



HIRSCHMANN

A **BELDEN** BRAND

User Manual

Basic Configuration

Dragon PTN Network Operation



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.

© 2020 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

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

1.	INTRODUCTION	7
1.1	General	7
1.2	Supported Hardware, Firmware, Software	7
1.3	Manual References	7
2.	PHYSICAL LINKS: CONNECT ALL NODES INTO A WAN NETWORK.....	8
2.1	General	8
2.2	Connect Optical Link via Fiber/SFP/XFP/QSFP+	8
2.3	Connect Electrical Link via Copper/RJ45	8
3.	HIPROVISION: DISCOVER NETWORK, DEPLOY DCN, CREATE LINKS.....	9
3.1	General	9
3.2	DCN Channel	9
3.3	DCN Bandwidth Profile	9
3.4	Link Capacity	10
3.5	Amount of Protected Tunnels	10
4.	HIPROVISION: SET THE LAN PORTS IN YOUR NETWORK	10
5.	HIPROVISION: CREATE MPLS-TP TUNNEL(S).....	11
5.1	General	11
5.2	Tunnel Creation	14
5.3	Subrings	22
5.4	Tunnel Modification	25
5.5	Monitor Protected Tunnel.....	25
5.6	Reporting	26
5.7	Tunnel Actions: Swap Working Path \leftrightarrow Protection Path.....	26
6.	CSM REDUNDANCY	29
7.	SYNCE.....	30
7.1	General	30
7.2	Configuration	32
7.3	Normal Clock Selection Process.....	34
7.4	Operation.....	35
8.	PTP IEEE 1588V2 TRANSPARENT CLOCK	36
8.1	General	36
8.2	IEEE 1588v2 within Dragon PTN.....	37
8.3	Configuration	40
8.4	Operation.....	41
9.	LOSS/DELAY/ASSURANCE MONITORING.....	41

9.1	General	41
9.2	Loss Measurement (=LM)	41
9.3	Delay Measurement (=DM)	45
9.4	Tunnel Ping	46
9.5	Tunnel Traceroute	49
10.	PERFORMANCE COUNTERS AND MONITORING.....	50
10.1	General	50
10.2	Port Performance	51
10.3	SyncE Performance	55
10.4	IEEE 1588 Performance	58
10.5	Health Monitor	59
11.	TROUBLESHOOTING.....	60
11.1	Health Monitor	60
11.2	Port Mirroring	61
11.3	Monitoring: Multiproperty View	64
11.4	Devices Summary	66
12.	PROTOCOL AND FEATURE SUPPORT MATRIX.....	68
13.	ABBREVIATIONS	72

List of figures

Figure 1	Dragon PTN Network Example	7
Figure 2	Link: DCN Bandwidth Profile	9
Figure 3	Ethernet Link: Link Capacity	10
Figure 4	LAN/WAN Settings.....	11
Figure 5	Tunnel Creation	12
Figure 6	Point-to-Point Tunnels	13
Figure 7	MultiPoint Tunnels	13
Figure 8	Logical Ring Tunnel.....	13
Figure 9	Subring Tunnel.....	14
Figure 10	Create Tunnels.....	14
Figure 11	Tunnel - Device Selection	15
Figure 12	Tunnel - Link Selection.....	15
Figure 13	Set Protection Mode of LSP.....	16
Figure 14	Tunnel HQoS / HQoS Application Priority	16
Figure 15	Protection Parameters	17
Figure 16	Example: Propagate Topology Change (=PTC)	19
Figure 17	Example: Main Ring + Subrings	19
Figure 18	RingX (=Main Ring): Ring Protection Tab	20
Figure 19	SubringX1: Ring Protection / Topology Change Propagation Tab.....	20

Figure 20 SubringX2: Ring Protection / Topology Change Propagation Tab.....	20
Figure 21 Share LSP: Shared/Non-Shared LSPs	21
Figure 22 LSP Sharing Possible?	22
Figure 1 Logical Ring / Interconnection Nodes / Subring / Ladder Topology	22
Figure 2 Logical Ring / Subring Setup	23
Figure 3 Subring Colors.....	23
Figure 4 Ladder Topology Example 1	24
Figure 5 Ladder Topology Example 2	24
Figure 6 Ladder Topology: Not Allowed: Shared Link	24
Figure 7 Ladder Topology: Not Allowed: Only 2 Nodes in Subring	25
Figure 8 Protected Tunnels: Protection Path, Blocked Port Indication: '/'	25
Figure 9 Protected Tunnel/Actions	26
Figure 10 Point-to-Point/Multipoint Action on Tunnel Window	27
Figure 11 Ring/SubRing Action on Tunnel Window	28
Figure 12 Clear Command in the Node Action List	28
Figure 13 Node with 2 CSMs, CSM Switchover Button	30
Figure 14 CSM Redundancy Status.....	30
Figure 15 Unidirectional/Bidirectional SyncE Examples.....	31
Figure 16 Bad SyncE Examples: Timing Loop	32
Figure 17 SyncE Member Ports	32
Figure 18 SyncE Clock Recovery Ports.....	34
Figure 19 IEEE 1588v2	37
Figure 20 1588 Protocol Messages	37
Figure 21 1588 on Port and Node Level for LERs and LSRs	38
Figure 22 1588 Enabled: Transparent Clock Correction.....	39
Figure 23 1588 Not Enabled: No Clock Correction.....	39
Figure 24 1588 Node Settings	40
Figure 25 1588 Port Settings	41
Figure 26 Assurance Wizard: Loss Measurement Configuration	43
Figure 27 Loss Measurement in Operation	44
Figure 28 Loss Measurement Result Values.....	44
Figure 29 Delay Measurement Result Values	46
Figure 30 Assurance Wizard: Ping Measurement Configuration	47
Figure 31 Tunnel Ping Result Values	48
Figure 32 Traceroute Results Overview	49
Figure 33 Performance Tab: Counter Control	50
Figure 34 CSM Ethernet Port Monitoring.....	52
Figure 35 L2 and L3 Ethernet Port Monitoring.....	54
Figure 36 CODIR Port Monitoring.....	55
Figure 37 SyncE Monitoring	56
Figure 38 IEEE 1588 Monitoring.....	58

Figure 39 Health Monitor	59
Figure 40 Port Mirroring.....	61
Figure 41 Port Mirroring Icon.....	61
Figure 42 Port Mirroring Wizard	62
Figure 43 Destination/Source Ports	62
Figure 44 Port Mirroring Sessions	63
Figure 45 Multiproperty View	65
Figure 46 Multiproperty View: Filter Example	66
Figure 47 Multiproperty View: Full Screen Results View + Export.....	66
Figure 48 Devices Summary	67

List of Tables

Table 1 Manual References.....	7
Table 2 Tunnel Topologies and Protection.....	12
Table 3 Tunnel Action Commands.....	29
Table 4 Provisioned QL Ordered According Quality.....	33
Table 1 CSM Ethernet Port Monitoring Fields.....	52
Table 2 CODIR Port Monitoring Fields.....	55
Table 3 SyncE Monitoring 'System Information' Fields.....	56
Table 4 SyncE Monitoring 'Clock Information' Fields.....	57
Table 5 IEEE 1588 Monitoring Fields	58
Table 6 CPU Status Monitoring	59
Table 7 Memory Status Monitoring	60
Table 8 Disk Status Monitoring	60
Table 9 Protocol and Feature Support Matrix.....	68

1. INTRODUCTION

1.1 General

This document is valid as of Dragon PTN Release 4.3DR.

This manual describes in detail how to set up the core Dragon PTN MPLS-TP network (without the application services), e.g. the DCN communication channel, the tunnels, etc....

Prerequisites: The HiProvision PC must have been configured and installed.

- ▶ To install the HiProvision PC and how to operate it: see Ref. [2Mgt] in Table 1;
- ▶ A detailed description to setup pure Ethernet services: see Ref. [2Eth] in Table 1;
- ▶ A detailed description to setup Legacy services: see Ref. [2Leg] in Table 1.

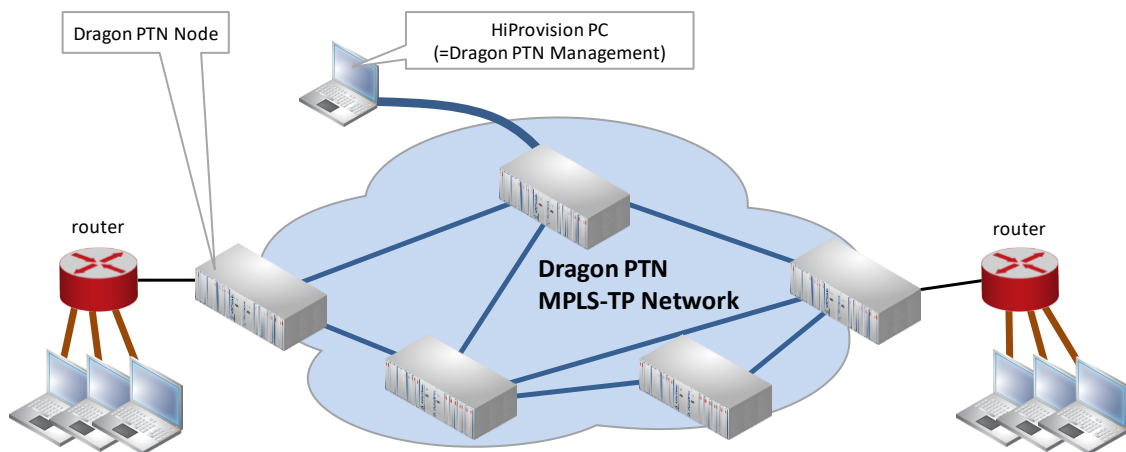


Figure 1 Dragon PTN Network Example

1.2 Supported Hardware, Firmware, Software

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

1.3 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. All 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
[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
[14]	DRF-DRM811-&-*	Dragon PTN TRMs (Transmit Receive Modules: SFP, XFP, QSFP+)
[24]	DRG-DRM826-&-*	HiProvision Add-on: Generic Reporting Engine

2. PHYSICAL LINKS: CONNECT ALL NODES INTO A WAN NETWORK

2.1 General

CAUTION: Maximum 255 nodes in series, maximum 255 hops;

- ▶ Optical WAN links can be created on (see WAN support in feature matrix §12):
 - ▶ 4-GC-LW/4-GCB-LW IFM (=interface module) → 1 Gbps, one link per module;
 - ▶ 4-GO-LW IFM → 1 Gbps, four links per module;
 - ▶ 1-10G-LW IFM → 10 Gbps, one link per module;
 - ▶ 4-10G-LW IFM → 10 Gbps, four links per module;
 - ▶ 1-40G-LW IFM → 40 Gbps, one link per module;
- ▶ Electrical WAN links can be created on:
 - ▶ a 4-GC-LW/4-GCB-LW IFM:
 - ▶ Four links per module if no optical link (port1) is coming up on this module;
 - ▶ Three links per module if an optical link (port1) is coming up on this module.

Connect all the links in all the nodes as described in the paragraphs below. Once the entire WAN network has been connected, ports not used as WAN port can be used as LAN port. The RJ45 port of combo port1 can only be used when there is no optical link on this port.

2.2 Connect Optical Link via Fiber/SFP/XFP/QSFP+

CAUTION:

Make sure that the used TRMs (=SFPs/XFPs/QSFPs+) are suited for the optical link distance. A received optical budget that exceeds the TRM receiver sensitivity level (or the transmitting TRM is too powerful for the link distance), could damage the receiving TRM. More information on the TRMs can be found in Ref.[14] in Table 1.

- ▶ Plug in TRM module:
 - ▶ SFP module into the SFP connector (=port1) of a 4-GC-LW/4-GCB-LW/4-GO-LW IFM;
 - ▶ XFP module into the XFP connector of a 1-10G-LW/4-10G-LW IFM;
 - ▶ QSFP+ module into the QSFP+ connector of a 1-40G-LW IFM;
- ▶ Plug in the optical fiber into the SFP/XFP/QSFP+ module;

NOTE: Smart SFP (see Ref. [2Leg] in Table 1) cannot be used to interconnect Dragon PTN nodes;

NOTE: Fiber optic reporting information is available via the Reporting Engine Add-on, see see Ref. [24] in Table 1.

2.3 Connect Electrical Link via Copper/RJ45

- ▶ Plug in the copper cable into an available RJ45 port of a 4-GC-LW IFM/4-GCB-LW;
- ▶ When using the RJ45 connector from combo port1 on the 4-GC-LW/4-GCB-LW IFM, make sure that no optical link will come up on the SFP of that combo port. Within a combo port, an upcoming optical link will always have priority over the electrical copper link, and as a result will disable the electrical port;

3. HIPROVISION: DISCOVER NETWORK, DEPLOY DCN, CREATE LINKS

3.1 General

The Dragon PTN network can be discovered via connecting the HiProvision PC to the Dragon PTN network, and start the Discovery function. The discovered network will be visualised in HiProvision and the discovered links can be created automatically after the discovery phase. More info on discovery and link creation in ref. [2Mgt] in Table 1.

3.2 DCN Channel

The DCN (=Data Communication Network) Channel is the Dragon PTN network management channel which is deployed dynamically over each link of the entire network during the discovery phase, see Ref. [2Mgt] in Table 1. HiProvision uses this channel to communicate with the entire Dragon PTN network.

3.3 DCN Bandwidth Profile

The bandwidth of the DCN channel can be configured per individual 1G/10G/40G Ethernet link, making part of the DCN channel, via Dashboard → Network Hardware → Links → Link → Generic: DCN Bandwidth Profile:

- ▶ 40 Mbps (=default): Use this value if you have plenty of bandwidth available in your network. All your management activities will go fast/normal;
- ▶ 20 Mbps;
- ▶ 5 Mbps;
- ▶ 1.5 Mbps: Use this value if you have to consume your bandwidth very efficiently or if you have lack of bandwidth in your network. Your management activities could go slow/slower depending on the network layout and load;

NOTE: The selected bandwidth also influences the number of protected tunnels through this link, see paragraph below.

NOTE: Management activity example: Load firmware into the network, see Ref. [2Mgt] in Table 1.

NOTE: The DCN Bandwidth Profile must always be less than the Link Capacity (see §3.4).

This configured bandwidth is automatically reserved during discovery.

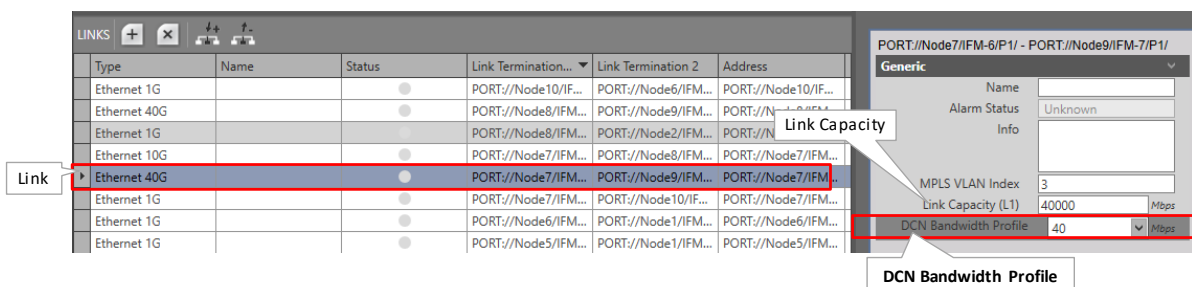


Figure 2 Link: DCN Bandwidth Profile

3.4 Link Capacity

The link capacity of the Ethernet link is the maximum data rate through a link cable. This value equals by default the port speed of the port in which the cable is plugged in. E.g. if a link cable is plugged in into a 1000 Mbps port, the Link Capacity is by default 1000 Mbps.

The Link Capacity can be configured or downscaled if desired via Dashboard → Network Hardware → Links → Link → Generic: Link Capacity (L1):

- ▶ Ethernet 1G: default = 1000 Mbps, Range [10...1000] Mbps;
- ▶ Ethernet 10G: default = 9294 Mbps, Range [10...10000] Mbps;
- ▶ Ethernet 40G: default = 40000 Mbps, Range [10...40000] Mbps;

NOTE: The Link Capacity must always be more than the DCN Bandwidth Profile (see §3.3);

Type	Name	Status	Link Termination...	Link Termination 2	Address
Ethernet 1G		●	PORT:/Node10/IF...	PORT:/Node6/IFM...	PORT:/Node10/IF...
Ethernet 40G		●	PORT:/Node8/IFM...	PORT:/Node9/IFM...	PORT:/Node8/IFM...
Ethernet 1G		●	PORT:/Node8/IFM...	PORT:/Node2/IFM...	PORT:/Node8/IFM...
Ethernet 10G		●	PORT:/Node7/IFM...	PORT:/Node8/IFM...	PORT:/Node7/IFM...
Ethernet 40G		●	PORT:/Node7/IFM...	PORT:/Node9/IFM...	PORT:/Node7/IFM...
Ethernet 1G		●	PORT:/Node7/IFM...	PORT:/Node10/IF...	PORT:/Node7/IFM...
Ethernet 1G		●	PORT:/Node6/IFM...	PORT:/Node1/IFM...	PORT:/Node6/IFM...
Ethernet 1G		●	PORT:/Node5/IFM...	PORT:/Node1/IFM...	PORT:/Node5/IFM...

Configuration panel for PORT:/Node7/IFM-6/P1/ - PORT:/Node9/IFM-7/P1/:

Generic

Name: []

Alarm Status: Unknown

Info: []

MPLS VLAN Index: 3

Link Capacity (L1): 40000 Mbps

DCN Bandwidth Profile: 40 Mbps

Figure 3 Ethernet Link: Link Capacity

3.5 Amount of Protected Tunnels


The number of logical ring, point-to-point/multipoint with protection and subring tunnels that can be configured through a link depends on the selected DCN Bandwidth profile for that link.

- ▶ 40 Mbps (=default): Maximum 128 protected tunnels possible;
- ▶ 20 Mbps: Maximum 64 protected tunnels possible;
- ▶ 5 Mbps: Maximum 8 protected tunnels possible;
- ▶ 1.5 Mbps: Maximum 2 protected tunnels possible;

4. HIPOVISION: SET THE LAN PORTS IN YOUR NETWORK

WAN ports interconnect nodes within the Dragon PTN network (MPLS-TP) whereas LAN ports interconnect the nodes with their applications.

By default, all the ports of the IFMs that support WAN ports (see §12) are WAN ports. This is because nodes are discovered via the HiProvision discovery function, which operates over MPLS-TP links that interconnect nodes via WAN ports. Ports that do not have a WAN link can be changed into a LAN port by using the network settings wizard.

The network settings wizard allows to easily set all the port configurations of multiple IFMs together, without having to open each IFM individually. Click the Network Settings Wizard button  (see previous paragraph) to open it.

The list below summarizes every page in the wizard:

- ▶ Information: Click Next>>;
- ▶ Selection: select Port Mode;
- ▶ Port Mode Settings: By default, all the ports of the IFMs that support WAN ports (see §12) are WAN ports. The ports with a connected WAN link, are indicated by **WAN ?**. These ports cannot be adapted anymore in this wizard. If all the other ports must be set to LAN, click the **LAN** button. If not, set the ports individually to LAN or WAN via the LAN/WAN drop-down selectors. See figure below.
- ▶ 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!

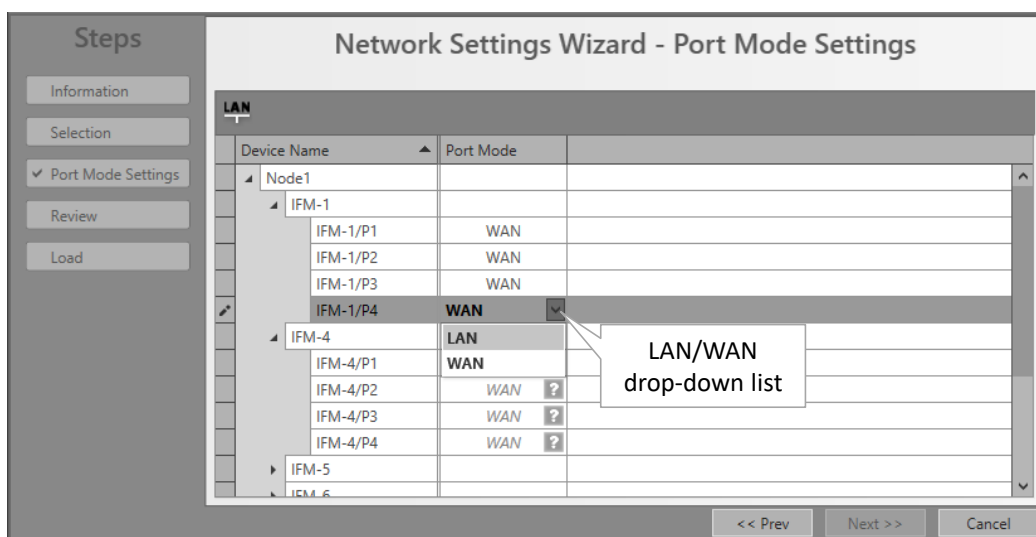


Figure 4 LAN/WAN Settings

5. HIPROVISION: CREATE MPLS-TP TUNNEL(S)

Prerequisite: all the necessary nodes and interface modules are configured in the database.

5.1 General

A tunnel is a virtual path through the physical network in which customer application services can be programmed later on. The concept of a tunnel can be found in the figure below. A network consists of nodes with links in between. The bandwidth within a link is divided over the configured tunnels through that link. The tunnels can start or end in a node (=LER) or just pass through a node (=LSR) and will be used to program customer application services in.

- ▶ LER: Label Edge Router = MPLS-TP access node with customer applications;

- ▶ LSR: Label Switching Router = MPLS-TP transfer node. A programmed service can have no end-points in an LSR node;

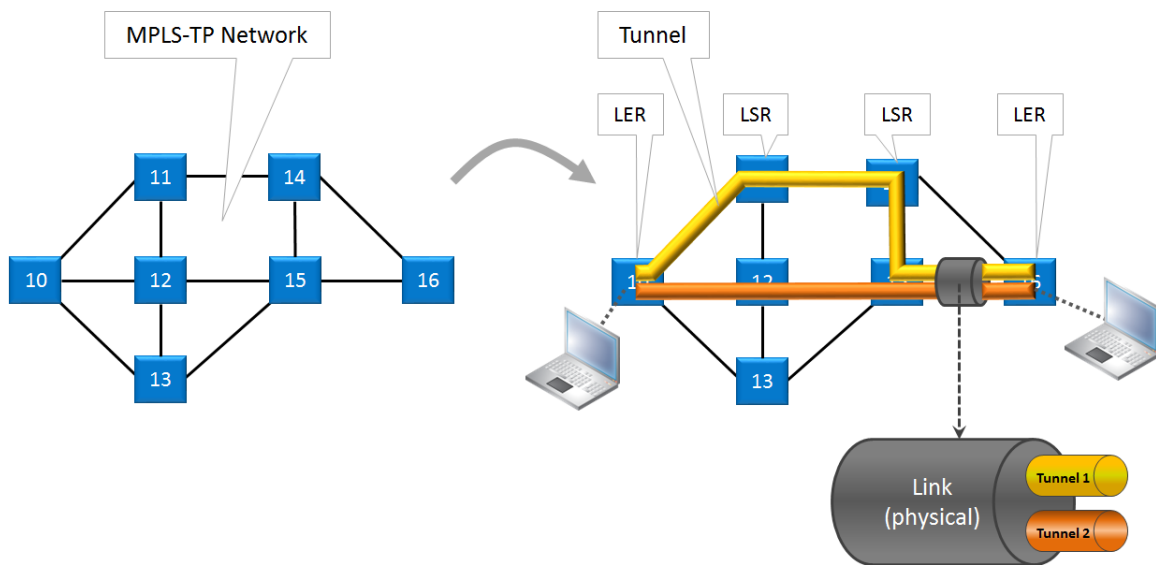


Figure 5 Tunnel Creation

In HiProvision, it is possible to create tunnels in a predefined topology, with or without a protection path. See the table and figures below for an overview:

Table 2 Tunnel Topologies and Protection

Tunnel Topology	Protection
Point-to-point	Optional
Multipoint	Optional
Logical Ring (max. 60 LERs per tunnel)	Always, included automatically via RPL (=Ring Protection Link)
Subring (max. 15 Subrings per Logical Ring)	Always, included automatically via RPL
External (*)	None
(*) Note: An 'External' tunnel type cannot be selected or created manually. Such a tunnel will be created automatically when creating an 'External E1 Link'. 'External E1 Links' must only be used when the Local Mode service is used on 2-OLS or 2-C37.94 IFMs, see Ref. [2Leg] in Table 1. This external tunnel cannot be modified/deleted. It will be deleted automatically when deleting the associated 'External E1 Link'.	

A tunnel with protection consists of a working and a protection path:

- ▶ Working path (yellow in the figures below): the active data path;
- ▶ Protection path (orange in the figures below): the standby or backup data path if the working path should fail. This path is optional for point-to-point and multi-point tunnels and mandatory for logical ring or subring tunnels. Switching between the working path and protection path occurs automatically due to a working path failure or can be initiated manually for maintenance reasons for example, see §5.7.
- ▶ The possible amount of protected tunnels through a link depends on the selected DCN bandwidth profile for that link, see §3.3.

