



HIRSCHMANN

A **BELDEN** BRAND

User Manual

Basic Configuration

Dragon PTN and HiProvision 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.

© 2019 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.doc.hirschmann.com).

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

Contents

1.	INTRODUCTION	19
1.1	General	19
1.2	Supported Hardware, Firmware, Software	19
1.3	Manual References	20
2.	STEPS FOR A BASIC SETUP	22
2.1	Prepare the Dragon PTN Hardware	22
2.2	Prepare the HiProvision PC	23
2.3	Physically Interconnect all Nodes into a WAN Network.....	26
2.4	Physically Interconnect HiProvision PC and Dragon PTN Network	27
2.5	Start Up and Initialize HiProvision	27
2.6	HiProvision: Discover and Approve the Dragon PTN Network Topology (DCN).....	34
2.7	HiProvision: Network Database Configuration	50
2.8	HiProvision: Check Network Hardware	56
2.9	HiProvision: Load Configuration into the Network	59
2.10	HiProvision: Set the Network Timing via an NTP Server	59
2.11	HiProvision: Set the LAN Ports in Your Network.....	62
2.12	HiProvision: Create MPLS-TP Tunnel(s).....	63
2.13	HiProvision: Service(s) between Customer Applications.....	71
3.	QUALITY OF SERVICE (=QOS)	90
3.1	General	90
3.2	Step1: QoS Parameters in Service Wizard	90
3.3	Step2: QoS Parameters in Detail in Service Wizard.....	94
3.4	Bandwidth/Burst Size: Service Based	95
3.5	Bandwidth/Burst Size: Endpoint Based.....	96
3.6	Values on the Network Drawing.....	96
3.7	Bandwidth Optimization, Bandwidth Efficiency (=BWE) (LAN → WAN).....	97
3.8	(Service) Bandwidth Already Configured on WAN Links	99
3.9	DCN Channel	103
3.10	Link Capacity	104
3.11	Storm Control on Ethernet LAN Port.....	104
4.	ALARM HANDLING	106
4.1	General	106
4.2	Hardware: Measured/Programmed/Configured Values	106
4.3	Alarm Sensitive Properties in HiProvision	107
4.4	Alarm Colors and Severity	107
4.5	Alarms Tile and Window	108
4.6	Alarms in (Monitoring) Network Tile	110
4.7	Alarms in (Configuration) Network Hardware Tile.....	114
4.8	Configure Alarms for NSM Digital Input Contacts.....	115

4.9	Device Alarms via Digital Output Contacts on the NSM	116
4.10	Alarms in Large Network Monitor (LNM)	117
5.	CONFIGURATION LOAD MANAGER.....	118
5.1	General	118
5.2	Persist Configuration?.....	118
5.3	Get Load Scenarios	119
5.4	Configuration Loading and Status.....	119
6.	DATABASES HANDLING AND BACKUPS	120
6.1	General	120
6.2	MySQL Server Database Settings.....	121
6.3	Activate a Database in HiProvision	123
6.4	Make a Backup	123
6.5	Restore a Backup	124
6.6	Migrate a Database	124
6.7	Export Database (*.bak, *.xml) to a Mail, USB,	125
6.8	Import Database (*.bak, *.xml) from a Mail, USB,	125
7.	PROTOCOLS	126
7.1	General	126
7.2	Protocol Interaction: MRP (=Media Redundancy Protocol).....	127
7.3	Layer 2: MSTP (=Multiple Spanning Tree Protocol).....	133
7.4	Layer 2: IGMP Snooping	139
7.5	Layer 3: Virtual Router, VRF	142
7.6	Layer 3 View: Virtual Router Connections Overview	145
7.7	Layer 3: Static Routing	146
7.8	Layer 3: VRRP (=Virtual Router Redundancy Protocol)	148
7.9	Layer 3: OSPF (=Open Shortest Path First)	153
7.10	Layer 3: PIM	159
7.11	Layer 3: IGMP	163
7.12	Layer 3: DHCP Relay.....	165
7.13	Security: IP ACL (= IP Access Control List)	168
7.14	Security: MAC ACL (= MAC Access Control List)	171
7.15	Other: Voice Protocol	173
8.	HIPROVISION REDUNDANCY	179
8.1	General	179
8.2	Set up HiProvision Redundancy	180
8.3	Stable State: Switchover from Started to Standby HiProvision PC.....	185
8.4	Unstable State: Error Situations	185
8.5	Revertive/Non-revertive Behavior	186
8.6	HiProvision Redundancy with Remote Client	186
9.	HIPROVISION CONNECTIVITY REDUNDANCY: USE CASES.....	187
9.1	General	187
9.2	Use Case 0: No Redundancy at All	187

9.3	Use Case 1: CSM Redundancy Only.....	188
9.4	Use Case 2: One HiProvision PC with Direct Dual Entry Point in One Node ..	189
9.5	Use Case 3: One HiProvision PC with Direct Dual Entry Point in Two Nodes ..	190
9.6	Use Case 4: One HiProvision PC with Dual Entry Point via Switch	191
9.7	Use Case 5: Redundant HiProvision PCs with Single Entry Point	192
9.8	Use Case 6: Redundant HiProvision PCs with Dual Entry Point via Switch ..	193
9.9	Use Case 7: Redundant HiProvision PCs with Direct Dual Entry Point.....	194
9.10	Use Case 8: One HiProvision PC with Dual Entry Point via Router	195
9.11	(Future) Use Case 9: Redundant HiProvision PCs with Dual Entry Point via Router	196
10.	EXTRAS.....	197
10.1	Connect HiProvision PC to another Node.....	197
10.2	Clear Node or Network	197
10.3	Reset Node or Network	198
10.4	Save User HiProvision Settings	199
10.5	2-OLS Settings	199
10.6	Tunnel Actions: Swap Working Path \leftrightarrow Protection Path.....	201
10.7	Hardware Edition of Dragon PTN Modules.....	204
10.8	Improve Performance Between HiProvision Server and External Devices: ARP Reduction.....	204
11.	CSM REDUNDANCY	205
12.	LOAD SOFTWARE/FIRMWARE INTO THE NETWORK	206
12.1	General	206
12.2	Firmware Upgrade/Commit/Accept and Other	208
12.3	Step 1: Upgrade	209
12.4	Step 2: Commit.....	210
12.5	Step 3: Accept.....	211
12.6	Step 4: Reload Network Configuration.....	212
12.7	Validation Rules.....	212
12.8	Revert to Backup	213
12.9	Reporting	214
13.	SYNCE.....	214
13.1	General	214
13.2	Configuration	216
13.3	Normal Clock Selection Process.....	218
13.4	Operation.....	219
14.	PTP IEEE 1588V2 TRANSPARENT CLOCK	219
14.1	General	219
14.2	IEEE 1588v2 within Dragon PTN.....	221
14.3	Configuration	223
14.4	Operation.....	224

15.	PERFORMANCE COUNTERS AND MONITORING.....	225
15.1	General	225
15.2	Port Performance	225
15.3	Test & Loopback Performance.....	230
15.4	Service Performance.....	236
15.5	SyncE Performance	239
15.6	QoS Performance.....	241
15.7	IEEE 1588 Performance	244
15.8	Health Monitor.....	246
16.	LOSS/DELAY/ASSURANCE MONITORING.....	248
16.1	General	248
16.2	Loss Measurement (=LM).....	248
16.3	Delay Measurement (=DM).....	251
16.4	Tunnel Ping	252
16.5	Tunnel Traceroute	254
17.	REMOTE CLIENT/SERVER.....	256
17.1	General	256
17.2	Example Use Cases	256
17.3	Configuration	258
17.4	Switchover GUI View from Redundant HiProvision Servers	260
17.5	Start Remote Client/Server System	261
18.	TEST & LOOPBACK CONFIGURATION	262
18.1	General	262
18.2	Loopbacks	263
18.3	BERT (=Bit Error Ratio Tester).....	264
18.4	Tone Generator/Level Meter	266
18.5	Combined BERT / Loopback Example.....	267
19.	HELP.....	268
20.	SERIAL KEY / VOUCHERS / LICENSE PACK	268
20.1	Serial Key	268
20.2	Voucher(s).....	268
20.3	License Pack	269
20.4	Generate License Pack and Install in HiProvision.....	270
20.5	Monitor Licenses in HiProvision	270
20.6	Licenses Operation	271
21.	POWER OVER ETHERNET (POE).....	272
21.1	General	272
21.2	Connect PoE Hardware	273
21.3	Configure PoE.....	273
21.4	PoE Configuration Rules.....	274
21.5	PoE Status	275

22.	SUBBRINGS.....	276
22.1	General	276
22.2	Ladder Topology Examples.....	277
22.3	Protected Tunnels.....	278
23.	SMART SFP	278
23.1	General	278
23.2	Configuration	279
23.3	Alarms.....	280
24.	TRAFFIC CONTROL / RESOURCE ALLOCATION	280
24.1	Security	280
25.	E-TREE	286
25.1	General	286
25.2	Configuration	287
26.	LAYOUTING HIPROVISION	287
26.1	Layouting Tables.....	287
26.2	Layouting Network Drawings	291
27.	LARGE NETWORK MONITOR (=LNM)	300
27.1	Prerequisite.....	300
27.2	General	300
27.3	Selecting Grid Layouts.....	301
27.4	Assign Layouts to Grid Sections	302
27.5	Multiple LNM Sessions.....	302
27.6	Large Network Monitor Live.....	303
28.	MULTIPLE LANGUAGE SUPPORT	303
29.	ADD-ONS.....	304
29.1	General	304
29.2	CAR IP	304
29.3	SNMP Northbound	304
29.4	Generic Reporting Engine.....	305
30.	PORT MIRRORING.....	306
30.1	General	306
30.2	Configuration	307
31.	ETHERNET SERVICES ON L2/L3 INTERFACE MODULES	310
31.1	General	310
31.2	Service Types on L2/L3 Interface Modules	310
31.3	VLAN Based Local Service.....	314

31.4	VRF Ports (Only L3 Interface Module)	315
31.5	Back End Ports (BEn)	316
31.6	L2VPN	317
31.7	L3VPN	318
32.	PROTOCOL AND FEATURE SUPPORT MATRIX	323
33.	EXTERNAL DEVICE TYPES	327
33.1	General	327
33.2	Add New External Device Type	327
33.3	Create New External Device	330
33.4	Linking External Devices to Dragon PTN	331
33.5	Monitoring and Alarming of External Devices	332
33.6	Usage of External Devices in HiProvision	343
34.	BPDU GUARD ON ETHERNET LAN PORT	344
35.	LAG (=LINK AGGREGATION GROUP)	345
35.1	Prerequisites	345
35.2	General	345
35.3	Configuration	346
36.	LOOPBACK INTERFACE	349
36.1	Prerequisites	349
36.2	General	350
36.3	Configuration	350
37.	OPEN SOURCE COMPONENTS	351
38.	TROUBLESHOOTING	353
38.1	Database Tile: Authentication Failed	353
38.2	View Device Info	353
38.3	Download Log Files from Nodes to HiProvision PC	355
38.4	Rollback	356
38.5	Firewall Ports	356
38.6	Test and Loopback	356
38.7	Server Does not Start (Server Tile Remains 'Starting')	356
38.8	Ethernet Service Fails with Multiple Tunnels on Same Link	357
38.9	Lost Tree View Structure Due to Older HiProvision Version	357
38.10	Debugging the Network via Port Mirroring	358
38.11	Health Monitor	358
39.	ABBREVIATIONS	358

List of figures

Figure 1 Dragon PTN Network Example	19
Figure 2 NSM Side View: Node Number.....	22
Figure 3 CSM Front Panel	23
Figure 4 HiProvision IP Address.....	25
Figure 5 Second IP Address on NIC.....	25
Figure 6 Allow HiProvision Processes.....	27
Figure 7 Dashboard View with User Database Request.....	29
Figure 8 Select User Database Server	30
Figure 9 HiProvision Client - Dashboard.....	30
Figure 10 Network Configuration Database.....	32
Figure 11 Start HiProvision Servers	32
Figure 12 Dashboard: HiProvision Almost Ready for Management.....	33
Figure 13 [i] Window: Dragon PTN Release, HiProvision Version	33
Figure 14 Create Discovery Entry	37
Figure 15 Discovery PollState	38
Figure 16 Network Discovery in Progress: Connecting	38
Figure 17 HiProvision Connected to Multiple Dragon PTN Networks.....	40
Figure 18 Network Fully Discovered and Approved: Ready/Measured Devices and Links.....	41
Figure 19 Active/Redundant Discovery Entry Point	43
Figure 20 Routed DCN: Routed Management Network.....	44
Figure 21 Entry Point with Routed Checked, Gateway Field.....	44
Figure 22 Routed DCN: Static Routes in Routed Network	45
Figure 23 Advanced Tab: CSM Front IP Addresses.....	47
Figure 24 Change Device IP Range	49
Figure 25 Discovery Tab: Auto-Creation of Network Elements in Database	50
Figure 26 Manual Configuration Devices/Links.....	51
Figure 27 Drag and Drop Modules into Device Picture	52
Figure 28 Create Links	53
Figure 29 Insert Node	54
Figure 30 Drop Node	55
Figure 31 Network Hardware Tab: Created Network Elements	56
Figure 32 Connect/Disconnect Buttons	57
Figure 33 Connection Status After Connect	58
Figure 34 Configuration Alarms.....	58
Figure 35 Load Configuration Into the Network	59
Figure 36 Status Color Change After Successful Loading	59
Figure 37 Network Settings Wizard Button.....	60
Figure 38 NTP Server IP Address	61

Figure 39 CSM NTP Settings	62
Figure 40 LAN/WAN Settings.....	63
Figure 41 Tunnel Creation	63
Figure 42 Point-to-Point Tunnels	64
Figure 43 MultiPoint Tunnels	64
Figure 44 Logical Ring Tunnel.....	65
Figure 45 Subring Tunnel.....	65
Figure 46 Create Tunnels.....	66
Figure 47 Tunnel - Device Selection	66
Figure 48 Tunnel - Link Selection.....	67
Figure 49 Set Protection Mode of LSP.....	67
Figure 50 Tunnel HQos (Future Support)	68
Figure 51 Protection Parameters	68
Figure 52 Share LSP: Shared/Non-Shared LSPs	70
Figure 53 LSP Sharing Possible?	70
Figure 54 Service Creation in Tunnels	72
Figure 55 Service Via Combined Tunnels	73
Figure 56 Create Services	75
Figure 57 Open Network Settings Wizard.....	77
Figure 58 Service Ports Selection	78
Figure 59 MAC Limit / E-Tree: Root & Leaf Ports Selection	78
Figure 60 Master/Slave Setting for Serial Ethernet.....	79
Figure 61 Voice Service: Port Selection.....	79
Figure 62 Port Based: VLAN Tagging/Untagging	81
Figure 63 VLAN Based: VLAN Tagging/Untagging	81
Figure 64 Ports to Tunnel Match.....	82
Figure 65 Selected Highlighted Tunnel.....	82
Figure 66 Service: Optical Low Speed Serial.....	84
Figure 67 FM0 Coding.....	84
Figure 68 Created 'Optical Low Speed Serial' Service	85
Figure 69 Serial Ethernet: Advanced Mode - Bandwidth Optimization	88
Figure 70 Multidrop Consistency Monitoring	89
Figure 71 Multidrop Consistency Alarm.....	89
Figure 72 QoS Parameters in the Ethernet Service Wizard.....	90
Figure 73 QoS Parameters in the Voice Service Wizard.....	91
Figure 74 Bandwidth/Burst Size Parameters in Detail	94
Figure 75 Bandwidth/Burst Size: Service Based	95
Figure 76 Bandwidth/Burst Size: Endpoint Based.....	96
Figure 77 Bandwidth/Burst Size on WAN Side	96
Figure 78 Bandwidth/Burst Size on LAN Side.....	97
Figure 79 Bandwidth Efficiency	97

Figure 80 Bandwidth Efficiency Examples in HiProvision.....	98
Figure 81 Connection Tab: Bandwidth Information.....	100
Figure 82 Bandwidth Percentage Label and Status Colors.....	101
Figure 83 Link Details	102
Figure 84 Highest Value and Severest Color	102
Figure 85 Link: DCN Bandwidth Profile	103
Figure 86 Ethernet Link: Link Capacity	104
Figure 87 Port Properties: Storm Control.....	105
Figure 88 Measured / Programmed / Configured Values	106
Figure 89 Alarm Sensitive Properties: Little Square Box	107
Figure 90 Alarms Window	108
Figure 91 Alarms in Example Network: Services Tab	110
Figure 92 Show Navigation (N) of Selected Device/Link/Tunnel/Service	111
Figure 93 Show Detailed Properties (P) of Selected Tunnel or Service.....	111
Figure 94 Selected Network Elements: X / (x) in Displayed Column.....	114
Figure 95 Protected Tunnels: Protection Path, Blocked Port Indication: '/'	114
Figure 96 NSM Digital I/O Contacts.....	115
Figure 97 Operation Of Device Alarms/Digital Outputs.....	116
Figure 98 From CSM to Device Settings	116
Figure 99 Device Settings: Clear Edge Triggered Alarm	117
Figure 100 Configuration Load Manager.....	119
Figure 101 Database Tile	120
Figure 102 Backup Databases.....	121
Figure 103 Restore Databases.....	121
Figure 104 Connect to MySQL Server.....	122
Figure 105 MySQL Workbench: Root Password Change.....	122
Figure 106 Connect to MySQL Server with New Password.....	123
Figure 107 MRP: General Example.....	128
Figure 108 Involved Node: Flush VFI	129
Figure 109 MRP: Select Ports	130
Figure 110 MRP: VLAN Based Services: Select MRP + Data Service.....	131
Figure 111 MRP: Port Based Services: Select Service.....	131
Figure 112 Dashboard → (Monitoring) Network Tile → Protocols Tab	132
Figure 113 Dashboard → (Monitoring) Protocols Tile	133
Figure 114 Region/MSTP Overview.....	134
Figure 115 Region/MSTP Actions	134
Figure 116 Bridge ID = Bridge Priority & MAC Address.....	136
Figure 117 Created Regions/MSTP Instances.....	138
Figure 118 PIM/IGMP/IMGP Snooping Overview	140
Figure 119 IGMP Snooping Common Properties	140
Figure 120 Virtual Router Icon	142

Figure 121 Virtual Router Example	143
Figure 122 Virtual Router Wizard - Creation.....	144
Figure 123 Virtual Router Wizard - Configuration.....	144
Figure 124 Virtual Router - Properties	145
Figure 125 Layer 3 View: Virtual Router Connections Overview	146
Figure 126 Static Routing Wizard - Creation	147
Figure 127 VRRP General.....	148
Figure 128 VRRP Example.....	149
Figure 129 VRRP Prerequisites	150
Figure 130 VRRP Creation	151
Figure 131 VRRP Creation: Group Added.....	151
Figure 132 VRRP Creation: Delete Group.....	152
Figure 133 VRRP - Configuration	152
Figure 134 OSPF: General Example	154
Figure 135 OSPF: Virtual Router Parameters	156
Figure 136 OSPF: Summarize External Routes	157
Figure 137 OSPF: Summarize Inter-Area Routes.....	157
Figure 138 OSPF: Interface Parameters	158
Figure 139 PIM/IGMP/IMGP Snooping Overview	160
Figure 140 Rendez-Vous Point Configuration	162
Figure 141 PIM/IGMP/IMGP Snooping Overview	163
Figure 142 DHCP Overview	166
Figure 143 DHCP Relay: Creation	167
Figure 144 DHCP Relay: Configuration	167
Figure 145 IP ACL: Port Configuration Example for Ethernet Interface Modules	169
Figure 146 IP ACL: Switch Port Configuration Example for L2/L3 Interface Modules.....	170
Figure 147 MAC ACL: Port Configuration Example for Ethernet Interface Modules	172
Figure 148 MAC ACL: Switch Port Configuration Example for L2/L3 Interface Modules.....	173
Figure 149 Voice Service Elements Overview	174
Figure 150 Dial Plan - Translation Pattern.....	177
Figure 151 Basic HiProvision Redundancy: Via Ethernet Service/External LAN.....	180
Figure 152 Master PC Only, No Redundancy	181
Figure 153 Discovery Entry Point: Redundant Management IP Address	182
Figure 154 HiProvision Redundancy Setup: NotRunning	182
Figure 155 Fill Out IP Addresses.....	183
Figure 156 HiProvision Redundancy Starting	183
Figure 157 HiProvision Redundancy Setup: Running	183
Figure 158 Servers Tile: HiProvision Redundancy	185
Figure 159 Use Case 0: No Redundancy at All.....	187
Figure 160 Use Case 1: CSM Redundancy Only.....	188
Figure 161 Use Case 2: One HiProvision PC with Direct Dual Entry Point in One Node	189

Figure 162 Use Case 3: One HiProvision PC with Direct Dual Entry Point in Two Nodes.....	190
Figure 163 Use Case 4: One HiProvision PC with Dual Entry Point via Switch	191
Figure 164 Use Case 5: Redundant HiProvision PCs with Single Entry Point	192
Figure 165 Use Case 6: Redundant HiProvision PCs with Dual Entry Point via Switch	193
Figure 166 Use Case 7: Redundant HiProvision PCs with Direct Dual Entry Point.....	194
Figure 167 Use Case 8: One HiProvision PC with Dual Entry Point via Router.....	195
Figure 168 Use Case 9: Redundant HiProvision PCs / Dual Entry Point / Redundant Router ...	196
Figure 169 Save HiProvision Settings	199
Figure 170 PTN-2-OLS Interface Module: Clock Source Settings	200
Figure 171 PTN-2-OLS Interface Module: Forced Power Mode	200
Figure 172 Protected Tunnel/Actions	201
Figure 173 Point-to-Point/Multipoint Action on Tunnel Window	202
Figure 174 Ring/SubRing Action on Tunnel Window	203
Figure 175 Clear Command in the Node Action List	203
Figure 176 Hardware Edition of Dragon PTN Modules	204
Figure 177 Node with 2 CSMs, CSM Switchover Button	205
Figure 178 CSM Redundancy Status.....	206
Figure 179 Firmware Upgrade Example: Upgrade to v1.1.7	208
Figure 180 Software/Firmware Action Buttons	208
Figure 181 Step1: Upgrade Firmware	210
Figure 182 Commit Reboot Warning.....	211
Figure 183 Step 2: Commit Firmware.....	211
Figure 184 Step3: Accept Firmware	212
Figure 185 Firmware Validation Rules	213
Figure 186 (In)Compatible Firmware Versions and Alarming	213
Figure 187 Revert to Backup Version	214
Figure 188 Unidirectional/Bidirectional SyncE Examples.....	215
Figure 189 Bad SyncE Examples: Timing Loop	216
Figure 190 SyncE Member Ports	216
Figure 191 SyncE Clock Recovery Ports.....	218
Figure 192 IEEE 1588v2	220
Figure 193 1588 Protocol Messages	221
Figure 194 1588 on Port and Node Level for LERs and LSRs	222
Figure 195 1588 Enabled: Transparent Clock Correction.....	222
Figure 196 1588 Not Enabled: No Clock Correction.....	223
Figure 197 1588 Node Settings	223
Figure 198 1588 Port Settings	224
Figure 199 Performance Tab: Counter Control	225
Figure 200 Ethernet Port Monitoring.....	226
Figure 201 CODIR Port Monitoring.....	229
Figure 202 E1/T1 Monitoring	230

Figure 203 C37.94 Monitoring.....	231
Figure 204 Serial Monitoring.....	232
Figure 205 4W Voice Monitoring	233
Figure 206 CODIR Monitoring	234
Figure 207 Low Speed Serial Monitoring	235
Figure 208 Services: Circuit Emulation Monitoring.....	236
Figure 209 Services: Serial Ethernet Monitoring.....	238
Figure 210 SyncE Monitoring	239
Figure 211 QoS Policer Monitoring	242
Figure 212 QoS Queue Monitoring	243
Figure 213 IEEE 1588 Monitoring.....	245
Figure 214 Health Monitor	246
Figure 215 Assurance Wizard: Loss Measurement Configuration	249
Figure 216 Loss Measurement in Operation.....	250
Figure 217 Loss Measurement Result Values.....	251
Figure 218 Delay Measurement Result Values	252
Figure 219 Assurance Wizard: Ping Measurement Configuration	253
Figure 220 Tunnel Ping Result Values	254
Figure 221 Traceroute Results Overview	255
Figure 222 Client-Server Connection: DCN Channel	256
Figure 223 Client-Server Connection: DCN Channel with Redundant Discovery Entry Point ...	257
Figure 224 Client-Server Connection: LAN (Ethernet Service)	257
Figure 225 Client-Server Connection: LAN (External LAN)	257
Figure 226 Client-Redundant Server Connection: LAN (External LAN)	258
Figure 227 Remote Client Via DCN Channel.....	259
Figure 228 Remote Client Viewing Standby Server.....	261
Figure 229 Remote Client Viewing Started Server	261
Figure 230 Please wait until loading is done	262
Figure 231 Loopback Functionality	263
Figure 232 BERT Module	264
Figure 233 Combined BERT / Loopback	268
Figure 234 Vouchers/Licenses Overview1	271
Figure 235 Vouchers/Licenses Overview2	271
Figure 236 Connect: Not Enough Vouchers	272
Figure 237 PoE Info on Node/Module/Port Level	273
Figure 238 Logical Ring / Interconnection Nodes / Subring / Ladder Topology	276
Figure 239 Logical Ring / Subring Setup	276
Figure 240 Subring Colors	277
Figure 241 Ladder Topology Example 1	277
Figure 242 Ladder Topology Example 2	278
Figure 243 Ladder Topology: Not Allowed: Shared Link	278

Figure 244 Ladder Topology: Not Allowed: Only 2 Nodes in Subring	278
Figure 245 Example: Smart SFPs Setup / PTP	279
Figure 246 Example: Smart SFPs in HiProvision	280
Figure 247 Sticky MAC Configuration.....	282
Figure 248 MAC Limit Configuration	283
Figure 249 Static MAC Table: Service/Port Selection.....	284
Figure 250 Static MAC Table: Add/Remove/Import	285
Figure 251 Example: MAC Monitor/MAC Address Table	286
Figure 252 E-Tree: Root/Leaf	286
Figure 253 Example: Ethernet + E-Tree Communication	287
Figure 254 Layouting Tables.....	288
Figure 255 Invoke Column Actions.....	288
Figure 256 Table Layout: Column Order	288
Figure 257 Table Layout: Hiding Columns.....	289
Figure 258 Hidden Group Panel / Shown Group Panel	289
Figure 259 Example: Grouped By Link Type.....	290
Figure 260 Filtering Tables	291
Figure 261 Layouting Network Drawings	292
Figure 262 Create Layout	293
Figure 263 Create Bend.....	297
Figure 264 Delete Bend.....	297
Figure 265 Before Sub Layout Creation.....	298
Figure 266 CityLayout View after Creation, No Mapping Yet	299
Figure 267 Final Result after Mapping Nodes into Sub Layouts	300
Figure 268 Large Network Monitor	301
Figure 269 Layout Grid Button Example	301
Figure 270 Grid Section: Layout Selector	302
Figure 271 Multiple LNM Sessions	303
Figure 272 Large Network Monitor Live.....	303
Figure 273 CAR IP Example.....	304
Figure 274 SNMP Northbound Example	305
Figure 275 General: Reporting Engine	306
Figure 276 Port Mirroring.....	306
Figure 277 Port Mirroring Icon.....	307
Figure 278 Port Mirroring Wizard	307
Figure 279 Destination/Source Ports	308
Figure 280 Port Mirroring Sessions	308
Figure 281 Port Based Service including L2/L3 Interface Modules: Mixed VLAN Service.....	311
Figure 282 Example1: Port Based Ethernet Service, Mixed VLANs, Back End Ports	312
Figure 283 Example1: Service Wizard - Mixed VLANs: Map L2/L3 Interface Module Front Ports to VLANs.....	313

Figure 284 Example1: Mixed VLAN Service Created, Result in Services List.....	314
Figure 285 Local Service: Close an MSTP, VRRP Ring Outside the Dragon PTN Network.....	314
Figure 286 VRF Port and Front Ports on L3 Interface Module	316
Figure 287 Default Back End Port View.....	316
Figure 288 Customize Back End Port Selection	317
Figure 289 L2VPN General.....	318
Figure 290 L3VPN General.....	318
Figure 291 L3VPN Detailed Example	319
Figure 292 Interconnect IP Subnet1 and 2	320
Figure 293 Assign IP Addresses to IP Subnet1 and 2.....	321
Figure 294 Interconnect IP Subnet2 and 3.....	321
Figure 295 Assign IP Addresses to IP Subnet2 and 3.....	321
Figure 296 Configure OSP: Select Both Virtual Routers	322
Figure 297 External Devices Types	327
Figure 298 Create External Device Type	328
Figure 299 External Device Type: Base Type and Image	328
Figure 300 External Device Type: Add Port.....	329
Figure 301 External Device Type: Drag & Drop Ports Into Place.....	329
Figure 302 External Device: New Device Type in Device List	330
Figure 303 External Device: Connection Parameters.....	331
Figure 304 External Device: Created External Device	331
Figure 305 Dragon PTN Network + External Devices	332
Figure 306 Default and Custom Properties	333
Figure 307 XML File: General Structure	335
Figure 308 External Device Picture In XML File	336
Figure 309 XML: Device Properties/Property Definition.....	337
Figure 310 XML: Port Properties/Property Definition.....	338
Figure 311 XML: AlarmDefinition Block per Alarm	340
Figure 312 Alarm Definitions Example	340
Figure 313 XML: Trap Registrations	342
Figure 314 BPDU Guard on Ethernet LAN Port	344
Figure 315 Link Aggregation and LAGs.....	345
Figure 316 Link Aggregation Configuration.....	346
Figure 317 Create LAG.....	347
Figure 318 Link Aggregation Failed: Aggregation Impossible	348
Figure 319 Created LAG.....	348
Figure 320 Modify LAG	349
Figure 321 Loopback Interface.....	350
Figure 322 Created Loopback Interface	350
Figure 323 Virtual Router Wizard: Loopback Interface.....	351
Figure 324 Database Tile: Authentication Failed	353

Figure 325 View Device Info: General	354
Figure 326 View Device Info: Port Mapping.....	355
Figure 327 Download Log Files.....	355
Figure 328 FTP Server Does Not Start	356
Figure 329 Ethernet Service Fails with Multiple Tunnels on Same Link.....	357
Figure 330 Lost Tree View Structure Due to Older HiProvision Version	358

List of Tables

Table 1 Manual References	20
Table 2 Installation Shortcuts.....	24
Table 3 Differences HiProvision Client / HiProvision LNM Client.....	28
Table 4 Discovery Menu Buttons	34
Table 5 Discovery: Poll States.....	35
Table 6 Devices: Neighbor Communication	36
Table 7 Links: Discovery	36
Table 8 Unapproved/Approved States In Normal Situation	41
Table 9 Status Bullets: Devices.....	57
Table 10 Status Bullets: Links	57
Table 11 Tunnel Topologies and Protection.....	64
Table 12 VLAN Tagging/Untagging.....	80
Table 13 Optical Low Speed Serial Bitrates.....	85
Table 14 Service, Priority, Frame Size, Bandwidth Input	91
Table 15 Menu Buttons.....	112
Table 16 Alarm Indications.....	112
Table 17 Load Manager Menu Buttons.....	119
Table 18 Protocol Scalability Parameters.....	127
Table 19 Default Path Cost.....	136
Table 20 Parameter Dependency.....	138
Table 21 VRRP States.....	149
Table 22 IGMP Version Dependencies	164
Table 23 8-FXS Port Properties (Remote Extension)	175
Table 24 Translated Pattern Parameters	177
Table 25 8-FXS Port Properties (SIP-Server)	178
Table 26 HiProvision Redundancy Status Info.....	184
Table 27 Tunnel Action Commands.....	204
Table 28 Software/Firmware Buttons	208
Table 29 Upgrade Status Overview	212
Table 30 Provisioned QL Ordered According Quality.....	217
Table 31 Ethernet Port Monitoring Fields.....	227
Table 32 CODIR Port Monitoring Fields.....	229

Table 33 E1/T1 Monitoring Fields	230
Table 34 C37.94 Monitoring Fields.....	231
Table 35 Serial Monitoring Fields.....	232
Table 36 4W Voice Monitoring Fields	233
Table 37 CODIR Monitoring Fields	234
Table 38 Low Speed Serial Monitoring.....	235
Table 39 Services: Circuit Emulation Monitoring 'Module' Fields.....	236
Table 40 Services: Circuit Emulation Monitoring 'Bundle' Fields.....	237
Table 41 Services: Serial Ethernet Monitoring 'Module' Fields	238
Table 42 Services: Serial Ethernet Monitoring 'Port' Fields	239
Table 43 SyncE Monitoring 'System Information' Fields.....	240
Table 44 SyncE Monitoring 'Clock Information' Fields.....	240
Table 45 QoS Policer Monitoring Fields	242
Table 46 QoS Queue Monitoring Fields	243
Table 47 IEEE 1588 Monitoring Fields	245
Table 48 CPU Status Monitoring	246
Table 49 Memory Status Monitoring	247
Table 50 Disk Status Monitoring	247
Table 51 Test & Loopback Support	262
Table 52 Loopback Settings.....	264
Table 53 BERT Settings	265
Table 54 Tone Generator/Level Meter Settings.....	267
Table 55 Available Vouchers	268
Table 56 PoE Configuration Parameters	273
Table 57 PoE Status Info.....	275
Table 58 Smart SFP Alarms.....	280
Table 59 Layout Buttons.....	294
Table 60 Protocol and Feature Support Matrix.....	323
Table 61 External Device Types: Menu Buttons.....	327
Table 62 XML File: Root Element Properties.....	335
Table 63 XML File: Root Child Elements	336
Table 64 XML File: PropertyDefinition Attributes	338
Table 65 Properties: Mapping: MIB Syntax / XML SnmpType	339
Table 66 Open Source Components.....	351

1. INTRODUCTION

1.1 General

This document is valid as of Dragon PTN Release 4.0DR.

This manual is a guide for both first time and advanced Dragon PTN users. It describes how to get a basic Dragon PTN MPLS-TP solution up and running for the first time after having unpacked the Dragon PTN hardware. Furthermore, it describes more advanced functions and settings to get the best out of your Dragon PTN solution.

The Dragon PTN MPLS-TP network must be managed via the HiProvision (=Dragon PTN Management System). See the figure below for an example:

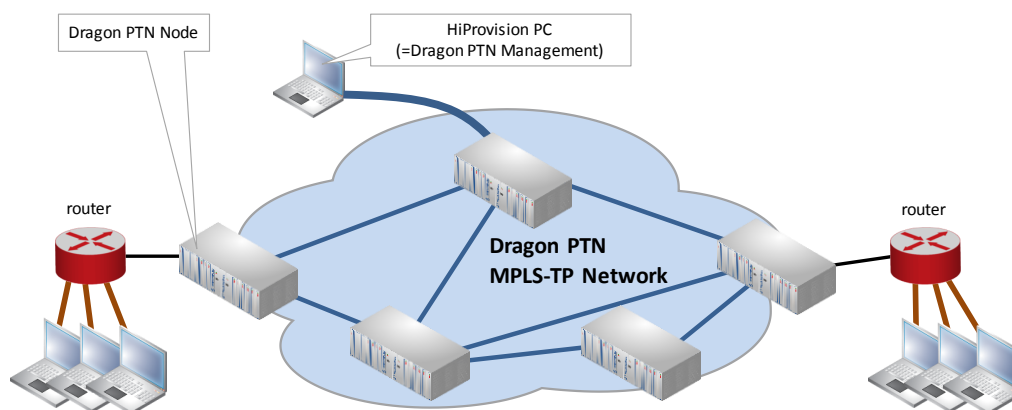


Figure 1 Dragon PTN Network Example

Prerequisites for a Dragon PTN solution setup:

a PC or laptop with a NIC is available that can be used as a HiProvision PC;
you are Administrator of the PC or laptop;
have your serial key and purchased vouchers ready before going online (see §20);
a network plan:

- ▶ How many nodes? See also Ref.[2] in Table 1;
- ▶ How many links per node?
- ▶ Optical fiber or electrical links?
- ▶ Which node numbers and node names must be used?
- ▶ Which front ports within the node will act as WAN port?
- ▶ Which front ports within the node will act as LAN port?
- ▶ How does my network look like? Network topology? Node interconnections?
- ▶ How do my customer applications connect to the network?

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. All these manuals can be found in the HiProvision Help function as well, see §19.

Table 1 Manual References

Ref.	Manual	Title
[1]	IG_Dragon-PTN_Installation-and-Operation_02_1019_en.pdf	Dragon PTN Installation and Operation
[2]	IG_Dragon-PTN_Nodes_02_1019_en.pdf	Dragon PTN Aggregation Nodes: PTN2210, PTN2206, PTN1104, PTN2209
[3]	IG_Dragon-PTN_PTN-CSM310-A_02_1019_en.pdf	Dragon PTN Central Switching Module: PTN-CSM310-A
[4]	IG_Dragon-PTN_PTN-4-GC-LW_PTN-4-GCB-LW_02_1019_en.pdf	Dragon PTN Interface Module: PTN-4-GC-LW/ PTN-4-GCB-LW
[5]	IG_Dragon-PTN_PTN-4-E1-L_PTN-4-T1-L_02_1019_en.pdf	Dragon PTN Interface Module: PTN-4-E1-L/4-T1-L
[6]	IG_Dragon-PTN_PTN-2-C37-94_02_1019_en.pdf	Dragon PTN Interface Module: PTN-2-C37.94
[7]	IG_Dragon-PTN_PTN-4-DSL-LW_02_1019_en.pdf	Dragon PTN Interface Module: PTN-4-DSL-LW
[8]	IG_Dragon-PTN_PTN-7-SERIAL_02_1019_en.pdf	Dragon PTN Interface Module: PTN-7-SERIAL
[9]	IG_Dragon-PTN_PTN-1-10G-LW_02_1019_en.pdf	Dragon PTN Interface Module: PTN-1-10G-LW
[10]	IG_Dragon-PTN_PTN-4-2-4WEM_02_1019_en.pdf	Dragon PTN Interface Module: PTN- 4-2/4WEM
[11]	IG_Dragon-PTN_PTN-4-CODIR_01_1019_en.pdf	Dragon PTN Interface Module: PTN-4-CODIR
[12]	IG_Dragon-PTN_PTN-4-GO-LW_01_1019_en.pdf	Dragon PTN Interface Module: PTN-4-GO-LW
[13]	IG_Dragon-PTN_PTN-2-OLS_E1_T1_01_1019_en.pdf	Dragon PTN Interface Module: PTN-2-OLS
[14]	IG_Dragon-PTN_TRMs_SFP_XFP_02_1019_en.pdf	Dragon PTN TRMs (Transmit Receive Modules: SFP, XFP)
[15]	UM_BasicConfig_HiProvision_User-Management_Rel_4-0DR_1019_en.pdf	HiProvision User Management
[18]	IG_Dragon-PTN_General-Specifications_01_1019_en.pdf	Dragon PTN General Specifications
[19]	UM_BasicConfig_HiProvision-Alarms-List_Rel_4-0DR_1019_en.pdf	HiProvision Alarms List
[20]	UM_BasicConfig_HiProvision-Add-on_CAR-IP_Rel_3-0DR_1019_en.pdf	HiProvision Add-on: CAR IP
[21]	UM_BasicConfig_HiProvision-Add-on_SNMP-Northbound_02_1019_en.pdf	HiProvision Add-on: SNMP Northbound
[22]	IG_Dragon-PTN_PTN-16-E1-L_PTN-16-T1-L_02_1019_en.pdf	Dragon PTN Interface Module: PTN-16-E1-L/ PTN-16-T1-L
[23]	IG_Dragon-PTN_PTN-9-L3A-L_PTN-9-L3EA_L_02_1019_en.pdf	Dragon PTN Interface Module: PTN-9-L3A-L (=main) / PTN-9-L3EA-L (=extension)
[24]	UM_BasicConfig_HiProvision-Add-on_Generic-Reporting_Engine_01_1019_en.pdf	HiProvision Add-on: Generic Reporting Engine
[25]	IG_Dragon-PTN_PTN-6-GE-L_01_1019_en.pdf	Dragon PTN Interface Module: PTN-6-GE-L
[100]	UM_Dragon-PTN_Bandwidth-Overview_01_1019_en.pdf	Dragon PTN Bandwidth Overview

2. STEPS FOR A BASIC SETUP

Following major steps are necessary to set up a basic Dragon PTN MPLS-TP solution. After having completed all the steps below, customer applications in the access networks will be able to communicate via a service over the Dragon PTN MPLS-TP network. Further on, these steps are worked out more into detail.

1. (§2.1) Prepare the Dragon PTN Hardware
2. (§2.2) Prepare the HiProvision PC
3. (§2.3) Physically Interconnect all Nodes into a WAN Network
4. (§2.4) Physically Interconnect HiProvision PC and Dragon PTN Network
5. (§2.5) Start Up and Initialize HiProvision
6. (§2.6) HiProvision: Discover and Approve the Dragon PTN Network Topology
7. (§2.7) HiProvision: Network Database Configuration
8. (§2.8) HiProvision: Check Network Hardware
9. (§2.9) HiProvision: Load Configuration into the Network
10. (§2.10) HiProvision: Set the Network Timing via an NTP Server
11. (§2.11) HiProvision: Set the LAN Ports in Your Network
12. (§2.12) HiProvision: Create MPLS-TP Tunnel(s)
13. (§2.13) HiProvision: Service(s) between Customer Applications

2.1 Prepare the Dragon PTN Hardware

NOTE: More information on all the modules can be found in Table 1;

1. Have your network plan ready, see prerequisites;
2. Set a node number for each node by setting the rotary switches S3 to S6 on the NSM (=Node Support Module) of each node, see Figure 2. Each node number must be unique in the network. Valid decimal node numbers range from 0001 to 8999. The configured node number can be verified later on via the CSM (=Central Switching Module) display, see Figure 3. See also the installation instructions in Ref. [1] in Table 1.

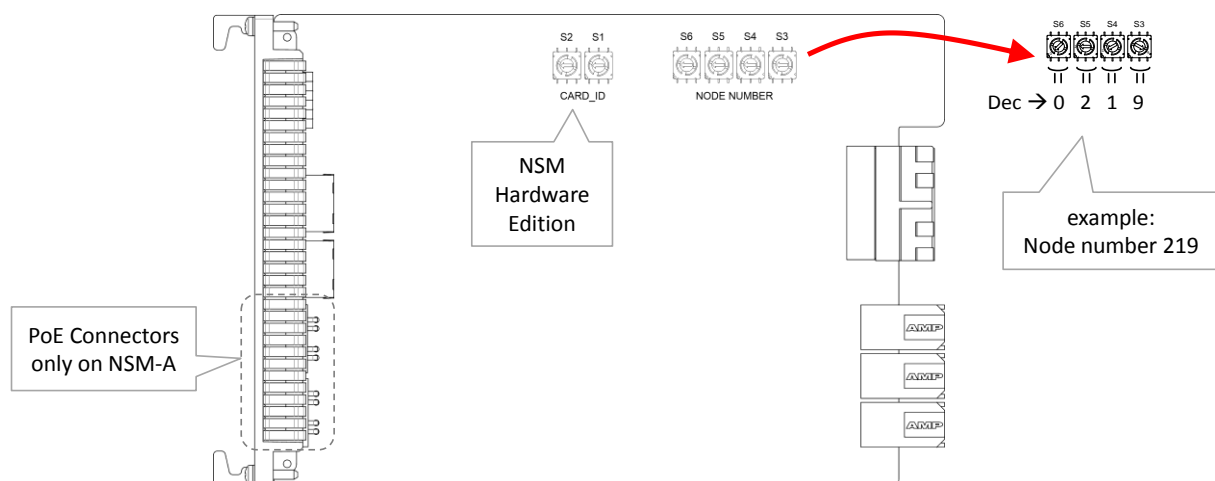


Figure 2 NSM Side View: Node Number

3. Plug in all the modules (minimum: NSM, one PSU, one CSM, one Interface Module that supports WAN ports, see §32) into the allocated slots in the nodes and tighten the fastening screws;

4. Power up the nodes via powering the PSUs;
5. Reset each node to factory defaults via pushing at least 7 seconds on the hidden reset button on the CSM front panel (figure below) of that node. If redundant CSMs are installed in the node, push on the reset buttons of both CSMs simultaneously for at least 7 seconds.

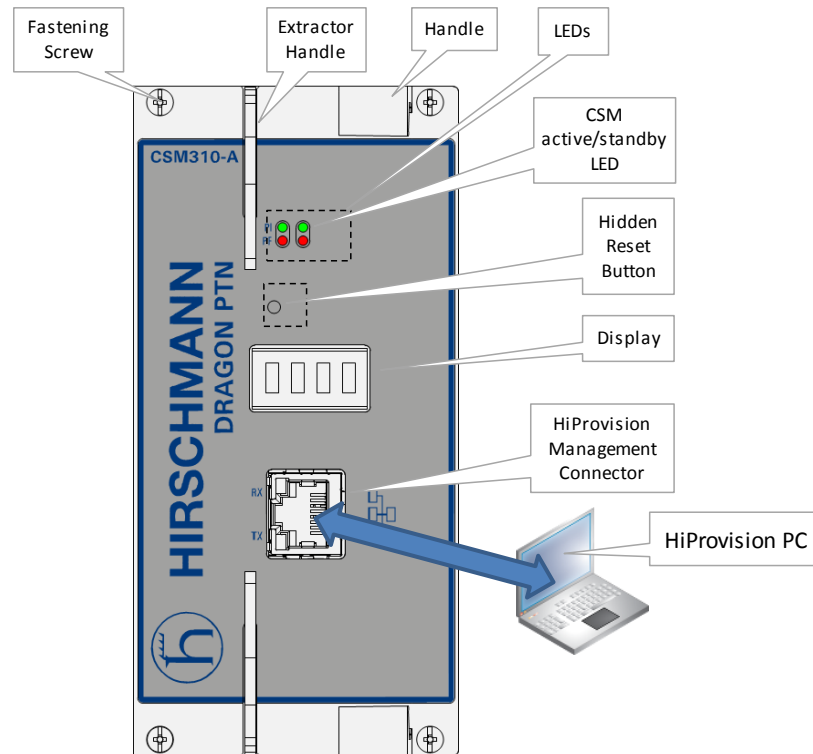


Figure 3 CSM Front Panel

2.2 Prepare the HiProvision PC

HiProvision is the software that manages the Dragon PTN network. Follow the steps below for further installation of HiProvision.

2.2.1 PC Requirements

The HiProvision PC requirements are listed in the 'Quick Installation Guide', see next paragraph.


2.2.2 Install HiProvision

HiProvision and a serial key can be downloaded from the Portal.

1. Surf to the Portal (= <https://hiprovision.hirschmann.com>) and log in;
2. Click on Shortcuts → Downloads;
3. Select the latest release or select another release via the drop down list;
4. Expand the 'Software' list;
5. Download all the components as described in the 'Quick Installation Guide'. The 'HiProvision' download automatically includes all the firmware files for the hardware and the product manuals or documentation;

6. Obtain a serial key via 'Shortcuts → Licenses HiProvision → Serial Key'. The Obtained HiProvision serial key will look like: 'DRN2-xxxx-xxxx-xxxx-xxxx-xxxx';
7. Installation on the HiProvision PC:
 - ▶ Make sure your PC meets the PC requirements listed in the 'Quick Installation Guide';
 - ▶ Follow the 'Quick Installation Guide' to install HiProvision with its serial key;
 - ▶ Default installation path: C:\Program Files (x86)\Hirschmann\HiProvision\;
 - ▶ Once the HiProvision has been installed (Complete Setup), five icons will be placed on the HiProvision desktop with X.Y.Z indicating the HiProvision version. It is also possible to install a custom installation via Custom button → Shortcuts when you don't need all shortcuts:

Table 2 Installation Shortcuts

Installer → Setup Type	 HiProvision Agent VX.Y.Z	 HiProvision Client VX.Y.Z	 HiProvision Remote Client VX.Y.Z	 HiProvision LNM Client VX.Y.Z	 HiProvision Remote LNM Client VX.Y.Z
Complete Button					
Complete	X	X	X	X	X
Custom Button → Shortcuts					
Local Client	X	X			
Remote Client			X		
LNLM Client	X			X	
Remote LNM Client					X

2.2.3 Configure Static IP Address on the NIC

a. One IP Address on the NIC

The IP address that must be configured on the NIC (=Network Interface Card) in the HiProvision PC depends on the CSM in the node to which the NIC is connected. Redundant CSMs are possible in the node which might result in two NICs in the HiProvision PC. Some use cases are available in §9.

Verify to which CSM the NIC is connected. In the IP Protocol settings of this NIC on the HiProvision PC, configure the following Internet Protocol Version4 (TCP/IPv4) Settings:

- ▶ CSM Front IP address: <IP address shown on the display of the connected CSM> + [1...13]. E.g. if the IP address on the CSM display = 172.16.25.33, set the IP address of this NIC to an IP address in the range 172.16.25.33 + [1..13] = 172.16.25.34 172.16.25.46. In case of redundant CSMs, both CSMs have an IP address in a different /28 subnet. Make sure to use the correct IP address in the NIC!
- ▶ Subnet mask: 255.255.255.240 (= /28 subnet mask).

NOTE: It is possible to change the IP address of the CSM, see §2.6.7.

Other fields: can be left empty;

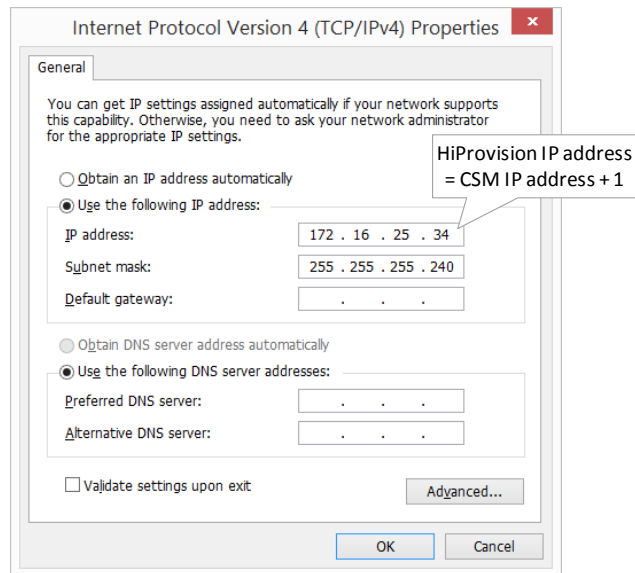


Figure 4 HiProvision IP Address

b. A Second IP Address on the NIC

A second IP address on the NIC is necessary when the HiProvision PC only has one NIC that must be connected via a switch to two different access or entry points to the Dragon PTN network (see §2.6.5).

In Figure 4, click on the 'Advanced...' button. The figure below pops up.

Click on the Add button, the TCP/IP Address window pops up;

Fill out the IP address and Subnet mask fields;

► Click the Add button;

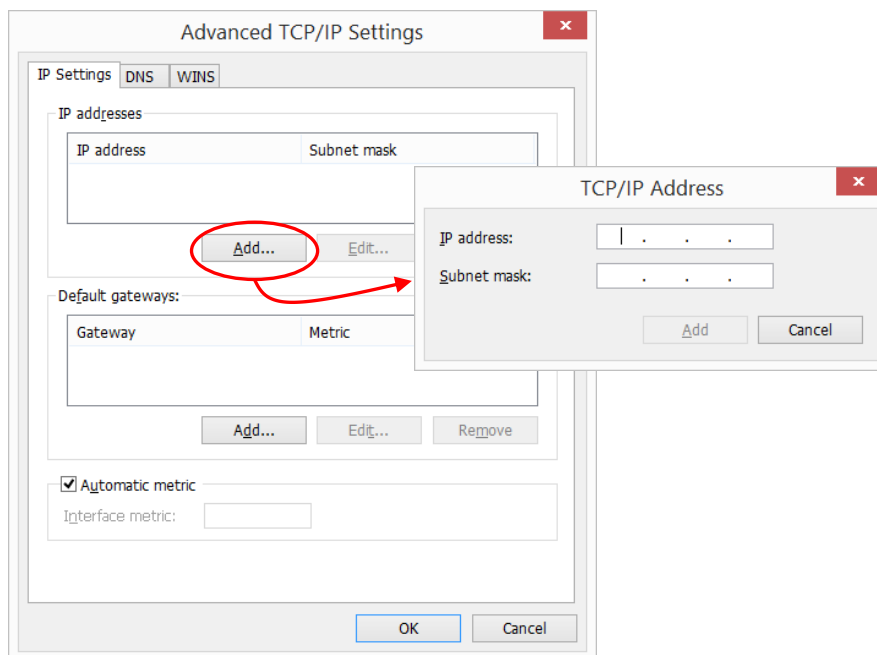


Figure 5 Second IP Address on NIC

CAUTION:

If you change your HiProvision connection e.g. from node x to node y, the IP address of the HiProvision PC must be configured with another IPv4 address. Follow the actions described in §10.1.

2.3 Physically Interconnect all Nodes into a WAN Network

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

Optical WAN links can be created on (see also §32):

- ▶ PTN-4-GC-LW/PTN-4-GCB-LW Interface Module → 1 Gbps, one link per module;
- ▶ PTN-4-GO-LW Interface Module → 1 Gbps, four links per module;
- ▶ PTN-1-10G-LW Interface Module → 10 Gbps, one link per module.

Electrical WAN links can be created on:

- ▶ a PTN-4-GC-LW/ PTN-4-GCB-LW Interface Module:
 - ▶ 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 still be used as LAN ports. The RJ45 port of combo port1 can only be used when there is no optical link on this port.

2.3.1 Connect Optical Link via Fiber/SFP/XFP:

CAUTION:

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

Plug in the SFP module into the SFP connector (=port1) of a PTN-4-GC-LW/ PTN-4-GCB-LW/ PTN-4-GO-LW Interface Module or plug in the XFP module into the XFP connector of a PTN-1-10G-LW Interface Module;

- ▶ Plug in the optical fiber into the SFP/XFP module;

NOTE: Smart SFP (see §23) cannot be used to interconnect Dragon PTN nodes;

NOTE: Fiber optic reporting information is available via the Reporting Engine Add-on, see §29.4.

2.3.2 Connect Electrical Link via Copper/RJ45:

Plug in the copper cable into an available RJ45 port of a PTN-4-GC-LW Interface Module/ PTN-4-GCB-LW;

When using the RJ45 connector from combo port1 on the PTN-4-GC-LW/ PTN-4-GCB-LW Interface Module, 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;

2.4 Physically Interconnect HiProvision PC and Dragon PTN Network

- ▶ Interconnect one or two NICs on the HiProvision PC with one single CSM or two redundant CSMs in a node in the Dragon PTN network. The connection(s) with the node occurs via plugging in the copper cable into the 'HiProvision Management Connector' of its CSM(s), see Figure 3;
- ▶ The IP address(es) of HiProvision directly connected to a CSM will by default be in the range of the CSM front IP address (172.16.0.1 → 172.20.100.209). This range can be different if a router is between HiProvision and the Dragon PTN network or if the CSM front IP address has been set in another IP range (see §2.6.7). The HiProvision IP addresses can be verified via the 'ipconfig' command in a command prompt on the HiProvision PC, see also §2.2.3;
- ▶ The CSM front IP address can be verified on the CSM display, see also (*) below;
- ▶ The HiProvision PC must be able to ping the connected node;

NOTE: The management port on the CSM can be disabled for security reasons via the Dashboard → Network Hardware → Devices → Node → CSM → Properties (Specific) → Management Port: Down. The management port is by default up.

NOTE: (*) It can be configured in HiProvision (**) how many times ('n') the IP address must scroll on the CSM display after plugging in the management cable. After these 'n' times, the IP address will not be displayed anymore e.g. for security reasons. If you want to show the IP address again for 'n' cycles, pull out the cable and plug it in again. By default, the IP address is always displayed in every CSM display-cycle.

NOTE: (**) 'n' can be configured via HiProvision → Network Hardware Tile → Devices → Select CSM → Display → Show IP address n Times: By default this field shows '-1' indicating that the value is displayed forever, '0' means never, 'n' with n > 0 means n times.

2.5 Start Up and Initialize HiProvision

2.5.1 Start Up HiProvision / Dashboard

1. Start up the **HiProvision Agent** first by double-clicking its icon on the desktop.
2. For a first time installation on the HiProvision PC, make sure to allow all the processes to pass through the Windows Firewall. Make sure that all the checkboxes are enabled in the figure below and click Allow access.



Figure 6 Allow HiProvision Processes

- Once the HiProvision Agent has started up successfully (a black HiProvision Agent window with 'Ready!' is visible), start up the **HiProvision Client** or the **HiProvision LNM Client** by double-clicking its icon on the desktop. The HiProvision Client is a full version including all features and applications, whereas the HiProvision LNM Client is a light or stripped version of the HiProvision Client. The differences between the two versions can be found in the table below:

Table 3 Differences HiProvision Client / HiProvision LNM Client

Tile Group	Dashboard Tile	HiProvision Client	HiProvision LNM Client
X = Tile or application available; --- = Tile or application not available;			
Administration	Database	X	X
	Servers (+Redundancy)	X	X
	Users (=HiProvision UM)	X	X
	Licenses	X	X
Configuration	Discovery	X	---
	Network Hardware	X	X
	Connections	X	---
	Layouts	X	X
	Protocols	X	---
Monitoring	Network	X	---
	Large Network (=LNM)	X	X
	Events	X	X
	Performance	X	---
	Alarms	X	X
	Assurance	X	---
	Protocols	X	---
Tools	Software	X	---
	Advanced	X	---
	Inventory (used in HiProvision Add-on: Generic Reporting Engine)	X	---
	Add-ons	X	---
	Help	X	X

- The HiProvision dashboard shows up including the user database pop-up below. The dashboard is divided in four main blocks, each block showing some tiles. Each tile is a shortcut to the mentioned function e.g. Database, Servers, Tiles with a white lock icon are currently locked or access denied.
- From now on HiProvision must be initialized, the first step is to create/select a user database, see figure below.

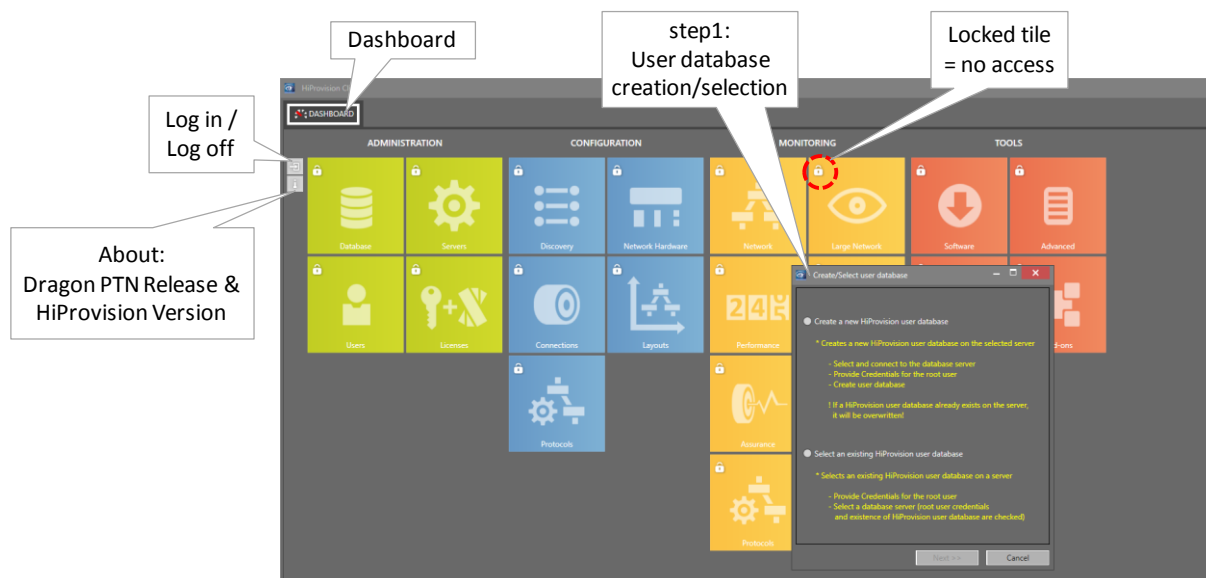


Figure 7 Dashboard View with User Database Request

2.5.2 Initialize HiProvision

This paragraph describes how to prepare or initialize HiProvision for a first time use. Basically following actions below must be done, find more detailed information further on:

Create/Select User Database

Log in

Create Network Configuration Database

Start Servers

Generate and Install License Pack

a. Create/Select User Database

1. In the user database request pop-up, select 'Create a new HiProvision user database'.

CAUTION: if a user database exists already on the connected server, it will be overwritten with the new created one.

2. The database server connection settings are listed. Make sure to fill out the IP address of the Server on which MySQL server runs, in the 'Server IP/Host Name' field. If it runs on the own HiProvision PC, fill out 127.0.0.1. The default **User Name = root** and **password = txcare**, but can be can be modified later on via §6.2.2. Click the Connect button. If the connection succeeds, it will be indicated by a pop-up. If the connection fails, see §38.1.
3. Password for root: Assign a new password to the master administrator by filling it out in the password field. Retype the password for confirmation.
4. Click the Create/Select button to create the user database, including the master administrator user with its password and some other predefined users in each group.

Figure 8 Select User Database Server

5. Click OK in the pop-up window indicating that the connection with the servers has failed, and restart the HiProvision Client.
6. From now on, the dashboard could look as in the figure below. This dashboard offers a compact overview of the entire HiProvision, which allows to manage the Dragon PTN network. The dashboard tab is fixed and thus cannot be closed.

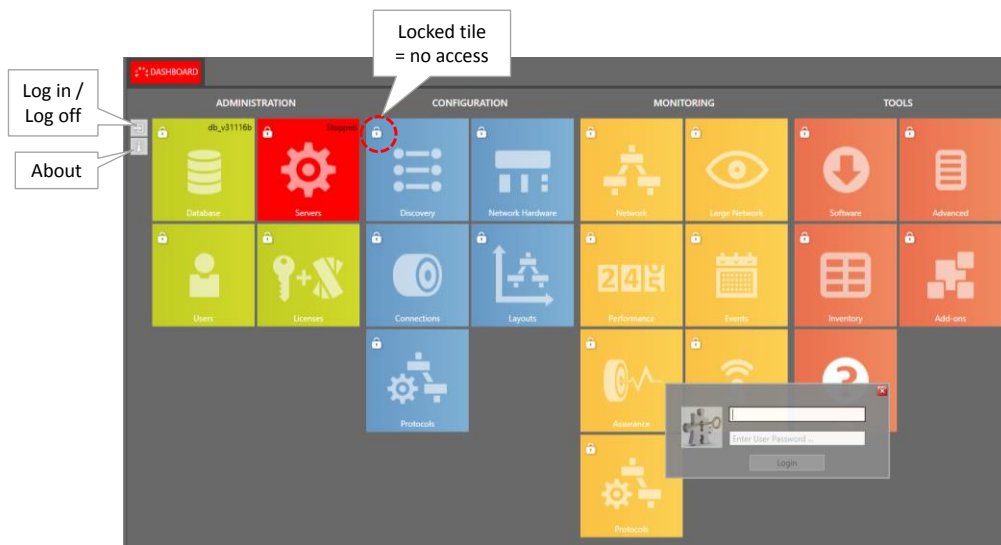


Figure 9 HiProvision Client - Dashboard

b. Log In

1. All tiles, except the Help tile, are locked (white lock icon). Log in first via the login box. If this is the first time login (e.g. after installation) or no administrators are created yet, fill out the credentials of the default admin user (user = admin, password = admin).
2. A successful login unlocks all the ADMINISTRATION tiles.

NOTE: Log in/log off can always be done via clicking  /  ;

NOTE: HiProvision User Management, including RADIUS authentication, is described in detail in Ref. [15] in Table 1;

c. Select Language

HiProvision supports multiple languages:

English (=default): no voucher or license required;

Chinese: voucher or license required, see §20.2.


► Polish: voucher or license required, see §20.2;

The used language in HiProvision depends on the logged in user. If no user is logged in yet, the HiProvision tiles will be displayed in English (=default language).

A language can be configured per HiProvision user after logging on. This must be done via the Dashboard → Users tile in the 'HiProvision User Management', see Ref. [15] in Table 1.


If you want to run HiProvision in a language (e.g. Chinese, Polish) different from the current language (e.g. English), follow the steps below:

If no user is logged in yet, the default start-up language is active:

► Log in via : HiProvision will run in the language assigned to the logged in user;


If a user is already logged in:

► Servers are not running:

► Log in via : HiProvision will run in the language assigned to the logged in user;






► Servers are running:

► Close HiProvision and restart it (only the Client, the Agent must not be restarted) or stop the Servers;

► Log in via : HiProvision will run in the language assigned to the logged in user.
Note: When a user tries to logon with a different user language when the servers are running, following warning pops up: 'The specified language for this user cannot be used at the moment. Please restart HiProvision or login with a different user.'

NOTE: A restart of HiProvision will always run HiProvision in the default language;

d. Create Network Configuration Database

1. Click the Database tile to open the Database tab in the figure below.
2. If you have chosen a custom installation path for MySQL Server at installation, change the default path first into the custom path via the options  button.
3. Create a (network configuration) database by clicking the  button for a new database or by selecting an existing database from an older version and click the select  button to start the migration of the older database to the newest version (see §6.6).
4. The newly created database shows up in the list and must be selected via clicking the select  button. The selected database, indicated by a green border, will be used in HiProvision for further network configurations. If desired, another database can be selected by clicking the  button again.

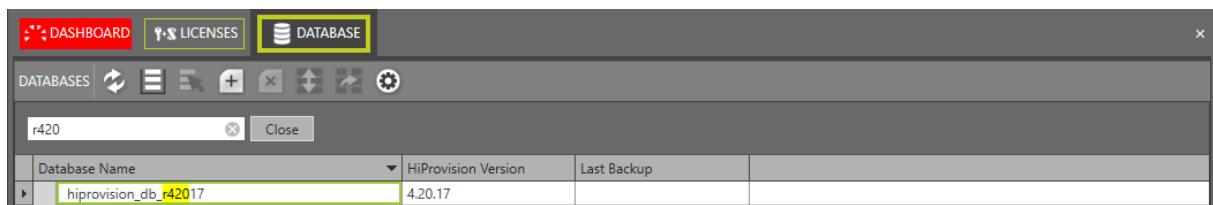



Figure 10 Network Configuration Database

e. Start Servers

1. Click the Servers tile in the Dashboard to open the Servers tab in the figure below.
2. Click the  button to start the HiProvision servers.
3. If this is the first time that the servers are started, the HiProvision processes must be allowed to pass through the firewall. Enable all the checkboxes for each window or process.
4. The servers are started when the Status has changed from Stopped into Started. A successful start also results in a green Servers tile. If the servers do not start, see §38.7.

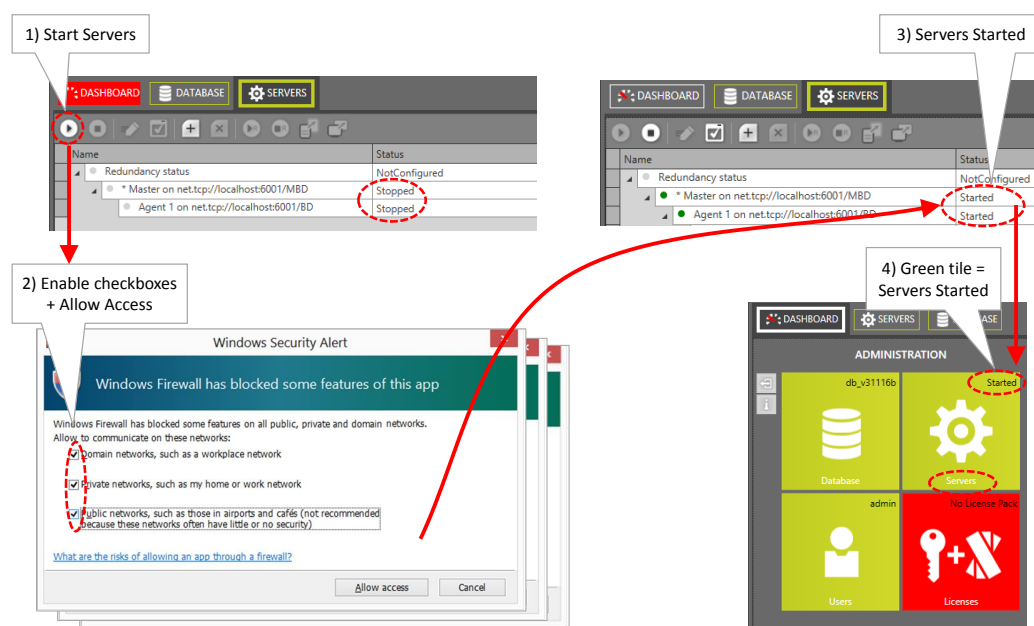



Figure 11 Start HiProvision Servers

5. Once the servers have been started, most of the ADMINISTRATION tiles turned green and most of the other tiles got unlocked (no more white lock). HiProvision is ready to discover the Dragon PTN network. Your dashboard tab could look as follows:




Figure 12 Dashboard: HiProvision Almost Ready for Management

f. Generate and Install License Pack

1. Have your serial key ready. The serial key can be found via the 'Licenses' tile or via the Info window  on the left-hand side.
2. Have your purchased voucher numbers ready. After having purchased vouchers, you have received a mail with voucher numbers in it. For more background info, read the entire chapter §20 first.
3. Follow the steps in §20.4 to install the licenses.

2.5.3 Dragon PTN Release, HiProvision Version, Care Program

Clicking the icon  on the left-hand side shows 'Dragon PTN Release a.bDR [HiProvision X.Y.Z]' used for installation. See figure below.

a.b = Dragon PTN Release;

► X.Y.Z = HiProvision Version;

A major Dragon PTN Release upgrade requires a 'Dragon PTN upgrade license'. This license might be covered by a Software Care or Total Care program. In a major upgrade, 'a' in 'a.b' increases. A major upgrade example: from Dragon PTN Release 3.1DR to 4.0DR. See §20.

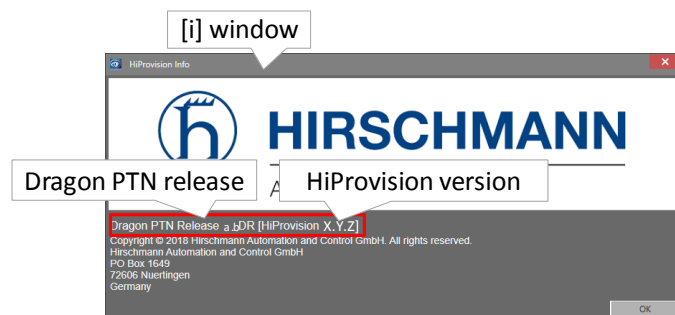


Figure 13 [i] Window: Dragon PTN Release, HiProvision Version

2.6 HiProvision: Discover and Approve the Dragon PTN Network Topology (DCN)

2.6.1 General

Prerequisites:

HiProvision must be able to ping the CSM front IP address (see §2.6.7) or device in the Dragon PTN network to which it is connected;

- ▶ The initial administration phase in HiProvision must have been successfully finished. See previous paragraphs.

Network Discovery will mainly do two things:

- ▶ Automatically set up a management path or DCN Channel in the live Dragon PTN network. This entire management path is called the Dragon PTN communication network. DCN = Data Communication Network. The bandwidth for this DCN Channel can be found in §3.9.
- ▶ Discover and visualize all the devices and links, it prepares HiProvision to approve (= to take a snapshot of) the Dragon PTN network topology.

Find more info in the paragraphs below:

Discovery Tile / Menu Buttons / States: see §2.6.2;

Discover Network Topology via Discovery Entry Point: see §2.6.3;

- ▶ HiProvision connected to one Dragon PTN network;
- ▶ HiProvision connected to multiple Dragon PTN networks;

Approve the network topology: see §2.6.4;

Redundant Discovery Entry Point: see §2.6.5;

Routed DCN: see §2.6.6;







CSM Front IP Address: see §2.6.7;

- ▶ Change the Device IP Range of the Dragon PTN Network: see §2.6.8.

2.6.2 Discovery Tile / Menu Buttons / States

Go to Dashboard → Discovery tile. A short description of the menu buttons and different discovery states are listed in the tables below.

Table 4 Discovery Menu Buttons

Button	Short Description
Discovery Entry	
	Create discovery entry point.
	Create redundant discovery entry point, see also §2.6.5.
	Delete selected discovery entry point.
	Activate the redundant or standby discovery entry point, see also §2.6.5.
	Approve the entire network topology which sets the expected IDs for all devices in the entire network.
	Clear the entire network approval which clears the expected IDs for all devices in the entire network.















Button	Short Description
	Modifies both the administration and authentication V3 SNMP passwords and applies it to the discovered devices.
	Apply the current configured V3 SNMP passwords to all the discovered devices, e.g. can be used after adding a new device into the live network.
	Deploy a new custom Device IP Range in the Dragon PTN network. This step is required if your HiProvision PC belongs to a routed network that has subnets with IP Ranges that conflict with the default Dragon PTN Device IP Range (10.255.x.y/16), see §2.6.8.
	Factory reset the Device IP Range in the Dragon PTN devices to 10.255.x.y/16.
	Refresh button. Click this button if you think the GUI has not updated the screen according the real situation.
Devices	
	Auto create devices: Clicking this button automatically creates the selected network element(s) in the HiProvision database. The parameters of the auto-created network elements will have default values.
	Clear neighbor approval and IP addresses: Use this button in case of link problems or if you want to insert/remove devices. This button is only active if you select a LinkEndPoint (or port). Clicking this button clears the expected IDs from the selected LinkEndPoint and it clears the IP addresses on the link. As a result, the link will be renegotiated so it becomes up and running and ready to be Approved (state 'Not Approved').
	Search functionality to sort/group network elements in a better way. When using the search, the network elements are by default grouped by Module Type for a better overview.
	Auto creation status in database, see §2.7.1 for more information.
	Refresh button. Click this button if you think the GUI has not updated the screen according the real situation.
Links	
	Auto create links: Clicking this button automatically creates the selected links in the HiProvision database. The parameters of the auto-created links will have default values.
	Link approval: Clicking this button approves and sets the selected link to 'OK'.
	Auto creation status in database, see §2.7.1 for more information.
	Refresh button. Click this button if you think the GUI has not updated the screen according the real situation.

Table 5 Discovery: Poll States

Poll State	Short Description
Discovering	Start of the HiProvision Discovery process.
Connecting	HiProvision is still discovering/measuring at least one network element in the network. This phase remains until all network elements have been measured.
Ready	All network elements have been discovered/measured.
Standby	Used in case of Redundant Entry points. This Entry Point is standby and ready to take over when the other Entry Point fails. See also §2.6.5.

Table 6 Devices: Neighbor Communication











Neighbor Communication	Status (*)	Priority (**)	Short Description
Not Approved (no border)			
Not Connected	Green	1 (=lowest)	No cable is plugged in on a WAN port, but not approved yet.
Connected	Green	2	The WAN port can communicate with the device connected to it, but not approved yet.
No Communication	Red	3 (=highest)	Error: The WAN port cannot communicate with the device connected to it. It is possible that the connected device is a replaced device with an invalid IP address configuration, but not approved yet. ACTION: select the LinkEndPoint row and Clear Neighbor Approvement and IP Addresses ().
Approved (green/red border, green = OK, red = Error)			
OK - Not connected (Green border)	Green	1 (=lowest)	No cable is plugged in on a WAN port and this is desired, has been approved.
OK - Connected (Green border)	Green	2	The WAN port can communicate with the device connected to it, and this is desired, has been approved.
No Communication (Red border)	Red	3	Error: Same as 'No Communication' description above but Approved.
Missing (Red border)	Red	4	Error: In the OK - Connected state, the WAN cable has been pulled out. ACTION: put in the existing cable again or Clear Neighbor Approvement and IP Addresses on this link (Devices: ) for new links/devices and approve the new situation (Links: ).
Not Allowed (Red border)	Red	5 (=highest)	Error: <ul style="list-style-type: none"> - In the OK - Connected state, a wrong or unexpected device has been connected to the WAN port. ACTION: connect the expected device again or Clear Neighbor Approvement and IP Addresses on this link (Devices: ) for new links/devices and approve the new situation (Links: ). - In the OK - Not Connected state, something has been connected to the WAN port. ACTION: remove the cable or Clear Neighbor Approvement and IP Addresses on this link (Devices: ) for new links/devices and approve the new situation (Links: ).
(*) Status: 'orange': HiProvision is rediscovering (or connecting) this network element, e.g. due to a change in the network; (**) Priority: The Neighbor Communication is the state of the selected network element or the worst resulting state (=state with the highest priority) of its child elements, if any. Example: An Interface Module has a 'Missing' (=prio 4) state on port 1 and a 'Not Allowed' (=prio 5) state on port 2. The Interface Module will show the 'Not Allowed' state because it has the highest priority.			

Table 7 Links: Discovery

Discovery	Short Description
OK (Green border)	The link has been discovered/measured by HiProvision and approved via  ;
Not Approved	The link has been discovered/measured by HiProvision but not approved yet  ;

2.6.3 Discover Network Topology via Discovery Entry Point

a. HiProvision Connected to One Network

- Configure the connection with the first CSM: Create Discovery Entry Point via clicking  in the 'Discovery Entry' section and fill out an Entry Point Name.

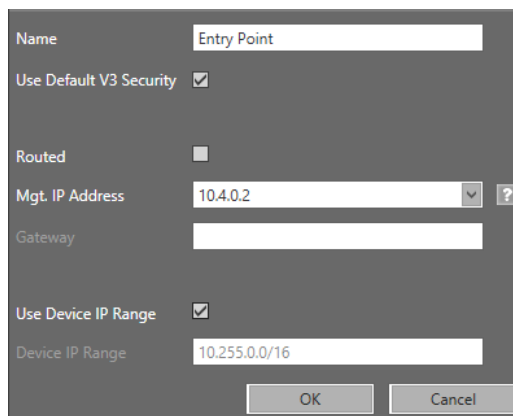


Figure 14 Create Discovery Entry

- First CSM = CSM in node to which the HiProvision PC has been connected;
- Entry Point = CSM management connector that interconnects a HiProvision PC with the Dragon PTN network;
- Keep the default SNMP settings ('Use Default V3 Security' = username, authentication password, private password). If your network already had a customized SNMP authentication in the devices, uncheck 'Use Default V3 Security' and fill out the credentials already available in the network.
- Routed: check this if your HiProvision PC is connected to the Dragon PTN network via a routed network, see §2.6.6.
- Mgt. IP Address: fill out the CSM front IP address of the first node via which HiProvision connects to the Dragon PTN network. This address can be viewed via the display on the CSM.
- Gateway: This field becomes active when Routed has been checked, see §2.6.6.
- Use Device IP Range (default = checked) / Device IP Range:
 - Unchecked:
 - Use only when you have multiple entry points and each entry point is connected to only one node;
 - With only a single node, no Device IP Range is needed or used. Instead, only the CSM front IP address of the connected node will be used. As a result, no additional routes in the router must be configured in case of a routed network;
 - Checked (=default):
 - Must be used when the entry point connects at least to two nodes;
 - The Device IP Range is the IP address range used by HiProvision to assign a unique address to the devices and to reach the device in the Dragon PTN network. If the Mgt. IP Address is reachable (detection phase is maximum 20 seconds), the

network can be detected. As a result, the detected Device IP Range is filled out automatically and greyed out. If the Mgt. IP Address is not reachable (e.g. offline), the Device IP Range can be filled out manually after the detection phase. In a detected live network, the device IP range can always be adapted, see §2.6.8. If the HiProvision PC has only one NIC, it does not matter which Device IP Range is selected. If HiProvision has more than one NIC, change the Device IP Range in such a way that the different IP networks connected to the HiProvision NICs, do not interfere with each other's Device IP Ranges.

The network discovery starts immediately after the Entry Point has been created → **PollState = Discovering** → **PollState = Connecting** (see figure below);

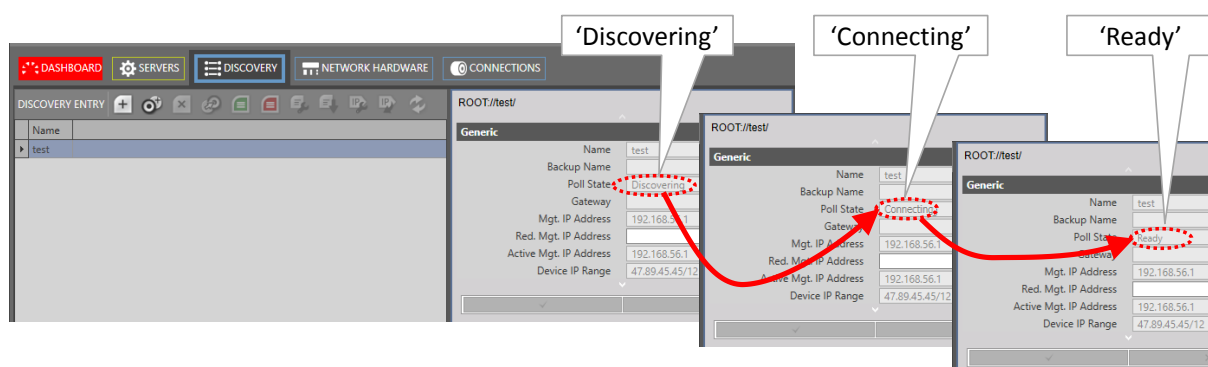


Figure 15 Discovery PollState

- ▶ In the discovering and connecting state:
 - ▶ The Devices/Status column shows an orange bullet;
 - ▶ The discovered devices will pop-up almost instantly within a few seconds in HiProvision. Each discovered device will automatically get a device IP address. A DCN will be set up automatically over the entire Dragon PTN network, see §3.9.

NOTE: DCN is an in-band Dragon PTN communication network which is only used by HiProvision to manage the Dragon PTN network.

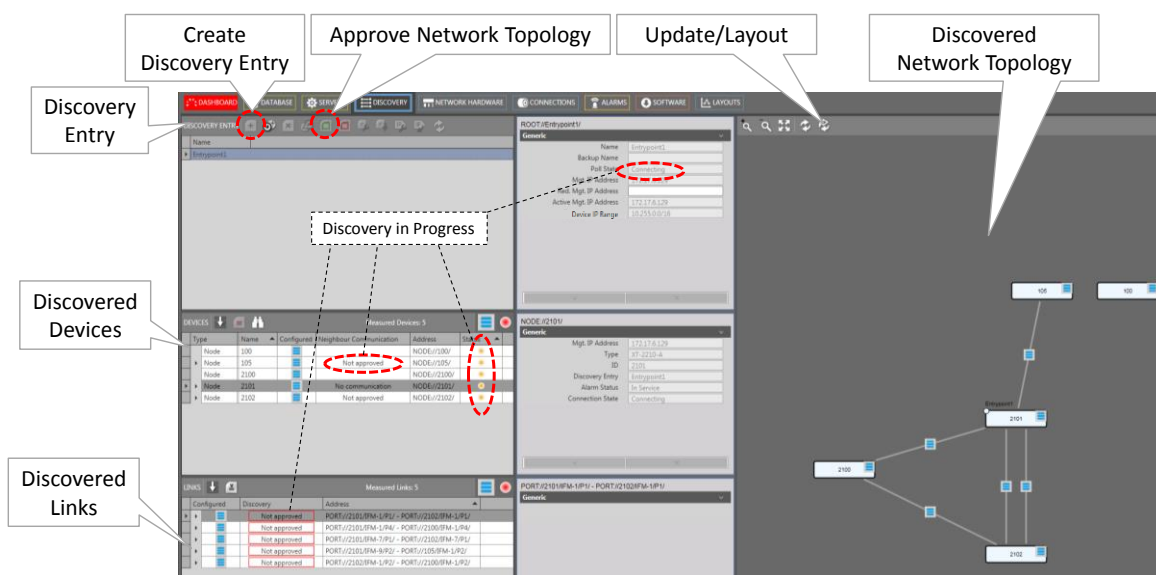



Figure 16 Network Discovery in Progress: Connecting

- ▶ Finally, the entire network (devices + links) is discovered and visualized in HiProvision: **PollState = Ready**. Also the number of discovered or measured devices and links is shown.
- ▶ Devices:
 - ▶ Neighbour Communication column:
 - ▶ First time discovery: network elements that are discovered for the first time show 'Connected' or 'Not Connected', they still have to be approved, see §2.6.4.
 - ▶ Network element already discovered and approved before: network element cell indicates 'OK - Connected' or 'OK - Not Connected' with a green border. Any other state/color indicates that something is wrong or unexpected, see Table 5 for more info;
 - ▶ Status column:
 - ▶ Green bullet: the network element and all its underlying child elements are not approved yet or approved and OK according to the approved network expectations;
 - ▶ Red bullet: the network element or one of its underlying child elements is in 'No Communication' or in another error state with a red border meaning a violation against the approved network expectations, see Table 5 for more info;
 - ▶ Orange bullet: the network element or one of its underlying child elements is again in connecting state meaning that HiProvision is (re)discovering that network element because something has changed in the network connections of that element, e.g. a cable has been pulled out.
- ▶ Links: Discovery column:
 - ▶ First time discovery: a first time discovered link shows 'not approved' with a red border;
 - ▶ Link already discovered and approved previously: the link indicates 'OK' with a green border;
 - ▶ If an expected link is not shown in the list, it means that the link is not there and not measured. The link cable is probably pulled out, check your hardware;
- ▶ Click the Update/Layout  button to update and layout the discovered devices properly;

If the full discovered network visualization is NOT as expected, it might mean that you have forgotten some links or that you have misconceptions. Verify your hardware and adapt the physical links where needed, see §2.3. The discovery function will automatically and almost instantly within a few seconds rediscover the modified network after changing the hardware configuration. Repeat this step until the visualization is as expected;

NOTE: The network layout in the Discovery tile is independent from the layouts available in the Layouts tile in §26.2.

NOTE: Hardware and Links Reporting information is available via the Reporting Engine Add-on, see §29.4.

b. HiProvision Connected to Multiple Networks

Per network to which HiProvision is connected, a new Entry Point must be created. Each entry point, connected to at least two nodes, must have its own unique Device IP Range. Unique means non-overlapping with the Device IP Range of the other Entry Points. A basic example is shown in figure below. To change the Device IP Range in the Entry Point, see §2.6.8.

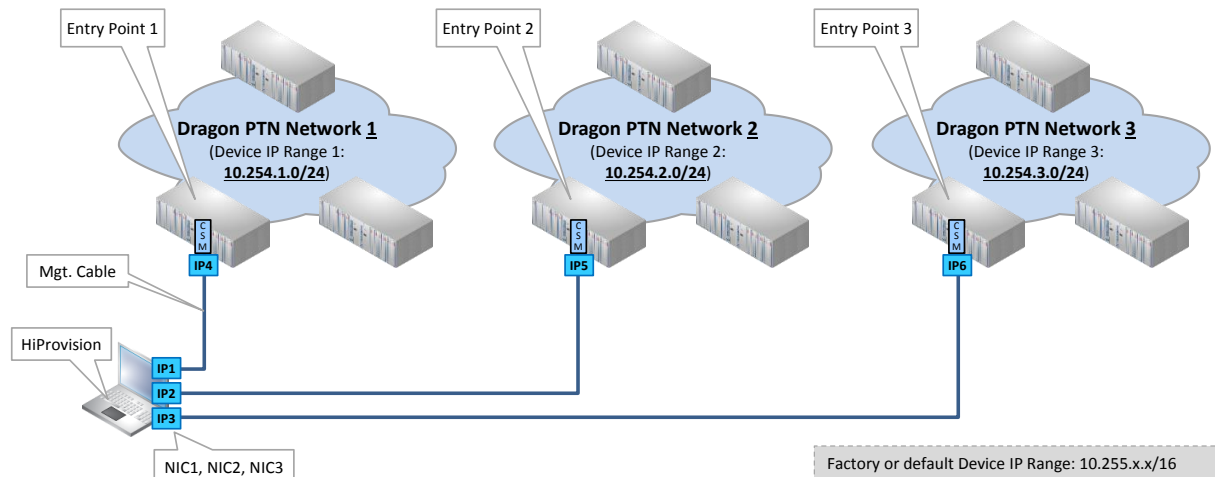


Figure 17 HiProvision Connected to Multiple Dragon PTN Networks

2.6.4 Approve Network Elements in the Network

Depending on the situation, you can either:

Approve the entire network after a first time discovery;

- ▶ Approve one or some network elements after network modifications.

a. Approve Entire Network after First Time Discovery

Prerequisite:

The network topology has been fully discovered (PollState = 'Ready') and its visualization is as expected;

- ▶ Understand measured/programmed (=expected)/configured values, see §4.2:

Approving the network topology means taking a snapshot of the discovered network that meets your expectations, and storing this expected snapshot into the network. As a result, every device will always expect the same neighbor device and links according to the stored snapshot.



After approving the network topology, any link alteration (e.g. broken link...) or device change (e.g. missing, unknown, intruder device....) in the network afterwards will cause a mismatch against this network snapshot and run into error states with red borders (see Table 5) and alarms in the dashboard.

- ▶ Unapproved network topology = network with no expectations, see Table 8.
- ▶ Approved network topology = network snapshot or expectations fully loaded into the network, values are according to Table 8;

Table 8 Unapproved/Approved States In Normal Situation

Section	Column Name	Column Value	
		Unapproved Network	Approved Network
Devices	Neighbor Communication	Not Approved / Not Connected	OK - Connected / OK - Not Connected
Links	Discovery	Not Approved	OK

Take a snapshot or approve the entire network topology in one click as follows:

- Click the  button in the Discovery Entry section. This action:
 - Copies all the measured values into the expected values in the devices;
 - Sets Approved values in Table 8. If a link is still 'Not approved' afterwards, select the row of this link and click the  button to set the link to 'OK'.

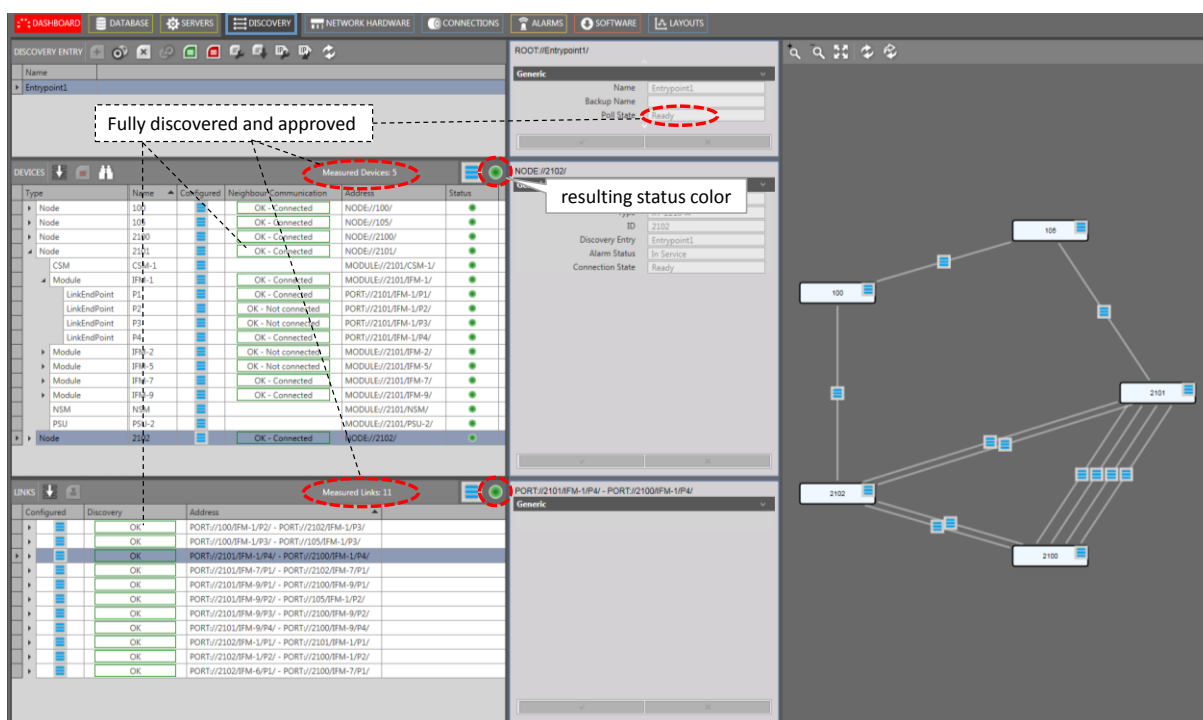


Figure 18 Network Fully Discovered and Approved: Ready/Measured Devices and Links

b. Approve Single Network Elements after Network Modifications

If small adaptations are done in an already approved network, e.g. an extra inserted device, an extra link etc... The impacted and neighbor network elements run into an error state with a red border, the other network elements remain OK. To solve these issues, follow the actions for the detected errors in Table 5.

2.6.5 Redundant Discovery Entry Point or Cable Connection

a. General

A redundant discovery entry point must only be created when one HiProvision PC needs two access points via two management cables into the Dragon PTN network, as a precaution to a management cable break.

NOTE: Redundant discovery entry points always share the same Device IP Range (or go to the same Dragon PTN network), whereas two individual created entry points always have a unique Device IP Range (or each go to a different Dragon PTN network);

It is strongly advised to do this! This feature is called 'Dual Access Discovery Entry Points'.

Number of NICs required in the Dragon PTN PC when configuring a redundant entry point:

two NICs: each NIC is directly connected to the Dragon PTN network via a management cable;



one NIC: the NIC is connected to a switch which is connected via two management cables to the Dragon PTN network. Two IP addresses, one for each access point, must be configured on the HiProvision NIC, see §2.2.3b.

When a cable break occurs with only one management cable between the HiProvision PC and the Dragon PTN network, the HiProvision PC loses connection with the Dragon PTN network. As a result, the Dragon PTN network stays alive but cannot be monitored/configured anymore.

NOTE: When two redundant HiProvision PCs each have one management cable connected to the network (see §9.7), it means only one discovery entry point per PC, no redundant discovery entry points are involved in this case.

b. Create Redundant Discovery Entry Point

Follow the steps below:

- ▶ Install a second NIC (if not already available) in the HiProvision PC and connect this NIC to another CSM in the same node (=redundant CSMs) or a CSM in another node as described in §2.4;
- ▶ Click the active or first entry point in the entry point list to highlight the  icon;
- ▶ Create the redundant entry point by clicking . It is similar as described in §2.6.2;
- ▶ After the redundant discovery, two entry points (in our example Entry Point1 and Entry Point2) will be visible in the list, see figure below:

Which entry point is the active one, which one is redundant or standby?

- ▶ PollState = Ready → active entry point;
- ▶ PollState = StandBy → standby entry point.

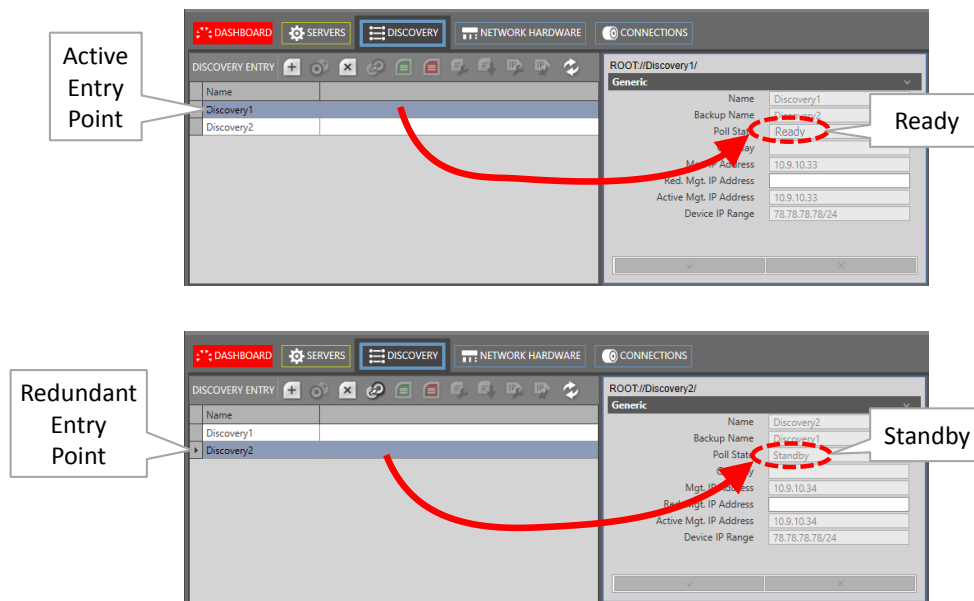



Figure 19 Active/Redundant Discovery Entry Point

c. Switchover Active and Standby Entry Point

There are three ways to switch over from the active to the standby entry point.

- ▶ Automatically via a NIC-CSM cable break of the active entry point;
- ▶ Manually via clicking the  button
- ▶ Connected CSM not reachable (e.g. reboot due load action sync...)

A switchover:

- ▶ makes the standby entry point the new active one, its PollState turns into 'Discovering' and finally results in 'Ready';
- ▶ makes the active entry point the new standby one, whatever the reason for the switchover was (manual, broken link, ...), its PollState turns into 'Standby'.

Revertive/Non-revertive behavior:

- ▶ The redundant entry points are always non-revertive: once a switchover of the entry point has occurred, the new active point stays active until a manual switchover or switchover caused by a cable break occurs again. No automatic switchback to the original entry point will occur, not even when a possible cable break has been recovered.

2.6.6 Routed DCN

a. General

The Dragon PTN discovery can be done via a routed management network where at least one router is between the HiProvision PC and Dragon PTN, see figure below. The routed DCN is only possible when the Routed checkbox has been checked in the Entry Point creation.

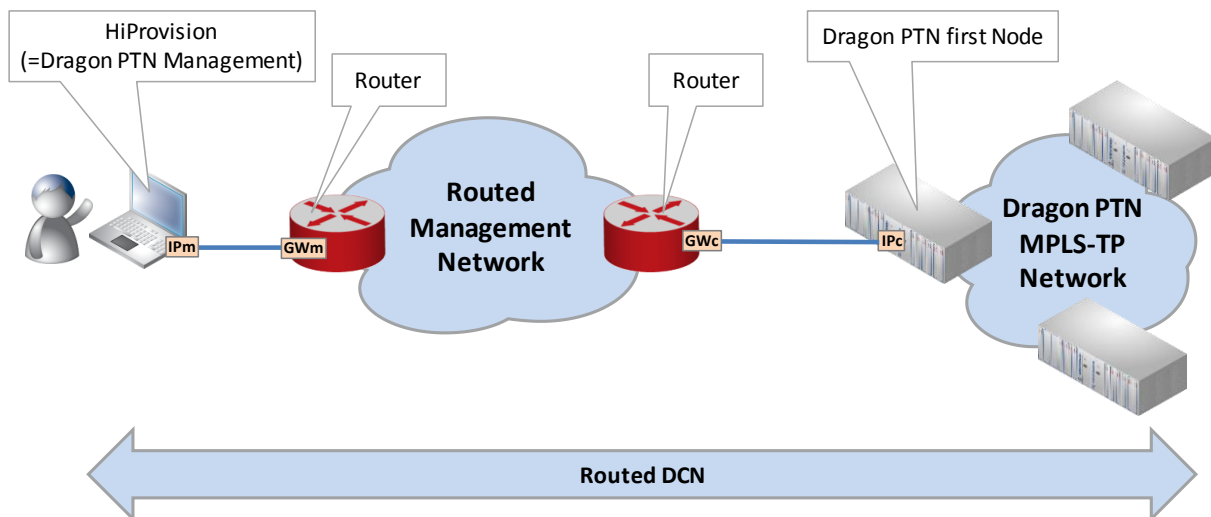


Figure 20 Routed DCN: Routed Management Network

b. Configuration: NIC in HiProvision PC

In the IP Protocol settings of the NIC on the HiProvision PC, configure:

- ▶ IP address 'IPm' (see picture above, 'm' refers to management PC);
- ▶ Gateway IP Address 'GWm';
- ▶ IP Subnet mask.

c. Configuration: CSM Gateway Address

Fill out a CSM Gateway Address 'GWc' in the CSM Front IP Address configuration to make sure that the first node can reach HiProvision again, see §2.6.7;

d. Configuration: Entry Point: Routed + Gateway Address

Create an Entry Point as described in previous paragraphs and check the 'Routed' checkbox. Fill out the Mgt. IP Address 'IPc' (=CSM IP address) and the Gateway address 'GWm' in the Gateway field. The Gateway field is only active when Routed has been checked.

The screenshot shows a configuration dialog box with the following fields and values:

- Name: [Empty text box]
- Use Default V3 Security: ☒
- Routed: ☒
- Mgt. IP Address: [Question mark icon]
- Gateway:
- Use Device IP Range: ☒
- Device IP Range:
- Buttons: OK, Cancel

Figure 21 Entry Point with Routed Checked, Gateway Field

e. Configuration: Routers

In the routers that are directly connected to the Dragon PTN network(s), every possible path from those routers to the Dragon PTN network(s) must be configured as a static route. Via a routing protocol in the Routers (e.g. OSPF), those static routes can be advertised to indirectly connected routers.

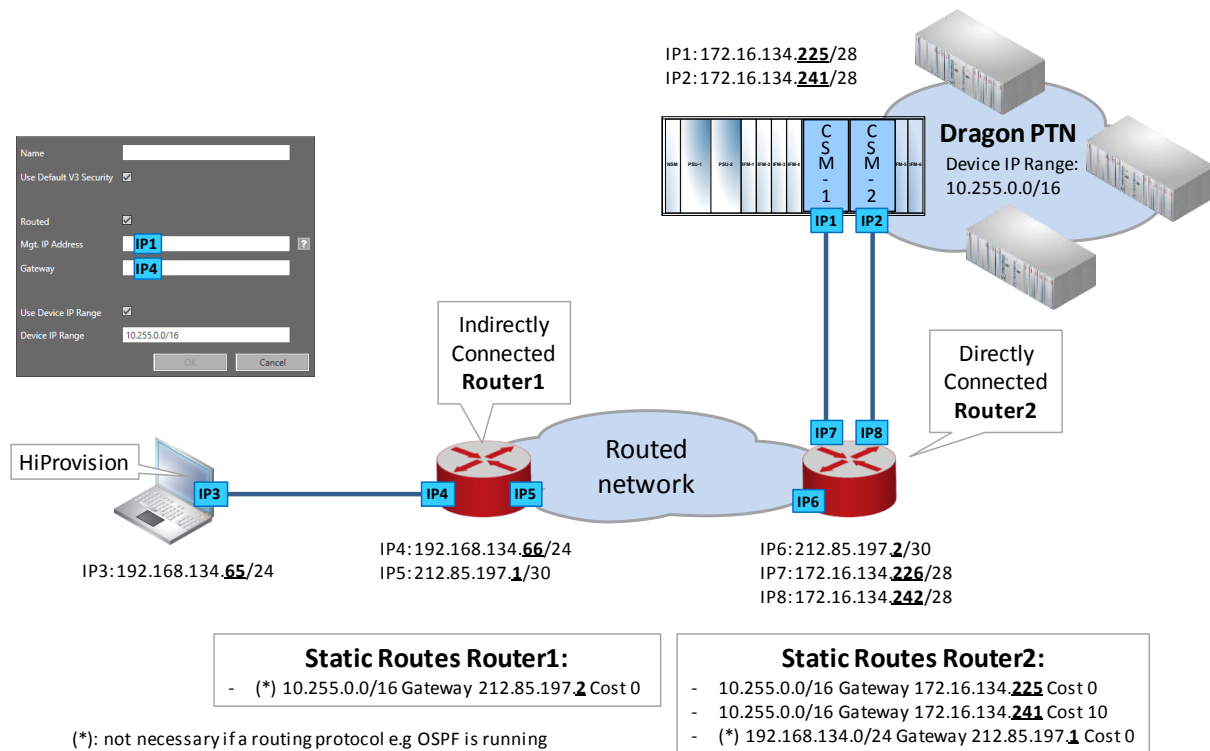


Figure 22 Routed DCN: Static Routes in Routed Network

Static Route example for directly connected routers (=Router2):

The Dragon PTN network must be reachable via the CSMs with front IP address 'IP1' and 'IP2';

Static Route: <Device IP Range> Gateway <CSM Front IP Address> Cost <cost value>;

See example routes in figure above;

2.6.7 CSM Front IP Address

a. General

Is the IP address on the management connector (see Figure 3) on the CSM front panel (=Mgt. IP Address in the Entry Point);

Is the IP address via which HiProvision connects to the Dragon PTN network, local connection;

Is default/factory in the CSM IP Range 172.x.y.z/28 and based on the node number (=device ID);

Is used by remote client to access HiProvision via DCN;

Must be changed when there is at least one router between the HiProvision PC and the Dragon PTN network or to avoid IP conflicts with a possible modified Device IP Range in the Dragon PTN network.

CAUTION: When changing IP addresses or IP ranges, make sure that the Device IP Range of your network does not conflict with the CSM Front IP Addresses of your entry points for this network. All these IP addresses and ranges can be verified in the Entry Point(s) in the Discovery Tile.

NOTE: This management port can be disabled for security reasons via the Dashboard → Network Hardware → Devices → Node → CSM → Properties (Specific) → Management Port: Down. This management port is by default up.

- ▶ Set CSM Front IP Address via Local Connection: see §b;
- ▶ Set CSM Front IP Address via Network Connection: see §c;
- ▶ Set CSM Front IP Address on New Second CSM in Live Existing Device: see §d;

Reset CSM Front IP Address to Factory Defaults: see §e;

b. Set CSM Front IP Address via Local Connection

By default, the node has a management IP address in the range 172.x.y.z/28 (based on the node number).

1. Power up the node that includes the CSM(s);
2. Visit the node locally and connect the HiProvision PC directly via an RJ-45 cable to the HiProvision management connector on a CSM in the node;
3. Verify the current CSM front IP address and write it down on a paper. This IP address is shown on the CSM display.

NOTE: It can be configured in HiProvision (*) how many times ('n') the IP address must scroll on the CSM display after plugging in the management cable. After these 'n' times, the IP address will not be displayed anymore e.g. for security reasons. If you want to show the IP address again for 'n' cycles, pull out the cable and plug it in again. By default, the IP address is always displayed in every CSM display-cycle.

NOTE: (*) The amount of times can be configured via HiProvision → Network Hardware Tile → Devices → Select CSM → Fill out 'Display' properties. By default the field shows '-1' indicating that the value is displayed forever, '0' means never, 'n' with $n > 0$ means n times.

4. Configure the IP address of the HiProvision PC (**) in the same IP address range as the one of the device. This can be done in the IP Protocol settings of the NIC (=Network Interface Card) on the HiProvision PC: configure IP address, IP Address subnet mask (Gateway will be filled out automatically later on by HiProvision, when configuring a routed entry point, see further);

NOTE: (**) This is just a temporary IP address for HiProvision to interconnect with the node.

- Go to Dashboard → Advanced (TOOLS) → CSM Front IP Addresses;

Figure 23 Advanced Tab: CSM Front IP Addresses

- Fill out the current IP address of the CSM in the 'Device Mgt. IP Address' field and click 'Ping' to check whether the HiProvision PC can reach the node;
- If the node is reachable, change the CSM IP address by filling out the new unique IP information per CSM. If you have redundant CSMs, fill out both the CSM-1 and CSM-2 fields. If only one CSM resides in the node, fill out the CSM-1 (CSM is plugged in on the left-hand CSM slot) or the CSM-2 (CSM is plugged in on the right-hand CSM slot) fields.
 - ▶ '<CSM-1/CSM-2> Front IP address of the node';
 - ▶ '<CSM-1/CSM-2> Subnet Mask' of the node;
 - ▶ '<CSM-1/CSM-2> Default Gateway Address of the node (only necessary if a router is between this node and the HiProvision PC).
- Click Apply. Click Reboot and confirm the pop-up;
- After the reboot of the node, the new IP address(es) will be set on the node or CSM(s).

NOTE: As of now, the node will be unreachable for the HiProvision PC when the HiProvision PC IP address range mismatches the new CSM IP address range(s);
- Configure the IP address of the HiProvision PC again in the new and same IP address range as the connected CSM to verify it is reachable again.

c. Set CSM Front IP Address via Network Connection

It is possible to change the CSM front IP address of any other node in the network, while HiProvision not being locally connected to that node. This can be useful if you want to prepare the IP configuration for a redundant set up and connection in your network.

- In Figure 23 in the 'Device Mgt. IP Address field', just fill out the Mgt. IP address (*) of the node with the CSM that must be have another IP configuration. Click 'Ping' to check whether the HiProvision PC can reach the node;

NOTE: (*): The Mgt. IP address can be found in Network Hardware → select device row → Generic Properties → Mgt. IP Address. This is the IP address which HiProvision uses to manage the device. This is either the Device IP Address for remote nodes or the CSM front IP address for the node connected to HiProvision.

2. Fill out the correct new IP address information in the other fields;
3. Click Apply. Click Reboot and confirm the pop-up;
4. The node will reboot with the new IP configuration on its CSM;

d. Set CSM Front IP Address on New Second CSM in Live Existing Device

Prerequisites: HiProvision can reach the node via the network. It is not a requirement that the second CSM is plugged in into the node to configure this IP information. The new configuration of the second CSM will be stored on the first CSM. The second CSM will get this information later on (when plugged in) from the first CSM.

1. Go to Dashboard → Advanced (TOOLS) → CSM Front IP Addresses;
2. In Figure 23, Fill out the current IP address of the device (or CSM that was already configured) in the 'Device Mgt. IP Address' field and Click 'Ping' to check whether the HiProvision PC can reach the device;
3. If the device is reachable, the IP information of the CSM already configured will be filled out. The IP information of the new CSM is filled out with zeros. Fill out or modify the fields of the new CSM, either CSM-1<IP fields> or CSM-2 <IP fields> with the new IP information.
 - ▶ '<CSM-1/CSM-2> Front IP address' of the device;
 - ▶ '<CSM-1/CSM-2> Subnet Mask' of the device;
 - ▶ '<CSM-1/CSM-2> Default Gateway Address' of the device.
4. Click Apply. Click Reboot and confirm the pop-up;
5. After the reboot of the node, the new IP address information will be configured.

e. Reset CSM Front IP Address to Factory Defaults

1. Go to Dashboard → Advanced (TOOLS) → CSM Front IP Addresses;
2. In Figure 23, Fill out the current IP address of the device that must be reset to factory defaults and click 'Ping' to check whether the HiProvision PC can reach the node;
3. If the node is reachable, the IP information of the configured CSM(s) will be filled out.
4. Click Factory Defaults and confirm the pop-up to reset the IP addresses in the CSM;
5. Click Reboot and confirm the pop-up;
6. After the reboot of the node, the new IP address information will be configured.

2.6.8 Device IP Address

a. General

is the IP address of the device, stored in the CSM and used by HiProvision to address the devices in the Dragon PTN network via DCN;

is default/factory in the Device IP Range 10.255.x.y/16 and based on the node number (=device ID);

is an IP address in the Device IP Range in the Entry Point;

can be changed, see paragraphs below.

CAUTION: When changing IP addresses or IP ranges, make sure that the Device IP Range of your network does not conflict with the CSM Front IP Addresses of your entry points for

this network. All these IP addresses and ranges can be verified in the Entry Point(s) in the Discovery Tile.

b. Set All Devices in Entire Network in the Custom Device IP Range

1. Click the  button;

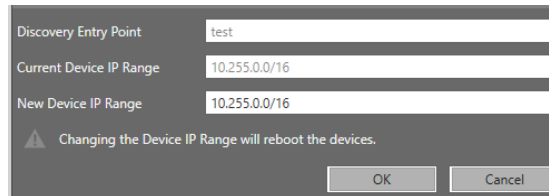



Figure 24 Change Device IP Range


2. The Current Device IP Range is shown. The New Device IP Range is by default filled out with the Current Device IP Range in the network. Fill out the new desired Device IP Range;
3. Click OK (no load action required!). CAUTION: All the devices in the network will reboot!
4. All the devices in the network will get a new device IP address in the configured Device IP Range. HiProvision will be able to communicate with these devices provided that HiProvision and the devices all reside in the same IP subnet.

c. Set New Devices in the Network in the Custom Device IP Range

If one or more devices, with an IP address in a wrong Device IP Range, are added to an existing operational network, these devices will be discovered by HiProvision but will remain grey in the network drawing. These new devices must get a new IP address in the same Device IP Range as the operational network.

1. Click the  button;
2. Both the Current Device IP Range and New Device IP Range field show the current Device IP range configured in the network.
3. Click OK (no load action required!);
4. The new devices will reboot and start up with an IP address in the New Device IP Range. The existing devices keep their IP addresses and will not reboot.
5. HiProvision will be able to communicate with these devices provided that HiProvision and the devices all reside in the same IP subnet.
6. Only new devices that are directly connected (= 1 hop) to the Dragon PTN network can be applied with the new Device IP Range. If you have added more than 1 hop, repeat previous steps for every hop until all hops have been discovered and assigned the correct IP address.


d. Factory Reset Device IP Range in the Entire Network




1. Click the  button and click OK to factory reset the Device IP Range to 10.255.x.y/16 for the entire network! CAUTION: All the devices in the network will reboot!

2.7 HiProvision: Network Database Configuration

The network database configuration can be done automatically via Dashboard → Discovery or manually via Dashboard → Network Hardware.

2.7.1 Automatic Configuration via Dashboard → Discovery

In the Discovery tab, select one or multiple network element(s) (or one or more of its children) and click the auto-creation icon  to create the selected devices/links automatically in the HiProvision database. The parameters of the auto-created network elements will have default values. Whether an element has already been created in the HiProvision database is indicated by following creation-status icon in the Configured column and the network visualization.

- ▶  = empty: network element not yet created in HiProvision database;
- ▶  = empty + blue: network element partially created in HiProvision database;
- ▶  = blue: network element fully created in HiProvision database.

Make sure that all the devices and links are fully created in the database. This can be easily verified by viewing the network drawing in the figure below: all creation-status icons must be blue.

