User Manual

Basic Configuration
Dragon PTN Ethernet Services

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

List of figures

List of Tables

1. INTRODUCTION

1.1 General

This document is valid as of Dragon PTN Release 4.3DR. This manual describes the configuration and monitoring of the Ethernet applications that can be used in Dragon PTN. An Ethernet application exchanges Ethernet traffic via the front ports of the IFMs to access the Dragon PTN network. An Ethernet service can be configured and monitored via the service type 'Ethernet' in HiProvision (=Dragon PTN Management System). Both port based and VLAN based services are supported. The Dragon PTN network is managed via HiProvision.

Prerequisites:

- The HiProvision PC must be configured/installed as described in Ref.[2Mgt] in Table 1.
- The Dragon PTN core network has been configured as described in Ref. [2Net] in Table 1.

NOTE: All applications that do not exchange Ethernet with Dragon PTN are called Legacy applications or Legacy services. More info Ref. [2Leg] in Table 1.

The supported hardware, firmware and software within this Dragon PTN release can be found on the Portal https://hiprovision.hirschmann.com via Shortcuts → Downloads.

1.2 Manual References

Table 1 is an overview of the manuals referred to in this manual. '&' refers to the language code, '*' refers to the manual issue. These manuals can be found in the HiProvision Help Tile.

Table 1 Manual References

Ref.	Number	Title
[1]	DRA-DRM801-&-*	Dragon PTN Installation and Operation
[2Mgt]	DRA-DRM830-&-*	HiProvision Management Operation
[2Eth]	DRA-DRM831-&-*	Dragon PTN Ethernet Services
[2Leg]	DRA-DRM832-&-*	Dragon PTN Legacy Services
[2Net]	DRA-DRM833-&-*	Dragon PTN Network Operation
[3]	DRB-DRM802-&-*	Dragon PTN Aggregation Nodes: PTN2210, PTN2206, PTN1104, PTN2209
[3b]	DRB-DRM840-&-*	Dragon PTN Core Nodes: PTN2215
[4]	DRD-DRM803-&-*	Dragon PTN Central Switching Module: PTN-CSM310-A/PTN-CSM540-A
[5]	DRE-DRM807-&-*	Dragon PTN Interface Module: PTN-4-GC-LW/ PTN-4-GCB-LW
[9]	DRE-DRM808-&-*	Dragon PTN Interface Module: PTN-1-10G-LW
[12]	DRE-DRM817-&-*	Dragon PTN Interface Module: PTN-4-GO-LW
[14]	DRF-DRM811-&-*	Dragon PTN TRMs (Transmit Receive Modules: SFP, XFP, QSFP+)
[23]	DRE-DRM823-&-*	Dragon PTN Interface Module: PTN-9-L3A-L (=main) / PTN-9-L3EA-L (=extension)
[24]	DRG-DRM826-&-*	HiProvision Add-on: Generic Reporting Engine
[25]	DRE-DRM827-&-*	Dragon PTN Interface Module: PTN-6-GE-L
[26]	DRE-DRM842-&-*	Dragon PTN Interface Module: PTN-1-40G-LW
[27]	DRE-DRM843-&-*	Dragon PTN Interface Module: PTN-4-10G-LW
[100]	DRA-DRM828-&-*	Dragon PTN Bandwidth Overview

2. ETHERNET

2.1 General

IFMs that support the Ethernet service:

- 4-GC-LW, 4-GCB-LW, 4-DSL-LW, 1-40G-LW, 4-10G-LW, 6-GE-L, 9-L3A-L (=main) / 9-L3EA-L (=extension)

The figure below shows an Ethernet application/service example:

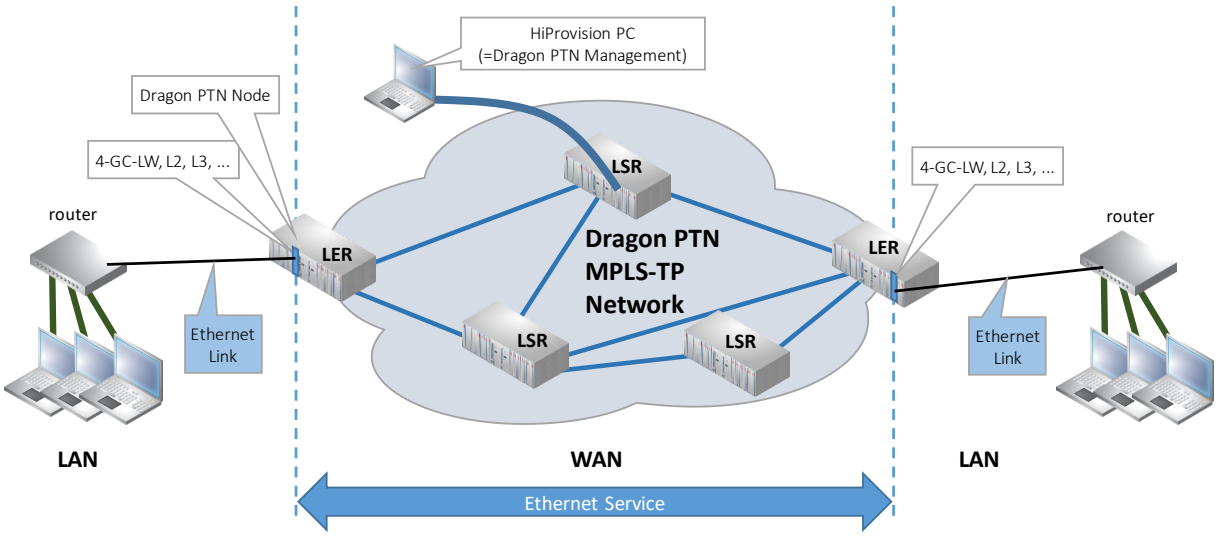

Figure 1 Ethernet Application/Service Example

2.2 Configure Service

2.2.1 Service Wizard

NOTE: The amount of services, not using a point-to-point tunnel, that can be created in a node is determined by the amount of available VFIs (= Virtual Forwarding Instance) in the CSM. Both the CSM310-A and CSM540-A currently support a maximum of 64 VFIs. Each such created service in a node consumes 1 VFI in that node. A second redundant CSM in the node does not increase the amount of VFIs in that node.

NOTE: If needed, a service can be modified later on as described in §2.3.

Prerequisite:

- At least one tunnel must have been created (except for the Local Mode), see Ref. [2Net] in Table 1;
- Before creating the service, best check if there is sufficient bandwidth available on the WAN links of the Dragon PTN network, see §3.3.2.
- Configure and load the necessary port properties first (via Dashboard → Network Hardware) before creating the service via the services wizard!
- Backup your database as described in Ref. [2Mgt] in Table 1.

A service connects front ports on one side of the tunnel to the front ports on the other side of the tunnel. The service can be programmed within one tunnel or within multiple combined tunnels with each tunnel already configured before. See figures below:

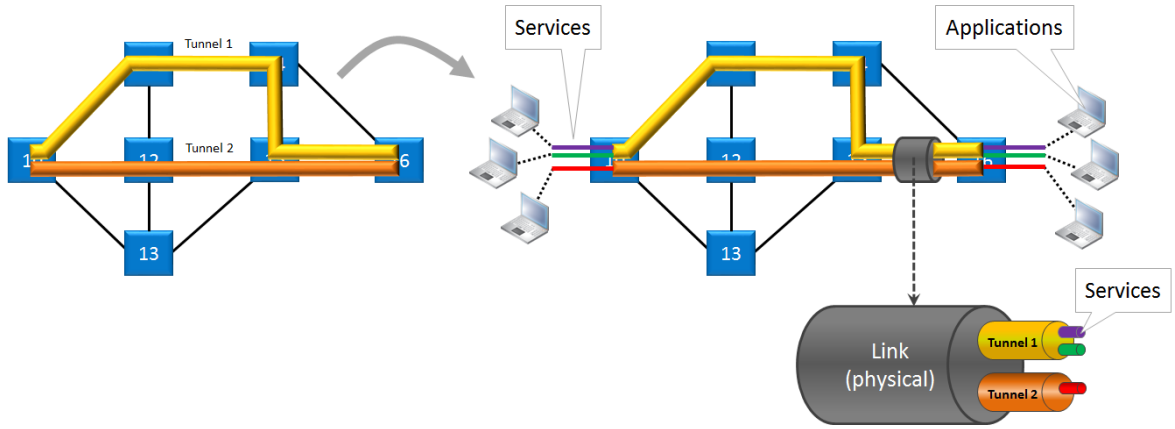

Figure 2 Service Creation in Tunnels

NOTE: If one tunnel cannot cover the required service path, multipoint, logical ring and subring tunnels can be combined into one big tunnel to provide the path. Tunnels must be combined in a Tunnel Combination Point, which is a node in which one tunnel ends and the other tunnel starts, see figure below.

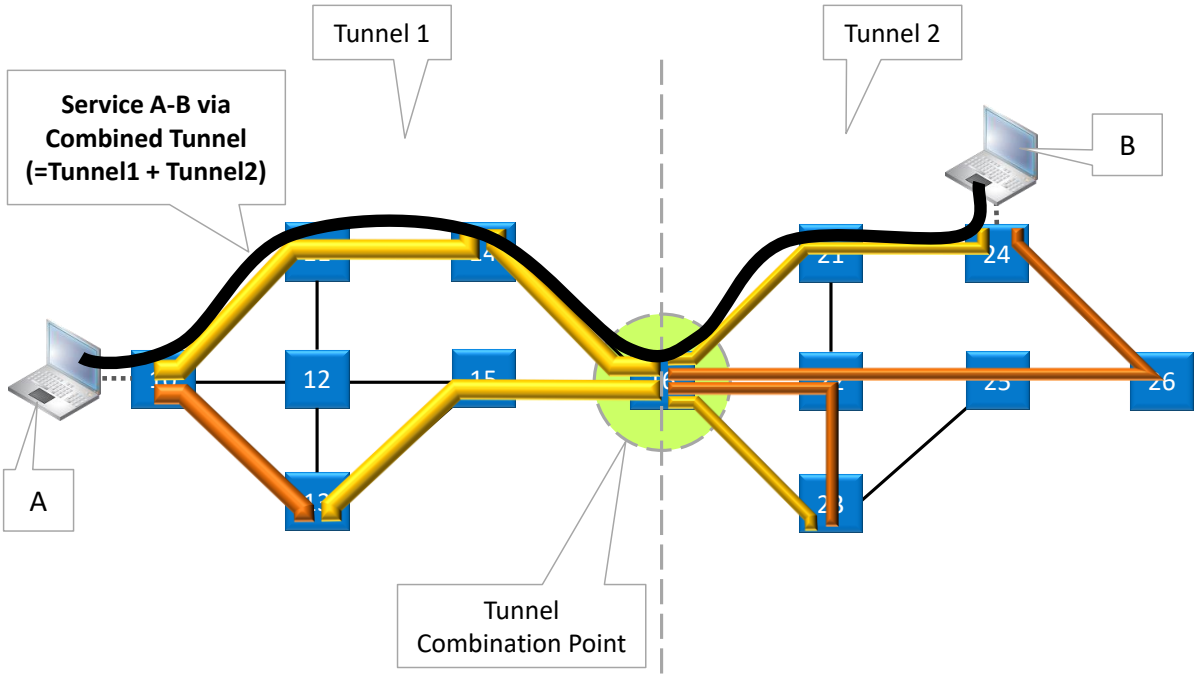

Figure 3 Service Via Combined Tunnels

In this manual, the following terminology is used for a better readability:

- 'main L3 IFM' = 9-L3A-L IFM, has its own switch ASIC onboard;
- 'extension L3 IFM' = 9-L3EA-L IFM;
- 'L3 IFM' could either mean:
  - 'main L3 IFM' only = 8+1 front ports;
  - The 'main L3 IFM' combined with an 'extension L3 IFM' = 16+2 front ports;
- L2 IFM = 6-GE-L IFM, has its own switch ASIC onboard;
- Ethernet IFM: All other IFMs that are Ethernet related. All these IFMs do not have a switch ASIC onboard. The switching happens on the CSM. The Ethernet IFM ports are in fact CSM switch ASIC ports. E.g 4-GC-LW, 4-GO-LW, …. IFMs. All these IFMs are listed in the Feature Support Matrix in Ref.[2Net] in Table 1.

NOTE: More information on all these service features can be found in the manuals of the IFMs listed in Table 1.

Click Dashboard → Configuration → Connections → Services → + to open the services wizard. See figure below.

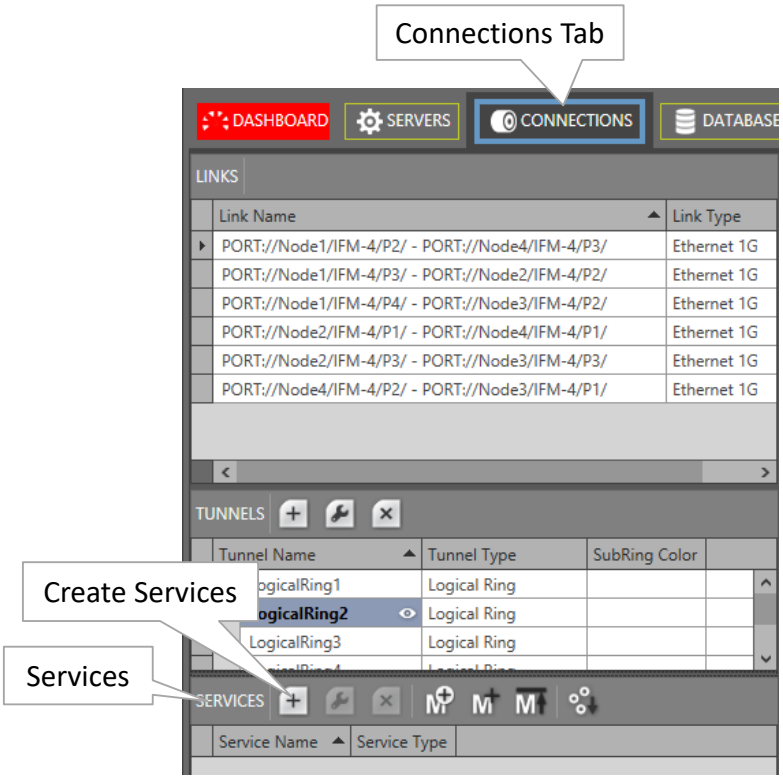

Figure 4 Create Services

The services wizard opens. The list below summarizes every page in the wizard:

- Page: Information: Click Next>>;
- Page: Service Name and Type Selection:
  - Service Name: enter a name for your service.
  - Service Type: Ethernet;

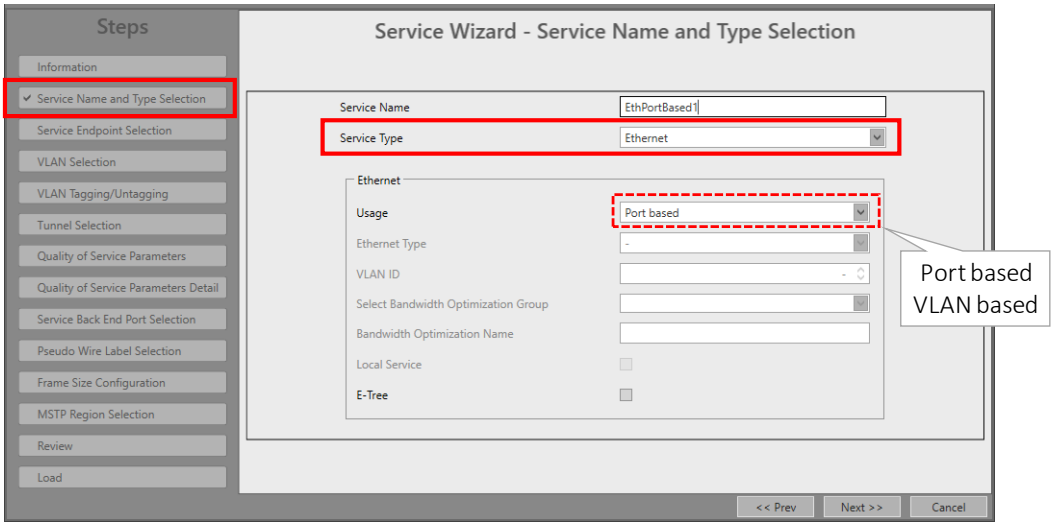

Figure 5 Service Type: Ethernet

- Usage:
  - Port Based (=default): Use this mode if all the traffic on a port must be transported in one and the same service;
  - VLAN Based: Use this mode in combination with the Ethernet Type option (see next) to transport one or more VLANs in one service;
- Ethernet Type (only for VLAN Based):
  - Single VLAN: Select this mode if you only want to transport one VLAN on a port;
    - VLAN ID: Set the default VLAN ID in the range [2-3699, 3802-4000] for this service. Ethernet packets with this VLAN ID will be forwarded in this service, other VLAN IDs and untagged packets will be dropped. This behaviour can be overruled by a more advanced VLAN processing in the 'VLAN Tagging/Untagging' feature further on this wizard;
    - Select Bandwidth Optimization Group: Grouping some non-overlapping single VLAN based services (in a logical ring) together in one group optimizes the consumed network bandwidth. CAUTION: This is an expert feature and is preferably used during the network design phase, see also §4.8.
    - Bandwidth Optimization Name: When creating a new Bandwidth Optimization Group, fill out the name of this new group;
    - Local Service (only for VLAN Based services on L2/L3 IFMs). See §4 for more information:
      - unchecked (=default): The service will go via tunnels, WAN ports and the Dragon PTN network;
      - checked: The service will only use the LAN side (or front ports) of L2/L3 IFMs, the service will not use tunnels, WAN ports nor the Dragon PTN network. It will not consume bandwidth on the Dragon PTN network.
  - Multi VLAN: Select this mode if you want to transport multiple VLANs on a L2/L3 port. Multiple VLANs are transported via adding a Q in Q VLAN ID (=outer-VLAN) around the original VLANs (=inner-VLANs) from LAN to WAN, and removing it again from WAN to LAN. See §4 for more information.

- Q in Q VLAN ID: fill out the outer-VLAN to transport multiple inner-VLANs;

- E-tree: yes/no(=default), see §9.1 and Figure 8 for more information;

- Page: Service End Point Selection:
  - Make sure that all your service ports are LAN ports. Normally, this has been done already in Ref. [2Net] in Table 1. But if it was forgotten for a port, it can still be set via the Network Settings wizard (see below) without leaving the services wizard.

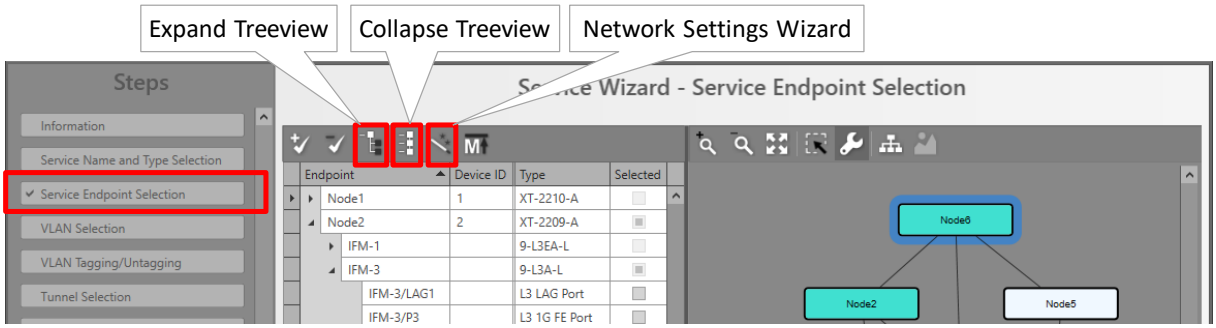

Figure 6 Open Network Settings Wizard

  - Select the front ports on the IFMs that must be part of the service. Make sure to select the ports in nodes that are linked by the same tunnel. Selecting ports can be done in two ways:
    - Via the table. The tree view can be expanded/collapsed via clicking the expand/collapse buttons. Just click the Selected checkbox to select the desired port.
    - Via clicking the node icons in the network drawing, see figure below.

    A port icon overview can be found below:

    - brown LAN port = available for this service, the port number is shown in the port icon when hovering over it;
    - brown bold LAN port = selected for this service;
    - white LAN port = unavailable for this service, cannot be selected (correct port type but already taken by another service or wrong port type);
    - white filled WAN port = Cannot be selected.
    - In most of the cases, available means not taken at all by any service. In case of an Ethernet IFM, available could additionally indicate a VLAN port which already has one or more VLAN based Ethernet services configured
    - Only on L2/L3 IFMs:
      - brown LAG port = available for this service;
      - brown LAG port = selected for this service;
      - white LAG port = unavailable for this service, cannot be selected (correct port type but already taken by another service or wrong port type);
    - Only on L3 IFMs (see also §4 for more info):
      - brown router : available VRF (=Virtual Routing and Forwarding) port which can be included in the service. Click this icon if this service must only reach the

virtual router instance and not the front ports in this IFM. If you click this icon, the front ports on this IFM will become unavailable ☐ for this service and vice versa.

- white router ⊗: 1) unavailable VRF port for this service because it is already included in another service... or 2) automatic included VRF port because normal L3 IFM LAN ports are selected for this service in this IFM.

NOTE: Per port, an extra Info field can be filled out later on via Network Hardware Devices → Select Node/IFM/Port → Generic → Info.

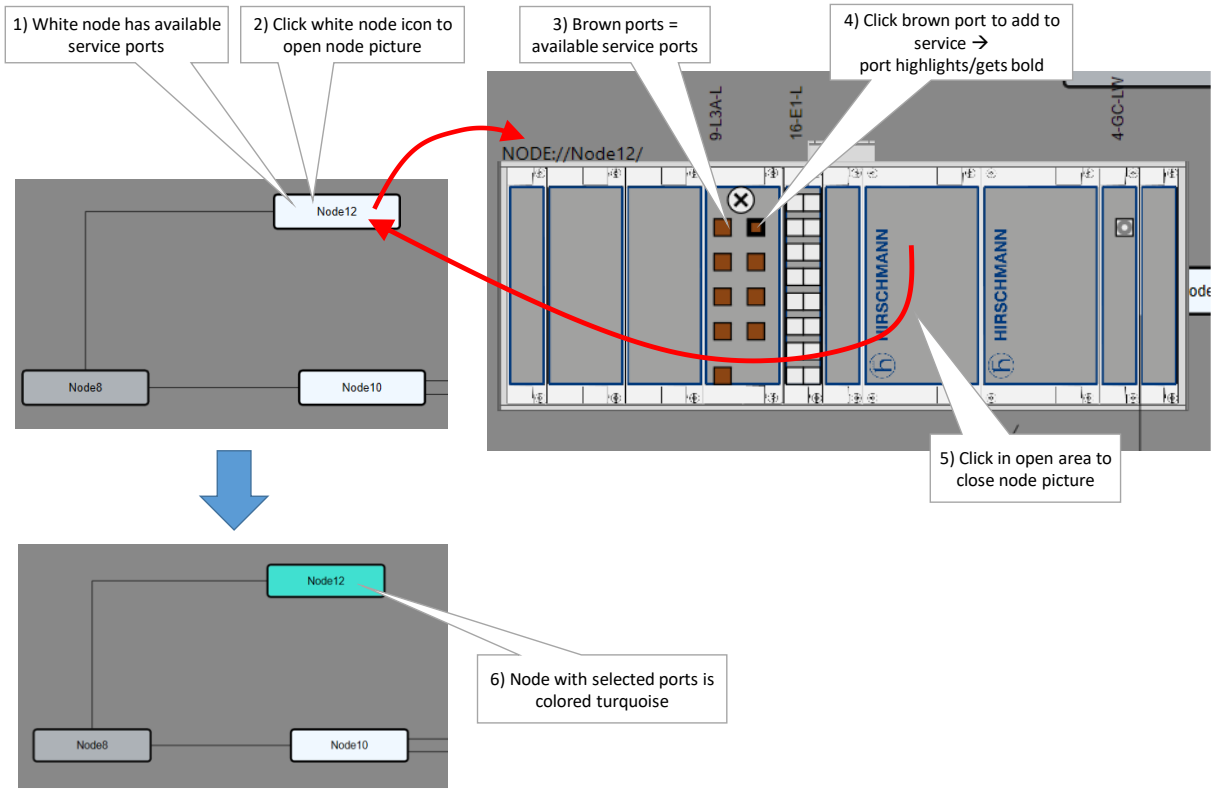

Figure 7 Service Ports Selection

- If E-tree was selected previously, all selected ports are by default set as **leaf** ports. Change at least 1 and maximum 4 of these ports into **root** ports (see §9.1 for more info on E-tree, see Ref. [2Net] in Table 1 which IFMs support E-tree). See the figure below.
- A node can have a maximum of 32767 MAC addresses. By default, per new Ethernet, 500/256 MAC addresses will be added to each LER node of the tunnel in which the Ethernet service resides (not for point-to-point tunnels). If the maximum number of MAC addresses on a node has been reached, an error warning will pop up. You have to decrease the number of MAC addresses assigned to other services in this node first via clicking the MAC limit button (see also §9.5). See the figure below:

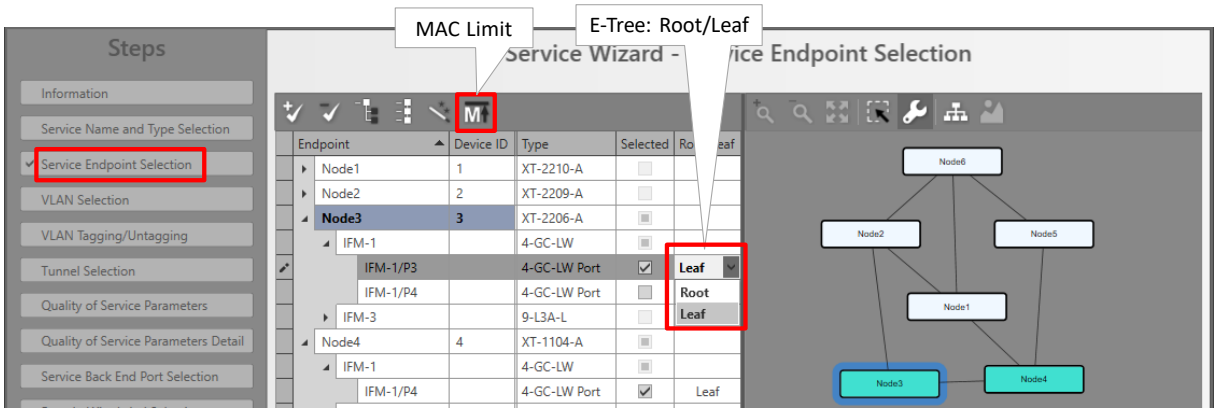

Figure 8 MAC Limit / E-Tree: Root & Leaf Ports Selection

- Page: VLAN Selection: This page is only relevant when L2/L3 IFM ports are involved in the service, see §4 for more info on VLAN selection and how to configure it.
- Page: VLAN Tagging/Untagging: HiProvision supports VLAN processing for 4-GC-LW, … ports in port based and single VLAN based services, not for L2/L3 ports. The possible actions depend on whether the service is port based or VLAN based.
  - ATTENTION: By default, the VLAN processing behavior in this wizard page is set up as described previously in the 'Service Name and Type Selection' page in this wizard: Only forward packets (ingress and egress) with the configured VLAN ID and drop all the other packets. When changing the settings in the 'VLAN Tagging/Untagging' window, it will overrule the default behavior.
  - The possible VLAN processing actions are described in the table below. Each port in the service can be configured with its own VLAN processing. For applying the same VLAN processing to multiple ports at once, use the Multiple Settings Mode button. Configure the VLAN settings and click the apply button Apply.

Table 2 VLAN Tagging/Untagging

Port/VLAN Based	Ingress/ Egress	Possible Actions	Description
Note: A Prio Tag is a VLAN tag with VLAN ID = 0 Note: the actions are only valid for the configured endpoints in the configured service Note: Ingress and Egress VLAN ID: the configured VLAN ID is the same for both INGRESS and EGRESS			
Port Based (see Figure 9 below)	Ingress	None	None
	Egress	Keep Tag	The VLAN or Prio tag is kept when sending out the Ethernet packet (transparent transport of packets).
		Untag	The VLAN or Prio tag is removed from the Ethernet packet when sending out the packet.
		PrioTag	Replace the VLAN tag with a Priority tag.
		Replace Tag	Replace the VLAN ID in the outgoing Ethernet packet with the configured VLAN ID in the range [2-3699, 3802-4000].
		Add Tag	A VLAN tag with the configured VLAN ID will be added to untagged packets.
VLAN Based	Ingress	Untagged: Drop	Incoming untagged Ethernet packets will be dropped.

Port/VLAN Based	Ingress/ Egress	Possible Actions	Description
(see Figure 10 below)		Untagged: Tag and forward (<configured VLAN ID>)	Incoming untagged Ethernet packets will be tagged with the configured VLAN ID in the range [2-3699, 3802-4000] and forwarded.
		Priority Tagged: Drop	Incoming priority tagged Ethernet packets will be dropped.
		Priority Tagged: Tag and forward (<configured VLAN ID>)	Replace the priority tag (=VLAN ID 0) in the incoming Ethernet packet with the configured VLAN ID in the range [2-3699, 3802-4000] and forward it.
	Egress	Keep Tag	The VLAN or Prio tag is kept when sending out the Ethernet packet (transparent transport of packets).
		Untag	The VLAN or Prio tag is removed from the Ethernet packet when sending out the packet.
		PrioTag	Replace the VLAN tag with a Priority tag.

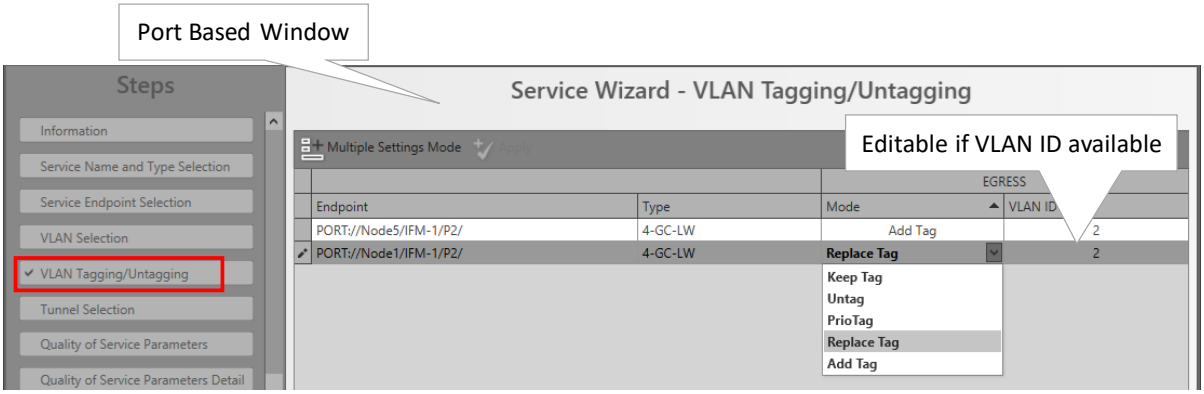

Figure 9 Port Based: VLAN Tagging/Untagging

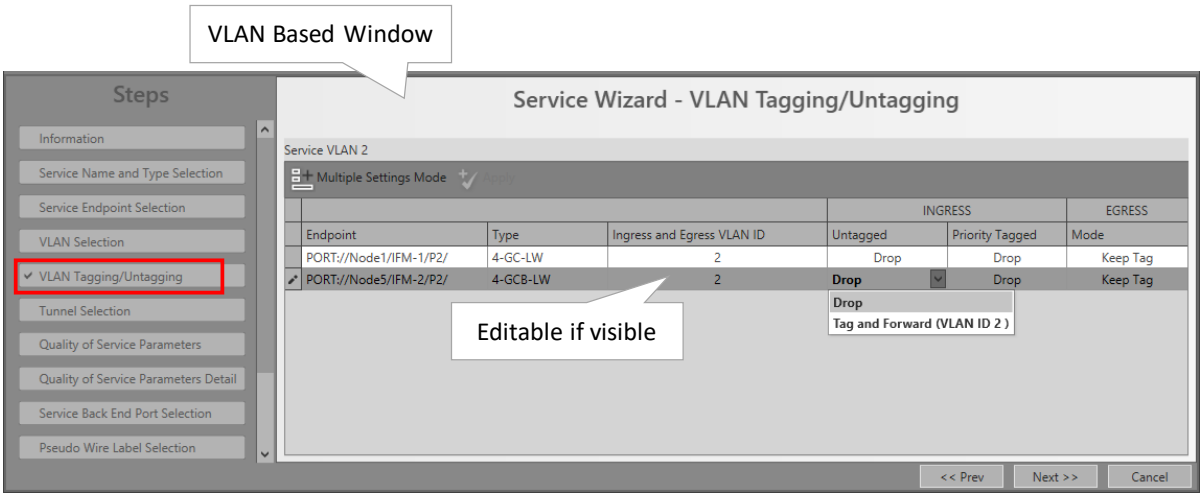

Figure 10 VLAN Based: VLAN Tagging/Untagging

- Page: Tunnel Selection: Select the required tunnels to transport your configured service via checking the 'Selected' checkbox.

- HQoS: Shows the 'HQoS Application Priority' for tunnels that had 'Use HQoS' activated at tunnel creation time (Ref. [2Net] in Table 1). Shows '-' for tunnels without HQoS;
- Match (x/y):
  - x: number of reachable service ports (or termination points) via this tunnel;
  - y: number of selected service ports (or termination points);
  - Perfect match: e.g. 3/3: all the selected service ports belong to nodes that are all linked to this tunnel. This tunnel can transport the service;
  - Mismatch: e.g. 2/3: at least one of the selected service ports belongs to a node that is not linked to this tunnel. A single selected tunnel with a mismatch cannot transport the service;
  - Selected: checkbox to select the tunnel.
- One tunnel: If only one tunnel is selected, this tunnel has to have a perfect match to transport the service;
- Combined tunnels: multiple tunnels can be selected or combined (by just selecting them in the tunnel list) into one big tunnel to transport the service. It is possible to combine single tunnels with a mismatch into one big combined tunnel that has a perfect match for the entire service. Point-to-point tunnels cannot be combined, see Figure 3;

NOTE: If no tunnel with a perfect match is available, it is also possible to create a new tunnel via clicking +. In doing so, the tunnel wizard will automatically select the needed devices for this service. After closing the tunnel wizard, the new tunnel will automatically appear in the tunnel list;

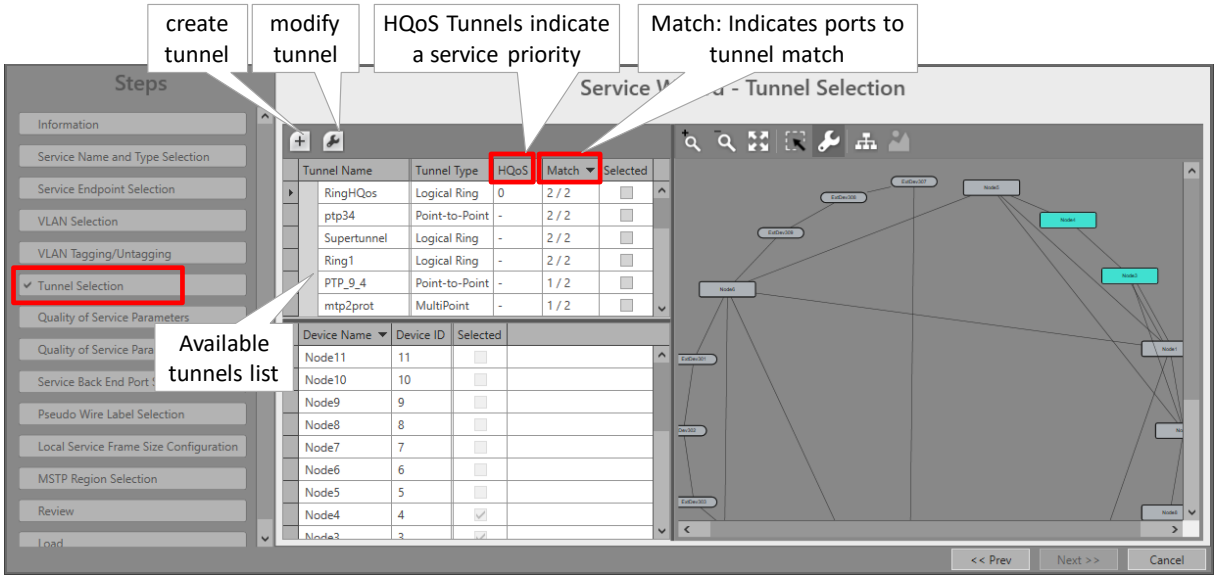

Figure 11 Ports to Tunnel Match

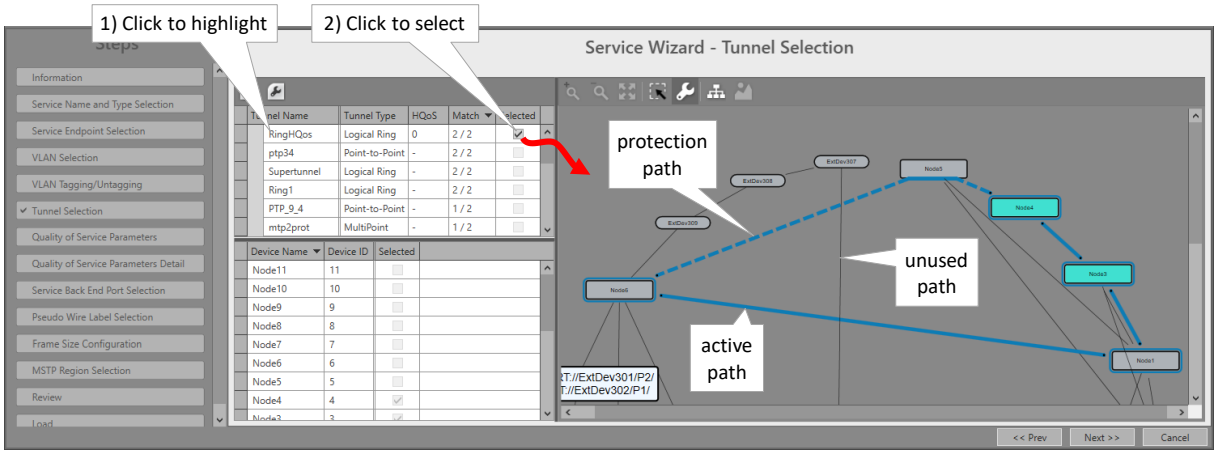

Figure 12 Selected Highlighted Tunnel

- Page: Quality of Service Parameters: In this page, Ethernet traffic engineering can be configured or tuned: 'Queueing/Scheduling' and 'Policing and Shaping'. See §3 for more information on traffic engineering and how to configure it.

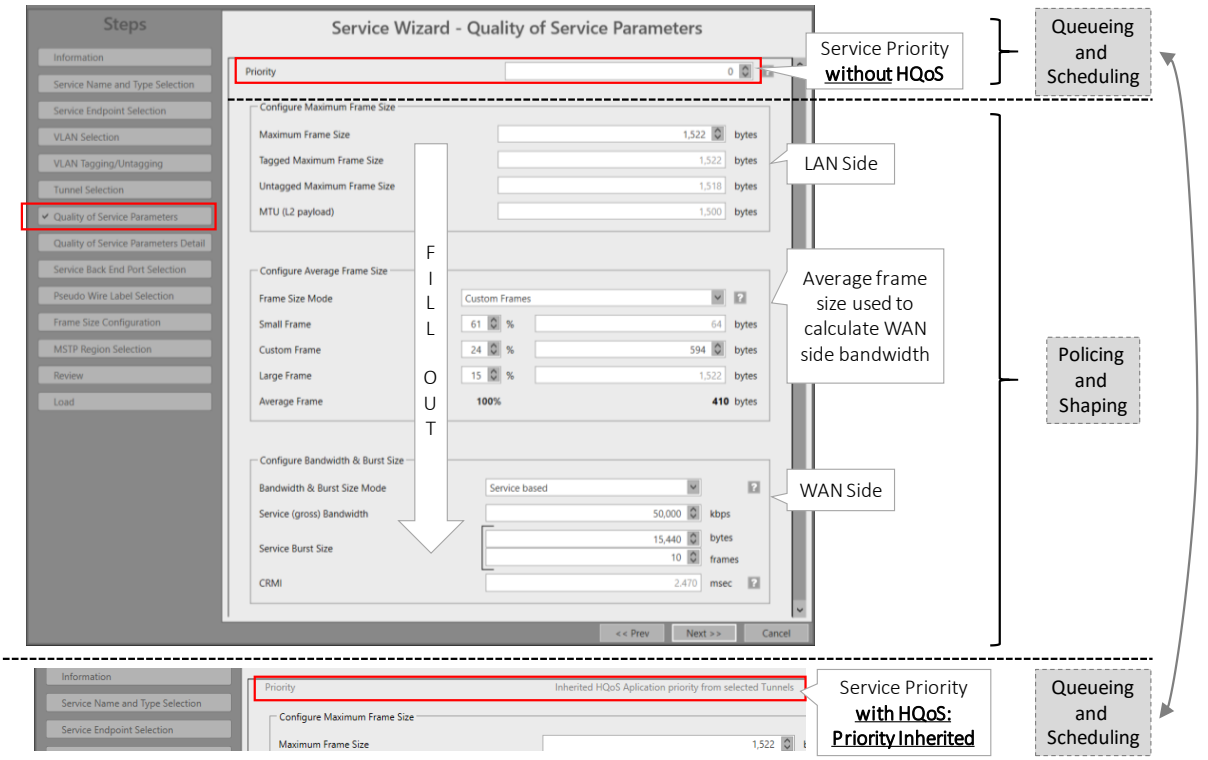

Figure 13 Quality of Service Parameters

- Page: Quality of Service Parameters Detail: This page allows advanced tuning for Policing and Shaping. HiProvision automatically calculates default values for all options in this page. If these values are fine for you, click Next. If you want/need advanced tuning, see §3.3.5 for detailed information and configuration.
- Page: Service Back Endpoint Selection: This page is only relevant when L2/L3 IFM ports are involved in the service, see §4 for more info;
- Page: Pseudo Wire Label Selection: leave this page as it is, the defaults are OK;

- Page: Frame Size Configuration: this page is hit when no tunnel is needed during the service creation. As a result, the normal 'Quality of Service Parameters' page is not hit, but instead, this page is hit. This is the case in the following scenarios below. The Maximum Frame Size [64..9238 bytes] can be configured in this page (default =1522 bytes). As a result, the Tagged Maximum Frame Size, Untagged Maximum Frame Size and MTU (L2 payload) are automatically defined as well.
  - 'Local Service' was selected in 'Service Name and Type Selection';
  - L2 or L3 ports (not a mix) were selected in a VLAN based (single VLAN) service in only one node.

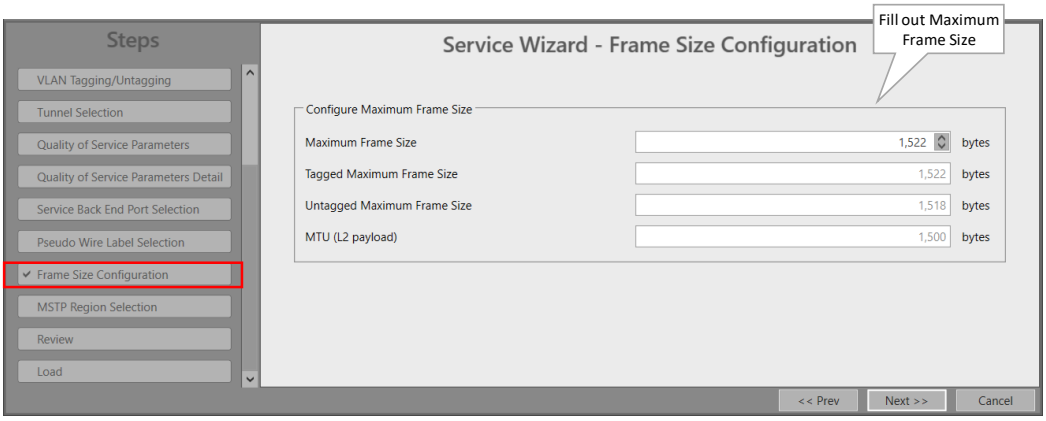

Figure 14 Frame Size Configuration

- Page: MSTP Region Selection (only when modifying an Ethernet service involved in Regions/MSTP (see §5.4) and adding a L2/L3 IFM which is still part of the default MSTP Region): A configured Ethernet service can overlap different MSTP regions. When adding a L2/L3 IFM to this service, the IFM will run with the default MSTP settings available on the IFM itself (not visible in HiProvision) and indicated by 'Default Region'. Loop protection is guaranteed via this 'Default Region'. If you immediately want to assign this IFM to an existing MSTP Region, select one from the Region drop-down list. If not, leave 'Default Region' selected. Later on in the MSTP wizard, you can still assign this IFM to a new or existing Region.
- Page: Review: The selected service ports will be shown. If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

- After this step, your customer applications connected to the front ports of the IFMs should be able to communicate over the Dragon PTN network.

2.2.2 Network Hardware → IFM Settings

None.

2.2.3 Network Hardware → IFM-Port Settings

After configuring the service via the service wizard, all port settings of the endpoints in this service will be set according to the service configuration. Some individual port settings might need extra tuning or must be overruled. Port Settings can be found via Dashboard → Network Hardware → Devices → Select Device → Select Ethernet IFM (e.g. 4-GC-LW…) → Select port.

The following settings can be configured on Port level. An overview of all the port settings can be found in the table at the bottom of this paragraph.

- Generic:
  - Info: This optional field allows to fill out some extra information on this port. E.g. Brussels Train Station Camera 100.
- Specific:
  - Admin Status: A LAN port in a service can be set Up/Down. A WAN port is always up.
  - Port Mode (LAN/WAN). An unused port is by default in WAN mode. If the port is not set as WAN port in a link, it can be set as LAN port via Dashboard → Network Hardware → Network Settings Wizard button =  → Port Mode. LAN ports can be used as ports in an Ethernet service.
  - PHY Mode (LAN/WAN) (only for 1-10G-LW ports: LAN is default, but when configured in WAN, the port operates in Sonet OC-192c. More info in Ref. [9] in Table 1.
  - Negotiation (Auto=default/No Negotiation): (only for copper 1 Gigabit Ethernet ports) Negotiation advertises and negotiates the speed and duplex mode(s) of this port with the destination port. If 'No Negotiation' is selected, fill out both the source and destination port with fixed settings:
    - Duplex Setting (Full/Half)
    - Speed Setting (10 Mbps/100 Mbps/1 Gbps)
    - Flow Control (Disable/Enable): Flow control is a traffic congestion control mechanism that uses pause frames to solve the congestion. If the destination receives too much traffic and Flow Control is enabled, it will send pause frames to the sending source. The pause frame instructs the source to stop sending packets for a specific period of time. If Flow Control is also enabled at the sending station, it waits the requested time before sending more data.

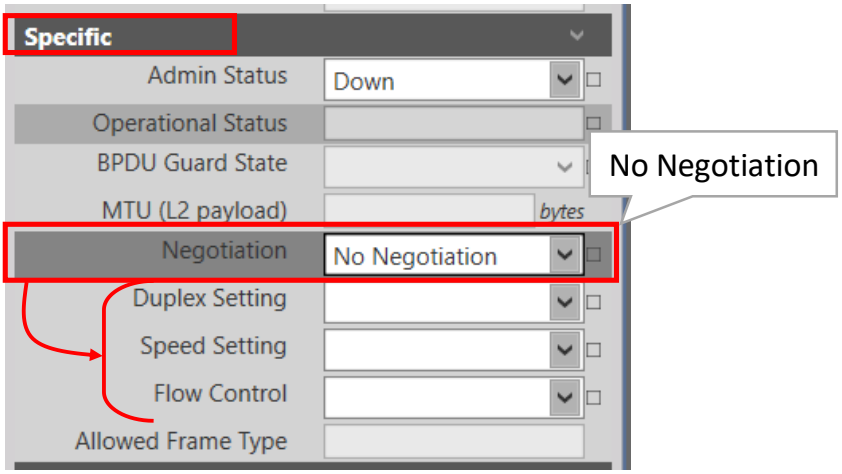

Figure 15 Negotiation: No Negotiation

NOTE: Optical LAN ports (1 Gbps, 10 Gpbs, 40 Gbps) always run in autonegotiation.

NOTE: Make sure both the source and destination port are configured with the same Negotiation/Speed/Duplex settings. Flow control could be different.

- BPDU Guard: see §9.3.
- QoS Classification (DSCP/VLAN Priority) used in HQoS for incoming traffic on LAN ports and back end ports on L2/L3 IFMs, see §3;

- Storm Control: on LAN front ports (4-GC-LW, L2, L3, …) and back end ports (L2, L3), see §9.2.
- Power Over Ethernet: PoE settings on copper LAN ports, see §6;
- SFP: see Ref. [14] in in Table 1;
- Smart SFP: see Ref. [2Leg] in Table 1;
- IEEE1588 Settings: see Ref. [2Net] in Table 1;
- Apply your changes and load these changes into the Dragon PTN network.

Table 3 Port Settings

IFM Type		Ethernet IFM												L2 IFM		L3 IFM			
Speed		1G		1G		1G		10G		10G		40G		1G		1G		10G	
IFM		4-GC-LW 4-GCB-LW		4-GO-LW		1-10G-LW		4-10G-LW		1-40G-LW		6-GE-L		9-L3A-L 9-L3EA-L					
Ports (O=Optical, E=Electrical, B=Back End)		p1(O)		p1-4(E)		p1-4(O)		p1(O)		p1-4(O)		p1(O)		p1-6(E)	P1-5(B)	p1-8(O)	p1-4(B)	p9(O)	p5(B)
Port Mode: LAN/WAN/Back End		L	W	L	W	L	W	L	W	L	W	L	W	L	B	L	B	L	B
Specific	(set) Admin Status	✓	---	✓	---	✓	---	✓	---	✓	---	✓	---	✓	✓	✓	✓	✓	✓
Specific	Negotiation	✓	---	✓	---	✓	---	---	---	---	---	---	---	✓	---	✓	---	---	---
Specific	(No Negotiation →) Speed, Duplex, Flow Control	✓	---	✓	---	---	---	---	---	---	---	---	---	✓	---	✓	---	---	---
Specific	BPDU Guard	✓	---	✓	---	✓	---	✓	---	✓	---	✓	---	✓(1)	---	✓(1)	---	✓(1)	---
Specific	QoS Classification	✓	---	✓	---	✓	---	✓	---	✓	---	✓	---	---	✓	---	✓	---	✓
Specific	PHY Mode	---	---	---	---	---	---	✓	✓	---	---	---	---	---	---	---	---	---	---
Storm Control	(all properties)	✓	---	✓	---	✓	---	✓	---	✓	---	✓	---	✓	✓	✓	✓	✓	✓
PoE Settings	(all properties)	---	---	✓(2)	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
PoE Diagnostics	(all properties)	---	---	✓(2)	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
IEEE1588 Settings (A)	(all properties)	✓(3)	✓(3)	✓(3)	✓(3)	✓(3)	✓(3)	✓	✓	---	---	---	---	---	---	---	---	---	---
Smart SFP	(all properties)	✓	✓	---	---	✓	✓	---	---	---	---	---	---	---	---	---	---	---	---
SFP	(all properties)	✓	✓	---	---	✓	✓	---	---	---	---	---	---	---	---	✓	---	---	---
XFP	(all properties)	---	---	---	---	---	---	✓	✓	✓	✓	---	---	---	---	---	---	✓	---
QSFP+	(all properties)	---	---	---	---	---	---	---	---	---	---	✓	✓	---	---	---	---	---	---
Note: (A): Only supported on Aggregation Nodes / (1): Via MSTP Wizard / (2): only for 4-GC-LW / (3): All parameters are supported on all ports except for 'IEEE1588 Encapsulation = Ethernet IP/UDP' wich is only supported on port 3 and 4.																			

2.3 Modify Service

Click Dashboard → Configuration → Connections → Services → select service →  to modify the service. The following parameters can be modified:

- Port Based/VLAN Based:
  - Service Name;
  - VLAN ID (VLAN Based)
  - Port Mode Settings;
  - E-Tree;
  - MAC Limits;
  - Add/Remove Ports → Possible 'QoS Parameters' pop-up if port input bandwidths have been customized previously. See §3.3.6 for more info.
  - VLAN Tagging/Untagging;
  - Selected tunnels;
  - Quality of Service Parameters;

2.4 Delete Service

After service creation, this service can be deleted if needed via Dashboard → Configuration → Connections → Services → select service →  ;

2.5 Troubleshooting

2.5.1 Ethernet Service Fails with Multiple Tunnels on Same Link

When a programmed Ethernet service arrives on Node x, Port y via Tunnel 1 in Link z, and it leaves the node via another Tunnel 2 in the same Link z, traffic will be blocked due to a broadcast flooding setting.

When you have a similar configuration and the problem occurs, contact https://hirschmannsupport.belden.eu.com for further assistance).

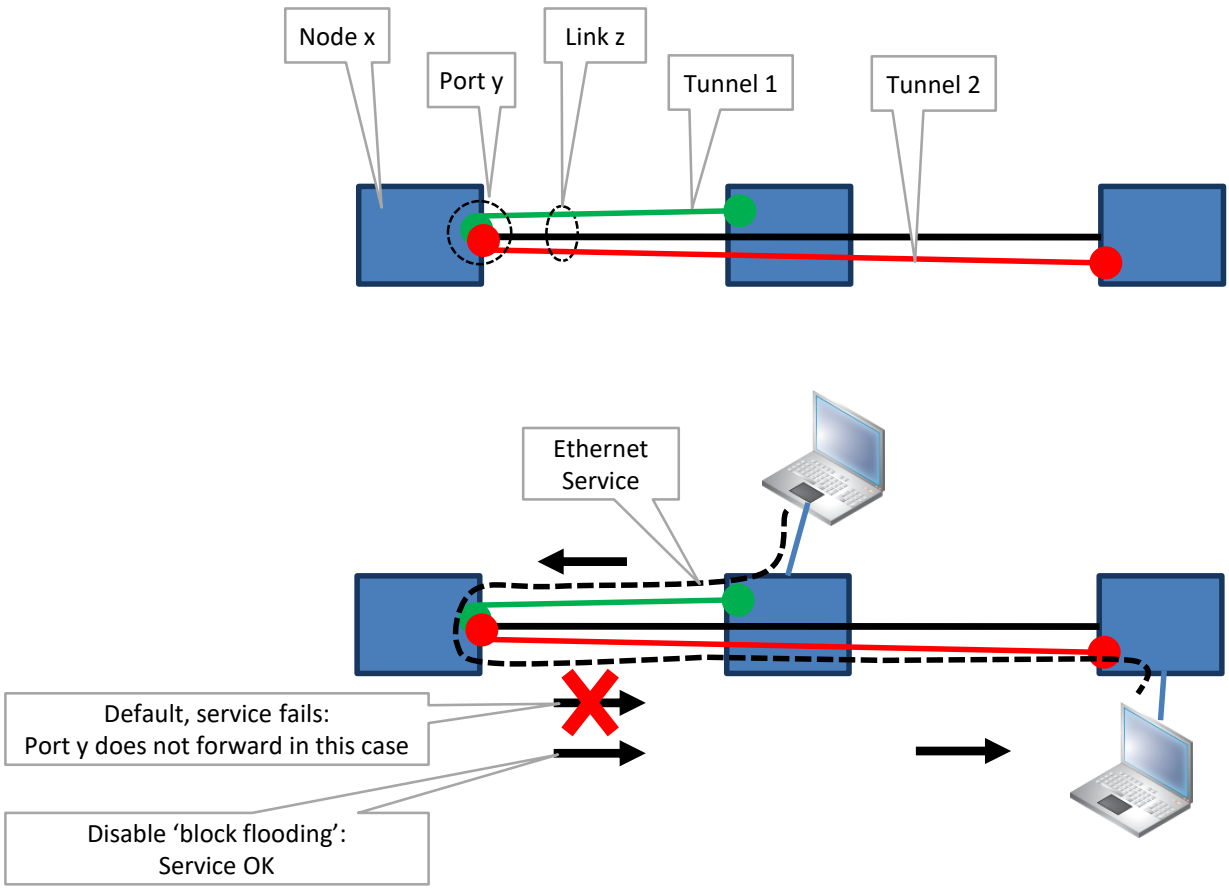

Figure 16 Ethernet Service Fails with Multiple Tunnels on Same Link

2.5.2 Debugging the Network via Port Mirroring

See Ref. [2Net] in Table 1.

2.6 Monitoring

2.6.1 (Configuration) Network Hardware Tile

None.

2.6.2 (Configuration) Connections Tile

What has been configured via the service wizard can also be viewed via Dashboard → Connections → Services → select service in the list. Some extra tabs with service configuration data will be shown.

CAUTION: The configuration that you see here is the service configuration done via the service wizard. Port settings could be tuned manually via §2.2.3 and as a result could be different from these service settings. Always verify these port settings as well, to know the exact port setting in the live network.

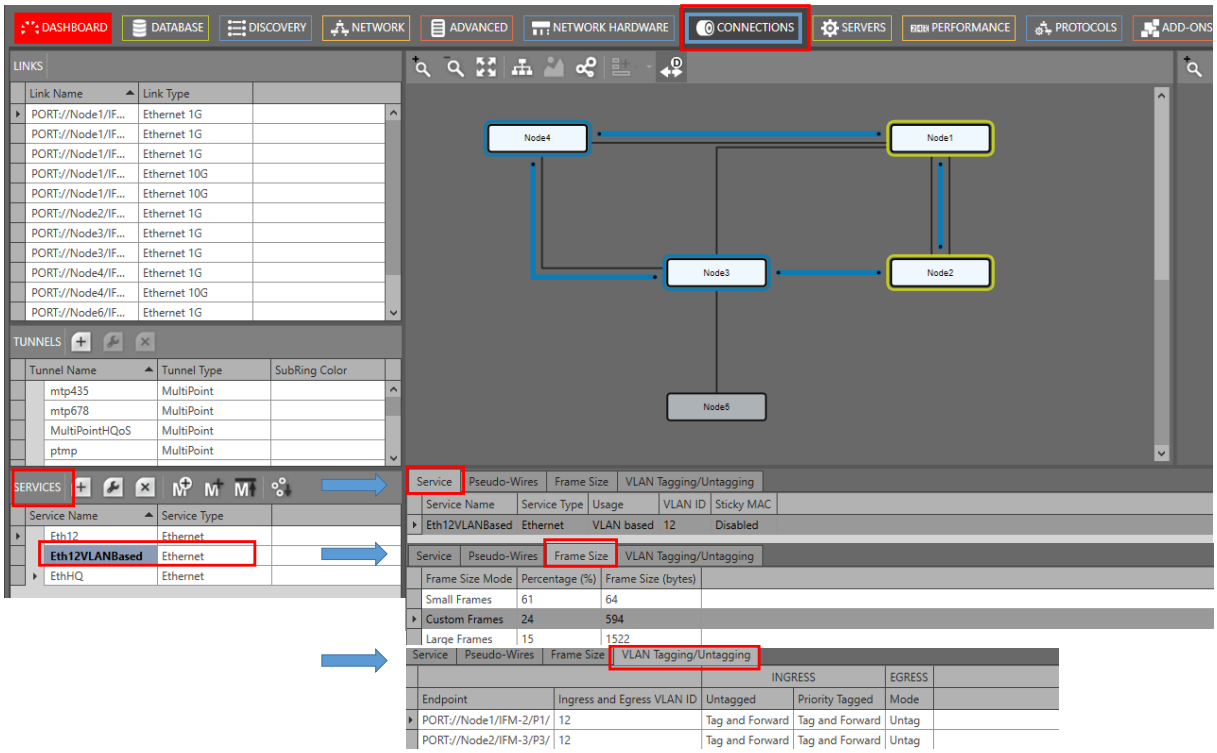

Figure 17 (Configuration) Connections Tile: Ethernet Service

2.6.3 (Monitoring) Network Tile

Live service data can be monitored via the Dashboard → Network → Services → select service in the list. The service will be shown in the network drawing. Click P to show extra monitoring properties for this service. Click N to show the used nodes/links/tunnels.