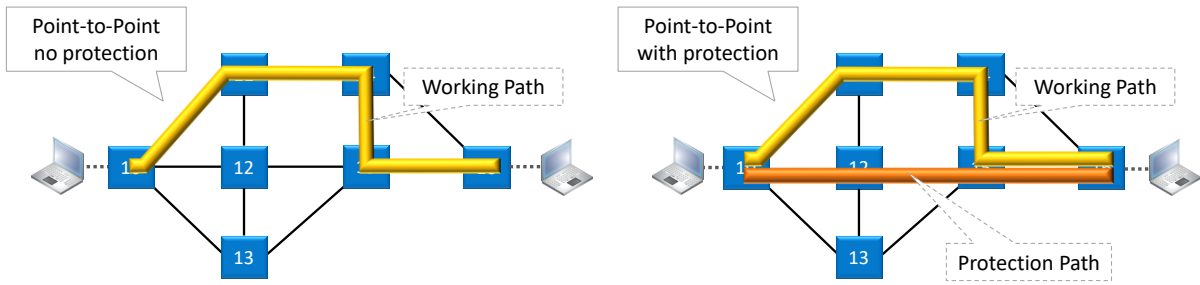


Figure 6 Point-to-Point Tunnels

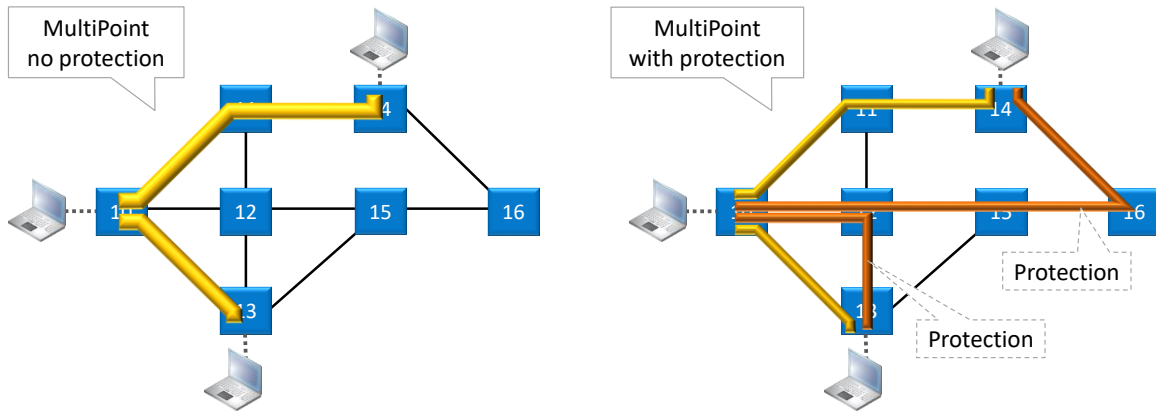


Figure 7 MultiPoint Tunnels

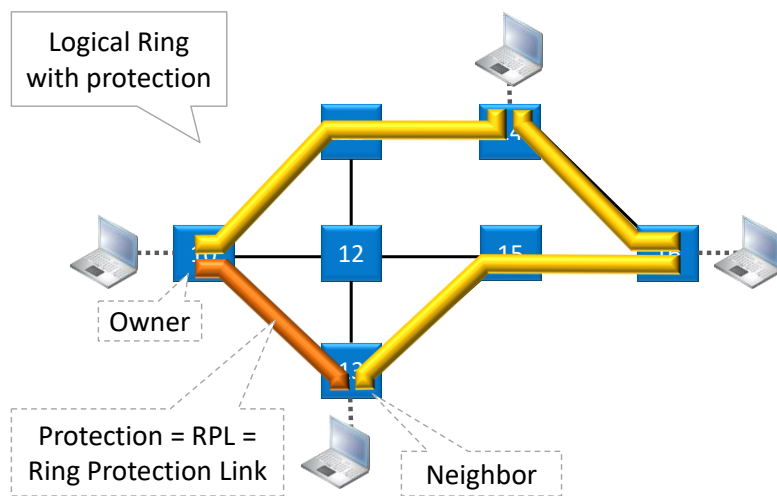


Figure 8 Logical Ring Tunnel

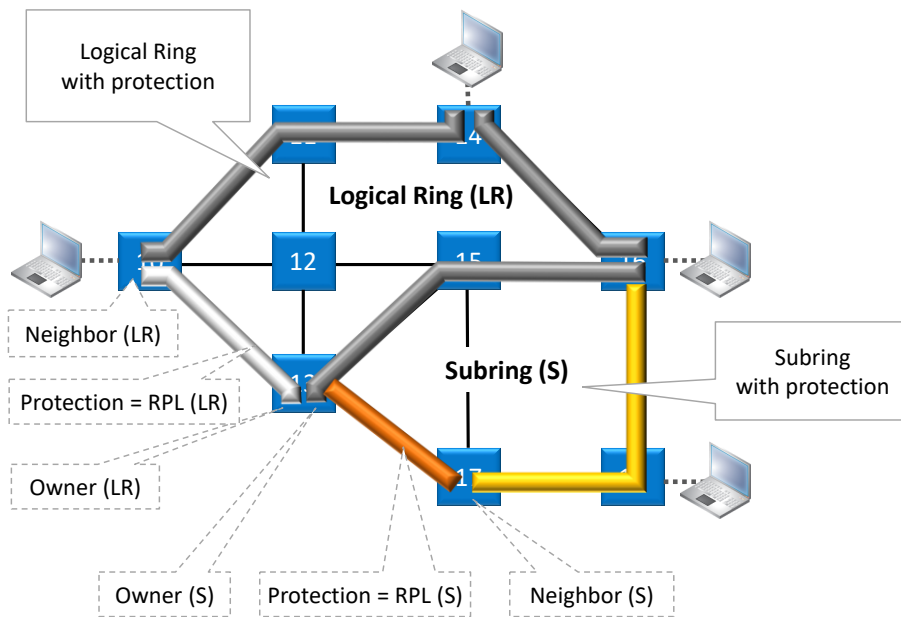


Figure 9 Subring Tunnel

5.2 Tunnel Creation

NOTE: If needed, a tunnel can be modified later on as described in §5.4.

NOTE: If you want to create a Subring tunnel, read §5.3 first.

Click Dashboard → Configuration → Connections → Tunnels → to open the tunnels wizard. See figure below.

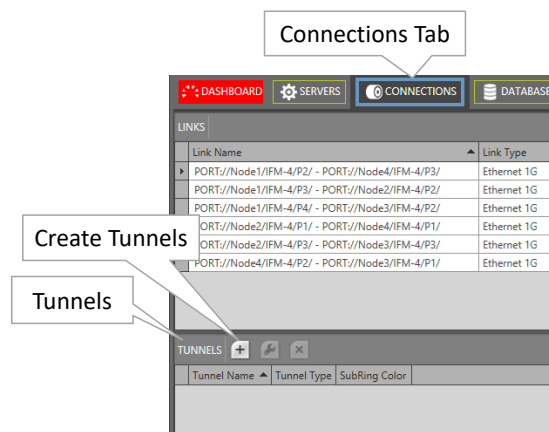




Figure 10 Create Tunnels

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

- ▶ Information: Click Next>>;
- ▶ Topology Selection: enter a tunnel name, select a topology (see also §5.1) with optional protection;
- ▶ Ring Tunnel Selection (only when SubRing topology was selected): a 'Logical Ring' must be chosen to configure subrings on. Select a Logical Ring in the Tunnels list.
- ▶ Device Selection:

- ▶ Select the nodes to which your customer applications for this tunnel will be connected later on. Only select LERs, no LSRs. For Subbrings: Select all the devices or nodes of the subbring including the interconnection nodes on the Logical Ring. A logical ring can have a maximum of 60 LERs.
- ▶ Subbring Interconnection nodes: see §5.3;
- ▶ A node can be selected by clicking the node icon or its 'Selected' checkbox. A selected node icon is colored turquoise, an unselected node icon is colored white. A node can be unselected by clicking again on the node icon or its 'Selected' checkbox. Make sure that your node selection makes sense for the selected topology. Multiple nodes can be selected/unselected at once via selecting a number of rows and clicking  / .

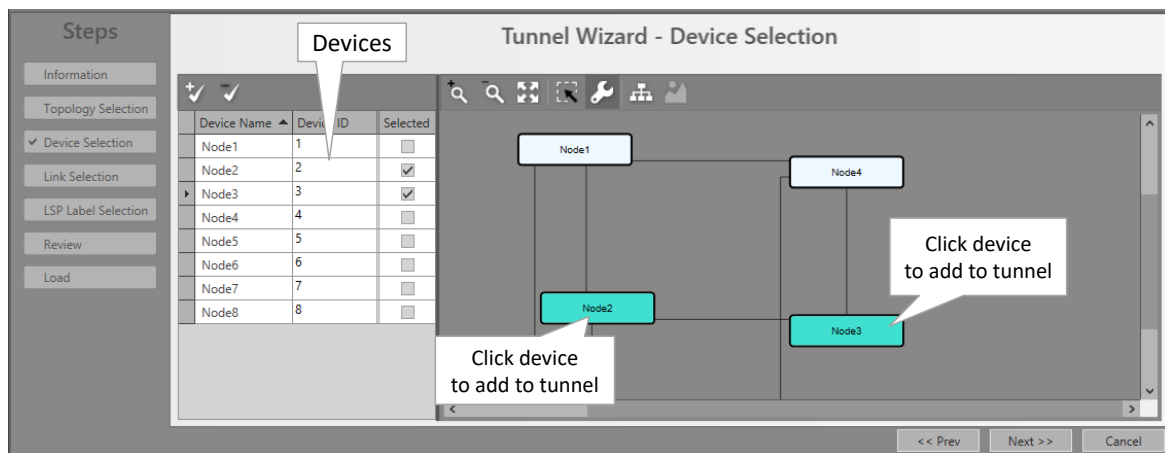




Figure 11 Tunnel - Device Selection

- ▶ Link Selection: Select the links that must be part of the tunnel. A link can be selected by clicking the link line between the node icons or by clicking the 'Selected' checkbox. A selected link is colored brown, an unselected link is colored grey. Click again on this link or its 'Selected' checkbox to unselect the link. Multiple links can be selected/unselected at once via selecting a number of rows and clicking  / .

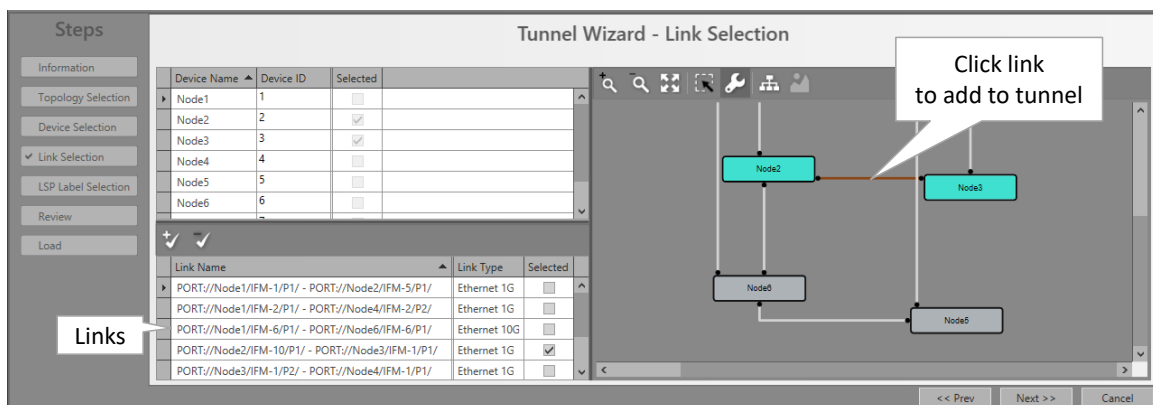


Figure 12 Tunnel - Link Selection

- ▶ Protection Setup (optional, if protection was selected in the Topology Selection):

- ▶ Point-to-point: Just select the links of the protection path to configure the protection path (link selection/unselection is similar as described above).
- ▶ Multipoint: at least one of the different working paths within the Multipoint tunnel must be protected. For each working path (or LSP) that is going to be protected:
 - ▶ Set the Protection Mode to 1:1, see figure below. The working path in the network drawing is blue, so that you know which path is going to be protected.



Figure 13 Set Protection Mode of LSP

- ▶ Next select all the links of the protection path (link selection/unselection is similar as described above). After this, the protection path is configured.
- ▶ Logical Ring: See next paragraph.
- ▶ QoS Parameters: HQoS (= is way to prioritize service traffic via assigning a priority to the tunnel in which the service data is transported).
 - ▶ Use HQoS/HQoS Application Priority (HQoS = Hierarchical Quality of Service):
 - ▶ Unchecked (=default): No HQoS will be used.
 - ▶ Checked: An HQoS Application Priority (0 = default = lowest priority, ..., 6 = highest priority) can be assigned to the tunnel if Use HQoS has been checked. More info on HQoS can be found in Ref. [2Eth] in Table 1. Click Next >>.

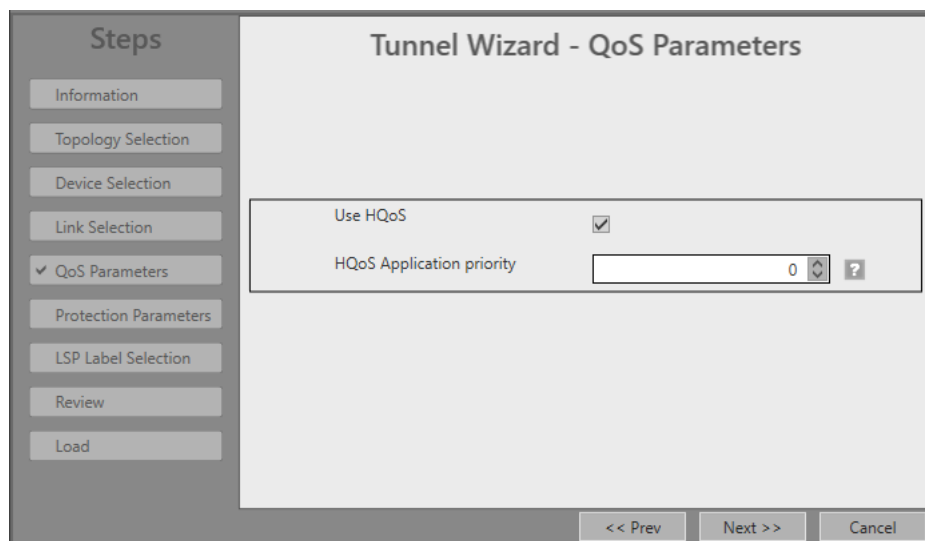


Figure 14 Tunnel HQoS / HQoS Application Priority

- ▶ Protection Parameters :

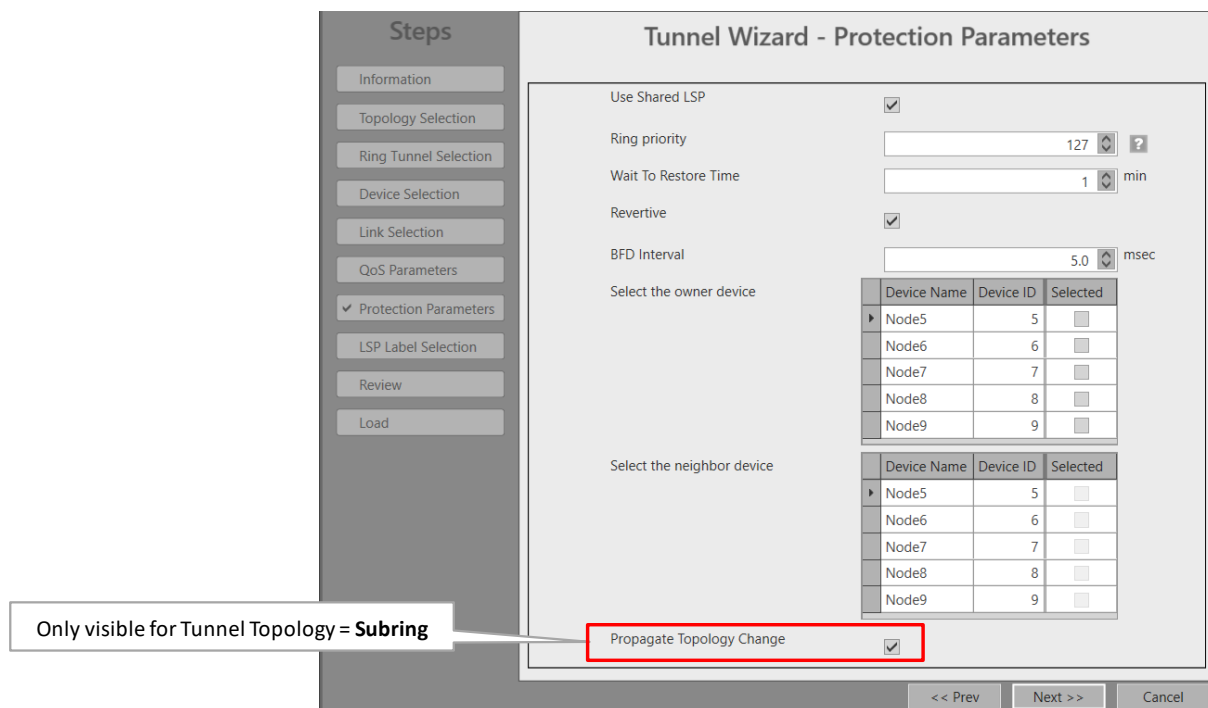



Figure 15 Protection Parameters

- ▶ Use Shared LSP (for Logical Ring and Subring tunnels):
 - ▶ checked (=default): Allows to reuse existing tunnel resources resulting in more performant and faster switchover times. Switchover from the working path to the protection path occurs when the normal working path gets broken.
 - ▶ unchecked: This tunnel will not reuse other tunnel resources and as a result, the switchover behavior becomes less performant.
- ▶ Ring Priority (default = 127, range[0-255]) (for Logical Ring and Subring tunnels): This field is only for tunnels using LSP sharing ('Use Shared LSP' = checked). It decides the switchover order when multiple shared rings have to switchover simultaneously due to a link break or recovery. The ring with the lowest ring priority value will switchover first. If some of these rings have the same priority, the ring that was created first will switchover first.
- ▶ Revertive/Wait to Restore time (=WTR) (default=1 minute, range[1..12] minutes):
 - ▶ Revertive = checked: Initial active path A (=working path) is the preferred path. If this path fails, it will become the active path again after it restores and being stable for at least a period indicated by the 'Wait to Restore Time'. In between, the redundant path B (=protection path) will be the active path;
 - ▶ Revertive = unchecked: If the initial active path A (=working path) fails, redundant path B (=protection path) becomes active and remains active even when path A repairs later on;
- ▶ BFD interval (default = 5ms, range[3-500]ms). Indicates the Bidirectional Forwarding Detection interval between BFD packets. BFD is used to detect the link status (e.g. is the link still up or down?). BFD packets are used in protected tunnels except in hitless switching tunnels. Monitored BFD information and protection info can be found in the Network tile. Select the desired tunnel and show its properties via the  button;

- ▶ Owner / Neighbor Device (only for Logical Ring and Subring): The Ring protection path is a link between two adjacent end nodes or LERs. This protection path is called the RPL or Ring Protection Link. These two end nodes are called the owner and the neighbor of the RPL. Only when the working path is broken this RPL will be activated.
 - ▶ Owner: is the owner or master controller of the RPL. Select the owner device in the Owner Device list by clicking the Selected checkbox;
 - ▶ Neighbor: is the neighbor or slave of the RPL, it listens to control packets of the owner, and as a result opens/closes its RPL port to open/close the RPL. If the working path is OK, this port is closed. Select the neighbor device in the Neighbor Device list by clicking the Selected checkbox. Only adjacent LER (=Label Edge Router) nodes of the owner node are selectable.
- ▶ Propagate Topology Change (= PTC = only for Subrings): Topology change propagation is a process that informs the network about path breaks (physical/logical) in one of its subrings. As a result, all the subrings between the broken subring up to the main ring will be able to flush their nodes. Flushing a node clears the learned MAC addresses to initiate new path recalculations to the broken subring. When the broken subring is connected to the main ring via a more complex network structure (e.g. sideway subring structures), the propagation always follows the shortest path towards the main ring.
 - ▶ Checked (=default): This subring communicates its own ring breaks (or topology changes) and also forwards incoming topology change notifications from other subrings.
 - ▶ Example (see figure below): LR = Logical Ring = Main Ring, S(n) = Subring(n). This subring = S2 and connected to other rings as follows: LR → S1 → S2 → S3;
 - ▶ If a path ring break occurs in this S2, a topology change will be communicated to S1 (= towards the main ring) but not to S3 (=away from the main ring);
 - ▶ Incoming topology changes in S2 from a lower S3, if any, will be forwarded to the higher S1;
 - ▶ After the subring tunnel creation, a 'Topology Change Propagation' tab can be viewed in the Connections Tile when selecting the subring in the TUNNELS list. It shows the RING IDs of the ring/subring that will be flushed by the PTC of this subring. The RING IDs of each ring/subring can be found in the 'Ring Protection' tab, see figures below.
 - ▶ Unchecked: This subring will not communicate its own ring breaks (or topology changes) nor forward incoming topology changes from other subrings.

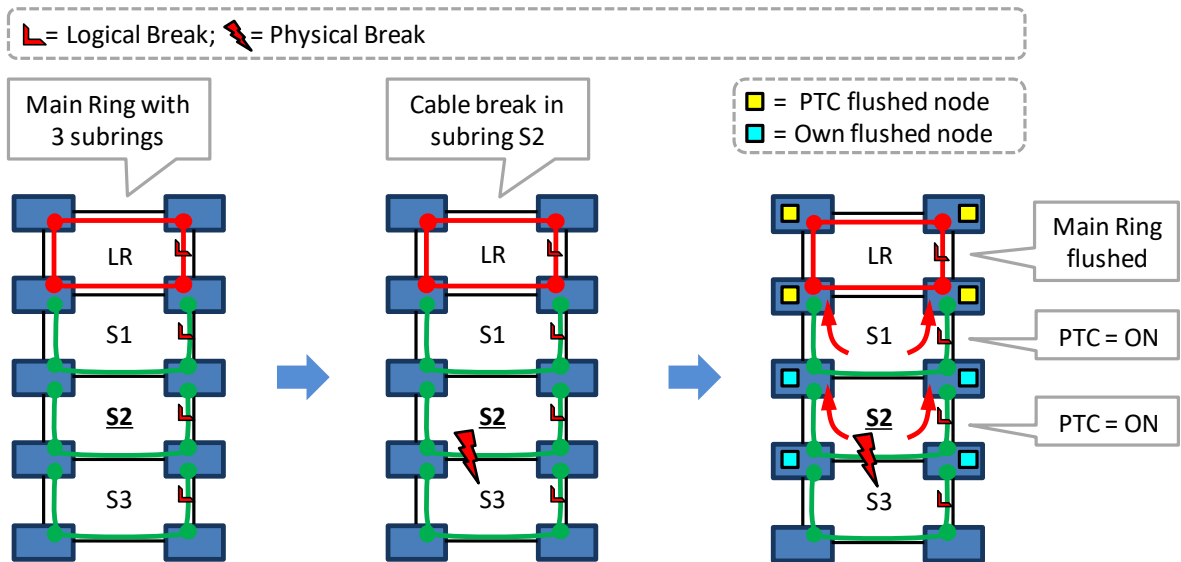


Figure 16 Example: Propagate Topology Change (=PTC)

DASHBOARD DATABASE NETWORK HARDWARE **CONNECTIONS** SERVERS

LINKS
 Link Name Link Type
 PORT://N... Etherne...
 PORT://N... Etherne...
 PORT://N... Etherne...
 PORT://N... Etherne...
 PORT://N... Etherne...
 PORT://N... Etherne...
 PORT://N... Etherne...
 Count=11

TUNNELS
 Tunnel Name Tunnel Type SubRing Color
RingX Logical Ring
 SubRingX1 Subring
 SubRingX2 Subring
 Supertunnel Logical Ring
 ptp12 Point-to-Point
 ptp12b Point-to-Point
 ptp19 Point-to-Point
 Count=7

SERVICES
 Service Name Service Type
 Eth1 Ethernet

RingX (Ring ID=4)
 SubRingX1 (Ring ID=5)
 SubRingX2 (Ring ID=7)

Tunnel	QoS	Ring Protection	Pseudo-Wires
Ring ID	Device Name	Device Role	RPL Port
4	Node2	Owner	RingX_RAPS: Node2/IFM-7/P1/ -> Node3/IFM-7/P1/
4	Node3	Neighbor	RingX_RAPS: Node2/IFM-7/P1/ -> Node3/IFM-7/P1/
4	Node1	--	--