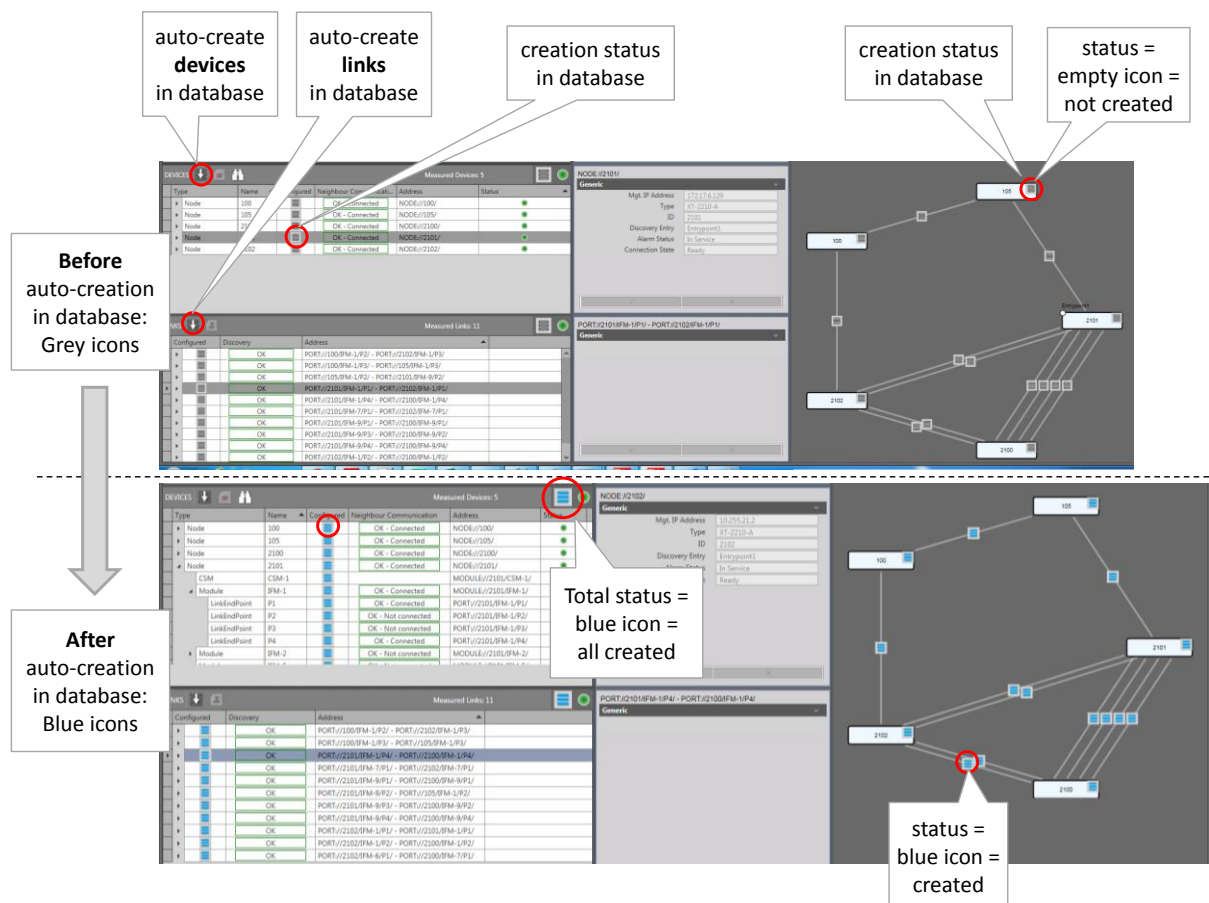


Figure 25 Discovery Tab: Auto-Creation of Network Elements in Database

2.7.2 Manual Configuration via Dashboard → Network Hardware

In this tab, device and links can be configured manually, see figure below:

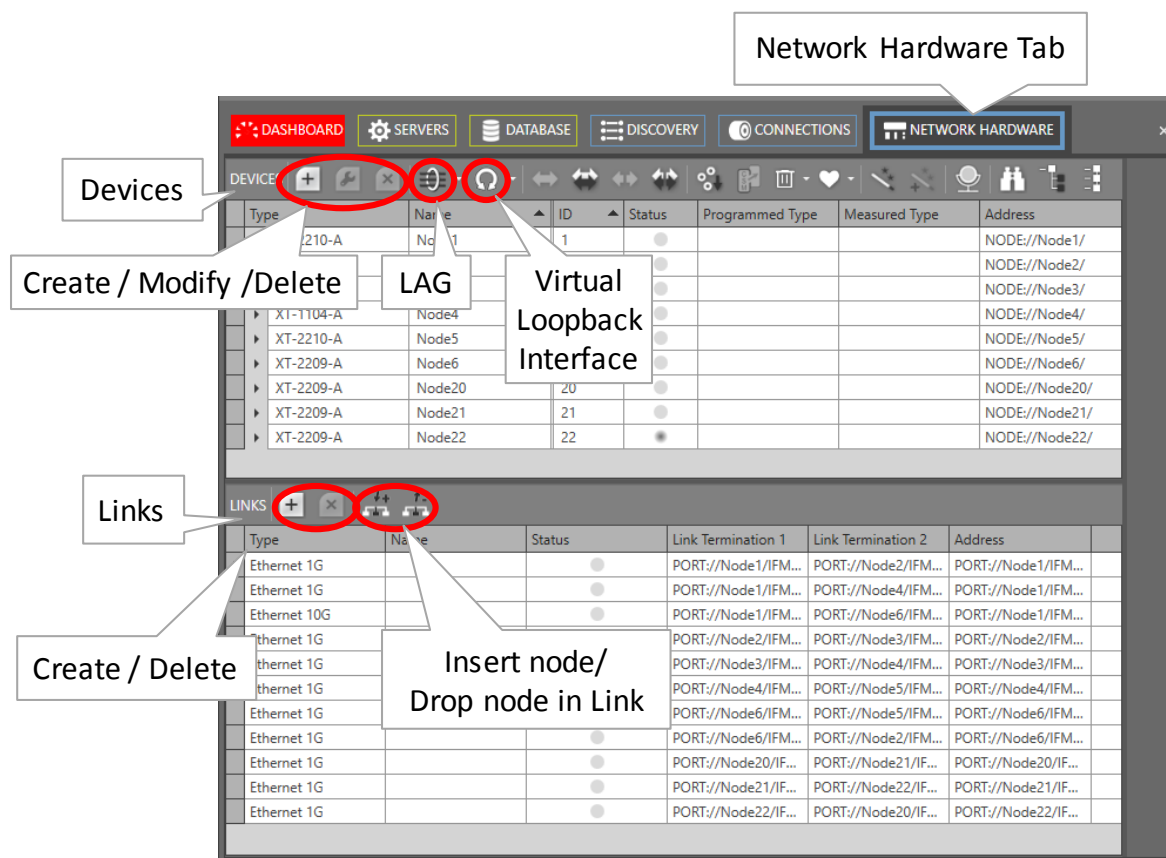


Figure 26 Manual Configuration Devices/Links

a. Devices:

- ▶ **+** Create:
 - ▶ Page1: Fill out the name (max. 128 characters), type and ID of the device or node. The ID must be the same as the node number configured on the NSM, see §2.1. It is possible to have External Devices types (=third party devices) in the list, see §1.
 - ▶ Page2: Select a module (Interface Module, CSM, PSU, NSM, ...) via the module selector (scroll the list for more pictures) and drag and drop it into a highlighted slot in the node. Only the allowed slots will highlight. It is not possible to drop a module in the wrong slot. Furthermore, it is possible to delete the dropped module if necessary.

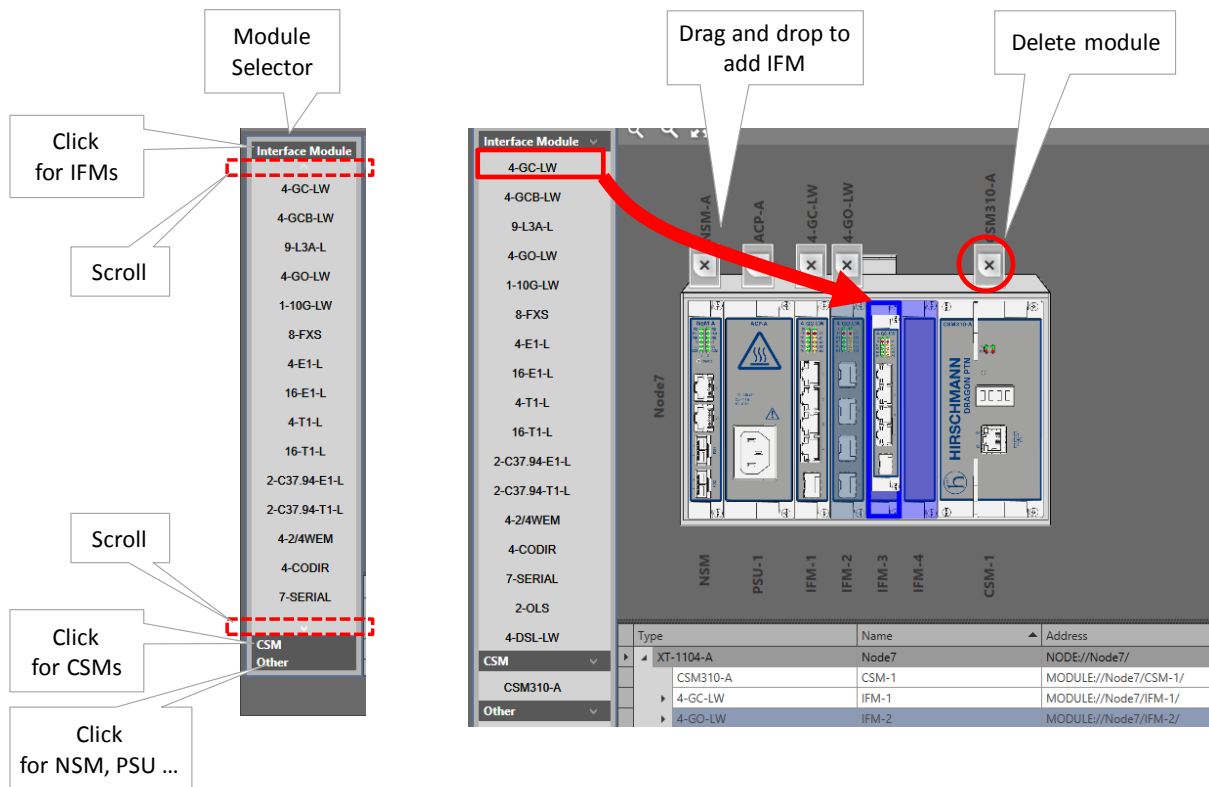




Figure 27 Drag and Drop Modules into Device Picture

- ▶ **Modify:** New modules can be dropped into the selected node or existing modules can be deleted from the selected node. Also the node name can be changed;
- ▶ **Delete:** the selected device or node can be deleted if its modules have been removed or deleted first. Its modules can be removed if they have been removed from links/tunnels/services first;
- ▶ **LAGs:** Create/Modify/Delete Link Aggregation Groups, see §35;

b. Links

- ▶ **Create:**
 - ▶ Select the link type of the WAN connections e.g. Ethernet 1G, Ethernet 10G, This type defines the bandwidth of the link, e.g. 1G, 10G, ... 'External E1 Links' must only be used between two E1 ports in PTN-2-OLS Interface Modules in a different node (when the PTN-2-OLS Interface Module is used in the converter/loopback mode, see Ref. [13] in Table 1). The 'External E1 Link' will be created beyond the Dragon PTN network and usually goes through an external network (e.g. SDH). An 'External E1 Link' will be indicated by a cloud icon . A 'Monitored Link' must be created between a Dragon PTN node and a third party or generic device (=non-Dragon PTN node) or between generic devices. This link type allows that the generic device is shown in all the network drawings and that the link towards these devices is monitored. When something goes wrong with the link, alarms will be raised. More info on Generic Devices in §33;
 - ▶ When having selected Ethernet 1G, nodes with 4-GC-LW/4-GCB-LW/4-GO-LW modules will have the Link Type checkbox checked and its node icon highlighted

(=white color) in the network drawing, if there are still some WAN ports available on the node. If the node does not highlight (=grey color), set some extra ports to WAN first via Dashboard → Network Hardware → Network Settings Wizard button =  → Port Mode;

- ▶ When having selected Ethernet 10G, nodes with available WAN ports on 1-10G-LW modules will have the Link Type checkbox checked and a white colored node icon in the network drawing. If the node does not color white and you need a WAN port on that node, plug in extra modules or set extra ports to WAN via Dashboard → Network Hardware → Network Settings Wizard button =  → Port Mode;
- ▶ Create a link between two white nodes by clicking the first node, clicking an available (=brown) WAN port and do the same for the second node, a port selection example can also be found in Figure 58.

NOTE: The Link Capacity can be tuned later on via §3.10.

NOTE: An additional Name and Info field can be filled out for each created link via Network Hardware → Links → Selected Link → Generic. The Info data, if filled out, will be displayed when hovering the link in the network drawings, e.g. in the network tile.

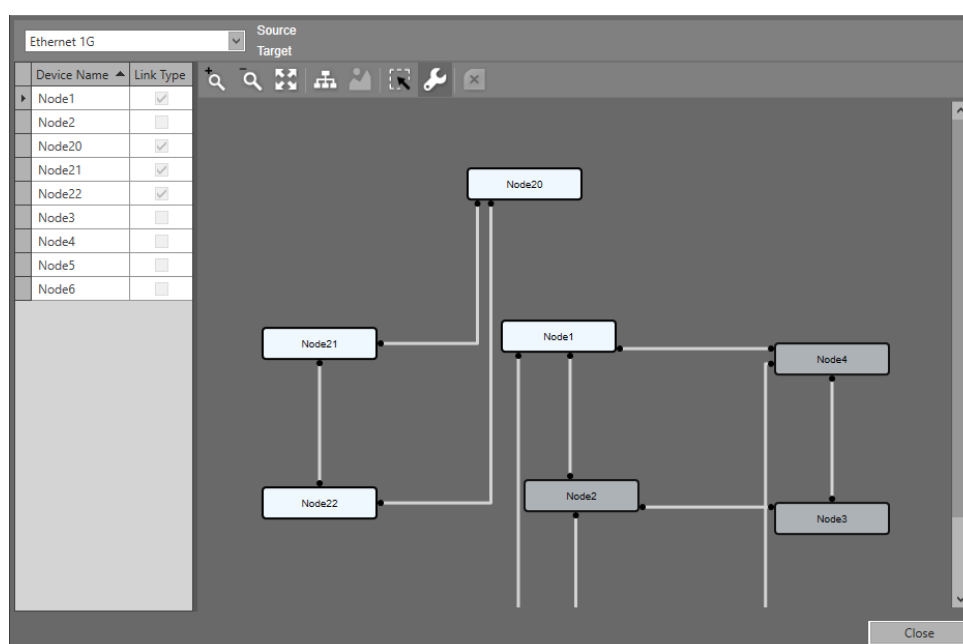




Figure 28 Create Links

- ▶  Delete: the selected link can be deleted if it is not in use anymore. A link can be selected by clicking the link;
- ▶  Insert Node: Inserts a new LSR node on a link in between two existing nodes without removing the configured tunnels and services on the existing link. When loading the changes of this wizard to the network, one of the two existing nodes and the new node will be reprogrammed by HiProvision. Follow the steps below to insert a node between two links in the live network.

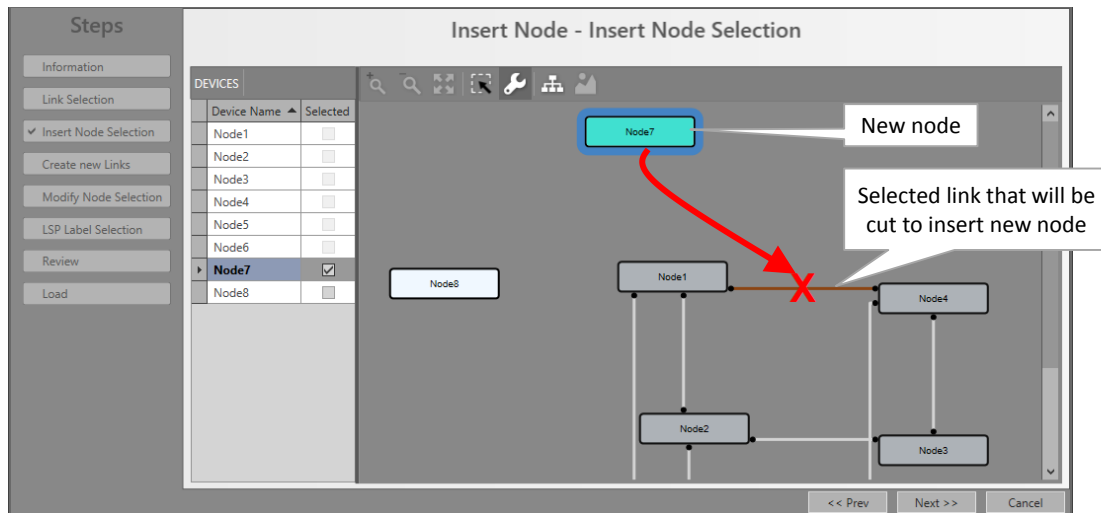



Figure 29 Insert Node

- ▶ **Hardware:** Power up and install the new node physically (do not insert it yet into the network), assign a node number, clear the CSM(s) and provide the necessary WAN ports (number & type);
- ▶ **Dashboard → Network Hardware:** Create the new node & configure its modules;
- ▶ **Insert Node Wizard:**
 - ▶ Prerequisites to insert: see §2.7.3;
 - ▶ Link Selection: Select the link (by clicking it) on which the node must be inserted;
 - ▶ Insert Node Selection: Select the new node that must be inserted in the red-crossed link. This red-crossed link will disappear afterwards;
 - ▶ Create New Links: Create new links between the new (cyan) and the two existing nodes (white) by clicking the nodes and selecting the link ports;
 - ▶ Modify Node Selection: One of the two existing nodes (white) must be reprogrammed by HiProvision (=will get new LSP labels). Select one of the two nodes that can be reprogrammed. If it does not matter which one, select just one of them;
 - ▶ LSP Label Selection: Shows the new LSP labels used to insert the new node. If desired, the labels can be modified by clicking the cell and changing the value;
 - ▶ Review: if ok, click Finish. The configuration load manager will be invoked. Do NOT load yet, it won't be possible as the new node is not reachable yet.
- ▶ **Hardware:** Re-wire your WAN cables (= insert the new node physically);
- ▶ **Dashboard → Discovery (see §2.6):**
 - ▶ Wait until the Discovery is ready again, verify the new situation;
 - ▶ Clear both Neighbor Approvements for the involved link;
 - ▶ Wait until the Discovery is ready again, verify the new situation;
 - ▶ Approve Link for both involved links;
- ▶ **Dashboard → Network Hardware:**
 - ▶ Connect to the new node;
 - ▶ Load to the network (see also §5).

-  **Drop Node:** drops (or removes) an LSR node between two existing nodes without removing the configured tunnels and services on the existing link. Follow the steps below to remove a node between two links in the live network.

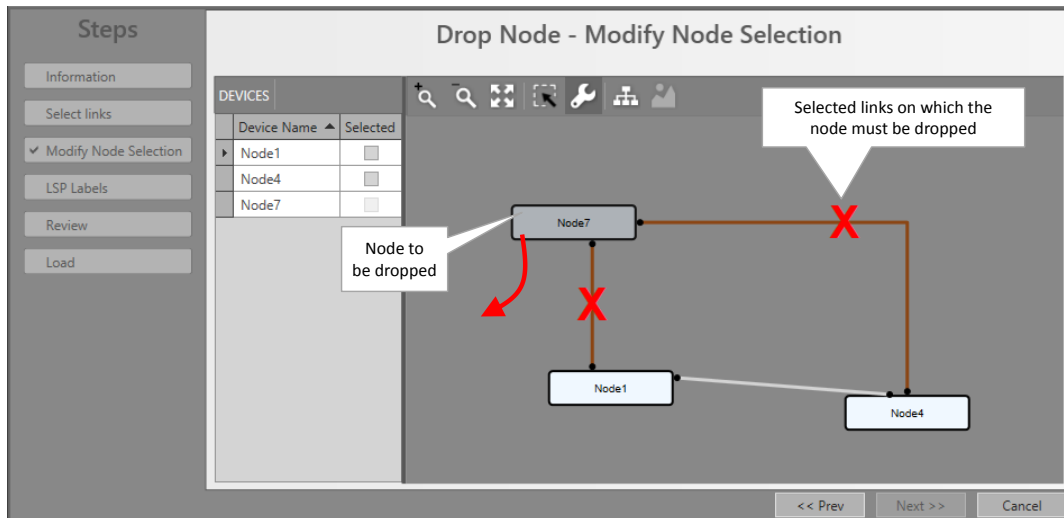


Figure 30 Drop Node

- **Drop Node Wizard:**
 - Prerequisites to drop: see §2.7.3;
 - Select Links: Select two links adjacent to the node that must be dropped;
 - Modify Node Selection: One of the two existing nodes (white) must be reprogrammed by HiProvision (=will get new LSP labels). Select one of the two nodes that can be reprogrammed. If it does not matter which one, select just one of them;
 - LSP Label Selection (read only): shows the resulting LSP labels after dropping the node;
 - Review: if ok, click Finish. The configuration load manager will be invoked. Do NOT load yet;
- Dashboard → Network Hardware: Optional: Only delete the node including its modules when the node is not used anymore afterwards or completely isolated;
- Hardware: Re-wire your WAN cables (= remove the node between the two links);
- Dashboard → Discovery (see §2.6):
 - Wait until the Discovery is ready again, verify the new situation;
 - Clear both Neighbor Approvements for the involved link;
 - Wait until the Discovery is ready again, verify the new situation;
 - Approve Link for the involved link;
- Dashboard → Network Hardware: Load to the network (see also §5);

2.7.3 Insert/Drop Prerequisites

a. Insert Prerequisites

If nothing can be inserted (everything is greyed out) in the wizard, one of the prerequisites below is NOT met:

At least one node must be 'insert-ready';

A node is 'insert-ready' when:

- ▶ it has been created in HiProvision having the necessary Interface Modules with WAN ports configured;
- ▶ it has at least 2 free WAN ports of the same type as the link-to-cut, e.g. 2 free 10G ports are required for a 10G link;
- ▶ it fulfils one of the following:
 - ▶ it is a new node: unlinked or isolated node;
 - ▶ it is an existing node: an already linked node in the network not part of any tunnel on the link-to-cut.

b. Drop Prerequisites

If nothing can be dropped (everything is greyed out) in the wizard, one of the prerequisites below is NOT met:

A least one node must be 'drop-ready';

A node is 'drop-ready' when:

- ▶ it has at least 2 links;
- ▶ its 2 adjacent links (link1 and link2), from which the node will be dropped, must have the same link type, e.g. both Ethernet 10G;
- ▶ it is an LSR node for all tunnels it belongs to;
- ▶ link1 and link2 have the same set of tunnels.

2.8 HiProvision: Check Network Hardware

Prerequisite: HiProvision is offline: grey status bullets in Network Hardware tab;

The created network elements can be verified in the database via the Dashboard → Configuration → Network Hardware. See figure below:

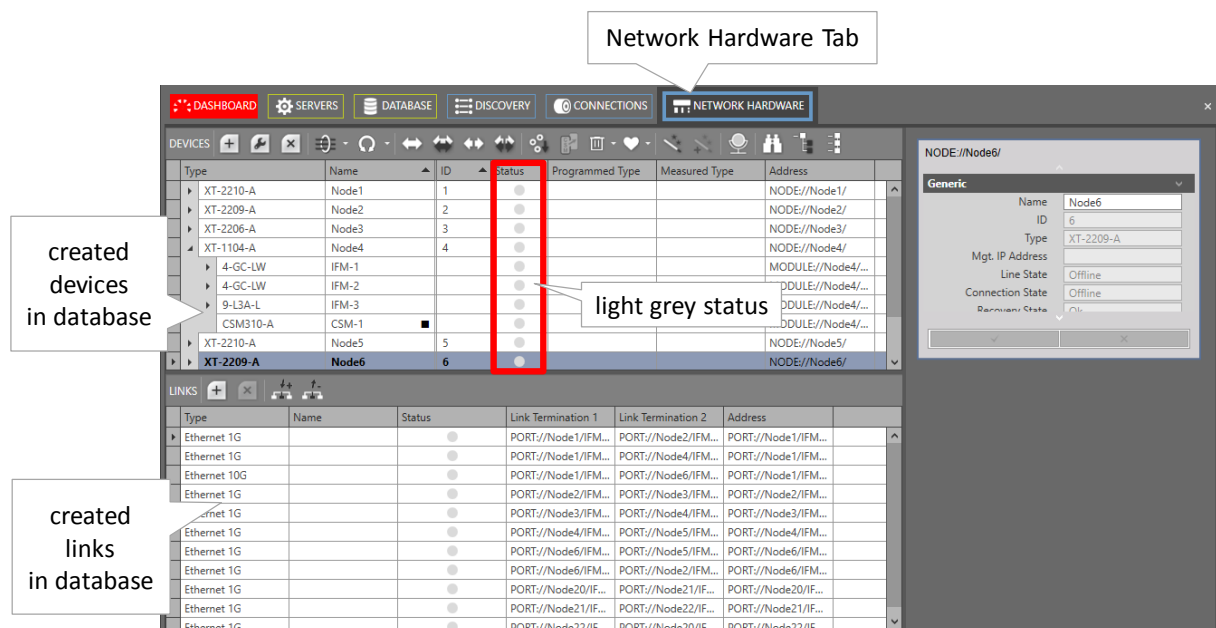



Figure 31 Network Hardware Tab: Created Network Elements

The purpose is to go online with HiProvision into the network in a controlled way, to make the network elements reachable for configuration. It is possible to go online with only one, some or all network elements together. When going online, the status bullets will be colored. The tables below show the meaning of the status bullets.

Table 9 Status Bullets: Devices

Bullet Color	Description
Light Grey	Not connected yet, network element is offline.
Dark Grey	Connected, device is unreachable (e.g. broken cable, missing device...)
Green	Connected, device is online/reachable and OK, device has no alarms.
Other color	Connected, device is online/reachable but has an alarm. The bullet color indicates the alarm color or severity. See §4.2 for the meaning of the alarm color.





Table 10 Status Bullets: Links

Bullet Color	Description
Light Grey	At least one of the two nodes to which the link is connected, is offline or not connected yet.
Green	Link is up and running, everything OK.
Red	Link is broken - Connected, device is unreachable (e.g. broken cable, missing device...) or - Connected, device is online/reachable but has an alarm on that link port. The bullet color indicates the alarm color or severity. See §4.2 for the meaning of the alarm color.
 + <colored bullet>	The link is an 'External E1 Link', the meaning of the color bullet is the same as described above.

CAUTION:

Make sure to have purchased a voucher for each node in your network before going online. A license pack is required to go online via the connect buttons below! See also §20.

HiProvision can go online (offline) via the connect (disconnect) buttons. See figure below:

-  : Go online, connect to all devices at once;
-  : Go online, Connect to all the selected devices (multiple via the CTRL and SHIFT keys);
-  : Go offline, Disconnect all devices at once;
-  : Go offline, Disconnect the selected devices;

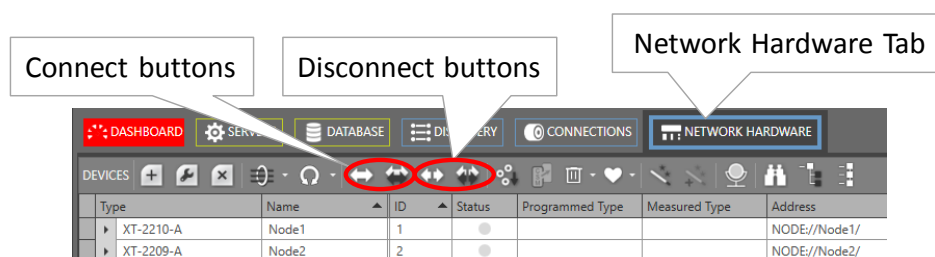


Figure 32 Connect/Disconnect Buttons

Click one of the connect buttons to go online. As a result, if this is the first connect ever and no database configuration was loaded into the network before, configuration alarms will be generated. These alarms are raised because there is a mismatch between what is measured and what is configured in the nodes. Loading the configuration into the network will clean up the mismatches and as a result solve the alarms.

The Alarms tile in the dashboard will turn dark red (=critical alarms). The tile color is the same as the alarm color of the alarm with the highest severity. All these alarms can be viewed more in detail via clicking the Alarms tile. See figures below.

Type	Name	ID	Status	Programmed Type	Measured Type	Address
XT-2210-A	Node1	1	Red			NODE://Node1/
XT-2209-A	Node2	2	Red			NODE://Node2/
XT-2209-A	Node3	3	Red			NODE://Node3/
XT-2210-A	Node4	4	Red			NODE://Node4/
XT-2210-A	Node5	5	Red			NODE://Node5/
XT-2209-A	Node6	6	Red			NODE://Node6/
XT-2209-A	Node20	20	Red			NODE://Node20/
XT-2209-A	Node21	21	Red			NODE://Node21/
XT-2209-A	Node22	22	Red			NODE://Node22/

Figure 33 Connection Status After Connect

Status	Severity	Created	Last Occurrence	Address ID	Address Name	Code	Color
Acknowledged	Minor	14/09/2017 10:14:13	14/09/2017 12:56:08	PORT://1/BFM-2/P7/	PORT://1/BFM-2/P7/	27.18	Yellow
Acknowledged	Minor	14/09/2017 10:14:13	14/09/2017 12:56:08	PORT://1/BFM-2/P6/	PORT://1/BFM-2/P6/	27.18	Yellow
Acknowledged	Minor	14/09/2017 10:14:13	14/09/2017 12:56:07	PORT://1/BFM-2/P5/	PORT://1/BFM-2/P5/	27.18	Yellow
Acknowledged	Minor	14/09/2017 10:14:12	14/09/2017 12:56:07	PORT://1/BFM-2/P4/	PORT://1/BFM-2/P4/	27.18	Yellow
Acknowledged	Minor	14/09/2017 10:14:12	14/09/2017 12:56:07	PORT://1/BFM-2/P3/	PORT://1/BFM-2/P3/	27.18	Yellow
Acknowledged	Minor	14/09/2017 10:16:27	14/09/2017 12:56:06	PORT://1/BFM-2/P2/	PORT://1/BFM-2/P2/	27.18	Yellow
Acknowledged	Minor	14/09/2017 10:14:11	14/09/2017 12:56:06	PORT://1/BFM-2/P1/	PORT://1/BFM-2/P1/	27.18	Yellow
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:58:08	MODULE://2/BFM-10/	MODULE://2/BFM-10/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:58:08	MODULE://2/BFM-9/	MODULE://2/BFM-9/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:58:08	MODULE://2/BFM-8/	MODULE://2/BFM-8/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:58:08	MODULE://2/BFM-7/	MODULE://2/BFM-7/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:58:08	MODULE://2/BFM-5/	MODULE://2/BFM-5/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:58:08	MODULE://2/BFM-4/	MODULE://2/BFM-4/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:58:08	MODULE://2/BFM-3/	MODULE://2/BFM-3/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:17	14/09/2017 11:57:39	MODULE://2/BFM-6/	MODULE://2/BFM-6/	5.7	Red
Acknowledged	Major	13/09/2017 17:08:45	14/09/2017 11:57:35	MODULE://1/BFM-10/	MODULE://1/BFM-10/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:45	14/09/2017 11:57:35	MODULE://1/BFM-9/	MODULE://1/BFM-9/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:45	14/09/2017 11:57:35	MODULE://1/BFM-8/	MODULE://1/BFM-8/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:57:35	MODULE://1/BFM-7/	MODULE://1/BFM-7/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:57:35	MODULE://1/BFM-5/	MODULE://1/BFM-5/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:57:35	MODULE://1/BFM-4/	MODULE://1/BFM-4/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:44	14/09/2017 11:57:35	MODULE://1/BFM-3/	MODULE://1/BFM-3/	5.1	Red
Acknowledged	Major	13/09/2017 17:08:28	14/09/2017 11:57:18	MODULE://1/BFM-6/	MODULE://1/BFM-6/	5.7	Red
Acknowledged	Minor	13/09/2017 17:08:09	14/09/2017 10:10:32	MODULE://3/PSU-1/	MODULE://3/PSU-1/	5.2	Yellow
Acknowledged	Major	13/09/2017 17:06:52	14/09/2017 10:08:56	MODULE://4/BFM-4/	MODULE://4/BFM-4/	5.7	Red


Figure 34 Configuration Alarms

An appearance of alarms means that HiProvision is online. The alarms itself indicate for example mismatch alarms (= mismatches between database and network) and status alarms (e.g. temperature too high, ...). There is no configuration yet in the network because it has not been loaded yet into the network so far (except for the discovery expected values).

NOTE: More information on alarm handling, severity and colors can be found in §4.2.

2.9 HiProvision: Load Configuration into the Network

Loading the database configuration into the network will configure the live network and clean up all the mismatch alarms between database and network. As a result, the red status bullets will turn into green bullets.

In the Network Hardware Tab, click the load icon  to start the configuration load manager. See §5 for an overview of this tool.

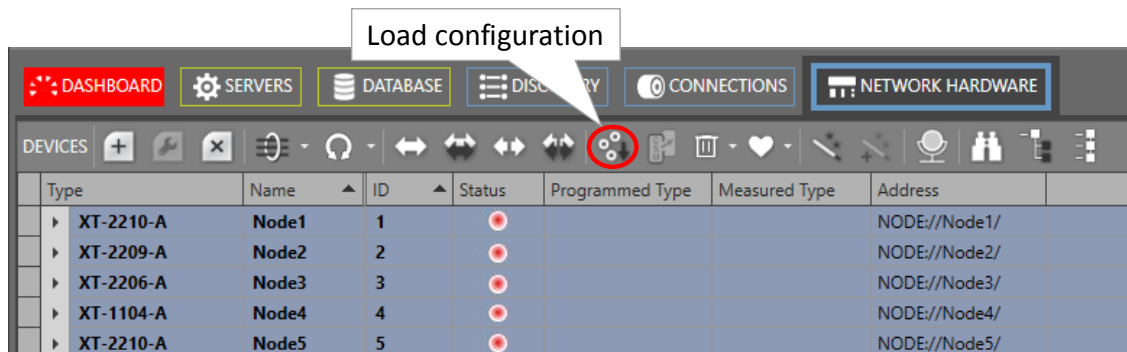


Figure 35 Load Configuration Into the Network

After everything has been loaded successfully, the status bullets in the Network Hardware tab should be green. If not, solve the mismatches. Next, load again. Repeat these steps until all bullets are green.

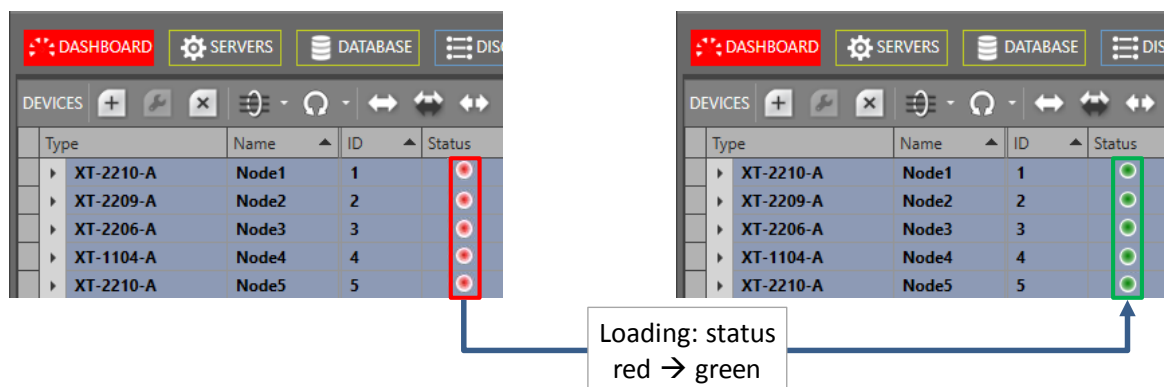


Figure 36 Status Color Change After Successful Loading

2.10 HiProvision: Set the Network Timing via an NTP Server

2.10.1 General

It is strongly advised to use an NTP Server. Do you have an NTP Server?

No:

- ▶ I want to use NTP:
 - ▶ Configure the HiProvision server PC as an NTP Server first: see §2.10.2;
 - ▶ Next, configure this NTP server in HiProvision (and backup NTP Server): see §2.10.3;

- I do not want to use NTP: see §2.10.4;

Yes:

- Configure this NTP server in HiProvision: see §2.10.3;

NOTE: NTP server is used for network timings that need seconds/milliseconds accuracy whereas IEEE 1588 (see §14) is used for applications that need micro/nanoseconds accuracy.

2.10.2 Configure HiProvision Server PC as NTP Server

If you don't have an external NTP Server and you still want to use NTP, it is possible to configure the HiProvision server as NTP Server as listed below:

Open the Windows Registry Editor;

Set following registry values:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config:
 - AnnounceFlags = 0x5
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer:
 - Enabled = 1

Close the Windows Registry Editor;


Open (as Administrator) a command prompt on the HiProvision Server PC;

Restart your time service via entering the command:

- net stop w32time && net start w32time

2.10.3 Configure NTP Server/Backup NTP Server in HiProvision

To make sure all the nodes in the Dragon PTN network use the same network timing (e.g. use of timestamps for logging etc...), an NTP server must be used. By default, no central network timing or NTP server is configured.

The network settings wizard allows to easily set the IP address of an NTP server. Click the Network Settings Wizard button , see figure below:

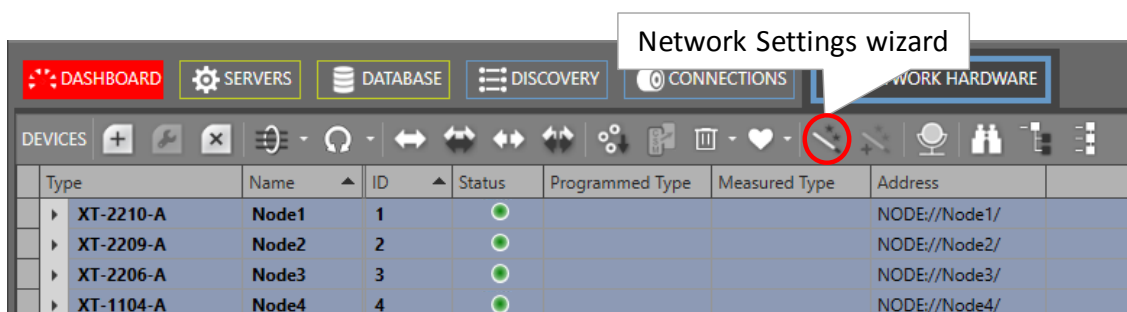






Figure 37 Network Settings Wizard Button

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

Information: Click Next>>;

Selection: select Time/Date Mode;

Time/Date Mode:

- ▶ Set Time/Date Mode
 - ▶ NTP (=default): Use this value. The NTP server will regularly update the Dragon PTN network timings with new timestamps;
 - ▶ Manual: see §2.10.4 below.
- ▶ NTP Server IP address is filled out with the HiProvision Server IP address. Overwrite this IP address (for all CSMs) with the IP address of an NTP server in your network. You can select each CSM individually or select them all at once via the  Multiple Settings Mode. Click  Apply after selecting the CSMs and filling out the IP address. See figure below;
- ▶ Backup NTP Server IP address:
 - ▶ 0.0.0.0 (=default): No backup NTP Server is used;
 - ▶ Custom IP address: Overwrite this IP address (for all CSMs) with the IP address of a backup NTP server in your network. You can select each CSM individually or select them all at once via the  Multiple Settings Mode. Click  Apply after selecting the CSMs and filling out the IP address. See figure below;

Review: if ok, click Finish. The configuration load manager will be invoked, see §5;

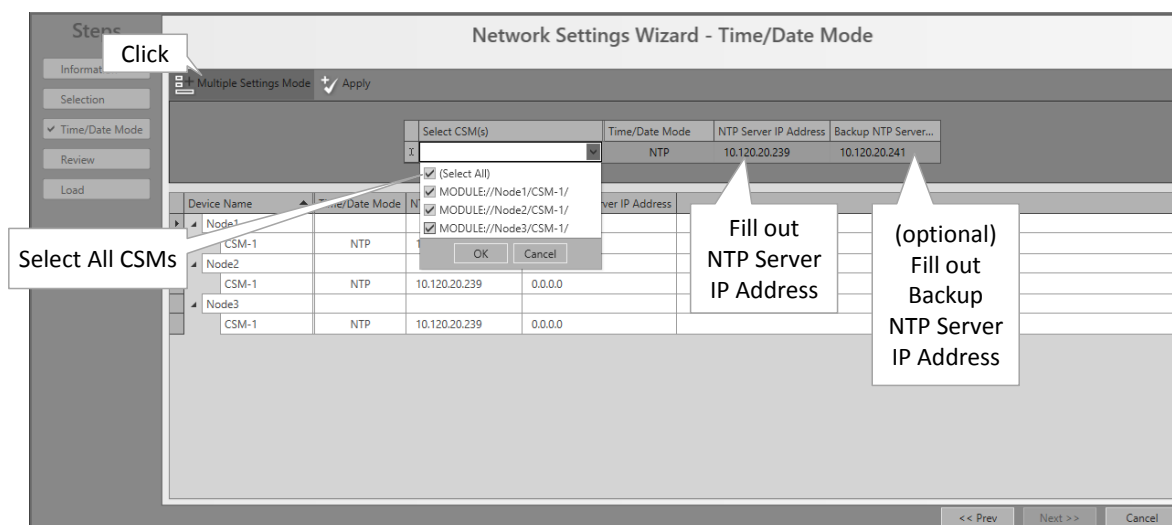


Figure 38 NTP Server IP Address

After loading the NTP configuration into the Network, the configured NTP settings are also visible in the Dashboard → Network Hardware tile → CSM → Specific:

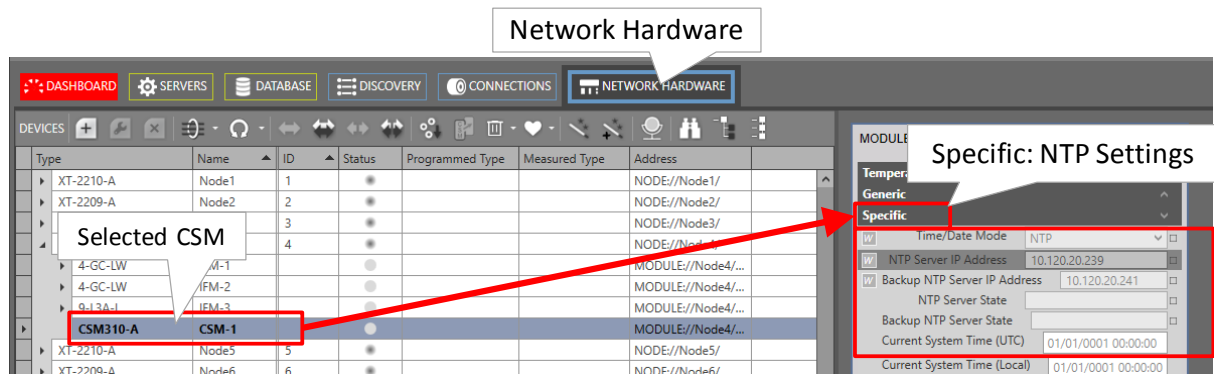


Figure 39 CSM NTP Settings


2.10.4 Manual Setting (=No NTP Server)

If you do not have an NTP server or don't want to use one, it is also possible to set Time/Date Mode to 'Manual' (Figure 38). As a result the HiProvision Server time and date will be pushed into the network only once and only when the load action occurs in this Time/Date wizard, just after clicking the Finish button.

2.11 HiProvision: 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 Interface Modules that support WAN ports (see §32) 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 Interface Modules together, without having to open each Interface Module 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 Interface Modules that support WAN ports (see §32) are WAN ports. The ports with a connected WAN link, are indicated by . These ports cannot be adapted anymore in this wizard. If all the other ports must be set to LAN, click the  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, see §5;

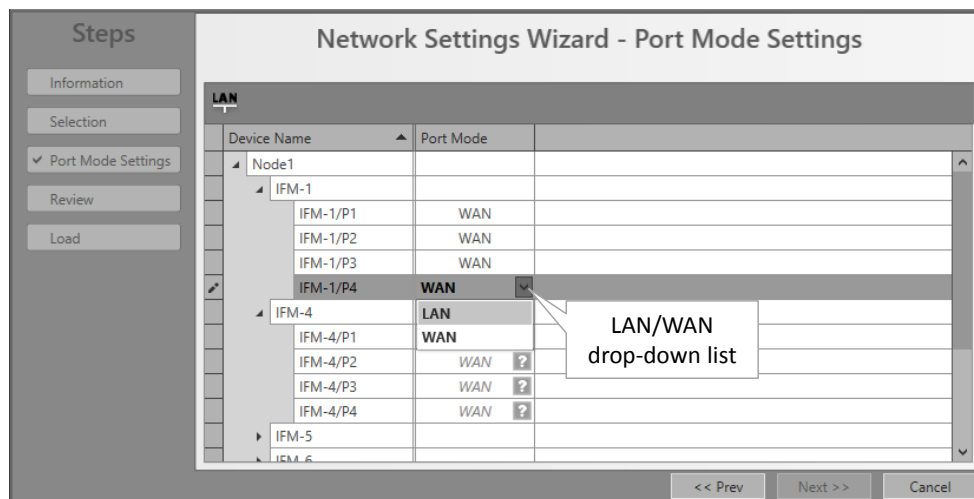


Figure 40 LAN/WAN Settings

2.12 HiProvision: Create MPLS-TP Tunnel(s)

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

2.12.1 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;

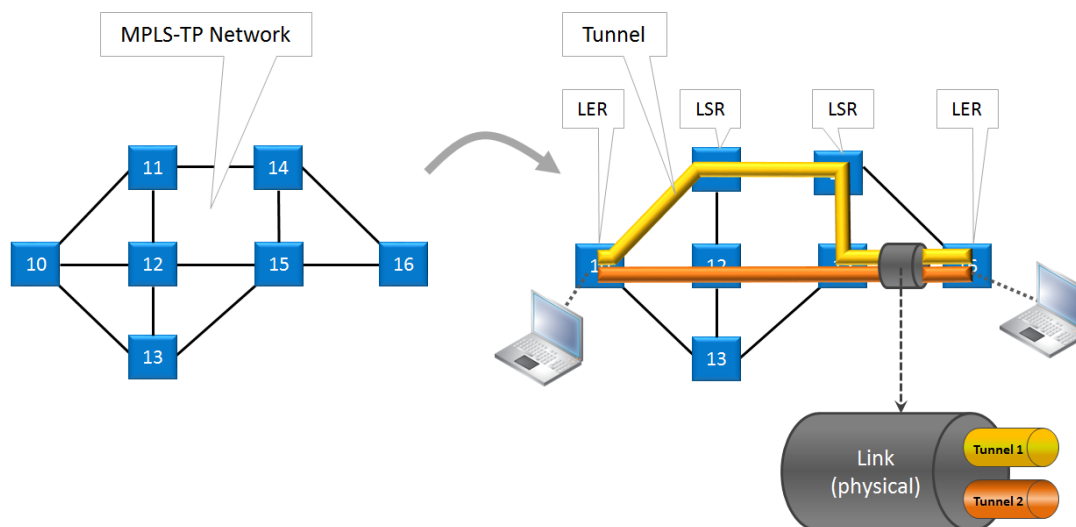


Figure 41 Tunnel Creation

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 11 Tunnel Topologies and Protection

Tunnel Topology	Protection
Point-to-point	Optional
Multipoint	Optional
Logical Ring	Always, included automatically via RPL (=Ring Protection Link)
Subring	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' between two E1 ports of two PTN-2-OLS Interface Modules (only when the PTN-2-OLS is used in converter/loopback mode, see Ref. [13] 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 §10.5.2.

The number of protected tunnels through a link depends on the selected DCN bandwidth profile for that link, see §3.9.2.

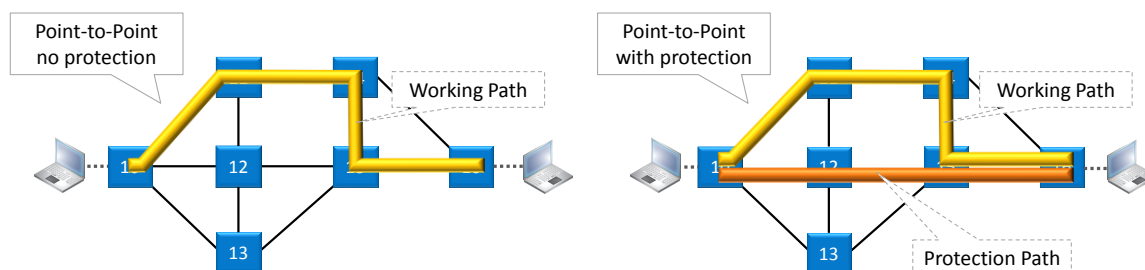


Figure 42 Point-to-Point Tunnels

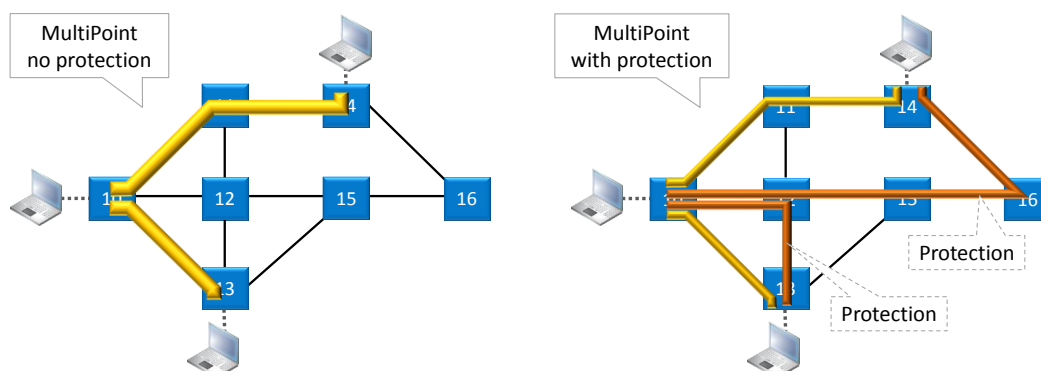


Figure 43 MultiPoint Tunnels

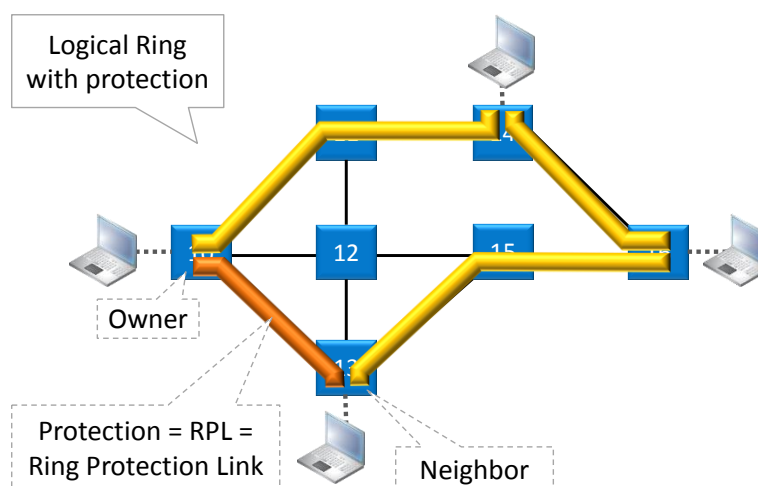


Figure 44 Logical Ring Tunnel

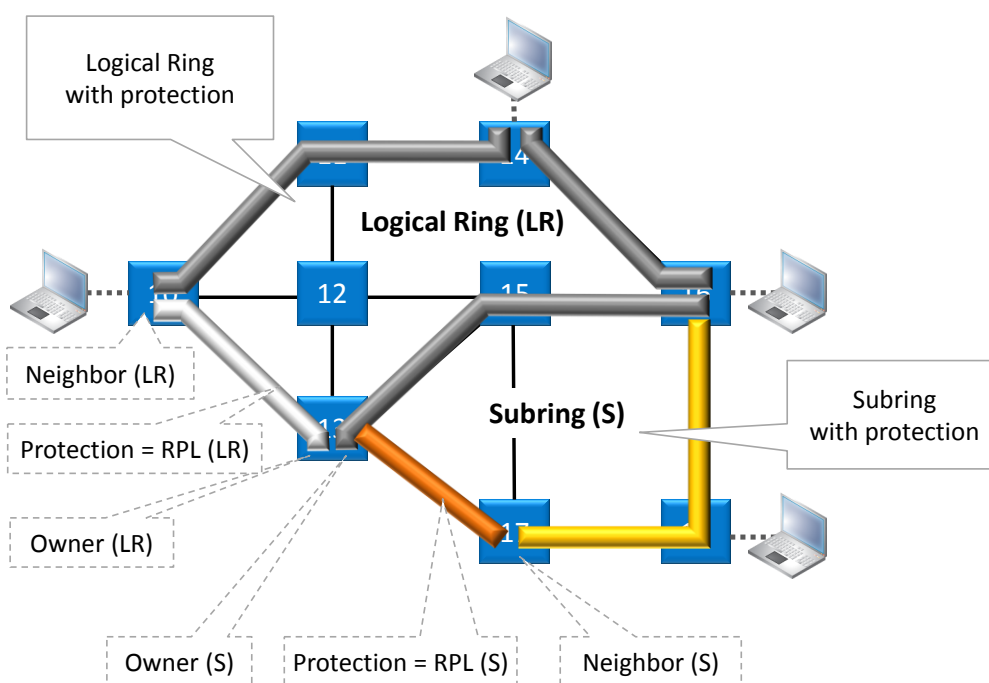



Figure 45 Subring Tunnel

2.12.2 Tunnel Creation

NOTE: If needed, a tunnel can be modified later on as described in §2.12.3.

NOTE: If you want to create a Subring tunnel, read §22 first.

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

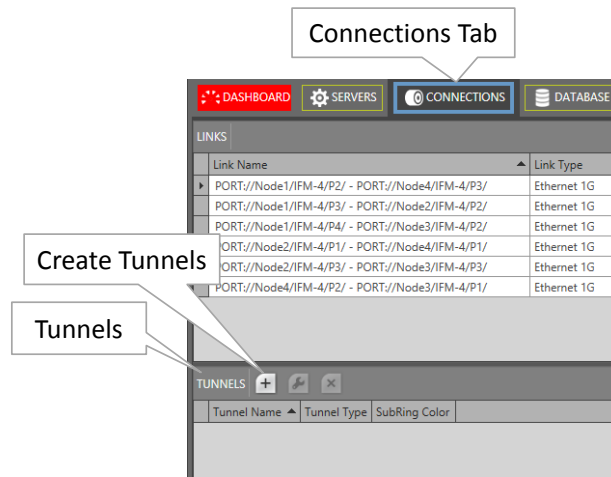


Figure 46 Create Tunnels

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 §2.12.1) 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 Subrings: Select all the devices or nodes of the subring including the interconnection nodes on the Logical Ring.
- Subring Interconnection nodes: see §22;
- 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 / .

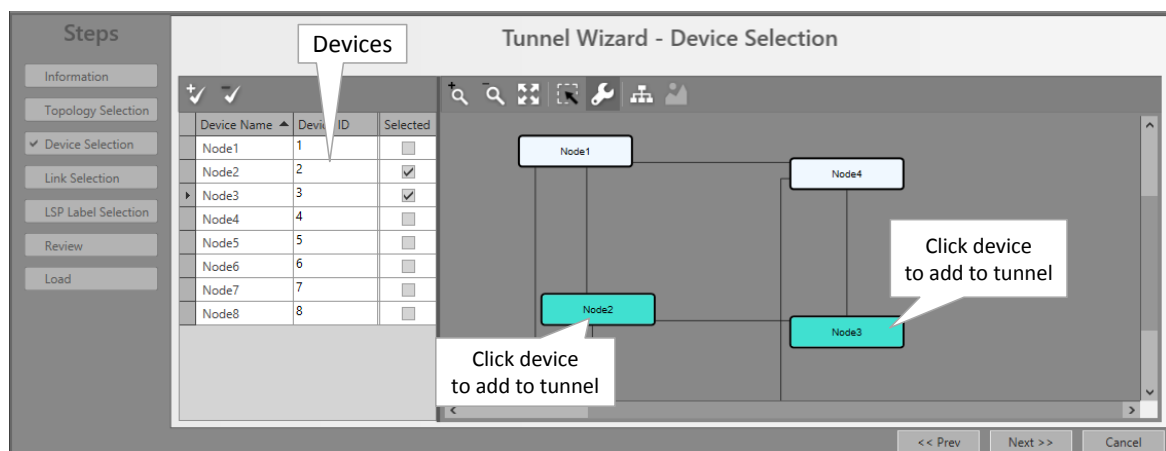




Figure 47 Tunnel - Device Selection

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  / .

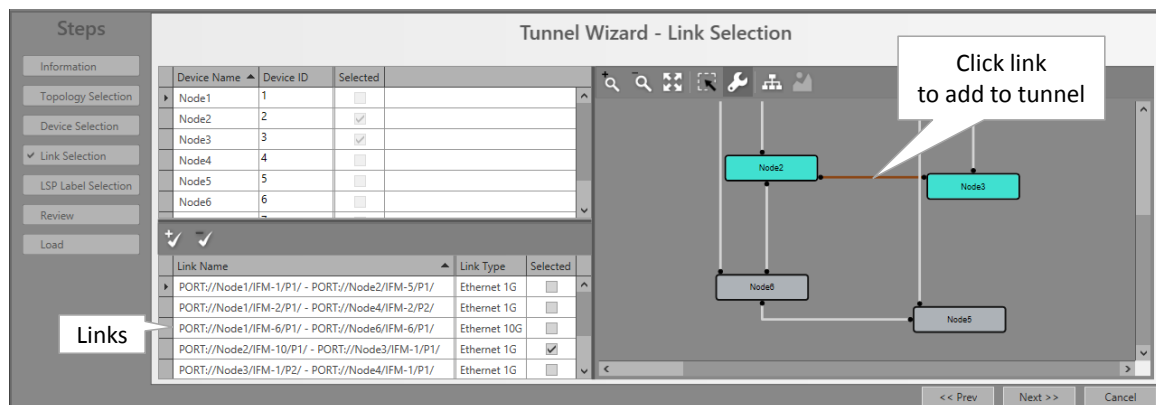


Figure 48 Tunnel - Link Selection

- 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 49 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 (future support): Use HQoS / HQoS Application Priority, Future support of HQoS, click Next >>.

Figure 50 Tunnel HQos (Future Support)


► Protection Parameters :

Device Name	Selected
Node1	<input type="checkbox"/>
Node4	<input type="checkbox"/>
Node2	<input type="checkbox"/>
Node3	<input type="checkbox"/>

Device Name	Selected
Node1	<input type="checkbox"/>
Node4	<input type="checkbox"/>
Node2	<input type="checkbox"/>
Node3	<input type="checkbox"/>

Figure 51 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. See §2.12 for more info on working/protection path.

- ▶ 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[5-500]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, see example Figure 93;
- ▶ 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.
- ▶ 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 53.

- Point-to-Point
- Multipoint

Sharing not relevant

Link	Forward Label	Reverse Label
NODE://Node1/ ==> NODE://Node2/		
PORT://Node1/IFM-4/P2/ - PORT://Node4/IFM-4/P3/ ?	200009	200010
PORT://Node2/IFM-4/P1/ - PORT://Node4/IFM-4/P1/ ?	200011	200012
NODE://Node1/ ==> NODE://Node2/		
PORT://Node1/IFM-4/P3/ - PORT://Node2/IFM-4/P2/	200007	200008
NODE://Node1/ ==> NODE://Node3/		
PORT://Node1/IFM-4/P4/ - PORT://Node3/IFM-4/P2/	200005	200006

- Logical Ring
- Subring

(Advised)
Use Shared LSP
→ Performant

Link	Forward Label	Reverse Label
NODE://Node1/ ==> NODE://Node4/	TUNNEL://LogicalRing1/ [5.0 ms]	
○ Create new [5.0 ms]		
● Share with TUNNEL://LogicalRing1/ [5.0 ms]		
PORT://Node1/IFM-4/P2/ - PORT://Node4/IFM-4/P3/	200013	200014
NODE://Node2/ ==> NODE://Node1/	Create new [5.0 ms]	
● Create new [5.0 ms]		
PORT://Node1/IFM-4/P3/ - PORT://Node2/IFM-4/P2/	200053	200054
NODE://Node4/ ==> NODE://Node2/	TUNNEL://LogicalRing1/ and 1 more tunnel(s) [5.0 ms]	
○ Create new [5.0 ms]		
PORT://Node2/IFM-4/P1/ - PORT://Node4/IFM-4/P1/	200051	200052
● Share with TUNNEL://LogicalRing1/ and 1 more tunnel(s) [5.0 ms]		
PORT://Node2/IFM-4/P1/ - PORT://Node4/IFM-4/P1/	200015	

Reuse (share) of resources

Link	Forward Label	Reverse Label
NODE://Node1/ ==> NODE://Node4/		
PORT://Node1/IFM-4/P2/ - PORT://Node4/IFM-4/P3/	200049	200050
NODE://Node2/ ==> NODE://Node1/		
PORT://Node1/IFM-4/P3/ - PORT://Node2/IFM-4/P2/	200053	200054
NODE://Node4/ ==> NODE://Node2/		
PORT://Node2/IFM-4/P1/ - PORT://Node4/IFM-4/P1/	200051	200052

Non-shared LSP
→ Less performant

No reuse of resources

Figure 52 Share LSP: Shared/Non-Shared LSPs

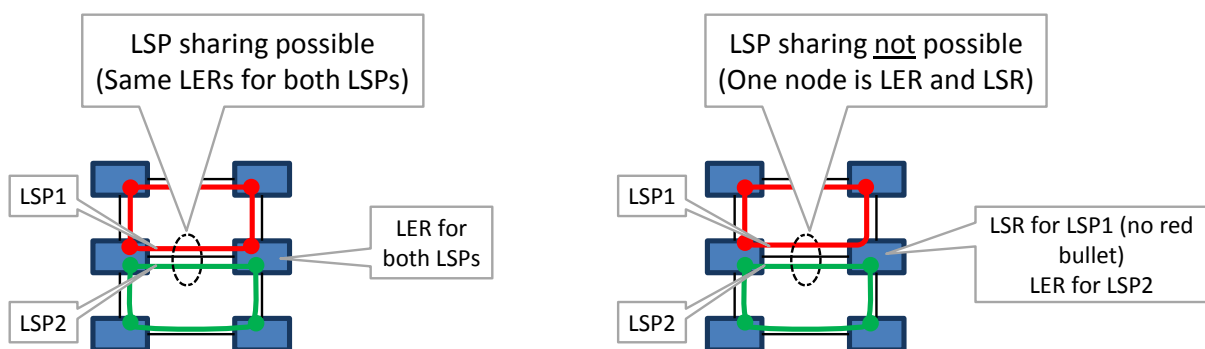


Figure 53 LSP Sharing Possible?

Review: if ok, click Finish, the configuration load manager will be invoked, see §5.

2.12.3 Tunnel Modification

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

Tunnel Name, Ring Priority (if LSP sharing is used).

2.12.4 Monitor Protected Tunnel

The working and protection path in a protected tunnel are visualized in §4.6.5.

2.12.5 Reporting

Tunnel Reporting information is available via the Reporting Engine Add-on, see §29.4.

2.13 HiProvision: Service(s) between Customer Applications

2.13.1 Service Creation

NOTE: The amount of services that can be created in a node is determined by the amount of available VFIs (= Virtual Forwarding Instance) in the CSM. The CSM310-A has maximum 64 VFIs available. Each created service in a node consumes 1 VFI in that node. With 2 CSMs in the node (CSM redundancy), the total remains 64 VFIs for the entire node.

NOTE: For Optical Low Speed Serial services, see §2.13.2.

NOTE: If needed, a service can be modified later on as described in §2.13.3.

Prerequisite:

At least one tunnel must have been created;

Before creating the service, it is always interesting to verify the bandwidth already configured through the WAN links and tunnels of your network, see §3.7.

When creating a Circuit Emulation Service (=CES, see further):

- ▶ Optimise jitter buffer (port level): set to 'false' when using SyncE (see §13) and internal clocking together. In any other case, set to 'true' (via Dashboard → Network Hardware → E1/T1/C37.94/Serial/2-4WEM ports);

CAUTION: If port parameter 'Optimise Jitter Buffer Reset' = 'true' (=default) in HiProvision, the jitter buffer will be reset for optimal processing 15 or 120 (*) seconds after one of the events below occur. This reset will cause a minimal loss of data:

- CES service creation/modification;
 - CES service recovery after a possible service failure;
 - Modifying clocking port parameters (clock source, bundle id for E1/T1) in HiProvision;
- (*): 120 seconds for PTN-16-E1-L/PTN-16-T1-L Interface Modules and 15 seconds for the other Interface Modules

- ▶ Start sending data: It can be configured when a SATOP service starts sending data when all the prerequisites below are met:
 - ▶ It concerns a service on E1/T1/C37.94 ports;
 - ▶ One of the both service ports is set to 'adaptive';

- ▶ Configuration via Dashboard → Network Hardware → E1/T1/C37.94 ports → Circuit Emulation → Send Data (Immediately (=default), After Clock PreLocked, After Clock Locked). Make sure that both ports of the service are configured the same.
- ▶ After Clock Prelocked: after 120 seconds for PTN-16-E1-L/PTN-16-T1-L Interface Modules, after 15 seconds for the other Interface Modules;
- ▶ After Clock Locked: after the 'Clock Recovery State' field on port level is in the 'Locked' state;
- ▶ Configure and load the necessary port properties first (via Dashboard → Network Hardware) before creating the service via the services wizard!

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

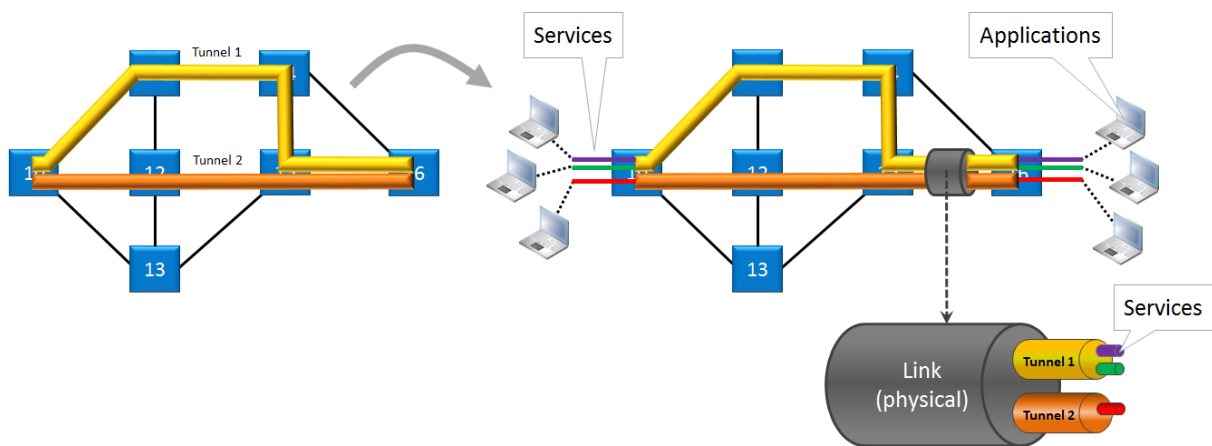


Figure 54 Service Creation in Tunnels

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

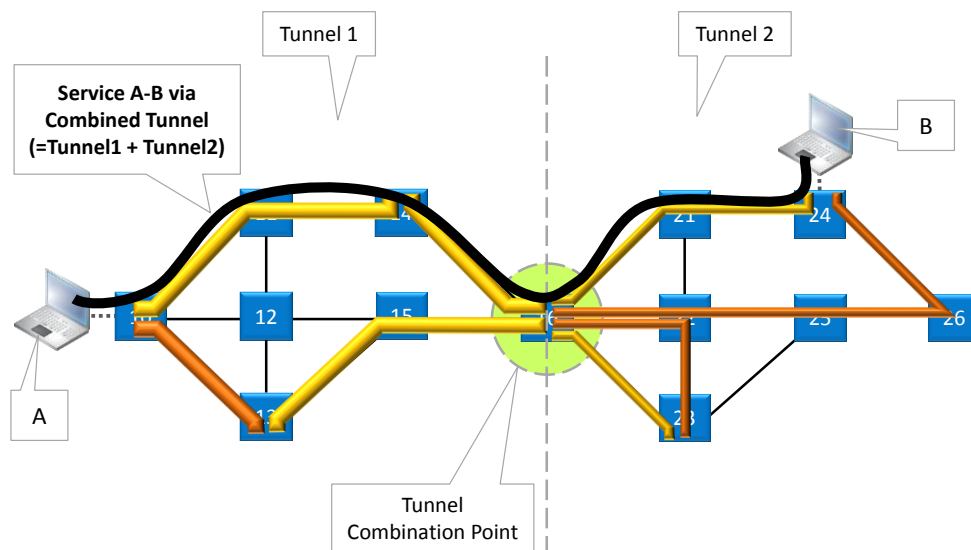


Figure 55 Service Via Combined Tunnels

In this manual, following terminology is used for a better readability, see also Ref.[23] in Table 1:

- ▶ 'main L3 Interface Module' = PTN-9-L3A-L Interface Module;
- ▶ 'extension L3 Interface Module' = PTN-9-L3EA-L Interface Module;
- ▶ 'L3 Interface Module' could either mean:
 - ▶ 'main L3 Interface Module' only = 8+1 front ports;
 - ▶ The 'main L3 Interface Module' combined with an 'extension L3 Interface Module' = 16+2 front ports;

Following services are possible:

Ethernet:

- ▶ interconnect Ethernet ports on Interface Modules that support the Ethernet service, see §32;
- ▶ port based or VLAN based;
- ▶ E-tree: yes/no (no=default), see §25 for more information;
- ▶ Local Service (only for VLAN Based services on L3 Interface Modules):
 - ▶ unchecked (=default): The service will go via tunnels, WAN ports and the Dragon PTN network;
 - ▶ checked: The service will only use the LAN side (or front ports) of L3 Interface Modules, the service will not use tunnels, WAN ports nor the Dragon PTN network. It will not consume bandwidth on the Dragon PTN network. See §31 for more info.

Optical Low Speed Serial:

- ▶ This service is a point-to-point service between two optical serial ports on the PTN-2-OLS Interface Module, each port located in a different node. This service converts the incoming serial signal into E1 and vice versa. Within one PTN-2-OLS Interface Module, [port1 <-> port3] and [port2 <-> port4] are always linked via a fixed local loopback including the conversion. See also Ref.[13] in Table 1 and §10.5;

- ▶ Loopback Mode: Internal Loopback (read only);
- ▶ Asynchronous / Synchronous (including bitrate);
- ▶ Enable / Disable FMO Coding.

Serial Ethernet:

- ▶ Used for point-to-multipoint and point-to-point services;
- ▶ interconnect ports on PTN-7-SERIAL Interface Modules: serial communication: RS232/RS422/RS485;
- ▶ Always Asynchronous;
- ▶ Master(s)/Slave(s) selection.


Circuit Emulation:

- ▶ Used for point-to-point services;
- ▶ E1, T1, C37.94: connect ports on PTN-4-E1-L/ PTN-4-T1-L, PTN-16-E1-L/ PTN-16-T1-L, PTN-2-C37.94 Interface Modules, PTN-2-OLS;
- ▶ Serial: connect ports on PTN-7-SERIAL Interface Modules: serial communication: RS232/RS422/RS485/ X.21 (X.21 only in synchronous mode);
- ▶ 2W/4W Voice: connect ports on PTN-4-4WEM-L Interface Modules;
- ▶ CODIR: connect PTN-4-CODIR ports;
- ▶ Optical Low Speed Serial: connects serial ports on the PTN-2-OLS Interface Modules;
- ▶ SAToP: one-to-one mapping of timeslots, C37.94/E1/T1 frame, 7-Serial or optical low speed serial data is transported transparently. Use this type when 'Differential Delay' (see Ref. [5], [6], [13], [22] in Table 1) is important for your application;
- ▶ CESoPSN: customized mapping of timeslots, only transmit used timeslots with real payload;
- ▶ Hitless Switching: switching between active and protection path stays synchronized;
- ▶ Single Path (Hitless Switching): The service can already start up with only one link up, coming out of a two-links-down situation with single path enabled. Do not use this option when 'Differential Delay' (see Ref. [5], [6], [13], [22] in Table 1) is important for your application.

Voice Service:

- ▶ Used to connect analog telephones (via PTN-8-FXS) or IP phones (via Ethernet Interface Modules, SIP-Server Mode) over the Dragon PTN network;
- ▶ Interconnects PTN-8-FXS ports and/or Ethernet ports (E.g. PTN-4-GC-LW, ...);
- ▶ Only VLAN based (VLAN ID assignment), not port based;
- ▶ 2 modes: Remote Extension (FXO Gateway), SIP-Server;
- ▶ Routable (with Gateway IP address).

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

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

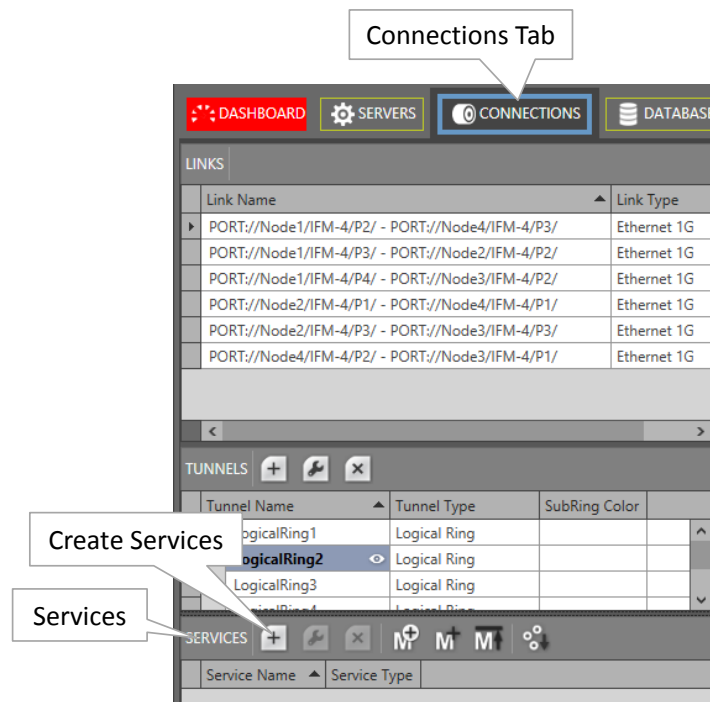


Figure 56 Create Services

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

Information: Click Next>>;

Service Name and Type Selection: enter a service name, select a service type:

- ▶ Ethernet:
 - ▶ Port Based: Use this mode if all the traffic on a port must be transported in one and the same service;
 - ▶ VLAN Based/VLAN ID: Use this mode if each VLAN on a port must have its own service. VLAN ID (only relevant for VLAN Based): Set the default VLAN ID in the range [2-3699, 3802-4000] for this service. Ethernet packets with this VLAN ID will be forwarded in this service, other VLAN IDs and untagged packets will be dropped. This behavior can be overruled by a more advanced VLAN processing in the 'VLAN Tagging/Untagging' feature further on this wizard;
 - ▶ E-tree: yes/no(=default), see §25 for more information;
- ▶ Optical Low Speed Serial:
 - ▶ Loopback Mode;
 - ▶ Synchronisation;
 - ▶ Bitrate;
 - ▶ FM0 Coding (in Synchronous mode);
- ▶ Serial Ethernet;
 - ▶ Interface Type: RS232/RS422/RS485;
 - ▶ Bitrate;
 - ▶ Data Bits;
 - ▶ Parity;
 - ▶ Stop Bits;
 - ▶ Multidrop Consistency (see §2.13.5);

- ▶ Advanced Mode (see §2.13.5): Fixed Block Size; Fixed Transmit Timer; Delimiter Line Termination Character; Delimiter Timeout; Timeout; Minimum Message Size;
- ▶ Circuit Emulation:
 - ▶ Protocol:
 - ▶ E1;
 - ▶ T1;
 - ▶ C37.94;
 - ▶ Serial (Synchronization / Interface Type / Bitrate / Pin Layout);
 - ▶ 2W/4W Voice;
 - ▶ CODIR;
 - ▶ Optical Low Speed Serial;
 - ▶ Usage:
 - ▶ SAToP (E1/T1/C37.94/7-Serial/Optical Low Speed Serial);
 - ▶ CESoPSN (E1/T1/C37.94/7-Serial/Optical Low Speed Serial);
 - ▶ Number of timeslots (for C37.94 using CESoPSN);
 - ▶ Differential Clocking: checked = differential / unchecked = adaptive clocking, see Ref. [5], [6], [8], [10], [13], [22] in Table 1 for more info (E1/T1/C37.94/CODIR/2-OLS. Note: for Serial: Adaptive clocking only);
 - ▶ Hitless Switching;
 - ▶ Hitless Switching → Single Path;
 - ▶ Serial: Synchronisation / Interface Type / Bitrate / Pin Layout;
 - ▶ Optical Low Speed Serial: Synchronisation / Bitrate (see §2.13.3) / FM0 Coding;
- ▶ Voice Service:
 - ▶ VLAN ID: Set the default VLAN ID in the range [3-3699, 3802-4000] for the Ethernet ports in this service. Ethernet packets with this VLAN ID will be forwarded in this service, other VLAN IDs and untagged packets will be dropped. This behavior can be overruled by a more advanced VLAN processing in the 'VLAN Tagging/Untagging' feature further on this wizard;
 - ▶ Mode: Remote Extension (FXO Gateway), SIP-Server, see §7.15 for more information;
 - ▶ Routable (including Gateway IP address): Enable this when your PTN-8-FXS Interface Modules, FXO Gateway or SIP Server are spread over multiple VLAN IP subnets. When enabling it, also fill out the Gateway IP address via which the FXO Gateway or SIP Server can be reached. One routed voice service is allowed per PTN-8-FXS Interface Module.

Service End Point Selection:

- ▶ For Ethernet services:
 - ▶ Make sure that all your service ports are LAN ports. Normally, this has been done already in §2.10. But if it was forgotten for a port, it can still be set via the Network Settings wizard without leaving the services wizard.

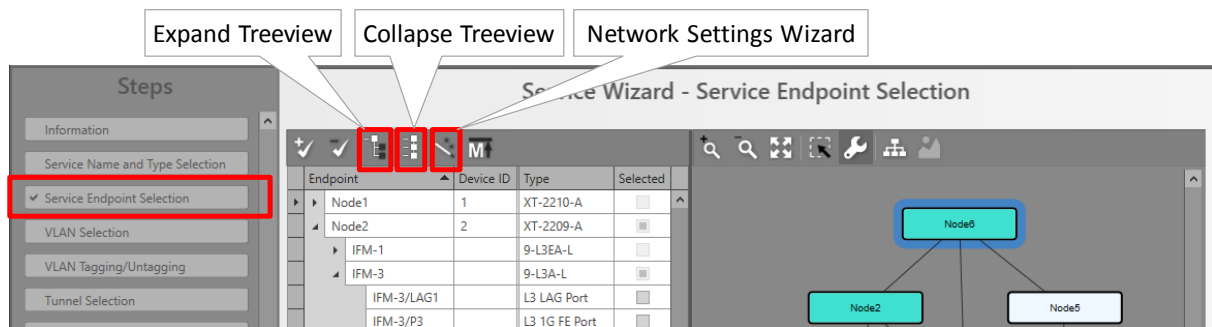


Figure 57 Open Network Settings Wizard

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

A port icon overview can be found below:

- ▶ brown LAN port = available for this service, the port number is shown in the port icon when hovering over it;
- ▶ brown bold LAN port = selected for this service;
- ▶ white LAN port = unavailable for this service, cannot be selected (correct port type but already taken by another service or wrong port type);
- ▶ white filled WAN port = Cannot be selected. In most of the cases, available means not taken at all by any service. In case of an Ethernet Interface Module (see Ethernet service in §32) it could mean a VLAN port as well which has already one or more VLAN based Ethernet services configured;
- ▶ Only on L3 Interface Modules (see also §31 for more info):
 - ▶ brown LAG port = available for this service;
 - ▶ brown LAG port = selected for this service;
 - ▶ white LAG port = unavailable for this service cannot be selected (correct port type but already taken by another service or wrong port type);
 - ▶ brown router : available VRF (=Virtual Routing and Forwarding) port which can be included in the service. Click this icon if this service must only reach possible virtual router and not the front ports in this Interface Module. If you click this icon, the front ports on this Interface Module will become unavailable for this service and vice versa.
 - ▶ white router : 1) unavailable VRF port for this service because already included in another service... or 2) automatic included VRF port because normal L3 Interface Module LAN ports are selected for this service in this Interface Module.

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

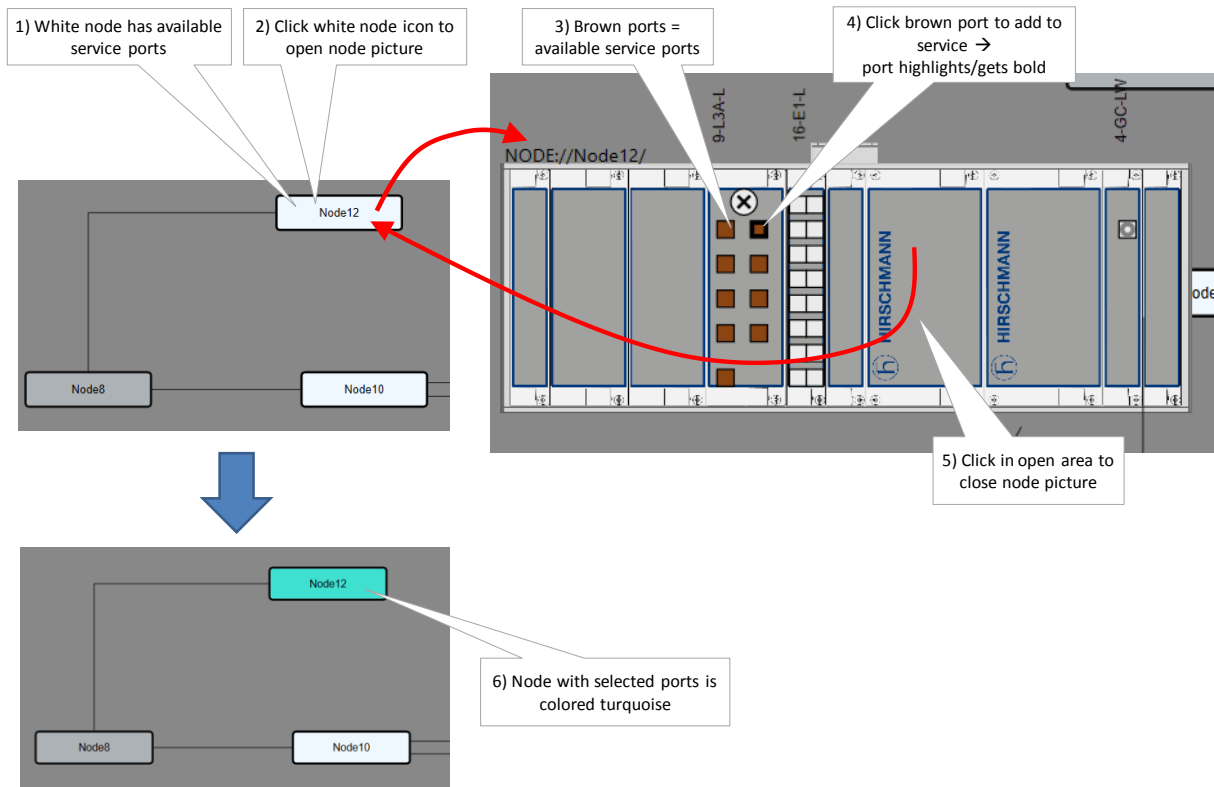



Figure 58 Service Ports Selection

- For the Ethernet service: If E-tree was selected previously, all selected ports are by default set as **leaf** port. Change at least 1 and maximum 4 of these ports into **root** ports (see §25 for more info on E-tree, see §32 which Interface Modules support E-tree). See the figure below.
- For the Ethernet/Serial Ethernet/Voice service: A node can have a maximum of 32767 MAC addresses. By default, per new Ethernet/Serial Ethernet/Voice service, 500/256 MAC addresses will be added to each LER node of the tunnel in which the service resides (not for point-to-point tunnels). If the maximum number of MAC addresses on a node has been reached, an error warning will pop up. You have to decrease the number of MAC addresses in this node from the other services first via clicking the MAC limit button  (see also §24.1.2). See the figure below:

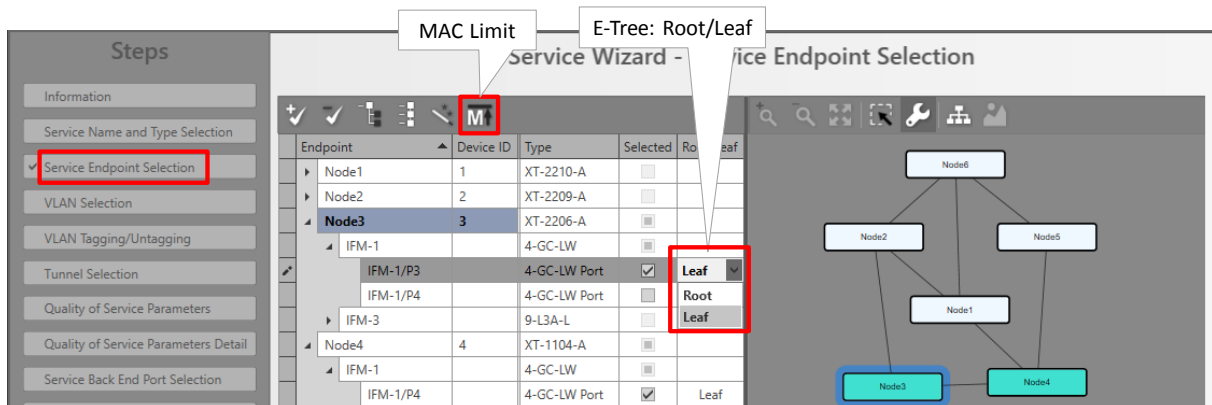



Figure 59 MAC Limit / E-Tree: Root & Leaf Ports Selection

- For the Serial Ethernet service, master(s)/slave(s) must be selected. By default, the end-point is set as slave but can be changed to master by clicking the cell, see figure below. In some network drawings the master will be indicated by .

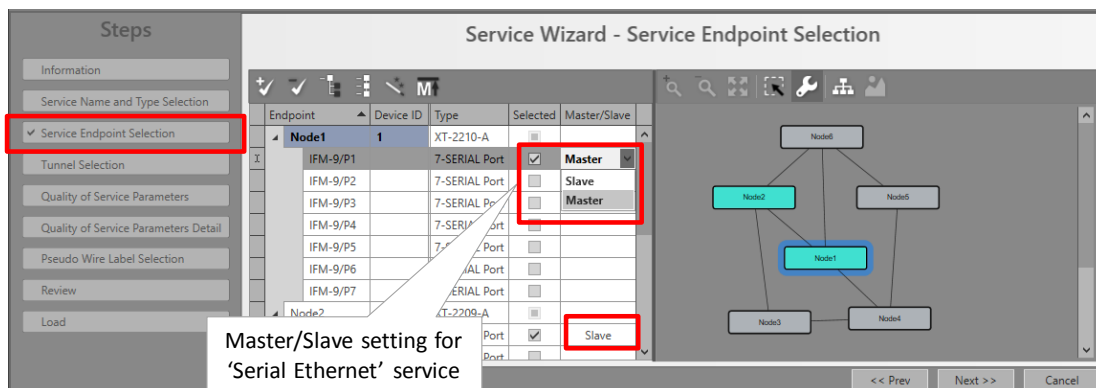


Figure 60 Master/Slave Setting for Serial Ethernet

- For the Voice service, a mix of Voice (8-FXS) and Ethernet (see §32) ports can be selected. Voice ports are always consumed per 2 ports or pair. Selecting one port automatically selects the second port or its pair partner. E.g. if you select port1, port2 will be selected automatically as well. If you only want to use one port (e.g. only connect one phone and not two), it is better to uncheck one of the two ports. The unchecked port will still be in use (=not available for other voice services), but it will not generate unnecessary alarms anymore.

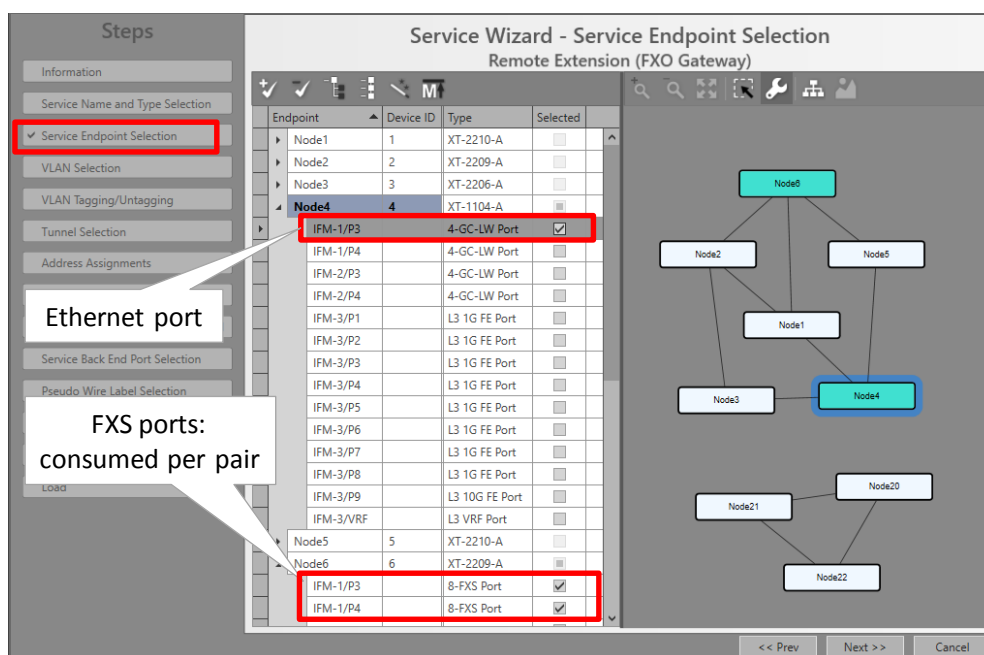


Figure 61 Voice Service: Port Selection

- VLAN Selection (Ethernet services): This page is only relevant when L3 Interface Module ports are involved in the service.... see §31 for more info and how to configure it.
- VLAN Tagging/Untagging (Ethernet (not L3 Interface Module)/Voice services): HiProvision supports VLAN processing for Ethernet and voice services. The possible

actions depend on whether the service is port based or VLAN based. The Voice service is always VLAN based.



- ▶ **ATTENTION:** By default, the VLAN processing behavior in this wizard page is as described previously in the 'Service Name and Type Selection' page in this wizard: Only forward packets (ingress and egress) with the configured VLAN ID and drop all the other packets. When changing the settings in the 'VLAN Tagging/Untagging' window, it will overrule the default behavior.
- ▶ The possible VLAN processing actions are described in the table below. Each port in the service can be configured with its own VLAN processing. For applying the same VLAN processing to multiple ports at once, use the  Multiple Settings Mode button. Configure the VLAN settings and click the apply button .

Table 12 VLAN Tagging/Untagging

Port/VLAN Based	Ingress/Egress	Possible Actions	Description
Note: A Prio Tag is a VLAN tag with VLAN ID = 0 Note: the actions are only valid for the configured endpoints in the configured service Note: Ingress and Egress VLAN ID: the configured VLAN ID is the same for both INGRESS and EGRESS			
Port Based (see Figure 62 below)	Ingress	None	None
	Egress	Keep Tag	The VLAN or Prio tag is kept when sending out the Ethernet packet (transparent transport of packets).
		Untag	The VLAN or Prio tag is removed from the Ethernet packet when sending out the packet.
		PrioTag	Replace the VLAN tag with a Priority tag.
		Replace Tag	Replace the VLAN ID in the outgoing Ethernet packet with the configured VLAN ID in the range [2-3699, 3802-4000].
		Add Tag	A VLAN tag with the configured VLAN ID will be added to untagged packets.
VLAN Based (see Figure 63 below)	Ingress	Untagged: Drop	Incoming untagged Ethernet packets will be dropped.
		Untagged: Tag and forward (<configured VLAN ID>)	Incoming untagged Ethernet packets will be tagged with the configured VLAN ID in the range [2-3699, 3802-4000] and forwarded.
		Priority Tagged: Drop	Incoming priority tagged Ethernet packets will be dropped.
		Priority Tagged: Tag and forward (<configured VLAN ID>)	Replace the priority tag (=VLAN ID 0) in the incoming Ethernet packet with the configured VLAN ID in the range [2-3699, 3802-4000] and forward it.
	Egress	Keep Tag	The VLAN or Prio tag is kept when sending out the Ethernet packet (transparent transport of packets).
		Untag	The VLAN or Prio tag is removed from the Ethernet packet when sending out the packet.
		PrioTag	Replace the VLAN tag with a Priority tag.

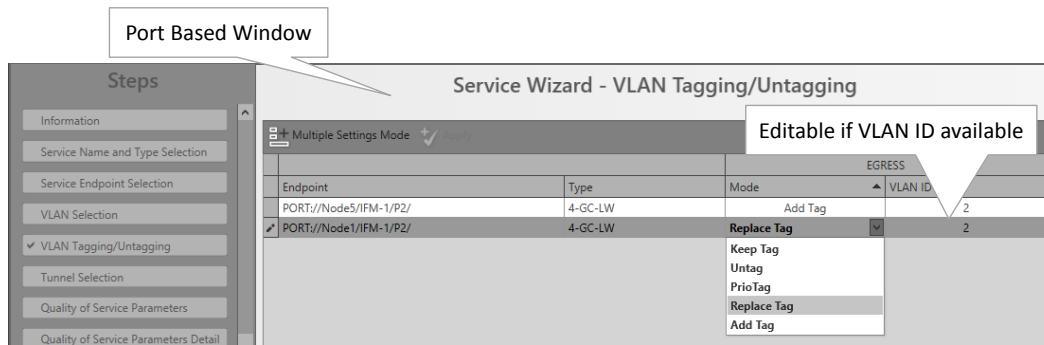


Figure 62 Port Based: VLAN Tagging/Untagging

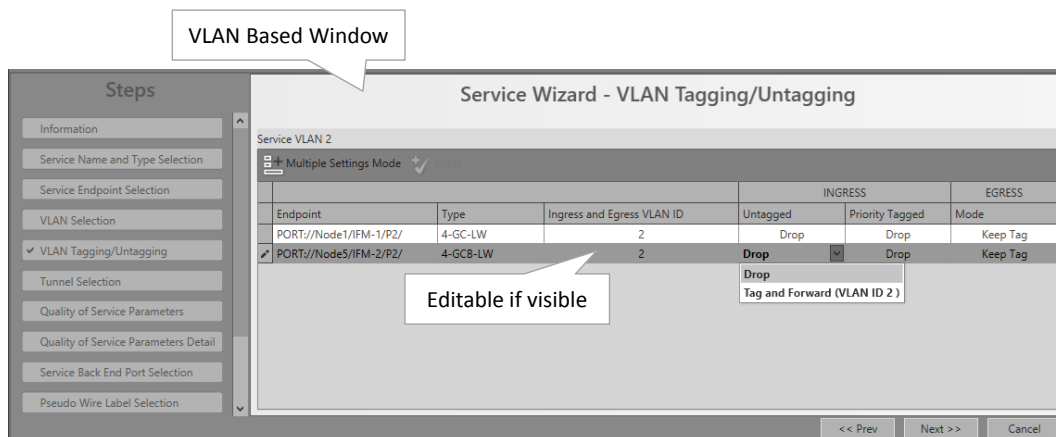




Figure 63 VLAN Based: VLAN Tagging/Untagging

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

- ▶ **Match (x/y):**
 - ▶ x: number of reachable service ports (or termination points) via this tunnel;
 - ▶ y: number of selected service ports (or termination points);
 - ▶ Perfect match: e.g. 3/3: all the selected service ports belong to nodes that are all linked to this tunnel. This tunnel can transport the service;
 - ▶ Mismatch: e.g. 2/3: at least one of the selected service ports belongs to a node that is not linked to this tunnel. A single selected tunnel with a mismatch cannot transport the required service;
 - ▶ Selected: checkbox to select the tunnel.
- ▶ **One tunnel:** If only one tunnel is selected, this tunnel has to have a perfect match to transport the required service;
- ▶ **Combined tunnels:** multiple tunnels can be selected or combined (by just selecting them in the tunnel list) into one big tunnel to transport the required service. It is possible to combine single tunnels with a mismatch into one big combined tunnel that has a perfect match for the entire service. Point-to-point tunnels cannot be combined, see Figure 55;
- ▶ **For Circuit Emulation Services (=CES):**
 - ▶ only point-to-point tunnels can be used;

- If hitless switching has been enabled, only point-to-point tunnels without protection can be used and will be listed. If no tunnel is listed, it means that no point-to-point tunnel without protection is available anymore to create the protection path for hitless switching. Create a new point-to-point tunnel without protection first.

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

NOTE: Future: a tunnel with a mismatch can be modified into a perfect match via ;

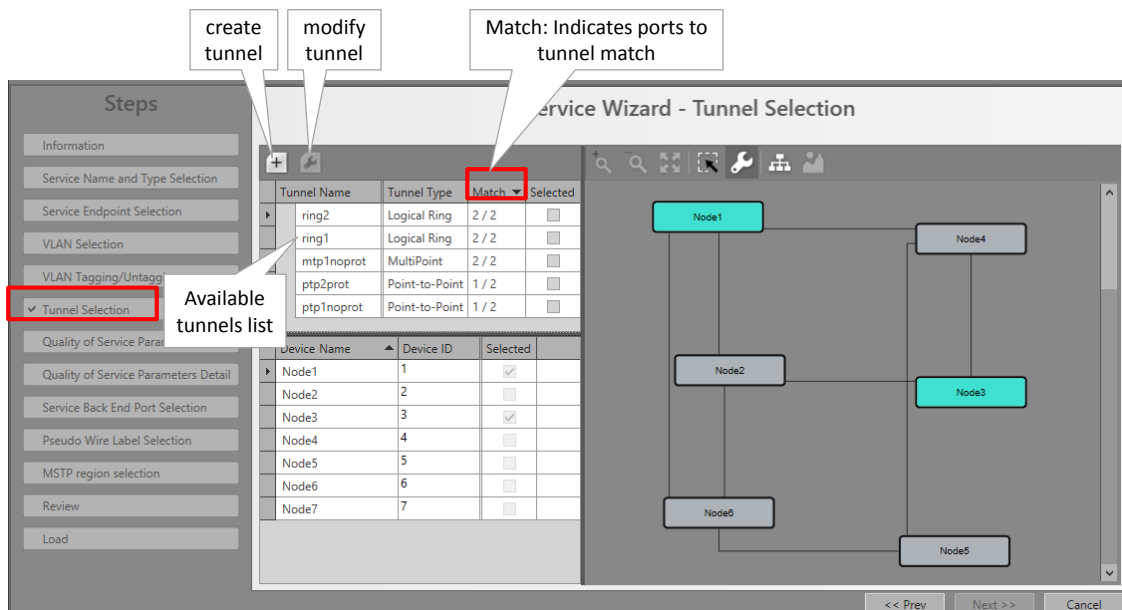


Figure 64 Ports to Tunnel Match

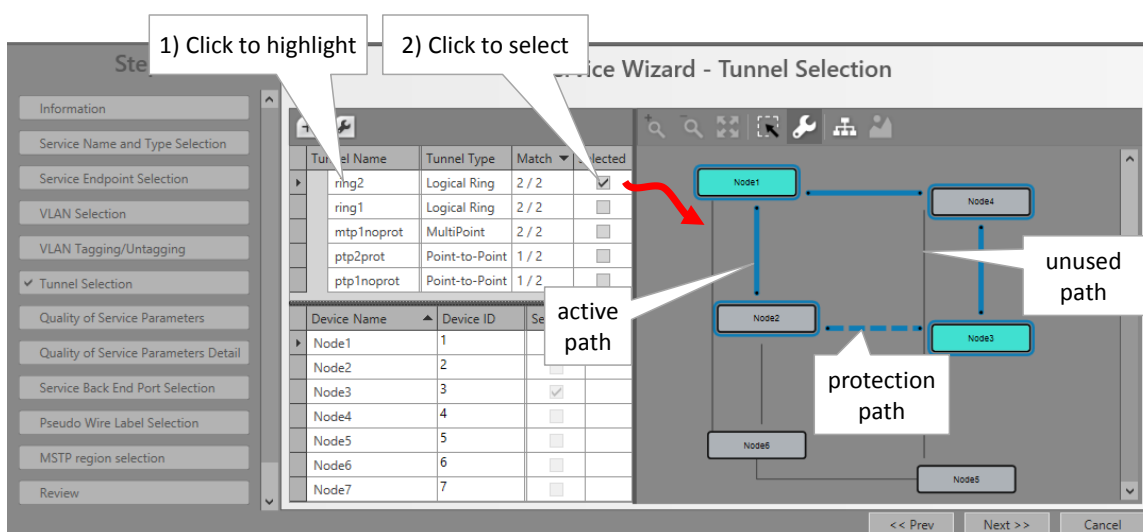


Figure 65 Selected Highlighted Tunnel

- ▶ Hitless Tunnel Selection (only visible for Circuit Emulation services with hitless switching): if no tunnel is listed, it means that no point-to-point tunnel without protection is available anymore. This type of tunnel is needed to create the protection path for hitless switching. Create a new point-to-point tunnel without protection first.
- ▶ Address Assignments (only visible for Voice services): Each 8-FXS module in a Voice service must be assigned an IP address to allow registration to the FXO gateway or the SIP Server later on. Fill out the IP Range Start and click the Auto Assign button. As a result, the 8-FXS modules will get an IP address assigned from this IP range. So all the phones connected to the ports within the same 8-FXS module have the same IP address. The phones can be differentiated based on the SIP account on application level. These automatically assigned IP addresses can be overruled or manually changed/edited.
- ▶ Service Back Endpoint Selection (Ethernet services): This page is only relevant when L3 Interface Module ports are involved in the service.... see §31 for more info;
- ▶ Circuit Emulation Parameters (only visible for Circuit Emulation services): fine-tuning of parameters, defaults are OK.
- ▶ Setting of service bandwidth or Quality of Service Parameters: see §2.13.6 for detailed information;
- ▶ Pseudo Wire Label Selection: leave this page as it is, defaults are OK;
- ▶ MSTP Region Selection (only when modifying an Ethernet service involved in Regions/MSTP (see §7.3) and adding a L3 Interface Module which is still part of the default MSTP Region): A configured Ethernet service can overlap different MSTP regions. When adding a L3 Interface Module to this service, the Interface Module will run with default MSTP settings available on the Interface Module itself (not visible in HiProvision) and indicated by 'Default Region'. Loop protection is guaranteed via this 'Default Region'. If you want to assign this Interface Module immediately to an existing MSTP Region, select one from the Region drop-down list. If not, leave 'Default Region' selected. Later on in the MSTP wizard, you can still assign this Interface Module to a new or existing Region.
- ▶ Review: The selected service ports will be shown: if ok, click Finish, the configuration load manager will be invoked, see §5;

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

2.13.2 Create External OLS Service (Converter/Loopback Type1)

The 'Optical Low Speed Serial service' is a point-to-point service between two optical serial ports on the PTN-2-OLS Interface Module, each port located in a different node. This service converts the incoming serial signal into E1 and vice versa.

Within one PTN-2-OLS Interface Module, [port 1 <-> port3] and [port 2 <-> port4] are always linked via a fixed local loopback including the conversion.

Figure 66 Service: Optical Low Speed Serial

1. Fill out a 'Service Name';
2. Select Service Type 'Optical Low Speed Serial';
3. Select Synchronisation: Asynchronous (=default) or Synchronous;
4. Synchronous:
 - ▶ Bitrate: See §2.13.3;
 - ▶ FM0 Coding: disabled/enabled:
 - ▶ disabled (=default): Normal data (without encoding) is expected at the optical serial RX ports; Normal data (without encoding) is generated at the optical serial TX ports;
 - ▶ enabled: FM0 encoded data is expected at the optical serial RX ports; FM0 encoded data is generated at the optical serial TX ports; With FM0 Coding enabled, a 0-bit (= 'space') will always have an extra transition halfway its bit time (=2 phases = biphase) whereas a 1-bit will have no transition within its bit time.

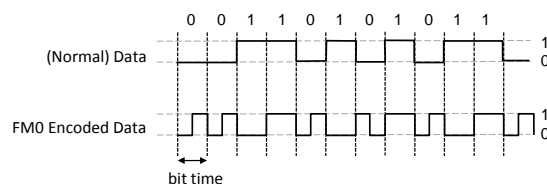



Figure 67 FM0 Coding

5. Asynchronous (=default):
 - ▶ Bitrate: See §2.13.3. When a bitrate is selected, an incoming serial signal with a lower bitrate will operate as well, because 2-OLS samples at 6.6 times the selected bitrate;
6. Click Next>>;
7. Select the end-points. It is point-to-point, so only select two end-points. The end-points are the optical serial ports of the PTN-2-OLS Interface Module; Make sure that the selected end-points are both part of the External E1 Link already created. If not, the Next button remains disabled. Note: Within one PTN-2-OLS Interface Module, [port 1 <-> port3] and [port 2 <-> port4] are always linked via a fixed local loopback including the conversion. E.g. It means that if port3 is used in the External E1 Link, port1 must be used (and not port2) as end-point to be able to use the External E1 Link.
8. Click Next>>;
9. Short Haul (refers to E1 ports on the PTN-2-OLS Interface Module): Long E1 links (>200m, Long Haul) have more E1 signal attenuation than shorter E1 links (<200m, Short Haul). As a result, the E1 signal levels or sensitivity ('0' or '1') on the receiver side depend on the

usage of Long Haul/Short Haul links. Check this parameter for Short Haul links and unchecked it (=default) for Long Haul links. This parameter can be set on port level in the Interface Module or at service creation.

- Once the service has been created, the Connections tab could look as in the figure below for this service. All External E1 Links, tunnels, services that go beyond the Dragon PTN network, are indicated by a cloud icon. Click the details  button to show more details.

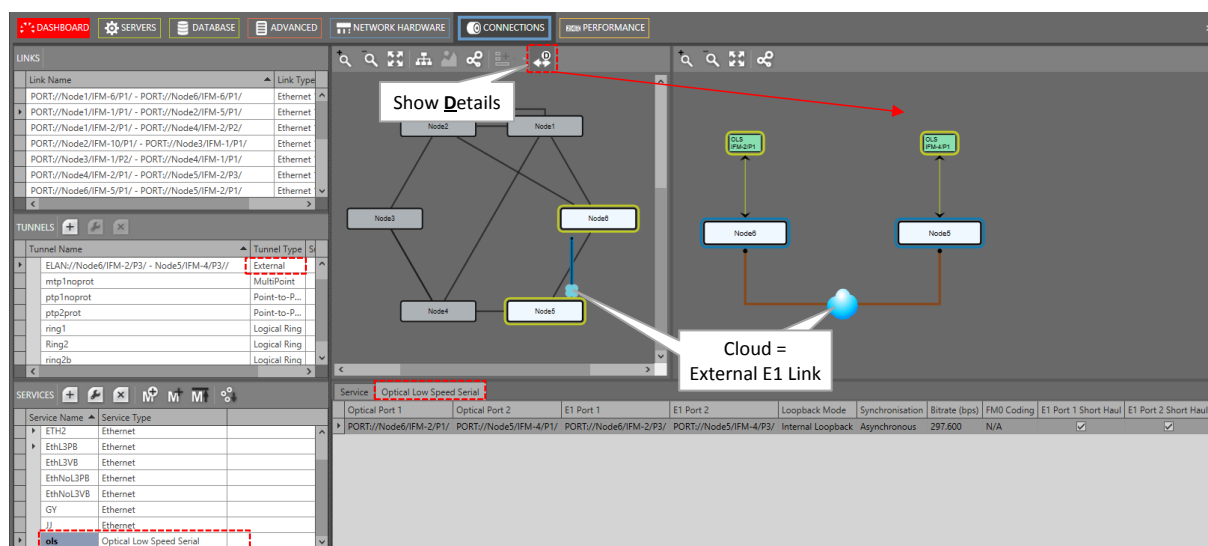


Figure 68 Created 'Optical Low Speed Serial' Service

NOTE: Also verify the extra 2-OLS settings in §10.5.


2.13.3 Optical Low Speed Serial Bitrates

'Service Type', 'Protocol', 'Usage', 'Synchronisation' and 'Bitrate' in the table below refer to the settings in the service wizard in HiProvision.

Table 13 Optical Low Speed Serial Bitrates

Service	Converter/Loopback Type1		Normal Type2			
Service Type	Optical Low Speed Serial		Circuit Emulation			
Protocol	---		Optical Low Speed Serial			
Usage	---		SAToP		CESoPSN	
Synchronisation	Async. (bps)	Sync. (kbps)	Async. (bps)	Sync. (kbps)	Async. (bps)	Sync. (kbps)
Bitrate	1200 2400 4800 9600 19200 38400 57600 76800 115200 297600	1x64k (64k) 2x64k (128k) 4x64k (256k) 8x64k (512k) 16x64k (1024k)	max bitrate is always 307200 bps	1x64k (64k) 2x64k (128k) 4x64k (256k) 8x64k (512k) 16x64k (1024k) 32x64k (2048k)	1200 2400 4800 9600 19200 38400 57600 76800 115200 297600	1x64k (64k) 2x64k (128k) 4x64k (256k) 8x64k (512k) 16x64k (1024k)

2.13.4 Service Modification

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

Ethernet:

- ▶ Port Based/VLAN Based:
 - ▶ Service Name;
 - ▶ VLAN ID (VLAN Based)
 - ▶ Port Mode Settings;
 - ▶ E-Tree;
 - ▶ MAC Limits;
 - ▶ Add/Remove Ports → 'Reconfigure Settings' in 'Quality of Service Parameters window' must be done to recalculate the bandwidth assignments over the resulting ports;
 - ▶ VLAN Tagging/Untagging;
 - ▶ Selected tunnels;
 - ▶ Quality of Service Parameters;

Serial Ethernet:

- ▶ Service Name;
- ▶ Bitrate;
- ▶ Multidrop Consistency;
- ▶ Advanced Mode;
- ▶ Block Size;
- ▶ Add/Remove Ports;
- ▶ Selected tunnels;
- ▶ Quality of Service Parameters;

Circuit Emulation:

- ▶ Service Name;
- ▶ Differential Clocking / Hitless Switching / Single Path Parameters;
- ▶ Bundle/Delay Parameters;
- ▶ Selected Tunnels;
- ▶ Priority;
- ▶ Frame Size;
- ▶ Bit Rate;

Voice Service:

- ▶ Service Name, VLAN ID, Mode, Routable;
- ▶ Add/Remove Ports;
- ▶ VLAN Tagging/Untagging;
- ▶ Selected Tunnels;
- ▶ IP Address Assignment;
- ▶ Quality of Service Parameters;

2.13.5 Serial Ethernet: Extras

a. Advanced Mode - Bandwidth Optimization

At service creation, fine-tuning the bandwidth and delay through the network is done via the Advanced Mode parameter. It groups payload data more efficiently in the transmit process resulting in less overhead. Note that less bandwidth results in more delay and vice versa.

Serial data is collected at the front ports and the payload data bits are buffered until one of the Advanced Mode events below is triggered. After the trigger, the payload data is packetized and sent over the Dragon PTN network.

Advanced Mode:

- ▶ Number of payload data bytes (=block) received at the front (Fixed Block size);
- ▶ Periodic transmit timer expires (Fixed Transmit Timer);
- ▶ Detection of a line termination character (Delimiter Line Termination Character);
- ▶ Timeout occurs after the last received byte (Delimiter Timeout).

Each mode is explained more in detail below:

- ▶ Fixed Block Size (=default): Whenever 'N' payload data bytes are received at the front port, a packet including 'N' bytes will be sent through the Dragon PTN network. Configure 'N' in the Block Size field (default=8 bytes, range[1..1000] bytes). If 'N' is never received, the packet will be sent anyway after a specific timeout based on 'N' and the bitrate. A small 'N' results in an inefficient bandwidth but a low delay and vice versa.
- ▶ Fixed Transmit Timer: Configure the Transmit Timer (default = 10 ms, range [0-10000] ms). This timer is started whenever a serial data message enters a front port of the PTN-7-SERIAL Interface Module. When the timer expires, a packet is transmitted through the Dragon PTN network and the timer is started again. This periodical process is repeated until the entire serial data message has been transmitted. The timer will only be started again when a new serial data message enters the PTN-7-SERIAL Interface Module.
- ▶ Delimiter Line Termination (=LT) Character: Whenever an LT character is received at the front port, a packet will be sent through the Dragon PTN network. Configure the decimal ASCII value in the 'Line Termination Character (decimal)' field. The LT character will be sent as well. E.g. two common LT characters are Line Feed ('\n' = ASCII decimal 10) and Carriage Return ('\r' = ASCII decimal 13). Also fill out the Minimum Message Size (default=8 bytes, range[1..1000] bytes), needed to calculate the required bandwidth. Attention: filling out a higher (incorrect) minimal value than the real minimum could cause data loss.
- ▶ Delimiter Timeout: Whenever a Timeout occurs after the last received byte at the front port, a packet will be sent through the Dragon PTN network. Configure the Timeout (default = 100000 µs, range [0-100000] µs). Also fill out the Minimum Message Size (default= 8 bytes, range[1..1000] bytes), needed to calculate the required bandwidth. Attention: filling out a higher (incorrect) minimal value than the real minimum could cause data loss.


Fixed Mode		Delimiter Mode	
<div>Advanced Mode Fixed Block Size</div> <div>Transmit Timer 0 msec</div> <div>Line Termination Character (decimal) 0</div> <div>Block Size 8 bytes</div>		<div>Advanced Mode Delimiter Line Termination Character</div> <div>Timeout 100 µsec</div> <div>Line Termination Character (decimal) 1</div> <div>Minimum Message Size 8 bytes</div>	
<div>Advanced Mode Fixed Transmit Timer</div> <div>Transmit Timer 10 msec</div> <div>Line Termination Character (decimal) 0</div> <div>Block Size 8 bytes</div>		<div>Advanced Mode Delimiter Timeout</div> <div>Timeout 100000 µsec</div> <div>Line Termination Character (decimal) 0</div> <div>Minimum Message Size 8 bytes</div>	

Figure 69 Serial Ethernet: Advanced Mode - Bandwidth Optimization

b. Multidrop Consistency

Multidrop Consistency is a polling mechanism, within a Serial Ethernet service, between the master(s) port(s) and the slave ports to check whether the slaves are still alive. The master Interface Module is the Interface Module connected to the master application, the slave Interface Module is the Interface Module connected to the slave application. Each slave will see the poll requests to other slaves as well, but only answers the poll request addressed to itself.

- ▶ Checked (=default): the polling occurs every 500 ms. If a polling error occurs, the necessary alarms will be raised. If there are two masters, both masters poll independently of each other;
- ▶ Unchecked: no polling occurs at all. No alarm will be raised or nothing will be reported in HiProvision when a slave is missing.

Following poll results are reported per master and per slave in HiProvision and visible via the Dashboard → Network → Services → Click Service in the list → Click Serial Ethernet tab. The polling results can be updated via the refresh button .

Poll Error Seen by Master:

- ▶ False: Everything OK, slave Interface Module has answered the poll request of the master Interface Module;
- ▶ True: Failure, slave Interface Module has not answered the poll request of the master Interface Module;

Poll Error Seen by Slave:

- ▶ False: Everything OK, the slave Interface Module receives all the poll requests to other slaves as well;
- ▶ True: Failure, the slave Interface Module does not receive at least one of the poll requests addressed to other slaves;

Specific Poll Error Seen by Slave:

- ▶ False: Everything OK, slave Interface Module has received a poll request of the master Interface Module;
- ▶ True: Failure, slave Interface Module has not received the poll request of the master Interface Module;

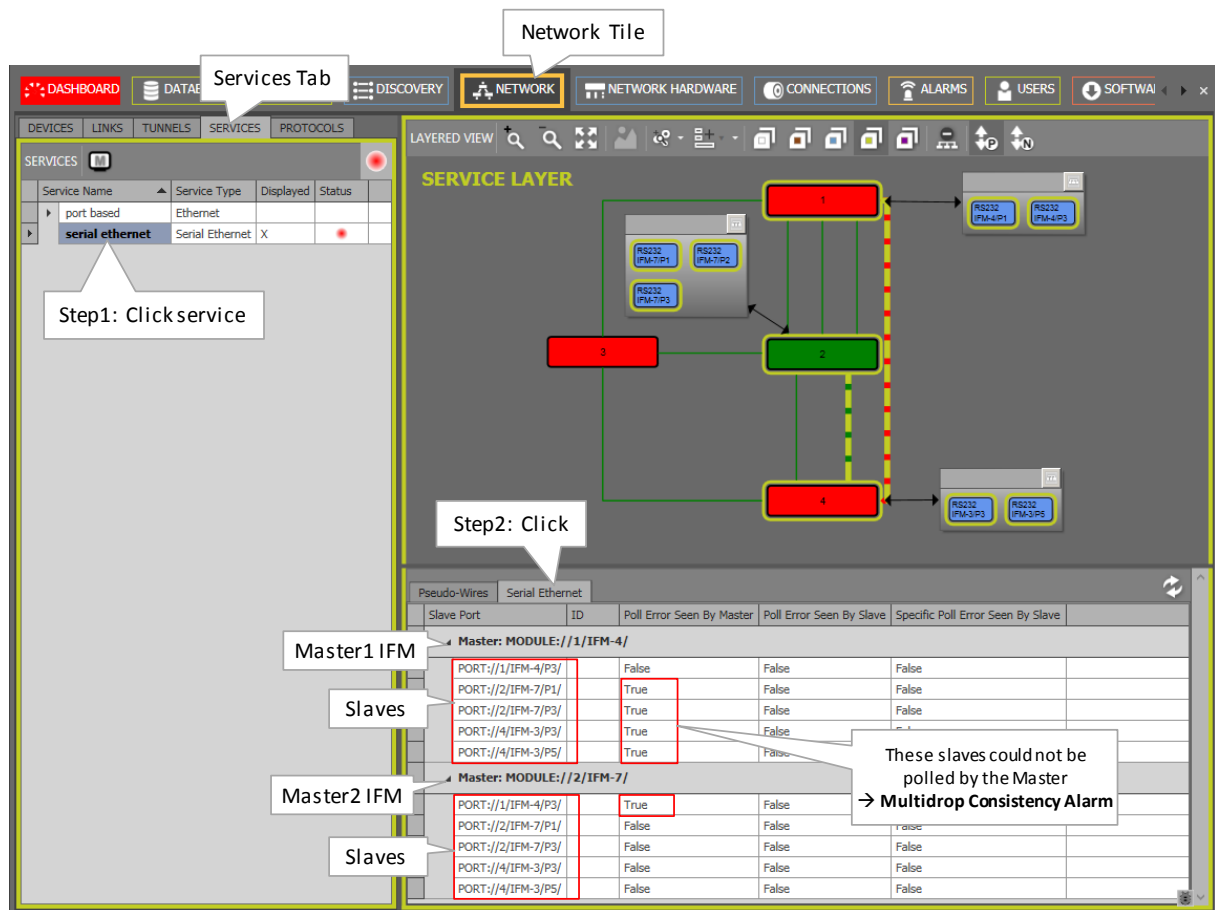


Figure 70 Multidrop Consistency Monitoring

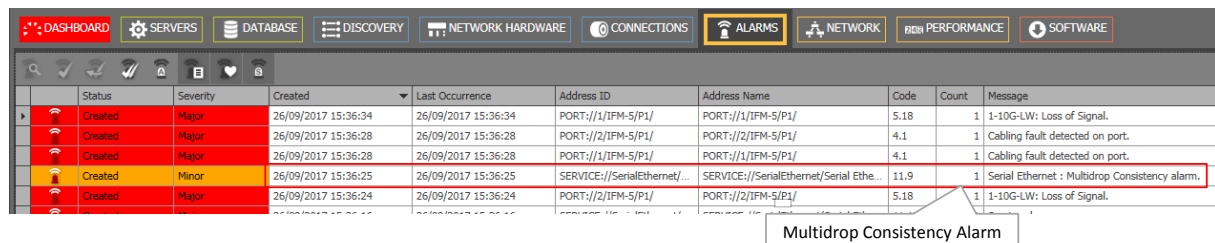


Figure 71 Multidrop Consistency Alarm

2.13.6 Reporting

Service and port reporting information is available via the Reporting Engine Add-on, see §29.4.