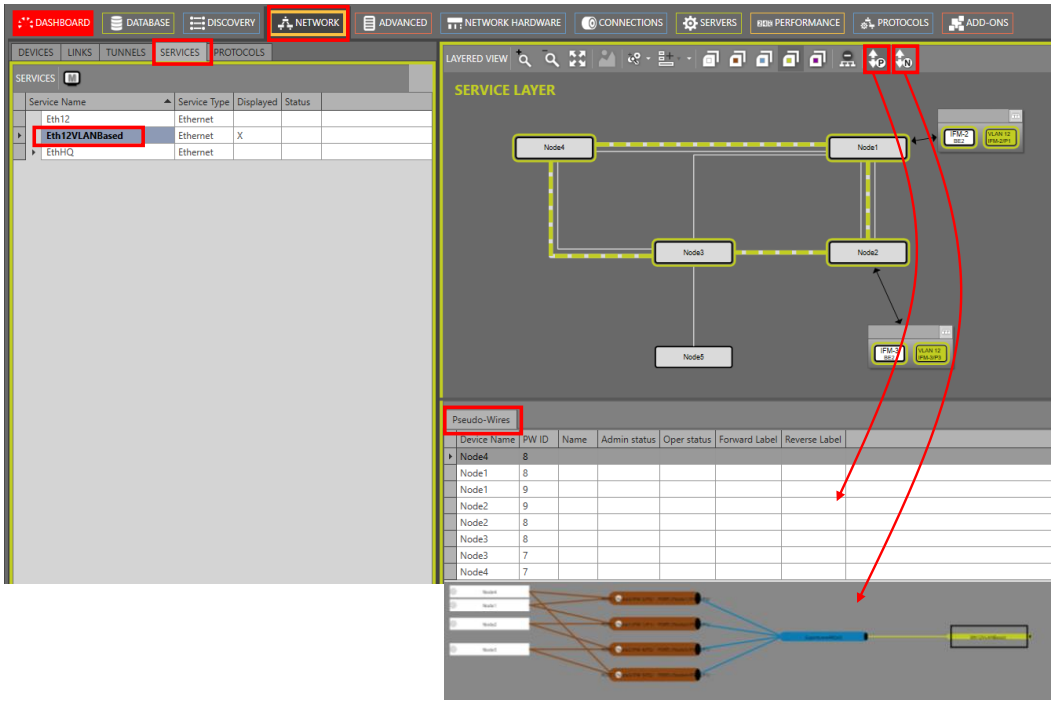

Figure 18 (Monitoring) Network Tile: Ethernet Service

2.6.4 Performance Counters

Performance counters can provide detailed statistics about the Dragon PTN network.

Ethernet port counters can be monitored via Dashboard → (Monitoring) Performance → Counter Control → Port Performance. QoS and HQoS can be monitored via QoS Performance. See figure and paragraphs below.

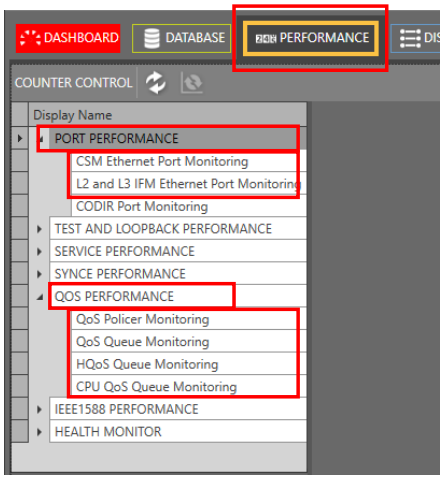

Figure 19 Performance Tab: Counter Control

a. Port Performance: CSM Ethernet Port Monitoring

Port counters for Ethernet IFMs (e.g. 4-GC-LW, …) can be found in 'CSM Ethernet Port Monitoring'. A detailed monitoring set-up description (adding counters to graphs etc…) and field explanation of both sections can be found in in Ref. [2Net] in Table 1.

b. Port Performance: L2 and L3 IFM Ethernet Port Monitoring

Port counters for L2/L3 IFMs (both front and back end ports) can be found in 'L2 and L3 IFM Ethernet Port Monitoring'. A detailed monitoring set-up description (adding counters to graphs etc…) and field explanation of both sections can be found in in Ref. [2Net] in Table 1.

c. QoS Performance Counters

See §3.5.

2.6.5 MAC Monitor

The MAC Monitor will show the MAC address table of the selected Node (=CSM) or L2/L3 IFM. This table includes all MAC addresses used on this device except for the MAC addresses that are used in a point-to-point tunnel. See §9.7 for more information.

2.6.6 HiProvision Add-on: Generic Reporting Engine

Service and port reporting information is available via the Reporting Engine Add-on, see Ref. [24] in Table 1.

3. TRAFFIC ENGINEERING

3.1 General

Ethernet traffic engineering is needed in a communication network to control the ethernet service level agreements on a network wide level regarding loss, delay, delay variation and bandwidth profile. It is an essential step to guarantee the performance of each individual ethernet service on the network.

A Dragon PTN network in combination with HiProvision offers an integrated traffic engineering solution. The traffic engineering algorithms run on the HiProvision server and calculate, based on the service parameters, a network wide configuration for each node. The result is programmed together with the other ethernet service parameters into the individual nodes when the ethernet service is loaded into the network.

Dragon PTN guarantees services on the network because it implements traffic engineering in a very strict manner. A Dragon PTN network cannot be oversubscribed. A Dragon PTN node uses the following three mechanisms to implement Ethernet traffic engineering:

- Classification;
- Policing and Shaping;
- Queueing and Scheduling.

The result of the traffic engineering algorithm is a set of individual settings for each node depending on the position in the network and service layout.

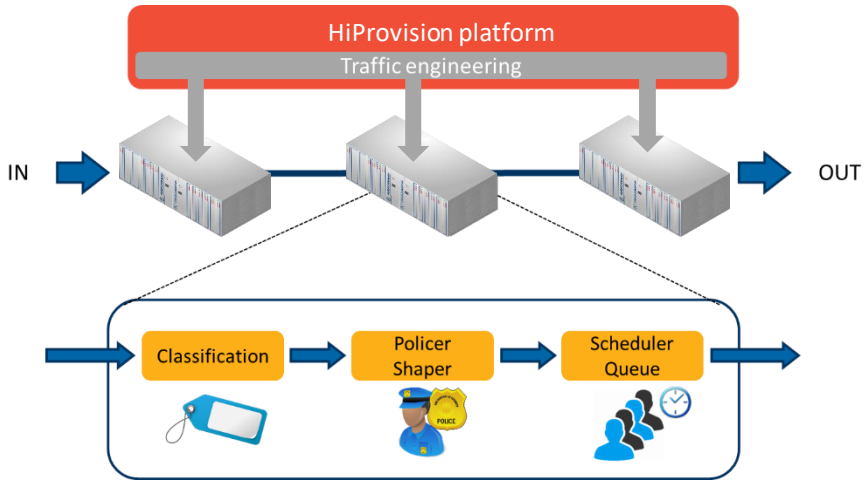

Figure 20 Dragon PTN and HiProvision: Integrated Ethernet Traffic Engineering

3.2 Classification

Classification is the method that maps the user data into the corresponding Ethernet service and on the network. Dragon PTN can classify incoming packets based on a certain port (port based services) or on a port/VLAN (VLAN based services).

In port based services, all packets received on a certain port go into the service whereas VLAN based services map all incoming data with a certain VLAN-ID into the service. All

incoming packets in the service are prioritized somehow, depending on the selected tunnel (HQoS on/off), service (service priority) or packet priority.

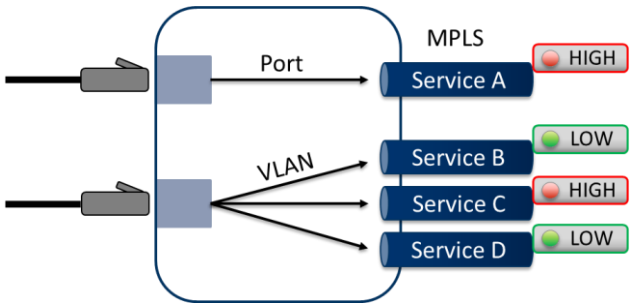

Figure 21 Dragon PTN Classification: Port Based / VLAN Based

3.3 Policing and Shaping

3.3.1 General

Policing and shaping is the method to check and adjust the incoming traffic to a preconfigured bandwidth profile and to remove any excess traffic if needed. Policing checks the bandwidth of the incoming traffic for excess traffic and a shaper will delay the excess traffic by using buffering. Both work in tandem to make sure that the dataflow of the service is not misbehaving on the network.

Because the HiProvision traffic engineering algorithm avoids over subscription of the bandwidth, the policer and shaper are matched. As a result the buffering should be minimal on the shaper. In Dragon PTN each service is configured with a guaranteed bandwidth. The bandwidth is checked when the traffic enters the network but also on each incoming MPLS interface. The last one protects the network against an overall flooding of the network in case a problem exists on the network.

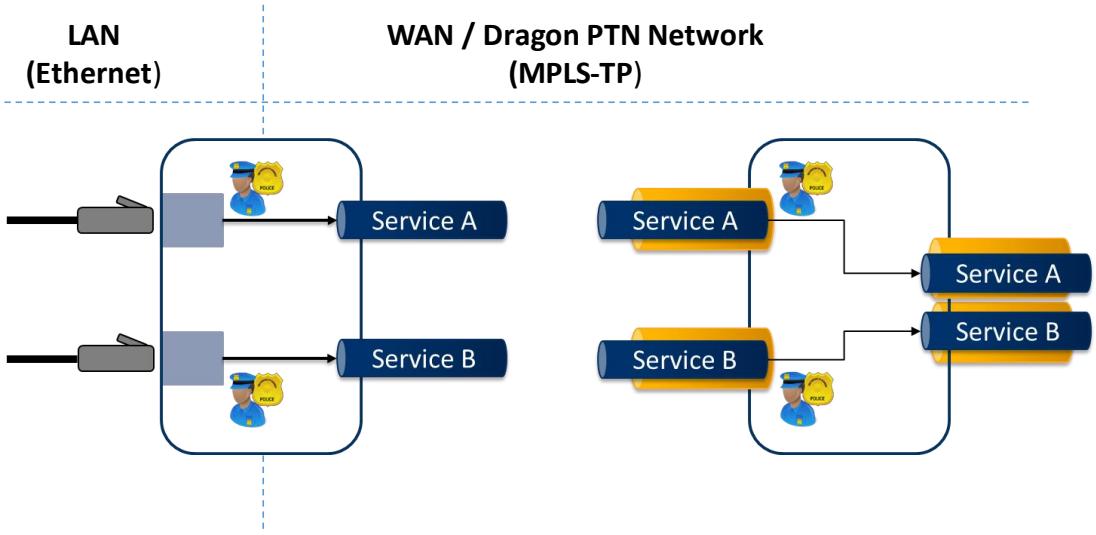

Figure 22 Dragon PTN Policing And Shaping

Because user data is mapped into MPLS-TP pseudowires and label switched paths, there is a difference between the useful bandwidth (Ethernet user traffic) and the gross bandwidth (user traffic mapped into MPLS-TP). HiProvision uses the information of the average packet size, entered by the user when creating the service, to calculate the allowed useful and gross bandwidth. The policers are configured accordingly. If the average packet size is not known HiProvision will suggest a safe value. The result is an exact configuration that offers a guaranteed transmission.

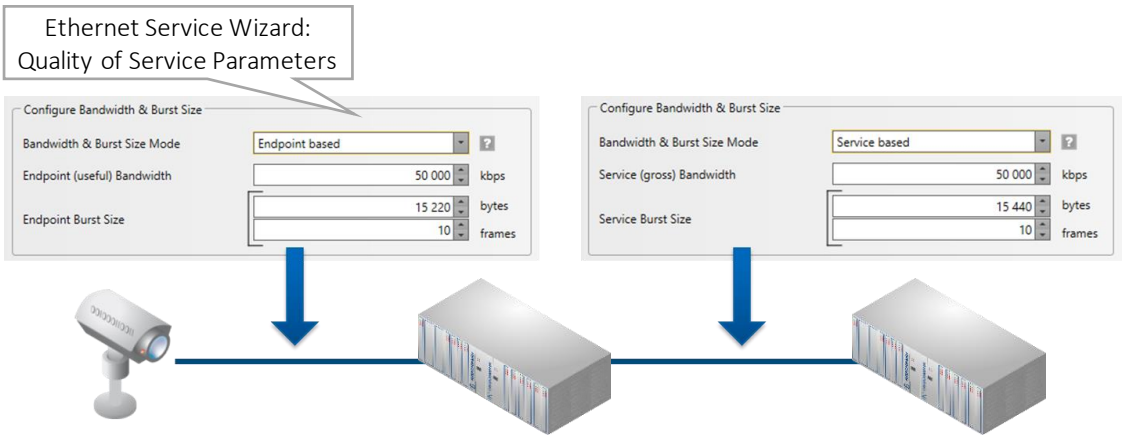

Figure 23 Bandwidth Profile Configured in the Ethernet Service Wizard

The result of the bandwidth provisioning in HiProvision is a configuration for LAN and WAN ports according to the calculated useful and gross bandwidth. This configuration is verified with the network configuration to check if the necessary capacity is available on the network.

This capacity is verified per link based on the available bandwidth on the link. In case of direct connections over fiber this is the link bandwidth reduced with the DCN bandwidth. In case Dragon PTN is transported over another network and the full link bandwidth is not available, the available bandwidth can be programmed in HiProvision. In that case the available bandwidth for services is the programmed bandwidth on the link reduced with the DCN bandwidth. Only if the necessary capacity is available on the network, the service can be loaded in the network.

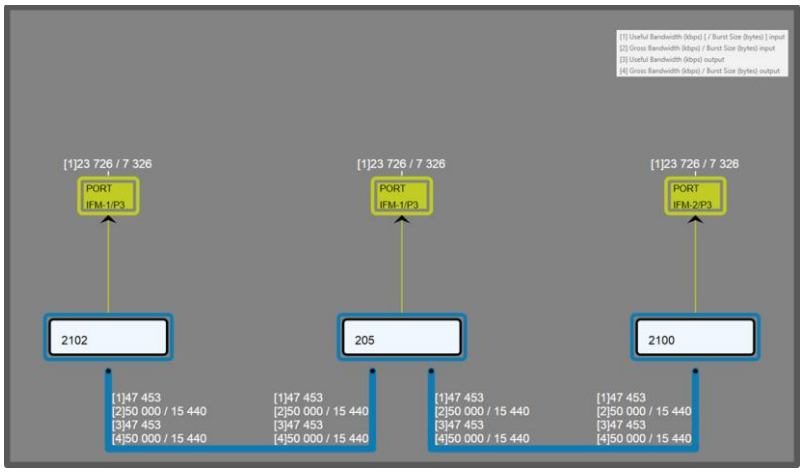

Figure 24 Resulting Bandwidth Profiling in HiProvision

A basic Policing and Shaping configuration can be done in the Ethernet Service Wizard page 'Quality of Service Parameters' below. The first section indicates value configurations on the LAN side while the second and third section refers to values used over the Dragon PTN network itself (=WAN side). The advised way to fill out this form is from top to bottom. Further details can be found in next paragraphs.

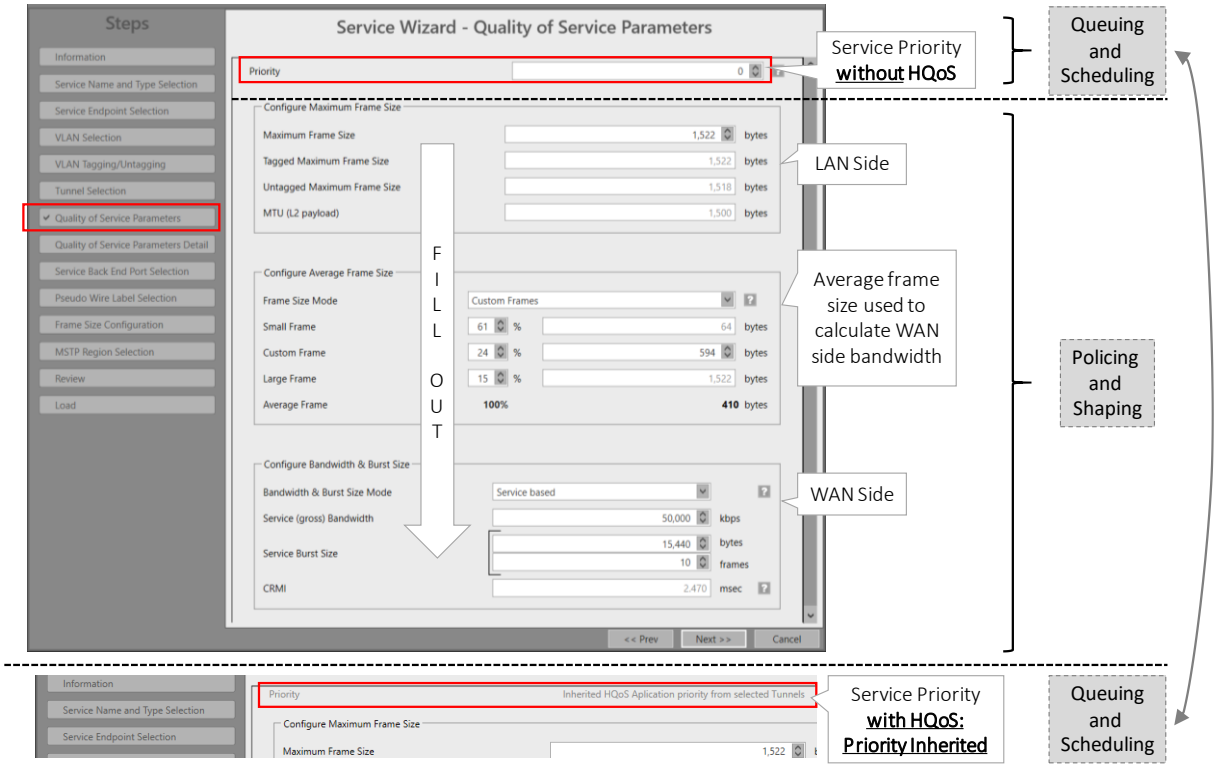

Figure 25 Wizard Page: Quality of Service Parameters

3.3.2 (Service) Bandwidth Already Configured on WAN Links

CAUTION: 'Bandwidth' in this paragraph always refers to the configured bandwidth!

a. General

If you want to configure new services, it is always nice to know how much bandwidth has been reserved (or configured) already on the link or how much is still available. This paragraph shows all the info you need to know about bandwidth usage within Dragon PTN, in order to configure it as efficiently as possible.

WAN links in the Dragon PTN network are Ethernet 1G, 10G or 40G links. They can carry 1, 10 or 40 Gbps in both directions on the link.

Max. Service Bandwidth = Max. WAN Link Bandwidth – Reserved Bandwidth

- Max. Service Bandwidth = Maximum available bandwidth on a link that a Dragon PTN user can configure in HiProvision when programming an Ethernet service. It also means that no other services are configured yet on this link.

- Max. WAN Link Bandwidth = Link Capacity:
  - The Link Capacity is by default the same as the original bandwidth of the selected link type (1 Gbps, 10 Gbps or 40 Gbps links). However the Link Capacity can be downscaled to a lower bandwidth if desired, see Link Capacity in Ref. [2Net] in Table 1.
- Reserved Bandwidth depends on:
  - DCN Channel Bandwidth: The DCN channel bandwidth is by default 40 Mbps but can be downscaled to 1.5 Mbps if desired. It is advised to keep 40 Mbps. See DCN Channel in Ref. [2Net] in Table 1.
  - Configured Average Frame Size: Small Frames (64 bytes) is more overhead than Large Frames (1522 bytes).
  - MACsec (1-10G-LW): A link with MACsec on has more overhead than a link with MACsec off;
  - PHY Mode setting (LAN/WAN) (1-10G-LW): WAN setting has more overhead;

The less reserved bandwidth, the more service bandwidth can be configured for applications.

Point-to-point service: a service bandwidth of ‘x’ Mbps on the link automatically results in a possible endpoint bandwidth of ‘y’ Mbps on the access port and vice versa.

- ‘x’ = service bandwidth including ‘L2 Ethernet Frame’ data and MPLS-TP overhead;
- ‘y’ = endpoint bandwidth including only ‘L2 Ethernet Frame’ data;
- ‘y’ is always less than ‘x’ with the maximum of ‘x’ depending on all the existing overhead described above;

By default, the service bandwidth is configured the same in both directions, but can be tuned individually if desired.

NOTE: The maximum bandwidth on the link is in both directions.

b. Connections Tab: Overview

Via the Connections tab, the bandwidth occupation (%, color) can be shown per link. Click a link in the Links table (see figure) to show the network drawing.

The link is encircled in the network drawing and a cross-section of that link with all its details is split out at the bottom section. The link colors indicate the bandwidth occupation severity, which can be adapted via the color slider.

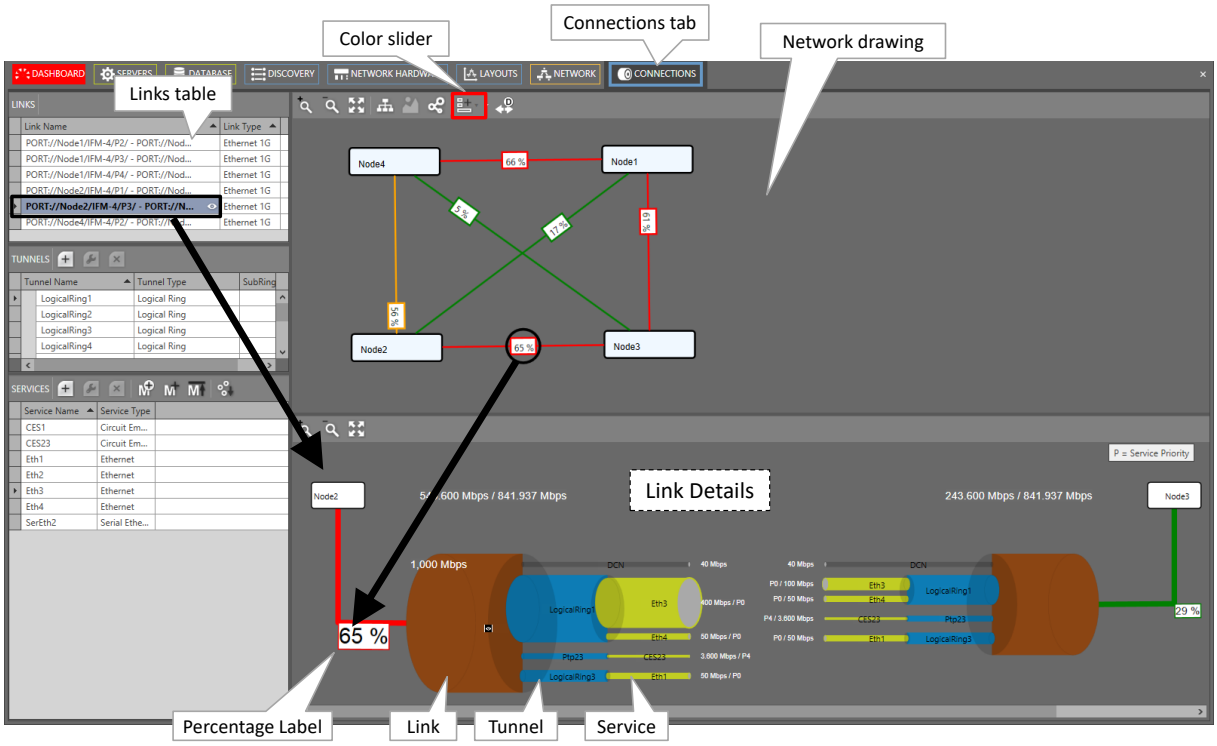

Figure 26 Connection Tab: Bandwidth Information

c. Connections Tab: Link Bandwidth Occupation: Percentage, Status Color

- Percentage label:
  - x%: used bandwidth, x percent of the available link bandwidth;
  - In the network drawing: If a percentage label hides another percentage label of an underlying link, the top label can be dragged aside after having it clicked first;
  - In the network drawing: clicking the button relayouts the percentage labels on the link;
- Status color = color indication of the bandwidth occupation percentage. The list below shows the colors for the default occupation ranges. The ranges can be modified via the color sliders:
  - green (0-30%): low;
  - orange (30-60%): medium;
  - red (60-80%): high;
  - dark red (80-100%): critical;

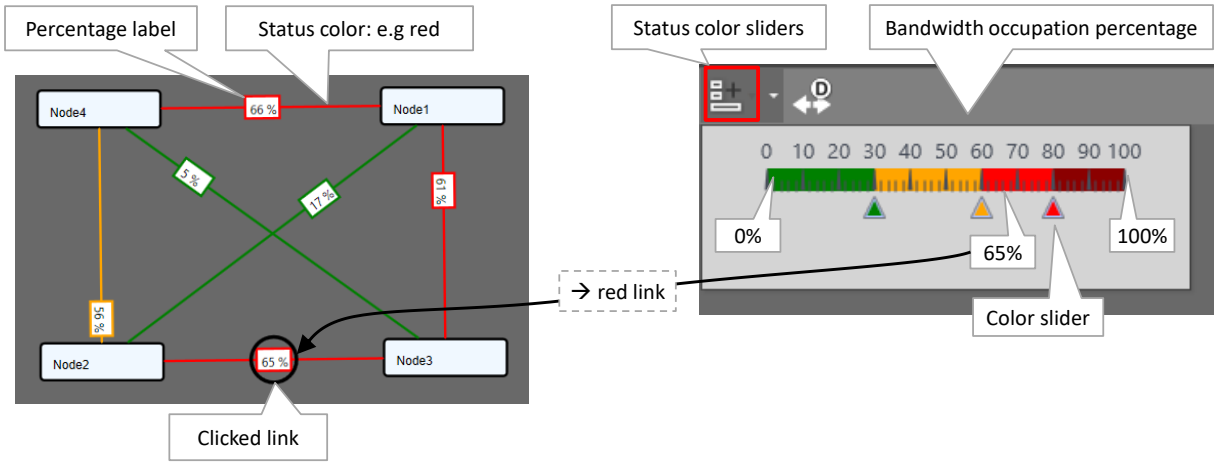

Figure 27 Bandwidth Percentage Label and Status Colors

d. Connections Tab: Link Details

In the figure below, the selected link shows all its tunnels including all its configured services. Each service also shows its bandwidth. The total bandwidth for the link in one direction from Node x → Node y, is the sum of the DCN bandwidth and all individual service bandwidths in that link in that direction, see figures below.

The 'Min. Total Link Bandwidth' including DCN: Indicates the minimum bandwidth that the configured services can address when consuming the bandwidth in the least efficient way (small packets, frame size = 64 bytes). As a result, when programming an additional service in a more efficient way (e.g. frame size = 500 bytes), this value will increase. The more efficient you use the bandwidth, the more total bandwidth can be consumed.

The bandwidth occupation for this link in this direction is 65% (= 543.6/841.937). This results in a red status color for the link according to the color slider settings. The used DCN bandwidth is also shown and depends on the link type, see Ref. [2Net] in Table 1.

NOTE: The greye (=zoom in) 'eye icon' becomes visible when hovering over the tunnel or the service pipes. Click this icon to zoom in. It also shows more detailed information in the right-hand side of the Connections Tab. After zooming in, the black (=zoom out) 'eye icon' becomes visible. Click this icon to zoom out again. Hovering over the labels in the figure below will zoom in the labels for a better view.

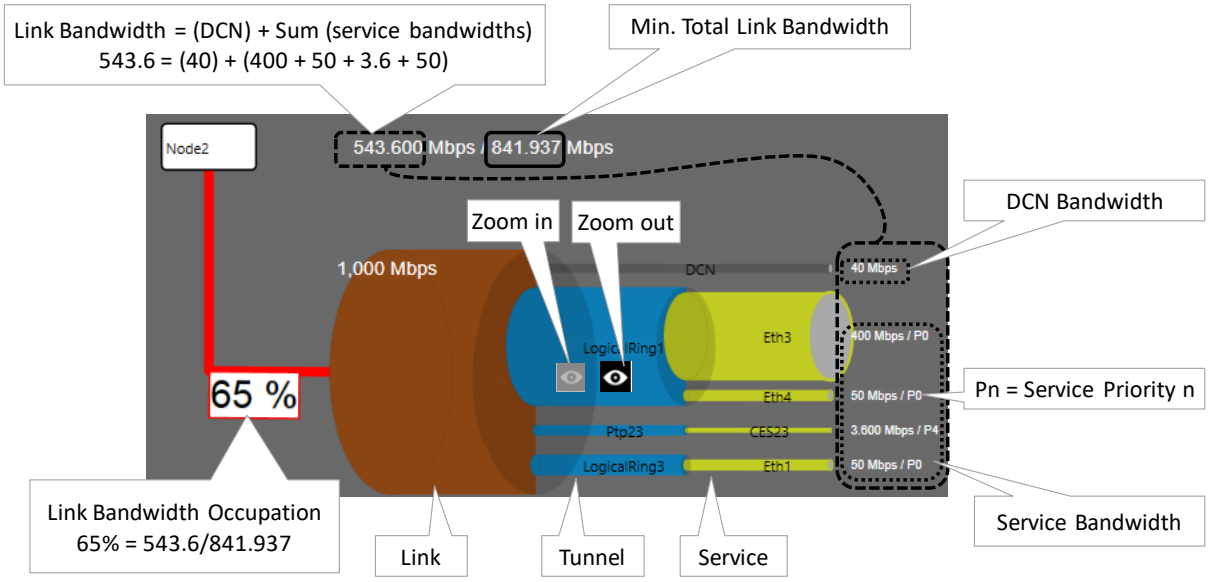

Figure 28 Link Details

e. Connections Tab: Two Bandwidth Directions in one Link

The bandwidths for a service is by default the same in both directions, but can be tuned differently if desired at service creation time. In the figure below, the thicker a pipe (link, tunnel or service), the more bandwidth it reflects. If the pipe of 'service x' is thicker in one direction than the other, it means that both directions have different bandwidths. The resulting link color is the severest status color of both directions (e.g. red is more severe than green). Also the highest percentage value of both directions will be taken.

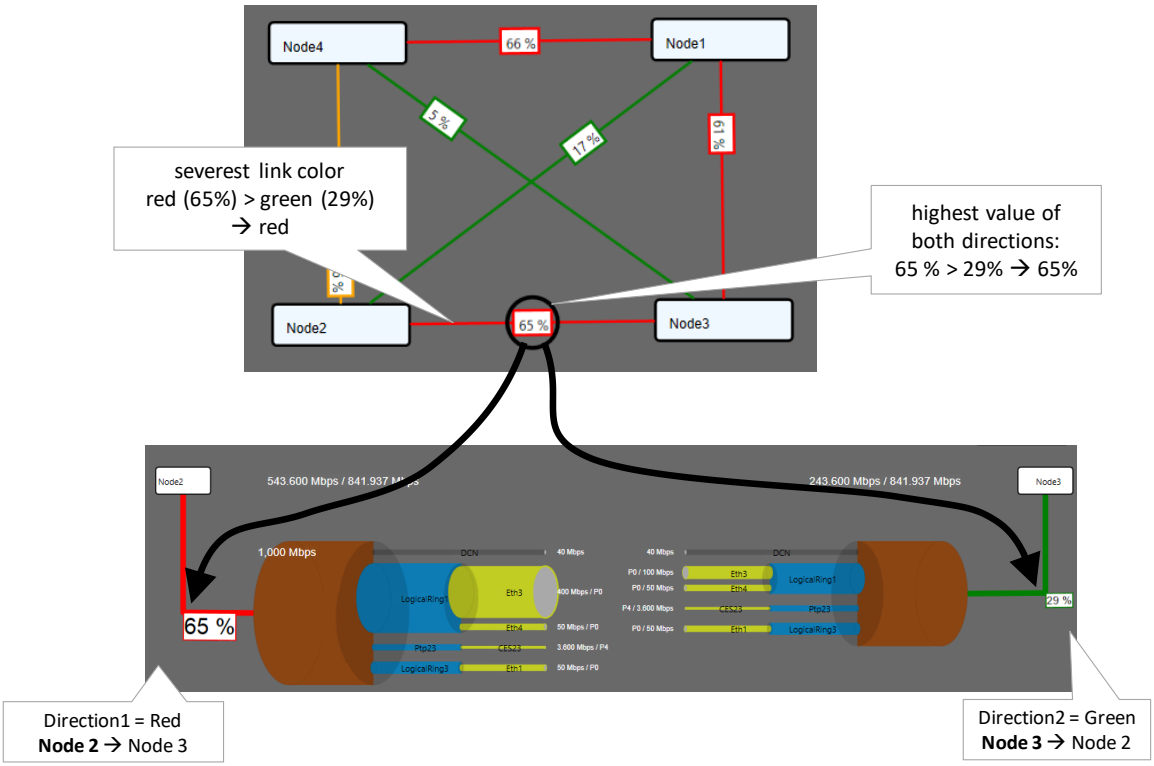

Figure 29 Highest Value and Severest Color

3.3.3 Bandwidth Optimization, Bandwidth Efficiency (=BWE) (LAN → WAN)

The BWE is the LAN to WAN bandwidth ratio. It compares the LAN bandwidth on a service port (see §3.3.4) to its required WAN or gross bandwidth to transport the service in a point-to-point service. The higher the BWE, the more efficient the WAN bandwidth is consumed.

BWE = LAN bandwidth / WAN bandwidth % = Useful Bandwidth / Gross Bandwidth %

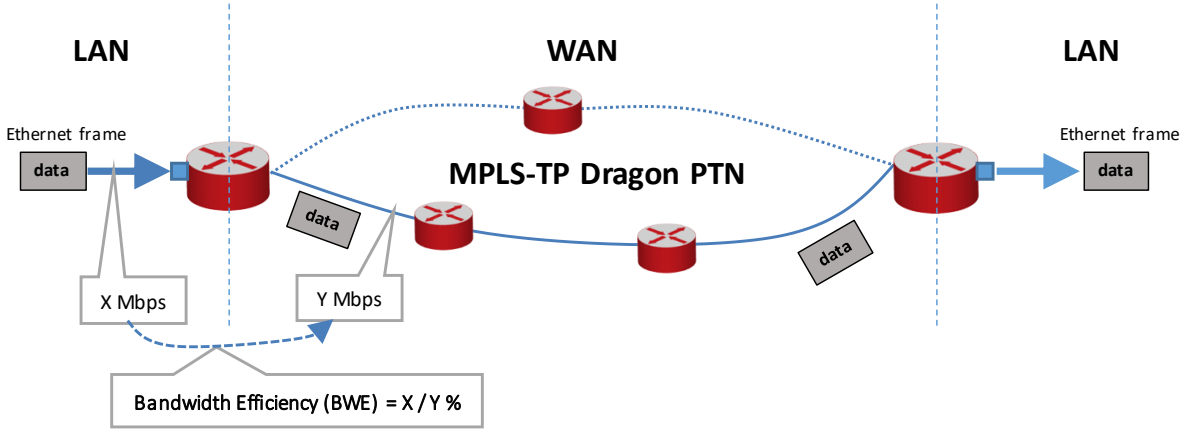

Figure 30 Bandwidth Efficiency

The bandwidth usage on the Dragon PTN network (=WAN) can be optimized via the frame size and/or the input bandwidth:

- Tuning the average frame size, see §a;
- Tuning the ports input bandwidth, see §b;
- Grouping VLAN based Ethernet services in a Bandwidth Optimization Group, see §4.8;

a. Bandwidth Optimization via Frame Size

How much bandwidth is required on the WAN side to transport a desired bandwidth on the LAN side? Due to extra MPLS-TP headers, the required WAN bandwidth is always more.

The calculated average frame size (see §3.3.5) through the configured service directly influences the BWE. The higher the frame size, the better or higher the BWE. A higher frame size automatically results in more payload bytes compared to overhead bytes, resulting in a better BWE. Examples:

- (small) frame size 64 bytes: BWE = 74 %;
- (custom) frame size 594 bytes: BWE = 94.9 %;
- (large) frame size 1522 bytes: BWE = 98.5 %;

HiProvision calculates and shows the average frame size based on the configured percentage of small, custom, large or a mix of frames within that service. These percentages can be configured in HiProvision, see figure below.

CAUTION:
When the real or measured average frame size is reasonably lower than the configured average frame size, extra delay and/or frame loss can occur! Following counters can be verified: 'Disc In Packets'/'Disc Out Packets' (→indicate frame loss) and 'Average Frame Size'. Counters can be found in 'Port Performance' in Ref. [2Net] in Table 1.
When the real or measured average frame size is reasonably higher than the configured average frame size, a lower BWE will be obtained but traffic will not be influenced.

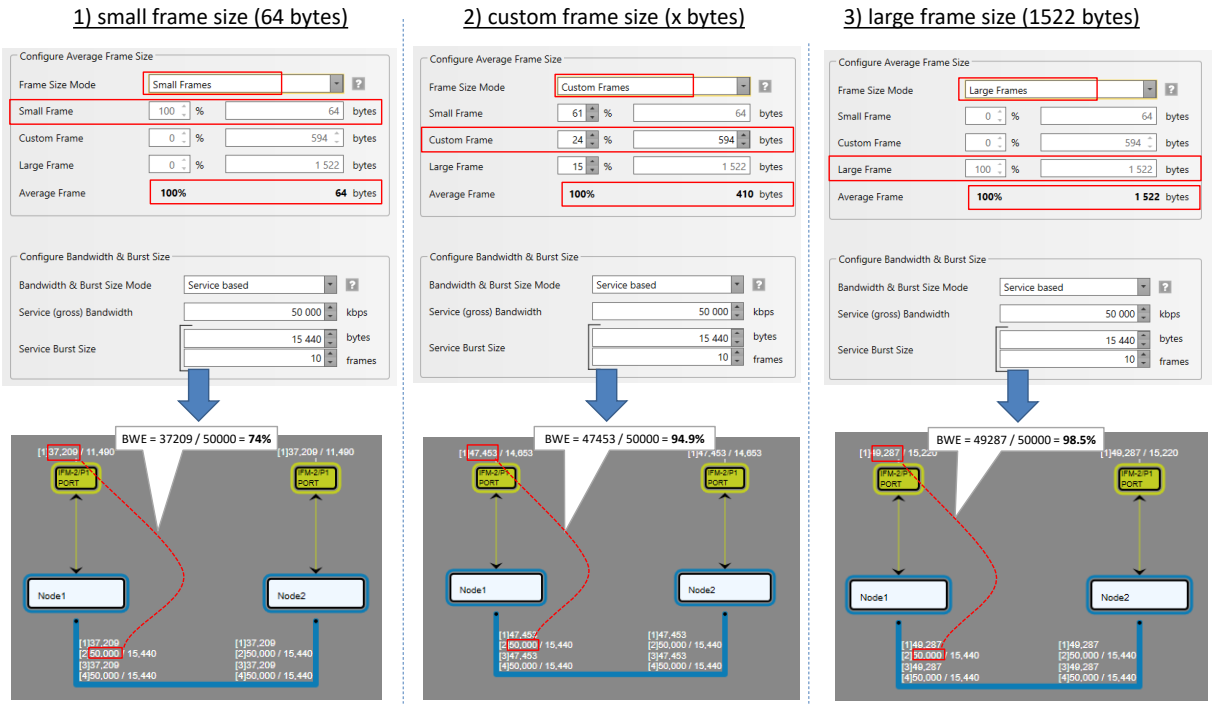

Figure 31 Bandwidth Efficiency Examples in HiProvision

b. Tuning the Ports Input Bandwidth

See §3.3.5.

3.3.4 Basic Configuration (Wizard: Quality of Service Parameters)

a. Configure Maximum Frame Size

- **Maximum Frame Size** (default = 1522 bytes, range [64..9238] bytes): The maximum frame size in bytes that is allowed at the LAN port(s) or LAN side of the service. This includes jumbo frames up to 9238 bytes.
- **Tagged Maximum Frame Size** (default = 1522 bytes, range [64..9238] bytes): Read-only field, is the same as the Maximum Frame Size field. It indicates the maximum length when the frame includes a VLAN tag field.
- **Untagged Maximum Frame Size** (default = 1518 bytes, range [64..9234] bytes): Read-only field, is the same as the Maximum Frame Size field minus 4 bytes, the length of VLAN tag field. It indicates the maximum length when the frame is untagged.

- **MTU (L2 payload)** (default = 1500 bytes, range [46..9216] bytes): Read-only field, indicates the net number of real data bytes, without headers.

b. Configure Average Frame Size

The better you know the traffic (and its frame sizes) in your network, the better you can tune the consumed bandwidth on the WAN side. The Average Frame Size indicates the Ethernet frame size = payload + Ethernet overhead. This parameter is used by HiProvision to tune the BWE (=Bandwidth Efficiency), see also §3.3.3.

- **Frame Size Mode**: if Configurable Average Frame Size = 'yes' in Table 4, the Frame Size Mode and the average frame size can be changed. if Configurable Average Frame Size = 'no', always 'Small frames' (=default) will be active;
  - Priority = 0: default Frame Size Mode = Custom frames;
  - Priority = 1: default Frame Size Mode = Small frames;
- **Small Frame, 100%**: HiProvision calculates the LAN to WAN bandwidth ratio as if the incoming LAN frame size is 64 bytes. These small frames always result in a congestion free flow through the MPLS-TP network but lead to a less efficient bandwidth usage. The bandwidth usage is less efficient because proportionally more header bytes are expected to be processed compared to the real payload data.
- **Custom Frame (=default)**: After selecting this value, the expected frame size percentages of small/custom/large frames on the LAN side can be changed. By default, these percentages are 61% small frames, 24% custom frames, 15% large frames. After configuring or modifying these percentages, Dragon PTN can tune the LAN to WAN bandwidth better resulting in a higher BWE. The Custom Frame size itself can also be configured. The average frame size indeed directly influences the BWE between the LAN and WAN. See §3.3.3 for more info.
- **Large Frame, 100%**: the most ideal situation, when all the LAN traffic has a frame size of the configured Maximum Frame Size bytes, the BWE will be the highest!
- **Average Frame**: is always 100% and indicates the configured Average Frame Size based on the previous settings;

CAUTION:
When the real or measured average frame size is reasonably lower than the configured average frame size, extra delay and/or frame loss can occur! Following counters can be verified: 'Disc In Packets'/'Disc Out Packets' (→indicate frame loss) and 'Average Frame Size'. Counters can be found in 'Port Performance' in Ref. [2Net] in Table 1.
When the real or measured average frame size is reasonably higher than the configured average frame size, a lower BWE will be obtained but traffic will not be influenced.

c. Configure Bandwidth & Burst Size

- **Bandwidth & Burst Size Mode = Service based (=default)**: The QoS parameters will be configured on the service tunnels. The configuration on the endpoints will be calculated by HiProvision based on the configured frame size and number of endpoints. See §3.3.5c;

- **Service (gross) Bandwidth (default = 50000 kbps)**: The maximum bandwidth in kbps that is allowed for this service on the link. This value includes 'L2 Ethernet frame' + 'MPLS-TP overhead';
- **Service Burst size**: Can be configured in bytes or frames:
  - **in bytes (default = 15440/15220 for Service Based/EndPoint Based)**: The maximum burst size in bytes that is allowed for this service on the link. This value includes 'L2 Ethernet frame' + 'MPLS-TP overhead';
  - **in frames (default = 10)**: The desired number of frames that will be buffered. Changing the number of frames will change the number of bytes and vice versa. The frames value is more indicative, while the resulting bytes value will be used for the real burst size calculation.

- **Bandwidth & Burst Size Mode = Endpoint based**: The QoS parameters will be configured on the endpoints. The configuration on the service tunnels will be calculated by HiProvision based on the configured frame size and the number of endpoints. See §3.3.5e.
  - **Endpoint (useful) Bandwidth**: The maximum bandwidth in kbps that the application is allowed to send on the service port (*). This value only includes 'L2 Ethernet frame';
  - **Endpoint Burst size**: Can be configured in bytes or frames:
    - **in bytes (default = 50000)**: The maximum burst size in bytes that the application is allowed to send on the service port. This value only includes 'L2 Ethernet frame';
    - **in frames (default = 10)**: The desired maximum number of frames that the application wants to send in one burst. Changing the number of frames will change the number of bytes and vice versa. The frames value is more indicative, while the resulting bytes value will be used for the real burst size calculation.

NOTE: (*) Service port: is a port that can be used as an endpoint in a service. It can be an IFM front port (e.g. port based Ethernet), a part of an IFM port (e.g. VLAN based Ethernet;

- CRMI (=Committed Rate Measurement Interval) (milliseconds): This parameter is some kind of delay indicator that shows how good the relationship is between your burst size and the bandwidth. It is the (Burst Size * 8)/Bandwidth. E.g, if your Burst Size is too high for the configured bandwidth, this CRMI will be too high also indicating too much delay. Too much delay could result in frame loss. For most applications, it is advised to keep CRMI between 0.025 and 10 ms to avoid Frame Delay (FD), Frame Delay Variation (FDV) and Frame Loss (FL). For high Variable BitRate (VBR) applications like video, a higher CRMI is needed and can be used.

CAUTION: All configured bandwidths in QoS configuration are L2 bandwidths!

3.3.5 Advanced Configuration (Wizard: Quality of Service Parameters Detail)

a. General

After configuring the QoS parameters in the wizard and clicking Next>>, the page with QoS Parameters Detail shows up. See figure below. This page by default shows a nice overview of the bandwidth and burst size usage of your configured service through the network.

Some values are configured, others are calculated by HiProvision based on the configured values. E.g. if the service values are configured (→ Bandwidth & Burst Size Mode = Service Based), the according service port values will be calculated automatically. Both configured and calculated values are visible in both the network drawing and tables in the Ports and LSPs tabs.

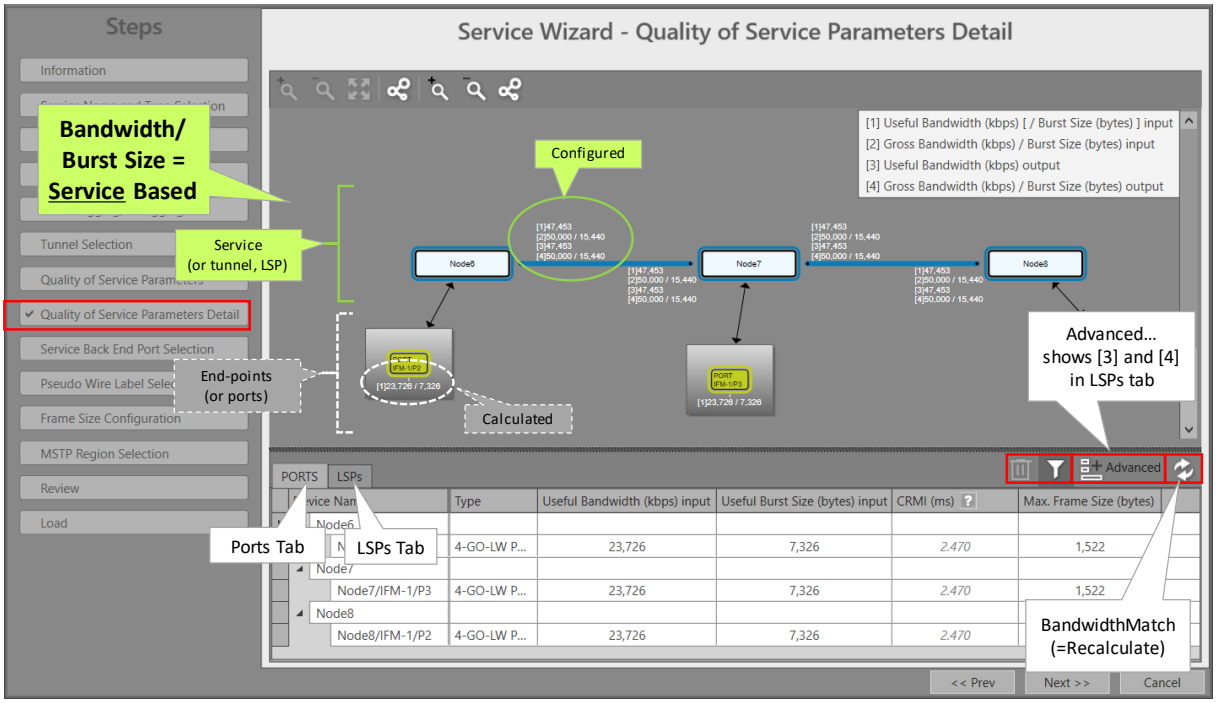

Figure 32 Bandwidth/Burst Size Parameters in Detail

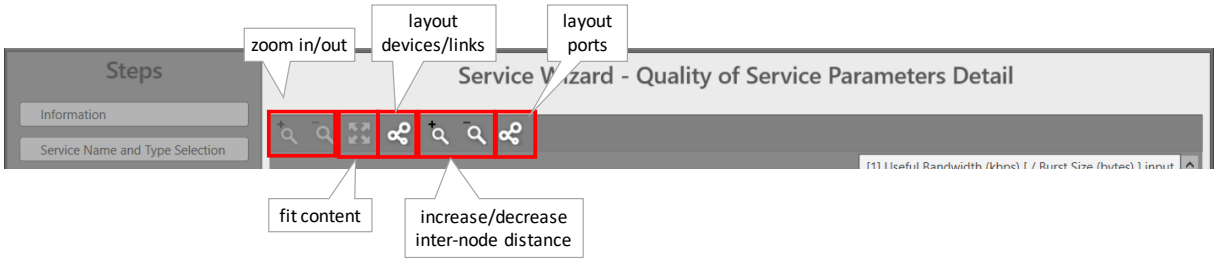

Figure 33 Grapic View Option Buttons

- Optional: Click cell to modify: bandwidth and burst size values in both the Ports (=LAN) and LSPs (=WAN) tab can be tuned manually and individually via clicking the cell and entering another value. Multiple edits/updates are also possible, see §b. The BandwidthMatch button can be used additionally, see below. Not clicking this button keeps all the individually tuned values.

CAUTION: Incorrectly tuned bandwidth or burst size values could result in extra delay and/or frame loss. Frame loss can be detected and verified via the 'Disc In Packets'/'Disc Out Packets' counters, see 'Port Performance' → 'CSM Ethernet Port Monitoring' in Ref. [2Net] in Table 1.

- Filter button : see §c.
- Clear Selection button : clears selected rows in the Ports/LSPs tab.
- Advanced button : clicking this button is only relevant in the LSPs tab and will additionally show the 'Gross Burst Size (bytes) Input', 'Gross Bandwidth (kbps) Output' and 'Gross Burst Size (bytes) Output' columns.
- BandwidthMatch button : Clicking this button makes bandwidth values in both the Ports and LSPs tab compatible with each other. It recalculates values and/or resets some other default values. Incompatible bandwidth values between these tabs could result in extra delay and/or packet loss. How the button acts depends on Endpoint/Service based.
  - Service Based: changed values in both the Ports and LSPs tab will be lost and reset with the values configured in the 'Quality of Service Parameters' page of the wizard.
  - Endpoint Based: changed values in the Ports tab will be kept, the values in the LSPs tab will be recalculated and changed according to the values in the Ports tab. In this way, it is easy to see how a bandwidth change on the LAN affects the bandwidths on the WAN.

b. Multiple Edit/Update Cell Values

It is possible to multiple edit/update cell values in the Ports and LSPs tab for easy and user friendly bandwidth assignments. Multiple updates are always done per column, not per row. There are two ways to mutiple update the table cells:

- Multiple update all cells in selected column → see steps below;
- Multiple update some selected cells in same column → see steps below;

- Steps: Multiple update all cells in selected column:

1. Click the column header cell of the cells that you want to update, to select the entire column;
2. The cell of the first row in this column turns into edit mode;
3. Update this cell via changing the drop-down selector or by just entering a numeric value;
4. Other selected grey cells in this column are updated automatically with the same new value;
5. See figure below;

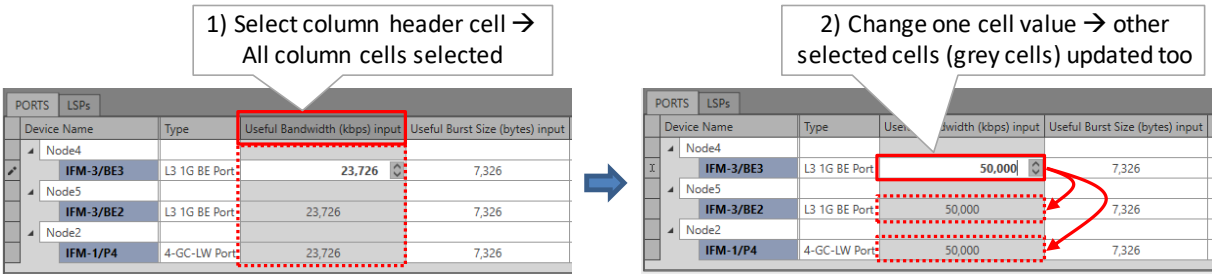

Figure 34 Multiple Update All Cells in Selected Column

- Steps: Multiple Update Some Selected Cells in Same Column:

1. Select the desired cells (in the same column) by clicking them while holding the CTRL or SHIFT key on your keyboard. Holding the SHIFT key selects ranges of cells while holding the CTRL key selects individual clicked cells;
2. The cell of the last selected row in this column turns into edit mode;
3. Update this cell via changing the drop-down selector or by just entering a numeric value;
4. Other selected grey cells in this column are updated automatically with the same new value;
5. See figure below;

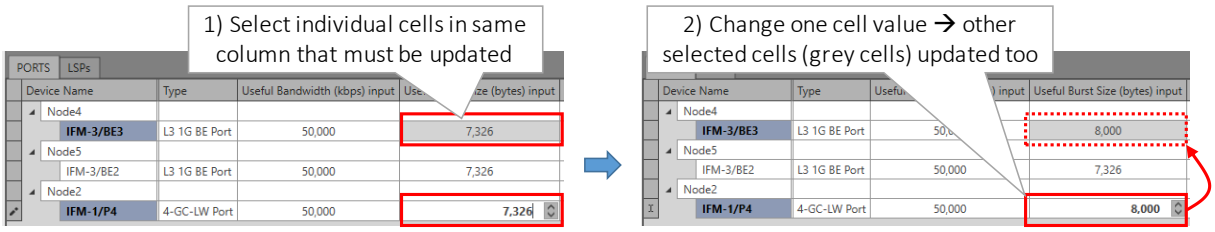

Figure 35 Multiple Update Some Selected Cells in Same Column

c. Filtering Tables

When a lot of nodes and/or links are in the network or in the tables, scrolling through the table records and comparing values of some records can sometimes be hard. Therefore to avoid too much scroll work, you can easily filtering out your needed Ports/LSPs to show less records.

- **Filtering Nodes/Ports**
  - Via network drawing: Just click one node or one port in the network drawing. The Ports tab becomes active, with the clicked node or port filtered out. Note: Multiple select is not possible via the network drawing.
  - Via table: Just click/select the port (device name column) in the Ports tab and click . Multiple records can be selected via holding the CTRL or SHIFT key and clicking/selecting ports followed by clicking .
  - If you made a wrong selection, just click the button to clear the selection.
  - Disable the filtering (and show all records) by just clicking the highlighted again.

- **Filtering Links (or LSPs)**
  - Via network drawing: Just click the link in the network drawing. The LSPs tab becomes active, with the clicked link filtered out. Note: Multiple select is not possible via the network drawing.
  - Via table: Just click/select the LSP (direction column) in the LSPs tab and click . Multiple records can be selected via holding the CTRL or SHIFT key and clicking/selecting LSPs followed by clicking .
  - If you made a wrong selection, just click the button to clear the selection.
  - Disable the filtering (and show all records) by just clicking the highlighted again.

d. Bandwidth/Burst Size: Service Based

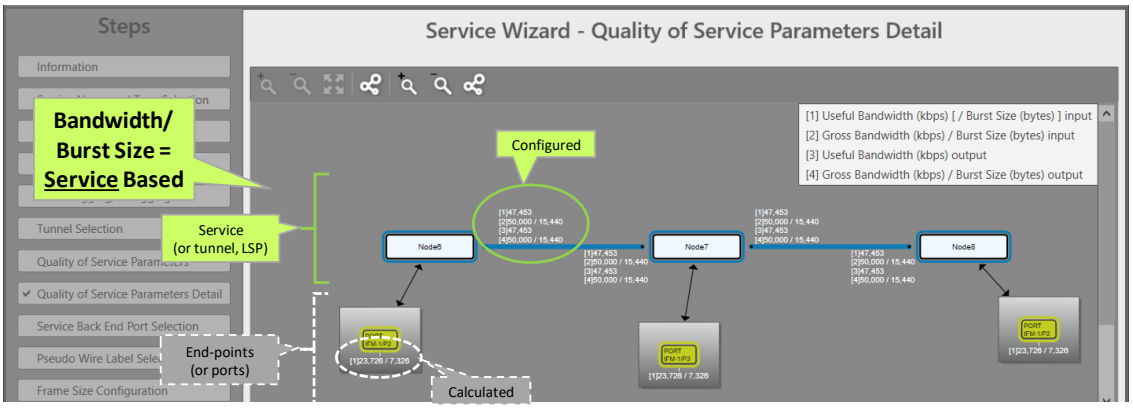

Figure 36 Bandwidth/Burst Size: Service Based

e. Bandwidth/Burst Size: Endpoint Based

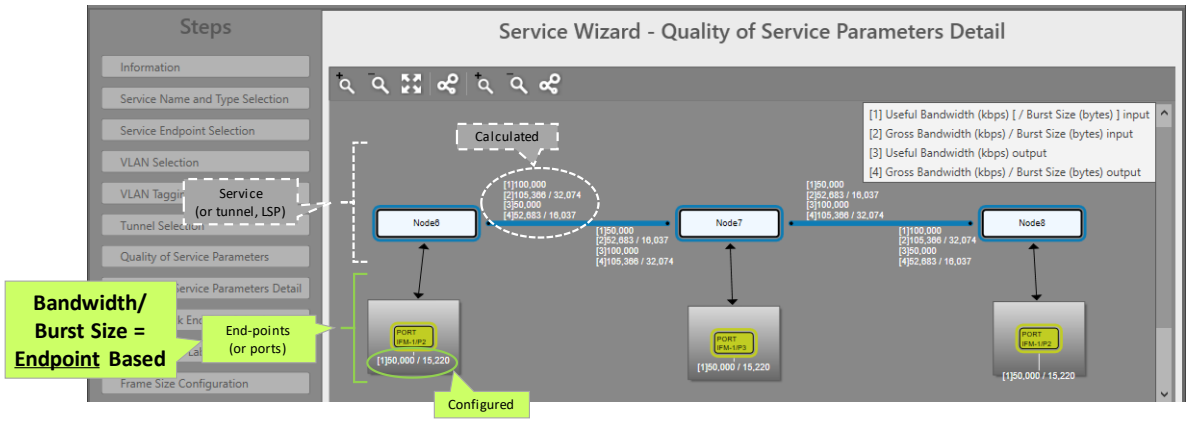

Figure 37 Bandwidth/Burst Size: Endpoint Based

f. Values on the Network Drawing

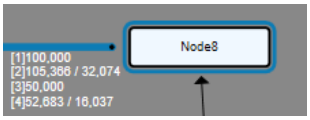

Figure 38 Bandwidth/Burst Size on WAN Side

- [1] = Node **input**: for this service, a useful bandwidth of 100000 kbps is available from link → node;
- [2] = Node **input**: for this service, a gross bandwidth of 105366 kbps and gross burst size of 32074 bytes is available from link → node;
- [3] = Node **output**: for this service, a useful bandwidth of 50000 kbps is available from node → link;
- [4] = Node **output**: for this service, a gross bandwidth of 52683 kbps and gross burst size of 16037 bytes is available from node→ link;

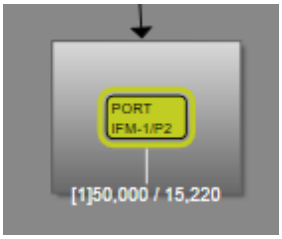

Figure 39 Bandwidth/Burst Size on LAN Side

- [1] = Node **input**: for this service, a useful bandwidth of 50000 kbps and a useful burst size of 15220 bytes is available from application → node;

3.3.6 Wizard: QoS Parameters Pop-Up

If you have changed the bandwidth input in the Ports tab in the 'Quality of Service Parameters Detail' page, and you pass again the 'Quality of Service Parameters' page (e.g. by going back in the Create wizard, or via a Modify wizard), it means that the bandwidth/burst size assignment must be recalculated. Click Yes (=advised) to let HiProvision recalculate and reconfigure the bandwidth and burst size settings over the resulting ports and tunnels. Click No (=expert), if you want to tune it all yourself, beyond HiProvision.