Figure 17 Example: Main Ring + Subrings

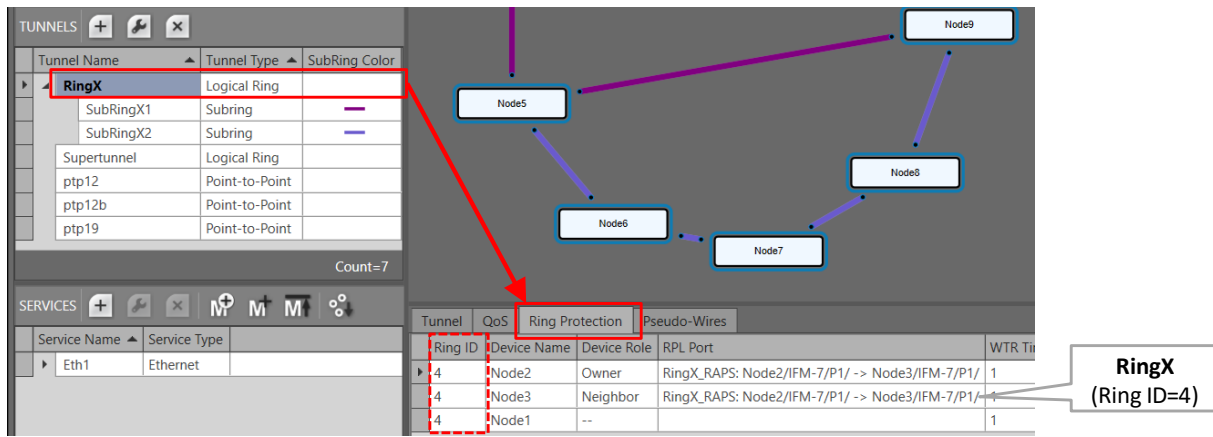


Figure 18 RingX (=Main Ring): Ring Protection Tab

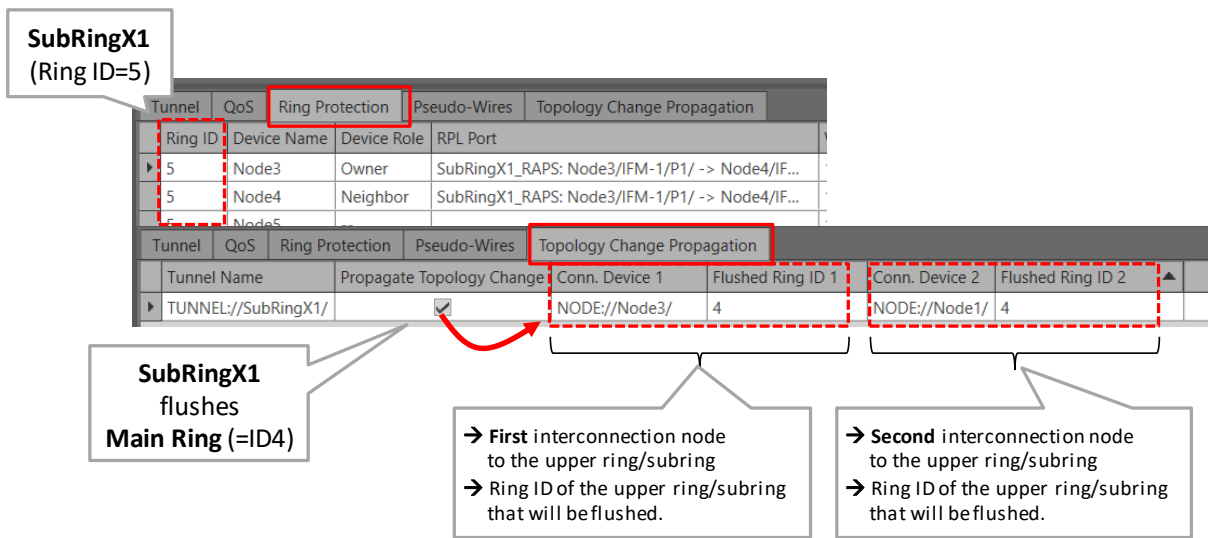


Figure 19 SubringX1: Ring Protection / Topology Change Propagation Tab

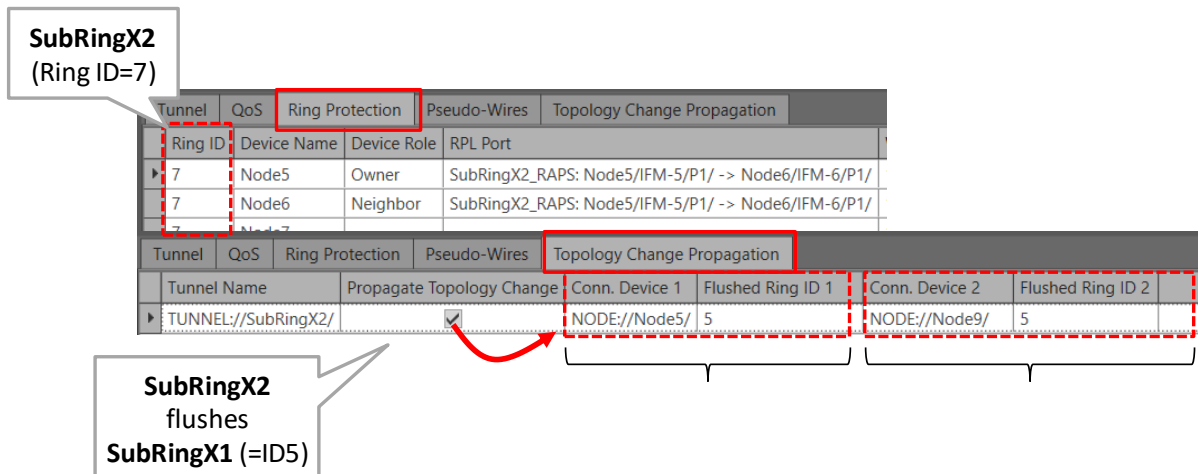


Figure 20 SubringX2: Ring Protection / Topology Change Propagation Tab

- ▶ LSP Label Selection: This page depends on the selected tunnel topology and the 'Use Shared LSP' (only for Logical Ring/Subring) setting from the previous wizard page.
 - ▶ Point-to-Point/Multipoint: LSP Sharing not relevant;
 - ▶ Logical Ring/Subring: reusing resources is more performant than not reusing resources, especially when multiple tunnels go over the same link. Reusing resources = reusing existing LSP labels from existing tunnels. Per link between two nodes, you can decide whether to share your new tunnel with other existing tunnels. This can be done via clicking the appropriate radio buttons or selecting the desired tunnel(s) to share with via the tunnel/link drop-down lists. By default, sharing is activated per link if any other tunnel is already available in this link. Sometimes, sharing is not possible, see Figure 22.

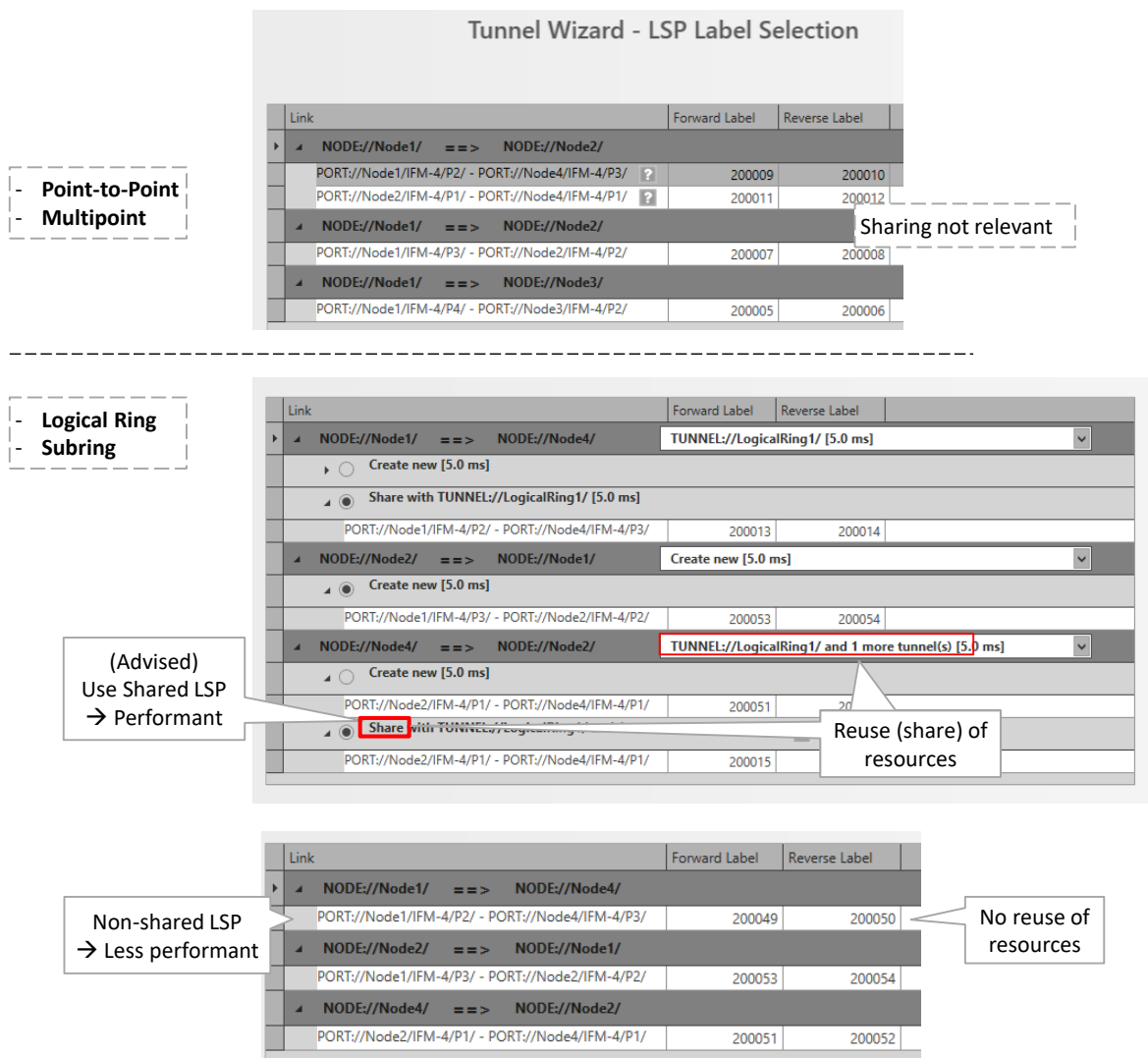


Figure 21 Share LSP: Shared/Non-Shared LSPs

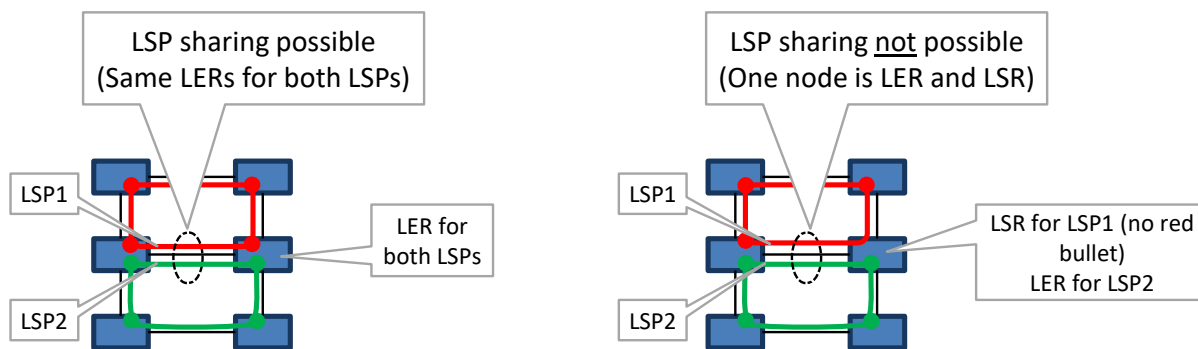


Figure 22 LSP Sharing Possible?

- ▶ 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 Subrings

5.3.1 General

A 'Logical Ring' tunnel can have a maximum of 60 LERs. It can be easily extended by connecting subrings (or 'Subring' tunnels) to it via two interconnection nodes which terminate the subring. Each subring has its own RPL (=ring protection link). The resulting network combining Logical Ring and one or more subrings is called a ladder topology. See figure below.

NOTE: The number of subrings through a link depends on the selected DCN bandwidth profile for that link, see §3.5.

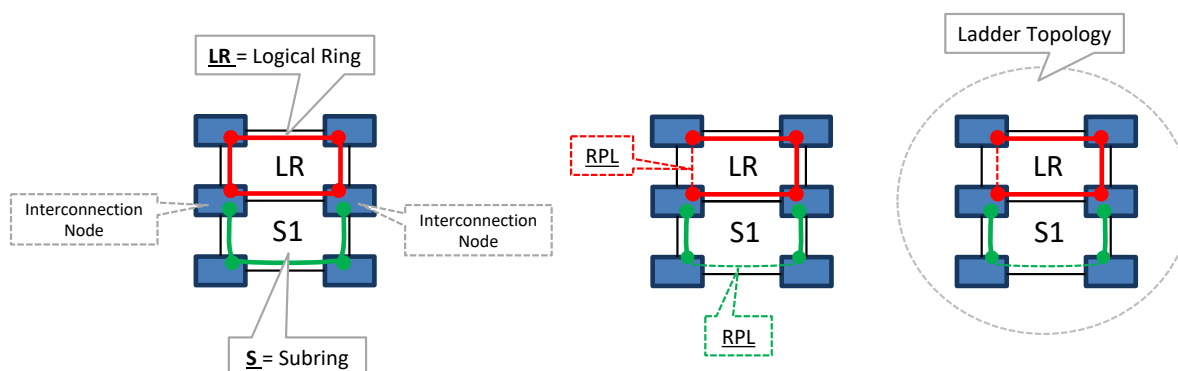


Figure 1 Logical Ring / Interconnection Nodes / Subring / Ladder Topology

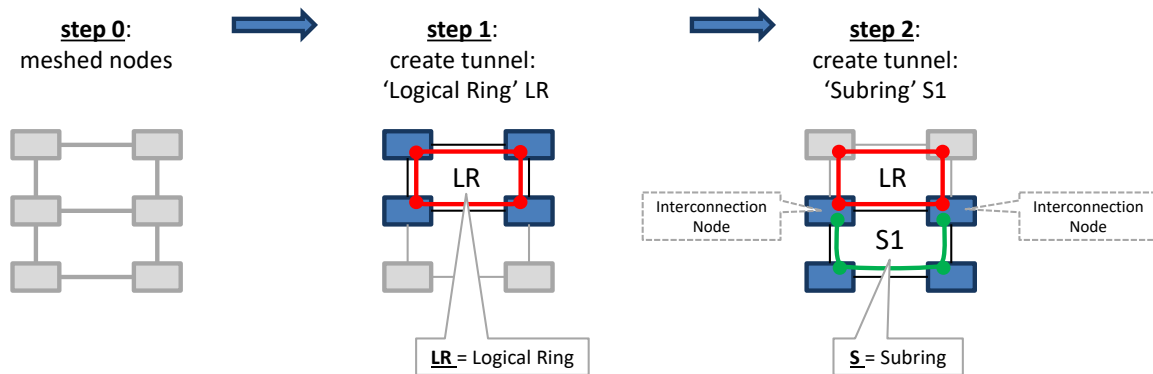


Figure 2 Logical Ring / Subring Setup

A Subring:

- ▶ is a tunnel topology type;
- ▶ is a tunnel extension of a 'Logical Ring' tunnel;
- ▶ must be connected via 2 interconnection nodes to a Logical Ring or the existing ladder topology;
- ▶ is terminated on the interconnection nodes;
- ▶ can be connected to maximum one logical ring;
- ▶ contains at least 3 nodes;
- ▶ has its own RPL;
- ▶ should not share a link with the ladder topology;

- ▶ Different configured Subrings in the same logical ring have another Subring color:

Tunnel Name	Tunnel Type	SubRing Color
ring2	Logical Ring	
Subring1	Subring	—
Subring2	Subring	—

Figure 3 Subring Colors

A Logical Ring:

- ▶ can nest subrings maximum 3 levels deep (Logical Ring not included);
- ▶ can have maximum 15 subrings connected, either directly or indirectly via other subrings or a mix;

An interconnection node:

- ▶ is a node in the ladder topology to which one side of a subring is connected;
- ▶ is always a LER node;
- ▶ can be (re)used or shared by multiple subrings;

Hint: Do not share a link with the ladder topology when configuring a subring.

5.3.2 Ladder Topology Examples

The figures below show example configurations with subrings. LR = logical ring; S = Subring.

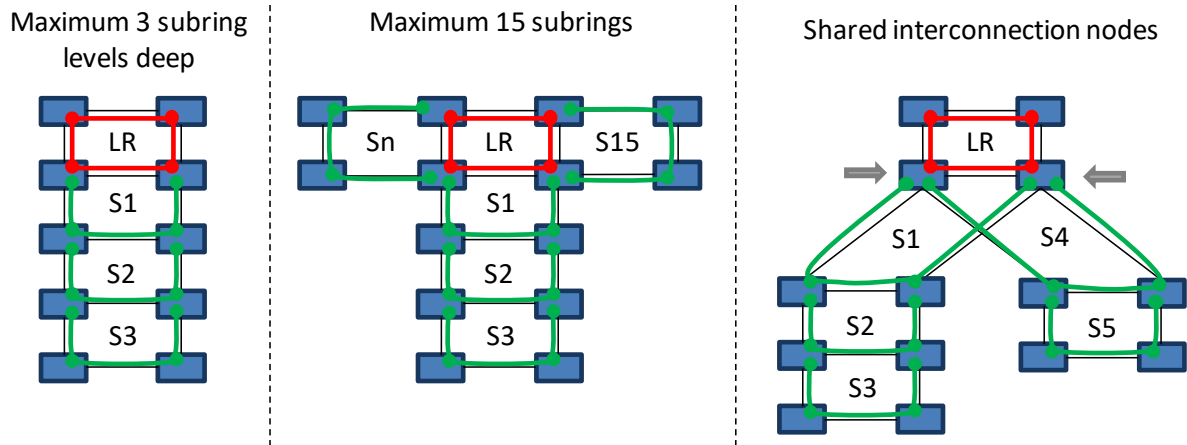


Figure 4 Ladder Topology Example 1

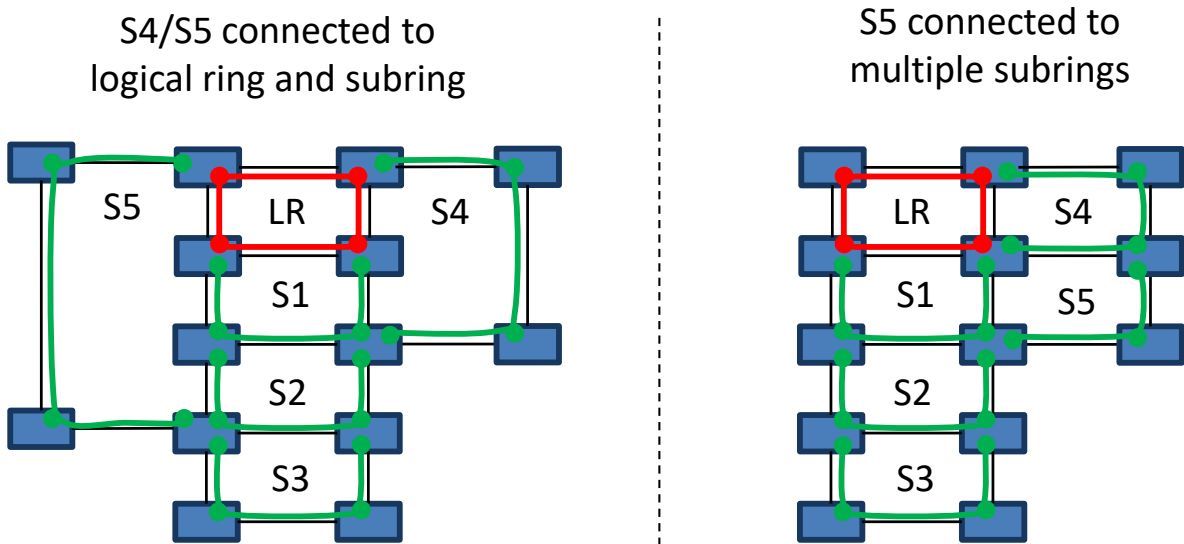


Figure 5 Ladder Topology Example 2

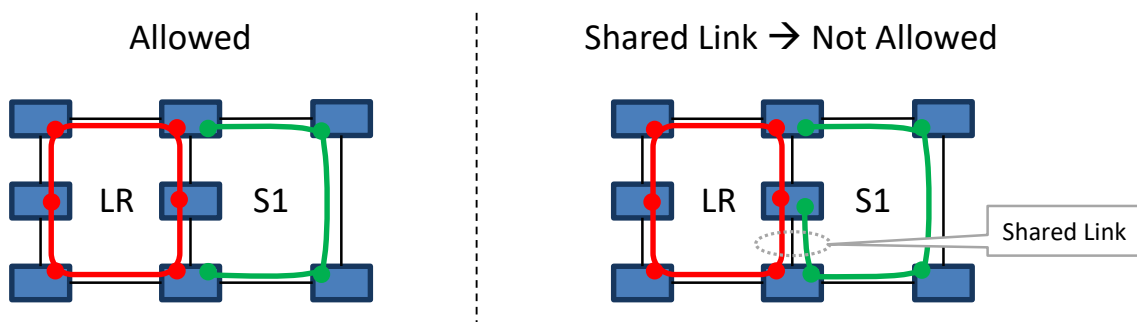


Figure 6 Ladder Topology: Not Allowed: Shared Link

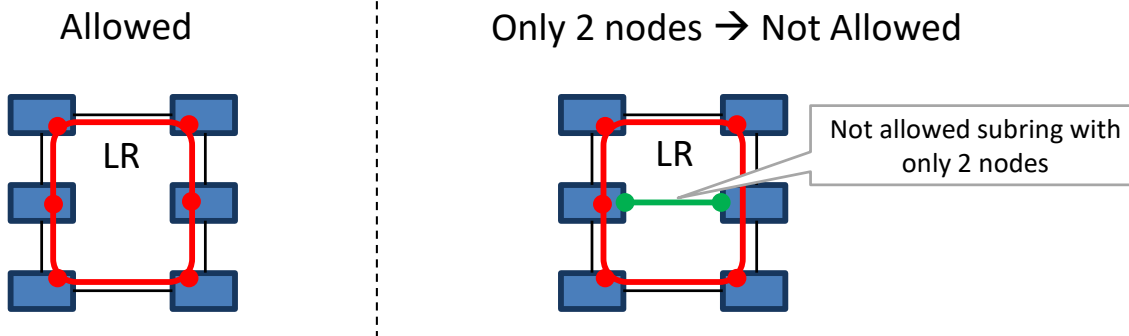



Figure 7 Ladder Topology: Not Allowed: Only 2 Nodes in Subring

5.3.3 Protected Tunnels

The working path and protection path in a protected tunnel are visualized in §5.5.

5.4 Tunnel Modification

Click Dashboard → Configuration → Connections → Tunnels → select tunnel →  to modify the tunnel. The following properties can be modified:

- ▶ Tunnel Name, Ring Priority (if LSP sharing is used);
- ▶ For Ring tunnels: Use HQoS, HQoS Application Priority.

5.5 Monitor Protected Tunnel

The working and protection path in a protected tunnel are visualized in the figure below. This view is visible when selecting a tunnel or tunnel layer in the (Monitoring) Network Tab.

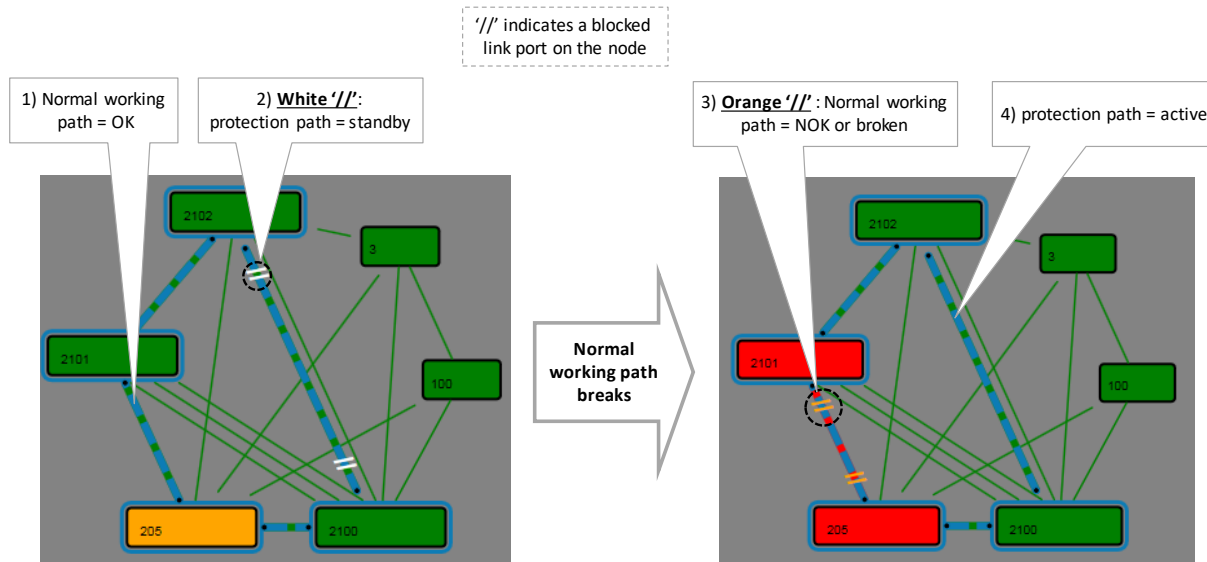


Figure 8 Protected Tunnels: Protection Path, Blocked Port Indication: '//'

5.6 Reporting



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

5.7 Tunnel Actions: Swap Working Path ↔ Protection Path

5.7.1 General

In a tunnel, it is possible to swap manually from the working to the protection path (=backup path) or vice versa. This is very handy for testing purposes or for link maintenance activities.

NOTE: Swapping paths can also be done the hardware way by just pulling out a link or cable when the protection switching is operational.

1. Go to Dashboard → (Monitoring) Network Tile → TUNNELS Tab;
2. Select a protected tunnel in the Tunnels list to highlight the tunnel action button ;
3. Click the tunnel action button ;

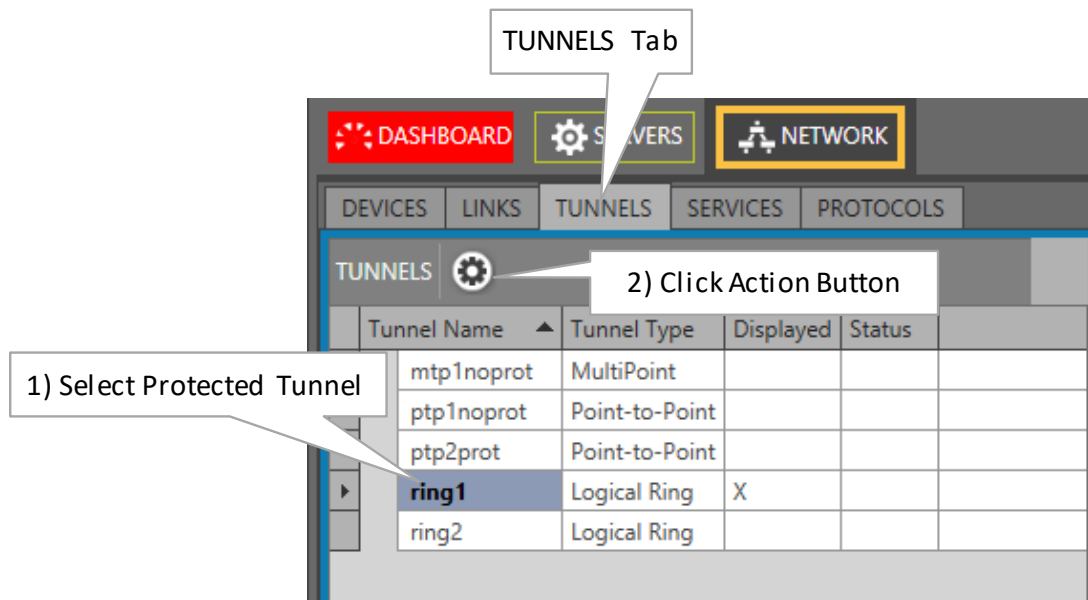


Figure 9 Protected Tunnel/Actions

4. The 'Action on Tunnel' window shows up and depends on the selected tunnel type:
 - ▶ Point-to-Point/Multipoint Tunnels: see §5.7.2;
 - ▶ Ring/Subring Tunnels: see §5.7.3;

5.7.2 Point-to-Point/Multipoint Tunnels

The 'Action on Tunnel' window looks as in the figure below.

