policy Order will be considered.
- If the knob is not enabled, the system will stick with the current link selection algorithm to send the traffic out through the selected PT.

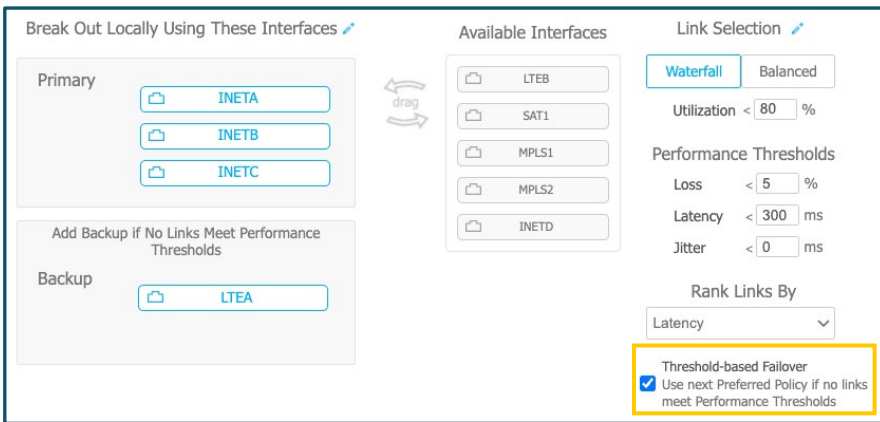


Figure 67 – Threshold-based Failover Setting

5.1.4.6 Consideration When Using “Threshold-based Failover”

If Break Out Locally is the only policy, OR if it is already placed as the last policy in the Preferred Policy Order, enabling “Threshold-based Failover” will result in traffic being dropped when the PTs exceed the performance thresholds because the next-based policy is the default action of “Drop”. Therefore, evaluate this knob carefully when designing BIO policy for internet breakout.

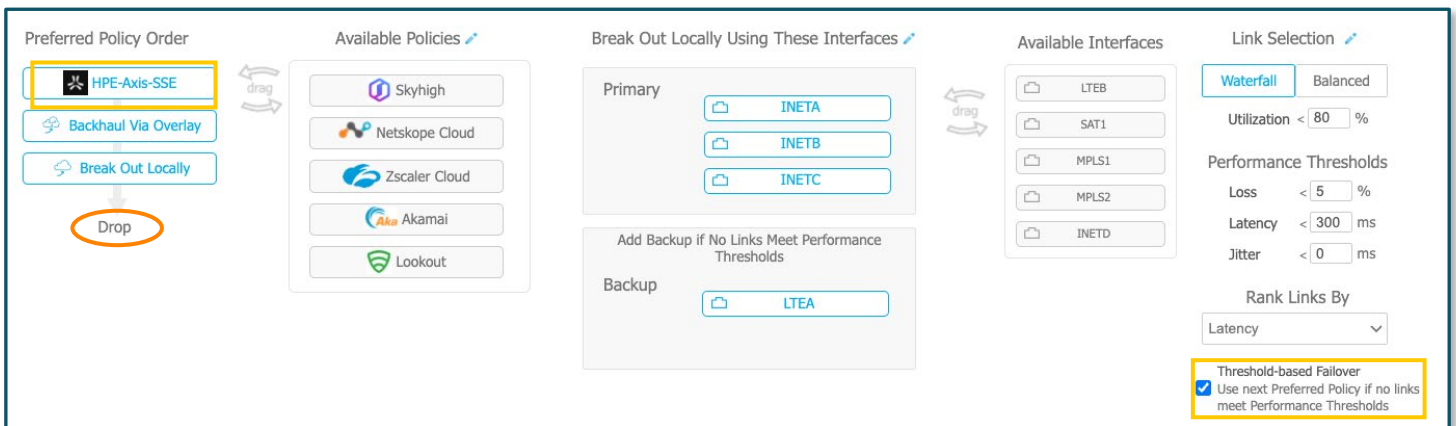


Figure 68 – Break Out Locally as Last Policy with Threshold-based Failover

5.1.5 Session Affinity for Break Out Local Traffic

EdgeConnect sends internet breakout traffic on a per-flow basis across available passthrough tunnels (PTs). When a flow for an Internal_External IP pair traverse through the system, session affinity is ensured for that IP pair by keeping current or new flows on the same PT if they arrive within the affinity timeout period (default is one minute). EdgeConnect keeps track of the Internal_External IP pair along with the last-used PT to ensure session affinity for the flows that arrive within the session affinity timeout value.

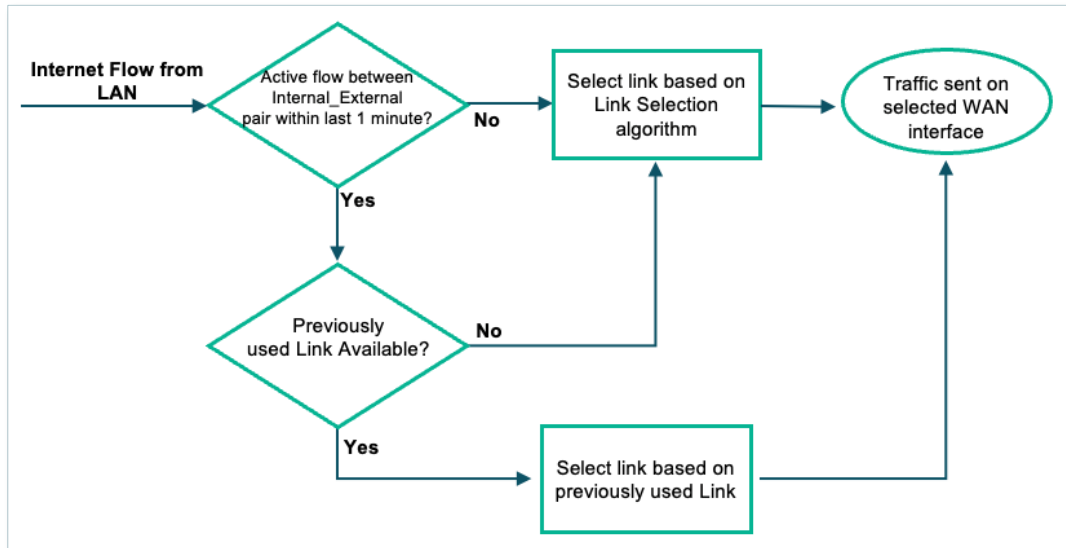


Figure 69 – Flowchart on Session Affinity Flow

Flow is kept on the same PT for a given Internal_External IP pair if the previously used PT is still available (even if the previous link is above utilization threshold). Session affinity matters only when more than one passthrough tunnel is available. It helps keep the flow symmetrical, especially when the traffic is traversing through another firewall.

Session affinity is not applicable for Service Tunnel or Backhaul via Overlay breakout policy.

Affinity Timeout is set on the BIO page (“**Breakout Traffic to Internet & Cloud Services**” → **Pencil icon** next to Link Selection).

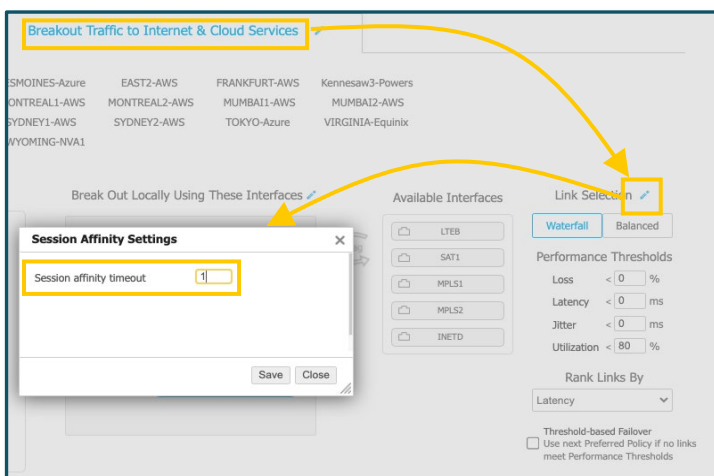


Figure 70 – Session Affinity Timeout Setting



The Affinity Timeout setting is a global setting (irrespective of overlay). When it is modified on any BIO, changes are pushed to all EdgeConnect appliances immediately.

5.2 Service Tunnels

Traffic is directed to the provisioned service tunnels using a round-robin load balance method. There are no inferred performance metrics used in service tunnel selection. Three types of service tunnels can be configured on an EdgeConnect appliance:

1. API-based Orchestrated Tunnels to Secure Web Gateways (SWG)
2. Service Orchestration-based Orchestrated Tunnels to Secure Web Gateways (SWG)
3. Manual Passthrough IPSec/GRE Tunnels

Breakouts using service tunnel underlays do not use any performance metrics for link selection. Service tunnels can have IP-SLA configured to actively probe the destinations (e.g., 8.8.8.8 or any known destination that can respond to ICMP or HTTPS probes) to ensure tunnel reachability. EdgeConnect will determine eligible tunnels based on IP-SLA state or simple tunnel up or down state (when no IP-SLA is configured).

After the eligible tunnels are identified, the system will simply load balance traffic between available tunnels on a per-flow basis. The system does not maintain any session affinity for the flow (meaning for a given Internal_External IP pair), but it will keep the flow on the same tunnel until that flow is completed. For any new flow for the same Internal_External IP pair, the system will pick the next available tunnel on a round-robin basis.

The flowchart shown in Figure 71 illustrates the flow of packets arriving on the LAN side and how the path for service tunnel is determined.