CAUTION: Clicking No and configuring wrong bandwidths or burst sizes, could cause traffic loss!

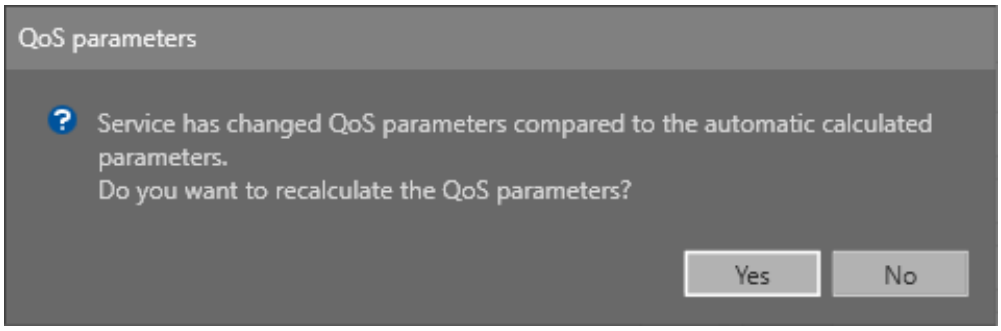

Figure 40 Modify Ethernet Service: QoS Parameters Recalculation

3.4 Queueing and Scheduling

3.4.1 General

Queueing and scheduling is the method to handle different priorities on the network. Based on the selected tunnel (HQoS on/off), service (service priority) or packet priority, the packet is put into a different queue. This queue is a temporary buffer where the packets of the same priority are waiting before they our outputted on the network. Which packet is send out first depends on the scheduler. The scheduler makes sure that packets are forwarded to the next node according to their priority. Scheduling is performed according to a specific scheduling algorithm. Dragon PTN uses **strict priority** scheduling to give absolute priority to critical services.

3.4.2 Difference QoS/HQoS

HQoS is a tunnel property that must be set at tunnel creation (see Ref. [2Net] in Table 1). If a tunnel is configured as an HQoS tunnel (Use HQoS = on), a more advanced and customized Queuing and Scheduling is possible compared to a basic QoS tunnel (Use HQoS = off). See also next paragraphs.

HQoS is supported for Ethernet ports that are directly connected via the backplane to the CSM. The HQoS processing itself occurs on the CSM towards these ports. The following ports can participate in HQoS:

- Front ports (LAN/WAN) of the Ethernet IFMs listed in support matrix in Ref. [2Net] in Table 1 (4-GC-LW, …);
- Back end ports (LAN) of the L2 IFMs;
- Back end ports (LAN) of the L3 IFMs;

3.4.3 Strict Priority

The strict priority method is used by the CSM and means that all Ethernet packets in the higher priority queues will be outputted first until the queue is empty, before the next lower priority queues are sequentially processed until they are empty and so on…. Because oversubscription is not allowed and prevented by HiProvision, the low priority queues and/or services have a guaranteed access on the network. The difference between a high and low priority packet is mainly resulting in delay variation. High priorities will go over the network with minimal queueing effects so the delay variation is very limited. Lower priority data might be queued because high priority packets are outputted first on a common link and therefore delay variation might be bigger. Spreading services over different queue sets is important to ensure service separation and limit influence between services.

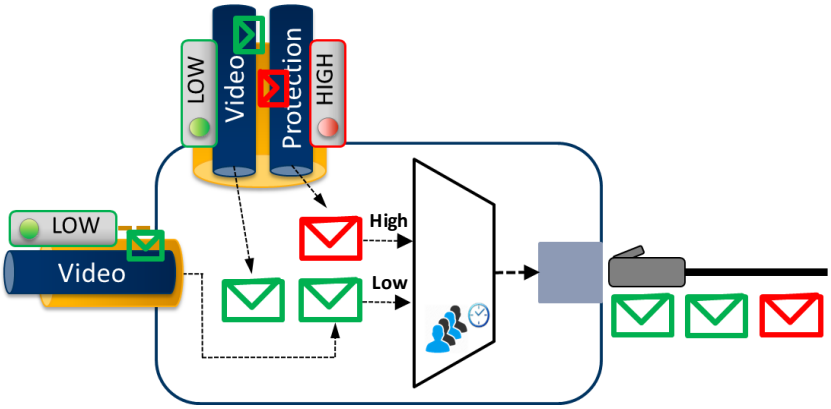

Figure 41 Scheduler Prioritizes Packets Based on Priority

3.4.4 Priority (Wizard: Quality of Service Parameters)

- **Ethernet Services with HQoS**

The service is configured in a HQoS tunnel. The service priority is inherited from the HQoS Application Priority (0 = default = lowest priority, …., 6 = highest priority) assigned to the tunnel at tunnel creation (tunnel creation: see Ref. [2Net] in Table 1).

- **Ethernet without HQoS**

The priority range [0…5] depends on the selected service. It configures the priority that will be assigned internally in the Dragon PTN node. 0 indicates the lowest priority, 5 the highest priority. In the Dragon PTN network, higher priority traffic will be processed before lower priority traffic so that high priority traffic will not be compromised. For example, priority 5 should be assigned to the most time-critical services. The table below indicates the possible priorities per service type. Whether the 'Average Frame Size' and 'Bandwidth Input' is configurable depends on the service and its priority.

Table 4 Service, Priority, Frame Size, Bandwidth Input

Service, Application	Max. Priority	Default Priority	Configurable Average Frame Size (*)	Configurable Bandwidth Input (**)
Ethernet: point-to-point	4	0	Yes, if priority <= 1	Yes, if priority <= 3
Ethernet: multipoint, ring	4	0	Yes, if priority <= 1	Yes, if priority <= 3
(*) Can be found in 'Quality of Service Parameters' window, see Figure 25. (**) Can be found in the 'Ports' tab in the 'Quality of Service Parameters Detail' window, see Figure 32.				

3.4.5 Priority Queue Selection

A Dragon PTN MPLS-TP network uses the parameters listed below to determine the priority or queue in which the incoming packet will be waiting before it is outputted on the network. The drawings below show all the possible parameter combinations and how they result in a queue (standard or extended) selection.

- HQoS Setting (On/Off) of the tunnel in which the service is programmed;
- HQoS Application Priority when HQoS = On in the selected tunnel;

- Service Priority in the Ethernet Service wizard;
- VLAN Priority (=L2) / DSCP(=L3) value in the incoming packet from the LAN side;

  NOTE: The VLAN Priority assigns a priority to outgoing packets containing the specified VLAN ID. This VLAN Priority is transferred in the 3-bits CoS field of an Ethernet packet.

- Port type: LAN/WAN;
- LER/LSR Node;
- MPLS TC (=Traffic Class) value in the MPLS (LSP) Header from the incoming WAN packets is used as priority, also known as E-LSP;

CAUTION: Standard queue sets have a higher priority than Extended queue sets!

For services mapped to the standard queue sets (=default behaviour) via the service priority, all traffic within the service is treated equal.

The extended queue sets (or application priorities) are available on WAN ports when Dragon PTN uses hierarchical QoS (= HQoS is enabled on the tunnel). Per application priority, configured in the tunnel, 1 queue set with 4 queues [0..3] is available. This allows to differentiate in 4 levels within a service (based on VLAN Prio/DSCP/MPLS TC value).

On LAN ports, Dragon PTN uses 8 standard queues [0..7] when HQoS = off (2 system queues [6,7], 6 user queues [0..5]), and 4 standard queues [0..3] when HQoS = on.

On WAN ports, Dragon PTN uses 8 standard queues [0..7] when HQoS = off and 7 extended queue sets [0..6], when HQoS = on, each set having 4 queues.

All scheduling is done on strict priority basis (SP).

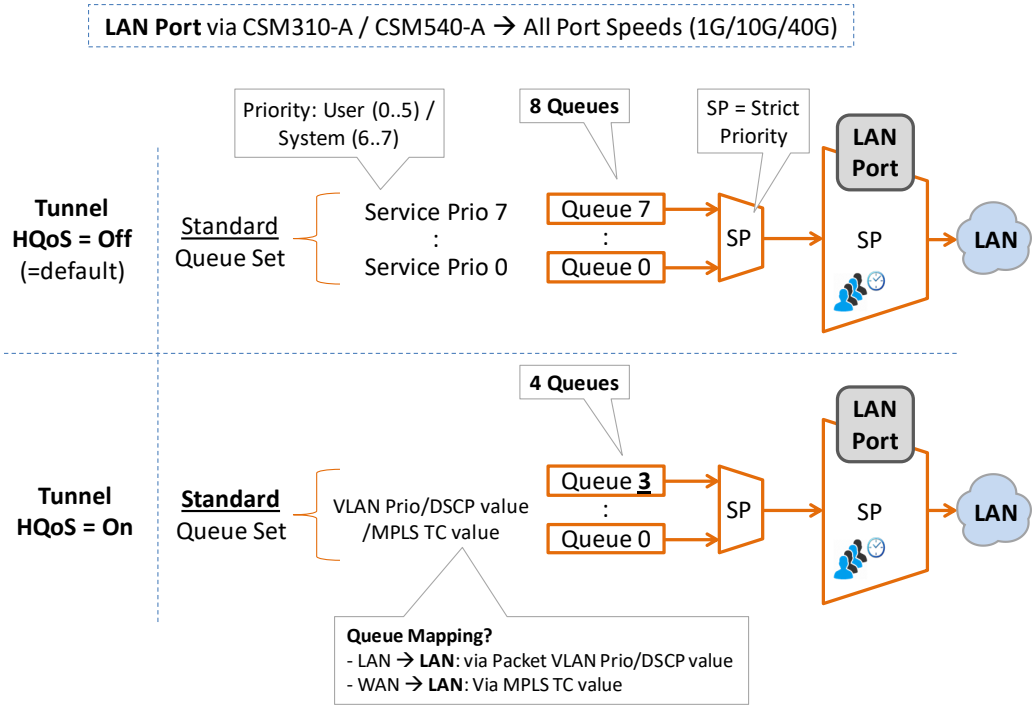

Figure 42 Priority Queue Selection and Scheduling on LAN Port

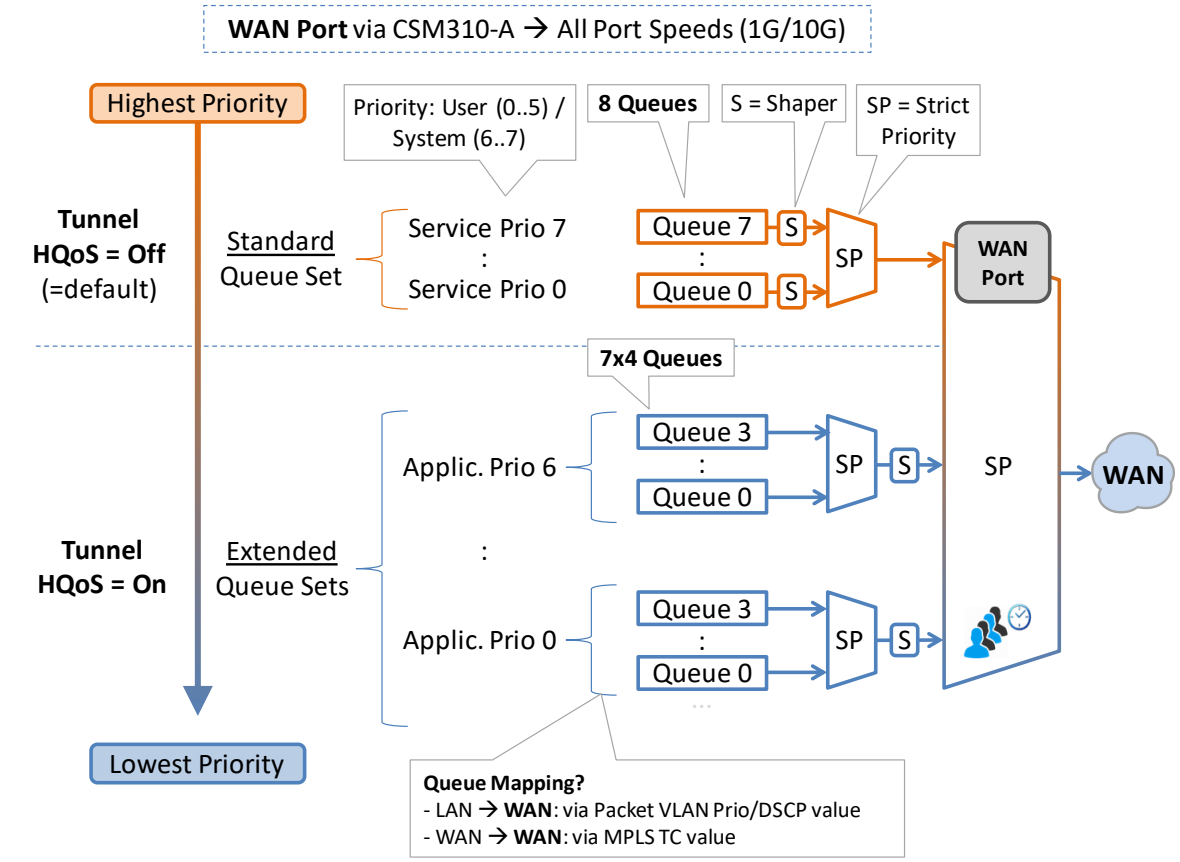

Figure 43 CSM310-A: Priority Queue Selection and Scheduling on WAN Port

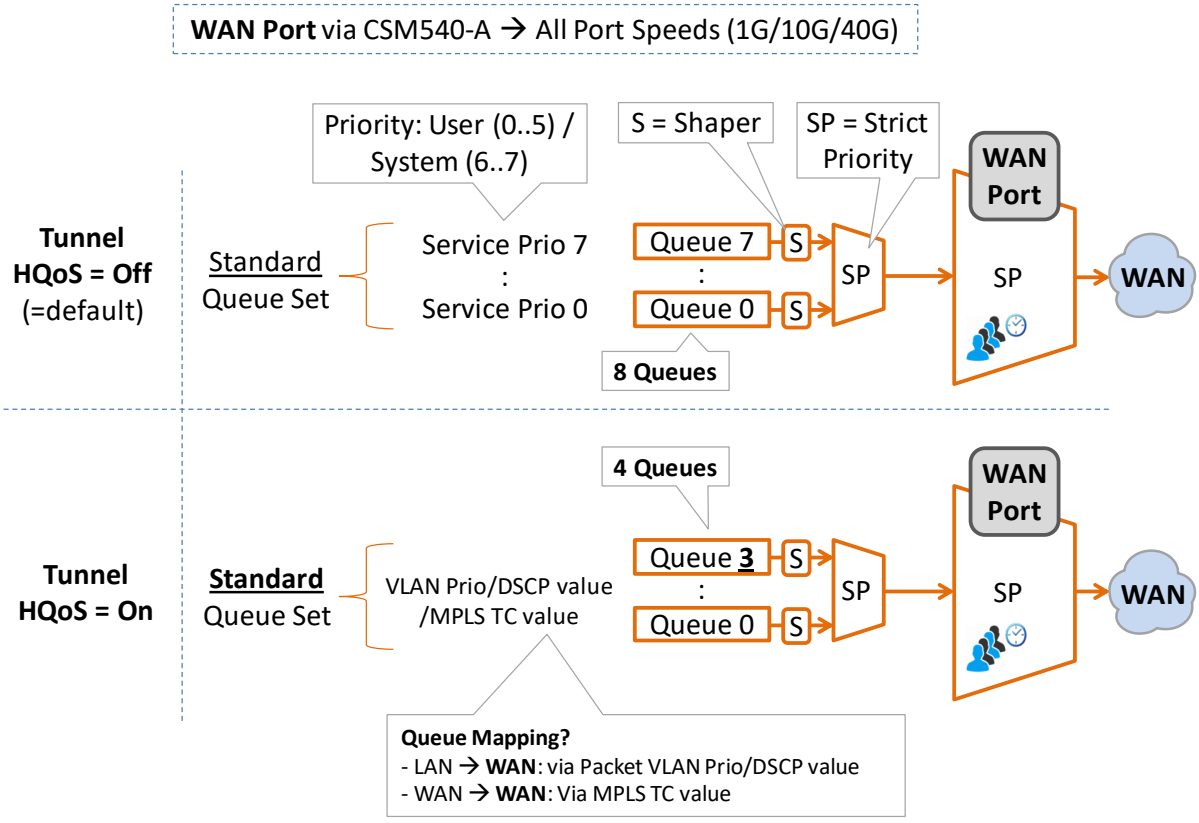

Figure 44 CSM540-A: Priority Queue Selection and Scheduling on WAN Port

a. HQoS = Off → Service Priority to Queue Mapping

When HQoS is Off, the mapping into the standard queue set is done based on the service priority (configured in §3.4.4). Priority 0 is the lowest priority and 7 is the highest priority. Priority 7 and 6 are used for network control and protection switching control (the main protocols to organize an MPLS-TP network). Priority 5 to 0 can be used for circuit emulation services. Priority 4 to 0 can be used for Ethernet services. Priority 4 is also used for the HiProvision management traffic and priority 2 is used in case new firmware is downloaded to the node. See also §3.4.4 for a list of priorities.

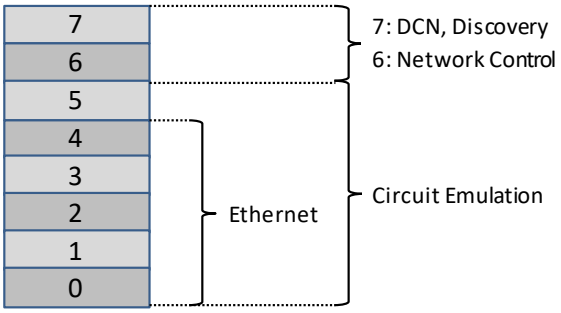

Figure 45 HQoS = Off → Service Priority Mapping

b. HQoS = On → VLAN Priority/DSCP/MPLS TC to Queue Mapping

When HQoS is On, the mapping into the queue is done based on VLAN Priority (= L2) or DSCP value (=L3) in the Ethernet Packet (for incoming LAN traffic) or based on the MPLS TC value (for incoming WAN traffic). For incoming LAN traffic, if both VLAN Priority and DSCP value are included in the incoming Ethernet packet, it can be configured which one has to be taken into account. Go to Network Hardware tile → Select Ethernet port → Specific section → QoS Classification. Select VLAN Priority (=default) or DSCP.

NOTE: For L2/L3 IFMs, the QoS Classification must be done on the back end port. For all other IFMs, the QoS Classification occurs on the front port.

- QoS Classification:
  - Incoming (=Ingress) LAN traffic:
    - VLAN Priority (=default) (=L2 classification):
      - Ethernet packet with VLAN priority value → map according Table 5;
      - Ethernet packet without VLAN priority value → map into queue 0;
    - DSCP (=L3 classification):
      - Ethernet packet with DSCP value → map according Table 5;
      - Ethernet packet without DSCP value → map according VLAN Priority (see previous VLAN Priority bullet);

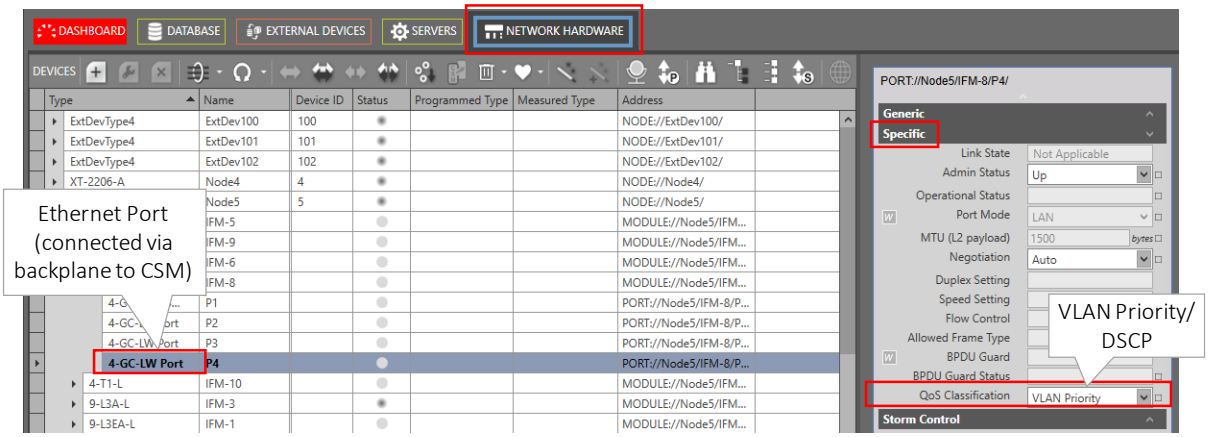

Figure 46 HQoS = On → QoS Classification: VLAN Priority/DSCP Setting

- Incoming (=Ingress) WAN traffic:
  - MPLS-TP packet with MPLS TC value → map according Table 5;

Table 5 HQoS = On: Resulting Application Priority Queue

Incoming from LAN		Incoming from WAN	→	Resulting Queue
VLAN Priority Value (=L2, in CoS field)	DSCP Value (=L3)	MPLS TC		
6-7	48-63	6-7	→	3
4-5	32-47	5-4	→	2
2-3	16-31	3-2	→	1
0-1 or untagged	0-15	1-0	→	0

3.4.6 MPLS TC Field Mapping

The MPLS TC field in WAN packets is a resulting priority of how the incoming packet from the LAN side (LER) or WAN side (LER/LSR) was prioritized inside the transmitting node, before it was sent to the WAN. Find below some figures and tables.

a. HQoS = Off

When HQoS is off, the MPLS TC field value in the WAN packets always equals the service priority value, and this for both LER and LSR nodes. The example below shows an Ethernet service with a normal (LER to LER) and a protection (LER to LER via LSR) path.

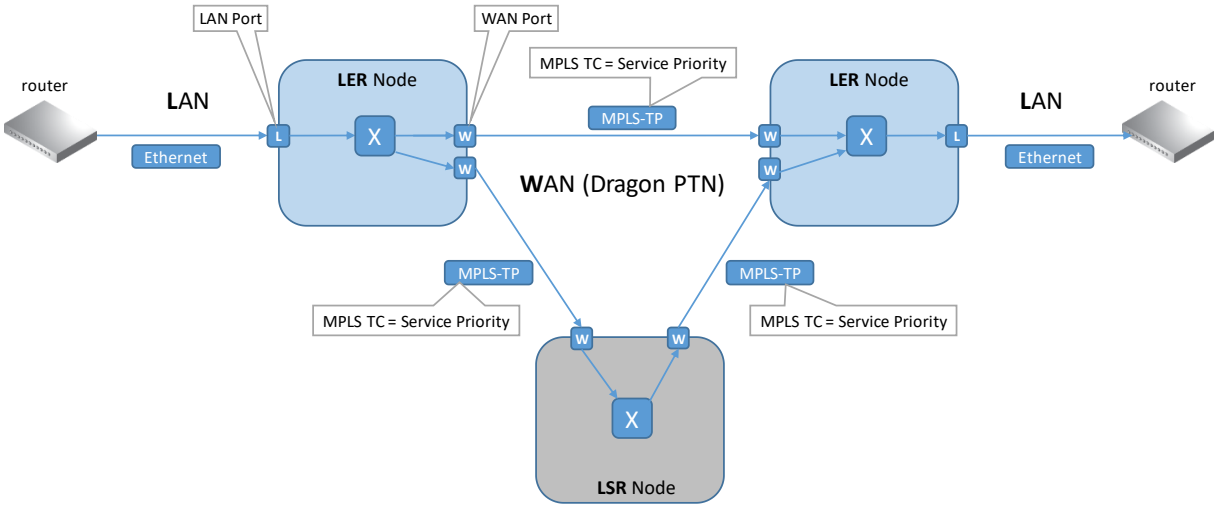

Figure 47 MPLS TC Mapping (HQoS = Off)

b. HQoS = On

When HQoS is on, the MPLS TC field value in the outgoing WAN packets depends on:

- (for LAN traffic via LER) the incoming VLAN Priority/DSCP field from the LAN packets;
- (for WAN traffic via LER/LSR) the incoming MPLS TC field from the WAN packets;

The figure in the example below shows an Ethernet service with a normal (LER to LER) and a protection (LER to LER via LSR) path.

Table 6 Outgoing MPLS TC Field Based on Incoming VLAN Priority/DSCP/MPLS TC

Incoming			→	Outgoing
LAN		WAN	→	WAN
VLAN Priority (=L2, in CoS field)	DSCP (=L3)	MPLS TC	→	MPLS TC
7	56-63	7	→	7
6	48-55	6	→	6
5	40-47	5	→	5
4	32-39	4	→	4
3	24-31	3	→	3
2	16-23	2	→	2
1	8-15	1	→	1
0 or untagged	0-7	0	→	0

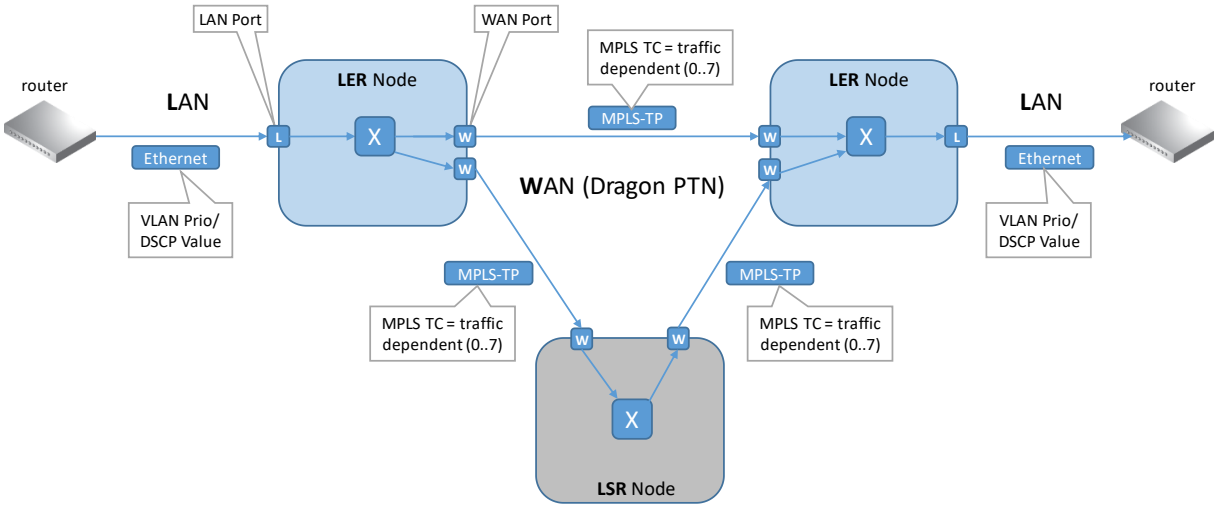

Figure 48 MPLS TC Mapping (HQoS = On)

3.5 Monitoring

3.5.1 General

Via HiProvision it is possible to display and monitor the performance counters of each service like average bandwidth, violated bytes, average frame size and so on. This allows the user to verify if the programmed service works according to specification and that resources on the network are effectively used. Next to this monitoring also the MPLS-TP OAM for loss and delay can be used to validate the performance of the service. More info on these counters in the paragraphs below.

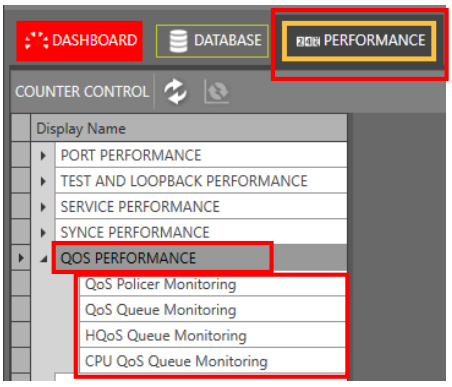

Figure 49 QoS Performance Counters

3.5.2 QoS Performance: QoS Policer Monitoring

The policer is a functionality on the CSM that measures the bandwidth profile (=bandwidth and burst size) of the incoming traffic on a LAN or WAN port. If these measurements are conform the configured bandwidth profile of that service, the packets are allowed and passed through (=conform packets, green packets). If not, the packets are dropped or violated (=violated packets, red packets). It also measures the 'Average Frame Size In' (not visible in the screenshot). This value can be used as input in the Average Package size settings in the service wizard QoS window to fine-tune the bandwidth efficiency, see §3.3.3.

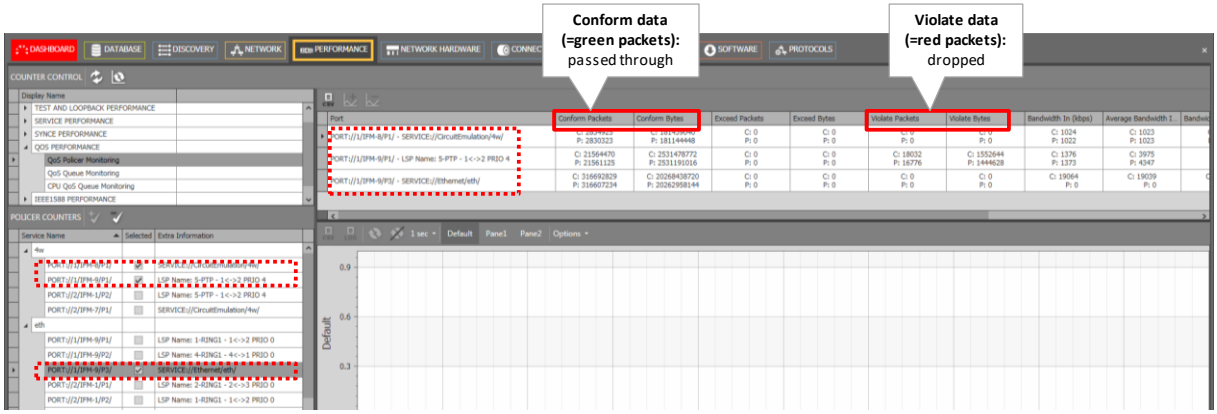

Figure 50 QoS Policer Monitoring

A detailed and similar monitoring set-up description (adding counters to graphs etc…) can be found in 'Port Performance' → 'CSM Ethernet Port Monitoring' in Ref. [2Net] in Table 1.

Table 7 QoS Policer Monitoring Fields

Field (*)	Values	Description	Curative Action
Port	value	Monitored port	
Conform Packets	packets	The number of packets within (or conform) the configured bandwidth profile (see description above in §3.5). None of these packets were dropped /discarded by the policer.	
Conform Bytes	bytes	Similar to 'Conform Packets' but with bytes instead of packets.	
Exceed Packets	packets	Not supported, always 0	
Exceed Bytes	bytes	Not supported, always 0	
Violate Packets	packets	The number of packets that mismatch or violate the configured bandwidth profile (see description above in §3.5). These packets were dropped by the policer.	Send less traffic or modify the configured bandwidth profile.
Violate Bytes	bytes	Similar to 'Violate Packets' but with bytes instead of packets.	Send less traffic or modify the configured bandwidth profile.
Bandwidth In (kbps)	kbps	The total incoming bandwidth between the current and the previous measurement: [(CurrentBytesIn - PreviousBytesIn)/1000/TimeInterval] kbps. Note: BytesIn = Total Incoming Bytes = Conform + Exceed + Violated	
Average Bandwidth In (kbps)	kbps	The average of the 5 latest 'Bandwidth In' measurements. Every (manual) refresh is a new measurement.	
Bandwidth Pass (kbps)	kbps	The resulting bandwidth that was OK and passed through the Policer. Example: if you have configured a service of 3 Mbps, and you receive 10 Mbps on the port, approximately 3 Mbps will be passed, the rest will be dropped.	Send less traffic or increase (or modify) the configured bandwidth if 'Bandwidth In' > 'Bandwidth Pass'. Verify 'Violate Bytes' counter.

Field (*)	Values	Description	Curative Action
Average Bandwidth Pass (kbps)	kbps	The average of the 5 latest 'Bandwidth Pass' measurements. Every (manual) refresh is a new measurement.	
Average Frame Size In (bytes)	bytes	The average frame size of all the frames (conform+exceed+violated) that are received on this port in the 5 latest measurements. Every (manual) refresh is a new measurement.	
Average Frame Size Pass (bytes)	bytes	The average frame size of frames that passed the policer in the 5 latest measurements. Every (manual) refresh is a new measurement.	
(*) Note: All fields are ingress fields **Note**: Click the Refresh button for the latest results; **Note**: Clear the counter values by clicking ; **Note**: 'C' value in cell = current value; 'P' value in cell = previous value;			

3.5.3 QoS Performance: QoS Queue Monitoring

This section shows how many packets go in/out the priority queue. E.g. if a service 'Video147' has been assigned priority 3, and port 7 is an endpoint of this service, packets received on port 7 and transmitted on the Dragon PTN network, will travel via priority queue 3.

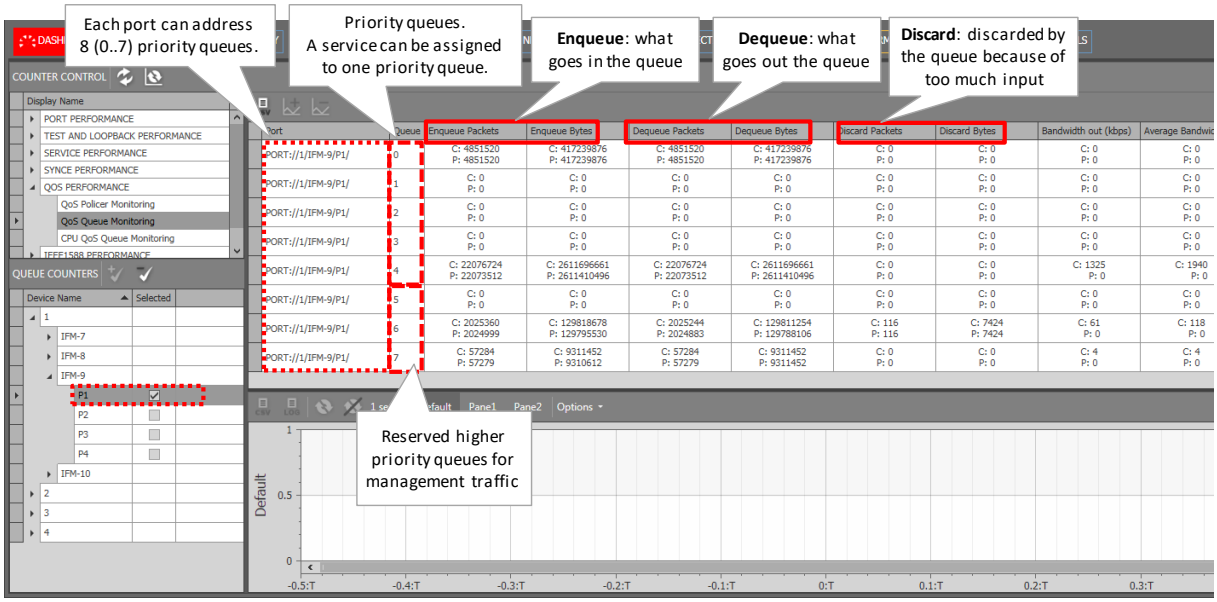

Figure 51 QoS Queue Monitoring

A detailed and similar monitoring set-up description (adding counters to graphs etc…) can be found in 'Port Performance' → 'CSM Ethernet Port Monitoring' in Ref. [2Net] in Table 1.

Table 8 QoS Queue Monitoring Fields

Field (*)	Values	Description	Curative Action
Port	value	Monitored port	
Queue	queue number	Each port has 8 priority queues [0..7], 0 = lowest priority, 7= highest priority. The higher priority queues 6 and 7 are reserved for management traffic (management protocol, discovery), other priorities can be used for services or user data, see also §3.4.4.	
Enqueue Packets	packets	Number of packets going in the queue, ready and waiting for transmittal	
Enqueue Bytes	bytes	Similar to 'Enqueue Packets' but with bytes instead of packets.	
Dequeue Packets	packets	Number of packets going out of the queue and transmitted via the port	
Dequeue Bytes	bytes	Similar to 'Dequeue Packets' but with bytes instead of packets.	
Discard Packets	packets	Number of packets discarded/ignored/dropped when arriving at the queue, only in some special cases. Example: the measured average frame size is reasonably lower than the configured average frame size. In normal circumstances, this counter should not increase	Verify your configured average frame size in the service wizard (QoS details)
Discard Bytes	bytes	Similar to 'Discard Packets' but with bytes instead of packets.	Verify your configured average frame size in the service wizard (QoS details)
Bandwidth Out (kbps)	kbps	The outgoing bandwidth between the current and the previous measurement: [(CurrentBytesOut - PreviousBytesOut)/1000/TimeInterval] kbps.	
Average Bandwidth Out (kbps)	kbps	The average of the 5 latest 'Bandwidth Out' measurements. Every (manual) refresh is a new measurement.	
Average Frame Size Out (bytes)	bytes	The average frame size of frames that are transmitted on this port in the 5 latest measurements. Every (manual) refresh is a new measurement.	
(*) Note: All fields are egress fields **Note**: Click the Refresh button for the latest results; **Note**: Clear the counter values by clicking  ; **Note**: 'C' value in cell = current value; 'P' value in cell = previous value;			

3.5.4 QoS Performance: HQoS Queue Monitoring

This section monitors the HQoS (=Hierarchical Quality of Service). It shows services that are programmed in an HQoS tunnel.

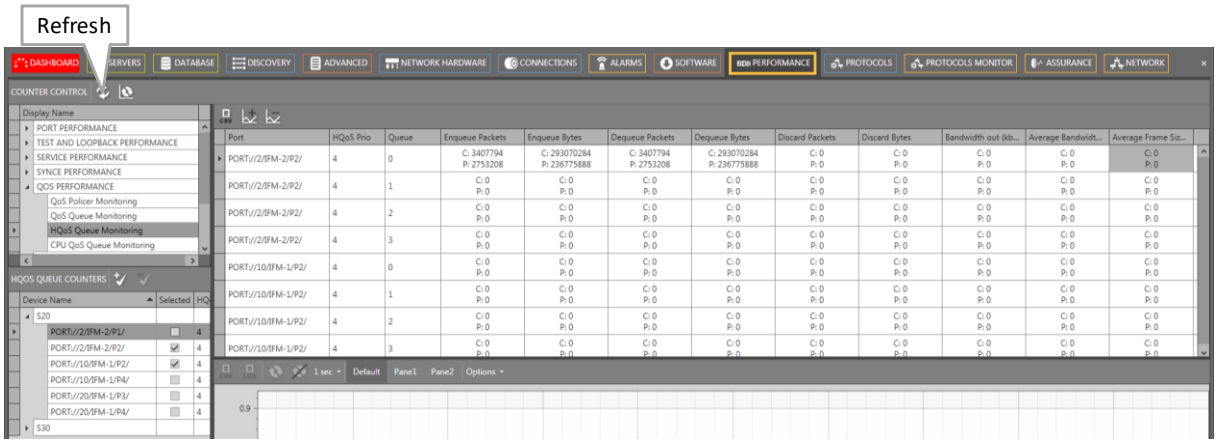

Figure 52 HQoS Queue Monitoring

Table 9 HQoS Queue Monitoring Fields

Field (*)	Values	Description	Curative Action
Port	value	Monitored port	
HQoS Prio	value	The application priority that is assigned to the tunnel, in which this service is programmed.	
Queue	queue number	Each port has 8 priority queues [0..7], 0 = lowest priority, 7= highest priority. The higher priority queues 6 and 7 are reserved for management traffic (management protocol, discovery), other priorities can be used for services or user data, see also §3.4.4.	
Other fields: Similar to fields in Table 8.			
(*) Note: All fields are egress fields **Note**: Click the Refresh button for the latest results; **Note**: Clear the counter values by clicking ; **Note**: 'C' value in cell = current value; 'P' value in cell = previous value;			

3.5.5 QoS Performance: CPU QoS Queue Monitoring

For Hirschmann service personnel only, for troubleshooting purposes!

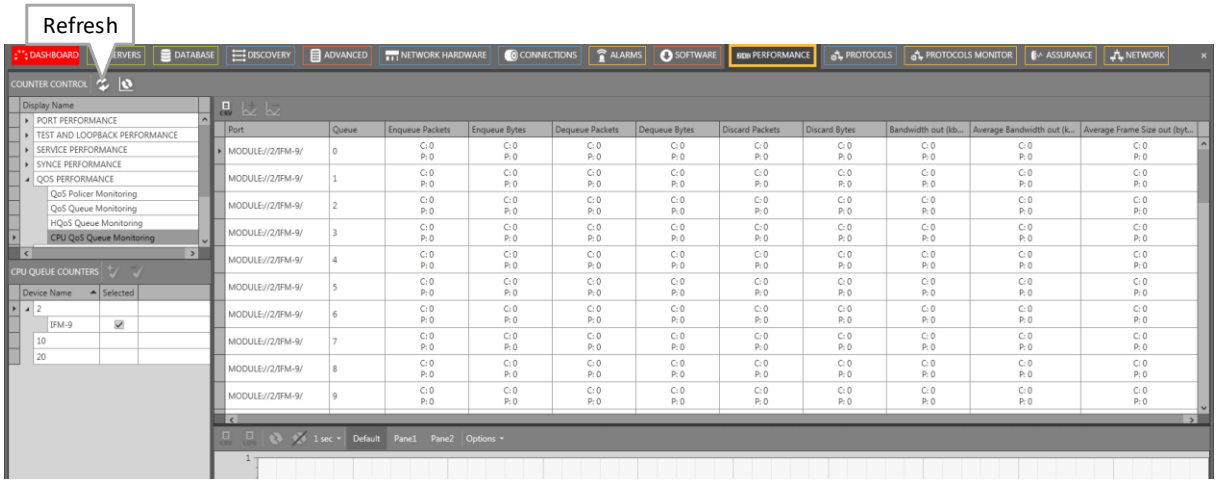

Figure 53 CPU QoS Monitoring

The field descriptions are similar to the fields described in Table 8.

4. ETHERNET SERVICES ON L2/L3 IFMS

4.1 General

L2/L3 IFMs (see support matrix in Ref. [2Net] in Table 1) are advanced IFMs that require some extra attention when programming them in Ethernet services:

- Service Types on L2/L3 IFM: see §4.2:
  - Port Based (=Mixed VLAN);
  - VLAN Based:
    - Single VLAN
      - Bandwidth Optimization Group, see §4.8;
      - Local Service, see §4.3;
    - Multi VLAN via QinQ;
- VRF Ports (only on L3 IFM), see §4.4;
- Back End Ports (BEn), see §4.5;
- L2VPN, see §4.6;
- L3VPN, see §4.7;

4.2 Service Types on L2/L3 IFMs

4.2.1 General

Some definitions that are used further on:

- Back End Port (BE): the backside port of the L2/L3 IFM that connects to the CSM via the node backplane;
- Back End Link: link between Back End Port and CSM;
- VFI: Virtual Forwarding Instance on the CSM. It is a virtual switch instance that learns MAC addresses and forwards packets based on source/destination MAC addresses;

The following service types can be used (see also overview in example figure below):

- **Port Based service** (=Mixed VLAN service):
  - On Ethernet IFMs (4-GC-LW,...): is VLAN unaware, transports frames of any VLAN ID;
  - On L2/L3 IFMs: is a hybrid or mixed VLAN service that partially acts as a pure Port based on the WAN side (VLAN unaware) and partially as a VLAN based (single VLAN) service on the LAN side, see picture below. The single VLAN services will be embedded (= child) in the port based service (=parent). As a result, the Quality of service, priority and bandwidth is configured on port based level and is the same for its childs. The available bandwidth will be divided amongst its child services.
  - One service consumes an entire Back End port to the CSM!
  - Detailed example in §4.9.

- **VLAN Based: Single VLAN service**: transports frames of a single VLAN ID through the Dragon PTN network. Multiple of these services can be configured per port, either front port or back end port;
  - Normal service (=not in a Bandwidth Optimization Group, not Local): A single VLAN service that has its own individual bandwidth, QoS, priority etc… and that goes through the Dragon PTN network;
  - Bandwidth Optimization Group (services grouped together for optimized bandwidth consumption): see §4.8;
  - Local Service: is a single VLAN based service between only LAN front ports on L2/L3 IFMs. See also §4.3 for more info.

- **VLAN Based: Multi VLAN service (QinQ)**:
  - With QinQ, a VLAN based service can carry multiple VLANs instead of just one. QinQ is a feature that operates at the back end ports of the L2/L3 IFM. For incoming traffic (LAN → WAN), this feature adds an outer VLAN (=QinQ VLAN, with EtherType 0x8100) around the existing VLANs resulting in double VLAN tagged Ethernet packets. For outgoing traffic (WAN → LAN), the QinQ VLAN is removed. Each back end port on the L2/L3 IFM can carry multiple VLAN based services. Ethernet IFMs (4-GC-LW,...) do not support QinQ. A QinQ VLAN ID on Ethernet IFMs will be handled as a normal VLAN ID. A switch that supports QinQ should be connected to these Ethernet IFM ports to process double VLAN tagged packets;
  - Detailed example in §4.9.

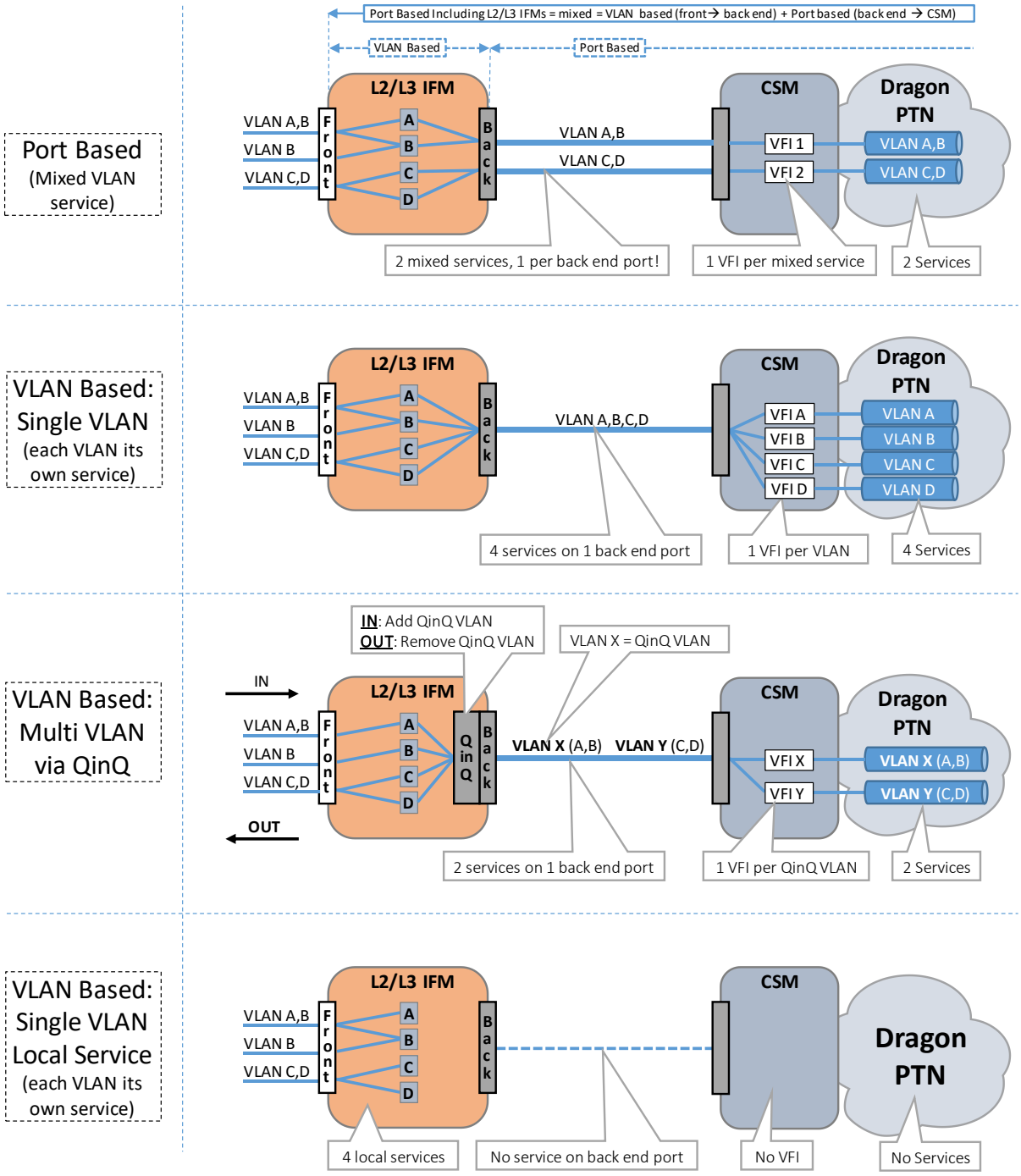

Figure 54 Ethernet Services Examples Overview in L2/L3 IFMs

4.2.2 When to Use Which Service Type?

Always try to use a single or multi VLAN Based service whenever possible. Most (if not all) complex types of VLAN use cases can be configured through a combination of VLAN services. However, there is a need to be able to 'bundle' several of these services port based into one logical instance. The main use case is where MSTP is needed over the Dragon PTN backbone. In this case, a port based service must be used. A port based service on an L2/L3 IFM will consume an entire Back End port, leaving other services one back end port less to use.

MSTP Use case:

- untagged BPDUs need to be sent over the back end links;
- these BPDUs need to travel the same path as the actual data traffic;

Table 10 Properties: When To Use Which Service Type in L2/L3 IFMs

Service Type	When to Use	Pros	Cons
What kind of service types you should use, strongly depends on the network design and the requirements. Below, you can find some guidelines for each service type.			
Port Based (=Mixed Service)	- when MSTP is required network wide - when you want to transport all data (tagged, untagged, mgt traffic, …) on a port in one service, QoS diversification is less important	Only one VFI per service used in the CSM	One back end port per service required. Each L2/L3 IFMs has 4 or 5 back end ports. Configuring 4 or 5 Port based services on a L2/L3 IFM means that no other service is possible on that L2/L3 IFM.
VLAN Based, Single VLAN	When QoS is really important for a specific VLAN	- Very good QoS possible per VLAN; - Very good finetuning of Unicast, Broadcast, Multicast traffic possible - Multiple services per back end port possible	One VFI per service (or VLAN) is consumed in the CSM. A lot of VLANs means a lot of VFIs used.
VLAN Based, Multi VLAN via QinQ → Best Practice	Best of both worlds. When none of the above solutions is needed/required. Transport a number of VLANs (=inner-VLAN) in the same service via adding an additional QinQ VLAN (=outer-VLAN).	- Very good QoS configuration possible per group of VLANs - Multiple services per back end port possible - The more VLANs you group via QinQ, the less VFIs are used in the CSM.	The same QoS will count for the entire group of VLANs, not per inner-VLAN. Some Unicast, Broadcast, Multicast traffic for a specific inner-VLAN could arrive in places where no port member for that VLAN is configured.This is because data travels in a VLAN combined way and the QinQ VLAN is only removed at the back end port of the L2/L3 IFM. It means that L2/L3 IFM will receive all traffic of all inner-VLANs in that QinQ group, even if no port-member for that VLAN is configured. When non-L2/L3 IFMs (e.g. 4-GC-LW) are involved, the QinQ VLAN tag is not removed when leaving the front port to the LAN. An external device (e.g. Hirschmann) must be used to interpret QinQ.

4.3 VLAN Based: Single VLAN with Local Service

4.3.1 General

A local service:

- is a single VLAN based service between only LAN front ports on L2/L3 IFMs;
- does not use back end ports, tunnels, WAN ports, the Dragon PTN network;
- does not consume network bandwidth;

- allows internal connections in the same L2/L3 IFM;
- configures the selected front ports in the selected VLAN;
- over two or more nodes can be used together with an extra cable to save Dragon PTN network bandwidth. E.g. to close the ring for MSTP (L2) or VRRP (L3) outside the Dragon PTN network via the external cable, see example figure below:

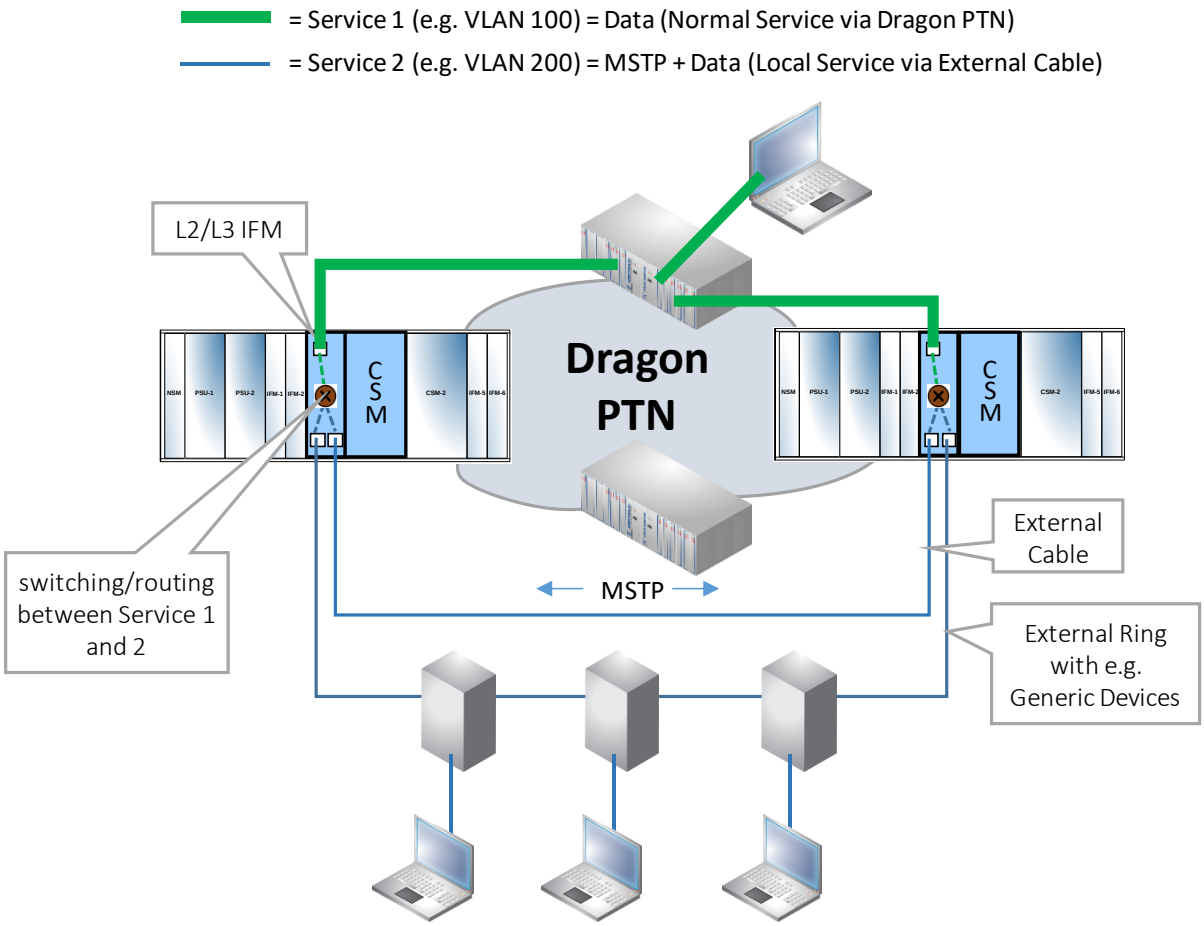

Figure 55 Local Service: Close an MSTP, VRRP Ring Outside the Dragon PTN Network

4.3.2 When to Use?

- When configuring a L2VPN/L3VPN, see further;
- When you don't want to waste L2/L3 IFM back end ports or network bandwidth on protocol management traffic (e.g. MSTP, VRRP, ...) and it is possible to create an external physical connection between the involved local service ports, e.g. 2 nodes in one room.

4.3.3 Configuration

- Service Wizard:
  - Service Name and Type Selection: Select VLAN based with Ethernet Type Single VLAN, fill out the VLAN ID and check the Local Service checkbox (=only active when selecting VLAN based, Single VLAN);
  - Service Endpoint Selection: Select the front ports on the L2/L3 IFMs that must be part of this local service. For example, if you want to couple an external ring with external

devices to the Dragon PTN network in Node1 and Node2, you will at least need two front ports in Node1 and two front ports in Node2 to complete the local service. Per node: One port to connect the external ring, and another port to connect the extra external cable (or network) to the other node;

- VLAN Tagging/Untagging: configure the VLAN tagging/untagging behavior;

- Optional: When you want to close a ring outside the Dragon PTN network (e.g. VRRP, MSTP), create a physical external connection between the selected front ports in the local service;

4.4 VRF Ports (Only L3 IFM)

A 'VRF port' is not a front port on a L3 IFM, but a special port inside the virtual router on the L3 IFM. A VRF port just terminates a VLAN. When a service does not use front ports of the virtual router, but still must be able to route between VLANs on that router, use the VRF port of the virtual router.

When configuring an Ethernet service on the L3 IFM, a VRF port ⊗ and a normal front port from the same L3 IFM can never be in the same VLAN. This results in the following service wizard behavior:

- For VLAN Based services:
  - Select VRF port: When a service must be configured on a Virtual Router on the L3 IFM and none of the front ports of the L3 IFM is part of the service, select the VRF port instead by clicking the VRF port icon ⊗. Other port icons will be disabled and cannot be selected anymore. Later on, when you decide to add front ports, modify the service by unselecting the VRF port and selecting front ports instead;
  - Select Front port: VRF port icon is disabled and is not relevant anymore when front ports are selected.

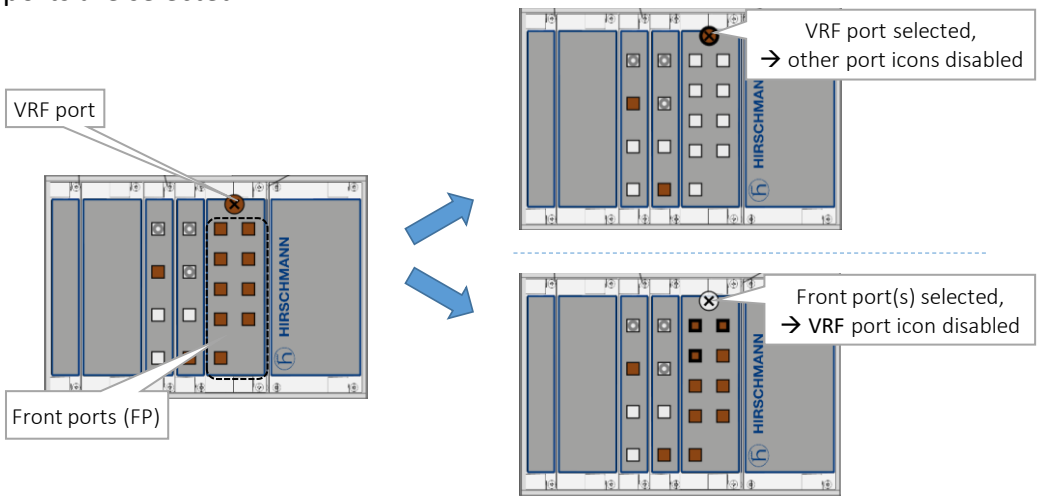

Figure 56 VRF Port and Front Ports on L3 IFM

- For Port Based services:
  - VRF ports and front ports of the same L3 IFM can be selected in the same service, provided that they are assigned to a different VLAN in the 'VLAN Selection' page in the wizard.

4.5 Back End Ports (BEn)

L2/L3 IFMs have both Front Port (=FP) and Back End (=BE) ports. The External LAN or network is connected to the FPs. The BEs are connected via the node backplane to the CSM.