NOTE: Click 'Working Path' or 'Protection Path' to highlight it in the network drawing.

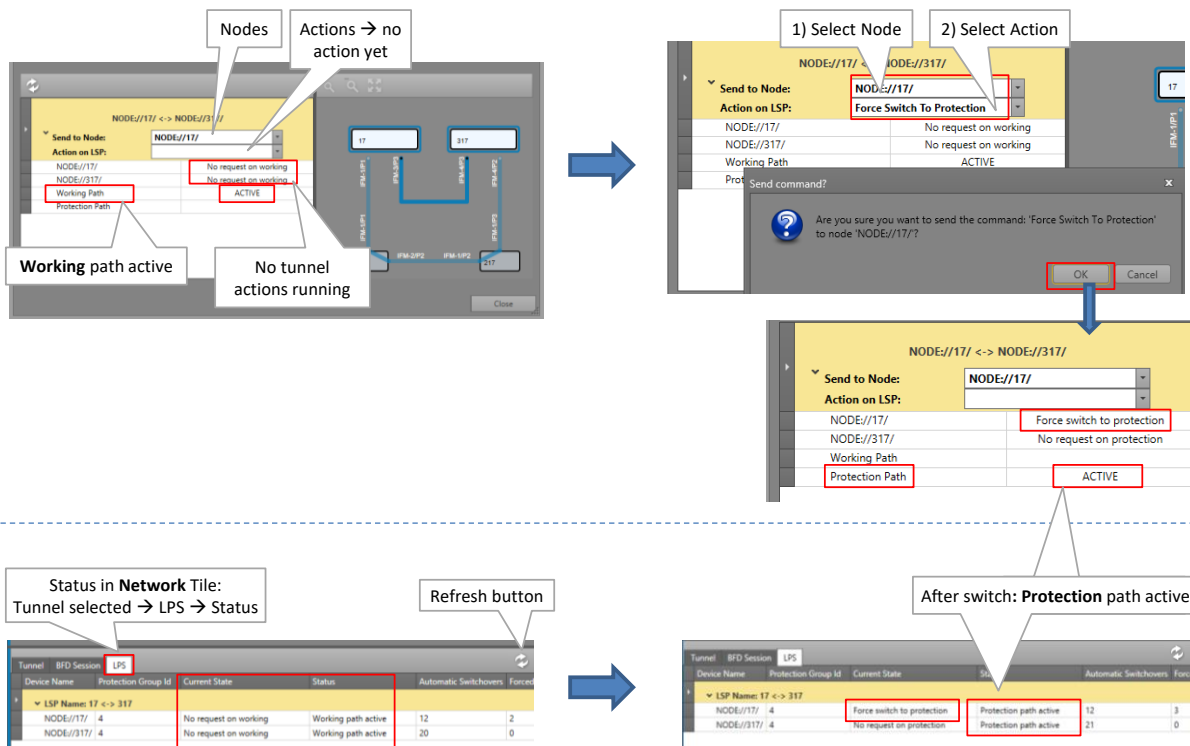


Figure 10 Point-to-Point/Multipoint Action on Tunnel Window

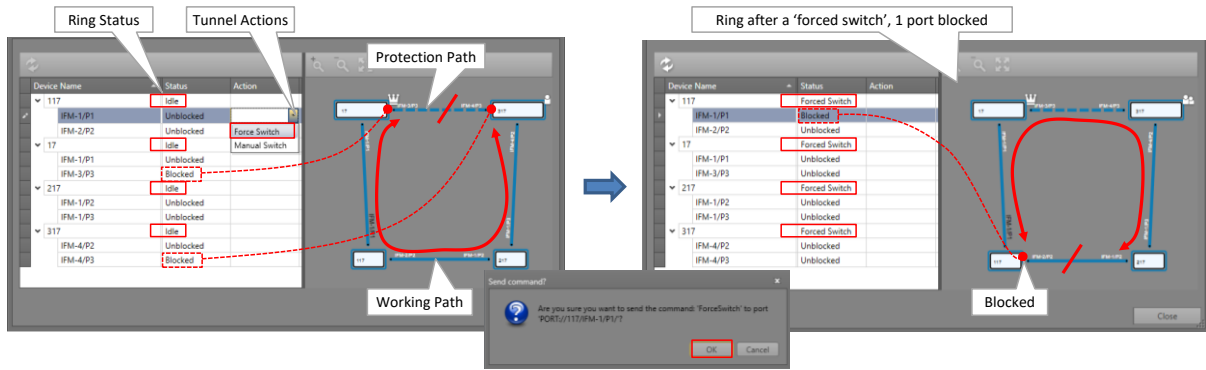
1. Select the node in the Send to Node list that must trigger the swap from working to protection path. For a point-to-point tunnel, either node is OK;
2. Select a '...Switch To...' command in the Action on LSP list, see Table 3 for a command overview. Click OK in the pop-up box to execute the command in the live network!
3. Some status info will change (Node://<node name>/, working path, protection path). For more detailed tunnel status information, click Close. Go to the Network tile → Select tunnel. Status info is shown in the Network drawing or properties tabs via P, e.g. LPS tab (=Linear Protection Switching). Click the Refresh button for faster feedback. Also have a look at §5.5.
4. If the swap is OK ('protection path active'), perform the required maintenance (if any);
5. If you are ready to swap back to the working path and you closed the Tunnel actions window, open it again via .
6. Swap back to the working path by selecting the Clear command in the Action on LSP list. Use 'Clear' only on the node where the '...Switch To...' command was executed! Click OK in the pop-up box to execute it! If the swap back does not occur immediately, probably a Wait to Restore timer has to expire first. The Wait to Restore time has been configured at the tunnel creation.

CAUTION: Use 'Clear' only on the node where the '...Switch To...' command was executed!

5.7.3 Ring/Subring Tunnels

The 'Action on Tunnel' window looks as in the figure below.

NOTE: An 'Idle' ring indicates an up and running ring, the working path (=full line) is active and the protection path (=dashed line) is in standby.



Status in Network Tile: Tunnel selected → Ring Protection

Tunnel	Ring Protection	Pseudo-Wires	BFD Session				
Device Name	Oper Mode	Ring State	Status	Port 1 Name	Port 1 Status	Port 2 Name	Port 2 Status
17	Revertive	Idle	Active	PORT://17/IFM-3/P3/	Blocked	PORT://17/IFM-1/P1/	Unlocked
117	Revertive	Idle	Active	PORT://117/IFM-2/P2/	Unlocked	PORT://117/IFM-1/P1/	Unlocked
217	Revertive	Idle	Active	PORT://217/IFM-1/P3/	Unlocked	PORT://217/IFM-1/P2/	Unlocked
317	Revertive	Idle	Active	PORT://317/IFM-4/P3/	Blocked	PORT://317/IFM-4/P2/	Unlocked

Tunnel	Ring Protection	Pseudo-Wires	BFD Session				
Device Name	Oper Mode	Ring State	Status	Port 1 Name	Port 1 Status	Port 2 Name	Port 2 Status
17	Revertive	Forced Switch	Active	PORT://17/IFM-3/P3/	Unlocked	PORT://17/IFM-1/P1/	Blocked
117	Revertive	Forced Switch	Active	PORT://117/IFM-2/P2/	Unlocked	PORT://117/IFM-1/P1/	Blocked
217	Revertive	Forced Switch	Active	PORT://217/IFM-1/P3/	Unlocked	PORT://217/IFM-1/P2/	Unlocked
317	Revertive	Forced Switch	Active	PORT://317/IFM-4/P3/	Unlocked	PORT://317/IFM-4/P2/	Unlocked

Port on which a 'Force Switch' was executed

Figure 11 Ring/SubRing Action on Tunnel Window

1. Decide which node must trigger, by blocking a port, a swap from working to protection path. For the port that must be blocked, select a port '...Switch' action. See Table 3 for a command overview. Click OK in the pop-up box to execute it in the live network!
2. Both the Node and Port status will change. For more detailed tunnel status information, click Close. Go to the Network tile → Select tunnel. Status info is shown in the Network drawing or properties tabs via P, e.g. Ring Protection tab. Click the Refresh button for faster feedback. Also have a look at §5.5.
3. If the swap is OK (Ring State is Forced Switch/Manual Switch and one port is blocked), perform the required maintenance (if any);
4. If you are ready to swap back to the working path and you closed the Tunnel actions window, open it again via .
5. Swap back to the working path by selecting the Clear command in the **Node** Action list of the node where the '...Switch' command was executed (see figure below). It is the node that has one port in the 'Blocked' state. Click OK in the pop-up box to execute the command! If the swap does not occur immediately, probably a Wait to Restore timer has to expire first. The Wait to Restore time has been configured at tunnel creation.

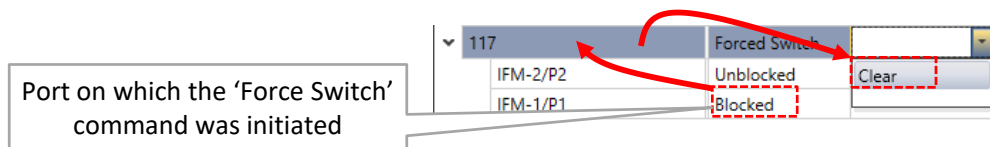


Figure 12 Clear Command in the Node Action List

CAUTION: Use 'Clear' only on the node where the '...Switch' command was executed!

5.7.4 Tunnel Action Commands

Table 3 Tunnel Action Commands

Tunnel Type	Level	Command	Description
Point-to-Point / Multipoint	Node	Clear	Swaps the tunnel back to the working path if this path is OK. Use this command only on the node where a Force/ Manual Switch to Protection command has been performed. If the swap back does not occur immediately, probably a Wait to restore timer has to expire first.
		Force Switch to Protection	- Swaps the tunnel in a forced way to the protection path, also if the protection path is not OK! Attention: if both the working and protection path are not OK, communication will be lost between the two end-points; - After the swap, if the protection path breaks, there will be no automatic swap to the working path.
		Manual Switch to Protection	- Swaps the tunnel to the protection path if all tunnel paths are ok, no error conditions! - After the swap, if the protection path breaks, the tunnel swaps back to the working path automatically if the tunnel was configured as revertive.
		Manual Switch to Working	- Swaps the tunnel to the working path only if the working path is OK! This is useful when your tunnel has swapped to the protection path automatically due to a real break (not via tunnel actions) and your tunnel is non-revertive; - This command has the same effect as the Clear command.
Ring / SubRing	Node	Clear	Same as 'Clear' command described above.
	Port	Force Switch	Same as 'Force Switch to Protection' command described above.
		Manual Switch	Same as 'Manual Switch to Protection' command described above.

6. CSM REDUNDANCY

Prerequisite: one CSM Redundancy voucher (see Ref. [2Mgt] in Table 1) or license is required for each node having two CSMs installed.

A node can have two CSMs installed for redundancy reasons. A CSM can be in the Active, Standby or Passive state. Normally, one CSM will be Active and the other will be Standby.

NOTE: More info on CSM Redundancy can be found in Ref.[2Mgt], [4] in Table 1 and in the redundancy cases in in Ref.[2Mgt];

CAUTION: Both CSMs must be connected with a management cable!

1. Both CSMs can be viewed via Dashboard → Network Hardware;
2. Select the node row in the list and expand it, the two CSMs will be visible if configured and the CSM switchover button becomes active;

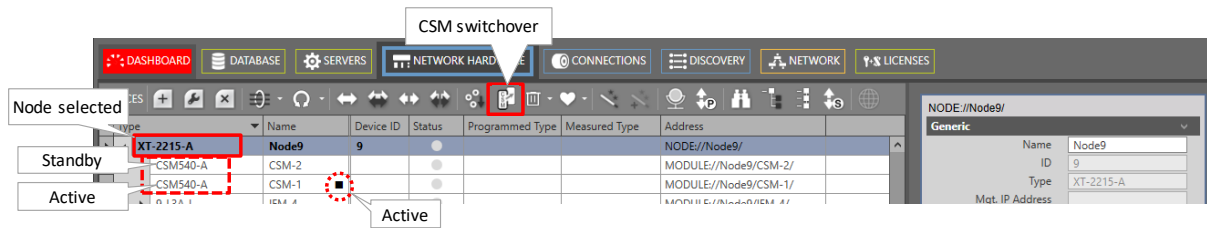


Figure 13 Node with 2 CSMs, CSM Switchover Button

3. The Active CSM is indicated with a little square (■).
4. The Redundancy State can be viewed in the Redundancy section after selecting a CSM:

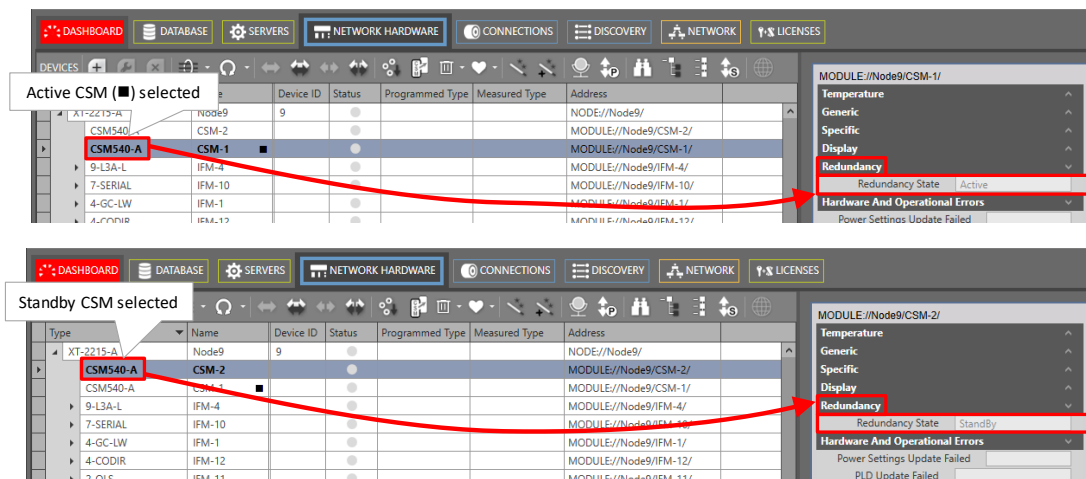



Figure 14 CSM Redundancy Status

5. With CSM redundancy, a switchover is only possible when both CSMs have the same firmware version and one CSM is 'active' and the other CSM is 'standby'.
6. To manually switchover the CSMs or make the Standby CSM the active one and vice versa, select the node row and click the CSM switchover button . More switchover possibilities are described Ref. [4];
7. CSM Redundancy is non-revertive.

7. SYNC E

7.1 General

SyncE is a protocol that manages the distribution of a synchronous clock, based on a PRC (=Primary Reference Clock), network wide over all the nodes that have SyncE configured. The protocol uses SSMs (= Synchronization Status Message) to inform the nodes about the quality of the clock on that link. The clock itself is recovered from the received electrical/optical signals on the configured recovery ports (see also Ref. [4] in Table 1). Recovery ports can be configured on the IFMs that support the SyncE feature, see §12.

Some facts:

- ▶ Maximum one SyncE recovery port per IFM;
- ▶ Maximum four SyncE recovery ports per Node;
- ▶ SyncE is non-revertive for clocks with the same quality and priority (see also §7.3).

All physical port interfaces from the IFMs listed above, support a unidirectional synchronization (=default). E.g. port y on Node2 recovers a clock from port x on Node1. Some interfaces support a bidirectional synchronization as well, e.g. Node2 is able to recover a clock from Node1 and vice versa on the same link. But in operation, the clock will only be recovered in one direction at the same time.

A bidirectional link is possible when both requirements below are met:

- ▶ both ports on the link are configured as recovery port;
- ▶ the physical interface matches one of the interfaces below:
 - ▶ Optical Ethernet (IFM 4-GC-LW/4-GCB-LW, 4-GO-LW, 1-10G-LW, 4-10G-LW, 1-40G-LW);
 - ▶ Optical C37.94 (IFM 2-C37.94);
 - ▶ Electrical Ethernet 100 Mbps (IFM 4-GC-LW/4-GCB-LW).

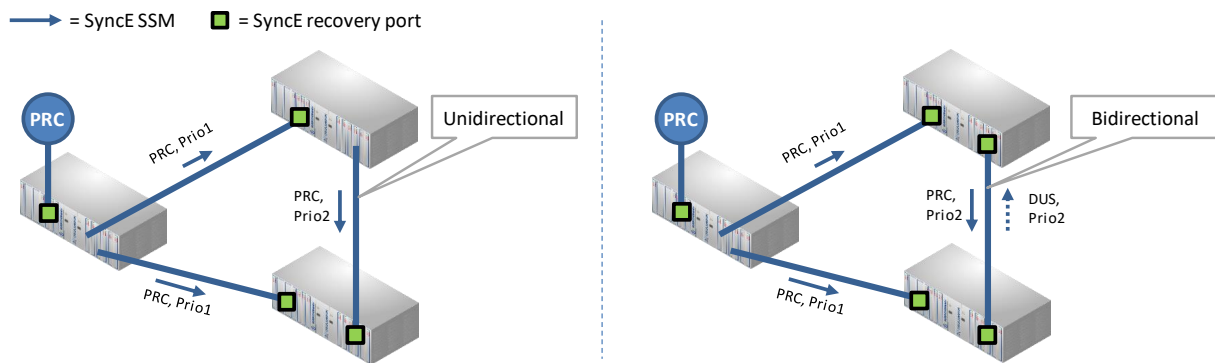


Figure 15 Unidirectional/Bidirectional SyncE Examples

Make sure not to configure timing loops when configuring SyncE. In a timing loop, when the master PRC node breaks down, the other nodes start synchronizing on each other, still believing the master PRC is up and running. As a result, the nodes in the timing loop slowly drift away from the rest of the network, and they possibly never pick up again with the PRC master whenever it comes back because of the non-revertive behavior (see §7.3).

Make sure to build in synchronization redundancy but be aware of timing loops!

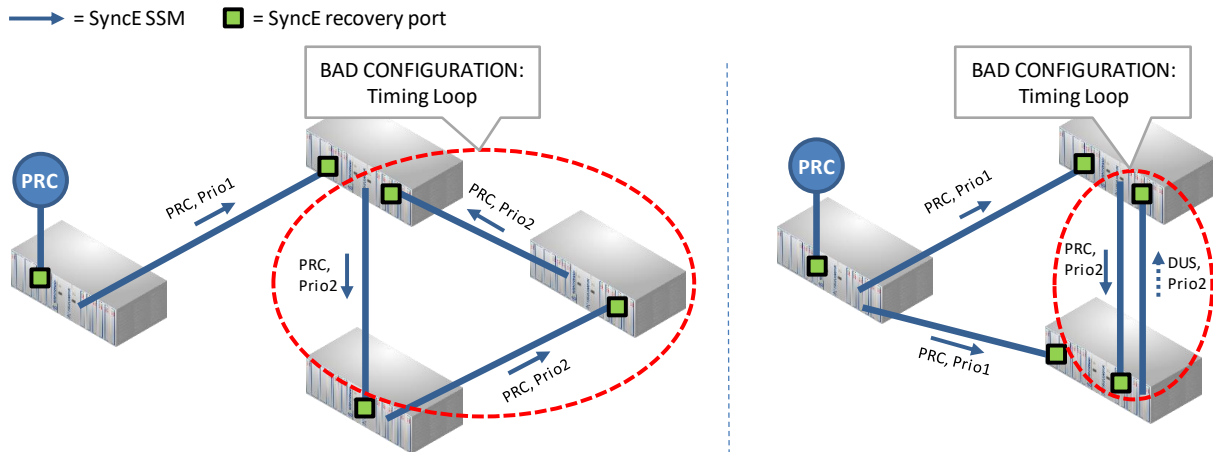


Figure 16 Bad SyncE Examples: Timing Loop

7.2 Configuration

SyncE can be configured/modified via the Dashboard → Network Hardware → Network Settings Wizard button = . The Network Settings wizard opens. The list below summarizes every page in the wizard:

- ▶ Information: Click Next>>;
- ▶ Selection: select SyncE;
- ▶ SyncE Member Ports: A SyncE member port is a port that participates in SyncE, either a port that recovers a clock or a port that forwards a clock. All the ports of the products listed below, are candidate SyncE member ports and show up in the HiProvision list. Set 'Port involved in SyncE = True' for all the ports that must participate in SyncE. Once SyncE has been configured and active later on, SSMs are exchanged between SyncE member ports, to notify the other side with clocking (quality/priority) information;

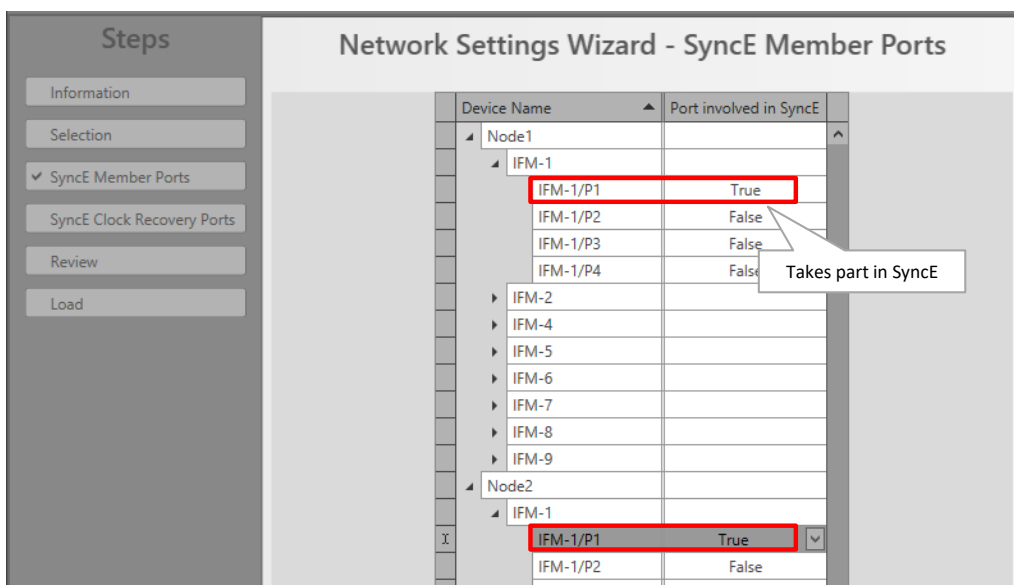


Figure 17 SyncE Member Ports

- ▶ SyncE Clock Recovery Ports: This page lists all the SyncE member ports. The ports that must recover a clock must be configured in this page. A node can have a maximum of 4 clock recovery ports: Clock1...Clock4.
- ▶ SyncE Enabled (default=unchecked): check this checkbox to enable the SyncE configuration screen. This checkbox is also handy later on to disable SyncE for testing purposes after SyncE has been configured, without losing the SyncE configuration.
- ▶ EEC mode (EEC = Ethernet Equipment Clock): fill out the EEC mode. This mode also defines which QL (=Quality Level) values are used. See table below.
 - ▶ EEC1 (=default)(used in Europe, Asia): E1/SDH based technology (2.048 Mbps);
 - ▶ EEC2 (used in North America): T1/SONET based technology (1.544 Mbps);
 - ▶ Disabled: No EEC mode is used, no SyncE will be configured.

Table 4 Provisioned QL Ordered According Quality

SSM Code	Provisioned QL	Description	Quality
See values below	Auto	Provisioned QL is dynamically retrieved from the SSM code in the SSM messages. The mapped Provisioned QL values are listed below.	See values below
EEC1 Mode (E1/SDH)			
2	PRC	Primary Reference Clock, the master clock	1 (=best)
4	SSUT	Synchronization Supply Unit Transit	2
8	SSUL	Synchronization Supply Unit Local	3
11	SEC	SDH Equipment Clock	4
15	DUS	Don't Use for Sync. For testing or maintenance purposes on the link.	5 (=worst)
EEC2 Mode (T1/SONET)			
1	PRS	Primary Reference Source, the master clock	1 (=best)
7	ST2	Stratum 2	2
10	ST3	Stratum 3	3
15	DUS	Don't Use for Sync. For testing or maintenance purposes on the link.	4
0	STU	Stratum Traceability Unknown	5 (=worst)
---	RES	Reserved	---

- ▶ Select Port: To assign a recovery port to Clock1, click the 'Select Port' cell in Clock1 and select the recovery port from the port list. Similar for Clock2, Clock3 and Clock4.
- ▶ Clock Priority (1:highest, 9:lowest) (default=0): see the normal clock selection process in §7.3 for more info. If no recovery port is selected, the value is 0. When a port is selected, the value automatically goes to 1;
- ▶ Provisioned QL (default=Auto): Quality Level of the delivered clock, see §7.3.
- ▶ Lockout:
 - ▶ False (=default): the received clock will be used in §7.3;
 - ▶ True: the received clock on this port will be locked out or not be used in §7.3;
- ▶ Switch Request: Possibility to force a clock usage or overrule the selected clock by the selection process in §7.3;

- ▶ Clear (=default): The normal clock selection process is active for this port, it will only be chosen if it delivers the best clock;
- ▶ Manual: Select the clock recovered on this port, even when it has a lower quality/priority than other clocks delivered to the node. But when the clock on this port gets lost (e.g. link down), another clock will be selected automatically;
- ▶ Force: Always select this recovery port to deliver the clock to the node, even when there is no clock available (anymore) on this port. When the clock gets lost on this port, the node turns into the status 'holdover' meaning that the internal chip clock of the node will be used.
- ▶ Clear WTR: WTR = Wait to Restore. After a synchronization link comes back up, after it was broken or the clock was lost on that port, a WTR timer starts to run on that port. After the WTR timer has timed out, the clock on the port will be available again for the normal clock selection in §7.3.
- ▶ False (=default): The WTR timer times out after 5 minutes.
- ▶ True: The WTR timer times out immediately and Clear WTR automatically drops back to 'False';

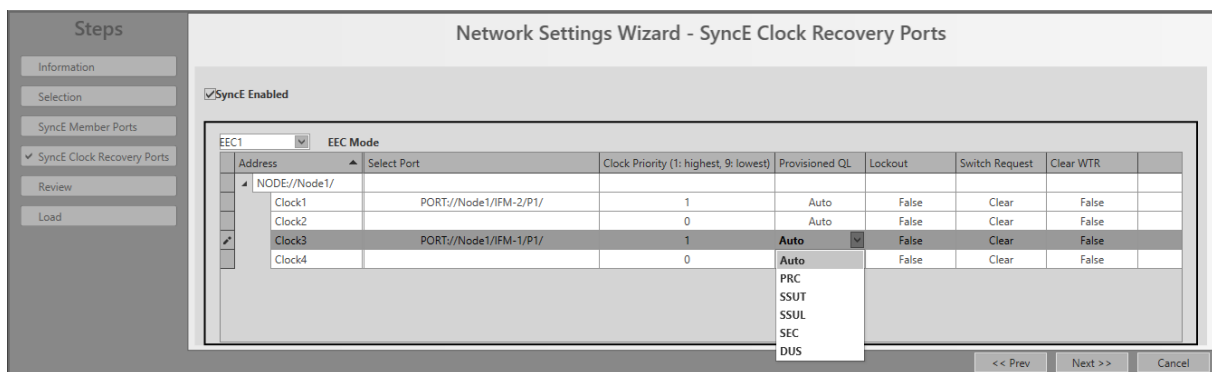


Figure 18 SyncE Clock Recovery Ports

- ▶ 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!