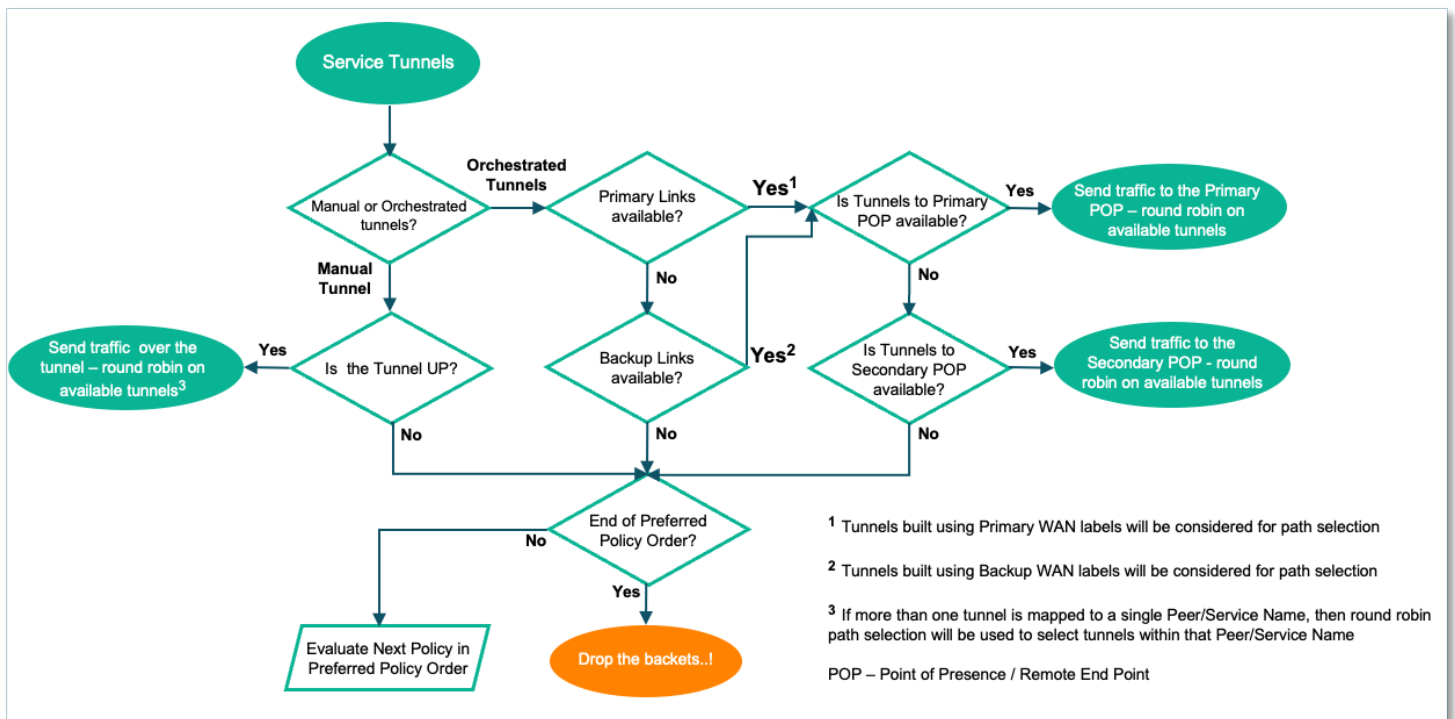


Figure 71 – Service Tunnel Path Selection (LAN to WAN Direction Flow)

The following sections provide details on each of the three methods of service tunnels and path selection.

5.2.1 API-based Orchestrated Tunnels to Secure Web Gateway

Orchestrator has a built-in capability to automate secure tunnels to the following vendors' cloud-based Secure Web Gateways (SWGs). This is an API-based integration between Orchestrator and these specified vendors.

- Zscaler
- Netskope

CLOUD SERVICES

AWS Network Manager

Check Point Harmony

Microsoft Azure Virtual WAN

Microsoft Office 365

Zscaler Internet Access

Netskope

Service Orchestration

After the initial cloud service configuration is completed on Orchestrator and is applied to the EdgeConnect appliances, each EdgeConnect will build IPsec tunnels or GRE tunnels (only Zscaler supported) to the nearest POP (point of presence) based on their geo-location.

Available Policies

HPE-Axis-SSE

Zscaler Cloud

Netskope Cloud

CheckPoint

Orchestrator will automatically create a policy for the cloud service under Available Policies (e.g., if deploying Zscaler SWG tunnels, Orchestrator will introduce Zscaler policy under the Available Policies section of the BIO).

5.2.2 Service Orchestration-based Orchestrated Tunnels to Secure Web Gateway

Service Orchestration is a vendor-agnostic, template-based feature that builds IPsec tunnels between EdgeConnect appliances and any vendor gateways. In this method, only IPsec tunnels are supported. Tunnel parameter details, such as Remote Endpoint IP addresses and IKE/IPsec parameters, must be identified before configuring Service Orchestration.

After the Service Orchestration knobs are fully configured, the configuration is applied to EdgeConnect appliances. Subsequently, EdgeConnect appliances build secure IPsec tunnels with remote endpoints.

CLOUD SERVICES

AWS Network Manager

Check Point Harmony

Microsoft Azure Virtual WAN

Microsoft Office 365

Zscaler Internet Access

Netskope

Service Orchestration

Available Policies

HPE-Axis-SSE

Zscaler Cloud

Netskope Cloud

CheckPoint

Orchestrator will automatically create a policy for the cloud service under the Available Policies section of the BIO (e.g., if deploying an HPE-Axis-SSE SWG tunnels, Orchestrator will introduce HPE-Axis-SSE policy under the Available Policy section of the BIO).



5.2.3 Path Selection for Orchestrated Service Tunnels

EdgeConnect builds tunnels using the WAN labels provisioned under Primary, Secondary, and Backup (Figure 72) on the Cloud Services configuration for a given vendor. Tunnels will be grouped based on the WAN label grouping (Primary, Secondary, or Backup) as shown in Figure 72.

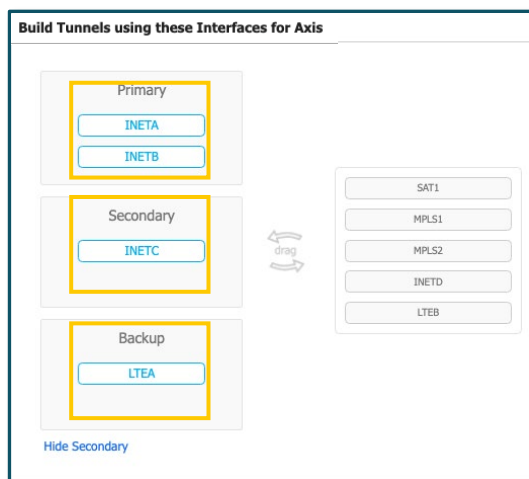


Figure 72 – Interface Label Section of Cloud Services Configuration

Internet traffic using service tunnel policy will consider all primary tunnels (tunnels built using primary WAN labels) to **POP1** (i.e., primary remote endpoint) as a first choice. If there are more than one primary WAN label, all tunnels using primary WAN label to POP1 will be considered as eligible for path selection on a round-robin basis.

Orchestrator will also automate IP-SLA rules to monitor tunnel availability by probing internet destinations.

In the following example (Figure 73), there are two primary WAN labels (INETA and INETB). EdgeConnect builds two primary tunnels to POP1 and two primary tunnels to POP2.

The order of operation in the diagram shows that the tunnel traffic starts with Primary WAN label (INETA and INETB) tunnels to POP1. Traffic moves to Primary WAN label (INETA and INETB) tunnels to POP2 only when all POP1 tunnels are DOWN.

Similarly, secondary tunnels (tunnels built using secondary WAN labels) are considered when all primary tunnels are down. Backup tunnels (tunnels built using backup WAN labels) are only eligible when both primary and secondary tunnels are DOWN.