When configuring an Ethernet service with L2/L3 IFM ports, the service goes via one of the available BEs to the CSM. The BE link bandwidth and the amount of BE links between the L2/L3 IFM and CSM depend on the Node type and the slot in which the L2/L3 IFM resides. See Ref.[100] in Table 1 below for an overview.

The back end ports can be viewed in the Ethernet service wizard in the 'Service Back End Port Selection' page. By default, a back end port for each L2/L3 IFM is selected by HiProvision. See figure below.

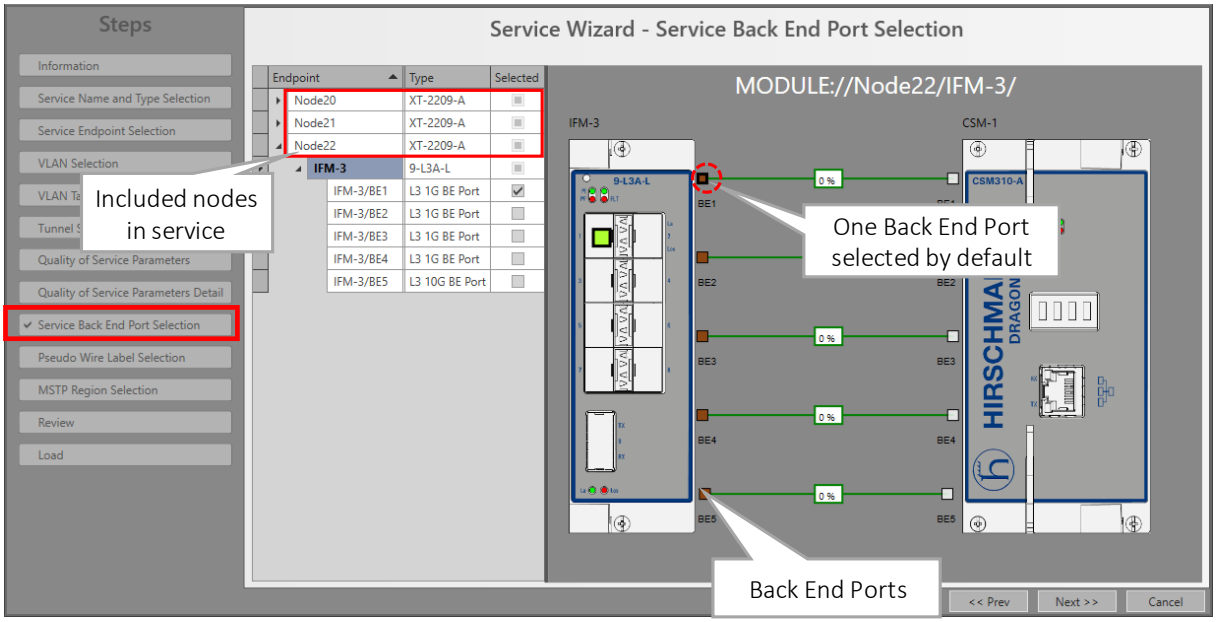

Figure 57 Default Back End Port View

If there is more than one BE link available, HiProvision tries to fill up by default the lowest BE number first e.g. BE1 link, then BE2 etc... If an additional service cannot fit anymore in the BE(n) link due to insufficient available bandwidth, or is port based, HiProvision tries to configure it in the BE(n+1) and so on. You can overrule this default programming behavior by selecting your desired BE link. For example, you could custom program your biggest services in the L3 IFM on BE5 (=10Gbps) (Node PTN2209) and program the smaller services on BE1-BE4 (=1Gbps).

Expand the desired L2/L3 IFM in the figure below to show its back end ports and the consumed bandwidth percentage on that back end link to the CSM. You could select another back end port for the service to fine-tune the bandwidth consumption on the back end links. Only one back end port can be selected.

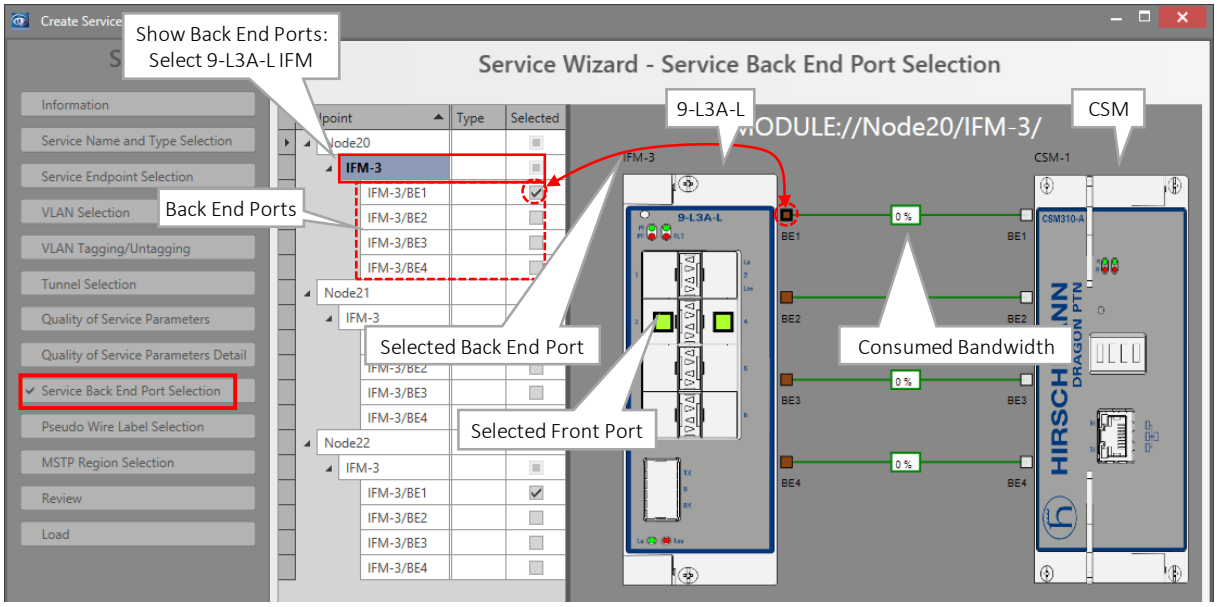

Figure 58 Customize Back End Port Selection

NOTE: When working offline, Back End Ports are only visible when a CSM has been configured in the database.

NOTE: Each configured Mixed VLAN or port based service exclusively consumes one entire back end port on the L2/L3 IFM. For example, when the L3 IFM has 5 back end ports, and you configure 5 port based services, all back end ports are used and no extra services can be configured on this L3 IFM. Instead, you could consider to configure VLAN based services instead which allows multiple services per back end port.

4.6 L2VPN

4.6.1 General

A L2VPN is any Ethernet service over Dragon PTN that does not include routing. The entire Dragon PTN network is located in same IP subnet. This service can include a mix of Ethernet IFMs (4-GC-LW, …), L2 IFMs and L3 IFMs, but never using a virtual router on the L3 IFMs.

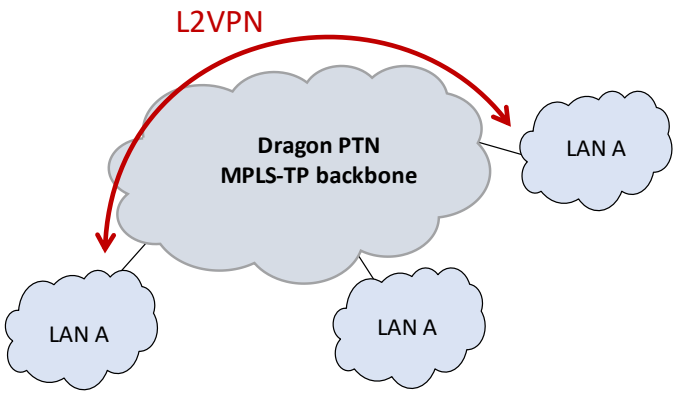

Figure 59 L2VPN General

4.6.2 Detailed Example

Example is similar to the port based service (=mixed VLAN) example, see §4.9.1.

4.7 L3VPN

4.7.1 General

A L3VPN is an Ethernet service over Dragon PTN that includes routing via a Virtual Router

A L3VPN (Layer3 VPN) is a routed network within Dragon PTN that interconnects one or more IP subnets via the MPLS-TP backbone. One or more Ethernet LAN ports from one IP subnet will be able to communicate with one or more Ethernet LAN ports in another IP subnet. The L3VPN is created via configuring an MPLS-TP service and one or more local LAN services interconnecting them via a virtual router on a L3 IFM.

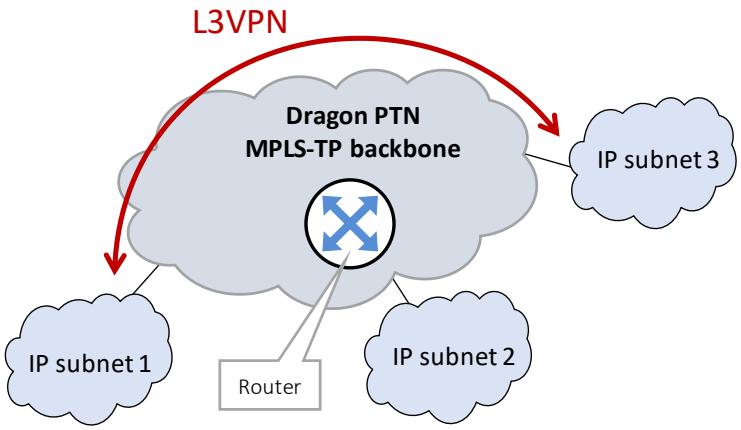

Figure 60 L3VPN General

General Steps to create a L3VPN:

1. MPLS-TP service creation. Bandwidth reservation and protection (ERPSv2 = Ethernet Ring Protection Switching) on backbone;
2. LAN creation (Local service connected to L3 IFM);
3. Virtual Router (VRF) creation: Interconnects MPLS-TP service Local LAN service;
4. (optional) Router Redundancy via VRRP (see §5.10);
5. Configure Routing protocol:
   - Only one router: no routing protocol must be configured;
   - Two routers: configure Static Routing (see §5.8);
   - More than two routers: configure a dynamic routing protocol OSPF (see §5.7);

4.7.2 Detailed Example

See §4.9.

4.8 Bandwidth Optimization Group

4.8.1 General

For readability reasons, if ‘group’ is mentioned further on, it means ‘Bandwidth Optimization Group’.

Grouping some non-overlapping single VLAN based services in a logical ring together in one group optimizes the consumed network bandwidth. All services grouped together in a group look like one big chained service on a ring because of the non-overlapping behavior.

CAUTION:
- This is an expert feature and is preferably discussed with Hirschmann Automation and Control GmbH during the network design phase.
- The first paragraphs below just focus on bandwidth optimization.
- Further on, a network design concept to optimize a ‘routed network’ is worked out.

- Services in a group must have the same ring (and subring) tunnel;
- The first created service in the group defines the service Priority for the entire group;
- No overlapping or LSP sharing allowed! See figure below. HiProvision will detect overlaps automatically.
- The maximum configured bandwidth per link:
  - In a subring: sum of the two highest service bandwidths in the group for that subring;
  - In a logical ring: the sum of the two highest service bandwidths for that logical ring and the highest service bandwidth of each connected subring, if any;
  - Some calculation examples in §4.8.2.
- The more services with similar bandwidths in a group, the higher the benefit. In the examples below, Group1 (=100 Mbps per link) has a higher benefit than Group2 (=420 Mbps per link)
  - Group1: 10 services with a bandwidth of 50 Mbps → bandwidth per link = sum 2 highest = 50 + 50 = 100 Mbps (gain or benefit = 400 Mbps);
  - Group2: 9 services of 10 Mbps and one 1 service of 410 Mbps → bandwidth per link = sum 2 highest = 10 + 410 = 420 Mbps (gain or benefit = 80 Mbps);

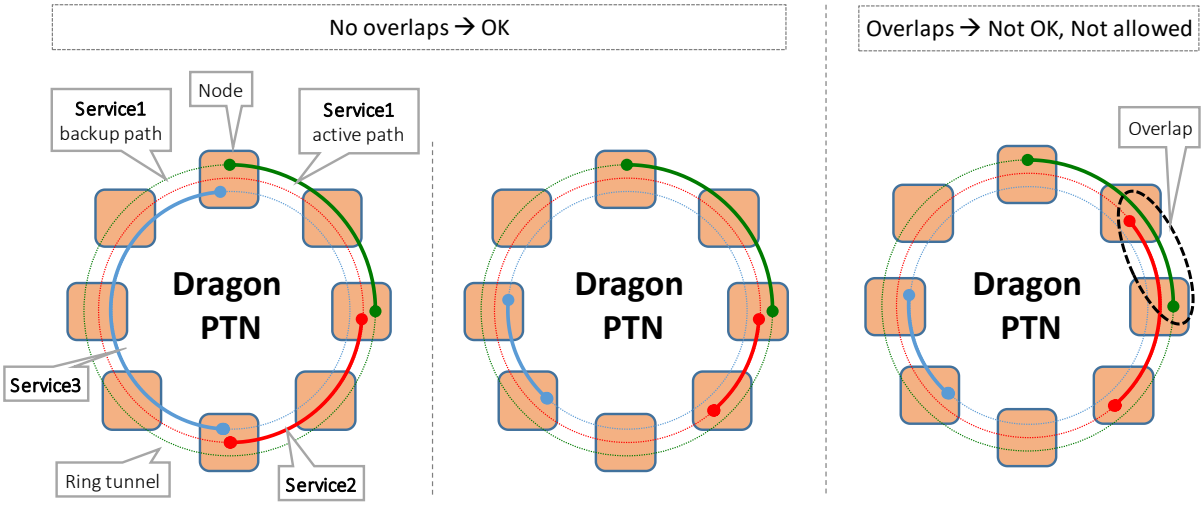

Figure 61 Bandwidth Optimization Group: Overlap Concept

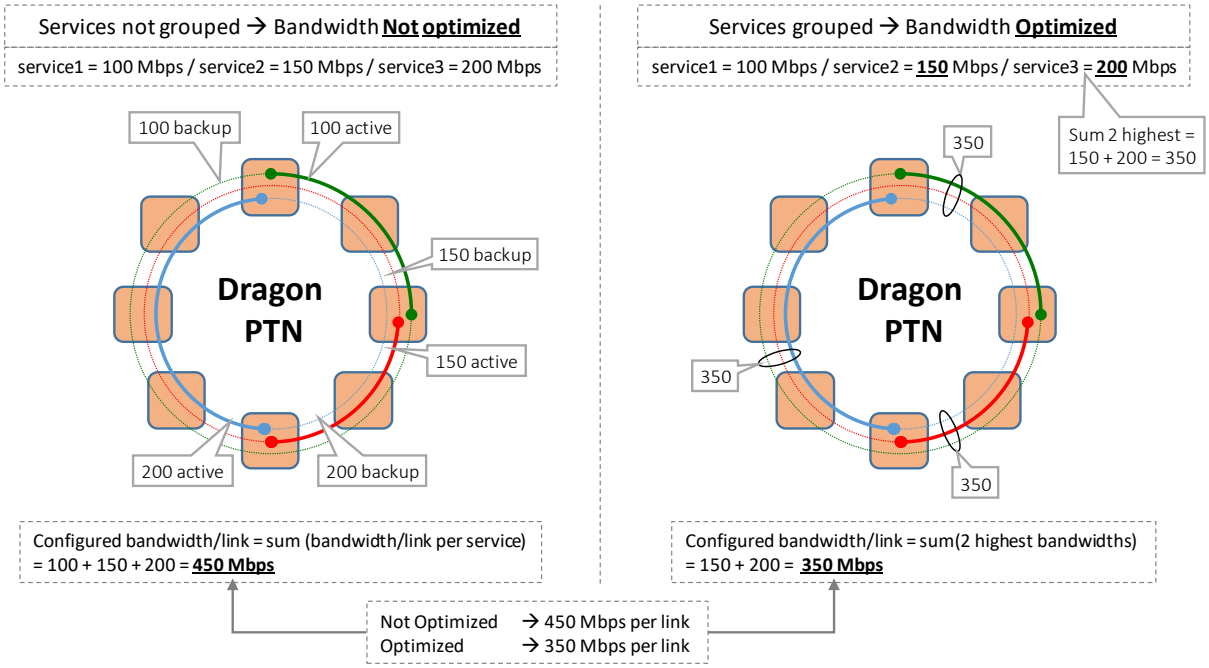

Figure 62 Bandwidth Optimization, Logical Ring Only (no Subring)

4.8.2 Bandwidth Optimizations with Combined Logical Ring and Subrings

The figures below show some examples of one Bandwidth Optimization Group, including 12 or 13 services (s1, s2, …, s12, s13) configured in logical ring and subring combinations. The first figure has 12 services with 4 services in the logical ring (s1,…,s4), 4 services (s5,…,s8) in subring1 and 4 services (s9,…,s12) in subring 2. This figure has no interconnection service (s13). An interconnection service has endpoints in both the logical ring and subring.

The other figures have an additional interconnecting service (s13). The bandwidth optimization is a little bit more complex in these cases. It just depends on how big its bandwidth (s13) is compared to other bandwidths (s1,…,s12) in that solution.

- The maximum configured bandwidth per link (=optimized bandwidth):
  - In a subring: sum of the two highest service bandwidths in the group for that subring;
  - In a logical ring: the sum of the two highest service bandwidths for that logical ring and the highest service bandwidth of each connected subring, if any;

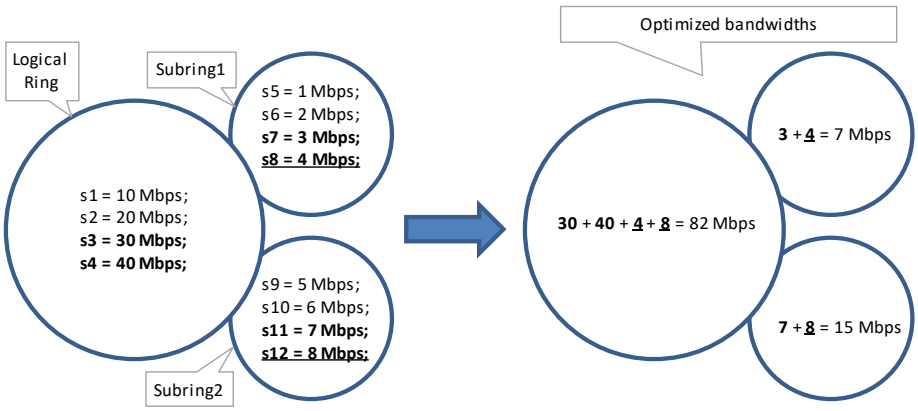

Figure 63 No Interconnecting Service between Logical Ring and Subrings

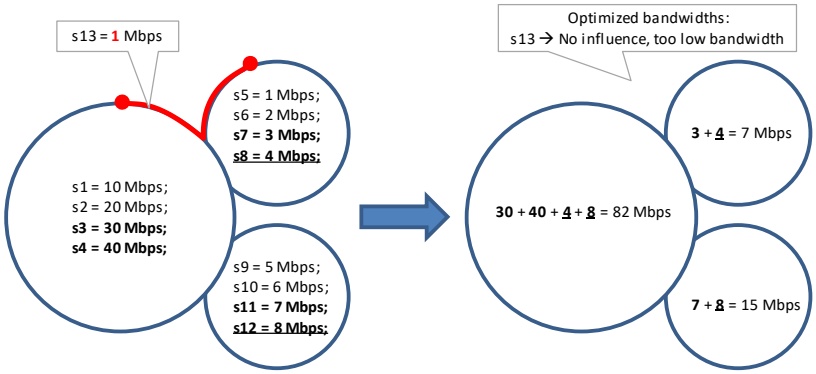

Figure 64 Interconnecting Service S13 Has No Influence

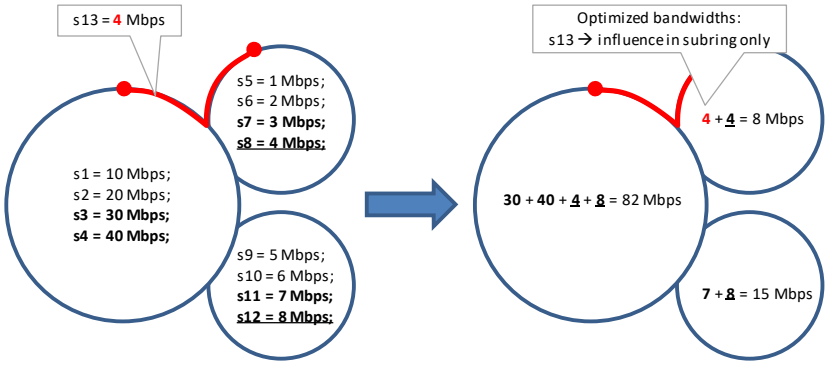

Figure 65 Interconnecting Service S13 Has Influence In Subring Only

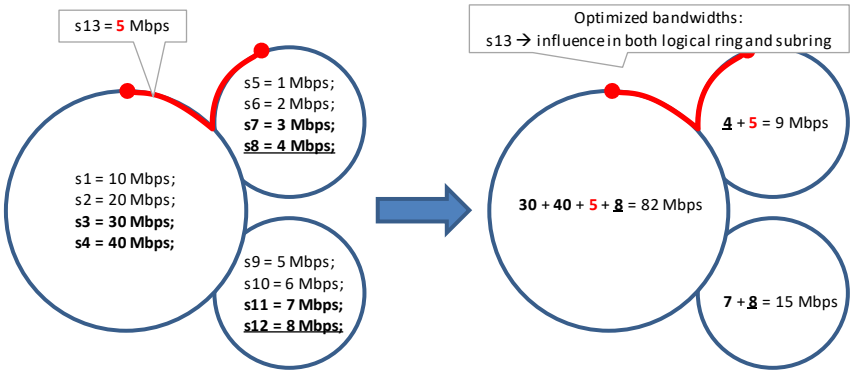

Figure 66 Interconnecting Service S13 Has Influence In Both Logical Ring and Subring

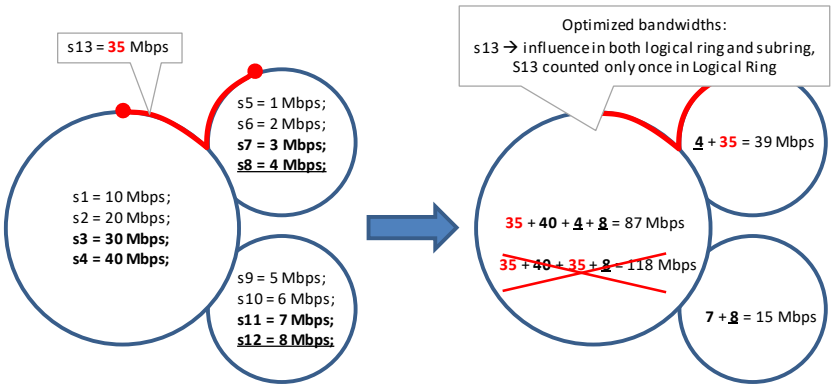

Figure 67 Interconnecting Service S13 Top 2 Highest Bandwidths in Logical Ring

4.8.3 Create Bandwidth Optimization Group, First Service in the Group

Create a group by defining the Bandwidth Optimization Name when creating the first Ethernet service in that group.

1. Go to the service wizard via Dashboard → Connections Tile → Services → Click '+' to create your first service in the group;

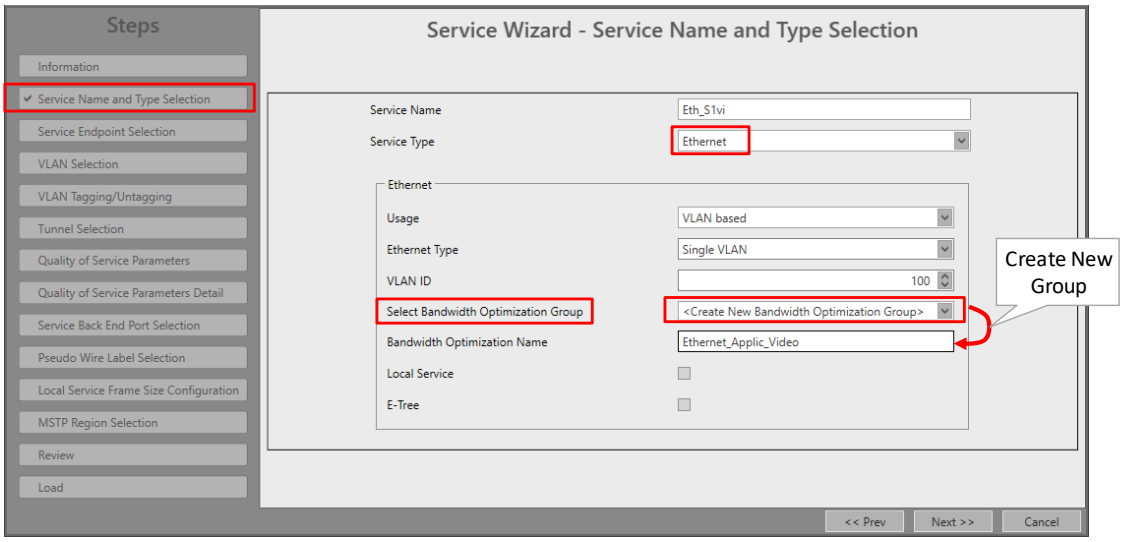

Figure 68 Service Wizard: Create New Bandwidth Optimization Group

2. Fill out a service name;
3. Select an 'Ethernet' service type, VLAN based, Single VLAN, fill out a VLAN ID;
4. Select '<Create New Bandwidth Optimization Group>' and fill out a Bandwidth Optimization name;
5. Click Next >>;
6. Select your endpoints;
7. Perform some extra VLAN actions if desired;
8. Select a logical ring or subring runnel, other tunnels are not shown;
9. In the Quality of Service Parameters page, fill out the Priority and bandwidth settings. The configure Priority of the first service will be used for the entire group. Bandwidth settings can still be done per service in the group;

CAUTION: Think twice about your priority and choose it right immediately. Modifying it afterwards is currently not supported. If you need another priority later on for the entire group, you have to delete the entire group first and rebuild it with the new priority.

10. In the Quality of Service Parameters Detail page, further bandwidth/burst size fine-tunings can be done (see also §3.3.3). Make sure that if you make a change in the LSPs tab, that the bandwidth/burst size of all LSPs in that service must be the same and changed accordingly. For updating multiple rows (or LSPs), the multiple update feature (see §3.3.5b) is advised to use. Make sure that if you change an input parameter (e.g. Gross Bandwidth (kbps) input) for an LSP, that you assign the same value to its output parameter (e.g. Gross Bandwidth (kbps) output → via Advanced button), and this for all LSPs;
11. For L2/L3 IFMs, select the desired Back End Ports;

12. Leave the Pseudo Wire Label Selection on its defaults;
13. Review;
14. Load, Finish.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

4.8.4 Assign Services to an Existing Bandwidth Optimization Group

Assign a second, third, …. service to an existing group via creating your second, third, … Ethernet service and select an existing group via the Bandwidth Optimization Group drop down.

1. Go to the service wizard via Dashboard → Connections Tile → Services → Click '+' to create your service;
2. Fill out all the service parameters and select the existing group in the Bandwidth Optimization Group drop-down list;
3. Click Next >>;
4. Select your endpoints, make sure not to overlap (or share same LSPs with) existing services in this group. HiProvision will detect overlaps automatically;
5. Perform some extra VLAN actions if desired;
6. The tunnel to use is already defined (by creating the first service in previous paragraph). No other tunnel can be selected;
7. In the Quality of Service Parameters page, the Priority is already defined (by creating the first service in previous paragraph). Bandwidth settings can still be configured per service in the group;
8. In the Quality of Service Parameters Detail page, further bandwidth/burst size fine-tunings can be done (see also §3.3.3). Make sure that if you make a change in the LSPs tab, that the bandwidth/burst size of all LSPs in that service must be the same and changed accordingly. For updating multiple rows (or LSPs), the multiple update feature (see §3.3.5b) is advised to use. Make sure that if you change an input parameter (e.g. Gross Bandwidth (kbps) input) for an LSP, that you assign the same value to its output parameter (e.g. Gross Bandwidth (kbps) output → via Advanced button), and this for all LSPs;
9. For L2/L3 IFMs, select the desired Back End Ports;
10. Leave the Pseudo Wire Label Selection on its defaults;
11. Review;
12. Load, Finish.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

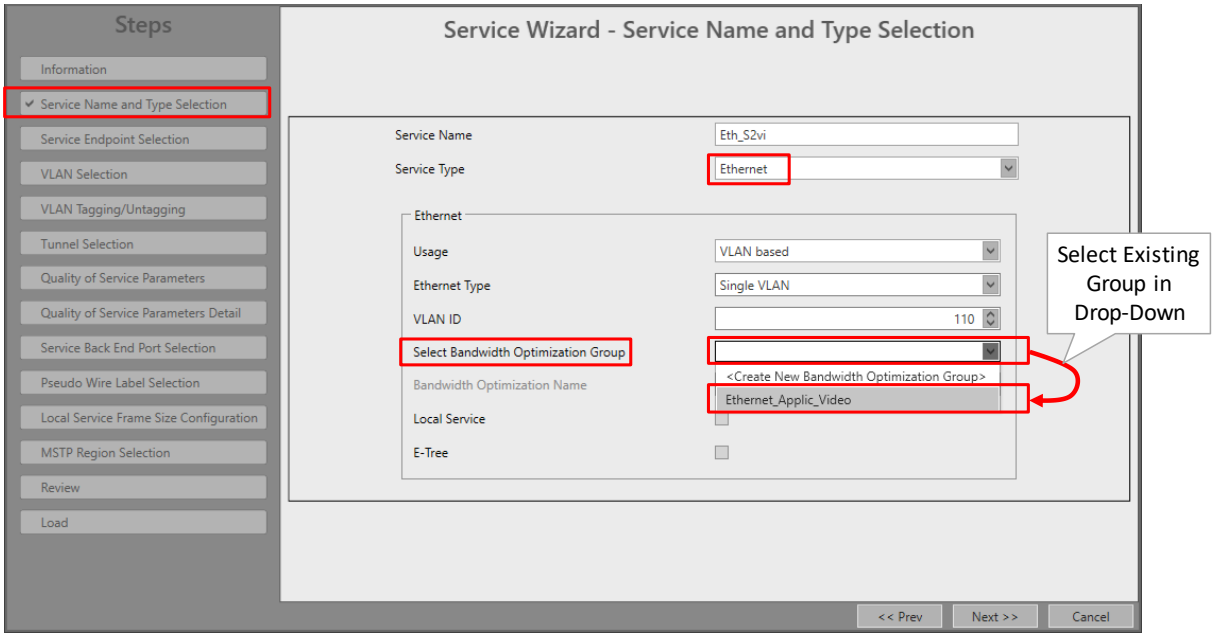

Figure 69 Service Wizard: Assign Service to Existing Bandwidth Optimization Group

4.8.5 Resulting Optimized Bandwidth in the Group

1. Go to the service wizard via Dashboard → Connections Tile → Services;
2. The Bandwidth Optimization Groups are visible in the services list. Just select/expand the desired group.
3. On the left-hand side, the included services in that group are shown. On the right-hand side, the configured bandwidth per service is shown.
4. Also the configured optimized bandwidth per link for the entire group is shown.

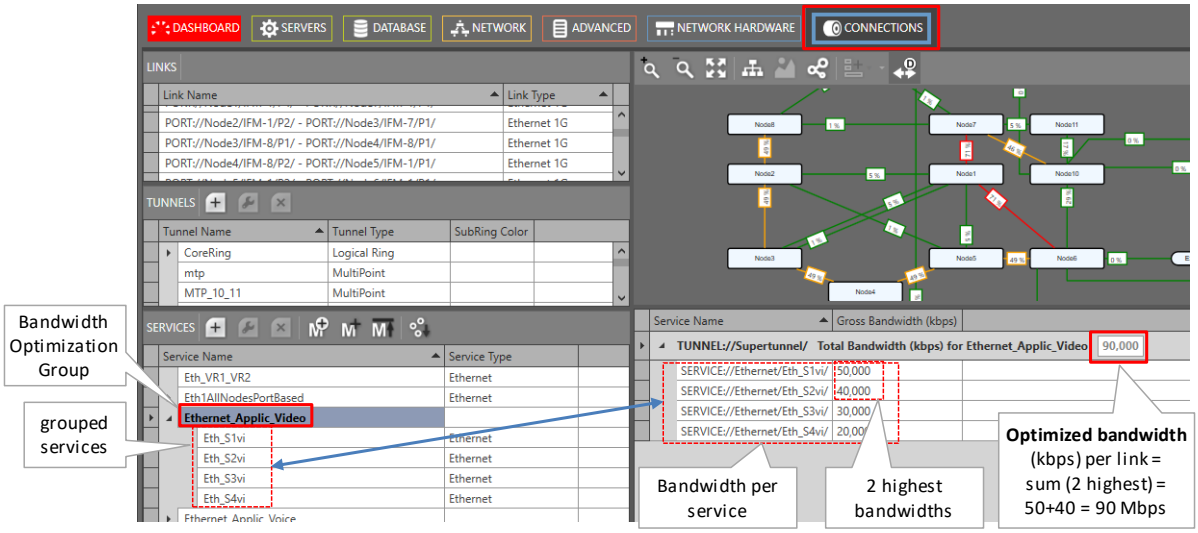

Figure 70 Resulting Optimized Bandwidth

4.8.6 Modify Bandwidth Optimization Group

The following parameters can be modified after creation:

- Bandwidth Optimization Group:
  - Currently, nothing can be modified.
- Included services in the Bandwidth Optimization Group:
  - Service Name;
  - VLAN ID;
  - E-Tree;
  - Add/Remove Endpoints;
  - CAUTION: Priority can not be modified. If you want another priority, you have to delete the entire group including all its services first, and rebuild everything from scratch;
  - Maximum/Average frame sizes;
  - Bandwidth/Burst sizes;

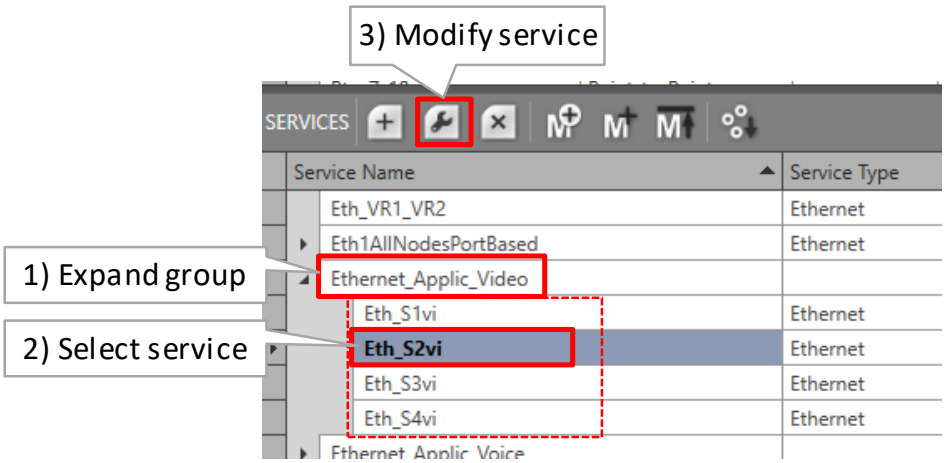

Figure 71 Modify Included Service

4.8.7 Delete Bandwidth Optimization Group

If you want to delete the group, you have to delete all its included services first. If you delete the last service in that group, the group itself will be deleted as well.

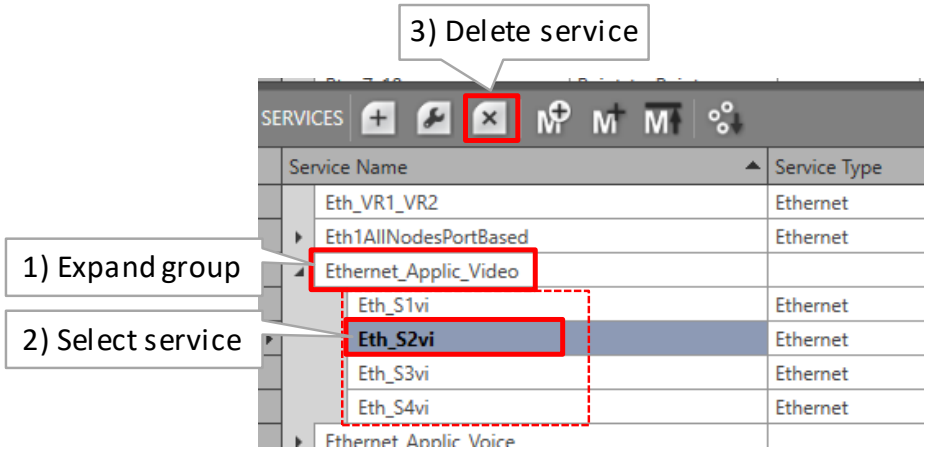

Figure 72 Delete Included Service

4.8.8 Network Design: Optimize a Routed Network via Bandwidth Opimization Groups

If a service keeps growing in amount of nodes, end points, VRFs, VLANs, OSFP neighbors etc…, sooner or later, some resource limits of a switch ASIC in the CSM or L2/L3 IFM will be reached. As a result, some configuration possibilities will decrease, e.g. no extra service can be configured, the maximum number of VFIs has been reached, running out of bandwidth etc…

Therefore, it is necessary in the network design phase to not overdesign your services, and keep the services rather medium sized and performant (with still some room for small changes) instead of an overdesigned solution.

The figure below shows an overdesigned network solution with 2 ethernet application services (video & voice), 120 nodes, each node having 2 VRFs, and 238 OSPF neighbors. This solution will not work because the amount of OSPF neigbors per L3 IFM (=238) and per VRF (=119) is higher than the allowed maxima of 128 per L3 IFM and 32 per VRF.

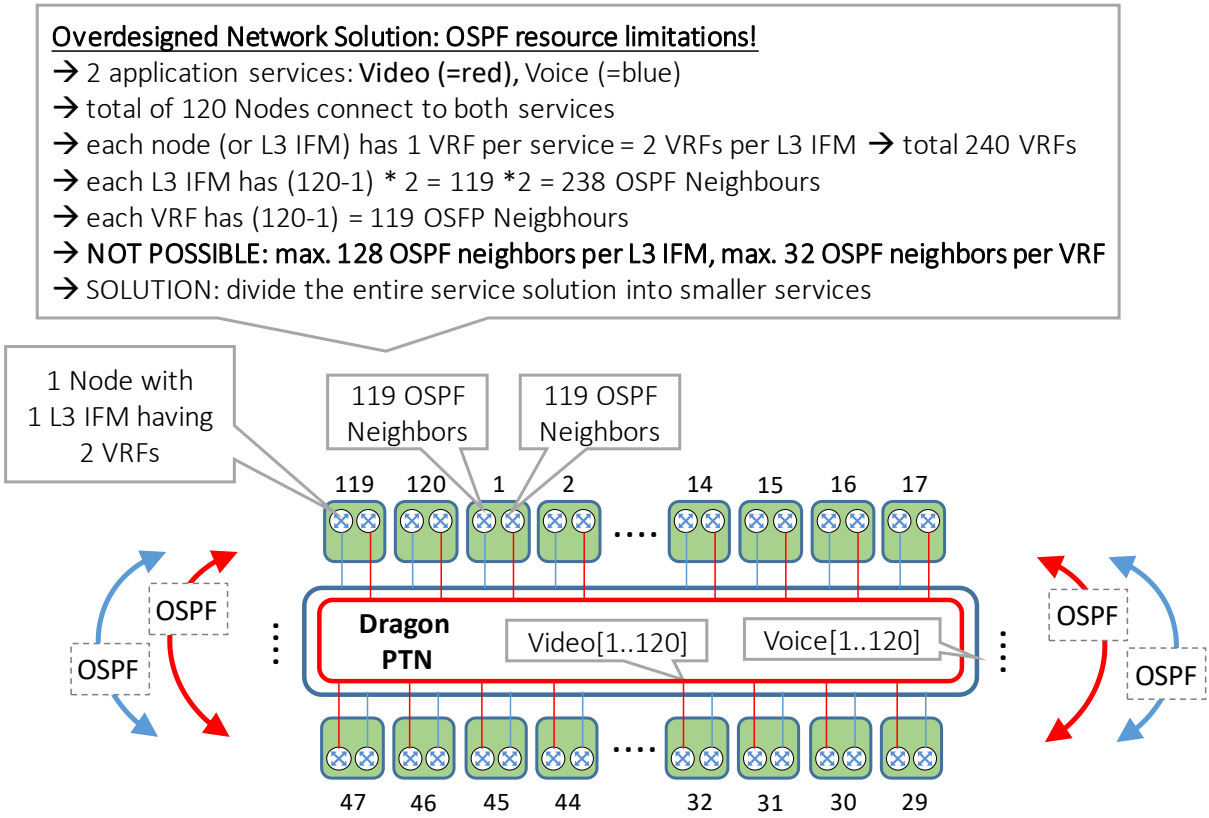

Figure 73 Overdesigned Network, Too Many OSPF Neighbors

Therefore, segment the applications services into smaller services in order to lower the amount of OSPF neighbors per VRF. If you configure these smaller services in addition into a Bandwidth Optimization Group, the total consumed bandwidth on the ring will be optimized as well.

NOTE: You have to configure manually the smaller services via HiProvision, HiProvision will not automatically convert a too big overdesigned service into smaller parts.

In the example below is shown how the big service can be segmented into 8 smaller services or segments (→ Segment1 = S1, …) to lower the amount of OSPF neighbors. Both the voice and video service will be segmented each in 8 services, resulting in a total of 16 services or segments.

Two segments are linked to each other by programming a same node (=shared node) in both service segments. The shared node interconnects both segments. The resources of a shared node are stressed more than the resources of non-shared nodes (=node only part of one segment).

If you have multiple application services (e.g. Video and Voice) that follow the same path, for the ease of configuration, you could use the same shared node (e.g. Node 16) for both applications. If you want to unstress the shared nodes even more, make use of shifted shared nodes, where each application has its own unique shared node.

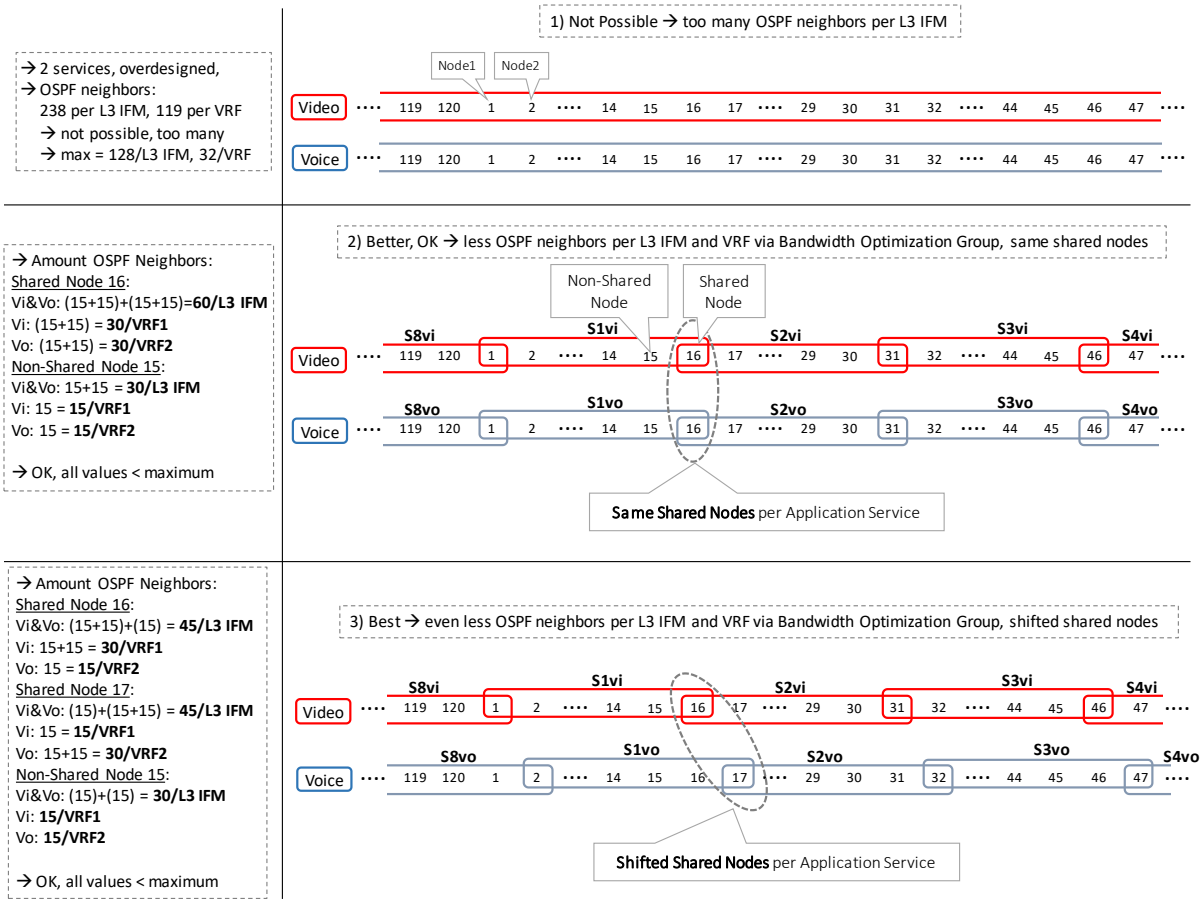

Figure 74 Different Ethernet Service Segmentation Examples

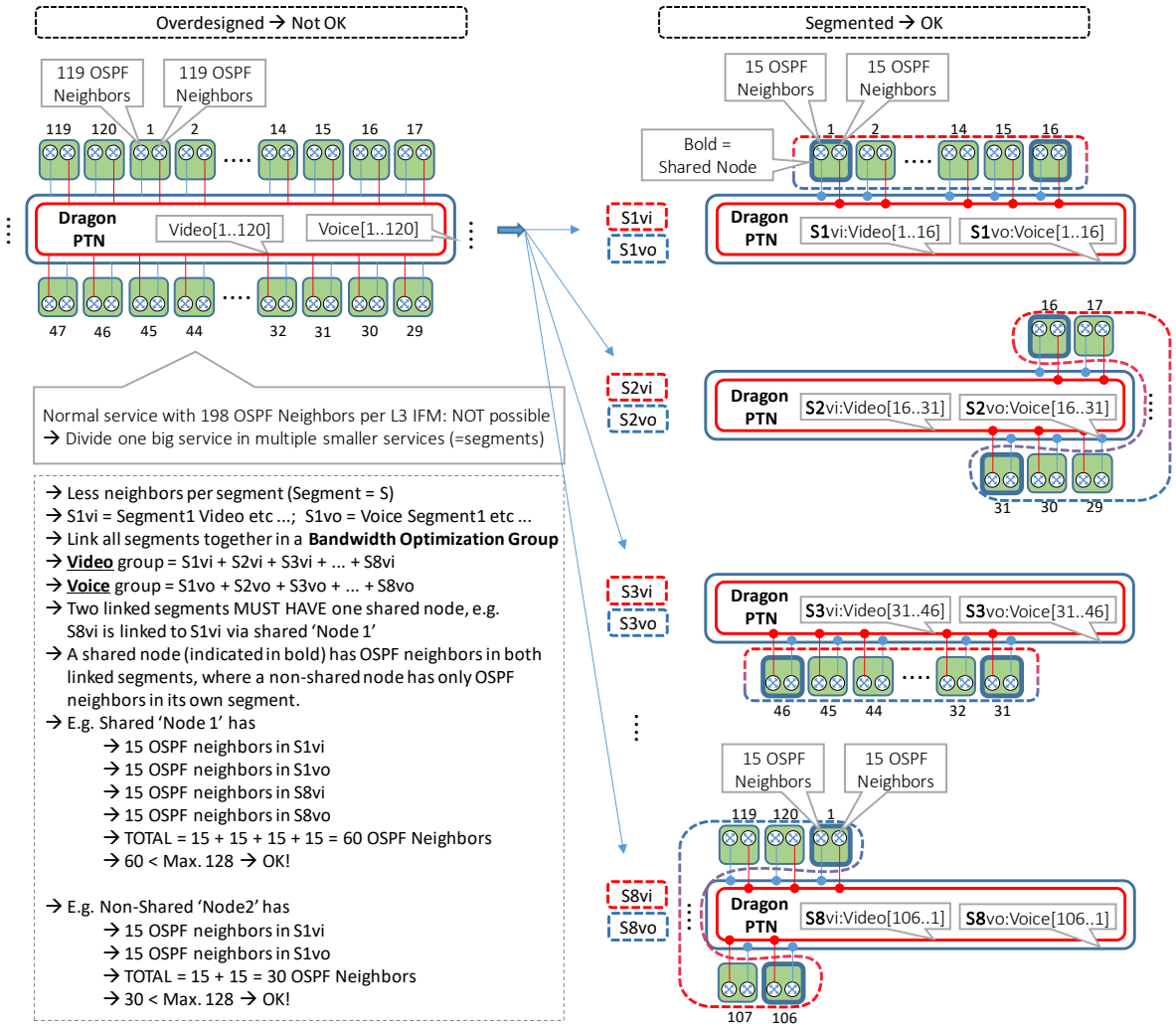

Figure 75 Segment Big Service into Smaller Services

4.9 Detailed Examples

4.9.1 Port Based Service (=Mixed VLAN) For MSTP

In general, it looks like the figure below:

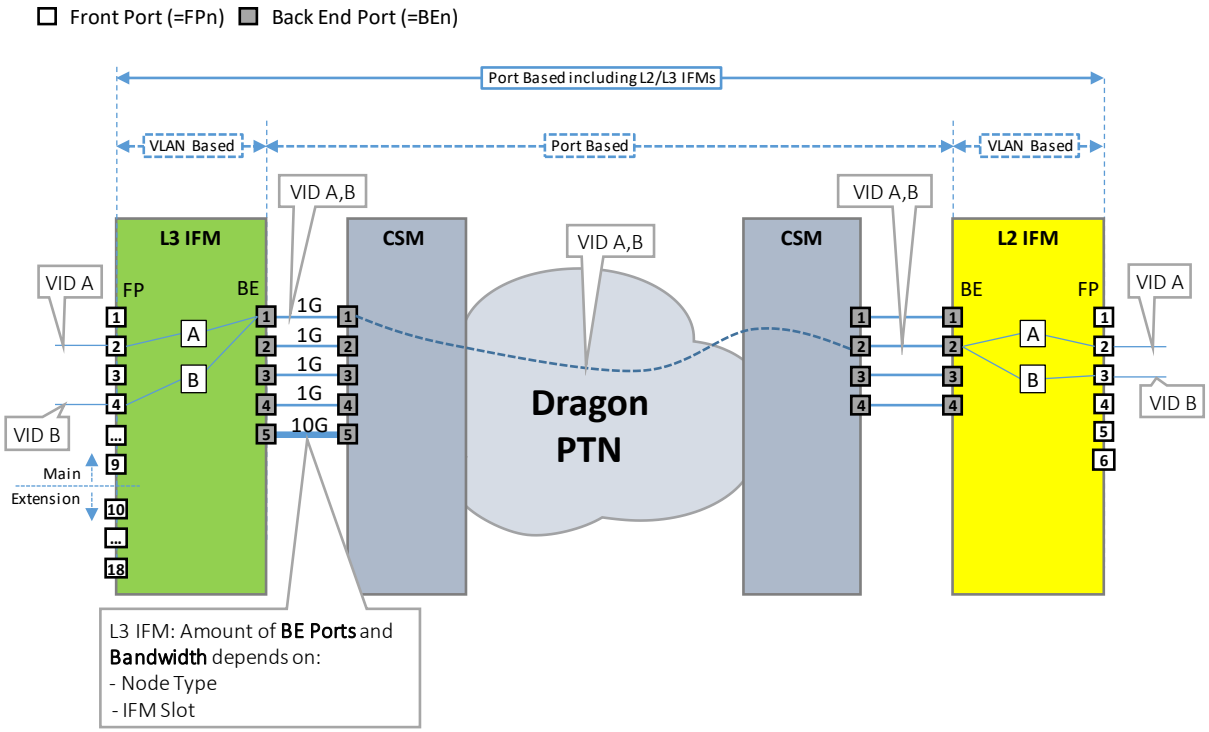

Figure 76 Example-General: Port Based Ethernet Service, Mixed VLANs, Back End Ports

The following detailed example with specific VLANs will be worked out more into detail:

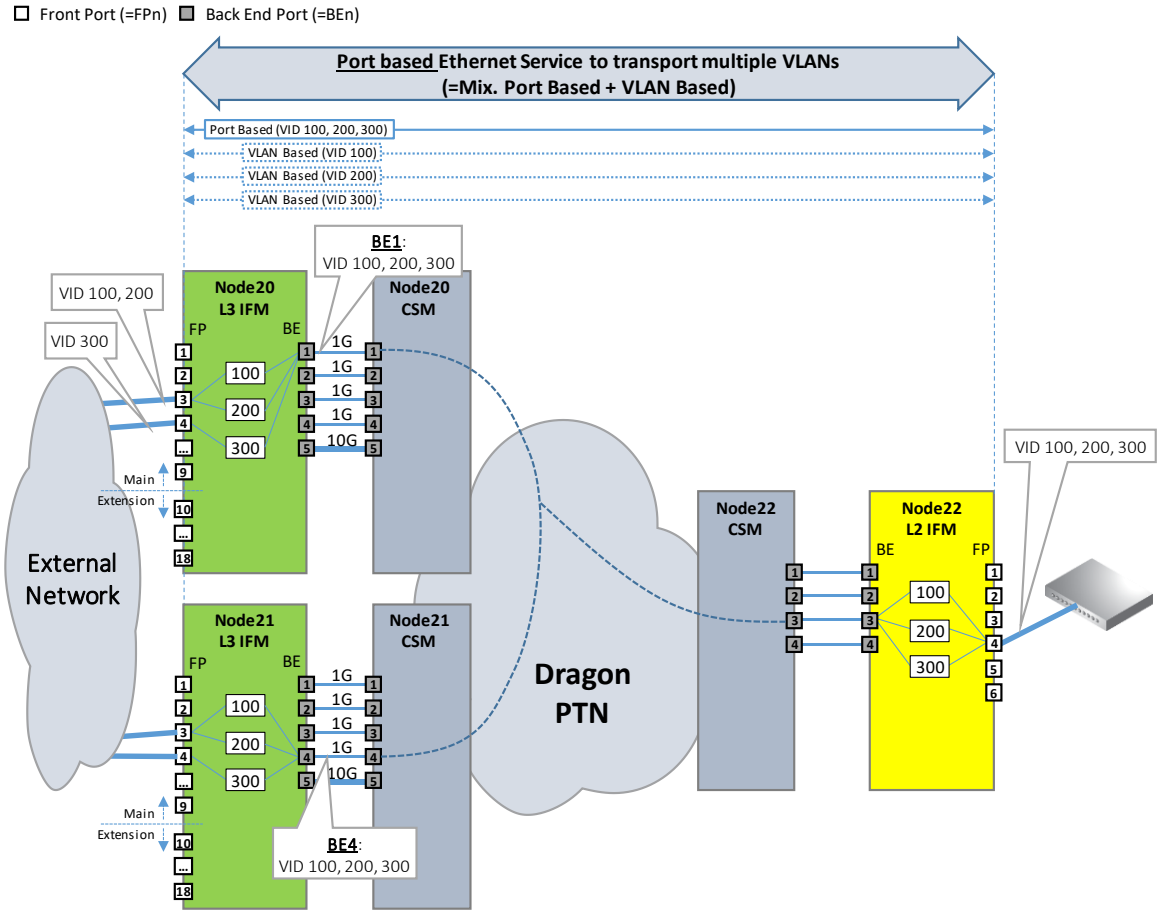

Figure 77 Example-Detailed: Port Based Ethernet Service, Mixed VLANs, Back End Ports

When configuring a Port Based Ethernet including L2/L3 IFM ports, HiProvision automatically and additionally configures a VLAN based service (=child) per VLAN included in the port based service (=parent).

When you finalized for example (see example pictures below) the creation of a port based service with VLANs 100, 200 and 300, HiProvision will have created 4 services (=1 port based + 3 VLAN based):

- One port based service (=parent) including VLANs 100, 200 and 300;
- (automatic) Three VLAN based services (=child):
  - VLAN based service including VLAN 100;
  - VLAN based service including VLAN 200;
  - VLAN based service including VLAN 300.

NOTE: A VLAN ID can be used once in the same service on the same L2/L3 IFM;

In the VLAN Selection Page in the Ethernet service wizard:

1. The screen below is shown when the port based service includes L2/L3 IFMs;
2. Every endpoint must be included in a VLAN. Fill out the VLANs from your incoming traffic in the 'Known VLANs' field and click the Add button.
3. Assign the L2/L3 IFM front ports to the correct VLANs via clicking the VLAN checkboxes;
4. Untagged traffic indicates untagged data frames. 'Don't use' must be used when there are no untagged frames expected in the incoming traffic. Untagged data frames will be dropped. 'Don't use' does not block the MSTP frames (which are always untagged). If you do expect untagged data frames, change 'Don't use' into 'tag with <VLAN ID>' by clicking the cell and selecting another value.

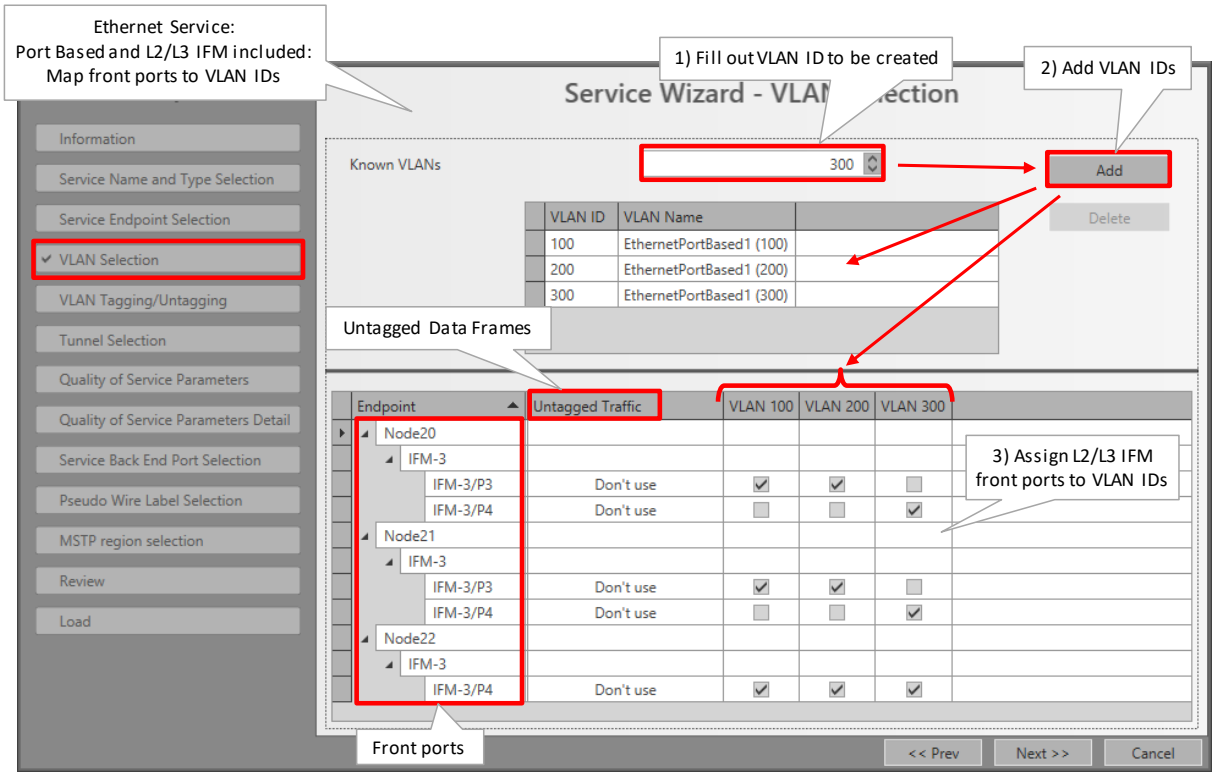

Figure 78 Example-Detailed: Port Based: Map L2/L3 IFM Front Ports to VLANs

After the Ethernet service wizard has been finished, both the parent and child services of the port based service are visible in the services list:

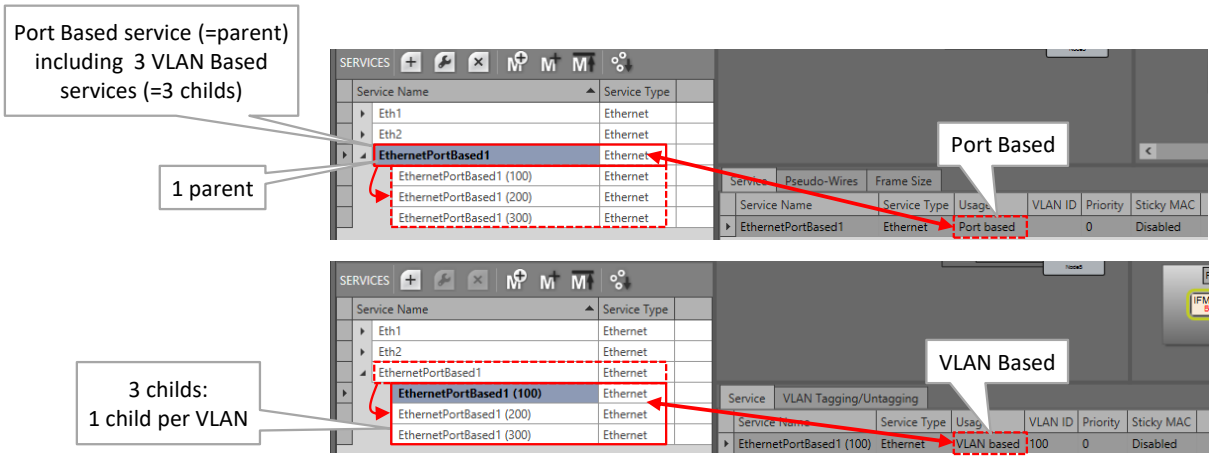

Figure 79 Example-Detailed: Port Based: Created, Result in Services List

4.9.2 VLAN Based Service: Multiple VLANs via QinQ

Prerequisite: The MPLS-TP network must have been created: Nodes, IFMs, WAN links.