3. QUALITY OF SERVICE (=QOS)

3.1 General

QoS is a common name for different methods that process Ethernet traffic in order to provide sufficient service delivery and bandwidth for critical applications.

HiProvision provides a few mechanisms in the Dragon PTN nodes to avoid congestion or to handle the congestion in an optimized way.

QoS is based on bandwidth/burst size, priority, and frame size per service and storm control. These parameters will be described more into detail in the paragraphs below.

3.2 Step1: QoS Parameters in Service Wizard

The QoS parameters in the screenshot below can be configured when creating an 'Ethernet' service. When creating a 'Circuit Emulation' or 'Serial Ethernet' service, only the Priority parameter can be configured, see Figure 72.

The first section indicates value configurations on the LAN side while the second and third section refers to values used over the Dragon PTN network itself (=WAN side). The advised way to fill out this form is from top to bottom.

When creating a 'Voice Service', the parameters in Figure 73 are described in §3.2.6.

Steps

- Information
- Service Name and Type Selection
- Service Endpoint Selection
- VLAN Selection
- VLAN Tagging/Untagging
- Tunnel Selection
- ✓ Quality of Service Parameters
- Quality of Service Parameters Detail
- Service Back End Port Selection
- Pseudo Wire Label Selection
- MSTP region selection
- Review
- Load

Service Wizard - Quality of Service Parameters

Priority: 0

Configure Maximum Frame Size

Parameter	Value	Unit
Maximum Frame Size	1,522	bytes
Tagged Maximum Frame Size	1,522	bytes
Untagged Maximum Frame Size	1,518	bytes
MTU (L2 payload)	1,500	bytes

Configure Average Frame Size

Frame Size Mode: Custom Frames

Frame Size Mode	Percentage	Value	Unit
Small Frame	61 %	64	bytes
Custom Frame	24 %	594	bytes
Large Frame	15 %	1,522	bytes
Average Frame	100%	410	bytes

Configure Bandwidth & Burst Size

Bandwidth & Burst Size Mode: Service based

Parameter	Value	Unit
Service (gross) Bandwidth	50,000	kbps
Service Burst Size	15,440	bytes
Service Burst Size	10	frames

Callouts:

- LAN Side
- Average frame size used to calculate WAN side bandwidth
- WAN Side

FILL OUT

<< Prev Next >> Cancel

Figure 72 QoS Parameters in the Ethernet Service Wizard

Figure 73 QoS Parameters in the Voice Service Wizard

3.2.1 Priority

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

Table 14 Service, Priority, Frame Size, Bandwidth Input

Service, Application	Max. Priority	Default Priority	Configurable Average Frame Size (*)	Configurable Bandwidth Input (**)
Circuit Emulation: E1, T1, Serial, C37.94, 2W/4W Voice, CODIR, Optical Low Speed Serial	5	4	No	No
Serial Ethernet	5	4	No	No
Ethernet: point-to-point	4	0	Yes, if priority <= 1	Yes, if priority <= 3
Ethernet: multipoint, ring	4	0	Yes, if priority <= 1	Yes, if priority <= 3
Voice Service	4	3	Yes, if priority <= 1	No
(*) Can be found in 'Quality of Service Parameters' window, see Figure 72.				
(**) Can be found in the 'Ports' tab in the 'Quality of Service Parameters Detail' window, see Figure 74.				

3.2.2 Reconfigure Settings (only for Service Modification of Ethernet Services)

If a port has been added/removed, it means that the bandwidth/burst size assignment must be recalculated. Click this checkbox to recalculate and reconfigure the bandwidth and burst size settings over the resulting ports and tunnels.

3.2.3 Configure Maximum Frame Size (Ethernet Services Only)

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

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

3.2.4 Configure Average Frame Size

For Ethernet **and Voice** services and according to Table 14.

The better you know the traffic (and its frame sizes) in your network, the better you can tune the consumed bandwidth on the WAN side. The Average Frame Size indicates the Ethernet frame size = payload + Ethernet overhead. This parameter is used by HiProvision to tune the BWE (=Bandwidth Efficiency), see also §3.7.

- ▶ **Average Frame Size** (Voice service): if Configurable Average Frame Size = 'yes' in Table 14, the Average Frame Size can be changed, if not always 64 bytes will be used;
- ▶ **Frame Size Mode** (Ethernet service): if Configurable Average Frame Size = 'yes' in Table 14, the Frame Size Mode and the average frame size can be changed. if Configurable Average Frame Size = 'no', always 'Small frames' (=default) will be active;
 - ▶ Priority = 0: default Frame Size Mode = Custom frames;
 - ▶ Priority = 1: default Frame Size Mode = Small frames;
- ▶ **Small Frame, 100%** (Ethernet service): HiProvision calculates the LAN to WAN bandwidth ratio as if the incoming LAN frame size is 64 bytes. These small frames always result in a congestion free flow through the MPLS-TP network but lead to a less efficient bandwidth usage. The bandwidth usage is less efficient because proportionally more header bytes are expected to be processed compared to the real payload data.
- ▶ **Custom Frame (=default)** (Ethernet service): After selecting this value, the expected frame size percentages of small/custom/large frames on the LAN side can be changed. By default, these percentages are 61% small frames, 24% custom frames, 15% large frames. By configuring or modifying these percentages, Dragon PTN can tune the LAN to WAN bandwidth better resulting in a higher BWE. The Custom Frame size itself can also be configured. The average frame size indeed directly influences the BWE between the LAN and WAN. See §3.7 for more info.
- ▶ **Large Frame, 100%** (Ethernet service): the most ideal situation, when all the LAN traffic has a frame size of the configured Maximum Frame Size bytes, the BWE will be the highest!

- **Average Frame:** is always 100% and indicates the configured Average Frame Size based on the previous settings;

CAUTION:

When the real or measured average frame size is reasonably lower than the configured average frame size, extra delay and/or frame loss can occur! Frame loss can be detected and verified via the 'Disc In Packets'/'Disc Out Packets' counters, see §15.2.1.

When the real or measured average frame size is reasonably higher than the configured average frame size, a lower BWE will be obtained but traffic will not be influenced.

3.2.5 Configure Bandwidth & Burst Size (Ethernet Services Only)

- **Bandwidth & Burst Size Mode = Service based (=default):** The QoS parameters will be configured on the service tunnels. The configuration on the endpoints will be calculated by HiProvision based on the configured frame size and number of endpoints. See §3.4;
 - **Service (gross) Bandwidth:** The maximum bandwidth in kbps that is allowed for this service on the link. This value includes 'L2 Ethernet frame' + 'MPLS-TP overhead';
 - **Service Burst size:** Can be configured in bytes or frames:
 - **in bytes (default = 50000):** The maximum burst size in bytes that is allowed for this service on the link. This value includes 'L2 Ethernet frame' + 'MPLS-TP overhead';
 - **in frames (default = 10):** The desired number of frames that will be buffered. Changing the number of frames will change the number of bytes and vice versa. The frames value is more indicative, while the resulting bytes value will be used for the real burst size calculation.
- **Bandwidth & Burst Size Mode = Endpoint based:** The QoS parameters will be configured on the endpoints. The configuration on the service tunnels will be calculated by HiProvision based on the configured frame size and the number of endpoints. See §3.5.
 - **Endpoint (useful) Bandwidth:** The maximum bandwidth in kbps that the application is allowed to send on the service port (*). This value only includes 'L2 Ethernet frame';
 - **Endpoint Burst size:** Can be configured in bytes or frames:
 - **in bytes (default = 50000):** The maximum burst size in bytes that the application is allowed to send on the service port. This value only includes 'L2 Ethernet frame';
 - **in frames (default = 10):** The desired maximum number of frames that the application wants to send in one burst. Changing the number of frames will change the number of bytes and vice versa. The frames value is more indicative, while the resulting bytes value will be used for the real burst size calculation.

NOTE: (*) Service port: is a port that can be used as an endpoint in a service. It can be an Interface Module front port (e.g. port based Ethernet), a part of an Interface Module port (e.g. VLAN based Ethernet, CES...) or more than one Interface Module port (e.g. Serial Ethernet);

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

3.2.6 Additional Ethernet Port Bandwidth (Voice Services only)

The Ethernet ports in a voice service consume a bandwidth which consists of voice channels and some additional bandwidth.

- **Number of Voice Channels:** (default = 1, maximum depends on the available bandwidth on the links) The number of voice channels that go via this port. HiProvision will reserve 100 kbps per voice channel;
- **Additional Bandwidth (kbps):** (default=0, maximum depends on the available bandwidth on the links) The additional or extra bandwidth that this port requires in this service to serve non-voice or different applications if any e.g. FTP server, ...

Burst Size (bytes): (default=0, maximum depends on the available bandwidth on the links)
The maximum burst size in bytes that can be sent on the service via this port.

3.3 Step2: QoS Parameters in Detail in Service Wizard

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

Some values are configured, others are calculated by HiProvision based on the configured values. E.g. if the service values are configured, the according service port values will be calculated automatically. Both configured and calculated values are visible in both the network drawing and tables in the Ports and LSPs tabs.

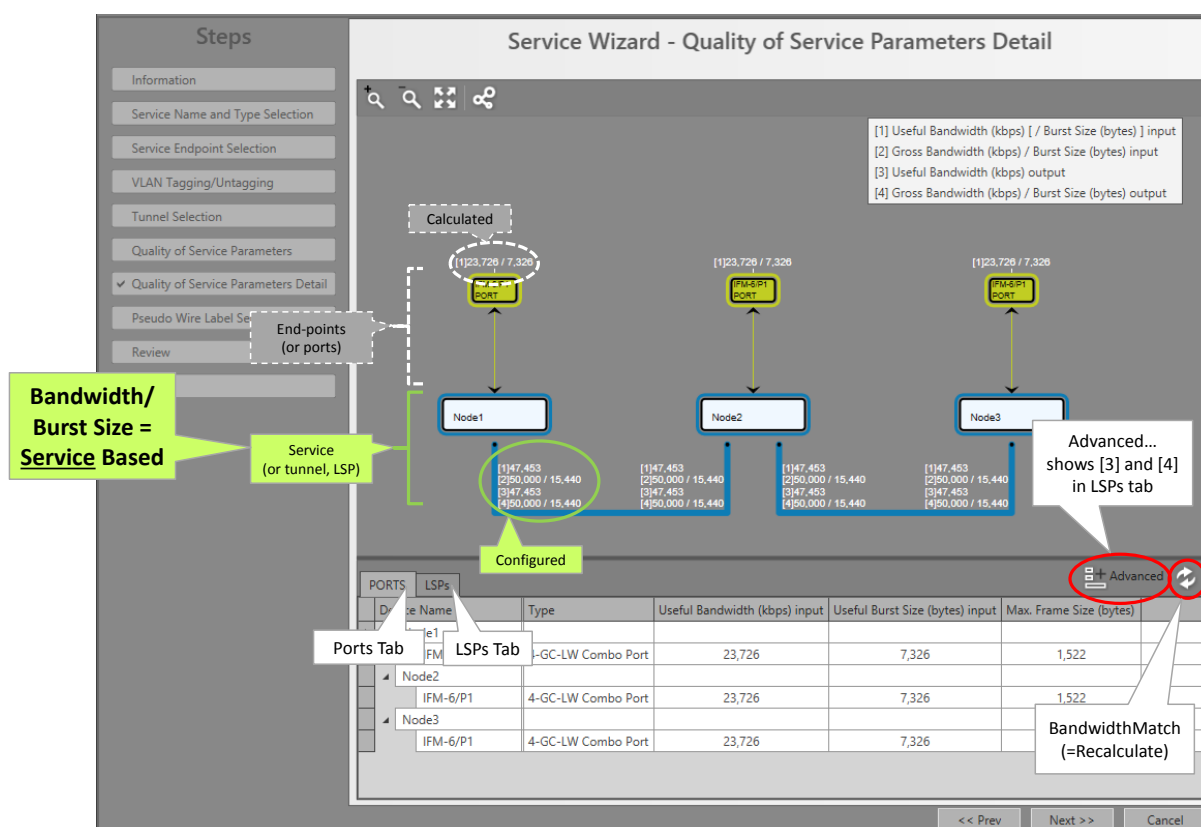





Figure 74 Bandwidth/Burst Size Parameters in Detail

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

CAUTION: Incorrectly tuned bandwidth or burst size values could result in extra delay and/or frame loss. Frame loss can be detected and verified via the 'Disc In Packets'/'Disc Out Packets' counters, see §15.2.1.

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

3.4 Bandwidth/Burst Size: Service Based

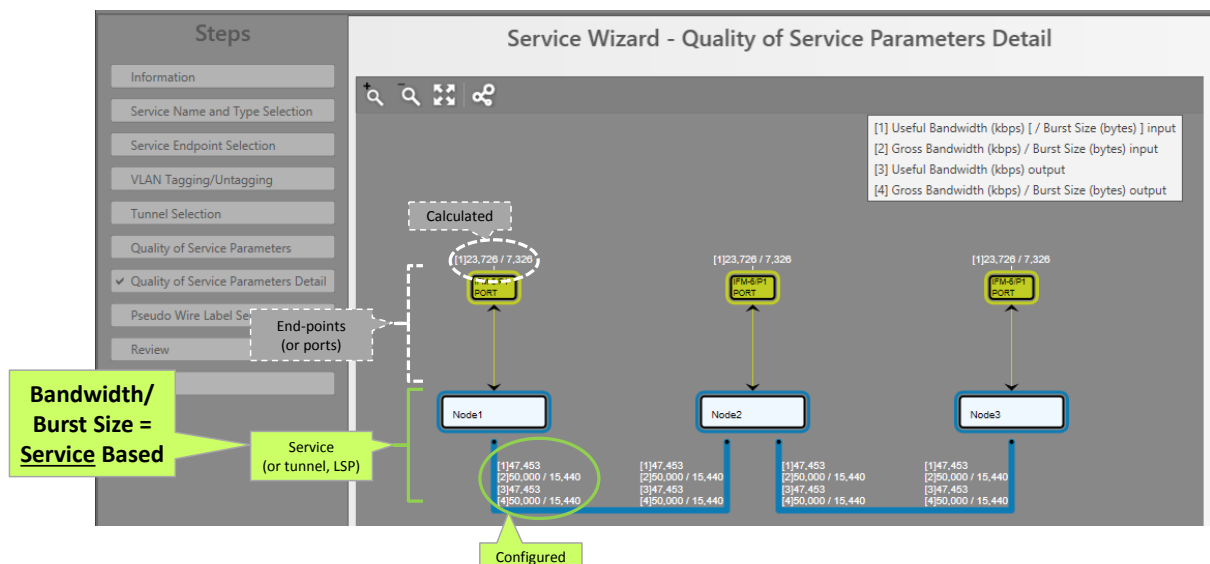


Figure 75 Bandwidth/Burst Size: Service Based

3.5 Bandwidth/Burst Size: Endpoint Based

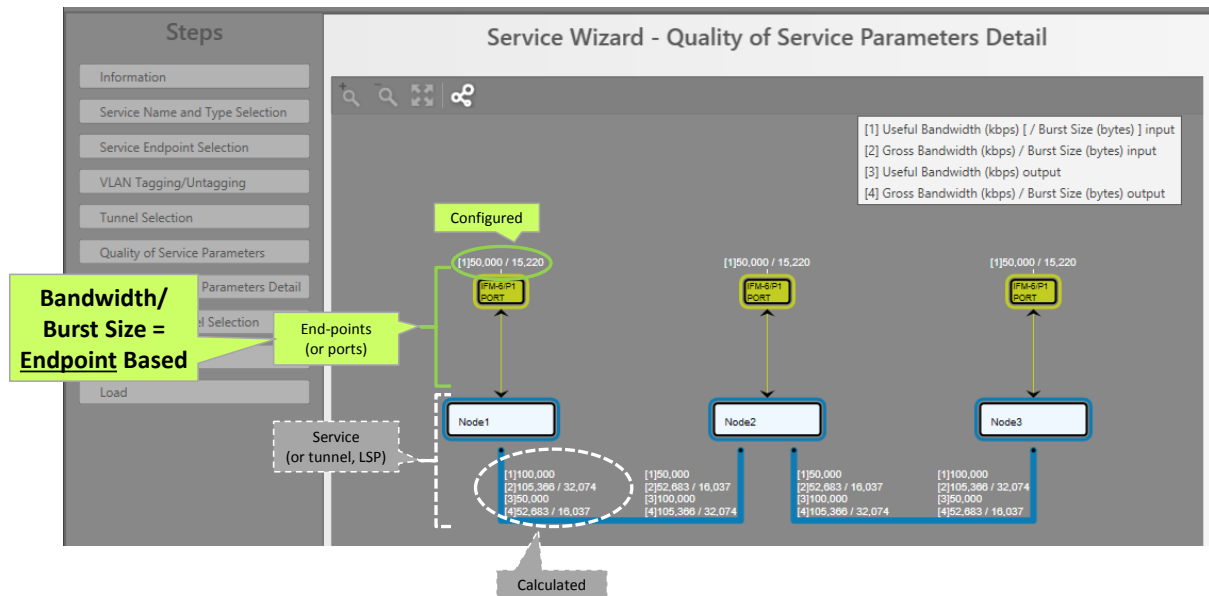


Figure 76 Bandwidth/Burst Size: Endpoint Based

3.6 Values on the Network Drawing

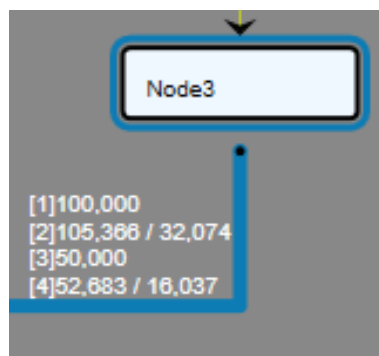


Figure 77 Bandwidth/Burst Size on WAN Side

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

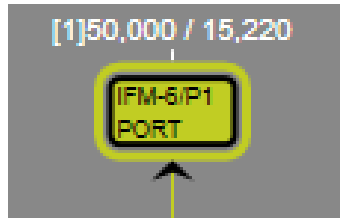


Figure 78 Bandwidth/Burst Size on LAN Side

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

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

The BWE is the LAN to WAN bandwidth ratio. It compares the LAN bandwidth on a service port (see §3.2) to its required WAN or gross bandwidth to transport the service in a point-to-point service. The higher the BWE, the more efficient the WAN bandwidth is consumed.

$$\text{BWE} = \text{LAN bandwidth} / \text{WAN bandwidth \%} = \text{Useful Bandwidth} / \text{Gross Bandwidth \%}$$

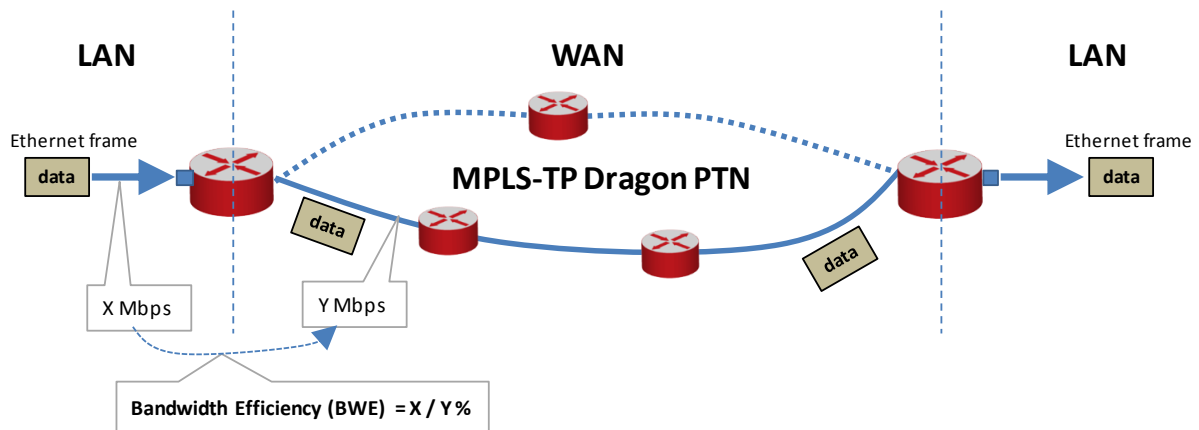


Figure 79 Bandwidth Efficiency

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

Tuning the average frame size, see §3.7.1;

Tuning the ports input bandwidth, see §3.7.2;

3.7.1 Bandwidth Optimization via Frame Size

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

The calculated average frame size (see §3.2) through the configured service directly influences the BWE. The higher the frame size, the better or higher the BWE. A higher frame

size automatically results in more payload bytes compared to overhead bytes, resulting in a better BWE. Examples:

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

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

CAUTION:

When the real or measured average frame size is reasonably lower than the configured average frame size, extra delay and/or frame loss can occur! Frame loss can be detected and verified via the 'Disc In Packets'/'Disc Out Packets' counters, see §15.2.1.

When the real or measured average frame size is reasonably higher than the configured average frame size, a lower BWE will be obtained but traffic will not be influenced.

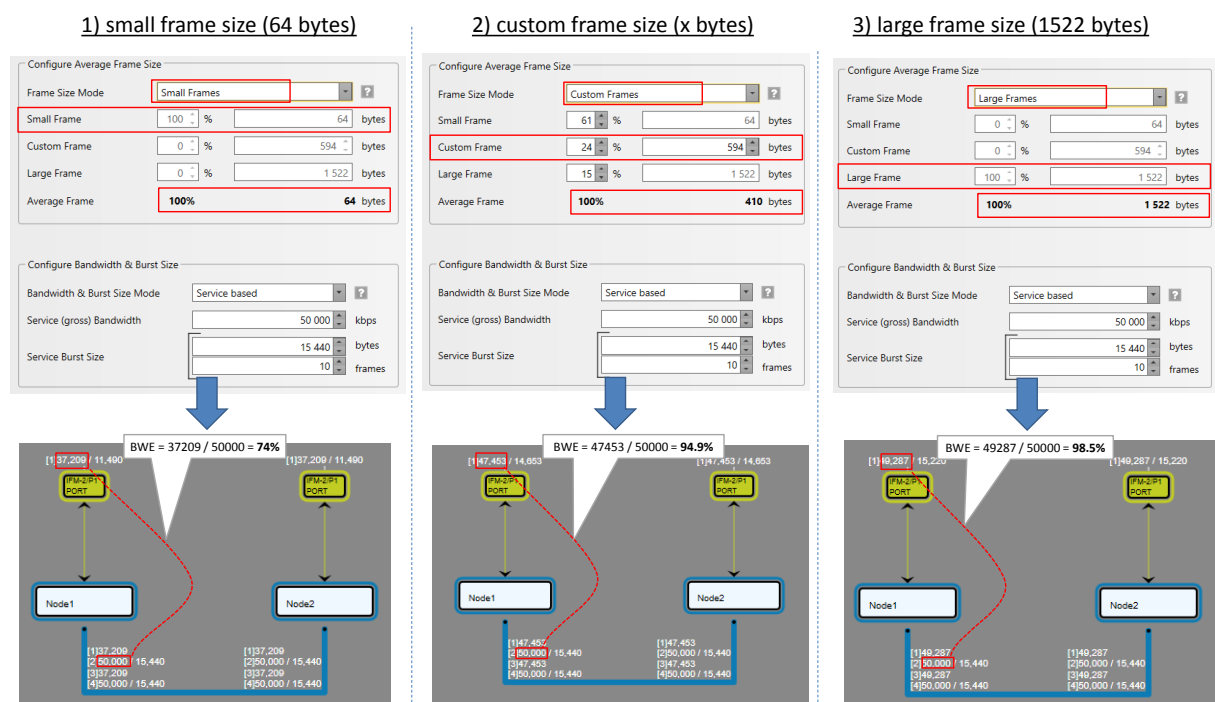


Figure 80 Bandwidth Efficiency Examples in HiProvision

3.7.2 Tuning the Ports Input Bandwidth

See §3.2.6.

3.7.3 Tuning Bandwidth/Delay for Serial Ethernet Services

See §2.13.5a.

3.8 (Service) Bandwidth Already Configured on WAN Links

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

3.8.1 General

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

Max. Service Bandwidth = Max. WAN link bandwidth – Overhead – DCN bandwidth

The overhead depends on:

The configured Average Frame Size;

► Bandwidth for the DCN Channel = depends on link type, see §3.9;

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

E.g. worst case scenario: inefficient Ethernet frames = frame size is 64 bytes = 100% small frames = little data with a lot of overhead.

Due to overhead and worst case scenarios (frame size is 64 bytes) and reserved bandwidth for the DCN Channel (see §3.9), the maximum service bandwidth can be configured up to 711 Mbps per WAN link in both directions. E.g. worst case scenario: inefficient Ethernet frames = 100% small frames = little data with a lot of overhead.

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

'x' = service bandwidth including 'L2 Ethernet Frame' data and MPLS-TP overhead;

'y' = endpoint bandwidth including only 'L2 Ethernet Frame' data;

► 'y' is always less than 'x' with the maximum of 'x' = 711 Mbps;

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

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

3.8.2 Connections Tab

a. Overview

Via the Connections tab, the bandwidth occupation (% , color) can be shown per link. Click a link in the Links table (see figure) to show the network drawing. The link is encircled in the network drawing and a cross-section of that link with all its details is split out at the bottom section. The link colors indicate the bandwidth occupation severity, which can be adapted via the color slider.

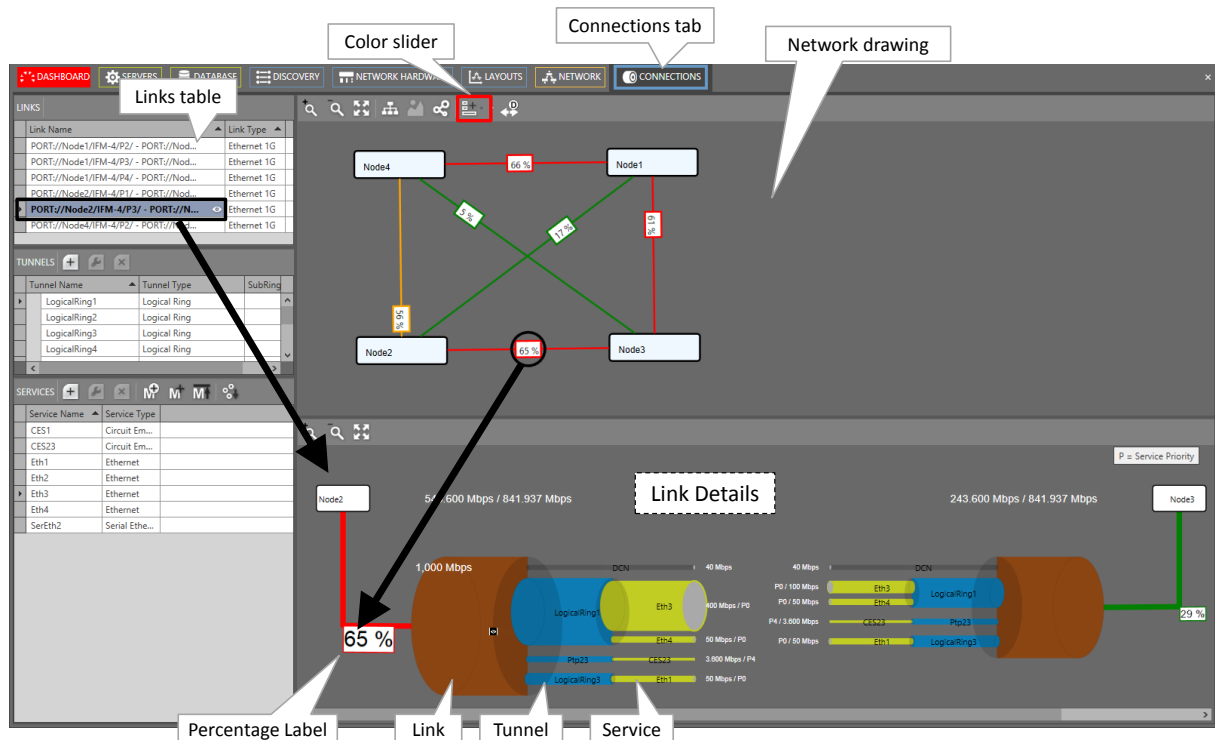



Figure 81 Connection Tab: Bandwidth Information

b. Link Bandwidth Occupation: Percentage, Status Color

Percentage label:

- ▶ x%: used bandwidth, x percent of the available link bandwidth;
- ▶ In the network drawing: If a percentage label hides another percentage label of an underlying link, the top label can be dragged aside after having it clicked first;
- ▶ In the network drawing: clicking the  button relays the percentage labels on the link;

Status color = color indication of the bandwidth occupation percentage. The list below shows the colors for the default occupation ranges. The ranges can be modified via the color sliders:

- ▶ green (0-30%): low;
- ▶ orange (30-60%): medium;
- ▶ red (60-80%): high;
- ▶ dark red (80-100%): critical;

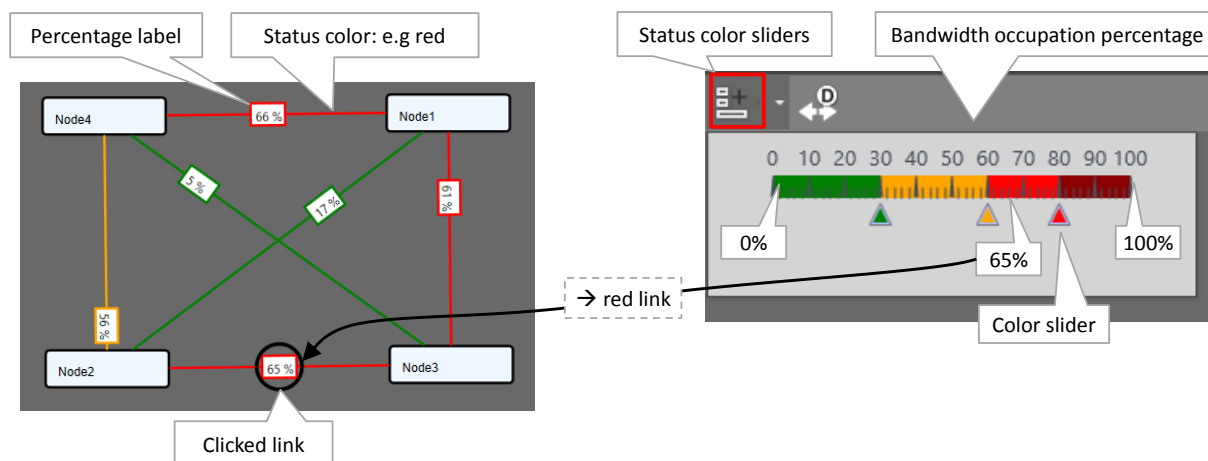




Figure 82 Bandwidth Percentage Label and Status Colors

c. Link Details

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

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

The bandwidth occupation for this link in this direction is 65% (= 543.6/841.937). This results in a red status color for the link according to the color slider settings. The used DCN bandwidth is also shown and depends on the link type, see §3.9.

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

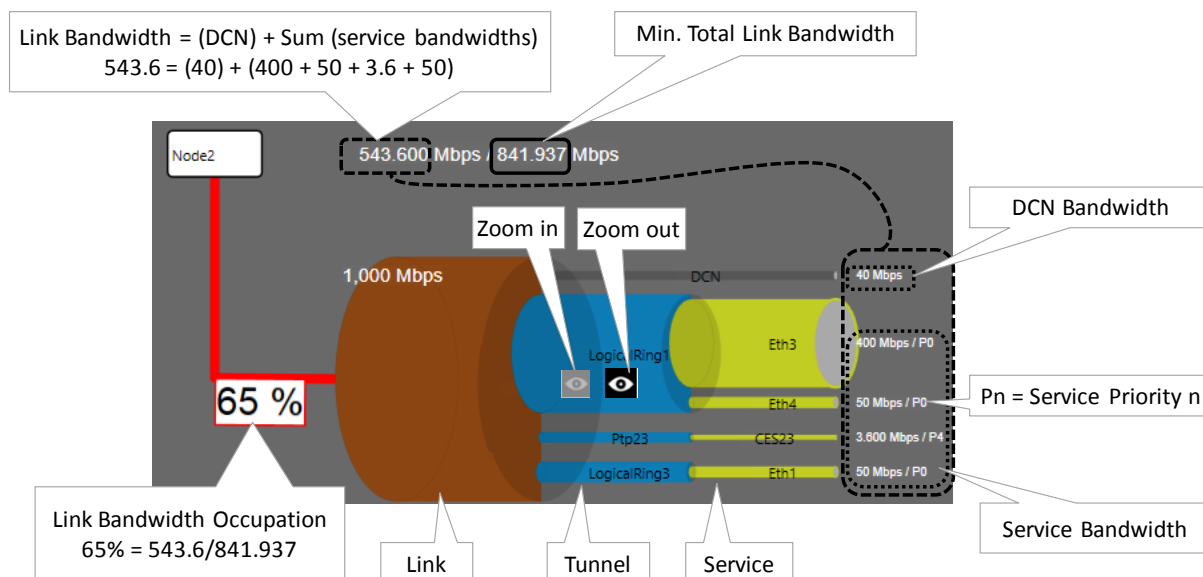


Figure 83 Link Details

d. Two Bandwidth Directions in one Link

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

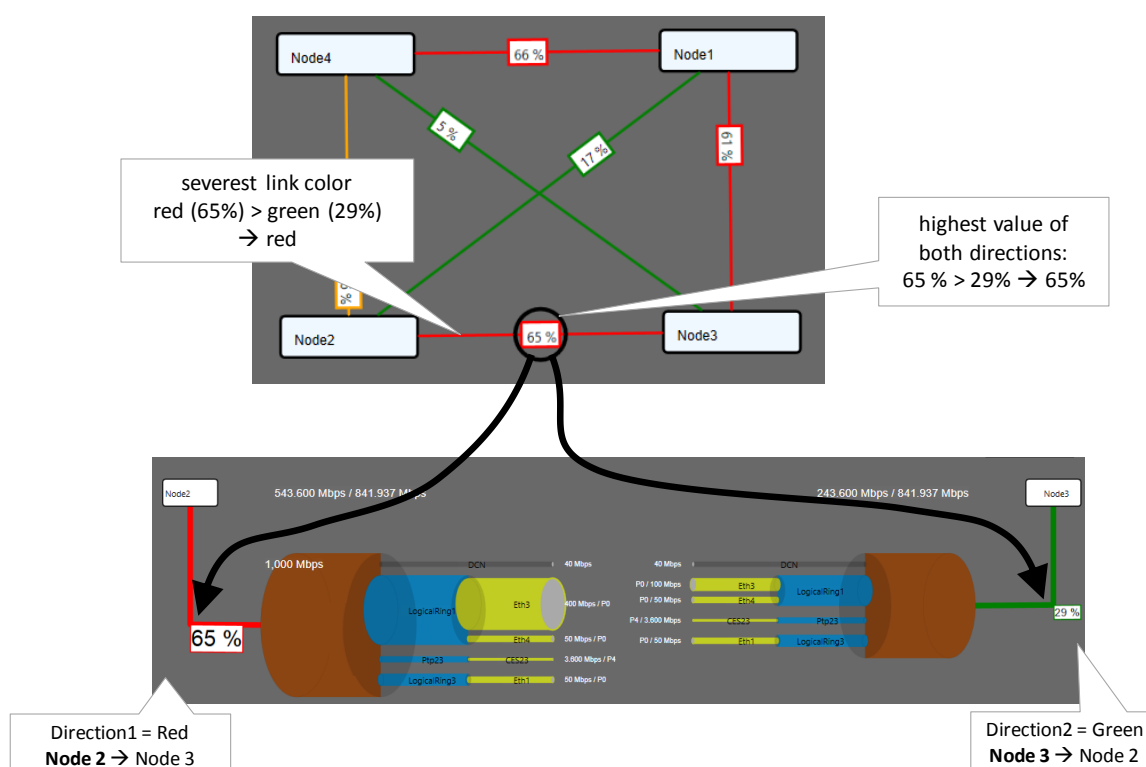


Figure 84 Highest Value and Severest Color

3.9 DCN Channel

3.9.1 Bandwidth Profile

DCN (=Data Communication Network). The DCN Channel is the Dragon PTN network management channel which is deployed dynamically over each link of the entire network during the discovery phase, see §2.6.

The bandwidth of this channel can be configured per individual 1G/10G 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 §12.

NOTE: The DCN Bandwidth Profile must always be less than the Link Capacity (see §3.10).

This configured bandwidth is automatically reserved during discovery.

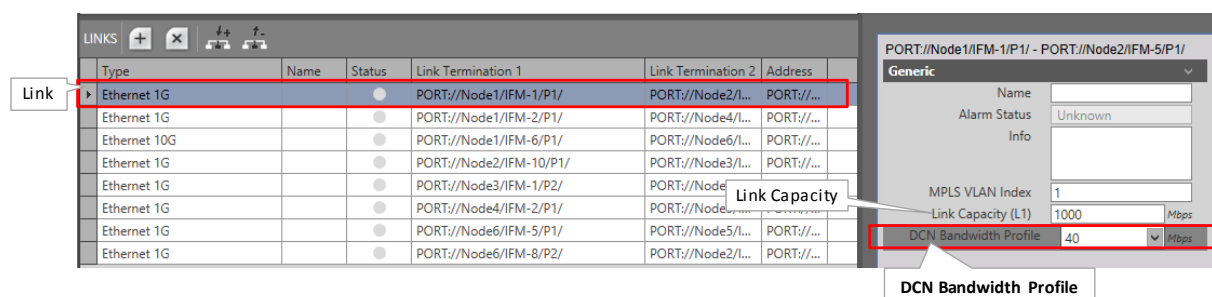


Figure 85 Link: DCN Bandwidth Profile

3.9.2 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;

3.10 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;

NOTE: The Link Capacity must always be more than the DCN Bandwidth Profile (see §3.9.1);

The screenshot shows the 'LINKS' table in the Network Hardware section. The first row, 'Ethernet 1G', is selected. To the right, the 'Generic' configuration panel is open for the selected link. In the 'Generic' panel, the 'Link Capacity (L1)' is set to 1000 Mbps, and the 'DCN Bandwidth Profile' is set to 40 Mbps. A red box highlights the 'Link Capacity (L1)' field, and a callout points to it with the text 'Link Capacity'. Another red box highlights the 'DCN Bandwidth Profile' field, and a callout points to it with the text 'DCN Bandwidth Profile'.

Type	Name	Status	Link Termination 1	Link Termination 2	Address
Ethernet 1G		●	PORT://Node1/IFM-1/P1/	PORT://Node2/L...	PORT://...
Ethernet 1G		●	PORT://Node1/IFM-2/P1/	PORT://Node4/L...	PORT://...
Ethernet 10G		●	PORT://Node1/IFM-6/P1/	PORT://Node6/L...	PORT://...
Ethernet 1G		●	PORT://Node2/IFM-10/P1/	PORT://Node...	PORT://...
Ethernet 1G		●	PORT://Node3/IFM-1/P2/	PORT://Node...	PORT://...
Ethernet 1G		●	PORT://Node4/IFM-2/P1/	PORT://Node5/L...	PORT://...
Ethernet 1G		●	PORT://Node6/IFM-5/P1/	PORT://Node5/L...	PORT://...
Ethernet 1G		●	PORT://Node6/IFM-8/P2/	PORT://Node2/L...	PORT://...

Generic configuration for PORT://Node1/IFM-1/P1/ - PORT://Node2/IFM-5/P1/:

- Name: [Empty]
- Alarm Status: Unknown
- Info: [Empty]
- MPLS VLAN Index: 1
- Link Capacity (L1): 1000 Mbps
- DCN Bandwidth Profile: 40 Mbps

Figure 86 Ethernet Link: Link Capacity

3.11 Storm Control on Ethernet LAN Port

3.11.1 General

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

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

The storm control feature:

is an extra protection against these traffic storms;

limits the amount of unlearned received data (Unicast, Broadcast, Multicast) on the LAN port ingress or input side;

limits the amount of transmitted data (all data) on the LAN port egress or output side;

Data that exceeds the configured limitations will be dropped. As a result, a possible data storm cannot overload the node processor or the node will limit outgoing data.

3.11.2 Configuration

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

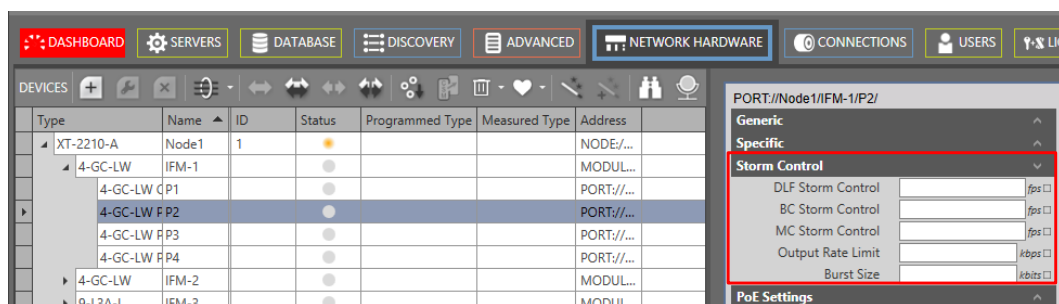


Figure 87 Port Properties: Storm Control

Ingress (or input) traffic on a LAN port:

- ▶ DLF (default = no limits, range [0-262142] fps): DLF = Destination Lookup Failure, limits the incoming unicast traffic with an unknown destination to the configured frames per second (=fps);
- ▶ BC (default = no limits, range [0-262142] fps): BC = Broadcast, limits the incoming Broadcast traffic to the configured frames per second (=fps);
- ▶ MC (default = no limits, range [0-262142] fps): MC = Multicast, limits the incoming Multicast traffic to the configured frames per second (=fps);

Egress (or output) traffic on a LAN port:

- ▶ Output Rate Limit (default = no limits, range [0-16777215] kbps): limits all outgoing traffic to the configured kbps;
- ▶ Burst Size (default = no limits, range [0-80000000] kbits): limits the outgoing burst size to the configured kbits;

▶ Click the Apply button;

Load (see §5) to network.


NOTE: Frame loss or drop can be detected and verified via dropped packet alarms (in the Alarms tile) and the 'Disc In Packets'/'Disc Out Packets' counters (in the performance Tile), see §15.2.1.

3.11.3 Reset Storm Control

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

3.11.4 When to Reset Storm Control on a Port?

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

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

4. ALARM HANDLING

4.1 General

When an alarm situation occurs in a Dragon PTN network, a corresponding alarm will be raised in HiProvision. These alarms can be detected and viewed in several ways in HiProvision:

- Dashboard → (Monitoring) Alarms Tile;
- Dashboard → (Monitoring) Network Tile;
- Dashboard → (Configuration) Network Hardware Tile;

A flashing dashboard tab indicates active alarms;

4.2 Hardware: Measured/Programmed/Configured Values

This paragraph describes the concept of configuration consistency and synchronization between HiProvision and the live network.

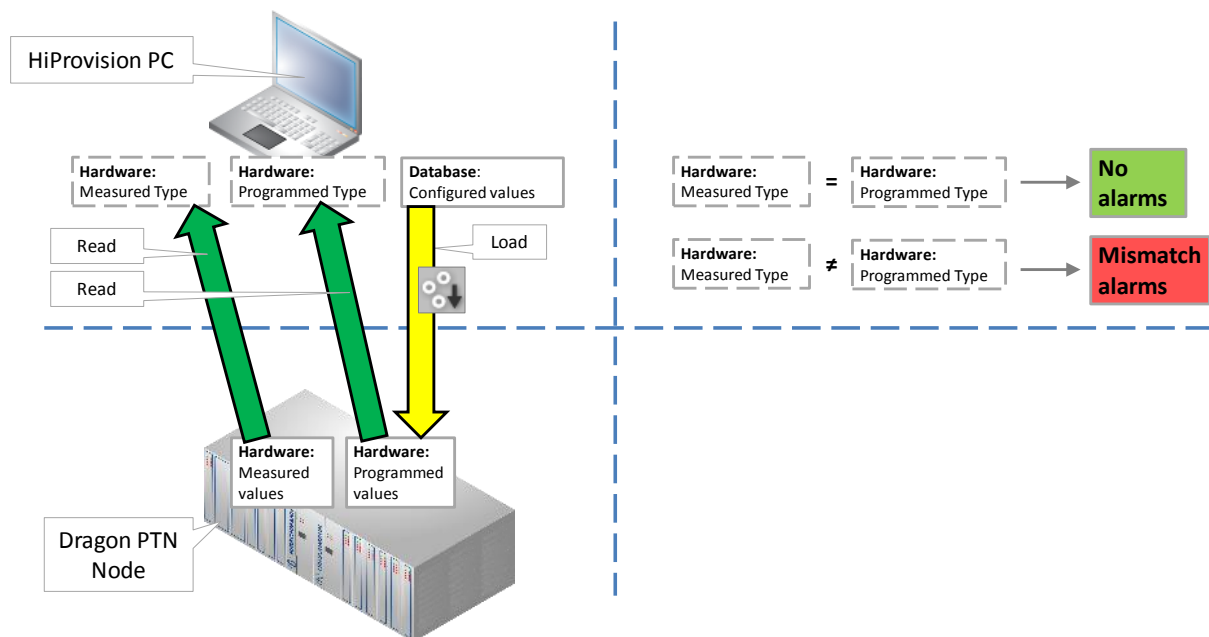


Figure 88 Measured / Programmed / Configured Values

- Measured values: network elements (e.g. PSUs, CSM, Interface Modules,) that are really physically present in the live network or nodes and which are measured or read by HiProvision. These values are read and filled out by HiProvision in the Measured Type field (Network Hardware tab) of the node modules;
- Programmed values (=expected values): programmed configuration (e.g. PSUs, CSM, Interface Modules,) available in the live network or nodes. This online configuration is a result of a load action via HiProvision. This programmed configuration is read and filled out by HiProvision in the Programmed Type field (Network Hardware tab) of the node modules;

- Configured values: database configuration (e.g. PSUs, CSM, Interface Modules, ...) that a HiProvision administrator configures in HiProvision. Via a load action, the database configuration is loaded from HiProvision into the programmed values in the live network.

If not all values (measured, programmed and configured) are the same, a mismatch alarm will be raised. E.g. if you configured and programmed a 4-GC-LW module in slot1 of node 100 but slot1 of node 100 is empty in the live network, a mismatch alarm will be raised.

4.3 Alarm Sensitive Properties in HiProvision

An alarm sensitive property in the Network Hardware tile is a property:

marked by a little square box behind the field, see figure below;

that has two fields:

- upper field1: Measured value from the live Dragon PTN network;
- lower field2: Configured expected value in HiProvision. This field is only visible after clicking the little square box;

HiProvision polls and measures the Dragon PTN network. If a mismatch occurs between the measured and the configured expected value for this property, an alarm is raised and the little square box gets the alarm color.

Little box color:

- Grey: everything is ok, no alarm;
- other color: alarm active, see §4.4;

The screenshot displays the 'NETWORK HARDWARE' section of the HiProvision interface. A table lists various ports, including 'ExtDevType2 - Port1' through 'Port8'. The 'Status' column shows a red square box next to 'Port1', indicating an alarm. A detailed view of 'PORT/ExtDev20/P1' is shown on the right, with 'User Defined Parameters' expanded. The 'Speed/Duplex' parameter is set to '100 Mbps Full Duplex' (measured) and '1000 Mbps Full Duplex' (configured). A red square box is placed over the '1000 Mbps Full Duplex' value. A callout box explains: 'Square box = Alarm sensitive: Click to configure expectation'. Another callout box explains: 'measured (100) ≠ configured (1000) → mismatch → little square = red = alarm raised'.

Figure 89 Alarm Sensitive Properties: Little Square Box

4.4 Alarm Colors and Severity

The severity of an alarm is indicated by a color:

Dark red: Critical alarm (highest severity);

Red: Major alarm;

Orange: Minor alarm;

Yellow: Warning (lowest severity);

4.5 Alarms Tile and Window

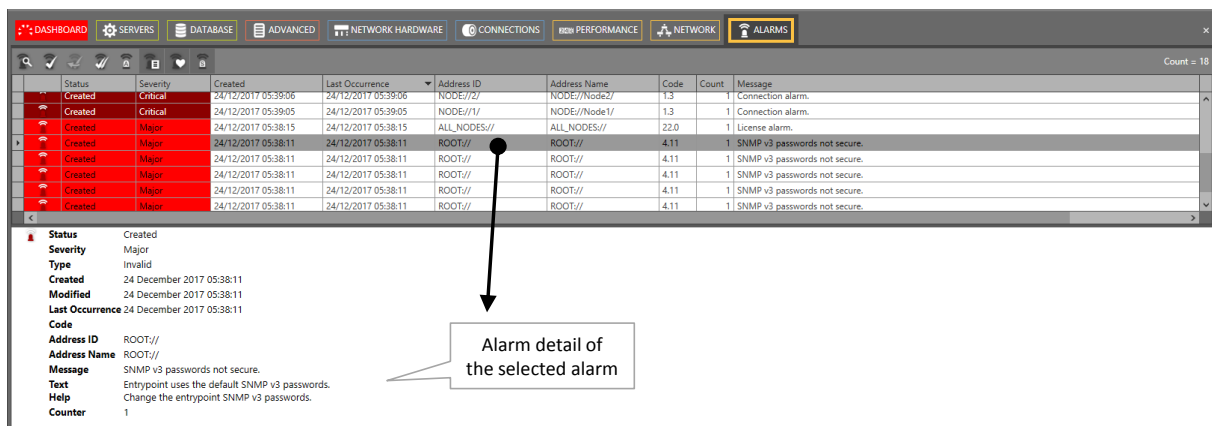
4.5.1 The Tile Itself

The Dashboard → Alarms tile itself indicates the active alarms. The tile color indicates the color of the severest alarm that is still active, see §4.2 for alarm colors and severity.

4.5.2 Alarms Window

Clicking the Alarms tile shows the window below. It lists all the alarms with some basic information whereas the bottom section shows detailed information of the selected alarm.

NOTE: An overview of all the possible alarms can be found in Ref.[19] in Table 1.



The screenshot shows the 'ALARMS' window with a table of active alarms. The table has columns: Status, Severity, Created, Last Occurrence, Address ID, Address Name, Code, Count, and Message. The selected alarm is highlighted in red. Below the table, the 'Alarm detail of the selected alarm' is shown, including fields for Status, Severity, Type, Created, Modified, Last Occurrence, Code, Address ID, Address Name, Message, Text, Help, and Counter.

Status	Severity	Created	Last Occurrence	Address ID	Address Name	Code	Count	Message
Created	Critical	24/12/2017 05:39:06	24/12/2017 05:39:06	NODE//2/	NODE//Node2/	1.3	1	Connection alarm.
Created	Critical	24/12/2017 05:39:05	24/12/2017 05:39:05	NODE//1/	NODE//Node1/	1.3	1	Connection alarm.
Created	Major	24/12/2017 05:38:15	24/12/2017 05:38:15	ALL_NODES//	ALL_NODES//	22.0	1	License alarm.
Created	Major	24/12/2017 05:38:11	24/12/2017 05:38:11	ROOT//	ROOT//	4.11	1	SNMP v3 passwords not secure.
Created	Major	24/12/2017 05:38:11	24/12/2017 05:38:11	ROOT//	ROOT//	4.11	1	SNMP v3 passwords not secure.
Created	Major	24/12/2017 05:38:11	24/12/2017 05:38:11	ROOT//	ROOT//	4.11	1	SNMP v3 passwords not secure.
Created	Major	24/12/2017 05:38:11	24/12/2017 05:38:11	ROOT//	ROOT//	4.11	1	SNMP v3 passwords not secure.
Created	Major	24/12/2017 05:38:11	24/12/2017 05:38:11	ROOT//	ROOT//	4.11	1	SNMP v3 passwords not secure.

Field	Value
Status	Created
Severity	Major
Type	Invalid
Created	24 December 2017 05:38:11
Modified	24 December 2017 05:38:11
Last Occurrence	24 December 2017 05:38:11
Code	ROOT//
Address ID	ROOT//
Address Name	ROOT//
Message	SNMP v3 passwords not secure.
Text	Endpoint uses the default SNMP v3 passwords.
Help	Change the endpoint SNMP v3 passwords.
Counter	1

Figure 90 Alarms Window

NOTE: You could use additional table filters for filtering out alarms, see also §26.1.2e.

NOTE: Raised Timestamp (field only visible in Alarms detail when alarm raised by hardware): In the Alarm Detail, 'Created' indicates the timestamp when the alarm was created in HiProvision whereas 'Raised Timestamp' indicates the timestamp when the alarm occurred somewhere in the hardware. Most of the time, the alarm is raised in HiProvision itself resulting in only the 'Created' field filled out. Some alarms are raised in hardware (not in HiProvision), resulting in both the 'Raised Timestamp' and 'Created' field filled out. Good to know: 'Raised Timestamp' = value set by node = UTC, 'Created' = MS Windows PC time UTC + offset!

4.5.3 Alarm Colors and Severity



The alarm severity is indicated in the Severity column and reflected by the row color in the list. The meaning of the colors can be found in §4.2.

4.5.4 Alarm Status

The alarm status is indicated by a status icon and column in the list, see below. An alarm disappears automatically out of the list after it has been cleared and acknowledged.












Created: alarm is active but not yet acknowledged;



- ▶  Acknowledged: alarm has been acknowledged, it means that the operator has indicated that he/she is aware of the alarm existence;
-  Cleared: alarm has disappeared or the error situation has gone before it has been acknowledged.

4.5.5 Action Buttons









The buttons below can be used to handle alarms in the alarm window:

- ▶ : Navigate to the source of the selected alarm or warning in HiProvision for further investigation;
- ▶ : Acknowledge the selected alarm or warning, the status icon changes into ;
- : Acknowledge all the alarms and warnings, all the status icons changes into ;
- ▶  (enabled): Auto-Acknowledge of alarms is enabled, all new alarms are acknowledged automatically without any user action. Clicking this icon disables it;
-  (disabled): Auto-Acknowledge of alarms is disabled. Clicking this icon enables it;
- ▶  (enabled): Alarm logging to a log file is enabled. Clicking this icon disables it;
- ▶  (disabled): Alarm logging to a log file is disabled. Clicking this icon enables it;

NOTE: Log file in <HiProvision Install
Path>\HiProvision\HiProvision_VX.Y.Z\Logging\System Logging\Alarms

- ▶  (enabled): 'Keep alarm logging alive' is enabled. If no alarm has been raised the last hour, an event is written to the Event log file. Clicking this icon disables it;
- ▶  (disabled): 'Keep alarm logging alive' is disabled. If no alarm has been raised the last hour, nothing is written to the Event log file. Clicking this icon enables it;

NOTE: Event log file in <HiProvision Install
Path>\HiProvision\HiProvision_VX.Y.Z\Logging\System Logging\LogEvents

- ▶  (enabled): All the alarms, including the SysLog alarms are shown together in one list in the alarm window. Clicking this icon disables it;
-  (disabled): SysLog alarms are filtered out from the other alarms and shown in a separate list at the bottom section of the alarm window. Clicking this icon enables it;
- ▶  (greyed out):  is enabled. Syslog events are integrated in the alarms list itself and as a result cannot be shown/hidden separately.
- ▶  (enabled):  is disabled. Shows the separate SysLog alarms at the bottom of the page.
-  (disabled):  is disabled. Hides the separate SysLog alarms at the bottom of the page.


SysLog alarms:

- ▶ are alarms and events generated by the system itself e.g. authentication failure etc. which are quite different from Dragon PTN network configuration alarms;
- ▶ are only visible in the Created state;
- ▶ are removed from the alarm list immediately after it has been acknowledged;
- ▶ never clear automatically, they will be cleared when they are acknowledged;

4.6 Alarms in (Monitoring) Network Tile

4.6.1 Network Example

Depending on the network element (device/link/tunnel/service), alarms are visualized in various ways (colors, colored bullets, cloud icons) on various locations (tables, network drawing, navigation section) in the Network Tile. See some example figures below. More information about the alarms and the meaning of them can be found further on.

NOTE: Cloud icons  refer to alarms related to 'External E1 Links' interconnecting the Dragon PTN network over an external network, see also §2.7.2b.

NOTE: Displayed Column: 'X' indicates the selected network element, '(x)' indicates a linked network element of the selected 'X' network element, see also §4.6.4.

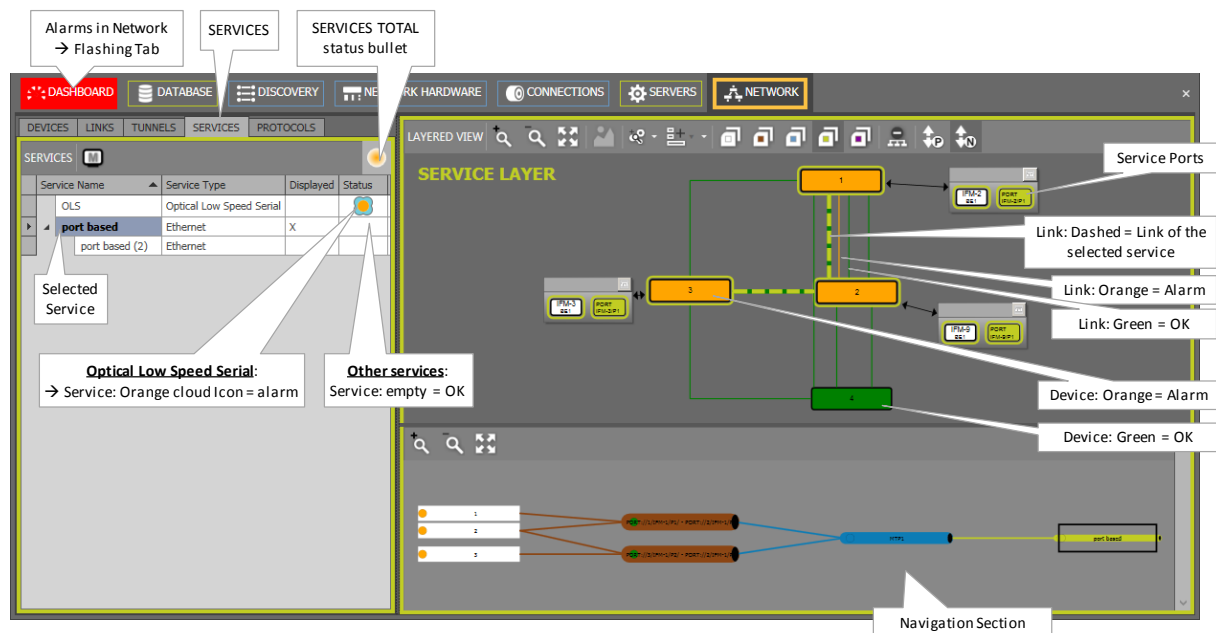


Figure 91 Alarms in Example Network: Services Tab

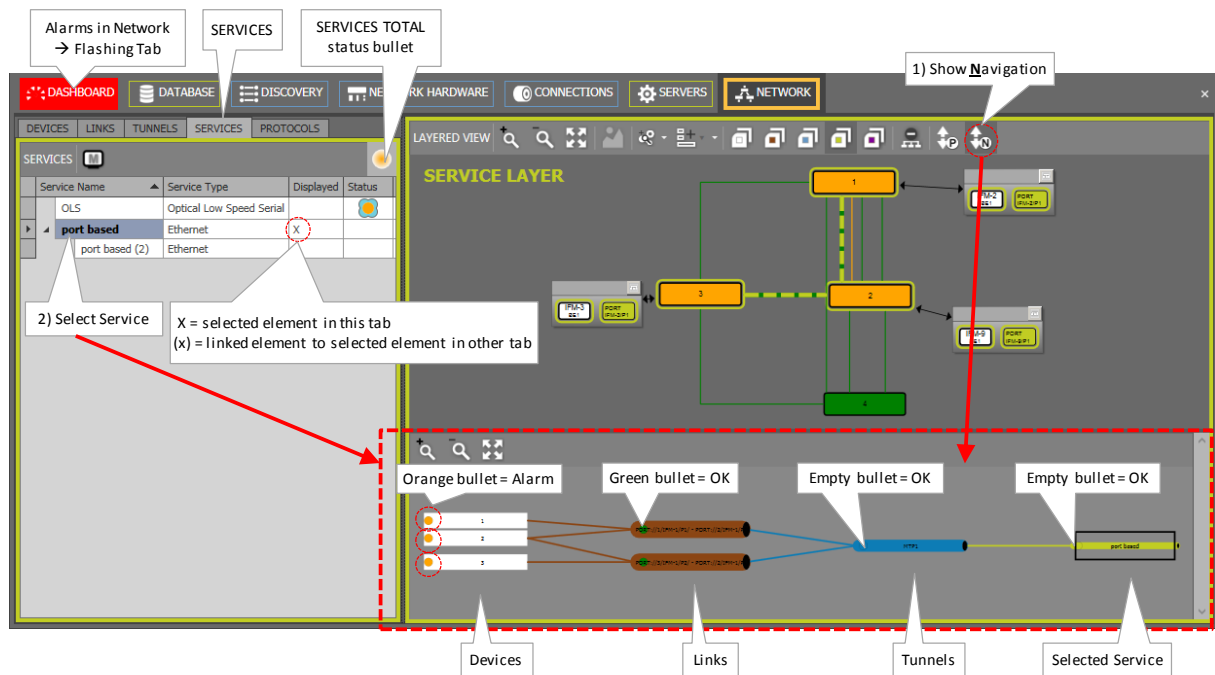


Figure 92 Show Navigation (N) of Selected Device/Link/Tunnel/Service

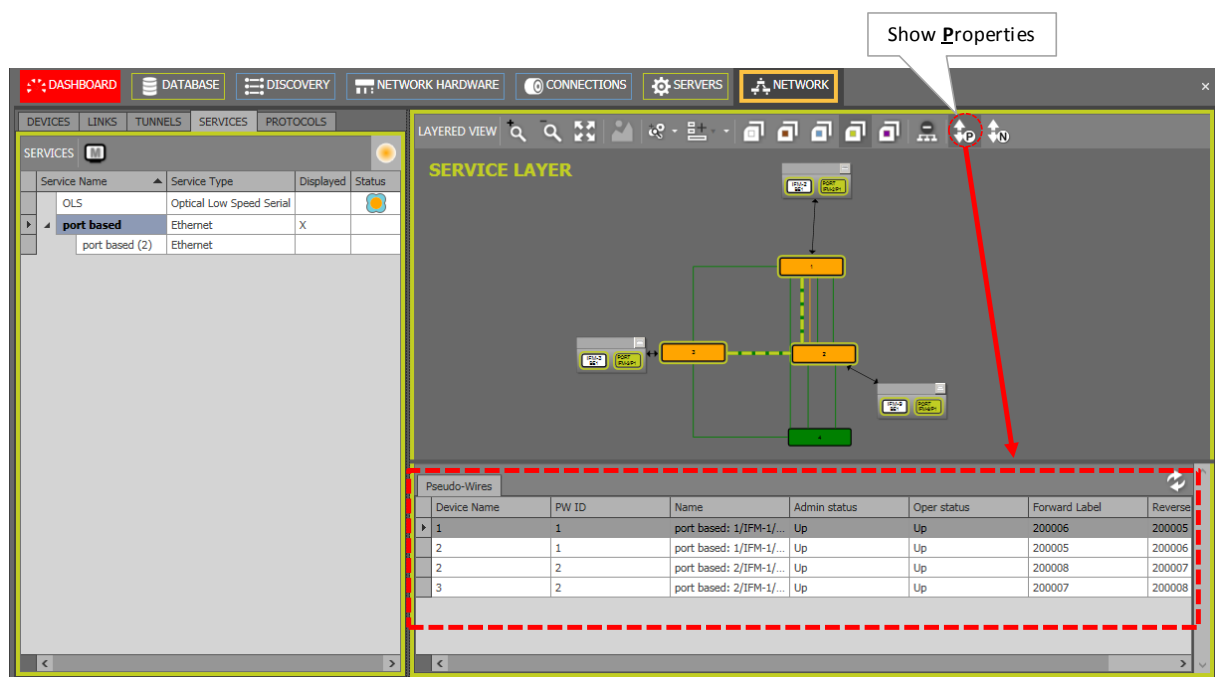


Figure 93 Show Detailed Properties (P) of Selected Tunnel or Service

4.6.2 Menu Buttons

Table 15 Menu Buttons

Button	Short Description
	Zoom in / Zoom out in the network drawing
	Fit content, the layout is maximally fitted within the HiProvision screen. If your nodes and links look lost, click this button to bring them back in focus.
	Shows/hides the background picture of this network drawing. If there is no background picture, the button will be greyed out.
	Commit: Commits the pending upgrades, modules or nodes will swap to another image and will reboot
	Checked/Unchecked: shows/hides the link labels (on both sides of the link) in the network drawings. A link label shows the Interface Module slot and the used link port in that Interface Module e.g. 'Interface Module-4/P2'.
	Displays the clicked or selected device Layer (white)/ Link Layer (brown) /Tunnel Layer (blue)/ Service Layer (green) / Protocols Layer (purple). Clicking or selecting a row in the associated table (or tab) has the same effect as clicking these buttons. Note: the Protocols Layer is used for MRP (see §7.2) monitoring.
	When having selected a service in the services table, this icon can be clicked to collapse all service port information in the network drawing. As a result, the network drawing is less detailed and shows a better overview. See the figure below for some extra options. <div data-bbox="383 952 1412 1220"> </div>
	Shows/hides the monitoring P roperties of the selected tunnel or services, see example Figure 93.
	Shows/hides the N avigation of the selected element. It shows how the selected network element is interconnected with other elements, see example Figure 92.

4.6.3 Status / Colors / Bullets / Clouds










The meaning of the alarm colors can be found in §4.2.

The table below lists the possible alarm indications and how they are visualized on the different network elements and locations.

When an alarm color turns green (devices/links) or disappears (tunnels/services), it means that the alarm has been cleared on this network element. It cannot be viewed in this screen whether an alarm has been acknowledged, see also §4.5.

Table 16 Alarm Indications

Network	Alarms in	Alarms in	Alarms in
---------	-----------	-----------	-----------

Element	Network Element Table (or Tab)	Network Drawing	(N) Navigation Section
Device	- per network element via colored status bullets; - per network element table (or tab): one colored status bullet for the entire table in the top right-hand corner indicating the severest alarm color of all its network elements in the table. E.g. if you have two devices e.g. with status bullet of device1 = 'orange' and status bullet of device3 = 'green', the total status bullet of the devices will be 'orange' (orange is more severe than green).	- Via colored device icons; - No alarm, everything ok = green device icon; - Offline: grey device icon;	- Via colored status bullets; - No alarm, everything ok = green status bullet; Offline = grey bullet;
Link		- Via colored links - No alarm, everything ok = green link; - Offline: grey link;	- Via colored status bullets; - No alarm, everything ok = green status bullet; - Offline = grey bullet;
Tunnel		None	- Via colored status bullets; - No alarm, everything ok, offline = Empty status bullet;
Service		None	- Via colored status bullets - No alarm, everything ok, offline = Empty status bullet;
Protocols	None	None	None
<p>Note: If the network element is involved in an 'External E1 Link', its colored status bullet will be embedded in the cloud icon  in the Tables and Navigation Section.</p> <ul style="list-style-type: none"> -  = External E1 Link: (empty): No 'Optical Low Speed Serial (=OLS)' service on this link → link ports and link are down; -  = External E1 Link: (grey) link status unknown, HiProvision offline; -  = External E1 Link: (green), OLS service on this link, link is up and running, all OK; -  = External E1 Link: (yellow), OLS service on this link, warning on link; -  = External E1 Link: (orange), OLS service on this link, minor alarm on link; -  = External E1 Link: (red), OLS service on this link, major alarm on link; -  = External E1 Link: (dark red), OLS service on this link, critical alarm on link; <p>If an 'External E1 Link' is selected, its cloud icon  will be shown on the link in the network drawing as well.</p>			

4.6.4 Selected Network Elements

In the table section on the left-hand side, the selected element shows an 'X' in the Displayed column. All the other related network elements in the other Tabs (e.g. Devices, Links, Tunnels) show a '(x)' in the Displayed column. In the network drawing, the selected network element will be highlighted.

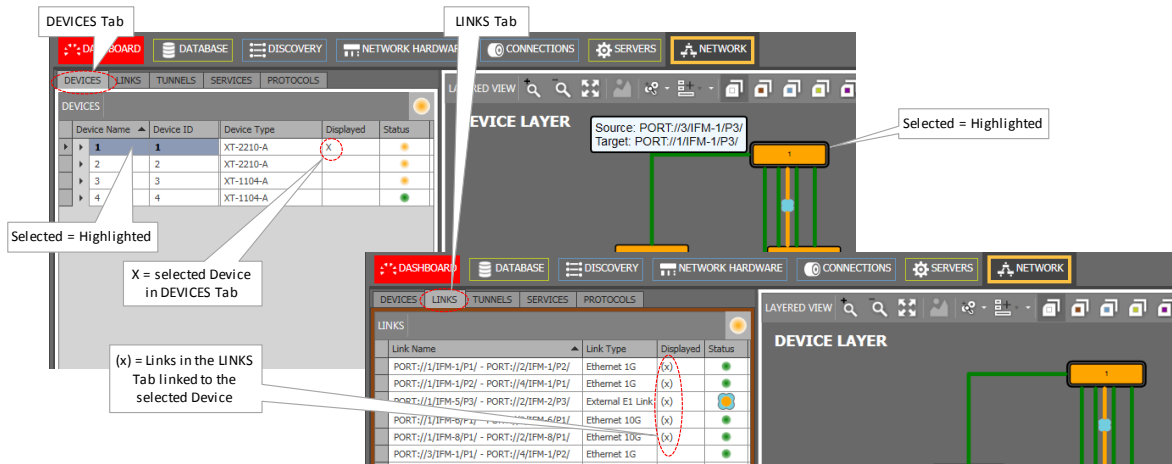


Figure 94 Selected Network Elements: X / (x) in Displayed Column

4.6.5 Protected Tunnel: Broken Working Path

The example below differs from the example in previous paragraph. It indicates via '//' how to see whether a working path in a protected tunnel is broken or the protection path is active. This view is visible when selecting a tunnel or tunnel layer in the (Monitoring) Network Tab. Also have a look at §10.5.2.

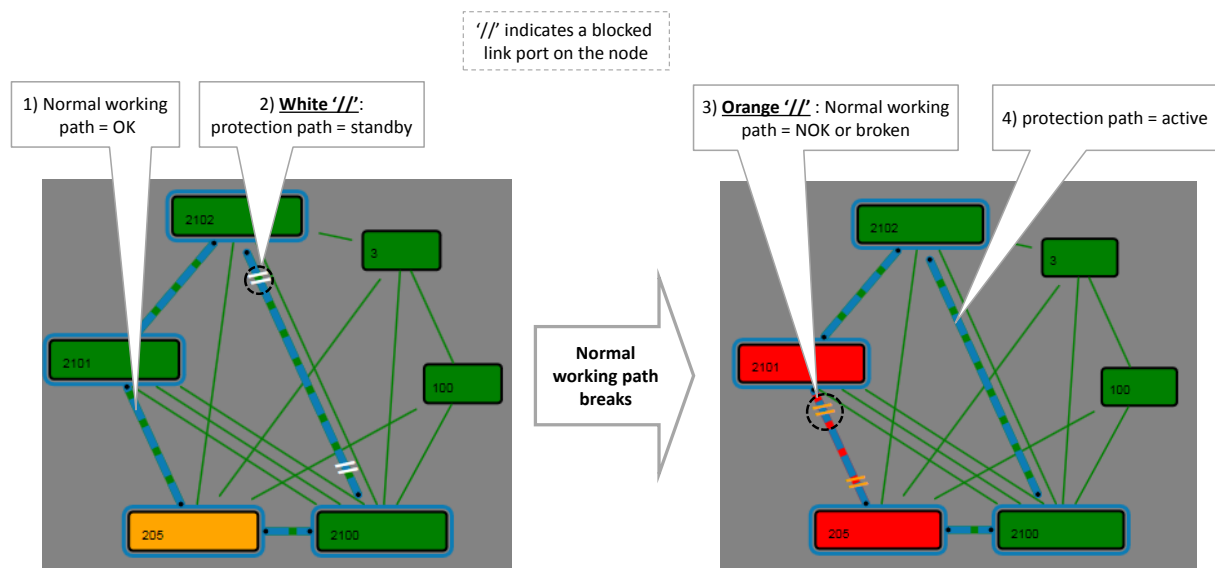


Figure 95 Protected Tunnels: Protection Path, Blocked Port Indication: '//'

4.7 Alarms in (Configuration) Network Hardware Tile

After clicking the Network Hardware tile, a window like Figure 33 pops up. The status bullets in the devices and links list indicate whether the network element has alarms or not. See §2.8 for more info.

4.8 Configure Alarms for NSM Digital Input Contacts

An alarm can be assigned to the NSM digital inputs DI1/DI2. It means that a change in these contacts can raise an alarm in the Alarms Window (see §4.5.2). The alarm can be configured via the Network Hardware tile by clicking the NSM in the desired node and filling out the I/O section on the right-hand side.

An alarm will be raised for DI1 when following two conditions are met (similar for DI2):

- ▶ 'DI1 Current Detected' mismatches the configured expectation for this field. The expectation can be configured via clicking the little square box behind the field and selecting Yes/No. Example mismatch: the expectation is 'Yes' and no current is detected (=DI1 Current Detected = 'No') (or vice versa);
- ▶ A severity different from 'none' has been configured;

Following fields can be configured for DI1 (similar for DI2):

DI1 Input:

- ▶ DI1 Current Detected (Yes/No): Indicates whether input current has been detected; Configure the expectation via the little square box;
- ▶ DI1 Alarm Severity: None (=default), Indeterminate, Warning, Minor, Major, Critical; 'None' means that no alarm will be raised for this input;
- ▶ DI1 Alarm message: Fill out a short alarm message that will appear in the (Alarms Window);
- ▶ DI1 Alarm Text: extra info to describe the alarm (Alarms Window - detail);
- ▶ DI1 Alarm Help: what to do when this alarm occurs (Alarms Window - detail).

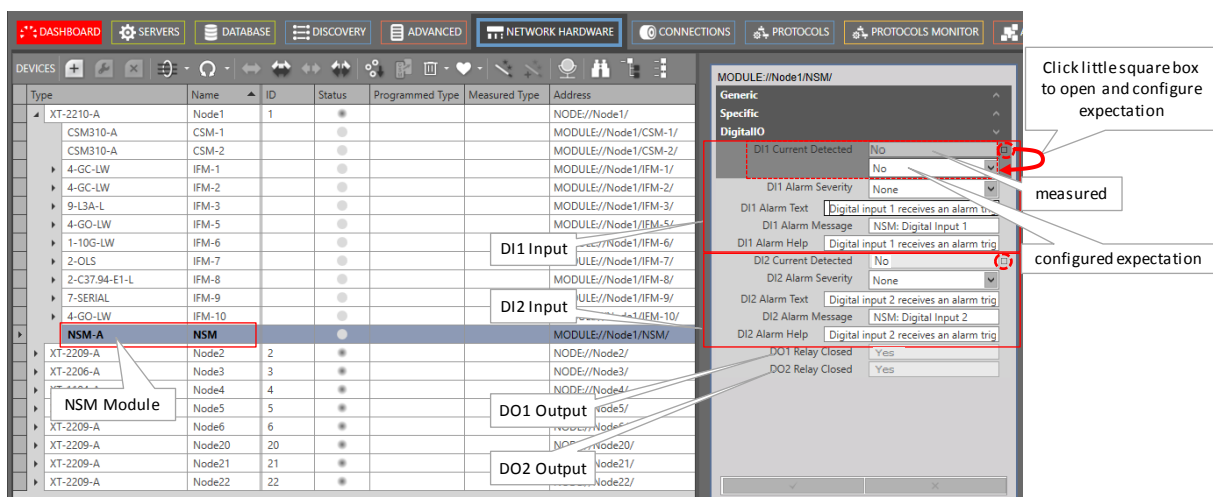


Figure 96 NSM Digital I/O Contacts

4.9 Device Alarms via Digital Output Contacts on the NSM

4.9.1 General

The CSM supervises all the hardware in the node and generates the necessary device alarms when something is wrong in the node. These alarms are collected by HiProvision. HiProvision can be configured to output one or more of these device alarms to the digital output contacts (DO1=minor, DO2=major) on the NSM (=Node Support Module).

NOTE: The measured state of the output contacts DO1/DO2 can be viewed in Figure 96.

These contacts can be used for example to activate an alarm siren. The NSM can be found in the nodes manual, see Ref. [2] in Table 1.

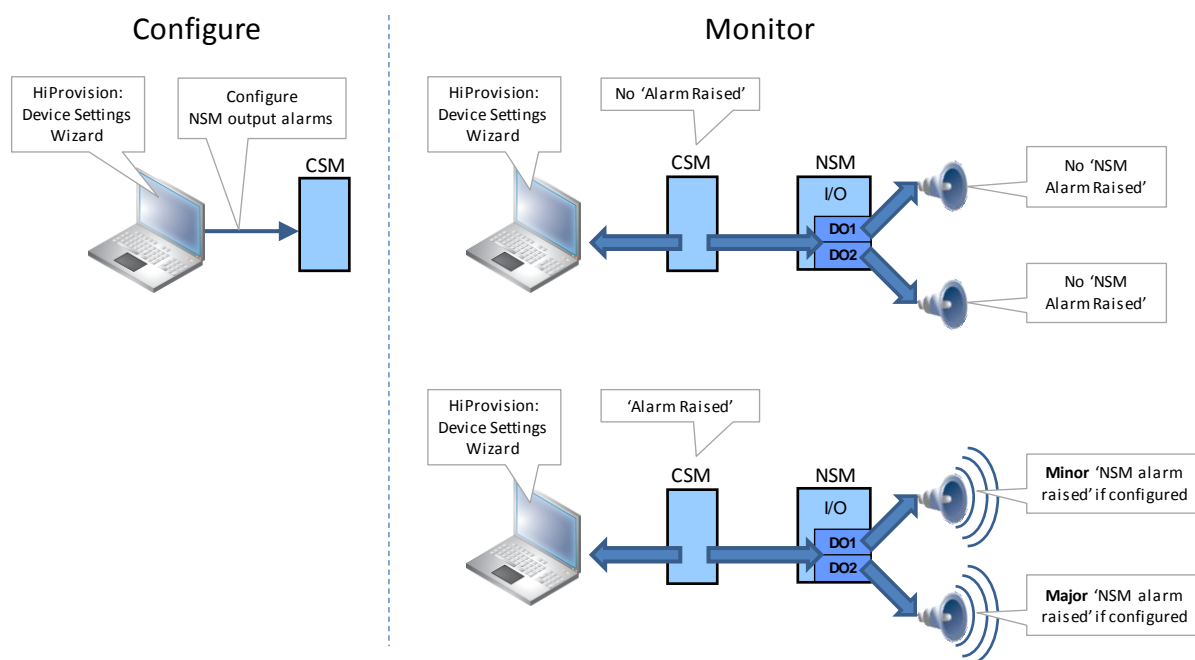



Figure 97 Operation Of Device Alarms/Digital Outputs

4.9.2 Device Settings Wizard

These alarms can be configured via the Device Settings. Select the CSM of the intended node, click the  button, select 'Digital Output' and fill out the Alarm Severity and Alarm Trigger by clicking the cell and selecting a value. Apply the changes. See figures below.

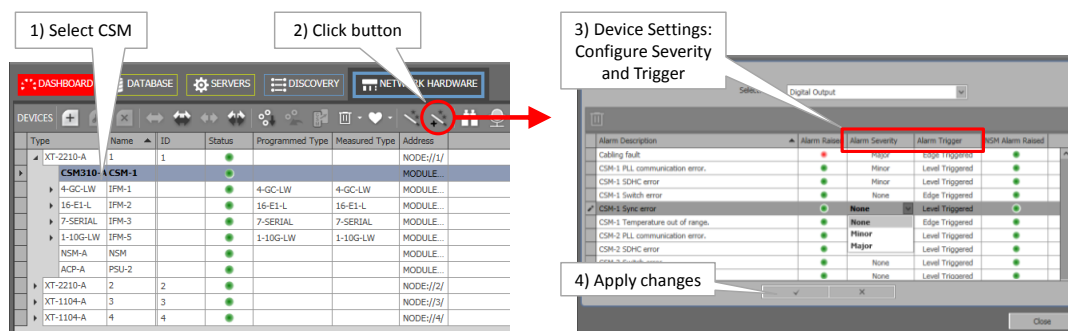


Figure 98 From CSM to Device Settings

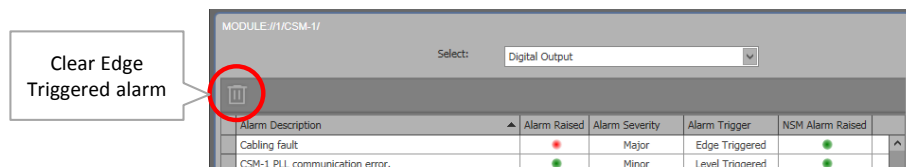


Figure 99 Device Settings: Clear Edge Triggered Alarm



Device Settings:

- ▶ Lists all the possible device alarms. These alarms can be configured towards the digital outputs (DO1/DO2) on the NSM, but can also be used to monitor these alarms via the 'Alarm Raised' and 'NSM Alarm Raised' LED. If one of these alarms occur, they will also appear in the general Alarms window in §4.5.2.
- ▶ Alarm Description: short description of the device alarm;
- ▶ Alarm Raised: this LED turns red if the associated alarm occurs. This LED turns green again when the alarm disappears. It just follows the alarm existence, regardless the configured Alarm Severity and Alarm Trigger;
 - ▶ green LED: alarm is not active on the CSM or in the node;
 - ▶ red LED: alarm is active on the CSM or in the node;

Alarm Severity: Click the cell to open a drop-down list. Select None, Minor or Major.

- ▶ None: this alarm will not be outputted on the NSM DO contacts, although the alarm may be active (Alarm Raised LED is red);
- ▶ Minor: if this alarm occurs on the CSM or in the node, it will deactivate the NSM **DO1** contact (if not already deactivated by another minor alarm). It will also darken the **DO1** LED on the NSM (if not already darkened by another minor alarm);
- ▶ Major: if this alarm occurs on the CSM or in the node, it will deactivate the NSM **DO2** contact (if not already deactivated by another major alarm). It will also darken the **DO2** LED on the NSM (if not already darkened by another major alarm);

Alarm Trigger / NSM Alarm Raised:

- ▶ Level Triggered: The 'NSM Alarm Raised' LED turns red if the associated alarm occurs. This LED turns green again when the alarm disappears. The clear button  will never be active for a Level Triggered alarm;
- ▶ Edge Triggered: The 'NSM Alarm Raised' LED turns red if the associated alarm occurs. This LED remains red (although the error may have disappeared) until the alarm has been selected and the clear button  has been clicked.

NOTE: If an alarm situation changes, the LEDs in HiProvision and the DO LEDs/DO contact on the NSM change a few seconds later;

4.10 Alarms in Large Network Monitor (LNM)

Alarm indications in the LNM tile occur in exactly the same way as alarm indications in the Network drawing of the Network tile.

For alarm indications in the Network tile, see §4.6.

For an overview of the LNM description, see §27.

5. CONFIGURATION LOAD MANAGER


5.1 General

The configuration load manager is a tool that starts and monitors the load process of loading a HiProvision configuration or database into the live network.

CAUTION:

- if you want to load a restored database (see §6.5) into the network, make sure to clear the entire network first. **THE ENTIRE NETWORK WILL GO OUT OF SERVICE AFTER CLEARING IT.** The clear function is explained in §10.2.
- loading will **FAIL** when there are more nodes configured in the network database than nodes measured in the live network.

This tool is invoked as follows:

- By clicking the load icon  in the Network Hardware tab. This button only becomes active when HiProvision is online;

Advancing into the last page of a wizard after clicking Next in the review page: Network Settings wizard, Tunnel wizard, services wizard,

Some definitions (more details in further paragraphs):

- Load: transmit or load the feature configurations from the HiProvision database into the live network. After a successful Load, the feature creations/configurations/modifications will be up and running in the live network;
- Load Scenario: a list of actions that HiProvision must perform to load the latest creations/configurations/modifications of the specific feature into the live network.

Persist checkbox: Possibility to persist the loaded configuration on the node.

5.2 Persist Configuration?

- Checked, Yes (default): A new restore point will be created in the node (= on the flash and Micro SD Memory Card on the CSM) and the configuration change will still be active in the node after a reboot of the node. A restore point is a saved snapshot of the node configuration at a specific time. Only the latest 5 restore points will be kept.

Unchecked, No: No restore point will be created in the node and the configuration change will be lost after a reboot of the node. The node falls back to the latest saved configuration or restore point.



5.3 Get Load Scenarios

Before loading the configuration into the network, sometimes the button 'Get Load Scenarios' appears on top of the page, especially in wizards. If this button appears, click on it to retrieve and show all the scenarios in the configuration load manager. Not clicking this button will forbid you to load into the network.

5.4 Configuration Loading and Status

By default, all the nodes are selected. Nodes can be unchecked individually if they do not have to be loaded. Click the Load button to start the configuration loading into the network. If the entire configuration has been loaded successfully, the configuration load status indicates 'Load success' with Warnings = 0, Errors = 0. If not, the load to one or more network elements has failed. See figure below.

Table 17 Load Manager Menu Buttons

Button	Short Description
	Expand/Collapse the network element treeview.
	Only active if the load has failed on at least one network element. Click these buttons to jump to the next/previous warning or error in the network element treeview. Hovering the error icon in the network element shows some error information, which is also available in the HiProvision log files.

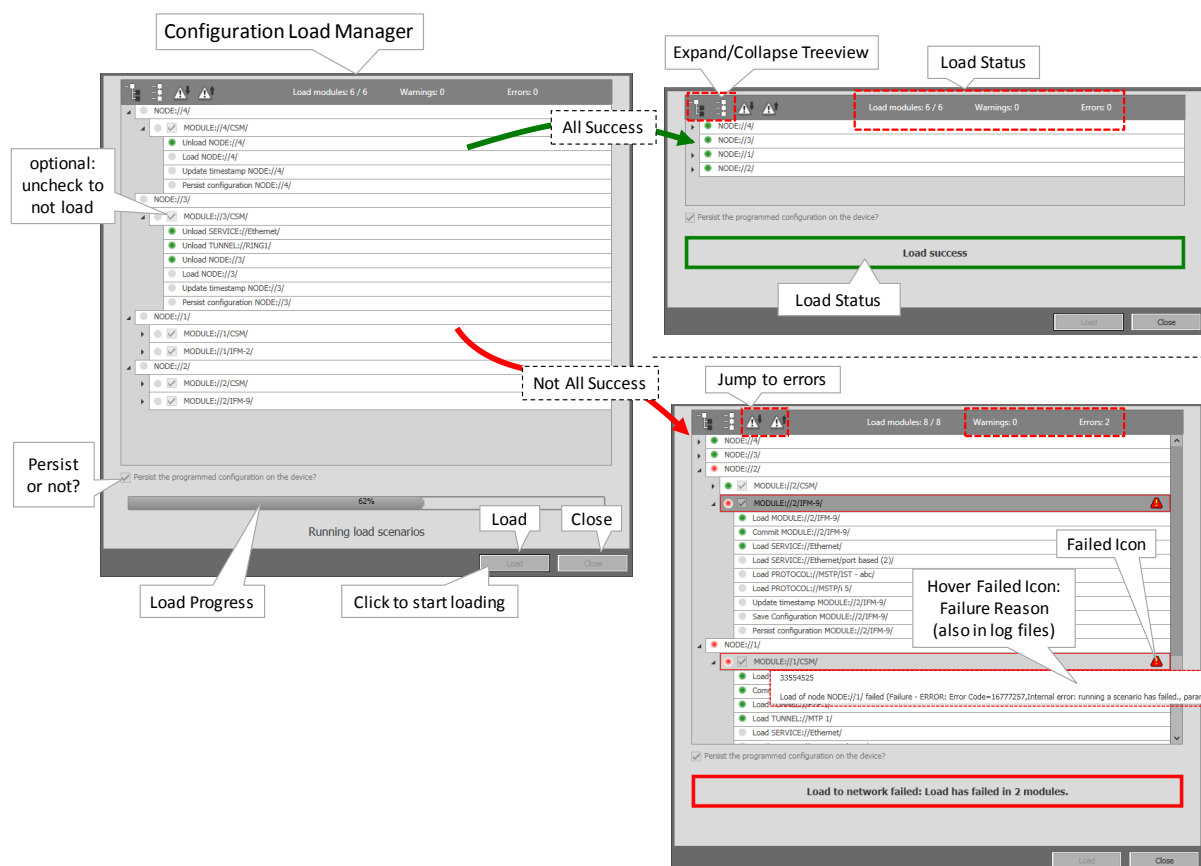


Figure 100 Configuration Load Manager

6. DATABASES HANDLING AND BACKUPS

6.1 General

Prerequisites: If you have chosen a custom installation path for MySQL Server at installation, change the path first as described in §6.2.1.

All database activities can be performed in the Dashboard → Database tile. The application behind the tile has three main sections, see figure below:

- Database s: All the network configuration databases available on the HiProvision server;
 - Active Database: database from the list that is really used by HiProvision. Only one database can be active at a time. The active one is marked with a green border;
- Local Backups: backups of one or more databases from the 'Databases' list. The local backups are stored on the HiProvision Server. The default path is <HiProvision installation Path>\HiProvision Backups. This is the default path filled out in the Backup Folder field at installation time.
- Network Backups: a network backup is a copy of a local backup and is stored in one or more CSMs in the network at the same time. Each node shows a list of its network backups. Network backups in a node are possible when the Micro SD card is plugged into the CSM (=Central Switching Module) of that node, see also Ref. [3] in Table 1. This is by default the case;

Databases (on HiProvision Server)

Database Name	HiProvision Version	Last Backup
127.0.0.1		
422_1_2	4.2.7	2/02/2018 15:44:18
425_mrp	4.2.5	24/01/2018 9:12:19
db_v424e	4.2.9	30/01/2018 10:09:24
marco	4.2.9	6/02/2018 10:10:29
new	4.2.1	21/01/2017 11:36:38

Active database = green border

LOCAL BACKUP DATABASES (on HiProvision Server)

Database Name	Backup Date	Backup Time	HiProvision Version	Info
422_1	09/01/2018	10:51:36	4.2.2	Backup before database migration
422_1_2	26/01/2018	11:59:15	4.2.6	Backup before database migration
422_1_2	31/01/2018	11:21:47	4.2.6	Backup before database migration
423test	12/01/2018	15:48:36	4.2.3	Backup before database migration
db_v424e	06/02/2018	09:44:18	4.2.9	MRP

NETWORK BACKUP DATABASES (on nodes)

Node	Database Name	Backup Date	Backup Time	Provision Version	Info
NODE://1/					
MODULE://1/CSM-1/					
	db_v424e	06/02/2018	09:44:18	4.2.9	MRP
NODE://30/					
NODE://113/					
NODE://828/					Database list empty
NODE://8999/					

backup (blue arrow) and **restore** (orange arrow) operations are indicated between the sections.

Figure 101 Database Tile

A database can be back upped locally on the HiProvision Server first (step1). If desired, it can be back upped further on in the network on one or more nodes (step2). During this backup

to the network, the targeted node(s) will not be affected or interrupted. The backup mechanism provides a lot of database redundancy. See figure below:

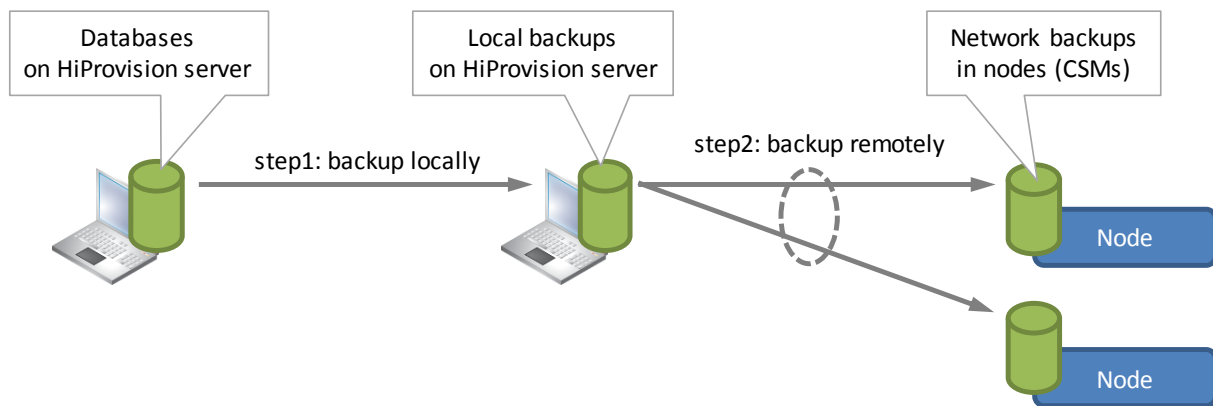


Figure 102 Backup Databases

A database can be restored from a network backup by restoring it first to a local backup (step1), followed by a restore from the local backups to the databases (step2). If a database must be restored only from a local backup, only step2 must be performed. See figure below:

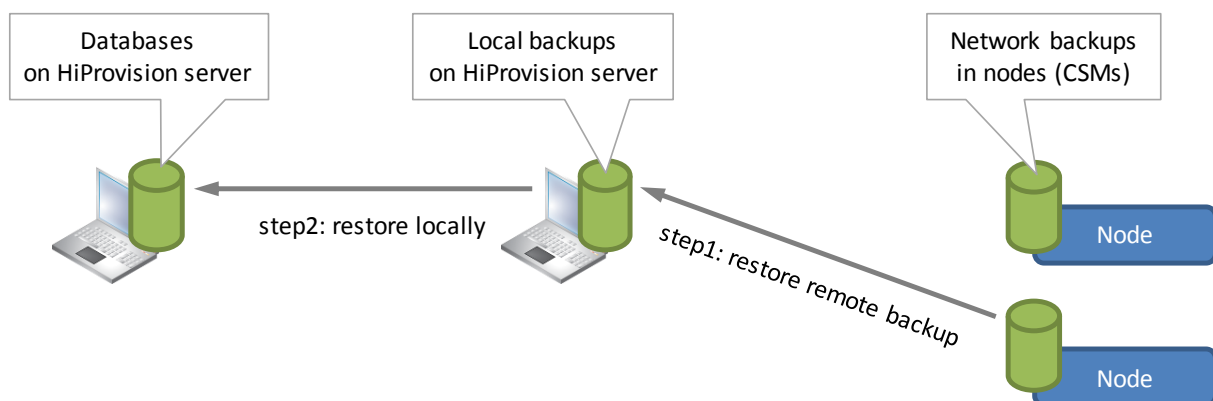



Figure 103 Restore Databases

6.2 MySQL Server Database Settings

6.2.1 Installation Path

The MySQL database server is by default installed in 'C:\Program Files\MySQL\MySQL Server x.y\bin'. If you have chosen another location at installation time, adapt the default path to the custom installation path via the options  button.

6.2.2 Change Password

CAUTION: In case of HiProvision Redundancy, always make sure that both MySQL servers have the same root password!

The default password of the MySQL Server used during installation can be changed afterwards via the MySQL Workbench tool:

1. Start the 'MySQL Workbench Tool' on the HiProvision PC. By default it is installed in C:\Program Files\MySQL\MySQL Workbench <version> CE\MySQLWorkbench.exe;
2. Connect to the HiProvision database via Database → Connect to Database, select your connection in 'Stored Connection' and click OK;
3. Log in: username = **root**, password = **txcare**

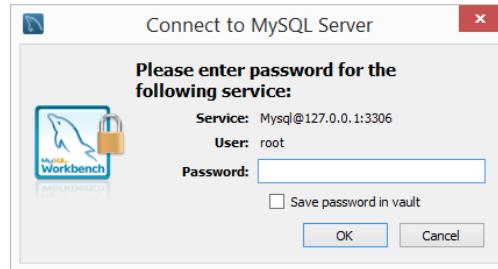


Figure 104 Connect to MySQL Server

4. On the left-hand side, click on Management → Users and Privileges;
5. For all 'root' accounts that have a 'From Host' filled out:
 1. Fill out the new password and confirm it;
 2. Click Apply;

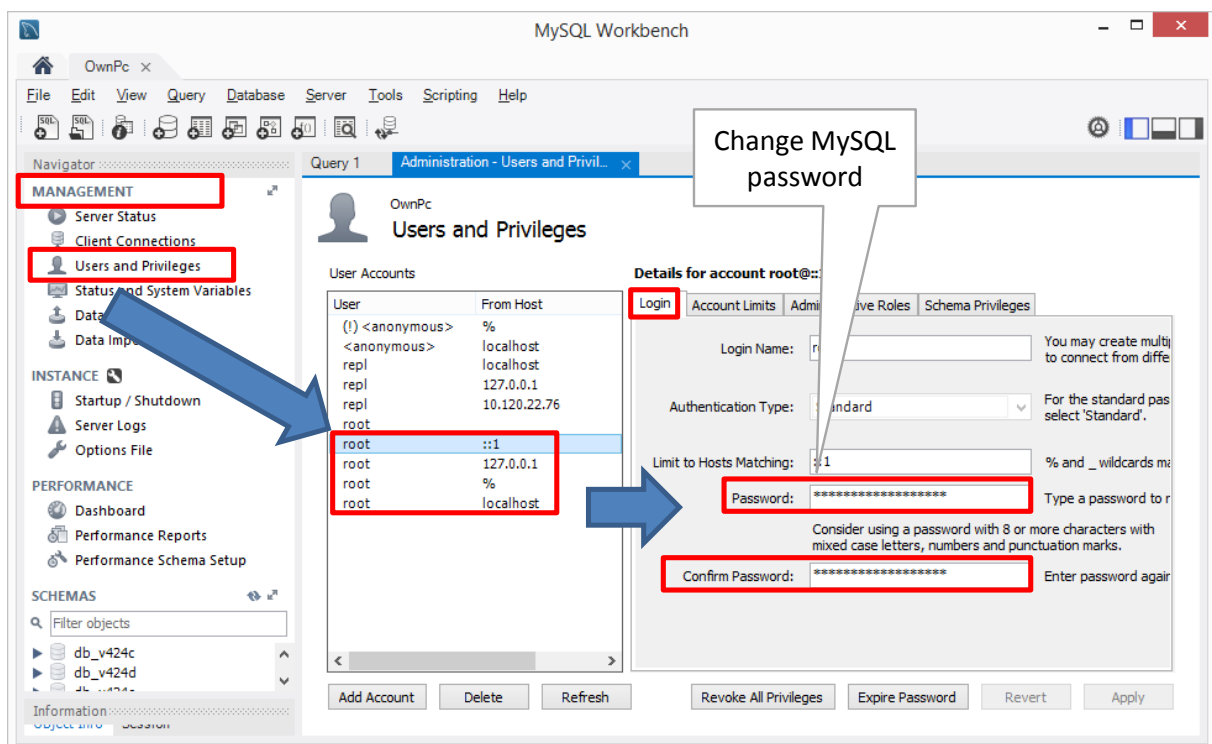



Figure 105 MySQL Workbench: Root Password Change

6. Close the MySQL Workbench;
7. Close and restart HiProvision (servers and client), log in with a HiProvision user authentication;
8. Click the Dashboard → Database tile (authentication failed) and click the database server button 

9. Fill out the new password in the screen below and click Connect and OK:

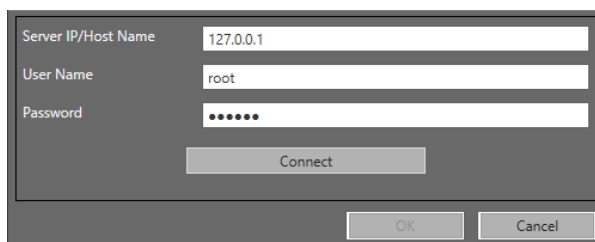





Figure 106 Connect to MySQL Server with New Password

If the connect succeeds, the password update was successful.

6.3 Activate a Database in HiProvision

CAUTION: Activating a database in HiProvision does not include loading the database into the network, see §5 to do so.

Only one database can be active at a time. Perform the steps below to activate a database:


1. Stop the servers via the Dashboard → Servers tile → ;
2. In the Dashboard → Database tile: Select the database that must become the active one by clicking it in the 'Databases' list;
3. Click the  button to activate the database, it will be marked with a green border;
4. Start the servers again via Dashboard → Servers Tile → .

6.4 Make a Backup

The backup functionality can be found in Dashboard → Database tile.

6.4.1 Make a Local Backup


From 'Databases' to 'Local Backups' list:

1. Click the database in the 'Databases' list that must be back upped;
2. Click the  button to create a local backup, a backup comment can be added, the new backup will appear in the 'Local Backups' list.

6.4.2 Make a Network Backup

Prerequisite: the servers in the Dashboard → Servers tile must be running.

From 'Local Backups' to 'Network Backups' list:

1. Click the local backup in the 'Local Backups' list that must be back upped;
2. Click the  button;
3. Select one or more CSMs in the network on which a backup must be stored. Only CSMs with a working SD memory card can be selected. The CSM must be in the ACT (active) or STB (standby) state to succeed;

4. The new backups show up in the 'Network Backups' list under the selected nodes.

6.5 Restore a Backup

The restore functionality can be found in Dashboard → Database tile.


CAUTION:

A restored backup does not automatically become the active database!

A restored backup is not automatically loaded into the network, see §5 to do so!

6.5.1 Restore a Local Backup

From 'Local Backups' to 'Databases':


1. Click the backup that must be restored in the 'Local Backups' list;
2. Click the  button to restore the backup into a new database file. An existing database cannot be overwritten, the new filename must be non-existing;
3. The new database file appears in the 'Databases' list;
4. If you want this file to become the active database, see §6.1.

6.5.2 Restore (or Retrieve) a Network Backup

Prerequisite: the servers in the Dashboard → Servers tile must be running;

From 'Network Backups' to 'Local Backups':

NOTE: If you want it to restore it further to your 'Databases' list, follow §6.5.1.



1. Select the backup from the 'Network Backups' by expanding the necessary node and CSM and selecting the desired backup by clicking the database row;
2. Click the  button to restore (or retrieve) the backup into the 'Local Backups' list. An existing database, meaning same filename and timestamp, in that list will be overwritten.

6.6 Migrate a Database


It is possible to migrate an older database version to the version required in the running HiProvision. Migration can be done in two ways:

Must the older database become the active one after migration?

Yes:

1. Select the older database in the 'Databases' list and click the select  button;
2. A pop-up requests for migration. Click the OK button in the pop-up. If the database already has the latest version, no migration will be requested;
3. A new migration window will appear. Click the Migrate button. A local backup of the older database will be created automatically and appear in the list after migration;
4. Migration starts, click the Close button after the migration, the database version has changed
5. Select the database in the list again and click the select  button to activate it.

No:


1. Select the older database in the 'Databases' list and click the migrate  button;
2. A new migration window will appear. Click the Migrate button. A local backup of the older database will be created automatically and appear in the list after the migration;
3. Migration starts, click the Close button after the migration, the database version has changed.

6.7 Export Database (*.bak, *.xml) to a Mail, USB, ...

1. Make a local backup first as described in §6.4.1;
2. Two files (*.bak and *.xml) are created in the back up folder `<HiProvision installation Path>\HiProvision Backups`. The filename includes the database name and a timestamp, for example:
 - ▶ db_v424_13012018_091142.bak
 - ▶ db_v424_13012018_091142.xml
3. These two files always belong together and must be exported together. These two files must be used later on when importing the database.
4. Just copy these two files on a USB or zip these two files first before sending them as a mail-attachment.

CAUTION: Database filenames must never be changed!

6.8 Import Database (*.bak, *.xml) from a Mail, USB, ...

1. A backed up database exists of two files: *.bak and *.xml. The filename includes the database name and a timestamp, for example:
 - ▶ db_v424_13012018_091142.bak
 - ▶ db_v424_13012018_091142.xml
2. Copy the two database files (unzip them first if zipped), from your USB or mail-attachment into the folder `<HiProvision installation Path>\HiProvision Backups` on the HiProvision PC;
3. In HiProvision, click the refresh button  in the LOCAL BACKUP DATABASES section. The database from your USB/mail will show up in the Local Backups list;
4. Restore this database as described in §6.5.1.

CAUTION: Database filenames must never be changed!

7. PROTOCOLS

7.1 General

Via Dashboard → (Configuration) Protocols, it is possible to configure protocols or interaction with them. Which protocols and features are supported on which Interface Modules can be found in §32. Protocols are available in following categories:

Protocol Interaction:

- ▶ MRP (see §7.2)

Layer 2:

- ▶ MSTP (see §7.3)
- ▶ IGMP Snooping (see §7.4)

Layer 3:

- ▶ Virtual Router, VRF (see §7.5)
- ▶ Static Routing (see §7.6)
- ▶ VRRP (see §7.8)
- ▶ OSPF (see §7.9)
- ▶ PIM (see §7.10)
- ▶ IGMP (see §7.11)
- ▶ DHCP Relay (see §7.12)

Security:

- ▶ IP ACL (see §7.13)
- ▶ MAC ACL (see §7.14)

Other

- ▶ Voice Protocol (see §7.15)

NOTE: If protocol monitoring info is available, it can be monitored via Dashboard → (Monitoring) Protocols which results in the Protocols Monitor tile.

Find below some protocol scalability parameters.

NOTE: The values in the table below remain the same when the main L3 Interface Module is used together with the extension L3 Interface Module.

Table 18 Protocol Scalability Parameters

Scalability Parameter	Per L2 Interface Module	L3 Interface Module	
		Per VRF in L3 Interface Module	Total per L3 Interface Module
VLAN IDs	4k		4K
VRFs	---	1	64
L3-VLANs / IP Interfaces	---	256	256
MAC addresses	16k		16k
ARP entries	---	2K	4K
Unicast routes	---	3K	12K
Multicast routes	---	1K	1K
MSTP instance	16		64
VRRP instance	---	64	64
OSPF Neighbors	---	32	128
MAC ACL	128		128
IP ACL	128		128

7.2 Protocol Interaction: MRP (=Media Redundancy Protocol)

7.2.1 General

The MRP is a protocol (IEC 62439-2) especially designed for industrial applications which need a predictable fail-over time. This protocol can only be used in a ring-topology network and makes sure that the ring network stays loop-free. The ring ports are Ethernet ports on an Interface Module. See §32 to find out which Interface Modules support MRP. MRP does in ring networks what spanning tree does in meshed networks but with much faster convergence times.

MRP runs in a ring of MRP-compatible access switches connected to two Dragon PTN nodes via a 'Monitored Link' to close the ring. The two Dragon PTN nodes have MRP activated; The ring has one selected MR Manager (MRM) and a number of MR Clients (MRC). The two Dragon PTN nodes act as MRC;

MRP logically blocks one of its uplink ports, to prevent a layer2 loop;

- When the access ring is broken (cable break or device down) the MRM will detect it and open its blocked uplink port;

The convergence time depends on the access switches and the network configuration;

- Some Hirschmann devices support MRP;
- Performance between the HiProvision server and the Hirschmann devices can be improved, see §10.8.

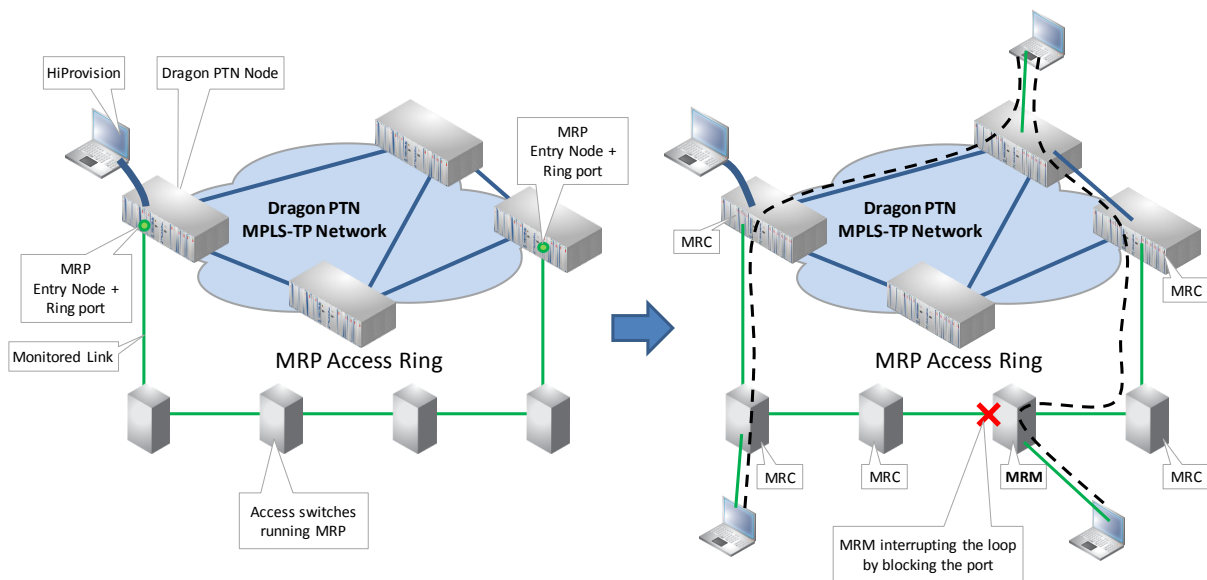


Figure 107 MRP: General Example

7.2.2 Prerequisite

- ▶ At least one Monitored Link and some Ethernet services, either VLAN and/or port based, must have been created in HiProvision. More info on 'Monitored Link' (§2.7.2b). The MRP Access ring must be connected in the 'Monitored Link';
- ▶ For VLAN-based data services, an extra MRP-service has to be provisioned for each MRP-ring, and with at least priority 2. The VLAN-based MRP services must have exact 2 ring ports;
- ▶ If external devices have been configured (=not required) in the monitored links, then they have to be external devices with base type 'Hirschmann' (see §33). Each Hirschmann device requires a Hirschmann Device voucher in the license pack, see §20.2. Creating these devices gives a better visual overview in the network drawing, but is not a requirement to configure MRP. The MRP frames of the Hirschmann devices must be VLAN tagged. When using port based services, the VLAN tag must be unique per MRP ring;
- ▶ A tunnel different from point-to-point must be used;
- ▶ Topology: an MRP service must at least go over a 'logical ring' or 'point-to-multipoint' tunnel. If there is a 'sub ring' tunnel in between, the MRP service must be connected up to the 'logical ring, see example figure below. The MRP service can maximum go over one 'logical ring'.

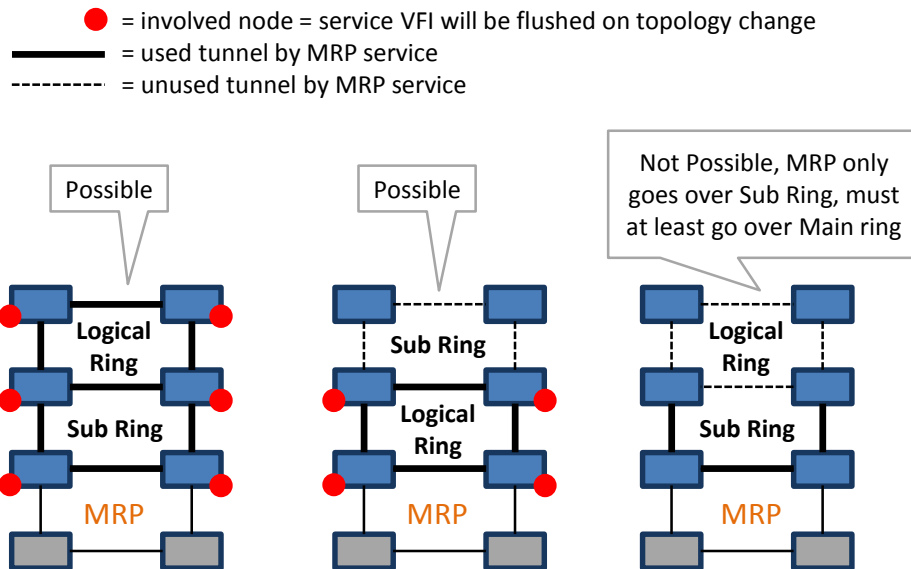


Figure 108 Involved Node: Flush VFI

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

7.2.3 Configuration

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

Information: Click Next >>;

Select Ports:

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

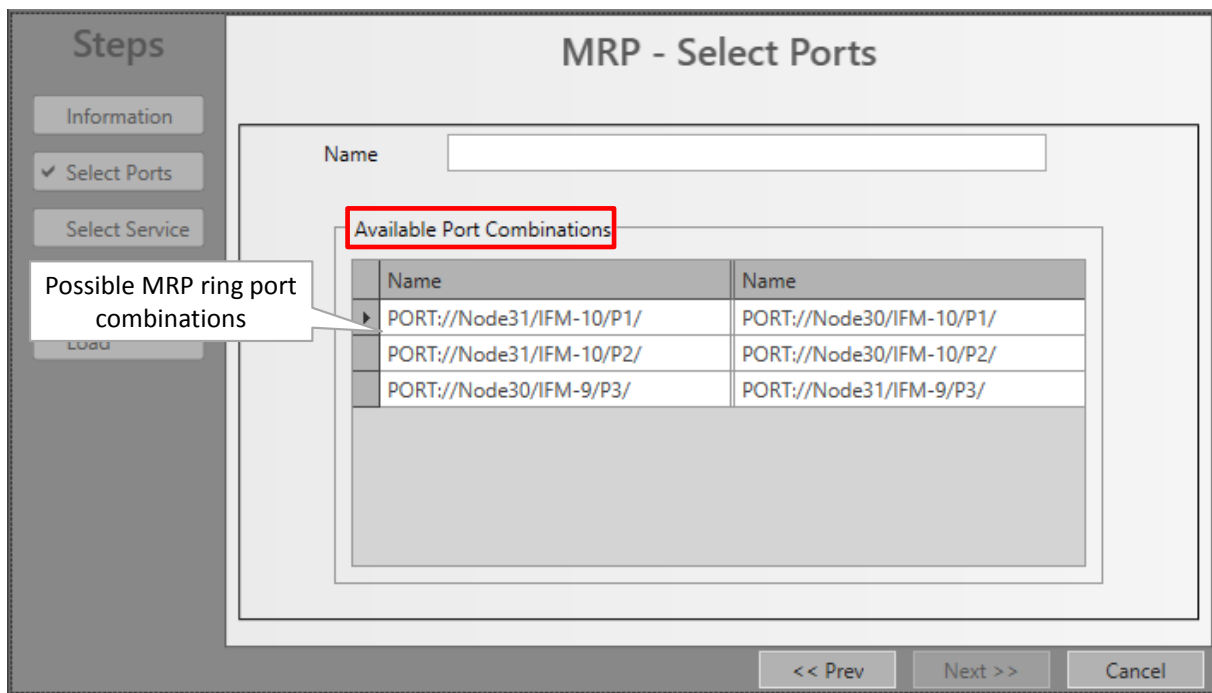


Figure 109 MRP: Select Ports

- Select Service:
 - Your port combination belongs to a **VLAN based service**: both the MRP protocol and the real data will be transported in their own VLAN based service, each having their own priority, quality of service, bandwidth. All tunnels used by the MRP services must be entirely part of the tunnels used by its involved data services.
 - Select MRP Service (to transport the MRP protocol): shows VLAN based Ethernet services that have only configured the selected ring port combination (=exact 2 ports) from previous screen and additionally have at least priority 2. Select one of these services to transport the MRP protocol which has MRP VLAN tagged packets;
 - Name: Name of the VLAN Based service used for the MRP protocol;
 - VLAN ID: VLAN ID for the VLAN Based service, this VLAN ID must match the VLAN ID of the MRP frames;
 - Involved Data Services (only informational, to transport the real data): This list shows the VLAN based services, that can be used to transport the real data, and that share the same selected port combination as the services in 'Select MRP Service'. In addition, these services have more ports configured than just the 2 ring ports. The VFI's of these services will be flushed as well when a topology change occurs in the MRP ring.