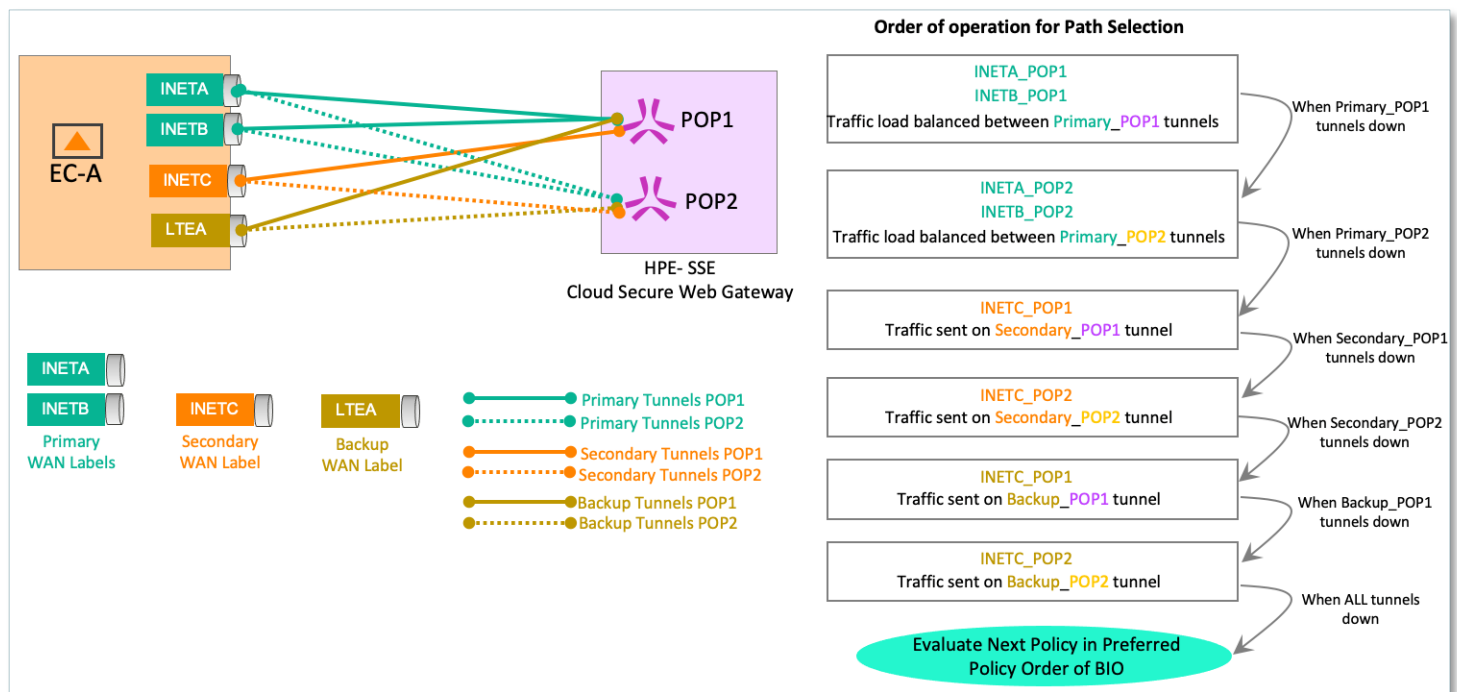


Figure 73 – Service Tunnel Path Selection - Order of Operation

When the tunnel is selected from the available list (round-robin), EdgeConnect sends internet traffic on a per-flow basis to the selected tunnel. When the flow for a given Internal_External IP pair is transported on a selected tunnel, it stays with that path until that flow is completed. Any **new** flow for the same Internal_External IP pair will be again subjected to a fresh round-robin path selection.

NOTE: EdgeConnects do NOT maintain session affinity for breakout traffic via service tunnels.

5.2.4 Manual Passthrough IPSec / GRE Tunnels

Where API-based or Service Orchestration-based orchestrated tunnel provisioning is not feasible, you can configure manual IPSec or GRE passthrough tunnels on a per-appliance basis.

EdgeConnect identifies manual passthrough tunnels based on the Peer/Service name (Figure 74) that is configured at the time of passthrough tunnel provisioning. If the passthrough tunnels are built to the same destination from multiple EdgeConnect appliances, it is important to use the same Peer/Service name. In the following example (Figure 74), two EdgeConnect appliances have passthrough tunnels provisioned with the same Peer/Service name.

Tunnels ?

Overlay Underlay Passthrough Status All

2/77 Rows

Edit	Segment	Appliance	Passthrough Tunnel	Peer/Service	Local IP	Remote IP	Status
	Default	Chelmsford-krisram1	ThirdParty_Manual_Primary_INETA_Primary_1	Manual_Primary_Node1	172.17.50.1	172.23.23.50	up - active
	Default	DAS-N2-EC1-5442	ThirdParty_Manual_Primary_INETA_Primary_1	Manual_Primary_Node1	172.23.23.1	172.23.23.50	up - active

Figure 74 – Manual Passthrough Tunnels with Peer/Service Name

After the passthrough tunnel is configured on at least one EdgeConnect appliance, the Peer/Service name can be assigned to the **Available Policies** section of the BIO. As seen in the example (Figure 75), Peer/Service name is what is considered as a policy and finally makes it to the Available Policies section for the processing of internet breakout traffic. If multiple Peer/Service names have been used during passthrough tunnel configuration, each of those Peer/Services must be added to the Available Policies section for policy processing.

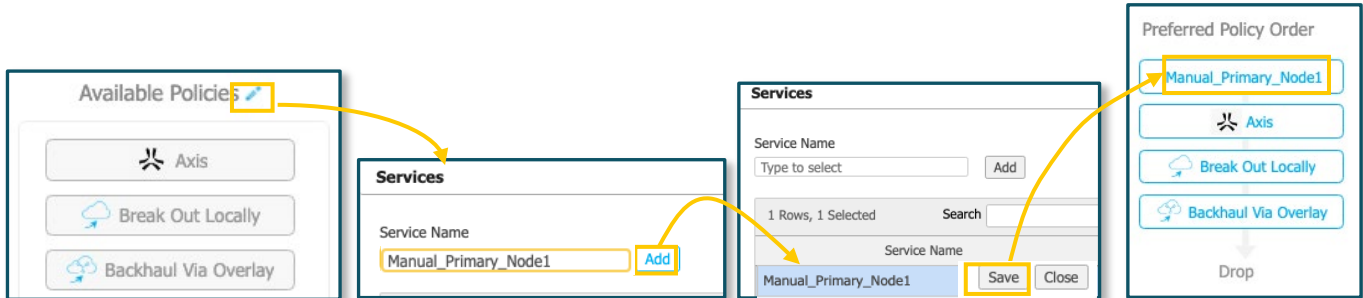


Figure 75 – Adding Manual Passthrough Tunnel as a Policy Under BIO



5.2.5 Path Selection for Manual Passthrough IPSec / GRE Tunnels

Tunnel path selection differs depending on how the manual passthrough tunnels are mapped to the Peer/Service name. Tunnels are not automatically grouped based on the WAN labels (primary, secondary, and backup) as in the case with orchestrated tunnels. EdgeConnect will consider tunnels under a common Peer/Service as a single policy.

In the following example (Figure 76), EdgeConnect EC-A has one primary WAN label and one secondary WAN label. Manual passthrough tunnels are configured between ECA-A and Third-party Gateway/FW **Node1** and **Node2**. To achieve redundancy using primary and secondary WAN labels, each passthrough tunnel is mapped to a unique Peer/Service name, such as Manual_Primary_Node1, Manual_Primary_Node2 and so forth.

On the BIO policy for Internet Traffic, each of those Peer/Service names is added under **Available Policies**. The order in which each of those policies is placed matters. EdgeConnect will process these policies from top to bottom. In this example (Figure 76), EdgeConnect will send the traffic over to the tunnel INETA-Node1 (Manual_Primary_Node1) all the time. Failover occurs to the INETA-Node2 tunnel if the INETA-Node1 tunnel is down (based on the preferred policy order list).

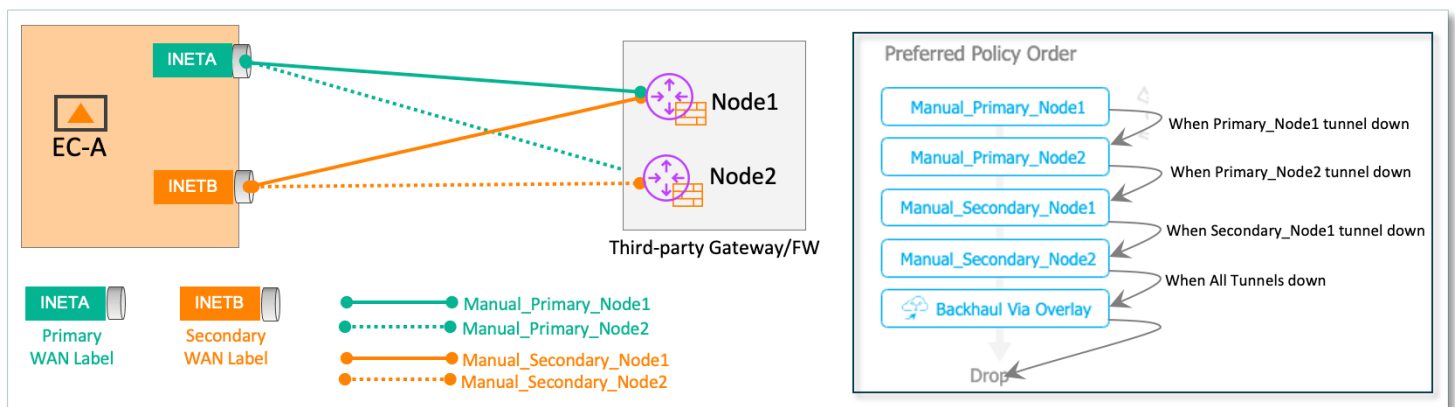


Figure 76 – Passthrough Tunnel Policy Provisioning in a Fixed Order

If only one passthrough tunnel is mapped under the Peer/Service name (Figure 76), traffic will always be sent on the same tunnel.

If multiple tunnels are mapped under the same Peer/Service name, traffic will be sent on a round-robin selected tunnel. It is important to map the passthrough tunnels going to the same destination under the same Peer/Service name because this will help the EdgeConnect to load balance the traffic between the provisioned passthrough tunnels.

After the tunnel is selected from the available list (round-robin), EdgeConnect sends internet traffic on a per-flow basis on the selected tunnel. After the flow for a given Internal_External IP pair is transported on a selected tunnel, it stays with that path until that flow is completed. Any **new** flow for the same Internal_External IP pair will be again subjected to round-robin path selection.

NOTE: EdgeConnects do not maintain session affinity for breakout traffic via service tunnel.

5.3 Backhaul via Overlay

When Preferred Policy is set to Backhaul Via Overlay, internet traffic will be sent over via bonded overlay tunnel. The use case for this type of policy is to send all or some of the internet traffic to a hub at the data center for centralized processing of internet traffic. Another use case is to use Backhaul Via Overlay as a backup policy to either Break Out Locally or breakout via service tunnel (in scenarios where local breakout interfaces or service tunnels are down).