Find below a QinQ example. Further on, the most important steps to configure this in HiProvision are shown.

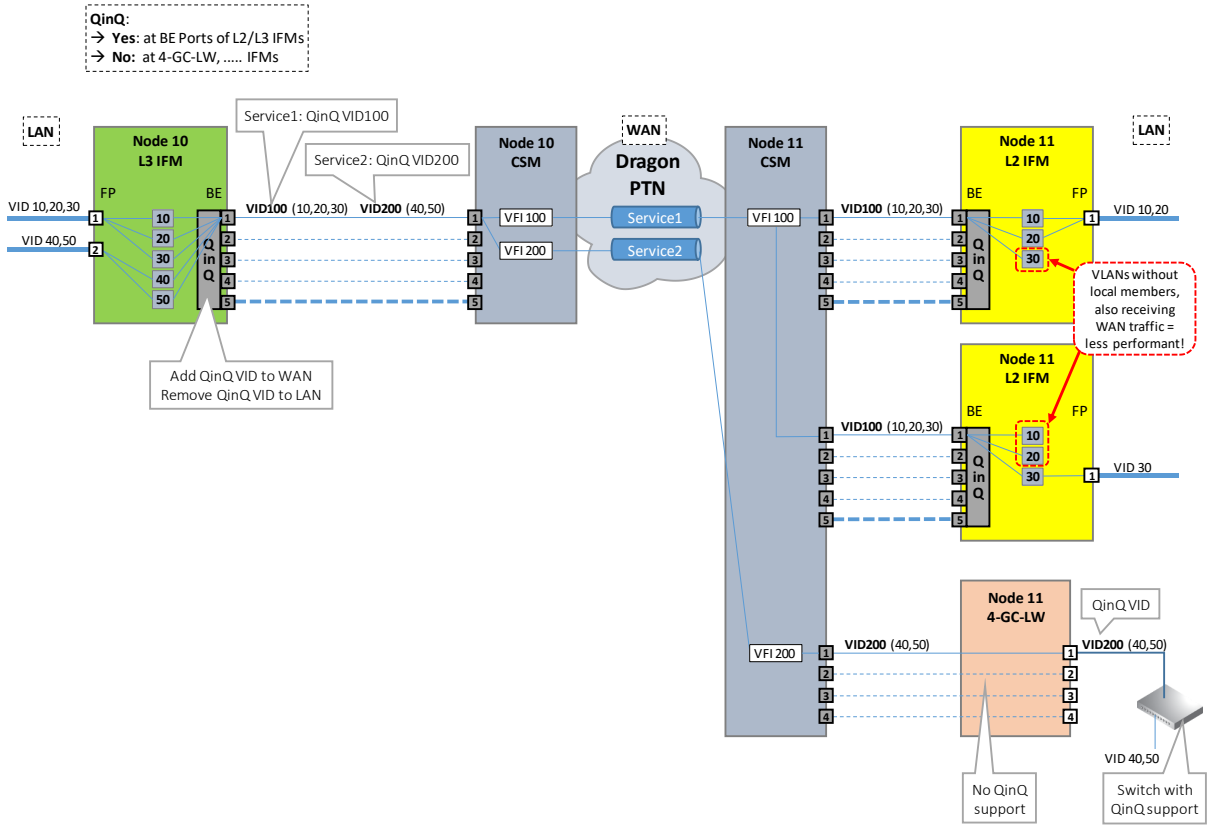

Figure 80 QinQ/Multiple VLAN Example

The steps below show the most important points of attention when creating this QinQ solution example with service1 and service2. Other QinQ cases need similar configurations.

1. Create Service1:
   - Service Type:
     - Ethernet Service;
     - VLAN Based, Multi VLAN: QinQ VLAN ID 100.

     NOTE: QinQ is not supported on Local Services because QinQ operation occurs at the back end ports of L2/L3 IFMs;

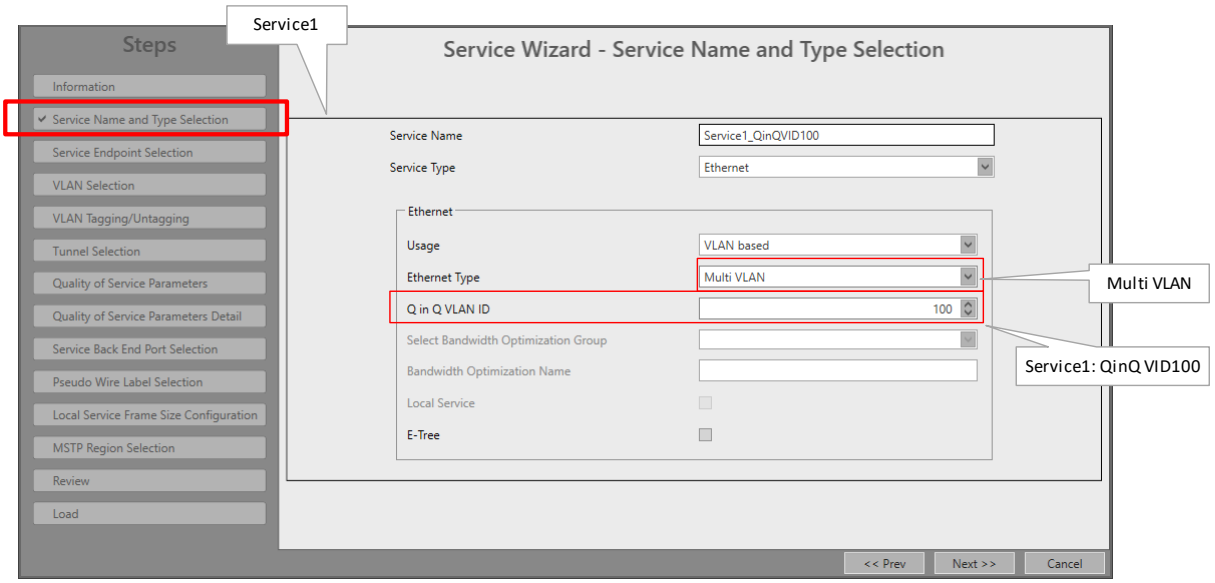

Figure 81 Multi VLAN/QinQ Service1: Start Creation/Define QinQ VLAN

   - Service End Point Selection:
     - Node 10:
       - L3 IFM: front port 1;
     - Node 11:
       - First L2 IFM: front port 1;
       - Second L2 IFM: front port 1;
   - VLAN Selection:
     - Create/Add VLANs 10,20,30;
     - Assign P1 of L3 IFM in Node 10 to VLAN 10,20,30;
     - Assign P1 of the first L2 IFMs in Node 11 to VLAN 10,20;
     - Assign P1 of the second L2 IFM in Node 11 to VLAN 30;

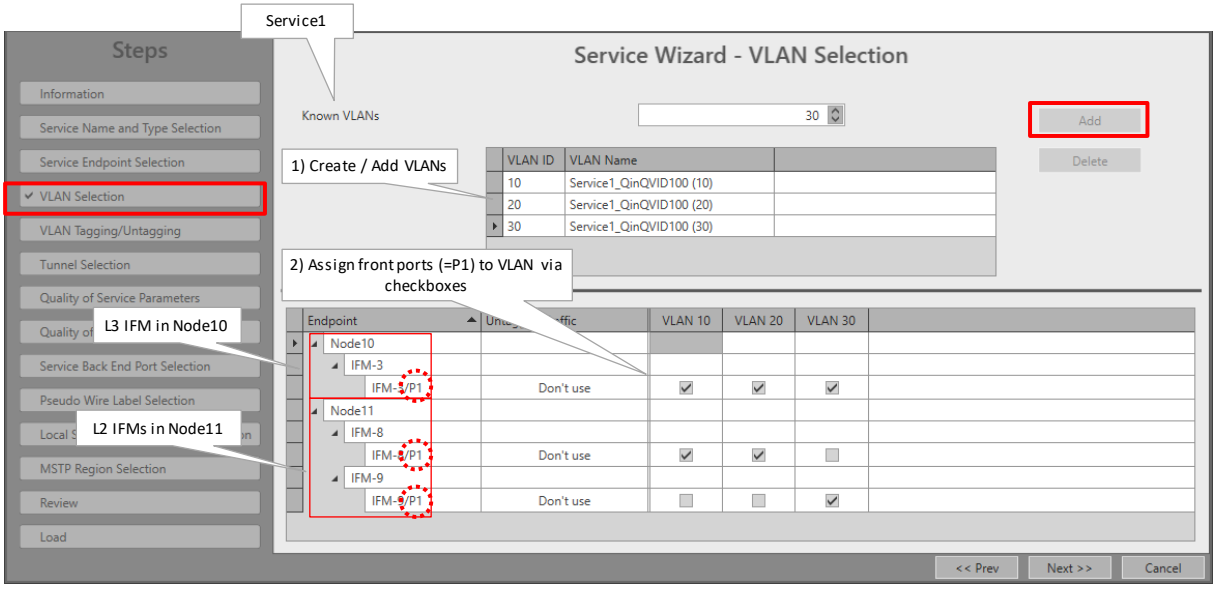

Figure 82 Multi VLAN/QinQ Service1: Add/Create VLANs and Assign Front Ports

2. Create Service2:
   - Service Type:
     - Ethernet Service;
     - VLAN Based, Multi VLAN: QinQ VLAN ID 200.

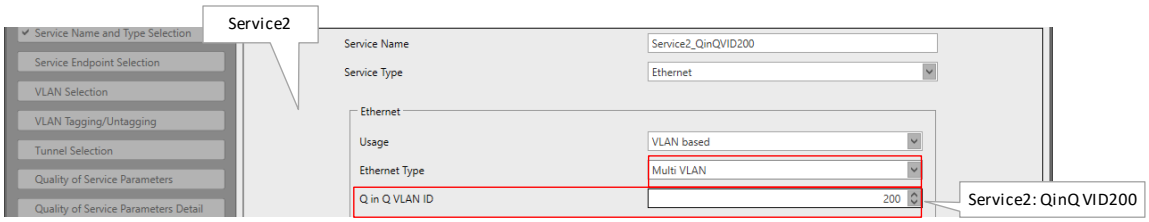

Figure 83 Multi VLAN/QinQ Service2: Start Creation/Define QinQ VLAN

   - Service End Point Selection:
     - Node 10:
       - L3 IFM: front port 2;
     - Node 11:
       - 4-GC-LW IFM: front port 1;
   - VLAN Selection:
     - Create/Add VLANs 40,50;
     - Assign P2 of L3 IFM in Node 10 to VLAN 40,50;
     - For the 4-GC-LW, no assignment must be done, because 4-GC-LW does not support QinQ. Ethernet packets will leave the front port double tagged (QinQ VLAN ID included). A switch that supports QinQ should be connected to the 4-GC-LW ports to process double VLAN tagged packets;

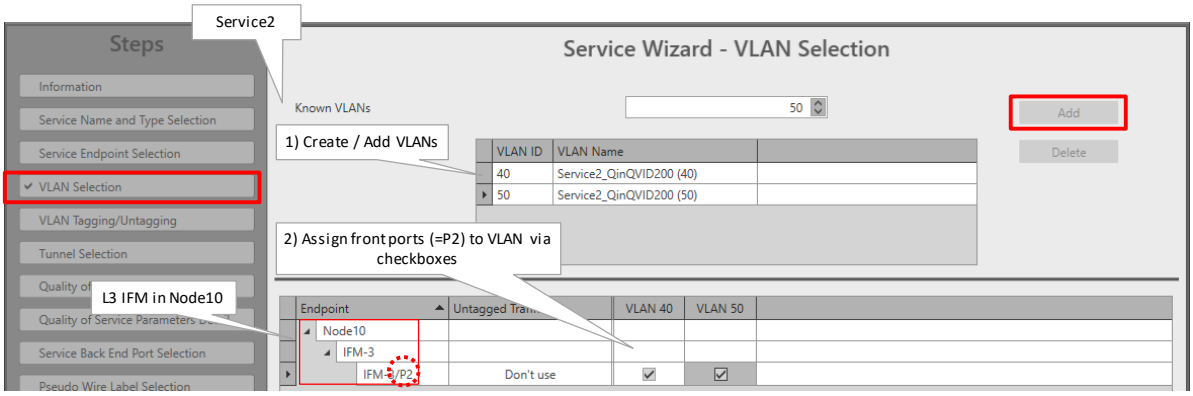

Figure 84 Multi VLAN/QinQ Service2: Add/Create VLANs and Assign Front Ports

3. Resulting created services are shown in the figure below. The listed service shows the QinQ VLAN ID, expanding the service shows the including inner-VLANs.

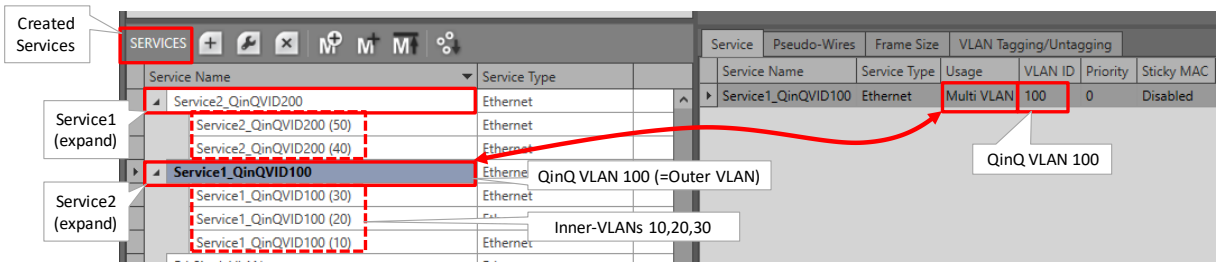

Figure 85 Multi VLAN/QinQ: Resulting Created Services

4.9.3 L3VPN

Prerequisite: The MPLS-TP network must have been created: Nodes, IFMs, WAN links, tunnels. The router node must have installed a L3 IFM. Other nodes must have IFMs with Ethernet LAN ports. A detailed example figure can be found below:

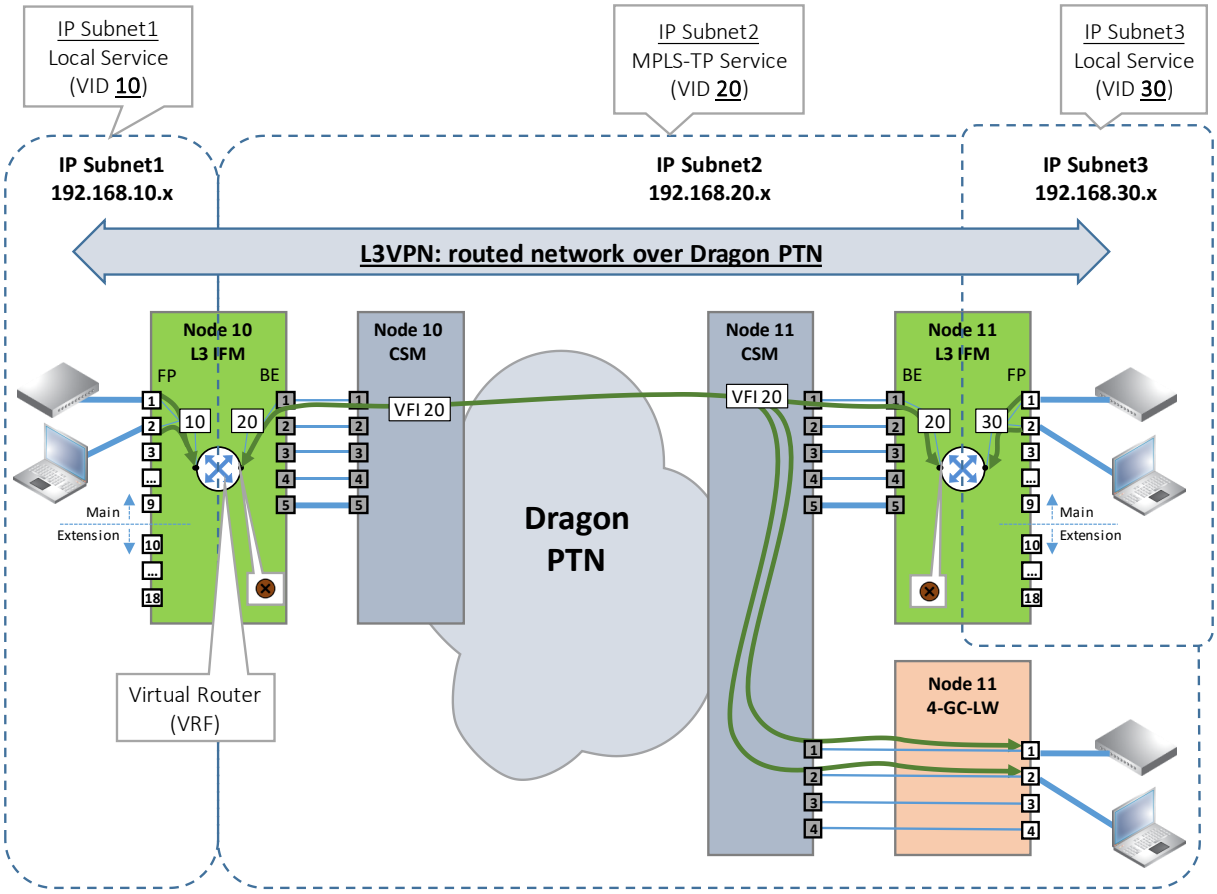

Figure 86 L3VPN Detailed Example

The steps below show the most important points of attention when creating this L3VPN example. Other L3VPN cases need similar configurations.

1. Create Local Service (IP Subnet1):
   - Service Type:
     - Ethernet Service;
     - VLAN Based, Single VLAN: VLAN ID 10, Local Service checked. Note: A normal VLAN based service (Local Service = unchecked) can be used as well, but is less easy to modify later on (e.g. add extra VRF due to VRRP etc...);
   - End Point Selection:
     - Node 10:
       - L3 IFM: front port 1 + port 2;
2. Create MPLS-TP service (IP Subnet2):
   - Service Type:
     - Ethernet Service;
     - VLAN Based: VLAN ID 20, Local Service unchecked;
   - End Point Selection:
     - Node 10: VRF port only on L3 IFM. This service has no LAN or front ports in this node, as a result only the VRF port ⊗ must be selected;
     - Node 11:
       - L3 IFM: VRF port only. This service has no LAN or front ports in this IFM, as a result only the VRF port ⊗ must be selected;

- 4-GC-LW: front port 1 + port 2;

- Back End Ports Selection on L3 IFM:
  - Node 10: BE1 (=default) is OK, any other port is also OK depending on your bandwidth customization;
  - Node 11: BE1 (=default) is OK, any other port is also OK depending on your bandwidth customization;

3. Create Local Service (IP Subnet3):
   - Service Type:
     - Ethernet Service;
     - VLAN Based, Single VLAN: VLAN ID 30, Local Service checked.

4. Create Virtual Router (VRF) in Node 10, interconnect IP Subnet1 and 2:
   - Protocols: Layer 3: Virtual Router (see §5.9 for all Virtual Router configuration details). Find below the most important steps for this example.
     - Creation:
       - Interface Selection: Node 10;
       - Port Selection: None;
       - Service Selection: Select both the IP Subnet1 Local Service and the IP Subnet2 MPLS-TP service to interconnect both IP Subnets via the Virtual Router;

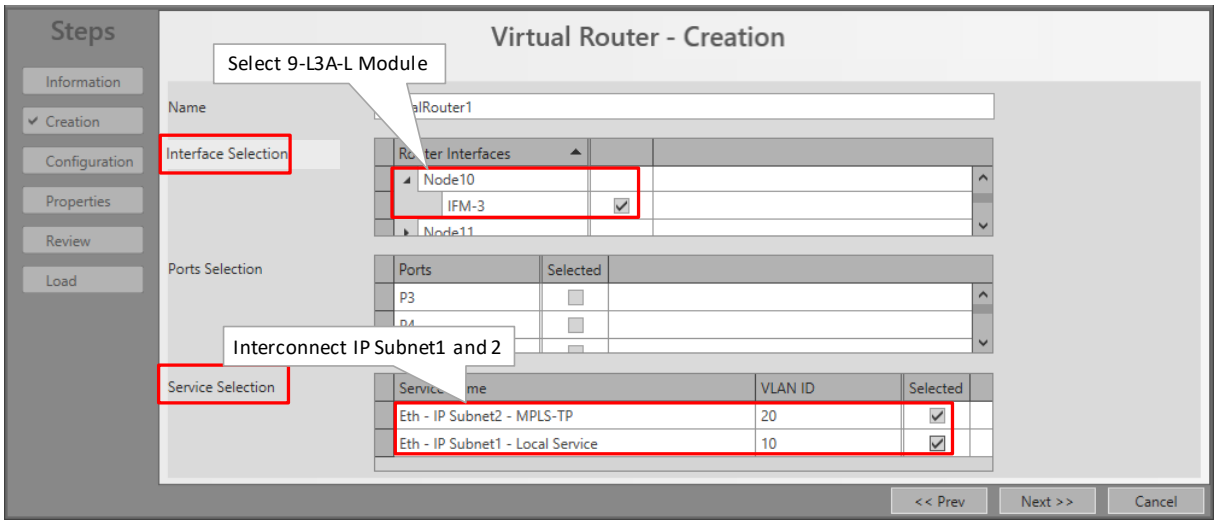

Figure 87 Interconnect IP Subnet1 and 2

- Configuration: Assign IP addresses to both IP Subnet1 and 2:

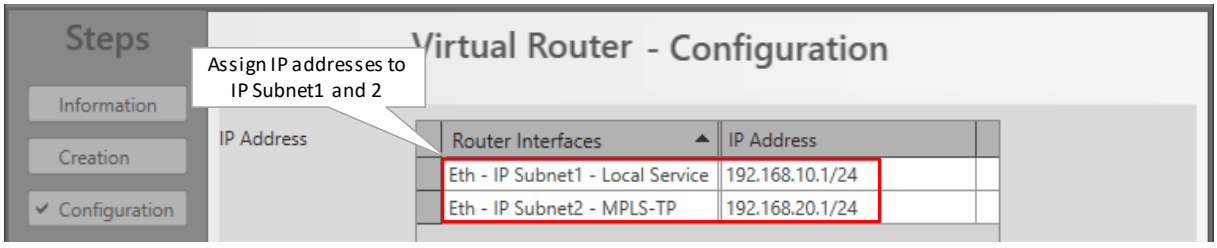

Figure 88 Assign IP Addresses to IP Subnet1 and 2

5. Create Virtual Router (VRF) in Node 11, interconnect IP Subnet2 and 3:

- Protocols: Layer 3: Virtual Router (see §5.9 for all Virtual Router configuration details). Find below the most important steps for this example.
  - Creation:
    - Module Selection: Node 11;
    - Port Selection: None;
    - Service Selection: Select both the IP Subnet3 Local Service and the IP Subnet2 MPLS-TP service to interconnect both IP Subnets via the Virtual Router;

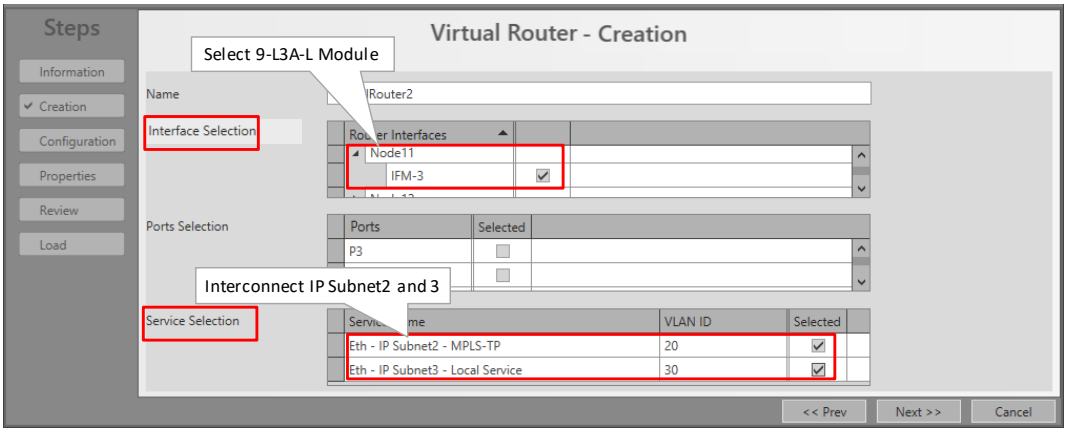

Figure 89 Interconnect IP Subnet2 and 3

- Configuration: Assign IP addresses to both IP Subnet2 and 3:

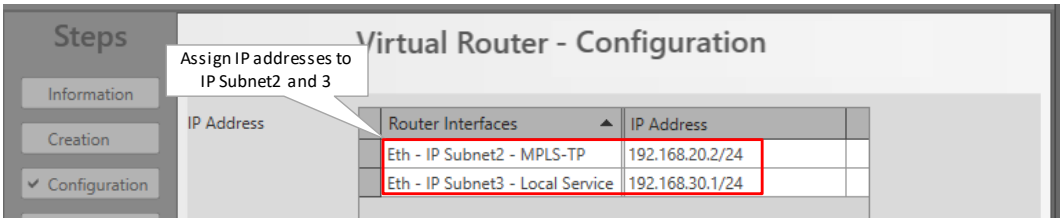

Figure 90 Assign IP Addresses to IP Subnet2 and 3

6. (Optional, not in this example) Create VRRP if you have configured two Virtual Routers and they have to be redundant (see §5.10);
7. Configure Routing if you have at least 2 virtual routers: For a small amount of virtual routers (e.g. 2), you could choose to configure Static Routing (see §5.8) or a dynamic routing protocol OSPF (see §5.7). For more than 2 routers, it is advised to use OSPF. In this example, we configure OSPF.

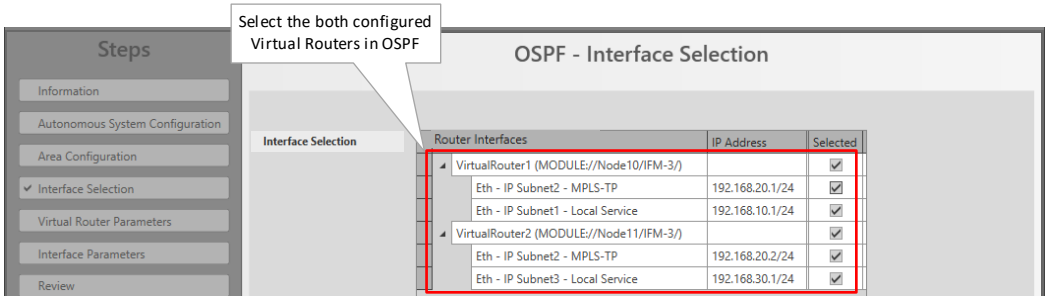

Figure 91 Configure OSP: Select Both Virtual Routers

5. PROTOCOLS

5.1 General

Via Dashboard → (Configuration) Protocols, it is possible to configure protocols or interaction with them. Which protocols and features are supported on which IFMs can be found in support matrix in Ref. [2Net] in Table 1. Protocols are available in the following categories:

- Protocol Interaction:
  - Backbone Isolation Guard (see §5.2)
  - MRP (see §5.2)
- Layer 2:
  - IGMP Snooping (see §5.3)
  - MSTP (see §5.4)
- Layer 3:
  - IGMP (see §5.5)
  - PIM (see §5.6)
  - OSPF (see §5.7)
  - Static Routing (see §5.8)
  - Virtual Router, VRF (see §5.9)
  - VRRP (see §5.10)
  - DHCP Relay (see §5.11)
- Security:
  - IP ACL (see §5.12)
  - MAC ACL (see §5.13)
- Other
  - Voice Protocol (see Ref. [2Leg] in Table 1)

NOTE: If protocol monitoring info or live data is available, it can be monitored via Dashboard → (Monitoring) Protocols which results in the 'Protocols Monitor tile'. In the right table section, it is possible to refresh, export CSV data and to filter data.

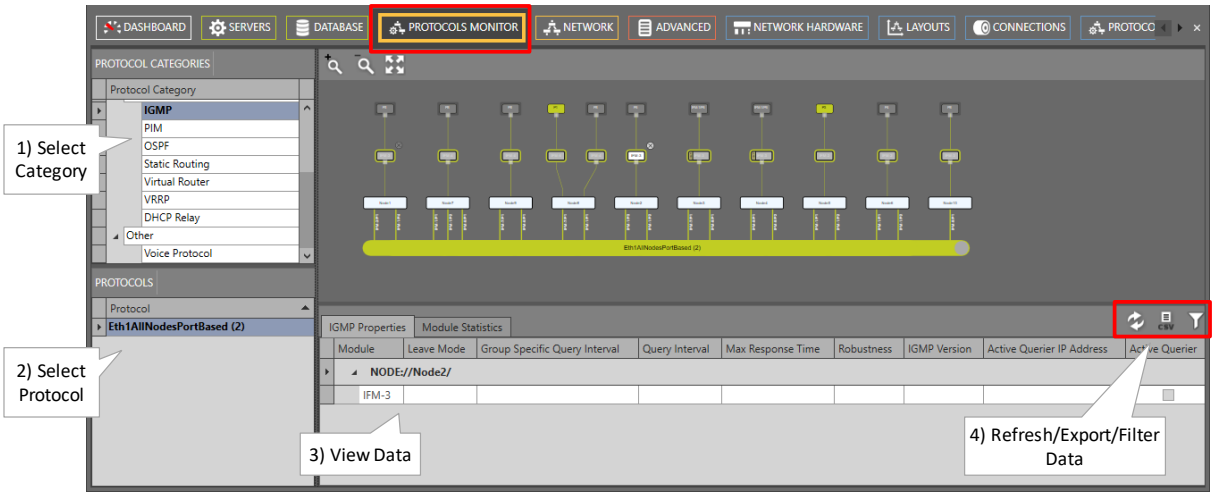

Figure 92 Protocol Monitoring / Protocols Monitor

5.2 Protocol Interaction: MRP (=Media Redundancy Protocol)

5.2.1 General

The MRP is a protocol (IEC 62439-2) especially designed for industrial applications which need a predictable fail-over time. This protocol can only be used in a ring-topology network and makes sure that the ring network stays loop-free. The ring ports are Ethernet ports on an IFM. See support matrix in Ref. [2Net] in Table 1 to find out which IFMs support MRP. MRP does in ring networks what spanning tree does in meshed networks but with much faster convergence times.

- MRP runs in a ring of MRP-compatible access switches connected to two Dragon PTN nodes via a 'Monitored Link' to close the ring. The two Dragon PTN nodes have MRP activated;
- The ring has one selected MR Manager (MRM) and a number of MR Clients (MRC). The two Dragon PTN nodes act as MRC;
- MRP logically blocks one of its uplink ports, to prevent a layer2 loop;
- When the access ring is broken (cable break or device down) the MRM will detect it and open its blocked uplink port;
- The convergence time depends on the access switches and the network configuration;
- Some Hirschmann devices support MRP;

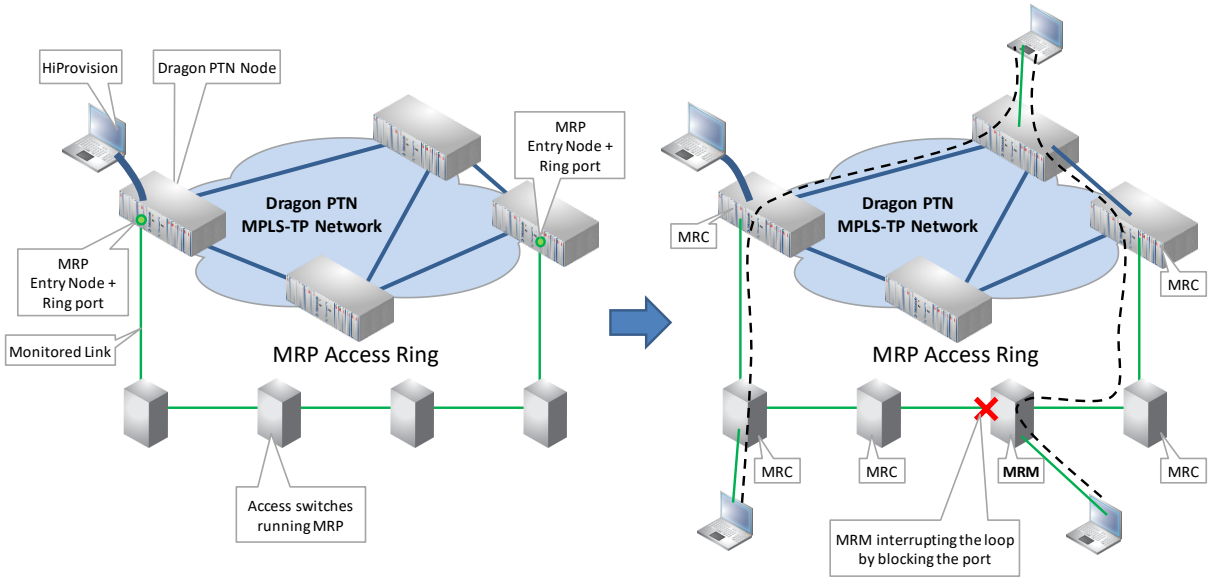

Figure 93 MRP: General Example

CAUTION:
- When connecting an Hirschmann devices ring to Dragon PTN, make sure to use an Ethernet service in a protected tunnel (see tunnel creation in Ref. [2Net] in Table 1) between the two Dragon PTN-Hirschmann device connection points. This results in a faster Dragon PTN-Hirschmann topology recovery when a link fails in the Dragon PTN part. Also unnecessary temporary broadcast storms will be avoided when a link recovers in the Dragon PTN part.
- Performance between the HiProvision server and the Hirschmann devices can be improved via 'ARP Reduction', see Ref. [2Mgt] in Table 1.

5.2.2 Prerequisite

- At least one Monitored Link and some Ethernet services, either VLAN and/or port based, must have been created in HiProvision. More info on 'Monitored Link' in Ref. [2Mgt] in Table 1. The MRP Access ring must be connected in the 'Monitored Link';
- For VLAN-based data services, an extra MRP-service has to be provisioned for each MRP-ring, and with at least priority 2. The VLAN-based MRP services must have exact 2 ring ports;
- If external devices have been configured (=not required) in the monitored links, then they have to be external devices with base type 'Hirschmann' (see external device types in Ref. [2Mgt] in Table 1). Each Hirschmann device requires a Hirschmann Device voucher in the license pack (see vouchers in Ref. [2Mgt] in Table 1). Creating these devices gives a better visual overview in the network drawing, but is not a requirement to configure MRP. The MRP frames of the Hirschmann devices must be VLAN tagged. When using port based services, the VLAN tag must be unique per MRP ring;
- A tunnel different from point-to-point must be used;
- Topology: an MRP service must at least go over a 'logical ring' or 'point-to-multipoint' tunnel. If there is a 'sub ring' tunnel in between, the MRP service must be connected up to the 'logical ring, see example figure below. The MRP service can maximum go over one 'logical ring'.

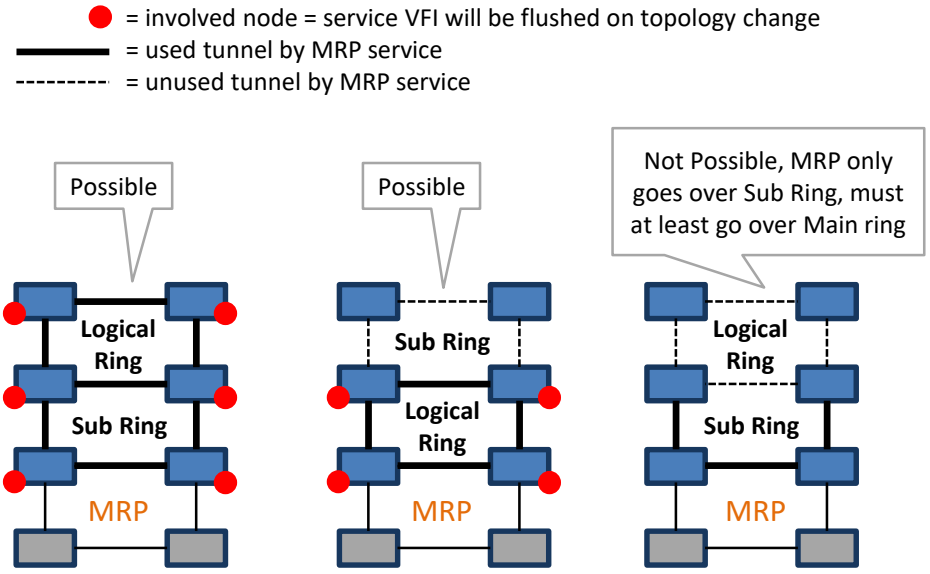

Figure 94 Involved Node: Flush VFI

NOTE: It is advised to use VLAN based services when configuring MRP;

5.2.3 Configuration

Go via Dashboard → (Configuration) Protocols → Protocol Categories → Protocol Interaction → MRP → (Protocols) +. The MRP wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next >>;
- Select Ports:
  - Name: fill out an MRP instance name;
  - Available Port Combinations: each line shows two ports, configured in a 'monitored link', which can be used as MRP ring ports. Select one line or port combination to which the MRP access ring will be connected. Each 'port combination' can have maximum one MRP instance configured. The selected combination is either part of a VLAN Based or Port based service, not both together. By selecting the port combination, you decide as well whether you are going to work VLAN based or Port based. The Next >> button is only active if an unused 'port combination' is selected.
    - When to use a Port based / VLAN based service?
      - Port Based: use such a service when all traffic (MRP protocol and real data) in the service should be treated with the same priority and quality of service;
      - VLAN Based: use such a service when both the MRP protocol and real data should have their own priority, quality of service and bandwidth;
      - Within one node, multiple MRP instances are possible provided that they all run in the same service mode, either port based or VLAN based;

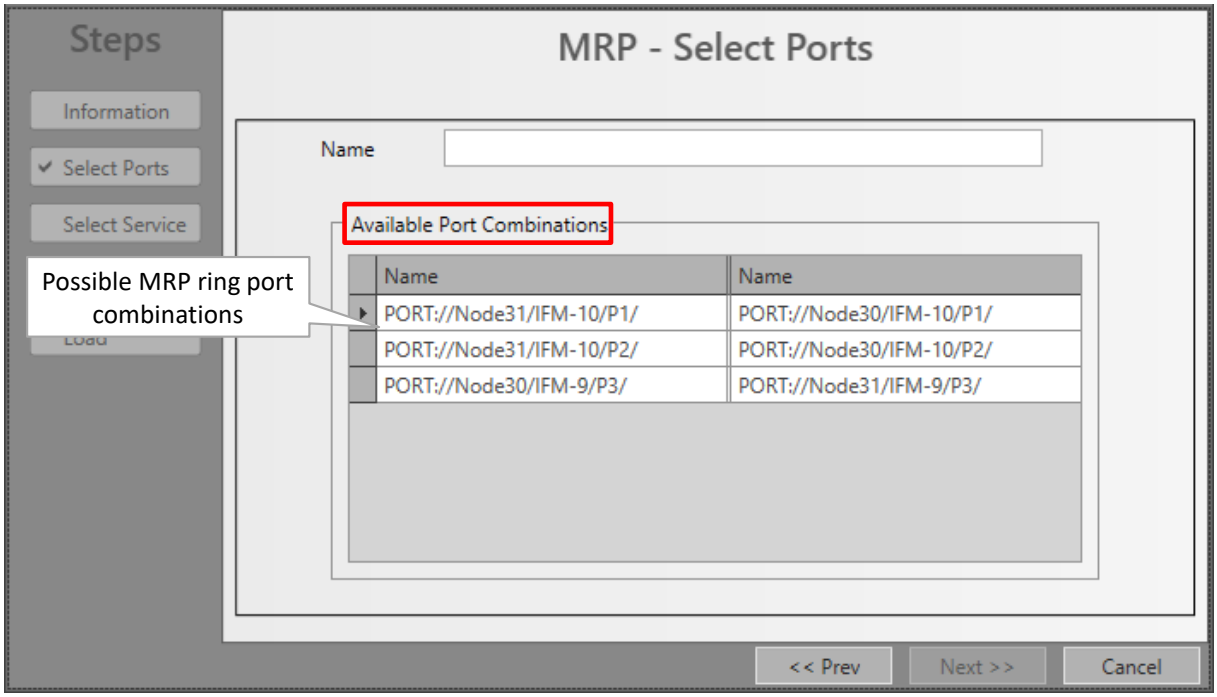

Figure 95 MRP: Select Ports

- Select Service:
  - Your port combination belongs to a **VLAN based service**: both the MRP protocol and the real data will be transported in their own VLAN based service, each having their own priority, quality of service, bandwidth. All tunnels used by the MRP services must be entirely part of the tunnels used by its involved data services.
    - Select MRP Service (to transport the MRP protocol): shows VLAN based Ethernet services that have only configured the selected ring port combination (=exact 2

ports) from previous screen and additionally have at least priority 2. Select one of these services to transport the MRP protocol which has MRP VLAN tagged packets;

- Name: Name of the VLAN Based service used for the MRP protocol;
- VLAN ID: VLAN ID for the VLAN Based service, this VLAN ID must match the VLAN ID of the MRP frames;

- Involved Data Services (only informational, to transport the real data): This list shows the VLAN based services, that can be used to transport the real data, and that share the same selected port combination as the services in 'Select MRP Service'. In addition, these services have more ports configured than just the 2 ring ports. The VFIs of these services will be flushed as well when a topology change occurs in the MRP ring.

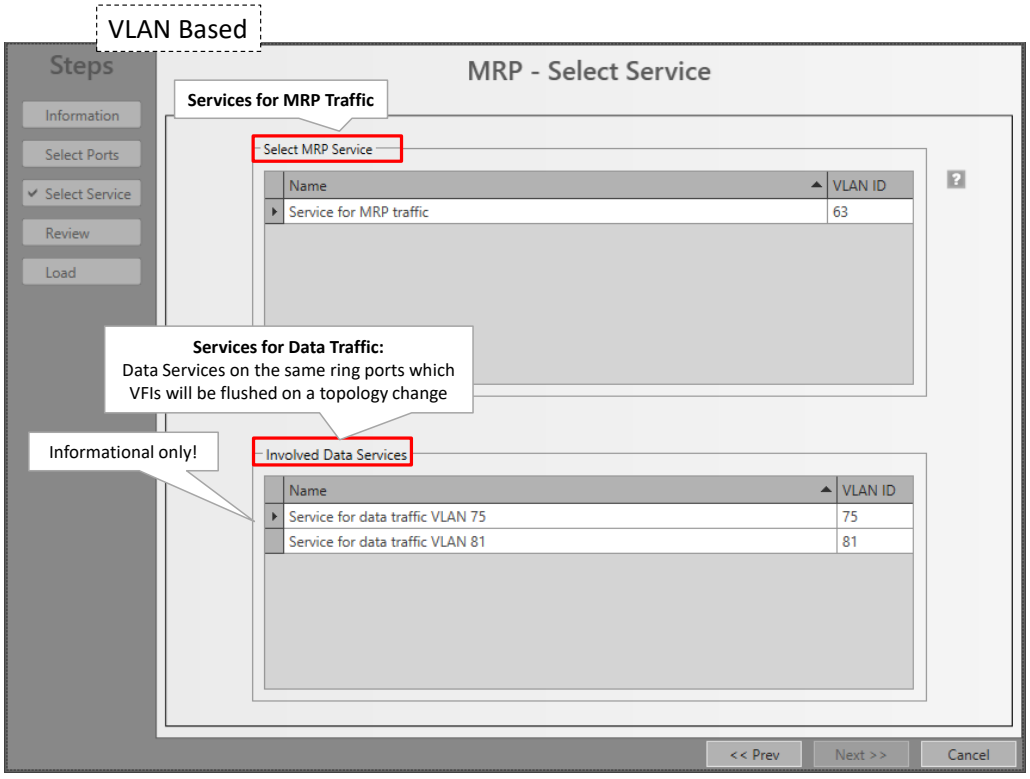

Figure 96 MRP: VLAN Based Services: Select MRP + Data Service

- Your port combination belongs to **Port based service**: both the MRP protocol and the real data will be transported in the same port based service, having one common priority, quality of service and bandwidth for the entire service.

  - Select MRP Service (to transport the MRP protocol + data): shows port based Ethernet services that have configured at least 3 ports: the selected ring port combination (= exact 2 ports) from previous screen + 1 or more other data port(s). Select one of these services to transport the MRP protocol + real data;
    - VLAN ID: this VLAN ID must match the VLAN ID of the MRP frames;
    - Name: Name of the Port Based service used for the MRP protocol + real data;

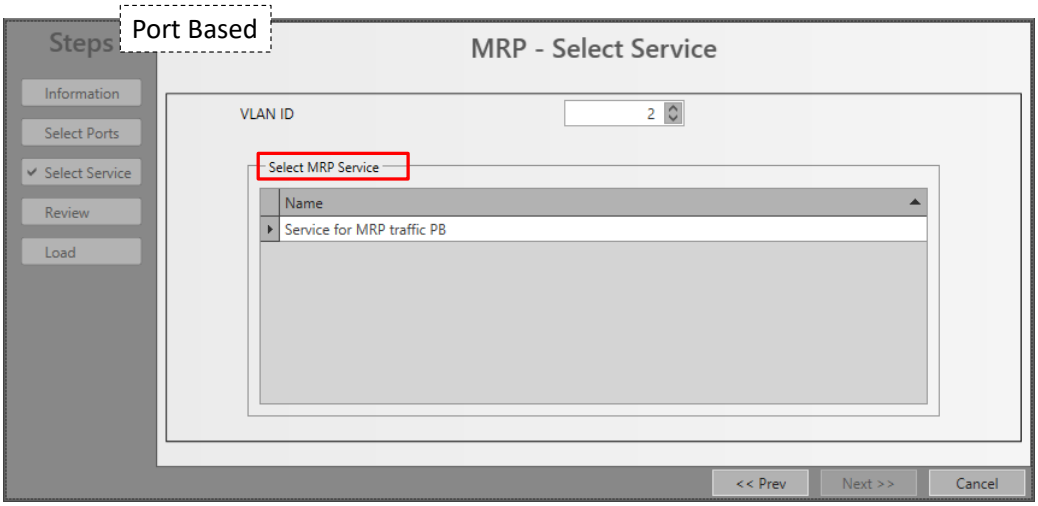

Figure 97 MRP: Port Based Services: Select Service

- Review: Involved Nodes: A data service node that is also positioned in the used tunnels of the MRP service. When a topology change occurs in the MRP ring, the VFIs of the involved services in that involved node will be flushed (see also Figure 94). This topology change has no impact on the other VFIs in that node. If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info;

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols and via Dashboard → (Monitoring) Network → Protocols Tab.

5.2.4 Monitoring

MRP Monitoring info is available via the two options below. Refresh/export/filter buttons are provided in the bottom-right corner of the screens below.

- Dashboard → (Monitoring) Network Tile → Protocols Tab. Example in figures below;
- Dashboard → (Monitoring) Protocols Tile. Example in figures below.

The major difference between the two views is that the Network tile shows a network layout with the used service not visible whereas the Protocols tile shows a more schematic layout with the used service visible. Both views show the same ring properties in the MRP table section.

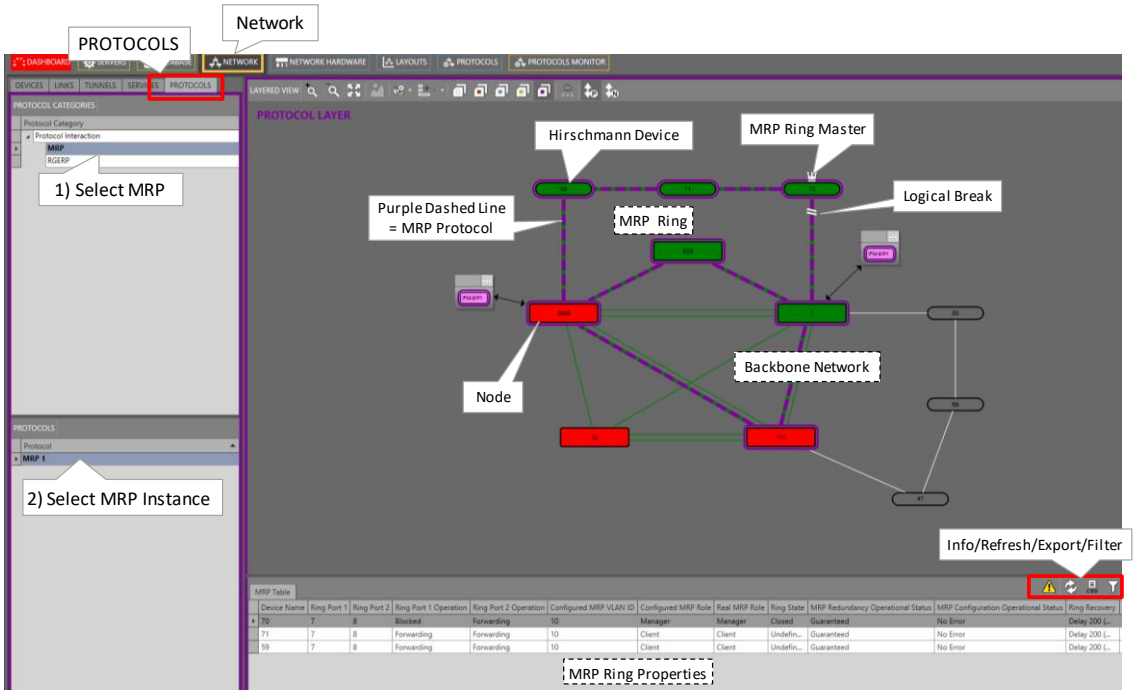

Figure 98 Dashboard → (Monitoring) Network Tile → Protocols Tab

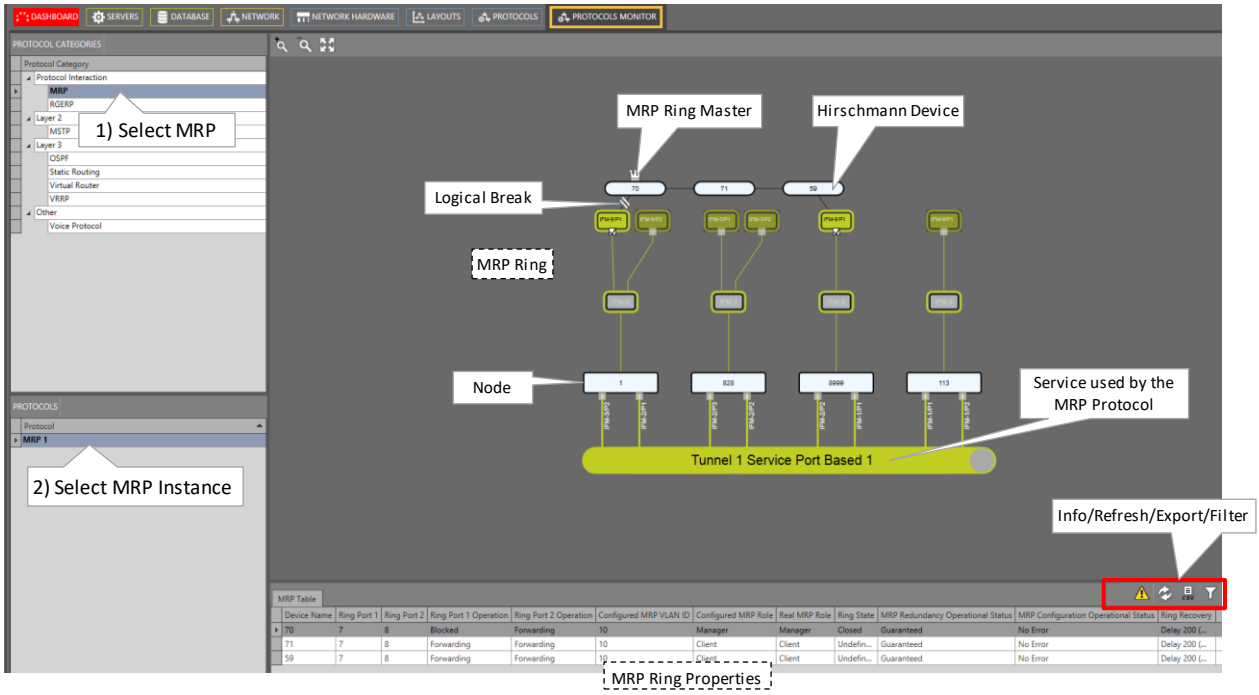

Figure 99 Dashboard → (Monitoring) Protocols Tile

The major difference between the two views is that the Network tile shows a network layout with the used service not visible whereas the Protocols tile shows a more schematic layout with the used service visible. Both views show the same ring properties in the MRP table section.

5.3 Layer 2: IGMP Snooping

5.3.1 General

IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. Via IFMs that support IGMP snooping (see Ref. [2Net] in Table 1), it provides the Dragon PTN nodes with a mechanism to diminish multicast traffic from links that do not contain a multicast listener (an IGMP client). The Dragon PTN node will, by default, flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). Multicast can cause unnecessary load on host devices by requiring them to process packets they have not solicited.

CAUTION: IGMP Snooping is MAC based on L2 IFMs and IP based on L3 IFMs.

IGMP snooping allows the Dragon PTN node to only forward multicast traffic to the ports that have solicited them. IGMP snooping is not a protocol but a layer 2 optimization for the layer 3 IGMP protocol (see §5.5). IGMP Snooping takes place internally on IFMs that support it. Snooping is therefore especially useful for bandwidth-intensive IP multicast applications such as IPTV.

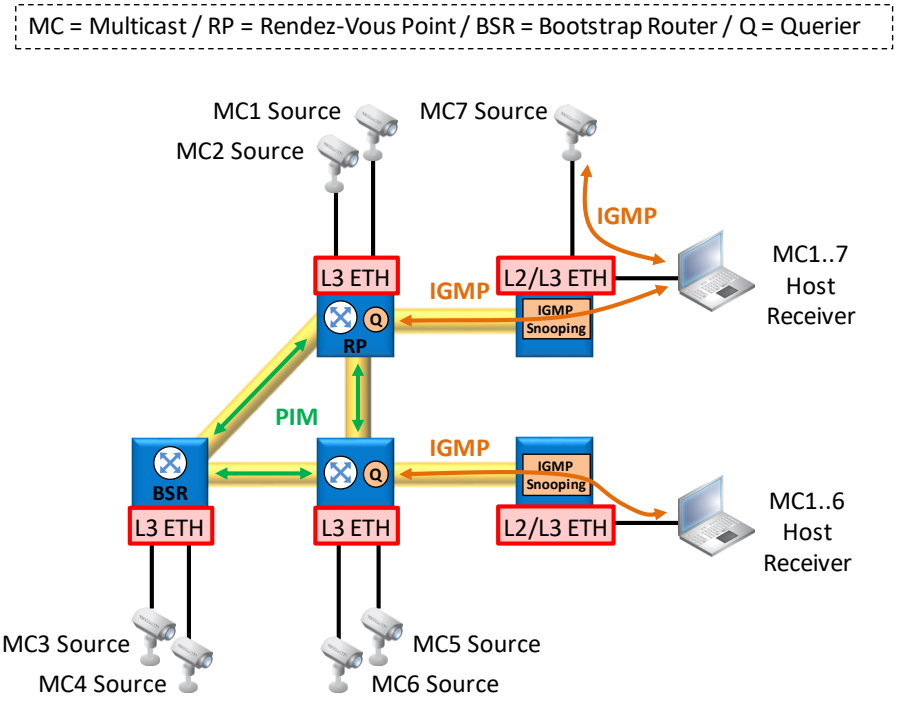

Figure 100 PIM/IGMP/IGMP Snooping Overview

5.3.2 Common IGMP Snooping Properties

Some common IGMP snooping properties can be changed in HiProvision. Just select the 'IGMP Snooping' line in the protocols list and click the protocol options button. Fill out or modify the desired properties and click the Close button. These property values are common and valid for all IGMP snooping instances.

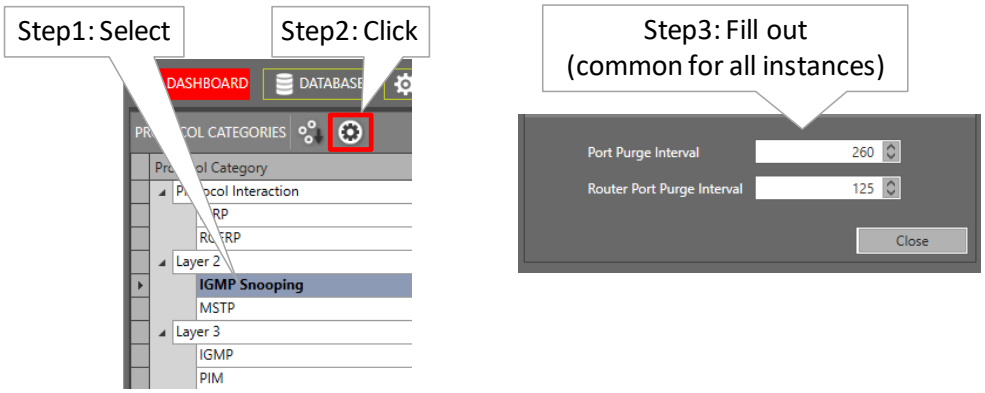

Figure 101 IGMP Snooping Common Properties

- Port Purge Interval: (default value = 260 s, min. 130 s, max. 1225 s) The expiry of the Port Purge Timer on the port for a particular multicast group results in the port being removed from the forwarding list of the corresponding multicast entry in the Multicast Forwarding Table.
- Router Port Purge Interval: (default value = 125 s, min. 60 s, max. 600 s) Sets the IGMP snooping router port purge time-out after which the port gets deleted if no IGMP router control packets are received.

5.3.3 Prerequisite

An Ethernet service must contain at least one of the following IFMs that support IGMP snooping, see Ref. [2Net] in Table 1.