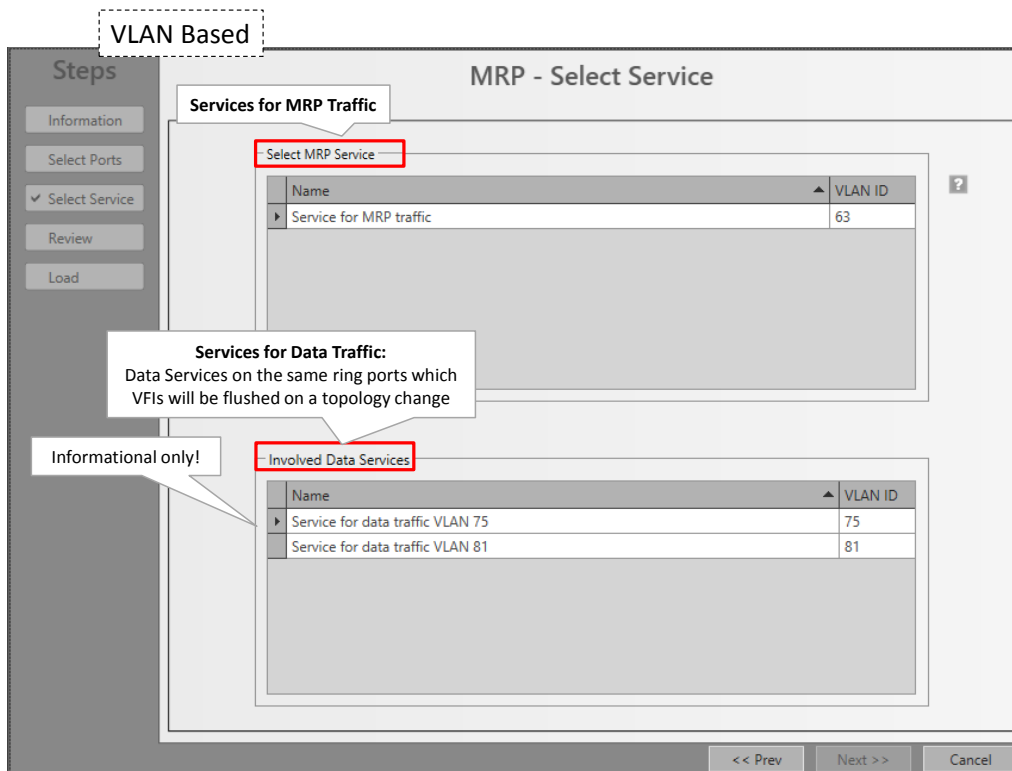


Figure 110 MRP: VLAN Based Services: Select MRP + Data Service

- ▶ Your port combination belongs to **Port based service**: both the MRP protocol and the real data will be transported in the same port based service, having one common priority, quality of service and bandwidth for the entire service.
- ▶ Select MRP Service (to transport the MRP protocol + data): shows port based Ethernet services that have configured at least 3 ports: the selected ring port combination (= exact 2 ports) from previous screen + 1 or more other data port(s). Select one of these services to transport the MRP protocol + real data;
 - ▶ VLAN ID: this VLAN ID must match the VLAN ID of the MRP frames;
 - ▶ Name: Name of the Port Based service used for the MRP protocol + real data;

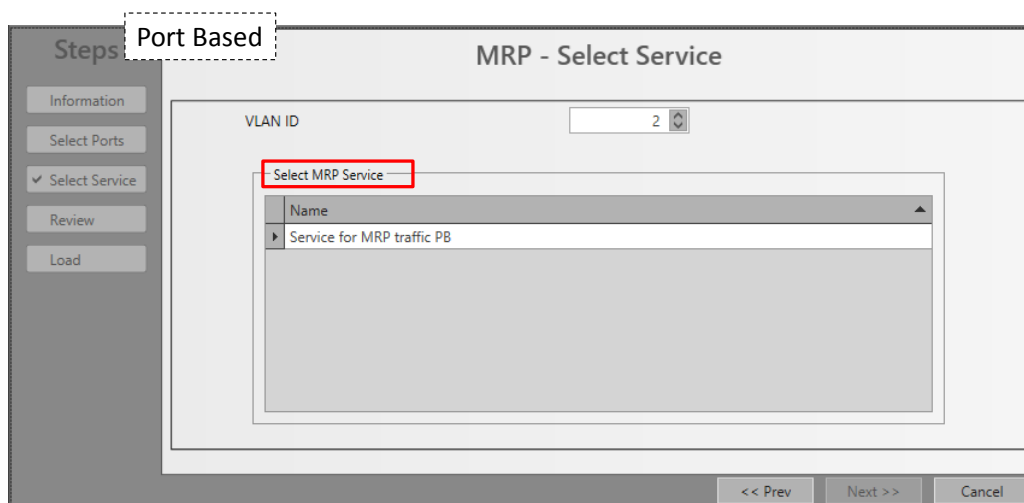


Figure 111 MRP: Port Based Services: Select Service

- Review: Involved Nodes: A data service node that is also positioned in the used tunnels of the MRP service. When a topology change occurs in the MRP ring, the VFI of the involved services in that involved node will be flushed (see also Figure 108). This topology change has no impact on the other VFIs in that node.
- If ok, click Finish. The configuration load manager will be invoked, see §5;

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

7.2.4 Monitoring

MRP Monitoring info is available via the two options below.

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

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

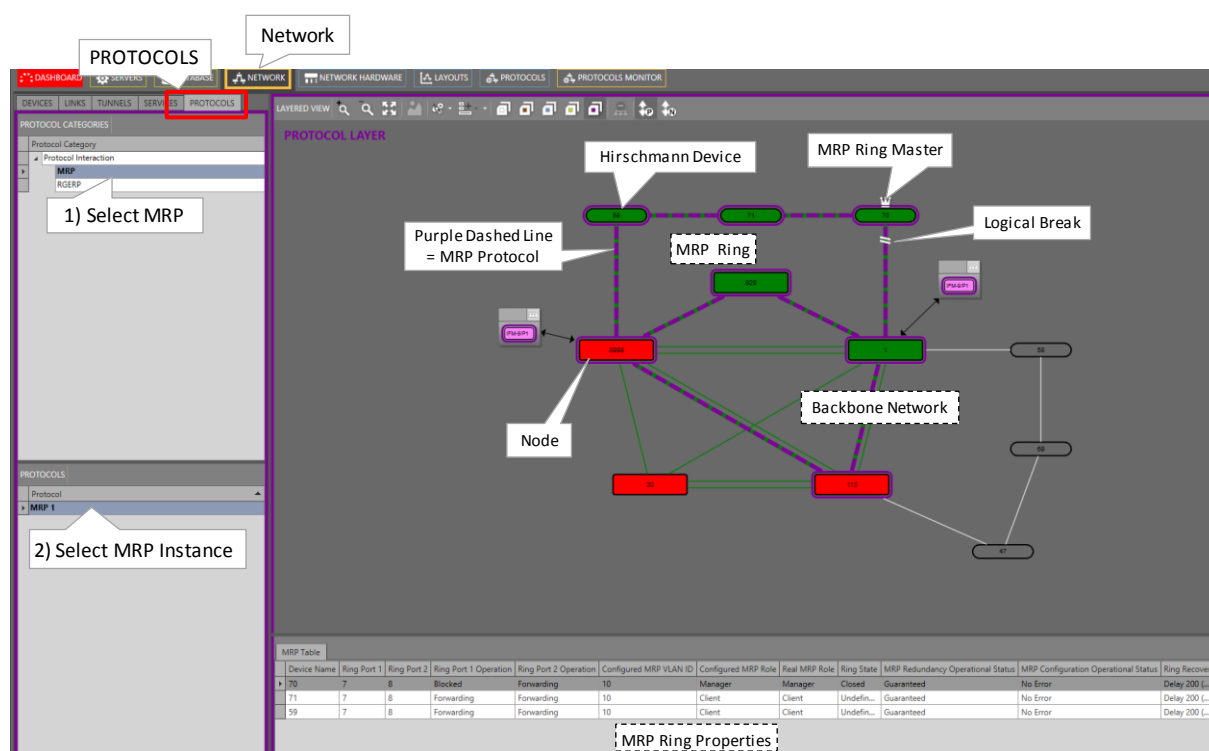


Figure 112 Dashboard → (Monitoring) Network Tile → Protocols Tab

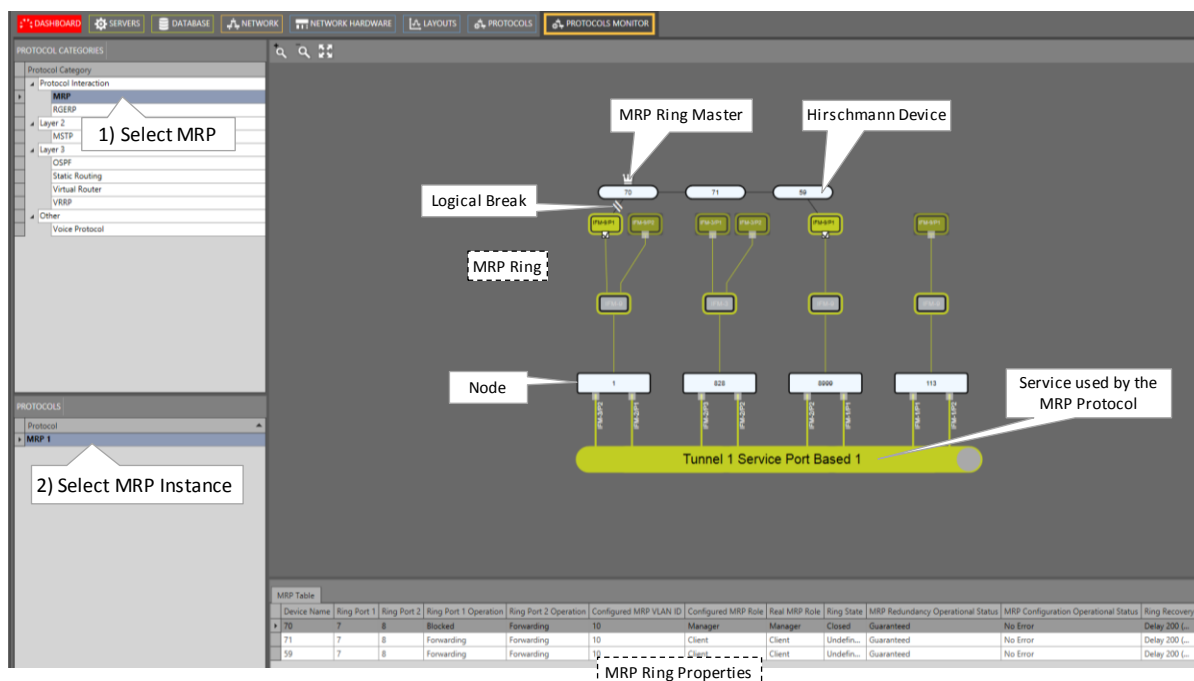


Figure 113 Dashboard → (Monitoring) Protocols Tile

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

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

7.3.1 General

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

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

MSTP in a port based service is supported network wide whereas MSTP in a VLAN based service is supported only locally (not over the L2/L3 Interface Module back end ports).

CAUTION: using MSTP with a VLAN based service over the back end ports could cause loops!

MSTP is fully supported on L2/L3 Interface Modules and partially (=transparent MSTP) on the other Ethernet Interface Modules, see also §31.2 and §32. On L2/L3 Interface Modules, there is always a default MSTP running (not visible in HiProvision).

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

NOTE: A basic port blocking (without MSTP) can be achieved via the BPDU Guard feature on ports that support this feature: see §32 and §34.

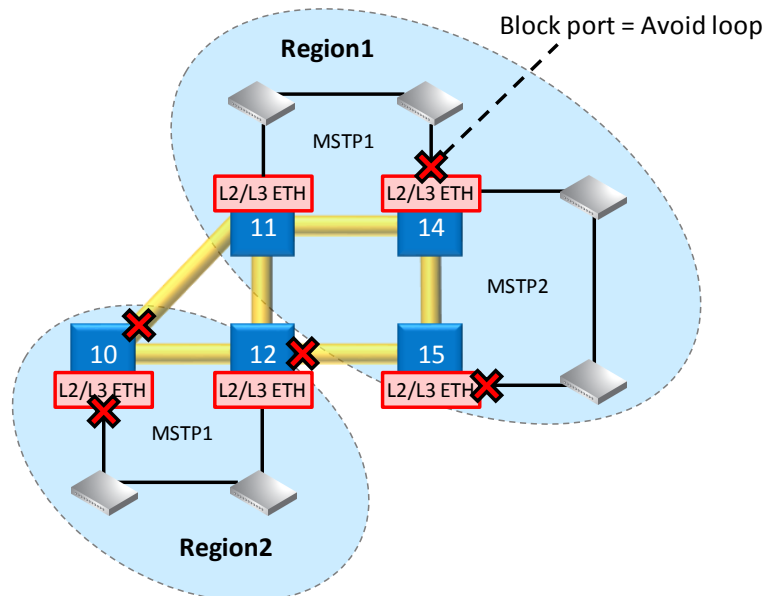


Figure 114 Region/MSTP Overview

7.3.2 Prerequisite

A Port based Ethernet service must contain at least one of the Interface Modules in §32 that support the Ethernet Service.

A VLAN based Ethernet service must contain only L2/L3 Interface Modules.

For L2/L3 Interface Modules, make sure that each Interface Module that must participate in the same MSTP Region, has exactly the same VLANs configured.

7.3.3 Configuration

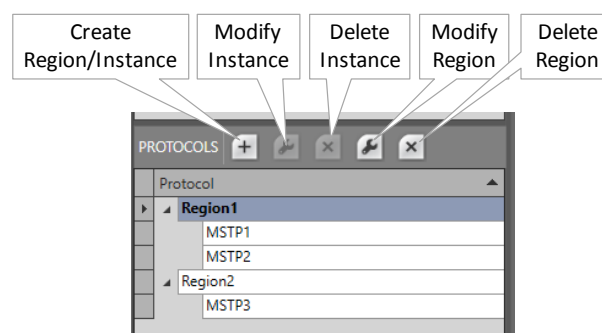



Figure 115 Region/MSTP Actions

(see §a) Active MSTP: L2/L3 Interface Modules Included;

(see §b) Transparent MSTP: Only LAN/WAN Ethernet Interface Modules (4-GC-LW, ...) Included;

a. Active MSTP: L2/L3 Interface Modules Included

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

Information: Click Next>>;


Region Selection:

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

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

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

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

- ▶ Select Region: Select a Region in which the MSTP instance must operate. If the list is still empty or you want to create and select a new Region, select <Create New Region> instead;
- ▶ Region Name: Name of the selected Region or fill out a new Region name when a new Region is being created;
- ▶ Revision (default = 0, range[0...65535]): identifies the Revision of the current MSTP instance. Fill out a new value when a new Region is being created;
- ▶ Region Configuration (only when creating the Region with first MSTP instance):
 - ▶ Service: Select a service. Best practice is to select all services that use the L2/L3 Interface Modules on which you want to configure MSTP;
 - ▶ Ports: If the service has been selected, a list with devices is shown. Expand the devices by clicking  in front of the device row. Select one or more L2/L3 Interface Modules or Ethernet ports before clicking the Next >> button. NOTE: a L2/L3 Interface Module can only belong to one Region;
- ▶ VLAN Selection (only when a L2/L3 Interface Module is involved and adding an MSTP instance, different from the IST, to an existing Region):
 - ▶ Instance ID (default=1; range[1..64]): Fill out an instance ID for this MSTP instance. Within the same Region, this instance ID must be unique;

- ▶ VLANs: Select one or more VLANs on which this spanning tree instance must run. This VLAN list is a result of the selected service during Region creation;

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

MSTP Configuration (only when a L2/L3 Interface Module is involved):

- ▶ Instance Properties (L2/L3 Interface Modules):
 - ▶ Device Name: Indicates the device or Interface Module on which MSTP is going to be configured;
 - ▶ Bridge Priority (default=32768, range[0, 4096, 8192, ..., 61440]): Select the bridge priority which must be an increment of 4096. 0 = lowest value = highest priority. The **Bridge Priority** together with the **Bridge MAC Address** determines the **Bridge ID** or the identity of the device. The Bridge ID is used by MSTP to determine the root bridge of the network. The device with the lowest Bridge ID becomes the root bridge. If all the devices have the same priority, the device with the lowest MAC address will then become the root bridge. If you want a device force to be the root bridge, make sure it has the lowest priority value of all devices in the network.

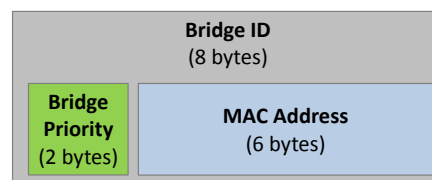


Figure 116 Bridge ID = Bridge Priority & MAC Address

- ▶ Port Properties (L2/L3 Interface Modules):

NOTE: '*' = indicates a shared property over all instances, see Table 20;

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

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

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

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

Table 19 Default Path Cost

Type	Default Path Cost
Front Port: 10G	2000

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

- ▶ Priority (default=128; range[0, 16, 32, ..., 240]): Select the port priority value, using increments of 16. 0 = lowest value = highest priority, 240 = highest value = lowest priority. The priority can be used to influence the root port selection of the downstream switch.
- ▶ Link Type: Indicate by selecting the Link Type whether your link interconnects more than 2 devices:
 - ▶ Point to Point (=default for access ports → e.g. Interface Module-3/P3): The connected link is a point-to-point link to just one other device. Point-to-point links make the node reconfigure quicker (e.g. after a loop reconfiguration) than a shared link;
 - ▶ Shared (=default for L2/L3 Interface Module **Back End** ports → e.g. Interface Module-3/BE4): The link is a shared segment and must be used when more than two devices must be interconnected. Shared links make the node reconfigure slower (e.g. after a loop reconfiguration) than a Point to Point link. E.g. when your shared link only interconnects two devices, the Link Type could better be set to Point to Point.
 - ▶ Auto: The device will auto detect the Link Type for MSTP;
- ▶ Port Fast:
 - ▶ Checked (=default for L2/L3 Interface Module access ports): immediately puts the port into STP forwarding mode upon linkup. The MSTP listening and learning phase is omitted. The port still participates in STP. So if the port is to be a part of the loop, the port eventually transitions into STP blocking mode. This setting is meant for access ports, which are connected to a single server/workstation/ end device where no loops are expected;
 - ▶ Unchecked (=default for L2/L3 Interface Module back end ports): puts the port first into STP blocking mode upon linkup. The MSTP listening and learning phase is active. Based upon these results, MSTP will keep the port in blocking mode or set it in in forwarding mode. Ports that are connected to switches or routers must use this setting.
- ▶ Root Guard: This setting manages the root bridge protection;
 - ▶ Checked: prevents this port to become a root port. As a result, it prevents the switch connected to this port to become the root bridge;
 - ▶ Unchecked (=default): allows this port to become a root port. As a result, it allows the switch connected to it to become the root bridge;
- ▶ BPDU Guard (BPDU = Bridge Protocol Data Unit);
 - ▶ Checked (=default for access ports): The BPDU guard is enabled. If a BPDU packet enters the port, the node will detect this immediately and block the port. The port can be re-enabled by setting the Admin Status of the port

properties Down and click Apply (and Load) and setting it back Up and click Apply (and Load). Checking BPDU Guard makes sure that external devices connected to this port are not able to influence the MSTP topology within the network borders resulting in a more stable network;

- ▶ Unchecked (=default for L2/L3 Interface Module Back End ports): The BPDU guard is disabled. The port will not be disabled when a BPDU packet enters the port. A connected device to this port is able to participate in the MSTP protocol and topology within the network. CAUTION: As a result, this connected device can also become the root bridge (see also Root Guard parameter for more information) of the network, resulting in possible major changes within the MSTP network or domain;
- ▶ BPDU Transmit:
 - ▶ Checked (=default): The Dragon PTN node can transmit (MSTP) BPDU packets on this port.
 - ▶ Unchecked: The Dragon PTN node does not transmit (MSTP) BPDU packets on this port.
- ▶ BPDU Receive:
 - ▶ Checked (=default): The Dragon PTN node can receive and process (MSTP) BPDU packets on this port.
 - ▶ Unchecked: The Dragon PTN node ignores incoming (MSTP) BPDU packets on this port;
- ▶ Hello Time (sec) (default=2 seconds; range[1,2]): This value configures the interval between the MSTP hello packets (= BPDUs), sent by the root bridge. Each MSTP node expects to receive a BPDU packet within three hello times.

Review: if ok, click Finish. The configuration load manager will be invoked, see §5.

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

PROTOCOLS

+

Protocol

R1

R11

Instance2

IST - R11

R14

R2

R3

R8

Region

Instances in Region

Instance Properties

Module Properties

Port Properties

Port

Path Cost

Priority

Link Type

Port Fast

BPDU Transmit

BPDU Receive

Hello Time (sec)

NODE5/Node5/

IFM-5/BE1

IFM-5/P1

IFM-5/P2

IFM-5/P3

IFM-5/P4

IFM-5/P5

IFM-5/P6

IFM-5/P7

IFM-5/P8

IFM-5/P9

20000

20000

20000

20000

20000

20000

20000

20000

20000

2000

128

128

128

128

128

128

128

128

128

128

Shared

Point To Point

Point To Point

Point To Point

Point To Point

Point To Point

Point To Point

Point To Point

Point To Point

Point To Point

☐

☒

☒

☒

☒

☒

☒

☒

☒

☒

☐

☐

☐

☐

☒

☒

☒

☒

☒

☒

☐

☒

☒

☒

☒

☒

☒

☒

☒

☒

☐

☒

☒

☒

☒

☒

☒

☒

☒

☒

2

2

2

2

2

2

2

2

2

2

Figure 117 Created Regions/MSTP Instances

Table 20 Parameter Dependency


Level	Parameter	MSTi Dependent (*)
Device	Bridge Priority	setting per MSTi
Port	Path Cost	setting per MSTi

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

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

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

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

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

Information: Click Next>>;

Region Selection:

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

Region Configuration:

- ▶ Select the services that use your LAN/WAN Ethernet Interface Modules;
- ▶ Select the ports that must participate;

Review: if ok, click Finish. The configuration load manager will be invoked, see §5. The resulting Regions with their MSTP instances are listed in the Protocols list.

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

7.4 Layer 2: IGMP Snooping

7.4.1 General

IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. Via Interface Modules that support IGMP snooping (see §32), it provides the Dragon PTN nodes with a mechanism to diminish multicast traffic from links that do not contain a multicast listener (an IGMP client). The Dragon PTN node will, by default, flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). Multicast can cause unnecessary load on host devices by requiring them to process packets they have not solicited.

IGMP snooping allows the Dragon PTN node to only forward multicast traffic to the ports that have solicited them. IGMP snooping is not a protocol but a layer 2 optimization for the layer 3 IGMP protocol (see §7.11). IGMP Snooping takes place internally on Interface Modules that support it. Snooping is therefore especially useful for bandwidth-intensive IP multicast applications such as IPTV.

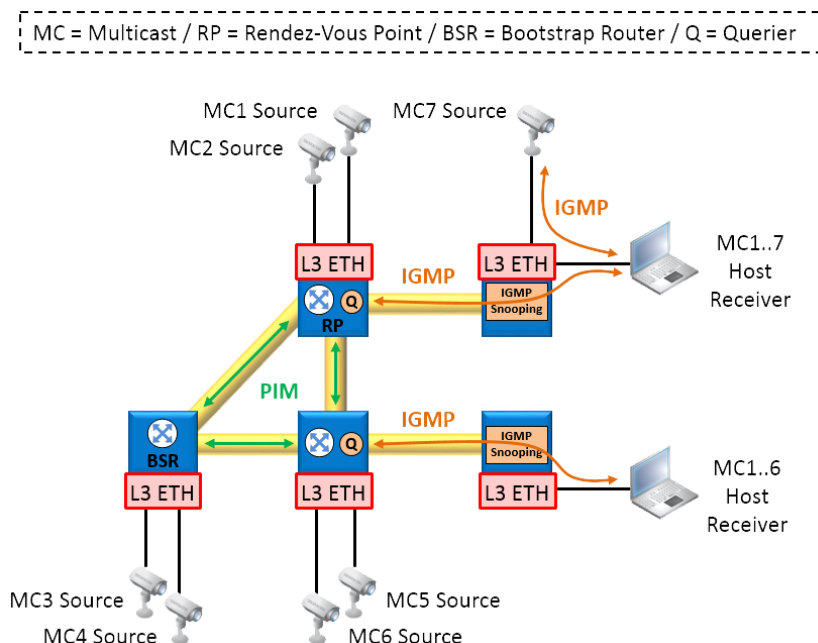


Figure 118 PIM/IGMP/IGMP Snooping Overview

7.4.2 Common IGMP Snooping Properties

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

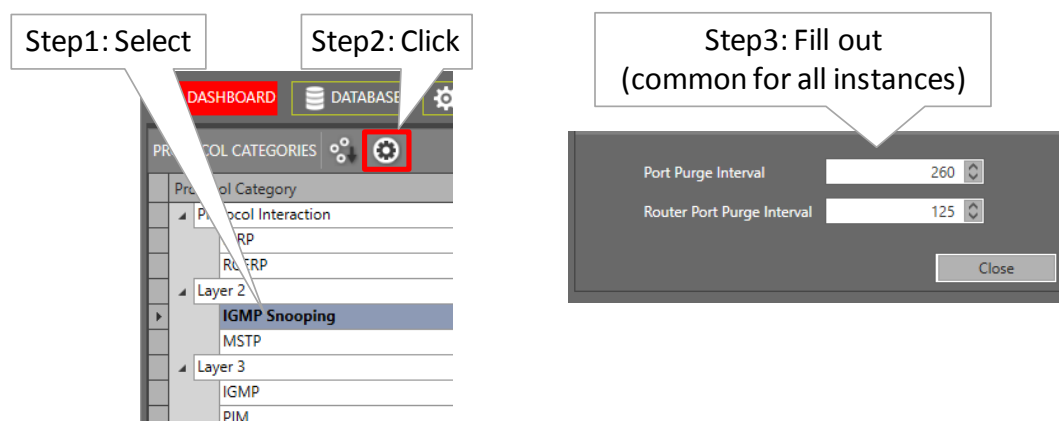


Figure 119 IGMP Snooping Common Properties

- Port Purge Interval: (default value = 260 s, min. 130 s, max. 1225 s) The expiry of the Port Purge Timer on the port for a particular multicast group results in the port being


removed from the forwarding list of the corresponding multicast entry in the Multicast Forwarding Table.

- ▶ Router Port Purge Interval: (default value = 125 s, min. 60 s, max. 600 s) Sets the IGMP snooping router port purge time-out after which the port gets deleted if no IGMP router control packets are received.

7.4.3 Prerequisite

An Ethernet service must contain at least one of the following Interface Modules that support IGMP snooping, see §32.

7.4.4 Configuration

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

Information: Click Next>>;

Service Selection: A list of Ethernet services is shown, select a service and click Next>>.

Module/Port Configuration:

- ▶ Module level:
 - ▶ Module: All the Interface Module modules that support IGMP snooping, part of the selected Ethernet service, are shown in this table;
 - ▶ Enabled:
 - ▶ checked (=default): IGMP snooping is enabled on this Interface Module;
 - ▶ unchecked: IGMP snooping is enabled on this Interface Module.
 - ▶ Snooping Mode:
 - ▶ Passive: All IGMP messages (membership queries, membership reports, leave group, group specific queries...) through this Interface Module always pass without interaction of this Interface Module itself. It is advised to use this setting when IGMP snooping, IGMP and PIM are configured together in this Interface Module.
 - ▶ Report Process:
 - ▶ Non Router Ports (=default): Non (Multicast) Router ports are ports where no IGMP Queries are received on. Normally end-devices are connected to these ports. Setting this value makes sure that Reports are only processed from non-router ports;
 - ▶ All Ports: Reports are processed from all Interface Module ports, either router or non router ports.
 - ▶ Report Forward :
 - ▶ Router Ports (=default): (Multicast) Router ports are ports where IGMP Queries are received on. Setting this value makes sure that Reports are only forwarded to router ports;
 - ▶ All Ports: Reports are forwarded to all Interface Module ports, either router or non router ports;
 - ▶ Non Edge Ports: Ports not connected to an end-station or application.

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

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

Review: if ok, click Finish. The configuration load manager will be invoked, see §5.

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

7.5 Layer 3: Virtual Router, VRF

7.5.1 General

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

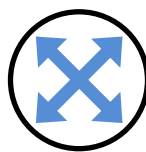


Figure 120 Virtual Router Icon

Virtual Router is a router (instance) created by HiProvision within a L3 Interface Module in a Dragon PTN node. 'Virtual' in this context refers to the fact that it is created programmatically and that multiple routers can be created within the same Interface Module, with each Virtual Router having its own independent routing table. Because the Virtual Routers are independent, the same or overlapping IP addresses can be used without conflicting with each other. These routing tables initially only have IP addresses/masks of directly connected networks. Later on, these routing tables will be extended by using Static Routing (see §7.6), OSPF (§7.9). Some scalability parameters can be found in Table 18.

Example figure below:

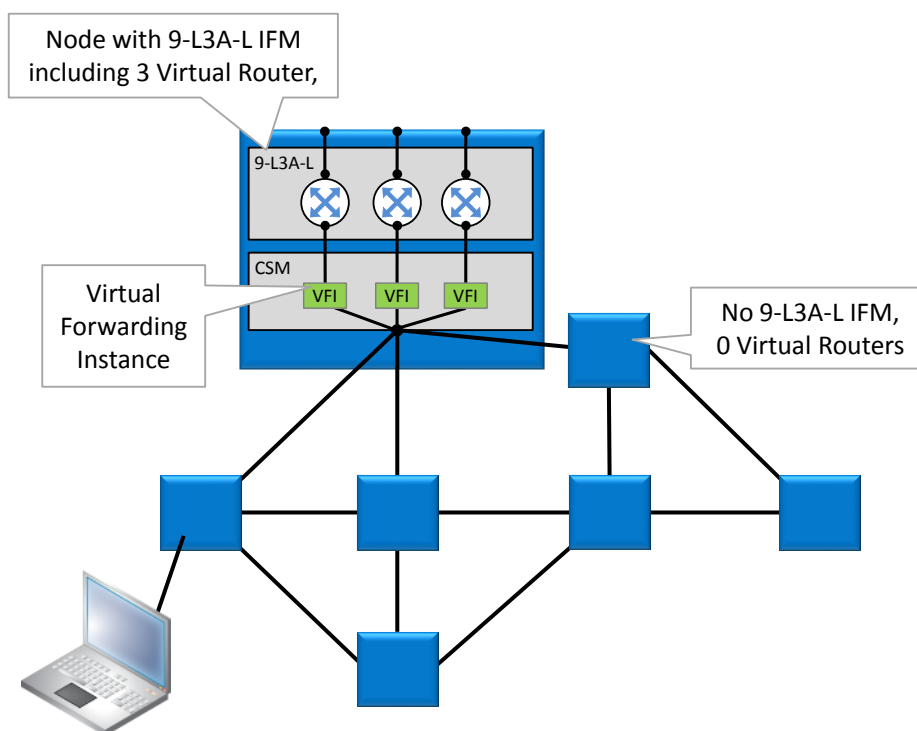


Figure 121 Virtual Router Example

7.5.2 Prerequisite

At least one L3 Interface Module must have been configured.

7.5.3 Configuration

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

Information: Click Next>>;

Creation:

- ▶ Name: Fill out a Virtual Router name;
- ▶ Module Selection: this list shows all the configured L3 Interface Modules. Select one L3 Interface Module on which the Virtual Router must be created by just clicking the Interface Module's Selected checkbox;

- Ports Selections (optional if you select a service in Service Selection): shows the available ports (=front ports, LAG ports, Loopback Interface ports = L3 virtual port) on the selected L3 Interface Module, not part of a VLAN or service yet. Add one or more ports to this Virtual Router by clicking one or more Selected checkboxes.
 - Service Selections (optional if you select a Port in Ports Selection): shows the available Ethernet services (VLANs) configured on the selected L3 Interface Module, not yet assigned to another Virtual Router. Select one or more services (VLANs) that must become a router interface by clicking one or more Selected checkboxes;
- NOTE:** At least one port or service must be selected.

Figure 122 Virtual Router Wizard - Creation

Configuration:

- IP Address: Assign (or fill out) the IP addresses in CIDR (=Classless Inter-Domain Routing) notation to the ports and interfaces of this virtual router;
- Click Next>>;

Figure 123 Virtual Router Wizard - Configuration

- Properties: Fill out the virtual router **properties**. In the figure below the default values are displayed. ICMP is a protocol for sending control and test messages across the IP network.

- ▶ Send ICMP redirects: (default=checked) An ICMP redirect message is used by a router to tell a previous router that it is better to use a different route next time. Sending these messages can be turned off;
- ▶ Send ICMP unreachable: (default=checked) An ICMP destination unreachable message indicates that a destination is unreachable. Sending these messages can be turned off;
- ▶ Send ICMP mask reply: (default=checked) If a station starts up, it will broadcast ICMP mask request to learn the used subnet mask. The router will send back an ICMP mask reply. Sending these messages can be turned off;
- ▶ Send ICMP echo reply: (default=checked) An ICMP echo reply message is a reaction on an ICMP echo request message, to tell that the receiver is alive and reachable. ICMP Echo replies are used by the well-known 'ping' command to test network connectivity. Sending these messages can be turned off;
- ▶ IP default TTL: (default=64, range [1,..,255]) Time to live hop counter, indicates how long (or how many hops) an IP message can survive in an IP network. Every hop, the TTL is decreased with one. If TTL reaches 0, the IP message is removed from the network;
- ▶ ARP timeout: (default=300 s, range [30,..,86400]) If an ARP entry is not used a specific amount of time, called the ARP timeout, the entry is removed from the caching table;
- ▶ ARP retries: (default=10, range [2,..,10]) indicates the number of times that the ARP cache manager attempts to resolve an IP address.

Figure 124 Virtual Router - Properties

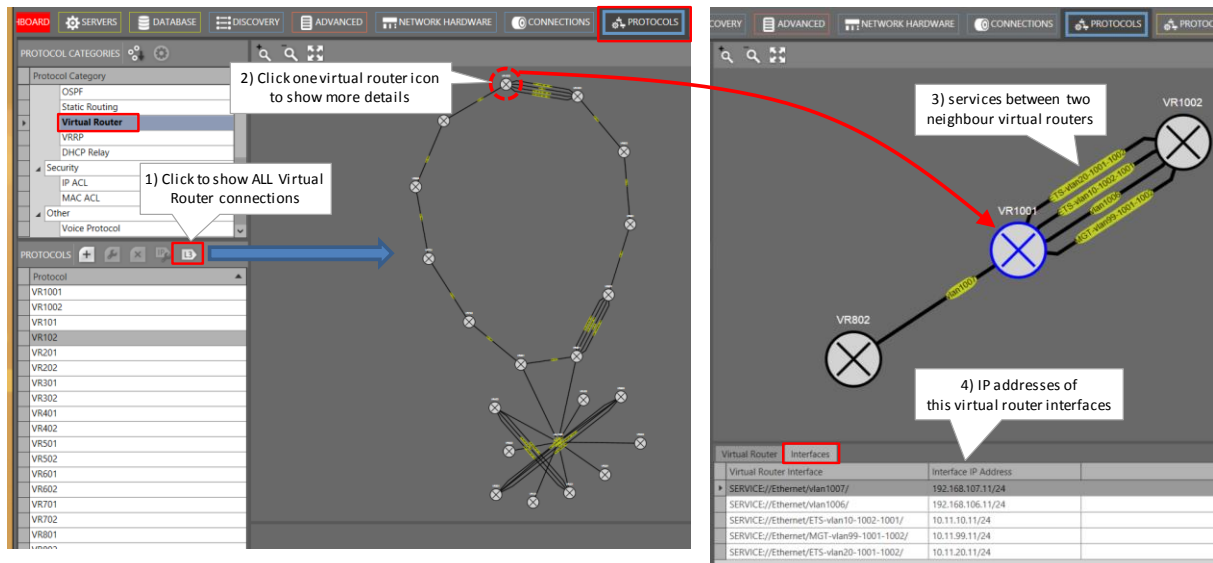
Review: if ok, click Finish. The configuration load manager will be invoked, see §5;

7.6 Layer 3 View: Virtual Router Connections Overview

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

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

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



7.7 Layer 3: Static Routing

7.7.1 General

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

7.7.2 Prerequisite

Some Ethernet services (different from a local service) must have been created on some L3 Interface Modules;

At least one virtual router must be configured before a static route can be configured.

7.7.3 Configuration

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

Information: Click Next>>;

Selection:

- ▶ Virtual Router Selection: Select a virtual router from the drop-down list on which the static routing table must be created;

Creation: In the figure below, static routes can be created by filling out a custom or selecting a detected 'Destination' and a 'Via' point. The 'Destination' point is connected indirectly

whereas the 'Via' point is directly connected to the selected virtual router. As a general example, consider that the packet has to travel from point A to point E via the path: A → B → C → D → E. This means that A = Source; B = Via; C, D, E = possible Destinations;

Static Routing Wizard - Creation

Steps: Selection, **Creation**, Review, Load

Destination

Default route: ☐ 30.30.30.0/24

Destination:

Name	Address	Selected
PORT2/Node2/IFM-3/P1/	20.20.20.0/24	<input type="checkbox"/>
PORT2/Node2/IFM-3/P2/	30.30.30.0/24	<input checked="" type="checkbox"/>

Via

Via:

Protocol:

Name	Address	Selected
SERVICE//Ethernet/Eth1 (4)/	192.168.10.2/24	<input checked="" type="checkbox"/>

Distance:

Added Static Routes

Destination	Via	Distance
20.20.20.0/24	192.168.10.2/24	1

Buttons: Add, Delete, Cancel

Navigation: << Prev, Next >>, Cancel

Figure 126 Static Routing Wizard - Creation

- ▶ **Default route:** A default route is the route of the last chance. It is the last route tried by a router, after trying and mismatching all the other routes or if no other route is available. The destination of the default route is always 0.0.0.0/0.
 - ▶ **Unchecked (=default):** The configured static route must not be the default route;
 - ▶ **Checked:** The configured static route must be the default route. In the listings later on, the default route can always be recognized as the route with 0.0.0.0/0;
 - ▶ **Destination:** Fill out a destination network IP address via either manually filling out a custom value e.g. 30.30.30.0/24 or via selecting a port from the router port list. The router port list only contains ports from other virtual routers that are connected in the same service as the selected virtual router. If Default route is checked, a destination cannot be filled out or selected as it will always be 0.0.0.0/0.
- NOTE:** A network IP address (e.g. 30.30.30.0/24) covers the entire network whereas a single IP address (e.g. 30.30.30.1/24) covers one host;
- ▶ **Via:** This is the next hop IP address 'B' via which the source 'A' initially will send its packets to finally reach destination 'E'. Fill out a single IP address via either manually filling out a custom value e.g. 192.168.10.2/24 or via selecting a service router port from the service list. This service router port list changes when selecting another Virtual router in the 'Via' virtual router list.

- Distance: (default = 1, range [1,..,254]) When there are multiple static routes with the same destination IP address but a different 'Via' IP address, the static route with the lowest Distance value will be taken.

- Review: if ok, click Finish. The configuration load manager will be invoked, see §5:

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §7.6.

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

7.8.1 General

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

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

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

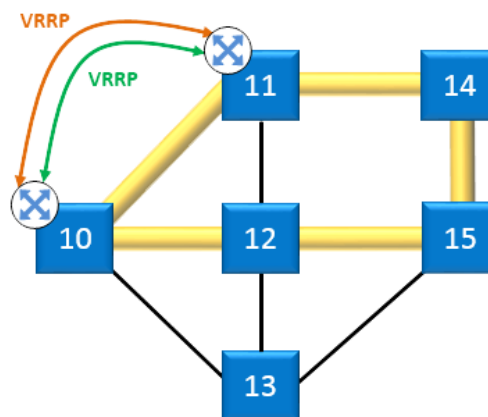


Figure 127 VRRP General

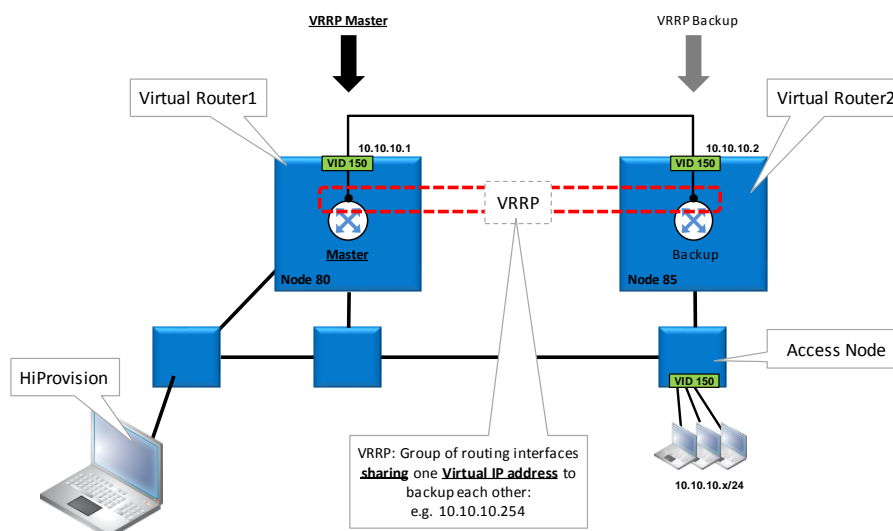


Figure 128 VRRP Example

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

Table 21 VRRP States

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

7.8.2 Prerequisite

Some Virtual Routers must have been created (see §7.5) and the router interfaces must be part of the same IP subnet. Furthermore, it is strongly advised that the redundant routers have similar configurations (*), to easily backup each other. See figure below:

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

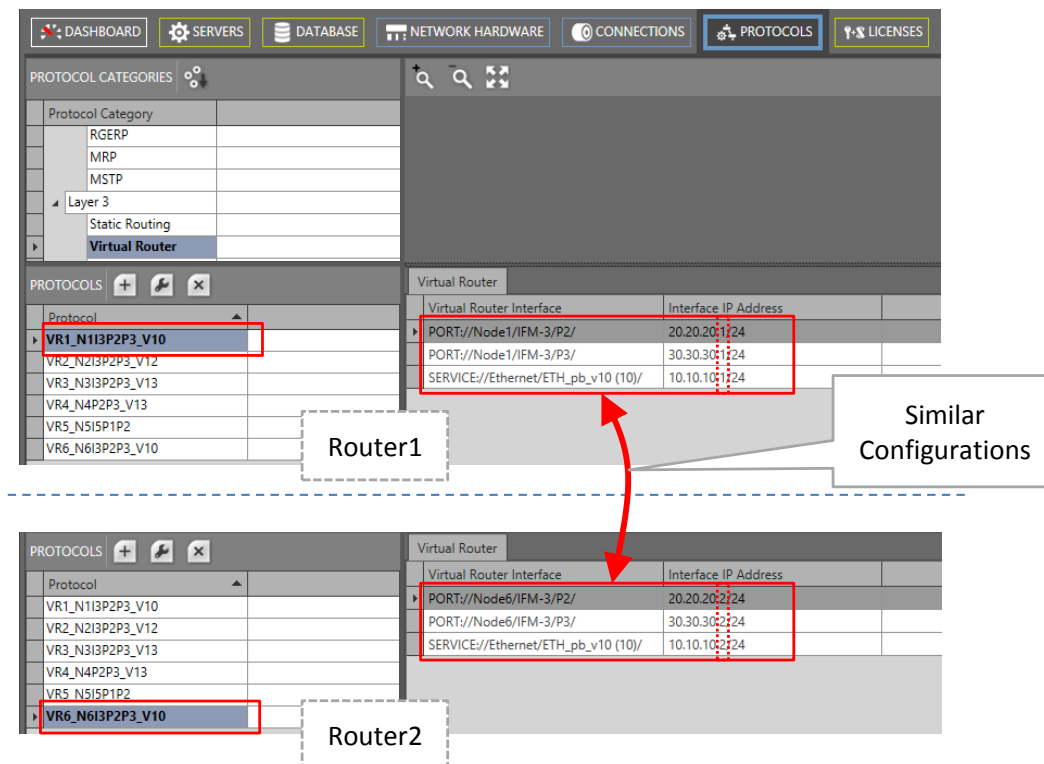


Figure 129 VRRP Prerequisites

7.8.3 Configuration

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

Information: Click Next>>;

Creation:

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

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

NOTE: The maximum amount of VRRP instances can be found in the scalability parameters in Table 18;

Figure 130 VRRP Creation

Figure 131 VRRP Creation: Group Added

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

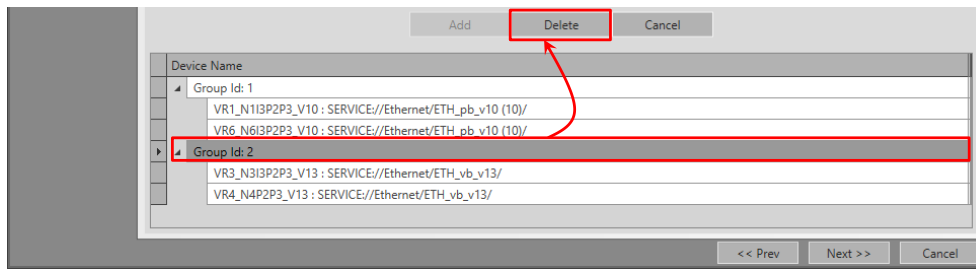


Figure 132 VRRP Creation: Delete Group

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

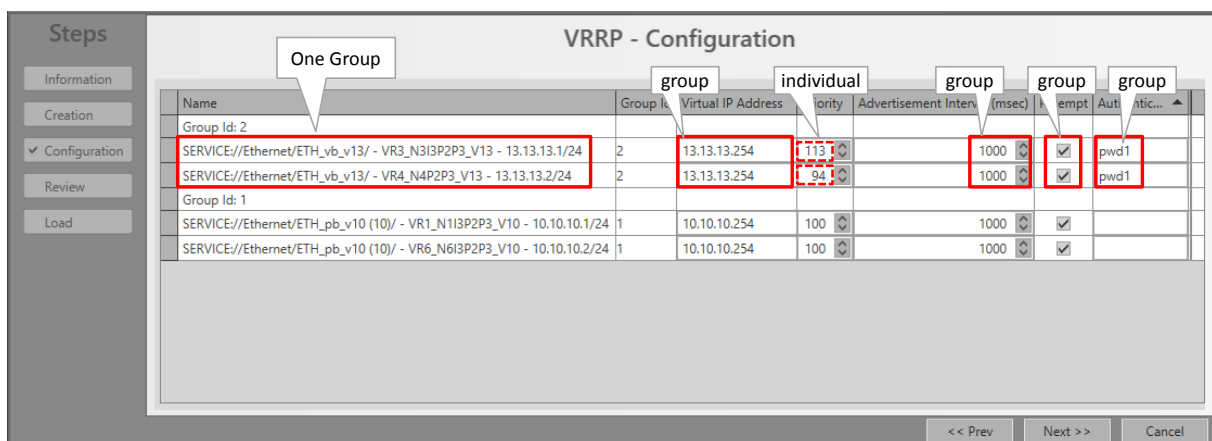


Figure 133 VRRP - Configuration

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

- ▶ Checked (=default): Inside a 'Group', the router interface with the highest priority value always becomes the master. Example with two interfaces on two different routers: interface router1 = priority 100 = master, interface router2 = priority 98 = backup. If router1 fails, router2 becomes the master. Now when the failing original master (router1) with the highest priority returns into the network again after recovery, it will automatically take over the mastership from the backup router (router2) that is also still alive;
- ▶ Unchecked: Inside a 'Group', the router interface that becomes master stays master until it fails. E.g., when a backup router interface becomes master after the original master fails, this backup router interface remains master, even if the original master with the highest priority value is up and running again (e.g. after failure recovery);
- ▶ Authentication (group): optional string field, maximum eight characters, allowed characters: 0...9, a...z, A...Z, !, @, #, \$, %, ^, &, *. An optional textual authentication string can be used to communicate within the 'Group' of that VRRP instance, e.g. 'pwd1'. A router ignores incoming VRRP packets for a specific 'Group', if the authentication string of the packets mismatches the Authentication (group) string configured for the 'Group'.

Review: if ok, click Finish. The configuration load manager will be invoked, see §5;

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §7.6.

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

7.9.1 General

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

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

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

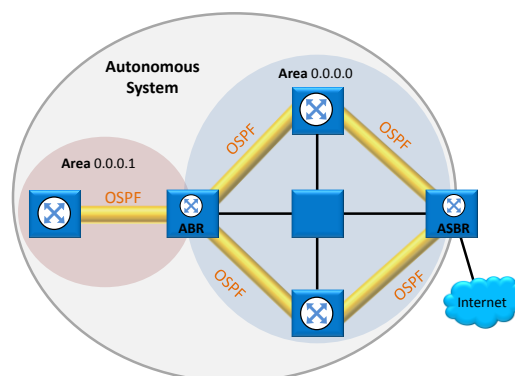


Figure 134 OSPF: General Example

CAUTION: If you want to enable OSPF on a LAG (see §35), configure the LAG in a VLAN. A LAG configured on router ports (L3 Interface Module) does not support OSPF!

Some definitions:

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


Autonomous System Boundary Router (ASBR): an ASBR must be part of the Backbone Area and connects the AS to another non OSPF AS. An ASBR can interconnect different routing protocols and exchange routing information between them. ASBRs typically run an exterior routing protocol or use static routes or a mix of them. An ASBR is used to distribute routes received from other, external Autonomous Systems throughout its own OSPF AS.

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

7.9.2 Prerequisite

At least one Virtual Router must have been created (see §7.5).

7.9.3 Configuration

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

Information: Click Next>>;

Autonomous System Configuration:

- ▶ Select Autonomous System: Select an AS in which the OSPF instance must operate. If the list is still empty or you want to create and select a new AS, select <Create New Autonomous System> instead;
- ▶ Autonomous System Name: fill out an AS name when creating a new AS;

Area Configuration:


- ▶ Area Name: Fill out an Area name;
- ▶ Area Type:
 - ▶ Backbone (=default): This is the master area within the OSPF network and has always Area Number '0.0.0.0'. A Backbone Area must always be created in the OSPF network. All other Stub or Totally Stub Areas will always be directly connected to this Backbone Area. A Backbone Area can receive routes from outside and inside the AS. If Dragon PTN is part of a bigger routed network, with already a Backbone area available outside Dragon PTN:
 - ▶ Creating a Backbone Area in Dragon PTN is not required;
 - ▶ Creating a Backbone Area in Dragon PTN will merge this Dragon PTN Backbone Area with the external backbone area into one bigger backbone area;
 - ▶ Stub: This Area is only connected to the Backbone Area and only receives routes from inside the AS. It also receives the default route from the ABR.
 - ▶ Totally Stub: This Area is only connected to the Backbone Area and only receives the default route (which gives access to the rest of the network) from the Backbone Area.
- ▶ Area Number: is a unique number in the Autonomous System that identifies the Area. This number is 0.0.0.0 for the Backbone Area and is different from 0.0.0.0 for any other Area.
- ▶ Compatible RFC 1583: Indicates how the 'Summary Route' route costs are calculated;
 - ▶ Checked (=default): The costs are calculated according standard RFC 1583 and is based on the lowest cost (=best cost) among the summarized routes. E.g. if the costs of three individual routes are 50, 100 and 200, the cost of the summarized route will be 50;
 - ▶ Unchecked: The costs are based on the highest cost (=worst cost) among the summarized routes. E.g. if the costs of three individual routes are 50, 100 and 200, the cost of the summarized route will be 200;

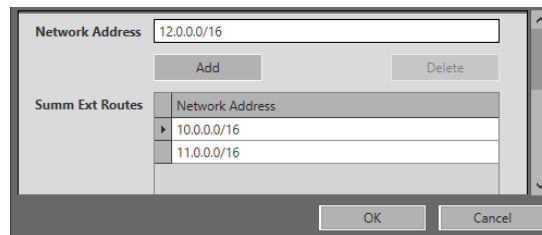
NOTE: Make sure to set Compatible RFC 1583 identically in the entire AS to minimize the chance of routing loops.

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

Figure 135 OSPF: Virtual Router Parameters


- VRF Name: indicates the name of the Virtual Router. Select the VR row in which you want to change configurations.
- Router ID: This is a unique number that identifies the OSPF router. It is pre-filled out with the IP address of the first listed router port of that Virtual Router. The Router ID field can be adapted but it has to be unique throughout the AS;
- ASBR Router: Check this checkbox if this Virtual Router must be configured as an ASBR. It can only be checked if it concerns a Virtual Router in the Backbone Area (0.0.0.0). For other areas, ASBR cannot be configured. External Route (=route from outside the AS) redistribution can only be performed by an ASBR. The fields listed below can be configured for an ASBR:
 - Redistr Conn:
 - Unchecked (=default): disables the redistribution of the networks directly connected to the virtual router;
 - Checked: enables the redistribution of the networks directly connected to the virtual router. If loopback interfaces (see §36) are used on this virtual router, make sure to check this checkbox or make the loopback interface a 'passive' interface (best practice is setting it to 'passive', see further). This is necessary for PIM (see §7.10), to make sure that this loopback interface is known within the entire PIM component;
 - Redistr Stat:
 - Unchecked (=default): disables route redistribution of the static routes into OSPF;
 - Checked: enables route redistribution of the static routes into OSPF;
 - Def Info Orig Always:
 - Unchecked (=default): the ASBR does not propagate a default route into the OSPF routing domain;
 - Checked: the ASBR propagates a default route into the OSPF routing domain;

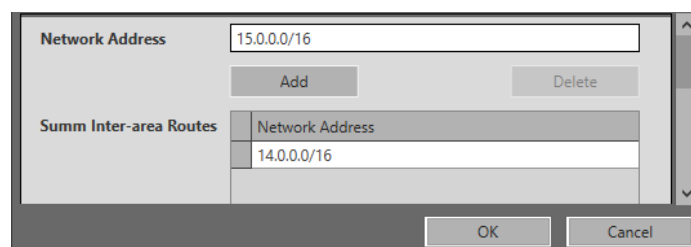
- ▶ Def Info Orig Always Cost: (default = 0, range [0,..,254]) fill out this parameter to assign a route cost to the default route (0.0.0.0/0);
- ▶ Summarize External Routes: Click the  button to create summarized external routes reports. Such a summary report is an aggregation of external routes or external Network Addresses (outside the AS). These summary reports will be distributed within the Areas. In the figure below, fill out the Network Address and click the Add button. E.g. if you have external addresses 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, 10.0.205.0/24, it could be summarized (or added) in the Summarize External Routes list as 10.0.0.0/16. Entries can be removed by selecting the row first and clicking the Delete button.



Network Address	12.0.0.0/16
Add Delete	
Summ Ext Routes	Network Address
	10.0.0.0/16
	11.0.0.0/16
OK Cancel	

Figure 136 OSPF: Summarize External Routes

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



Network Address	15.0.0.0/16
Add Delete	
Summ Inter-area Routes	Network Address
	14.0.0.0/16
OK Cancel	

Figure 137 OSPF: Summarize Inter-Area Routes

Interface Parameters:

VRF Name	Retransmit Interval (sec)	Transmit Delay (sec)	Hello Interval (sec)	Dead Interval (sec)	Priority	Cost	Auth Type	Auth Field	Passive
VR (MODULE/Node1/IFM-3/)									<input type="checkbox"/>
PORT1/Node1/IFM-3/P1/ (44.44.44.44/24)	5	1	10	40	1	10	None		<input type="checkbox"/>
PORT2/Node1/IFM-3/P2/ (66.66.66.66/24)	5	1	10	40	1	10	None		<input type="checkbox"/>
PORT3/Node1/IFM-3/P3/ (55.55.55.55/24)	5	1	10	40	1	10	None		<input type="checkbox"/>

Figure 138 OSPF: Interface Parameters

- ▶ **VRF Name:** indicates the name of the Virtual Router. Select the VR row in which you want to change configurations;
- ▶ **Retransmit Interval (sec) (default=5 s, range [1,...,3600]):** This value configures the time interval between the retransmission of successive LSAs. Each new LSA must be acknowledged. The LSA will be retransmitted by the originating router according the Retransmit Interval until it has been acknowledged by the neighbor router;
- ▶ **Transmit Delay (sec) (default=1 s, range [1,...,3600]):** This value configures the estimated time required to transmit a link state update packet on the interface using this configuration. This variable adds a specified time to the age field of an update. If the delay is not added before transmission over a link, the time in which the link-state advertisement (LSA) propagates over the link is not considered. This parameter has more significance on very low-speed links;
- ▶ **Hello Interval (sec) (default=10 s, range [1,...,65535]):** This value configures the (OSPFv2 Hello) interval between the hello packets sent on the interface. Hello Packets are sent between two OSPF neighbors to maintain connectivity. The Hello Interval must be the same for all (virtual) router interfaces attached to the same link. See also the Dead Interval parameter. ATTENTION: OSPF neighbors must have the same Hello Interval value!
- ▶ **Dead Interval (sec) (default=40 s, range [1,...,65535]):** The Dead Interval and Hello Interval work together to maintain the operational link between two OSPF neighbors. If a virtual router interface does not receive a Hello packet within the configured Dead Interval, the (virtual) router decides that the neighboring (virtual) router is dead or down. By default, the Dead Interval is four times the Hello Interval. ATTENTION: OSPF neighbors must have the same Dead Interval value!
- ▶ **Priority (default=1, range [0,...,255]):** This value configures the interface priority to determine the Designated Router (DR) for the link connected to the interface. In the DR election process the highest Priority value wins and becomes DR. If the two DR candidates have the same Priority, the highest Router Id (RID) wins. Priority '0' means that the virtual router does not participate in the DR election process and as result cannot become the DR;
- ▶ **Cost (default=10, range [1,...,65535]):** This value configures the cost metric value added to a route on this interface. Following formula can be used as a rule of thumb to define the Cost for a specific route. $Cost = \frac{\text{Highest link speed in the OSPF domain in Mbps}}{\text{Current link speed in Mbps}}$, e.g. if the highest link speed is 10 Gbps,

and the current link speed = 100 Mbps, then the Cost for this link could be $10000/100 = 100$. The Cost for a link with the highest speed would be $10000/10000 = 1$.

- ▶ Auth Type: OSPF authentication can be done via selecting one of the following authentication types listed below. ATTENTION: Make sure that neighboring routers (or virtual router interfaces) use the same Auth Type and Auth Field;
 - ▶ None (=default): There is no OSPF authentication at all on this virtual router interface;
 - ▶ Auth Text: Authentication on this virtual router interface is done based on Simple Password Authentication, a password must be specified in the Auth Field (alphanumeric input) which is to be used by the neighboring routers that are using the OSPF simple password authentication. ATTENTION: OSPF neighbors must have the same password;
 - ▶ Messages Digest: Authentication on this virtual router interface is done via md5 cryptographic authentication. A password must be specified in the Auth Field (alphanumeric input) which is to be used by the neighboring routers that are using the OSPF Message Digest authentication;
- ▶ Auth Field: (alphanumeric input) Fill out a password or an authentication key that must be used for authentication when Auth Type is Auth Text or Message Digest. ATTENTION: Make sure that neighboring routers (or virtual router interfaces) use the same Auth Type and Auth Field.
- ▶ Passive:
 - ▶ Unchecked (=default): This virtual router interface is active, it participates in the OSPF protocol;
 - ▶ Checked: This virtual router interface is passive, it ignores routing updates on this interface and does not send 'Hello' packets and routing updates. A passive interface could be set for interfaces that do not have neighbors. This parameter can also be used for testing or troubleshooting purposes. If loopback interfaces (see §36) are used on this virtual router, make sure to check this checkbox (=best practice) or check the 'Redistr Conn' checkbox (see before). This is necessary for PIM (see §7.10), to make sure that this loopback interface is known within the entire PIM component;

- ▶ Review: if ok, click Finish. The configuration load manager will be invoked, see §5:

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §7.6.

7.10 Layer 3: PIM

7.10.1 General

PIM (Protocol-Independent Multicast) is a multicast routing protocol. It is protocol independent because PIM does not have a network topology discovery mechanism like other routing protocols have. PIM uses routing information supplied by other routing protocols. PIM builds up Multicast Distribution Trees for each IP Multicast Group Address. As a result, data packets from senders to a multicast group reach all receivers that have joined the group via IGMP.

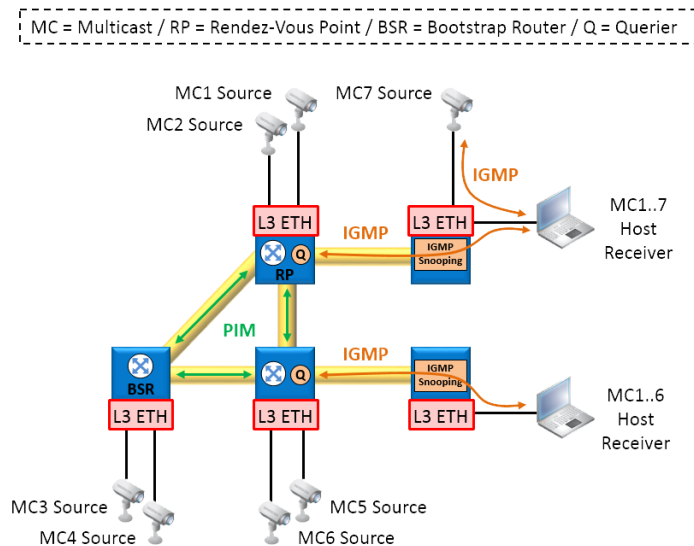


Figure 139 PIM/IGMP/IMGP Snooping Overview

Some definitions:

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

Designated Router (DR): Using PIM when a host expresses interest in joining a multicast group, it does so using IGMP. For each (sub-) network, a single router is elected to be the


DR for the network. When an IGMP message is seen by the DR it then uses PIM to send a message to the RP, for the multicast group.

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

7.10.2 Prerequisite

At least one Virtual Router (on an L3 Interface Module) and an Ethernet service must have been created (see §7.5).

7.10.3 Configuration

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

Information: Click Next>>;

Creation:

- ▶ Name: Assign a name to the PIM component. A PIM component corresponds to the PIM domain and classifies it as Sparse mode. A PIM domain is defined as an area of the network over which bootstrap messages are forwarded. Typically, a PIM router will be a member of exactly one domain;
- ▶ Component Number (default=1, range[1,..,254]): HiProvision automatically assigns a number to the PIM component;
- ▶ Interface Selection: Select the interfaces from the L3 Interface Modules that participate in PIM;

Interface Configuration:

- ▶ Query Interval (default=30 s, range[1,..,18725]s): sets the frequency in seconds at which PIM Hello (=query) messages are transmitted on this interface. The query message informs the presence of a PIM router on this interface to the neighboring PIM routers;
- ▶ Message Interval (default=60 s, range[10,..,600]s): sets the frequency in seconds at which Join messages are transmitted on this interface to keep the receipt of a joined multicast stream alive. The same Join message interval must be used on all the PIM routers in the PIM domain. If all the routers do not use the same timer interval, the performance of PIM can be adversely affected;
- ▶ DR Priority (default=1, range[1,..,65535]): This value indicates the Designated Router (=DR) priority. This value is used to determine the Designated Router for the link connected to the interface. In the DR election process the highest Priority wins and becomes DR. If the two DR candidates have the same Priority, the highest Router Id (RID) wins.
- ▶ Bootstrap Selection: out of the previously selected Virtual Router interfaces, indicate which one must act as Bootstrap Router Candidate (BSR-C). Later on, when PIM is up and


running in the network, the Bootstrap Router (BSR) will be elected dynamically by means of bootstrap messages and the BSR-C Priority. The highest BSR-C priority wins, and will become the active BSR. The other candidates become standby BSRs;

► **Bootstrap Configuration:**

- Priority (default=1, range[1,..,255]): The Priority will be used for the BSR election process later on in the network. The highest priority wins.

► **Rendez-Vous Point Selection:** out of the previously selected Virtual Router interfaces, indicate which one must act as Rendez-Vous Point Candidate (RP-C). Later on, when PIM is up and running in the network, the RP-Cs will advertise themselves to the BSRs;

► **Rendez-Vous Point Configuration:**

- Hold-time (default=80, range[3,..,255]): When the router is a RP candidate in the local domain, this field defines the time interval (in seconds) till which the RP candidate advertisement is valid. The Hold-time defines the age for the RP advertisement.
- Priority (default=192, range[1,..,255]): Indicates the Priority for each RP-C which will be used later on for electing a specific RP for a specific Multicast address group or range. For the same multicast address ranges, the lowest Priority wins and becomes the RP for that multicast address range. The other interfaces become standby RPs.
- Fill out a Rendez-Vous Point Range for each Rendez-Vous Point:
 - Select the Rendez-Vous Point Line and click the  icon. A new window pops up:
 - Network Address: Fill out a valid multicast address range e.g. 224.100.100.3/24 for which this RP is responsible. Click the Add button to add this address to the 'Rendez-Vous Point Ranges' address list. Repeat this step until all the multicast address ranges are configured for this RP. Click OK.
 - See figure below:

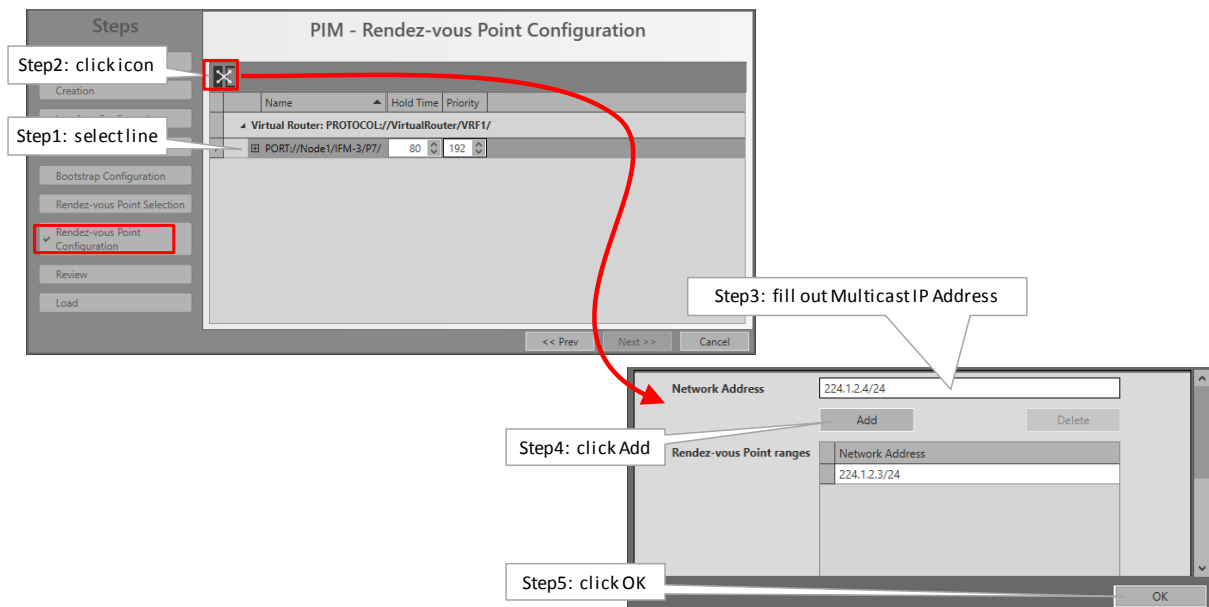


Figure 140 Rendez-Vous Point Configuration

- Review: if ok, click Finish. The configuration load manager will be invoked, see §5:

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §7.6.

7.11 Layer 3: IGMP

7.11.1 General

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

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

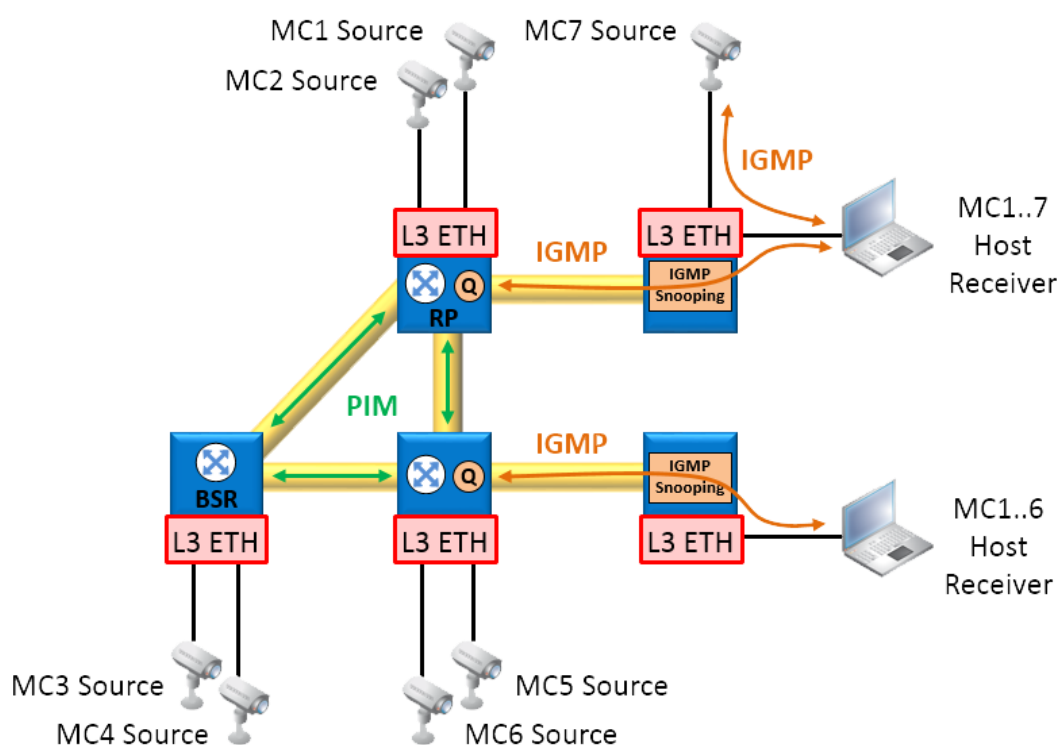


Figure 141 PIM/IGMP/IGMP Snooping Overview

Some definitions:

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

Leave a multicast-group: The hosts can leave (or disconnect from) a multicast stream via a time-out (IGMPv1), Leave group requests (IGMPv2).

IGMP is VLAN based and runs between the router itself and the VLANs connected to its router interfaces. As a result, if a host that is part of a VLAN joins a multicast stream, all the other members of the VLAN will receive the multicast-stream as well. To prevent this, configure IGMP snooping (see §7.4) on this router interface to make sure that only the stream requester(s) is (are) receiving the stream, and not all the other uninterested members of the VLAN.

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


Table 22 IGMP Version Dependencies

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

7.11.2 Prerequisite

At least one Virtual Router (on L3 Interface Module) and an Ethernet service must have been created (see §7.5). Make sure that the Ethernet service has been selected in the Virtual Router.

7.11.3 Configuration

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

Information: Click Next>>;

Service Selection: Select the service on which IGMP must be configured;

Virtual Router Selection: Select the Virtual Router(s) on which IGMP must be configured;

Properties:

- ▶ Leave Mode:
 - ▶ Normal (=default): the port will not be removed immediately from the multicast group when a leave message is detected on that port. First some group specific queries are sent on that port, and if no membership report is received within a time interval on that port for that multicast group, the port will be removed from that multicast group.
 - ▶ Fast: the port will be removed immediately from the multicast group when a leave message is detected on that port.
 - ▶ Last Member Query Interval (default=10 s, range[1,...,255] s): Configures the time interval that is used by the L3 Interface Module to send group specific queries on a its configured IGMP ports.

- ▶ Query Interval (default = 125 s, min. range[11,...,65535] s): is the amount of time in seconds between IGMP General Query messages sent by the querier, if this node is the querier.
 - ▶ Max Response Time (default = 100 '1/10 s' = 10 seconds, range[1,...,255] '1/10 s'): Specifies the period in tenths of a second in which the host is expected to respond to an IGMP query.
 - ▶ Robustness (default = 2, range[2,...,7]): Configure this parameter to indicate how well your network can recover from lost IGMP packets. If you have a very stable network, the Robustness value will be very low. For less stable networks, the Robustness value must be set higher or high. E.g. if the Robustness value = '3', your network can recover from (robustness-1) IGMP packets = (3-1) = 2 IGMP Packets. Changing the Robustness variable automatically modifies certain IGMP message intervals for IGMPv2. Increasing this value allows for more packet loss but increases the leave latency of the subnetwork.
 - ▶ IGMP Version: Indicates the used IGMP version: V1, V2 (=default);
 - ▶ Review: if ok, click Finish. The configuration load manager will be invoked, see §5:
- NOTE:** Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §7.6.

7.12 Layer 3: DHCP Relay

7.12.1 General

DHCP (=Dynamic Host Control Protocol) is a network configuration protocol in IP networks which allows that IP clients at start-up automatically request IP configuration data from a DHCP Server. This data is necessary for the client to be able to communicate with other IP clients within the IP network. The most important IP configuration data for the IP client is:

Own IP Address;

Subnet Mask;

Default Gateway IP Address;

DNS Server IP Address(es)-Domain Name;

- ▶ Lease Time (amount of time that the IP configuration data is valid for this IP client).

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

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

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

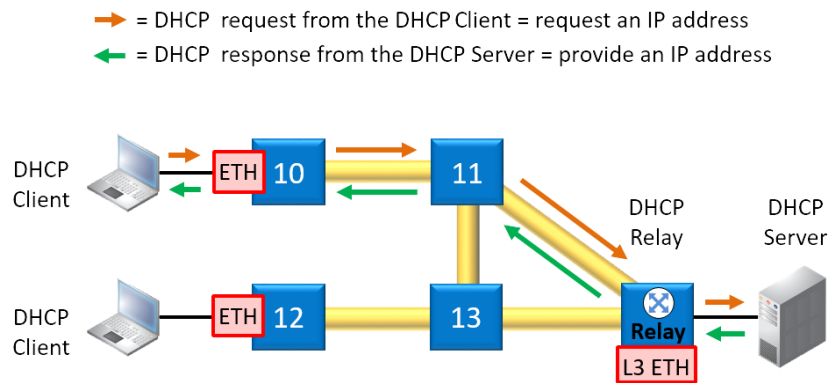


Figure 142 DHCP Overview

7.12.2 Prerequisite

At least one Virtual Router (on L3 Interface Module) and an Ethernet service must have been created (see §7.5). Make sure that the Ethernet service has been selected in the Virtual Router.

7.12.3 Configuration

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

Information: Click Next>>;

Creation:

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

Steps

- Information
- ✓ Creation
- Configuration
- Review
- Load

DHCP Relay - Creation

Name: Relay3

Information Option: ☒

Virtual Router Selection

Name	
VRF3	<input type="checkbox"/>

<< Prev Next >> Cancel

Figure 143 DHCP Relay: Creation

Configuration:

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

Steps

- Information
- Creation
- ✓ Configuration
- Review
- Load

DHCP Relay - Configuration

DHCP Server IP Address: 192.172.16.5

Add Remove

DHCP Servers

IP Address
192.172.16.5

<< Prev Next >> Cancel

Figure 144 DHCP Relay: Configuration

- ▶ **Review:** if ok, click Finish. The configuration load manager will be invoked, see §5:

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols. A Layer 3 view with all the virtual router interconnections can be found in §7.6.

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


7.13.1 General

An Access Control List (=ACL) restricts communication access on a port in an Ethernet service. IP ACL permits access based on a source and/or destination IP address range of the incoming packets. If no ACL rules are created, all traffic is allowed. On a port (front, back end, LAG), either MAC ACL (see §7.14) or IP ACL can be configured. On Ethernet Interface Module (see §32) ports, combining MAC and IP ACL is not possible. On L2/L3 Interface Modules, combining MAC and IP ACL is possible. When both are combined, first IP ACL will be checked then MAC ACL.

7.13.2 Prerequisite

An Ethernet service must have been configured between Interface Modules that support the Ethernet service, see §32. A tunnel different from point-to-point must be used.

7.13.3 Configuration

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

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

Information: Click Next>>;

Service Selection: select the Ethernet service for which an IP ACL must be configured;

► Port Configuration (only for Ethernet Interface Modules, see §32):

► Enable ACL:

► Unchecked (=default): IP ACL is disabled for this port, all incoming packets from any source and destination IP address are allowed on this port.

► Checked: IP ACL is enabled for this port. Source/Destination Address filled out: If the source/destination IP address of the incoming Ethernet packet is in the range of the configured Source/Destination Address, the packet will be allowed. If both addresses are filled out, both addresses of the incoming packet must be in their configured range. If none of the above conditions are met, the packet will be dropped;

► Greyed out checkbox: IP ACL cannot be configured on this port because a MAC ACL (see §7.14) has already been configured on this port. Per port, only MAC ACL or IP ACL can be configured, not both together;

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

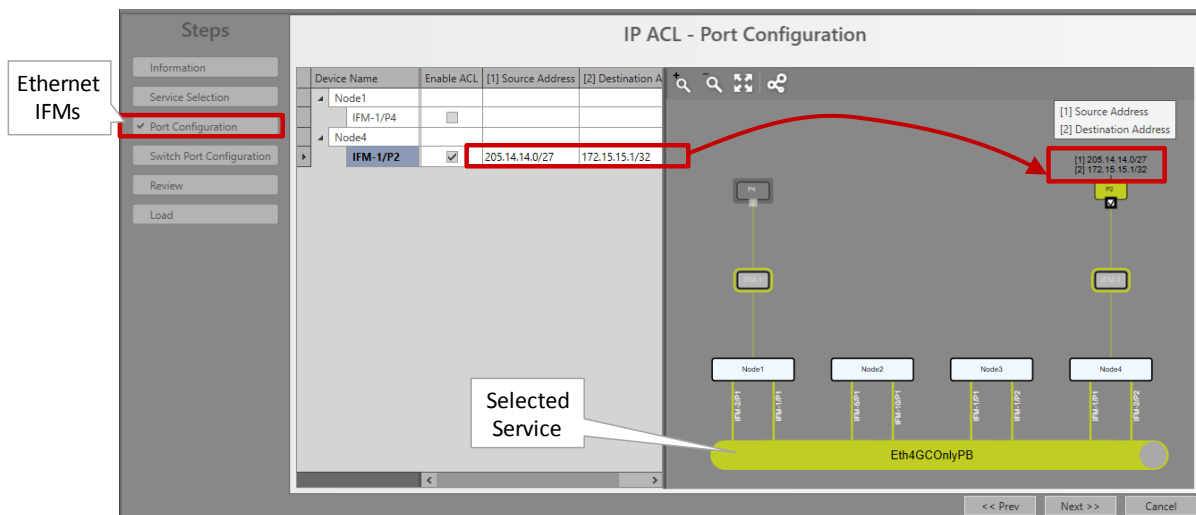


Figure 145 IP ACL: Port Configuration Example for Ethernet Interface Modules

- **Switch Port Configuration (only for L2/L3 Interface Modules, see §32):** By default, no IP ACL rules are created per Interface Module and as a result, all traffic is allowed. To configure IP ACL on a front or back end port, create an ACL rule first in the Configuration section (parameters described below), add it to a port and then check Enable ACL in the Interface Module row. Multiple rules can be added per port.
- **Add rule:** select a port row in the device tree view and click the Add Rule button to add the rule to this port. It is possible to select multiple ports by clicking each row while holding the CTRL key pressed, or even by clicking the entire Interface Module, or by clicking in the tree view area and press CTRL+A to select all Interface Modules. When clicking the Add Rule button, the configured rule will be added to all selected Interface Modules.
- **Delete rule:** select a rule row in the device tree view and click the Delete Rule(s) button. It is possible to select multiple rule rows by clicking each row while holding the CTRL key pressed, or even by clicking in the tree view area and press CTRL+A to select all rules. When clicking the Delete Rule(s) button, all selected rules will be deleted.
- **Configuration Section:**
 - **Filter:**
 - **Permit (=default):** Permit (=allow) all incoming messages on a port according to the configured IP Addresses and Priority;
 - **Deny:** Deny (=block) all incoming messages on a port according to the configured IP Addresses and Priority;
 - **Source/Destination Address:** the IP address range (or network address) that must be matched when IP ACL is enabled on this port. Format of this field: the IP address range must have a valid subnet mask notation, e.g. a , 192.168.5.64/26, 205.14.14.0/27. For a single host, e.g. 172.15.15.1, fill out 172.15.15.1/32. If nothing is filled out, any IP address counts.
 - **Priority (default = 1, value[1..100]):** Indicates the priority in which this configured rule on a specific port within an Interface Module will be processed. Value '1' has

the lowest priority, value '100' has the highest priority. Rules with the highest priority are processed first. If the priority of multiple rules within an Interface Module is the same, the rule that was created first will be processed first. A rule is hit when the IP address of both the data packet and the configured rule match. If a rule is hit, the remaining rules for the same port will not be processed anymore.

► Device Tree view:

► Enable ACL:

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

The screenshot shows the 'IP ACL - Switch Port Configuration' window. On the left, a 'Steps' sidebar has 'Switch Port Configuration' selected. The main area is divided into 'Configuration' and a table of device rules.

Configuration Section:

- Filter: Permit
- [1] Source Address: 205.14.14.0/27
- [2] Destination Address: 172.15.15.1/32
- Priority: 1

Table of Rules:

Device Name	Enable ACL	[1] Source Address	[2] Destination Address	Filter	Priority
Node20					
IFM-3/BE2	<input type="checkbox"/>				
IFM-3/P1	<input type="checkbox"/>				
Node21					
IFM-3/BE2	<input type="checkbox"/>				
IFM-3/P1	<input type="checkbox"/>				

Annotations:

- Step1: Configure Rule:** Points to the configuration fields.
- Step2: Select port row:** Points to the IFM-3/BE2 row for Node20.
- Step3: Click Add Rule:** Points to the 'Add Rule' button.
- Step4: Rule Added:** Points to the newly added 'Rule 1' in the table.
- Step5: Enable ACL to activate rule:** Points to the 'Enable ACL' checkbox for Rule 1.

Figure 146 IP ACL: Switch Port Configuration Example for L2/L3 Interface Modules

► Review: if ok, click Finish. The configuration load manager will be invoked, see §5;

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

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

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


7.14.1 General

An Access Control List (=ACL) restricts communication access on a port (front, back end, LAG) in an Ethernet service. MAC ACL permits access based on the source MAC address of the incoming packets. On Ethernet Interface Module (see §32) ports, combining MAC and IP ACL is not possible. On L2/L3 Interface Modules, combining MAC and IP ACL is possible. When both are combined, first IP ACL will be checked then MAC ACL.

7.14.2 Prerequisite

An Ethernet service must have been configured between Interface Modules that support the Ethernet service, see §32. A tunnel different from point-to-point must be used.

7.14.3 Configuration

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

NOTE: If both MAC ACL and Sticky MAC (see §24.1.1) are active, a packet from a source MAC address is only allowed when the MAC address is allowed in both features.

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

Information: Click Next>>;

Service Selection: select the Ethernet service for which a MAC ACL must be configured;

► Port Configuration (only for Ethernet Interface Modules, see §32):

► Enable ACL:

► Unchecked (=default): MAC ACL is disabled for this port, all incoming packets from any source MAC address are allowed on this port.

► Checked: MAC ACL is enabled for this port. If the source MAC address of the incoming Ethernet packet matches the configured MAC address, the packet will be allowed. If not, the packet will be dropped;

► Greyed out checkbox: MAC ACL cannot be configured on this port because an IP ACL (see §7.13) has already been configured on this port. Per port, only MAC ACL or IP ACL can be configured, not both together;

► MAC Address: the MAC Address that must be matched when ACL is enabled. One address can be configured per port. Allowed formats: 'XX-XX-XX-XX-XX-XX', 'XX:XX:XX:XX:XX:XX' or 'XXXXXXXXXXXX' with X=[0..9] [A..F];

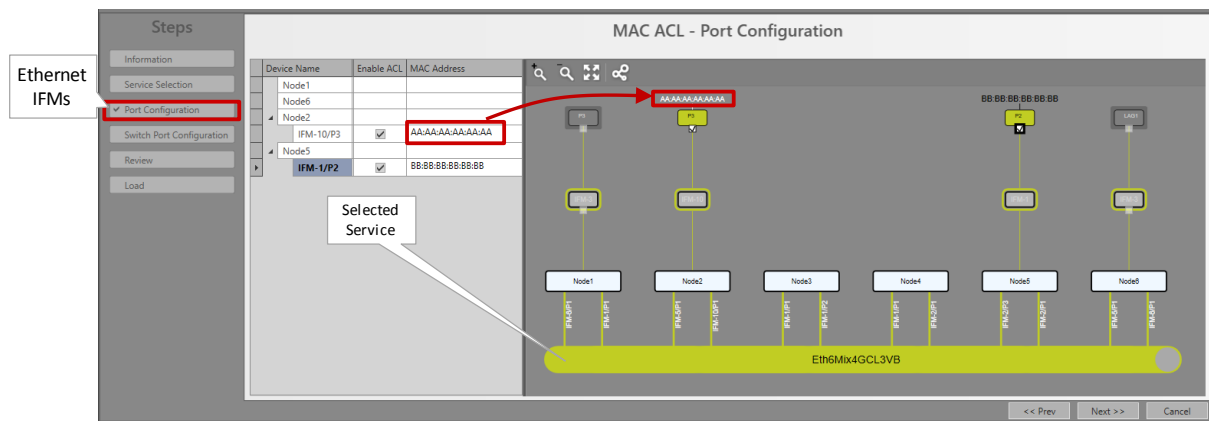


Figure 147 MAC ACL: Port Configuration Example for Ethernet Interface Modules

- Switch Port Configuration (only for L2/L3 Interface Modules, see §32): By default, no MAC ACL rules are created per Interface Module and as a result, all traffic is allowed. To configure MAC ACL on a front or back end port, create an ACL rule first in the Configuration section (parameters described below), add it to a port and then check Enable ACL in the Interface Module row. Multiple rules can be added per port.
- Add rule: select a port row in the device tree view and click the Add Rule button to add the rule to this port. It is possible to select multiple ports by clicking each row while holding the CTRL key pressed, or even by clicking the entire Interface Module, or by clicking in the tree view area and press CTRL+A to select all Interface Modules. When clicking the Add Rule button, the configured rule will be added to all selected Interface Modules.
- Delete rule: select a rule row in the device tree view and click the Delete Rule(s) button. It is possible to select multiple rule rows by clicking each row while holding the CTRL key pressed, or even by clicking in the tree view area and press CTRL+A to select all rules. When clicking the Delete Rule(s) button, all selected rules will be deleted.
- Configuration Section:
 - MAC Address: the MAC Address that must be matched when ACL is enabled.
Allowed formats: 'XX-XX-XX-XX-XX-XX', 'XX:XX:XX:XX:XX:XX' or 'XXXXXXXXXXXX' with X=[0..9] [A..F];
- Device Tree view:
 - Enable ACL:
 - Unchecked (=default): MAC ACL is disabled for this port, all incoming packets from any MAC address are allowed on this port;
 - Checked: MAC ACL is enabled for this port. MAC Address filled out: If the MAC address of the incoming Ethernet packet matches the filled out MAC address the packet will be allowed. If not, the packet will be dropped.

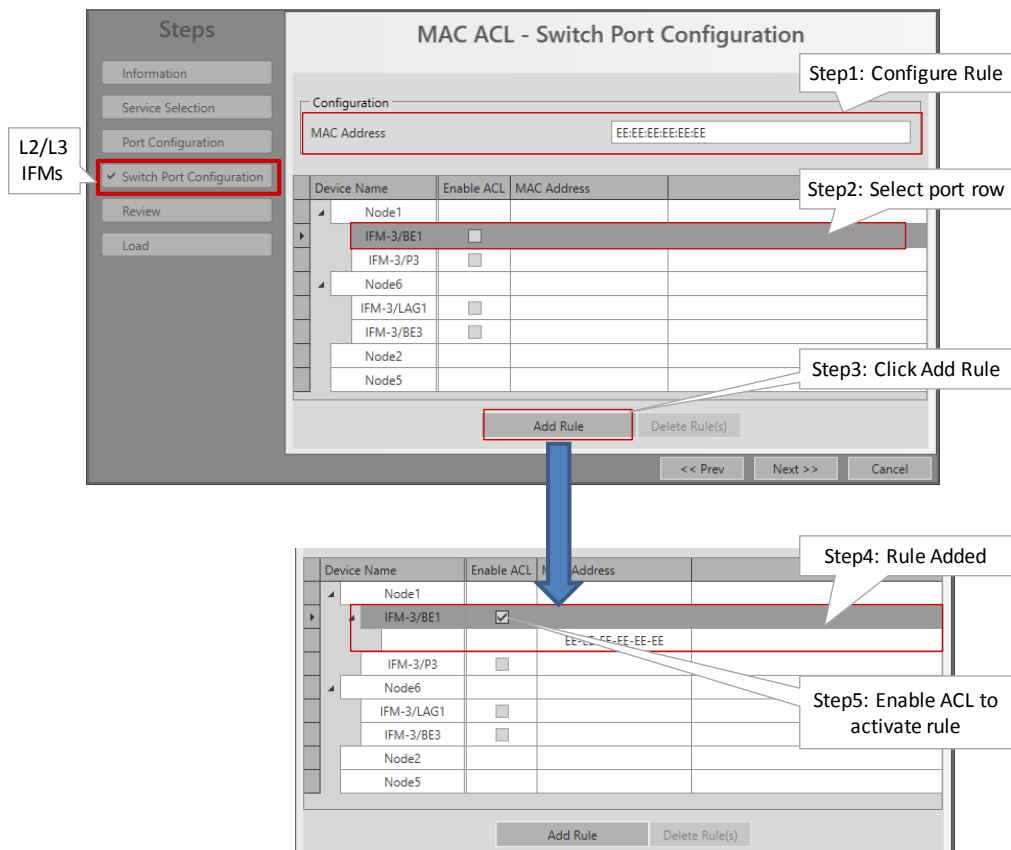


Figure 148 MAC ACL: Switch Port Configuration Example for L2/L3 Interface Modules

Review: if ok, click Finish. The configuration load manager will be invoked, see §5;

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

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

7.15 Other: Voice Protocol

7.15.1 General

The Voice Protocol must be configured to configure extra service properties. An overview can be found below:

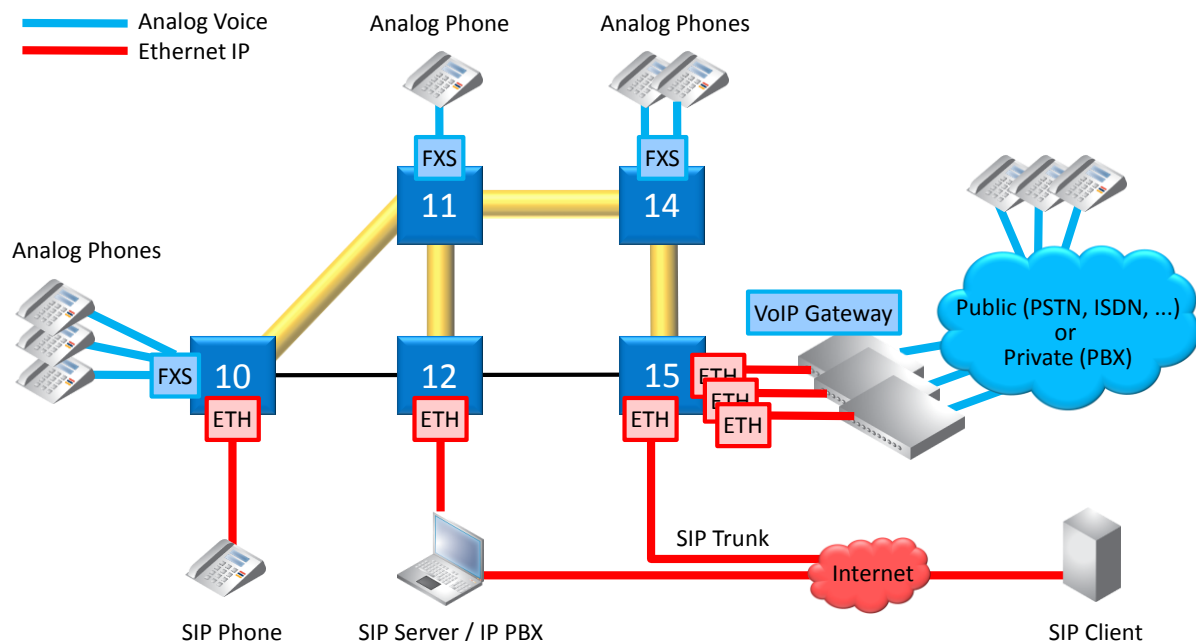


Figure 149 Voice Service Elements Overview

7.15.2 Prerequisite

A Voice service must have been created.

7.15.3 Configuration

Go to Dashboard → (Configuration) Protocols → Protocol Categories → Other → Voice Protocol → (Protocols) .

Depending on the configured voice type in the service, the settings will differ:

Remote Extension Mode: see §7.15.4;

SIP-Server Mode: see §7.15.5;

7.15.4 Remote Extension (FXO Gateway) Mode

a. General

See Figure 149: connections between FXS ↔ VoIP Gateway (=FXO Gateway);

Analog phones in the Dragon PTN network are a remote extension of the public (PSTN) and/or private (PBX) telephone network. The extension is possible via a third party VoIP Gateway (e.g. Patton), in this case an FXO Gateway;

Analog phones are connected to an FXS interface (8-FXS module);

FXO Gateways are connected to an Ethernet interface (e.g. 4-GC-LW module);

Voice switching and telephony feature handling between all phones are performed in the PSTN or PBX;

DTMF (=Dual Tone Multi-Frequency) must be used for number dialing;

Analog speech and signaling are converted and packetized by the FXS interface and the FXO Gateway towards the Dragon PTN network;

b. Configuration

Information: Click Next>>;

- ▶ Service Selection: select the Voice service in the list for which you want extra configuration and registration settings. Only the voice services without Voice Protocol configuration yet will be listed. Click Next>>;

Service Properties:

- ▶ DTMF Transmit Mode: DTMF is a voice-frequency signaling system that generates tones when the caller presses numbers on its phone. This field has only impact when the call has already been set up. During a call, when the caller is requested to enter some extra numbers for selecting a menu (e.g. press '1' for sales, '2' for services etc...), the selected DTMF Transmit Mode below configures how these entered numbers are transmitted on the line. Make sure that this setting matches the setting in the FXO Gateway. Click Next>>;
- ▶ Audio Passthrough: Transports the DTMF tones transparently inband between the two SIP endpoints, the caller and callee. The tones are encoded within the voice. When using this method, it is strongly advised to use a G711 Audio Codec (G729 could compress the tones too much resulting in unrecognized tones at the receiving side);
- ▶ Rtp: Inband method that sends DTMF tones separately in dedicated RTP packets, distinct from audio packets.
- ▶ Sip (=default): Inband method that sends DTMF tones separately in dedicated SIP packets, distinct from audio packets.

8-FXS Port Properties: Each phone connected to an 8-FXS port has some properties that can be configured in this page. Click the arrow in the Device Name column to expand/collapse the node to show/hide the 8-FXS ports in this service. Configure the port property via clicking a cell in the port row and start typing to enter or select a value;

Table 23 8-FXS Port Properties (Remote Extension)

Field	Values	Description
Device Name	<ports>	Shows the selected 8-FXS ports in the voice service that must be configured.
Display Name (=future support)	<text>	Name that must be displayed on the telephone display on the receiver side (=callee) when a call is set up.
Telephone Number	<number>	Telephone number that is assigned to the telephone connected to this 8-FXS port (=caller).
Auth User Name	<text>	User name assigned to this FXS port. This user name will be used in the SIP messages to

Field	Values	Description
		authenticate this FXS port to the VoIP Gateway when it requests some client authentication.
Auth Password	<text>	Password assigned to this FXS port. This password will be used in the SIP messages to authenticate this FXS port to the VoIP Gateway when it requests some client authentication.
Audio Codec	G711a (=default) G711u G729	Encoding/Decoding standards that encodes/decodes analog voice into digital data or vice versa. G711a is the preferred Codec. Fallback to one of the other Codecs is possible if the SIP-server or remote side does not support this preferred Codec. The G711 codec provides an uncompressed high voice quality but requires almost 3 times more bandwidth (87 kbps) than the G729 codecs (32 kbps) which transmit a more compressed voice quality. So G729 calls have less voice quality than G711 calls, but are still good enough for most calls. So it is a tradeoff between voice quality and bandwidth. When using the Audio Passthrough DTMF transmit mode (see previous), it is strongly advised to use a G711 Audio Codec whereas the G729 could compress the tones too much resulting in unrecognized tones. The G711u (=µlaw) Codec is mostly used in Northern-America and Japan whereas G711a (=A-Law) is mostly used in the rest of the world.
VoIP Gateway	<ip address>	Default = 0.0.0.0. IP address of the VoIP Gateway.
Remote SIP Port	<number>	Default = 5060. Indicates the remote SIP port that the VOIP Gateway is listening to for SIP traffic. The local SIP port on the PTN-8-FXS Interface Module is not configurable and is by default 5060.

Review: if ok, click Finish. The configuration load manager will be invoked, see §5.

NOTE: Monitoring info available via Dashboard → (Monitoring) Protocols → Other → Voice or via Dashboard → (Monitoring) Performance → Port Performance → Ethernet Port Monitoring.

7.15.5 SIP-Server Mode

a. General

See Figure 149: SIP elements like a SIP Phone and VoIP gateways can be registered on and handled by the SIP Server;

Analog phones are connected to an FXS interface (8-FXS module) which are registered on a SIP Server;

Voice switching and telephony feature handling for all calls are performed in the SIP Server;

Possible SIP telephony features depend on the used SIP devices and their interoperability.

b. Configuration

Information: Click Next>>;

► Service Selection: select the Voice service in the list for which you want extra configuration and registration settings. Only the voice services without Voice Protocol configuration yet will be listed. Click Next>>;

Service Properties:

► DTMF Transmit Mode: See §7.15.4;

- Dial Plan - Translation Pattern (default = e#r*~, use Reset button to set back to default): The Dial Plan specifies how a PTN-8-FXS Interface Module must interpret digit sequences dialed by the caller, and how to convert the digit input into an outgoing dial string. The rules will be applied to all the PTN-8-FXS Interface Modules in the service. Optional, click the Configure button to configure a more advanced Dial Plan - Translation Pattern. NOTE: it is also possible to overwrite this field manually without using the Dial Plan wizard (for advanced users!).

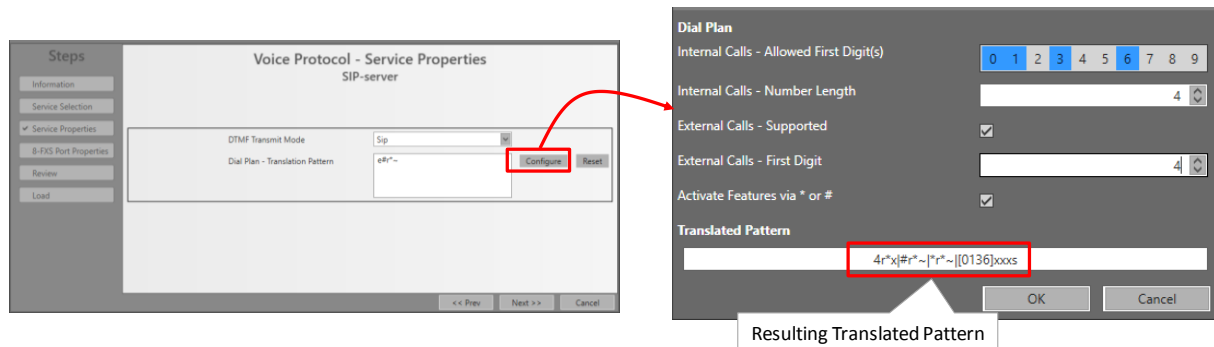


Figure 150 Dial Plan - Translation Pattern

- Internal Calls - Allowed First Digit(s): (default = no allowed first digits = no internal calls allowed) Click the numbers that are allowed as first digit when dialing a number for an internal call.
- Internal Calls - Number Length: (default = 4, range [1..10]) Fill out the allowed dialed number length for internal calls e.g. internal number 4831 has length 4.
- External Calls - Supported:
 - Checked (=default): external calls supported;
 - Unchecked: external calls not supported.
- External Calls - First Digit: (default = 0, range [0..9]) If external calls are supported, fill out the number that must be used as first digit to set up external calls.
- Activate Features via */ #:
 - Checked (=default): telephone features are activated and can be accessed via dialing first the '*' or '#' key. See your SIP-server documentation to find the allowed feature codes;
 - Unchecked: telephone features are disabled.
- Example Resulting Translated Pattern: 4r*x|#r*~|*r*~|[0136]xxxx
 - 4r*x = Indicates that external calls (with first digit = 4) are supported;
 - r*~ = indicates allow any digit (0-9, a-d, *, #) until the timeout or the terminating character is found;
 - #r*~ = allows the digit string to start with '#';
 - *r*~ = allows the digit string to start with '*';
 - [0136]xxxx = Internal calls with a length of 4 characters and starting with 0, 1, 3 or 6 are allowed;

Table 24 Translated Pattern Parameters

Parameters	Description
------------	-------------

Parameters	Description
	separates different possible patterns
r	repeat by following a number (1-9), letter (a-z for 10 to 35 times) or "*", "+" or "." to mean any number of times (255 times)
.	repeat previous digit any number of times (0 to 255)
+	repeat previous digit any number of times (0 to 255)
x	match any numerical digit (0-9)
~	match any digit (0-9, A-D, *, #) excluding any specified terminators
!	disallows pattern
\$	indicates secondary dialing to follow - used only by fixed dial strings
<:>	replace group to replace left digit(s) with right digit(s)
[]	selection group of candidate digits
[^]	exclusion group of digits
[0-9]	selection range of candidate numerical digits
[a-d]	selection range of candidate letter digits
s	seize on string as only candidate if match to this point
e	specify ending termination digit which follows (usually * or #)
f	pause timeout causes failure instead of dial
p	set digit pause to number of seconds which follow (1-9) for current pattern
t	set digit timeout to default for current pattern
-	human readable spacing which is ignored
<space>	human readable spacing which is ignored

- **8-FXS Port Properties:** Each phone connected to an 8-FXS port has some properties that can be configured in this page. Click the arrow in the Device Name column to expand/collapse the node to show/hide the 8-FXS ports in this service. Configure the port property via clicking a cell in the port row and start typing to enter or select a value;

Table 25 8-FXS Port Properties (SIP-Server)

Field	Values	Description
Device Name	<ports>	Shows the selected 8-FXS ports in the voice service that must be configured.
Display Name (=future support)	<text>	Name that must be displayed on the telephone display on the receiver side (=callee) when a call is set up.

Field	Values	Description
Telephone Number	<number>	Telephone number that is assigned to the telephone connected to this 8-FXS port (=caller).
Auth User Name	<text>	User name assigned to this FXS port. This user name will be used in the SIP messages to authenticate this FXS port to the SIP Server when it requests some client authentication.
Auth Password	<text>	Password assigned to this FXS port. This password will be used in the SIP messages to authenticate this FXS port to the SIP Server when it requests some client authentication.
Audio Codec	G711a (=default) G711u, G729	See Table 23.
Use Hot Line Dialing	Yes/No	Hotline means that if you pick up a phone or initiate a call, an immediate direct connection will be set up with the configured 'Hot Line Dialing Number' without the need of manual dialing a number yourself. A client that has a hotline configured will not be able to call any other number besides the hot line number. No (=default): Hot Line dialing is disabled. Yes: Hot Line dialing is enabled.
Hot Line Dialing Number	<number>	Default = empty. Indicates the number that must be dialed when a client with 'Use Hot Line Dialing=Yes' picks up a phone to initiate a call.
Use Call Waiting (future use)	Yes/No	No (=default): The call waiting feature is disabled on this client. This client cannot accept a second call when a first call is already in progress. Yes: The call waiting feature is enabled on this client. This client can temporarily suspend or set on hold the first call to accept a second incoming call. This client can switch between the two calls.
SIP Server	<ip address>	Default = 0.0.0.0. IP address of the SIP Server.
SIP Server (R)	<ip address>	Default = 0.0.0.0. IP address of the Redundant SIP Server.
Registration Server (=future use)	<ip address>	Default = 0.0.0.0. IP address of the Registration Server. Current behavior: Registration will be done on the SIP Server.
Registration Server (R) (=future use)	<ip address>	Default = 0.0.0.0. IP address of the Redundant Registration Server. Current behavior: Registration will be done on the SIP Server.
Remote SIP Port	<number>	default = 5060. Indicates the remote SIP port that the SIP server is listening to for SIP traffic. The local SIP port on the PTN-8-FXS Interface Module is not configurable and is by default 5060.

Review: if ok, click Finish. The configuration load manager will be invoked, see §5.

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

8. HIPROVISION REDUNDANCY

8.1 General

Prerequisite: The HiProvision Redundancy feature needs one voucher or license for the entire Dragon PTN network. The generated license pack or file must be placed on both the HiProvision Servers. See §20 for more voucher and license info.

HiProvision Redundancy means that two HiProvision PCs are connected to the Dragon PTN network via a CSM with each CSM located in a different node. If one HiProvision PC fails the other PC will take over in order to maintain network connectivity.

One PC is the Master while the other is the Redundant PC. The Master PC is the PC on which all the redundancy configurations will be done (see further).

At startup, the Master is 'Started' and the Redundant PC is 'Standby'. The 'Started' PC will be able to do all the network configurations and monitoring. The 'Standby' PC is just waiting and will not be able to configure/monitor the network, all tiles (except database and servers tile) will be locked on the 'Standby' PC.

The 'Started' PC will push all its network modifications to the 'Standby' PC (=database replication, synchronization). In case of problems or a switchover request, the 'Standby' PC becomes 'Started' and the previous 'Started' one becomes 'Standby'. In some problem scenarios, both PCs can be 'Started' at the same time.

HiProvision Redundancy is non-revertive.

Both PCs communicate via heartbeat signals over DCN through the Dragon PTN network. Database replication and synchronization occurs via an Ethernet service through Dragon PTN or via an external LAN. Using an external LAN is better for redundancy reasons. An external LAN requires an extra NIC (=Network Interface Card) per PC. A basic HiProvision Redundancy set up can be found in the picture below:

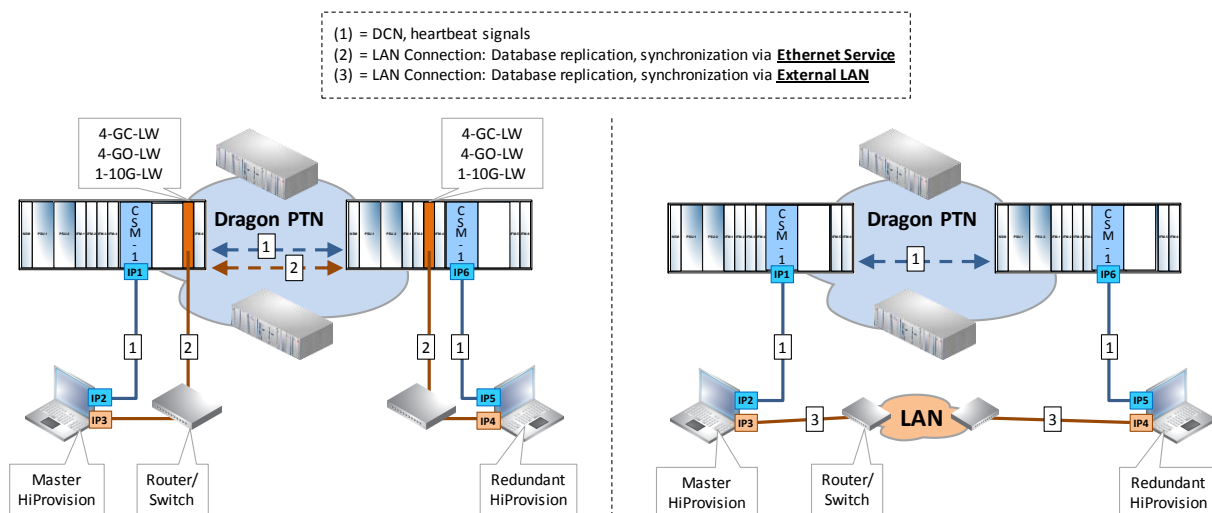


Figure 151 Basic HiProvision Redundancy: Via Ethernet Service/External LAN

8.2 Set up HiProvision Redundancy

Prerequisites:

- Make sure that both PCs are correctly connected to the Dragon PTN network via the CSMs with respect to the correct IP ranges;
- Both HiProvision PCs must have a full HiProvision Installation;

- Make sure that HiProvision Redundancy voucher or license is installed on both the servers, the entire license pack (or *.dat file) must be copied from the master server to the redundant server;

8.2.1 Actions on the Redundant HiProvision PC

On the Redundant HiProvision PC, only the HiProvision Agent must be started. All other configuration actions must be done on the Master HiProvision PC.

NOTE: Starting the HiProvision Agent is enough to make HiProvision Redundancy operational. In addition, If you want to look/manage the network via the HiProvision client of the Redundant HiProvision PC, the client has to be started manually.

8.2.2 Actions on the Master HiProvision PC

Follow the steps below to set up and start HiProvision Redundancy:

1. Click on the Dashboard → Servers Tile. Without a Redundant setup, only a Master Server PC will be visible:

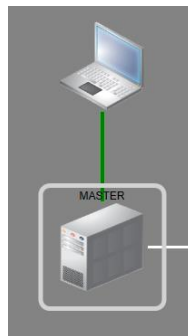



Figure 152 Master PC Only, No Redundancy

2. Start the servers via clicking the play button ;
3. Only one Discovery Entry Point must be created for a solution where both redundant PCs have only one cable connection to the Dragon PTN network. Make sure that both 'Mgt. IP Address' and 'Red. Mgt. IP Address are filled' out in the Discovery Entry Points, see figure below.

NOTE: Other HiProvision Redundancy use cases between the HiProvision PCs and the Dragon PTN network, and their corresponding Entry Points can be found in §9.

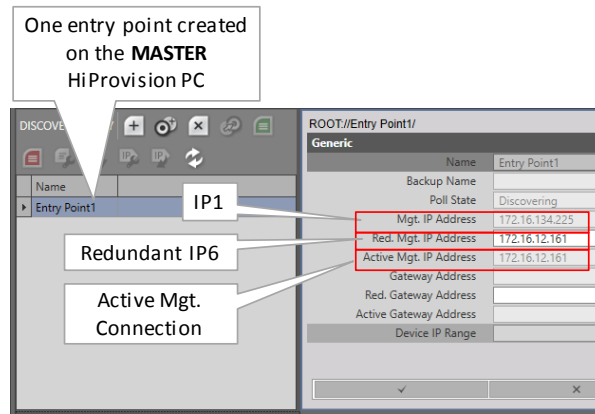




Figure 153 Discovery Entry Point: Redundant Management IP Address

NOTE: More info on Discovery Entry Points, see §2.6.2. More redundancy use cases with IP address examples can be found in §9;

- Click the add button  to create a HiProvision Redundancy setup. As a result, both a Master and Redundant Server will be visible. Just after creation or when Redundancy has been stopped later on via , the Master will be 'started' (=green) and the Redundant server will be 'unknown' (=red). See the global status on the left-hand side.

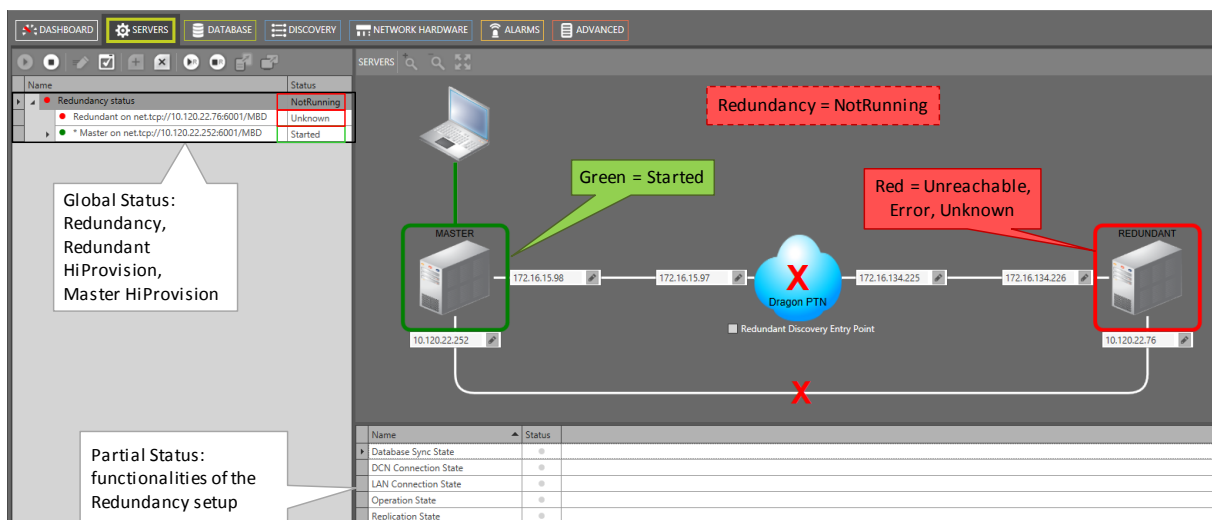



Figure 154 HiProvision Redundancy Setup: NotRunning

- In case of redundant Entry Points, click the 'Redundant Discovery Entry Point' checkbox first. Fill out the IP addresses by clicking the IP address field and pressing ENTER or clicking  in the IP address field.