5.3.1 LAN to External Flow – Backhaul via Overlay

The following flowchart (Figure 77) provides an overview of the flow in determining the path for external/internet bound traffic from LAN to WAN (L2W) or LAN to LAN (L2L) direction.

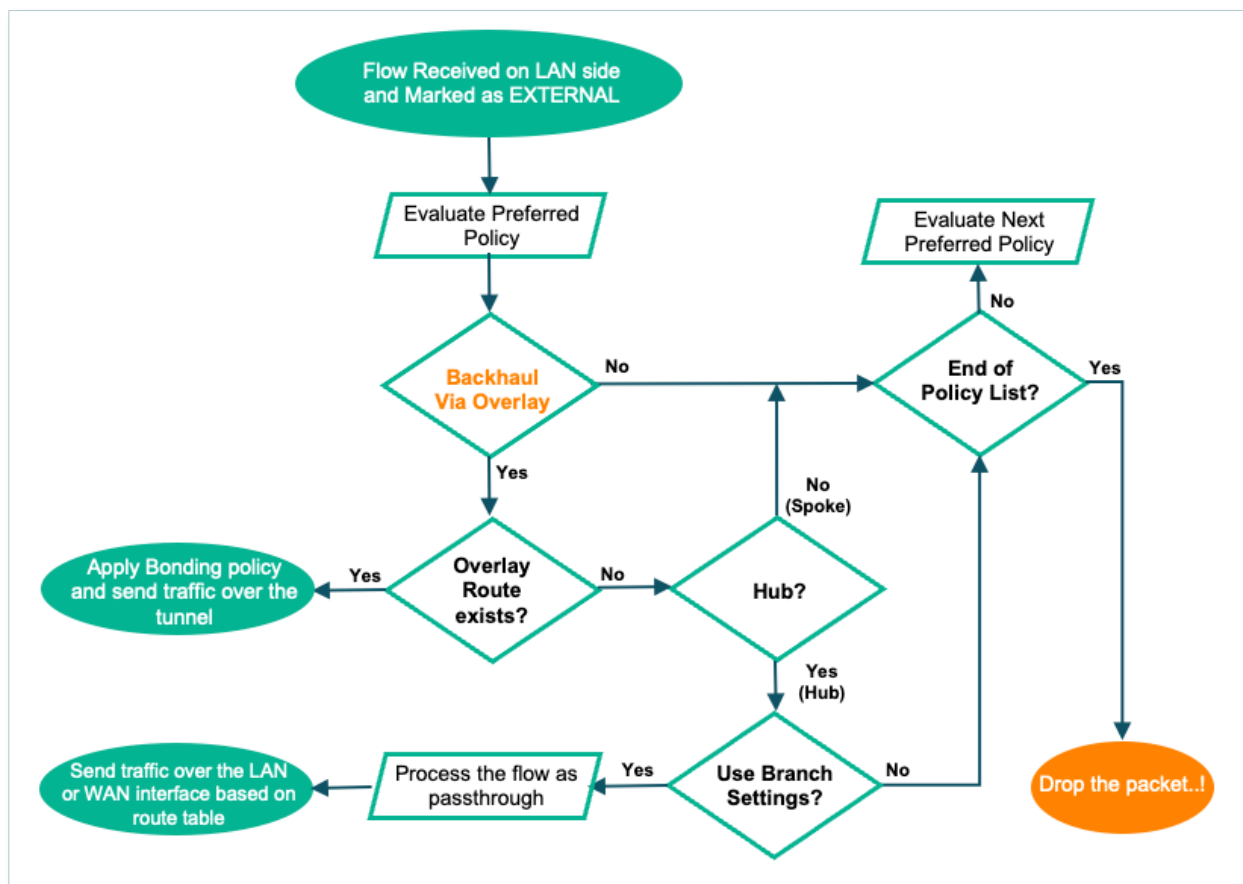


Figure 77 – Processing of Backhaul Traffic When Received on the LAN Side

5.3.2 LAN to External – Backhaul Flow: Peer Unavailable Scenario

There is a difference in the behavior on a hub EC vs. spoke EC for an external flow that needs to exit as passthrough traffic when the overlay tunnel is unavailable (remote peer unavailable). This scenario is detailed in Figure 78 and Figure 79. Summary of behavior follows:

- For a flow coming from the LAN side and unable to find an overlay tunnel, the next policy would be evaluated if the device is a non-hub.
- For a flow coming from the LAN side and unable to find an overlay tunnel, the next policy would be evaluated if the device is a hub BUT Use Branch Settings on BIO page is UNCHECKED.
- If Backhaul Via Overlay is the last policy in the preferred policy order, the flow (L2W) will be dropped because there is an explicit Deny policy at the end of the preferred policy order.
- In the case of a hub device with Use Branch Settings CHECKED and the flow cannot be transported over a bonded overlay tunnel due to peer unavailable, the hub will attempt to send the traffic over either the WAN (Figure 78) side or LAN side (Figure 79) as a passthrough (depending on the route table).

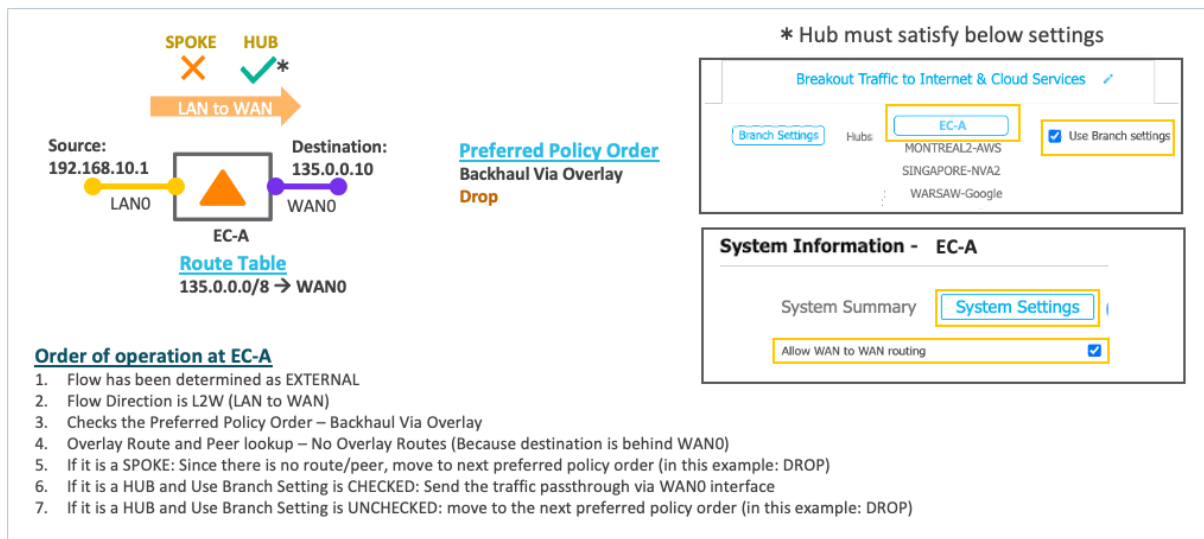


Figure 78 – Outbound Flow - Peer Unavailable: WAN Side Drain

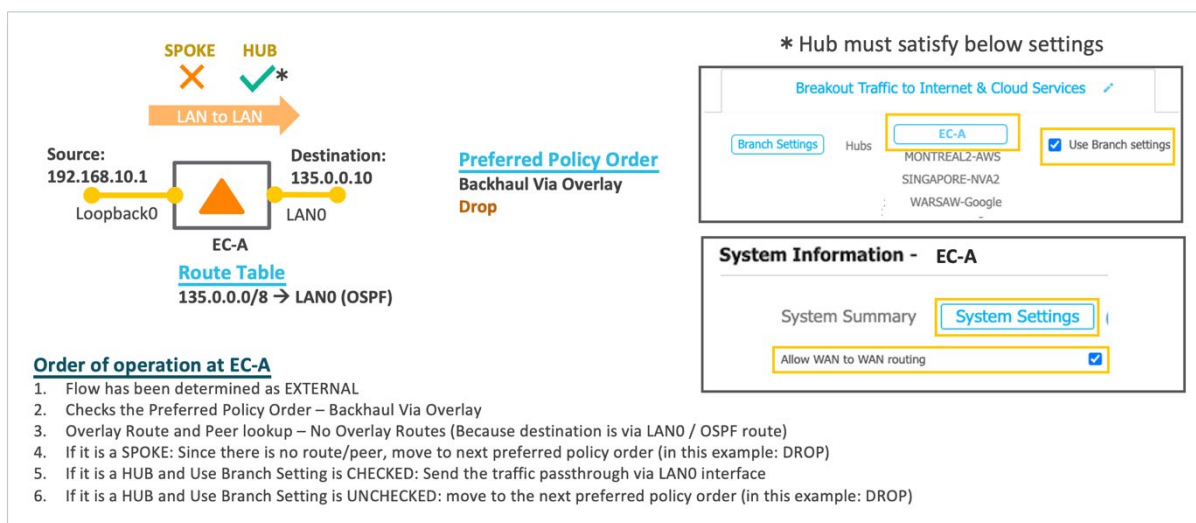


Figure 79 – Outbound Flow - Peer Unavailable: LAN Side Drain

5.3.3 WAN to External – Backhaul via Overlay

The following flowchart (Figure 80) provides an overview of the flow in determining the path for external/internet bound traffic from WAN to WAN (W2W) or WAN to LAN (W2L) direction.