5.3.4 Configuration

Go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 2 → IGMP Snooping → (Protocols)  . The IGMP Snooping wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Service Selection: A list of Ethernet services is shown, select a service and click Next>>.
- Module/Port Configuration:
  - Module level:
    - Module: All the IFM modules that support IGMP snooping, part of the selected Ethernet service, are shown in this table;
    - Enabled:
      - checked (=default): IGMP snooping is enabled on this IFM;
      - unchecked: IGMP snooping is disabled on this IFM.
    - Snooping Mode:
      - Passive: All IGMP messages (membership queries, membership reports, leave group, group specific queries...) through this IFM always pass without interaction of this IFM itself. It is advised to use this setting when IGMP snooping, IGMP and PIM are configured together in this IFM.
    - Report Process:

- Non Router Ports (=default): Non (Multicast) Router ports are ports where no IGMP Queries are received on. Normally end-devices are connected to these ports. Setting this value makes sure that Reports are only processed from non-router ports;
- All Ports: Reports are processed from all IFM ports, either router or non router ports.

- Report Forward :
  - Router Ports (=default): (Multicast) Router ports are ports where IGMP Queries are received on. Setting this value makes sure that Reports are only forwarded to router ports;
  - All Ports: Reports are forwarded to all IFM ports, either router or non router ports;
  - Non Edge Ports: Ports not connected to an end-station or application.

- Port level:
  - Port: All the ports from IFMs that support IGMP snooping and part of the selected Ethernet service, are shown in this table;
  - Blocked Port:
    - unchecked (=default): Multicast traffic is allowed on this port;
    - checked: No multicast traffic is outputted on this port;
  - Static Router Port:
    - unchecked (=default): If no queries are received on this port, this port will be a non-router port. If after some time queries are received on this port and Router Port Learning is enabled, this port will turn into a dynamically learnt router port;
    - checked: This port is assigned as a fixed (or static) router port, this router port is always there, and is not the result of a dynamic learning process;
  - Router Port Learning Disabled:
    - unchecked (=default): Router port learning is enabled. It means that this port can become a dynamic learnt router port when queries are received on this port and this port is not yet a static router port;
    - checked: Router port learning is disabled. This port is not allowed to become a dynamic router port;
  - Leave Mode (*):
    - Normal (=default): the port will not be removed immediately from the multicast group when a leave message is detected on that port. First some group specific queries are sent on that port, and if no membership report is received within a time interval on that port for that multicast group, the port will be removed from that multicast group;
    - Fast: the port will be removed immediately from the multicast group when a leave message is detected on that port;

  NOTE: (*) Leave mode will be configured for all the VLANs since it's a port based property.

- Review: If OK, click Finish. The configuration load manager will be invoked.

- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.3.5 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols.

5.4 Layer 2: MSTP (=Multiple Spanning Tree Protocol)

5.4.1 General

MSTP originally defined in IEEE 802.1s and later merged into IEEE 802.1Q-2003, defines an extension to RSTP to further develop the usefulness of VLANs. This MSTP instance configures a separate Spanning Tree for all VLANs included in this instance and blocks all but one of the possible alternate paths within each Spanning Tree.

If there is only one VLAN in the network, single (traditional) STP works appropriately. If the network contains more than one VLAN, the logical network configured by single STP would work, but it is possible to make better use of the alternate paths available by using an alternate spanning tree for different VLANs or groups of VLANs. More than one VLAN can be assigned to one MST instance. Multiple MST regions can be operational, each having its own MSTP instances. The IST (MSTP) instance monitors the entire Region, the CST (MSTP) instance monitors the links between the regions.

MSTP in a port based service is supported network wide whereas MSTP in a VLAN based service is supported only locally (not over the L2/L3 IFM back end ports). CAUTION: using MSTP with a VLAN based service over the back end ports could cause loops!

MSTP is fully supported on L2/L3 IFMs and partially (=transparent MSTP) on the other Ethernet IFMs, see also §4.2 and 'Support Matrix' in Ref. [2Net] in Table 1. On L2/L3 IFMs, there is always a default MSTP running (not visible in HiProvision).

When configuring MSTP (=transparent) only on Ethernet IFMs (4-GC-LW, ...) and not on L2/L3 IFMs, it is advised to create an IST only, in a dummy region.

NOTE: A basic port blocking (without MSTP) can be achieved via the BPDU Guard feature on ports that support this feature: see support matrix in Ref. [2Net] in Table 1 and §9.3.

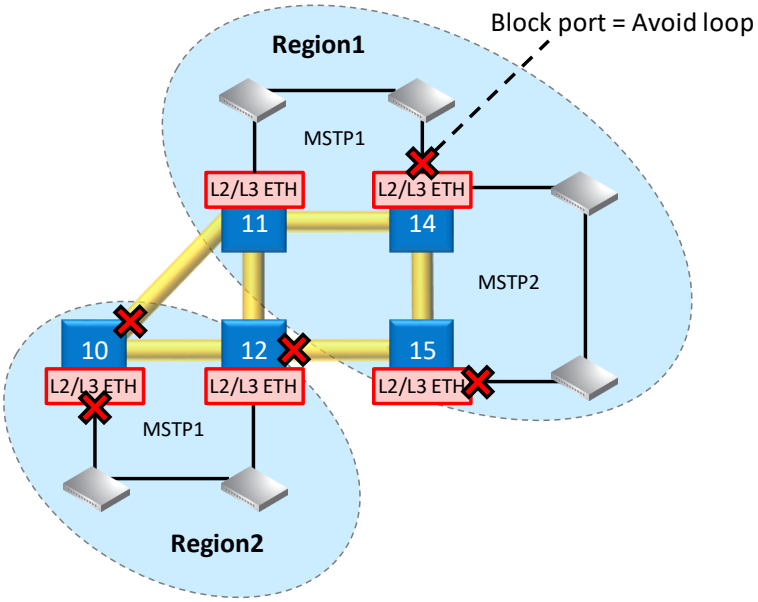

Figure 102 Region/MSTP Overview

5.4.2 Prerequisite

- A Port based Ethernet service must contain at least one of the IFMs in support matrix in Ref. [2Net] in Table 1 that support the Ethernet Service.
- A VLAN based Ethernet service must contain only L2/L3 IFMs.
- For L2/L3 IFMs, make sure that each IFM that must participate in the same MSTP Region, has exactly the same VLANs configured.

5.4.3 Configuration

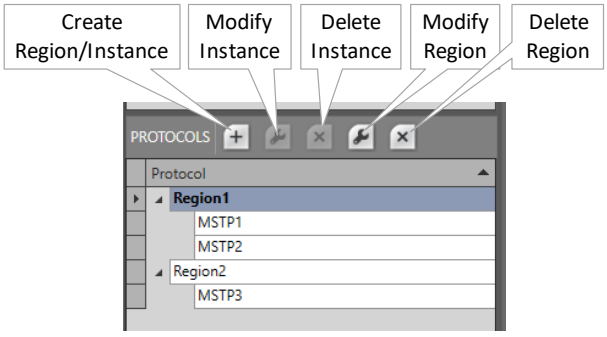

Figure 103 Region/MSTP Actions

- (see §a) Active MSTP: L2/L3 IFMs Included;
- (see §b) Transparent MSTP: Only LAN/WAN Ethernet IFMs (4-GC-LW, …) Included;

a. Active MSTP: L2/L3 IFMs Included

Go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 2 → MSTP → (Protocols)  . The MSTP wizard opens. The list below summarizes every page in the wizard.

- Information: Click Next>>;
- Region Selection:

- Instance Name: fill out an MSTP instance name;
- IST: Is the default or root spanning tree (instance 0) that runs within a Region. The IST always contains and monitors all the ports that are configured in the entire Region. It also monitors the VLANs that are not already monitored by another instance.
  - unchecked (=default): This MSTP instance will not be the IST in the Region. If the first instance that you create in the Region is not the IST, then an IST instance will be created automatically in addition. There must always be an IST before any another instance can be created;
  - checked: This MSTP instance will be the IST;

  NOTE: Best practice: when creating the first MSTP instance in a region, it is best practice to check the IST checkbox.

  NOTE: an IST monitors an entire Region whereas a CST monitors the links between Regions. Both can be viewed via Dashboard → (Monitoring) Protocols;

  NOTE: When configuring MSTP (=transparent) only on Ethernet LAN/WAN IFMs (4-GC-LW, ...) and not on L2/L3 IFMs, it is advised to create an IST only, in a dummy region.

- Select Region: Select a Region in which the MSTP instance must operate. If the list is still empty or you want to create and select a new Region, select <Create New Region> instead;
- Region Name: Name of the selected Region or fill out a new Region name when a new Region is being created;
- Revision (default = 0, range[0...65535]): identifies the Revision of the current MSTP instance. Fill out a new value when a new Region is being created;

- Region Configuration (only when creating the Region with first MSTP instance):
  - Service: Select a service. Best practice is to select all services that use the L2/L3 IFMs on which you want to configure MSTP;
  - Ports: If the service has been selected, a list with devices is shown. Expand the devices by clicking in front of the device row. Select one or more L2/L3 IFMs or Ethernet ports before clicking the Next >> button. NOTE: a L2/L3 IFM can only belong to one Region;

- VLAN Selection (only when a L2/L3 IFM is involved and adding an MSTP instance, different from the IST, to an existing Region):
  - Instance ID (default=1; range[1..64]): Fill out an instance ID for this MSTP instance. Within the same Region, this instance ID must be unique;
  - VLANs: Select one or more VLANs on which this spanning tree instance must run. This VLAN list is a result of the selected service during Region creation;

  NOTE: Make sure that each IFM that participates in the same MSTP instance must have exactly the same VLANs;

- MSTP Configuration (only when a L2/L3 IFM is involved):
  - Instance Properties (L2/L3 IFMs):
    - Device Name: Indicates the device or IFM on which MSTP is going to be configured;

- Bridge Priority (default=32768, range[0, 4096, 8192, ..., 61440]): Select the bridge priority which must be an increment of 4096. 0 = lowest value = highest priority. The **Bridge Priority** together with the **Bridge MAC Address** determines the **Bridge ID** or the identity of the device. The Bridge ID is used by MSTP to determine the root bridge of the network. The device with the lowest Bridge ID becomes the root bridge. If all the devices have the same priority, the device with the lowest MAC address will then become the root bridge. If you want a device force to be the root bridge, make sure it has the lowest priority value of all devices in the network.

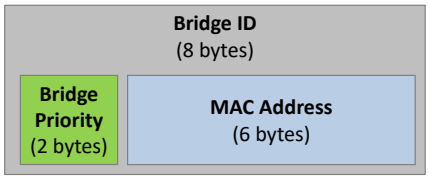

Figure 104 Bridge ID = Bridge Priority & MAC Address

- Port Properties (L2/L3 IFMs):

NOTE: '*' = indicates a shared property over all instances, see Table 12;

NOTE: Some MSTP port settings can be greyed out or read-only when:

- A back end port is part of a VLAN based service;
- The port is already in use by another protection protocol, e.g. MRP…

- Path Cost (default=see table below; range[1...200000000]): The value can be modified. The Path Cost represents the “cost” and influences the root port selection when going from this port to the root bridge (direction = upstream). If there are multiple paths from this node towards the root bridge, the path or port with the lowest path cost will be the selected path for data transmittal (=forwarding state), the other paths will be blocked via blocking the connected ports.

NOTE: The back end port Path Cost is only calculated if the corresponding port based service is selected in the Region configuration.

Table 11 Default Path Cost

Type	Default Path Cost
Front Port: 40G	200
Front Port: 10G	2000
Front Port: 1G	20000
Front Port: 100MB	200000
Front Port: 10MB	2000000
Back End Port: <bandwidth in kbps>	2000000 / <bandwidth in kbps>

- Priority (default=128; range[0, 16, 32, ..., 240]): Select the port priority value, using increments of 16. 0 = lowest value = highest priority, 240 = highest value = lowest priority. The priority can be used to influence the root port selection of the downstream switch.

- Link Type (*): Indicate by selecting the Link Type whether your link interconnects more than 2 devices:
  - Point to Point (=default for access ports → e.g. IFM-3/**P**3): The connected link is a point-to-point link to just one other device. Point-to-point links make the node reconfigure quicker (e.g. after a loop reconfiguration) than a shared link;
  - Shared (=default for L2/L3 IFM **B**ack **E**nd ports → e.g. IFM-3/**BE**4): The link is a shared segment and must be used when more than two devices must be interconnected. Shared links make the node reconfigure slower (e.g. after a loop reconfiguration) than a Point to Point link. E.g. when your shared link only interconnects two devices, the Link Type could better be set to Point to Point.
  - Auto: The device will auto detect the Link Type for MSTP;

NOTE: (*) below Indicates a shared port property. It means that this property value is shared with all other MSTP instances.

- Port Fast (*):
  - Checked (=default for L2/L3 IFM access ports): immediately puts the port into STP forwarding mode upon linkup. The MSTP listening and learning phase is omitted. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode. This setting is meant for access ports, which are connected to a single server/ workstation/ end device where no loops are expected;
  - Unchecked (=default for L2/L3 IFM back end ports): puts the port first into STP blocking mode upon linkup. The MSTP listening and learning phase is active. Based upon these results, MSTP will keep the port in blocking mode or set it in in forwarding mode. Ports that are connected to switches or routers must use this setting.

NOTE: When a monitored link is created on an access port, the Port Fast is by default unchecked or disabled on this port unless the port is part of an MRP protocol, then the default port settings of the MRP are configured;

- Root Guard (*): This setting manages the root bridge protection;
  - Checked: prevents this port to become a root port. As a result, it prevents the switch connected to this port to become the root bridge;
  - Unchecked (=default): allows this port to become a root port. As a result, it allows the switch connected to it to become the root bridge;
- BPDU Guard (*) (BPDU = Bridge Protocol Data Unit);
  - Checked (=default for access ports): The BPDU guard is enabled. If a BPDU packet enters the port, the node will detect this immediately and block the port. The port can be re-enabled by setting the Admin Status of the port properties Down and click Apply (and Load) and setting it back Up and click Apply (and Load). Checking BPDU Guard makes sure that external devices connected to this port are not able to influence the MSTP topology within the network borders resulting in a more stable network;
  - Unchecked (=default for L2/L3 IFM Back End ports): The BPDU guard is disabled. The port will not be disabled when a BPDU packet enters the port. A connected

device to this port is able to participate in the MSTP protocol and topology within the network. CAUTION: As a result, this connected device can also become the root bridge (see also Root Guard parameter for more information) of the network, resulting in possible major changes within the MSTP network or domain;

NOTE: When a monitored link is created on an access port, the BPDU Guard is by default unchecked or disabled on this port unless the port is part of an MRP protocol, then the default port settings of the MRP are configured;

- BPDU Transmit (*):
  - Checked (=default): The Dragon PTN node can transmit (MSTP) BPDU packets on this port.
  - Unchecked: The Dragon PTN node does not transmit (MSTP) BPDU packets on this port.
- BPDU Receive (*):
  - Checked (=default): The Dragon PTN node can receive and process (MSTP) BPDU packets on this port.
  - Unchecked: The Dragon PTN node ignores incoming (MSTP) BPDU packets on this port;
- MSTP Disabled (*):
  - Checked: disable MSTP on this port;
  - Unchecked (=default): do not disable MSTP on this port;
- Hello Time (*) (sec) (default=2 seconds; range[1,2]): This value configures the interval between the MSTP hello packets (= BPDUs), sent by the root bridge. Each MSTP node expects to receive a BPDU packet within three hello times.

- Review: If OK, click Finish. If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

- The resulting Regions with their MSTP instances are listed in the Protocols list, see below:

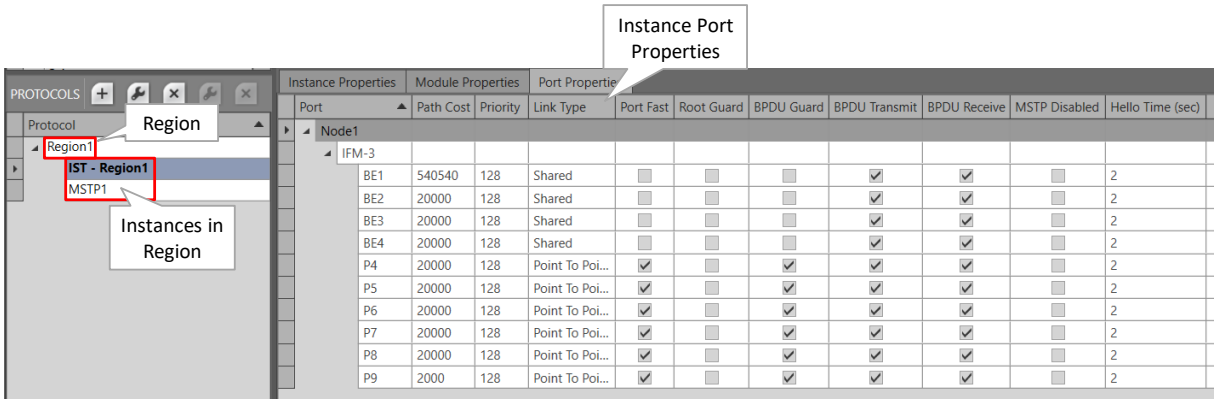

Figure 105 Created Regions/MSTP Instances

Table 12 Parameter Dependency

Level	Parameter	MSTi Dependent (*)
Device	Bridge Priority	setting per MSTi
Port	Path Cost	setting per MSTi
Port	Priority	setting per MSTi
Port	Link Type	common setting shared over all MSTis in the Region
Port	Port Fast	common setting shared over all MSTis in the Region
Port	Root Guard	common setting shared over all MSTis in the Region
Port	BPDU Guard	common setting shared over all MSTis in the Region
Port	BPDU Transmit	common setting shared over all MSTis in the Region
Port	BPDU Receive	common setting shared over all MSTis in the Region
Port	MSTP Disabled	common setting shared over all MSTis in the Region
Port	Hello Time (sec)	common setting shared over all MSTis in the Region

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols.

b. Transparent MSTP: Only LAN/WAN Ethernet IFMs (4-GC-LW, …) Included

Best practice: Create only a dummy IST in a dummy Region, and no other MSTP instances.

Go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 2 → MSTP → (Protocols)  . The MSTP wizard opens.

- Information: Click Next>>;
- Region Selection:
  - Fill out an instance name;
  - Check the IST checkbox;
  - Create New Region (Name, Revision);
  - Click Next>>;
- Region Configuration:

- Select the services that use your LAN/WAN Ethernet IFMs;
- Select the ports that must participate;

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

- The resulting Regions with their MSTP instances are listed in the Protocols list.

NOTE: Parameters in this wizard are explained in more detail in §a.

5.4.4 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols.

5.5 Layer 3: IGMP

5.5.1 General

IGMP is a protocol used between hosts and neighboring local multicast routers. This protocol manages multicast-group memberships. If a host wants to receive a multicast stream, the host must be member of the multicast group. IGMP can be used to manage/distribute multicast streaming video and allows more efficient use of the available bandwidth and resources.

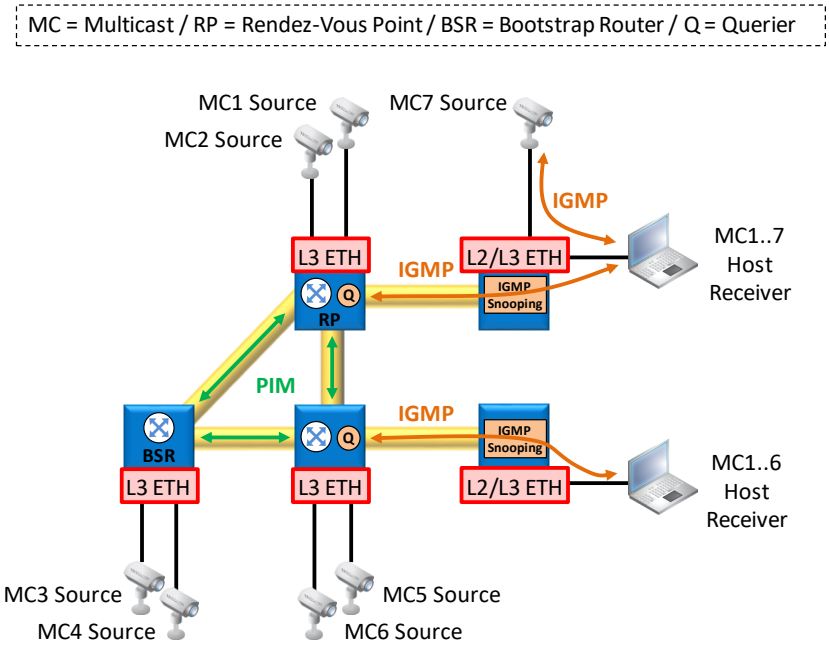

Figure 106 PIM/IGMP/IGMP Snooping Overview

Some definitions:

- Membership queries: The local multicast router sends out membership queries to check if any of the hosts is interested in an available multicast stream. The host can join a multicast group via sending membership reports to the membership querier.
- Join a multicast-group: The hosts or clients request membership for a specific multicast stream (=multicast-group with specific multicast IP address) via membership reports.
- Leave a multicast-group: The hosts can leave (or disconnect from) a multicast stream via a time-out (IGMPv1), Leave group requests (IGMPv2).

IGMP is VLAN based and runs between the router itself and the VLANs connected to its router interfaces. As a result, if a host that is part of a VLAN joins a multicast stream, all the other members of the VLAN will receive the multicast-stream as well. To prevent this, configure IGMP snooping (see §5.3) on this router interface to make sure that only the stream requester(s) is (are) receiving the stream, and not all the other uninterested members of the VLAN.

Depending on the used IGMP version (V1 or V2), querying/joining/leaving a group may differ. Find an overview in the table below:

Table 13 IGMP Version Dependencies

IGMP Version	Query	Join a Group	Leave a Group
V1	General Query	Membership Report	via time-out mechanism
V2	- General Query - Group Specific Query	Membership Report	via Leave Group messages

5.5.2 Prerequisite

At least one Virtual Router (on L3 IFM) and an Ethernet service must have been created (see §5.9). Make sure that the Ethernet service has been selected in the Virtual Router.

5.5.3 Configuration

In HiProvision, go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → IGMP → (Protocols)  . The IGMP wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Service Selection: Select the service on which IGMP must be configured;
- Virtual Router Selection: Select the Virtual Router(s) on which IGMP must be configured;
- Properties:
  - Leave Mode:
    - Normal (=default): the port will not be removed immediately from the multicast group when a leave message is detected on that port. First some group specific queries are sent on that port, and if no membership report is received within a time

interval on that port for that multicast group, the port will be removed from that multicast group.

- Fast: the port will be removed immediately from the multicast group when a leave message is detected on that port.

- Last Member Query Interval (default=10 s, range[1,...,255] s): Configures the time interval that is used by the L3 IFM to send group specific queries on a its configured IGMP ports.
- Query Interval (default = 125 s, min. range[11,...,65535] s): is the amount of time in seconds between IGMP General Query messages sent by the querier, if this node is the querier.
- Max Response Time (default = 100 '1/10 s'= 10 seconds, range[1,...,255] '1/10 s'): Specifies the period in tenths of a second in which the host is expected to respond to an IGMP query.
- Robustness (default = 2, range[2,...,7]): Configure this parameter to indicate how well your network can recover from lost IGMP packets. If you have a very stable network, the Robustness value will be very low. For less stable networks, the Robustness value must be set higher or high. E.g. if the Robustness value = '3', your network can recover from (robustness-1) IGMP packets = (3-1) = 2 IGMP Packets. Changing the Robustness variable automatically modifies certain IGMP message intervals for IGMPv2. Increasing this value allows for more packet loss but increases the leave latency of the subnetwork.
- IGMP Version: Indicates the used IGMP version: V1, V2 (=default);

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.5.4 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §5.9.4.

5.6 Layer 3: PIM

5.6.1 General

PIM (Protocol-Independent Multicast) is a multicast routing protocol. It is protocol independent because PIM does not have a network topology discovery mechanism like other routing protocols have. PIM uses routing information supplied by other routing protocols. PIM builds up Multicast Distribution Trees for each IP Multicast Group Address. As

a result, data packets from senders to a multicast group reach all receivers that have joined the group via IGMP.

MC = Multicast / RP = Rendez-Vous Point / BSR = Bootstrap Router / Q = Querier

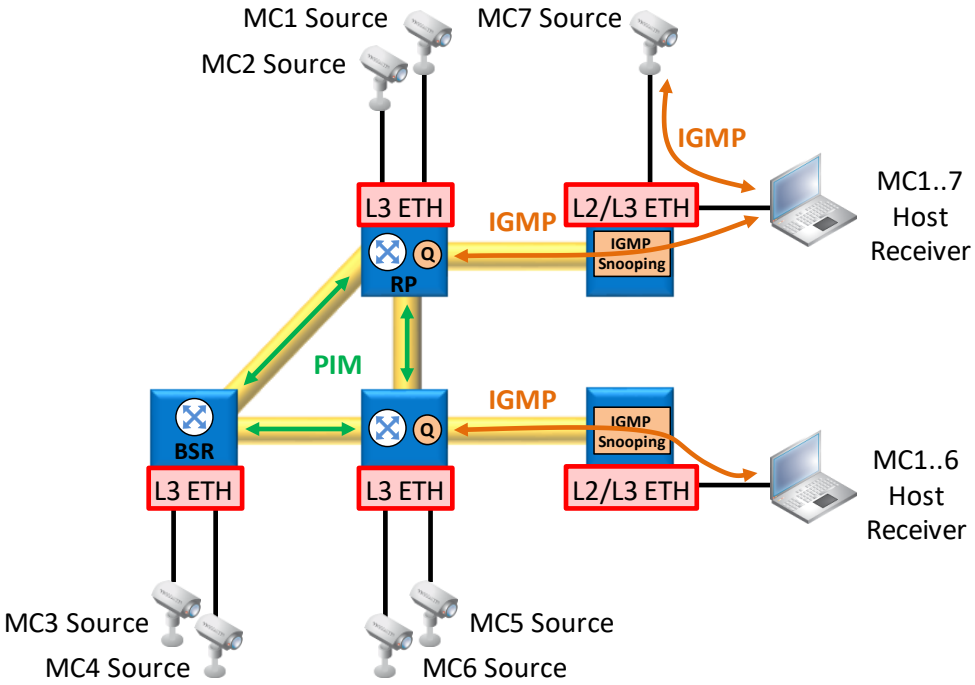

Figure 107 PIM/IGMP/IGMP Snooping Overview

Some definitions:

- First Hop Router (FHR): This is the router that connects the multicast source (e.g. video server) to the PIM network.
- Last Hop Router (LHR): This is the router that connects the multicast receiver or client (=host) to the PIM network.
- Bootstrap Router (BSR): A BSR is a router which is elected amongst BSR candidates. A BSR can be considered as the master of the PIM component within the network. BSR is also a standard-based protocol in PIMv2. The Rendez-Vous Point (RP) candidates (see below) will report their candidacy to the elected BSR. Out of these candidates, the BSR generates multicastgroup-to-RP mappings and distributes these to all the routers in the PIM domain through Bootstrap messages. As a result, each router knows via where it can get a specific multicast stream.
- Rendez-Vous Point (RP):
  - An RP is a router acting as a central multicast stream collector for a specific multicast range. Each new stream that enters the network via the FHR, must first be registered via unicast traffic to one of the available RPs. During registration, the multicast stream is embedded in the unicast traffic.

- If a host wants to receive a multicast stream, it must first join the stream via the LHR that forwards the join message to the RP. Once the LHR receives the stream, it knows the source of the multicast stream. At that point, it is more efficient that the LHR bypasses the RP (for this multicast stream) and communicates directly to the multicast source. As a result, the LHR will send a prune message to the RP and a join message to the multicast source for this multicast stream.

- Designated Router (DR): Using PIM when a host expresses interest in joining a multicast group, it does so using IGMP. For each (sub-) network, a single router is elected to be the DR for the network. When an IGMP message is seen by the DR it then uses PIM to send a message to the RP, for the multicast group.

- Querier: A querier is a router that sends out IGMP group membership queries on a timed interval, to retrieve IGMP membership reports from active members, and to allow updating of the group membership tables. Without a querier, these tables are not created and IGMP/IGMP snooping will not work.

5.6.2 Prerequisite

At least one Virtual Router (on an L3 IFM) and an Ethernet service must have been created (see §5.9).

5.6.3 Configuration

In HiProvision, go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → PIM → (Protocols)  . The PIM wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Creation:
  - Name: Assign a name to the PIM component. A PIM component corresponds to the PIM domain and classifies it as Sparse mode. A PIM domain is defined as an area of the network over which bootstrap messages are forwarded. Typically, a PIM router will be a member of exactly one domain;
  - Component Number (default=1, range[1,..,254]): HiProvision automatically assigns a number to the PIM component;
  - Interface Selection: Select the interfaces from the L3 IFMs that participate in PIM;
- Interface Configuration:
  - Query Interval (default=30 s, range[1,..,18725]s): sets the frequency in seconds at which PIM Hello (=query) messages are transmitted on this interface. The query message informs the presence of a PIM router on this interface to the neighboring PIM routers;
  - Message Interval (default=60 s, range[10,..,600]s): sets the frequency in seconds at which Join messages are transmitted on this interface to keep the receival of a joined multicast stream alive. The same Join message interval must be used on all the PIM routers in the PIM domain. If all the routers do not use the same timer interval, the performance of PIM can be adversely affected;

- DR Priority (default=1, range[1,..,65535]): This value indicates the Designated Router (=DR) priority. This value is used to determine the Designated Router for the link connected to the interface. In the DR election process the highest Priority wins and becomes DR. If the two DR candidates have the same Priority, the highest Router Id (RID) wins.

- Bootstrap Selection: out of the previously selected Virtual Router interfaces, indicate which one must act as BootStrap Router Candidate (BSR-C). Later on, when PIM is up and running in the network, the Bootstrap Router (BSR) will be elected dynamically by means of bootstrap messages and the BSR-C Priority. The highest BSR-C priority wins, and will become the active BSR. The other candidates be-come standby BSRs;
- Bootstrap Configuration:
  - Priority (default=1, range[1,..,255]): The Priority will be used for the BSR election process later on in the network. The highest priority wins.
- Rendez-Vous Point Selection: out of the previously selected Virtual Router interfaces, indicate which one must act as Rendez-Vous Point Candidate (RP-C). Later on, when PIM is up and running in the network, the RP-Cs will advertise themselves to the BSRs;
- Rendez-Vous Point Configuration:
  - Hold-time (default=80, range[3,..,255]): When the router is a RP candidate in the local domain, this field defines the time interval (in seconds) till which the RP candidate advertisement is valid. The Hold-time defines the age for the RP advertisement.
  - Priority (default=192, range[1,..,255]): Indicates the Priority for each RP-C which will be used later on for electing a specific RP for a specific Multicast address group or range. For the same multicast address ranges, the lowest Priority wins and becomes the RP for that multicast address range. The other interfaces become standby RPs.
  - Fill out a Rendez-Vous Point Range for each Rendez-Vous Point:
    - Select the Rendez-Vous Point Line and click the  icon. A new window pops up:
      - Network Address: Fill out a valid multicast address range e.g. 224.100.100.3/24 for which this RP is responsible. Click the Add button to add this address to the ‘Rendez-Vous Point Ranges’ address list. Repeat this step until all the multicast address ranges are configured for this RP. Click OK.
      - See figure below:

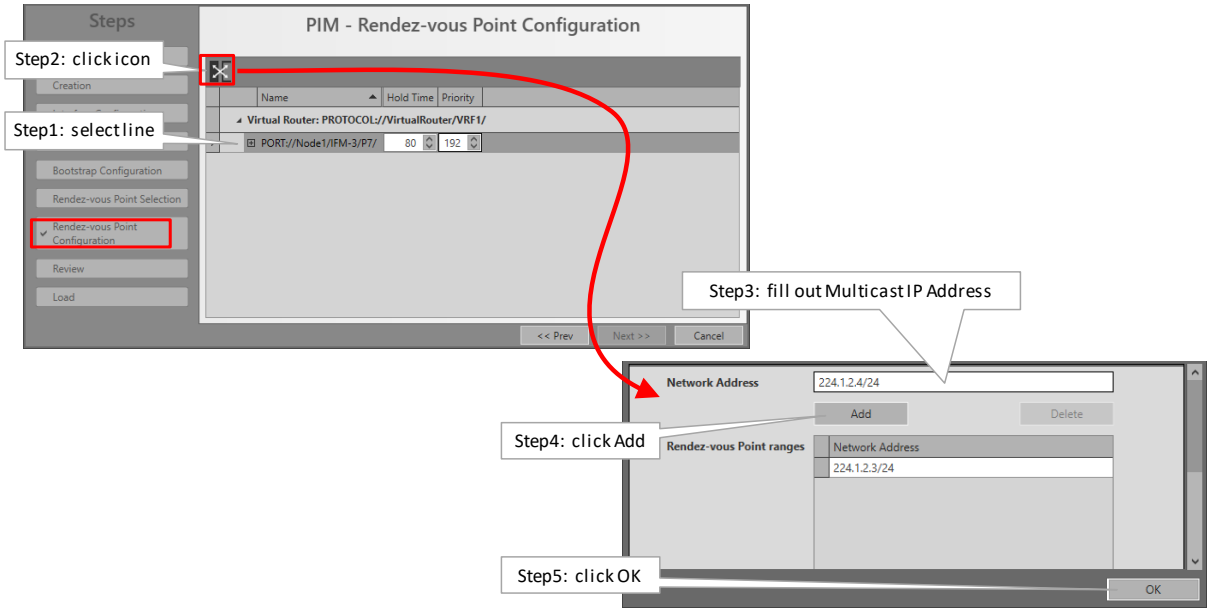

Figure 108 Rendez-Vous Point Configuration

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.6.4 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §5.9.4.

5.7 Layer 3: OSPF (=Open Shortest Path First)

5.7.1 General

OSPF is a dynamic routing protocol for IP networks. A dynamic routing protocol always determines the best possible routing path. For example, determined routes may dynamically change because a specific route becomes less or more preferred than before.

The concept of OSPF is that routers advertise **updates** of their **link states** to neighboring routers. And the neighboring router does the same to its neighboring router and so on…. In other words, each router learns from the other routers based on **link state advertisements** (=LSA). OSPF is a fast protocol because only updates are advertised.

OSPF checks the availability of others routers in the network by sending 'Hello' packets. If the other router does not respond then that router is assumed to be down.

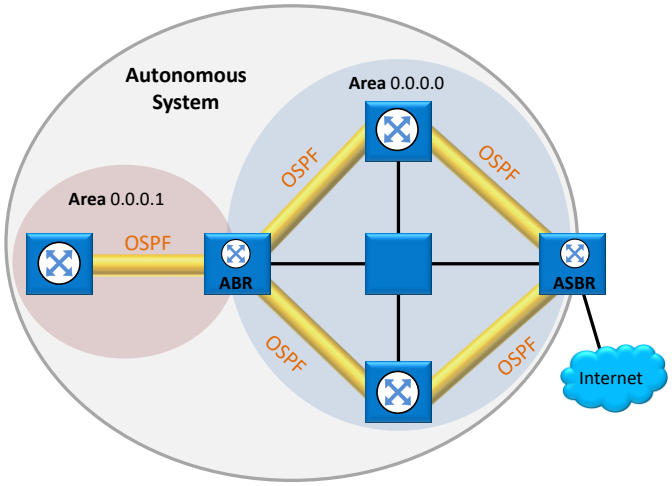

Figure 109 OSPF: General Example

CAUTION: If you want to enable OSPF on a LAG (see §7), configure the LAG in a VLAN. A LAG configured on router ports (L3 IFM) does not support OSPF!

Some definitions:

- Autonomous System (=AS): largest entity within the OSPF routing hierarchy, a logical unit used in OSPF to segment a large network into smaller parts, a collection of networks that share the same OSPF routing instance.
- Area: a group of routers and hosts which is a subset of the entire AS, an AS can be organized in a number of Areas. Each Area has its own routing topology, resulting in reduced routing table sizes and processor load. It also limits the amount of flooding of link state updates over the entire network.
  - Backbone Area (=Area 0.0.0.0): it is the central Area that distributes routing information between other Areas, there is only one backbone Area within an AS.
  - Stub Area: is only connected to the Backbone Area. Stub Areas only receive routes from within the AS (not from outside the AS).
  - Totally Stub Area: is only connected to the Backbone Area. Totally Stub Areas do not advertise routes from outside its Area. The only route that is advertised is the default route from the ABR (=Area Border Router) to the rest of the routers in the Totally Stub Area. The Totally Stub Area communicates with the rest of the network via this default route.
- Area Border Router (ABR): an ABR connects one or more Stub or Totally Stub Areas to the Backbone Area. An ABR has multiple copies of the link-state database in memory, one copy for each area to which that ABR is connected. Routers in areas use ABR as next hop to access external addresses. ABR forwards packets to the ASBR that announces the external addresses.
- Autonomous System Boundary Router (ASBR): an ASBR must be part of the Backbone Area and connects the AS to another non OSPF AS. An ASBR can interconnect different routing protocols and exchange routing information between them. ASBRs typically run an exterior

routing protocol or use static routes or a mix of them. An ASBR is used to distribute routes received from other, external Autonomous Systems throughout its own OSPF AS.

- Designated Router (DR): in order to limit the exchange of information between adjacent routers on a segment, one Designated Router (=DR) and backup Designated Router (=BDR) will be elected by OSPF amongst all these routers. The DR is the central agent of all these adjacent routers. If a router wants to exchange link state advertisements (=LSA) on the segment, it will only send this info to the DR. The DR will distribute this info to other routers on the segment. The DR election process is done via sending Hello packets on each segment. More info on the DR election process can be found in the description of the Priority parameter, see further.

5.7.2 Prerequisite

At least one Virtual Router must have been created (see §5.9).

5.7.3 Configuration

In HiProvision, go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → OSPF → (Protocols)  . The OSPF wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Autonomous System Configuration:
  - Select Autonomous System: Select an AS in which the OSPF instance must operate. If the list is still empty or you want to create and select a new AS, select <Create New Autonomous System> instead;
  - Autonomous System Name: fill out an AS name when creating a new AS;
- Area Configuration:
  - Area Name: Fill out an Area name;
  - Area Type:
    - Backbone (=default): This is the master area within the OSPF network and has always Area Number '0.0.0.0'. A Backbone Area must always be created in the OSPF network. All other Stub or Totally Stub Areas will always be directly connected to this Backbone Area. A Backbone Area can receive routes from outside and inside the AS. If Dragon PTN is part of a bigger routed network, with already a Backbone area available outside Dragon PTN:
      - Creating a Backbone Area in Dragon PTN is not required;
      - Creating a Backbone Area in Dragon PTN will merge this Dragon PTN Backbone Area with the external backbone area into one bigger backbone area;
    - Stub: This Area is only connected to the Backbone Area and only receives routes from inside the AS. It also receives the default route from the ABR.
    - Totally Stub: This Area is only connected to the Backbone Area and only receives the default route (which gives access to the rest of the network) from the Backbone Area.

- Area Number: is a unique number in the Autonomous System that identifies the Area. This number is 0.0.0.0 for the Backbone Area and is different from 0.0.0.0 for any other Area.
- Compatible RFC 1583: Indicates how the 'Summary Route' route costs are calculated;
  - Checked (=default): The costs are calculated according standard RFC 1583 and is based on the lowest cost (=best cost) among the summarized routes. E.g. if the costs of three individual routes are 50, 100 and 200, the cost of the summarized route will be 50;
  - Unchecked: The costs are based on the highest cost (=worst cost) among the summarized routes. E.g. if the costs of three individual routes are 50, 100 and 200, the cost of the summarized route will be 200;

  NOTE: Make sure to set Compatible RFC 1583 identically in the entire AS to minimize the chance of routing loops.

- Interface Selection:
  - Select the OSPF interfaces on the virtual routers that will be part of the configured Area (maximum 32 OSPF interfaces per virtual router, maximum 128 OSPF interfaces per L3 IFM). A Virtual Router can only be part of one OSPF AS, thus it cannot be split over two or more Autonomous Systems, even if the Virtual Router would be configured as an ASBR.
- Virtual Router Parameters:

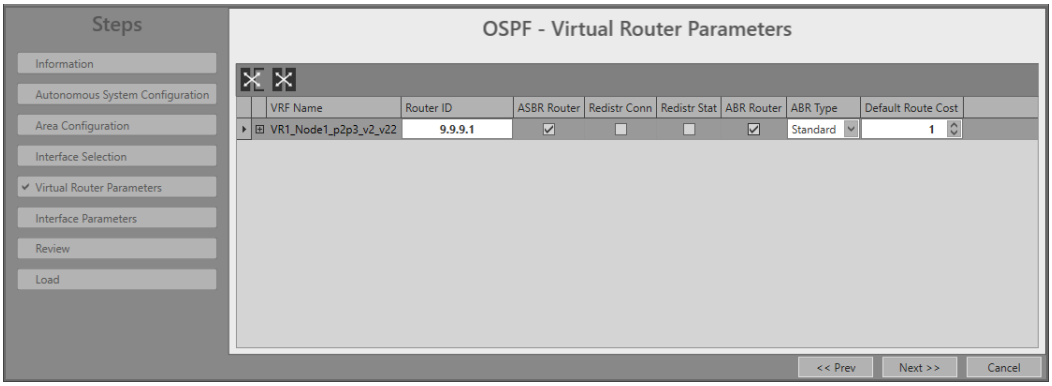

Figure 110 OSPF: Virtual Router Parameters

- VRF Name: indicates the name of the Virtual Router. Select the Virtual Router row in which you want to change configurations.
- Router ID: This is a unique number that identifies the OSPF router. It is pre-filled out with the IP address of the first listed router port of that Virtual Router. The Router ID field can be adapted but it has to be unique throughout the AS;
- ASBR Router: Check this checkbox if this Virtual Router must be configured as an ASBR. It can only be checked if it concerns a Virtual Router in the Backbone Area (0.0.0.0). For other areas, ASBR cannot be configured. External Route (=route from outside the AS) redistribution can only be performed by an ASBR. The fields listed below can be configured for an ASBR:

- Redistr Conn:
  - Unchecked (=default): disables the redistribution of the networks directly connected to the virtual router;
  - Checked: enables the redistribution of the networks directly connected to the virtual router. If loopback interfaces (see §8) are used on this virtual router, make sure to check this checkbox or make the loopback interface a 'passive' interface (best practice is setting it to 'passive', see further). This is necessary for PIM (see §5.6), to make sure that this loopback interface is known within the entire PIM component;
- Redistr Stat:
  - Unchecked (=default): disables route redistribution of the static routes into OSPF;
  - Checked: enables route redistribution of the static routes into OSPF;
- Summarize External Routes: Click the button to create summarized external routes reports. Such a summary report is an aggregation of external routes or external Network Addresses (outside the AS). These summary reports will be distributed within the Areas. In the figure below, fill out the Network Address and click the Add button. E.g. if you have external addresses 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, 10.0.205.0/24, it could be summarized (or added) in the Summarize External Routes list as 10.0.0.0/16. Entries can be removed by selecting the row first and clicking the Delete button.

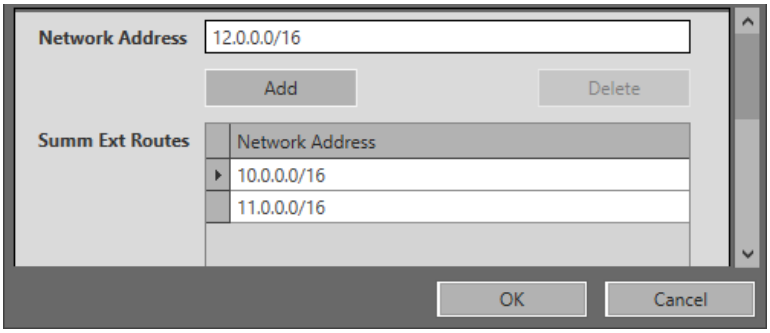

Figure 111 OSPF: Summarize External Routes

- ABR Router: Check this checkbox if this Virtual Router must be configured as an ABR. It can always be configured in any Area. The fields below can be configured for an ABR:
  - ABR Type: Standard (=default), Cisco or IBM (refer to RFC 3509);
  - Default Route Cost: (default = 1, range [0,..,30]) fill out this parameter to assign a cost to the default route which is propagated into this Stub or Totally Stub Area;
  - Summarize Inter-area Routes: Click the button to create Inter-area summary reports. Such a summary report is an aggregation of Inter-area routes (outside the Area, but inside the AS). These summary reports will be distributed within the Area, never outside the Area. In the figure below, fill out the Network Address and click the Add button. E.g. if you have external addresses 15.0.1.0/24, 15.0.2.0/24, 15.0.3.0/24, 15.0.205.0/24, it could be summarized (or added) in the Summarize Inter-area Routes list as 15.0.0.0/16. Entries can be removed by selecting the row first and clicking the Delete button.

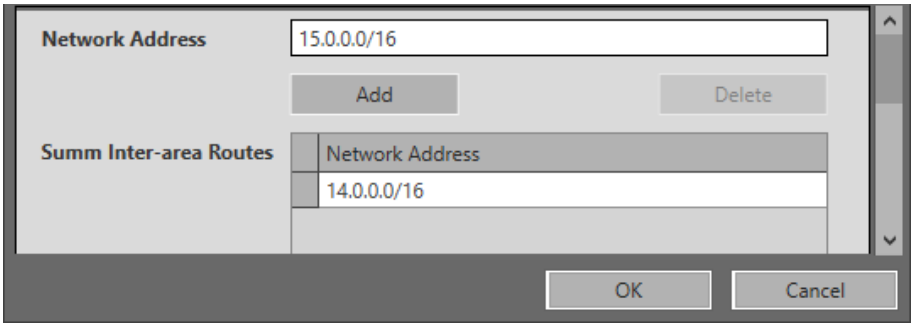

Figure 112 OSPF: Summarize Inter-Area Routes

- Interface Parameters:

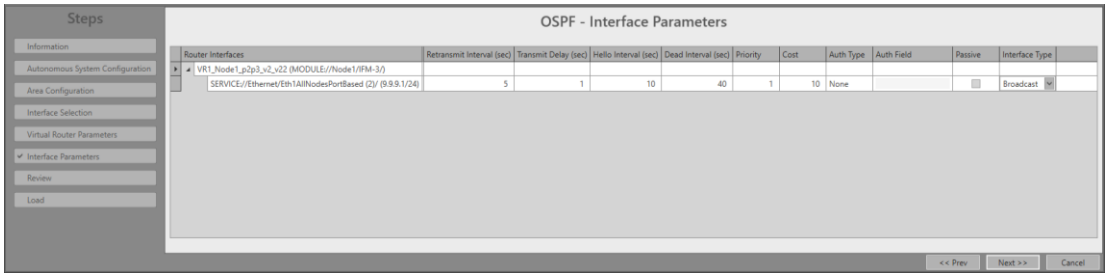

Figure 113 OSPF: Interface Parameters

- Router Interfaces: indicates the router interface. Select the interface row in which you want to change configurations;
- Retransmit Interval (sec) (default=5 s, range [1,..,3600]): This value configures the time interval between the retransmission of successive LSAs. Each new LSA must be acknowledged. The LSA will be retransmitted by the originating router according to the Retransmit Interval until it has been acknowledged by the neighbor router;
- Transmit Delay (sec) (default=1 s, range [1,..,3600]): This value configures the estimated time required to transmit a link state update packet on the interface using this configuration. This variable adds a specified time to the age field of an update. If the delay is not added before transmission over a link, the time in which the link-state advertisement (LSA) propagates over the link is not considered. This parameter has more significance on very low-speed links;
- Hello Interval (sec) (default=10 s, range [1,..,65535]): This value configures the (OSPFv2 Hello) interval between the hello packets sent on the interface. Hello Packets are sent between two OSPF neighbors to maintain connectivity. The Hello Interval must be the same for all (virtual) router interfaces attached to the same link. See also the Dead Interval parameter. ATTENTION: OSPF neighbors must have the same Hello Interval value!
- Dead Interval (sec) (default=40 s, range [1,..,65535]): The Dead Interval and Hello Interval work together to maintain the operational link between two OSPF neighbors. If a virtual router interface does not receive a Hello packet within the configured Dead Interval, the (virtual) router decides that the neighboring (virtual) router is dead or

down. By default, the Dead Interval is four times the Hello Interval. ATTENTION: OSPF neighbors must have the same Dead Interval value!

- Priority (default=1, range [0,..,255]): This value configures the interface priority to determine the Designated Router (DR) for the link connected to the interface. In the DR election process the highest Priority value wins and becomes DR. If the two DR candidates have the same Priority, the highest Router Id (RID) wins. Priority '0' means that the virtual router does not participate in the DR election process and as result cannot become the DR;
- Cost (default=10, range [1,..,65535]): This value configures the cost metric value added to a route on this interface. The following formula can be used as a rule of thumb to define the Cost for a specific route. Cost = <Highest link speed in the OSPF domain in Mbps> / <Current link speed in Mbps>, e.g. if the highest link speed is 10 Gbps, and the current link speed = 100 Mbps, then the Cost for this link could be 10000/100 = 100. The Cost for a link with the highest speed would be 10000/10000 = 1.
- Auth Type: OSPF authentication can be done via selecting one of the following authentication types listed below. ATTENTION: Make sure that neighboring routers (or virtual router interfaces) use the same Auth Type and Auth Field;
  - None (=default): There is no OSPF authentication at all on this virtual router interface;
  - Auth Text: Authentication on this virtual router interface is done based on Simple Password Authentication, a password must be specified in the Auth Field (alphanumeric input) which is to be used by the neighboring routers that are using the OSPF simple password authentication. ATTENTION: OSPF neighbors must have the same password;
  - Messages Digest: Authentication on this virtual router interface is done via md5 cryptographic authentication. A password must be specified in the Auth Field (alphanumeric input) which is to be used by the neighboring routers that are using the OSPF Message Digest authentication;
- Auth Field: (alphanumeric input) Fill out a password or an authentication key that must be used for authentication when Auth Type is Auth Text or Message Digest. ATTENTION: Make sure that neighboring routers (or virtual router interfaces) use the same Auth Type and Auth Field.
- Passive:
  - Unchecked (=default): This virtual router interface is active, it participates in the OSPF protocol;
  - Checked: This virtual router interface is passive, it ignores routing updates on this interface and does not send 'Hello' packets and routing updates. A passive interface could be set for interfaces that do not have neighbors. This parameter can also be used for testing or troubleshooting purposes. If loopback interfaces (see §8) are used on this virtual router, make sure to check this checkbox (=best practice) or check the 'Redistr Conn' checkbox (see before). This is necessary for PIM (see §5.6), to make sure that this loopback interface is known within the entire PIM component;
- Interface Type:

- Broadcast (=default)/Point to Point: If two router interfaces of two neighbouring routers are directly connected to each other, you could set both Interface Types to 'Point to Point'. In any other case, e.g. if there is a network in between, make sure to set the value to 'Broadcast'. 'Point to point' is a little bit more performant than 'Broadcast'.

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.7.4 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §5.9.4.

5.8 Layer 3: Static Routing

5.8.1 General

This static routing wizard configures or creates static routes (on the virtual routers) throughout the network. A route is a path from a source towards a destination via which the message has to travel to reach the destination IP network. There can exist multiple paths from source to destination, but only one path will be the most efficient one. Routes (with a same destination) can be favored via a distance parameter.

5.8.2 Prerequisite

- Some Ethernet services (different from a local service) must have been created on some L3 IFMs;
- At least one virtual router must be configured before a static route can be configured.

5.8.3 Configuration

Go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → Static Routing → (Protocols)  . The Static Routing wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Selection:
  - Virtual Router Selection: Select a virtual router from the drop-down list on which the static routing table must be created;
- Creation: In the figure below, static routes can by created by filling out a custom or selecting a detected 'Destination' and a 'Via' point. The 'Destination' point is connected indirectly whereas the 'Via' point is directly connected to the selected virtual router. As a general example, consider that the packet has to travel from point A to point E via the

path: A → B → C → D → E. This means that A = Source; B = Via; C, D, E = possible Destinations. A Destination can be selected from the Destinations list below if the selected virtual router is connected at least to another virtual router.

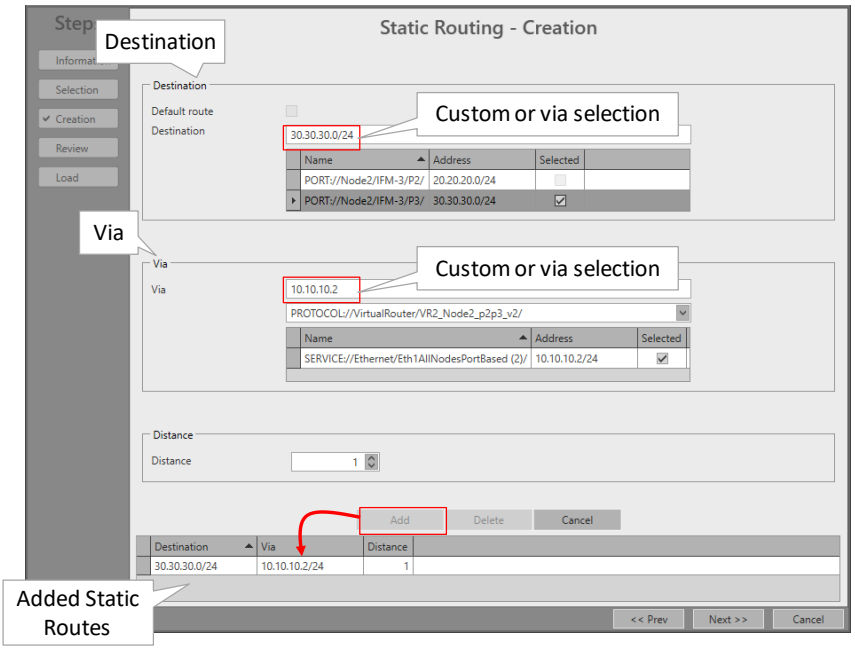

Figure 114 Static Routing - Creation

- Default route: A default route is the route of the last chance. It is the last route tried by a router, after trying and mismatching all the other routes or if no other route is available. The destination of the default route is always 0.0.0.0/0.
  - Unchecked (=default): The configured static route must not be the default route;
  - Checked: The configured static route must be the default route. In the listings later on, the default route can always be recognized as the route with 0.0.0.0/0;
- Destination: Fill out a destination network IP address via either manually filling out a custom value e.g. 30.30.30.0/24 or via selecting a port from the router port list. The router port list only contains ports from other virtual routers that are connected in the same service as the selected virtual router. If Default route is checked, a destination cannot be filled out or selected as it will always be 0.0.0.0/0.

  NOTE: A network IP address (e.g. 30.30.30.0/24) covers the entire network whereas a single IP address (e.g. 30.30.30.1/24) covers one host;

- Via: This is the next hop IP address 'B' via which the source 'A' initially will send its packets to finally reach destination 'E'. Fill out a single IP address via either manually filling out a custom value or via selecting a service router port from the service list (e.g. 10.10.10.2/24). This service router port list changes when selecting another Virtual router in the 'Via' virtual router list. VRRP virtual IP addresses are also shown in this list.
- Distance: (default = 1, range [1,..,254]) When there are multiple static routes with the same destination IP address but a different 'Via' IP address, the static route with the lowest Distance value will be taken.

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.8.4 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §5.9.4.

5.9 Layer 3: Virtual Router, VRF

5.9.1 General

The icon below is used in the HiProvision Wizard info pages to indicate a virtual router or VRF (=Virtual Routing and Forwarding).

Figure 115 Virtual Router Icon

Virtual Router is a router (instance) created by HiProvision within a L3 IFM in a Dragon PTN node. 'Virtual' in this context refers to the fact that it is created programmatically and that multiple routers can be created within the same IFM, with each Virtual Router having its own independent routing table. Because the Virtual Routers are independent, the same or overlapping IP addresses can be used without conflicting with each other. These routing tables initially only have IP addresses/masks of directly connected networks. Later on, these routing tables will be extended by using Static Routing (see §5.8), OSPF (§5.7).

Example figure below:

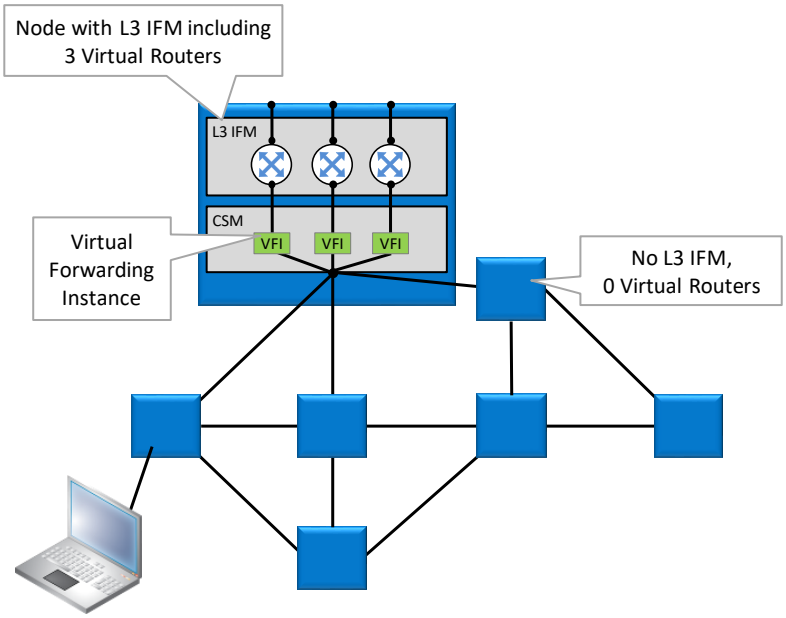

Figure 116 Virtual Router Example

5.9.2 Prerequisite

At least one L3 IFM must have been configured.

5.9.3 Configuration

Go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → Virtual Router → (Protocols) . The Virtual Router wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Creation:
  - Name: Fill out a Virtual Router name;
  - Interface Selection: this list shows all the configured L3 IFMs. Select one L3 IFM on which the Virtual Router must be created by just clicking the IFM's Selected checkbox;
  - Port Selection (optional if you select a service in Service Selection): shows the available ports (=front ports, LAG ports, Loopback Interface ports = L3 virtual port) on the selected L3 IFM, not part of a VLAN or service yet. Add one or more ports to this Virtual Router by clicking one or more Selected checkboxes.
  - Service Selection (optional if you select a Port in Ports Selection): shows the available Ethernet services (VLANs) configured on the selected L3 IFM, not yet assigned to another Virtual Router. Select one or more services (VLANs) that must become a router interface by clicking one or more Selected checkboxes;

NOTE: At least one port or service must be selected.

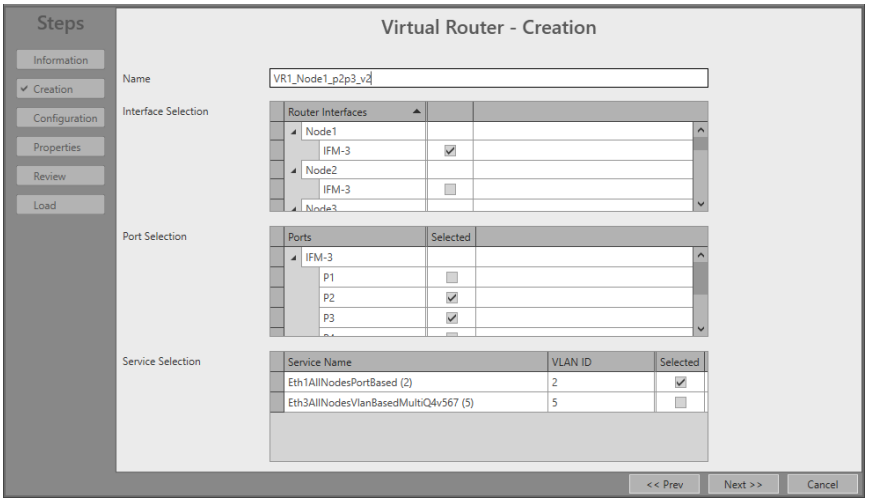

Figure 117 Virtual Router – Creation

- Configuration:
  - IP Address: Assign (or fill out) the IP addresses in CIDR (=Classless Inter-Domain Routing) notation to the ports and interfaces of this virtual router;
  - Gratuitous ARP (=GARP): A GARP is a sort of notification in advance, it updates the ARP cache of other systems before they ask for it via a normal ARP request. A GARP is broadcasted by the virtual router interface into the network to announce or update its own IP/MAC address and announce its presence in the network. When the network replies to a GARP, it indicates a duplicate IP address or IP conflict in the network. The transmit interval is configured via the Gratuitous ARP Transmit Timer in the next wizard page.
    - Unchecked (=default): Do not broadcast GARP messages from this interface into the network (except for the Link-Up event, see below);
    - Checked: Broadcast GARP messages from this interface into network.