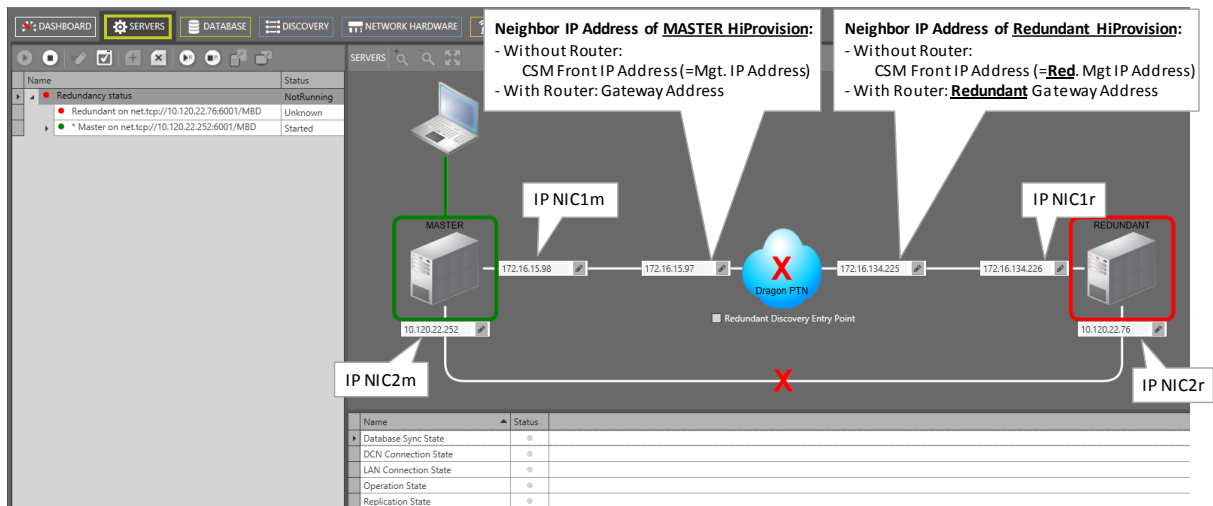


Figure 155 Fill Out IP Addresses

- At this moment the Redundancy status is 'NotRunning'. Make sure that the HiProvision agent is running on the Redundant PC. Start HiProvision Redundancy via clicking the redundancy play button . The Redundancy starts:

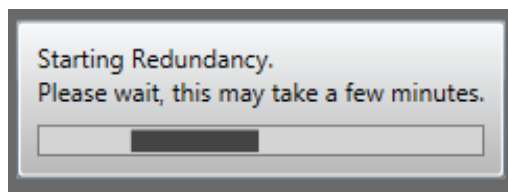


Figure 156 HiProvision Redundancy Starting

- After the Redundancy has been started and is up and running, it could look like in the figure below. If the Redundancy would not work, verify that some external LAN ports are not blocked by a possible firewall, see §38.5;

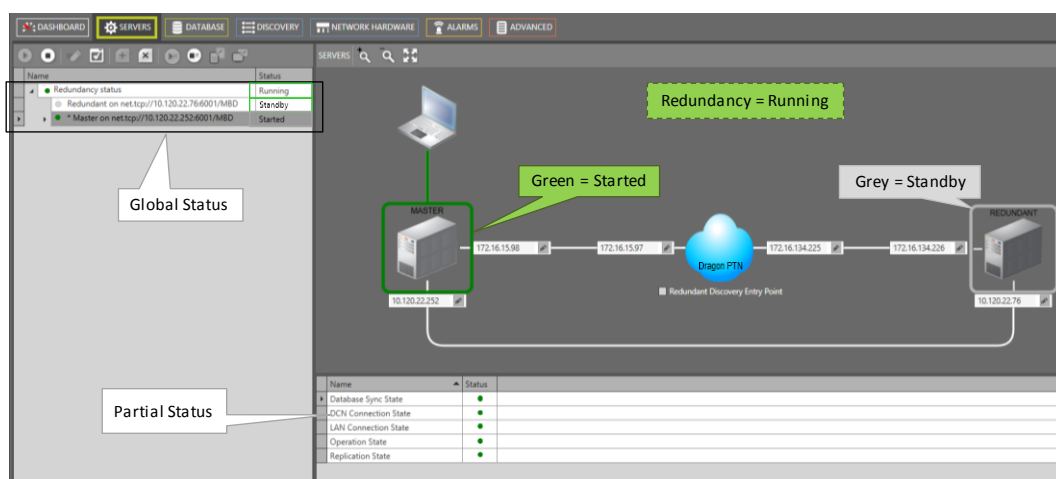






Figure 157 HiProvision Redundancy Setup: Running

Table 26 HiProvision Redundancy Status Info

Status	Description
Global Status	
Redundancy Status	<p>Running: The redundancy setup has been started via the play button  and is active now.</p> <p>NotRunning: The redundancy setup has been stopped via the play button  and is not active anymore.</p> <p>RedundancyError: Something is wrong with the Redundancy, check the Partial States (see further) to solve the problem;</p>
Master on net.tcp...	<p>Unknown: Only possible on the Redundant Server. It means that Redundant Server cannot communicate with the Master Server.</p> <p>Started: The Master server is the 'Started' one. HiProvision processes have been started on this server. It means that all the network configurations/monitoring must be done via this PC.</p> <p>Standby: The Master server is 'Standby'. It is ready to take over in case something goes wrong on the other side or a switchover is initiated via clicking ;</p>
Redundant on net.tcp..	<p>Unknown: Only possible on the Master Server. It means that the Master Server cannot communicate with the Redundant Server.</p> <p>Started: The Redundant server is the 'Started' one. HiProvision processes have been started on this server. It means that all the network configurations/monitoring must be done via this PC.</p> <p>Standby: The Redundant server is 'Standby'. It is ready to take over in case something goes wrong on the other side or a switchover is initiated via clicking ;</p>
Partial Status	
DCN Connection State	<p>Heartbeat signals are exchanged between the two servers over the DCN channel through the Dragon PTN network.</p> <p>Green/Red: This server can/cannot communicate with the other server via heartbeat signals.</p>
LAN Connection State	<p>Database replication and synchronization occurs via an external LAN network or via a programmed Ethernet service over the Dragon PTN network.</p> <p>Green/Red: This server can/cannot communicate with the other server via the external LAN path or via a configured Ethernet service in the Dragon PTN Network.</p>
Replication State	<p>Green: database replication between the two servers is OK.</p> <p>Red: database replication between the two fails or is not OK. This can be due to a failure in the external LAN path, configured Ethernet service or a replication failure on the MySQL Server.</p>
Database Sync State	<p>Green: databases on both servers are (or can be) perfectly synchronized</p> <p>Red: databases on both servers cannot be synchronized. This can be due to a failure in the external LAN path, configured Ethernet service or database mismatches due to manual database modifications on both sides. Manual modifications on both sides can be done if both servers become 'Started' during a DCN connection state failure. The user must indicate which of both databases the correct one is when this failure occurs.</p>
Operation State	<p>Green: The redundancy setup is up and running without errors.</p> <p>Red: Both servers are in the 'Started' state which is a failure situation. This is only possible when both servers cannot communicate via DCN and as a result, the server that was in 'Standby' will start itself as a precaution.</p>

8. The Dashboard Servers tile indicates whether the HiProvision Redundancy has been set up or not. A double gear on the Tile means that HiProvision Redundancy has been configured. A green color and 'started' means that the own server is running in case the Redundancy has been stopped or no redundancy or that the redundancy has been started and running without errors.

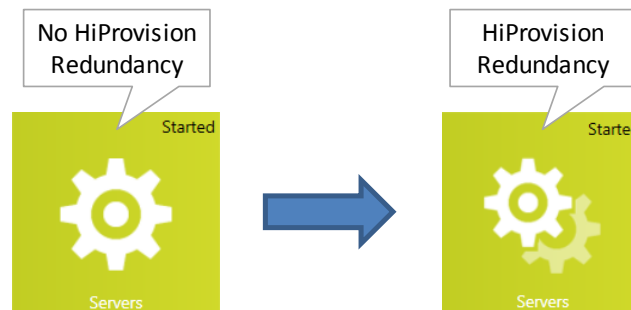



Figure 158 Servers Tile: HiProvision Redundancy

8.3 Stable State: Switchover from Started to Standby HiProvision PC

A manual switchover can be performed when HiProvision redundancy is up and running and everything is fine, no error situations active.

- ▶ can be initiated via clicking the server switchover button ;
- ▶ makes the 'Standby' PC the 'Started' one and vice versa;
 - ▶ Stops the server processes on the 'Started' PC. This PC turns into 'Standby' mode;
 - ▶ Starts the server processes on the 'Standby' PC. This PC turns into 'Started' mode;
- ▶ can only be performed if one PC is 'Started' and the other is 'Standby';
- ▶ can take a few minutes, the total switchover time depends on the database and network size;

does not cause network interruptions;

8.4 Unstable State: Error Situations

Some common situations are explained below provided that HiProvision Redundancy is up and running.

8.4.1 One or More Server Process Errors on the 'Started' PC

Prerequisites: DCN channel and LAN connection are fine.

If one or more processes on the 'Started' PC fail or don't start for some reason, the 'Started' PC will turn into a 'Failure' state. As a result, an automatic switchover occurs in which the 'Standby' PC becomes 'Started'.

8.4.2 DCN Path Break

Prerequisites: All server processes and LAN connection are fine.

A DCN path break can be the result of a cable break between HiProvision PC and the CSM or a path break somewhere in the Dragon PTN Network. As a result, no more heartbeat signals are possible between the 'Started' and 'Standby' server. Both servers become 'Started'.

The partial states 'DCN Connection state' turns red. If the LAN connection is configured via an Ethernet service, the partial states 'Replication state' and 'Database Sync' turn red as well.

The Redundancy status turns into 'Redundancy Error'. The databases between the two servers cannot be synchronized anymore.

When the DCN connection will be restored later on, it must be decided which of both servers must be the 'Started' one and which one 'Standby'.

8.4.3 LAN Connection Cable Break

Prerequisites: All server processes and DCN channel are fine.


The 'Started' server just keeps running and remains 'Started'. The 'Standby' server remains 'Standby'. The partial states 'LAN Connection state', 'Replication state' and 'Database Sync' turn red. The Redundancy status turns into 'Redundancy Error'. The databases between the two servers cannot be synchronized anymore.

When the LAN connection will be restored later on, the 'Standby' PC will synchronize its database with the one on the 'Started' PC.

8.5 Revertive/Non-revertive Behavior

HiProvision Redundancy is non-revertive: once a switchover of the HiProvision PC has occurred, the new 'Started' HiProvision PC stays 'Started' until a manual switchover or switchover caused by a cable break occurs again. No automatic switchback to the original HiProvision PC will occur when it is up and running again after a breakdown or a failure.

8.6 HiProvision Redundancy with Remote Client

If a remote client is used in combination with HiProvision Redundancy, it is possible to switchover the GUI view of the remote client from one server to the other via the GUI switchover button . See §17 for more information.

9. HIPROVISION CONNECTIVITY REDUNDANCY: USE CASES

9.1 General

In Dragon PTN, some redundancy solutions are available to provide an enhanced failure proof HiProvision connectivity to the Dragon PTN network. Without HiProvision connectivity, a Dragon PTN network cannot be monitored or configured/modified! Therefore some redundancy is strongly advised.

Depending on the needs, a combination of the solutions below can be implemented to tune or optimize your HiProvision connectivity:

- CSM redundancy (feature license required per node);
- HiProvision PC redundancy (feature license required);
- Management cable/entry point redundancy.

The paragraphs below show some use cases starting from no redundancy at all up to a higher level of redundancy combining one or more of these redundancy solutions.

NOTE: 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 'standby'.

9.2 Use Case 0: No Redundancy at All

The HiProvision PC is directly connected via one management cable to a node with only one CSM.

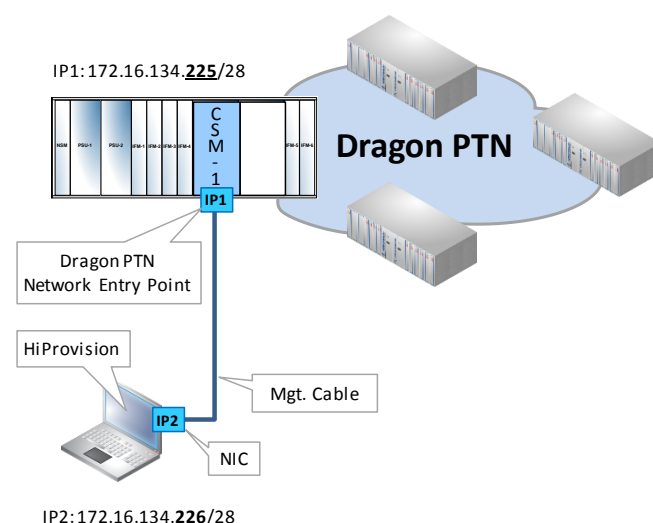
Configuration:

One IP address on the HiProvision NIC, see §2.2.3;

- One entry point in HiProvision, see §2.6.2;

HiProvision connectivity is lost when:

- The HiProvision PC, management cable or the CSM breaks. When the CSM breaks, the node goes out of service as well.



Redundant:

- Redundant CSM : No
- Redundant Management Cable : No
- Redundant HiProvision : No
- Redundant Discovery Entry Point : No

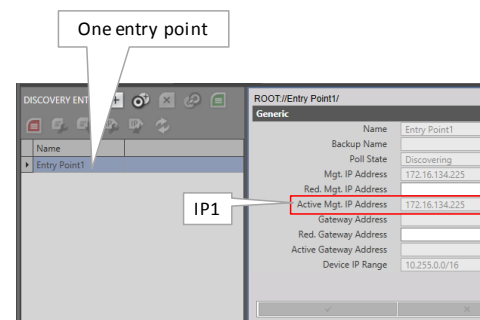
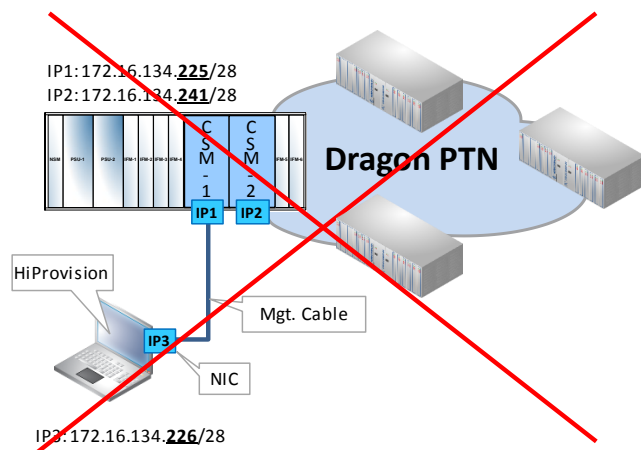


Figure 159 Use Case 0: No Redundancy at All

9.3 Use Case 1: CSM Redundancy Only

CAUTION: The case below is NOT supported. When using CSM Redundancy, HiProvision must always be connected to both CSMs (=each CSM having its own management cable), either directly or via a router/switch, see Use Case 2.



Redundant:

- Redundant CSM : Yes
- Redundant Management Cable : No
- Redundant HiProvision : No
- Redundant Discovery Entry Point : No

Figure 160 Use Case 1: CSM Redundancy Only

9.4 Use Case 2: One HiProvision PC with Direct Dual Entry Point in One Node

The HiProvision PC with 2 NICs is directly connected via two management cables to a node with redundant CSMs. If the active CSM fails, the standby CSM takes over to keep the node alive.

Configuration:

One IP address on both NICs in the HiProvision PC, see §2.2.3;

► Two redundant entry points in HiProvision, see §2.6.2 and §2.6.5;

HiProvision connectivity is protected against:

► one CSM failure or a single cable break.

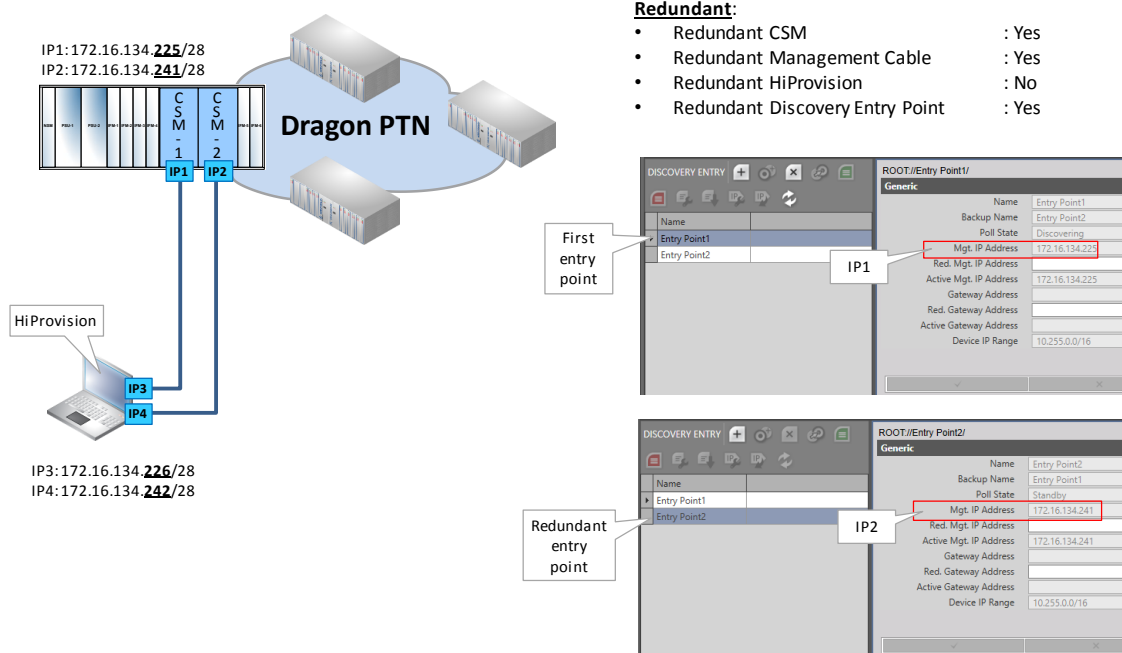


Figure 161 Use Case 2: One HiProvision PC with Direct Dual Entry Point in One Node

9.5 Use Case 3: One HiProvision PC with Direct Dual Entry Point in Two Nodes

The HiProvision PC with 2 NICs, is directly connected via two management cables to two nodes with one CSM in each node. If the first node fails (first entry point), the network can still be configured/monitored via the second entry point.

Configuration:

► One IP address on both NICs in the HiProvision PC, see §2.2.3;

Two redundant entry points in HiProvision, see §2.6.2 and §2.6.5;

HiProvision connectivity is protected against:

one CSM failure or a single cable break.

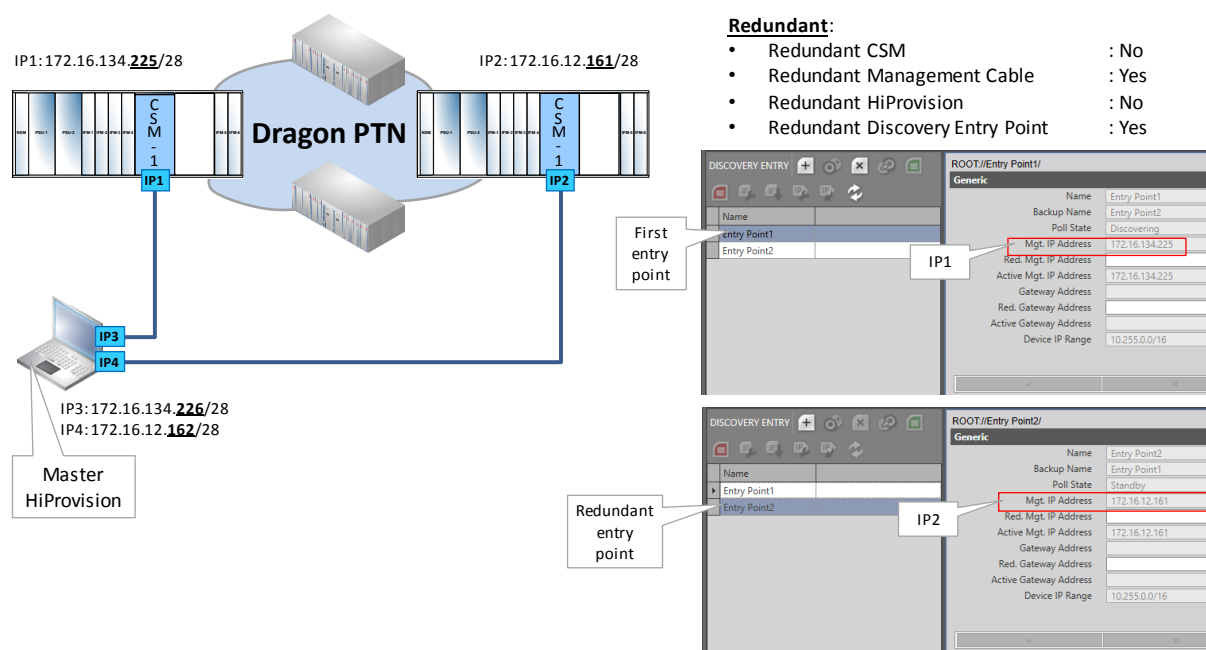


Figure 162 Use Case 3: One HiProvision PC with Direct Dual Entry Point in Two Nodes

9.6 Use Case 4: One HiProvision PC with Dual Entry Point via Switch

The HiProvision PC with 1 NIC, is directly connected via one management cable to a switch. The switch has a double connection to a node with redundant CSMs. If the active CSM fails, the redundant CSM takes over to keep the node alive.

Configuration:

► Two IP addresses on one NIC in the HiProvision PC, see §2.2.3 and §2.2.3b;

Two redundant entry points in HiProvision, see §2.6.2 and §2.6.5;

HiProvision connectivity is protected against:

one CSM failure or single cable break between switch and node.

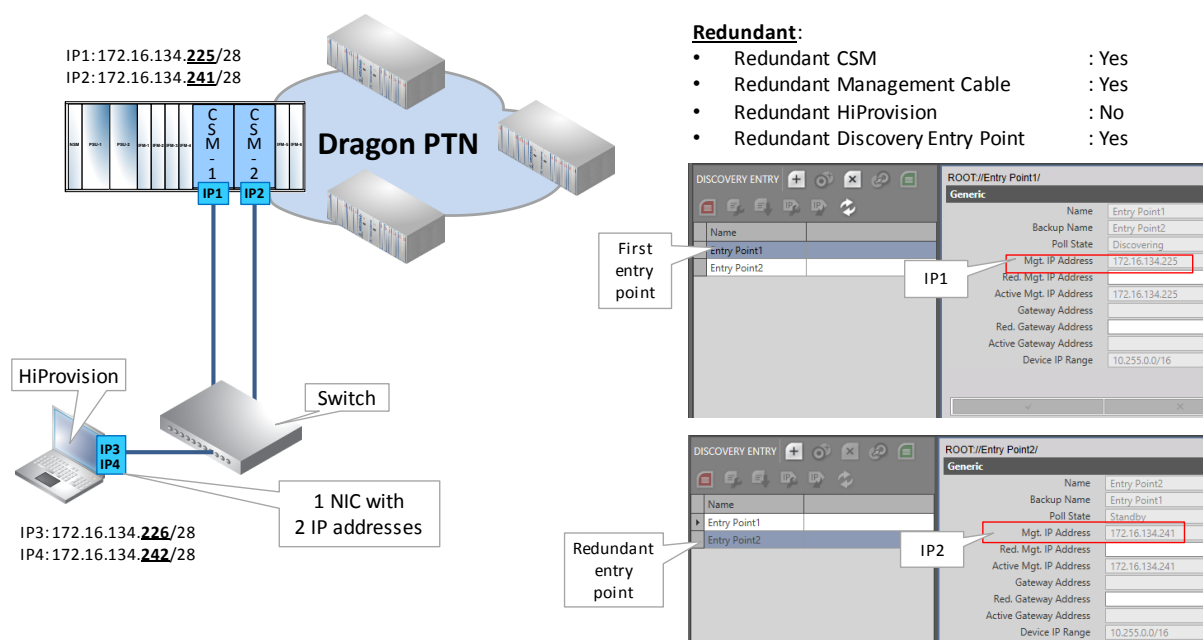


Figure 163 Use Case 4: One HiProvision PC with Dual Entry Point via Switch

9.7 Use Case 5: Redundant HiProvision PCs with Single Entry Point

Two redundant HiProvision PCs, each having 2 NICs, are directly connected via one management cable to a node with only one CSM. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

► One IP address on both NICs on both HiProvision PCs, see §2.2.3;

One entry point on the MASTER HiProvision PC, see §2.6.2;

HiProvision connectivity is protected against:

A HiProvision PC break, a connected node breakdown, a CSM failure or a cable break. The node of a broken CSM goes down but connectivity remains. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

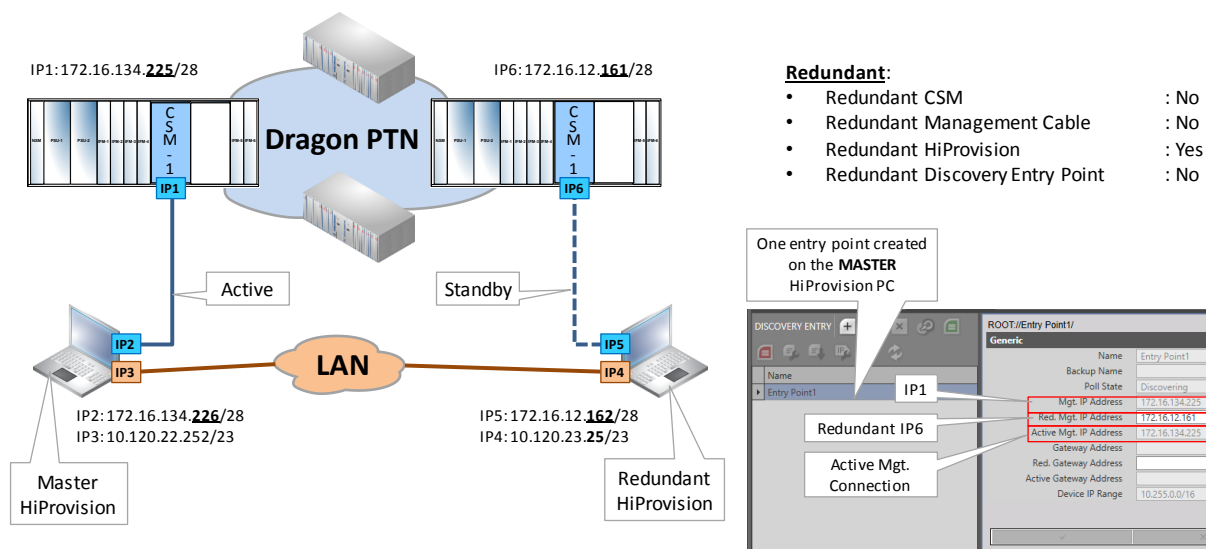


Figure 164 Use Case 5: Redundant HiProvision PCs with Single Entry Point

9.8 Use Case 6: Redundant HiProvision PCs with Dual Entry Point via Switch

Two redundant HiProvision PCs, each having 2 NICs are each directly connected via one management cable to a dedicated switch. Each switch has a double connection to a node with redundant CSMs. If an active CSM fails, the redundant CSM takes over to keep the connected node alive. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

► Two IP addresses on one NIC in each HiProvision PC, see §2.2.3 and §2.2.3b;

Two redundant entry points on the MASTER HiProvision PC, see §2.6.2 and §2.6.5;

HiProvision connectivity is protected against:

a HiProvision PC break, a connected node breakdown, a CSM failure or cable break somewhere between HiProvision PC and node. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

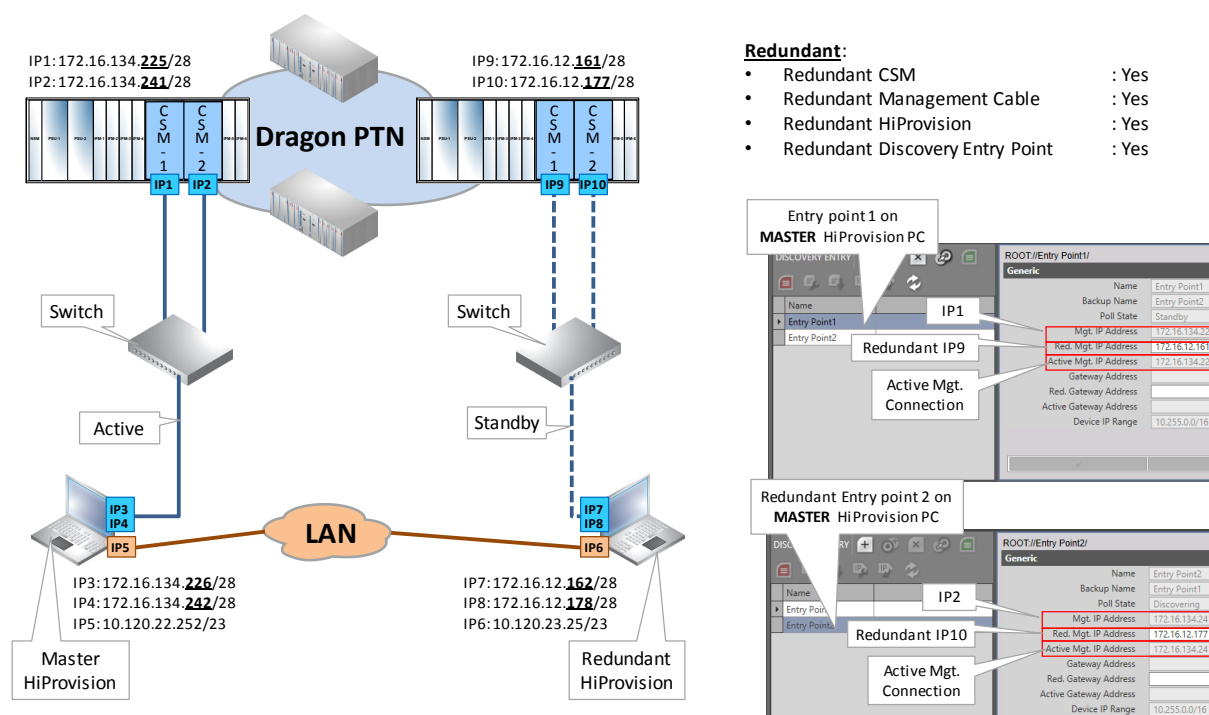


Figure 165 Use Case 6: Redundant HiProvision PCs with Dual Entry Point via Switch

9.9 Use Case 7: Redundant HiProvision PCs with Direct Dual Entry Point

Two redundant HiProvision PCs, each having 3 NICs are each directly connected via two management cables to a node with redundant CSMs. If an active CSM fails, the redundant CSM takes over to keep the connected node alive. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

► One IP address on three NICs in each HiProvision PC, see §2.2.3;

Two redundant entry points on the MASTER HiProvision PC, see §2.6.2 and §2.6.5;

HiProvision connectivity is protected against:

a HiProvision PC break, a connected node breakdown, a CSM failure or a single cable break somewhere between one HiProvision PC and the connected node. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

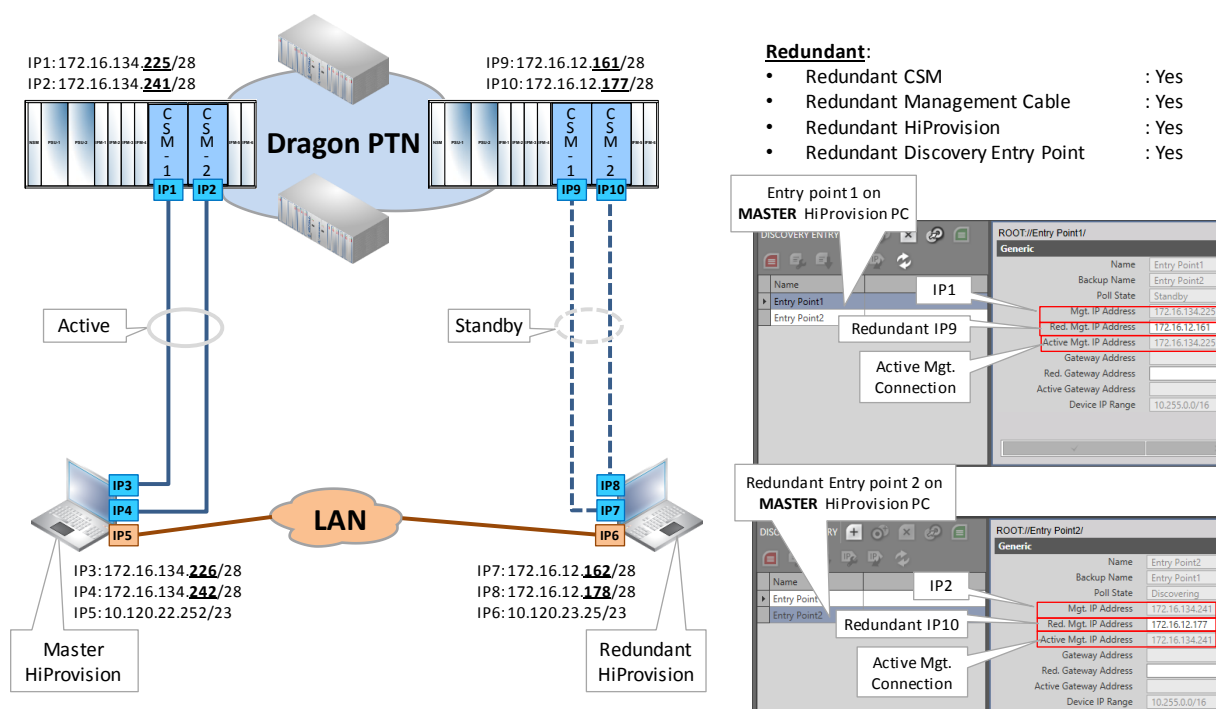


Figure 166 Use Case 7: Redundant HiProvision PCs with Direct Dual Entry Point

9.10 Use Case 8: One HiProvision PC with Dual Entry Point via Router

The HiProvision PC with 1 NIC, is directly connected via one management cable to a router. The router has a double connection to a node with redundant CSMs. If the active CSM fails, the redundant CSM takes over to keep the node alive.

Configuration:

One IP address on one NIC in the HiProvision PC, see §2.2.3;
Two redundant 'routed' entry points in HiProvision, see §2.6.2;
Gateway configuration in the both the Redundant Entry Points;
Gateway configuration in the CSM front IP Addresses;
Static Routes on the router, see an example in §2.6.6e;

HiProvision connectivity is protected against:

one CSM failure or single cable break between router and node.

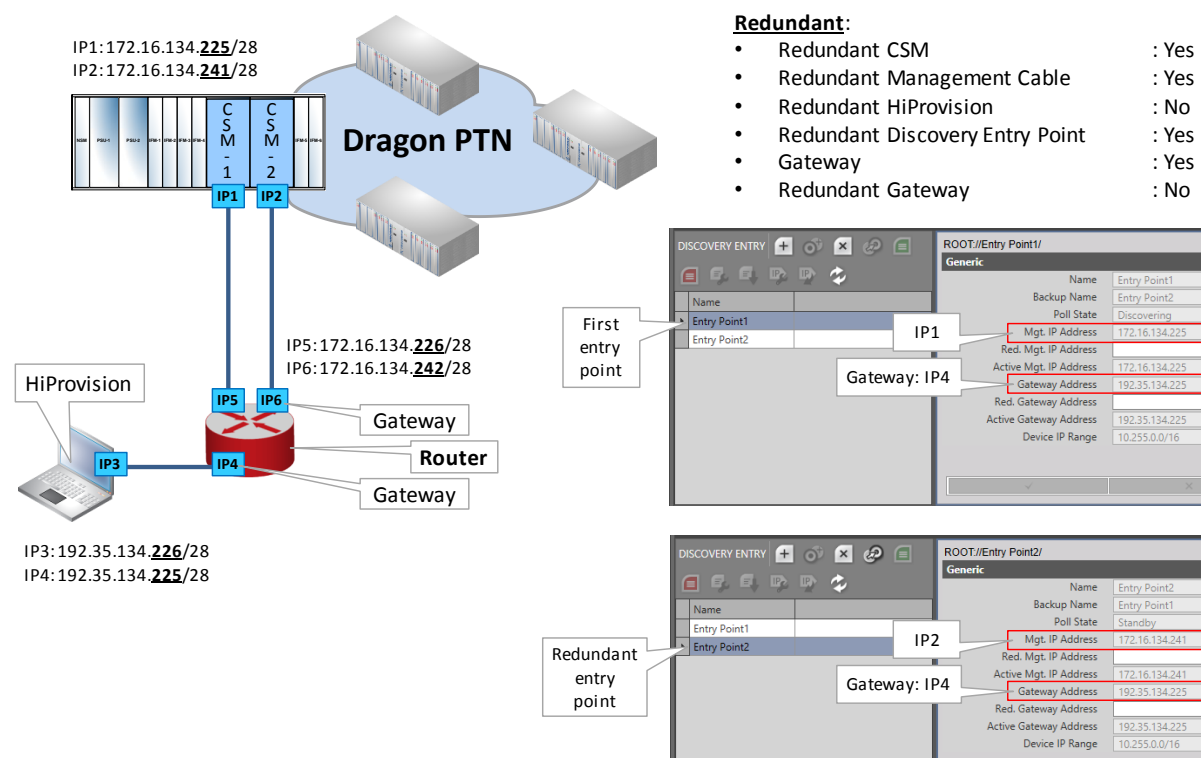


Figure 167 Use Case 8: One HiProvision PC with Dual Entry Point via Router

9.11 (Future) Use Case 9: Redundant HiProvision PCs with Dual Entry Point via Router

Two redundant HiProvision PCs, each having 2 NICs are each directly connected via one management cable to a router. Each router has a double connection to a node with redundant CSMs. If an active CSM fails, the redundant CSM takes over to keep the connected node alive. The redundant HiProvision PCs are synchronized over an external LAN.

Configuration:

One IP address on one NIC in each HiProvision PC, see §2.2.3;
Two redundant 'routed' entry points in HiProvision, see §2.6.2;
Gateway configuration in the both the Redundant Entry Points;
Gateway configuration in the CSM front IP Addresses;
Static Routes on the routers, see an example in §2.6.6e;

HiProvision connectivity is protected against:

A HiProvision PC break, a connected node breakdown, a CSM failure or cable break somewhere between HiProvision PC and node. A cable break between the two HiProvision PCs remains HiProvision connectivity but eliminates HiProvision Redundancy.

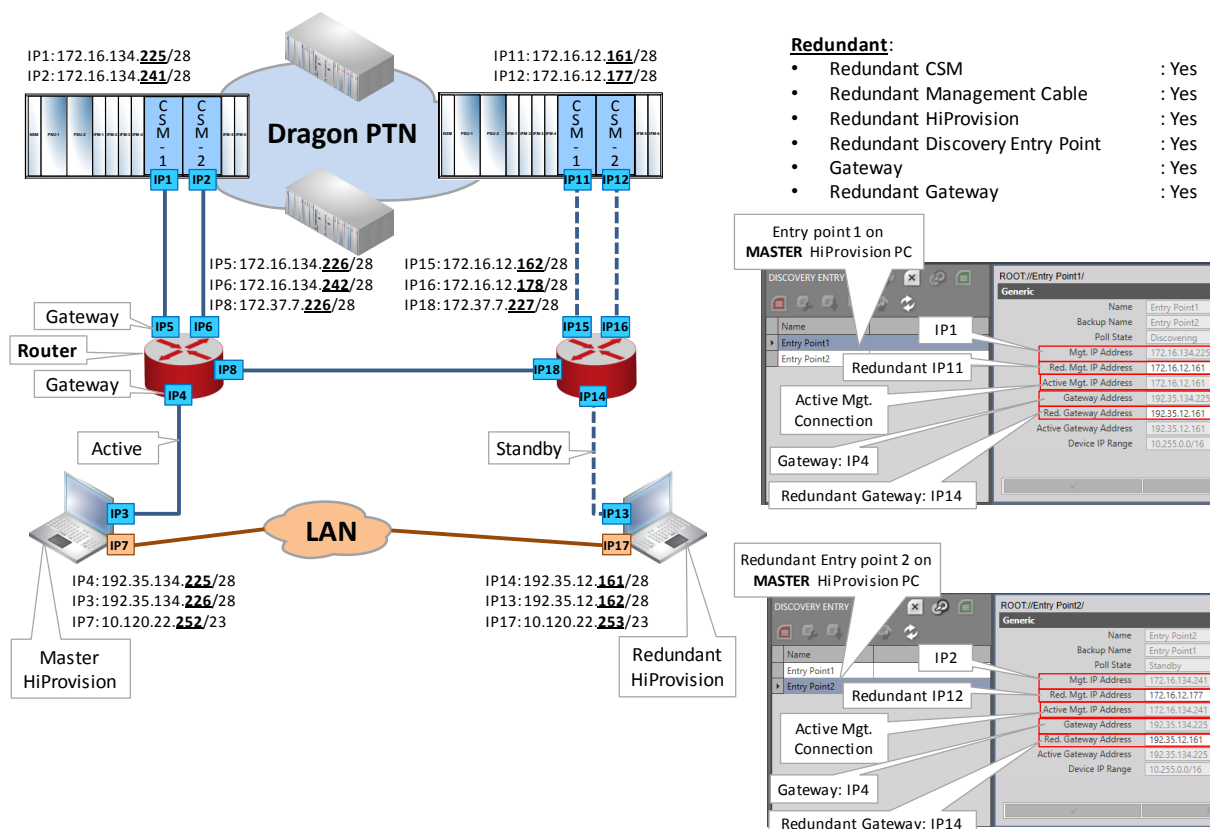


Figure 168 Use Case 9: Redundant HiProvision PCs / Dual Entry Point / Redundant Router

10. EXTRAS

10.1 Connect HiProvision PC to another Node

By changing the HiProvision PC connection from one node to another node, the discovery entry point (see §2.6.2) changes. Follow the steps below to make a successful connection change:

Before changing the HiProvision connection, go in HiProvision to Discovery → Discovery Entry;

Delete the Discovery Entry by selecting it in the list and clicking ;

Remove the HiProvision cable from one node;

Configure a new HiProvision IP address according to §2.2.3;

Plug in the HiProvision cable into the other node;

► Discover the network topology again as described in, see §2.6.2;

10.2 Clear Node or Network

Prerequisite: HiProvision must be online or connected to the network;

10.2.1 General

The clear command should be used when:

an erroneous CSM in that same node, with a correct configuration, is reused, see Ref.[3] in Table 1;

HiProvision cannot load the node configuration into the network, e.g. due to timestamp mismatches,;

you are not sure of the loaded configuration within a node;

Clearing a node:

erases all data (services and configured Interface Modules) in the CSM of that node;



only affects data in the real network, the data in the HiProvision database is not touched;

does NOT erase the discovery or DCN configuration, the communication with the node or management path stays alive;

Result: All the Interface Modules in that node stay in the configured state, alarms will be raised in HiProvision with 'type mismatch' because the hardware is different from the database configuration.



10.2.2 Clear one Node

CAUTION: The entire node goes out of service after clearing it!

1. Go to Dashboard → Network Hardware;
2. Select the node in the devices list;
3. Click  →  Clear. This node will go out of service after confirmation!

10.2.3 Clear the Entire Network

CAUTION: THE ENTIRE NETWORK GOES OUT OF SERVICE AFTER CLEARING IT!

1. Go to Dashboard → Network Hardware;
2. Select all the nodes in the devices list (via CTRL and/or SHIFT keys);
3. Click  →  Clear. THE ENTIRE NETWORK GOES OUT OF SERVICE after confirmation!

10.3 Reset Node or Network

Prerequisite: HiProvision must be online or connected to the network;

10.3.1 General

The Reset command should be used when:



you want to set the node back to its factory default settings;
a new CSM module is implemented, unless the Micro SD memory card from an erroneous CSM in that same node, with a correct configuration is reused, see Ref.[3] in Table 1.
A new node is added to the network;

Resetting a node:

sets the node back to its default settings;
erases the discovery or DCN configuration, the communication with the node or management path to the node will be lost;
only affects data in the real network, the data in the HiProvision database is not touched;

10.3.2 Reset one Node



CAUTION: The entire node goes out of service after resetting it!

1. Go to Dashboard → Network Hardware;
2. Select the node in the devices list;
3. Click  →  Reset. This node will go out of service!

NOTE: Also possible via pushing the hidden reset button on the CSM for at least 7 seconds (see §2.1);

10.3.3 Reset the Entire Network

CAUTION: THE ENTIRE NETWORK GOES OUT OF SERVICE AFTER RESETTING IT!

1. Go to Dashboard → Network Hardware;
2. Select all the nodes in the devices list (via CTRL and/or SHIFT keys);
3. Click  →  Reset. THE ENTIRE NETWORK GOES OUT OF SERVICE!

10.4 Save User HiProvision Settings

When a user logs off/closes HiProvision/stops the servers, he will have the option to save its personal HiProvision settings as shown in the box below:

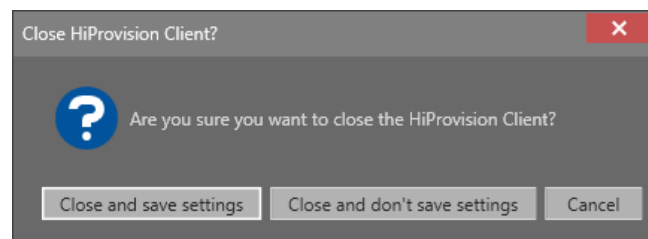


Figure 169 Save HiProvision Settings

Which HiProvision settings?

Table layouts (shown fields, order of fields etc...), see §26.1;

Opened tabs;

Large Network Monitor tab state information, see §26.2.4;

When the user logs on again and ...

- ▶ ... settings were saved: HiProvision starts up and automatically opens the last saved tabs, uses the last saved table layouts and Large Network settings;

... settings were never saved: HiProvision starts up with the default setup.

To clear all the saved settings:

See Ref.[15] in Table 1;

10.5 2-OLS Settings

10.5.1 Verify PTN-2-OLS Interface Module Clock Settings

The ports of the PTN-2-OLS Interface Module have by default the settings below which are OK if the Interface Module can slave to the external E1 network.

Within one PTN-2-OLS Interface Module, the E1 ports will slave to the external network e.g. SDH (=Rx Clock). The optical serial ports slave to their associated E1 ports (=Through Timing). Port 1 slaves to Port3 and Port2 slaves to Port4;

Port Settings: Clock Source:

- ▶ Optical Serial Port1: Through Timing;
- ▶ E1 Port3: Rx Clock;
- ▶ Optical Serial Port2: Through Timing;
- ▶ E1 Port4: Rx Clock;

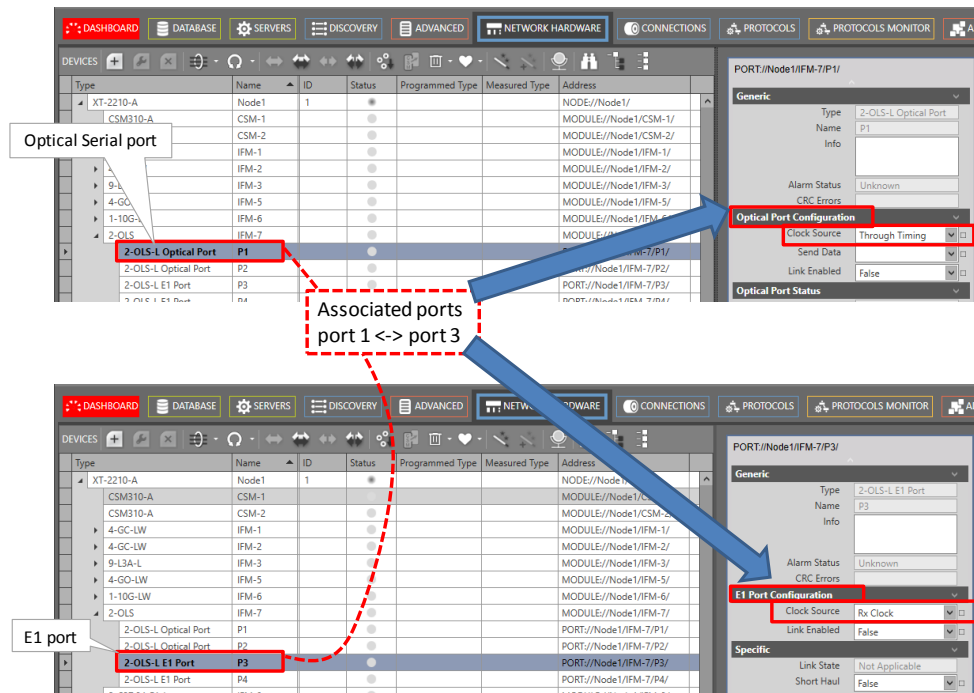


Figure 170 PTN-2-OLS Interface Module: Clock Source Settings

10.5.2 Forced Power Mode

The powering of the PTN-2-OLS Interface Module can be configured by the 'Forced Power Mode' parameter on the PTN-2-OLS Interface Module in HiProvision. The setting of this parameter determines whether a CSM is required in the node for powering the PTN-2-OLS Interface Module.

The parameter can be found in the Network Hardware tile → PTN-2-OLS Interface Module → Specific → Forced Power Mode.

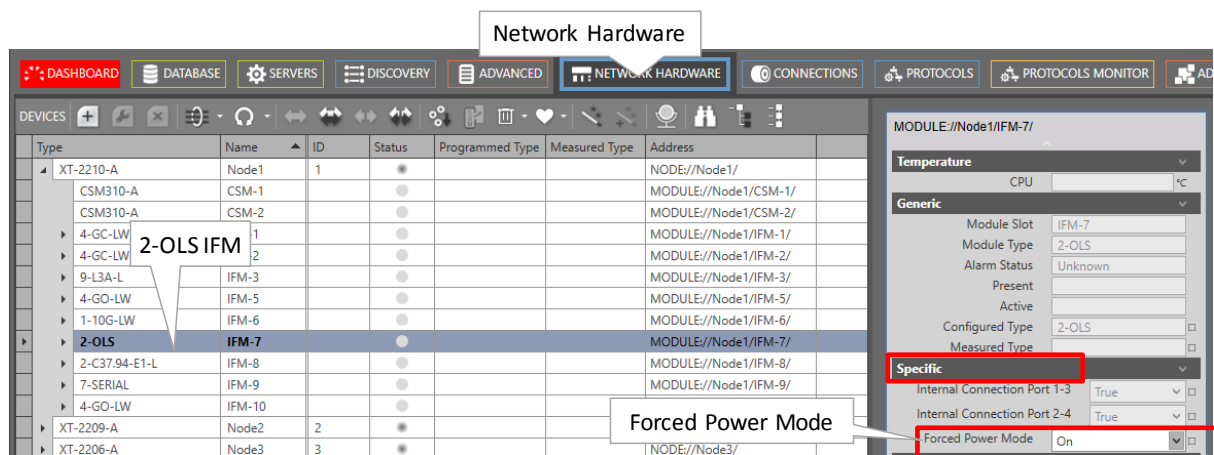


Figure 171 PTN-2-OLS Interface Module: Forced Power Mode

- ▶ **Forced Power Mode:**
 - ▶ **On (=default):** Once the PTN-2-OLS Interface Module has been configured by the CSM, the CSM can be removed from the node if desired. After removing the CSM, the PTN-2-OLS Interface Module remains powered and a configured Converter/Loopback

Type1 service (=Optical Low Speed Serial service, see §2.13.2) on this Interface Module remains operational;



- ▶ Off: the PTN-2-OLS Interface Module always needs an operational CSM in the node for powering and for normal operation. After removing the CSM from the node, the PTN-2-OLS Interface Module will be powered off automatically and goes out of service.
- ▶ Best Practice:
 - ▶ If a Converter/Loopback Type1 service is configured on the PTN-2-OLS Interface Module and you want to remove the CSM from the node later on, set Forced Power Mode = 'On'. In any other case, set it to 'Off'.

10.6 Tunnel Actions: Swap Working Path ↔ Protection Path

10.6.1 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 ;

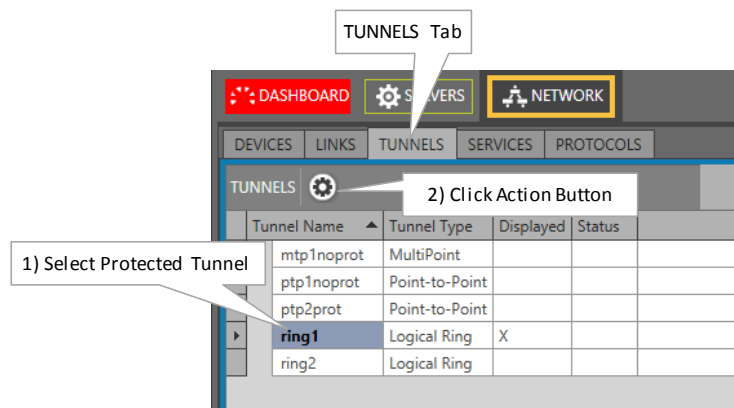


Figure 172 Protected Tunnel/Actions

4. The 'Action on Tunnel' window shows up and depends on the selected tunnel type:
 - ▶ Point-to-Point/Multipoint Tunnels: see §10.6.2;
 - ▶ Ring/Subring Tunnels: see §10.6.3;

10.6.2 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.

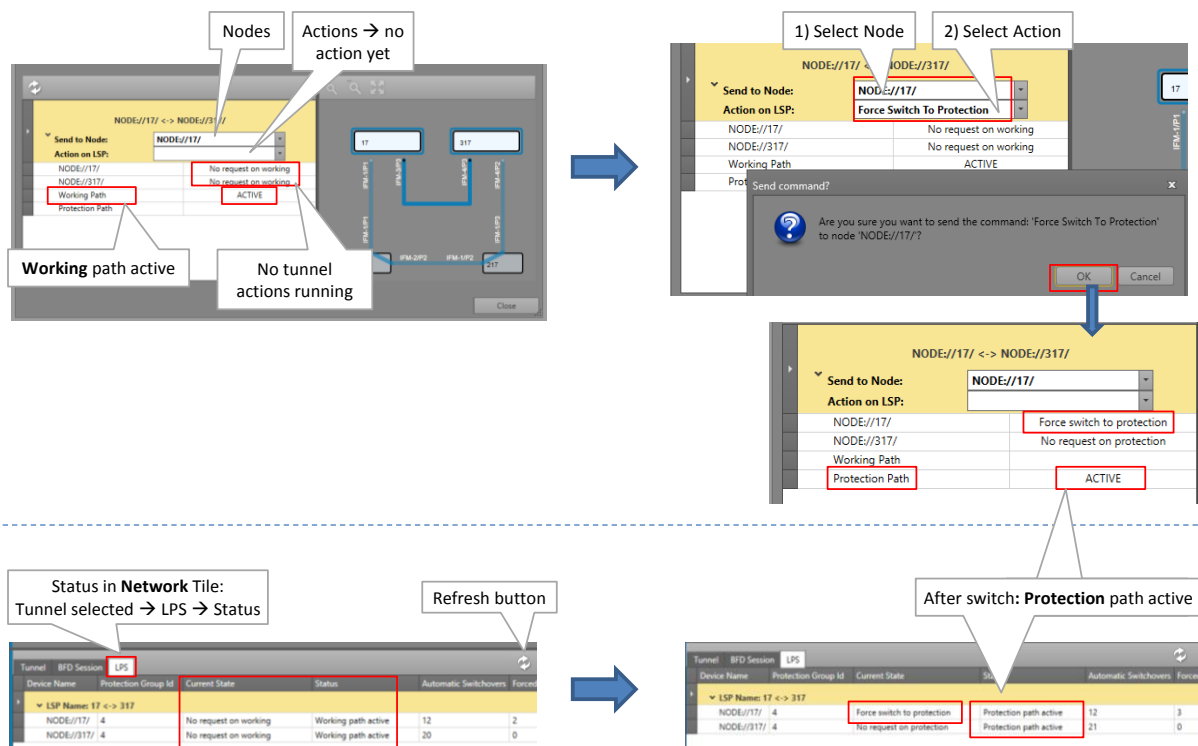


Figure 173 Point-to-Point/Multipoint Action on Tunnel Window

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 27 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 (e.g. LPS tab (=Linear Protection Switching)). Click the Refresh button for faster feedback. Also have a look at §4.6.5.
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!

10.6.3 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.

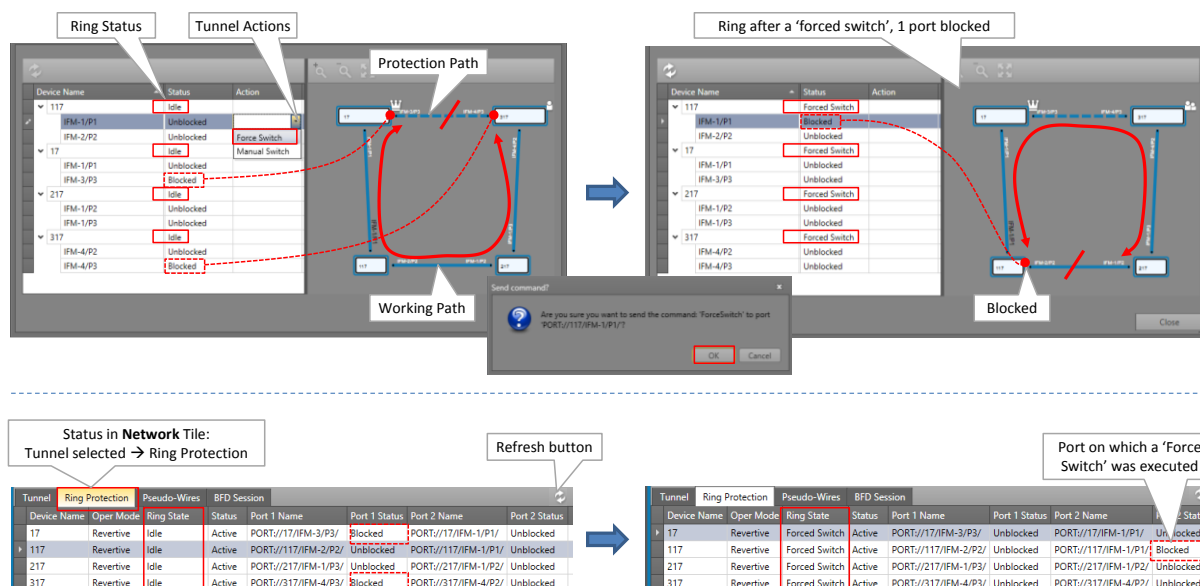




Figure 174 Ring/SubRing Action on Tunnel Window

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 27 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 , e.g. Ring Protection tab. Click the Refresh button for faster feedback. Also have a look at §4.6.5.
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.

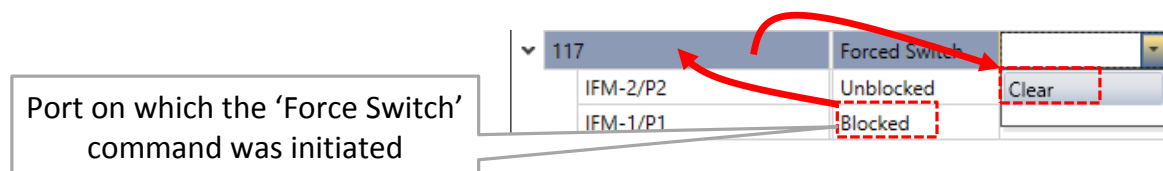


Figure 175 Clear Command in the Node Action List

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

10.6.4 Tunnel Action Commands

Table 27 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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	<ul style="list-style-type: none"> - 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.

10.7 Hardware Edition of Dragon PTN Modules

The hardware edition of the Dragon PTN modules has been factory set and cannot be changed. It can be read out via the Dashboard → Software tile → Hardware Edition, see figure below:

Display Name	Module Type	Compatible	Active Version	Accept Time (min)	Upgrading To	Upgrade Status	Upgrade Progress (%)	Backup Version	Hardware Edition	Boot Loader Version	Load Name	Power File Version	PLD Version	Measured Devices
MODULE/J/CSM-1/	CSM		100.9.255.2		-	No Upgrade Planned		4.2.51	5	1.0.7	CSM310-A_Q500	v0.5	15	
MODULE/J/10PH-1/	4-GC-LW		100.9.255		-	No Upgrade Planned		6.4.3	7	1.0.7	4-GC-LW_Q203	v6.2	-	
MODULE/J/10PH-2/	16-EL-L		100.9.255		-	No Upgrade Planned		100.9.255	4	1.0.7	16-EL-L_Q215	v2.0	-	
MODULE/J/10PH-3/									0				-	

Figure 176 Hardware Edition of Dragon PTN Modules

10.8 Improve Performance Between HiProvision Server and External Devices: ARP Reduction

Reduce the number of ARP (=Address Resolution Protocol) messages for better performance between the HiProvision server and the external devices (Hirschmann, ...). This can be done

by setting following parameters in the 'Hirschmann, ...' management NIC in the HiProvision PC:

the 'Base reachable timer' = 300000 ms (=5min);

► the 'Retransmittime' = in the range of [3000 ms... 10000 ms].

This can be done via opening the command prompt as administrator and enter the command below (fill out the correct <interface>):

netsh interface ipv4 set interface <interface> basereachable=300000;

► netsh interface ipv4 set interface <interface> retransmittime=<wanted time in ms>.

NOTE: To run as administrator, right-click the CMD(.exe) icon and select 'Run as Administrator'.

11. CSM REDUNDANCY

Prerequisite: one CSM Redundancy voucher (see §20.2) 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 Table 1 Ref. [3] and in the redundancy cases in §9;

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;

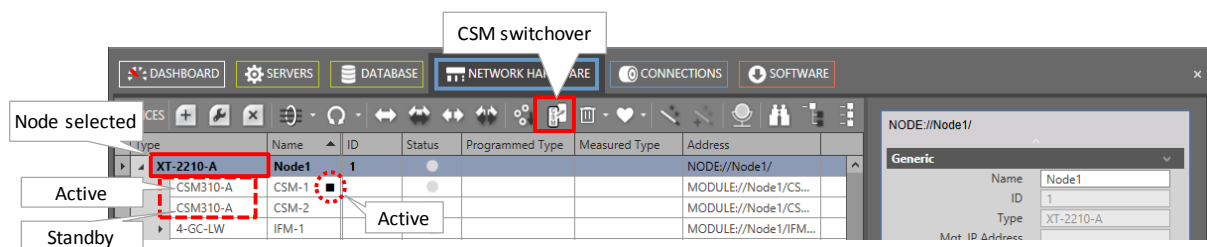


Figure 177 Node with 2 CSMs, CSM Switchover Button

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:

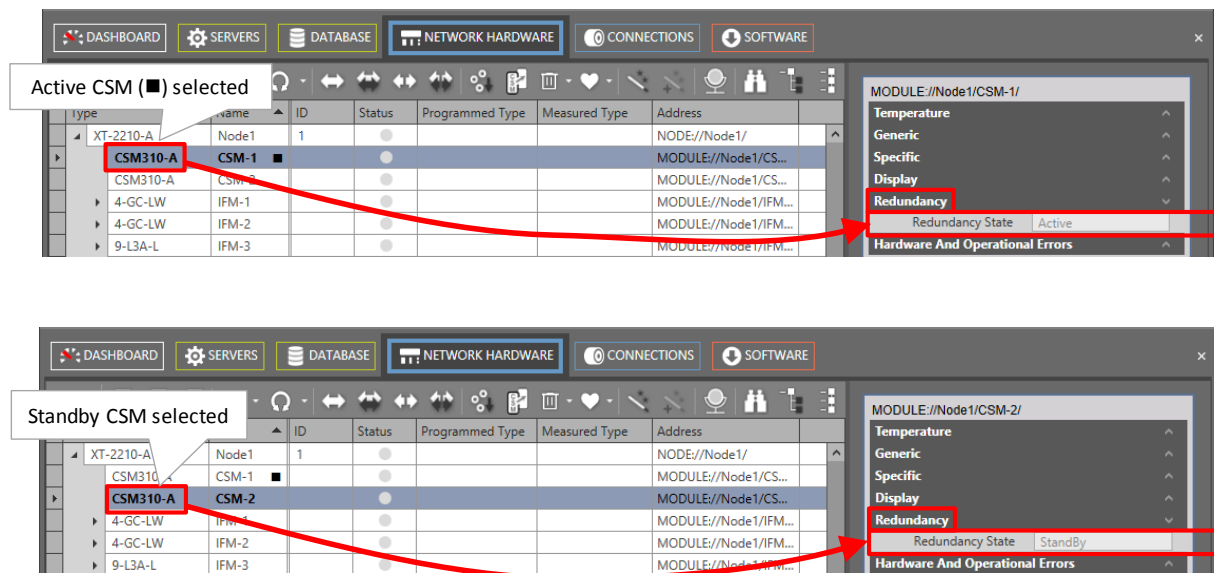



Figure 178 CSM Redundancy Status


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. [3];
7. CSM Redundancy is non-revertive.

12. LOAD SOFTWARE/FIRMWARE INTO THE NETWORK

12.1 General

Via HiProvision, it is possible to upgrade or downgrade software/firmware at once on multiple modules in the live network. The upgrade/downgrade process can be monitored by a progress bar per module.

It is also possible to list all the active and backup firmware versions on all the modules in the network. Furthermore, validation on this firmware version list can be done to make sure that all the same module types have the same firmware version. An alarm can be raised when firmware inconsistencies or incompatibilities occur.

CAUTION: To improve Dragon PTN security, as of Dragon PTN Release 3.1, only signed firmware () can be loaded into the network. Signed firmware is firmware that has been factory encrypted with a special signature or certificate.

Basically, following major steps are required in the entire process in HiProvision:

- ▶ Upgrade (wizard);
- ▶ Commit (wizard);
- ▶ Accept (wizard);

Reload network configuration into the node after a CSM firmware update;


The general principle is as follows:

- ▶ All available firmware images are stored as an individual zip file in the folder 'C:\FtpRoot\Firmware'. An FTP server, running on the HiProvision PC, uses this folder as a source folder to transfer zip files to the node.

CAUTION: Make sure that a firewall on the HiProvision PC is totally switched off otherwise the FTP cannot send the software to the nodes!

- ▶ HiProvision can instruct the modules to fetch a new firmware image;
- ▶ Fetched firmware images will overwrite the current standby or backup firmware on the module. When the fetch is complete, a module will wait for a commit command from HiProvision before it will switch to its new firmware image;
- ▶ After receiving the commit command, the module will reboot with its new image. The module will wait for an additional accept command from HiProvision. When the accept command is not sent within 20 minutes, the module will automatically reboot and switch back to its previous image.

For an overview or general example, see the example below:

- ▶ Up till now, a module has two firmware versions onboard with v1.1.6 the active version (=A) and v1.1.5 the backup version (=B);
- ▶ Upgrade: The operator wants to upgrade the module to signed firmware version v1.1.7. Via the upgrade wizard, the desired firmware version must be selected.
- ▶ Upgrade: Only if the firmware is signed (), the upgrade wizard will overwrite the backup version v1.1.5 in the module with the new version v1.1.7.
- ▶ Commit: Next, this new version must be committed via the commit wizard. It means that the module will reboot with the new version as the active version for the chosen module. The previous active version will now become the backup version.
- ▶ Next, if the new version is accepted via the accept wizard within 20 minutes, the new version stays the active version. If it is not accepted within 20 minutes, the module reboots automatically and falls back to the previous active version v1.1.6 for this module;

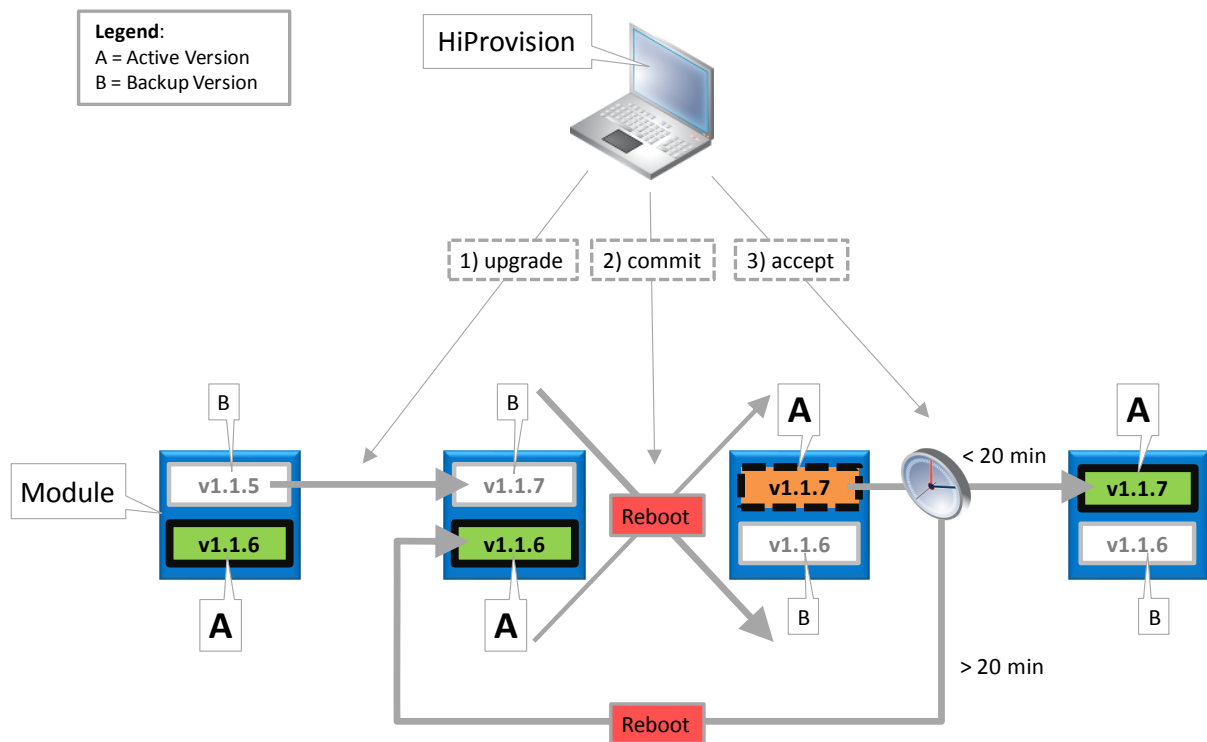


Figure 179 Firmware Upgrade Example: Upgrade to v1.1.7

12.2 Firmware Upgrade/Commit/Accept and Other

The firmware tools can be found via clicking the tile Dashboard → Tools → Software Tile. The screenshot below pops up. In the figure below, the most important buttons are indicated. The entire top menu and buttons is explained in the table below.

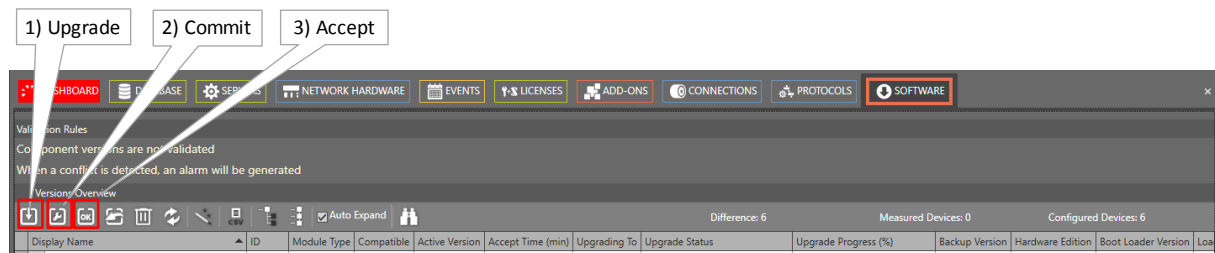









Figure 180 Software/Firmware Action Buttons

Table 28 Software/Firmware Buttons

Item	Short Description
	Upgrade: Starts a wizard to upgrade modules to a selected firmware image.
	Commit: Commits the pending upgrades, modules or nodes will swap to another image and will reboot.
	Accept: Accepts the committed upgrades, if not accepted in time, modules will switch back to their previous version.
	Reverts to the backup version. Clicking this button opens a wizard to let modules and/or nodes revert to their backup version. Selected modules/nodes in this wizard will reboot and start up with their backup version.

Item	Short Description
	Resets the upgrade status to 'No Upgrade Planned'.
	Refreshes all data.
	Starts a wizard to set the validation rules.
	Exports to a CSV file.
	Expands/Collapses all entries in the table.
	Checked/Unchecked: Auto expands/collapses new discovered devices in the table list.
	Search functionality to sort/group network elements in a better way. When using the search, the network elements are by default grouped by Module Type. In this way, you get a better overview to see if all the modules of a same type (e.g. CSM) have the same firmware version.
Device Count	<p>Difference: Indicates the count difference between measured devices in the live network and configured devices in the HiProvision database. The difference should be 0 just to make sure that no device is forgotten when upgrading firmware!</p> <p>Measured Devices: Indicates how many devices are measured in the live network.</p> <p>Configured Devices: Indicates how many devices are configured in the HiProvision database.</p>

12.3 Step 1: Upgrade

Purpose: Load a new firmware version into one or more modules in the network;


NOTE: Downgrade = upgrade to a lower version;


Click the upgrade button (see Figure 180) to start the upgrade wizard. The list below summarizes every page in the wizard:

About: Click Next>>;

- Select Firmware Image: select Module Type and the Upgrade Version. The Upgrade Version drop-down list will read out the 'C:\FtpRoot\Firmware' folder.

NOTE: If you need a firmware version that is not available in this list, you might download a new version for a module from the Portal via <https://hiprovision.hirschmann.com> → Shortcuts → Downloads. Once you have the firmware image, save or copy the entire zip file in the 'C:\FtpRoot\Firmware'. Do not rename or unzip the file. Close and reopen the Upgrade wizard.

- Module Selection: by default, all the modules in the list are selected for an upgrade. To unselect one or more modules, select the module(s) in the list and click the unselect button .
- Review: The selected modules will be shown: if ok, click Start Upgrade. The upgrade wizard closes and starts the upgrade process which can be followed by the upgrade status and upgrade process bar.

NOTE: The firmware must be signed (). If the firmware is unsigned or incorrectly signed, the Upgrade step will fail. As a result, the firmware can not be downloaded into the network. Make sure to get the correct signed firmware!

- In the example below, the 16-E1-L module in Node1/Slot2 is upgraded from v1.0.13 to v1.0.14. It means that v1.0.14 will be initially stored as backup version on the module prior to activating it (= committing and accepting) to become the active version.

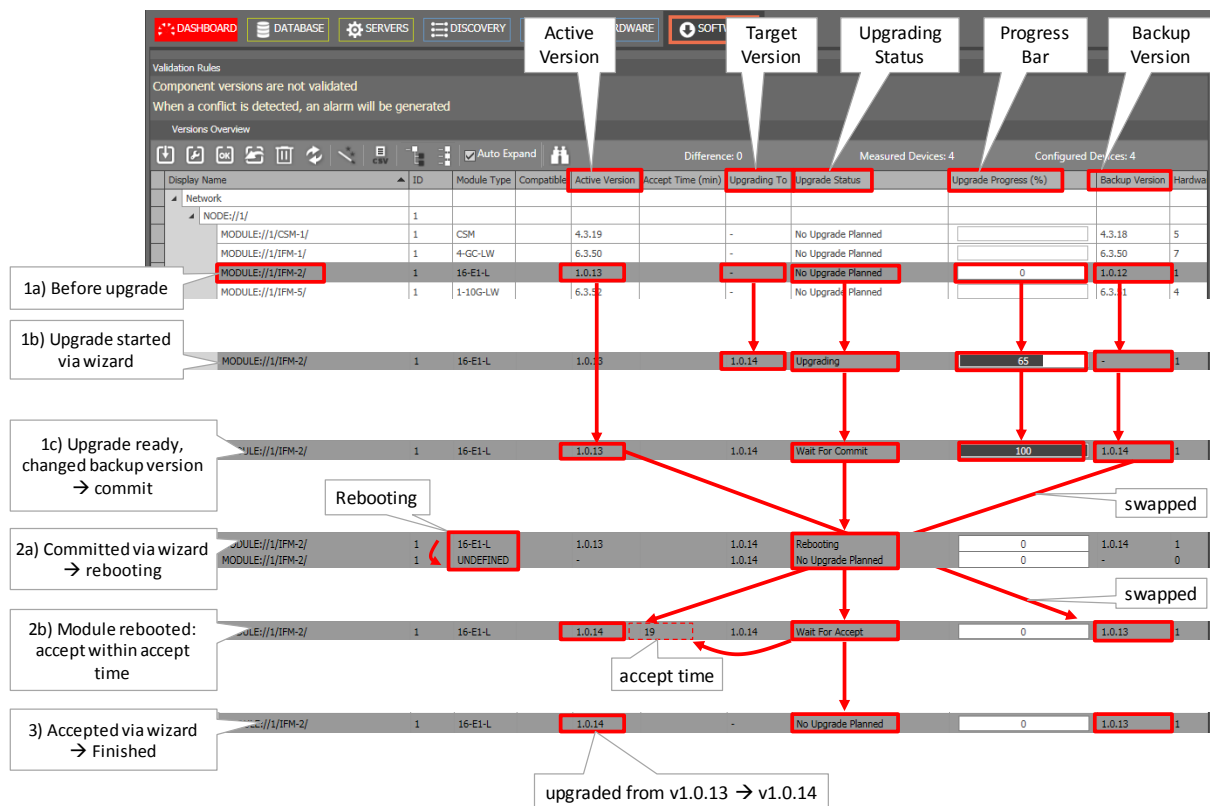


Figure 181 Step1: Upgrade Firmware

12.4 Step 2: Commit

Purpose: Swap to the new pending upgraded firmware version;

Click the commit button (see Figure 180) to start the commit wizard. The list below summarizes every page in the wizard:

Info Page: Click Next>>;

► Module Selection:

- by default, all the modules in the list are selected for a commit. To unselect one or more modules, select the module(s) in the list and click the unselect button ☐.
- Configuration action (only relevant for CSM firmware upgrades):
 - keep configuration (=default): The existing configuration on the CSM is kept, no extra (re)load of the configuration is necessary afterwards;
 - clear configuration: clears the CSM or node configuration, see §10.2;
 - reset configuration: resets the CSM or node configuration, see §10.3;
- Review: The selected modules will be shown: if ok, click Commit. The commit wizard closes and commits the selected pending upgrades. A reboot warning will pop-up, see figure below. Click Ok to continue;

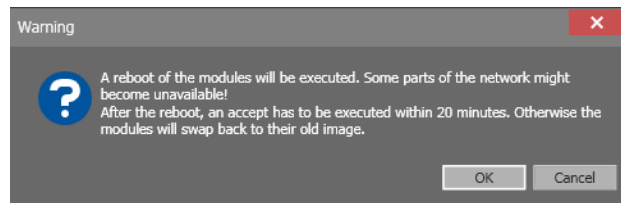


Figure 182 Commit Reboot Warning

- Result: commit was sent successfully, modules will reboot. Click Close;
- In the example below, after a commit, Node 1/slot2/16-E1-L is rebooting to swap the active and backup version. After the reboot, the status turns into 'Wait for Accept' and the backup version has become the active version and vice versa. The remaining accept time is shown in the field 'Accept Time' (min) and starts with 20 minutes.

NOTE: A 'wait for commit' never times out. If you have uploaded for example a wrong version, a rollback is not available but the 'Step1:Upgrade' must be executed again with the correct version.

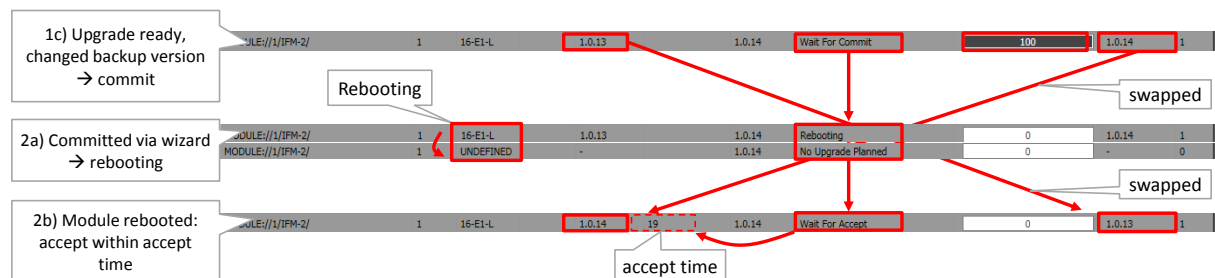


Figure 183 Step 2: Commit Firmware

12.5 Step 3: Accept

Purpose: Accept the new activated firmware version to keep it active without falling back after 20 minutes to the previous active version;

Click the accept button (see Figure 180) to start the accept wizard. The list below summarizes every page in the wizard:

About: Click Next>>;

- **Module Selection:** by default, all the modules in the list are selected for an accept. To unselect one or more modules, select the module(s) in the list and click the unselect button ☐.
- **Review:** The selected modules will be shown: if ok, click Accept. The accept wizard closes and accepts the committed upgrades.

Result: accept was sent successfully, modules will not reboot after 20 minutes and will not fall back to the previous active version. Click Close;



Figure 184 Step3: Accept Firmware

Table 29 Upgrade Status Overview

Status	Description
No Upgrade Planned	The module is not involved in an upgrade, commit or accept step. This status can turn in an 'Upgrading' status. It is also the new state of the module after accepting a committed upgrade.
Upgrading	The module is in the upgrade process, it means that at this moment, the backup firmware version is being overwritten by the new or target firmware version. This status will finally turn into the 'Wait for Commit' status.
Wait for Commit	The upgrade has been finished, the module is waiting for a commit to reboot and activate the new firmware version.
Rebooting	The module is rebooting due to a commit or not accepting within 20 minutes;
Wait for Accept	The module reboots after a commit and turns into a Wait for Accept status. You have 20 minutes to accept this new firmware version, otherwise the module will reboot automatically and fall back to its previous active version. The remaining accept time is shown in the field Accept Time (min).
Commit Failed or not accepted	You have not committed within the required 20 minutes or the commit has failed for some reason. As a result, a fall back occurs to its previous active version.

12.6 Step 4: Reload Network Configuration

Only perform this step when both conditions below are fulfilled:


the CSM FW has been upgraded;

- In the Commit (wizard) phase, the 'Configuration action' for this CSM was set to:
 - Clear configuration;
 - Reset Configuration;

NOTE: To load the network configuration, see §5.

12.7 Validation Rules

It is possible to validate if all the modules of the same type have the same firmware version.

Click the validation rules button  in Figure 180. A window pops up, select 'Make sure...'.

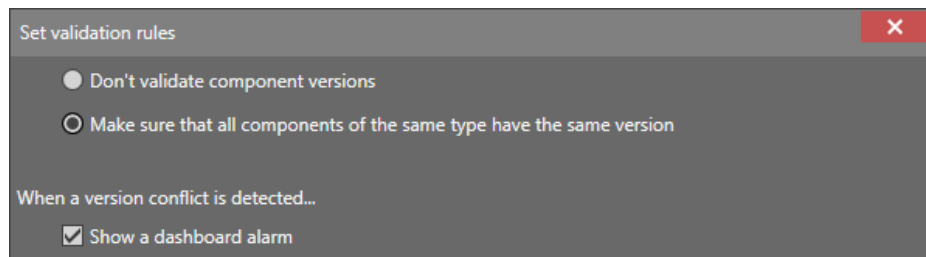


Figure 185 Firmware Validation Rules

After clicking OK in this window, the validation starts immediately. The results of the validation will appear in the compatible column.

When alarming is activated in the figure above, alarms will be generated as well when incompatible versions are detected, see figure below. Incompatibilities can be solved by upgrading or downgrading firmware versions as described in the paragraphs before.

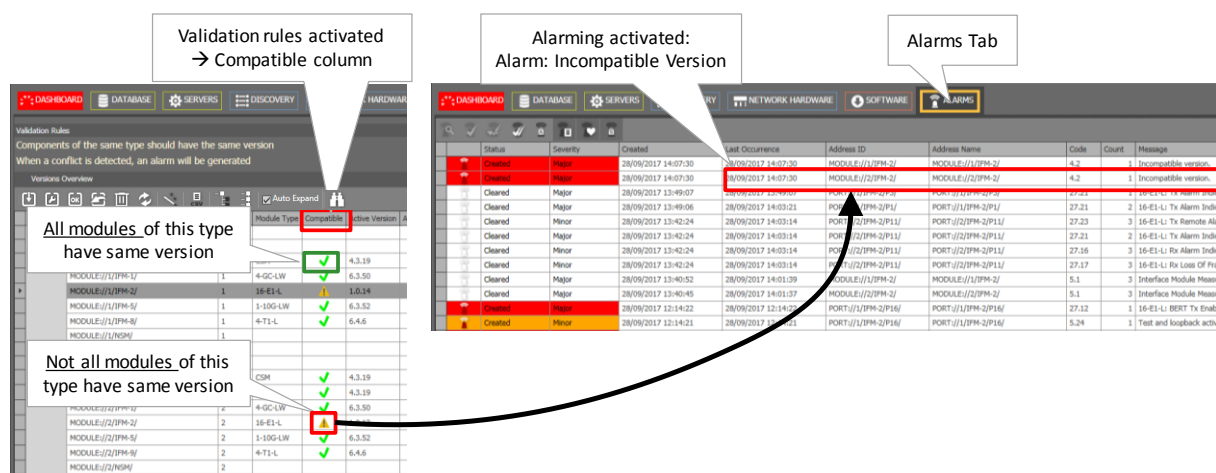



Figure 186 (In)Compatible Firmware Versions and Alarming


12.8 Revert to Backup

Purpose: Revert or fall back to the backup version e.g. when something went wrong during the loading of a new firmware version.

CAUTION: 'Revert to Backup' on a CSM reverts not only to the firmware version but to the configuration as well. This means that the function will also revert to the configuration running with the reverted firmware version. This absolutely supposes that no change has been made to the configuration since the previous FW version has been in use, and that the HiProvision database is still unchanged. 'Revert to Backup' on an Interface module will only revert the firmware version.

Click the revert button  (see Figure 180) to start the 'Revert to backup version' wizard. The list below summarizes every page in the wizard:

► About: Click Next>>;

- **Module Selection:** Select the modules via clicking the Selected checkbox. To unselect one or more modules, select the module(s) in the list and click the unselect button .

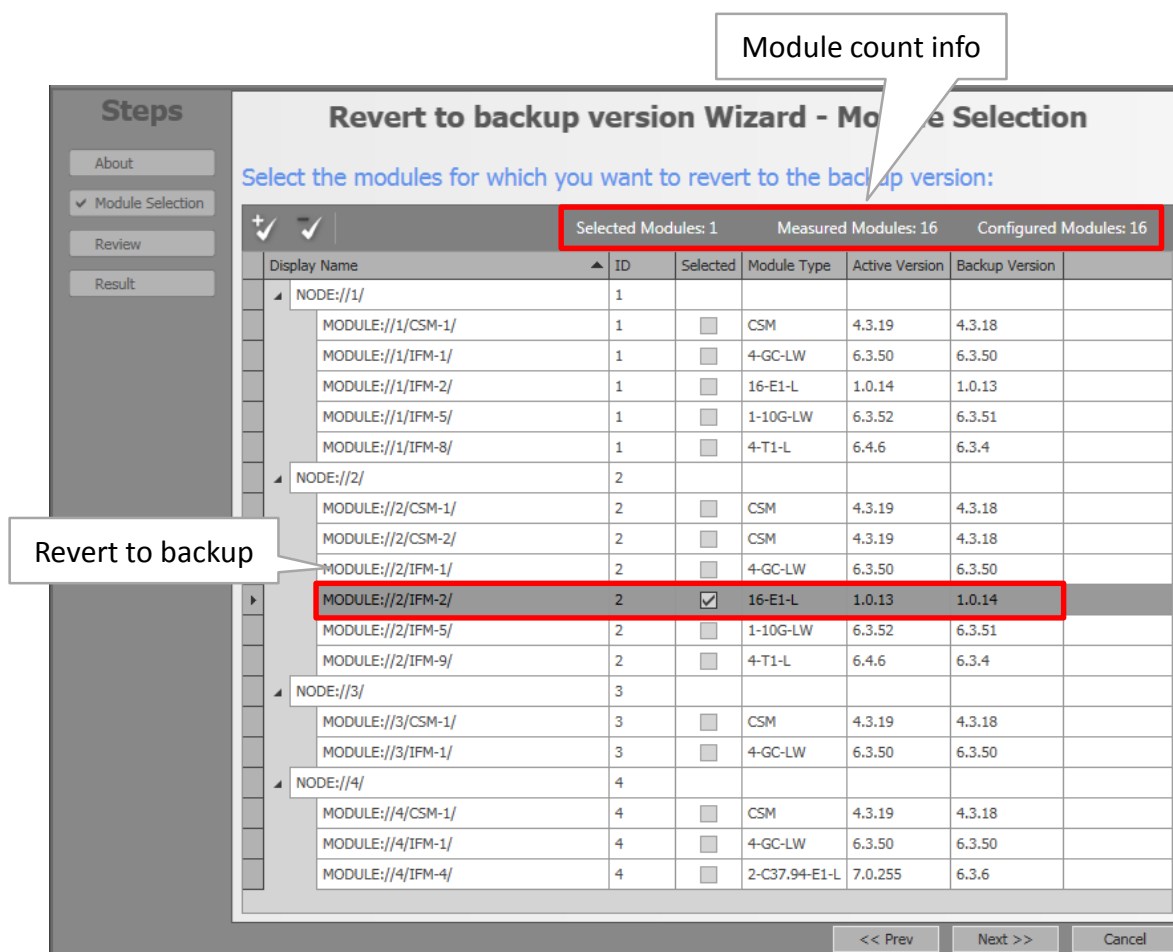



Figure 187 Revert to Backup Version

- **Review:** The selected modules will be shown: if ok, click Revert To Backup Version. A revert command will be sent to the network to initiate the revert action;

Result: Revert command was successfully sent, the revert action has been started and the progress for each selected module can be followed in the versions overview list in the Software tab. Click the Close button to close the wizard. In the version overview list, press the refresh button  from time to time, or faster progress feedback.

12.9 Reporting

Reporting information is available via the Reporting Engine Add-on, see §29.4.

13. SYNC E

13.1 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. [3] in Table 1). Recovery ports can be configured on the Interface Modules that support the SyncE feature, see §32.

Some facts:

Maximum one SyncE recovery port per Interface Module;

Maximum four SyncE recovery ports per Node;

► SyncE is non-revertive for clocks with the same quality and priority (see also §13.3).

All physical port interfaces from the Interface Modules 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 (Interface Module PTN-4-GC-LW/ PTN-4-GCB-LW, PTN-4-GO-LW, PTN-1-10G-LW);
- Optical C37.94 (Interface Module PTN-2-C37.94);
- Electrical Ethernet 100 Mbps (Interface Module PTN-4-GC-LW/ PTN-4-GCB-LW).

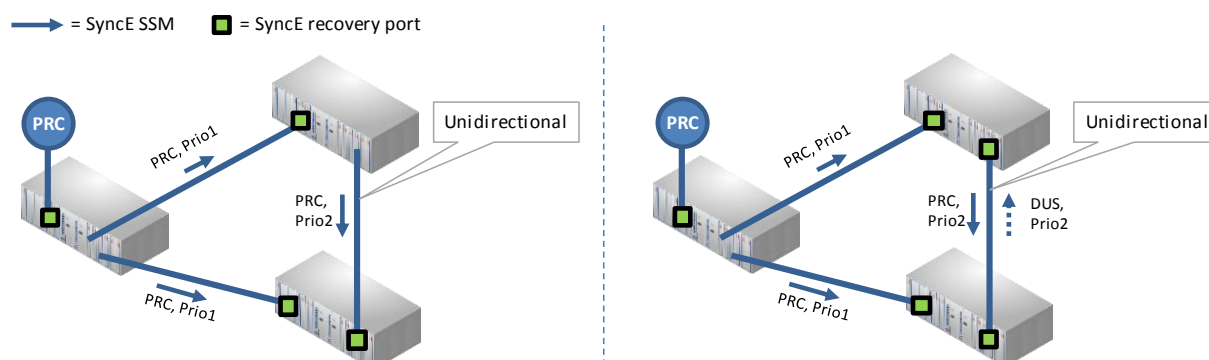


Figure 188 Unidirectional/Bidirectional SyncE Examples

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 §13.3).

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

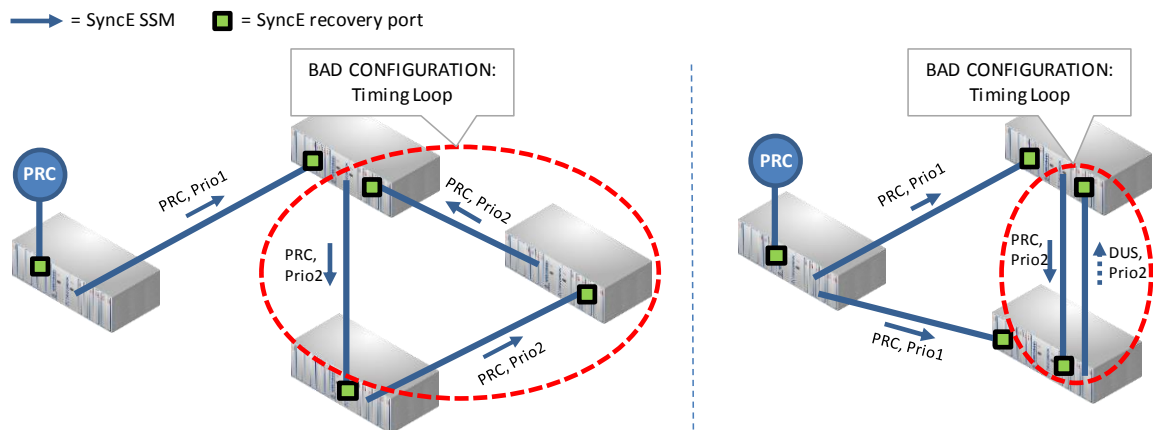



Figure 189 Bad SyncE Examples: Timing Loop

13.2 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;

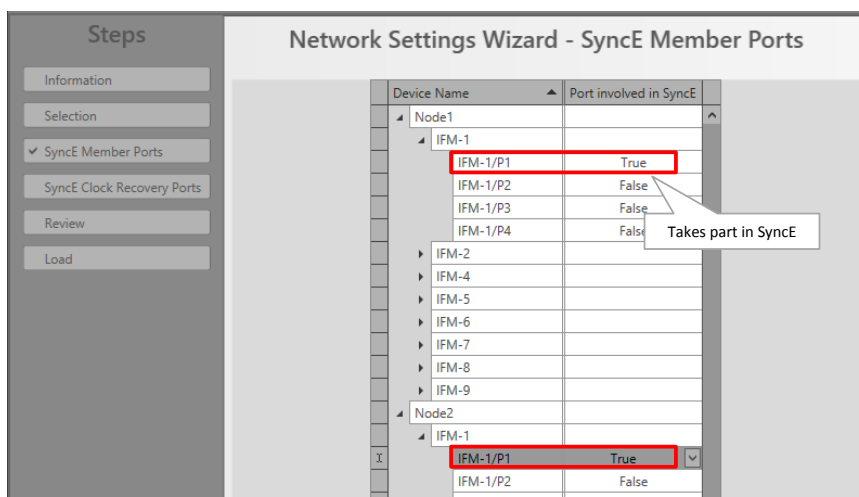


Figure 190 SyncE Member Ports

- 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 30 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 §13.3 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 §13.3.
- ▶ Lockout:
 - ▶ False (=default): the received clock will be used in §13.3;
 - ▶ True: the received clock on this port will be locked out or not be used in §13.3;
- ▶ Switch Request: Possibility to force a clock usage or overrule the selected clock by the selection process in §13.3;
 - ▶ 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 §13.3.
- ▶ 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';

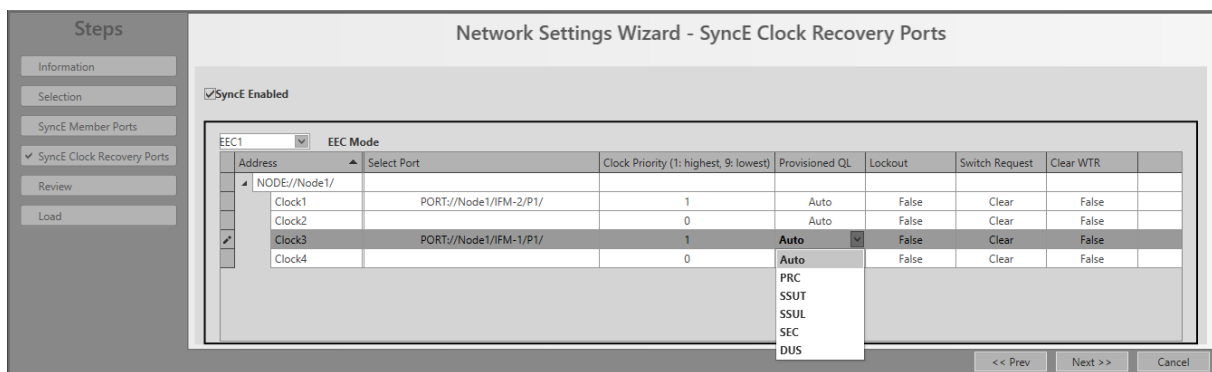


Figure 191 SyncE Clock Recovery Ports

Review: if ok, click Finish. The configuration load manager will be invoked, see §5.

13.3 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 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 30), 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 30 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 §13.2;

13.4 Operation

Once the SyncE has been configured and loaded in the network, it is up and running. To monitor the running SyncE, see Figure 209.

13.4.1 Reporting

Reporting information is available via the Reporting Engine Add-on, see §29.4.

14. PTP IEEE 1588V2 TRANSPARENT CLOCK

14.1 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.

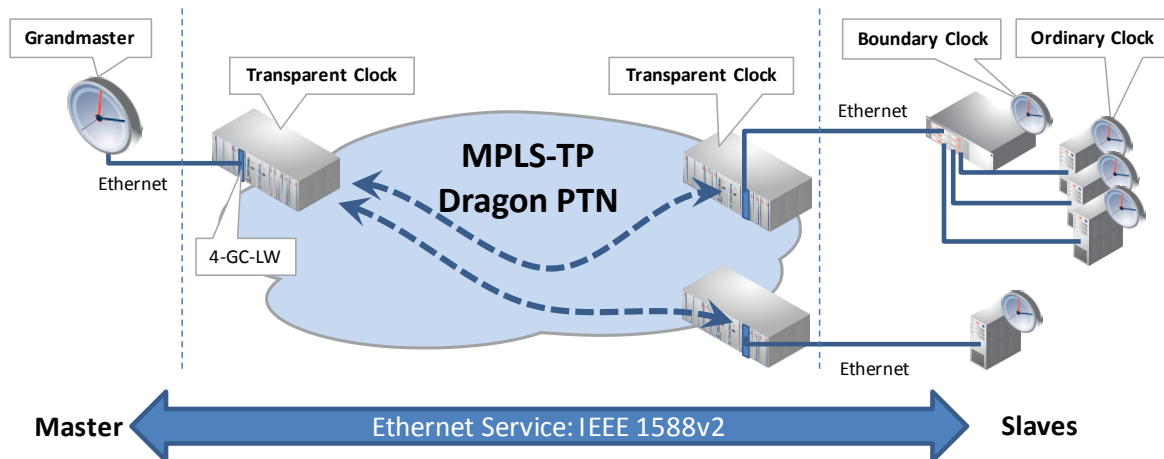


Figure 192 IEEE 1588v2

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 T1, T1', T2 and T2' 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.

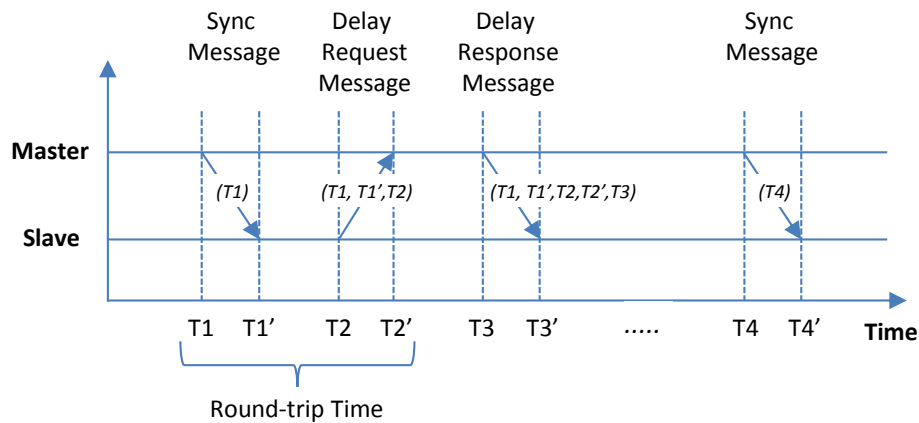


Figure 193 1588 Protocol Messages

14.2 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 §32 to find the Interface Modules 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;**

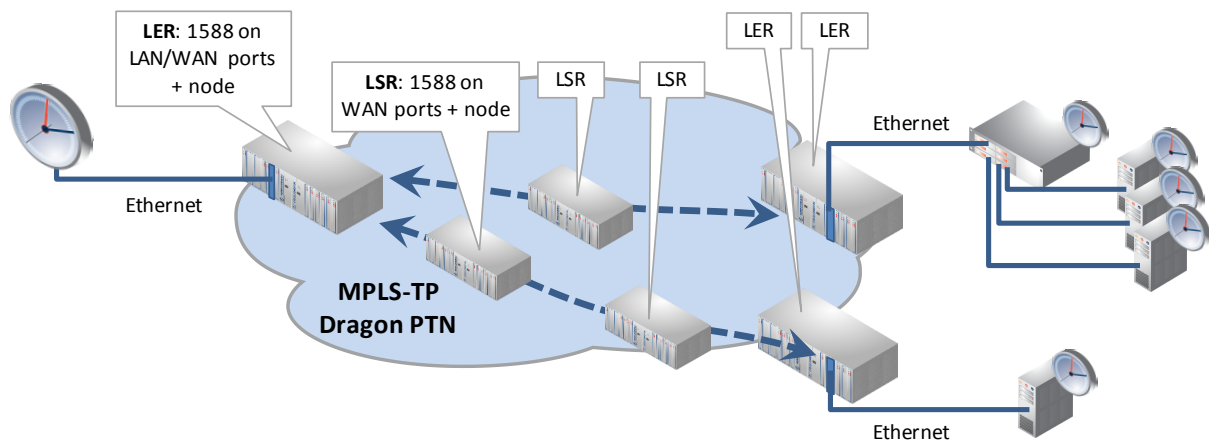


Figure 194 1588 on Port and Node Level for LERs and LSRs

- An external 1588 grandmaster clock broadcasts Sync messages with timestamp 'x' to the Dragon PTN network via Ethernet ports on the supported Interface Modules. 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.

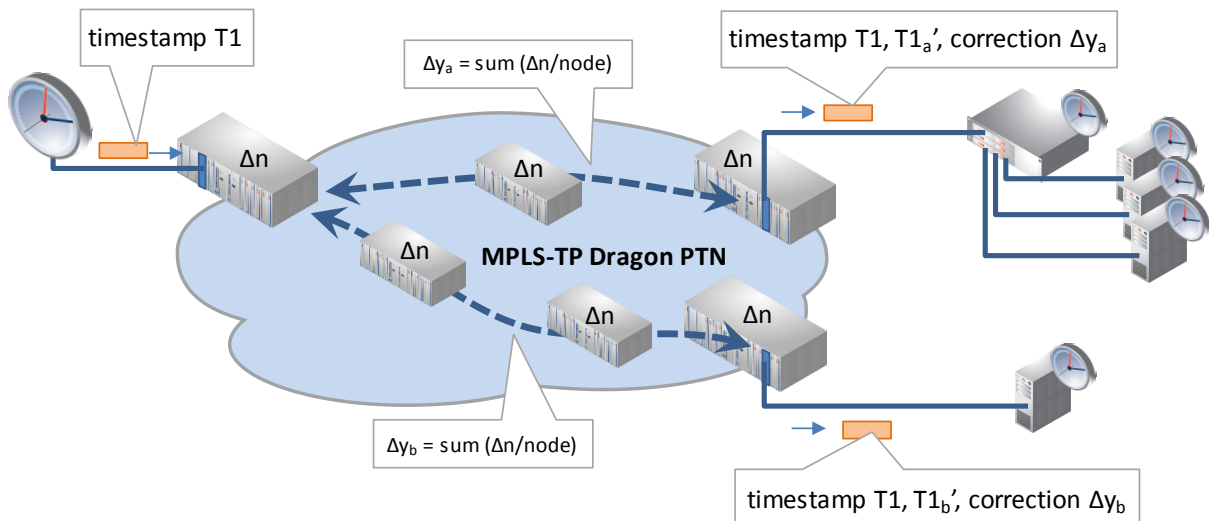


Figure 195 1588 Enabled: Transparent Clock Correction

- **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.

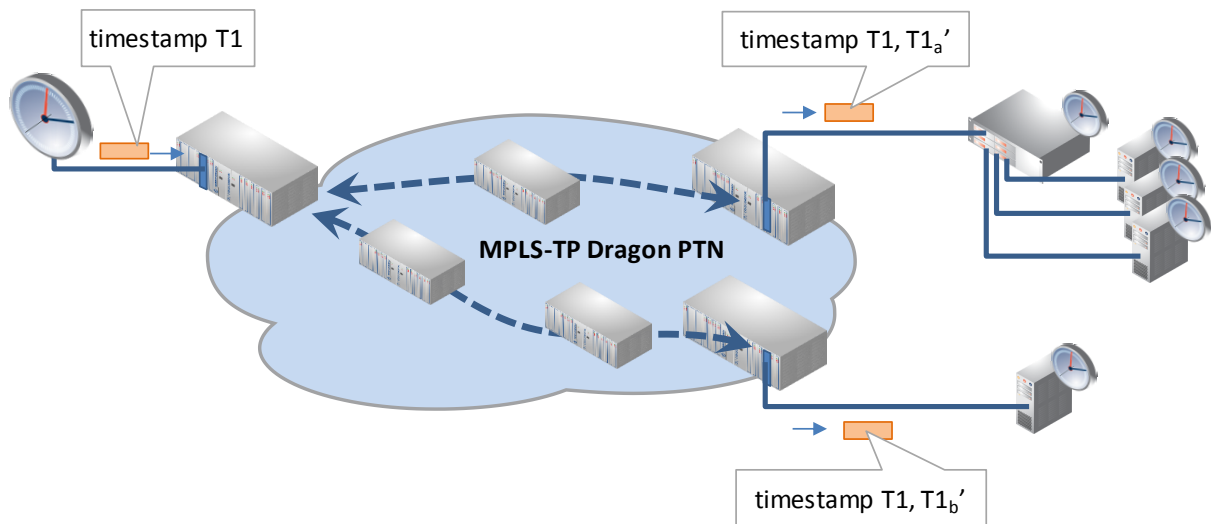


Figure 196 1588 Not Enabled: No Clock Correction

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;

14.3 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;

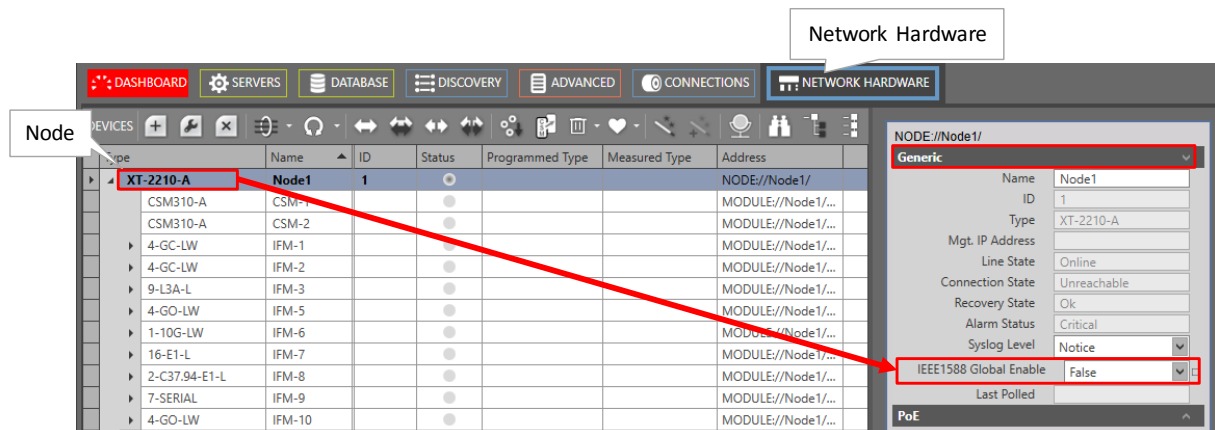


Figure 197 1588 Node Settings

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 PTN-4-GC-LW, PTN-4-GCB-LW, PTN-4-GO-LW cards Interface Modules.
- ▶ 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!

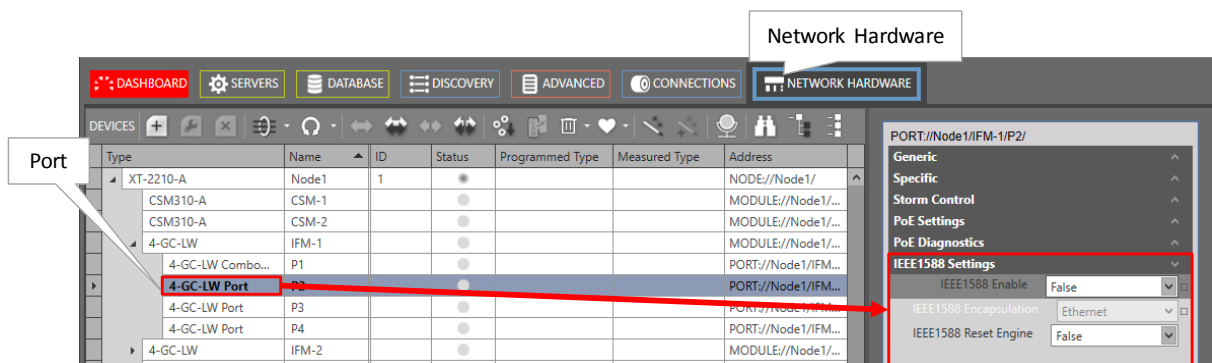



Figure 198 1588 Port Settings

3. Load changes via Network Hardware Tab →  into the live network to activate them. It starts the configuration load manager. See §5 for an overview of this tool.

14.4 Operation

Once the 1588 has been configured and loaded in the network, it is up and running. To monitor the running 1588, see §15.7.

15. PERFORMANCE COUNTERS AND MONITORING

15.1 General

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

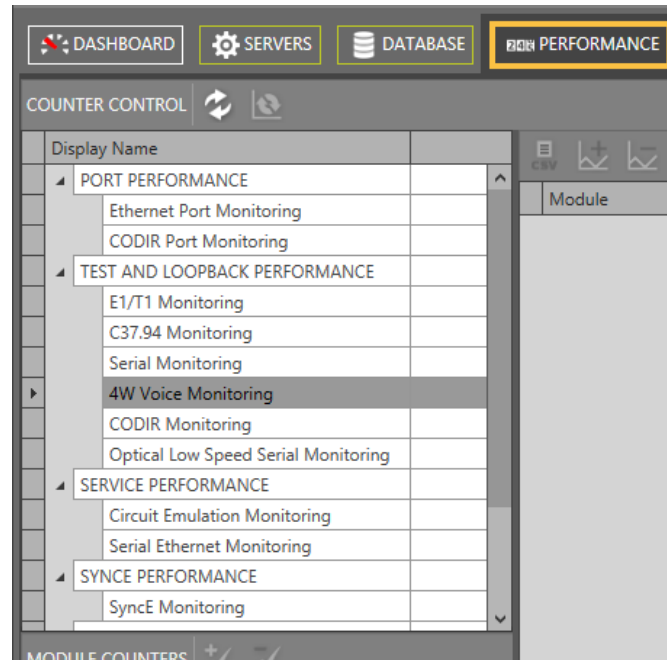


Figure 199 Performance Tab: Counter Control

Below, find the performance overview and cross references:


- ▶ Port Performance: §15.2;
- ▶ Test & Loopback Performance: §15.3;
- ▶ Service Performance: §15.4;
- ▶ SyncE Performance: §15.5;
- ▶ QoS Performance: §15.6;
- ▶ IEEE 1588 Performance: §15.7;









Health Monitor: §15.8;

15.2 Port Performance

15.2.1 Ethernet Port Monitoring

Follow the steps below to monitor some ports:

1. In the 'Counter Control' section, click  to expand Port Performance;
2. Click Ethernet Port Monitoring, see Figure 200;
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 Interface Modules 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. Click  in the Counter Control section to refresh all counter values;
 10. Click  to reset counter values;
- NOTE:** For 'Test & Loopback Performance', another reset method must be used, see further;
11. 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;
 12. Options: The graphs can be optimized (labels etc.) via the Options drop-down list;

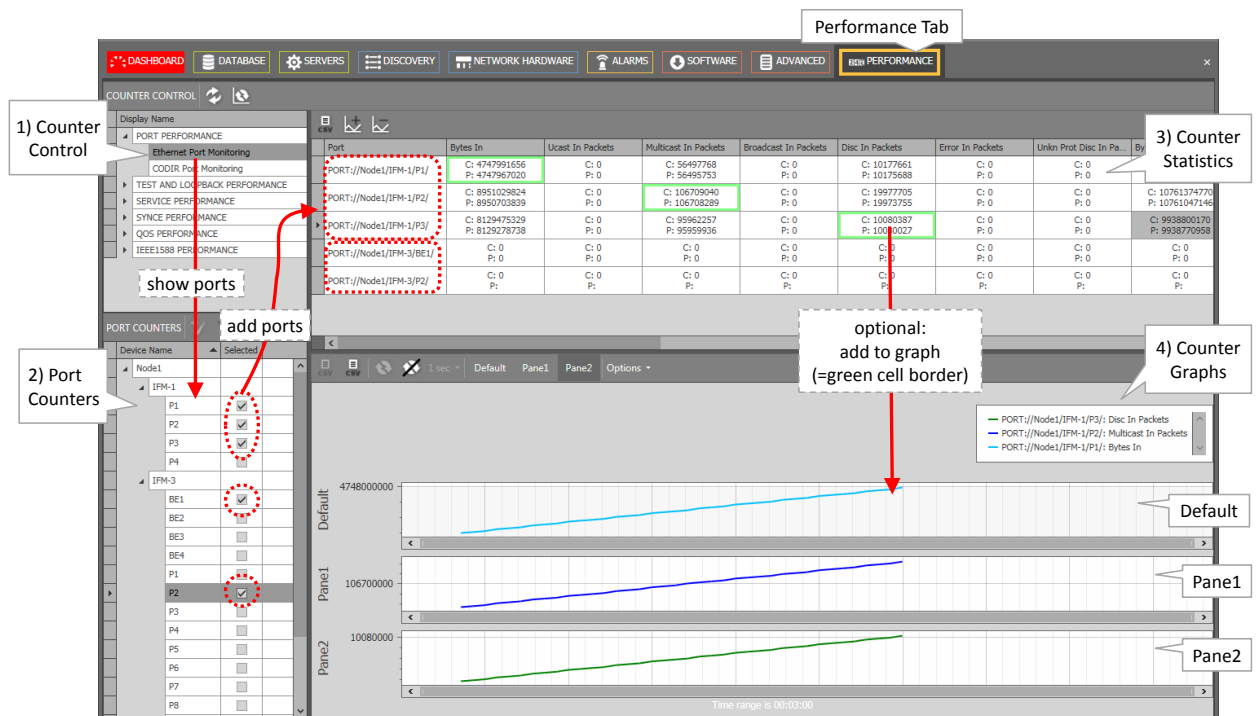



Figure 200 Ethernet Port Monitoring

Table 31 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 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	

Field	Values	Description	Curative Action
		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: - 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: - 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...
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.
<p>Note: Click the Refresh button for the latest results;</p> <p>Note: Clear the counter values by clicking ;</p> <p>Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

15.2.2 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 §15.2.

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

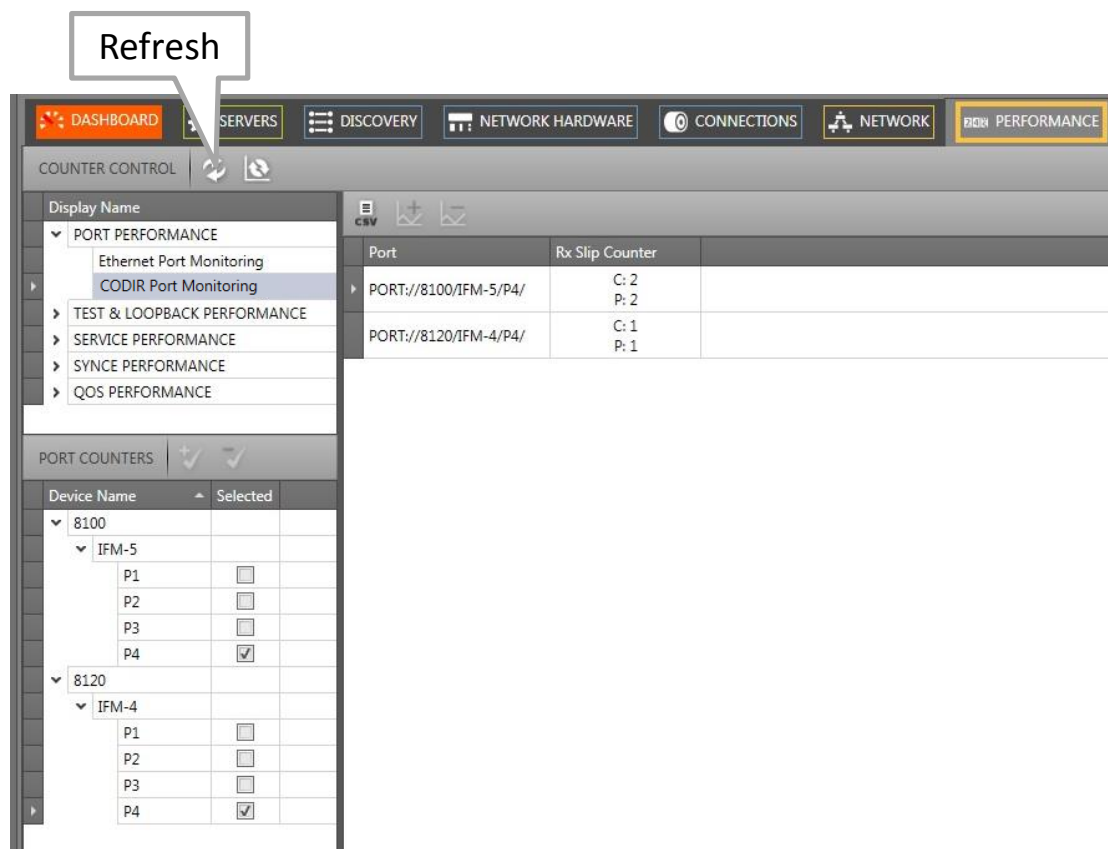


Figure 201 CODIR Port Monitoring

Table 32 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;</p> <p>Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

15.3 Test & Loopback Performance

15.3.1 E1/T1 Monitoring

E1/T1 monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §15.2.