7.3 Normal Clock Selection Process

If you have configured some clock recovery ports in a node, which clock will be used as slave clock for the node?

The normal clock selection process in the node is driven by the following parameters:

- ▶ Provisioned QL;
- ▶ Clock Priority;

The Provisioned QL on a port is provisioned either dynamically via SSMs or statically forced via HiProvision.

- ▶ Dynamically: set Provisioned QL to 'Auto' in HiProvision;
- ▶ Statically: forces the Provisioned QL for this port to a value listed in HiProvision (Table 4), regardless the Provisioned QL from received SSMs;

The selection process:

- ▶ Is the synchronization link available?
- ▶ Provisioned QL: will be verified first. The port with the best (=lowest value) Provisioned QL wins and delivers the clock to the node. Table 4 shows the QL list ordered according quality. E.g., if one port is SSUT and a second port is SEC, SSUT wins. If both ports are SSUT, the Clock Priority will be checked;
- ▶ Clock Priority: Will only be verified when two or more recovered clocks in a node are equally the best according to the provisioned QL. In this case, the clock with the highest priority (=lowest value) will win;
- ▶ SyncE is non-revertive for clocks with same quality and priority: When a recovery port has been selected to deliver the clock (A) to the node, and that clock(A) is lost after a while e.g. due to a link break, a new clock(B) in the node will be selected. When after a while clock(A) is alive again and detected, clock(B) remains selected if clock(B) has the same quality and priority as clock(A). Though, if clock(A) is better than clock(B) according to the selection process, clock(A) will win.

NOTE: The normal clock selection process can be overruled by a Lock Out of a port, or a Forced Switch Request. See also §7.2;

7.4 Operation

Once the SyncE has been configured and loaded in the network, it is up and running. To monitor the running SyncE, see §10.3.

7.4.1 Reporting

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

8. PTP IEEE 1588V2 TRANSPARENT CLOCK

8.1 General

The Precision Time Protocol (=PTP), as defined in IEEE 1588v2, is a protocol that manages the distribution of a synchronous timestamp clock (micro-second accuracy), network wide between an external grandmaster clock and its slaves or substations.

NOTE: For readability reasons, 'IEEE 1588v2' will be further referred to as '1588';

NOTE: In respect to the definitions below, a Dragon PTN node can only act as Transparent Clock, not as Grandmaster, Boundary clock nor Ordinary Clock;

Some definitions:

- ▶ **Grandmaster:** The root-timing device of the synchronization network. At least one grandmaster has to be available in a synchronization network;
- ▶ **Boundary Clock:** Device with multiple network connections where one network connection receives the clock from a master and other network connections are master for a set of slaves. Via this function, one segment is synchronized to another segment;
- ▶ **Ordinary Clock:** Device with a single network connection that is usually a slave, but becomes a master when there is no better master available;
- ▶ **Residence time:** The time that a 1588 packet needs to pass through the device;
- ▶ **End-to-end Transparent Clock (Dragon PTN Node):** A device or node between master and slave clock that just measures and adds the residence time into the correction field of the 1588 packets. The correction field allows the slaves to filter out the variable network delay to obtain a much more accurate timestamp (nano-second accuracy!). It is advised to have a maximum of 20 nodes in the path between Master and Slave.
- ▶ **Network delay:** The total time that a 1588 packet needs to travel from master to slave (or vice versa). 1588 needs the same delay in both directions to work properly;
- ▶ **Clock Offset:** The difference between master clock and slave clock at a specific timestamp 'Tx'. For example, if the master clock indicates 12h:00m:00s at timestamp 'Tx' whereas the slave clock indicates 12h:00m:15s, then the offset between the two clocks is 15s.
- ▶ **Round-trip time:** Time needed for a message to go from master to slave and back to master via the network.

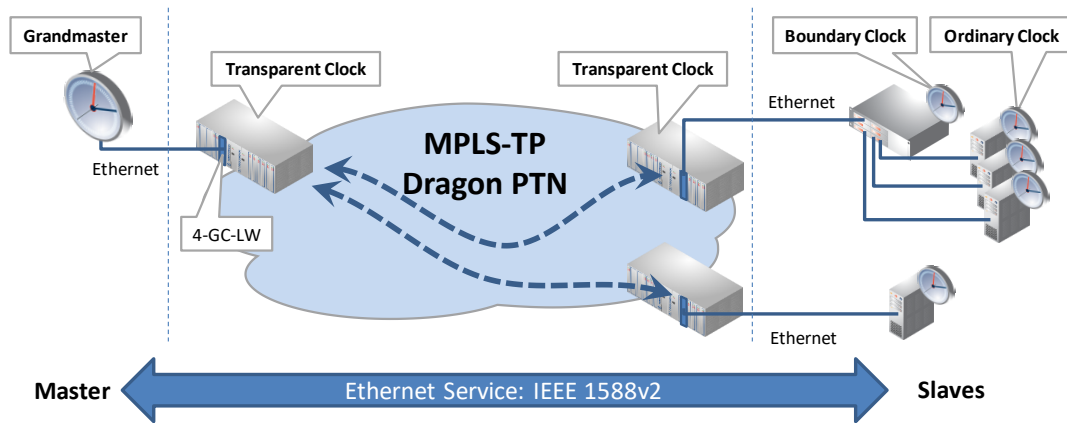


Figure 19 IEEE 1588v2

The master periodically broadcasts the current timestamp as a Sync message to the ordinary clocks to manage and synchronize the time distribution system.

The figure below shows the most important 1588 protocol messages. The slave is able to calculate the network delay and clock offset based on the timestamps T_1 , T_1' , T_2 and T_2' which are passed via the 1588 messages. As a result, the slaves can synchronize to the grandmaster timestamp clock. In addition, it is possible to use get a more accurate timestamp via using the correction field in Transparent Clocks, see further on.

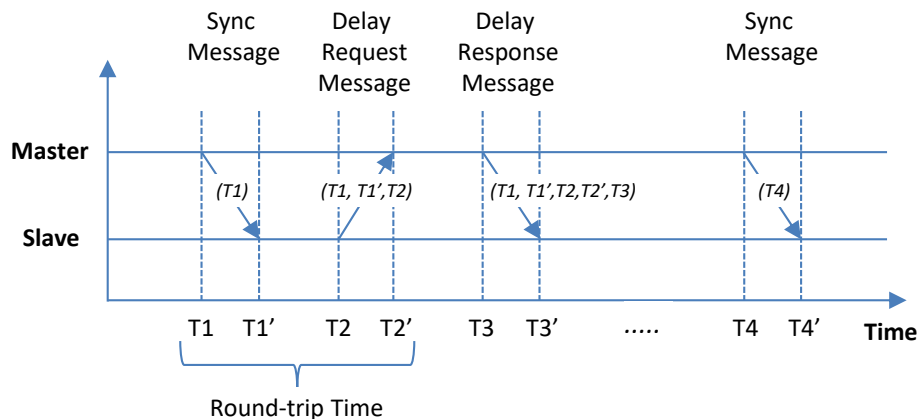


Figure 20 1588 Protocol Messages

8.2 IEEE 1588v2 within Dragon PTN

- ▶ A device or node can only be configured as end-to-end 1588 Transparent Clock, with 1 step synchronization. 1 step means that each message gets the correct timestamp (or correction) when leaving the device, whereas a 2 step synchronization always requires a second message to carry the timestamp;
- ▶ See §12 to find the IFMs that support 1588;
- ▶ 1588 supports multicast traffic (Future: unicast traffic);
- ▶ Enabling 1588 in the paragraphs below means configuring a Dragon PTN node as 1588 Transparent Clock;

- ▶ Not enabling 1588 on the nodes in the 1588 service path means that the nodes will not adapt the 1588 correction field. As a result, applications just exchange 1588 messages via a Dragon PTN Ethernet service, without node interaction, resulting in a less accurate timing.
- ▶ Enabling/Disabling can be done on one or more nodes in the 1588 service path. Enabling 1588 in all/some/none of the nodes in the service path results in very/medium/low accurate timing.

Operation:

- ▶ Transporting 1588 packets requires a port-based Ethernet service;
- ▶ For best timing accuracy, all the **LER and LSR** ports that participate in 1588 must have 'IEEE 1588' enabled on both **port and node level** because all of these nodes cause a transition delay that must be taken into account;

CAUTION: if you enable 1588 in Dragon PTN:

- LER node: enable it on both the node, the LAN and WAN ports of the service;

- LSR node: enable it on both the node and the WAN ports of the service;

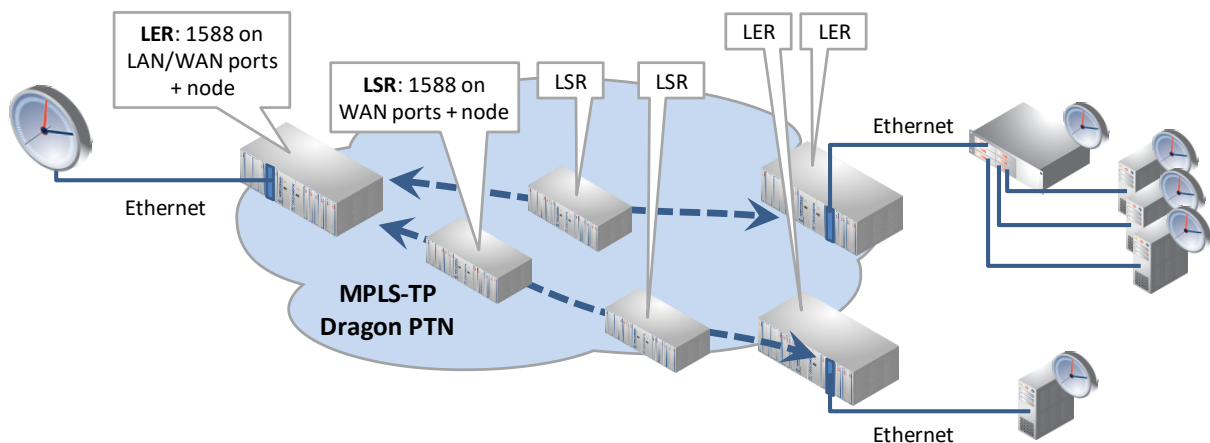


Figure 21 1588 on Port and Node Level for LERs and LSRs

- ▶ An external 1588 grandmaster clock broadcasts Sync messages with timestamp 'x' to the Dragon PTN network via Ethernet ports on the supported IFMs. Multiple masters are possible, the best master clock will be selected by the slaves based on a priority field.
- ▶ 1588 enabled in Dragon PTN?
 - ▶ **Yes:** Nodes are configured as transparent clock and fill out the correction field in the 1588 messages. Each node adds its own ' Δn ' (=the time needed to pass the node) to the correction field. The total time correction for the entire path through Dragon PTN ' Δy ' = the sum of all ' Δn 's of each node on that path. Multiple message 1588 sequences (n) will result in a lot of ' Δy 's and will finally average in ' Δz '. This average correction has filtered out the variable networking delay resulting in a very accurate calculated timestamp in the slaves.

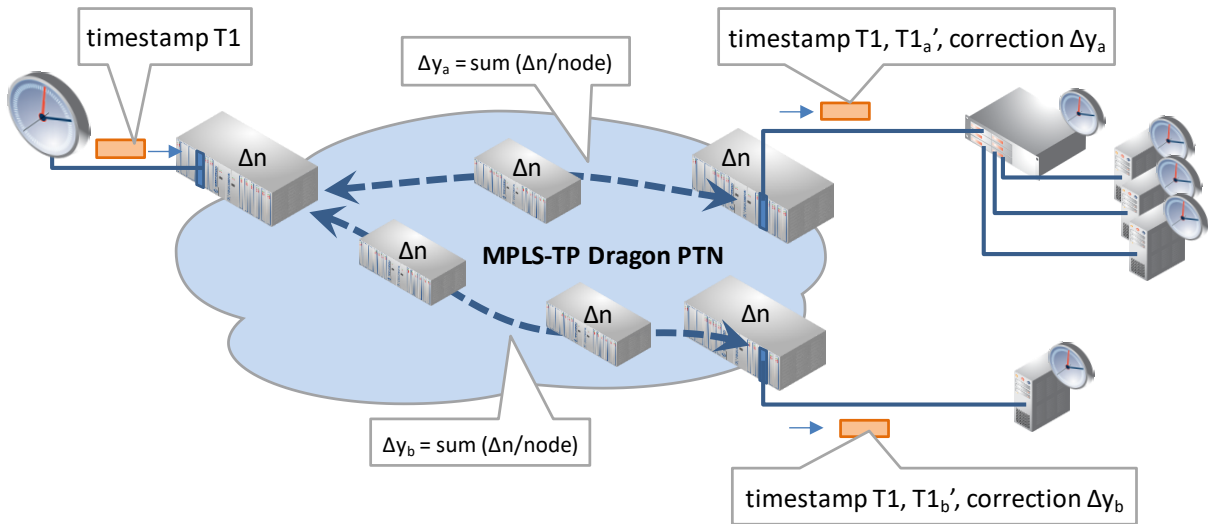


Figure 22 1588 Enabled: Transparent Clock Correction

- ▶ **No:** The 1588 protocol messages are only transported via the Ethernet service, the nodes do not interact with the messages, no correction field is filled out. The resulting calculated timestamps in the slaves will be less accurate.

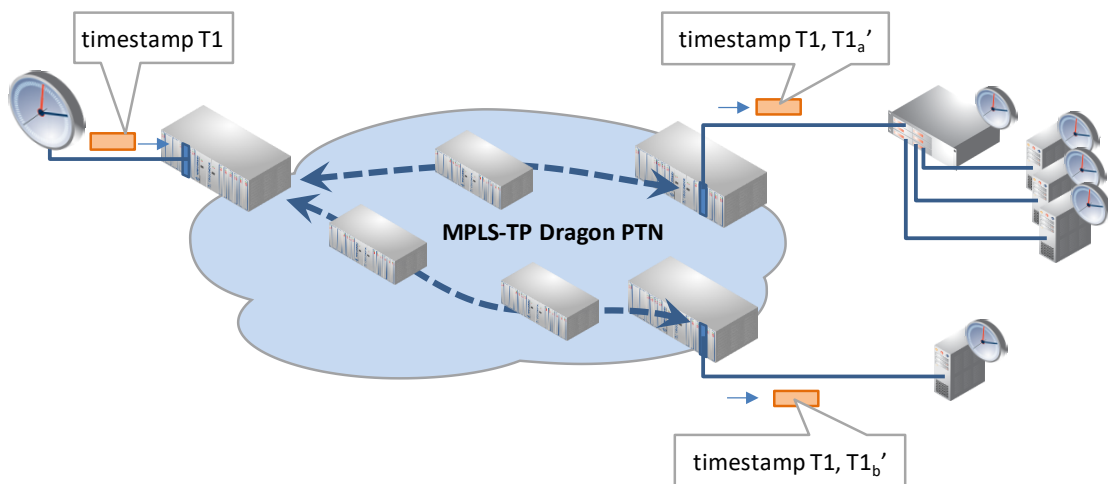


Figure 23 1588 Not Enabled: No Clock Correction

- ▶ Different encapsulation types can be configured in HiProvision to transport the messages. Within an Ethernet service, all the LER and LSR ports that participate in 1588 must have configured the same encapsulation type;

8.3 Configuration

Follow the steps below to configure 1588 in the Dragon PTN network:

1. Node level: Enable 1588 on each LER and LSR node of the Ethernet service:

- ▶ Node: Dashboard → Network Hardware → (DEVICES) Node → Generic → IEEE 1588 Global Enable:
 - ▶ True: 1588 is enabled in this node;
 - ▶ False (=default): 1588 is disabled on this node. No port in this node will be able to participate in 1588;

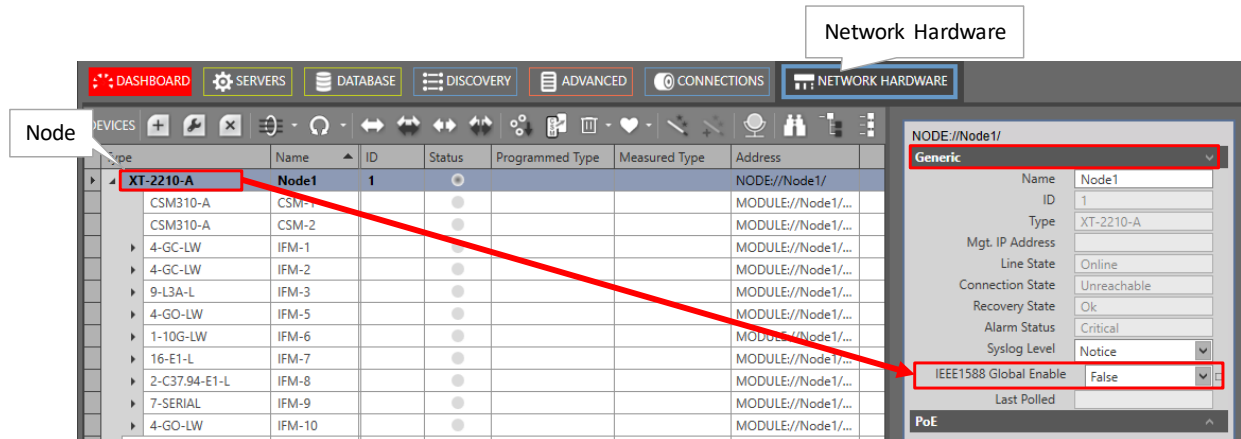


Figure 24 1588 Node Settings

2. Port level: Enable 1588 on each port of the Ethernet service (including LAN and WAN ports) of all the LER and LSR nodes of that Ethernet service and set the correct (and same) encapsulation type:

- ▶ Port: Dashboard → Network Hardware → (DEVICES) Port → IEEE1588 Settings;
 - ▶ IEEE1588 Enable:
 - ▶ True: If the IEEE 1588 Global Enable on node level is True, this port participates in 1588;
 - ▶ False (=default): This port will not participate in 1588;
 - ▶ IEEE1588 Encapsulation: 'Ethernet' or 'Ethernet IP/UDP'. Find below the required values of the different fields (provided by the applications) in the received 1588 messages.
 - ▶ **Ethernet**: Ptp in pure Ethernet, Destination MAC address = 01-1B-19-00-00-00, Ethertype = 0x88F7, VLAN = not checked, Domain = 0..3;
 - ▶ **Ethernet IP/UPD (*)**: Ptp in UDP/IP, Destination MAC address = any multicast, Ethertype = 0x0800, UDP port = 319, Destination IP address = 224.0.1.129, VLAN = not checked, Domain = 0..3;
 - ▶ (*) : currently not possible on ports 1 and 2 of the 4-GC-LW, 4-GCB-LW, 4-GO-LW cards IFMs.
 - ▶ IEEE1588 Reset Engine: False/True: Set to True and click the apply button to reset the 1588 engine immediately on that port, no load required!

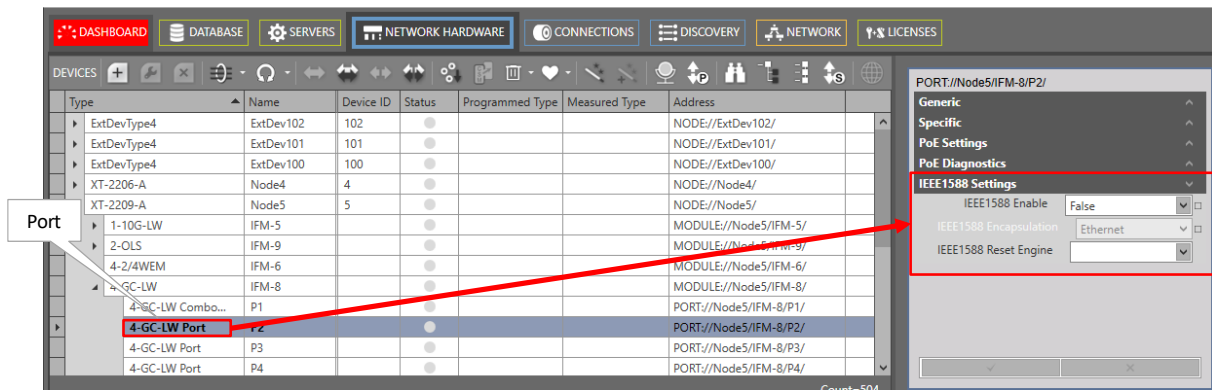



Figure 25 1588 Port Settings

3. Load changes via Network Hardware Tab →  into the live network to activate them. It starts the configuration load manager. See Ref. [2Mgt] in Table 1 for an overview of this tool.

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!

8.4 Operation

Once the 1588 has been configured and loaded in the network, it is up and running. To monitor the running 1588, see §10.4.

9. LOSS/DELAY/ASSURANCE MONITORING

9.1 General

Prerequisite: Some services must have been created. Any type of service is OK.

The Assurance tile on the dashboard allows to execute some network performance tests:

- ▶ Loss Measurement, see §9.2;
- ▶ Delay Measurement, see §9.3;
- ▶ Tunnel Ping, see §9.4;
- ▶ Tunnel Traceroute, see §9.5;

9.2 Loss Measurement (=LM)

9.2.1 General

Loss measurement monitors if there is any message loss on the route between two nodes (=source and destination) in a service. The measurement process is performed by sending LM test messages over the selected route. The LM test messages will compare port counters of the source and destination port.

CAUTION: Loss Measurement depends on the traffic that goes through the selected service and requires ONLY unicast traffic in the service to operate correctly.

9.2.2 Configuration

To create such a measurement, follow the steps below:

1. Click the Assurance tile on the dashboard;
2. Create a loss measurement by clicking the button (multiple measurement entities can be created, e.g. an entity for each route, and started afterwards). The Assurance wizard opens;
3. Measurement Selection:
 - ▶ Fill out a measurement name and select the type 'Loss Measurement';
 - ▶ Select the service on which a loss measurement must be performed;
4. Node Selection:
 - ▶ Select the source and destination node by clicking the node in the drawing or by clicking the 'Selected' checkbox;
 - ▶ Select the route between the two nodes on which you want to verify if there is any loss. This can be done via clicking a 'Selected' checkbox in the 'Possible Routes' list.

NOTE: In a point-to-point and multipoint tunnel, a single route (line) between two nodes implies both the active and protection path (if any).

CAUTION: When another LER is located between the selected source and destination, an unintentional loss can be measured, because the extra in-between LER could take its part of the traffic as well.

5. Measurement Parameters:
 - ▶ Priority: Indicates the priority that was assigned during service creation. The loss measurement messages will have the same priority.
 - ▶ Interval (default = 1s, range[100ms, 1s, 10s, 1min, 10min]): Loss measurement messages are sent according to the configured interval. By default, such a message will be sent every second.
 - ▶ Max Time (default = 4s, range[4-172800s]): Configures the maximum amount of time that the loss measurement can last;
 - ▶ Number of Messages (default = 3, range[3-8192]): Configures the number of messages that can be sent during the measurement. The sending of messages will stop when the Max Time has expired or the number of messages sent equals the configured Number of Messages;

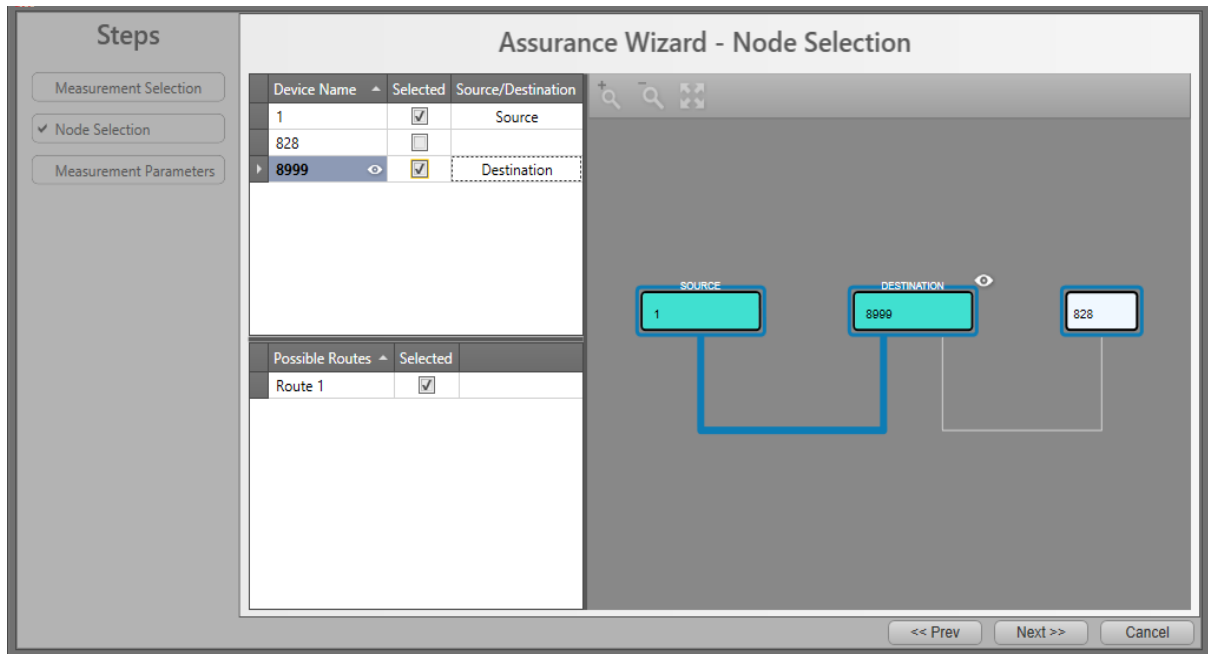




Figure 26 Assurance Wizard: Loss Measurement Configuration

9.2.3 Operation

a. Single Measurement

Once the configuration has been done, click the play button  to start the measurement. The Status field indicates 'running'.