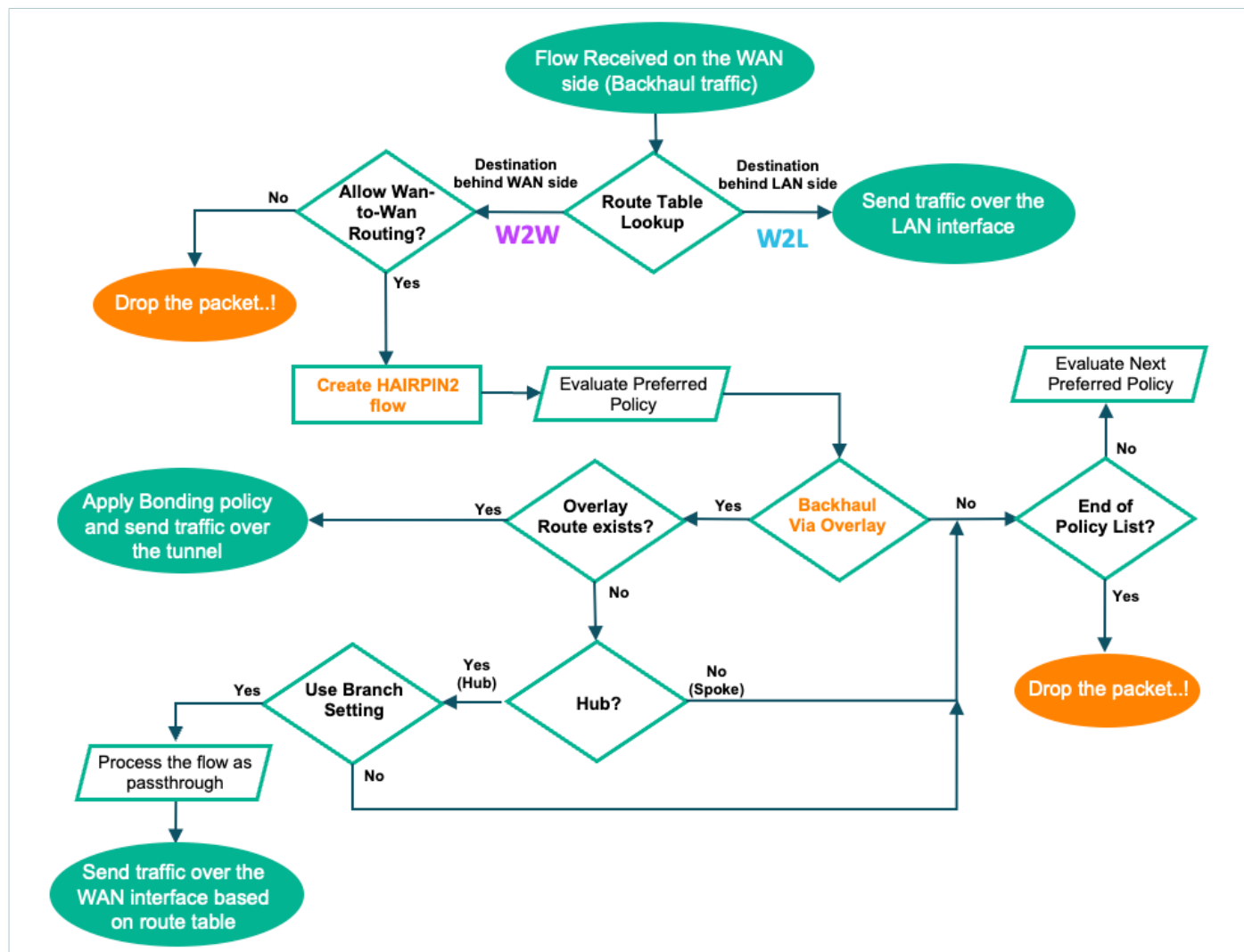


Figure 80 – Processing of Backhaul Traffic When Received via Overlay Tunnel

5.3.4 WAN to WAN Backhaul Flow – LAN-side Drain on the Receiving EdgeConnect

For a flow received via the overlay tunnel (backhaul traffic), and if the receiving EdgeConnect has a route to the destination via LAN interface, the traffic will be sent out through the LAN interface as a passthrough-unshaped traffic. If the LAN-side drain fails, a new flow named HAIRPIN2 will be created for WAN-side drain (System Setting: Allow WAN to WAN routing MUST be enabled). See section 5.3.5 for more about WAN-side drain behavior.

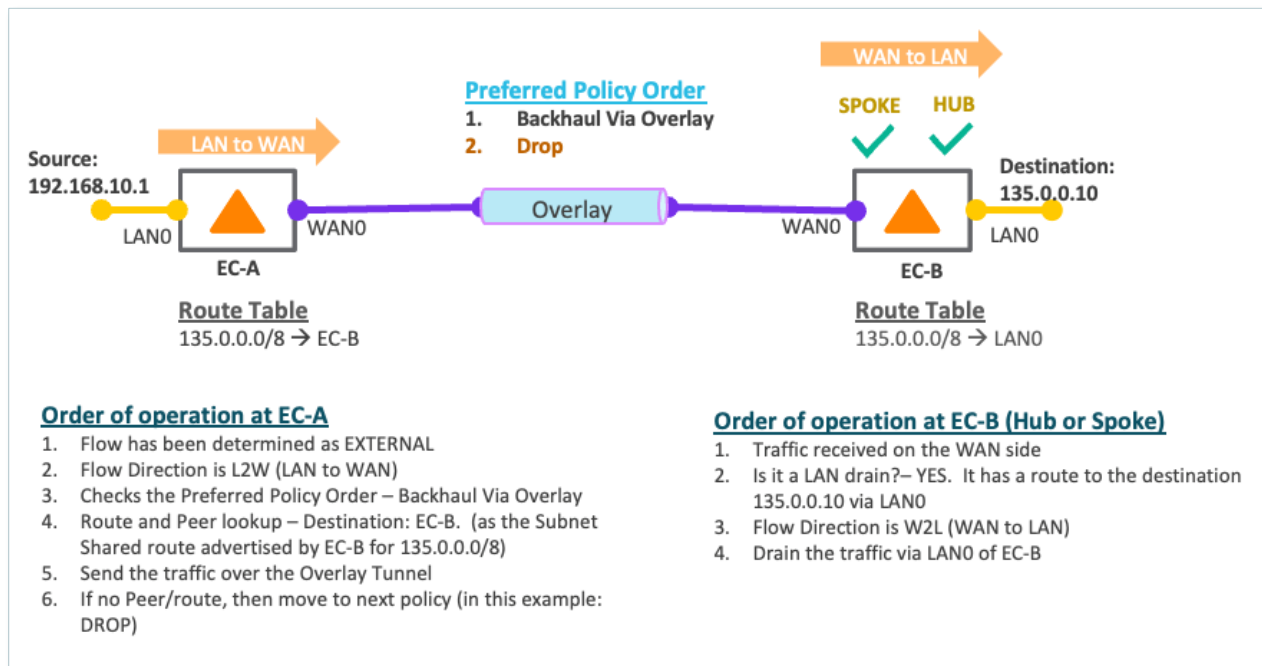


Figure 81 – Backhaul Via Overlay - WAN to WAN flow – LAN-side Drain

5.3.5 WAN to WAN Backhaul Flow – WAN-side Drain on the Receiving EdgeConnect

For a flow received via the overlay tunnel (backhaul traffic), there is a difference in the behavior between a hub EC and spoke EC for WAN-side drain. Traffic can be WAN-side drained only if the receiving EdgeConnect is a HUB and the system setting has Allow WAN to WAN routing enabled and Use Branch Setting on the BIO page is checked. This scenario is detailed in Figure 82. Summary of behavior follows:

- Flow received via the overlay tunnel (WAN) will attempt to go forward through the LAN side if the destination is routed via LAN interface (LAN-side drain).
- If the LAN-side drain fails and Allow WAN-to-WAN routing setting enabled on the EC, a new HAIRPIN2 flow is created. If WAN-to-WAN routing is disabled, traffic will be dropped.
- HAIRPIN2 flow is a LAN-to-WAN flow. Therefore, the internet policy will be evaluated freshly for this HAIRPIN2 flow.
- If the preferred policy selected is Backhaul Via Overlay and the destination is reachable via remote peer, the traffic will be sent over the bonded tunnel to the remote EC.
- If the preferred policy selected is Backhaul Via Overlay and the remote peer is unavailable, the next policy in the preferred policy order will be evaluated.
- In the case of a hub device, if the traffic cannot be transported over a bonded overlay tunnel due to peer unavailable, the hub will attempt to send the traffic over the WAN side as a passthrough (if route to the destination exists) when certain conditions are met. See Figure 82, which shows a scenario with respective EC setting.