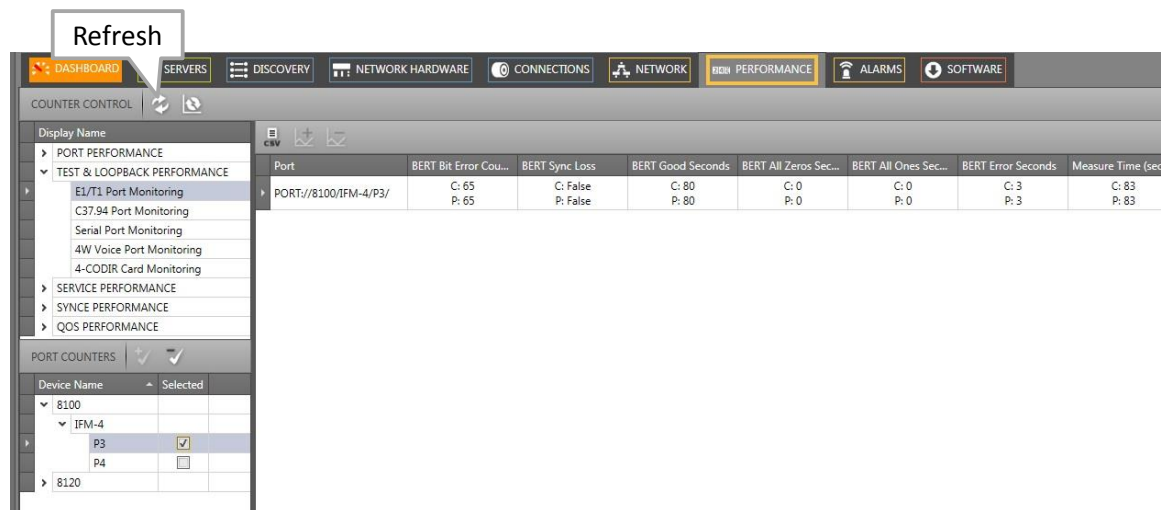


Figure 202 E1/T1 Monitoring

Table 33 E1/T1 Monitoring Fields

Field	Values	Description	Curative Action
Port	value	Monitored port	
BERT Bit Error Counter	bit errors	increasing = NOT OK: The number of bit errors received by the BERT receiver, this should be zero for a successful test.	
BERT Sync Loss	True/False	True: the BERT receiver is not synchronized with the BERT transmitter, the measurement is failing. False: the BERT receiver is synchronized with the BERT transmitter.	True: Verify the clocking settings, BERT settings, broken paths,
BERT Good Seconds	seconds	increasing = OK: The total amount in seconds that the test traffic received by the BERT receiver was OK, meaning synchronized and no errors	
BERT All Zeros Seconds	seconds	increasing = NOT OK: The total amount in seconds that the BERT receiver was receiving all zeros	
BERT All Ones Seconds	seconds	increasing = NOT OK: The total amount in seconds that the BERT receiver was receiving all ones	
BERT Error Seconds	seconds	increasing = NOT OK: The total amount in seconds that the BERT receiver was receiving bit errors, an increasing value does not result in synchronization loss	
Measure Time (seconds)	seconds	The total amount in seconds that the BERT receiver has been measuring	

Note: Click the Refresh button for the latest results;

Note: Clear the counter values by disabling and enabling the BERT via the Interface Module/port settings in the network hardware tile;

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

15.3.2 C37.94 Monitoring

C37.94 monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §15.2.

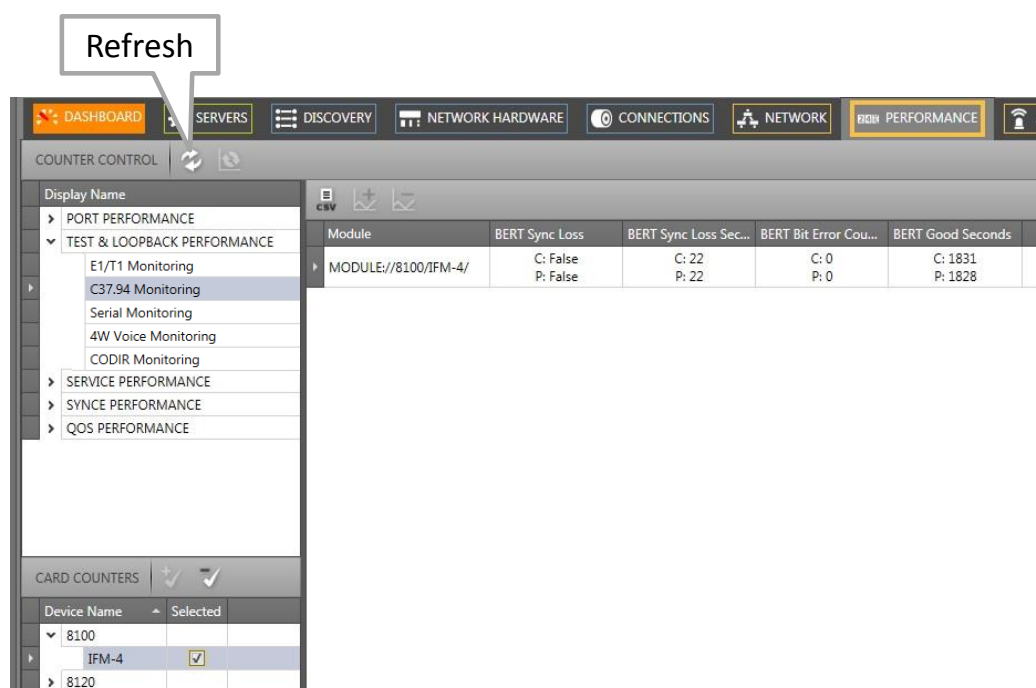


Figure 203 C37.94 Monitoring

Table 34 C37.94 Monitoring Fields

Field	Values	Description	Curative Action
Module	value	Monitored module	
BERT Sync Loss	True/False	True: the BERT receiver is not synchronized with the BERT transmitter, the measurement is failing. False: the BERT receiver is synchronized with the BERT transmitter.	True: Verify the clocking settings, BERT settings, broken paths,
BERT Sync Loss Seconds	seconds	increasing = NOT OK: The total amount in seconds that the BERT receiver is not synchronized with the BERT transmitter	True: Verify the clocking settings, BERT settings, broken paths,
BERT Bit Error Counter	number	increasing = NOT OK: The number of bit errors received by the BERT receiver, this should be zero for a successful test.	
BERT Good Seconds	seconds	increasing = OK: The total amount in seconds that the test traffic received by the BERT receiver was OK, meaning synchronized and no errors	
<p>Note: Click the Refresh button for the latest results;</p> <p>Note: Clear the counter values by disabling and enabling the BERT via the Interface Module/port settings in the network hardware tile;</p> <p>Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

15.3.3 Serial Monitoring

Exactly the same description as in §15.3.2.

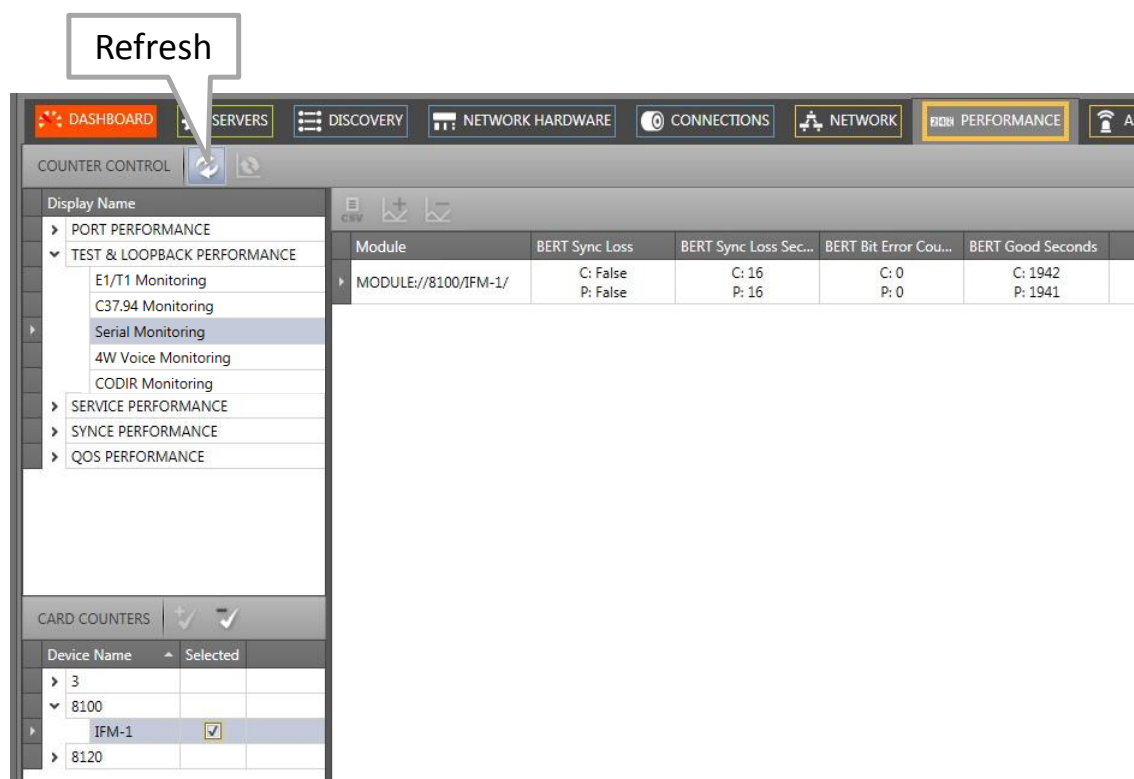


Figure 204 Serial Monitoring

Table 35 Serial Monitoring Fields

Field	Values	Description	Curative Action
Module	value	Monitored module	
BERT Sync Loss	True/False	True: the BERT receiver is not synchronized with the BERT transmitter, the measurement is failing. False: the BERT receiver is synchronized with the BERT transmitter.	True: Verify the clocking settings, BERT settings, broken paths,
BERT Sync Loss Seconds	seconds	increasing = NOT OK: The total amount in seconds that the BERT receiver is not synchronized with the BERT transmitter	True: Verify the clocking settings, BERT settings, broken paths,
BERT Bit Error Counter	number	increasing = NOT OK: The number of bit errors received by the BERT receiver, this should be zero for a successful test.	
BERT Good Seconds	seconds	increasing = OK: The total amount in seconds that the test traffic received by the BERT receiver was OK, meaning synchronized and no errors	
<p>Note: Click the Refresh button for the latest results;</p> <p>Note: Clear the counter values by disabling and enabling the BERT via the Interface Module/port settings in the network hardware tile;</p> <p>Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

15.3.4 4W Voice Monitoring

4W Voice monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §15.2.

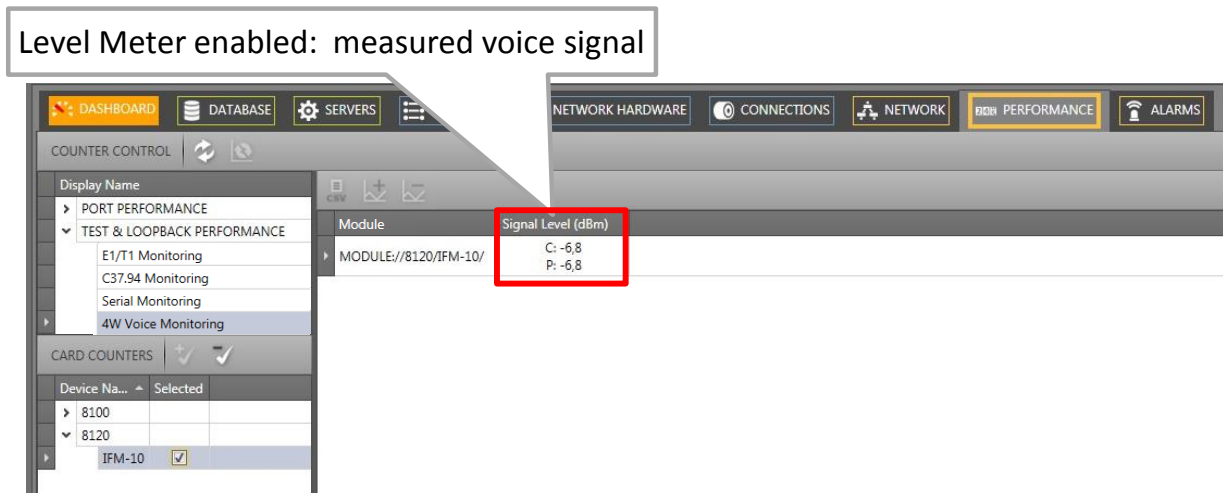


Figure 205 4W Voice Monitoring

Table 36 4W Voice Monitoring Fields

Field	Values	Description
Module	value	Monitored module
Signal Level (dBm)	dBm	The 'Signal Level (dBm)' of an incoming voice signal can be measured if 'Level Meter' has been enabled on a specific port, see also §18.4 for more information and to know which port is being measured. The accuracy of the measurement is +/- 0.5 dBm.
Note: Click the Refresh button for the latest results; Note: 'C' value in cell = current value; 'P' value in cell = previous value;		

15.3.5 CODIR Monitoring

CODIR monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §15.2. The example below is the monitoring of Figure 233.

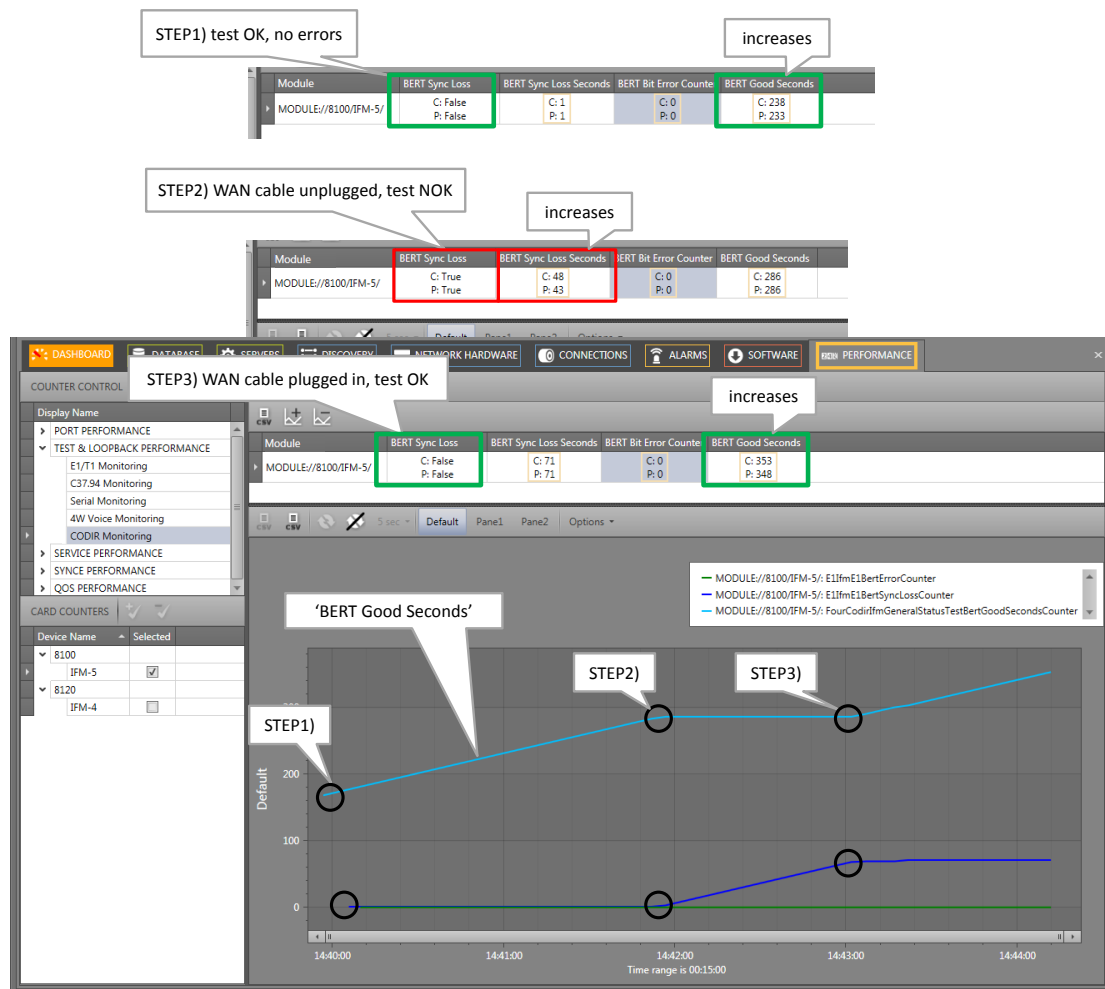


Figure 206 CODIR Monitoring

Table 37 CODIR Monitoring Fields

Field	Values	Description	Curative Action
Module	value	Monitored module	
BERT Sync Loss	True/False	True: the BERT receiver is not synchronized with the BERT transmitter, the measurement is failing. False: the BERT receiver is synchronized with the BERT transmitter.	True: Verify the clocking settings, BERT settings, broken paths,
BERT Sync Loss Seconds	seconds	increasing = NOT OK: The total amount in seconds that the BERT receiver is not synchronized with the BERT transmitter	Verify the clocking settings, BERT settings, broken paths,
BERT Bit Error Counter	number	increasing = NOT OK: The number of bit errors received by the BERT receiver, this should be zero for a successful test.	
BERT Good Seconds	seconds	increasing = OK: The total amount in seconds that the test traffic received by the BERT receiver was OK, meaning synchronized and no errors	

Note: Click the Refresh button for the latest results;

Note: Clear the counter values by disabling and enabling the BERT via the Interface Module/port settings in the network hardware tile;

Field	Values	Description	Curative Action
Note: 'C' value in cell = current value; 'P' value in cell = previous value;			

15.3.6 Optical Low Speed Serial Monitoring

Optical Low Speed Serial monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §15.2.

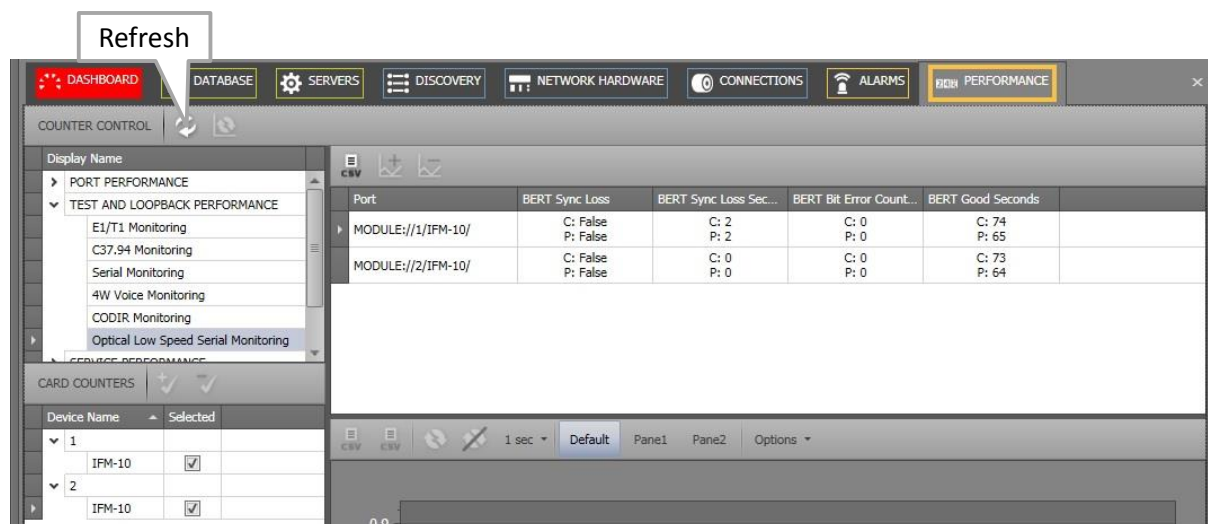


Figure 207 Low Speed Serial Monitoring

Table 38 Low Speed Serial Monitoring

Field	Values	Description	Curative Action
Port	value	Monitored port	
BERT Sync Loss	True/False	True the BERT receiver is not synchronized with the BERT transmitter, the measurement is failing. False: the BERT receiver is synchronized with the BERT transmitter.	True: Verify the clocking settings, BERT settings, broken paths,
BERT Sync Loss Seconds	seconds	increasing = NOT OK: The total amount in seconds that the BERT receiver is not synchronized with the BERT transmitter	Verify the clocking settings, BERT settings, broken paths,
BERT Bit Error Counter	number	increasing = NOT OK: The number of bit errors received by the BERT receiver, this should be zero for a successful test.	
BERT Good Seconds	seconds	increasing = OK: The total amount in seconds that the test traffic received by the BERT receiver was OK, meaning synchronized and no errors.	
Note: Click the Refresh button for the latest results; Note: Clear the counter values by disabling and enabling the BERT via the Interface Module/port settings in the network hardware tile; Note: 'C' value in cell = current value; 'P' value in cell = previous value;			

15.4 Service Performance

15.4.1 Circuit Emulation Monitoring

A Circuit Emulation service monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §15.2 except that now services have to be added instead of ports. The monitoring window shows 2 sections:

- ▶ Interface Module Parameters;
- ▶ Service Parameters;

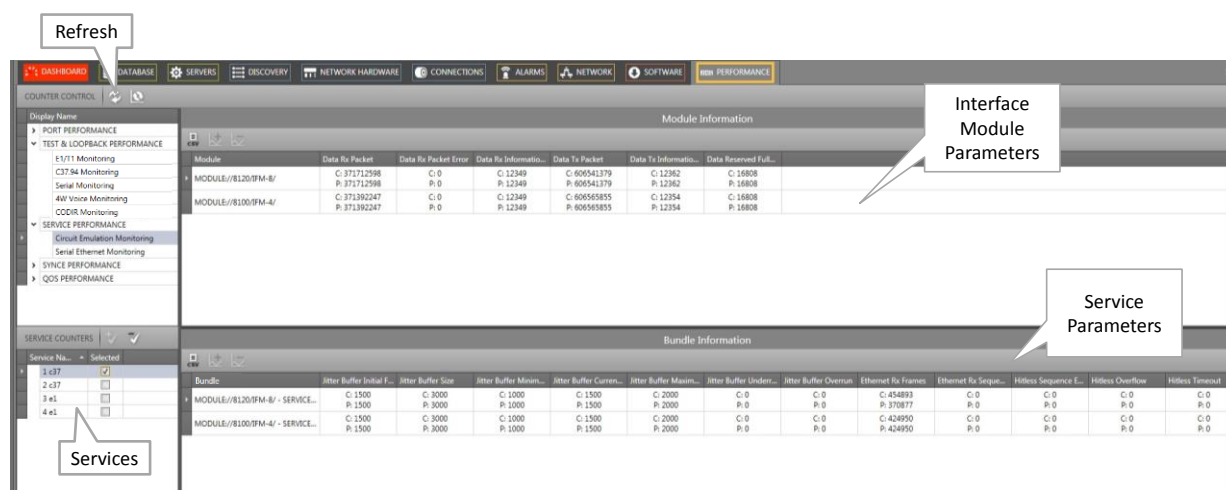



Figure 208 Services: Circuit Emulation Monitoring

Table 39 Services: Circuit Emulation Monitoring 'Module' Fields

Field	Values	Description
Module	value	Monitored module
Data Rx Packet	packets	The number of received data packets.
Data Rx Packet Error	packets	The number of received erroneous data packets. The packets had for example a CRC error.
Data Rx Information Bandwidth	kbps	The reserved module bandwidth for only the payload data on the ingress side. This value remains the same until the HiProvision bandwidth configuration changes.
Data Tx Packet	packets	The number of transmitted data packets.
Data Tx Information Bandwidth	kbps	The reserved module bandwidth for only the payload data on the egress side. This value remains the same until the HiProvision bandwidth configuration changes.
Data Reserved Full Bandwidth	kbps	The reserved full module bandwidth including both overhead and payload data. This value remains the same until the HiProvision bandwidth configuration changes.

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;

Table 40 Services: Circuit Emulation Monitoring 'Bundle' Fields

Field	Values	Description	Curative Action
Bundle	value	The monitored bundle or stream	
Total Buffer Initial Fill Level	μs	The start level of the buffer right after resetting/rebooting the Interface Module	
Total Buffer Size	μs	This is the reserved jitter buffer size. It is the absolute maximum that a buffer level can reach. The size is based on the configuration parameters. If the current buffer level would increase above the buffer size (which is not possible), a buffer overrun occurs and packets are lost.	verify the Service wizard → Circuit emulation parameters / QoS configuration in HiProvision
Total Buffer Minimum Level	μs	The minimum (current) level that has been reached so far	no drifting, and close to minimum size (0) due to network jitter or hitless path interruption, verify buffers configuration, buffer too small?
Total Buffer Current Level	μs	The current fill level of the buffer	if this level is drifting, verify clocking settings master/slave
Total Buffer Maximum Level	μs	The maximum (current) level that has been reached so far	no drifting, and close to maxsize (=size buffer) due to network jitter, verify buffers configuration, buffer too small?
Total Buffer Underrun	count	The number of that times that a buffer has underrun. A buffer underrun occurs when the buffer is filled slower than packets in the buffer are processed. As a result, the buffer will finally run empty which results in an underrun. If an underrun occurs, the buffer will be reset to the initial level.	verify clock settings master/slave, jitter buffer might be too small.... verify the Service wizard → Circuit emulation parameters in HiProvision
Total Buffer Overrun	count	The number of times that a buffer has overrun. A buffer overrun occurs when the buffer is filled faster than packets in the buffer are processed. As a result, the buffer fill level will grow up to the maximum or buffer size, and finally will overflow or overrun. After an overrun, the buffer will be reset to the initial level.	verify clock settings master/slave, jitter buffer might be too small.... verify the Service wizard → Circuit emulation parameters in HiProvision.
Ethernet Rx Frames	frames	The number of received Ethernet frames.	
Ethernet Rx Sequence Number Drop Errors	frames	The number of received Ethernet frames that were dropped due to an invalid sequence number.	
Hitless Sequence Error	count	The number of times that a sequence number error occurred	
Hitless Overflow	count	The number of times that the hitless buffer (in FPGA) overflow occurred	verify the Service wizard → Circuit emulation parameters / QoS configuration in HiProvision
Hitless Timeout	count	The number of times that a timeout occurred on one of the hitless paths. E.g. pulling out the WAN link of the hitless path will increase the counter by	

Field	Values	Description	Curative Action
		one.	
Reserved Information Bandwidth	kbps	The reserved bundle bandwidth for only the payload data. This value remains the same until the HiProvision bandwidth configuration changes.	
Reserved Full Bandwidth	kbps	The reserved full bundle bandwidth including both overhead and payload data. This value remains the same until the HiProvision bandwidth configuration changes.	
Bundle	value	The monitored bundle or stream	
Total Buffer Initial Fill Level	μs	The start level of the buffer right after resetting/rebooting the Interface Module	

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;

15.4.2 Serial Ethernet Monitoring

A Serial Ethernet service monitoring can be found in the figure below. A detailed monitoring set-up description is similar to the description in §15.2 except that now services have to be added instead of ports.

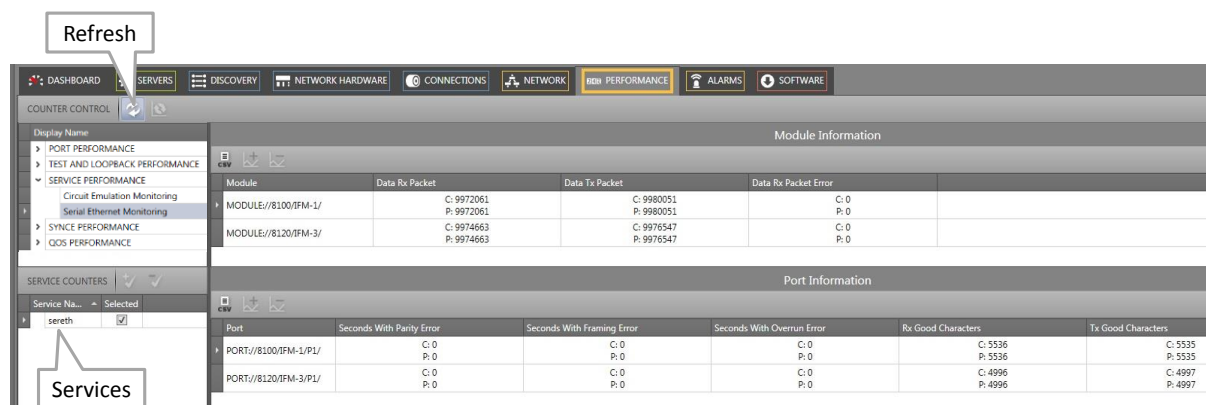


Figure 209 Services: Serial Ethernet Monitoring

Table 41 Services: Serial Ethernet Monitoring 'Module' Fields

Field	Values	Description
Module	value	Monitored module
Data Rx Packet (ingress)	packets	The number of received data packets.
Data Tx Packet (egress)	packets	The number of transmitted data packets.
Data Rx Packet Error (ingress)	packets	The number of received erroneous data packets. The packets had for example a CRC error.

Note: Click the Refresh button for the latest results; 'C' value in cell = current value; 'P' value in cell = previous value;

Table 42 Services: Serial Ethernet Monitoring 'Port' Fields

Field	Values	Description
Port	value	Monitored port
Seconds With Parity Errors (ingress)	seconds	increasing = NOT OK: The total amount in seconds that frames with parity errors were received
Seconds With Framing Errors (ingress)	seconds	increasing = NOT OK: The total amount in seconds that frames with framing errors were received
Seconds With Overrun Errors (ingress)	seconds	increasing = NOT OK: The total amount in seconds that buffer overrun errors occurred
Rx Good Characters (ingress)	characters	The number of valid or good received characters. A good character contains 8 bits and has no errors in it. Character validation is based on start/stop/parity bits.
Tx Good Characters (egress)	characters	The number of valid or good transmitted characters. A good character contains 8 bits and has no errors in it. Character validation is based on start/stop/parity bits.
<p>Note: Click the Refresh button for the latest results;</p> <p>Note: Clear the counter values by disabling and enabling the BERT via the Interface Module/port settings in the network hardware tile;</p> <p>Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>		

15.5 SyncE Performance

Once SyncE has been configured as described in §13, 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 §15.2. This monitoring does not support graph monitoring as in §15.2.

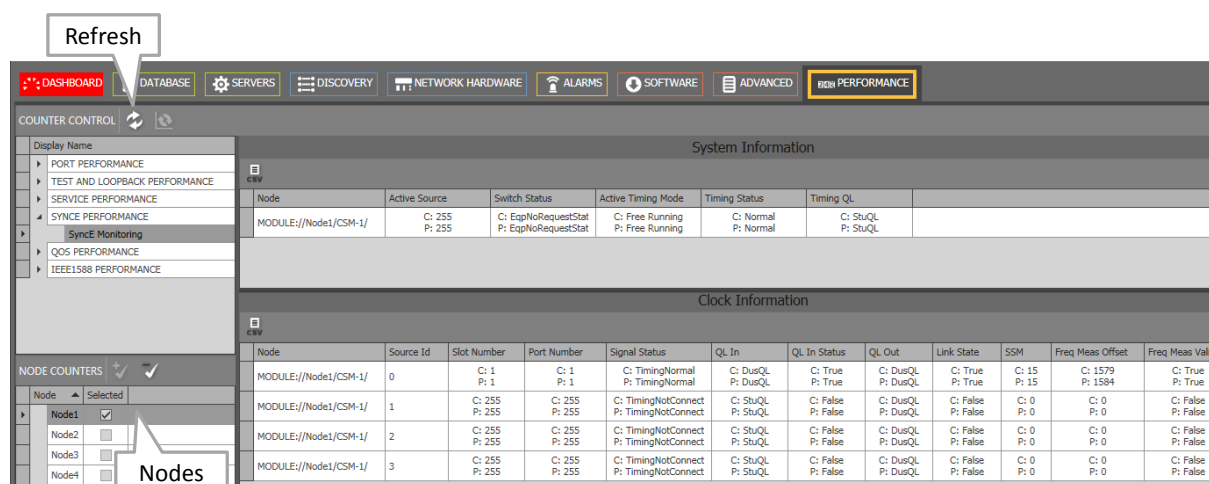


Figure 210 SyncE Monitoring

Table 43 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 QI	quality values in Table 30	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 30.	
Note: Click the Refresh button for the latest results; Note: 'C' value in cell = current value; 'P' value in cell = previous value;			

Table 44 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	

Field	Values	Description	Curative Action
		(=5 minutes) TimingNotConnected: no clock configured or defined on this clock input source or recovery port.	
QI In (ingress)	quality values in Table 30	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 30	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 30	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
Note: Click the Refresh button for the latest results; Note: 'C' value in cell = current value; 'P' value in cell = previous value;			

15.6 QoS Performance

QoS Performance monitoring can be found in the figure below. It shows 2 sections:

QoS Policer Monitoring (Figure 211): The policer is a functionality on the CSM that measures the bandwidth profile (=bandwidth and burst size) of the incoming traffic on a LAN or WAN port. If these measurements are conform the configured bandwidth profile of that service, the packets are allowed and passed through (=conform packets, green packets). If not, the packets are dropped or violated (=violated packets, red packets). It also measures the 'Average Frame Size In' (not visible in the screenshot). This value can be used as input in the Average Package size settings in the service wizard QoS window to fine-tune the bandwidth efficiency, see §3.7.

QoS Queue Monitoring (Figure 212): shows how many packets go in and out the priority queue. E.g. if a service 'Video147' has been assigned priority 3, and port 7 is an endpoint of this service, packets received on port 7 and transmitted on the Dragon PTN network, will travel through priority queue 3.

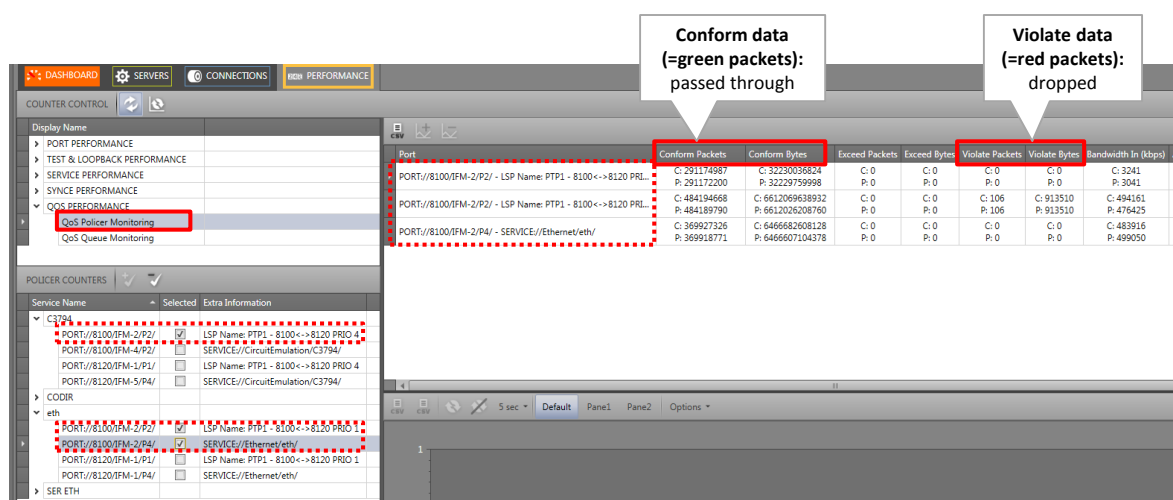



Figure 211 QoS Policer Monitoring

Table 45 QoS Policer Monitoring Fields

Field (*)	Values	Description	Curative Action
Port	value	Monitored port	
Conform Packets	packets	The number of packets within (or conform) the configured bandwidth profile (see description above in §15.6). None of these packets were dropped /discarded by the policer.	
Conform Bytes	bytes	Similar to 'Conform Packets' but with bytes instead of packets.	
Exceed Packets	packets	Not supported, always 0	
Exceed Bytes	bytes	Not supported, always 0	
Violate Packets	packets	The number of packets that mismatch or violate the configured bandwidth profile (see description above in §15.6). These packets were dropped by the policer.	Send less traffic or modify the configured bandwidth profile.
Violate Bytes	bytes	Similar to 'Violate Packets' but with bytes instead of packets.	Send less traffic or modify the configured bandwidth profile.
Bandwidth In (kbps)	kbps	The total incoming bandwidth between the current and the previous measurement: [(CurrentBytesIn - PreviousBytesIn)/1000/TimeInterval] kbps. Note: BytesIn = Total Incoming Bytes = Conform + Exceed + Violated	
Average Bandwidth In (kbps)	kbps	The average of the 5 latest 'Bandwidth In' measurements. Every (manual) refresh is a new measurement.	
Bandwidth Pass (kbps)	kbps	The resulting bandwidth that was ok and passed through the Policer. Example: if you have configured a service of 3 Mbps, and you receive 10 Mbps on the port, approximately 3 Mbps will be passed, the rest will be dropped.	Send less traffic or increase (or modify) the configured bandwidth if 'Bandwidth In' > 'Bandwidth Pass'. Verify 'Violate Bytes' counter.
Average Bandwidth Pass (kbps)	kbps	The average of the 5 latest 'Bandwidth Pass' measurements. Every (manual) refresh is a new measurement.	

Field (*)	Values	Description	Curative Action
Average Frame Size In (bytes)	bytes	The average frame size of all the frames (conform+exceed+violated) that are received on this port in the 5 latest measurements. Every (manual) refresh is a new measurement.	
Average Frame Size Pass (bytes)	bytes	The average frame size of frames that passed the policer in the 5 latest measurements. Every (manual) refresh is a new measurement.	

(*) **Note:** All fields are ingress fields
Note: Click the Refresh button for the latest results;
Note: Clear the counter values by clicking ;
Note: 'C' value in cell = current value; 'P' value in cell = previous value;

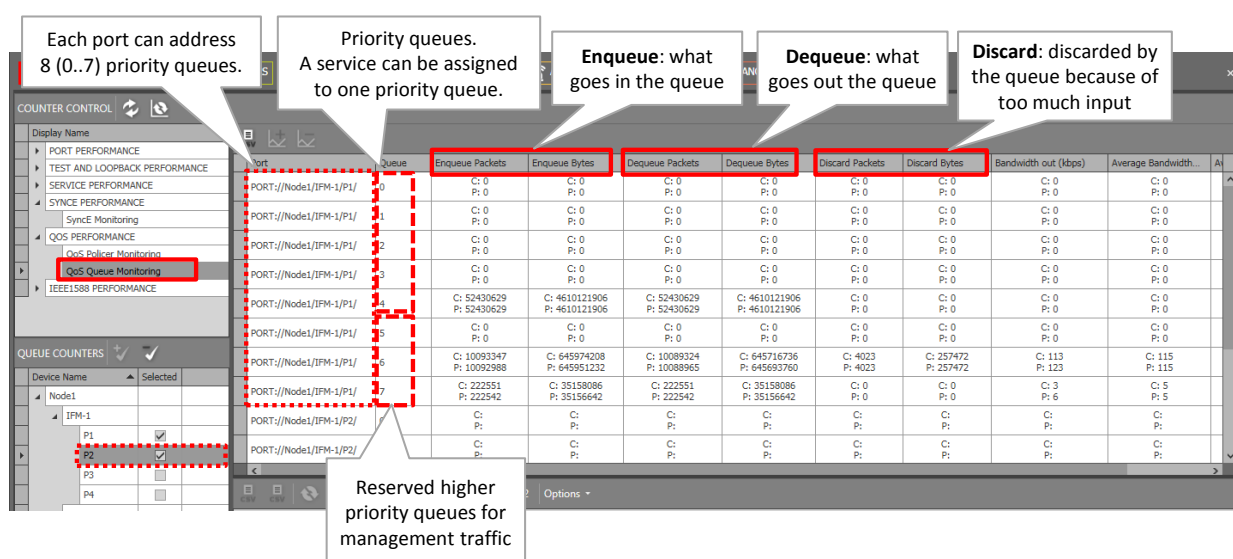



Figure 212 QoS Queue Monitoring

A detailed monitoring set-up description is similar to the description in §15.2.

Table 46 QoS Queue Monitoring Fields

Field (*)	Values	Description	Curative Action
Port	value	Monitored port	
Queue	queue number	Each port has 8 priority queues [0..7], 0 = lowest priority, 7= highest priority. The higher priority queues 6 and 7 are reserved for management traffic (management protocol, discovery), other priorities can be used for services or user data, see also §3.2.1.	
Enqueue Packets	packets	Number of packets going in the queue, ready and waiting for transmittal	
Enqueue Bytes	bytes	Similar to 'Enqueue Packets' but with bytes instead of packets.	

Field (*)	Values	Description	Curative Action
Dequeue Packets	packets	Number of packets going out of the queue and transmitted via the port	
Dequeue Bytes	bytes	Similar to 'Dequeue Packets' but with bytes instead of packets.	
Discard Packets	packets	Number of packets discarded/ignored/dropped when arriving at the queue, only in some special cases. Example: the measured average frame size is reasonably lower than the configured average frame size. In normal circumstances, this counter should not increase	Verify your configured average frame size in the service wizard (QoS details)
Discard Bytes	bytes	Similar to 'Discard Packets' but with bytes instead of packets.	Verify your configured average frame size in the service wizard (QoS details)
Bandwidth Out (kbps)	kbps	The outgoing bandwidth between the current and the previous measurement: [(CurrentBytesOut - PreviousBytesOut)/1000/TimeInterval] kbps.	
Average Bandwidth Out (kbps)	kbps	The average of the 5 latest 'Bandwidth Out' measurements. Every (manual) refresh is a new measurement.	
Average Frame Size Out (bytes)	bytes	The average frame size of frames that are transmitted on this port in the 5 latest measurements. Every (manual) refresh is a new measurement.	
<p>(*) Note: All fields are <u>egress</u> fields</p> <p>Note: Click the Refresh button for the latest results;</p> <p>Note: Clear the counter values by disabling and enabling the BERT via the Interface Module/port settings in the network hardware tile;</p> <p>Note: Clear the counter values by clicking ;</p> <p>Note: 'C' value in cell = current value; 'P' value in cell = previous value;</p>			

15.7 IEEE 1588 Performance

Once IEEE 1588 has been configured as described in §14, 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 §15.2.

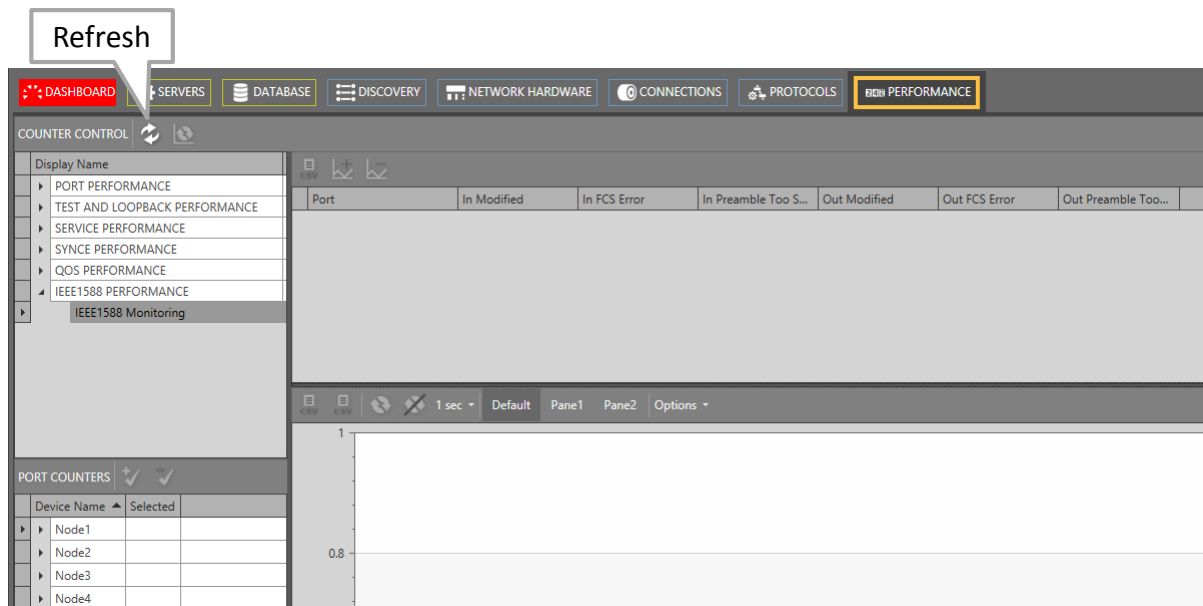



Figure 213 IEEE 1588 Monitoring

Table 47 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.	
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;			

15.8 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 §15.2.

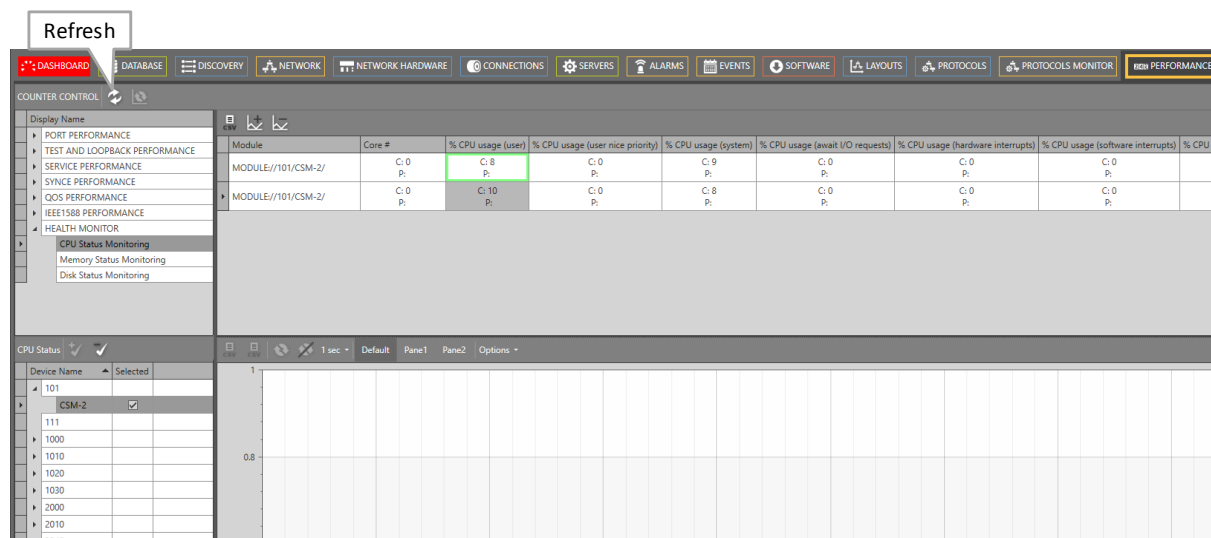


Figure 214 Health Monitor

Table 48 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 49 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 50 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;	

16. LOSS/DELAY/ASSURANCE MONITORING

16.1 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 §16.2;

Delay Measurement, see §16.3;

Tunnel Ping, see §16.4;

Tunnel Traceroute, see §16.4.3;

16.2 Loss Measurement (=LM)


16.2.1 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.

16.2.2 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;

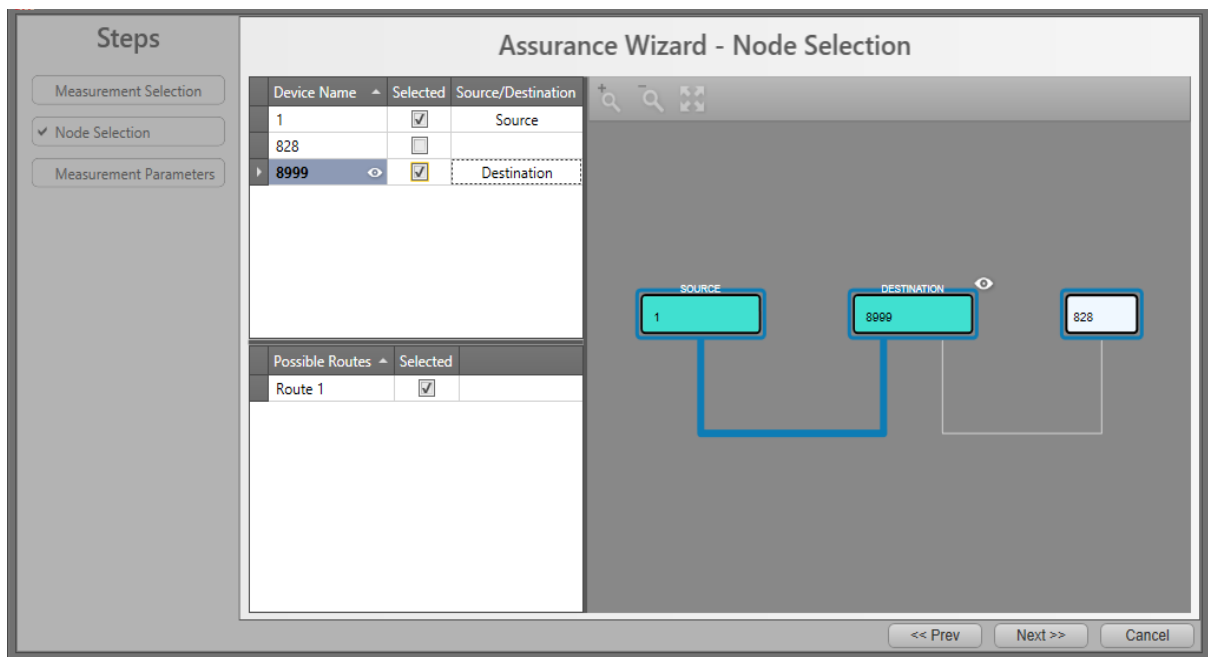




Figure 215 Assurance Wizard: Loss Measurement Configuration

16.2.3 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;

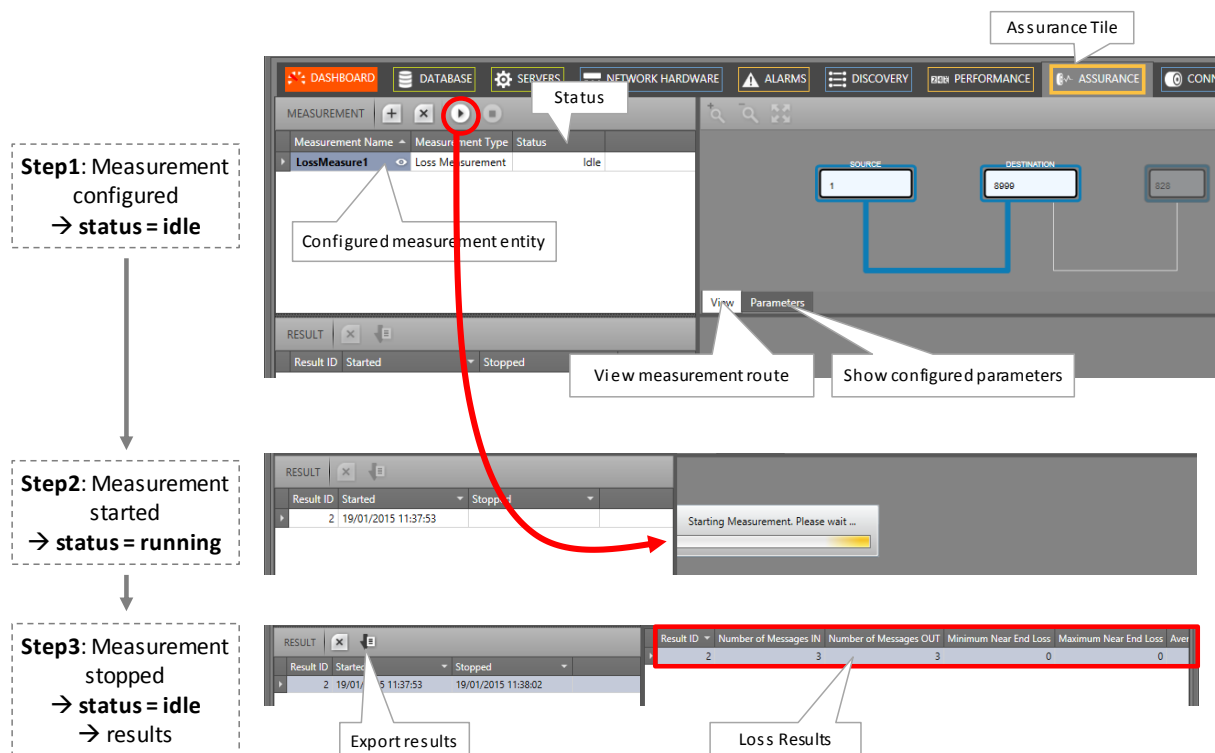


Figure 216 Loss Measurement in Operation

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 217 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 .

16.3 Delay Measurement (=DM)

16.3.1 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.

16.3.2 Configuration

Similar to the configuration of Loss Measurement, see §16.2.2;

Differences with Loss Measurement:

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

16.3.3 Operation

a. Single Measurement

Similar to Loss Measurement, see §16.2.3a;

b. Multiple Measurements

Similar to Loss Measurement, see §16.2.3b;

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 218 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 .

16.4 Tunnel Ping

16.4.1 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.

16.4.2 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. See also §3.2.1.

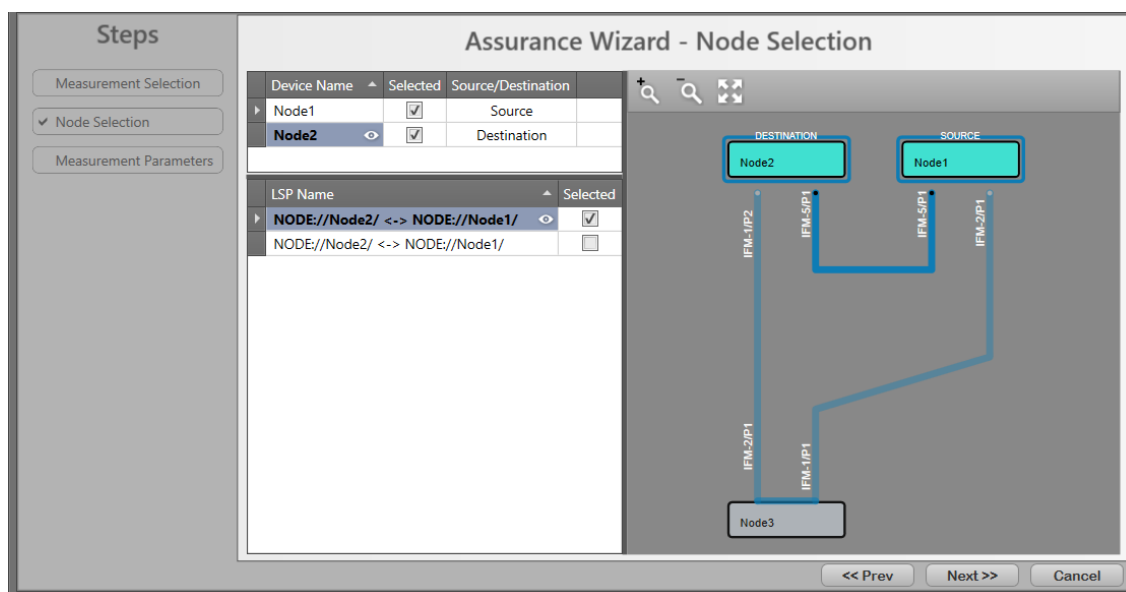


Figure 219 Assurance Wizard: Ping Measurement Configuration

16.4.3 Operation

a. Single Measurement

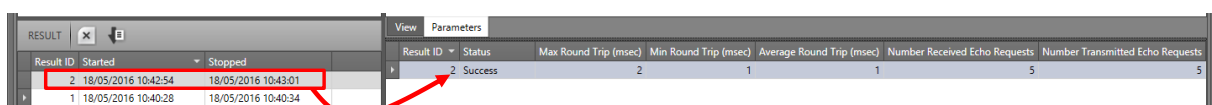
Similar to Loss Measurement, see §16.2.3a;

b. Multiple Measurements

Similar to Loss Measurement, see §16.2.3b;

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		
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

Parameters						
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 220 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 .

16.5 Tunnel Traceroute

16.5.1 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.

16.5.2 Configuration

Similar to the configuration of Tunnel Ping, see §16.4.2;

Differences with Tunnel Ping:

No TTL must be configured.

16.5.3 Operation

a. Single Measurement

Similar to Loss Measurement, see §16.2.3a;

b. Multiple Measurements

Similar to Loss Measurement, see §16.2.3b;

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:

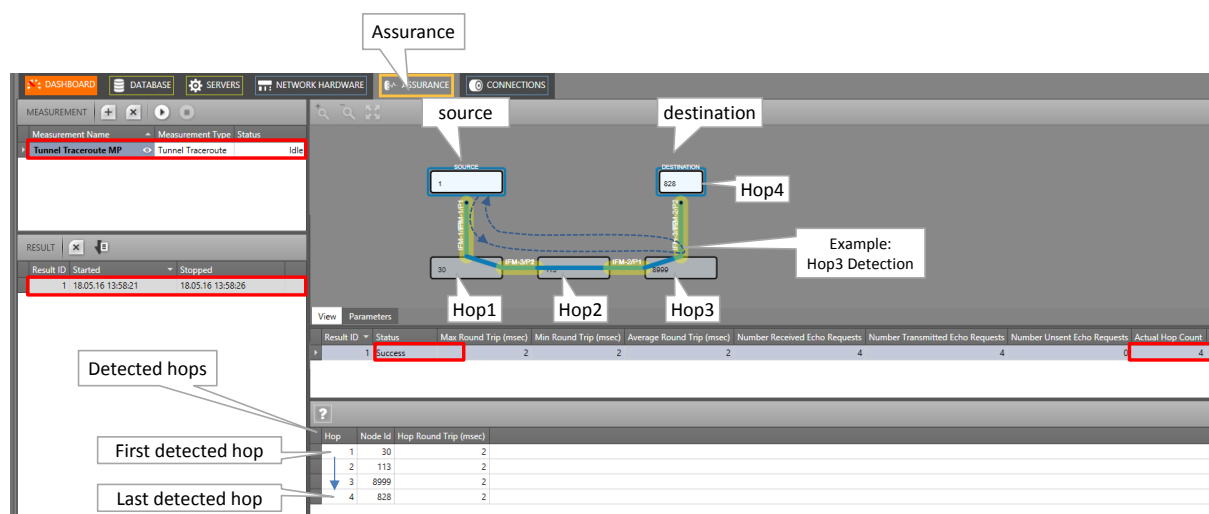




Figure 221 Traceroute Results Overview

Similar to the results of Tunnel Ping, see §16.4.3c. 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 .

17. REMOTE CLIENT/SERVER

17.1 General

Prerequisite: HiProvision must be fully installed on both the server and remote client PC;

Before a remote client/server system can be used or started, it must be configured first. This configuration depends on how the remote client is connected to the server. A remote client can talk to the server via:

the DCN Channel;

the DCN Channel with redundant discovery entry point;

a LAN:

- ▶ Programmed Ethernet service over the Dragon PTN network;
- ▶ connection via an external LAN;

§17.2 shows some example use cases, whereas §17.3 describes how to configure them.

Directly after this configuration has been done, the remote client/server system will be up and running automatically. Later on, if you have to start the remote client/server again after it was shut down, follow the steps in §17.4.

17.2 Example Use Cases

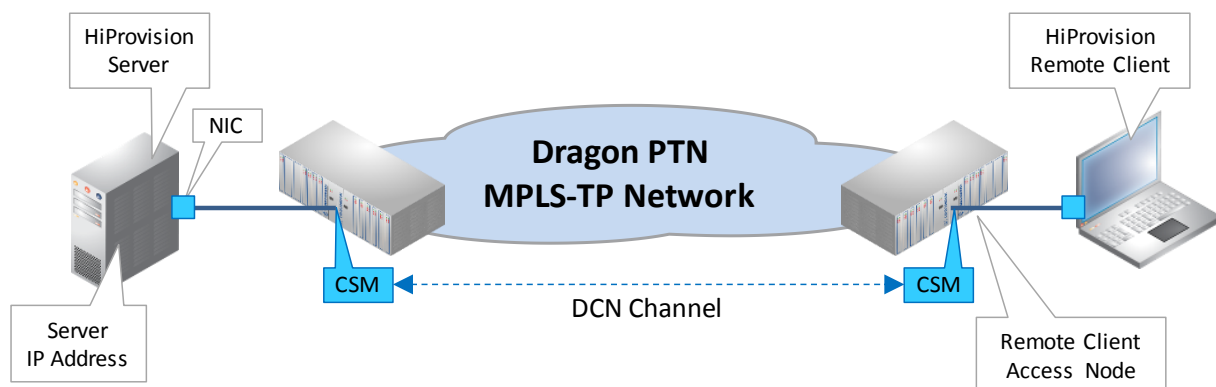


Figure 222 Client-Server Connection: DCN Channel

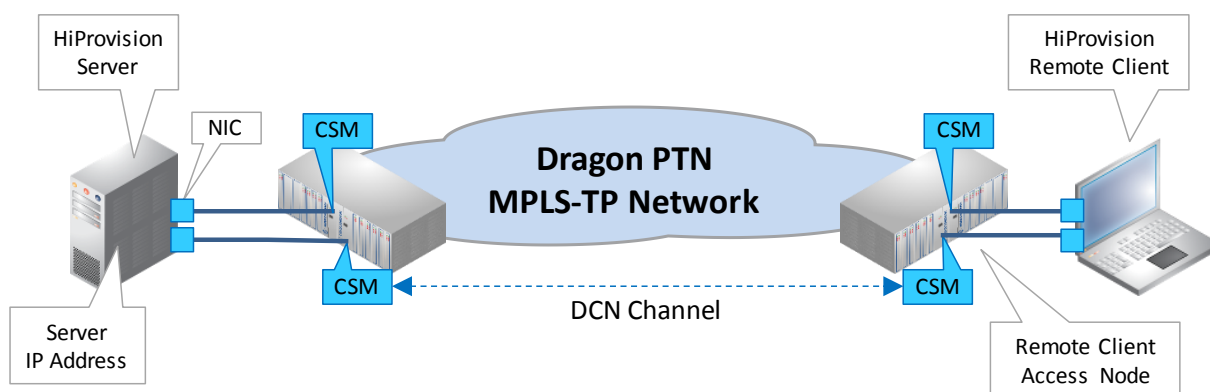


Figure 223 Client-Server Connection: DCN Channel with Redundant Discovery Entry Point

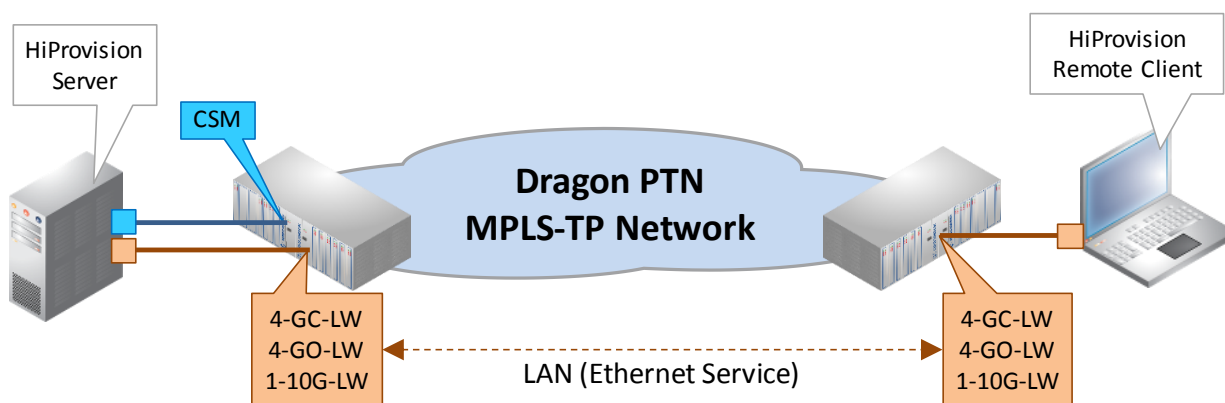


Figure 224 Client-Server Connection: LAN (Ethernet Service)

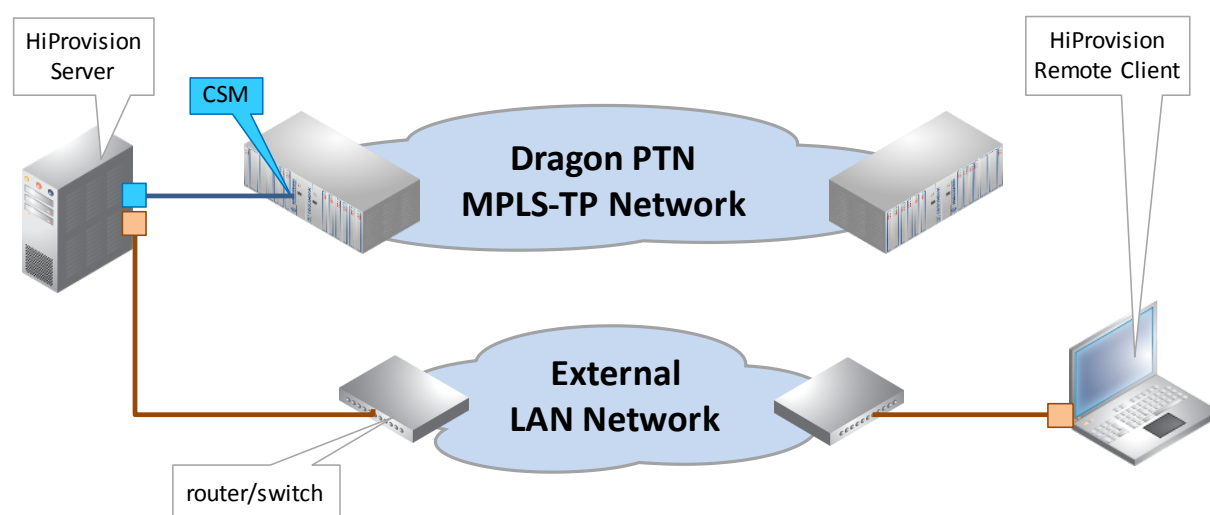


Figure 225 Client-Server Connection: LAN (External LAN)

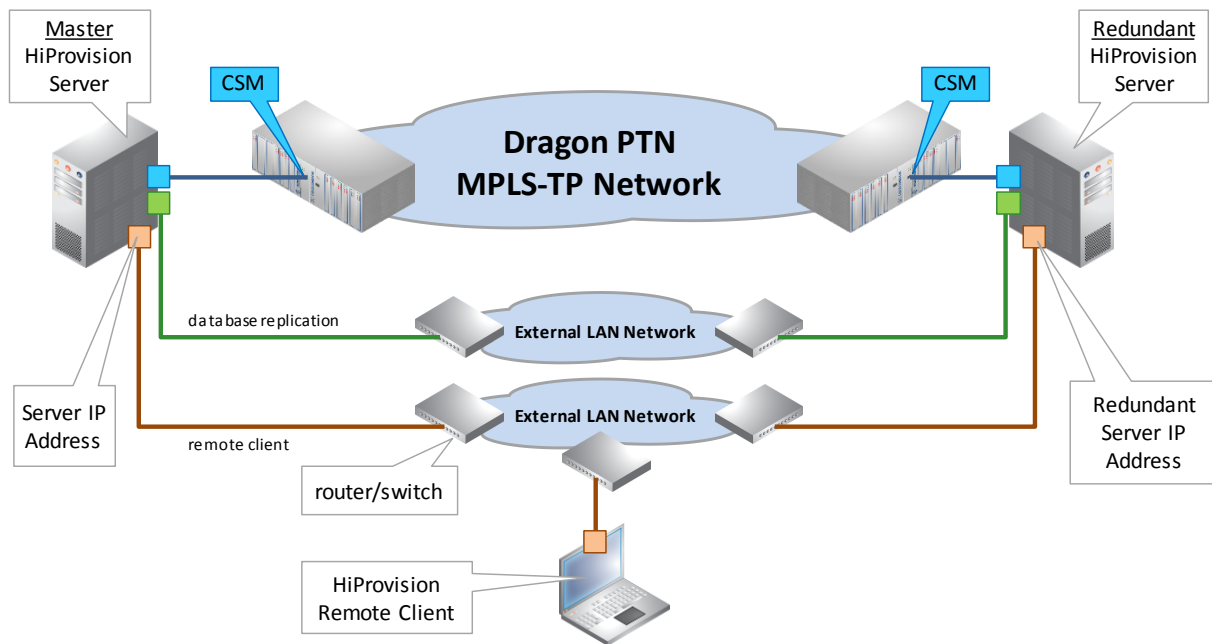


Figure 226 Client-Redundant Server Connection: LAN (External LAN)

17.3 Configuration

Follow the steps below to configure a remote client setup, first on the server PC and next on the remote client PC.


17.3.1 Step1: On the HiProvision Server PC

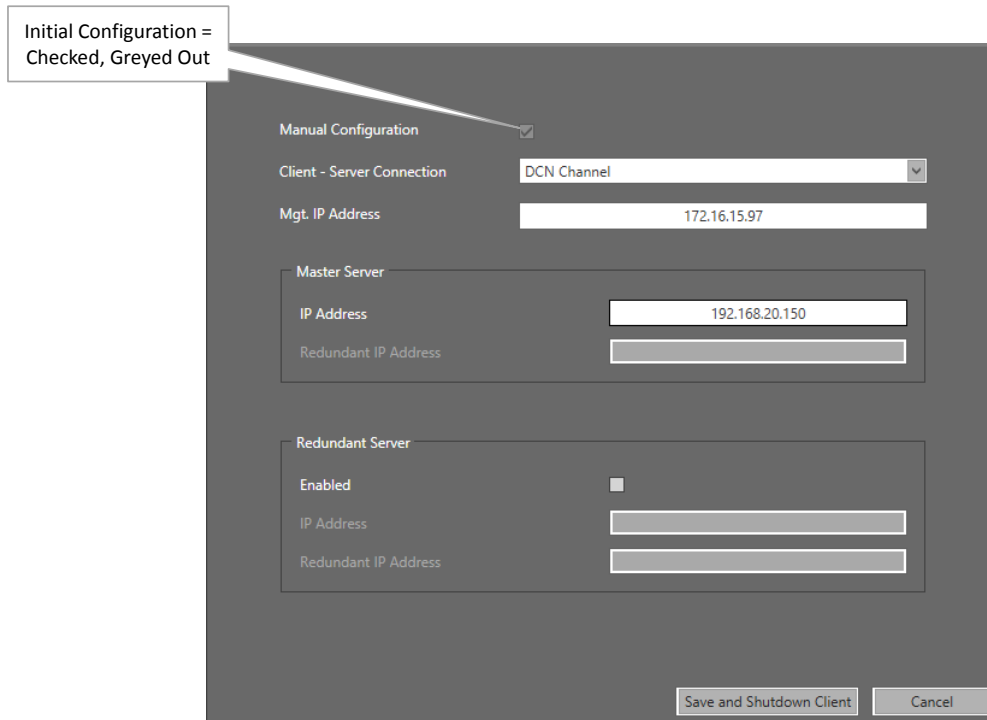
Prerequisites: HiProvision has been initialized, has discovered the network with the correct entrypoints (§2.6, §9) and is up and running (HiProvision Agent and Client have been started);

1. If the remote client must connect to the server via a LAN, provide an extra NIC on the server PC and connect this extra NIC to :
 - ▶ an Ethernet Port on an Interface Module to provide/use the Ethernet service (see §32);
 - ▶ an External LAN network in any other case;
2. If the remote client must connect to the server via the Dragon PTN network (with either one or two (=redundant) discovery entry points):
 - ▶ DCN Channel: Indicate the access nodes for the remote client via Dashboard → Servers Tile → ☒. Select the node(s) and click the ☒ button to make these nodes accessible via a CSM for the remote client;
 - ▶ Ethernet Service: program an Ethernet service between Interface Modules that support the Ethernet Service (see §32) to interconnect the HiProvision server(s) and the remote client;
3. Close the 'HiProvision Client', only the 'HiProvision Agent' is allowed to run;

17.3.2 Step2: On the HiProvision Remote Client PC

CAUTION: Do not start the 'HiProvision Agent', only the 'HiProvision Remote Client' is allowed to run on the remote client PC;

1. Start the 'HiProvision Remote Client' via double-clicking this icon on the desktop;
2. For a first time start of the 'HiProvision Remote Client', the connection with the server will fail;
3. The Servers tile is always unlocked, no need to log in yet;
4. In the Dashboard → Servers Tile, click the  button, the figure below pops up:



Initial Configuration = Checked, Greyed Out

Manual Configuration ☒

Client - Server Connection DCN Channel

Mgt. IP Address 172.16.15.97

Master Server

IP Address 192.168.20.150

Redundant IP Address

Redundant Server

Enabled ☐

IP Address

Redundant IP Address

Save and Shutdown Client Cancel

Figure 227 Remote Client Via DCN Channel

5. The 'Manual Configuration' checkbox is checked and greyed out for a first time configuration. The IP addresses have to be filled out manually. Later on, when the remote client has been configured and this setup is opened again, some IP addresses might be detected automatically in case of HiProvision Redundancy and Manual Configuration is unchecked.
6. Client - Server Connection:
 - ▶ LAN: Select this option when the remote client communicates to the server via an Ethernet service over the Dragon PTN Network or via an external LAN network. Make sure that this PC is connected to:
 - ▶ an Ethernet Port on an Interface Module that supports the Ethernet service (see §32);
 - ▶ an External LAN network in any other case;
 - ▶ DCN Channel: Select this option when the remote client PC is connected one CSM and using the DCN path to communicate to the server;

- ▶ DCN Channel with Redundant Discovery Entry Point: Select this option when the remote client PC is connected to two CSMs and using the DCN path to communicate to the server;
7. (Only with DCN Channel) Mgt. IP Address: Fill out the IP address of the node or the CSM to which the remote client PC has been connected;
 8. Master Server:
 - ▶ IP Address: IP address of the NIC in the HiProvision Server PC that is communicating with the Remote Client;
 - ▶ Redundant IP Address: (only when 'DCN Channel with Redundant Discovery Entry Point' was selected) IP address of the NIC in the HiProvision Server PC that is connected to the second CSM (=redundant entry point);
 9. Redundant Server:
 - ▶ Enabled: Check this checkbox if you have a redundant HiProvision server;
 - ▶ IP Address: IP address of the NIC in the Redundant HiProvision Server PC that is communicating with the Remote Client;
 - ▶ Redundant IP Address: (only when 'DCN Channel with Redundant Discovery Entry Point' was selected) IP address of the NIC in the Redundant HiProvision Server PC that is connected to the second CSM (=redundant entry point);
 10. Click Save and Shutdown Client. The client will shut down;
 11. Start the 'HiProvision Remote Client' via double-clicking this icon on the desktop;
 12. Log in;
 13. The connection between the remote client and server(s) should be OK and visible after clicking the Servers tile. Your remote client will be operational to manage the Dragon PTN network. Starting the Remote Client/Server system as described in §17.4 is not necessary anymore. If the remote client would not work, verify that some ports are not blocked by a possible firewall, see §38.5;

17.4 Switchover GUI View from Redundant HiProvision Servers

In case of redundant servers and having configured the remote Client as described in previous paragraphs, the logical setup can be viewed via Dashboard → Servers tile.

The green line or 'viewing line' from the Remote HiProvision Client to the Server indicates which server is being viewed in the Remote Client. In the figure example below, the Remote client is viewing the Master HiProvision Server.

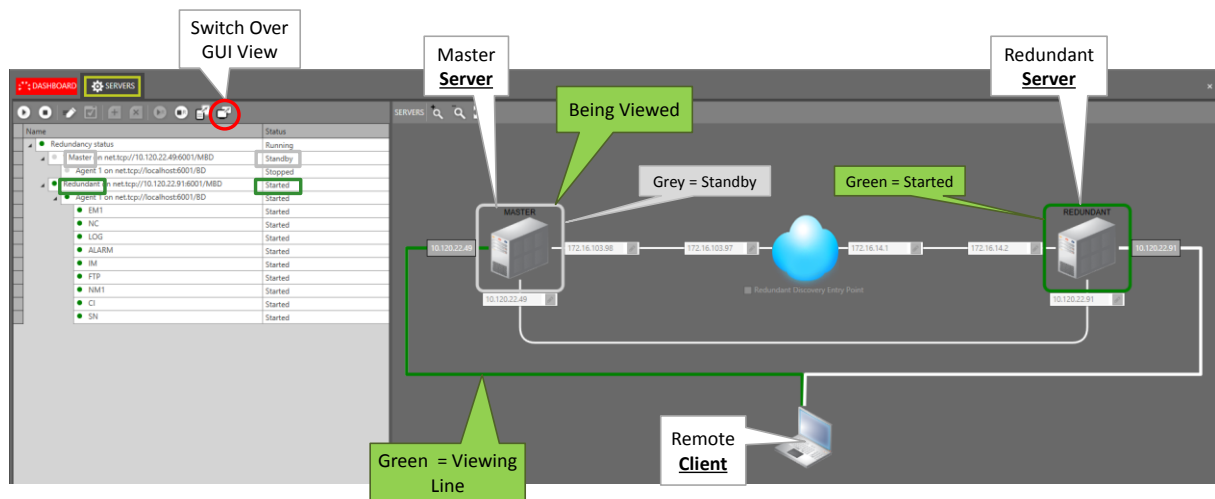



Figure 228 Remote Client Viewing Standby Server

The Master Server PC is in 'Standby' mode (= grey border). It is more interesting to view the 'Started' server PC (= green border). At this moment, the Redundant Server PC is the 'Started' one. Click the GUI switchover button  to make the remote client view the other server. As a result in this example, the remote client views the 'Started' server. It could look as follows:

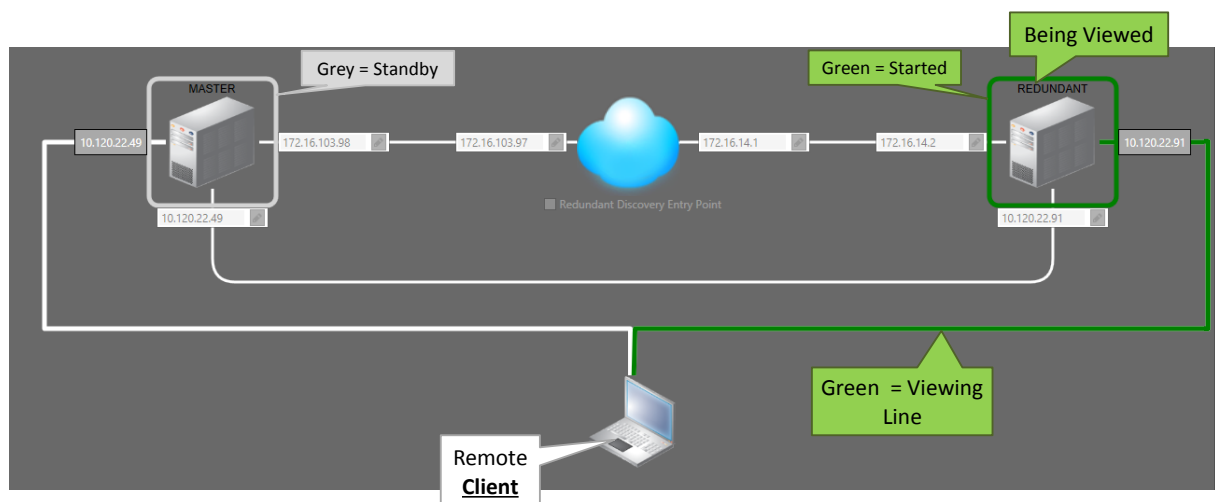


Figure 229 Remote Client Viewing Started Server

17.5 Start Remote Client/Server System

Prerequisite: the Client/Server system has been configured as described in previous paragraphs.

17.5.1 Step1: On the HiProvision (Master) Server PC

1. Start the 'HiProvision Agent' via double-clicking this icon on the desktop;
2. (The 'HiProvision Client' does not have to be started).

17.5.2 Step2: On the HiProvision Remote Client PC

1. Start the 'HiProvision Remote Client' via double-clicking this icon on the desktop;
2. A login window pops up, log in;
3. After logging in, your remote client will be operational to manage the Dragon PTN network.

NOTE: The same user cannot be logged in together on both the local (on the server PC) and the remote client (on the remote client PC) at the same time. The last login on one PC will automatically log off the same user on the other PC;

CAUTION: when a load is started in the configuration load manager (§5) in a client, all the other (remote) client GUIs will freeze (no user action possible) until the load has finished in the client that initiated the load action. A popup will be shown on the frozen GUIs as in the figure below.



Figure 230 Please wait until loading is done

18. TEST & LOOPBACK CONFIGURATION

18.1 General

Test and Loopback self-tests can be performed in all Circuit Emulation services (=CES) or in the 4-DSL-LW Ethernet service, e.g. when configuring or troubleshooting a service. The available self-test functions are listed below. Where these functions are supported is listed in Table 51.

Loopbacks: on backplane or front port both supporting two directions: towards line (=application) or network;

BERT: test traffic generation and verification = Bit Error Ratio Tester;

Tone Generation/Level Metering: test tone signal generation.

The table below shows which Interface Modules support the functionalities:

Table 51 Test & Loopback Support

Interface Module	Loopbacks		BERT		Tone Generation /Level Metering
	Backplane	Front Port	One Port per Interface Module	Per Port	
X = supported; --- = not supported					
PTN-4-E1-L/ PTN-4-T1-L	X	X	---	X	---
PTN-16-E1-L/	X	X	---	X	---

PTN-16-T1-L					
PTN-4-DSL-LW	---	X	---	---	---
PTN-2-C37.94	X	X	X (for C37.94 ports)	X (for E1/T1 ports)	---
PTN-7-SERIAL	X	X	X	---	---
PTN-4-CODIR	X	X	X	---	---
PTN-4-4WEM-L	X	X	---	---	X
PTN-2-OLS	---	X	X	X (for E1 ports)	---

18.2 Loopbacks

18.2.1 General

A loopback can be configured on the backplane (=Interface Module settings) or front port (=port settings). It just loops back the received traffic on an Rx pin towards its associated Tx pin on a specific port. If a backplane loopback has been configured enabled, all the ports on the Interface Module will be in loopback. Each loopback can be enabled towards the line interface (=application side) or network side. An overview can be found in the figure below.

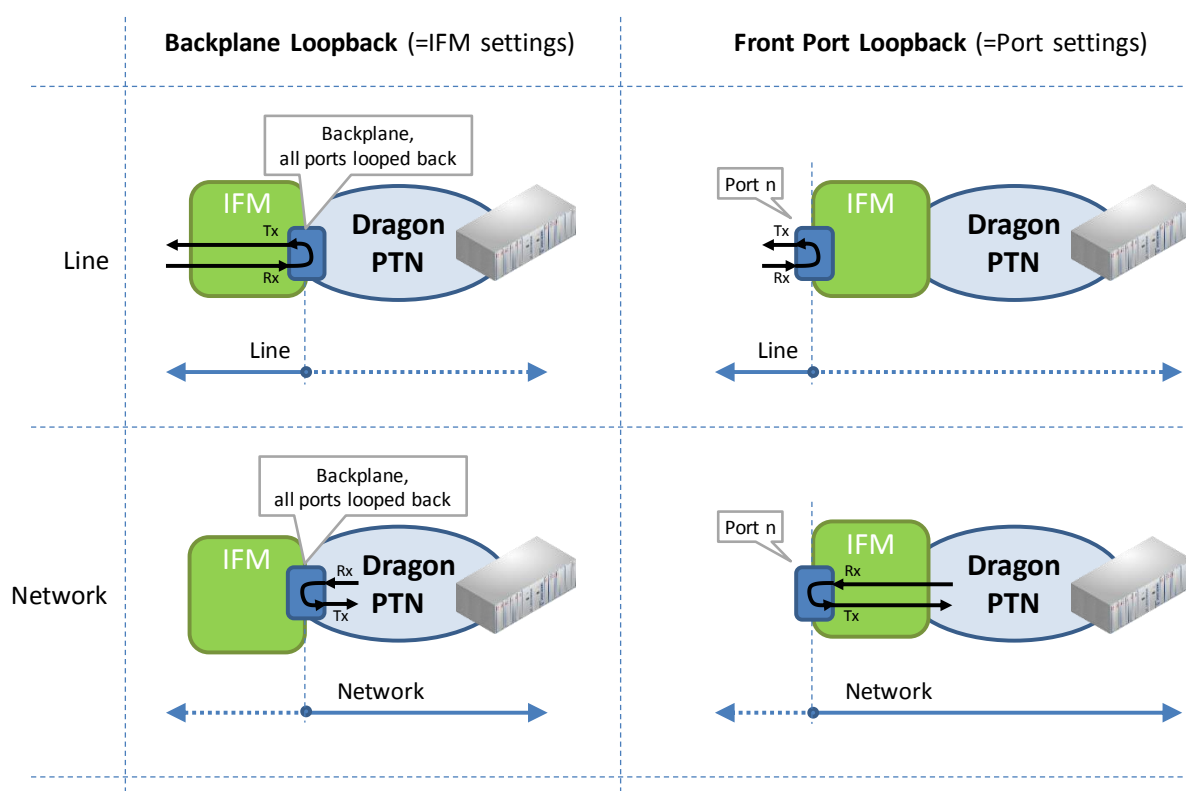


Figure 231 Loopback Functionality

18.2.2 Configuration

Go to Dashboard → Network Hardware and select a supported Interface Module or port (from Table 51) in the device list. The settings are shown in the 'Test and Loopback' section on the right-hand side. Always load the configuration into the network to activate it. Activating loopbacks will also generate a 'Test and Loopback active' alarm in HiProvision.

CAUTION: enabling/disabling loopbacks disables/resumes normal service traffic on a port. Verify alarms!

Table 52 Loopback Settings

Settings	Field	Values	Description
Interface Module(1)	Loopback Network Data	On/Off	Enable/Disable the backplane loopback towards the network. As a result, all/no ports in service will be looped back on the backplane!
	Loopback Line Data	On/Off	Enable/Disable the backplane loopback towards the line or application. As a result, all/no ports in service will be looped back on the backplane!
Port	Loopback(2)	Off Line Network	Off: Disable the front port loopback Line: Enable the front port loopback towards the line or application Network: Enable the front port loopback towards the network

Note: by default, all the loopbacks have been disabled
 (1): Supported on Interface Modules: PTN-4-E1-L/ PTN-4-T1-L, PTN-16-E1-L/ PTN-16-T1-L, PTN-2-C37.94, PTN-7-SERIAL, PTN-4-4WEM-L, PTN-4-CODIR, PTN-2-OLS.
 (2): Supported on ports on Interface Modules listed in (1), including the ports on the PTN-4-DSL-LW Interface Module. For PTN-7-SERIAL, this setting will only become visible after this port has been configured in a service.

18.3 BERT (=Bit Error Ratio Tester)

18.3.1 General

The BERT module allows the Interface Module to send test traffic on a selected service port towards the line interface (=application side) or network side. This module also allows to listen on a port for incoming test traffic and verify it.

The test results of the test traffic can be easily monitored via the 'Test & Loopback Performance' in the Dashboard → Monitoring → Performance tile, see also §Table 31.

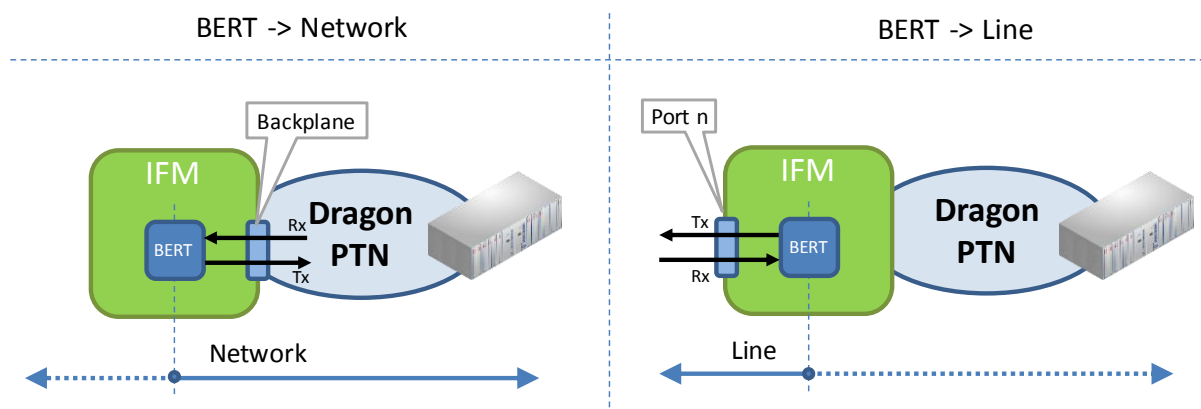


Figure 232 BERT Module

CAUTION: Enabling BERT to send test traffic on a service port will disable the normal service traffic on that port!

18.3.2 Configuration

To configure BERT, go to Dashboard → Network Hardware and select a supported Interface Module or port (from Table 51) in the device list. The BERT settings are shown in the 'Test and Loopback' section on the right-hand side. Always load the configuration into the network to activate them. Activating BERT will also generate a 'Test and Loopback active' alarm in HiProvision.

CAUTION: enabling/disabling BERT disables/resumes normal service traffic on a port. Verify alarms!

Table 53 BERT Settings

Settings	Field	Values	Description
PTN-2-C37.94 Interface Module	BERT Tx Direction	Port 1 Line Port 1 Network Port 2 Line Port 2 Network	Port n Line: If BERT is enabled, BERT module transmits test traffic towards the line or application side via port n Port n Network: If BERT is enabled, BERT module transmits test traffic towards the network side via backplane port n
	BERT Rx Direction	Port 1 Line Port 1 Network Port 2 Line Port 2 Network	Port n Line: If BERT is enabled, BERT module listens to the line or application side to receive and verify test traffic via port n Port n Network: If BERT is enabled, BERT module listens to the network side to receive and verify test traffic via backplane port n
	BERT Tx/Rx Enable	True/False	Enable/Disable both the transmit and receive functionality on the BERT module, only for the C37.94 ports, not for the E1 and T1 ports.
PTN-7-SERIAL Interface Module PTN-4-CODIR Interface Module PTN-2-OLS Interface Module	BERT Tx Direction	Line Network	Line: If BERT is enabled, BERT module transmits test traffic towards the line or application side via the BERT Tx Port (=front port) Network: If BERT is enabled, BERT module transmits test traffic towards the network side via the BERT Tx Port (=backplane port)
	BERT Tx Port	Port 1..4 (PTN-4-CODIR) Port 1,2,4,6 (PTN-7-SERIAL) Port 1,2 (PTN-2-OLS)	The port on which the BERT module will transmit test traffic either on the front or backplane port, based on the selected direction.
	BERT Rx Direction	Line Network	Line: If BERT is enabled, BERT module listens to the line or application side to receive and verify test traffic via the BERT Rx Port (=front port). Network: If BERT is enabled, BERT module listens to the network side to receive and verify test traffic via the BERT Rx Port (=backplane port).
	BERT Rx Port	Same ports as BERT Tx Ports	The port on which the BERT module will listen to receive test traffic and verify it. Either on the front or backplane port, based on the selected direction.
	BERT Tx/Rx Enable	True/False	True: BERT module will transmit test traffic on the Tx port and listen on the Rx port to verify incoming test traffic. False: BERT module will not transmit test traffic on the Tx port and not listen on the Rx port to verify incoming test traffic.
	BERT Bitrate (only CES on PTN-7-SERIAL and PTN-2-OLS Interface Module)	<value 1...n> PTN-7-SERIAL: n=24 PTN-2-OLS:	Set the bitrate for asynchronous CES. The resulting bitrate = n * 4800 bps. 4800 bps (with n=1) is ok if 1200 bps or 2400 bps are required. For synchronous CES, always the service bitrate is taken.

Settings	Field	Values	Description
		n=64	
E1/T1 Port (3)	BERT Pattern Select	PRBS 2e9-1 PRBS 2e11-1 PRBS 2e15-1 QRSS	PRBS = Pseudo Random Bit Sequence; Select which bit test pattern must be generated by BERT: PRBS 2e9-1 : Maximum of 8 consecutive zeros and 9 consecutive ones. Bit pattern length = 511 bits. PRBS 2e11-1 : Maximum of 10 consecutive zeros and 11 consecutive ones. Bit pattern length = 2047 bits. PRBS 2e15-1 : Maximum of 14 consecutive zeros and 13 consecutive ones. Bit pattern length = 32767 bits. QRSS (= Quasi Random Signal Source): Modified version of PBRS that allows 20 consecutive ones. Bit pattern length = 1048575 bits.
	BERT Tx/Rx Direction	Line Network	Line : If BERT enabled, BERT module transmits test traffic towards the line or application side and listens to the same side to receive test traffic and verify it. Network : If BERT enabled, BERT module transmits test traffic towards the network side and listens to the same side to receive test traffic and verify it.
	BERT Tx/Rx Timeslot	<number>	The number is a decimal representation of the timeslots that have BERT enabled. Each timeslot represents a bit of the 32/24 timeslots in E1/T1, with E1: timeslot 0, 1, ..., 31 = 1st, 2nd, ..., 32nd bit T1: timeslot 1, 2, ..., 24 = 1st, 2nd, ..., 24th bit Example1 : Enable BERT module on all E1 timeslots: Binary (32 bits): 1111 1111 1111 1111 1111 1111 1111 1111 Decimal = <number> = 4294967295 Example2 : Enable BERT module on E1 timeslots 1, 5, 6: Binary (32bits): 0000 0000 0000 0000 0000 0000 0110 0010 Decimal = <number> = 98
	BERT Tx Enable	True/False	BERT module will transmit/not transmit test traffic on the Tx port
	BERT Rx Enable	True/False	True : BERT module will listen on the Rx port and verify the incoming test traffic False : BERT module will not listen on the Rx port for incoming test traffic
<p>Note: by default, all the test traffic generation has been disabled</p> <p>(2): Only ports that are not configured yet in a Serial Ethernet service will show up</p> <p>(3): E1/T1 port on either PTN-4-E1-L/ PTN-4-T1-L, PTN-16-E1-L/ PTN-16-T1-L, PTN-2-C37.94 Interface Module or PTN-2-OLS</p>			

18.4 Tone Generator/Level Meter

18.4.1 General

Each port on the PTN-4-4WEM-L Interface Module has a test tone generator that can generate two tones: 1000 or 1500 Hz. Each PTN-4-4WEM-L Interface Module can measure an incoming voice signal on one selected port. The received voice signal level can be easily monitored via the 'Test & Loopback Performance' in the Dashboard → Monitoring → Performance tile, see also §15.3.4.

18.4.2 Configuration

Go to Dashboard → Network Hardware and select a PTN-4-4WEM-L Interface Module or port in the device list. The settings are shown in the 'Test and Loopback' section on the right-hand side. Always load the configuration into the network to activate them. Activating it will also generate a 'Test and Loopback active' alarm in HiProvision.

Table 54 Tone Generator/Level Meter Settings

Settings	Field	Values	Description
PTN-4-4WEM-L Interface Module	Level Meter Enabled	True/False	The signal level meter on the PTN-4-4WEM-L Interface Module will listen/not listen to an incoming voice signal on the selected port (Level Meter Port Selection).
	Level Meter Port Selection	Port1..4	Select the port which incoming voice signal must be measured. Example: test tones will be have approximately following levels: Test tone 1000Hz: 1V ptp @ 600 ohm results in -6.81dbm Test tone 1500Hz: 1.5V ptp @ 600 ohm results in -3.92dbm These measured levels can be viewed in §15.3.4.
PTN-4-4WEM-L Port	Tone Generator	No Tone Generator 1000 Hz /1500 Hz	No Tone Generator: Disable the test tone generation n Hz: The test tone generator will generate an n Hz test signal on this port

Note: by default, all the test tone generation has been disabled

18.5 Combined BERT / Loopback Example

In the example below, activating BERT on one side and activating port loopback on the other side sets up a test traffic flow through a configured CES in the Dragon PTN network. The results can be easily monitored in §15.3.5.

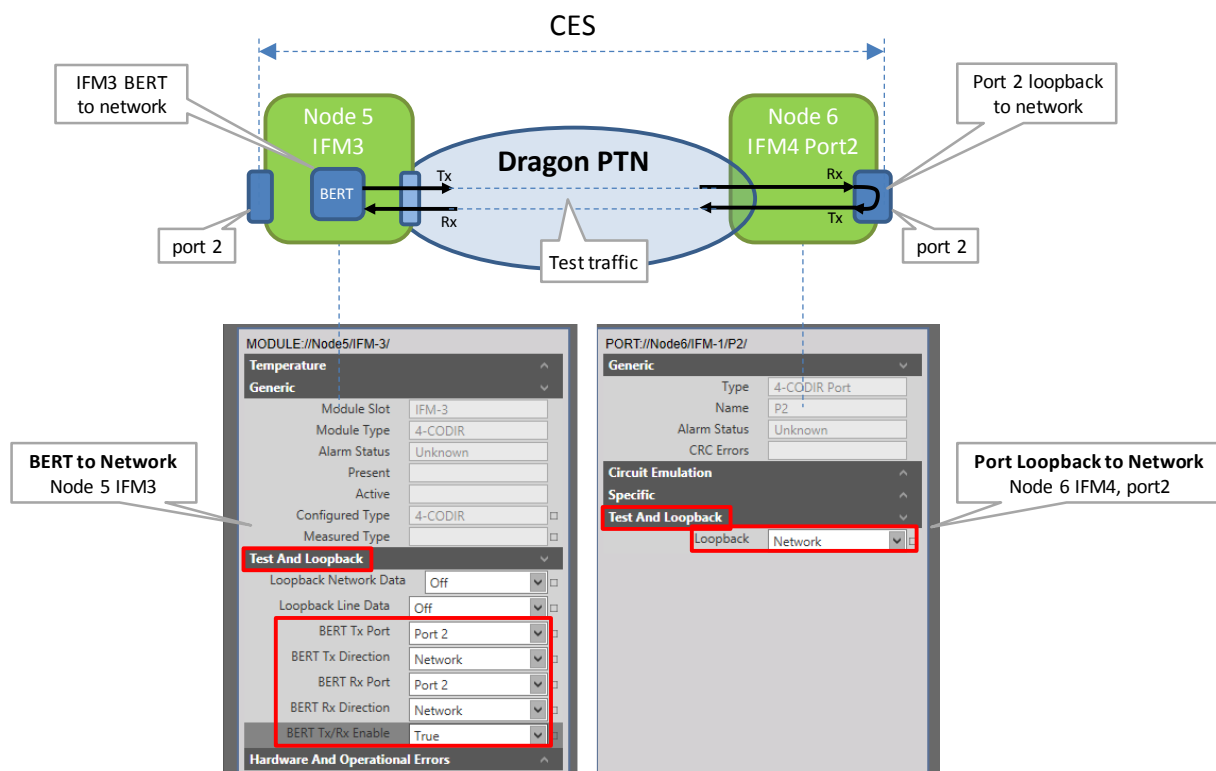


Figure 233 Combined BERT / Loopback

19. HELP

Clicking the Help tile on the dashboard shows an inline help function having listed all the Dragon PTN documentation (manuals, install guides, release note...) for this Dragon PTN release on the left-hand side. Click a document in the list to open it. Search and zoom functionalities are available. A maximum of 5 documents can be opened at the same time, each document in its own tab. In the figure example below, the 'Dragon PTN and HiProvision Operation manual' has been opened in the Tab.

NOTE: These documents are also located in:

<HiProvision Installation path>\HiProvision_V<version>\Documentation.

20. SERIAL KEY / VOUCHERS / LICENSE PACK

The licenses concept consists out of three parts:

Serial Key (see §20.1);
Voucher(s) (see §20.2);
License Pack (see §20.3);

How to deal with licenses can be found in:

Generate License Pack and Install in HiProvision (see §20.4);
Monitor Licenses in HiProvision (see §20.5);
Licenses Operation (see §20.6);

20.1 Serial Key

is required for the HiProvision installation and looks like 'N2-aaaa-aaaa-aaaa-aaaa-aaaa-aaaa';
is available for free via <https://hiprovision.hirschmann.com> → Shortcuts → Licenses
HiProvision → Serial Key;
must only be used for one unique single HiProvision installation;
is valid for future HiProvision upgrades on the same HiProvision PC.

20.2 Voucher(s)

is a unique number that grants the permission to use a specific node or run a specific feature within the Dragon PTN network for a specific major Dragon PTN Release (=Release Dependent, see §2.5.3);
must be purchased via Hirschmann Automation and Control GmbH;
▶ following vouchers types are available and must be purchased if needed:

Table 55 Available Vouchers

Voucher	Voucher Prefix	Release Dependent (*)	Amount
---------	----------------	-----------------------	--------

Voucher	Voucher Prefix	Release Dependent (*)	Amount
Dragon PTN R4.x: Node PTN2210	DRX40	Yes	1 Per Node
Dragon PTN R4.x: Node PTN1104	DRX41	Yes	1 Per Node
Dragon PTN R4.x: Node PTN2206	DRX42	Yes	1 Per Node
Dragon PTN R4.x: Node PTN2209	DRX43	Yes	1 Per Node
Dragon PTN Upgrade: Node PTN2210	DRX90	No	1 Per Node
Dragon PTN Upgrade: Node PTN1104	DRX91	No	1 Per Node
Dragon PTN Upgrade: Node PTN2206	DRX92	No	1 Per Node
Dragon PTN Upgrade: Node PTN2209	DRX93	No	1 Per Node
CSM Redundancy	DRX0	No	1 Per CSM Redundant Node
HiProvision Redundancy	DRX1	No	1 Per Serial Key
HiProvision Add-on: SNMP NorthBound	DRX2	No	1 Per Serial Key
HiProvision Add-on: CAR IP	DRX3	No	1 Per Serial Key
HiProvision Add-on: Generic Reporting Engine	DRS3	No	1 Per Serial Key
Large Network Monitor	DRS2	No	1 Per Serial Key
OTN Device	DRO0	No	1 Per OTN Device
Hirschmann Device	DRH0	No	1 Per Hirschmann Device
Generic Device	DRS1	No	1 Per Generic Device
Dragon PTN R4.x Chinese Language	DRL40	Yes	1 Per Serial Key
Dragon PTN Upgrade: Chinese Language	DRL90	No	1 Per Serial Key
Dragon PTN R4.x German Language	DRL41	Yes	1 Per Serial Key
Dragon PTN Upgrade: German Language	DRL91	No	1 Per Serial Key
Dragon PTN R4.x Polish Language	DRL42	Yes	1 Per Serial Key
Dragon PTN Upgrade: Polish Language	DRL92	No	1 Per Serial Key
(*) Release Dependent (Yes/No): Yes: These vouchers will work in all the major Release not higher than the mentioned Major Release (e.g. R4.x), upgrading to a higher future major release later on (e.g. R5.x) requires to purchase the vouchers again for the new major release or to purchase Upgrade vouchers or having a Total/Software Care contract; No: These vouchers will work in any Dragon PTN Version;			

will be sent to you in an email after having it purchased;

always looks like '<Voucher Prefix>-aaaa-aaaa-aaaa-aaaa-aaaa';

E.g. **DRX40**-1234-5678-9012-3456-7890-1234 represents a voucher for the **PTN2210** node for Dragon PTN Release 4.x.

20.3 License Pack

is a unique '*.dat' file including your Serial Key and vouchers;

is generated via <https://hiprovision.hirschmann.com> → Licenses HiProvision → Get License Pack based on your Serial Key and Vouchers;

grants HiProvision the permission to manage/monitor nodes and features in the live network;

must be placed in the License folder on the HiProvision PC;

20.4 Generate License Pack and Install in HiProvision

NOTE: Offline configuration in HiProvision can be done without a License Pack. When going online (connect to nodes in the live network), a License Pack is required.

1. If there is no license pack installed yet, the Licenses tile shows 'No License Pack';
2. Generate the license pack via <https://hiprovision.hirschmann.com> → Licenses HiProvision → Get License Pack;
3. You will receive a license pack (*.dat file) via mail (or directly via download);
4. Save the license pack in the license folder (see Licenses Tile) on the HiProvision PC. In case of HiProvision Redundancy, save the license pack on both PCs;

CAUTION:

Only one License Pack or '*.dat' file is allowed in the license folder. Make sure to remove the old License Pack when replacing it by a new one.

5. Stop and restart the Servers;
6. HiProvision reads out the license pack in the license folder and updates its license information on the tile and behind the tile.

20.5 Monitor Licenses in HiProvision

Example: We have a network with 4 'PTN2210' nodes and configured it in HiProvision. We purchased 1 voucher for an PTN2210 node, 1 voucher for an PTN2206 node and 2 vouchers for an PTN1104 node. Furthermore, we tried to 'connect' (see §20.6) all the nodes in the live network.

Result: there are 4 'PTN2210' nodes, which means that 4 'PTN2210' vouchers are required (=Vouchers Required). Only 1 voucher is purchased (=Vouchers Available) for this type of node. It means that only 1 of 4 nodes can be connected (=Vouchers Used) and 3 extra vouchers must be purchased to connect all the nodes. No 'PTN2206' and 'PTN1104' nodes are configured, so none of these vouchers are required or used.

NOTE: The hardware configuration can be verified via the Network Hardware tile;

NOTE: Only as many nodes can be connected as there are Vouchers Available;

NOTE: Also the Serial Key used during installation, License folder and License Pack (=license file) are shown;

Click on the License tile to see all the voucher and license info of your system:

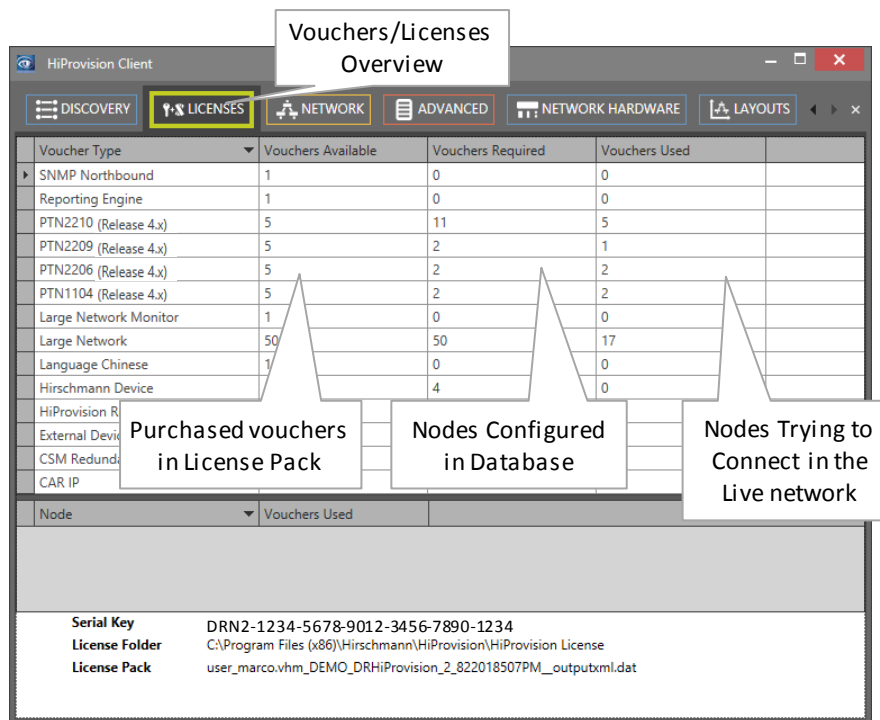


Figure 234 Vouchers/Licenses Overview1

Clicking on a voucher type in the list, shows the nodes that need such a voucher type to get online or connected. HiProvision cannot monitor or manage a live node if it cannot connect to it.

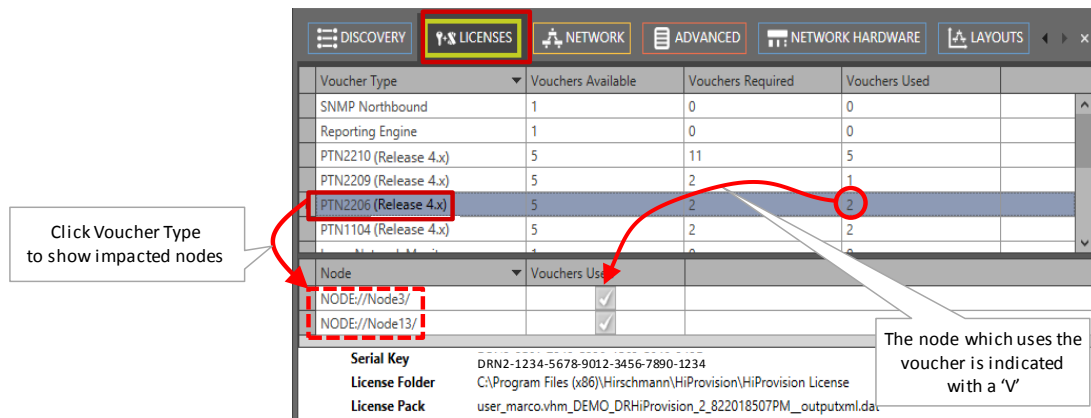


Figure 235 Vouchers/Licenses Overview2

20.6 Licenses Operation

When the operator goes online via a 'connect', HiProvision verifies the all the voucher/license info.

Enough node vouchers available for all nodes:

- ▶ if a voucher is available for each configured node, HiProvision can connect to each node and the entire live network can be managed/monitored. Both 'connect' (↔) or 'connect all' (↔) buttons in the 'Network Hardware' tab can be used to go online.

Not enough node vouchers available for all nodes:

- ▶ Make sure that tunnel and service configuration is limited to only those nodes that will use the voucher. Use 'connect' (↔) to connect each of these nodes with a voucher individually. Do not use a 'connect all' (↔) which will connect nodes randomly;
- ▶ The live nodes that have a voucher can be managed/configured by HiProvision;
- ▶ A major '**License Alarm**' will be raised when you configure offline/online more nodes (=required vouchers) in HiProvision than you have vouchers purchased (=available vouchers) (*);
- ▶ A '**Node Connect Failed**' pop-up will show up when you try to connect online more nodes (=used vouchers) than you have vouchers purchased (=available vouchers) (*). HiProvision only connects as many nodes as there are vouchers available. Only the connected nodes can be managed/monitored. A 'connect all' will try to connect all the nodes;

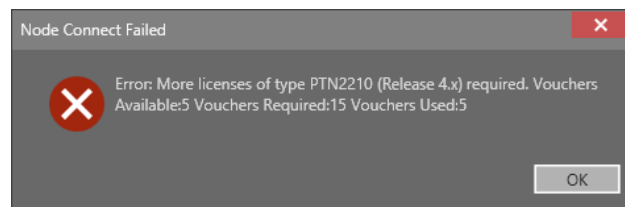


Figure 236 Connect: Not Enough Vouchers

NOTE: (*): Not having enough LNM vouchers will not raise alarms but generate a license error message instead as shown in Figure 268.

21. POWER OVER ETHERNET (POE)

21.1 General

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

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

Electrical RJ45 ports of the Interface Modules that support PoE (see §32) in the Dragon PTN nodes are able to deliver PoE when external PoE PSUs are connected to the NSM-A (**).

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

If PoE is needed:

Connect PoE hardware, see §21.2;

Configure PoE settings, see §21.3;

- ▶ Status info on the running PoE, see §21.4;

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

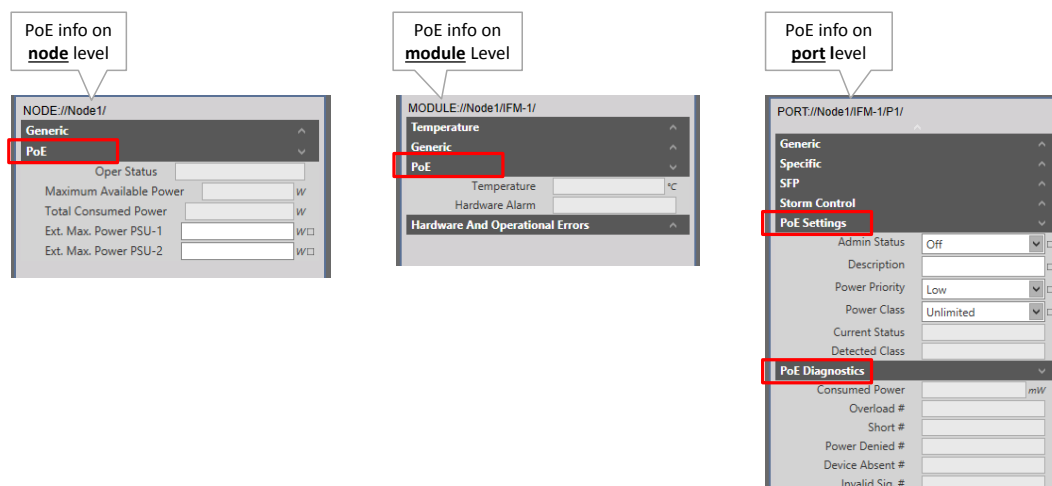


Figure 237 PoE Info on Node/Module/Port Level

21.2 Connect PoE Hardware

1. Connect external PoE PSUs to the NSM-A in the node as described in Ref.[2];
2. Connect the PDs to the PSEs, the PSEs are the electrical RJ45 ports on Interface Modules that support PoE (see §32);

21.3 Configure PoE

The PoE settings that can be configured in Figure 237 are explained in the table below. The configuration must be done on node and port level.

Table 56 PoE Configuration Parameters

Level	Parameter	Values	Description
Node: PoE Information	Ext. Max. Power PSU-1/ Ext. Max. Power PSU-2	<value>	PoE PSU1 = PSU connected to PoE1 connector on the NSM-A; PoE PSU2 = PSU connected to PoE2 connector on the NSM-A; These fields represent the power (in Watt) delivered to the node by the PoE PSUs: If PoE PSU1 is used, fill out Ext. Max. Power PSU-1; If PoE PSU2 is used, fill out Ext. Max. Power PSU-2; ATTENTION: Follow the configuration rules below §21.4:
Port: PoE Settings	Admin Status	On/Off	On: Enables PoE on this port. It still depends on the Power Priority, Classes and Budgets whether power will be delivered effectively. Off: Disables PoE on this port.
	Description	<text>	Port description e.g. 'Camera parking1'
	Power Priority	Low/ High/ Critical	Assigns a Power Priority for PoE to the port. 'Critical priority' ports will always get power first, 'Low priority' ports will always get power as last. 'High priority' is in between. If it

			concerns ports with the same Power Priority, the lowest port numbers on the lowest Interface Module numbers will get power first.
	Power Class	Unlimited Class 1 Class 2 Class 3/0 Class 4	<p>Configure the desired power class for this PoE port, according to the configuration rules in §21.4: A connected PoE device to this port will always get power, but never more than the configured Power Class. Use Unlimited (=40W) when you don't know yet the Power Class of the connected device (=Detected Class). As a result, the device will always get power, and its power class can be detected. When it has been detected, the administrator can change Unlimited into the same class as the Detected Class.</p> <p>According to the configured Power Class, following power levels are delivered at the PoE ports by the node (=PSE side) :</p> <p>Class 0: 15.4 Watt Class 1: 4.0 Watt Class 2: 7.0 Watt Class 3: 15.4 Watt Class 4: 32.0 Watt Unlimited: 40.0 Watt.</p>

21.4 PoE Configuration Rules

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

21.4.1 Only one PoE PSU Connected

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

- Node: Fill out 300W in 'Ext. Max. Power PSU-1';
- Ports: Configure the desired Power Class on the desired ports in the node. Make sure to configure a maximum of $300W - 30W = 270W$ on these ports. 30W is reserved for internal use. E.g. you could configure 8 ports in Class4 ($8 \times 32.0 = 256W$) and 1 port in Class 2 ($1 \times 7.0 = 7W$) $\rightarrow 256 + 7 = 263W < 270W$;

Configuring more than 270W on the ports is NOT allowed!

21.4.2 Two PoE PSUs Connected

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

a. Lowest Power Example

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

b. Power Calculation Example

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

- ▶ Node: Fill out 300W in 'Ext. Max. Power PSU-1' and 480W in 'Ext. Max. Power PSU-2';
- ▶ lowest power = 300W;
- ▶ Ports: Configure the desired Power Class on the desired ports in the node. Make sure to configure a maximum of $\text{lowest PSU power} - \text{internal power} = 300\text{W} - 30\text{W} = 270\text{W}$ on these ports. 30W is reserved for internal use. E.g. you could configure 8 ports in Class4 ($8 \times 32.0 = 256\text{W}$) and 2 ports in Class 2 ($2 \times 7.0 = 14\text{W}$) $\rightarrow 256 + 14 = 270\text{W} \leq 270\text{W}$;

Configuring more than 270W on the ports is NOT allowed!

21.5 PoE Status

The PoE status info available in Figure 237 is explained in the table below:

Table 57 PoE Status Info

Level	Parameter	Values	Description
Node	Oper Status	On/Off/Faulty	On: PoE module is up and running Off: PoE module is down Faulty: No PoE is delivered due to a failure
	Maximum Available Power	<value>	The total power (in Watt) that the node can deliver. If two PoE PSUs are connected to the NSM-A, it will be the lowest value of both 'Ext. Max Power PSU-1' and 'Ext. Max Power PSU-2' values filled out.
	Total Consumed Power	<value>	The total PoE power (in Watt) that all the ports together in the node deliver, e.g. if 4 cameras are connected to 4 ports, each consuming 5 Watt, then the Total Consumed Power will be $4 \times 5\text{W} = 20\text{W}$ for this node.
Module	Temperature	<value>	The temperature of the PoE chip in °C.
	Hardware Alarm	OK/PoE Alarm	OK: no alarm on the PoE chip, everything fine PoE Alarm: PoE chip failure, reboot the Interface Module, replace the Interface Module if the failure persists.
Port: PoE Settings	Current Status	Disabled Searching DeliveringPower Fault OtherFault Testing	Searching: The Node is checking the connected Power Device (PD) before power delivery. The node negotiating the class, priority... No power is delivered yet to the PD. DeliveringPower: There is enough power budget left to deliver power to this PD, the node is really delivering power to the PD. Fault: There is an external problem on the PoE line or port, e.g. the PD requests power beyond its allowed power range. No power is delivered to the PD. OtherFault: PoE chip has been disabled due to external power problem. Testing: Port in test mode.
	Detected Class	Class 0 Class 1 Class 2 Class 3 Class 4	The measured or detected power class of the connected PoE device (PD). By default, when no PoE device is connected yet, 'Class 0' is indicated. When the PoE device (e.g. Class 2) is connected afterwards, its Power Class (Class 2) will be indicated. Afterwards, when the PoE device has been removed, the last remembered Power Class (Class 2) is still displayed, although no device is connected at that time.
Port: PoE Diagnostics	Consumed Power	<value>	The consumed power in milliWatt that the power device (PD) currently is consuming.