The measurement will stop when one of the 3 events below occur:

- ▶ the configured maximum time has expired;
- ▶ the configured number of messages has been sent;
- ▶ the stop button  has been clicked;

Once the measurement has stopped, the Status field indicates 'idle' and the results are filled out. See further on for more info on the results.

NOTE: When the service is configured in a protected point-to-point or point-to-multipoint tunnel, the measurement will be performed on the active path. If the protection path becomes the new active path (after a switchover, e.g. cable break) the measurement continues on the new active path;

NOTE: Point-to-point, Point-to-Multipoint tunnel: In the case of a switchover of the active path, a loss might occur,

NOTE: Ring Tunnel: In the case of a switchover to the protection RPL path during the measurement, a loss will only occur if the only path left from source to destination is via the RPL path;

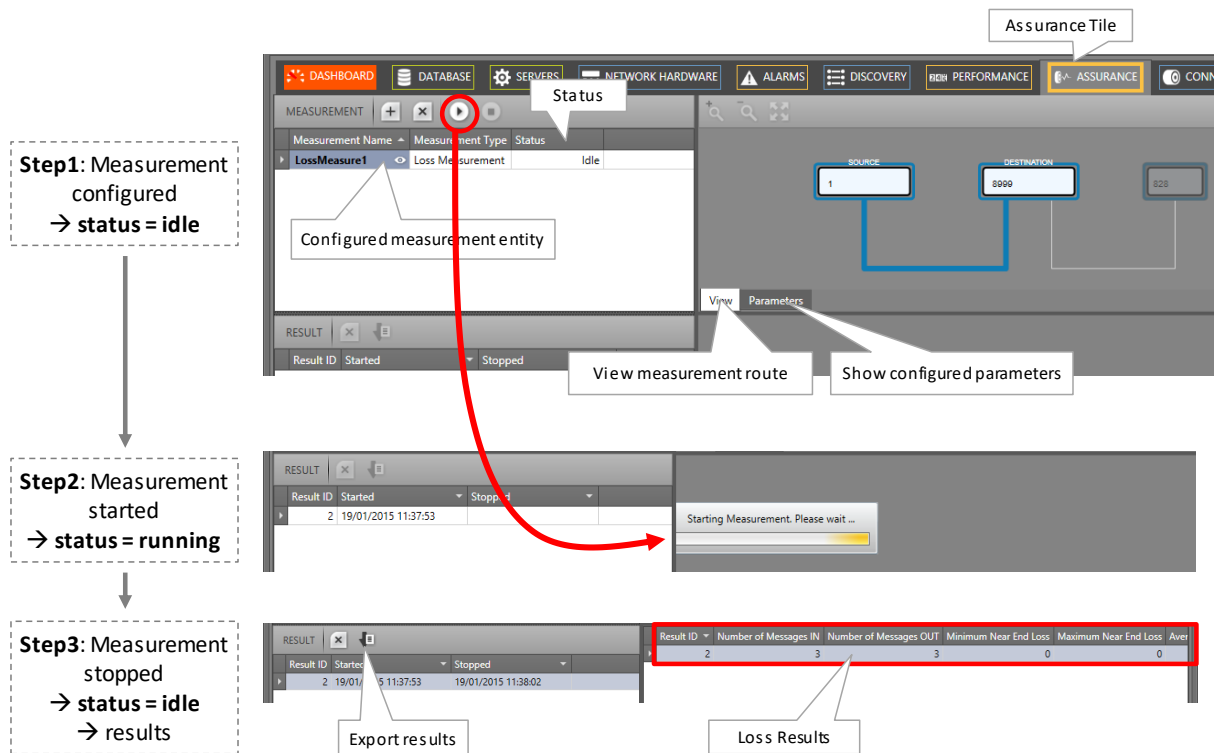


Figure 27 Loss Measurement in Operation

b. Multiple Measurements

Within the same service, multiple measurements can run simultaneously provided that both measurements have no common part in the selected route.

Within different services, multiple measurements of different services can run simultaneously.

NOTE: Maximum 5 measurements (regardless the performance test) can be started and run simultaneously per node.

c. Results, Loss, No Loss

The LM test compares port counters of the source and destination port. Based on these values during the entire period of the loss measurement, the result fields will be filled out. When multiple loss measurement entities are configured, click the entity in the result list to show its results. An overview of the result values can be found below:

Result ID	Number of Messages IN	Number of Messages OUT	Minimum Near End Loss	Maximum Near End Loss	Average Near End Loss	Minimum Far End Loss	Maximum Far End Loss	Average Far End Loss
2	3	3	0	0	0	0	0	0

Figure 28 Loss Measurement Result Values

CAUTION: a loss occurred when 'Number of Messages IN' <> 'Number of Messages Out' or one of the other 'Loss' fields <>0

- ▶ Number of Messages IN: The number of LM test messages that have made the entire round trip from source to destination and back to source;
- ▶ Number of Messages OUT: The number of LM test messages that has been sent out from the source to the destination. In normal circumstances, 'Number of Messages IN' = 'Number of messages Out';
- ▶ Near End Loss:
 - ▶ Value = 0: No loss;
 - ▶ Value > 0: Indicates a loss on the source side. The destination side has sent more traffic to the source than the source has received from the destination. The 'value' indicates the difference in measured packets. Each LM test message results in a 'value'. At the end of the measurement, a minimum, maximum and average of these 'values' is filled out.
- ▶ Far End Loss:
 - ▶ Value = 0: No loss;
 - ▶ Value > 0: Indicates a loss on the destination side. The source side has sent more traffic to the destination than the destination has received from the source. The 'value' indicates the difference in measured packets. Each LM test message results in a 'value'. At the end of the measurement, a minimum, maximum and average of these 'values' is filled out.

NOTE: The results can be exported via clicking the export button .

9.3 Delay Measurement (=DM)

9.3.1 General

Delay measurement measures the delay on the route between two nodes (=source and destination) in a service. The measurement process is performed by sending DM test messages over the selected route. The measured delay is a round-trip delay. It means that the delay is measured from the source to the destination and back to the source.

9.3.2 Configuration

Similar to the configuration of Loss Measurement, see §9.2.2;

Differences with Loss Measurement:

- ▶ Type Selection: Delay Measurement;
- ▶ Interval range: default = 1s, range [1-1000]s;

9.3.3 Operation

a. Single Measurement

Similar to Loss Measurement, see §9.2.3a;

b. Multiple Measurements

Similar to Loss Measurement, see §9.2.3b;

c. Results, Delay

When multiple delay measurement entities are configured, click the entity in the result list to show its results. An overview of the result values can be found below:

Result ID	Number of Messages IN	Number of Messages OUT	Minimum Delay (ms)	Maximum Delay (ms)
1	3	3	0.021	0.022

Figure 29 Delay Measurement Result Values

- ▶ Number of Messages IN: The number of DM test messages that have made the entire round trip from source to destination and back to source;
- ▶ Number of Messages OUT: The number of DM test messages that has been sent out from the source to the destination. In normal circumstances, 'Number of Messages IN' = 'Number of messages Out';
- ▶ Delay (ms): Indicates the roundtrip delay for a DM test message to travel from the source to the destination port and back to the source. Each DM test message measures a Delay. At the end of the measurement, a minimum and maximum of these values is filled out.

NOTE: If all the DM test messages are lost (no DM test message returns back to the source), then the delay is infinite and all the delay fields remain empty.

NOTE: The results can be exported via clicking the export button .

9.4 Tunnel Ping


9.4.1 General

Tunnel Ping is a simple and efficient mechanism to detect data plane failures in MPLS LSPs or tunnels in Dragon PTN. Tunnel Ping is used to detect connectivity between two adjacent LER nodes via Echo Request messages on the selected LSP in a tunnel.

The measured delay is indicative and is a round-trip delay. It means that the delay is measured from the source to the destination and back to the source.

9.4.2 Configuration

To create such a measurement, follow the steps below:

1. Click the Assurance tile on the dashboard;
2. Create a Tunnel Ping measurement by clicking the  button (multiple measurement entities can be created and started afterwards). The Assurance wizard opens;
3. Measurement Selection:
 - ▶ Fill out a measurement name and select the type 'Tunnel Ping';
 - ▶ Select the tunnel on which a measurement must be performed. By default, all tunnels are shown in the tunnel list, but can be filtered by using the service filter;

4. Node Selection:
 - ▶ Select the source and destination node by clicking the node in the drawing or by clicking the 'Selected' checkbox.
 - ▶ Select the LSP between the two nodes on which the ping must be performed via clicking the 'Selected' checkbox in the 'LSP Name' list.
5. Measurement Parameters:
 - ▶ Number of Echo Requests (default = 5, range[1-500]): the number of Echo Request messages to send from source to destination.
 - ▶ Packet Size (default = 200 bytes, range[100-1450] bytes): the size in bytes of each Echo Request.
 - ▶ TTL Value Time (default = 255, range[1-255]): TTL (= Time to Live) limits the number of node hops or LSR nodes. If the Echo Request does not reach the destination within <TTL value> LSR nodes, the tunnel ping has failed;
 - ▶ Receive Timeout (default = 2sec, range[1-1000]msec/sec/min): configures a tunnel ping receive timeout. If the source does not receive an Echo Reply from the destination within the configured timeout, the tunnel ping has failed.
 - ▶ Send Interval (default = 1sec, range[1-1000]msec/sec/min): configures the time interval between two consecutive Echo Requests;
 - ▶ Traffic Class (default = 4, range[0-5]): Configures the priority of the Echo Request packets. A higher value indicates a higher priority. Higher priority packets will have less delay through the network.

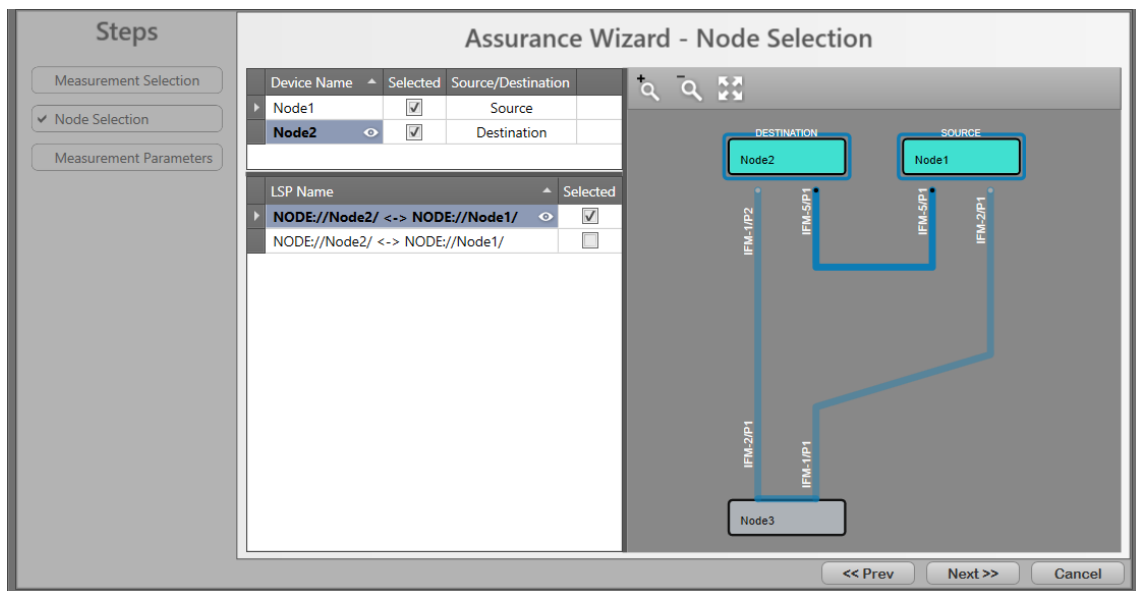


Figure 30 Assurance Wizard: Ping Measurement Configuration

9.4.3 Operation

a. Single Measurement

Similar to Loss Measurement, see §9.2.3a;

b. Multiple Measurements

Similar to Loss Measurement, see §9.2.3b;

c. Results, Tunnel Ping

When multiple Tunnel Ping measurement entities are configured, click the entity in the result list to show its results. An overview of the result values can be found below:


Result ID	Started	Stopped
2	18/05/2016 10:42:54	18/05/2016 10:43:01
1	18/05/2016 10:40:28	18/05/2016 10:40:34

Result ID	Status	Max Round Trip (msec)	Min Round Trip (msec)	Average Round Trip (msec)	Number Received Echo Requests	Number Transmitted Echo Requests
2	Success	2	1	1	5	5

Figure 31 Tunnel Ping Result Values

- ▶ **Status:**
 - ▶ In Progress: The measurement is ongoing, new measured values will be updated automatically until the status is Success or Failure;
 - ▶ Success: The measurement has finished successfully, the destination was reachable within the configured parameters;
 - ▶ Failure: The measurement has failed, the destination was not reachable within the configured parameters e.g. because of a broken link. Try again with adapted configuration parameters e.g. higher Receive Timeout etc... If the problem persists, investigate the path.
- ▶ **Max/Min/Average Round Trip:** Maximum/minimum/average round trip delay of all the send out Echo Requests;
- ▶ **Number Received Echo Requests:** the number of transmitted echo requests that made the total round-trip from source to destination and back to the source;
- ▶ **Number Transmitted Echo Requests:** the number of transmitted echo requests from source to destination;

NOTE: In normal circumstances, 'Number Received Echo Requests' = 'Number Transmitted Echo Requests' and the delays are rather small (some milliseconds). If this is not the case, something might be wrong in the path between source and destination.

The results can be exported via clicking the export button .

9.5 Tunnel Traceroute

9.5.1 General

If Tunnel Ping failed in reaching the destination, Tunnel Traceroute can be used to detect a potential blocking point along a selected tunnel segment. It measures all the nodes or hops along the selected tunnel segment (or LSP) between the source and destination node until a possible blocking point has been reached (e.g. broken link..). As a result, you know where the blocking is located. If Traceroute can reach the selected destination, no blocking point was found and the entire path between source and destination is OK.

Furthermore, Traceroute measures a round-trip delay from source to each hop and back to the source. The measured delay is indicative. The measurement process is performed by sending Echo Request messages over the selected tunnel segment to each hop.

9.5.2 Configuration

Similar to the configuration of Tunnel Ping, see §9.4.2. Differences with Tunnel Ping:

- ▶ No TTL must be configured.

9.5.3 Operation

a. Single Measurement

Similar to Loss Measurement, see §9.2.3a;

b. Multiple Measurements

Similar to Loss Measurement, see §9.2.3b;

c. Results, Tunnel Traceroute

When multiple Traceroute measurement entities are configured, click the entity in the result list to show its results. A result overview can be found below:

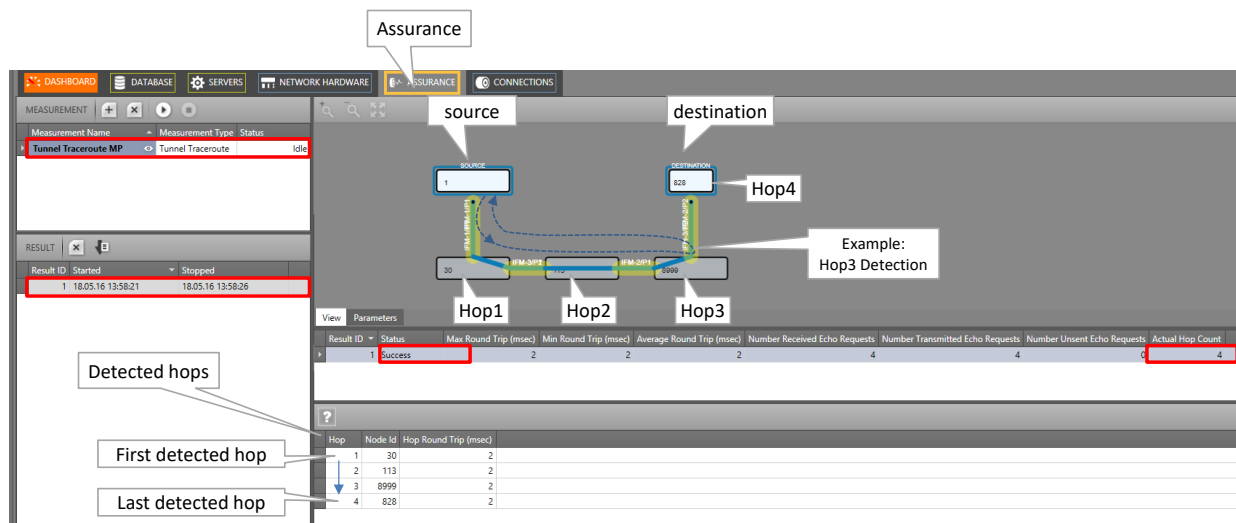




Figure 32 Traceroute Results Overview

Similar to the results of Tunnel Ping, see §9.4.3c. Differences with results of Tunnel Ping:

- ▶ Actual hop count: indicates which hop is being measured at that time. All the result fields in that row are related to the hop measured at that time. These fields will be overwritten when the next hop (=Actual Hop Count + 1) is being measured;
- ▶ After each hop that has been measured, a new hop row will be added in the Detected Hops list, indicating the Node Id and Hop Round Trip time.

NOTE:  If an expected hop is not shown in the 'Detected Hops' list, it means that the tunnel is down on one or both sides of the expected hop.

The results can be exported via clicking the export button .

10. PERFORMANCE COUNTERS AND MONITORING

10.1 General

Performance counters can provide detailed statistics about the Dragon PTN network. The counters can that can be configured and viewed are listed in Dashboard → Performance → Counter Control List. See figure below:

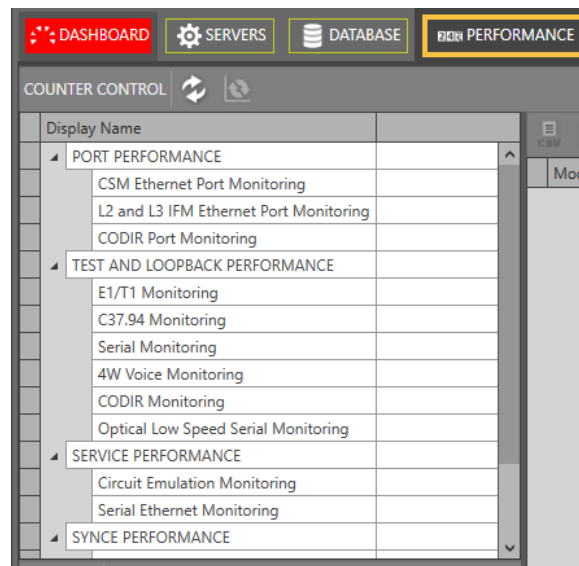


Figure 33 Performance Tab: Counter Control

Below, find the performance overview and cross references:











- ▶ Port Performance: §10.2;
- ▶ SyncE Performance: §10.3;
- ▶ IEEE 1588 Performance: §10.4;
- ▶ Health Monitor: §10.5;

10.2 Port Performance



10.2.1 CSM Ethernet Port Monitoring

Follow the steps below to monitor Ethernet ports from Ethernet IFMs (e.g. 4-GC-LW, ...) directly interconnected with the CSM.

NOTE: Monitoring ports from L2/L3 IFMs can be monitored in the next paragraph.

1. In the 'Counter Control' section, click  to expand Port Performance;
2. Click CSM Ethernet Port Monitoring, see Figure 34;
3. In the 'Port Counters' section, a list with devices or nodes pops up;
4. To monitor some port counters, expand the node and its IFMs to show its ports;
5. Check (= ) / uncheck(= ) the port Selected checkbox to show/hide the available port counters (e.g. 'Bytes in', ...) in the Counter statistics section;
6. 'C' indicates the current or latest value, 'P' the previous value of a specific counter;
7. Optional: Select one or more cells and click  to show the counters in a graph overview. These cells will be highlighted with a green border. Add counters to different graph panes via selecting default/pane1/pane2 before adding the counter. Maximum 4 counters can be shown in a graph. To remove a counter from the graph, click the highlighted counter cell in the table and click .
8. Repeat previous steps for all the ports and/or counters that must be monitored;
9. In the table section, click the CSV icon  to export the counter table data into a csv file;
10. In the graph section, click the CSV icon  to export the counter graph data into a csv file;
11. In the graph section, click the Log icon  to continuously plot (according to the configured refresh rate, see below) the counter graph data into a csv file;
12. Click  in the Counter Control section to refresh all counter values;
13. Click  to reset counter values;

NOTE: For 'Test & Loopback Performance', another reset method must be used, see further;

14. By default, automatic refreshing is disabled. It can be enabled/disabled by clicking  /  in the Counter Graphs section. The automatic refresh rate can be configured via the drop-down list 1s, 5s, 10s, The automatic refreshing applies to the counters in the graph, including the highlighted cells in the statistics table;
15. Options: The graphs can be optimized (labels etc.) via the Options drop-down list;

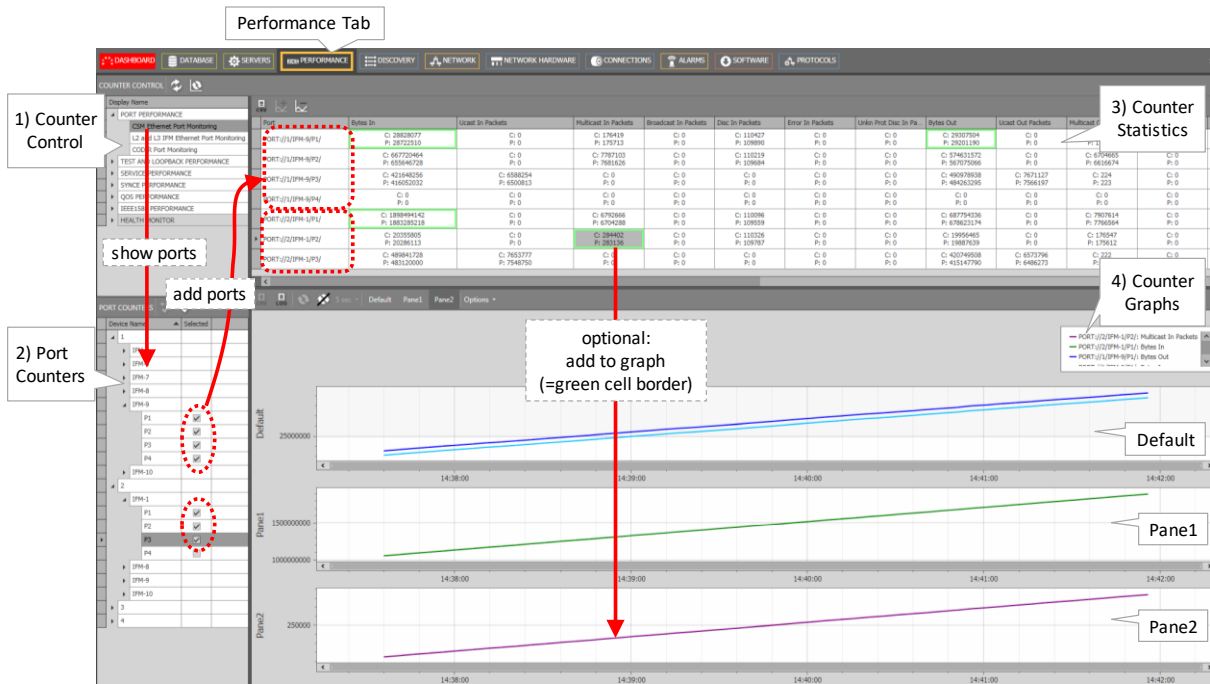


Figure 34 CSM Ethernet Port Monitoring


Table 1 CSM Ethernet Port Monitoring Fields

Field	Values	Description	Curative Action
Port	value	Monitored port	
Bytes In (ingress)	bytes	The total number of L2 bytes that the interface has received.	
Ucast In Packets (ingress)	packets	The number of packets, delivered by this sub-layer to a higher (sub-) layer, which were not addressed to a multicast or broadcast address at this sub-layer.	
Multicast In Packets (ingress)	packets	The number of multicast packets received by the interface.	
Broadcast In Packets (ingress)	packets	The number of received Broadcast Packets	
Disc In Packets (ingress)	packets	The number of discarded inbound packets (even though no errors had been detected in these packets) and not delivered to a higher-layer protocol. Example: free up buffer space, packets without labels, routing problems, unknown VLANs...	Verify your HiProvision configuration.
Error In Packets (ingress)	packets	Number of incoming packets that had an error and as a result were dropped. This error could be for example, FCS errors.....	Verify also other counters, e.g. FCS error, Jabber error, MTU error
Unkn Prot In Packets (ingress)	packets	Not supported, should always be zero	
Bytes Out (egress)	bytes	The total number of L2 bytes that the interface has transmitted.	
Ucast Out Packets (egress)	packets	The total number of packets that higher-level protocols requested to be transmitted, and which were not	

Field	Values	Description	Curative Action
		addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.	
Multicast Out Packets (egress)	packets	The number of multicast packets transmitted by the interface.	
Broadcast Out Packets (egress)	packets	The number of transmitted Broadcast Packets	
Disc Out Packets (egress)	packets	The number of discarded or untransmitted outbound packets (even though no errors had been detected). Example: free up buffer space, packets without labels, routing problems, unknown VLANs...	Verify your HiProvision configuration.
Error Out Packets (egress)	packets	Number of outgoing packets that had an error and as a result were dropped. This error could be for example, FCS, CRC errors.....	Verify also other counters, e.g. FCS error, Jabber error, MTU error
Bandwidth In (kbps) (ingress)	kbps	The consumed incoming bandwidth in the last measurement = (('Bytes In Current' - 'Bytes In Previous')/1000)/Time	
Average Bandwidth In (kbps) (ingress)	kbps	The average of the 5 latest 'Bandwidth In' measurements. Every (manual) refresh is a new measurement.	
Bandwidth Out (kbps) (egress)	kbps	The consumed outgoing bandwidth in the last measurement = (('Bytes Out Current' - 'Bytes Out Previous')/1000)/Time	
Average Bandwidth Out (kbps) (egress)	kbps	The average of the 5 latest 'Bandwidth Out' measurements. Every (manual) refresh is a new measurement.	
Average Frame Size In (bytes) (ingress)	bytes	The average frame size of all the frames that are received on this port in the 5 latest measurements. Every (manual) refresh is a new measurement.	
Average Frame Size Out (bytes) (egress)	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.	
Oversized Frames (ingress)	frames	The number of Ethernet frames that had an Ethernet frame size bigger than the fixed oversize limit of 1544 bytes, but smaller or equal than the configured MTU size in HiProvision. These frames were NOT dropped!	
Jabber Error (ingress)	frames	The number of Ethernet frames that matched all the conditions below: <ul style="list-style-type: none"> - Ethernet frame had an FCS error (= Frame Check Sequence error indicating that the frame was being corrupted during transmission → CRC mismatch) - Ethernet frame size > oversize (=1544 bytes, fixed) - Ethernet frame size <= MTU size (=configured in HiProvision) These frames were dropped!"	Transmission problems, bit failures, check cabling...
Fcs Error (ingress)	frames	The number of Ethernet frames that matched all the conditions below: <ul style="list-style-type: none"> - Ethernet frame had an FCS error (= Frame Check Sequence error indicating that the frame was being corrupted during transmission → CRC mismatch) - Ethernet frame size <= oversize (=1544 bytes, fixed) 	Transmission problems, bit failures, check cabling...