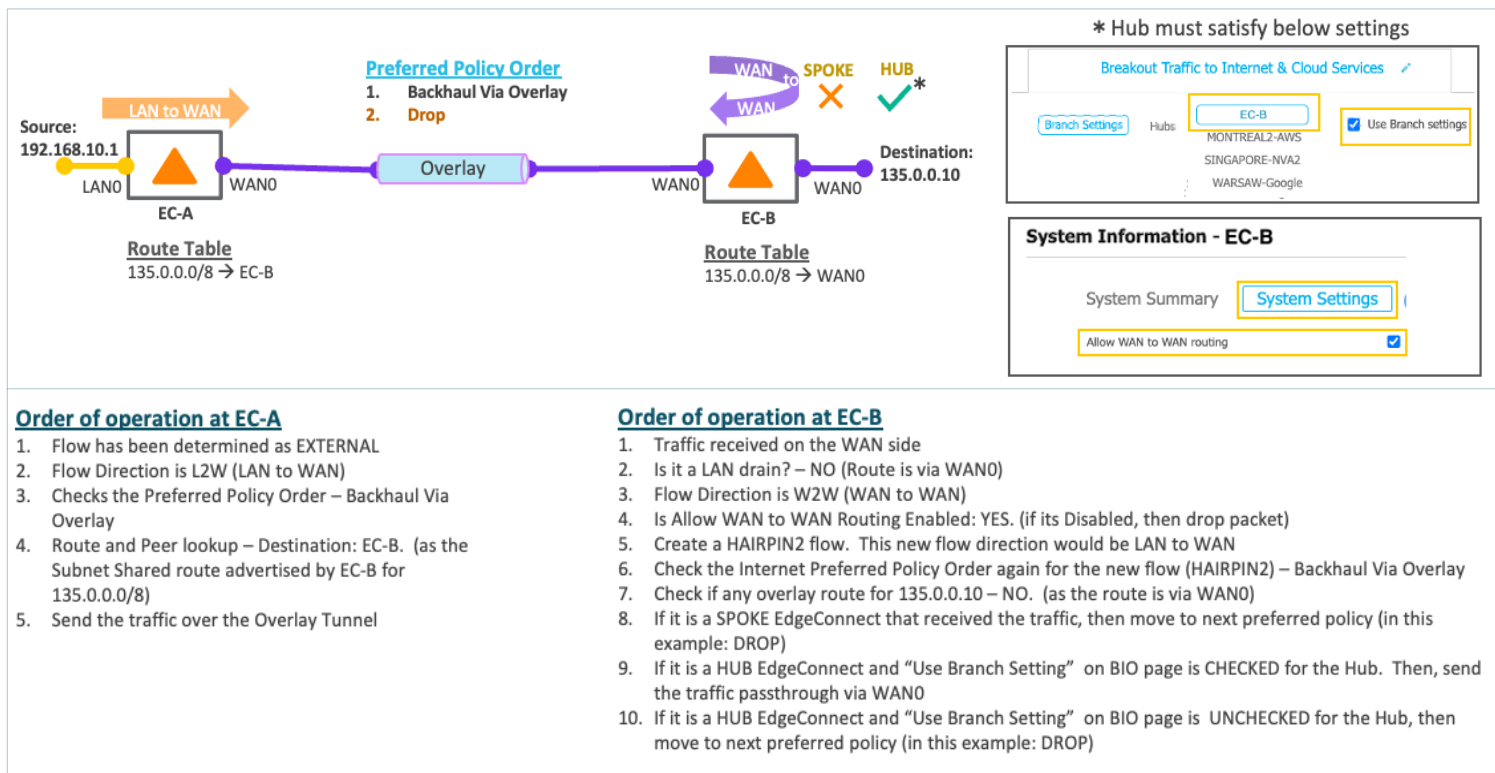


Figure 82 – Backhaul via Overlay - WAN to WAN flow - Peer Unavailable: WAN-side Drain

5.3.6 Advertising Internet Routes to Attract Internet Traffic

For the Internet traffic via Backhaul to work, the remote-end EdgeConnect (typically the hub EdgeConnect appliance) should be announcing a default route to the peers. In the following example (Figure 83), the hub appliance (EC-B) announces 0.0.0.0/0 route. Therefore, EC-A can transport user internet traffic over the bonded tunnel.

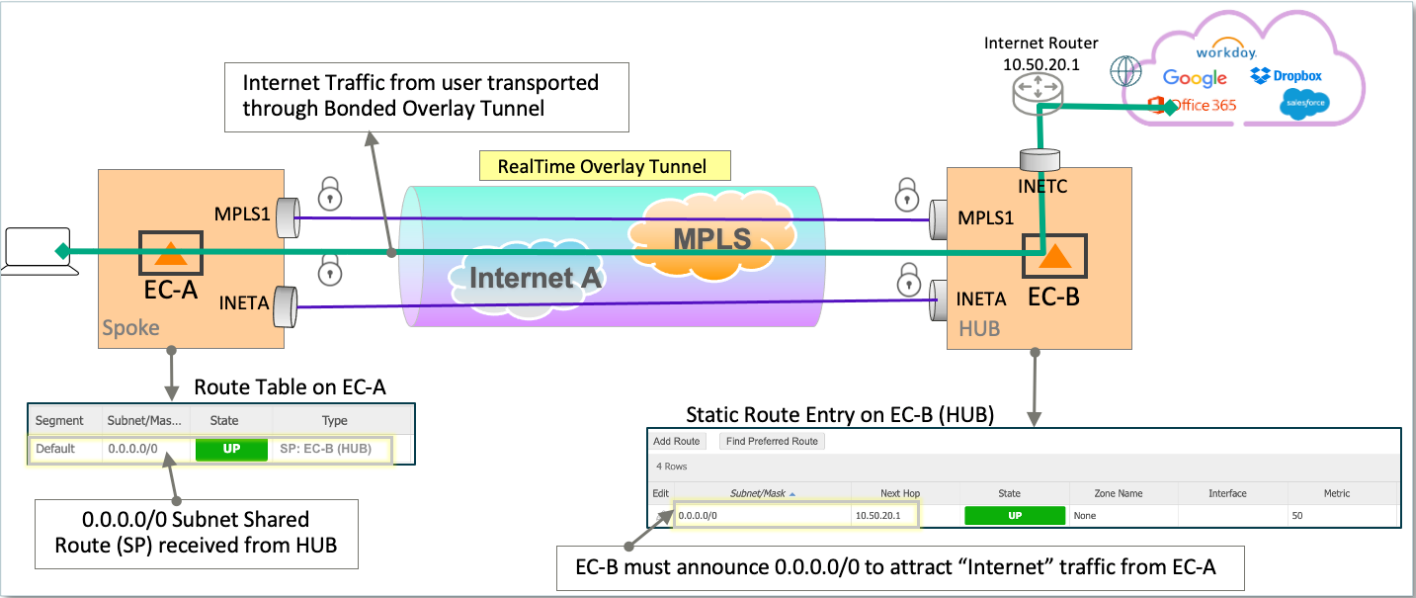


Figure 83 – Backhaul via Overlay - Local Breakout at the Hub

5.3.7 Bonding Policy and Path Selection for Backhaul Traffic

Backhaul Via Overlay traffic attracts the same benefits of Link Bonding policy that are applicable to an SD-WAN traffic. Depending on the overlay, if the internet traffic type matches, Link Bonding policy corresponding to that matched overlay will be applied to the traffic. For example, if the internet traffic matches an overlay named “RealTime” that has “High Availability” as Link Bonding policy, internet traffic will benefit from the features, such as dynamic path selection based on metrics, protection against packet loss (due to FEC being applied,) and Packet Order Correction (when packet arrives out of sequence).

Internet traffic backhauled via overlay tunnel is sent out to respective overlay tunnels on a per-packet basis using the intelligent dynamic path selection engine. Bonding Policy configured for that overlay defines which path the overlay traffic takes. It could constantly change based on the WAN interface performance metrics (See section 4 for more details on bonding policies for SD-WAN traffic).

NOTE: EdgeConnects do not maintain session affinity for internet traffic via overlay tunnel.



5.4 Hairpinning and Allow WAN-to-WAN Routing

Any time traffic is received on the EdgeConnect WAN side, and if that traffic needs to exit through that appliance WAN side (either passthrough or to another EC peer via overlay tunnel), that flow is considered WAN-to-WAN flow. Following are two use cases where an EdgeConnect received traffic on the WAN side and sent the traffic back on the WAN side:

- Internet traffic backhauled from remote EdgeConnect to a hub and that internet traffic broke out locally on the hub EdgeConnect WAN interface
- In a Hub and Spoke topology, Spoke1 communicates to Spoke2 via a hub

In both the cases, the traffic is received on the WAN side (through an overlay tunnel) and exits the EC on the WAN side, creating a hairpin flow behavior. This communication (HAIRPIN flow) by default is allowed using the feature called “Allow WAN-WAN routing”, Figure 84 shows the **System Settings** page where the Allow WAN-WAN routing feature is enabled. This setting is enabled by default.

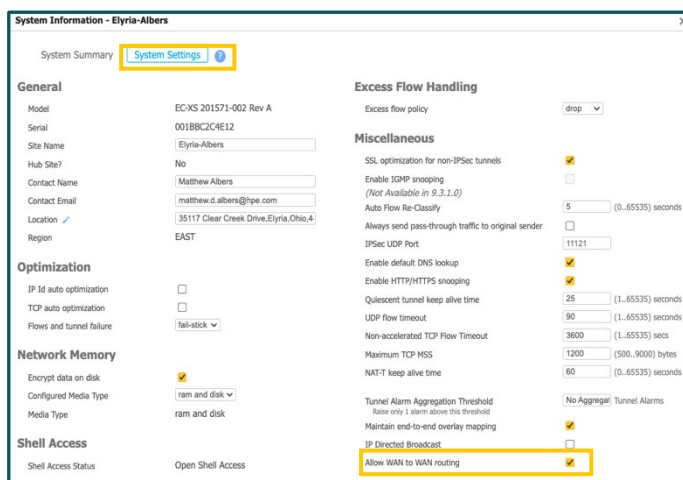


Figure 84 – System Setting Showing Allow WAN to WAN Routing

When “**Allow WAN to WAN routing**” is **ENABLED** and LAN-side drain is not available, EdgeConnect creates hairpin flows (HAIRPIN1 and HAIRPIN2) to facilitate WAN-to-WAN transit. This shown in Figure 85.