Level	Parameter	Values	Description
	Overload #	<value>	The number of overload conditions so far. Each time the PD on this port asks more power than its configured class allows, the counter increases with one.
	Short #	<value>	The number of shortcut conditions on this port so far.
	Power Denied #	<value>	The number of times that power delivery has been denied on this port.
	Device Absent #	<value>	The number of times that power has been removed because a powered device dropout was detected.
	Invalid Sig. #	<value>	The number of times that an invalid signature on PD has been detected. A signature indicates that a PD is a valid PD or not.

22. SUBRINGS

22.1 General

A 'Logical Ring' tunnel can have a maximum of 16 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 §3.9.2.

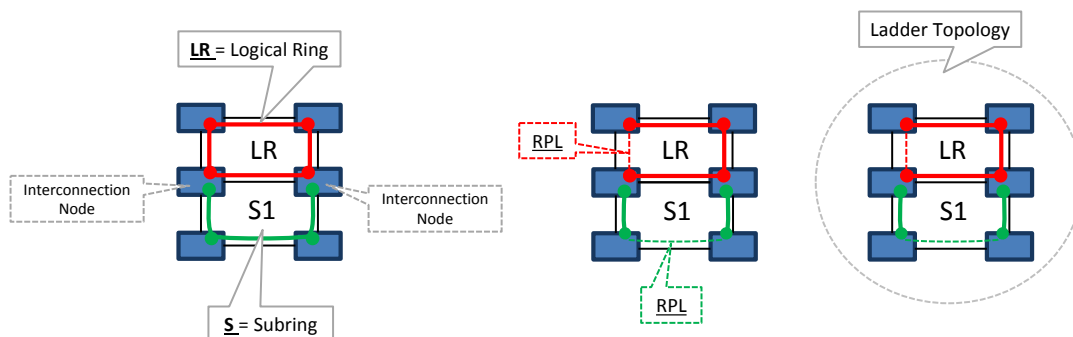


Figure 238 Logical Ring / Interconnection Nodes / Subring / Ladder Topology

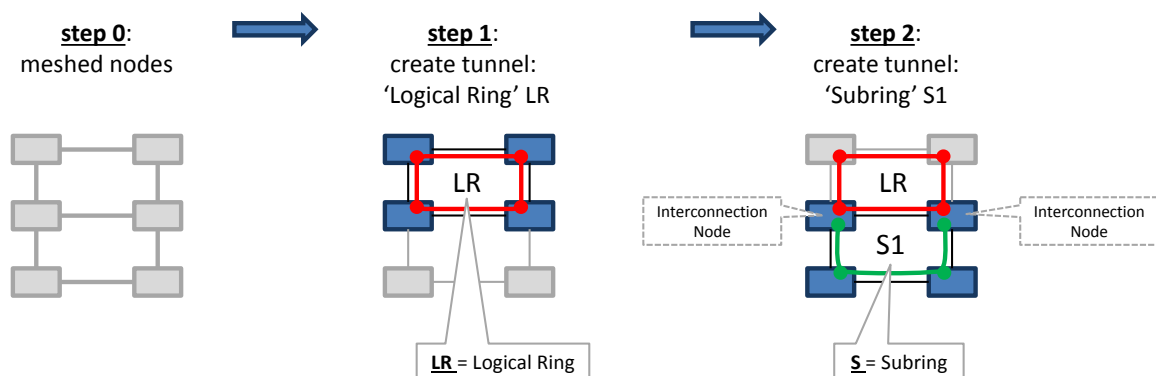


Figure 239 Logical Ring / Subring Setup

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 a another Subring color:

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

Figure 240 Subring Colors

A Logical Ring:

can nest subrings maximum 3 levels deep (Logical Ring not included);

► can have maximum 5 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.

22.2 Ladder Topology Examples

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

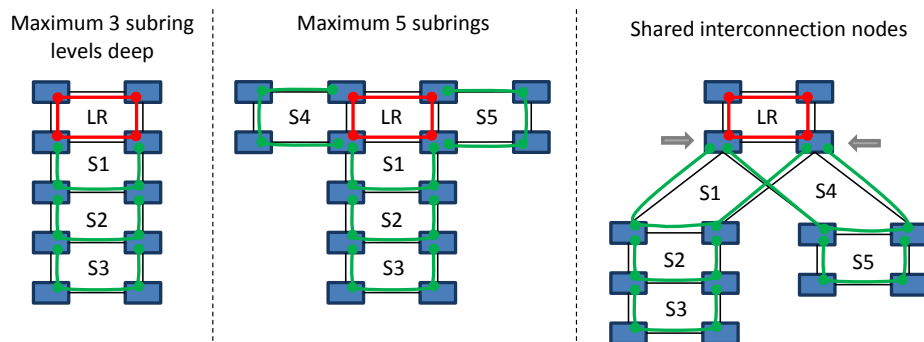


Figure 241 Ladder Topology Example 1

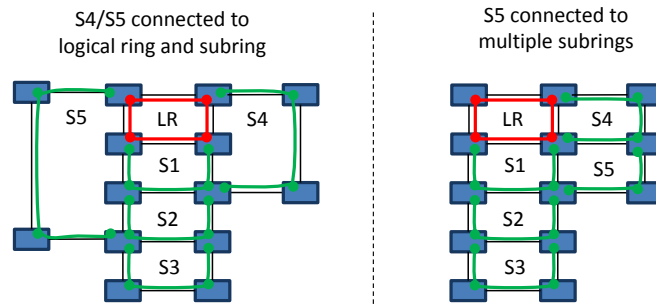


Figure 242 Ladder Topology Example 2

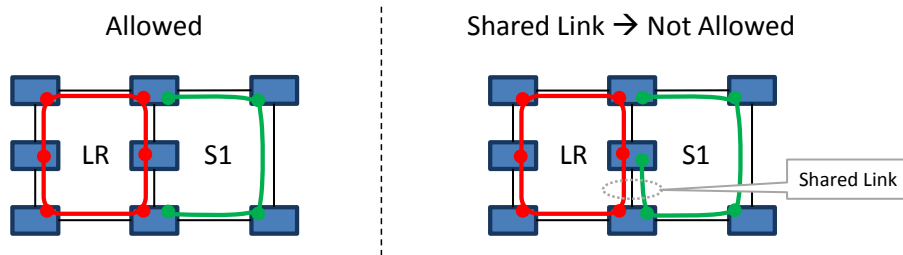


Figure 243 Ladder Topology: Not Allowed: Shared Link

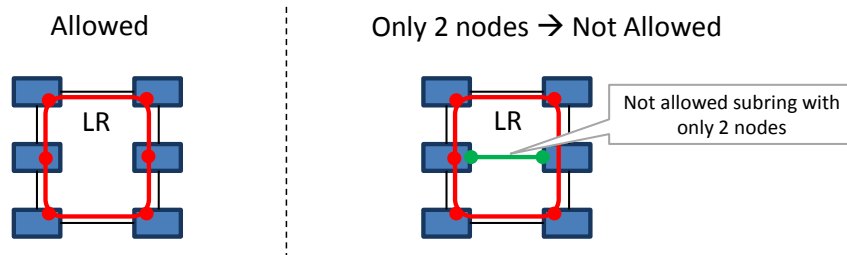


Figure 244 Ladder Topology: Not Allowed: Only 2 Nodes in Subring

22.3 Protected Tunnels

The working path and protection path in a protected tunnel are visualized in §4.6.5.

23. SMART SFP

23.1 General

Smart SFP is a hot-pluggable optical transceiver that converts incoming STM/OC frames from a fiber-optic SDH/SONET network into Ethernet frames or vice versa for outgoing frames. This conversion occurs at ports or Interface Modules that support smart SFP, see §32.

Smart SFPs must be used in a point-to-point (1st/2nd Smart SFP, see figure below) port based Ethernet service over Dragon PTN.

As a result, Dragon PTN allows to transparently transport synchronous digital bit streams from an SDH/SONET network via the Interface Modules that support smart SFP. The available Smart SFPs can be found in Ref. [14] in Table 1.

For clocking/synchronization, SyncE (see §13) must be configured in the nodes that have Smart SFPs plugged in.

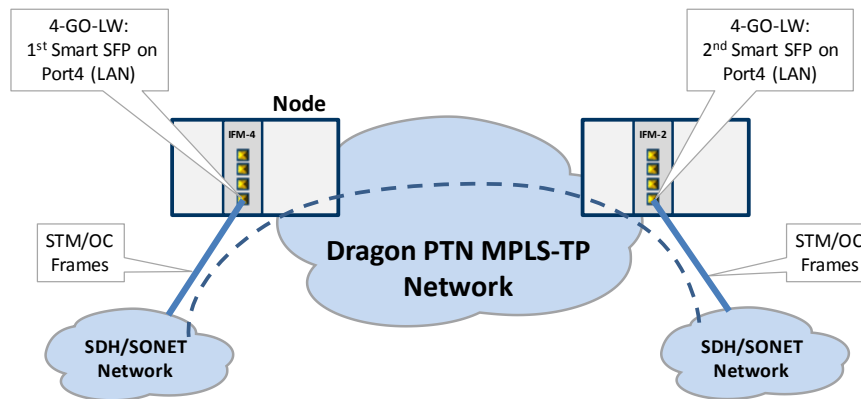


Figure 245 Example: Smart SFPs Setup / PTP

23.2 Configuration

Prerequisite: Make sure to have two Smart SFPs (with the right speed, see Ref. [14] in Table 1) plugged in somewhere in the Dragon PTN network an Interface Module that supports smart SFP. These ports must have been configured as LAN port.

1. Configure SyncE in the nodes that have plugged in the Smart SFPs, see §13;
2. In HiProvision, configure a point-to-point port based Ethernet service with these two Smart SFP ports. Configure the service with following QOS parameters:
 - ▶ frame size mode = custom frames;
 - ▶ small frame = 1% : 64 bytes;
 - ▶ custom frame = 99%: 848 bytes;
 - ▶ large frame = 0%;
 - ▶ Bandwidth & burst size mode: Endpoint Based;
 - ▶ Endpoint (useful) Bandwidth:
 - ▶ STM-1/OC-3 Smart SFP: 167 Mbps (or 167 000 kbps);
 - ▶ STM-4/OC-12 Smart SFP: 655 Mbps (or 655 000 kbps);
3. Load the service;
4. If your Smart SFPs are plugged in and the port is up, HiProvision must show both basic SFP and Smart SFP info after selecting the ports, see figure below. Also the Link Active (LA) LED of the Interface Module will blink immediately after plugging in the Smart SFPs.
5. Each Smart SFP has its own MAC address. It is possible to add extra security to the point-to-point connection. You can configure that the 1st Smart SFP only communicates with the 2nd one and vice versa. This can be done by filling out the **Destination MAC Address** of the other Smart SFP and setting the **Destination MAC Check** to **true**. This must be done on both Smart SFPs. As a result, if you plug in another Smart SFP with another MAC address, the point-to-point connection will not work anymore.
6. Connect your two fiber-optic SDH/SONET points to the Smart SFPs;
7. If your link is up and running, the 'TSoP Tx/Rx' counters increase (refresh rate takes a few seconds). Counters can be cleared via the 'Clear Counters' drop down.
8. If you think the link is not up and running, you could reboot the smart SFP by selecting a warm (=no traffic loss) or a cold (=traffic loss) reboot in the 'Reboot' dropdown.

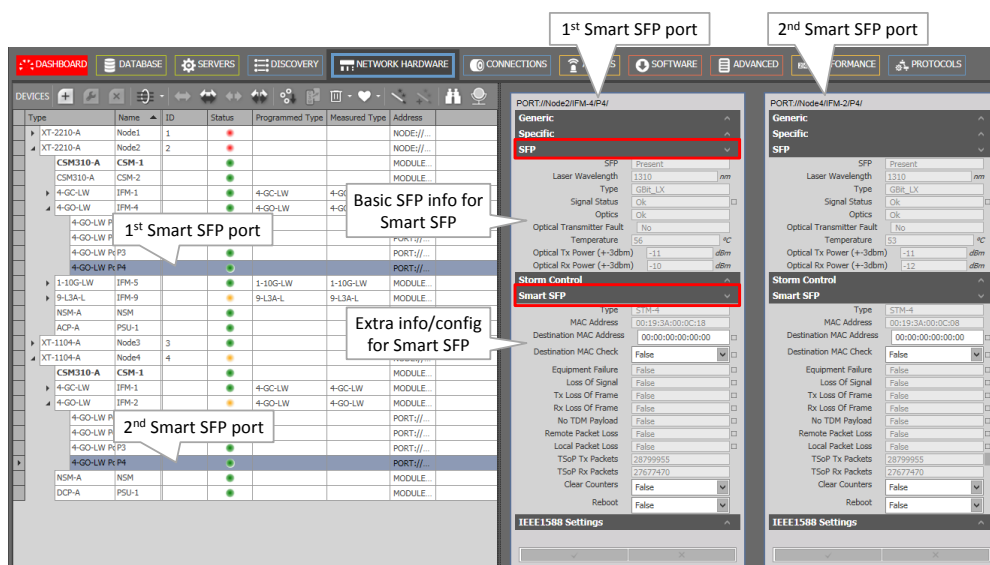


Figure 246 Example: Smart SFPs in HiProvision

23.3 Alarms

Some alarms are provided which can be found in the table below.

Table 58 Smart SFP Alarms

Condition	Alarm 1st Smart SFP	Alarm 2nd Smart SFP
Pull out Rx at 1st Smart SFP	Loss Of Signal, Rx Loss Of Frame	Tx Loss Of Frame, No TDM Payload
Pull out Tx at 1st Smart SFP	no alarms	no alarms
Pull out Rx & Tx at 1st Smart SFP	Loss Of Signal, Rx Loss Of Frame	Tx Loss Of Frame, No TDM Payload
Stop Ethernet traffic going to 1st Smart SFP	Local Packet Loss, Tx Loss Of Frame	Remote Packet Loss
Pull out WAN link between two Dragon PTN nodes	Local Packet Loss, TX Loss Of Frame	Local Packet Loss, TX Loss Of Frame
Pull out 1st Smart SFP	no alarms	Tx Loss Of Frame, No TDM Payload, Local Packet Loss

24. TRAFFIC CONTROL / RESOURCE ALLOCATION

24.1 Security

24.1.1 Sticky MAC

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

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

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

NOTE: Sticky MAC and MAC Limiting (§24.1.2) cannot be used together on the same node.

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

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

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

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

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

Information: Click Next>>;

Sticky MAC Parameters:

- ▶ Services: **Enabled:**
 - ▶ unchecked (=default): Sticky MAC is not enabled meaning that the dynamic MAC address learning process is active. New MAC addresses can be connected to the service ports, and will be learned by the nodes. If the Sticky MAC feature was enabled and you disable or uncheck it, the static stored MAC addresses will be cleared for this service and the dynamic MAC address learning process will be reactivated.
 - ▶ checked: Sticky MAC is enabled meaning that the dynamic MAC address learning process is not active or blocked for this service. Only static MAC addresses available in the MAC address table (see §24.1.3) are allowed. New devices or MAC addresses will not be allowed. If the feature was disabled or unchecked, enabling it will convert all the dynamically learned MAC addresses into static MAC addresses for all the ports in the selected Ethernet service. Furthermore, the dynamic learning process will be blocked.
- ▶ Ports: Trusted Port:
 - ▶ unchecked (=default): This is not a trusted port and must be secured. This port operates according to the Sticky MAC feature.
 - ▶ checked: This is a trusted port and must not be secured, it will ignore the Sticky MAC feature. The dynamic MAC address learning process remains active.
- ▶ If ok, click Finish. The configuration load manager will be invoked, see §5.

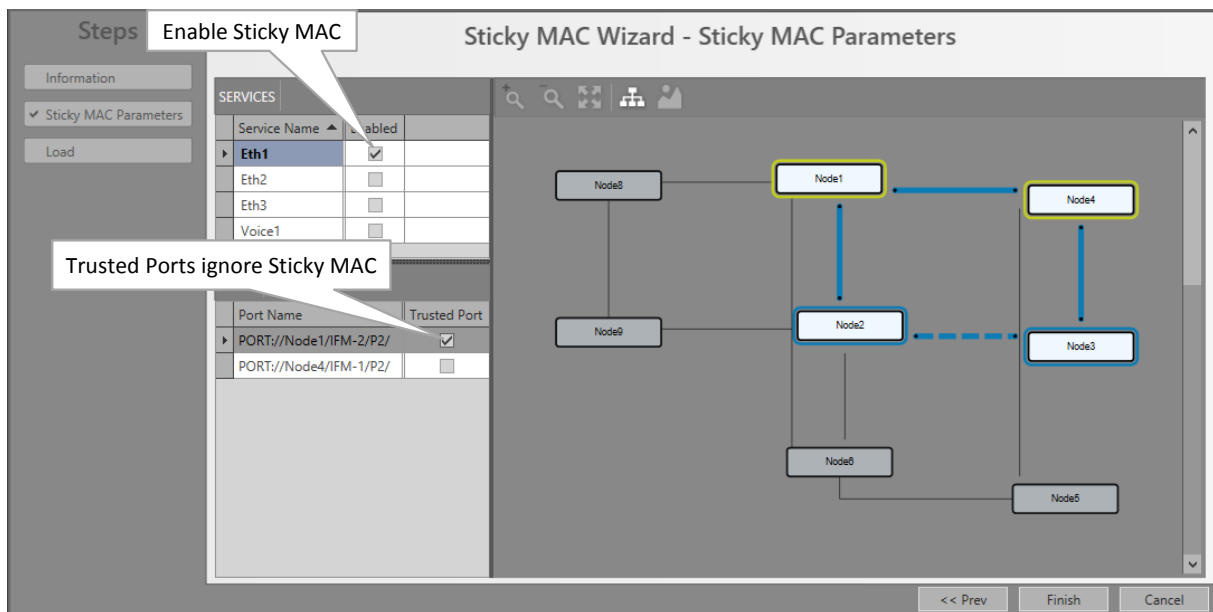


Figure 247 Sticky MAC Configuration

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

NOTE: If both MAC ACL (see §7.14) and Sticky MAC are active, a packet from a source MAC address is only allowed when the MAC address is allowed in both features.


NOTE: MAC Monitor (§24.1.4) shows the MAC Address table in the live network.

24.1.2 MAC Limit

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

NOTE: Sticky MAC (§24.1.1) and MAC Limit cannot be used together on the same node.

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

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

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

Information: Click Next>>;

MAC Limit Parameters:

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

- **Services: Table Size** (default = 500 for Ethernet service; default = 256 for Serial Ethernet and Voice service): Only relevant when MAC limit is enabled on the device. Configure the Table Size to limit the number of MAC addresses allowed per service on this device. Try to estimate how many MAC addresses or external devices (e.g. cameras, etc.) that will be used in this service on all nodes, and add some extra addresses for some extra margin. Configure this total amount in the Table size field. The maximum sum of all Table Sizes in a device is 32767.
- If ok, click Finish. The configuration load manager will be invoked, see §5.

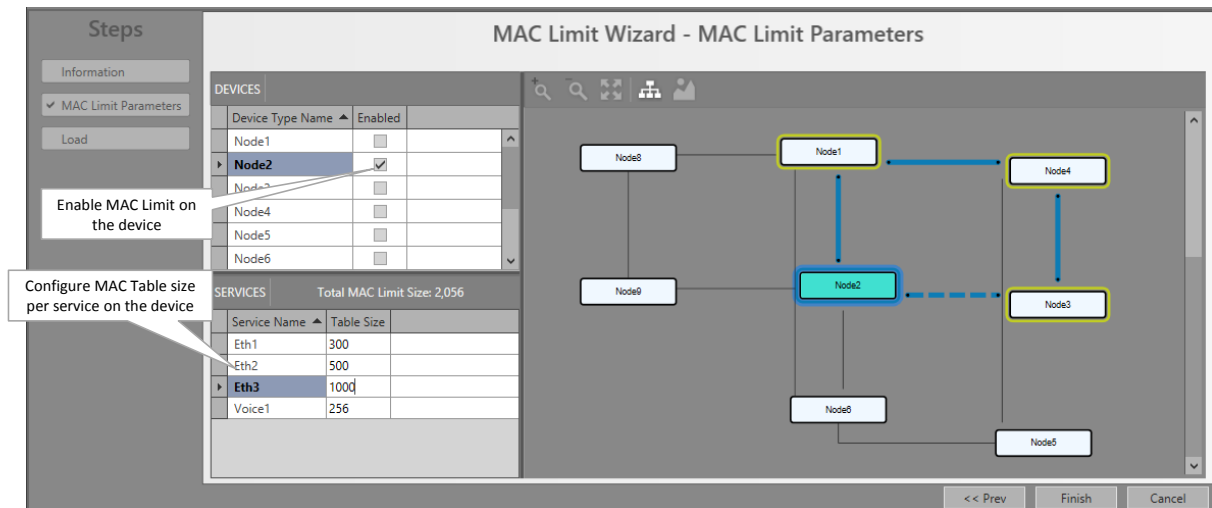


Figure 248 MAC Limit Configuration

- NOTE:** Best practice to set the same MAC limit on all nodes within a service.
- NOTE:** When you disable MAC limit on a device, all the dynamic learned MAC addresses (for all services) will be flushed or cleared on this device.
- NOTE:** When you modify the Table size, the dynamic learned MAC addresses for this service will be flushed or cleared.
- NOTE:** MAC Monitor (§24.1.4) shows the MAC Address table in the live network.

24.1.3 Static MAC Table

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

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

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

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

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

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

Information: Click Next>>;

Select Port and Service: Select the service and port on which static MAC addresses must be configured.

- ▶ Click the **Selected** checkbox to select the service;
- ▶ Click the **Selected** checkbox to select the port.
- ▶ Click Next>>;

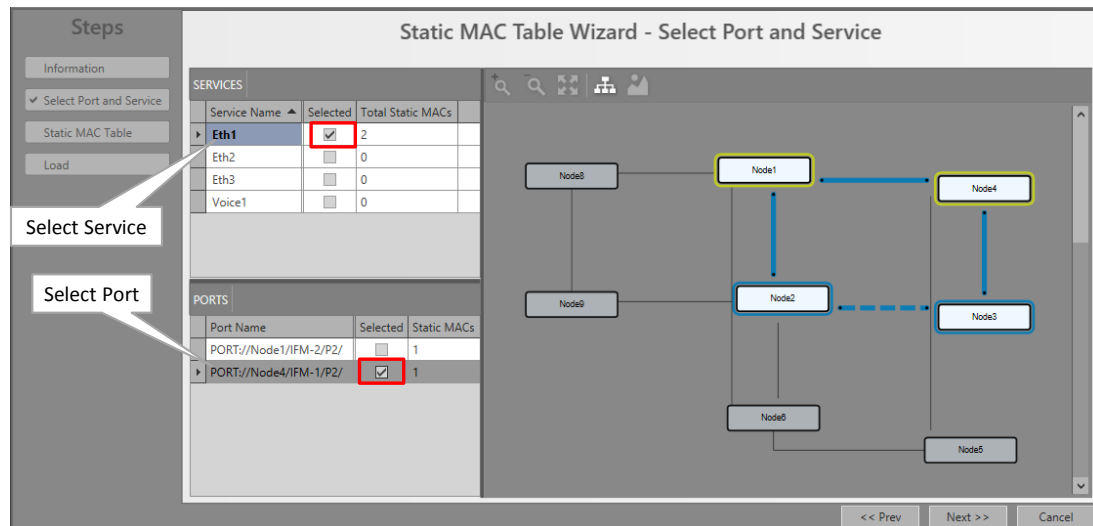




Figure 249 Static MAC Table: Service/Port Selection

Static MAC Table:

- ▶ Click  to add a static MAC address in the node and the HiProvision database;
- ▶ Click  to import static MAC addresses from the node into the HiProvision database. This import is useful for static MAC addresses that were created on the node via the Sticky MAC feature;
- ▶ A **Source** field indicates whether the MAC address was added manually or by import.
- ▶ If ok, click Finish. The configuration load manager will be invoked, see §5.

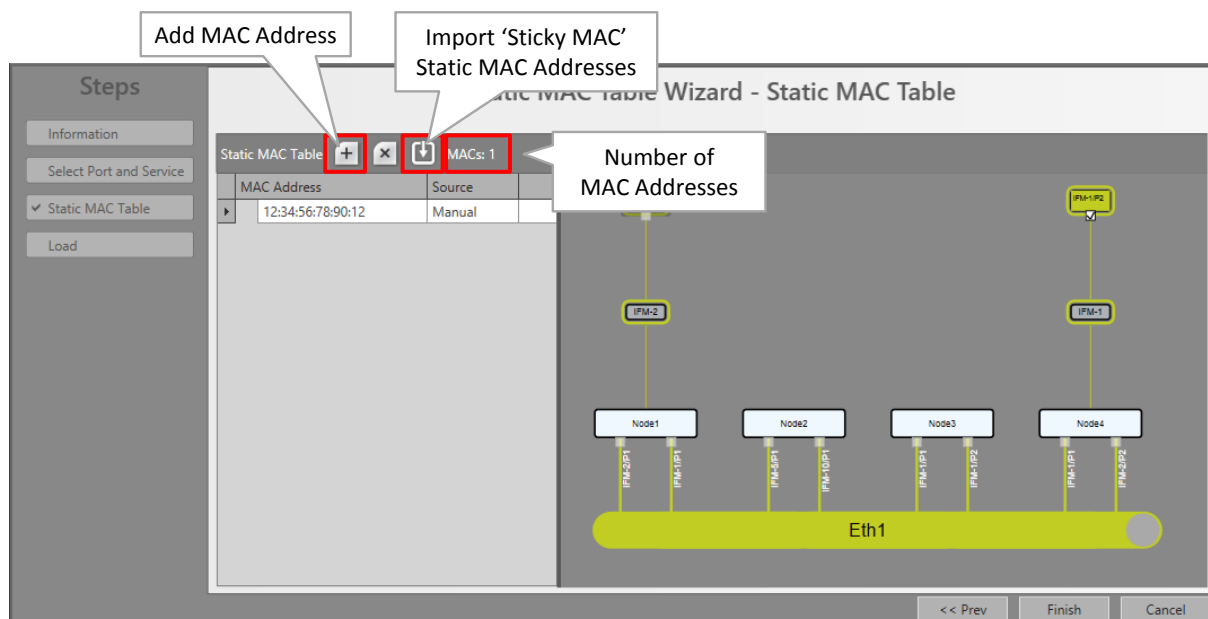


Figure 250 Static MAC Table: Add/Remove/Import

NOTE: MAC Monitor (§24.1.4) shows the MAC Address table in the live network.

24.1.4 MAC Monitor

Prerequisite: HiProvision has to be online.

The MAC Monitor will show the MAC address table of the selected device. This table includes all MAC addresses used on this device except for the MAC addresses that are used in a point-to-point tunnel. The MAC Address table is influenced by the following features:

- Sticky MAC (see §24.1.1);
- MAC Limit (see §24.1.2);
- Static MAC (see §24.1.3);
- MAC ACL (see §7.14);

Click Dashboard → (Monitoring) Network → Services → ;

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

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

Devices

DEVICES		SERVICES		MAC Addresses: 14	
Device Name		Service Name	MAC	Source Address	Source Node
1					
2					
3					
4					

Grouped by 'Service Name'

Service Name:	
38:9F:83:03:5A:40	PORT://2/IFM-1/P1/
38:9F:83:03:25:C0	PORT://2/IFM-1/P2/
38:9F:83:03:23:40	PORT://2/IFM-1/P3/
38:9F:83:03:23:40	PORT://2/IFM-4/P1/
38:9F:83:03:23:40	PORT://2/IFM-4/P3/

Total number of MAC addresses in this device

Service Name: SERVICE://Ethernet/vlan mixed/	
00:04:9F:EF:3F:18	TUNNEL://MTP 1/
00:04:9F:EF:3F:3D	PORT://2/IFM-9/P5/
00:10:94:10:00:01	TUNNEL://MTP 1/
00:10:94:20:00:01	PORT://2/IFM-9/P5/
00:10:94:47:00:01	TUNNEL://MTP 1/
00:10:94:47:00:02	PORT://2/IFM-9/P5/
00:19:99:A0:25:85	TUNNEL://MTP 1/
38:9F:83:00:D0:47	PORT://2/IFM-9/P5/
38:9F:83:00:D0:BB	PORT://2/IFM-9/P5/

Close

Figure 251 Example: MAC Monitor/MAC Address Table

25. E-TREE

25.1 General

NOTE: Supported on Interface Modules according §32.

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

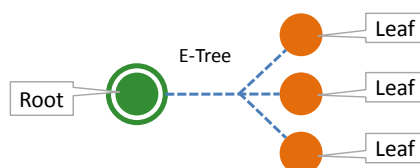


Figure 252 E-Tree: Root/Leaf

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

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

► Security:

- **Leaf:** Can only communicate with one or more 'roots', not with other 'leaves';

- **Root:** Can communicate with any element ('root' or 'leaf') in the service. Multiroot is possible to obtain load sharing and redundancy. Up to a maximum of 4 roots and 128 leafs per service can be configured;

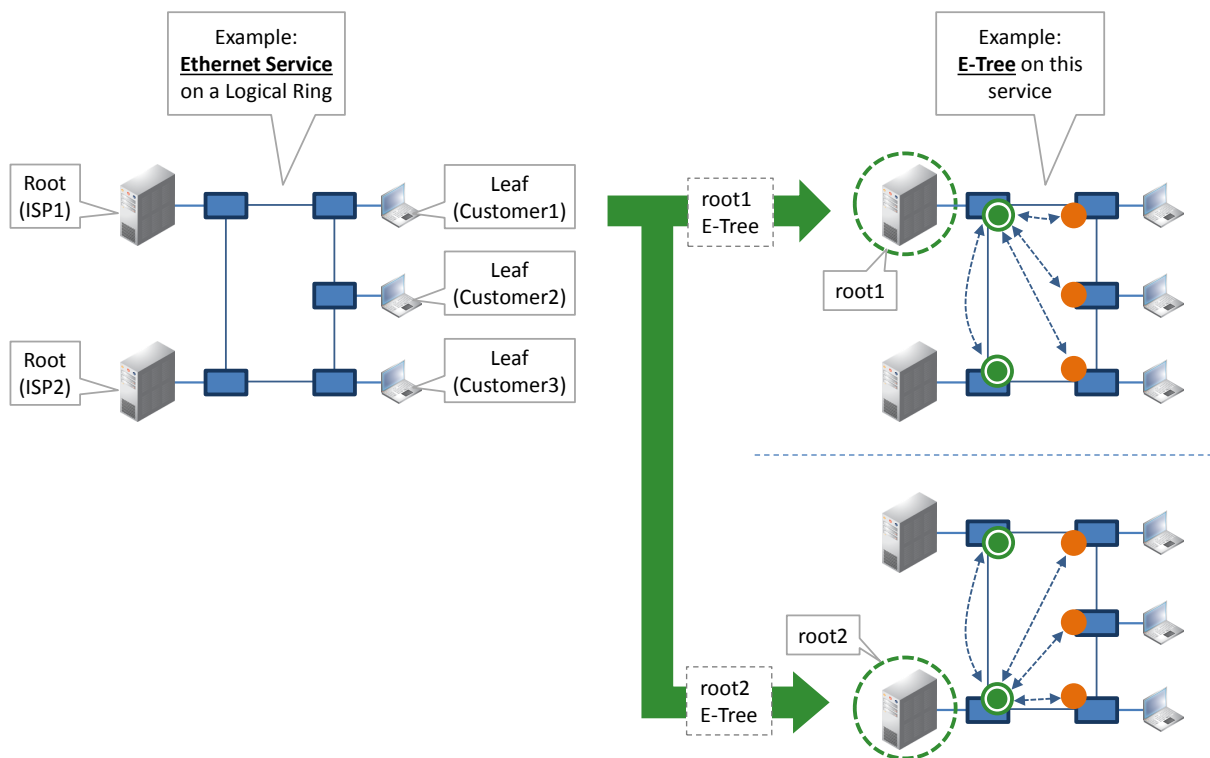


Figure 253 Example: Ethernet + E-Tree Communication

25.2 Configuration

See Ethernet Service wizard in §2.13.

26. LAYOUTING HIPROVISION

26.1 Layouting Tables

26.1.1 General

A table example is shown in the figure below. You can lay out any HiProvision table in any tab. Following layout actions are possible:

- modify column order;
- sorting the columns;
- hiding/showing columns;
- grouping columns (not all tables)
- filter editor (not all tables);

Closing a tab or the GUI will save the changed layouts automatically for the logged in user. The next time that this user opens a tile, the saved table layouts for this tile will be active.

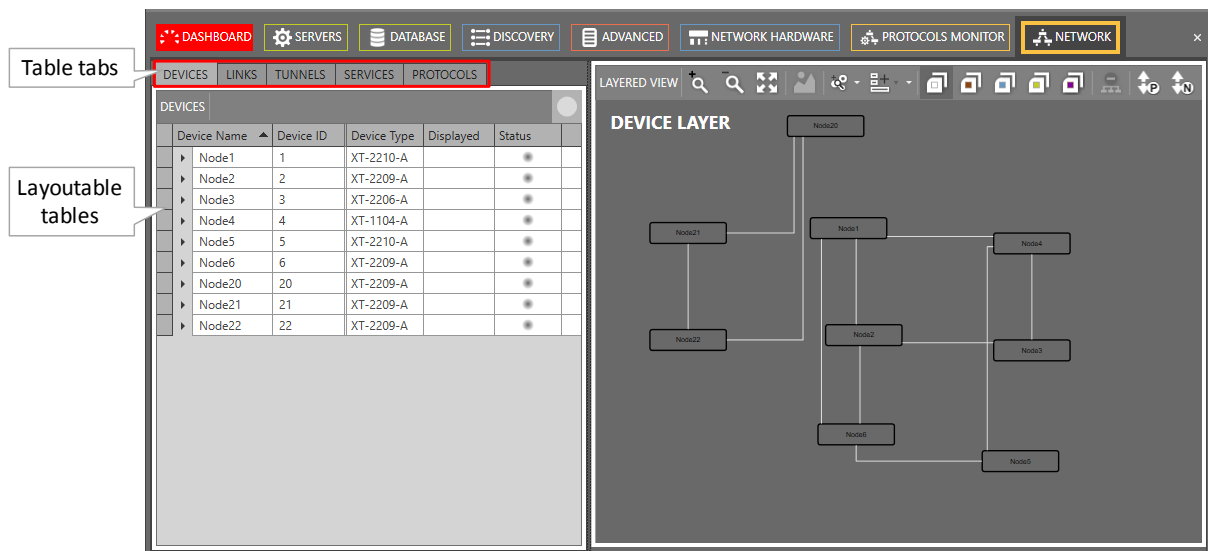


Figure 254 Layouting Tables

26.1.2 Layout Actions

The layout actions for a specific column can be invoked by right-clicking its header cell.

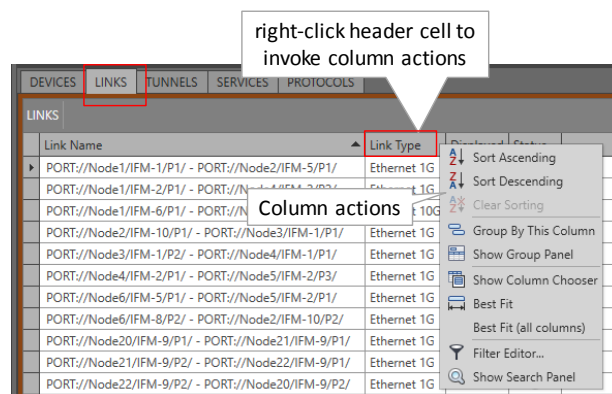


Figure 255 Invoke Column Actions

a. Column Order

The column order can be changed without the layout or column actions menu. Instead, it can be changed by dragging and dropping the column header cell before/after any other column. While moving the column, double-arrow indicators pop up when you can drop the dragged column into place.

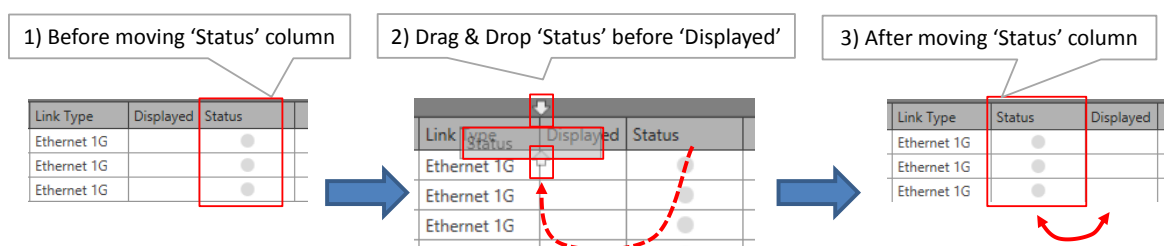


Figure 256 Table Layout: Column Order

b. Sorting Columns

Click 'Sort Ascending' or 'Sort Descending' in Figure 255 or left-click the header cell of the column a few times to sort the column.

c. Hide/Show Columns

Click 'Show Column Chooser' in Figure 255. Drag & drop a column header into Column Chooser and close the Column Chooser to hide a column.

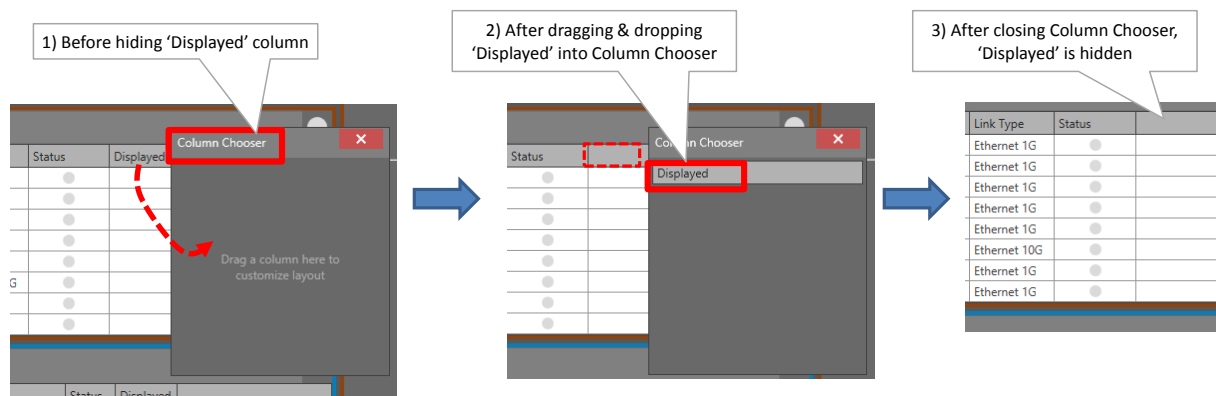


Figure 257 Table Layout: Hiding Columns

To show hidden columns, click 'Show Column Chooser' in Figure 255. Drag & drop a column header from the Column Chooser into the table header to unhide or show a hidden column. Close the Column Chooser. It is similar to the 'Hiding Columns' paragraph but in the reverse order.

d. Grouping/Ungroup Columns

Columns can be grouped for a better overview in the tables. Click the 'Show Group Panel' in the in Figure 255 to show the group panel. This panel will show which columns are grouped. If this panel is empty, none of the columns is grouped.

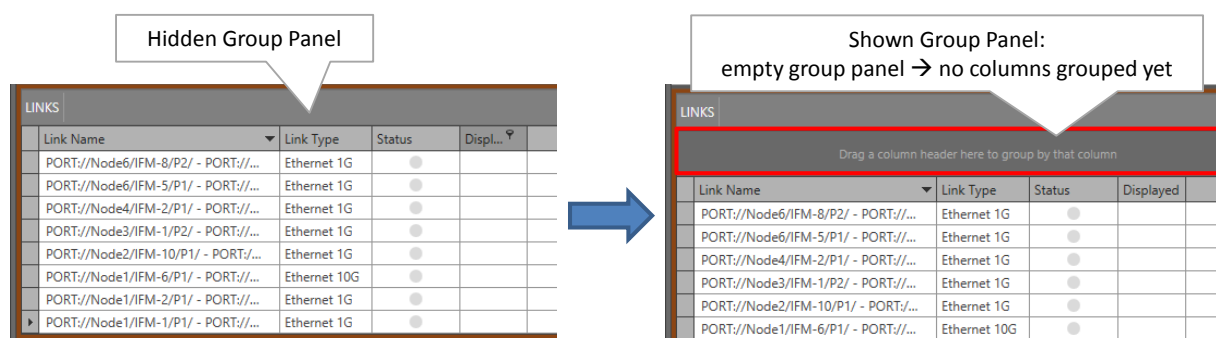


Figure 258 Hidden Group Panel / Shown Group Panel

To group a table by a column, follow one of the two actions below:

click 'Group By This column' in the layout actions menu of this column;

Drag the column header into the Group Panel.

As a result, the table will be grouped by this column and the column header appears in the Group Panel. It is possible to group additional columns as well by repeating previous action for additional columns. A grouping example is shown below.

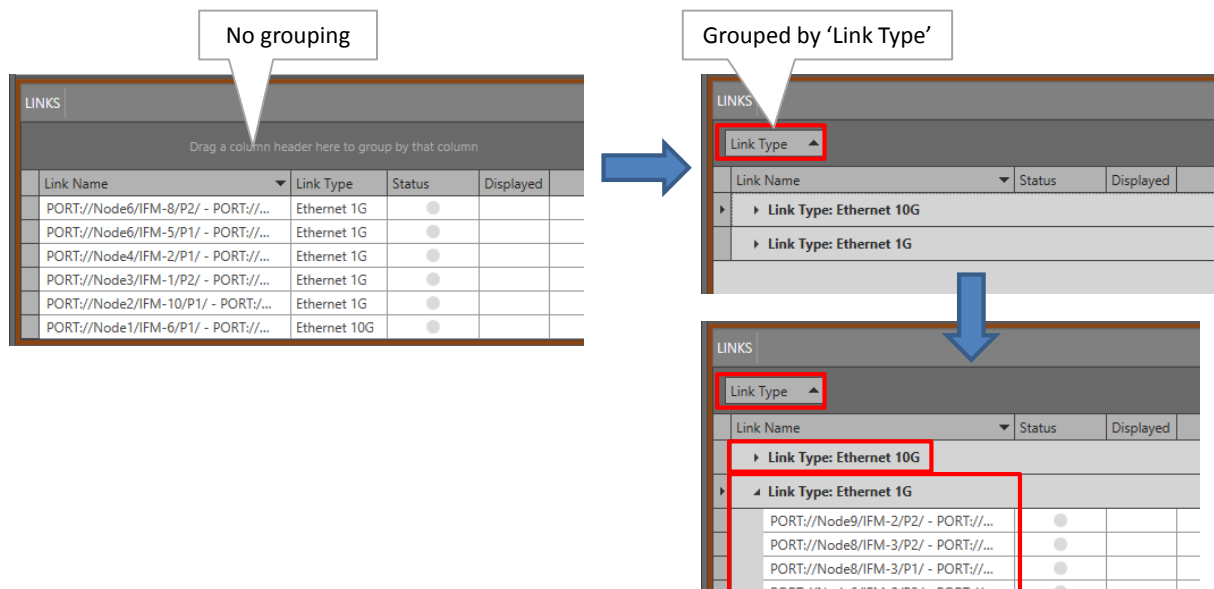


Figure 259 Example: Grouped By Link Type

To ungroup or to clear the grouping of columns, do one of the actions below:

Drag and drop the column from the group panel into the header row of the table;
Right-click the group panel and click 'Clear Grouping'.

e. Filter Tables

Tables can be filtered via creating one or more filters in a Filter Editor. Click the 'Filter Editor' in Figure 255 to show the Filter Editor.

In this editor, just click the required filter operators and fields and fill out the desired filter values. Click OK or Apply to create and activate the filter. Each time you adapt your filter or create a new one, the adapted/new filter will be stored in the History Filter List. Later on, you can apply these stored filters again by just selecting them from this History Filter List.

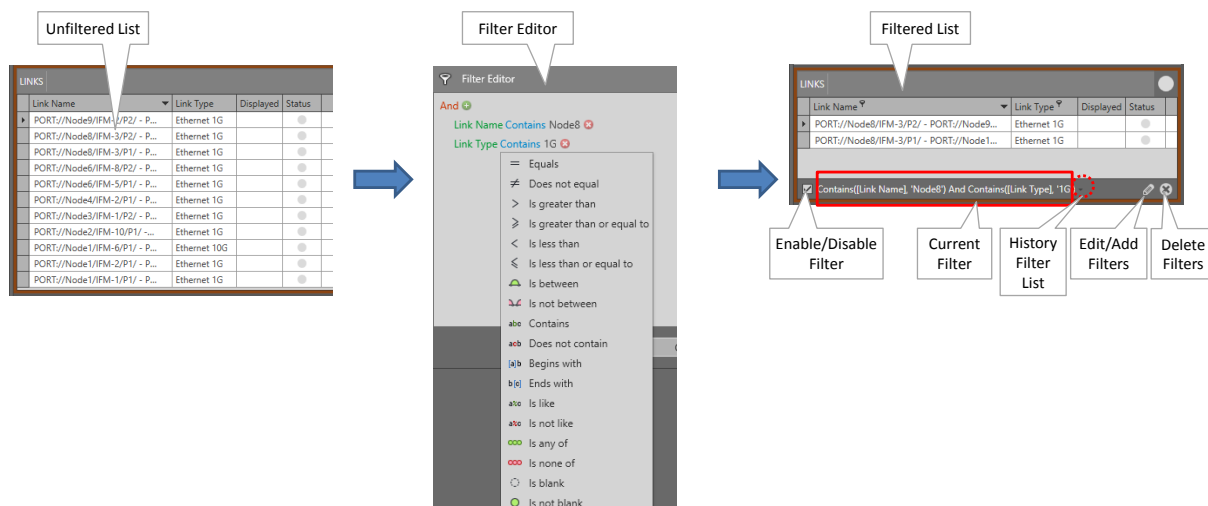



Figure 260 Filtering Tables

26.1.3 Restore Default Table Layouts

1. Go to Dashboard → Users (only allowed for administrators),
2. Select the user for which the table layouts must be cleared by expanding the 'Groups and users' and clicking the desired user row;
3. Click the trashcan icon  to reset the customized table layouts.

CAUTION: this action will also reset or clear some other data, see Ref. [15] in Table 1.

4. Click OK to confirm;
5. If you open a tile now, it will restore the default table layouts;

26.2 Layouting Network Drawings

26.2.1 General

This paragraph describes how to place (or layout) the nodes and links into a desired place in relation to each other and/or in relation to an optional background picture. The layout is not fixed in relation to the HiProvision screen (*).

Multiple layouts can be created, saved and organized in one or more layout trees.


Some definitions:

- Layout Tree: A collection of layouts that is related to each other in different levels via nesting;
- Top Layout: The highest level or layout in a layout tree;
- Sub Layout: The child or lower level layouts of a top layout in a layout tree. Sub layouts are designed for tuning multiple views in the Large Network Monitor (see §27) and cannot be used elsewhere in HiProvision;

- **Default Layout:** The layout that is available in HiProvision from the start without a layout tree, top or sub layout being created. The default layout is an 'Orthogonal Device Layout'.
- **Active Layout:** The layout that is currently used in all the HiProvision screens that have a network drawing displayed (except for the Discovery and Large Network Monitor (=LNM) tiles). When no layout has been created yet, the default layout is the active layout.
- **Device:** Node;
- **Object:** Node (devices) or link;

Hierarchy Node: a light green bullet in a layout or network drawing indicating a link with nodes in another layout, see further.

CAUTION:

- Only a top layout without sub layouts can be set as active layout;
- (*) The layouting area will center relatively to a boundary around all nodes in the layout. This happens after creating a new, opening or refreshing a layout, or simply after clicking the fit-content button . When you create your layouts, backgrounds and objects (nodes and links) need to be put manually on top of each other. The background map needs to be resized to fit the boundary of all objects. The objects themselves need to be positioned on the background map. Different layouter options will be helpful here, as well as zooming in/out the entire layouting area.

To process layouts, go to Dashboard → Layouts.

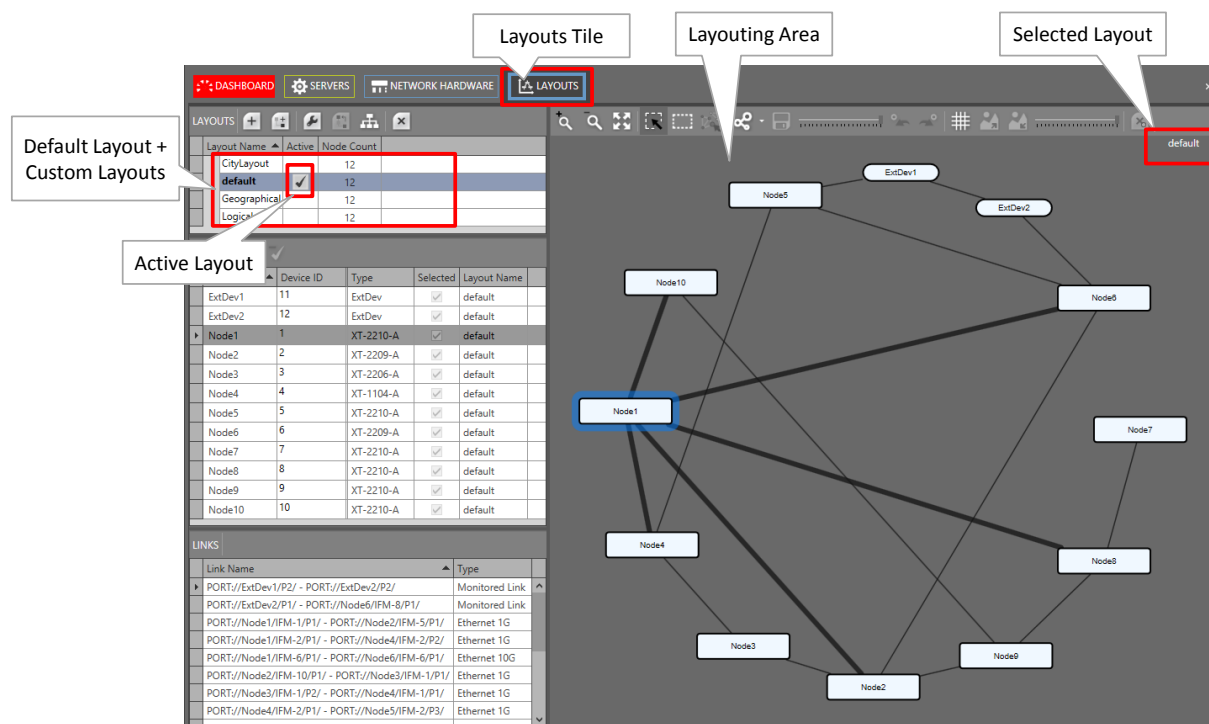


Figure 261 Layouting Network Drawings

NOTE: Layouts can be modified/deleted, but the last remaining layout cannot be deleted.

26.2.2 Layout Guidelines

There are many layout options but in most cases, following typical network layouts are desired:

Geographical layout: network is mapped on a geographical map or ground plan etc...;

Logical layout: network is layouted according to a logical network or company topology;

Don't care: layout is not relevant at all, just use the default layout.

A short description how to set up such a layout can be found below.

NOTE: A full description of all the layout options can be found in §26.2.3. Other layout types can be created by creating new layouts and exploring all the layout options in this section.

a. Geographical Layout

1. Create a new layout (+) including a background picture (=map, ground plan...) of maximum 9 Mb via the Browse button. *.JPG and *.PNG files are allowed as background picture;

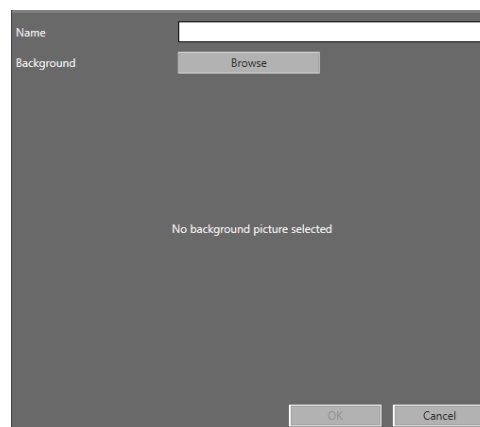








Figure 262 Create Layout



2. Resize the background picture until it has the desired size (↔/↕);
3. Apply some transparency to the background picture via the right-hand slider (▬);
4. Position a node:
 - ▶ Select the desired nodes first:
 - ▶ Click (🖱️) (= single node select) and click one node so it highlights;
 - ▶ Click (🖱️) (= multi node select) and click/drag a rectangular selection area around the desired nodes. The selected nodes will be highlighted;
 - ▶ Position the selected node(s) via drag and drop into place according to the desired spot on the background picture;
5. After placing the nodes, your links layout could be messed up a bit. You can layout them better if desired. Exact geographical links are required?
 - ▶ Yes: Click (🖱️) first and drag and drop each link manually (create bends etc...) onto the exact location. You could still straighten up one link via selecting the link (bold black line) and clicking (🔗) → Straight Link Layout;

- ▶ No: choose one of the layouters () below for an automatic link layout:
 - ▶ Straight Link Layout;
 - ▶ Orthogonal Link Layout;
 - ▶ Organic Link Layout;
- 6. Save the layout (
- 7. To activate this layout for the entire HiProvision (except for Discovery and Large Network Monitor), set this layout as 'Active' (

b. Logical Layout





1. Play around first with one of the automatic () layouters listed below and select the layout that suits the best for your project:
 - ▶ Orthogonal Device Layout;
 - ▶ Circular Device Layout;
 - ▶ Organic Device Layout;
2. Fine-tune your layout further via drag/drop your devices and links manually as described in the previous paragraph §a;
3. Save the layout (
4. To activate this layout for the entire HiProvision (except for Discovery and Large Network Monitor), set this layout as 'Active' (

c. Don't Care


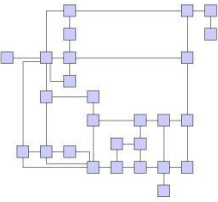
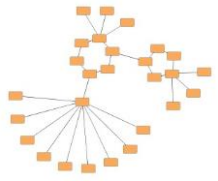
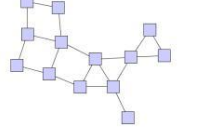
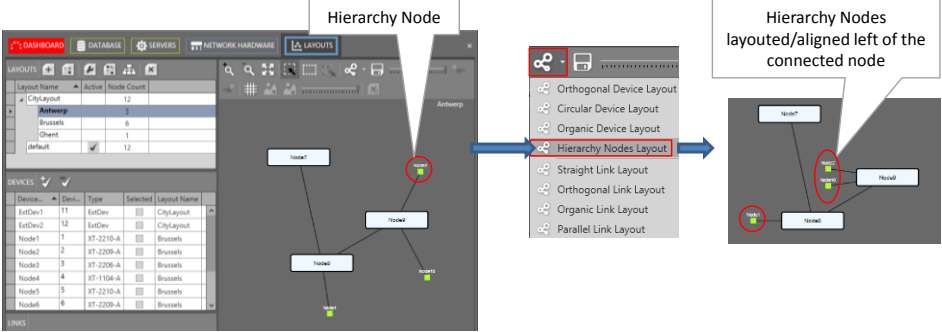
If the layout is not important at all, do nothing. HiProvision applies a 'default' layout to your network based on the automatic 'Orthogonal Device Layout' layouter (). This 'default' layout is by default 'Active' () in the entire HiProvision (except for Discovery and Large Network Monitor).

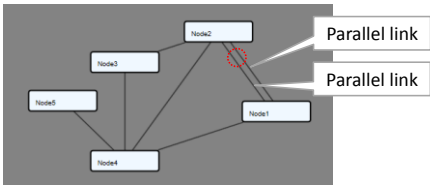


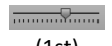







26.2.3 Layout Menu and Options

Table 59 Layout Buttons

Button	Short Description
LAYOUTS	
	Create new (top) layout. This is a layout at the highest or top level.
	Create new sub layout for using in the Large Network tile (see §26.2.4). The sub layout will be created in the selected layout. Sub layouts can be created up to 10 levels deep starting from the top layout. Sub layouts cannot be created in the active layout. So if there is only the default layout (and as result, automatically the active layout), another top layout must be created first. The Node Count field indicates exactly how many nodes are involved in a specific sub layout. The Node Count is also visible in the sub layout icons in the network drawing. A maximum of 100 sub layouts can be created per top layout. Example to create sub layouts: see §26.2.4.
	Modify selected layout: Possibility to change the layout name and/or background picture.
	Move a sub layout (=reparenting): Move an existing sub layout from its parent to another parent layout within the same top layout in the layout tree. Note: Reparenting can also be done (without this button) by just drag & drop a sub layout to another parent layout. This drag and drop will show whether the drag & drop is possible.

Button	Short Description
	<div> <div> </div> <div> </div> </div>
	Sets the selected top layout as active layout. Only layouts without sub layouts can be set as active because sub layouts are only meant for the Large Network tile (see §26.2.4). All the HiProvision screens that have a network drawing displayed, will display it according to the active layout. By default, the 'default' layout is active.
	Delete selected layout from the layout list. Neither the last remaining layout nor the active layout can be deleted.
Layouting Area	
	Zoom in / Zoom out of the layouting area. CAUTION: Zoom in / Zoom out results will not be saved when saving the layout.
	Fit all nodes and links in the center of the layouting area. If your nodes and links look lost, click this button to bring them back in focus in the center of the layouting area.
	<p>View mode: select one object (node or link) at a time, in this mode you can:</p> <ul style="list-style-type: none"> - Drag & drop the entire layouting area in a specific position (CAUTION: this new position will not be saved). - Layout objects into place by drag & drop the selected object. - Click on single objects (node or link) to select them. A selected node has a blue-grey-blue border, a selected link is shown in a bold black line. A selected bend in a link shows a black bullet. - Create a bend in a link by drag & drop on the link where the bend must be made, see Figure 263. - Delete a bend in a link by selecting the bend and clicking see Figure 264. <p>NOTE: unselect the selection via clicking on the background.</p>
	<p>Selection mode: select multiple objects (node or link) at a time, in this mode you can:</p> <ul style="list-style-type: none"> - Select multiple objects via a rectangular selection area. Links that have at least one end point in the selection area will be selected as well. - Click on single objects (node or link) to select them. A selected node has a blue-grey-blue border, a selected link is shown in a bold black line. A selected bend in a link shows a black bullet. - Layout objects into place by drag & drop the selected object or object group (=group of selected objects). <p>NOTE: unselect the selection via clicking on the background.</p>
	<p>Selects all remaining network elements that are directly or indirectly (*) connected to an existing selection of network elements.</p> <p>For example by using this button, you can select a subnetwork in just 2 clicks: click1= select one element from the subnetwork, click2 = click this button.</p> <p>(*) : indirectly means that the network element is connected via another network element to the current selection.</p> <p>NOTE: unselect the selection via clicking on the background.</p>
	<p>The layout selector button provides a few automatic layouter methods that can be used optionally to optimize your layout.</p> <p>NOTE: You could layout your devices and links manually as described in / without a layouter.</p> <p>Layout only a part of your network?</p> <p>YES:</p> <ul style="list-style-type: none"> - (advised) manual layout: select objects that must be layouted and then drag & drop manually; - automatic layout: select objects that must be layouted and select a layouter from the list. <p>NO, entire network:</p>

Button	Short Description
	<p>- automatic layout: select a layouter from the  list without selecting objects first.</p> <p>Layouters: Entire layouts (devices + links):</p> <ul style="list-style-type: none"> - Orthogonal Device Layout (=default): produces compact drawings without overlaps, few crossings and few bends  <ul style="list-style-type: none"> - Circular Device Layout: produces interconnected ring and star topologies  <ul style="list-style-type: none"> - Organic Device Layout: produces a well-balanced distribution of nodes with edge crossings, similar to organic structures in outside nature.  <ul style="list-style-type: none"> - Hierarchy Nodes Layout: This layouter becomes active in sub layouts containing at least one hierarchy node. A hierarchy node is a light green bullet indicating the link with nodes in another layout. Clicking 'Hierarchy Nodes Layout' aligns the light green bullets nicely on the left-hand side of its connected node for a better overview. If you select... : <ul style="list-style-type: none"> - Nothing: the layouter layouts all hierarchy nodes; - an object (one or more nodes, one or more hierarchy nodes): the layouter layouts only the hierarchy nodes from the selected objects.  <p>Link Layouts: Layouts the selected link in a straight/orthogonal/organic/parallel way. If no link is selected, ALL your links will be layouted accordingly. Devices are not touched. Use this option when you have layouted your devices manually and your links are messed up a bit.</p> <ul style="list-style-type: none"> - Straight Link Layout: for straight links; - Orthogonal Link Layout: for right or squared angled links; - Organic Link Layout: for well-balanced distributed links; - Parallel Link Layout: a link that has a neighbor link between the two same nodes is called a parallel link, see figure below. If nothing is selected only all parallel links (and not single links) in the drawing will be affected.

Button	Short Description
	
	Saves your layout.
	Undo previous action(s) / Redo undone action(s) on nodes and links. Clicking multiple times on this button undoes/redoes the next action in the history action list. This history action list will be cleared when a node or sub layout is added, deleted or moved to another layout.
 (1st)	Sets the sub layout group icon transparency. Only active if the selected layout has sub layouts. Set this slider to the left/right for maximal/minimal transparency. The transparency can be set per group icon.
	Hides/shows the data grid points in the layouting area. When the grid is on, layouting or dragging/dropping the links or bends in the link will be magnetized by the grid points.
	Only relevant if a background image has been inserted in the layout. Click  /  to increase / decrease the size of the background image, click as many times as needed until the desired size has been reached.
 (2nd)	Sets the background image transparency (if any). Only active if a background image has been inserted in the layout. Set this slider to the left/right for maximal/minimal transparency.
	Deletes the selected bend in a link. As a result, the link will be straightened up. A bend must be selected first in mode by clicking the bend. A bend is only selected when a black bullet is visible on the bend. See Figure 264. 

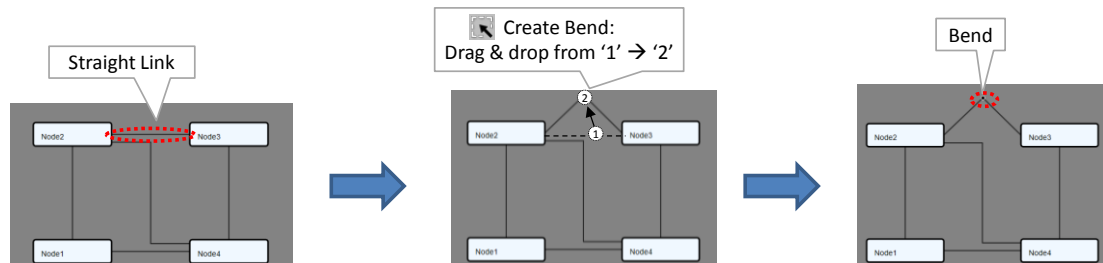


Figure 263 Create Bend

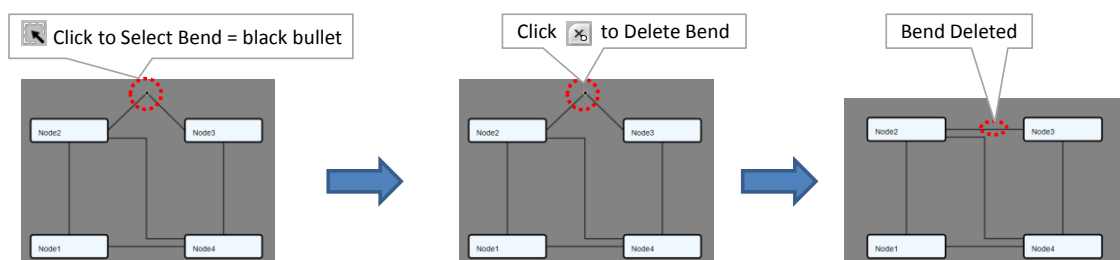


Figure 264 Delete Bend

26.2.4 Example Sub Layouts

As an example, we will show you how to map an example network with 12 nodes into sub layouts according to some cities. We will create a top layout 'CityLayout' first, next we will create sub layouts with the following Belgian cities: 'Antwerp', 'Brussels', 'Ghent'. Background maps are possible but not used in this example.

CityLayout (=top → has 12 nodes: device [1,...,12]);

- ▶ Brussels (=sub → has 6 nodes: device [1,2,3,4,5,6]);
- ▶ Antwerp (=sub → has 3 nodes: device [7,8,9]);
- ▶ Ghent (=sub → has 1 node: device [10]);
- ▶ Device [11,12] remain in the 'top' CityLayout;

Without creating a top or sub layout, a default layout is always available from the beginning:

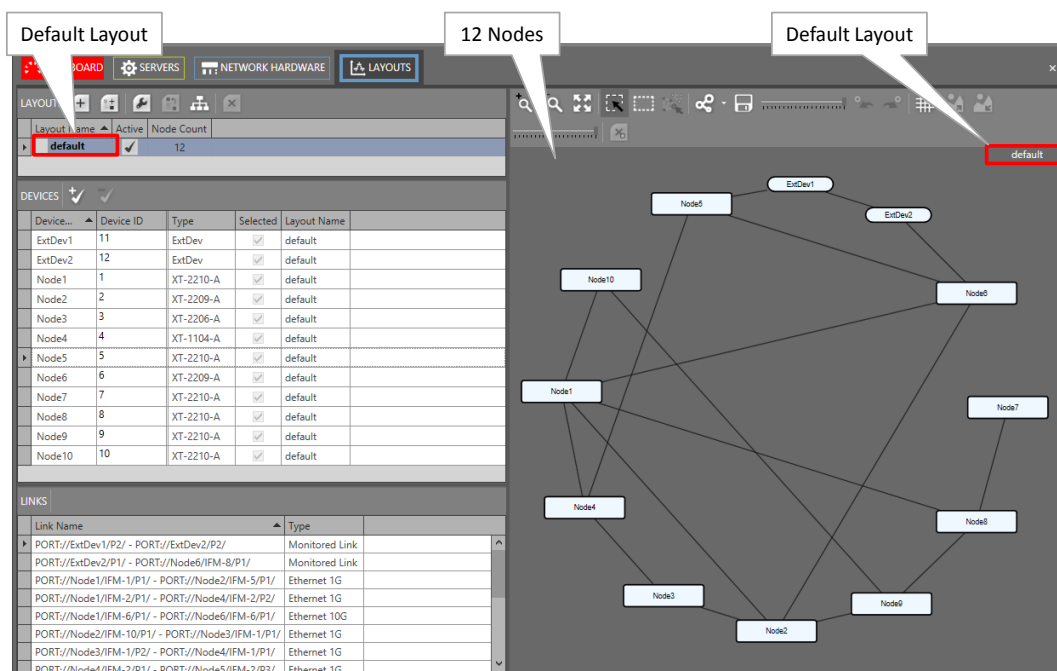







Figure 265 Before Sub Layout Creation

Follow the steps below to create a top and sub layouts:

1. 'CityLayout': Create a new top layout first via clicking  and fill out 'CityLayout' in the Name field. Optionally, a background image can be added (not in this example);
2. 'Brussels': Select the 'CityLayout' line in the LAYOUTS table and click , fill out 'Brussels' in the Name field;
3. 'Antwerp': Select the 'CityLayout' line in the LAYOUTS table and click , fill out 'Antwerp' in the Name field;
4. 'Ghent': Select the 'CityLayout' line in the LAYOUTS table and click , fill out 'Ghent' in the Name field;
5. Give an initial layout via clicking  and selecting Circular Device Layout;
6. The result looks like the figure below. No nodes have been mapped to a sub layout yet;

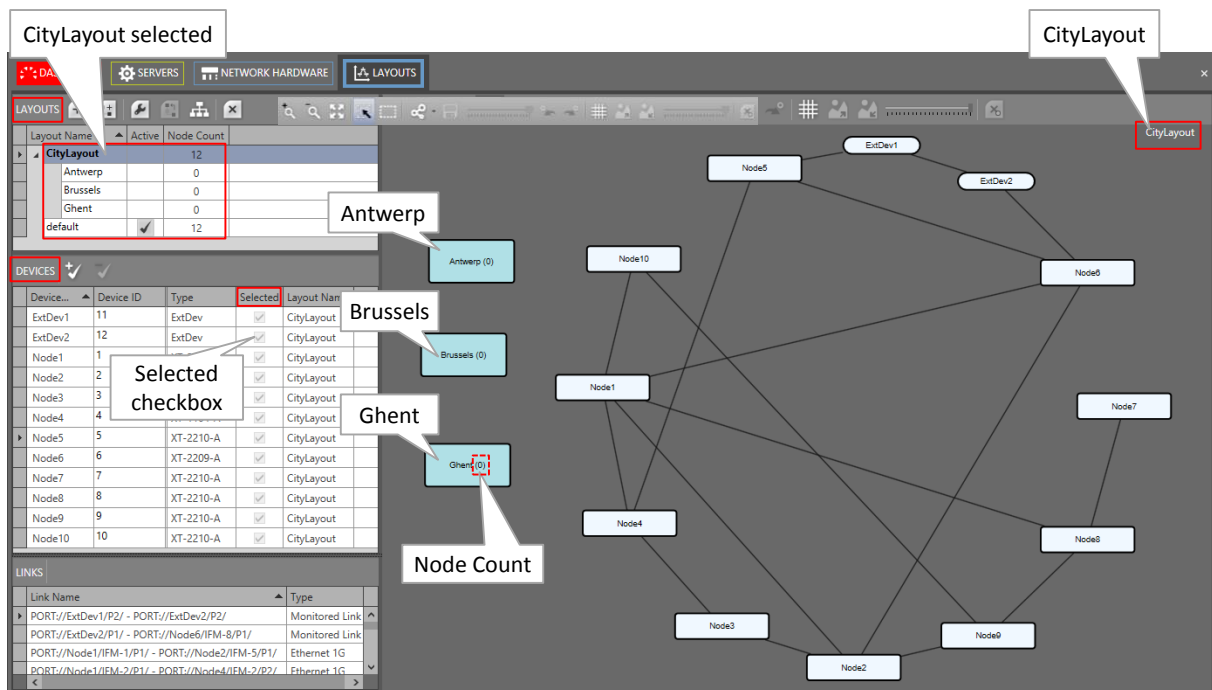


Figure 266 CityLayout View after Creation, No Mapping Yet

7. Map Node[1..6] into the sub layout 'Brussels' via one of the methods below:

- **Method1:** Choose the sub layout 'Brussels' by clicking the 'Brussels' row in the LAYOUTS list. Map the nodes Node[1..6] into this layout by clicking its 'Selected' checkbox in the DEVICES list. 'Brussels' will appear in the Layout Name column;
- **Method2:** In the parent layout 'CityLayout', select the Node[1..6] icon in the network drawing (in mode or) or select multiple nodes at once by dragging a selection area around them (in mode). Once the nodes are selected, press and hold the SHIFT key on your keyboard and drop the selected nodes onto the node group icon of

the desired sub layout (e.g. + SHIFT + hover it with selected nodes = . Drop handles turn into an entire icon border when zooming in more.);

8. Similar to above, map Node[7..9] into the sub layout 'Antwerp';
9. Similar to above, map Node[10] into the sub layout 'Ghent';
10. In this example, Node[11,12] remain in the parent 'CityLayout';
11. Verify all the top and sub layouts whether they are OK. If a layout is not OK (e.g. node icons on top of each other etc...), layout them until it is OK as described in §26.2.2. Save each layout by clicking the save button
12. Everything should be OK now. The final result could look as in the figure below;

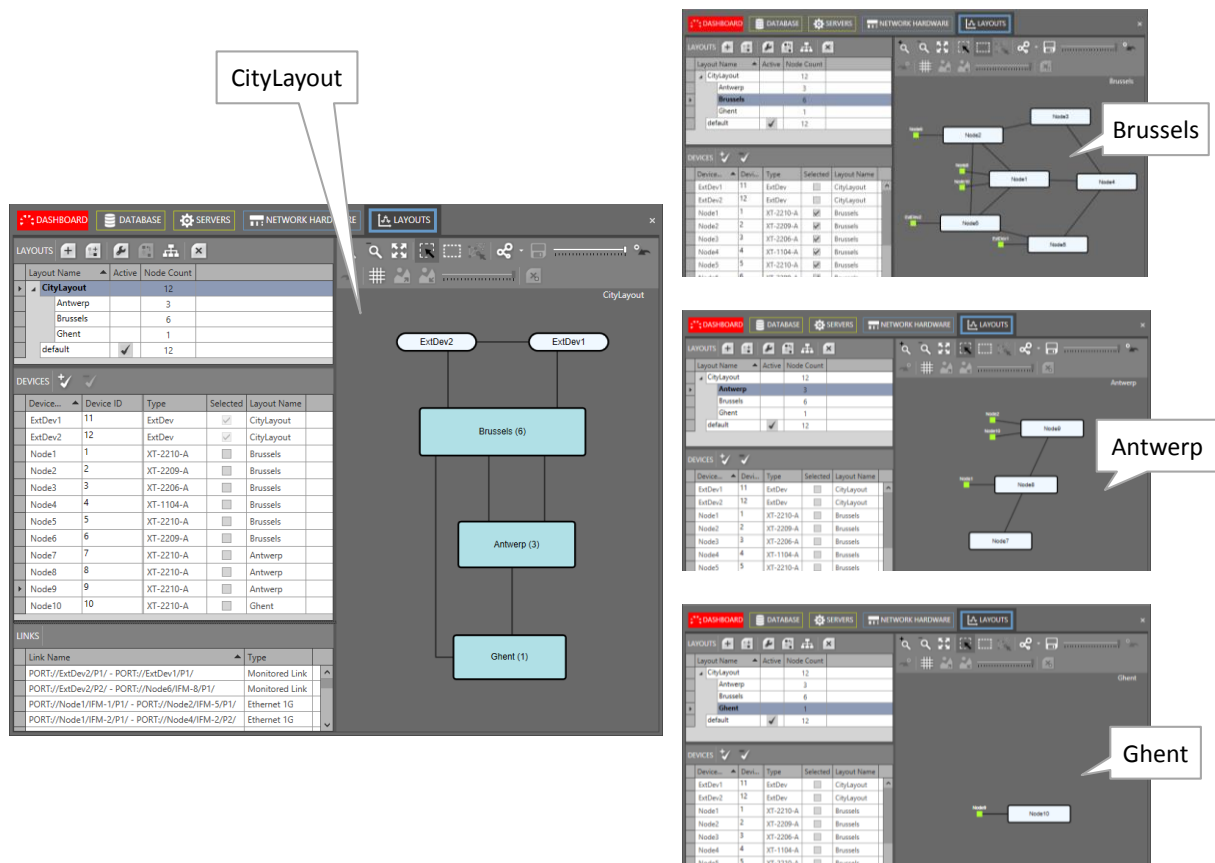


Figure 267 Final Result after Mapping Nodes into Sub Layouts

27. LARGE NETWORK MONITOR (=LNM)

27.1 Prerequisite

Divide the large network into smaller parts for better monitoring by grouping parts of the network in layouts and/or sub layouts. It can be done via the Dashboard → Layout tile (see also §26.2). The grouping could either be functional, geographical...

CAUTION: An LNM voucher or license must have been purchased and installed per serial key. Without these vouchers, only offline configuration is possible. See also §20.

27.2 General

The LNM allows to monitor large networks in an elegant way. This feature can be used via the Dashboard → (Monitoring) Large Network. An example can be found below.

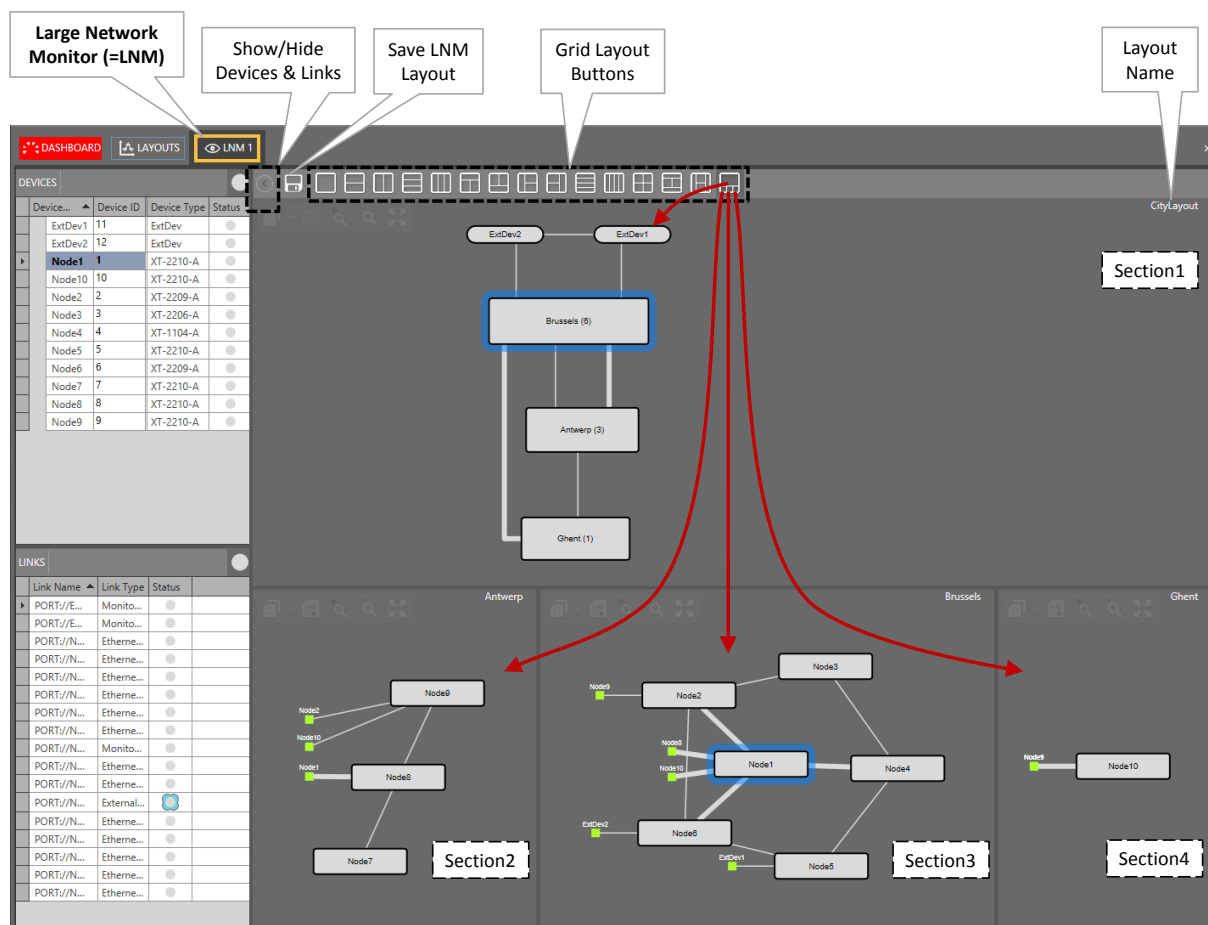




Figure 268 Large Network Monitor

27.3 Selecting Grid Layouts

Different **grid layouts** are by default available. Each grid layout has one or more (up to four) grid sections and can be selected via the grid layout buttons. Swapping from one grid layout to another is possible in just one click via these buttons. The  button can be used to show/hide the Devices and Links tables for a wider view without tables. Use the save button  to save your optimized view after completing the next paragraphs.

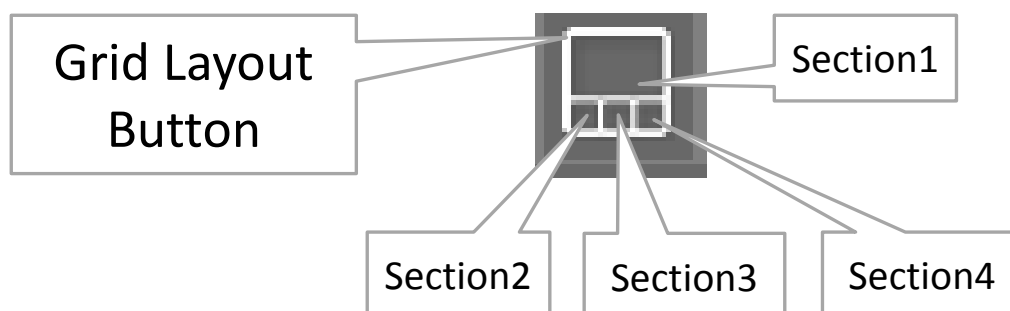







Figure 269 Layout Grid Button Example

27.4 Assign Layouts to Grid Sections

Each layout configured in the Layout tile can be assigned to any grid section via the layout selector . This selector and other buttons pop-up after hovering over the grid section. After having assigned a layout to a grid section, following buttons can be used per grid section:

- ▶ : 'Go back to Parent' button to navigate one level up or to assign the parent layout to this section;
- ▶  / : zoom in / zoom out buttons;
- ▶ : to fit and center your layout in the grid section or bring back the layout in focus when it looks lost beyond the section borders;

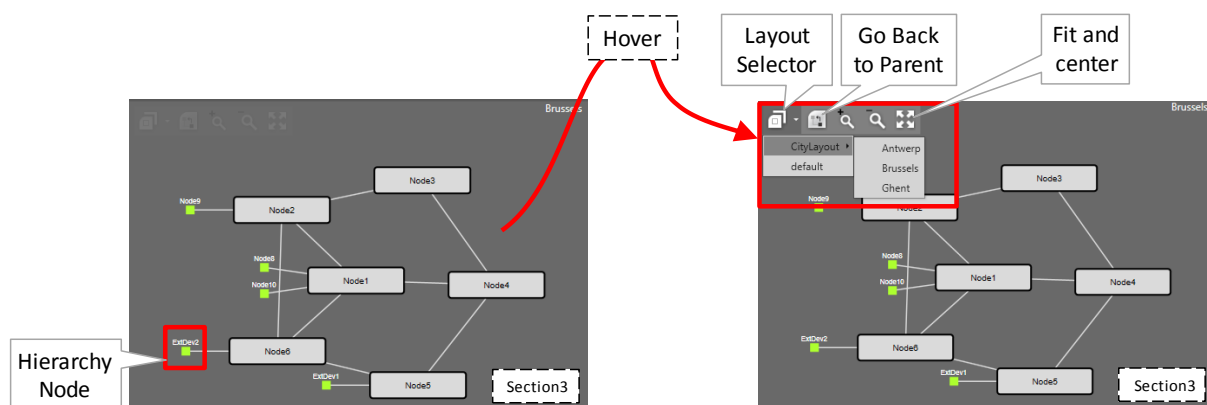



Figure 270 Grid Section: Layout Selector

NOTE: Make sure to save your layout via the save button  after having it optimized. The Hierarchy Node (see §26.2.1) can be clicked to navigate one level up.

27.5 Multiple LNM Sessions

A maximum of 4 LNM sessions can be opened simultaneously. Each time you click the 'Large Network' tile, a new LNM session (or tab) will be opened, always starting with LNM1. Each LNM session can have its own grid layout as described in previous paragraphs. Each opened LNM session has its own dedicated shortcut (or checkbox) on the 'Large Network' tile. The first checkbox (most left) always refers to LNM1,..., the last checkbox (most right) always refers to LNM4.

NOTE: If no LNM session is opened yet and you want to open for example LNM3, you have to open the lower-numbered sessions LNM1 and LNM2 first.

You can jump to an LNM session by clicking its checkbox on the tile or its tab.

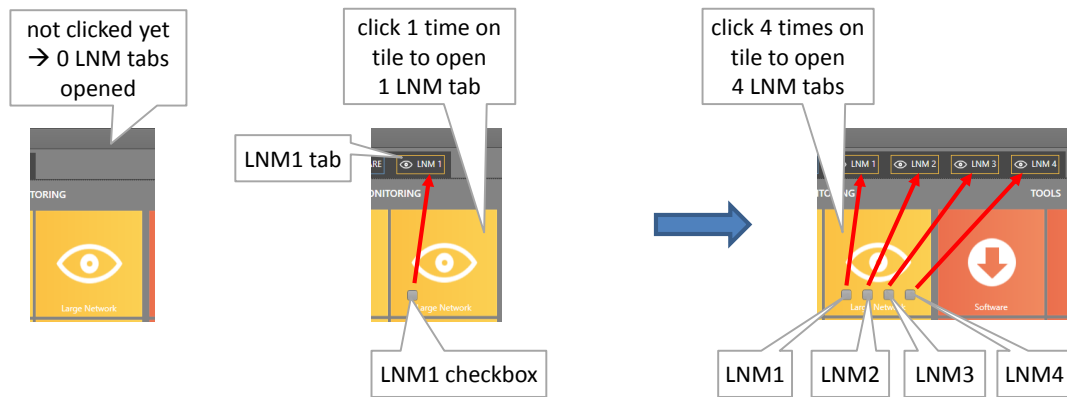


Figure 271 Multiple LNM Sessions

27.6 Large Network Monitor Live

The example screenshot below shows multiple LNM tabs (LNM1 and LNM2) with each tab its own grid layout. LNM1 shows a node rack background picture and country maps of Belgium including nodes and networks. LNM2 shows some more detailed network layouts per Belgian province. The node icon colors (red, green...) indicate the severest alarm color that is present in that node. For more info on LNM alarms, see §4.10.

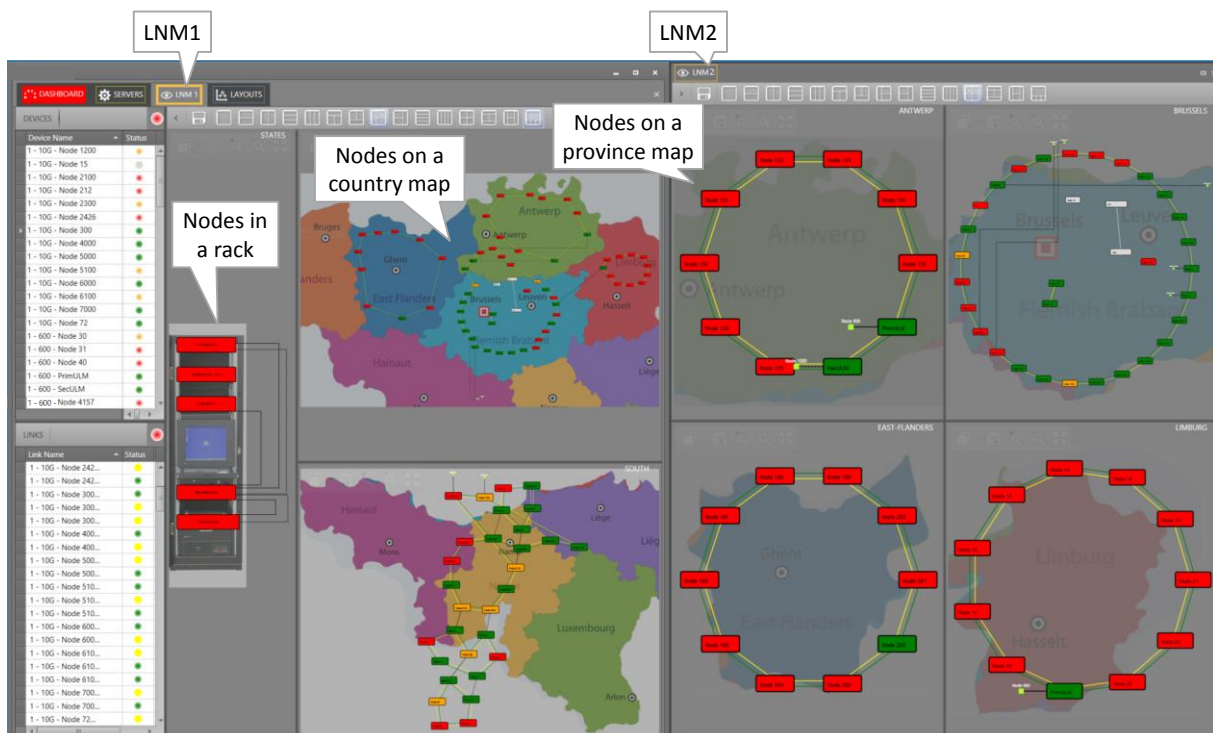


Figure 272 Large Network Monitor Live

28. MULTIPLE LANGUAGE SUPPORT

See §2.5.2c.

29. ADD-ONS

29.1 General

Add-ons provide extra integrated functionality in HiProvision and require purchased vouchers or licenses to operate. The available add-ons can be found in HiProvision via Dashboard → (Tools) Add-ons and are shortly described in the paragraphs below.

29.2 CAR IP

The CAR IP (=Central Alarm Reporter IP) add-on is an alarm interface between HiProvision and a CAS (=Central Alarm System) or umbrella management system both connected through an Ethernet link (UDP). This add-on requires a 'CAR IP Add-on' voucher (see §20.2) or license that must be purchased. A general CAR IP example can be found in the figure below. Find more information on this add-on in manual Ref.[20] in Table 1.

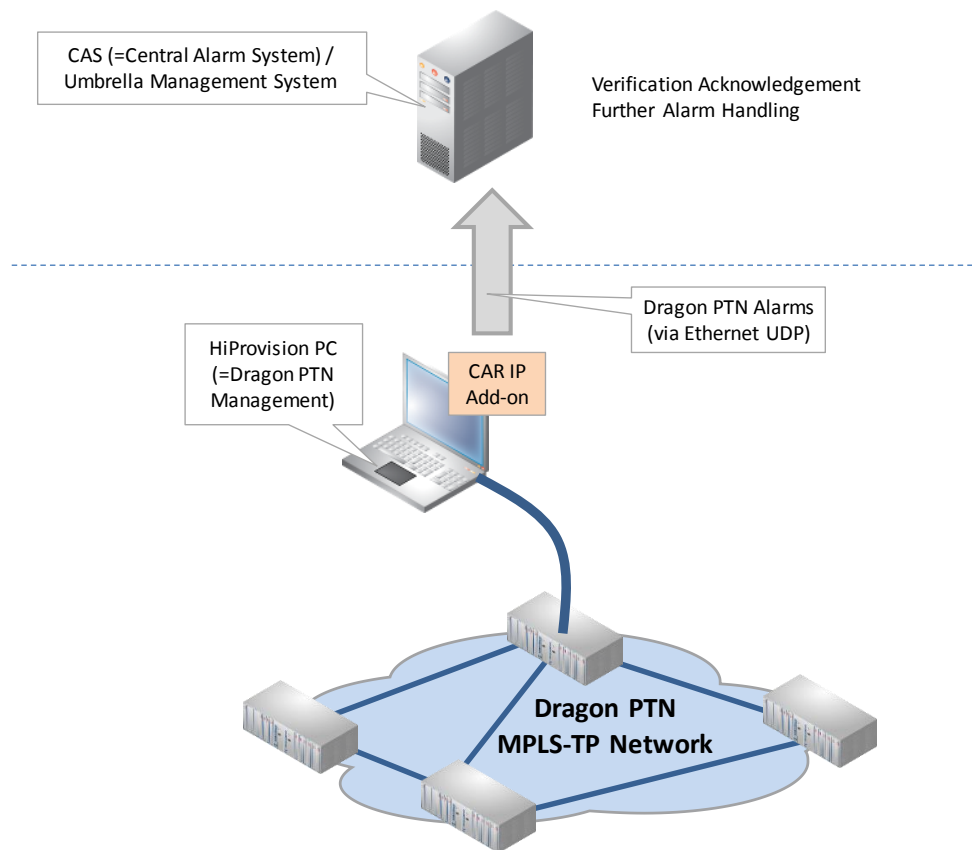


Figure 273 CAR IP Example

29.3 SNMP Northbound

This add-on provides alarm, counter and configuration status information from the Dragon PTN network through an SNMP (=Simple Network Management Protocol) interface to an upper management system (=umbrella system). This add-on requires an 'SNMP Northbound Add-on' voucher (see §20.2) or license that must be purchased. A general SNMP Northbound example can be found in the figure below. Find more information on this add-on in manual Ref.[21] in Table 1.

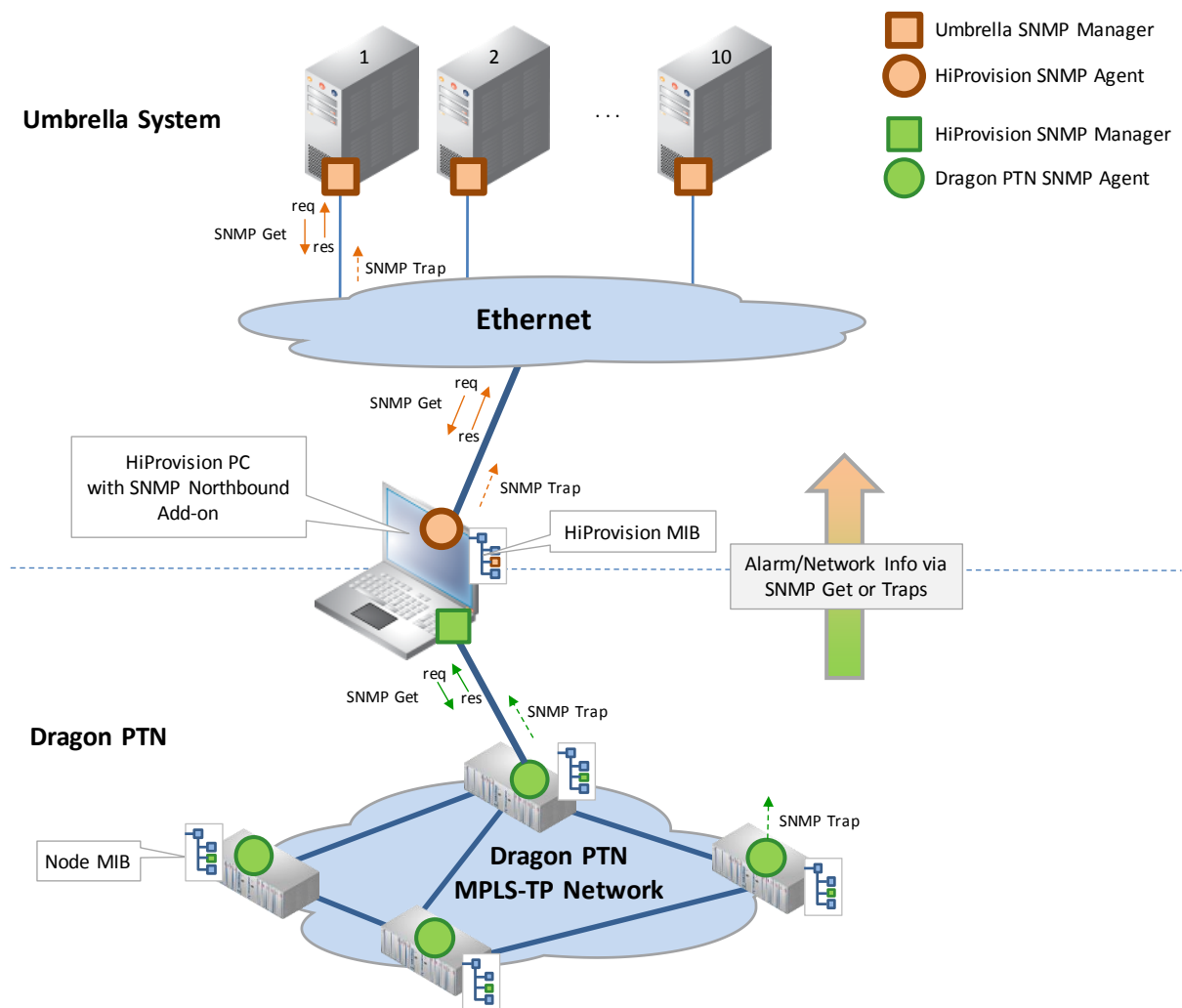


Figure 274 SNMP Northbound Example

29.4 Generic Reporting Engine

This add-on provides the possibility to generate different detailed Dragon PTN reports (template based), exported in different output formats. This add-on requires a 'Reporting Engine Add-on' voucher (see §20.2) or license that must be purchased. A general Reporting Engine example can be found in the figure below. Find more information on this add-on in manual Ref.[24] in Table 1.

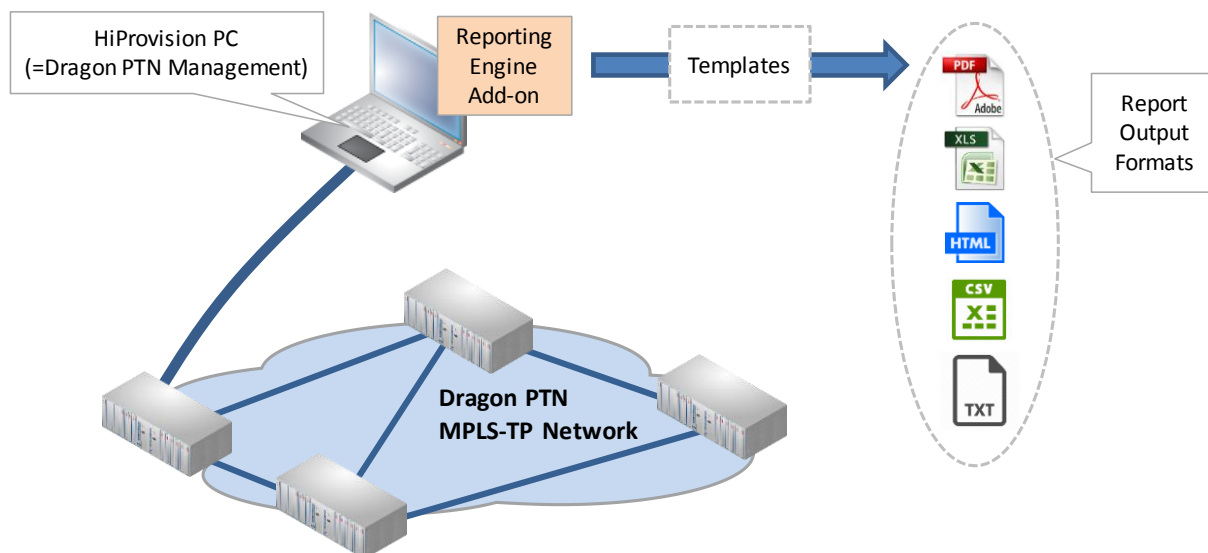


Figure 275 General: Reporting Engine

30. PORT MIRRORING

30.1 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 Interface Modules as described in §32.

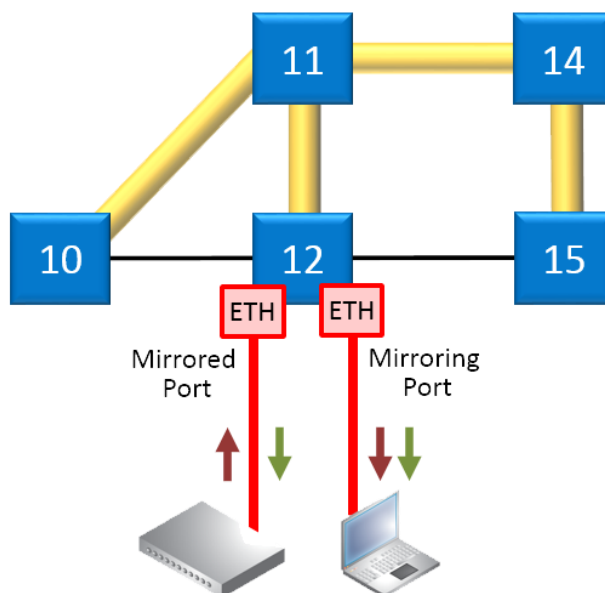



Figure 276 Port Mirroring

30.2 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 in §5.
- 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 → ;

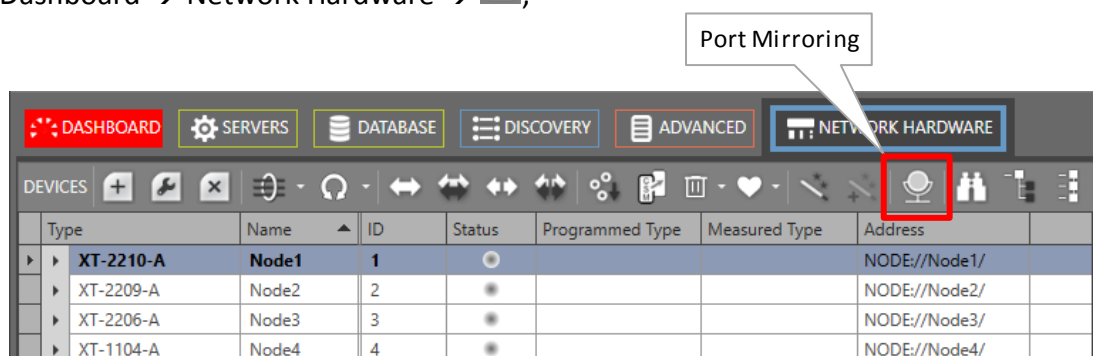


Figure 277 Port Mirroring Icon

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

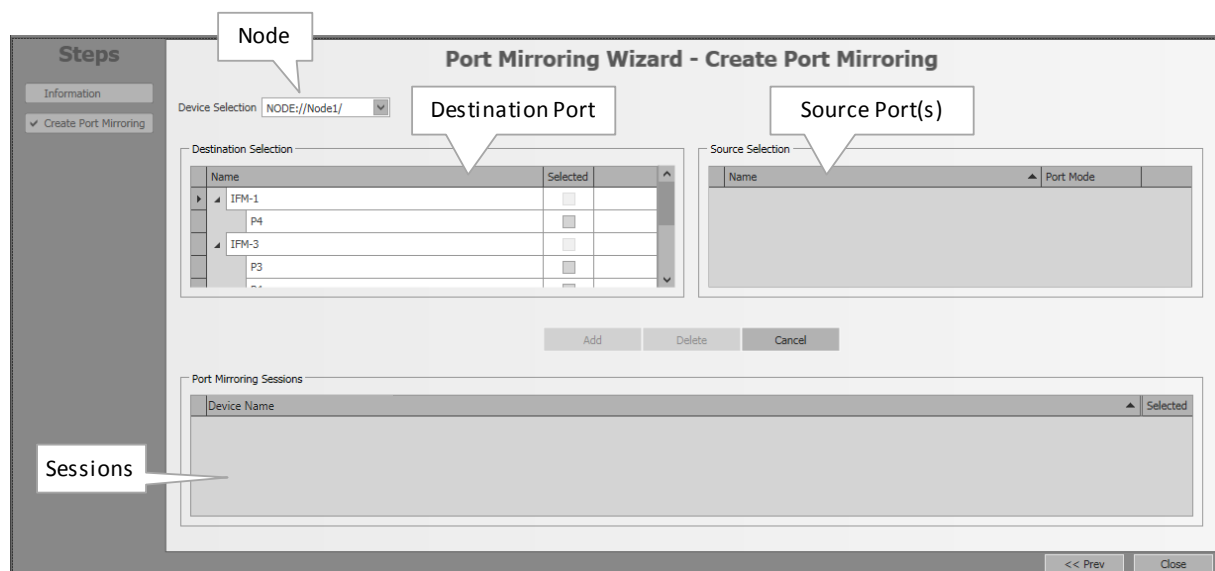


Figure 278 Port Mirroring Wizard

4. Follow the paragraphs below for further configuration.

30.2.1 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 Interface Modules 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.

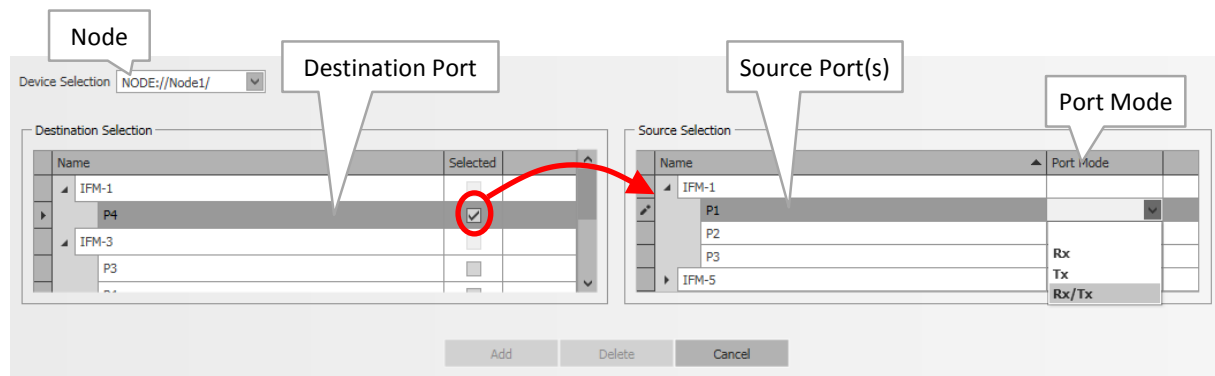


Figure 279 Destination/Source Ports

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.

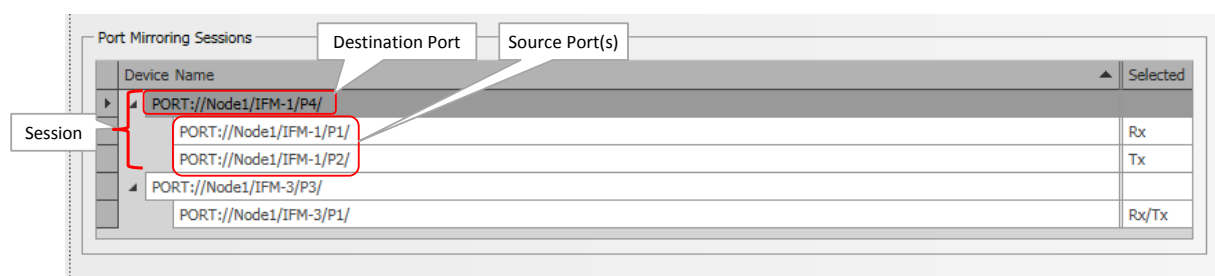


Figure 280 Port Mirroring Sessions

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.

30.2.2 Modify Port Mirroring

a. 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.

b. 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.

c. 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.

d. Change the Destination Port of a Mirroring Session

Not supported. The entire Mirroring session with the wrong destination port must be deleted first (see §30.2.3a). Next, a new mirroring session with the correct destination port must be added again (see §30.2.1).

30.2.3 Delete Port Mirroring

a. 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 that must be deleted 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.

b. Disable Port Mirroring on the Entire Node

Delete all mirroring sessions from the node by deleting session per session as described in §30.2.3a.

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 §30.2.3b.

31. ETHERNET SERVICES ON L2/L3 INTERFACE MODULES

31.1 General

L2/L3 Interface Modules (see §32) are advanced Interface Modules that require some extra attention when programming them in Ethernet services:

Service Types on L2/L3 Interface Module: see §31.2:

- ▶ Port Based;
- ▶ VLAN Based;
- ▶ Mixed VLAN;

VLAN Based Local Service, see §31.3;

VRF Ports (only on L3 Interface Module), see §31.4;

Back End Ports (BEn), see §31.5;

L2VPN, see §31.6;

L3VPN, see §31.7;

31.2 Service Types on L2/L3 Interface Modules

31.2.1 General

Some definitions that are used further on:

Back End Port (BE): the backside port of the L2/L3 Interface Module that connects to the CSM;

- ▶ Back End Link: link between Back End Port and CSM;

Basically you have 'single VLAN service' (=VLAN based) and 'mixed VLAN service' (=Port based).

- ▶ Single VLAN service: transports frames of a single VLAN ID through the Dragon PTN network. Multiple of these services can be configured per port, either front port or back end port;

Mixed VLAN service (=Port Based service):

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

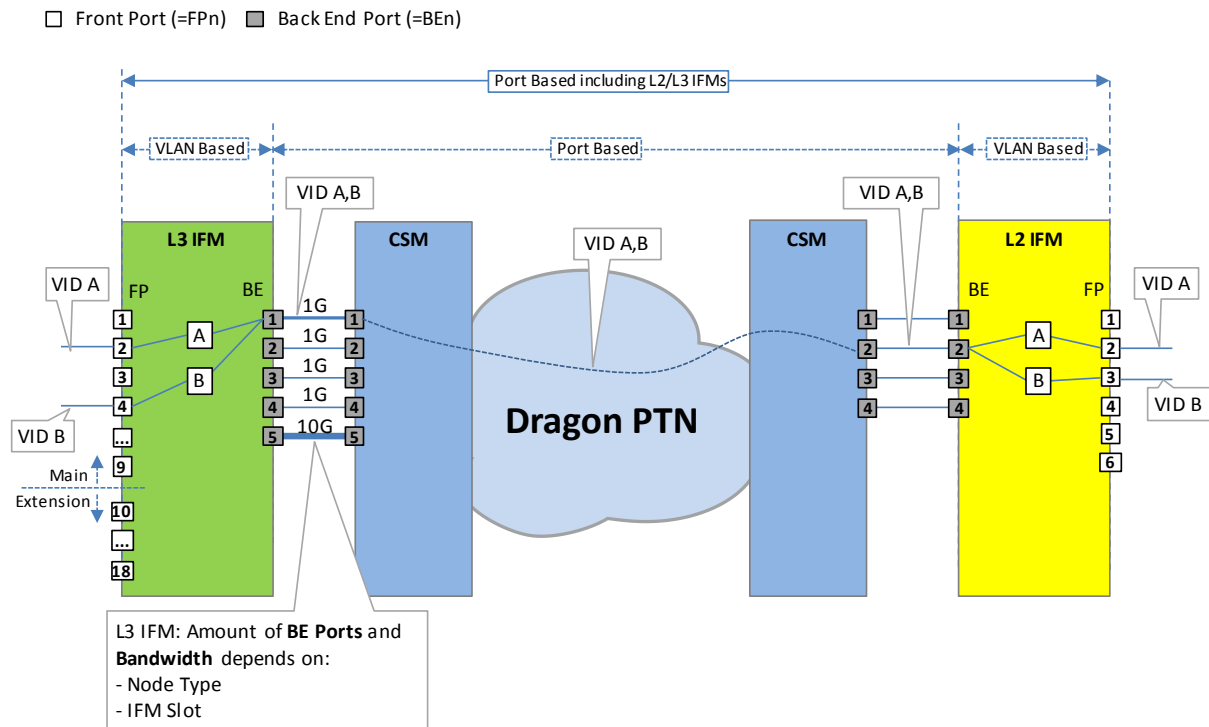


Figure 281 Port Based Service including L2/L3 Interface Modules: Mixed VLAN Service

31.2.2 When to Use Single VLAN/Mixed VLAN?

Mixed VLAN (port based):

- ▶ when MSTP is required network wide;
- ▶ (best practice) when you can combine some VLANs in one port based service (one common QoS) and almost consume the bandwidth of one entire Back End port to the CSM. VFI efficient: only consumes one VFI on the CSM (=max. 64 VFIs)!
- ▶ (best practice) Single VLAN based: probably any other use case than mentioned above. 1 VFI consumed on the CSM per single VLAN based service!

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

MSTP Use case:

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

31.2.3 Example: Mixed VLANs (=Port Based Service) For MSTP

Following example will be worked out more into detail:

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

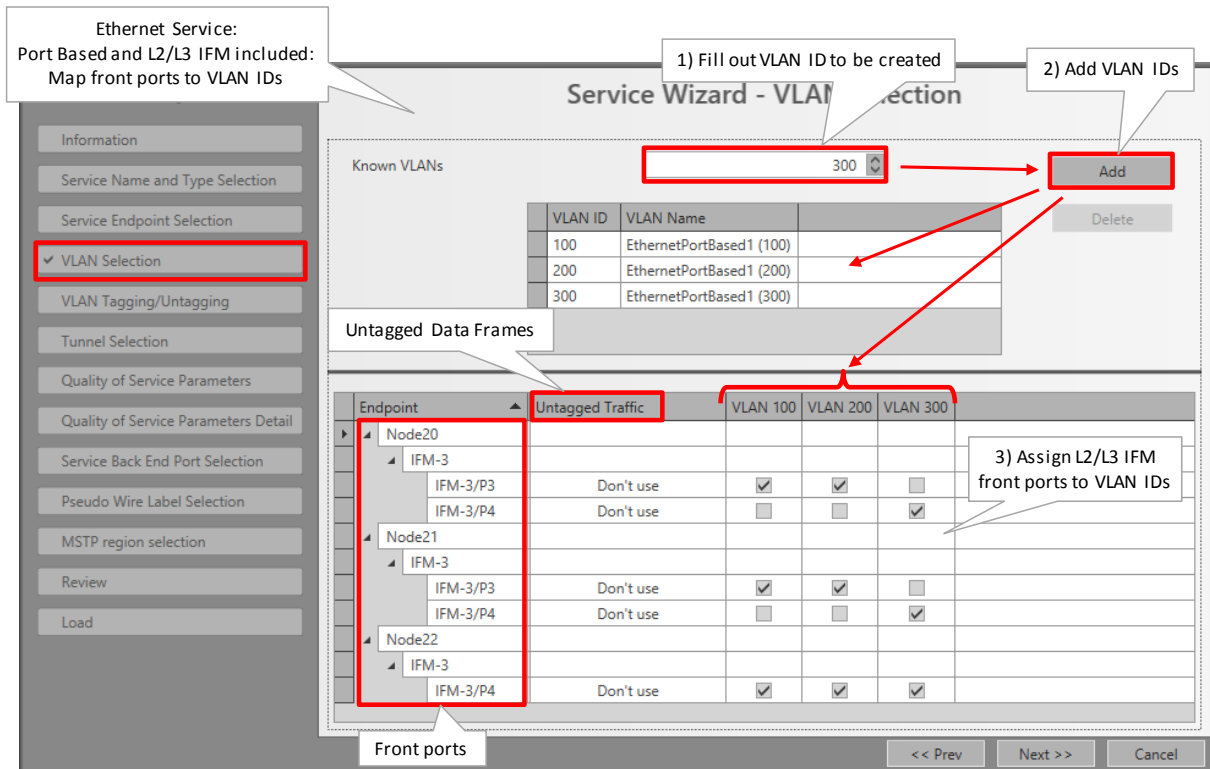


Figure 283 Example1: Service Wizard - Mixed VLANs: Map L2/L3 Interface Module Front Ports to VLANs

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

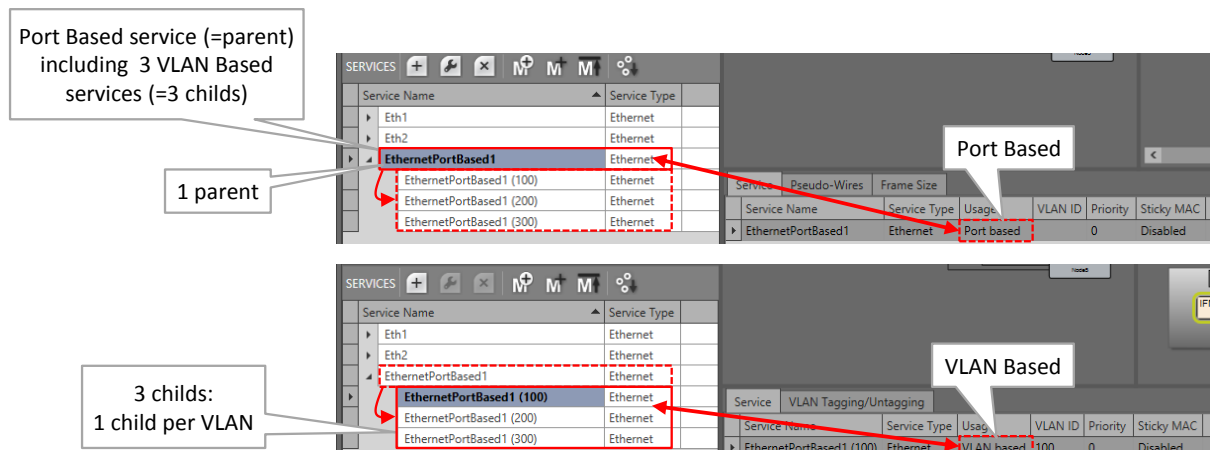


Figure 284 Example1: Mixed VLAN Service Created, Result in Services List

31.3 VLAN Based Local Service

31.3.1 General

A local service:

- ▶ is a VLAN based service between only LAN front ports on L2/L3 Interface Modules;
- ▶ does not use back end ports, tunnels, WAN ports, the Dragon PTN network;
- ▶ does not consume network bandwidth;
- ▶ allows internal connections in the same L2/L3 Interface Module;
- ▶ configures the selected front ports in the selected VLAN;
- ▶ over two or more nodes can be used together with an extra cable to save Dragon PTN network bandwidth. E.g. to close the ring for MSTP (L2) or VRRP (L3) outside the Dragon PTN network via the external cable, see example figure below:

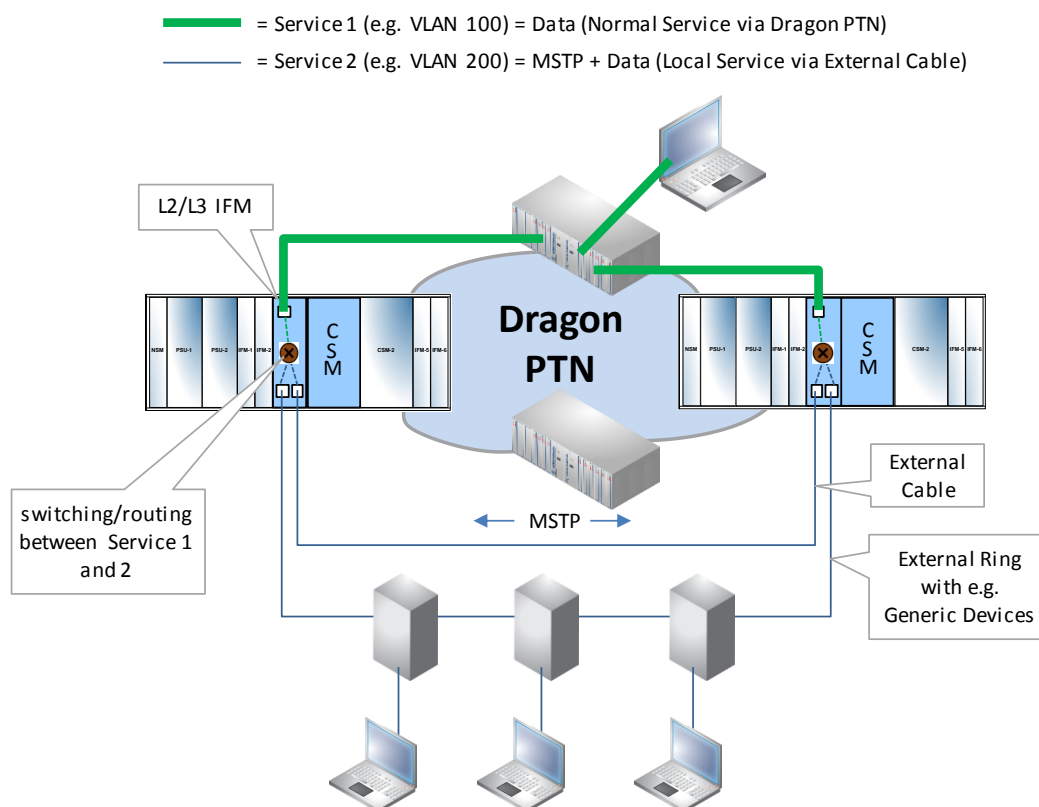


Figure 285 Local Service: Close an MSTP, VRRP Ring Outside the Dragon PTN Network

31.3.2 When to Use?

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

31.3.3 Configuration

- ▶ Service Wizard:
 - ▶ Service Name and Type Selection: Select VLAN based, fill out the VLAN ID and check the Local Service checkbox (=only active when selecting VLAN based);
 - ▶ Service Endpoint Selection: Select the front ports on the L2/L3 Interface Modules that must be part of this local service. For example, if you want to couple an external ring with external devices to the Dragon PTN network in Node1 and Node2, you will at least need two front ports in Node1 and two front ports in Node2 to complete the local service. Per node: One port to connect the external ring, and another port to connect the extra external cable (or network) to the other node;
 - ▶ VLAN Tagging/Untagging: configure the VLAN tagging/untagging behavior;

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

31.4 VRF Ports (Only L3 Interface Module)

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

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

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

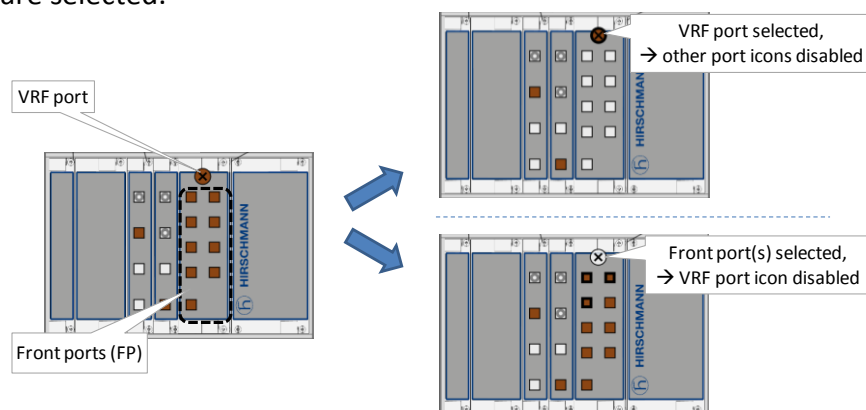


Figure 286 VRF Port and Front Ports on L3 Interface Module

For Port Based services:

- ▶ VRF ports and front ports of the same L3 Interface Module can be selected in the same service, provided that they are assigned to a different VLAN in the 'VLAN Selection' page in the wizard.