Field	Values	Description	Curative Action
		- Ethernet frame size <= MTU size (=configured in HiProvision) These frames were dropped!"	
Mtu Error	frames	Ethernet frame size > MTU size: The number of Ethernet frames that had an Ethernet frame size bigger than the configured MTU size in HiProvision. These frames were dropped! These frames could have a valid or invalid FCS (for example if frames are concatenated).	Possible Transmission problems, bit failures, check cabling... also possible FCS error. If no problems of this kind, just increase the configured MTU size in HiProvision or lower your application MTU size.

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;

10.2.2 L2 and L3 Ethernet Port Monitoring

L2 and L3 Ethernet Port Monitoring can be found in the figure below. This section must be used to show counter and performance data of both the front (P1...Pn) and back end (BE1...BE_m) ports of the L2/L3 IFMs. A detailed monitoring set-up description and the fields description is the same as in §10.2.1.

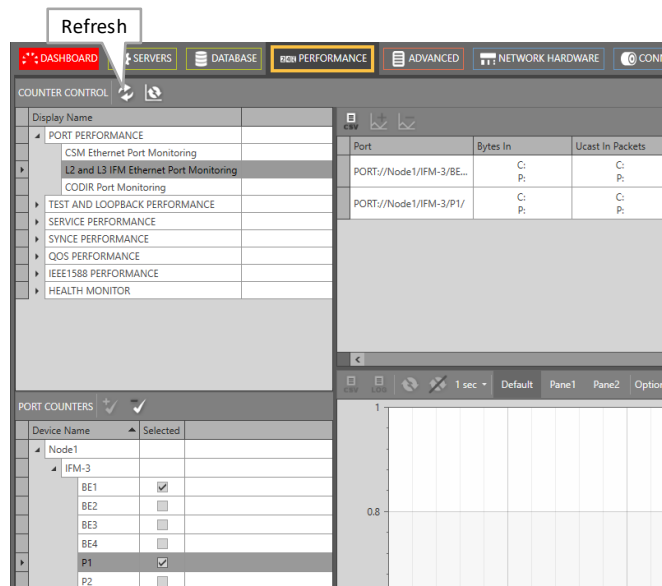


Figure 35 L2 and L3 Ethernet Port Monitoring

10.2.3 CODIR Port Monitoring

CODIR Port monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §10.2.1.

NOTE: See also Ref. [11] in Table 1 for more info on ITU-T G.703 Code Conversion and the violation block.

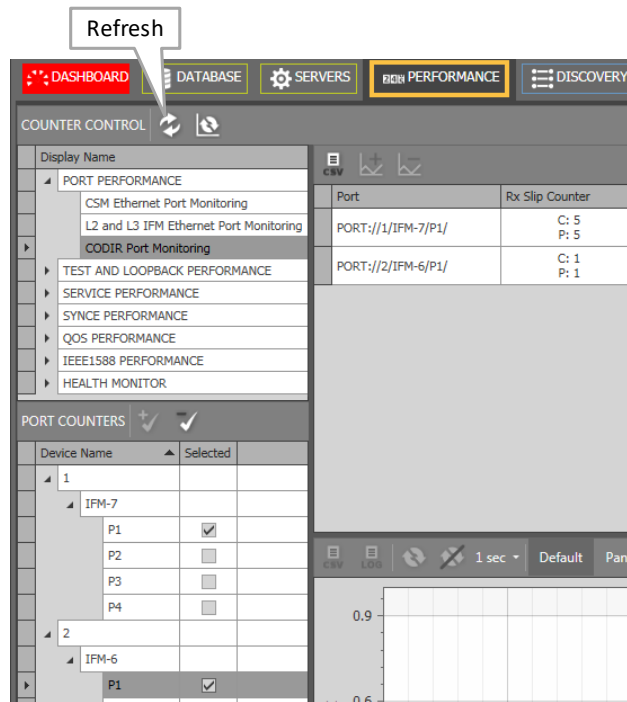


Figure 36 CODIR Port Monitoring

Table 2 CODIR Port Monitoring Fields

Field	Values	Description	Curative Action
Port	value	Monitored port	
Rx Slip Counter (ingress)	count	In ITU-T G.703 Code Conversion (64kbps), the alternation in polarity of the blocks is violated every eighth block. The violation block marks the last bit in an octet. If the violation block is not received as expected, the 'Rx Slip Counter' will increase and might indicate a synchronization problem between source and destination.	Check synchronization between source and destination when this counter increases
<p>Note: Click the Refresh button for the latest results; Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

10.3 SyncE Performance

Once SyncE has been configured as described in §7, it can be monitored. SyncE monitoring can be found in the figure below. It shows 2 sections:

- ▶ System Information;
- ▶ Clock Information;

A detailed monitoring set-up description is similar to the description in §10.2. This monitoring does not support graph monitoring as in §10.2.1.

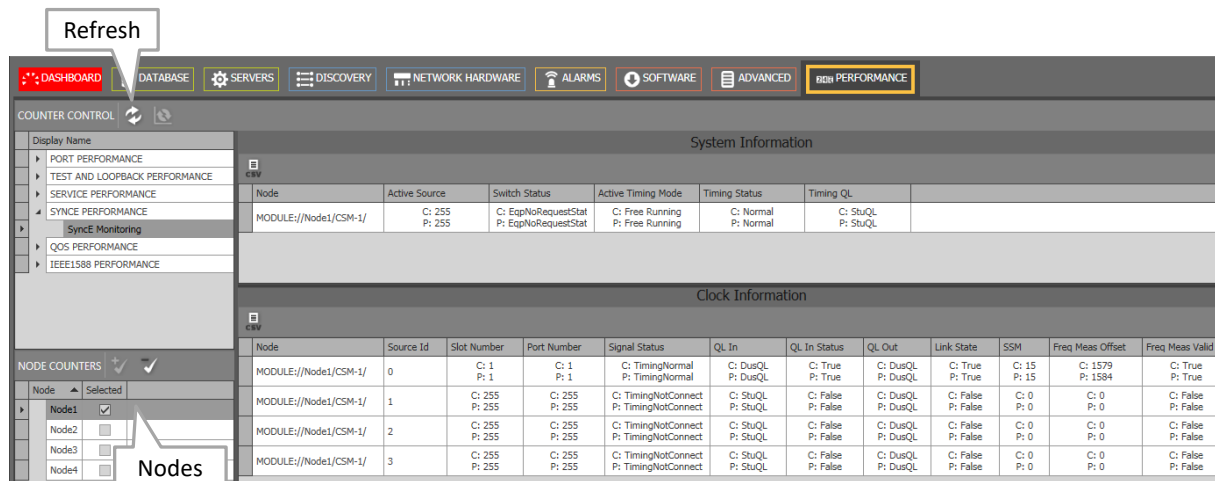


Figure 37 SyncE Monitoring

Table 3 SyncE Monitoring 'System Information' Fields

Field	Values	Description	Curative Action
Node	url	Monitored node	
Active Source	value	The active source is the index[0..3] of the recovered clock to which the node is currently locked or slaving. A node can have a maximum of 4 clock recovery ports configured in the SyncE wizard in row[1..4]. Row[1..4] maps to index[0..3]. Index 255 means that the node has no valid clock to slave on due to e.g. free running, holdover, ...	
Switch Status	value	EqpNoRequestStatus: no forced or manual clock has been set, normal dynamic clock selection is active, EqpManualStatus: manual clock has been configured via switch request. EqpForcedStatus: forced clock has been configured via switch request. EqpUndefined: the clock status is unknown.	Only during maintenance, a state different from EqpNoRequestStatus is expected. If not, verify your configuration.
Active Timing Mode	value	The configured active timing mode: Freerunning: SyncE is not enabled on the node, normal node internal clock is in use Locked: SyncE is enabled on the node and the node clock is locked on one of the recovered clock sources Holdover: SyncE is enabled but the node clock is not locked on any of the recovered clock sources.	
Timing Status	value	Normal: Either no SyncE is enabled (=freerunning) or SyncE is enabled and the node is slaving to clock. Holdover: The clock to which the node slaved got lost. The node turned into the status 'holdover' meaning that the internal node clock will be used further on.	Holdover: problem with incoming links; link down, no SSMs, clock too unstable... Verify the incoming links
Timing QL	quality values in Table 4	The resulting clock quality of the node, either based on a fixed clock configuration or a dynamic clock selection process. The possible quality levels can be found in Table 4.	

Note: Click the Refresh button for the latest results;

Note: 'C' value in cell = current value; 'P' value in cell = previous value;

Table 4 SyncE Monitoring 'Clock Information' Fields

Field	Values	Description	Curative Action
Node	url	Monitored node	
Source ID	value	The clock source index of the configured recovery port. Index [0..3] maps onto row[1..4] in the SyncE configuration wizard.	
Slot Number	value	The node slot number in which the clock source is recovered	
Port Number	value	The port number in which the clock source is recovered	
Signal Status	value	TimingNormal: the clock on this interface is available and ready for use TimingFailed: this clock cannot be used e.g. clock out of spec, etc... TimingWTR: clock is valid but must stabilize first until the Wait to restore timer (WTR) expires (=5 minutes) TimingNotConnected: no clock configured or defined on this clock input source or recovery port.	
QI In (ingress)	quality values in Table 4	The clock quality on the clock input source. This value can be a fixed configured value or a dynamic quality via detected SSM messages.	
QI In Status (ingress)	True/False	True: quality of this clock input has been configured/detected False: quality not present or not configured/detected yet.	
QI Out (egress)	quality values in Table 4	The clock quality that the node sends out to neighbor nodes. It is the resulting best clock that is available in the node.	
Link State	True/False	True: the link is up on this port False: the link is down on this port	If the link is down, verify your links.
SSM	quality values in Table 4	Last received SSM value.	
Freq Meas Offset	ppb	Parts Per Billion (=PPB) frequency difference between the recovered clock (if any) and the internal node clock.	
Freq Meas Valid	True/False	True: the measured Freq Meas Offset could be measured and is valid False: the measured Freq Meas Offset could not be measured and is invalid	false and link is up: clock is too unstable... verify connected device or recovered clock
<p>Note: Click the Refresh button for the latest results; Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

10.4 IEEE 1588 Performance

Once IEEE 1588 has been configured as described in §8, it can be monitored. IEEE 1588 monitoring can be found in the figure below. In normal IEEE1588 operation, the 'In Modified' and 'Out Modified' counters should increase, the other counters should remain 0. A detailed monitoring set-up description is similar to the description in §10.2.1.

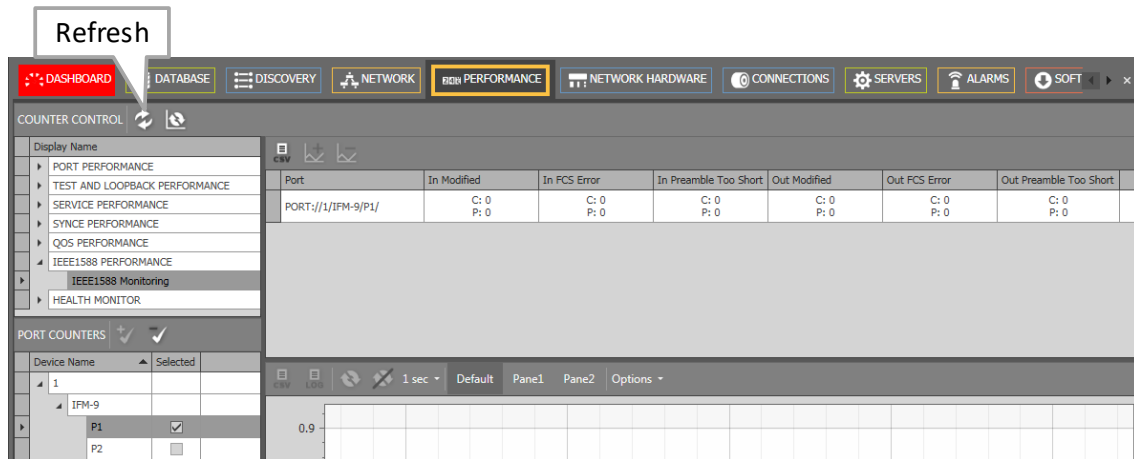


Figure 38 IEEE 1588 Monitoring

Table 5 IEEE 1588 Monitoring Fields

Field (*)	Values	Description	Curative Action
Port	value	Monitored port	
In Modified (ingress)	frames	The number of received IEEE 1588 frames on this port. These frames carry a valid timestamp from the master. This frame has been prepared by the node to measure the travel time through this node. If this counter increases, it means that IEEE 1588 is operating normally.	
In Fcs Error (ingress)	frames	The number of received Ethernet frames that had an FCS error (= Frame Check Sequence error) indicating that the frame was being corrupted during transmission → CRC mismatch. These frames will be dropped by the node!	Transmission problems, bit failures, check cabling...
In Preamble Too Short	frames	The number of received IEEE 1588 frames with a preamble that was too short. The preamble is a 7 byte pattern preceding an Ethernet frame and is used for clock synchronizing between devices.	
Out Modified (egress)	frames	The number of outgoing IEEE 1588 frames on this port. The travel time through the node has been measured. This time has been filled out in the IEEE 1588 correction field of the outgoing IEEE 1588 frame. If this counter increases, it means that IEEE 1588 is operating normally.	
Out FCS Error (egress)	frames	Similar to 'In FCS Error' but for outgoing frames.	
Out Preamble Too Short	frames	Similar to 'In Preamble Too Short' but for outgoing frames.	
<p>Note: Click the Refresh button for the latest results; Clear the counter values by clicking ; 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

10.5 Health Monitor

The Health Monitor is a performance tool that monitors the CPU, the memory and the disk (disk = flash and SD card) status of the CSM(s) in node. A detailed monitoring set-up description is similar to the description in §10.2.1.

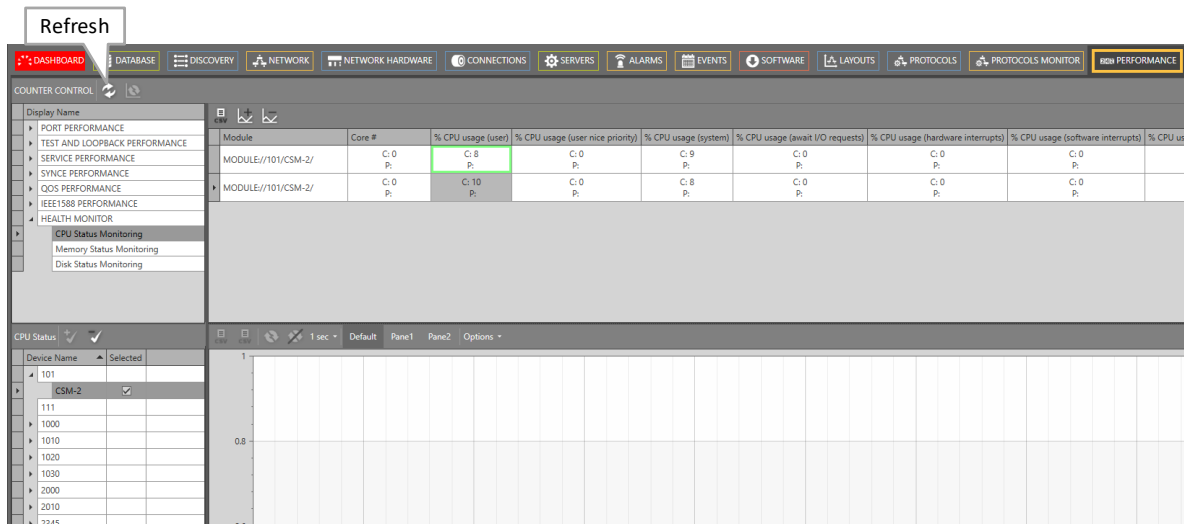


Figure 39 Health Monitor

Table 6 CPU Status Monitoring

Field (*)	Description
Module	Monitored Module
Core#	Indicates the core number on the monitored module
%CPU Usage (user)	the percentage * 100 of CPU utilization that occurred while executing at the user level (application).
%CPU Usage (user nice priority)	the percentage * 100 of CPU utilization that occurred while executing at the user level with nice priority. The 'nice' CPU percentage is the % of CPU time occupied by user level processes that are nice to have, so background process that are not critical. A nice to have process has a positive nice value (lower scheduling priority). It is the CPU time that's currently 'in use', but if a normal (nice value 0) or high-priority (negative nice value) process comes along, those 'nice to have' programs (positive nice value) will only be scheduled when the CPU has some free time.
%CPU Usage (system)	the percentage * 100 of CPU utilization that occurred while executing at the system level (kernel).
%CPU Usage (await I/O requests)	the percentage * 100 of time that the CPU or CPUs were idle during which the system had an outstanding disk I/O request.
%CPU Usage (hardware interrupts)	the percentage * 100 of time spent by the CPU or CPUs to service hardware interrupts.
%CPU Usage (software interrupts)	the percentage * 100 of time spent by the CPU or CPUs to service software interrupts.
%CPU Usage (stolen by other virtual processors)	the percentage * 100 of time spent in involuntary wait by the virtual CPU or CPUs while the hypervisor was servicing another virtual processor.
%CPU Usage (virtual processors)	the percentage * 100 of time spent by the CPU or CPUs to run a virtual processor.


Field (*)	Description
%CPU Usage (idle)	the percentage * 100 of time that the CPU or CPUs were idle and the system did not have an outstanding disk I/O request.
Note: Click the Refresh button for the latest results; Clear the counter values by clicking  ; 'C' value in cell = current value; 'P' value in cell = previous value;	

Table 7 Memory Status Monitoring



Field (*)	Description
Module	Monitored Module
Total Memory (KB)	Total memory present on the board in Kilobytes
Free Memory (KB)	Number of free memory in Kilobytes
Note: Click the Refresh button for the latest results; Clear the counter values by clicking  ; 'C' value in cell = current value; 'P' value in cell = previous value;	

Table 8 Disk Status Monitoring

Field (*)	Description
Module	Monitored Module
Disk Name	There are two disks on the CSM, either the flash or the SD memory card. The name indicates which disk values are shown.
Disk Size (KB)	Indicates the total disk size in kilobytes
Disk Size Used (KB)	Indicates the used disk size in kilobytes
Disk Size Available (KB)	Indicates the available disk size in kilobytes
Disk Size Percentage Filled	Indicates the used percentage of the disk
Note: Click the Refresh button for the latest results; Clear the counter values by clicking  ; 'C' value in cell = current value; 'P' value in cell = previous value;	

11. TROUBLESHOOTING

11.1 Health Monitor

If you have problems with a specific node, a service in a node, responsiveness of a node, possible traffic loss in a node, it is always a good idea to verify the Health Monitor (see §10.5).

This monitor shows more info on the CSM(s) usage in a node:

- ▶ CPU usage
- ▶ Memory usage
- ▶ Disk (=Flash, SD memory card) usage

11.2 Port Mirroring

11.2.1 General

Port Mirroring is a network debugging or monitoring feature. It is used in the Dragon PTN node to send a copy of network packets seen on a source port (=mirrored port) to a destination port (=mirroring port). This feature can be used for network appliances that require monitoring of network traffic, such as an intrusion-detection system etc...

NOTE: Port Mirroring is supported on IFMs as described in §12.

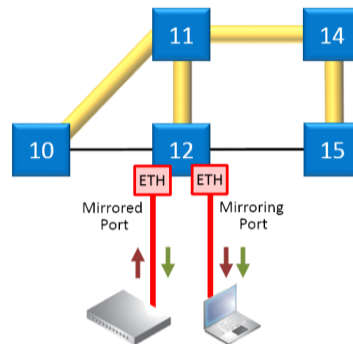



Figure 40 Port Mirroring

11.2.2 Configuration

CAUTION:

- Port Mirroring will be configured directly in the live network, it cannot be configured in the HiProvision database. As a result, HiProvision must be online for configuration!
- Port Mirroring changes will NOT be persistent in the network after adding/deleting them. Changes will be lost after reboot/clear node unless they were made persistent later on via the Load Manager (see Ref. [2Mgt] in Table 1).
- Port Mirroring can be done from multiple source ports to one destination port, not to multiple destination ports.

1. Make sure that your HiProvision is online. Port Mirroring can be configured via Dashboard → Network Hardware → ;

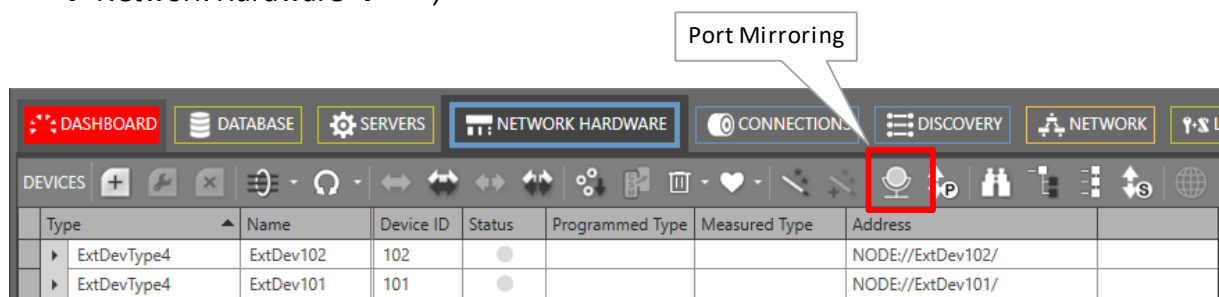


Figure 41 Port Mirroring Icon

2. The Information page opens. Click Next>>;
3. The Create Port Mirroring page opens:

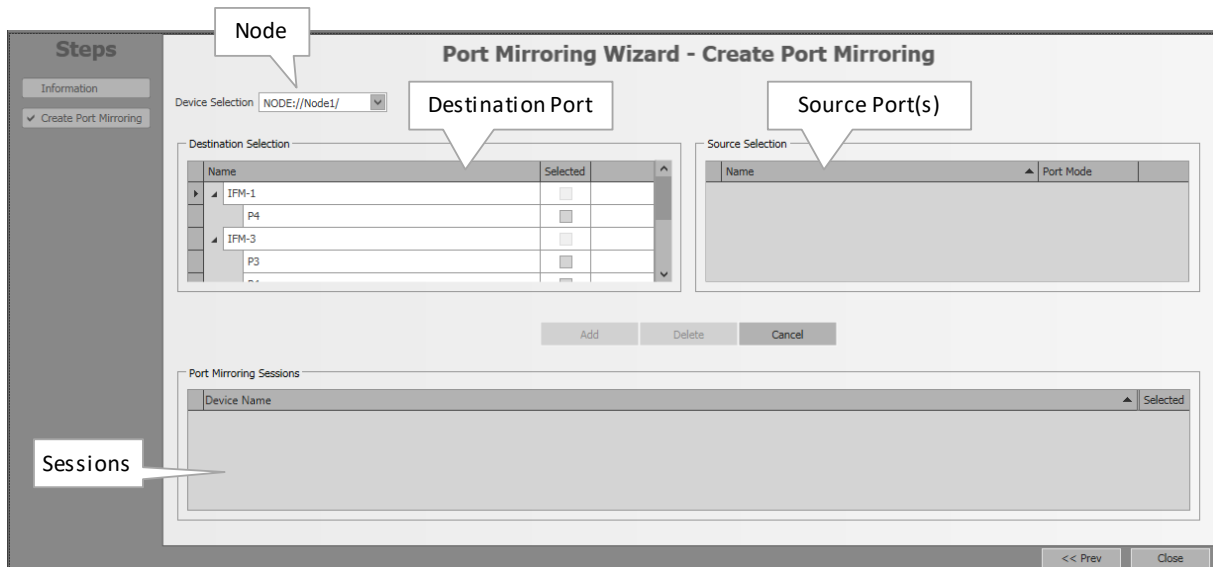


Figure 42 Port Mirroring Wizard

4. Follow the paragraphs below for further configuration.

a. Add Port Mirroring

1. Port Mirroring will be configured per node. Select a node from the Device Selection list on which you want to add Port Mirroring. This list shows only the nodes that have one or more supported Ethernet IFMs onboard. By default, the first node in the list is preselected.
2. The Destination Selection shows the available destination ports on the selected node. Select a desired destination port from the list by clicking its Selected checkbox.

NOTE: Active WAN ports, ports in a service or source ports will not be shown in this destination selection list.