When **Allow WAN to WAN routing** is **DISABLED**, EdgeConnect disables internal hairpinning lookup and attempts to send the packet straight out on the LAN side for incoming WAN packets:

1. From tunnels (SD-WAN traffic from peers)
2. From WAN interface (passthrough traffic)

If there are no LAN routes for the destination, traffic is dropped.

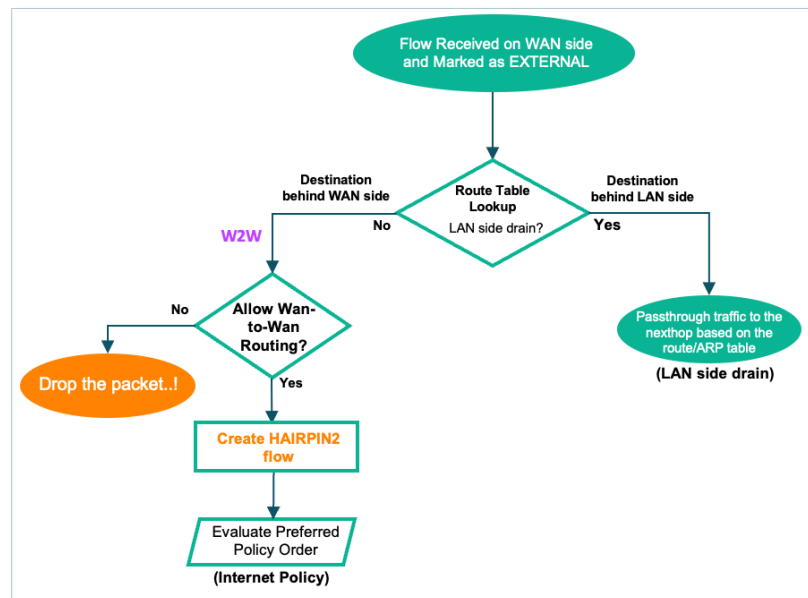


Figure 85 – HAIRPIN2 Flow

Figure 86 shows that a flow that originated on the Spoke side was backhauled to the hub via RealTime overlay. When the packet is received at the hub appliance, it creates two flows for that inbound traffic. HAIRPIN1 flow represents the inbound flow via the RealTime overlay, and HAIRPIN2 flow is the actual breakout traffic to the internet via the INETC WAN interface.

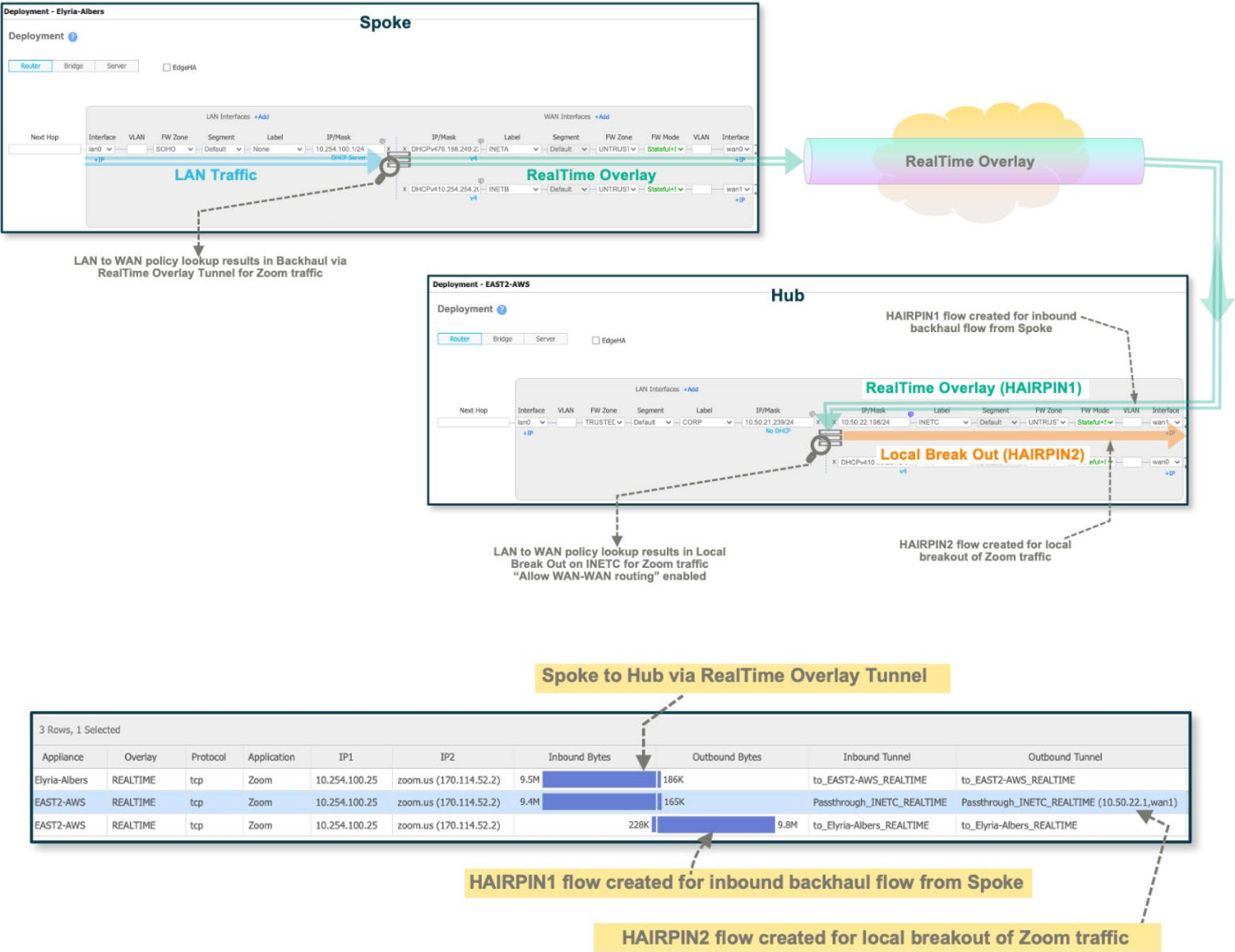
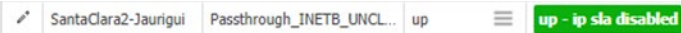
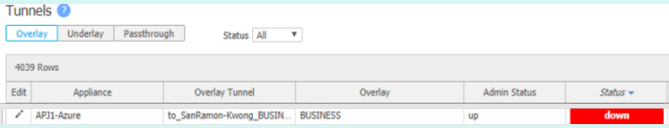
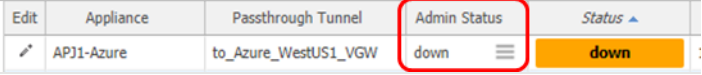


Figure 86 – Backhaul via Overlay - Hairpin Flows

6 Underlay Tunnel States, Settings, and State Behavior

6.1 Orchestrator Tunnel States

Tunnel states shown in the following table represent tunnel states as viewed on Orchestrator. They are primarily controlled by the Tunnel Health mechanism.

Tunnel State	Definition
Up – Idle	The tunnel is up and active. It has not had recent activity in the past five minutes and has slowed the rate of issuing keep-alive packets.
Up – Active	The tunnel is up and active. Traffic destined for this tunnel is being forwarded to the remote EdgeConnect.
Up – Reduced Functionality	The tunnel is up and active. However, the two endpoint appliances are running mismatched software releases that provide no performance benefit.
Up – IP SLA Disabled	Passthrough tunnels only. The tunnel is up (has connectivity) but it is down because of a configured IP SLA consequent action. 
Down (Red)	The tunnel is down. This can occur because the tunnel cannot communicate with the appliance at the other end. 
Down (Orange)	The tunnel is down. This can occur because the tunnel administrative setting is down. 
Down – In progress	The tunnel is down. Meanwhile, the appliance is exchanging control information with the appliance at the other end, trying to bring up the tunnel.
Down – Misconfigured	The two appliances are configured with the same System ID.
UNKNOWN	The tunnel status is unknown. This can occur because the appliance is unable to retrieve the current tunnel status.