    NOTE: GARP should only be used on router interfaces connected to static routes configured via Static Routing (§5.8). GARPs keep the static routes alive resulting in faster processing of routed traffic over these routes.
  - Gratuitous ARP on Link-Up: It is possible to broadcast GARP messages in the network when the link comes up (= link-up event). How many messages are sent depends on both settings, see table below.

Table 14 Amount of GARP Messages on Link-Up Event

Gratuitous ARP	Gratuitous ARP on Link-Up	Amount of GARP Messages on Link-Up
---	---	0
---	✓	1
✓	---	3 (1 message/second)
✓	✓	3 (1 message/second)
✓ = checked; --- = unchecked		

NOTE: Left-hand (/) = multiple (de)selection of Gratuitous ARP;

NOTE: Right-hand (/) = multiple (de)selection of Gratuitous ARP on Link-Up;

NOTE: Select items or checkboxes: Individual select: Just click checkboxes of the desired items. Multiple select: first select the desired rows (via CTRL+Click or SHIFT+Click or CTRL+A (=all rows)). Then click to check the checkboxes of the selected rows. Click to uncheck the checkboxes of the selected rows.

- Click Next>>;

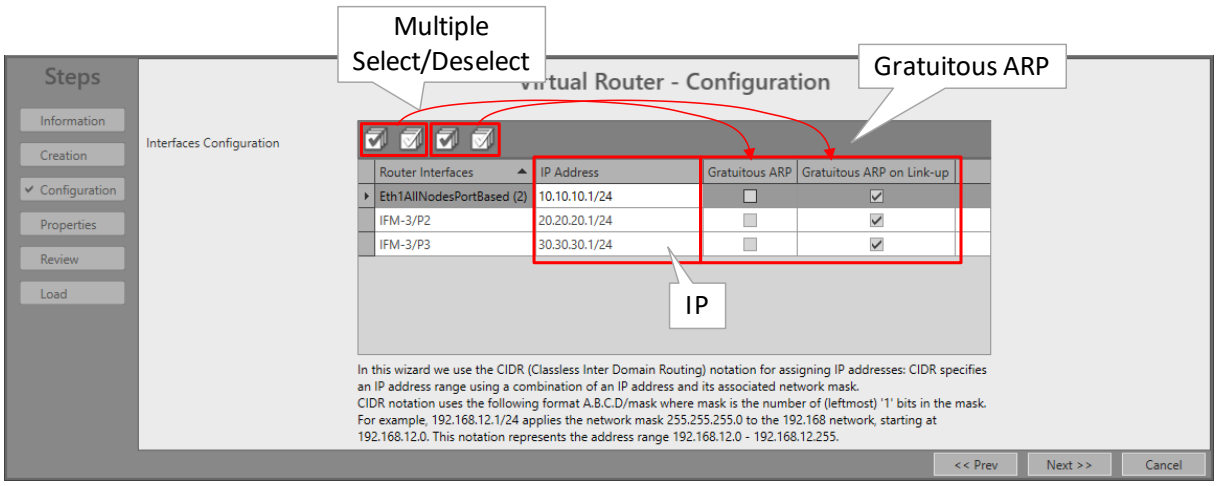

Figure 118 Virtual Router – Configuration

- Properties: Fill out the virtual router **properties**. In the figure below the default values are displayed. ICMP is a protocol for sending control and test messages across the IP network.
  - Send ICMP Redirects: (default=checked) An ICMP redirect message is used by a router to tell a previous router that it is better to use a different route next time. Sending these messages can be turned off;
  - Send ICMP Unreachables: (default=checked) An ICMP destination unreachable message indicates that a destination is unreachable. Sending these messages can be turned off;
  - Send ICMP Mask Reply: (default=checked) If a station starts up, it will broadcast ICMP mask request to learn the used subnet mask. The router will send back an ICMP mask reply. Sending these messages can be turned off;
  - Send ICMP Echo Reply: (default=checked) An ICMP echo reply message is a reaction on an ICMP echo request message, to tell that the receiver is alive and reachable. ICMP Echo replies are used by the well-known 'ping' command to test network connectivity. Sending these messages can be turned off;
  - IP Default TTL: (default=64, range [1,..,255]) Time to live hop counter, indicates how long (or how many hops) an IP message can survive in an IP network. Every hop, the TTL is decreased with one. If TLL reaches 0, the IP message is removed from the network;

- ARP Timeout: (default=300 s, range [30,..,86400]) If an ARP entry is not used a specific amount of time, called the ARP timeout, the entry is removed from the caching table;
- ARP Retries: (default=10, range [2,..,10]) indicates the number of times that the ARP cache manager attempts to resolve an IP address;
- Gratuitous ARP Transmit Timer *: (default = 120 s, range [15,..,86385]) This value configures the time interval between the retransmission of GARP broadcast messages into the Dragon PTN network. If Gratuitous ARP is checked on this interface, each time this timer expires, a new GARP broadcast message is sent and the timer is restarted;

  NOTE: This timer is not valid for the the link-up event, see Table 14.

NOTE: *: Gratuitous ARP settings are shared between all virtual routers on the same IFM. So changing this setting for one Virtual Router means that it is changed automatically for the other Virtual Routers (if any) on the same IFM.

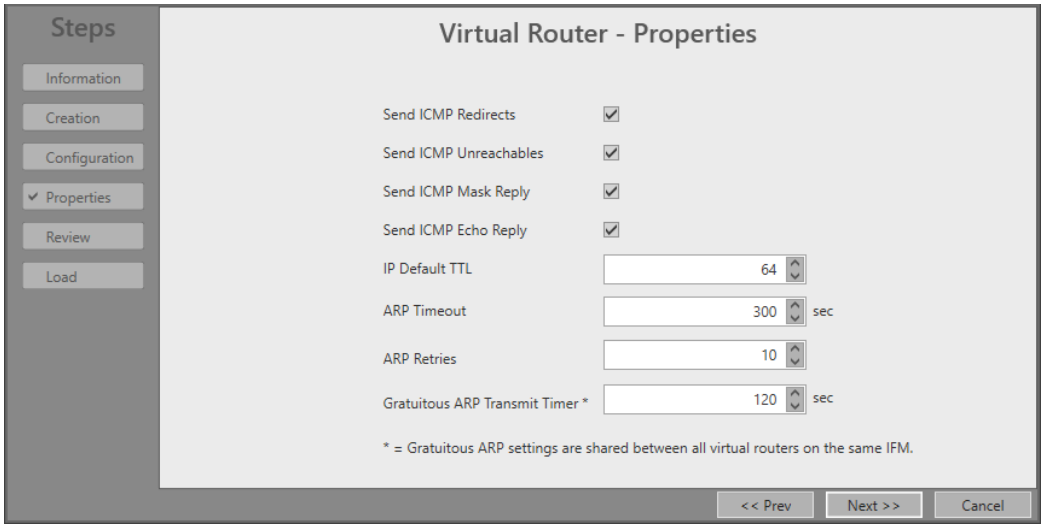

Figure 119 Virtual Router – Properties

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.9.4 Layer 3 View: Virtual Router Connections Overview

Go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → Virtual Router → (Protocols) → L3 icon.

Clicking this icon shows a full overview of all the Virtual Router connections. Next, if you click on a virtual router icon in this drawing, a more detailed view is shown of this virtual router.

Only the virtual routers that are connected to this virtual router are shown, including the services that interconnect these virtual routers. The interface IP addresses of the clicked virtual router are shown as well.

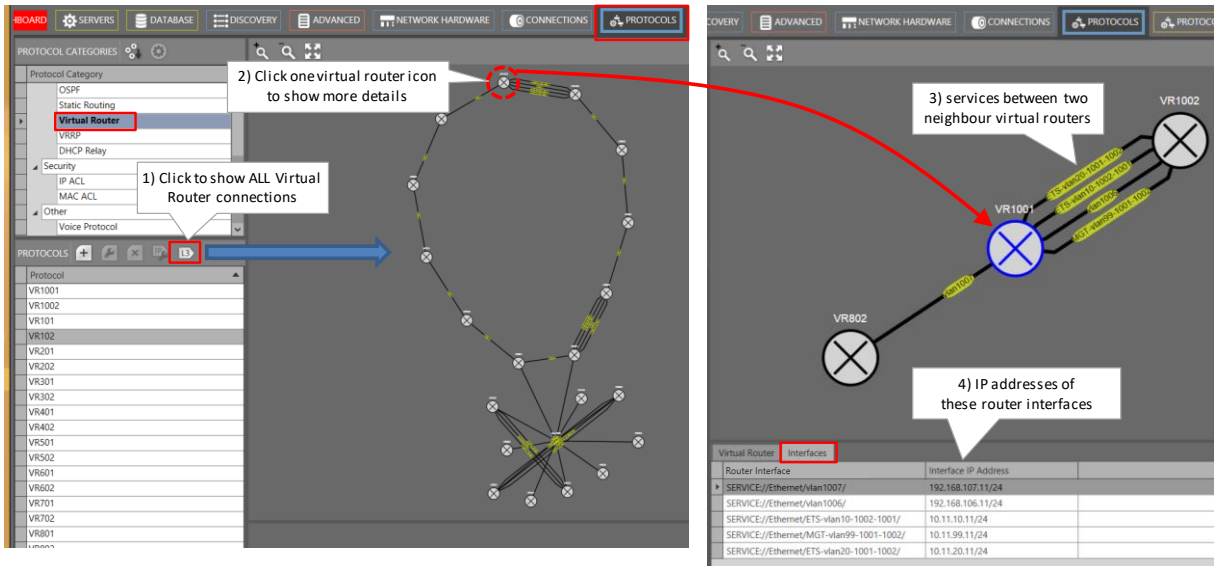

Figure 120 Layer 3 View: Virtual Router Connections Overview

5.9.5 Monitoring

None.

5.10 Layer 3: VRRP (=Virtual Router Redundancy Protocol)

5.10.1 General

VRRP (=Virtual Router Redundancy Protocol) is a protocol which increases the availability of the router of a subnet. This redundancy technology is based upon the **sharing** of a **virtual IP Address** amongst all the router interfaces being part of the same VRRP **Group**. This is achieved by combining a master and one or more backup router interfaces into one **Group**. The actual routing within the Group is done by the master (=active) router interface whereas the others act as backup. A router interface becomes master after a master election process.

All the router interfaces within a Group use the same unique virtual IP address, e.g 10.10.10.1. The virtual IP address and router interfaces must be in the same subnet. The virtual IP address will be the default gateway for its associated VLAN e.g. VLAN with VID 150.

This VRRP wizard can create one or more VRRP instances. Each VRRP instance can be configured between two or more routers (advised: one master + one or two backup routers). As a result, a Group will always have one or more backup router interfaces whenever its active router goes down.

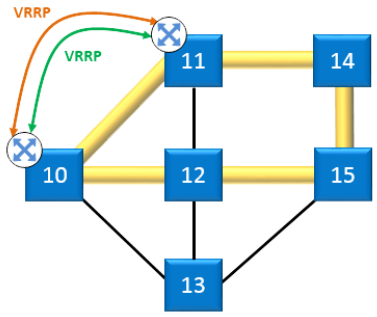

Figure 121 VRRP General

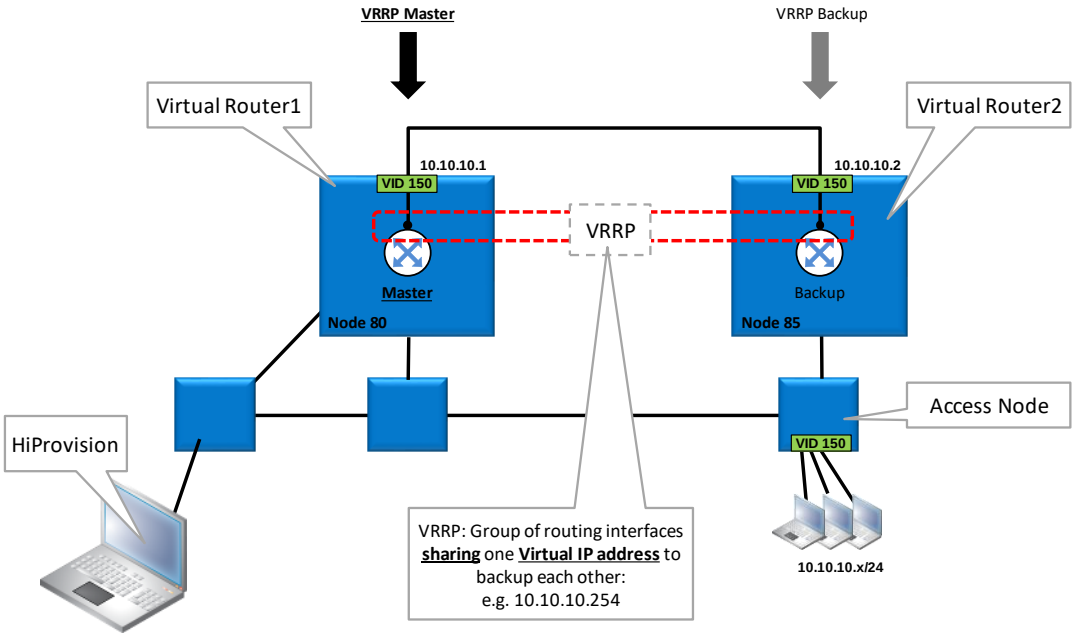

Figure 122 VRRP Example

- Status Changes (from → to):
  - Init → Backup
  - Backup → Master
  - Master → Backup
  - Backup → Init
  - Master → Init

Table 15 VRRP States

State	Description
Init	VRRP is initializing. In case no ports are up in the VRRP, the state remains idle.
Master	The interface (VLAN) is acting as a Master router. In this Master state the router operates as the forwarding router for the IP address(es) associated with the virtual router.
Backup	The interface (VLAN) is acting as a Backup router. The purpose of this Backup state is to monitor the availability and state of the Master Router.

5.10.2 Prerequisite

Some Virtual Routers must have been created (see §5.9) and the router interfaces must be part of the same IP subnet. Furthermore, it is strongly advised that the redundant routers have similar configurations (*), to easily backup each other. See figure below:

NOTE: (*): same amount of router interfaces, same IP subnets, same VLANs;

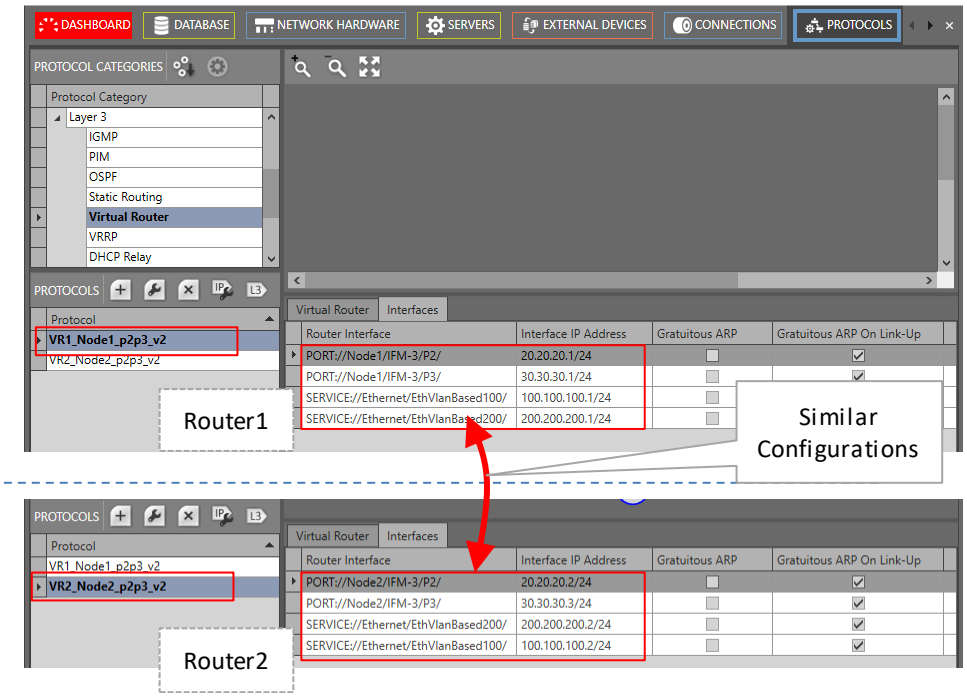

Figure 123 VRRP Prerequisites

5.10.3 Configuration

In HiProvision, go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → VRRP → (Protocols)  . The VRRP wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Creation:
  - Name: Fill out a VRRP instance name;
  - VRRP ID (default = 1, range [1..255]): Assign an ID to this VRRP instance by filling it out or selecting it. This number is also known as the VRRP instance number;
  - Virtual Router Selection: The list is filled with available Virtual Routers that can participate in a new VRRP instance.
    - Select the Service VLAN router interfaces that must backup each other by clicking the Selected checkboxes. If you click a checkbox, only interfaces in the same VLAN as the first one will remain to be selected. If the required interfaces are selected, click the **Add** button to group them into one 'Group'. The 'Group' will be added to the list.

    NOTE: This example has only two routers that backup each other. A maximum of three redundant routers (one master + two backups) per VRRP instance can be configured.

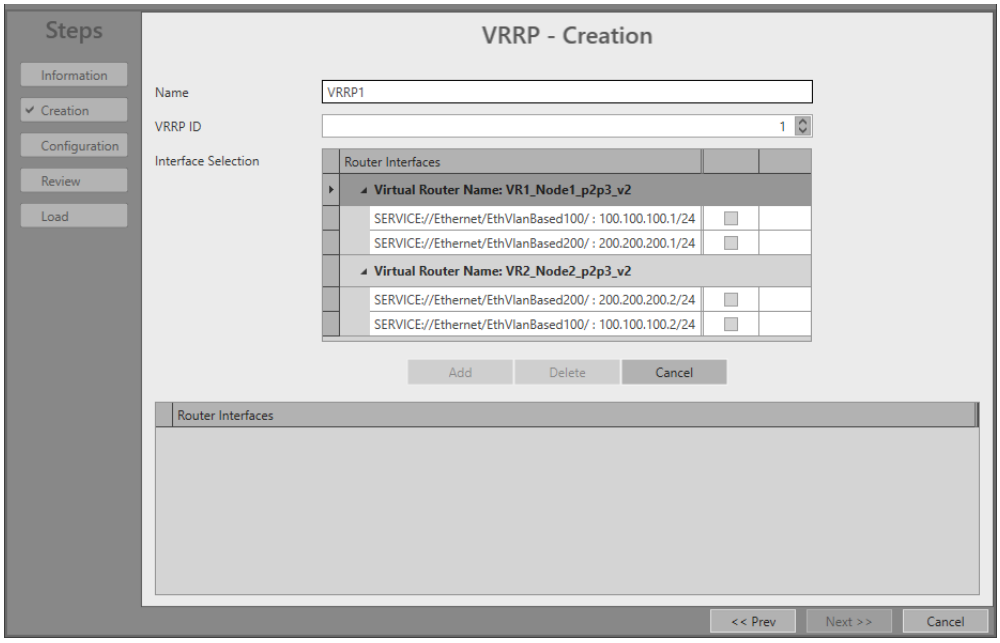

Figure 124 VRRP Creation

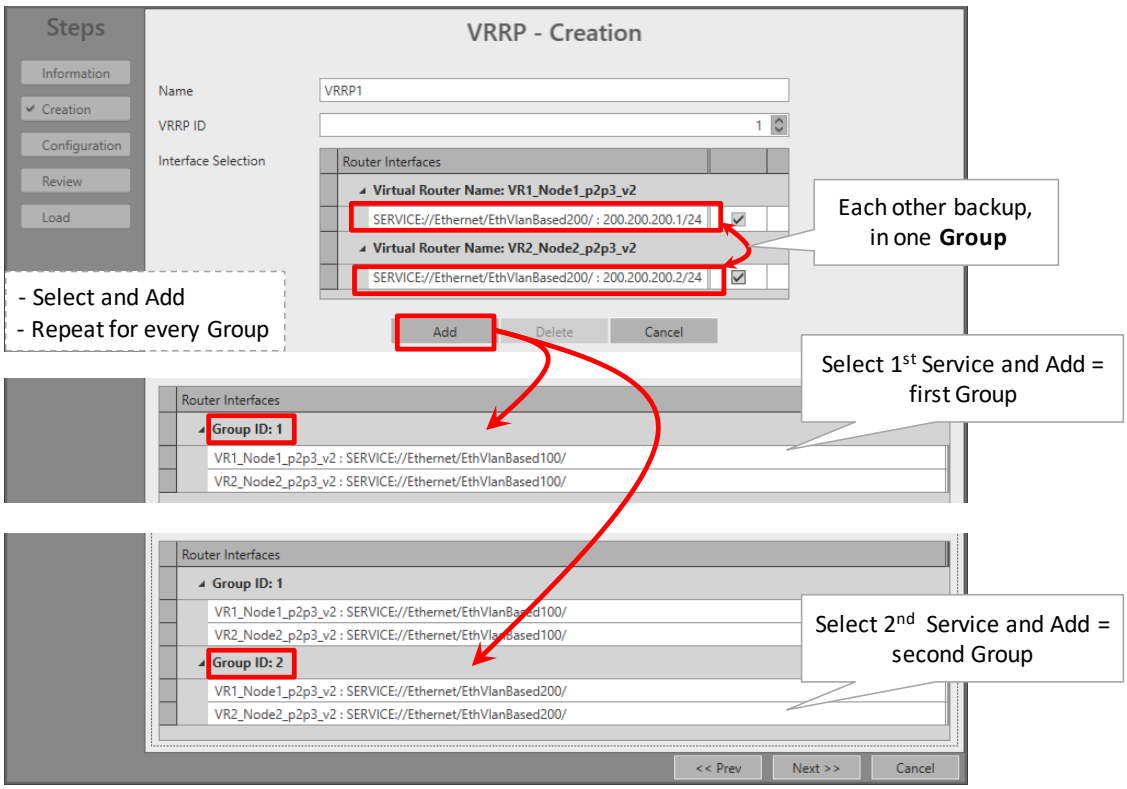

Figure 125 VRRP Creation: Group Added

- Modify/Delete Group: Once a router interface is part of a Group, it cannot be selected anymore to add it to another Group. If a port has been accidently added to a wrong Group, the port can be selected again in the Virtual Router Selection after deleting the wrong Group first. A Group can be deleted by selecting a row from that Group and clicking the Delete button. Deleting all Groups must be done

by deleting each Group individually or by deleting or cancelling the entire VRRP creation and start over again from scratch.

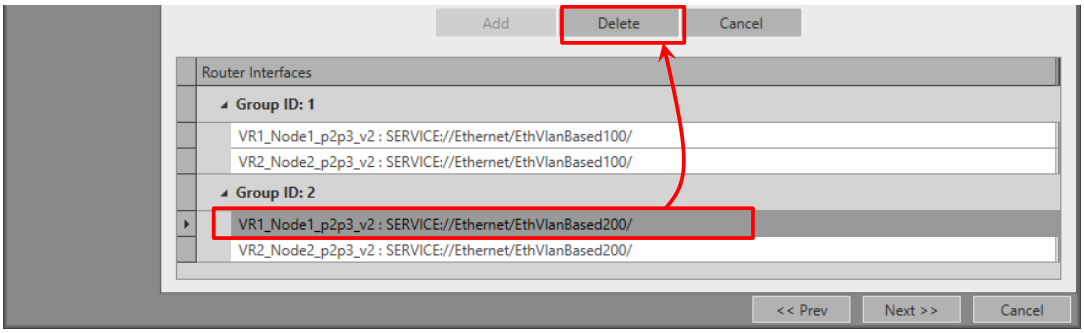

Figure 126 VRRP Creation: Delete Group

- Configuration: Fill out the fields below. Fields can have a 'group' or 'individual' behavior:
  - group: (e.g. Virtual IP Address) Field values are always the same within the same Group. If you change a field value in a Group, you change all values automatically of the same field in the same Group;
  - individual: (e.g. Priority) Field values can be different within the same Group. They can be changed independently within the same group.

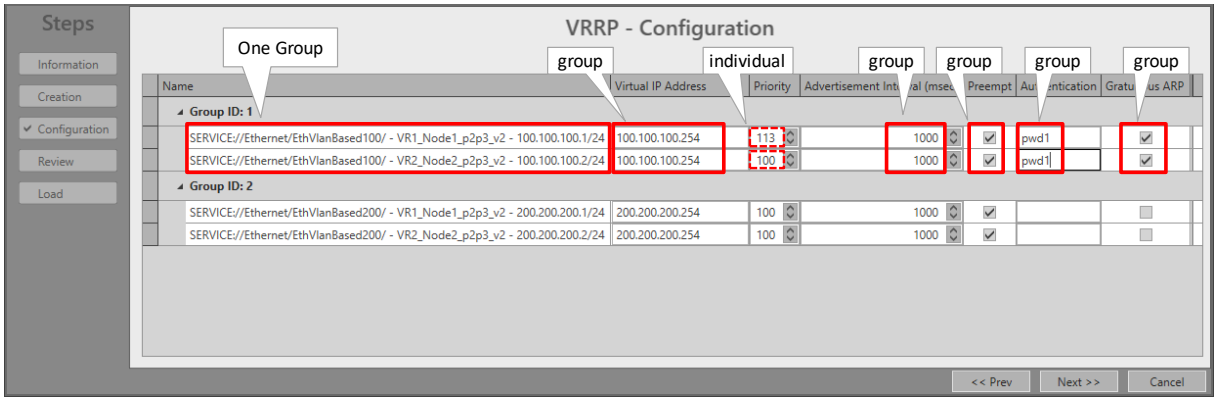

Figure 127 VRRP – Configuration

- Virtual IP Addresses (group): Fill out an available unique virtual IP address for each 'Group'. Each router interface of the same 'Group' will always be mapped to the same virtual IP address. If one router fails, the other redundant router takes over and will still process the same virtual IP and MAC address. In this way, redundancy is created.
- Priority (individual): (default = 100, range [1,..,254]) Configures the Priority of each individual router interface within the Group. The higher value, the higher the priority. In case the router interfaces have the same priority value, the higher IP address is favored as master. The Priority and Preempt fields depend on each other, see further.
- Advertisement Interval, msec (group): default value = 1000 msec, value [100,..,255000], step size = 100; the master router interface within the VRRP instance communicates its state and priority via advertisements towards the other backup router interface. This advertising occurs according to the filled out Advertisement Interval (configured on 'Group' level);

- Preempt (group), see also Priority field:
  - Checked (=default): Inside a 'Group', the router interface with the highest priority value always becomes the master. Example with two interfaces on two different routers: interface router1 = priority 100 = master, interface router2 = priority 98 = backup. If router1 fails, router2 becomes the master. Now when the failing original master (router1) with the highest priority returns into the network again after recovery, it will automatically take over the mastership from the backup router (router2) that is also still alive;
  - Unchecked: Inside a 'Group', the router interface that becomes master stays master until it fails. E.g., when a backup router interface becomes master after the original master fails, this backup router interface remains master, even if the original master with the highest priority value is up and running again (e.g. after failure recovery);
- Authentication (group): optional string field, maximum eight characters, allowed characters: 0…9, a…z, A…Z, !, @, #, $, %, ^, &, *. An optional textual authentication string can be used to communicate within the 'Group' of that VRRP instance, e.g. 'pwd1'. A router ignores incoming VRRP packets for a specific 'Group', if the authentication string of the packets mismatches the Authentication (group) string configured for the 'Group'.
- Gratuitous ARP:
  - Unchecked (=default): This virtual interface will not broadcast Gratuitous ARP messages in the network.
  - Checked: This virtual interface will broadcast Gratuitous ARP messages in the network. This is only possible if the individual router interfaces (§5.9) inside the group have disabled Gratuitous ARP.
- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.10.4 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §5.9.4.

5.11 Layer 3: DHCP Relay

5.11.1 General

DHCP (=Dynamic Host Control Protocol) is a network configuration protocol in IP networks which allows that IP clients at start-up automatically request IP configuration data from a

DHCP Server. This data is necessary for the client to be able to communicate with other IP clients within the IP network. The most important IP configuration data for the IP client is:

- Own IP Address;
- Subnet Mask;
- Default Gateway IP Address;
- DNS Server IP Address(es)-Domain Name;
- Lease Time (amount of time that the IP configuration data is valid for this IP client).

The DHCP Server assigns IP addresses from an administrated IP address pool, to its clients. Multiple DHCP servers in the IP network are possible. All DHCP servers are stand-alone and do not know each other. The DHCP makes sure that only one DHCP server finally supplies an IP address (and other data) to the client.

More information can be requested from the DHCP server via the Options parameter. When using multiple subnets, it is possible that there is no DHCP server available in the client subnet but only a DHCP Relay function. This DHCP Relay forwards or relays the DHCP messages from clients to the DHCP Server in another subnet and vice versa.

In HiProvision, a DHCP Relay agent can be configured on the L3 IFMs to forward IP address requests/responses towards external DHCP Servers/DHCP Clients.

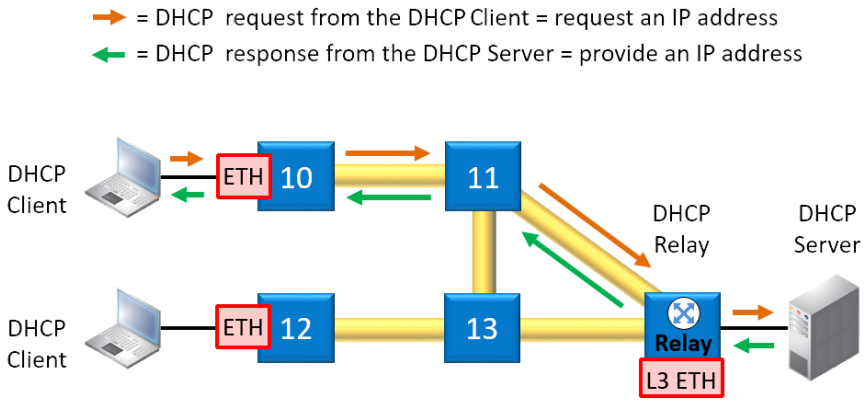

Figure 128 DHCP Overview

5.11.2 Prerequisite

At least one Virtual Router (on L3 IFM) and an Ethernet service must have been created (see §5.9). Make sure that the Ethernet service has been selected in the Virtual Router.

5.11.3 Configuration

In HiProvision, go via Dashboard → (Configuration) Protocols → Protocol Categories → Layer 3 → DHCP Relay → (Protocols) +. The DHCP Relay wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Creation:
  - Name: Fill out a name for the DHCP Relay instance;

- Information Option:
  - Unchecked (=default): the DHCP relay will not send the option 82 values in the DHCP discover packets;
  - Checked: the DHCP relay will send the option 82 values in the DHCP discover packets and DHCP server can decide based on those values.
- Virtual Router Selection: Select the Virtual Router on which DHCP Relay agent must be configured;

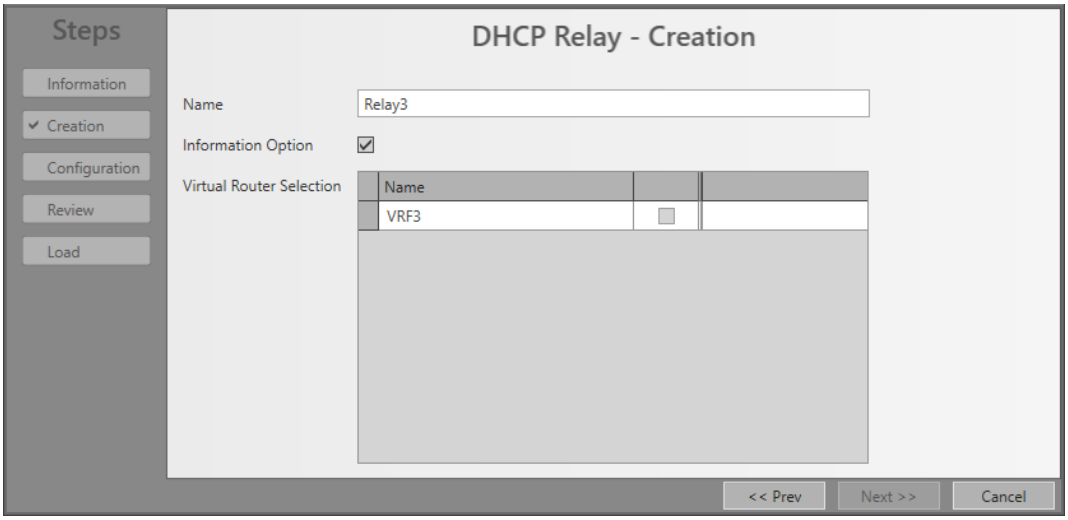

Figure 129 DHCP Relay: Creation

- Configuration:
  - DHCP Server IP Address: Fill out the IP address of the DHCP server and click the Add button to add this server to the DHCP Servers list;
  - DHCP Servers: list of DHCP servers to which the Relay agent will forward DHCP requests. A DCHP server can be removed after selecting it and clicking the Remove button.

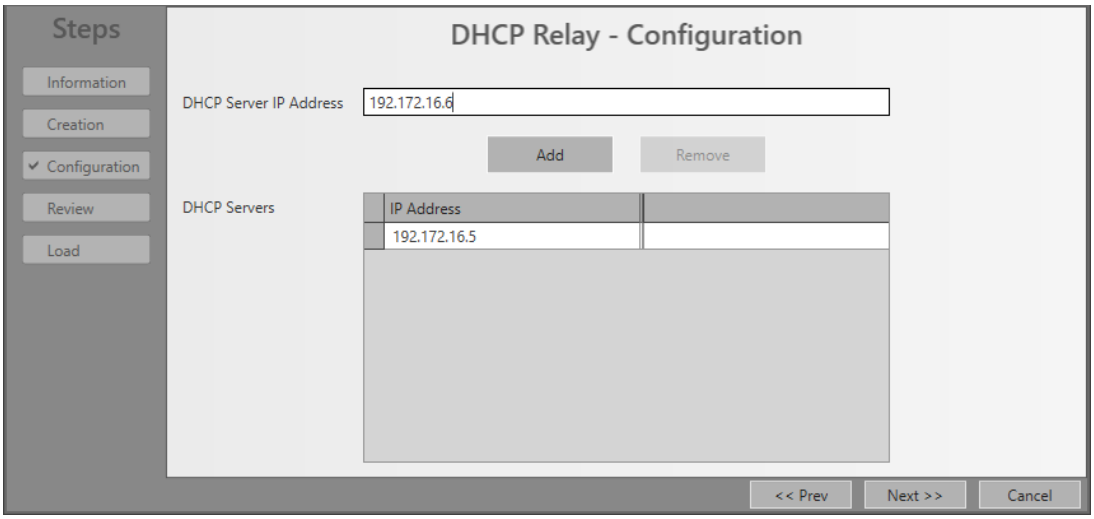

Figure 130 DHCP Relay: Configuration

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

5.11.4 Monitoring

Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §5.9.4.

5.12 Security: IP ACL (= IP Access Control List)

5.12.1 General

An Access Control List (=ACL) restricts communication access on a port in an Ethernet service. IP ACL permits access based on a source and/or destination IP address range of the incoming packets. If no ACL rules are created, all traffic is allowed. On a port (front, back end, LAG), either MAC ACL (see §5.13) or IP ACL can be configured. On Ethernet IFM (see 'Support Matrix' in Ref. [2Net] in Table 1) ports, combining MAC and IP ACL is not possible. On L2/L3 IFMs, combining MAC and IP ACL is possible. When both are combined, first IP ACL will be checked then MAC ACL.

5.12.2 Prerequisite

An Ethernet service must have been configured between IFMs that support the Ethernet service, see Ref. [2Net] in Table 1. A tunnel different from point-to-point must be used.

5.12.3 Configuration

Go to Dashboard → (Configuration) Protocols → Protocol Categories → Security → IP ACL → (Protocols)  .

The IP ACL wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Service Selection: select the Ethernet service for which an IP ACL must be configured;
- Port Configuration (only for Ethernet IFMs, see 'Support Matrix' in Ref. [2Net] in Table 1, for L2/L3 IFMs, see 'Switch Port Configuration' further on):
  - Port Type: shows the IFM port type, e.g. 4-GC-LW;
  - Enable ACL:
    - Unchecked (=default): IP ACL is disabled for this port, all incoming packets from any source and destination IP address are allowed on this port.
    - Checked: IP ACL is enabled for this port. Source/Destination Address filled out: If the source/destination IP address of the incoming Ethernet packet is in the range

of the configured Source/Destination Address, the packet will be allowed. If both addresses are filled out, both addresses of the incoming packet must be in their configured range. If none of the above conditions are met, the packet will be dropped;

- Greyed out checkbox: IP ACL cannot be configured on this port because a MAC ACL (see §5.13) has already been configured on this port. Per port, only MAC ACL or IP ACL can be configured, not both together;

- Source/Destination Address: the IP address range (or network address) that must be matched when IP ACL is enabled on this port. Format of this field: the IP address range must have a valid subnet mask notation, e.g. 192.168.0.0/24, 192.168.5.64/26, 205.14.14.0/27. For a single host, e.g. 172.15.15.1, fill out 172.15.15.1/32.

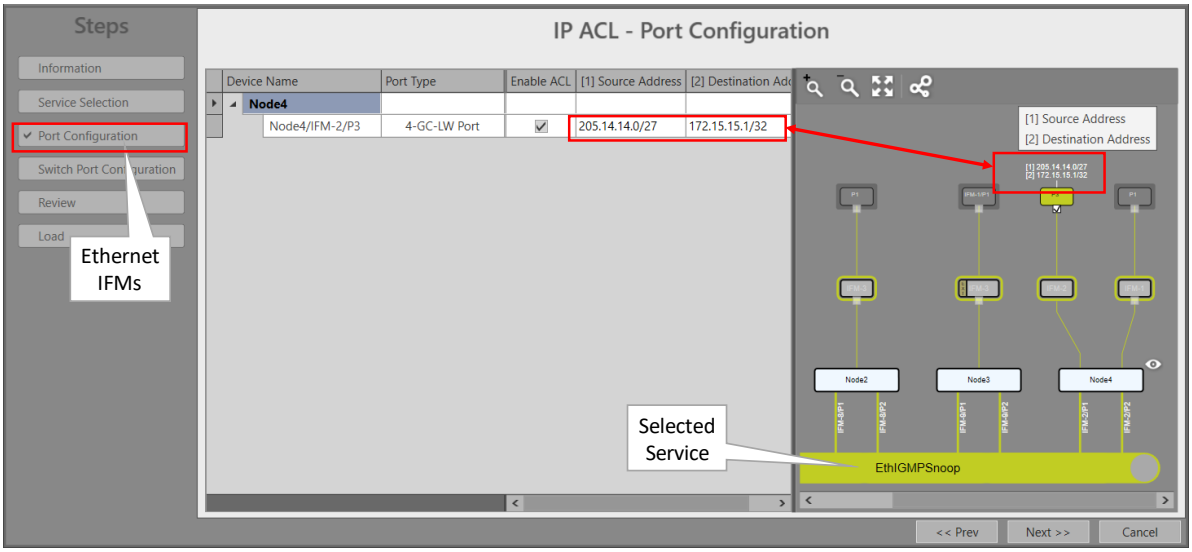

Figure 131 IP ACL: Port Configuration Example for Ethernet IFMs

- Switch Port Configuration (only for L2/L3 IFMs, see 'Support Matrix' in Ref. [2Net] in Table 1): By default, no IP ACL rules are created per IFM and as a result, all traffic is allowed. To configure IP ACL on a front or back end port, create an ACL rule first in the Configuration section (parameters described below), add it to a port and then check Enable ACL in the IFM row. Multiple rules can be added per port.

  - Add rule: select a port row in the device tree view and click the Add Rule button to add the rule to this port. It is possible to select multiple ports by clicking each row while holding the CTRL key pressed, or even by clicking the entire IFM, or by clicking in the tree view area and press CTRL+A to select all IFMs. When clicking the Add Rule button, the configured rule will be added to all selected IFMs.

  - Delete rule: select a rule row in the device tree view and click the Delete Rule(s) button. It is possible to select multiple rule rows by clicking each row while holding the CTRL key pressed, or even by clicking in the tree view area and press CTRL+A to select all rules. When clicking the Delete Rule(s) button, all selected rules will be deleted.

  - Configuration Section:
    - Filter:

- Permit (=default): Permit (=allow) all incoming messages on a port according to the configured IP Addresses and Priority;
- Deny: Deny (=block) all incoming messages on a port according to the configured IP Addresses and Priority;

- Source/Destination Address: the IP address range (or network address) that must be matched when IP ACL is enabled on this port. Format of this field: the IP address range must have a valid subnet mask notation, e.g. 192.168.0.0/24, 192.168.5.64/26, 205.14.14.0/27. For a single host, e.g. 172.15.15.1, fill out 172.15.15.1/32. If nothing is filled out, any IP address counts.
- Priority (default = 1, value[1..100]): Indicates the priority in which this configured rule on a specific port within an IFM will be processed. Value '1' has the lowest priority, value '100' has the highest priority. Rules with the highest priority are processed first. If the priority of multiple rules within an IFM is the same, the rule that was created first will be processed first. A rule is hit when the IP address of both the data packet and the configured rule match. If a rule is hit, the remaining rules for the same port will not be processed anymore.

- Device Tree view:
  - Port type: show the IFM port type;
  - Enable ACL:
    - Unchecked (=default): IP ACL is disabled for this port, all incoming packets from any source and destination IP address are allowed on this port.
    - Checked: IP ACL is enabled for this port. Source/Destination Address filled out: If the source/destination IP address of the incoming Ethernet packet is in the range of the configured Source/Destination Address, the packet will be allowed. If both addresses are filled out, both addresses of the incoming packet must be in their configured range. If none of the above conditions are met, the packet will be dropped;

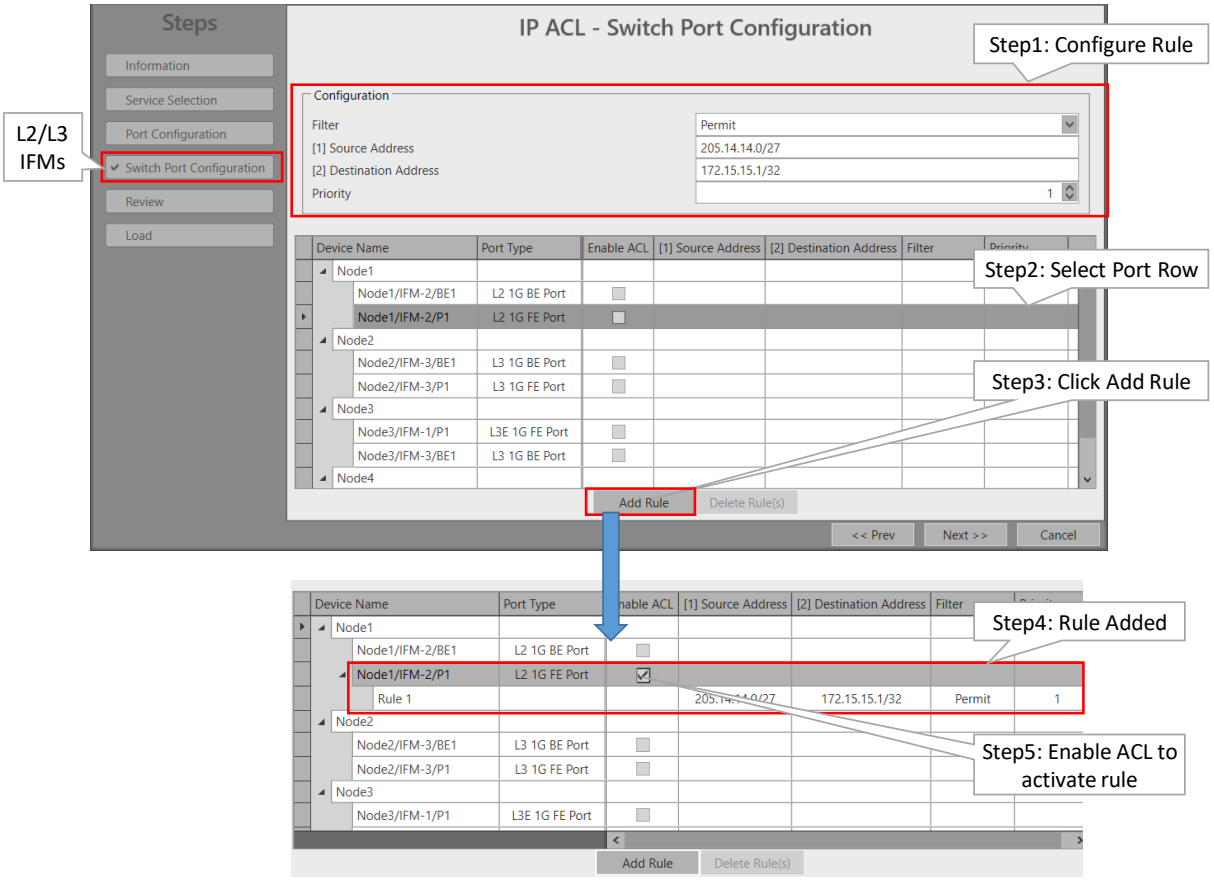

Figure 132 IP ACL: Switch Port Configuration Example for L2/L3 IFMs

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

NOTE: The IP ACL for a service can be modified/deleted later on via selecting the service in the IP ACL list and clicking the / button.

5.12.4 Monitoring

None.

5.13 Security: MAC ACL (= MAC Access Control List)

5.13.1 General

An Access Control List (=ACL) restricts communication access on a port (front, back end, LAG) in an Ethernet service. MAC ACL permits access based on the source MAC address of the incoming packets. On Ethernet IFM (see 'Support Matrix' in Ref. [2Net] in Table 1) ports, combining MAC and IP ACL is not possible. On L2/L3 IFMs, combining MAC and IP ACL is possible. When both are combined, first IP ACL will be checked then MAC ACL.

5.13.2 Prerequisite

An Ethernet service must have been configured between IFMs that support the Ethernet service, see Ref. [2Net] in Table 1. A tunnel different from point-to-point must be used.

5.13.3 Configuration

Click Dashboard → (Configuration) Protocols → Protocol Categories → Security → MAC ACL → (Protocols)  .

NOTE: If both MAC ACL and Sticky MAC (see §9.4) are active, a packet from a source MAC address is only allowed when the MAC address is allowed in both features.

The MAC ACL wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Service Selection: select the Ethernet service for which a MAC ACL must be configured;
- Port Configuration (only for Ethernet IFMs, see 'Support Matrix' in Ref. [2Net] in Table 1):
  - Port Type: shows the IFM port type;
  - Enable ACL:
    - Unchecked (=default): MAC ACL is disabled for this port, all incoming packets from any source MAC address are allowed on this port.
    - Checked: MAC ACL is enabled for this port. If the source MAC address of the incoming Ethernet packet matches the configured MAC address, the packet will be allowed. If not, the packet will be dropped;
    - Greyed out checkbox: MAC ACL cannot be configured on this port because an IP ACL (see §5.12) has already been configured on this port. Per port, only MAC ACL or IP ACL can be configured, not both together;
  - MAC Address: the MAC Address that must be matched when ACL is enabled. One address can be configured per port. Allowed formats: 'XX-XX-XX-XX-XX-XX', 'XX:XX:XX:XX:XX:XX' or 'XXXXXXXXXXXX' with X=[0..9] [A..F];

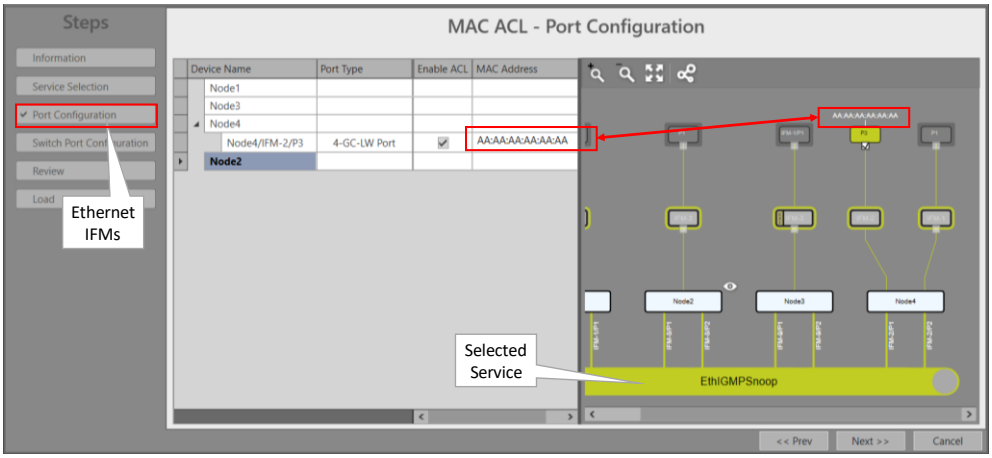

Figure 133 MAC ACL: Port Configuration Example for Ethernet IFMs

- Switch Port Configuration (only for L2/L3 IFMs, see 'Support Matrix' in Ref. [2Net] in Table 1): By default, no MAC ACL rules are created per IFM and as a result, all traffic is allowed. To configure MAC ACL on a front or back end port, create an ACL rule first in the Configuration section (parameters described below), add it to a port and then check Enable ACL in the IFM row. Multiple rules can be added per port.
  - Add rule: select a port row in the device tree view and click the Add Rule button to add the rule to this port. It is possible to select multiple ports by clicking each row while holding the CTRL key pressed, or even by clicking the entire IFM, or by clicking in the tree view area and press CTRL+A to select all IFMs. When clicking the Add Rule button, the configured rule will be added to all selected IFMs.
  - Delete rule: select a rule row in the device tree view and click the Delete Rule(s) button. It is possible to select multiple rule rows by clicking each row while holding the CTRL key pressed, or even by clicking in the tree view area and press CTRL+A to select all rules. When clicking the Delete Rule(s) button, all selected rules will be deleted.
  - Configuration Section:
    - MAC Address: the MAC Address that must be matched when ACL is enabled. Allowed formats: 'XX-XX-XX-XX-XX-XX', 'XX:XX:XX:XX:XX:XX' or 'XXXXXXXXXXXX' with X=[0..9] [A..F];
  - Device Tree view:
    - Port Type: shows the IFM port type;
    - Enable ACL:
      - Unchecked (=default): MAC ACL is disabled for this port, all incoming packets from any MAC address are allowed on this port;
      - Checked: MAC ACL is enabled for this port. MAC Address filled out: If the MAC address of the incoming Ethernet packet matches the filled out MAC address the packet will be allowed. If not, the packet will be dropped.

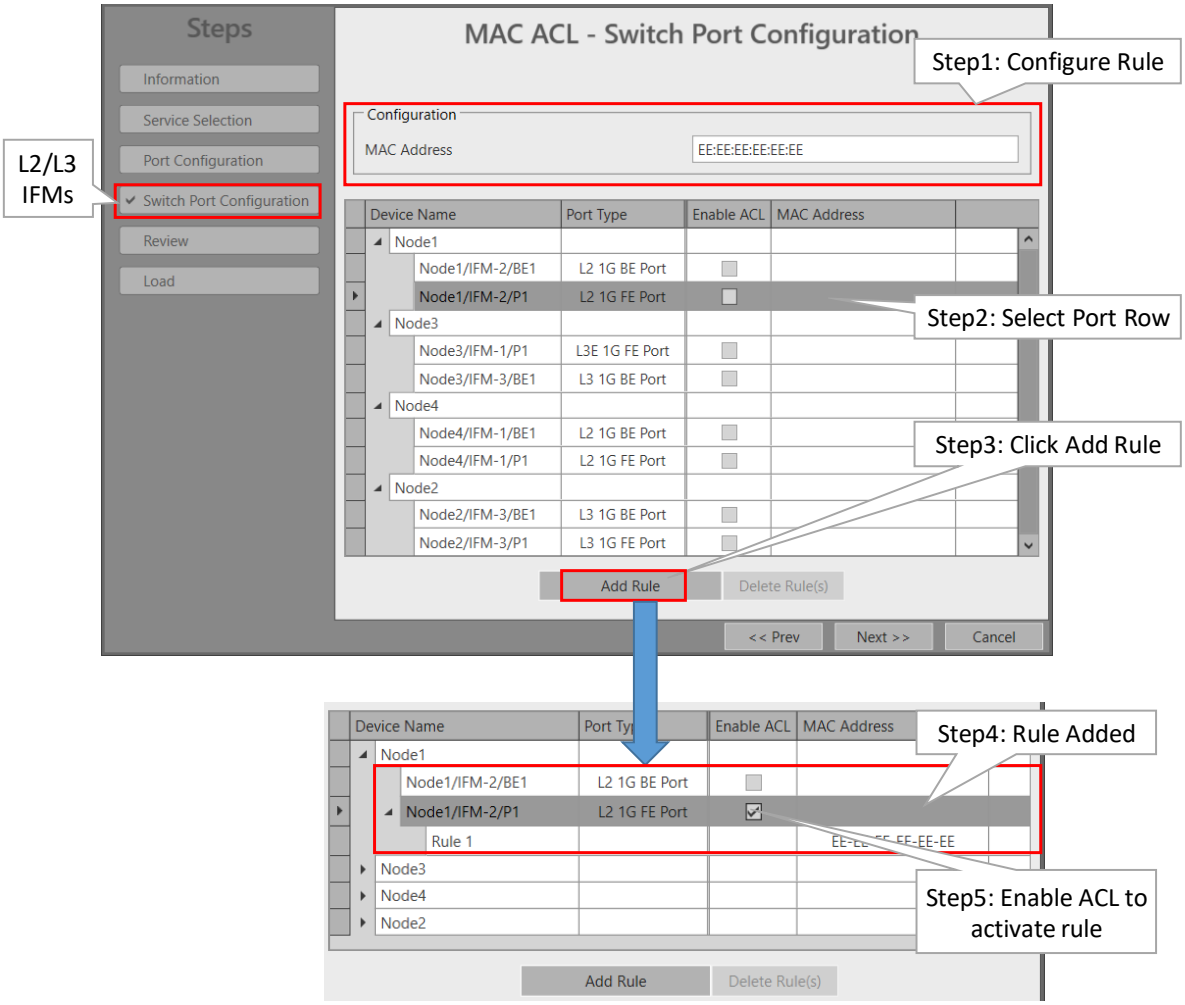

Figure 134 MAC ACL: Switch Port Configuration Example for L2/L3 IFMs

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

NOTE: The MAC ACL for a service can be modified/deleted later on via selecting the service in the MAC ACL list and clicking the / button.

5.13.4 Monitoring Monitoring

None.

6. POWER OVER ETHERNET (POE)

6.1 General

PoE is a technology that allows a 'Powered Device' (=PD, e.g. IP telephones, IP cameras etc.) to receive power from 'Power Sourcing Equipment' (=PSE, e.g. the Dragon PTN node).

PoE delivers a minimum of 48V of DC power over shielded/unshielded twisted-pair wiring for terminals consuming less than 25.5 Watts of power.

Electrical RJ45 ports of the IFMs that support PoE (see support matrix in Ref. [2Net] in Table 1) in the Dragon PTN nodes are able to deliver PoE when external PoE PSUs are connected to the NSM-A (**).

NOTE: (**): NSM-B has no PoE support;

If PoE is needed:

- Connect PoE hardware, see §6.2;
- Configure PoE settings, see §6.3;
- PoE Configuration Rules, see §6.4;
- Status info on the running PoE, see §6.5;

PoE settings and status info can be found in the 'Network Hardware' tile or tab on node, module and port level by selecting a row in the DEVICES list, see figure and paragraphs below.

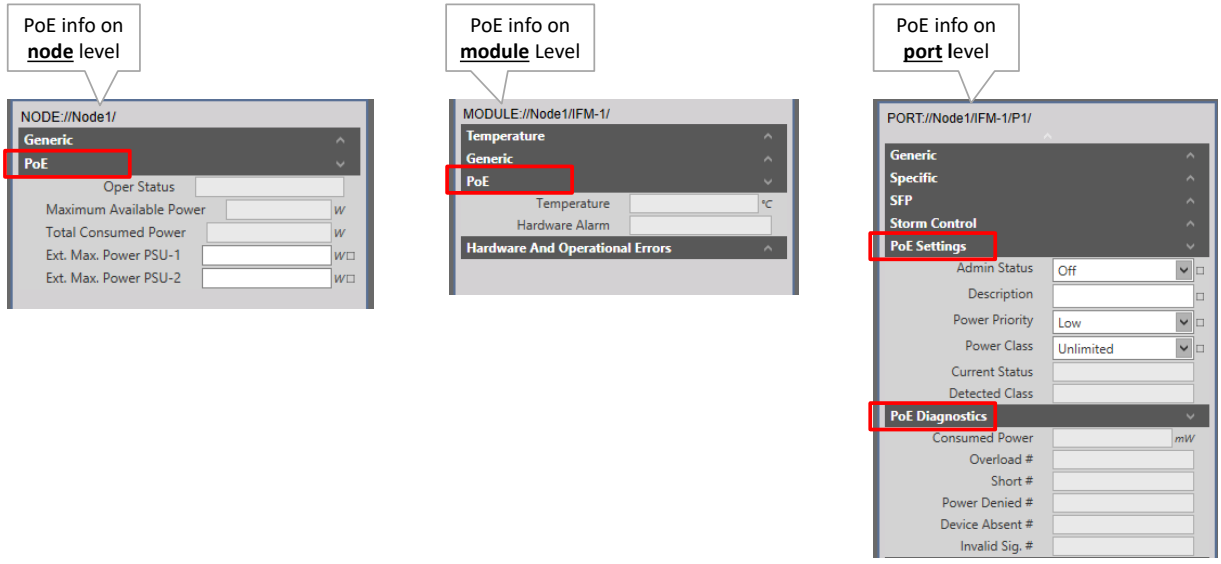

Figure 135 PoE Info on Node/Module/Port Level

6.2 Connect PoE Hardware

1. Connect external PoE PSUs to the NSM-A in the node as described in Ref.[3], [3b];
2. Connect the PDs to the PSEs, the PSEs are the electrical RJ45 ports on IFMs that support PoE (see Ref. [2Net] in Table 1);

6.3 Configure PoE

The PoE settings that can be configured in Figure 135 are explained in the table below. The configuration must be done on node and port level.

Table 16 PoE Configuration Parameters

Level	Parameter	Values	Description
Node: PoE Information	Ext. Max. Power PSU-1/ Ext. Max. Power PSU-2	<value>	PoE PSU1 = PSU connected to PoE1 connector on the NSM-A; PoE PSU2 = PSU connected to PoE2 connector on the NSM-A; These fields represent the power (in Watt) delivered to the node by the PoE PSUs: If PoE PSU1 is used, fill out Ext. Max. Power PSU-1; If PoE PSU2 is used, fill out Ext. Max. Power PSU-2; **ATTENTION**: Follow the configuration rules below §6.4:
Port: PoE Settings	Admin Status	On/Off	**On**: Enables PoE on this port. It still depends on the Power Priority, Classes and Budgets whether power will be delivered effectively. **Off**: Disables PoE on this port.
	Description	<text>	Port description e.g. 'Camera parking1'
	Power Priority	Low/ High/ Critical	Assigns a Power Priority for PoE to the port. 'Critical priority' ports will always get power first, 'Low priority' ports will always get power as last. 'High priority' is in between. If it concerns ports with the same Power Priority, the lowest port numbers on the lowest IFM numbers will get power first.
	Power Class	Unlimited Class 1 Class 2 Class 3/0 Class 4	Configure the desired power class for this PoE port, according to the **configuration rules** in §6.4: A connected PoE device to this port will always get power, but never more than the configured Power Class. Use Unlimited (=40W) when you don't know yet the Power Class of the connected device (=Detected Class). As a result, the device will always get power, and its power class can be detected. When it has been detected, the administrator can change Unlimited into the same class as the Detected Class. According to the configured Power Class, following power levels are delivered at the PoE ports by the node (=PSE side) : Class 0: 15.4 Watt Class 1: 4.0 Watt Class 2: 7.0 Watt Class 3: 15.4 Watt Class 4: 32.0 Watt Unlimited: 40.0 Watt.