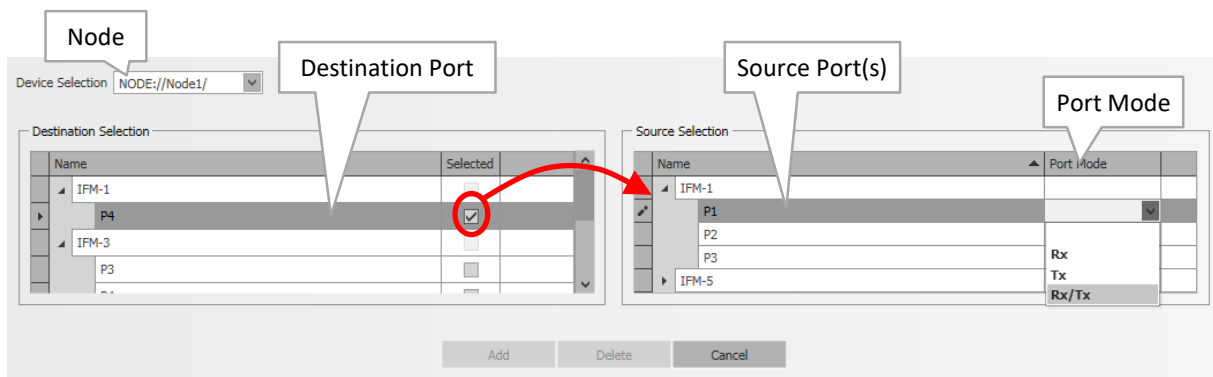


Figure 43 Destination/Source Ports

3. The Source Selection shows possible source ports in the same node for the selected destination port. Assign a source port to the destination port by selecting a value in its Port Mode (Rx, Tx, or Rx/Tx: Rx = Receive traffic, Tx= Transmit traffic, Rx/Tx = all traffic). Multiple source ports can be assigned to one destination port.

4. The Add button becomes active. Click the Add button to configure port mirroring in the live network. CAUTION: this click configures the node in the live network immediately without load manager or confirmation.
5. The Port Mirroring Sessions show the configured sessions on this node in the live network so far. The added source ports will not be available anymore in the destination ports list.

Device Name	Destination Port	Source Port(s)	Selected
PORT://Node1/IFM-1/P4/		PORT://Node1/IFM-1/P1/ (Rx) PORT://Node1/IFM-1/P2/ (Tx)	
PORT://Node1/IFM-3/P3/			
PORT://Node1/IFM-3/P1/			Rx/Tx

Figure 44 Port Mirroring Sessions

6. If desired, multiple mirroring sessions can be added in the same or different nodes by repeating previous steps in this paragraph.
7. Port Mirroring is up and running in the live network for the configured sessions.

b. Modify Port Mirroring

► Modify Port Mode of a Source Port in a Mirroring Session:

1. Select a node from the Device Selection list on which you want to modify Port Mirroring.
2. Select its destination port in the Destination Selection by clicking its Selected checkbox.
3. The assigned source ports show up with their Port Mode in the Source Selection.
4. Change the Port Mode of the desired source port.
5. Click the Add button to configure the modification in the live network.
6. The Port Mirroring Session shows the changed Port Mode.

► Add a Source Port to a Mirroring Session:

1. Select a node from the Device Selection list on which you want to modify Port Mirroring.
2. Select its destination port in the Destination Selection by clicking its Selected checkbox.
3. Source ports with an empty Port Mode are still available and can be added by just selecting a Port Mode for this port.
4. Click the Add button to configure the modification in the live network.
5. The source port will be added to the existing Port Mirroring Session and is removed from the Destination Selection.

► Remove a Source Port from a Mirroring Session:

1. Select a node from the Device Selection list on which you want to modify Port Mirroring.
2. Select the source port (row) that must be removed, in the Port Mirroring Sessions.
3. Click the Delete button to remove the port and to configure it in the live network.
4. The source port will be removed from the Port Mirroring Session and appears again in the Destination Selection.

► Change the Destination Port of a Mirroring Session:

Not supported. The entire Mirroring session with the wrong destination port must be deleted first (see §c). Next, a new mirroring session with the correct destination port must be added again (see §a).

c. Delete Port Mirroring

► Delete a Mirroring Session:

1. Select a node from the Device Selection list on which you want to delete a session.
2. Select the session by selecting the destination port (row) in the Port Mirroring Sessions.
3. Click the Delete button to remove the session and to configure it in the live network.
4. Both destination and source ports will be removed from the Port Mirroring Session and appear again in the Destination Selection.

► Disable Port Mirroring on the Entire Node:

Delete all mirroring sessions from the node by deleting each individual session, see §c . .

► Disable Port Mirroring in the Dragon PTN Network:


Delete all mirroring sessions from all nodes by deleting all sessions node per node, as described in §c.

11.3 Monitoring: Multiproperty View

11.3.1 General

The Multiproperty View allows to monitor/trace any status parameter of any network element in the Dragon PTN network. This tool is only for monitoring, not for configuration.

11.3.2 Get Monitored Results

1. Go to the Network Hardware Tile → Click the  (=properties) menu button;
2. The Multiproperty view is opened as a new window, see figure below;

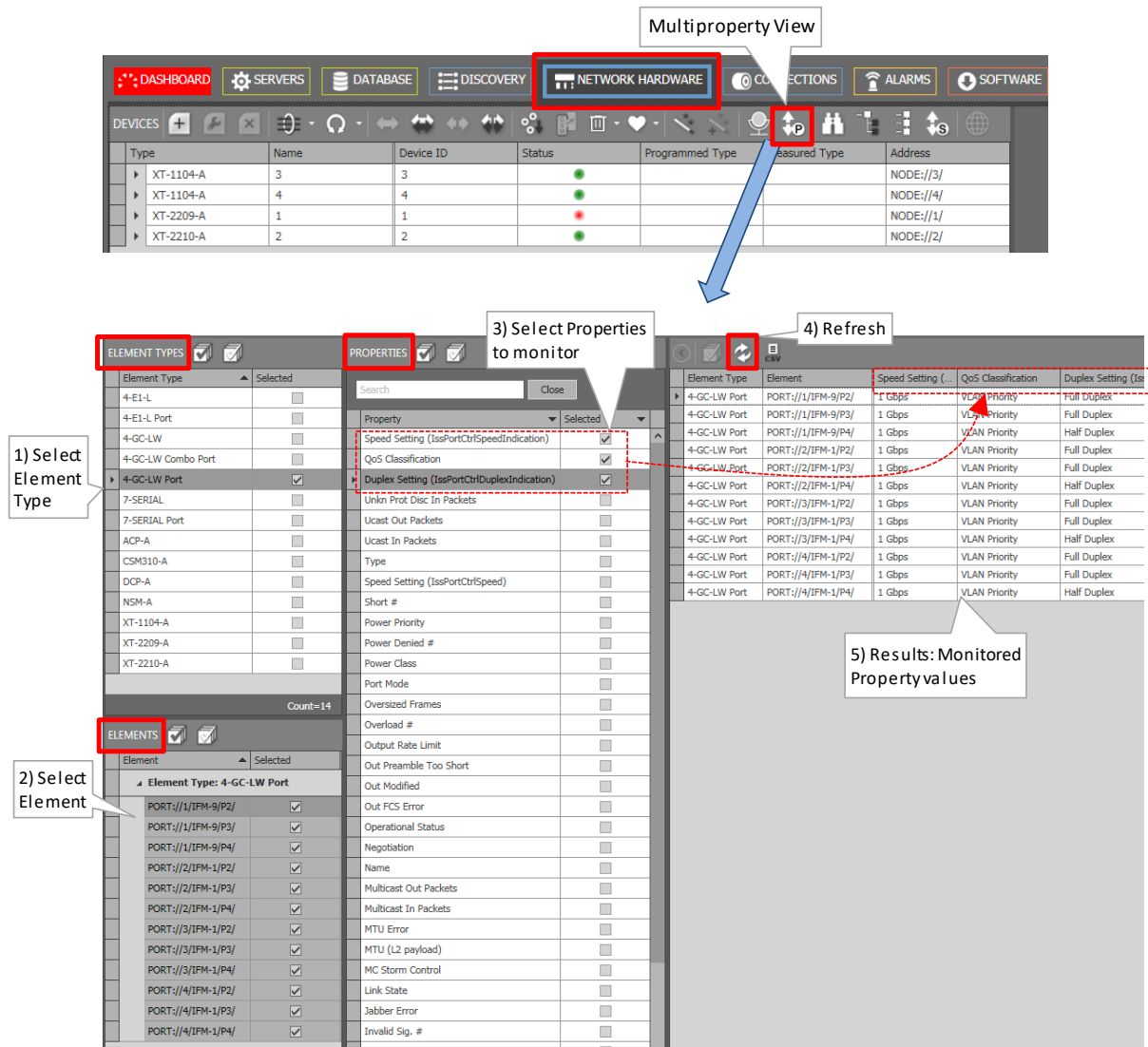


Figure 45 Multiproperty View

3. In this window, follow the steps below to monitor properties:

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.

1. Select one or more Element Types that you want to monitor. An element type is an object in your network that has monitorable properties. It could be a node, IFM, port etc... The ELEMENT TYPES section shows all the unique element types in your network.
2. Select one or more Elements that you want to monitor. The ELEMENTS section shows all your network elements that match the selected Element Types.
3. Select one or more Properties to monitor. Each selected property will create a new property column in the Results section on the right-hand side. The PROPERTIES section shows all the properties that are available on the selected Elements.
4. Click the Refresh button to fill out the monitored values of the selected properties.

- Results section shows all the monitored values.
- Right-clicking header cells of each section shows extra sort and search functions to filter your properties easier. See example below.

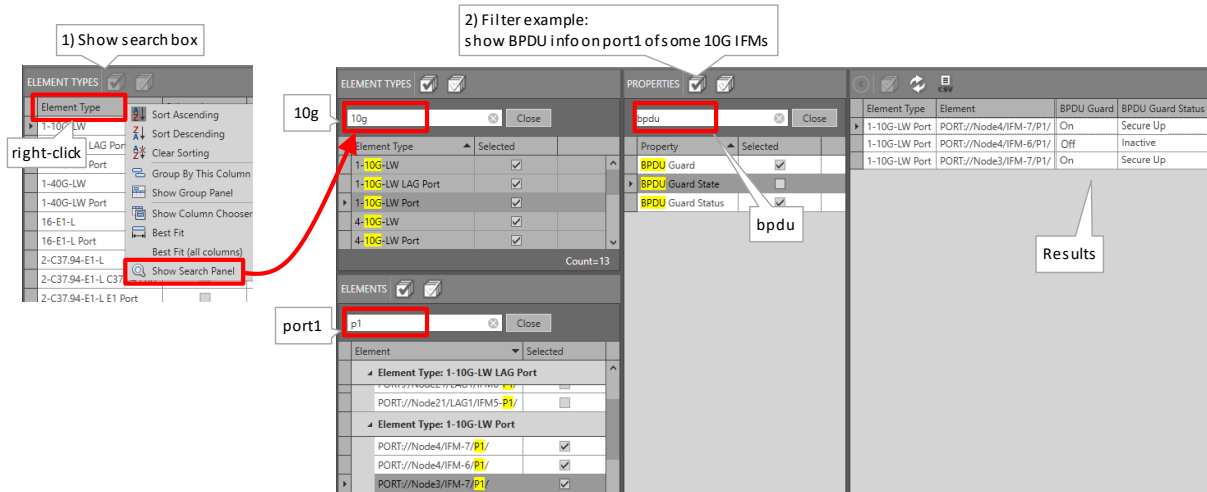


Figure 46 Multiproperty View: Filter Example

- In the results window below, click the button to optimize the results into a full screen view. Click the CSV icon to export the results into a csv file. Exported CSV files are by default saved in the <HiProvision installation path>\Logging\System Logging folder. Example CSV filename: Property Values-2020-01-22 10u50.48.csv.

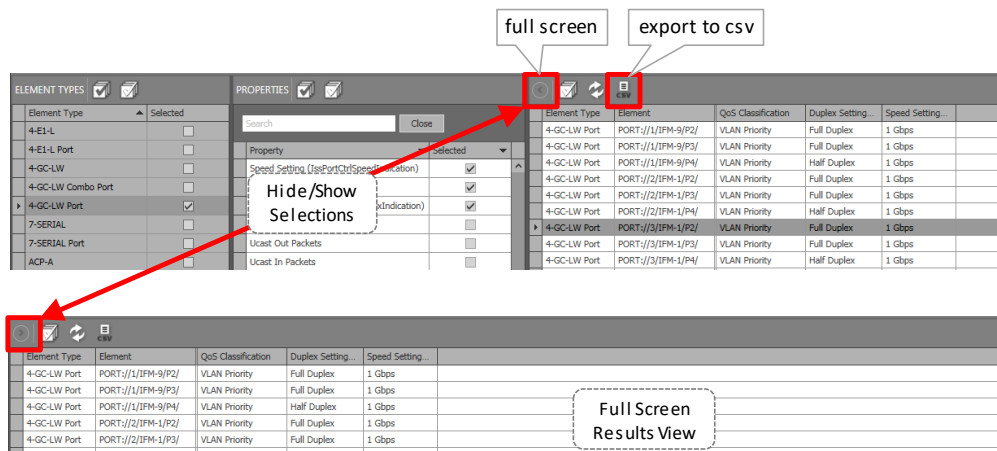


Figure 47 Multiproperty View: Full Screen Results View + Export

11.4 Devices Summary

11.4.1 General

The Devices Summary is an extra monitoring table in the Network Hardware tile that shows some extra handy statistics when monitoring and/or bringing your network. This table can be shown/hidden by clicking the menu button. Each network element with a switch ASIC onboard will be listed in this table: Nodes (with switch ASIC on CSM), L2 IFM, L3 IFM, external devices... This table mainly shows the connection and reachability status of all these elements.

- ▶ Total: the total amount of network elements of this Type found in your network;
- ▶ Offline, Measuring or Alarmstate unknown: the amount of network elements of this Type found in your network that are offline, measuring or have an unknown alarm state;
 - ▶ Offline: these network elements have not been connected yet by HiProvision;
 - ▶ Measuring: these network elements are in the connection phase with HiProvision. HiProvision is still busy measuring and trying to communicate with these elements;
 - ▶ Alarmstate Unknown: the network element might be reachable, but in some special cases, the alarmstate is unknown;
- ▶ Reachable: the amount of network elements that are connected via HiProvision and that could be reached via HiProvision. HiProvision can monitor and configure these elements;
- ▶ Unreachable: the amount of network elements that are connected via HiProvision but unfortunately could not be reached by HiProvision. HiProvision is not able to communicate with these elements. These elements are probably down, or disconnected from the Dragon PTN network.

The screenshot shows the 'NETWORK HARDWARE' section of a management interface. It features a table of devices with columns for Type, Name, Device ID, Status, Programmed Type, Measured Type, and Address. Below the table is a 'DEVICES SUMMARY' table with columns for Type, Total, Offline, Measuring or AlarmState unknown, Reachable, and Unreachable. A red arrow points from a 'Show/Hide Devices Summary' button to the summary table.

Type	Name	Device ID	Status	Programmed Type	Measured Type	Address
▶ XT-2215-A	4041	4041	●			NODE://4041/
▶ XT-2215-A	4215	4215	●			NODE://4215/
▶ XT-2210-A	180	180	●			NODE://180/
▶ XT-2215-A	102	102	●			NODE://102/
▶ XT-2215-A	4226	4226	●			NODE://4226/
▶ XT-2210-A	200	200	●			NODE://200/
▶ XT-2215-A	4510	4510	●			NODE://4510/
▶ XT-2210-A	160	160	●			NODE://160/
▶ XT-2210-A	111	111	●			NODE://111/
▶ XT-2215-A	1610	1610	●			NODE://1610/
▶ XT-2210-A	101	101	●			NODE://101/
▶ XT-2209-A	170	170	●			NODE://170/
▶ XT-2215-A	4001	4001	●			NODE://4001/
▶ XT-2215-A	2510	2510	●			NODE://2510/
▶ XT-2215-A	4002	4002	●			NODE://4002/

Type	Total	Offline, Measuring or AlarmState unknown	Reachable	Unreachable
XT-2215-A	9	3	5	1
XT-2210-A	5	1	4	0
XT-2209-A	1	0	1	0
6-GE-L	1	0	1	0
9-L3A-L	2	0	2	0

Figure 48 Devices Summary

12. PROTOCOL AND FEATURE SUPPORT MATRIX

Table 9 Protocol and Feature Support Matrix

Protocol, Feature	Ref.	IFMs					
		8-FXS	4-2/4WEM, 4-CODIR, 7-SERIAL, 2-OLS, 4-DSL-LW	4-E1-L/4-T1-L, 16-E1-L/16-T1-L, 2-C37.94	Ethernet IFMs: 4-GC-LW, 4-GCB-LW, 4-GO-LW, 1-10G-LW, 4-10G-LW, 1-40G-LW	Layer2 IFMs: 6-GE-L	Layer3 IFMs: 9-L3A-L 9-L3EA-L
Backbone MPLS-TP Network							
WAN Ports	§2	---	---	---	Yes	---	---
MACsec (Only in Aggregation Node)	Ref.[2Mgt]	---	---	---	Yes on 1-10G-LW WAN ports	---	---
Synchronisation							
SyncE	§7	---	Yes on 2-OLS E1 ports	Yes	Yes	---	---
PTP IEEE 1588v2 (Only in Aggregation Node)	§8	---	---	---	Yes: as Transparent Clock, not as Grandmaster, Boundary clock nor Ordinary Clock (not for 4-10G-LW, 1-40G-LW)	---	---
Hardware							
LAG + LACP (Only LAN ports)	Ref.[2Eth]	---	---	---	In Aggregation Nodes: LAG: Yes / LACP: No In Core Nodes: LAG: No / LACP: No	Yes	Yes
PoE	Ref.[2Eth]	---	---	---	Yes, on 4-GC-LW	---	---
Smart SFP	Ref.[2Leg]	---	---	---	Yes on 4-GO-LW ports or 4-GC-LW/4-GCB-LW front port 1 (not for 4-10G-LW, 1-40G-LW)	---	---

Protocol, Feature	Ref.	IFMs					
		8-FXS	4-2/4WEM, 4-CODIR, 7-SERIAL, 2-OLS, 4-DSL-LW	4-E1-L/4-T1-L, 16-E1-L/16-T1-L, 2-C37.94	Ethernet IFMs: 4-GC-LW, 4-GCB-LW, 4-GO-LW, 1-10G-LW, 4-10G-LW, 1-40G-LW	Layer2 IFMs: 6-GE-L	Layer3 IFMs: 9-L3A-L 9-L3EA-L
Services							
Ethernet	Ref.[2Eth]	Yes	Yes on 4-DSL-LW	---	Yes	Yes	Yes
Ethernet: Local Service	Ref.[2Eth]	---	---	---	---	Yes	Yes
Circuit Emulation	Ref.[2Leg]	---	Yes (except for 4-DSL-LW)	Yes	---	---	---
Serial Ethernet	Ref.[2Leg]	---	Yes on 7-SERIAL	---	---	---	---
Voice	Ref.[2Leg]	Yes (analog Voice)	---	---	Yes (VoIP)	Yes (VoIP)	Yes (VoIP)
Local Mode	Ref.[2Leg]	---	Yes on 2-OLS	Yes on 2-C37.94	---	---	---
Protocol Interaction (Layer2 Access Ring Protection Protocols)							
MRP	Ref.[2Eth]	---	---	---	Only MAC flush on topology change, immediate switchover. Port based and VLAN based services.	Only MAC flush on topology change, immediate switchover. Port based and VLAN based services.	Only MAC flush on topology change, immediate switchover. Port based and VLAN based services.
Layer2							
LLDP	---	---	---	---	Yes	Yes	Yes
IGMP Snooping	Ref.[2Eth]	---	---	---	---	Yes, MAC based	Yes, IP based
MSTP	Ref.[2Eth]	---	---	---	MAC flush on topology change, immediate switchover. Port based service: Network wide	Yes Port based service: Network wide VLAN based service: Local in Node	Yes Port based service: Network wide VLAN based service: Local in Node

Protocol, Feature	Ref.	IFMs					
		8-FXS	4-2/4WEM, 4-CODIR, 7-SERIAL, 2-OLS, 4-DSL-LW	4-E1-L/4-T1-L, 16-E1-L/16-T1-L, 2-C37.94	Ethernet IFMs: 4-GC-LW, 4-GCB-LW, 4-GO-LW, 1-10G-LW, 4-10G-LW, 1-40G-LW	Layer2 IFMs: 6-GE-L	Layer3 IFMs: 9-L3A-L 9-L3EA-L
Layer3							
Virtual Router	Ref.[2Eth]	---	---	---	---	---	Yes
Static Routing	Ref.[2Eth]	---	---	---	---	---	Yes
VRRP	Ref.[2Eth]	---	---	---	---	---	Yes
OSPF	Ref.[2Eth]	---	---	---	---	---	Yes
L3VPN	Ref.[2Eth]	---	---	---	---	---	Yes
PIM	Ref.[2Eth]	---	---	---	---	---	Yes
IGMP	Ref.[2Eth]	---	---	---	---	---	Yes
DHCP Relay	Ref.[2Eth]	---	---	---	---	---	Yes
Traffic Control / Security							
Ethernet: E-Tree	Ref.[2Eth]	---	---	---	Yes	Yes, only back end ports	Yes, only back end ports
Storm Control	Ref.[2Eth]	---	---	---	Yes, Port Properties	Yes, Port Properties	Yes, Port Properties
BPDU Guard	Ref.[2Eth]	---	---	---	Yes, Port Properties	Yes, included in Layer2 MSTP Wizard	Yes, included in Layer2 MSTP Wizard
IP ACL	Ref.[2Eth]	---	---	---	Yes (max. 1 rule)	Yes (max. 128 rules)	Yes (max. 128 rules)
MAC ACL	Ref.[2Eth]	---	---	---	Yes (max. 1 rule)	Yes (max. 128 rules)	Yes (max. 128 rules)
Sticky MAC	Ref.[2Eth]	Yes	---	---	Yes	Yes (Back End Ports)	Yes (Back End Ports)
MAC Limit (Only in Aggregation Node)	Ref.[2Eth]	Yes	---	---	Yes (not for 4-10G-LW, 1-40G-LW)	Yes	Yes
Static MAC Table	Ref.[2Eth]	Yes	---	---	Yes	Yes (Back End Ports)	Yes (Back End Ports)

Protocol, Feature	Ref.	IFMs					
		8-FXS	4-2/4WEM, 4-CODIR, 7-SERIAL, 2-OLS, 4-DSL-LW	4-E1-L/4-T1-L, 16-E1-L/16-T1-L, 2-C37.94	Ethernet IFMs: 4-GC-LW, 4-GCB-LW, 4-GO-LW, 1-10G-LW, 4-10G-LW, 1-40G-LW	Layer2 IFMs: 6-GE-L	Layer3 IFMs: 9-L3A-L 9-L3EA-L
Test & Debugging							
Test & Loopback	Ref.[2Leg]	---	Yes	Yes	---	---	---
Loss Measurement (LM) (Only in Aggregation Node)	§9.2	Yes	Yes	Yes	Yes (not for 4-10G-LW, 1-40G-LW)	---	---
Delay Measurement (DM) (Only in Aggregation Node)	§9.3	Yes	Yes	Yes	Yes (not for 4-10G-LW, 1-40G-LW)	---	---
Tunnel Ping	§9.4	Yes	Yes	Yes	Yes	---	---
Tunnel Traceroute	§9.5	Yes	Yes	Yes	Yes	---	---
Port Mirroring	§11.2	Yes, intra node: - can only be a source, can be mirrored to Ethernet IFMs	Yes, intra node: - can only be a source, can be mirrored to Ethernet IFMs	Yes, intra node: - can only be a source, can be mirrored to Ethernet IFMs	Yes, intra node: - source can be any IFM except L3 IFM - destination: Ethernet IFMs	Yes, same IFM: source and destination must be same L2 IFM	Yes: source and destination can be a mix of main and extension L3 IFM
MAC Monitor	Ref.[2Eth] Ref.[2Leg]	Yes (Node level)	Yes on 7-SERIAL (Node level)	---	Yes	Yes	Yes

13. ABBREVIATIONS

ACL	Access Control List
ASIC	Application-Specific Integrated Circuit
BC	Broadcast
BFD	Bi-directional Forwarding Detection
BIG	Backbone Isolation Guard
BPDU	Bridge Protocol Data Unit
CAS	Central Alarm System
CES	Circuit Emulation Service
CPU	Central Processing Unit
CSM	Central Switching Module
CSV	Comma Separated Values
DCN	Data Communication Network
DHCP	Dynamic Host Control Protocol
DM	Delay Measurement
DR	Designated Router
DUS	Don't Use for Sync
EEC	Ethernet Equipment Clock
FCS	Frame Check Sequence
HQoS	Hierarchical Quality of Service
IFM	InterFace Module
IP	Internet Protocol
L2	Layer2
L3VPN	Layer3 Virtual Private Network
LAG	Link Aggregation Group
LAN	Local Area Network
LER	Label Edge Router
LLDP	Link Layer Discovery Protocol (IEEE)
LM	Loss Measurement
LNM	Large Network Monitor
LPS	Linear Protection Switching
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
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
PRC	Primary Reference Clock
PRS	Primary Reference Source
PSU	Power Supply Unit
PTN	Packet Transport Network
PTP	Precision Time Protocol
QL	Quality Level
QoS	Quality of Service
QSFP	Quad SFP
RADIUS	Remote Authentication Dial In User Service
RES	Reserved
RGERP	Redundant Gigabit Ethernet Ring Protocol
RID	Router ID
RPL	Ring Protection Link
SAToP	Structured Agnostic TDM over Packet
SD	Secure Digital
SDH	Synchronous Digital Hierarchy
SEC	SDH Equipment Clock
SFP	Small Form Factor Pluggable
SONET	Synchronous Optical Network
SSM	Synchronization Status Message
SSUL	Synchronization Supply Unit Local
SSUT	Synchronization Supply Unit Transit
STU	Stratum Traceability Unknown

ST2	Stratum 2
ST3	Stratum 3
TC	Traffic Class
TRM	Transmit Receive Module
TTL	Time to Live
HiProvision	Dragon PTN Management System
UDP	Universal Data Protocol
UM	User Management
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WTR	Wait to Restore
XFP	10 Gigabit Small Form Factor Pluggable