6.2 Live View

Orchestrator Live View shows current data and includes the following states:

1. Up (Green)
2. Not Meeting Service Levels (Orange; service level threshold is exceeded)
3. Down (Red)

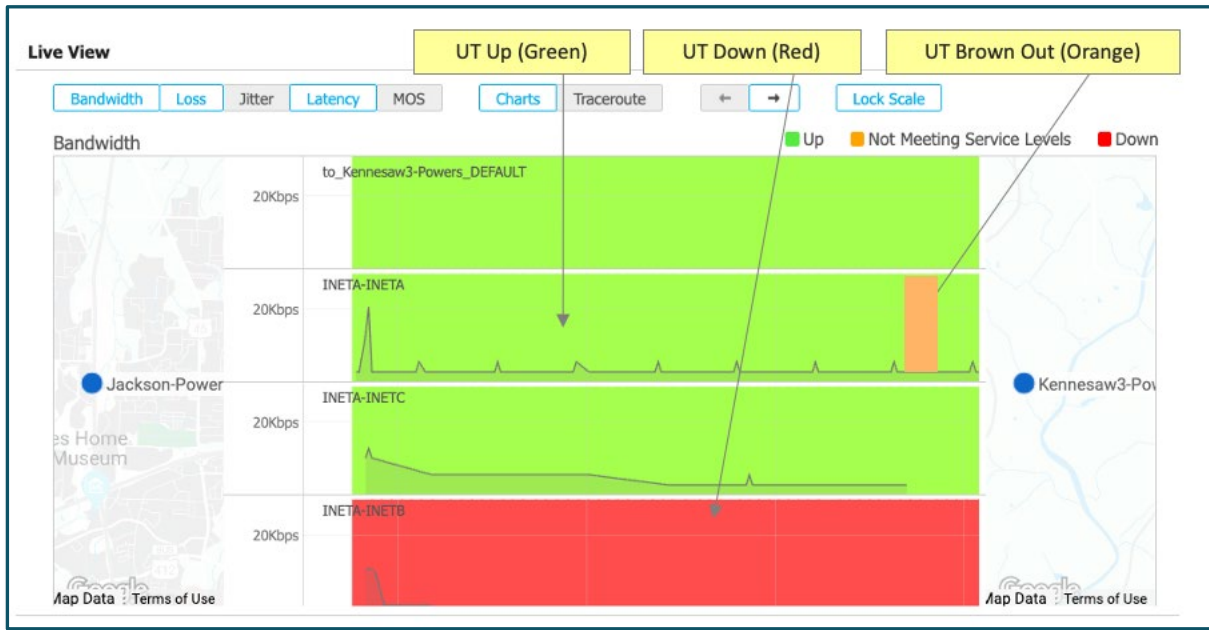


Figure 87 – Live View Showing UT Link State

NOTE: Available bandwidth capacity for UT is not considered part of link state.

6.3 Global Tunnel Settings

When using Business Intent Overlays (BIOs), Orchestrator automatically builds both underlay tunnels and overlay tunnels based on a given appliance's membership to BIOs. In other words, Orchestrator will only build underlay and overlay tunnels based on BIO topology (Hub & Spoke or Full-Mesh) and BIO application (to nodes). Tunnel settings are defined globally by Orchestrator as the following figure shows.

Tunnel Settings ?

Settings for Tunnels created by Business Intent Overlays

WAN Interface Labels

- MPLS1
- INET1
- LTE
- INET2
- MPLS2

General | IPsec

General

Mode: IPSec UDP

Auto Max BW Enabled: ☒

Auto Discover MTU Enabled: ☒

MTU: 1500 Bytes

Packet

Reorder Wait: 100 ms

FEC: disable

FEC Ratio: 1:10

Tunnel Health

Retry Count: 30

DSCP: be

FastFail Thresholds

Fastfail Enabled: enable (Use "enable" for best performance)

Latency: 0 ms

Loss: 0 %

Jitter: 0 ms

Fastfail Wait-time Base Offset: 150 ms

Fastfail RTT Multiplication Factor: 5

Do not use Fast Fail settings with EdgeConnect > 8.1.9.5

Do Not Use these tunnel settings with Overlays

Figure 88 – Global Underlay Tunnel Configuration

Some settings in Orchestrator/Tools/Tunnel Settings are legacy and should not be used. Packet reorder wait time, FEC, and FEC Ratio are attributes that are set on the Business Intent Overlay provisioning screen. These parameters should not be set here.

Similarly, FastFail mode was employed in EdgeConnect releases up to 8.1.7. With releases 8.1.9.5 and beyond, FastFail mode is replaced with the Path Characterization. The FastFail parameters are still shown on the configuration screen, but they will be removed in later releases of Orchestrator.

6.4 Underlay Tunnel Degraded / Down States

An underlay tunnel can be in a state of UP (Green), Brownout (Orange), or Down (Red). These states determine whether a tunnel is eligible to be used by an overlay. In some cases, states of all other tunnels must be taken into consideration. When an underlay tunnel enters the Brownout state because of a degraded condition, it can be disqualified for use by an overlay. However, if all UTs are in brownout, the UT is made eligible for use. The following diagram shows these states.

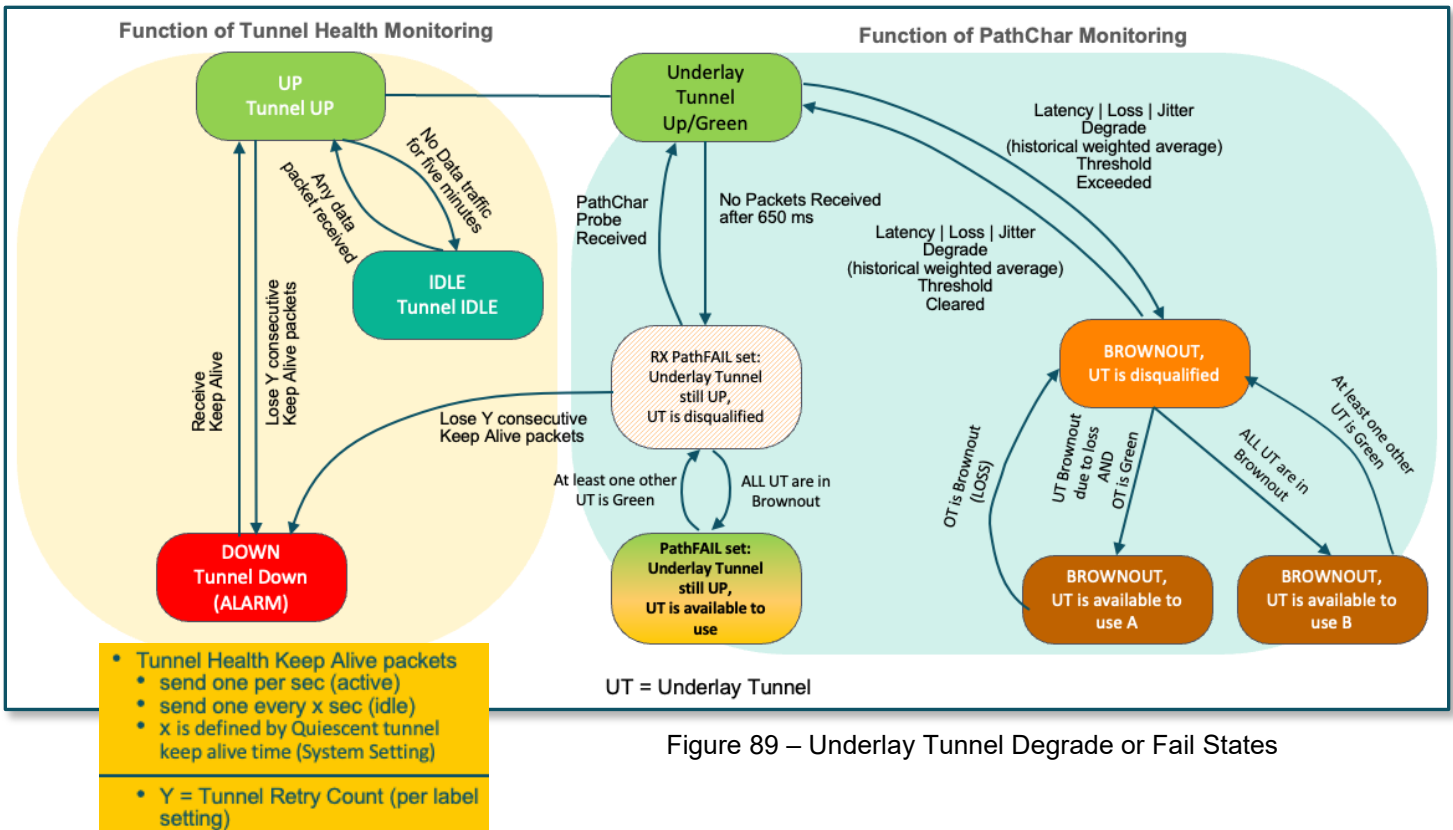


Figure 89 – Underlay Tunnel Degrade or Fail States

For underlay tunnel failure conditions, there are two actions:

1. Disqualify this UT – This is primarily controlled by PathChar/PathFAIL
2. Raise tunnel down alarm – This is primarily controlled by Tunnel Health

7 Link Bonding Policy Recommendations

Orchestrator ships with “default values” that are designed to make the SD-WAN work right out of the box. These provisioning and configuration settings have been tuned based on Aruba’s experience and direct engagement with thousands of enterprise customers who run their business operations over EdgeConnect SD-WAN. Default Orchestrator settings include four Business Intent Overlays that have pre-built Access Control Lists for each overlay with a ready-made list of applications (including SaaS applications) appropriate for the Business Intent Overlay.

Table 2 – Default Business Intent Overlay Configuration Summary

Priority	Overlay	Topology	Link Bonding Policy	Switch to Backup	Boost	Traffic Class
1	Real Time	Mesh	High Availability	Primary down	Disabled	1
2	Critical Apps	Mesh	High Quality	Primary down	Disabled	2
3	Bulk Apps	Mesh	High Quality	Primary down	Disabled	3
4	Default	Mesh	High Quality	Primary down	Disabled	4

When considering mapping applications to Link Bonding Policies, Aruba recommends the following:

Link Bonding Policy	Application Requirements	Best Used
High Availability	Extremely low packet loss and low jitter. Ideal for real-time applications, such as VoIP.	Typically for less than 20% of traffic by bandwidth.
High Quality	Low packet loss and jitter. Used for most enterprise applications.	Enterprise-critical or important traffic.
High Throughput	Low packet loss; tolerant of jitter.	Larger bandwidth underlay is preferred if underlay links are different sizes.
High Efficiency	Bulk data transfer that is tolerant to packet loss.	Bulk traffic where application layer is tolerant of packet loss.

End of Document.