6.4 PoE Configuration Rules

Depending on the PSUs, some configuration rules must be taken into account.

6.4.1 Only one PoE PSU Connected

Example, one 300W PoE PSU is connected to PoE1 on the NSM-A.

- Node: Fill out 300W in ‘Ext. Max. Power PSU-1’;
- Ports: Configure the desired Power Class on the desired ports in the node. Make sure to configure a maximum of 300W - 30W = 270W on these ports. 30W is reserved for internal use. E.g. you could configure 8 ports in Class4 (8*32.0 = 256W) and 1 port in Class 2 (1*7.0 = 7W) → 256 + 7 = 263W < 270W;
- Configuring more than 270W on the ports is NOT allowed!

6.4.2 Two PoE PSUs Connected

HiProvision always uses the lowest PSU power of both PSUs to calculate the delivered power. Power aggregation is not supported, also not when both PSU powers are equal.

a. Lowest Power Example

- Same PSU power: both PoE1 and PoE2 PSU deliver 300W → lowest PSU power = 300W;
- Different PSU power: PoE1 delivers 300W, PoE2 480W → lowest PSU power = 300W;

b. Power Calculation Example

Example, the PoE1 PSU delivers 300W and PoE2 PSU delivers 480W.

- Node: Fill out 300W in ‘Ext. Max. Power PSU-1’ and 480W in ‘Ext. Max. Power PSU-2’;
- lowest power = 300W;
- Ports: Configure the desired Power Class on the desired ports in the node. Make sure to configure a maximum of <lowest PSU power> - <internal power> = 300W - 30W = 270W on these ports. 30W is reserved for internal use. E.g. you could configure 8 ports in Class4 (8*32.0 = 256W) and 2 ports in Class 2 (2*7.0 = 14W) → 256 + 14 = 270W <= 270W;
- Configuring more than 270W on the ports is NOT allowed!

6.5 PoE Status

The PoE status info available in Figure 135 is explained in the table below:

Table 17 PoE Status Info

Level	Parameter	Values	Description
Node	Oper Status	On/Off/Faulty	**On**: PoE module is up and running **Off**: PoE module is down **Faulty**: No PoE is delivered due to a failure
	Maximum Available Power	<value>	The total power (in Watt) that the node can deliver. If two PoE PSUs are connected to the NSM-A, it will be the lowest value of both 'Ext. Max Power PSU-1' and 'Ext. Max Power PSU-2' values filled out.
	Total Consumed Power	<value>	The total PoE power (in Watt) that all the ports together in the node deliver, e.g. if 4 cameras are connected to 4 ports, each consuming 5 Watt, then the Total Consumed Power will be 4*5W = 20W for this node.
Module	Temperature	<value>	The temperature of the PoE chip in °C.
	Hardware Alarm	OK/PoE Alarm	**OK**: no alarm on the PoE chip, everything fine **PoE Alarm**: PoE chip failure, reboot the IFM, replace the IFM if the failure persists.
Port: PoE Settings	Current Status	Disabled Searching DeliveringPower Fault OtherFault Testing	**Searching**: The Node is checking the connected Power Device (PD) before power delivery. The node negotiating the class, priority... No power is delivered yet to the PD. **DeliveringPower**: There is enough power budget left to deliver power to this PD, the node is really delivering power to the PD. **Fault**: There is an external problem on the PoE line or port, e.g. the PD requests power beyond its allowed power range. No power is delivered to the PD. **OtherFault**: PoE chip has been disabled due to external power problem. **Testing**: Port in test mode.
	Detected Class	Class 0 Class 1 Class 2 Class 3 Class 4	The measured or detected power class of the connected PoE device (PD). By default, when no PoE device is connected yet, 'Class 0' is indicated. When the PoE device (e.g. Class 2) is connected afterwards, its Power Class (Class 2) will be indicated. Afterwards, when the PoE device has been removed, the last remembered Power Class (Class 2) is still displayed, although no device is connected at that time.
Port: PoE Diagnostics	Consumed Power	<value>	The consumed power in milliWatt that the power device (PD) currently is consuming.
	Overload #	<value>	The number of overload conditions so far. Each time the PD on this port asks more power than its configured class allows, the counter increases with one.
	Short #	<value>	The number of shortcut conditions on this port so far.
	Power Denied #	<value>	The number of times that power delivery has been denied on this port.
	Device Absent #	<value>	The number of times that power has been removed because a powered device dropout was detected.
	Invalid Sig. #	<value>	The number of times that an invalid signature on PD has been detected. A signature indicates that a PD is a valid PD or not.

7. LAYER2: LINK AGGREGATION/LAG (=LINK AGGREGATION GROUP)

7.1 Prerequisites

At least one node must have configured an IFM that supports LAG. Only available LAN ports that are not yet configured in a service can be selected to create a LAG. See the feature matrix in Ref. [2Net] in Table 1 to find out which IFMs support LAG.

7.2 General

Link Aggregation is the bundling (=aggregation) of multiple physical Ethernet links between a source and destination side into one combined logical Ethernet link. A LAG is a combination of multiple Ethernet LAN ports within one logical port group, maximum 8 ports per LAG and 8 LAGs per node. The Link Aggregation is the communication between two LAGs. E.g. one LAG in one Dragon PTN node and the second LAG in a third party switch/application. For 1G ports, all the ports of the source and destination LAG must be in autonegotiation. On the Dragon PTN side, ports with the same speed and linked to the same switch ASIC (CSM, L2 or L3) can be added to the same LAG. Each bullet shows the possible LAG ports per switch ASIC:

- CSM: all Ethernet IFM ports (4-GC-LW, …) of the same speed in the same node;
- L2: all 6-GE-L IFM ports;
- L3: all 9-L3A-L / 9-L3EA-L IFM ports of the same speed;

NOTE: Example: Ports in different nodes can not be added to the same LAG because they are linked to different switch ASICs. CSM (4-GC-LW, …), L2 and L3 ports in a same node can not be added to the same LAG because they are linked to different switch ASICs.

NOTE: LAG on WAN ports and L2/L3 back end ports is not supported.

The resulting combined logical link:

- has at least the bandwidth of one individual link (1 Gbps bandwidth for a 1G port, 10 Gbps for a 10G port), but can have more bandwidth if both conditions below are met:
  - multiple streams from different MAC addresses are streamed over the LAG;
  - the LAG algorithm loadshares these streams over different links within the LAG;
- offers loadsharing based on the source and destination MAC addresses;
- offers redundancy in case one of the individual links should fail.

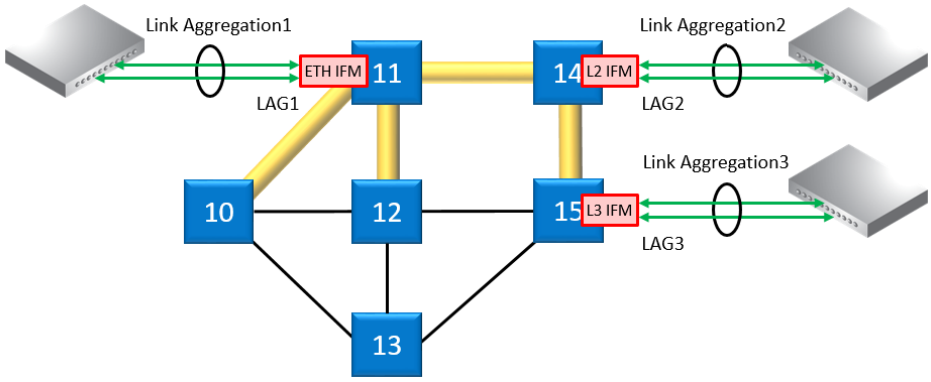

Figure 136 Link Aggregation and LAGs

CAUTION: If you want to enable OSPF on a LAG, configure the LAG in a VLAN. A LAG configured on router ports (L3 IFM) does not support OSPF (see §5.7)!

7.3 Configuration

1. Link Aggregation can be configured via Dashboard → Network Hardware → Select Node with IFM that supports LAG → click ;

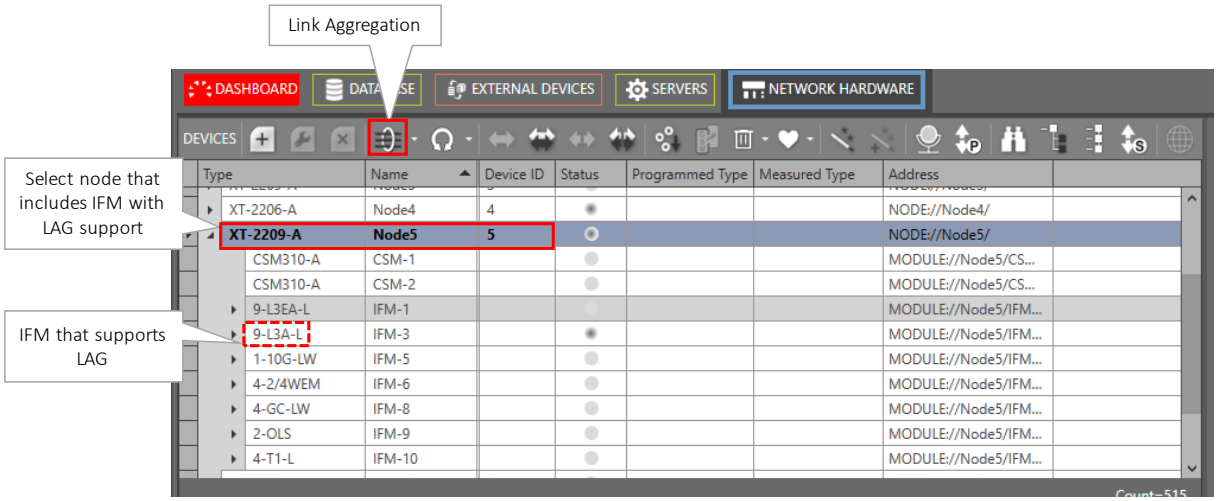

Figure 137 Link Aggregation Configuration

2. Options:
   - Create LAG (see §7.3.1);
   - Modify LAG (see §7.3.2);
   - Delete LAG (see §7.3.3);

7.3.1 Create LAG

NOTE: Maximum 8 LAGs per node can be created.

1. Select a node (by selecting the row) in the Devices list that has at least one IFM that supports LAG (see Ref. [2Net] in Table 1).
2. Click → Create LAG;
3. The Link Aggregation wizard opens. The list below summarizes every page in the wizard:
   - Information: Click Next>>;
   - Creation: Fill out the parameters below. The example figure below shows a LAG configuration between a main and an extension L3 IFM. A LAG can be created as well between Ethernet IFM ports linked to the same CSM switch ASIC or a LAG can be created between the L2 IFM ports.

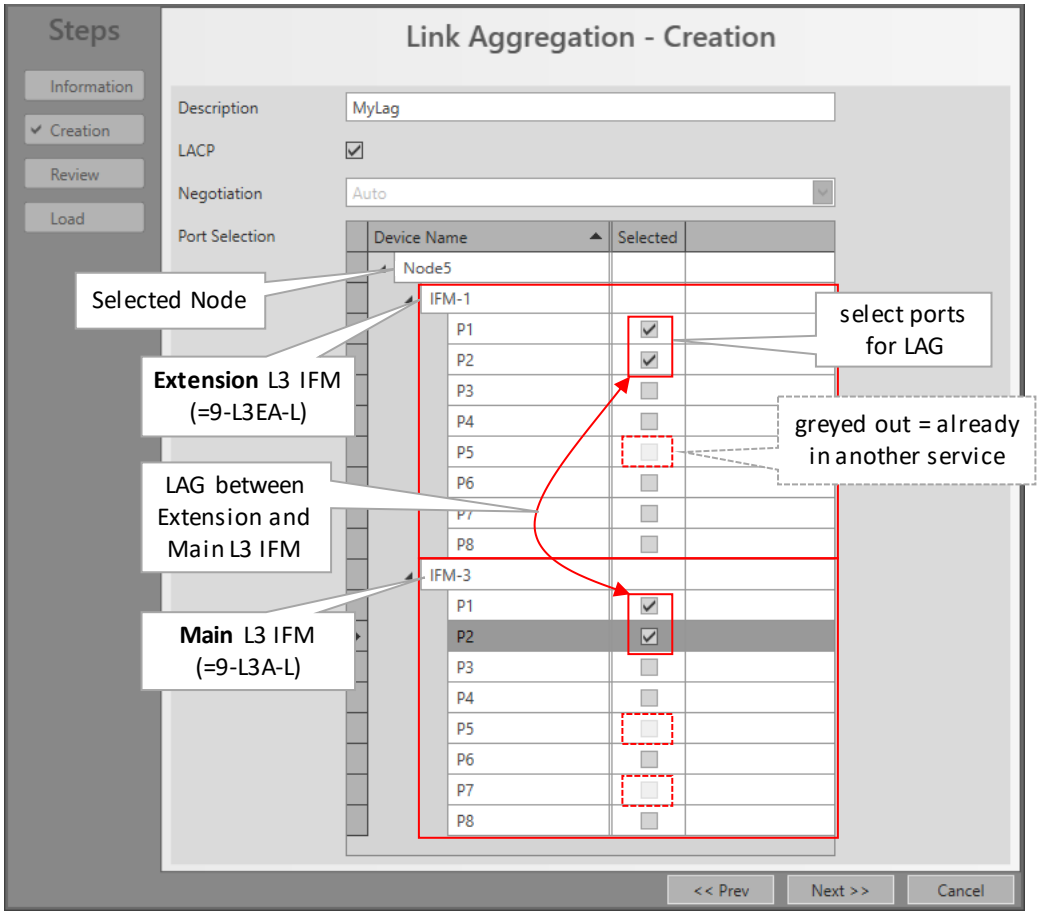

Figure 138 Create LAG

- Description: a short description for this LAG instance;
- LACP (=Link Aggregation Control Protocol): LACP provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
  - unchecked (=default): LACP is disabled, the LAG will still performs some kind of basic bundle negotiation with the other side;
  - checked: LACP is enabled;
- Negotiation:
  - Auto (=default): All the ports in the LAG will be configured in AutoNegotiation. AutoNegotiation advertises and negotiates the speed and duplex mode(s) of the ports within the LAG, with the destination LAG. The individual configured port speed and duplex modes in HiProvision will be ignored;
- Port Selection: Shows the selected node with all the IFMs that support LAG and its available LAN ports (=not yet configured in a service or another LAG). Click the Selected checkbox to add a port to the LAG:
  - If you select a port, only ports of the same speed and ports connected to the same switch ASIC remain selectable, other ports will be greyed out. Combining ports between the main L3 IFM and its extension L3 IFM is possible because they both share the same switch ASIC;

- a LAG requires minimum 2 ports and maximum 8 ports. Selecting more than 8 ports will result in the figure below later on when finishing the wizard:

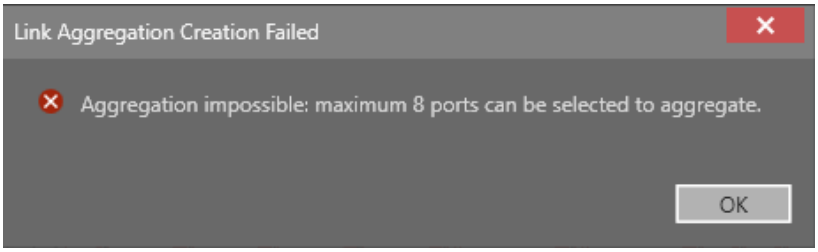

Figure 139 Link Aggregation Failed: Aggregation Impossible

- Review: If OK, click Finish. The configuration load manager will be invoked.
- Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

- After creation, the LAG will be visible in the IFM with the configured LAG, see figure below. For LAGs on an extension L3 IFM, its LAG will be visible in its associated main L3 IFM;

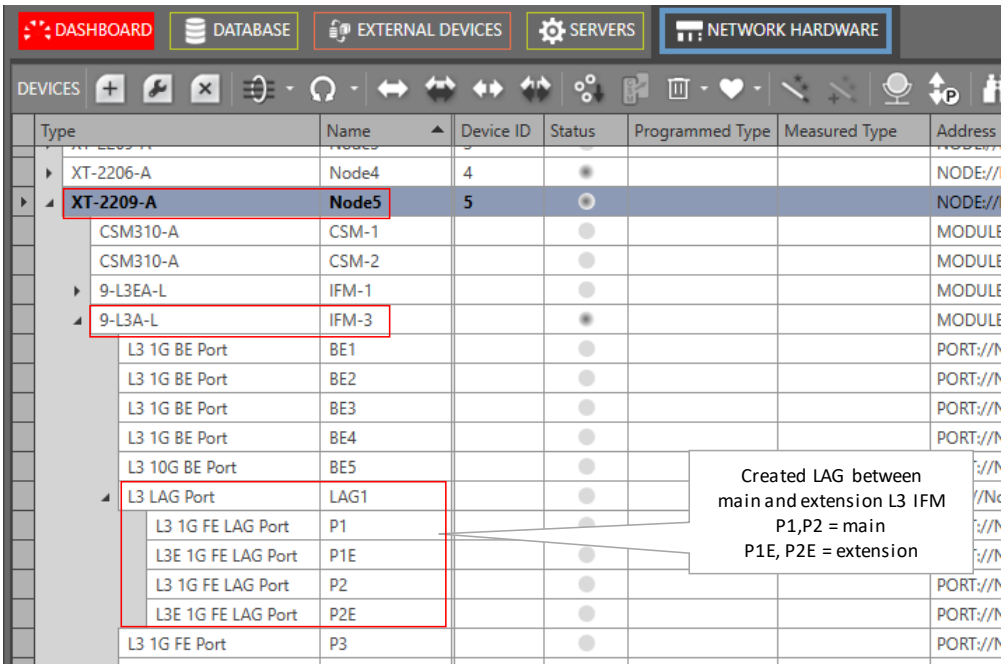

Figure 140 Created LAG

7.3.2 Modify LAG

1. Select the LAG that must be modified via selecting its '<IFM> LAG Port' row in Figure 140.

2. Click → Modify LAG;
3. The Link Aggregation wizard opens. The list below summarizes every page in the wizard:
   - Information: Click Next>>;
   - Modification:
     - Description: can be modified;
     - LACP: can not be modified;
     - Negotiation: can not be modified;
     - Port Selection: can be modified. Unselected ports are ports of the same speed that are neither configured in a service nor configured in another LAG.

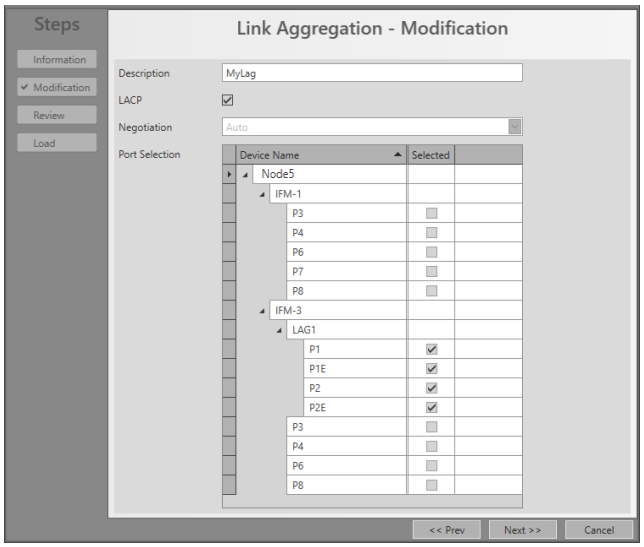

Figure 141 Modify LAG

   - Review: If OK, click Finish. The configuration load manager will be invoked.
   - Load: The configuration load manager is a tool that starts and monitors the load process of a HiProvision configuration. Click the Load button to load the new HiProvision configuration into the live network. See Ref. [2Mgt] in Table 1 for more info.

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

   - After modification, the modified LAG will be visible in the IFM with the configured LAG. For LAGs on an extension L3 IFM, its LAG will be visible in its associated main L3 IFM;

7.3.3 Delete LAG

1. Select the LAG that must be deleted via selecting its '<IFM> LAG Port' row in Figure 140.
2. Click → Delete LAG;
3. The LAG will be removed from the port list.

8. LOOPBACK INTERFACE

8.1 Prerequisites

At least one node must have configured a L3 IFM.

8.2 General

The loopback interface is a virtual interface meant for management purposes. This loopback interface will be mainly used by the PIM (see §5.6) and the OSPF (see §5.7) protocol.

This interface can be added to a Virtual Router and is always up and running. It assures that a PIM-SM or OSPF instance on this virtual router remains up and running. In the Virtual Router, an IP address (not in the range 127.x.x.x/24) must be assigned to this loopback interface.

8.3 Configuration

1. Loopback Interface can be configured via Dashboard → Network Hardware → Select Node with IFM that supports Loopback Interface → click → Create Loopback Interface;

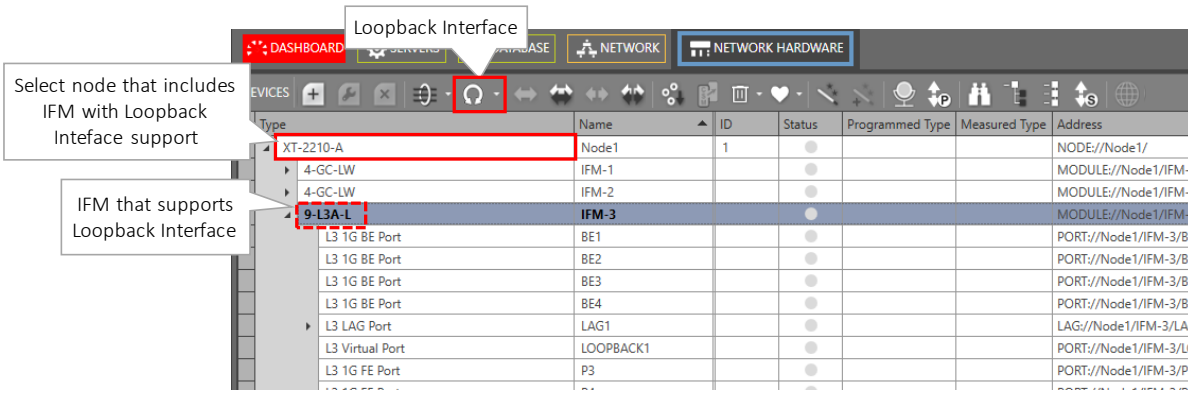

Figure 142 Loopback Interface

2. After creation, the loopback interface shows up as a 'L3 Virtual Port' in the IFM treeview:

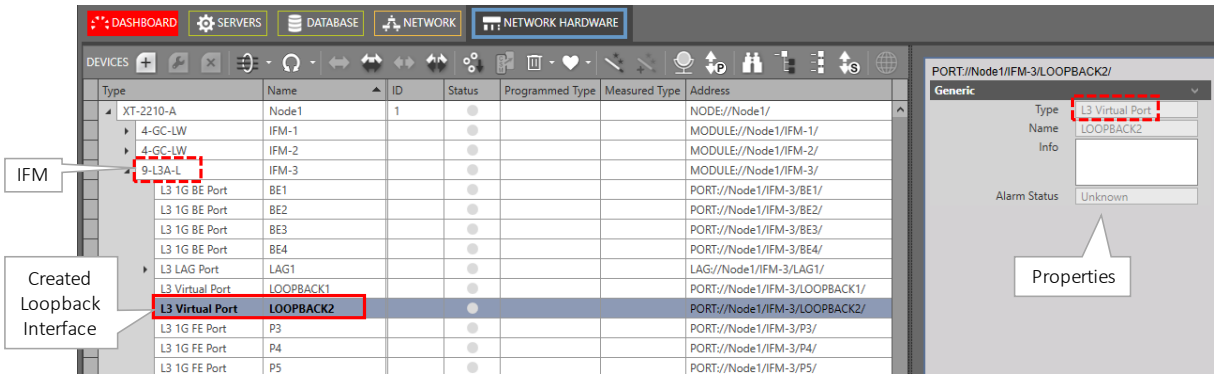

Figure 143 Created Loopback Interface

NOTE: A loopack interface can be deleted via selecting L3 Virtual Port in the treeview → click → Delete Loopback Interface.

3. The created loopback interface can be used later on in the port selection of the Virtual Router wizard (§5.9), see below:

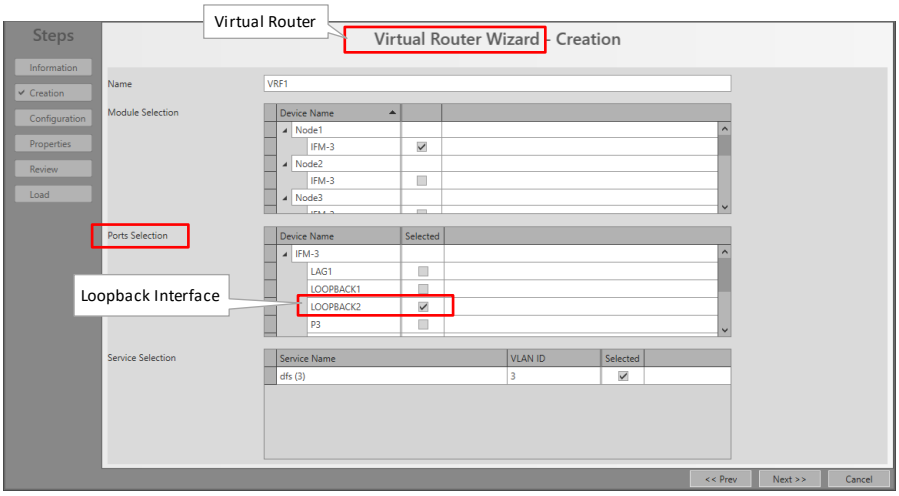

Figure 144 Virtual Router Wizard: Loopback Interface

9. TRAFFIC CONTROL / SECURITY

9.1 E-Tree

9.1.1 General

NOTE: Supported on IFMs according feature matrix in Ref. [2Net] in Table 1.

An E-Tree is a rooted (not routed) point-to-multipoint partial service within a programmed Ethernet service, see figure below. This E-Tree can be used on any tunnel topology except a point-to-point topology.

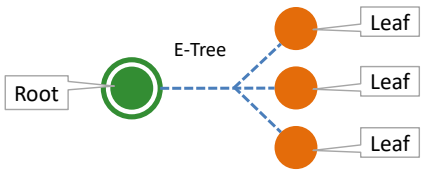

Figure 1 E-Tree: Root/Leaf

E-Tree can be used as a security precaution to separate different customers using the same Ethernet service while accessing one or more roots (e.g. ISPs).

When an E-Tree is used, each service endpoint is designated as either **leaf** or **root**.

- Security:
  - **Leaf**: Can only communicate with one or more 'roots', not with other 'leafs';
  - **Root**: Can communicate with any element ('root' or 'leaf') in the service. Multiroot is possible to obtain load sharing and redundancy. Up to a maximum of 4 roots and 128 leafs per service can be configured;

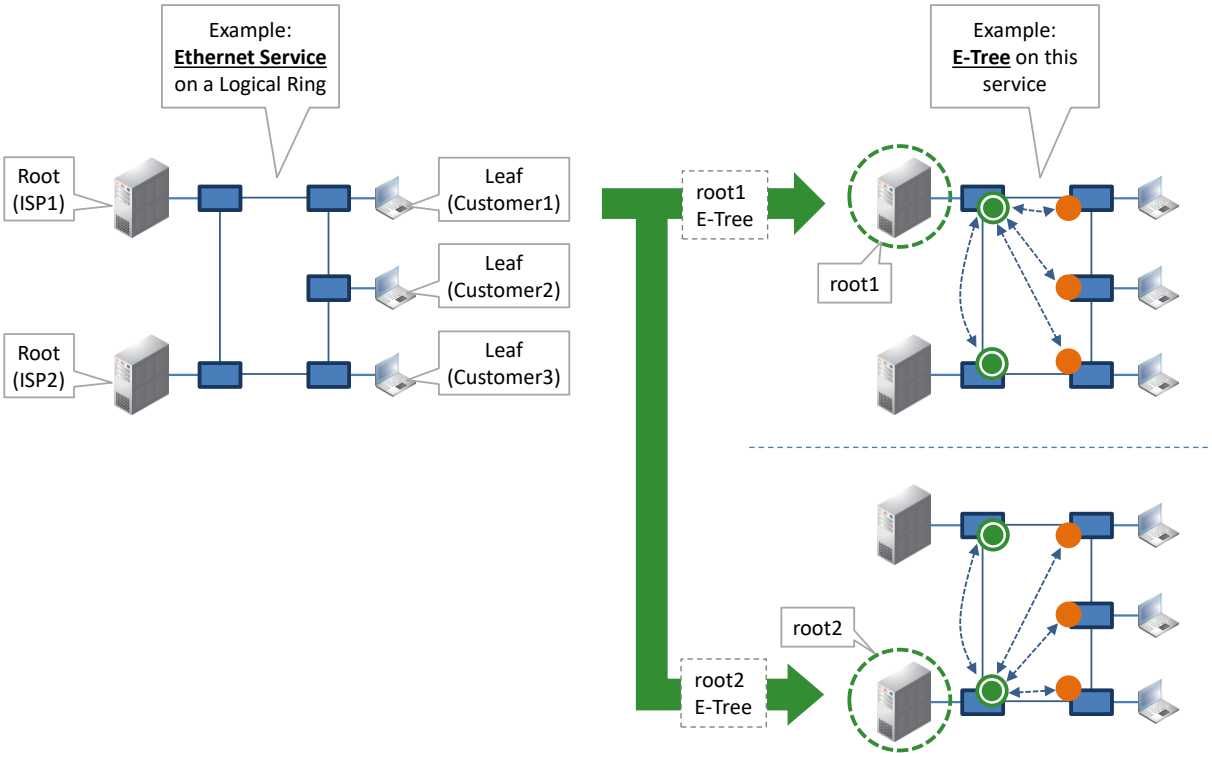

Figure 2 Example: Ethernet + E-Tree Communication

9.1.2 Configuration

See Ethernet Service wizard in §2.

9.2 Storm Control on Ethernet LAN Port

9.2.1 General

NOTE: Storm Control is not relevant/supported on WAN Ports;

A traffic storm is the growing of excessive network traffic due to Ethernet packets flooding the LAN. Such a storm can for example occur because of a data loop in the network due to no or misconfiguration of MSTP. These storms degrade the network performance and must be avoided whenever possible.

The storm control feature:

- is an extra protection against these traffic storms;
- limits the amount of unlearned received data (Unicast, Broadcast, Multicast) on the LAN port ingress or input side;
- limits the amount of transmitted data (all data) on the LAN port egress or output side;
- Data that exceeds the configured limitations will be dropped. As a result, a possible data storm cannot overload the node processor or the node will limit outgoing data.

9.2.2 Configuration

Storm control can be configured on the port properties of an Ethernet LAN port in the Network Hardware tile, see figure below.

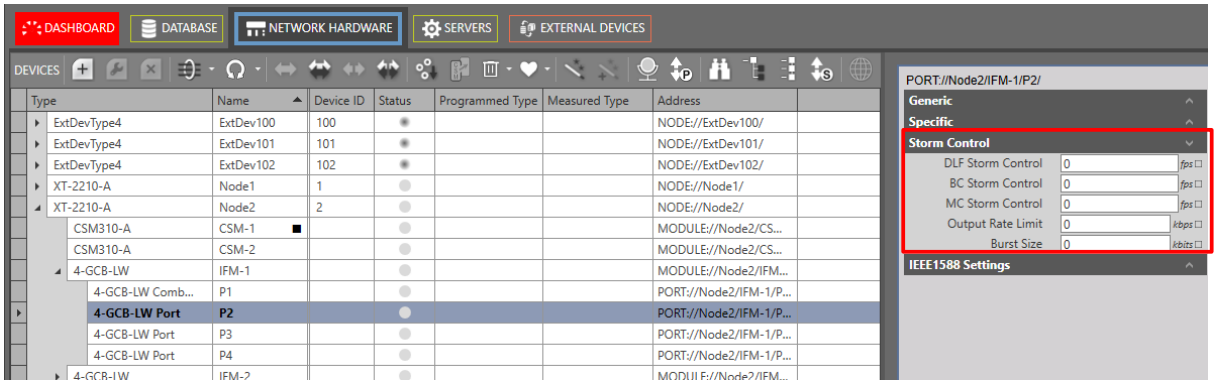

Figure 3 Port Properties: Storm Control

- Ingress (or input) traffic on a LAN port:
  - DLF (default = no limits, range [0-262142] fps): DLF = Destination Lookup Failure, limits the incoming unicast traffic with an unknown destination to the configured frames per second (=fps);
  - BC (default = no limits, range [0-262142] fps): BC = Broadcast, limits the incoming Broadcast traffic to the configured frames per second (=fps);
  - MC (default = no limits, range [0-262142] fps): MC = Multicast, limits the incoming Multicast traffic to the configured frames per second (=fps);
- Egress (or output) traffic on a LAN port:
  - Output Rate Limit (default = no limits, range [0-16777215] kbps): limits all outgoing traffic to the configured kbps;
  - Burst Size (default = no limits, range [0-80000000] kbits): limits the outgoing burst size to the configured kbits;
- Click the Apply button;
- Load to network (see 'Load Manager' Ref. [2Mgt] in Table 1 for more info).

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

NOTE: Frame loss or drop can be detected and verified via dropped packet alarms (in the Alarms tile) and the 'Disc In Packets'/'Disc Out Packets' counters (in the performance Tile), see 'Port Performance' → 'CSM Ethernet Port Monitoring' in Ref. [2Net] in Table 1.

9.2.3 Reset Storm Control

Enter value '0' or erase the field value in these fields to disable or reset the limitation for this specific field. As a result, all traffic will be processed again for the field and port that has been reset.

9.2.4 When to Reset Storm Control on a Port?

- When you have customized storm control on a port and one of the following events occur on this port:

- the Port Mode (LAN/WAN) changes via Dashboard → Network Hardware → Network Settings Wizard button = → Port Mode;
- the port is removed from a service;
- the entire service including this port, has been deleted.

9.3 BPDU Guard on Ethernet LAN Port

NOTE: See Ref. [2Net] in Table 1 where the port propery feature BPDU Guard is supported. It is not relevant/supported on WAN Ports. BPDU Guard on L2/L3 IFMs is supported via the MSTP protocol wizard, see §5.4;

BPDU Guard (=Bridge Protocol Data Unit) is a LAN port property or feature that shuts down the LAN port when a BPDU packet enters this port. As a result, this feature or IFM:

- protects the network against possible loops created via this IFM, although this IFM does not support MSTP;
- protects a running MSTP protocol somewhere else in the Dragon PTN network from external MSTP influences via this LAN port, e.g. root bridge protection etc...

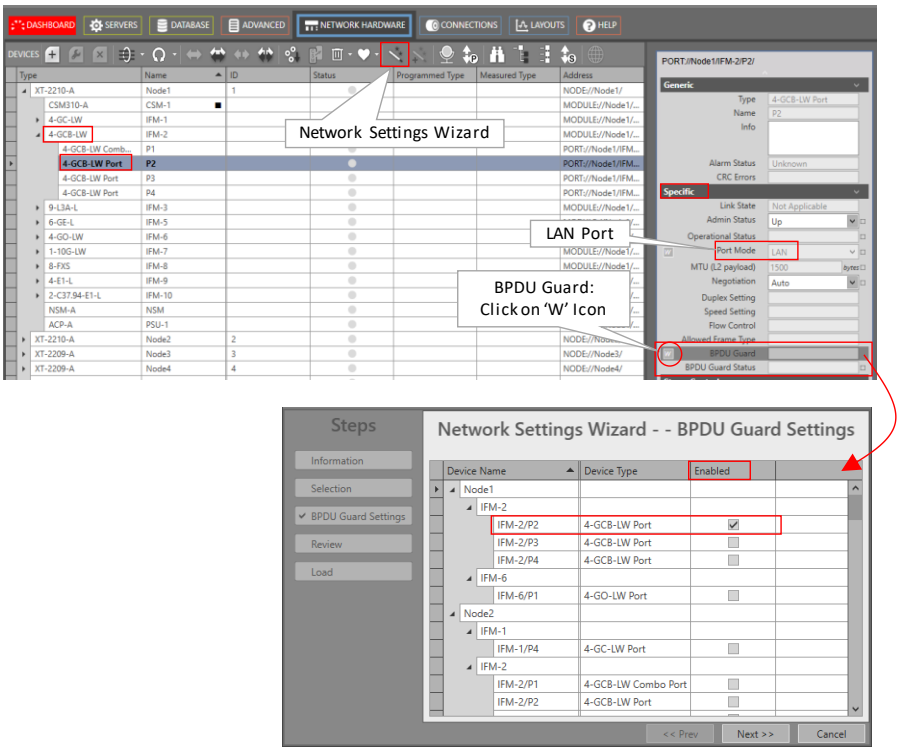

Figure 4 BPDU Guard on Ethernet LAN Port

There are two ways to configure this setting:

1. Via clicking the 'W' icon on port level in the Network Hardware tile→ Network Settings – BPDU Guard wizard opens;
2. Going directly to the Network Settings wizard via Network Hardware tile → Network Settings Wizard button = → BPDU Guard Mode → Network Settings – BPDU Guard wizard opens.

- In the BPDU Guard wizard, find your LAN port that must be configured. If your port is not in the list, it is probably a WAN port;
- Configure the 'Enabled' checkbox of your port:
  - Disabled (=default, enabled = unchecked):
    - the port will not send out dummy BPDU packets;
    - the port remains up in case of a loop;
    - the port will not be disabled when a BPDU packet enters the port. As a result, a possible running Dragon PTN MSTP instance in the same service as the port, is not protected from external MSTP influences via this port. CAUTION: a device connected to this port could be selected as MSTP root bridge when a Dragon PTN MSTP is running in the same service, resulting in a topology change in the Dragon PTN network.
  - Enabled (=checked):
    - the port will send out dummy BPDU packets itself;
    - the port will be disabled when a BPDU packet enters the port. Possible running Dragon PTN MSTP instances are protected from external MSTP influences via this port. The port can be re-enabled by setting the Admin Status of the port properties Down and click Apply (and Load) and setting it back Up and click Apply (and Load).
- BPDU Guard Status:
  - Inactive: BPDU Guard is disabled;
  - Secure Up: BPDU Guard is enabled and no BPDU packet has entered the port yet. The port is still up. All traffic allowed;
  - Port Shutdown: BPDU Guard is enabled and a BPDU packet has entered the port. As a result, the port has been shut down. No traffic possible via this port;
  - Secure Down: BPDU Guard is configured but could not be enabled because of a conflict with other features.

9.4 Sticky MAC

Prerequisite: Ethernet service must have been created on a tunnel different from a point-to-point tunnel.

Sticky MAC is a Layer2 service security feature that allows new MAC addresses to be learned until 'Sticky MAC' has been enabled.

Enabling it converts all the dynamically learned MAC addresses into static MAC addresses for all the ports in the selected Ethernet service. Furthermore, it disables the dynamic MAC address learning for this service entering these ports.

NOTE: Sticky MAC and MAC Limiting (§9.5) cannot be used together on the same node.

NOTE: These settings and MAC address tables remain after a reboot.

If sticky MAC has been enabled, received packets from unknown MAC addresses will be dropped. The unknown device will have no access to this service.

Exceptions can be made by configuring a port as 'trusted port'. A 'trusted port' will still have the dynamic MAC address learning process available and also allow new MAC addresses.

To configure Sticky MAC, click Dashboard → Connections → Services →  ;

The Sticky MAC wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Sticky MAC Parameters:
  - Services: **Enabled**:
    - unchecked (=default): Sticky MAC is not enabled meaning that the dynamic MAC address learning process is active. New MAC addresses can be connected to the service ports, and will be learned by the nodes. If the Sticky MAC feature was enabled and you disable or uncheck it, the static stored MAC addresses will be cleared for this service and the dynamic MAC address learning process will be reactivated.
    - checked: Sticky MAC is enabled meaning that the dynamic MAC address learning process is not active or blocked for this service. Only static MAC addresses available in the MAC address table (see §9.6) are allowed. New devices or MAC addresses will not be allowed. If the feature was disabled or unchecked, enabling it will convert all the dynamically learned MAC addresses into static MAC addresses for all the ports in the selected Ethernet service. Furthermore, the dynamic learning process will be blocked.
  - Ports: Trusted Port:
    - unchecked (=default): This is not a trusted port and must be secured. This port operates according to the Sticky MAC feature.
    - checked: This is a trusted port and must not be secured, it will ignore the Sticky MAC feature. The dynamic MAC address learning process remains active.
  - If OK, click Finish. The configuration load manager will be invoked. The configuration load manager is a tool that starts and monitors the load process, after clicking the Load button, of loading a HiProvision configuration or database into the live network. See Ref. [2Mgt] in Table 1 for more info;

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

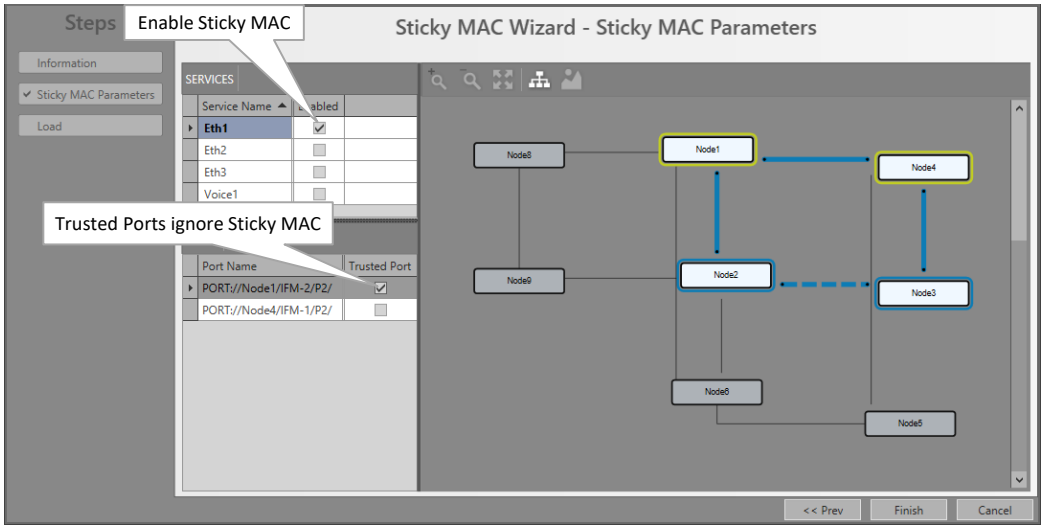

Figure 5 Sticky MAC Configuration

NOTE: When it concerns a VLAN based Ethernet service, the Sticky MAC feature and Trusted Port only have impact on the VLANs within the ports, and not the entire port.

NOTE: If both MAC ACL (see §5.13) and Sticky MAC are active, a packet from a source MAC address is only allowed when the MAC address is allowed in both features.

NOTE: MAC Monitor (§9.7) shows the MAC Address table in the live network.

9.5 MAC Limit

Prerequisite: Ethernet service must have been created on a tunnel different from a point-to-point tunnel.

NOTE: Sticky MAC (§9.4) and MAC Limit cannot be used together on the same node.

MAC Limit is a Layer2 node security feature that sets or limits the number of MAC addresses that a service in a node (or device) can hold in its MAC table.

To configure MAC Limit, click Dashboard → Connections → Services →  ;

The MAC limit wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- MAC Limit Parameters:
  - Devices: **Enabled**:
    - unchecked (=default): MAC limitation is disabled on the device meaning that the device can address the maximum MAC address table size (=32767 MAC addresses). If you want to fine-tune the MAC address usage per configured service on this device, check this checkbox.
    - checked: MAC limitation is active on the device. Per service, the number of MAC addresses can be limited by configuring the **Table Size**.

- Services: **Table Size** (default = 500 for Ethernet service): Only relevant when MAC limit is enabled on the device. Configure the Table Size to limit the number of MAC addresses allowed per service on this device. Try to estimate how many MAC addresses or external devices (e.g. cameras, etc.) that will be used in this service on all nodes, and add some extra addresses for some extra margin. Configure this total amount in the Table size field. The maximum sum of all Table Sizes in a device is 32767.
- If OK, click Finish. The configuration load manager will be invoked. The configuration load manager is a tool that starts and monitors the load process, after clicking the Load button, of loading a HiProvision configuration or database into the live network. See Ref. [2Mgt] in Table 1 for more info;

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

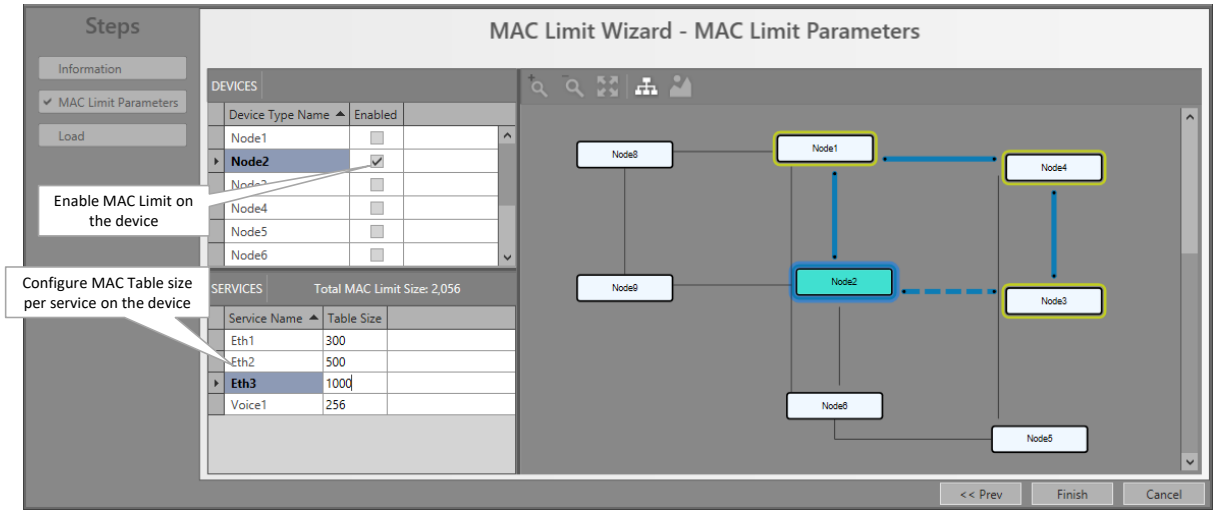

Figure 6 MAC Limit Configuration

NOTE: Best practice to set the same MAC limit on all nodes within a service.

NOTE: When you disable MAC limit on a device, all the dynamic learned MAC addresses (for all services) will be flushed or cleared on this device.

NOTE: When you modify the Table size, the dynamic learned MAC addresses for this service will be flushed or cleared.

NOTE: MAC Monitor (§9.7) shows the MAC Address tables in the live network.

9.6 Static MAC Table

Prerequisite: Ethernet must have been created on a tunnel different from a point-to-point tunnel.

Via the Static MAC Table, it is possible to manually add/remove static MAC addresses per port in a service. The addresses will be added to/removed from the node and the HiProvision database.

Furthermore it is possible to import 'Sticky MAC' static MAC addresses from the node into the HiProvision database.

All these static MAC addresses will be stored in the HiProvision database. As a result, these addresses will not be lost at reboot or clear of the node.

To configure Static MAC addresses, click Dashboard → Connections → Services →  ;

The static MAC wizard opens. The list below summarizes every page in the wizard:

- Information: Click Next>>;
- Select Port and Service: Select the service and port on which static MAC addresses must be configured.
  - Click the **Selected** checkbox to select the service;
  - Click the **Selected** checkbox to select the port.
  - Click Next>>;

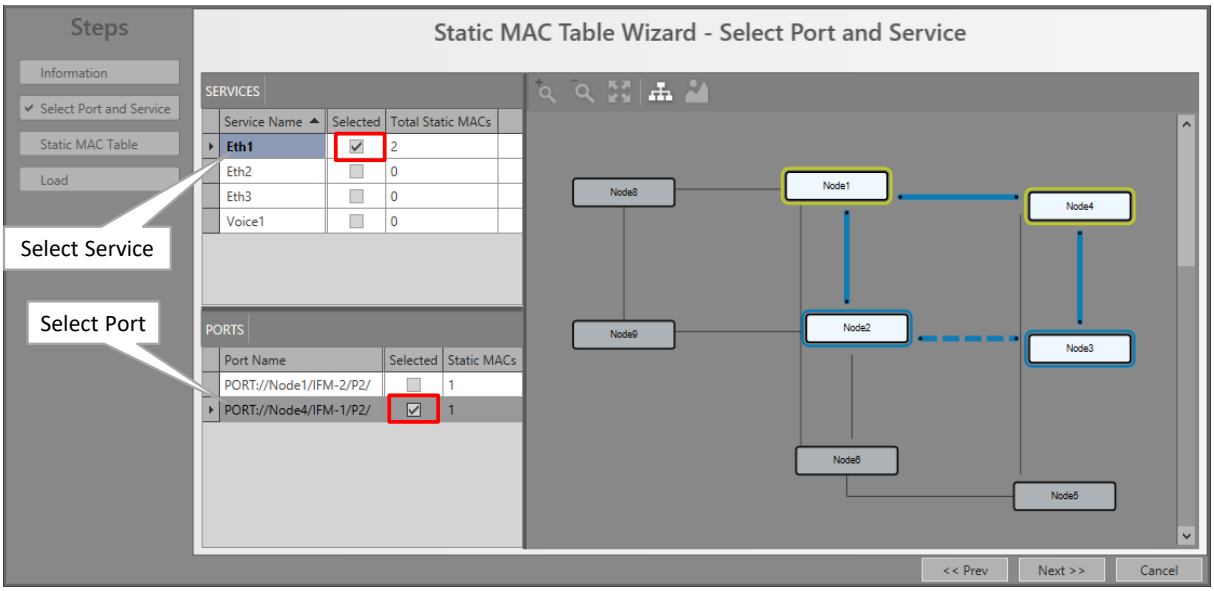

Figure 7 Static MAC Table: Service/Port Selection

- Static MAC Table:
  - Click  to add a static MAC address in the node and the HiProvision database;
  - Click  to import static MAC addresses from the node into the HiProvision database. This import is useful for static MAC addresses that where created on the node via the Sticky MAC feature;
  - A **Source** field indicates whether the MAC address was added manually or by import.
  - If OK, click Finish. The configuration load manager will be invoked. The configuration load manager is a tool that starts and monitors the load process, after clicking the Load

button, of loading a HiProvision configuration or database into the live network. See Ref. [2Mgt] in Table 1 for more info;

CAUTION: While the loading to the Dragon PTN network is in progress, do not turn off, shut down or restart the HiProvision Server or Agent, since this may cause database corruption and network problems!

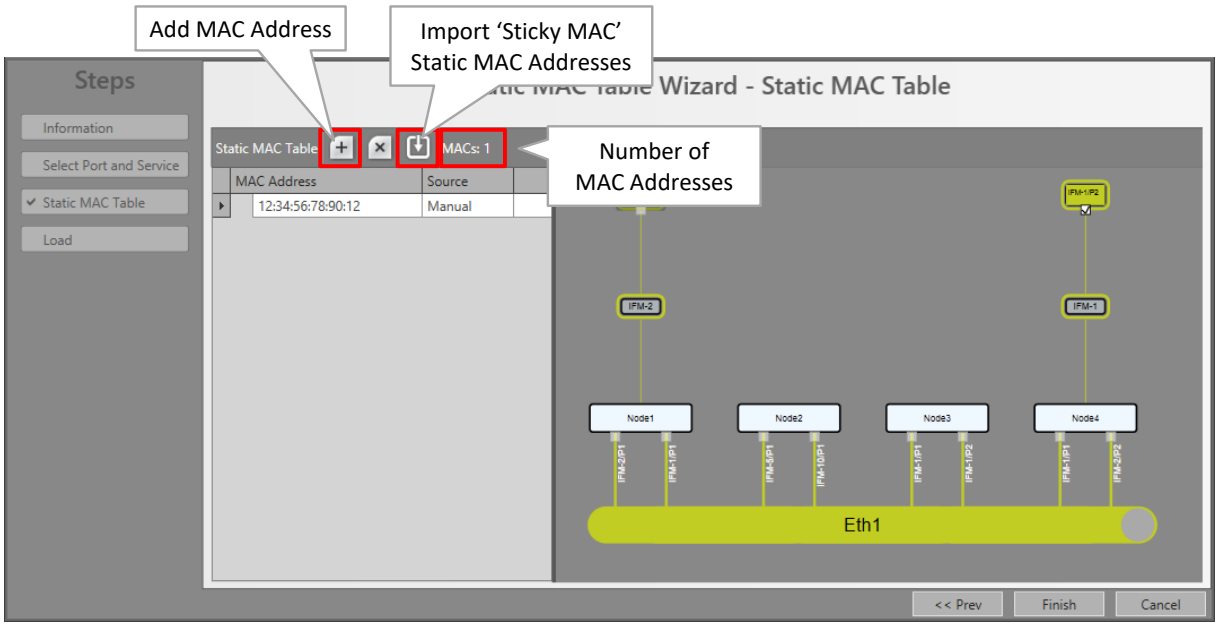

Figure 8 Static MAC Table: Add/Remove/Import

NOTE: MAC Monitor (§9.7) shows the MAC Address tables in the live network.

9.7 MAC Monitor

Prerequisite: HiProvision has to be online.

The MAC Monitor will show the MAC address table of the selected Node (=CSM), L2 or L3 module. This table includes all MAC addresses used on this device except for the MAC addresses that are used in a point-to-point tunnel. The MAC Address table is influenced by the following features:

- Sticky MAC (see §9.4);
- MAC Limit (see §9.5);
- Static MAC (see §9.6);
- MAC ACL (see §5.13);

Click Dashboard → (Monitoring) Network → Services → ;

Click the Device in the devices list to show its MAC Address table. The MAC addresses are by default grouped per service. If you want to ungroup them, drag and drop the 'Service Name' field in the table header row. If the service name is empty, it concerns MAC addresses from neighboring nodes that cannot be mapped on a service.

The total number of MAC addresses in the device is indicated in the top-right hand corner.

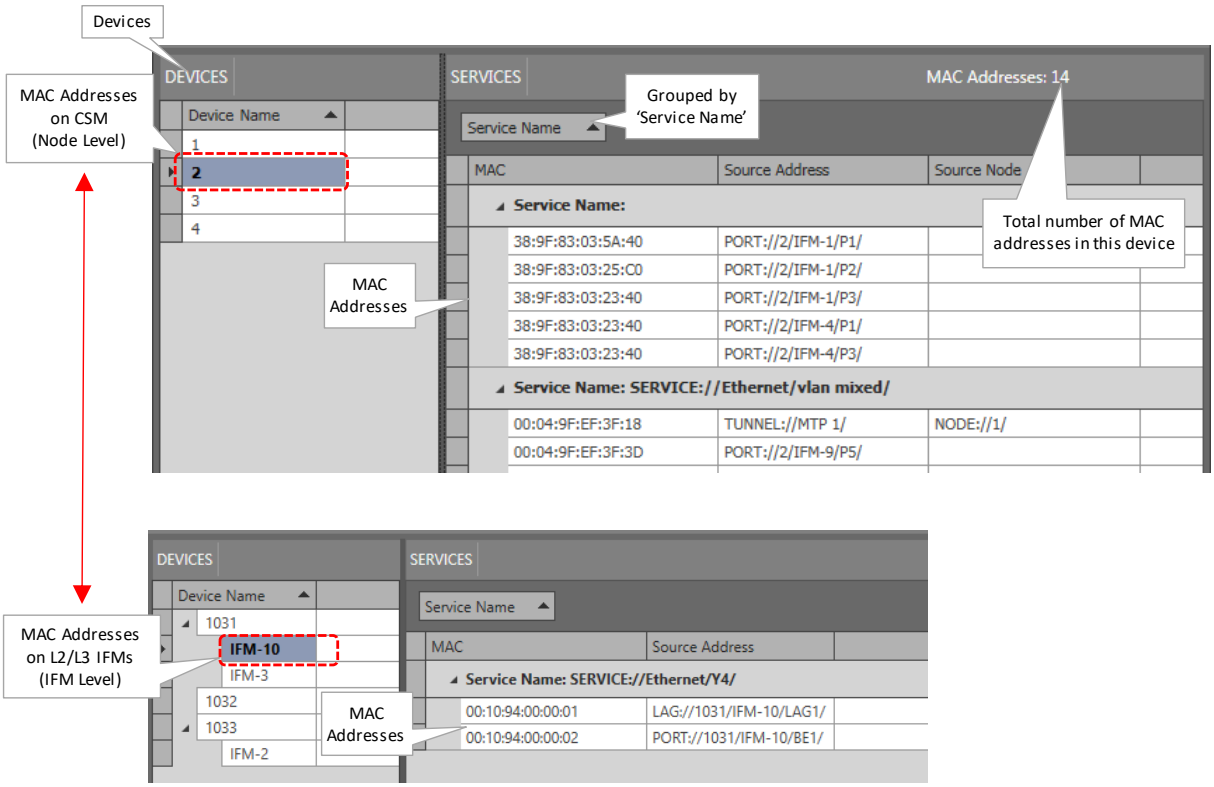

Figure 9 Example: MAC Monitor/MAC Address Table

9.8 MAC ACL (=MAC Access Control List)

See §5.13.

9.9 IP ACL (=IP Access Control List)

See §5.12.

10. ABBREVIATIONS

ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ASIC	Application-Specific Integrated Circuit
BC	Broadcast
BDR	Backup Designated Router
BPDU	Bridge Protocol Data Unit
BWE	Bandwidth Efficiency
CAR IP	Central Alarm Reporter Internet Protocol

CAS	Central Alarm System
CIDR	Classless Inter-Domain Routing
CFM	Connectivity Fault Management
CPU	Central Processing Unit
CRMI	Committed Rate Measurement Interval
CSM	Central Switching Module
CSV	Comma Separated Values
DCN	Data Communication Network
DHCP	Dynamic Host Control Protocol
DLF	Destination Lookup Failure
DR	Designated Router
DSCP	Differentiated Services Code Point
ERPS	Ethernet Ring Protection Switching
FDV	Frame Delay Variation
GARP	Gratuitous ARP
HQoS	Hierarchical Quality of Service
ICMP	Internet Control Message Protocol
IFM	InterFace Module
IP	Internet Protocol
ISP	Internet Service Provider
L2	Layer2
L3VPN	Layer3 Virtual Private Network
LAG	Link Aggregation Group
LAN	Local Area Network
LER	Label Edge Router
LM	Loss Measurement
LSA	Link State Advertisements
LSP	Label Switched Path
LSR	Label Switching Router
LT	Line Termination Character
MAC	Media Access Control
MC	Multicast
MPLS-TP	Multiprotocol Label Switching – Transport Profile
MRC	Media Redundancy Clients

MRM	Media Redundancy Manager
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NIC	Network Interface Card
NSM	Node Support Module
NTP	Network Timing Protocol
OSPF	Open Shortest Path First
PD	Powered Device
PRBS	Pseudo Random Bit Sequence
PRC	Primary Reference Clock
PRS	Primary Reference Source
PSE	Power Source Equipment
PSU	Power Supply Unit
PTN	Packet Transport Network
PTP	Precision Time Protocol
QL	Quality Level
QoS	Quality of Service
QSFP	Quad SFP
RES	Reserved
RID	Router ID
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SEC	SDH Equipment Clock
SFP	Small Form Factor Pluggable
SONET	Synchronous Optical Network
SSM	Synchronization Status Message
TC	Traffic Class
TRM	Transmit Receive Module
TSoP	Transparent Sonet/SDH over Packet
TTL	Time to Live
UDP	Universal Data Protocol
UM	User Management
UTC	Coordinated Universal Time

VFI	Virtual Forwarding Instance
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
XFP	10 Gigabit Small Form Factor Pluggable