31.5 Back End Ports (BEn)

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

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

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

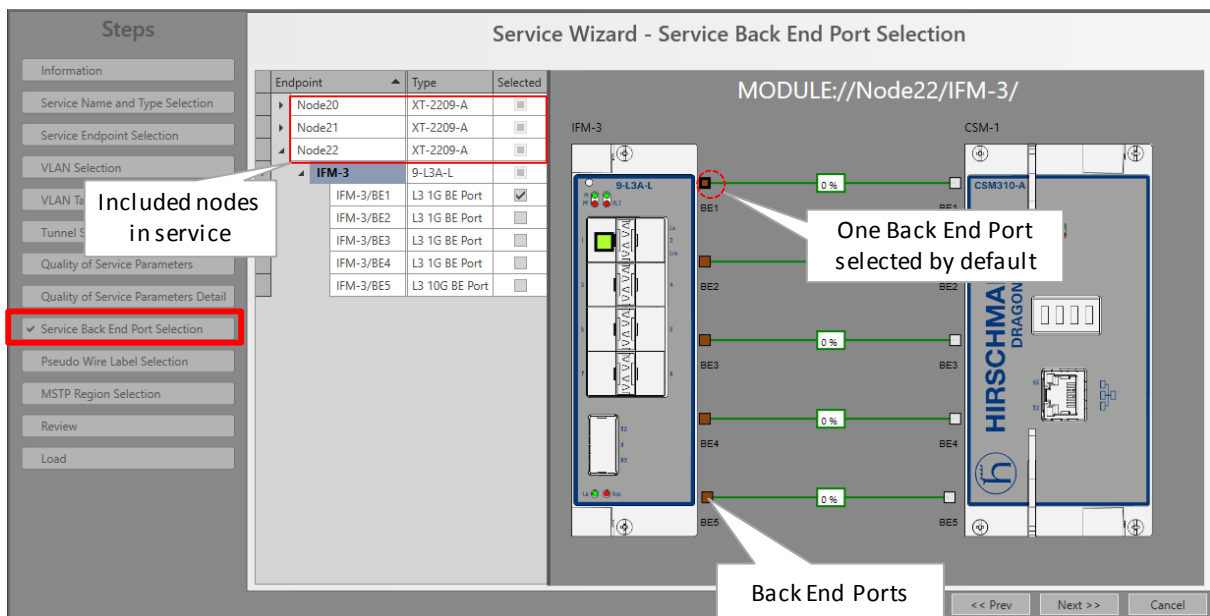


Figure 287 Default Back End Port View

If there is more than one BE link available, HiProvision tries to fill up by default the lowest BE number first e.g. BE1 link, then BE2 etc... If an additional service cannot fit anymore in the BE(n) link due to insufficient available bandwidth, or is port based, HiProvision tries to configure it in the BE(n+1) and so on. You can overrule this default programming behavior by selecting your desired BE link. For example, you could custom program your biggest services in the L3 Interface Module on BE5 (=10Gbps) (Node XT-2209-A) and program the smaller services on BE1-BE4 (=1Gbps).

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

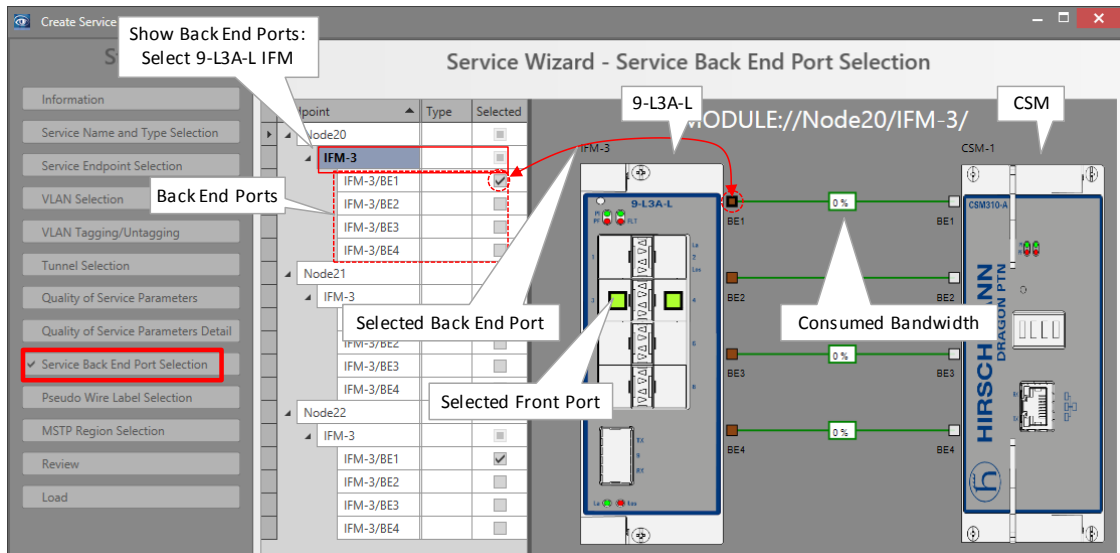


Figure 288 Customize Back End Port Selection

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

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

31.6 L2VPN

31.6.1 General

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

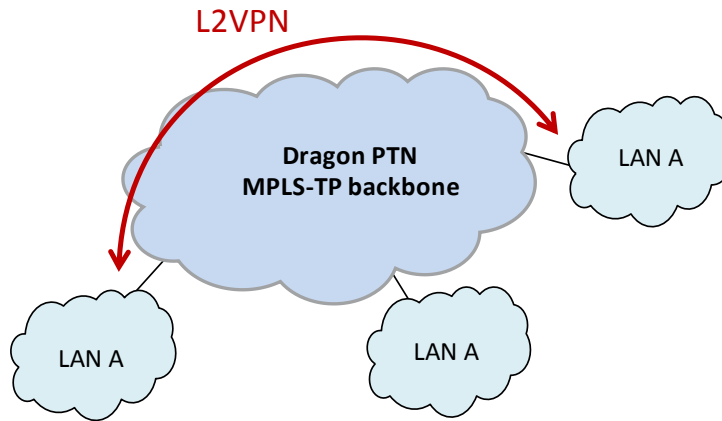


Figure 289 L2VPN General

31.6.2 Detailed Examples

See §31.2.

31.7 L3VPN

31.7.1 General

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

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

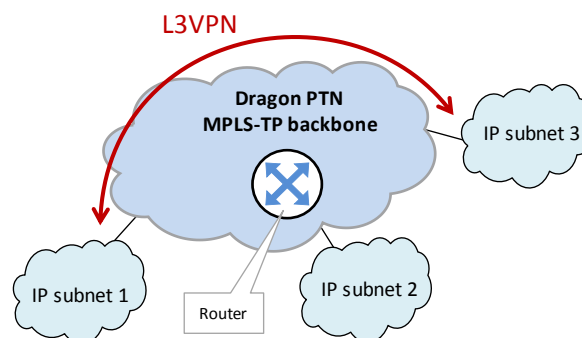


Figure 290 L3VPN General

General Steps to create a L3VPN:

1. MPLS-TP service creation. Bandwidth reservation and protection (ERPSv2 = Ethernet Ring Protection Switching) on backbone;
2. LAN creation (Local service connected to L3 Interface Module);
3. Virtual Router (VRF) creation: Interconnects MPLS-TP service Local LAN service;
4. (optional) Router Redundancy via VRRP (see §7.8);

5. Configure Routing protocol:
 - ▶ Only one router: no routing protocol must be configured;
 - ▶ Two routers: configure Static Routing (see §7.6);
 - ▶ More than two routers: configure a dynamic routing protocol OSPF (see §7.9);

31.7.2 Detailed Example: Steps

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

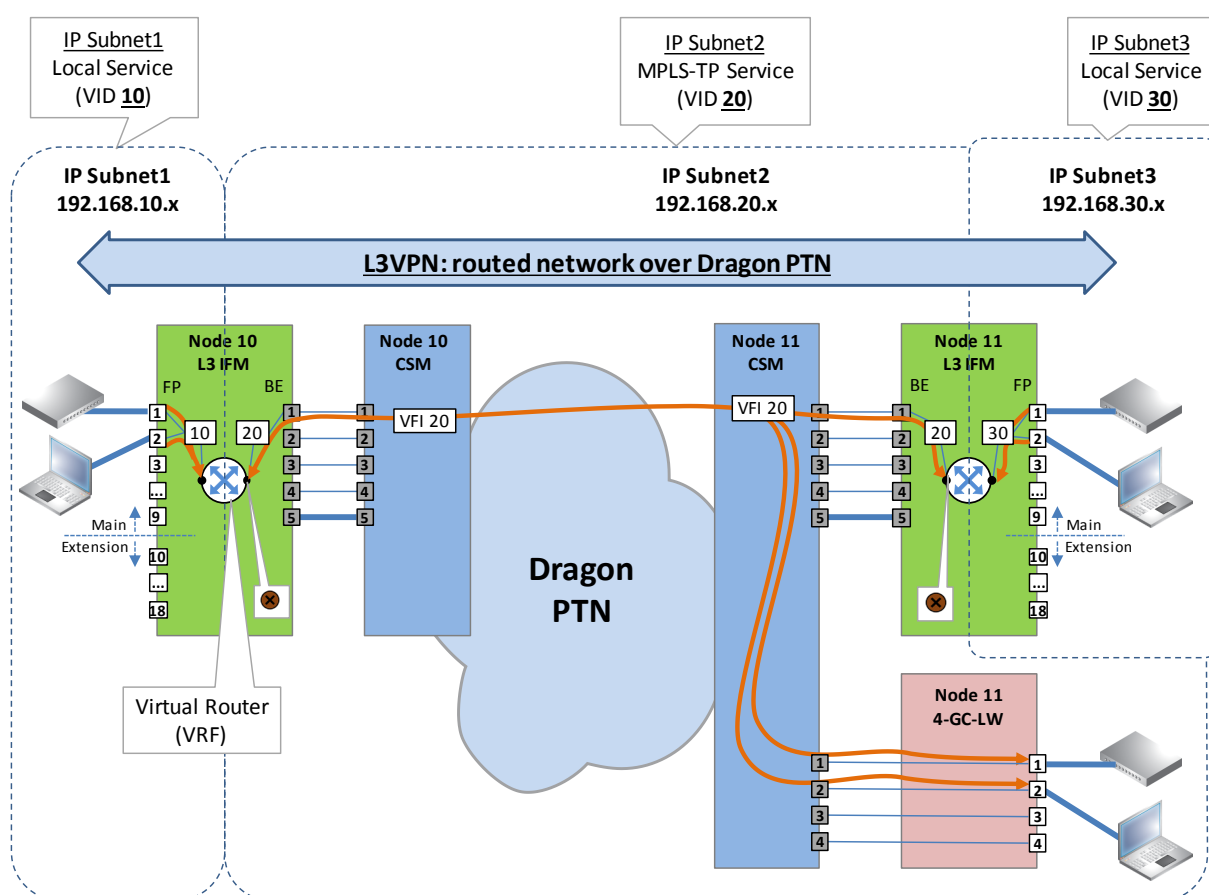


Figure 291 L3VPN Detailed Example

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

1. Create Local Service (IP Subnet1):
 - ▶ Service Type:
 - ▶ Ethernet Service;
 - ▶ VLAN Based: VLAN ID 10, Local Service checked. Note: A normal VLAN based service (Local Service = unchecked) can be used as well, but is less easy to modify later on (e.g. add extra VRF due to VRRP etc...);
 - ▶ End Point Selection:
 - ▶ Node 10:

- ▶ L3 Interface Module: front port 1 + port 2;
2. Create MPLS-TP service (IP Subnet2):
 - ▶ Service Type:
 - ▶ Ethernet Service;
 - ▶ VLAN Based: VLAN ID 20, Local Service unchecked;
 - ▶ End Point Selection:
 - ▶ Node 10: VRF port only on L3 Interface Module. This service has no LAN or front ports in this node, as a result only the VRF port ☒ must be selected;
 - ▶ Node 11:
 - ▶ L3 Interface Module: VRF port only. This service has no LAN or front ports in this Interface Module, as a result only the VRF port ☒ must be selected;
 - ▶ 4-GC-LW: front port 1 + port 2;
 - ▶ Back End Ports Selection on L3 Interface Module:
 - ▶ Node 10: BE1 (=default) is OK, any other port is also OK depending on your bandwidth customization;
 - ▶ Node 11: BE1 (=default) is OK, any other port is also OK depending on your bandwidth customization;
 3. Create Local Service (IP Subnet3):
 - ▶ Service Type:
 - ▶ Ethernet Service;
 - ▶ VLAN Based: VLAN ID 30, Local Service checked.
 4. Create Virtual Router (VRF) in Node 10, interconnect IP Subnet1 and 2:
 - ▶ Protocols: Layer 3: Virtual Router (see §7.5 for all Virtual Router configuration details). Find below the most important steps for this example.
 - ▶ Creation:
 - ▶ Module Selection: Node 10;
 - ▶ Port Selection: None;
 - ▶ Service Selection: Select both the IP Subnet1 Local Service and the IP Subnet2 MPLS-TP service to interconnect both IP Subnets via the Virtual Router;

Virtual Router Wizard - Creation

Steps: Information, **Creation**, Configuration, Properties, Review, Load

Module Selection

Name: VirtualRouter1

Device Name	Service Name	Selected
Node10	IFM-3	<input checked="" type="checkbox"/>
Node11		

Ports Selection

Device Name	Selected
P3	<input type="checkbox"/>
P4	<input type="checkbox"/>

Service Selection

Service Name	VLAN ID	Selected
Eth - IP Subnet2 - MPLS-TP	20	<input checked="" type="checkbox"/>
Eth - IP Subnet1 - Local Service	10	<input checked="" type="checkbox"/>

<< Prev Next >> Cancel

Figure 292 Interconnect IP Subnet1 and 2

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

Steps

- Information
- Creation
- ✓ Configuration

Virtual Router Wizard - Configuration

Assign IP addresses to IP Subnet1 and 2

Device Name	IP Address
Eth - IP Subnet1 - Local Service	192.168.10.1/24
Eth - IP Subnet2 - MPLS-TP	192.168.20.1/24

Figure 293 Assign IP Addresses to IP Subnet1 and 2

- Create Virtual Router (VRF) in Node 11, interconnect IP Subnet2 and 3:
 - Protocols: Layer 3: Virtual Router (see §7.5 for all Virtual Router configuration details). Find below the most important steps for this example.
 - Creation:
 - Module Selection: Node 11;
 - Port Selection: None;
 - Service Selection: Select both the IP Subnet3 Local Service and the IP Subnet2 MPLS-TP service to interconnect both IP Subnets via the Virtual Router;

Steps

- Information
- ✓ Creation
- Configuration
- Properties
- Review
- Load

Virtual Router Wizard - Creation

Select 9-L3A-L Module

Name: VRRouter2

Module Selection

Device Name	Selected
Node11	<input checked="" type="checkbox"/>
IFM-3	<input checked="" type="checkbox"/>

Ports Selection

Device Name	Selected
P3	<input type="checkbox"/>

Interconnect IP Subnet2 and 3

Service Selection

Service Name	VLAN ID	Selected
Eth - IP Subnet2 - MPLS-TP	20	<input checked="" type="checkbox"/>
Eth - IP Subnet3 - Local Service	30	<input checked="" type="checkbox"/>

<< Prev Next >> Cancel

Figure 294 Interconnect IP Subnet2 and 3

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

Steps

- Information
- Creation
- ✓ Configuration

Virtual Router Wizard - Configuration

Assign IP addresses to IP Subnet2 and 3

Device Name	IP Address
Eth - IP Subnet2 - MPLS-TP	192.168.20.2/24
Eth - IP Subnet3 - Local Service	192.168.30.1/24

Figure 295 Assign IP Addresses to IP Subnet2 and 3

- (Optional, not in this example) Create VRRP if you have configured two Virtual Routers and they have to be redundant (see §7.8);
- Configure Routing if you have at least 2 virtual routers: For a small amount of virtual routers (e.g. 2), you could choose to configure Static Routing (see §7.6) or a dynamic

routing protocol OSPF (see §7.9). For more than 2 routers, it is advised to use OSPF. In this example, we configure OSPF.

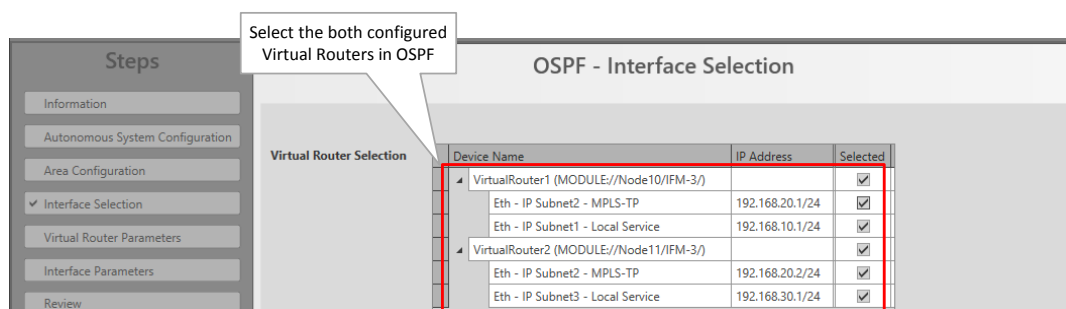


Figure 296 Configure OSP: Select Both Virtual Routers

32. PROTOCOL AND FEATURE SUPPORT MATRIX

Table 60 Protocol and Feature Support Matrix

Protocol, Feature	Ref.	Interface Modules					
		PTN-8-FXS	PTN-4-4WEM-L, PTN-4-CODIR, PTN-7-SERIAL, PTN-2-OLS, PTN-4-DSL-LW	PTN-4-E1-L/ PTN-4-T1-L, PTN-16-E1-L/ PTN-16-T1-L, PTN-2-C37.94	Ethernet Interface Modules: PTN-4-GC-LW, PTN-4-GCB-LW, PTN-4-GO-LW, PTN-1-10G-LW	Layer2 Interface Modules: PTN-6-GE-L	Layer3 Interface Modules: PTN-9-L3A-L PTN-9-L3EA-L
Backbone MPLS-TP Network							
WAN Ports	§2.11	---	---	---	Yes	---	---
Synchronisation							
SyncE	§13	---	Yes on PTN-2-OLS E1 ports	Yes	Yes	---	---
PTP IEEE 1588v2	§14	---	---	---	Yes, as Transparent Clock, not as Grandmaster, Boundary clock nor Ordinary Clock	---	---
Hardware							
LAG + LACP	§35	---	---	---	---	Yes	Yes
PoE	§21	---	---	---	Yes, on PTN-4-GC-LW	---	---
Smart SFP	§23	---	---	---	Yes on PTN-4-GO-LW ports or PTN-4-GC-LW /PTN-4-GCB-LW front port 1	---	---
Services							
Ethernet	§2.13	Yes	Yes on PTN-4-DSL-LW	---	Yes	Yes	Yes
Ethernet: Local Service	§31.3	---	---	---	---	Yes	Yes
Circuit Emulation	§2.13	---	Yes (except PTN-4-DSL-LW)	Yes	---	---	---
Serial Ethernet	§2.13	---	Yes on PTN-7-SERIAL	---	---	---	---

Protocol, Feature	Ref.	Interface Modules					
		PTN-8-FXS	PTN-4-4WEM-L, PTN-4-CODIR, PTN-7-SERIAL, PTN-2-OLS, PTN-4-DSL-LW	PTN-4-E1-L/ PTN-4-T1-L, PTN-16-E1-L/ PTN-16-T1-L, PTN-2-C37.94	Ethernet Interface Modules: PTN-4-GC-LW, PTN-4-GCB-LW, PTN-4-GO-LW, PTN-1-10G-LW	Layer2 Interface Modules: PTN-6-GE-L	Layer3 Interface Modules: PTN-9-L3A-L PTN-9-L3EA-L
Voice	§2.13	Yes (analog Voice)	---	---	Yes (VoIP)	Yes (VoIP)	Yes (VoIP)
Optical Low Speed Serial	§2.13	---	Yes on PTN-2-OLS	---	---	---	---
Protocol Interaction (Layer2 Access Ring Protection Protocols)							
MRP	§7.2	---	---	---	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	§7.4	---	---	---	---	---	Yes
MSTP	§7.3	---	---	---	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
Layer3							
Virtual Router	§7.5	---	---	---	---	---	Yes
Static Routing	§7.6	---	---	---	---	---	Yes
VRRP	§7.8	---	---	---	---	---	Yes
OSPF	§7.9	---	---	---	---	---	Yes

Protocol, Feature	Ref.	Interface Modules					
		PTN-8-FXS	PTN-4-4WEM-L, PTN-4-CODIR, PTN-7-SERIAL, PTN-2-OLS, PTN-4-DSL-LW	PTN-4-E1-L/ PTN-4-T1-L, PTN-16-E1-L/ PTN-16-T1-L, PTN-2-C37.94	Ethernet Interface Modules: PTN-4-GC-LW, PTN-4-GCB-LW, PTN-4-GO-LW, PTN-1-10G-LW	Layer2 Interface Modules: PTN-6-GE-L	Layer3 Interface Modules: PTN-9-L3A-L PTN-9-L3EA-L
L3VPN	§31.6	---	---	---	---	---	Yes
PIM	§7.10	---	---	---	---	---	Yes
IGMP	§7.11	---	---	---	---	---	Yes
DHCP Relay	§7.12	---	---	---	---	---	Yes
Traffic Control / Security							
Ethernet: E-Tree	§25	---	---	---	Yes	---	---
Storm Control	§3.11	---	---	---	Yes, Port Properties	Yes, Port Properties	Yes, Port Properties
BPDU Guard	§34	---	---	---	Yes, Port Properties	Yes, included in Layer2 MSTP Wizard	Yes, included in Layer2 MSTP Wizard
IP ACL	§7.13	---	---	---	Yes (max. 1 rule)	Yes (max. 128 rules)	Yes (max. 128 rules)
MAC ACL	§7.14	---	---	---	Yes (max. 1 rule)	Yes (max. 128 rules)	Yes (max. 128 rules)
Sticky MAC	§24.1.1	Yes	Yes on PTN-7-SERIAL	---	Yes	Yes (Back End Ports)	Yes (Back End Ports)
MAC Limit	§24.1.2	Yes	Yes on PTN-7-SERIAL	---	Yes	Yes	Yes
Static MAC Table	§24.1.3	Yes	---	---	Yes	Yes (Back End Ports)	Yes (Back End Ports)
Test & Debugging							
Test & Loopback	§15.3, §18	---	Yes	Yes	---	---	---
Loss Measurement (LM)	§16.2	Yes	Yes	Yes	Yes	---	---
Delay Measurement (DM)	§16.3	Yes	Yes	Yes	Yes	---	---
Tunnel Ping	§16.4	Yes	Yes	Yes	Yes	---	---

Protocol, Feature	Ref.	Interface Modules					
		PTN-8-FXS	PTN-4-4WEM-L, PTN-4-CODIR, PTN-7-SERIAL, PTN-2-OLS, PTN-4-DSL-LW	PTN-4-E1-L/ PTN-4-T1-L, PTN-16-E1-L/ PTN-16-T1-L, PTN-2-C37.94	Ethernet Interface Modules: PTN-4-GC-LW, PTN-4-GCB-LW, PTN-4-GO-LW, PTN-1-10G-LW	Layer2 Interface Modules: PTN-6-GE-L	Layer3 Interface Modules: PTN-9-L3A-L PTN-9-L3EA-L
Tunnel Traceroute	§16.5	Yes	Yes	Yes	Yes	---	---
Port Mirroring	§30	Yes, intra node: - can only be a source, can be mirrored to Ethernet Interface Modules	Yes, intra node: - can only be a source, can be mirrored to Ethernet Interface Modules	Yes, intra node: - can only be a source, can be mirrored to Ethernet Interface Modules	Yes, intra node: - source can be any Interface Module except L3 Interface Module - destination: Ethernet Interface Modules	Yes, same Interface Module: source and destination must be same L2 Interface Module	Yes: source and destination can be a mix of main and extension L3 Interface Module
MAC Monitor	§24.1.4	Yes	Yes on PTN-7-SERIAL	---	Yes	Yes	Yes

33. EXTERNAL DEVICE TYPES

33.1 General

It is possible in HiProvision to create External Device Types in order to monitor third party devices. Also the links from Dragon PTN to these devices and the links between them will be monitored.

1. Create new External Devices types: Dashboard → Advanced tile, see §33.2;
2. Create new devices based on this new type: Dashboard → Network Hardware tile → Devices, see §33.3;
3. Create Monitored Links via Dashboard → Network Hardware tile → Links, see §33.4:
 - ▶ between the Dragon PTN network and these devices;
 - ▶ between these devices themselves;
4. Configure Monitoring and Alarming of External Devices, see §33.5;

33.2 Add New External Device Type

1. Go to Dashboard → Advanced → External Devices Types;

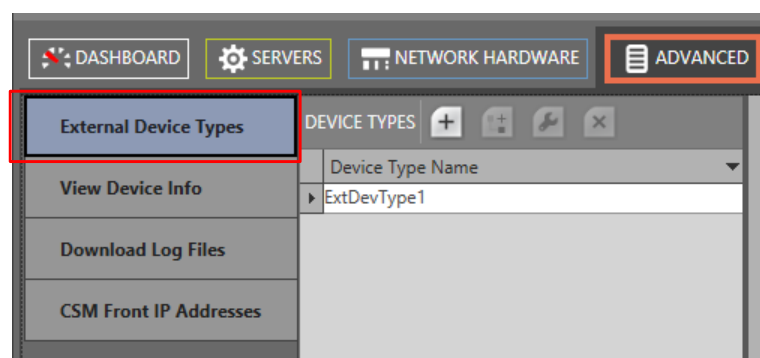







Figure 297 External Devices Types

Table 61 External Device Types: Menu Buttons

Button	Short Description
	Adds a new External Device Type.
	Copies the selected Device Type.
	Rename the existing Device Type. CAUTION: Renaming the device type automatically deletes all existing devices in HiProvision with the original Device Type Name.
	Deletes the selected Device Type. CAUTION: it also deletes all the configured devices of this type.

2. Click Devices Types →  to add a device type. Fill out the device type in the figure below, e.g. ExtDevType2 and click OK;

CAUTION: Use correct spelling! Renaming afterwards automatically deletes all existing devices in HiProvision of the original Device Type Name.

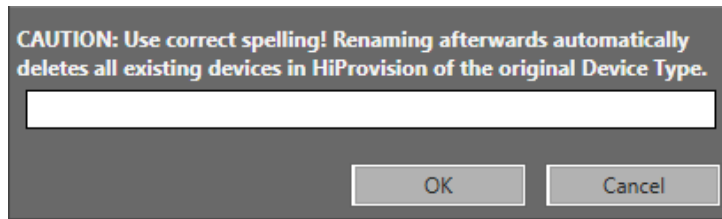


Figure 298 Create External Device Type

3. The window below is shown. Assign the correct Base Type to the created device type. Select Hirschmann for Hirschmann devices and Generic for any other device type. In this example, select Generic.
4. System OID: For custom alarming/monitoring: Fill out the System OID from the MIB file of the external device type, e.g. 1.2.3.4.5.6.7. More info on the System OID in §33.5.4 and Table 62.
5. Monitoring Table Version (only visible for Hirschmann devices):
 - ▶ Classic (=default): uses OID **1.3.6.1.4.1.248.14.5.3** as reference monitoring OID;
 - ▶ HiOS: uses OID **1.3.6.1.4.1.248.11.40.1.1.1** as reference monitoring OID;
6. Monitoring Table OID:
 - ▶ For Hirschmann devices: Only fill out this field when another OID must be used than the one defined in the 'Monitoring Table Version' field. If the 'Monitoring Table OID' is filled out, the Classic/HiOS selection still matters to know which parameters or column names must be monitored.
7. Supports (Optional): Check the protocol that your external device supports: MRP. If MRP is checked, external devices connected to Dragon PTN will be detected for participating in the MRP protocol in §7.2.
8. Version (Optional): This can be used by the user for versioning, but it's not used by the Generic Device framework.
9. Cycle Interval (default = 60000 ms): indicates the interval in which HiProvision polls (via SNMP poll) and measures the external devices of this device type.
10. Click the Image Select button to assign an image to the device type;

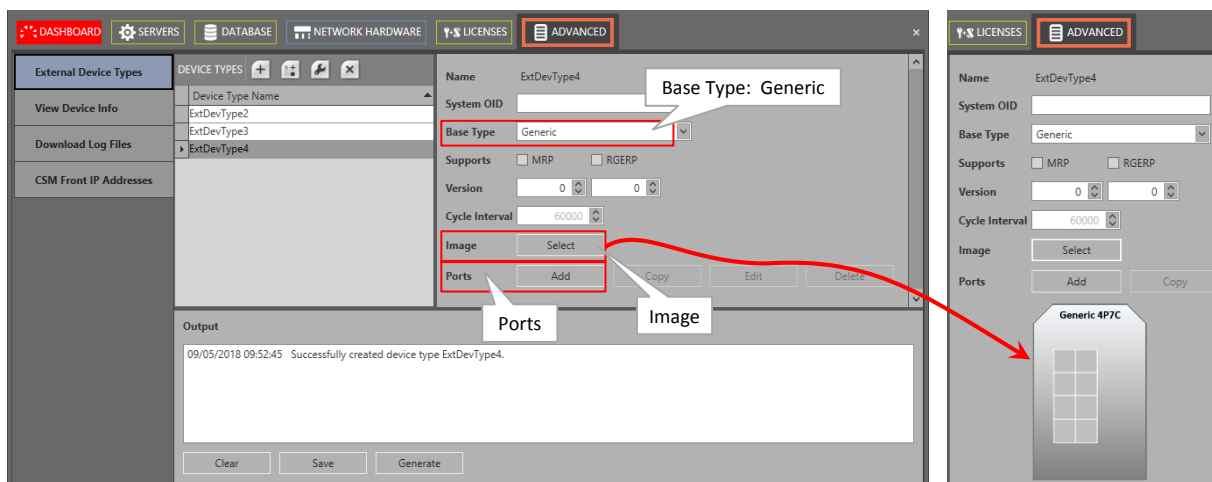


Figure 299 External Device Type: Base Type and Image

11. Click the Ports Add button to add a port. The window below pops up. The name is by default 'Port<n>'. <n> is a number that automatically increases with every port that you add. If desired, change and customize the Name and click Close.
- NOTE:** Ports can be copied, edited and deleted via the Copy/Edit/Delete buttons.



Figure 300 External Device Type: Add Port

12. A red border port icon ■ will be placed somewhere onto the device type picture. Drag and drop the port icon into the right place on the corresponding port slot. Repeat these two steps until all ports are added and positioned in the correct port slot.

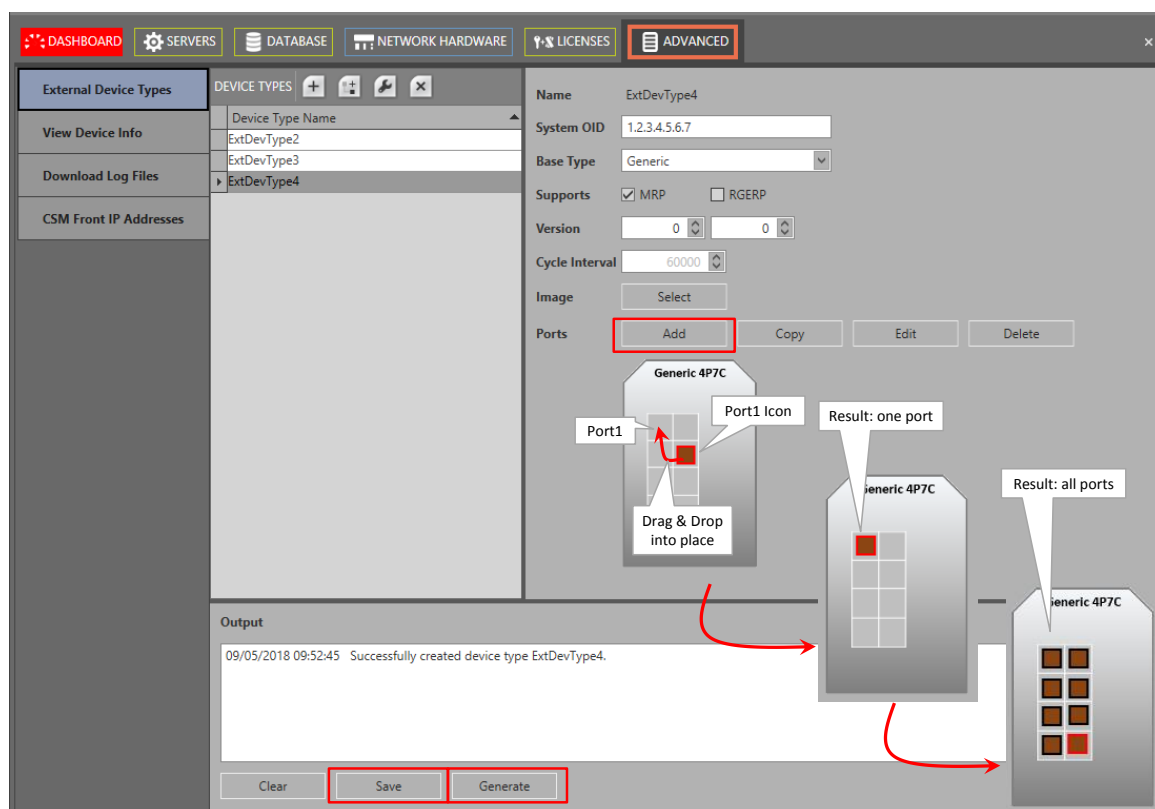



Figure 301 External Device Type: Drag & Drop Ports Into Place

13. Click the Save button to save your configuration and generate an XML file which might be needed later on to customize monitoring and alarming of properties;
14. Click the Generate button to make these new device types available later on in the Device Type list in the Network Hardware Tile;

15. To update the devices types list in the Network Hardware Tile: stop the Servers (Servers Tile → stop button) first, then shut down and restart both the HiProvision Client and Agent;
16. Login in HiProvision and start the Servers via the Servers Tile → play button;
17. From now, this new type can be selected to create devices, see the following paragraph;

33.3 Create New External Device

1. Go to Network Hardware Tile → Devices → ;
2. The newly created external device type shows up in the Device Type list and can be selected to create a new device for your network drawings. Fill out the Name, Type and ID and click the Create button.

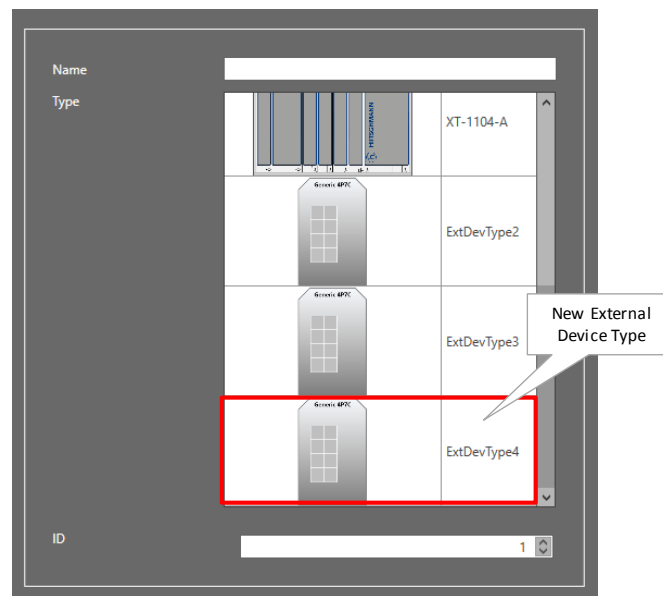


Figure 302 External Device: New Device Type in Device List

3. Fill out the connection parameters below, allowing HiProvision to monitor this device.
 - ▶ Mgt. IP Address: the IP address of the external device;
 - ▶ SNMP V2:
 - ▶ checked (=default): use SNMP V2;
 - ▶ unchecked: use SNMP V3;
 - ▶ Community:
 - ▶ private (=default): indicates read-write access to the external devices, write access is required to set trap registrations on the external devices;
 - ▶ public: indicates read access only.

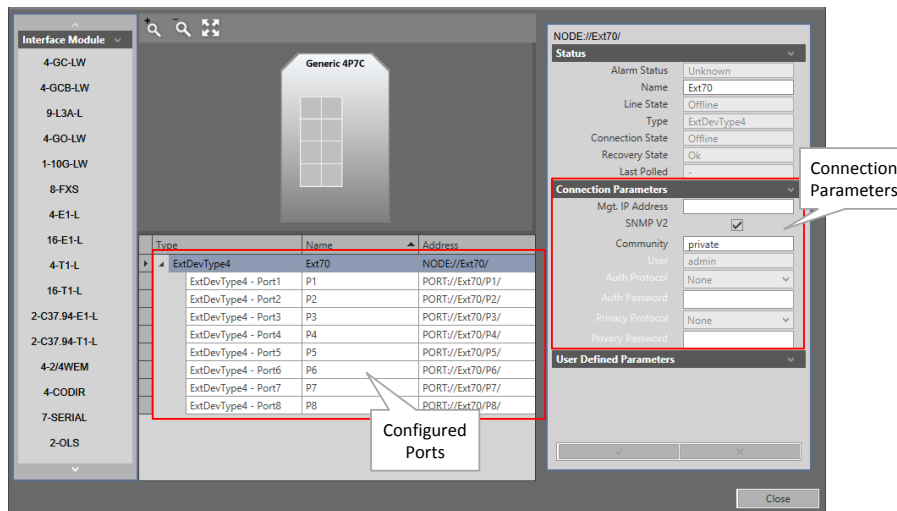


Figure 303 External Device: Connection Parameters

- Click the Close button. The created external device appears in the Devices list.

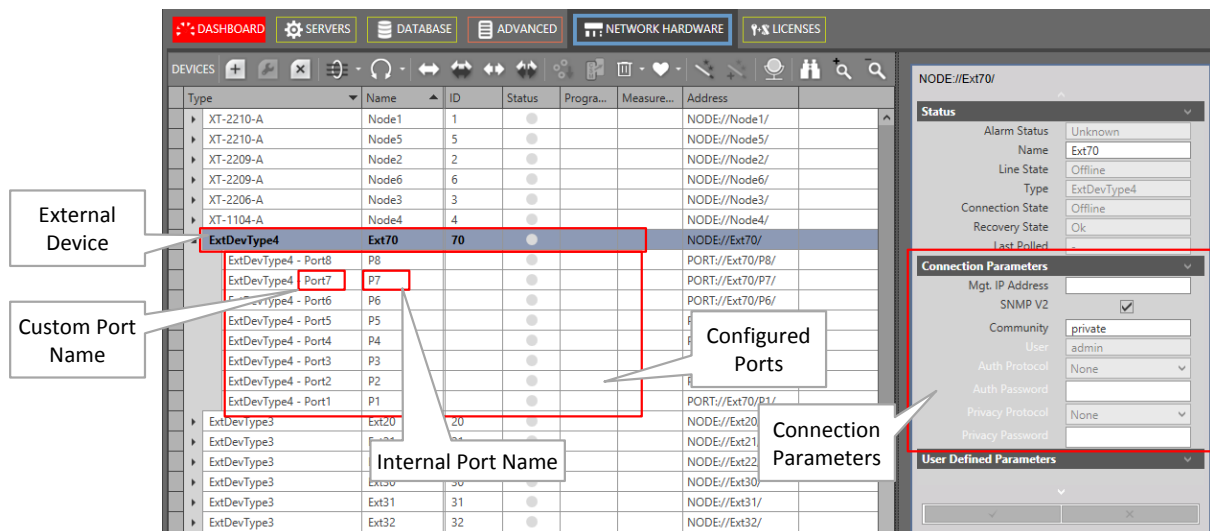



Figure 304 External Device: Created External Device



33.4 Linking External Devices to Dragon PTN

Prerequisite: make sure that the correct vouchers are purchased and the corresponding license pack has been installed.

Once the External Devices have been created, they still have to be connected to the Dragon PTN network.

- Make a physical connection between the External Devices and Dragon PTN via connecting the device to an Ethernet LAN port on an Ethernet Interface Module (PTN-4-GC-LW...) or an L2/L3 Interface Module in Dragon PTN;
- Create a 'Monitored Link' (via Network Hardware Tile → Links →  → Monitored Link) between all the external devices and the Ethernet ports in Dragon PTN;
- Make sure that all the external devices are reachable via the filled out connection parameters in previous paragraph. HiProvision cannot discover the external devices via

the normal DCN path. Therefore, an extra physical path between a second NIC in the HiProvision PC and the external devices must be created, e.g. via an external network or via a configured Ethernet service over Dragon PTN, either routed or not.

4. Connect via clicking the buttons  or  in the network hardware tile;
5. If the External Devices can be connected via HiProvision, the External Devices (=rounded icons) including the Monitored Links should turn green, indicating that all is OK (=no alarms). Any other color than green indicates some kind of alarm.

NOTE: If there are problems with a link not coming up, verify the IfTableIndex of all the <port> tags in the XML file (see §33.5.4f). The IfTableIndex value of each <port> tag must match with its value in the MIB file of the external device. If the IfTableIndex is missing in the <port> tag, add it with the correct value from the MIB;

NOTE: Performance between the HiProvision server and the external devices can be improved, see §10.8.

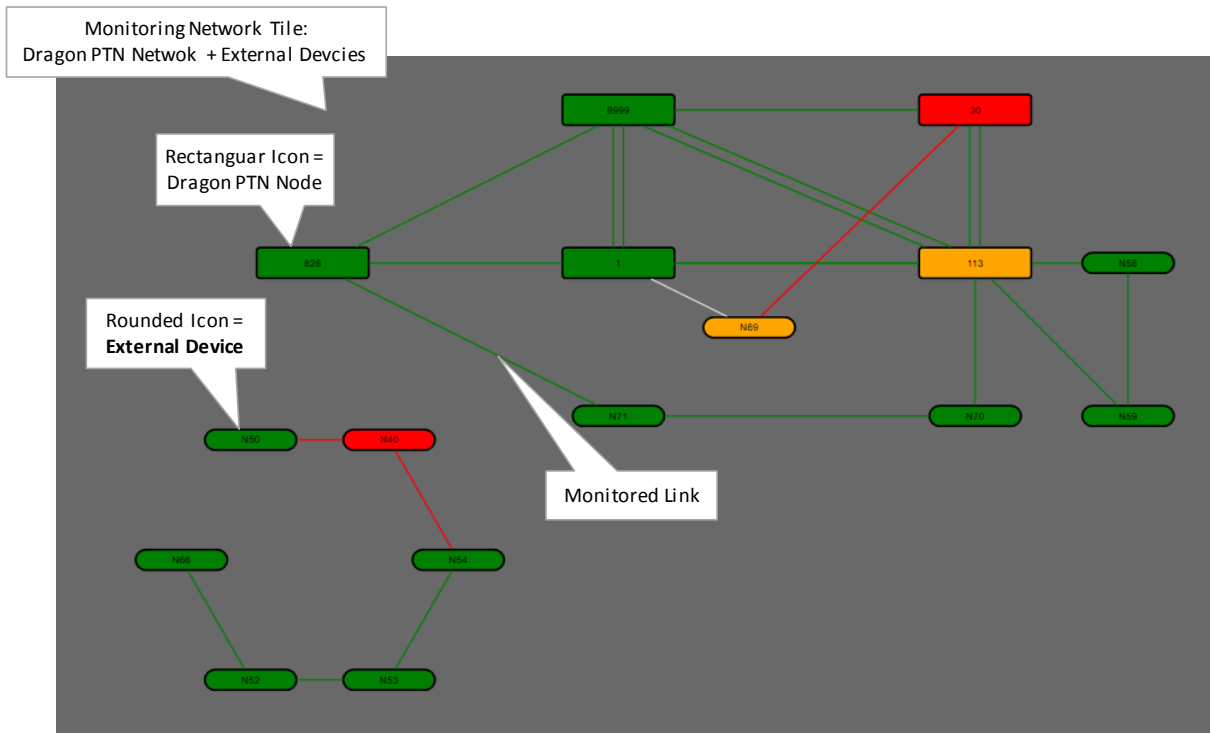


Figure 305 Dragon PTN Network + External Devices

NOTE: The Discovery function (see §2.6) is not relevant for External Devices.

33.5 Monitoring and Alarming of External Devices

33.5.1 Prerequisites

Make sure that HiProvision can connect to the external devices as described in previous paragraph.

33.5.2 General

The external device and port properties in the Network Hardware tile in the figure below are monitored in HiProvision via SNMP Poll and Trap (→SNMP Poll and Trap, see §33.5.3).

The default properties are always available in HiProvision. Custom properties in the 'User Defined Parameters' section can be added via customizing an XML file per external device type, not per device.

The MIB file of the external device type must be used as a source or reference to customize the XML file syntactically correct (→ XML file customization, see §33.5.4).

Figure 306 Default and Custom Properties

33.5.3 SNMP Poll and Trap

HiProvision combines the SNMP Poll and Trap techniques to monitor (=measure) the External Devices.

► SNMP Poll:

- HiProvision starts the communication;
- Periodic: HiProvision periodically requests, by default every 60 seconds, information from all the configured External Devices. This polling interval can be overruled by setting the 'CycleIntervalOverride' property of the root element in the XML (see Table 62) or by filling it out in §33.2;
- Trap-based: HiProvision also re-polls the External Device that sends an SNMP trap to HiProvision. This extra poll will request all the parameter info from the device and not only the parameter that trapped;
- Updates (the measured values off) the default and custom properties in HiProvision;
- Polling cannot be disabled.

► SNMP Trap:

- The external device starts the communication;
- A message that External Devices immediately send to notify HiProvision when something occurs in the External Devices, e.g. port down, temperature too high, PoE disabled....;

- ▶ Trap generation can be enabled/disabled per property (see §33.5.4j);
- ▶ Does not influence a HiProvision device/port property directly, it triggers HiProvision to start a new poll cycle.

33.5.4 XML File Customization for Custom Properties

a. General

All External Device configuration files are placed in `<HiProvision Installation path>\GenericDevices`. This allows multiple HiProvision installations to reuse the same configuration files. These files are insensitive to HiProvision upgrades. The GenericDevices folder contains two subfolders:

Config folder: contains all the XML configuration files, one XML file per device type. E.g. ExtDevType2.xml;

Resources folder: contains the images for the External Device Types;

XML example files, see `<HiProvision Installation path>\HiProvision_V<version>\Documentation\GenericDevices`. This folder could be entirely copied to `<HiProvision Installation path>\HiProvision_V<version>\GenericDevices` or you could copy some XML files from these folders as a sort of template to start with.

b. Step Overview

Follow the steps below to add custom properties for monitoring. All these steps are explained in more detail in the paragraphs below.

1. Open the MIB file (e.g. via a MIB browser) of your external device;
2. Decide which device and port properties you want to monitor;
3. Search these properties in the MIB file of the external device type;
4. Open the XML file in a text editor, e.g. Notepad;
5. Add the desired device properties in the XML file with respect to the syntax and case-sensitivity used in the MIB file;
 - ▶ Name;
6. Repeat the same for all the desired port properties. Note that you have multiple ports using the same properties. Use the IfTableIndex and RowIndex attribute to differentiate between ports;
 - ▶ Name, IfTableIndex, RowIndex, ;
7. Add a PropertyDefinition for each unique device and port property in the XML file;
 - ▶ Name, Oid, PropertyType, SnmpType, Alarm (optional);
8. Add an AlarmDefinition in the XML file for each unique PropertyDefinition that has PropertyType="Reading";
 - ▶ Name, Severity, Message, Text, Help;
9. Add a TrapRegistration for each desired property that must send traps to HiProvision:
 - ▶ Oid, Value, RowIndex, SnmpType, Comment;
10. Save and Close the XML file;
11. Apply XML changes in HiProvision and the live Dragon PTN network, see §33.5.4k;

c. XML Structure Overview

CAUTION: XML file content is case-sensitive! XML tags must have the exact same case as used in the examples below. Properties, attributes, values must have the exact same case as used in the MIB files of the device type!

A basic XML file structure has following major parts (=root element + root child elements). The parts are still empty, but are explained further on;

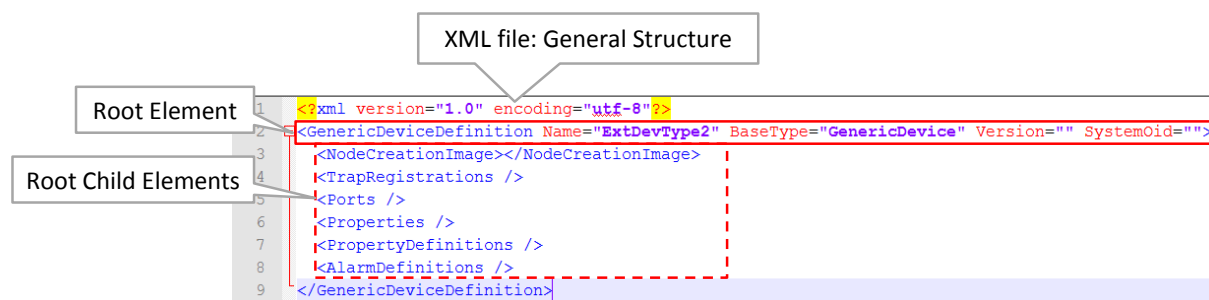


Figure 307 XML File: General Structure

GenericDeviceDefinition: the root element of the External Device, having its own properties e.g. Name, BaseType... all its properties are listed in the table below;

Table 62 XML File: Root Element Properties

Root Element Property	Short Description
Name	The name of the device type.
BaseType	Must be one of the following values: Generic, Hirschmann.
Version (optional)	This can be used by the user for versioning, but it's not used by the Generic Device framework. Can be filled out as well via §33.2.
SystemOid	The root OID of the system in the external device MIB. This makes it easier to change it later in one place instead of numerous places in the XML. It's also used by the properties. For example, let's say that all external devices have a system name property with OID '{{SystemOid}}.1.1'. The first bit of the OID is usually the same and the second part differs per external device type. This way the property can be defined in a generic way. The {{SystemOid}} pattern is replaced at runtime by the actual SystemOid of the device. Can be filled out as well via §33.2.
HirschmannMonitoringFamily	Only visible for Hirschmann devices: - Classic (=default): uses OID 1.3.6.1.4.1.248.14.5.3 as reference monitoring OID - HiOS: uses OID 1.3.6.1.4.1.248.11.40.1.1.1 as reference monitoring OID Can be filled out as well via §33.2.
MonitoringTableOid	For Hirschmann devices: OID required to fill out the Hirschmann MRP Monitoring tables (see §7.2.4) in TXCare. Only use this field if the OID is different from the Classic or HiOS OID defined via the HirschmannMonitoringFamily parameter. Can be filled out as well via §33.2.
CycleIntervalOverride (optional)	Generic devices have a slow polling interval combined with updates when traps are received (trap-based polling). By default the cycle interval is 60000 ms (=60 seconds). Use this property to override this interval. The value must be in milliseconds. Can be filled out as well via §33.2.

TrapReceivePortOverride (optional)	Traps are received on port 6021 and 6022 by default. Some Generic Devices send traps to other ports (162 by default). Use this attribute to make HiProvision listen on extra ports.
SupportsMrp (optional)	If the value=True, then external devices of this device type support MRP. Can be filled out as well via §33.2.

All the child elements of the root element are described in the table below.

Table 63 XML File: Root Child Elements

Root Child Element	Short Description
NodeCreationImage	The file name (without extension) of the image for this device type. The image will be used in different HiProvision screens. Do not change manually, only change images via the wizard!
TrapRegistrations (optional)	If you want to receive traps from a device of this type, certain OIDs have to be set on the device (such as the IP address of HiProvision). The trap registrations are a list of all OIDs that have to be set to certain values for a device of this type to enable the traps that you're interested in.
PropertyDefinitions	Definitions of all the properties that you want to monitor on this device and its ports. The definitions include things such as OID, SNMP type, display name, possible min and max value, enum values, translations, ... Adding a property here, does not automatically add it to the device type. You still have to reference it in the Properties section of the device or the ports. - IntPropertyDefinition: the property is numeric, e.g. portStatusIndex; - StringPropertyDefinition: the property is not numeric but a string, IpAddress, MacAddress, ..., e.g. systemName; - EnumPropertyDefinition: the property has a set of values e.g. portStatusLink (value1 = up; value2 = down);
AlarmDefinitions	The alarm definitions for the properties defined in the PropertyDefinitions section that can raise alarms. An alarm definition includes things such as the severity, the message or help texts and possible translations.
Properties	The properties that you want to monitor on the device level (=not port level). Each of these properties has its own PropertyDefinition.
Ports	The list of port definitions for this device type. Every port has a name, a location (=XY coordinates) and a list of properties that you want to monitor. Each of these properties has its own PropertyDefinition.

d. XML: Device Picture

- **NodeCreationImage:** the filename of the device image (in the Resources folder) after generating the External Device in via the Generate button. Do not change manually in the XML, only change images via the wizard!

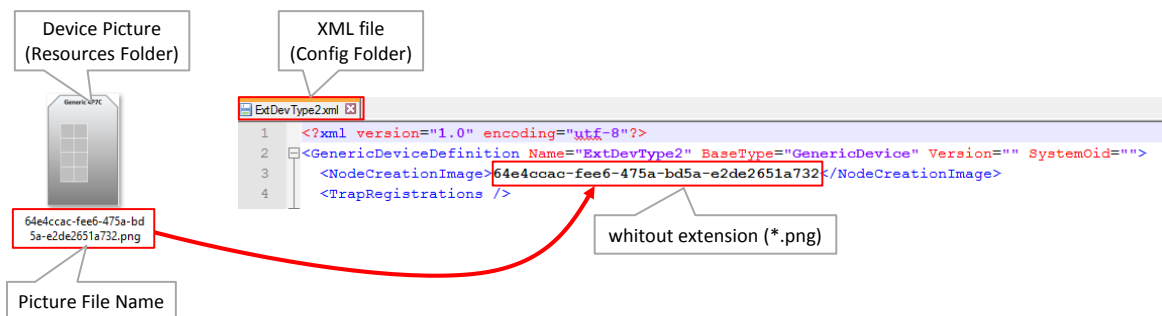


Figure 308 External Device Picture In XML File

e. XML: Device Properties

A device has multiple properties and each unique property in the XML file must have a Property Definition, referred by Name. If the property must be able to raise alarms, set the PropertyType = "Reading" in the Property Definition and add an Alarm Definition, see further. If no alarms are needed, set PropertyType = "Indication".

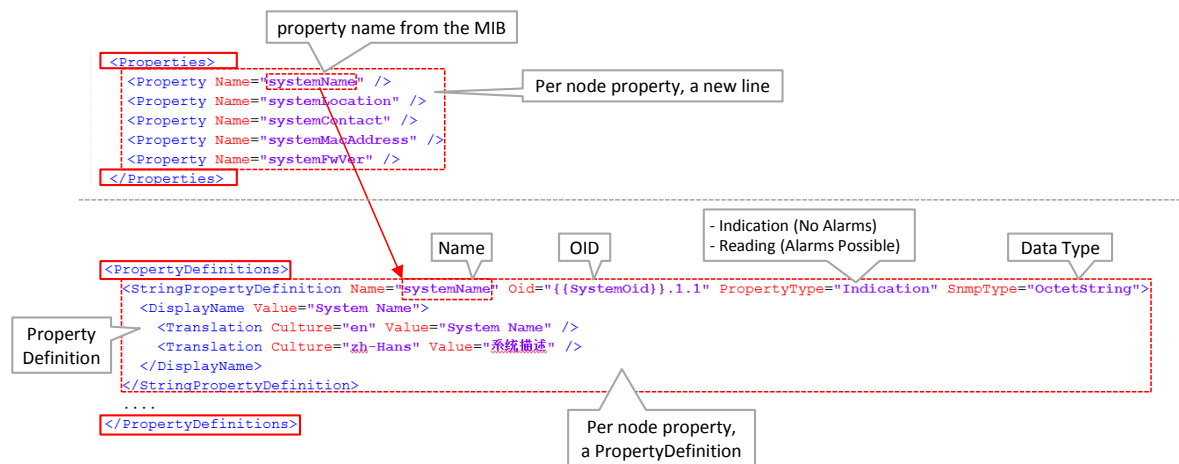


Figure 309 XML: Device Properties/Property Definition

f. XML: Port Properties

A port has multiple properties. Each unique port is identified by the value of the IfTableIndex attribute in the <port> tag. Each unique property in the XML file must have a Property Definition as well. If the property must be able to raise alarms, set the PropertyType = "Reading" in the Property Definition and add an Alarm Definition, see further. If no alarms are needed, set PropertyType = "Indication".

A port contains the following attributes:

Name: the name of the port;

RelativeLocation: the XY location of the port icon on the device Image, the port icon is used to create links in the link wizard. Valid values range from -0.5 to 0.5 in both x and y direction. (0, 0) would be the center of the image, while (0.5, -0.5) would be the upper right image corner;

IfTableIndex: the index in the IF table in the MIB. This value identifies the correct port. This value is used as RowIndex value in the <property> tag. Make sure this value is filled out for each port.

A port has the following child elements:

Properties: a list of properties to monitor on this port. Every property refers to a property definition by name. Every property must have a RowIndex to differentiate between ports with the same properties. The RowIndex can contain the {{IfTableIndex}} pattern, in which case it is replaced by the value of the IfTableIndex property on the port definition.

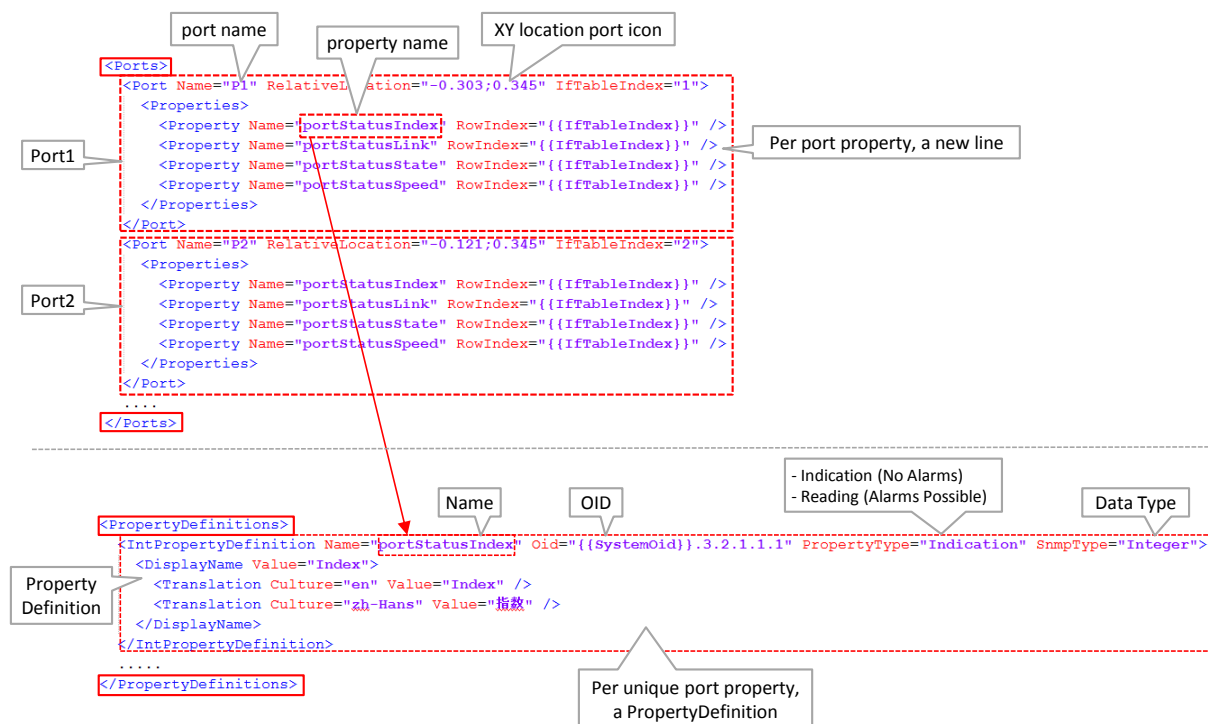


Figure 310 XML: Port Properties/Property Definition

g. XML: Property Definitions

There are 3 types of property definitions:

IntPropertyDefinition: the property is numeric, e.g. portStatusIndex;

StringPropertyDefinition: the property is not numeric but a string, IpAddress, MacAddress, ..., e.g. systemName;

EnumPropertyDefinition: the property has a set of values e.g. portStatusLink (value1 = up; value2 = down);

Table 64 XML File: PropertyDefinition Attributes

Attribute	Short Description
Required	
Name	The name of the property in the MIB. This is used to refer to it, in the Properties section of the device type or the Properties sections of the ports (see below).
Oid	The full OID in the MIB. It is advised to replace the root OID part with the {{SystemOid}} variable for a better overview and more consistency in your XML file. Example: You can use: <GenericDeviceDefinition Name="ExtDevType2" BaseType="GenericDevice" SystemOid="1.2.3.4.5"> <IntPropertyDefinition Name="portStatusIndex" Oid="1.2.3.4.5.1.2" PropertyType="Indication" SnmpType="Integer"> or (better, advised): <GenericDeviceDefinition Name="ExtDevType2" BaseType="GenericDevice" SystemOid="1.2.3.4.5"> <IntPropertyDefinition Name="portStatusIndex" Oid="{{SystemOid}}.1.2" PropertyType="Indication" SnmpType="Integer">
PropertyType	- Indication: does not raise alarms - Reading: can raise alarms
SnmpType	The data type definition, it has to match a value in 'XML SnmpType' column in Table 65.
Alarm (required for 'Reading' properties)	A reference to the alarm definition in 'AlarmDefinitions' that has to be used when this property raises an alarm.

Attribute	Short Description																
Optional																	
DefaultValue	The default value used by 'Reading' properties to check if an alarm has to be raised. A string for string properties, an integer for integer and enum properties.																
MinimumValue (only for integer properties)	The minimum value used by 'Reading' properties to check if an alarm has to be raised.																
MaximumValue (only for integer properties)	The maximum value used by 'Reading' properties to check if an alarm has to be raised.																
EnumValues (only for enum properties)	<p>A set of values (=EnumValues). Every enum value has a name, an id, a value and optional translations. The Name and Id have to match the value list in the MIB description. How the value is displayed in HiProvision can be tuned via the Value attribute and/or Translation lines.</p> <p>Example: The port status can be up or down: - portStatusLink in MIB (values {up(1), down(2)})</p> <div style="display: flex; align-items: center;"> <div style="margin-right: 20px;"> <p>Enum Values: {Name(Id), ...}</p> <table border="1"> <tr><td>Name</td><td>portStatusLink</td></tr> <tr><td>OID</td><td>.1.3.6.1.4.1.3185.4.1.3.3.2.1.1.3</td></tr> <tr><td>Syntax</td><td>INTEGER {up(1),down(2)}</td></tr> <tr><td>Access</td><td>read-only</td></tr> <tr><td>Status</td><td>current</td></tr> <tr><td>DefVal</td><td></td></tr> <tr><td>Indexes</td><td>portStatusIndex</td></tr> <tr><td>Descr</td><td>Indicate the link state of the port.</td></tr> </table> </div> <div style="text-align: center;"> <p>MIB</p> <p>↓</p> <p>XML</p> <p>→</p> <p>TXCare</p> </div> </div> <pre> <EnumPropertyDefinition Name="portStatusLink" Oid="{[SystemOid]}.3.2.1.1.3" PropertyType="Reading" SnmpType="Integer" Alarm="portStatusLinkAlarm"> <DisplayName Value="Link"> <Translation Culture="en" Value="Link" /> <Translation Culture="zh-Hans" Value="链接" /> </DisplayName> <EnumValues> <EnumValue Name="up" Id="1" Value="Up"> <Translation Culture="en" Value="Up" /> <Translation Culture="zh-Hans" Value="向上" /> </EnumValue> <EnumValue Name="down" Id="2" Value="Down"> <Translation Culture="en" Value="Down" /> <Translation Culture="zh-Hans" Value="向下" /> </EnumValue> </EnumValues> </EnumPropertyDefinition> </pre> <div style="margin-top: 20px;"> </div>	Name	portStatusLink	OID	.1.3.6.1.4.1.3185.4.1.3.3.2.1.1.3	Syntax	INTEGER {up(1),down(2)}	Access	read-only	Status	current	DefVal		Indexes	portStatusIndex	Descr	Indicate the link state of the port.
Name	portStatusLink																
OID	.1.3.6.1.4.1.3185.4.1.3.3.2.1.1.3																
Syntax	INTEGER {up(1),down(2)}																
Access	read-only																
Status	current																
DefVal																	
Indexes	portStatusIndex																
Descr	Indicate the link state of the port.																

h. Mapping: MIB Syntax / XML SnmpType

Table 65 Properties: Mapping: MIB Syntax / XML SnmpType

MIB Syntax	XML SnmpType	Short Description
OCTET STRING, DISPLAYSTRING	BitString	String that has only 0 and 1, that represents binary data
OCTET STRING, DISPLAYSTRING	BitStringToInteger	String containing a bit-representation of an integer value (ex: "10111101001")
Counter32	Counter32	Unsigned 32-bit counter.
Counter64	Counter64	Unsigned 64-bit counter
Gauge32	Gauge	SNMP gauge
OCTET STRING	HexOctetStringInteger	A hex octet string (in SNMP) representing a specific elapsed time in milliseconds
OCTET STRING, DISPLAYSTRING	HexString	String containing a hexadecimal value (ex: "f044d2")
INTEGER	Integer	SNMP integer
IPADDRESS	IpAddress	SNMP ipaddress
MACADDRESS	MacAddress	SNMP macaddress
Link to other table	ObjectIdentifier	Value containing an oid (ex: 1.2.3.4.5.6)
OCTET STRING	OctetString	SNMP normal string
OCTET STRING	OctetStringDateTime	An octet string (in SNMP) representing a DateTime (formatted as YYYYMMDDHHMMSS)
OCTET STRING	OctetStringIpAddress	An octet string (in SNMP) representing an IP address (formatted as xx.xx.xx.xx)
OCTET STRING	OctetStringToVersion	Provides a conversion from OctetString to version

MIB Syntax	XML SnmpType	Short Description
TimeTicks	TimeTicks	SNMP time
TruthValue	TruthValue	SNMP boolean
Unsigned32	UInteger	SNMP unsigned integer.
Unsigned32	UIntEnum	Provides a conversion from UInt for enums

i. XML: Alarm Definitions

An alarm definition must be added or created per PropertyDefinition that must be able to raise alarms (PropertyType = "Reading"). The alarm definitions below define how the alarm looks when it appears in the Alarms tile in HiProvision. See §33.5.5 to find out when an alarm is really raised.

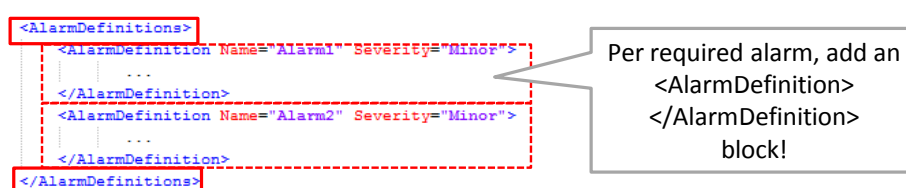


Figure 311 XML: AlarmDefinition Block per Alarm

The Alarm attribute in the PropertyDefinition must refer to the name in the AlarmDefinition, see an example below. Also add a severity

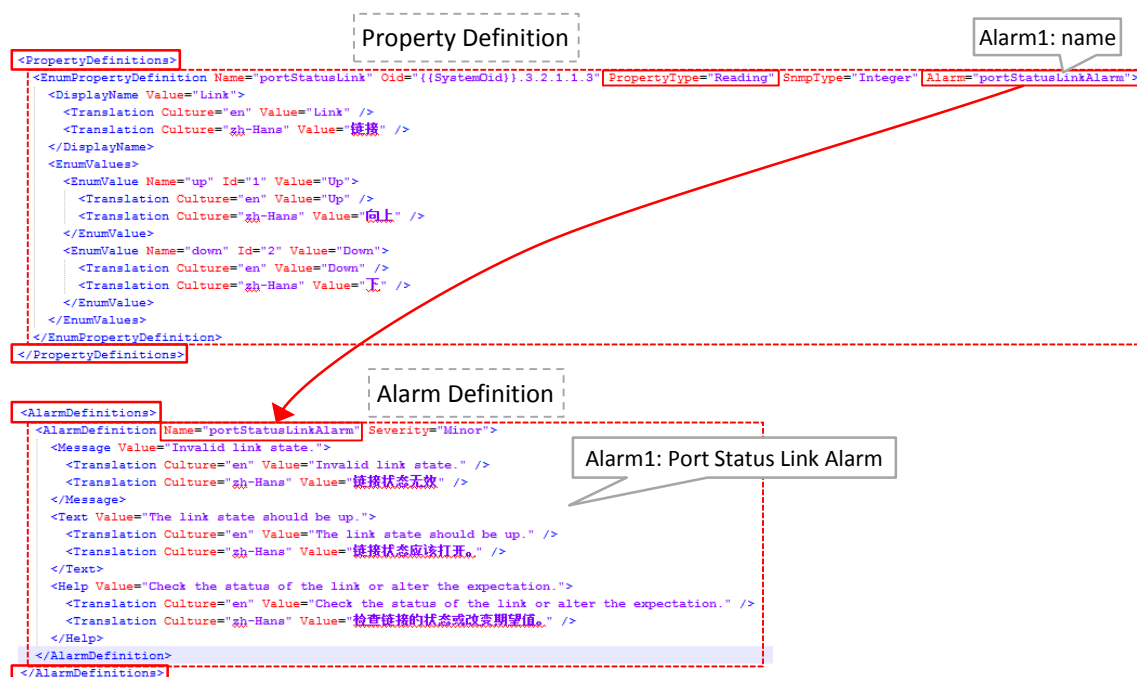


Figure 312 Alarm Definitions Example

An alarm definition contains the following attributes:

Name: the name of the alarm definition. This is used to refer to it by the property that uses this alarm data. See the alarm attribute on a property definition;

Severity (optional) (default = Minor, values [Warning, Minor, Major, Critical]: the alarm severity.

An alarm definition has the following child elements:

Message: the alarm message or title in the Alarms tile in HiProvision. Translations can also be provided. Culture indicates the language code: en = English, zh-Hans = Chinese; pl = Polish;

Text: the alarm text or body in the Alarms tile in HiProvision. Translations can also be provided.

Help: the help text in the Alarms tile in HiProvision. Translations can also be provided.

j. XML Trap Registrations

HiProvision can receive traps from external devices. A received trap does not influence directly a property in HiProvision, but it triggers HiProvision to poll the external device again (=trap-based poll). It is these poll results that can influence the properties in HiProvision.

So if you configure for example a trap for disabling PoE on a port, make sure that you also configure a PoE property and PropertyDefinition in the XML for polling purposes. Not doing so, and receiving a trap for a PoE disabled port, will initiate a new poll and not influence any custom property/alarms in HiProvision.

To make HiProvision receive traps from a device of this device type, the actions below must be performed on the external device itself.

CAUTION: Setting trap registrations (=write action) on the external device itself can be done via the XML file. It impacts ALL the external devices of this device type at once. If you don't want this (e.g. you only want to impact some devices and not all), do not use the XML for trap registrations. Instead, configure each external device individually e.g. via a local configuration tool or web interface on the external device.

Disable trap server;

Initialize trap operations:

- ▶ traps have to be enabled;
- ▶ set up the trap agent:
 - ▶ the HiProvision server IP address has to be filled out in the value field of the IpAddress trap registration;
 - ▶ the community and version has to be set;
- ▶ Configure the trap events via the OID in which you are interested. There is no strict mapping in the XML file required between a registered trapped property and a PropertyDefinition.

Enable trap server;

NOTE: These steps are device type specific and could differ for other device types;

NOTE: HiProvision receives traps by default on port 6021 and 6022. An extra port to which HiProvision must listen can be added via the 'TrapReceivePortOverride' attribute in the root element, see Table 62.

Find an XML example below with trap registrations.



Figure 313 XML: Trap Registrations

A trap registration contains the following attributes:

- **Oid:** the full OID in the Mib. It is advised to use the {{SystemOid}} pattern in combination with the SystemOid attribute on the root element;

Value:

- 1 = enabled, up or... depending on the property, see MIB;
- 2 = disabled, down or... depending on the property, see MIB;
- 3 = both '1' and '2'. Example: if value="3" is set for the Link Status property, then HiProvision will receive a trap when the link goes up on that specific port and another trap when the link goes down;
- **RowIndex:** the row index is required when the OID of the trap refers to a table in the MIB. Use the row index to select the desired row from the table. If the OID does not refer to a table, the RowIndex attribute must be empty or omitted;
- **SnmpType:** the SNMP Type or data type, has to match a value in the XML SnmpType column in Table 65;

Comment (optional): not used by the Generic Device framework but it's handy for the user to comment and remember what each setting does.

k. Apply XML File Changes to Live Network

Once you have changed, optimized and saved your XML file, follow the steps below to apply these changes on the external devices in the live network:

1. (Skip this step when HiProvision is already running) Start HiProvision Agent + HiProvision Client;
2. (Skip this step when the Advanced tile is already closed) Close the Advanced tile;
3. Open the Advanced tile;
4. Press the Generate button to configure the XML file input of ALL external device types, into HiProvision;
5. In the Servers tile, stop Servers (not just close HiProvision);
6. Close HiProvision Client and HiProvision Agent;
7. Restart HiProvision Agent and HiProvision Client;
8. The XML changes that should cause changes in the external devices in the HiProvision GUI (e.g. new properties on port or node level, etc...) should be visible now in the Network Hardware Tile via node properties, port properties etc...
9. Make a Connect in HiProvision. Trap registration in the external devices will be done just after the connect;
10. As of now, everything should be up and running. Properties should be monitored according the configured poll/trap settings, and alarms should be raised when properly configured.

33.5.5 Raising Alarms

Alarms are raised when HiProvision monitors and detects mismatches on alarm sensitive properties. Alarm sensitive properties have a little square box, see §4.3.

Custom properties, created via XML, must have a PropertyDefinition with the attribute PropertyType ="Reading" to be alarm sensitive.

33.6 Usage of External Devices in HiProvision

External Devices appear in HiProvision on the following places:

Dashboard → Tools → Advanced Tile → External Devices Types;
Dashboard → Configuration → Network Hardware Tile: Devices + Monitored Links;
Dashboard → Configuration → Protocols → MRP;
Dashboard → Monitoring → Network Tile;
Dashboard → Monitoring → Alarms Tile;
Dashboard → Administration → Licenses Tile;

Not Relevant for External Devices:

Discovery, Tunnels, Services (Wizards), Performance counters, Protocols;

34. BPDU GUARD ON ETHERNET LAN PORT

NOTE: See §32 where the port property feature BPDU Guard is supported. It is not relevant/supported on WAN Ports. BPDU Guard on L2/L3 Interface Modules is supported via the MSTP protocol wizard, see §7.3;

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

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

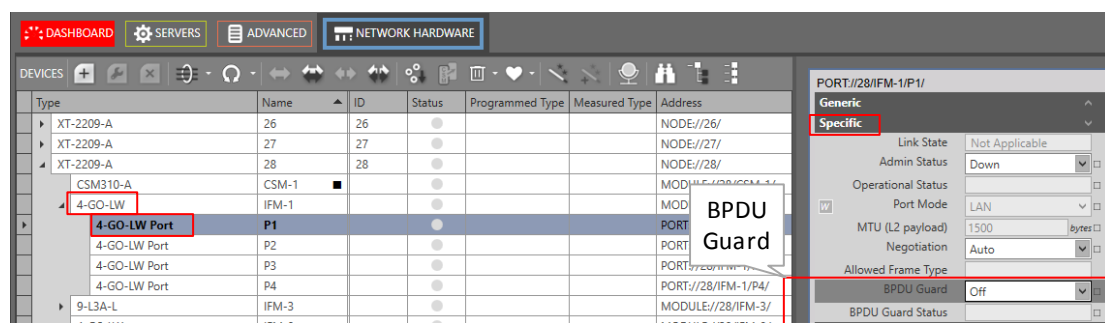


Figure 314 BPDU Guard on Ethernet LAN Port

- ▶ Configuration: Dashboard → Network Hardware → Port → Specific → BPDU Guard:
 - ▶ Off (=default):
 - ▶ the port will not send out dummy BPDU packets;
 - ▶ the port remains up in case of a loop;
 - ▶ the port will not be disabled when a BPDU packet enters the port. As a result, a possible running Dragon PTN MSTP instance in the same service as the port, is not protected from external MSTP influences via this port. CAUTION: a device connected to this port could be selected as MSTP root bridge when a Dragon PTN MSTP is running in the same service, resulting in a topology change in the Dragon PTN network.
 - ▶ On:
 - ▶ the port will send out dummy BPDU packets itself;
 - ▶ the port will be disabled when a BPDU packet enters the port. Possible running Dragon PTN MSTP instances are protected from external MSTP influences via this port. The port can be re-enabled by setting the Admin Status of the port properties Down and click Apply (and Load) and setting it back Up and click Apply (and Load).
- ▶ BPDU Guard Status:
 - ▶ Inactive: BPDU Guard is disabled;
 - ▶ Secure Up: BPDU Guard is enabled and no BPDU packet has entered the port yet. The port is still up. All traffic allowed;

- ▶ Port Shutdown: BPDU Guard is enabled and a BPDU packet has entered the port. As a result, the port has been shut down. No more traffic possible via this port possible;
- ▶ Secure Down: BPDU Guard is configured but could not be enabled because of a conflict with other features.

35. LAG (=LINK AGGREGATION GROUP)

35.1 Prerequisites

At least one node must have configured a Interface Module that supports LAG. See §32 which Interface Modules support LAG.

35.2 General

Link Aggregation is the bundling (=aggregation) of multiple parallel 1 Gbps links between a source and destination into one logical link. The resulting combined logical link:

- ▶ has at least one 1 Gbps bandwidth, but can have more bandwidth if both conditions below are met:
 - ▶ multiple streams from different MAC addresses are streamed over the LAG;
 - ▶ the LAG algorithm results in loadsharing these streams over different links within the LAG;
- ▶ offers loadsharing;
- ▶ offers redundancy in case one of the individual links should fail.

Link Aggregation is obtained via creating two LAGs: one LAG on the source and one LAG on the destination side. A LAG on the Dragon PTN side is a combination of multiple ethernet LAN ports within a L2/L3 Interface Module into one logical port group. All the ports of the source and destination LAG must be 1000 Mbps ports and must be in autonegotiation.

NOTE: LAG on LAN ports and back end ports is not supported.

The Link Aggregation is the communication between two LAGs. E.g. one LAG in one Dragon PTN node and the second LAG in another Dragon PTN node or a third party switch/application/...

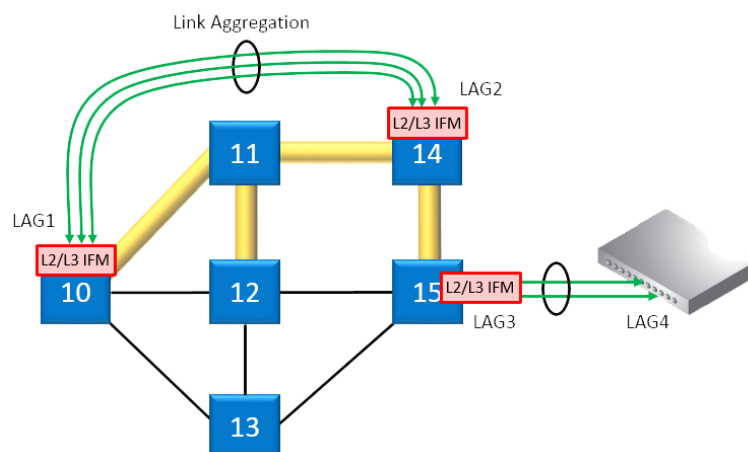



Figure 315 Link Aggregation and LAGs

CAUTION: If you want to enable OSPF on a LAG, configure the LAG in a VLAN. A LAG configured on router ports (L3 Interface Module) does not support OSPF (see §7.9)!

35.3 Configuration

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

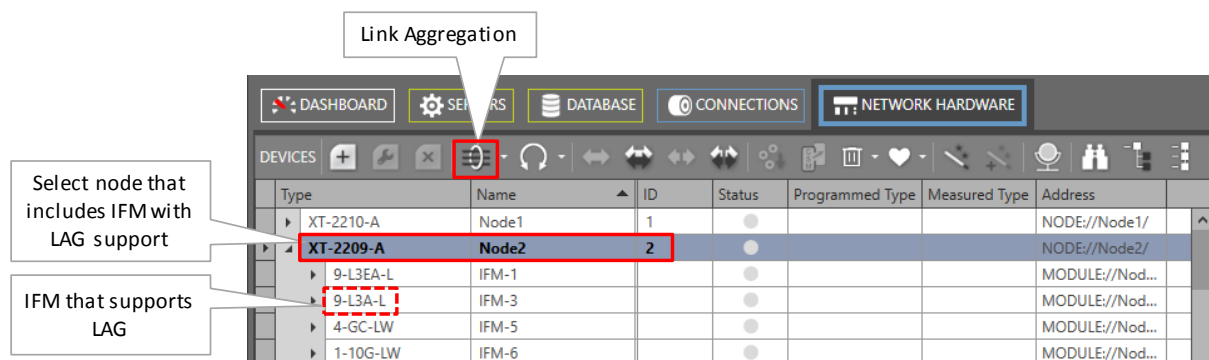



Figure 316 Link Aggregation Configuration

2. Options:
 - ▶ Create LAG (see §35.3.1);
 - ▶ Modify LAG (see §35.3.2);
 - ▶ Delete LAG (see §35.3.3);

35.3.1 Create LAG

1. Select a node (by selecting the row) in the Devices list that has at least one Interface Module that supports LAG (see §32).
2. Click  → Create LAG;
3. The Link Aggregation wizard opens. The list below summarizes every page in the wizard:
 - ▶ Information: Click Next>>;
 - ▶ Creation: Fill out the parameters below.

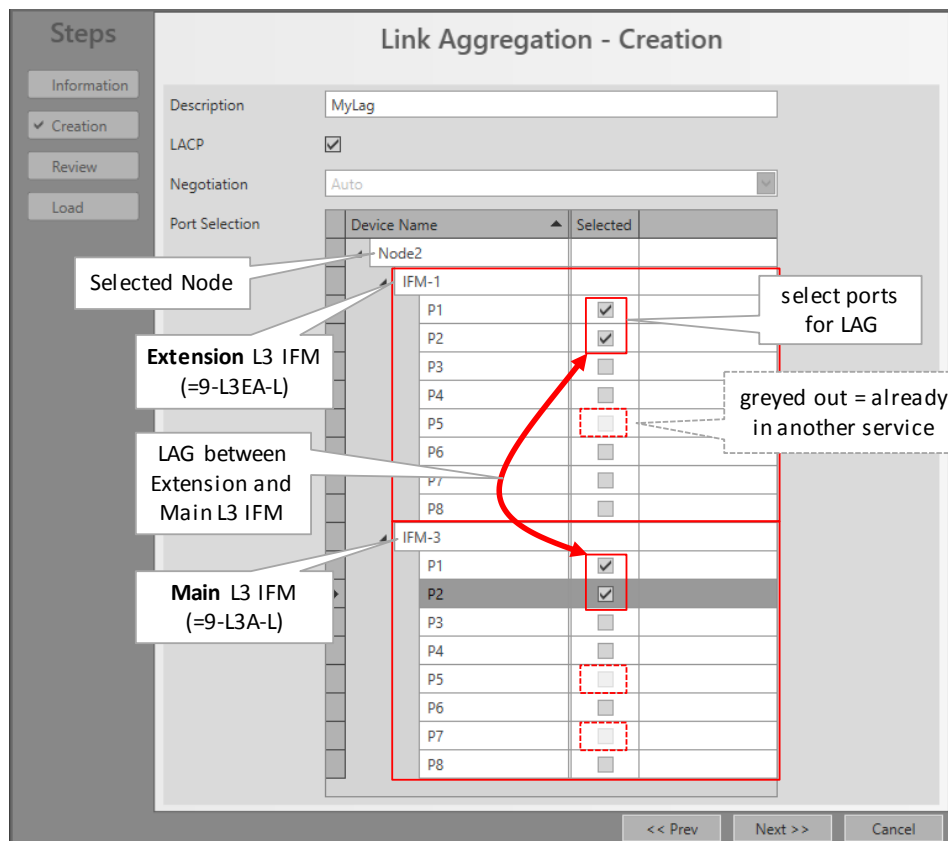


Figure 317 Create LAG

- Description: a short description for this LAG instance;
- LACP (=Link Aggregation Control Protocol): LACP provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP).
 - unchecked (=default): LACP is disabled, the LAG will still performs some kind of basic bundle negotiation with the other side;
 - checked: LACP is enabled;
- Negotiation:
 - Auto (=default): All the ports in the LAG will be configured in AutoNegotiation. AutoNegotiation advertises and negotiates the speed and duplex mode(s) of the ports within the LAG, with the destination LAG. The individual configured port speed and duplex modes in HiProvision will be ignored;
- Port Selection: Shows the selected node with all the Interface Modules that support LAG and its ports. Click the Selected checkbox to add a port to the LAG:
 - a LAG must contain ports of the same Interface Module (except if you combine ports between the main L3 Interface Module and the extension L3 Interface Module). As a result, selecting ports in one Interface Module will grey out the ports in other Interface Modules in the same node;
 - a LAG requires minimum 2 ports and maximum 8 ports. Selecting more than 8 ports will result in the figure below later on when finishing the wizard:

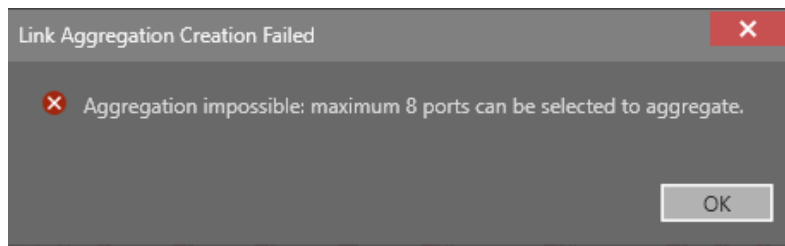


Figure 318 Link Aggregation Failed: Aggregation Impossible

- ▶ the LAG ports must either be in the same service or no service at all. If you select a port, and other ports in the same node grey out, it means one of the following:
 - ▶ the other ports are configured in a service whereas the selected port is not or vice versa;
 - ▶ the other ports and the selected port are configured in a different service;

NOTE: Port9 (P9) of a L3 Interface Module is not shown because this is the only 10G port on this Interface Module, it can have different speed settings than the other 1G ports in the LAG, and this is not allowed. Link aggregation between the two 10G ports of the L3 and L3 extension Interface Module in one node is not supported.

- ▶ Review: if ok, click Finish. The configuration load manager will be invoked, see §5;
- ▶ After creation, the LAG will be visible in the Interface Module with the configured LAG, see figure below. For LAGs on an extension L3 Interface Module, its LAG will be visible in its associated main L3 Interface Module;

The screenshot shows a software interface with tabs: DASHBOARD, SERVERS, DATABASE, CONNECTIONS, and NETWORK HARDWARE. The NETWORK HARDWARE tab is active. Below it is a table of network hardware components. A red box highlights the 'L3 LAG Port' row, which is labeled 'LAG1'. A tooltip points to this row with the text: "Created LAG between main and extension L3 IFM P1,P2 = main P1E, P2E = extension".

Type	Name	ID	Status	Programmed Type	Measured Type
XT-2210-A	Node1	1			
XT-2209-A	Node2	2			
9-L3EA-L	IFM-1				
9-L3A-L	IFM-3				
L3 1G BE Port	BE1				
L3 1G BE Port	BE2				
L3 1G BE Port	BE3				
L3 1G BE Port	BE4				
L3 10G BE Port	BE5				
L3 LAG Port	LAG1				
L3 1G FE LAG Port	P1				
L3E 1G FE LAG Port	P1E				
L3 1G FE LAG Port	P2				
L3E 1G FE LAG Port	P2E				
L3 1G FE Port	P3				

Figure 319 Created LAG

35.3.2 Modify LAG

1. Select the LAG that must be modified via selecting its '<Interface Module> LAG Port' row in Figure 319.
2. Click → Modify LAG;
3. The Link Aggregation wizard opens. The list below summarizes every page in the wizard:
 - ▶ Information: Click Next>>;


- Modification:
 - Description: can be modified;
 - LACP: can not be modified;
 - Negotiation: can not be modified;
 - Port Selection: can be modified;
- NOTE:** Only the ports are shown that are configured in the same service as the original selected ports. If none of the original ports is configured in a service, only ports that are not configured in a service are shown.

Device Name	Selected	
Node2		
IFM-1		
P3	<input type="checkbox"/>	
P4	<input type="checkbox"/>	
P6	<input type="checkbox"/>	
P7	<input type="checkbox"/>	
P8	<input type="checkbox"/>	
IFM-3		
LAG1		
P1	<input checked="" type="checkbox"/>	
P1E	<input checked="" type="checkbox"/>	
P2	<input checked="" type="checkbox"/>	
P2E	<input checked="" type="checkbox"/>	
P3	<input type="checkbox"/>	
P4	<input type="checkbox"/>	
P6	<input type="checkbox"/>	
P8	<input type="checkbox"/>	

Figure 320 Modify LAG

- Review: if ok, click Finish. The configuration load manager will be invoked, see §5;
- After modification, the modified LAG will be visible in the Interface Module with the configured LAG. For LAGs on an extension L3 Interface Module, its LAG will be visible in its associated main L3 Interface Module;

35.3.3 Delete LAG

1. Select the LAG that must be deleted via selecting its '<Interface Module> LAG Port' row in Figure 319.
2. Click  → Delete LAG;
3. The LAG will be removed from the port list. If the LAG was configured in a service, its included ports automatically remain configured in the service.

36. LOOPBACK INTERFACE

36.1 Prerequisites


At least one node must have configured a L3 Interface Module.

36.2 General

The loopback interface is a virtual interface meant for management purposes. This loopback interface will be mainly used by the PIM (see §7.10) and the OSPF (see §7.9) protocol.

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

36.3 Configuration

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

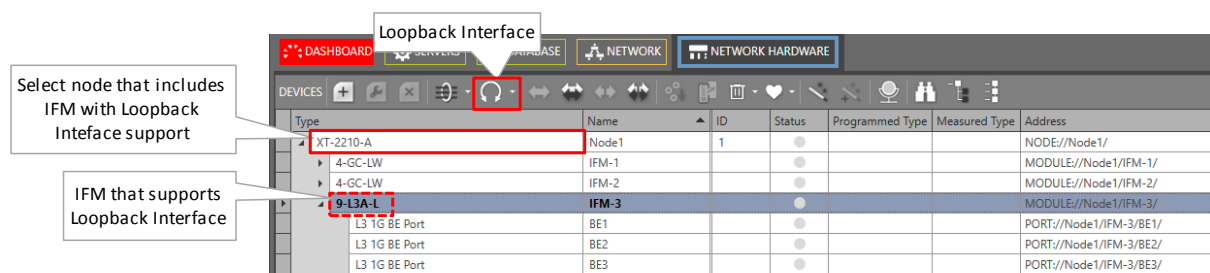


Figure 321 Loopback Interface

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

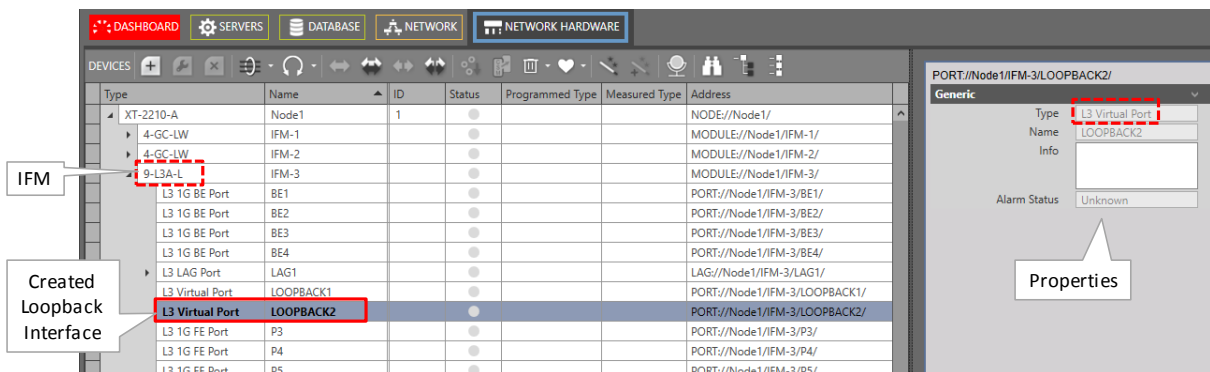



Figure 322 Created Loopback Interface

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

3. The created loopback interface can be used later on in the port selection of the Virtual Router wizard (§7.5), see below:

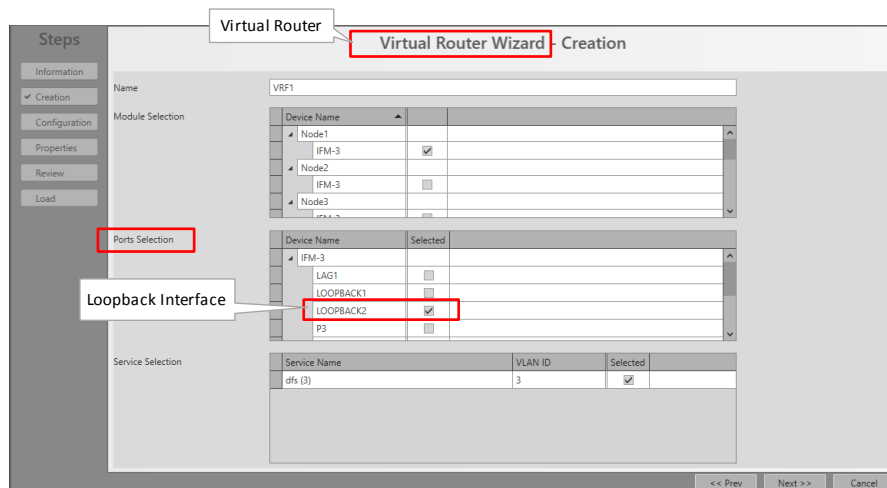


Figure 323 Virtual Router Wizard: Loopback Interface

37. OPEN SOURCE COMPONENTS

The open source components listed below are used in Dragon PTN.

Table 66 Open Source Components

Component Type	Component	License
LTIB (LINUX)	Apptk-Base	MIT
LTIB (LINUX)	base_libs	LGPLv2.1
LTIB (LINUX)	bash	GPLv2
LTIB (LINUX)	bridge-utils	GPLv2
LTIB (LINUX)	busybox	GPLv2
LTIB (LINUX)	cramfs	GPLv2
LTIB (LINUX)	curl	Curl License
LTIB (LINUX)	dropbear	MIT Style License
LTIB (LINUX)	e2fsprogs	GPLv2
LTIB (LINUX)	ethtool	GPLv2
LTIB (LINUX)	flex	BSD
LTIB (LINUX)	gdb	GPLv2
LTIB (LINUX)	i2c-tools	GPLv2
LTIB (LINUX)	inet-tools	GPLv2
LTIB (LINUX)	iperf	Iperf License
LTIB (LINUX)	iproute	GPLv2
LTIB (LINUX)	ipsecadm	GPLv2
LTIB (LINUX)	ipsec-tools	BSD
LTIB (LINUX)	iptables	GPLv2
LTIB (LINUX)	iputils	GPLv2
LTIB (LINUX)	kernel	GPLv2

Component Type	Component	License
LTIB (LINUX)	libelf	LGPLv2.1
LTIB (LINUX)	libtermcap	LGPLv2.1
LTIB (LINUX)	lzo	GPLv2
LTIB (LINUX)	merge	GPLv2
LTIB (LINUX)	modeps	GPLv2
LTIB (LINUX)	mtd-utils	GPLv2
LTIB (LINUX)	ncurses	MIT
LTIB (LINUX)	netcat	Public Domain
LTIB (LINUX)	net-tools	GPLv2
LTIB (LINUX)	ntpcient	GPLv2
LTIB (LINUX)	openssl	OpenSSL License
LTIB (LINUX)	pciutils	GPLv2
LTIB (LINUX)	portmap	BSD
LTIB (LINUX)	quotatools	LGPLv2.1
LTIB (LINUX)	screen	GPLv2
LTIB (LINUX)	strace	BSD
LTIB (LINUX)	sysconfig	GPLv2
LTIB (LINUX)	tcp_wrappers	BSD
LTIB (LINUX)	tcpdump	BSD
LTIB (LINUX)	termcap	BSD
LTIB (LINUX)	u-boot	GPLv2
LTIB (LINUX)	vsftpd	GPLv2
LTIB (LINUX)	zlib	Zlib License
CSM	boost	Boost License
CSM	curl	
CSM	DCN	
CSM	emlog	GPLv2
CSM	net-snmp	BSD Like
CSM	olsr	BSD style
ISS	openssh	BSD
ISS	openssl	OpenSSL License
Software	Enterprise Library	Microsoft Public License
Software	GalaSoft.mvvmLight	MIT License
Software	Python	PSF license (GPL compatible)
Software	Quartz scheduling framework for .NET	Apache License 2.0
Software	UDP log	GPLv1 or GPLv2

38. TROUBLESHOOTING

38.1 Database Tile: Authentication Failed

An 'Authentication Failed' error on the database tile means that HiProvision tries to connect to the MySQL server with the wrong authentication credentials. See figure below.

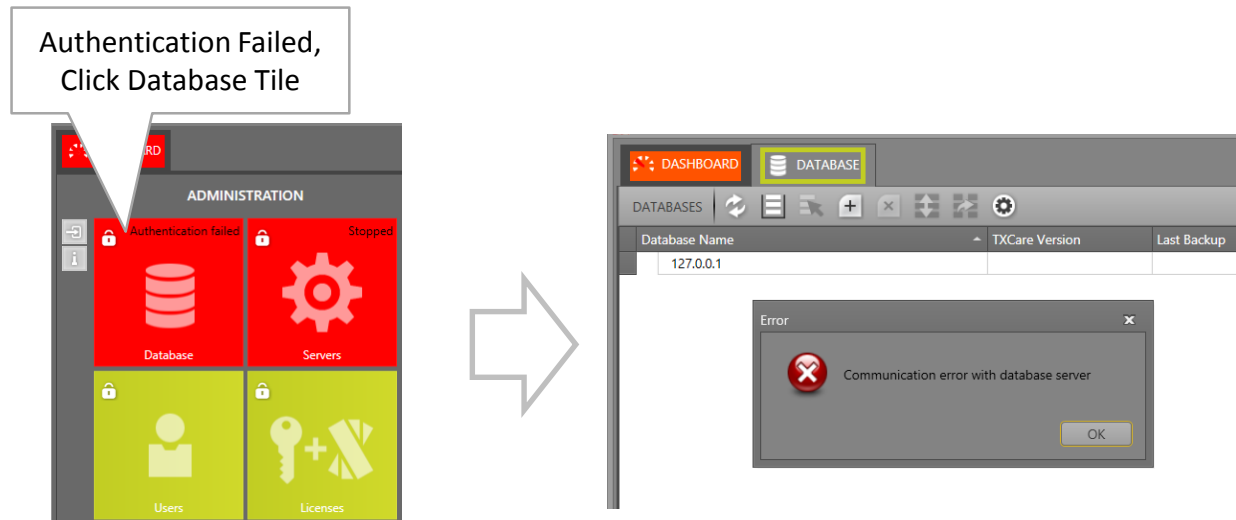


Figure 324 Database Tile: Authentication Failed

Make sure that the configured MySQL database password (default password = **txcare**) and the password that HiProvision uses to connect is the same. See §6.2.2 how to change passwords and connect with the right credentials.

38.2 View Device Info

The View Device Info tool allows to show more node or L3 Interface Module information based on a selected CLI command. It can be found via Dashboard → Tools → Advanced → View Device Info;

1. Select the desired node or L3 Interface Module in the devices list;
2. Select the desired CLI command via the CLI command selector;
3. Click the Execute button;
4. The CLI command output is shown. It can be cleared via the Clear button if desired. If you want to reuse the previous command, select the command from the History dropdown and click Repeat.

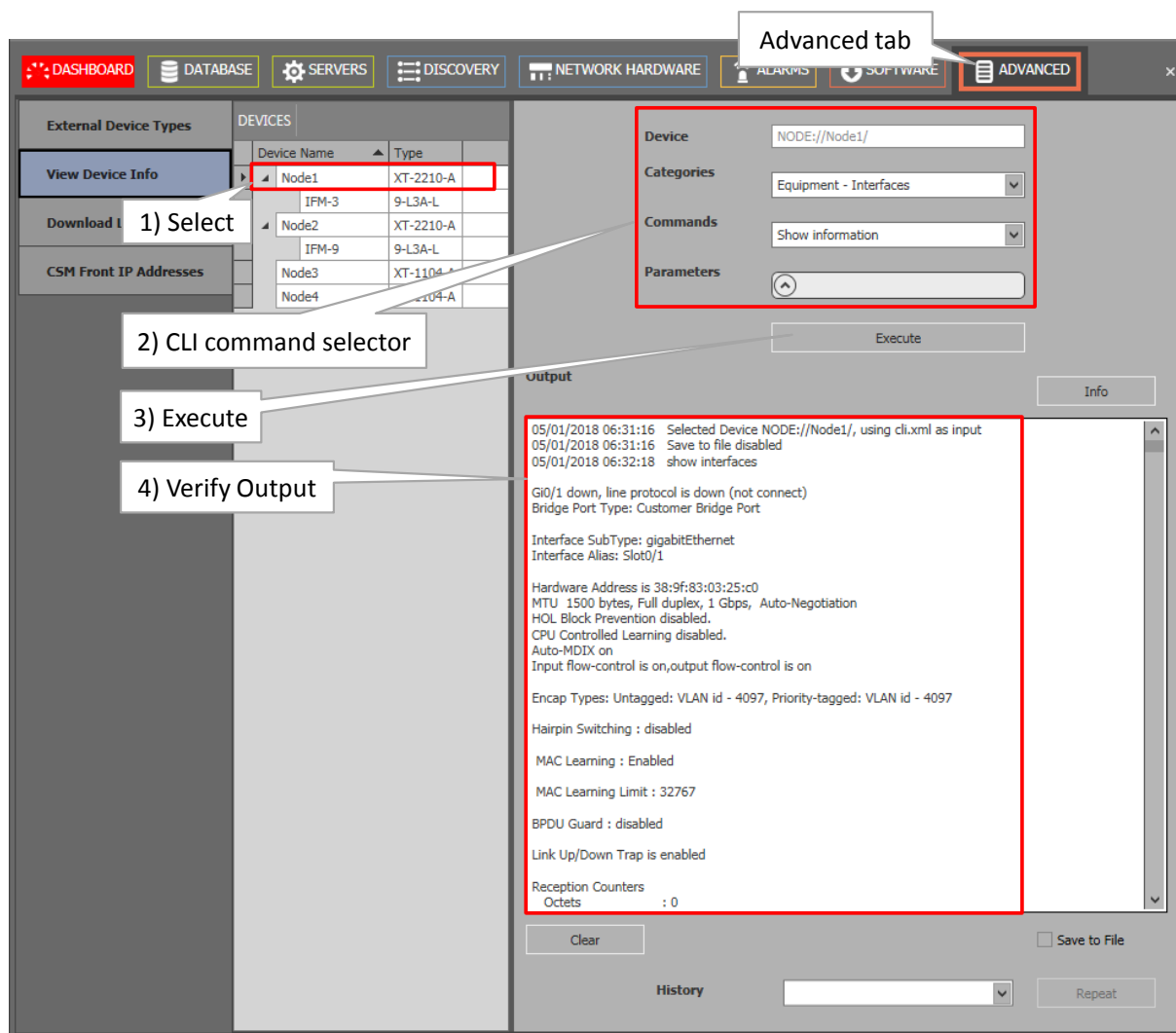


Figure 325 View Device Info: General

5. Port names used in CLI commands are different from the slot/port naming. Therefore, a port mapping table is required to understand which port is meant. This port mapping table can be invoked by clicking the Info button. See figure below.

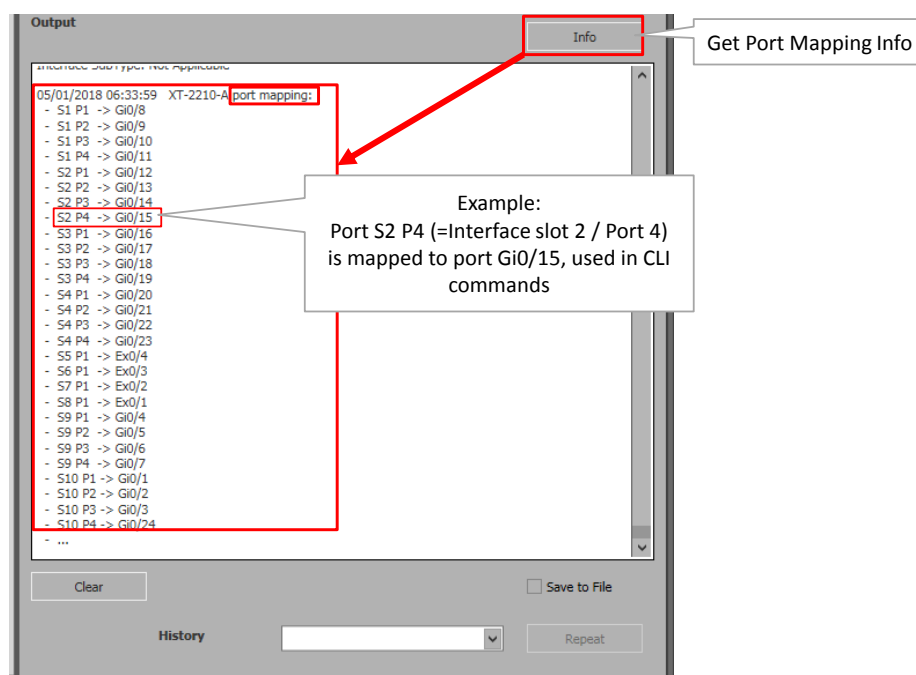




Figure 326 View Device Info: Port Mapping

38.3 Download Log Files from Nodes to HiProvision PC

The 'Download Log Files' tool allows to download log files from your nodes to the HiProvision PC. It can be found via Dashboard → Tools → Advanced → Download Log Files.

1. Select the desired node in the devices list or expand the node and select an Interface Module only;
2. Click the  button to start the download from the live node to the HiProvision PC;
3. An FTP command has been successfully started, downloading is ongoing into directory C:\FtpRoot\Logs\Node<Node Number>. The 'Download Result' is in the state pending;
4. Click the refresh button  until the 'Download Result' is success;
5. View your downloaded log files in C:\FtpRoot\Logs\Node<Node Number>.

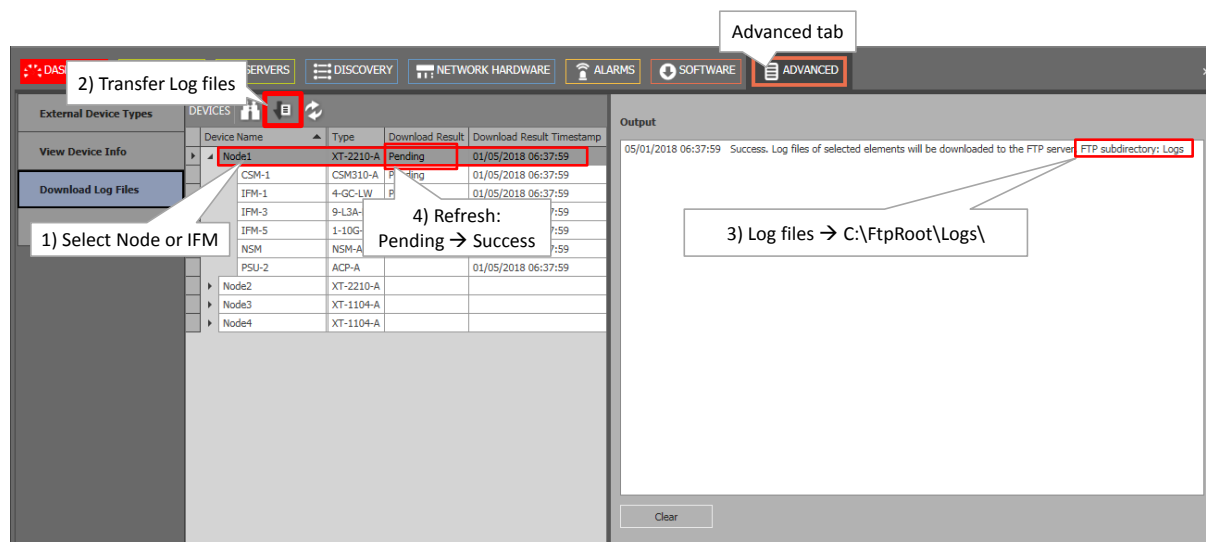



Figure 327 Download Log Files

38.4 Rollback

If something goes wrong and a pop-up in HiProvision asks for a rollback of a node:

1. Go to Dashboard → Network Hardware.
2. Select the node (or all nodes) that must be roll backed and click the rollback button . As a result, the node goes back to a previous restore point (see §5.2) with a working configuration.

38.5 Firewall Ports

If one or the other external LAN connection should not work as expected (e.g. external LAN connections in HiProvision Redundancy, Remote Client,), verify your firewall port settings. Make sure that the ports below are not blocked by the firewall:

TCP 20, 21, 22, 6001, 3306;

► UDP 123, 161, 6020, 6021, 6022, 3306;

NOTE: Remote Client uses TCP 6001;

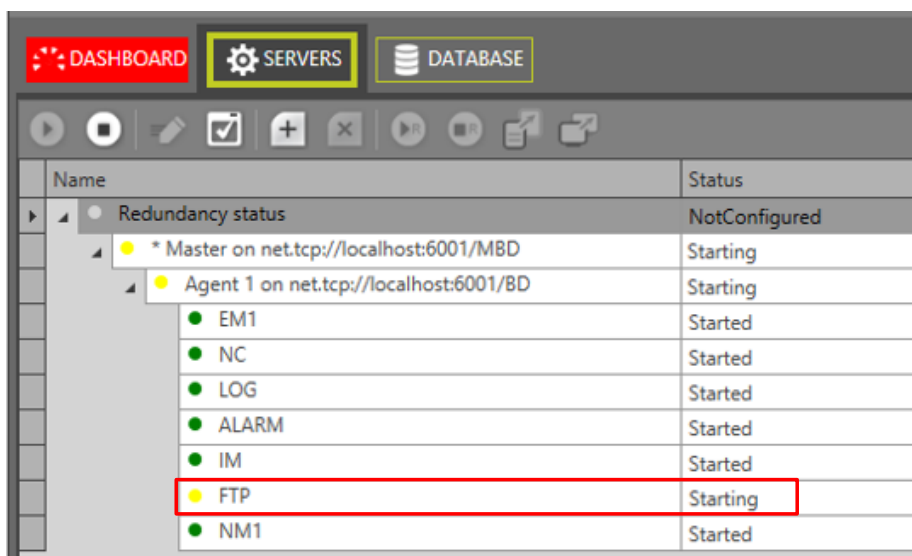
38.6 Test and Loopback

To troubleshoot the data traffic path of programmed Circuit Emulation (=CES) or 4-DSL-LW Ethernet services, it is possible to use 'test and loopback functionalities' as described in §18.

38.7 Server Does not Start (Server Tile Remains 'Starting')

Verify your FTP server via the Servers tile. If the bullet remains yellow, HiProvision does not succeed in starting the FTP server. As a result the entire HiProvision does not start.

Verify if the HiProvision PC has running another FTP server besides the HiProvision processes. If so, shut down the other third party FTP server and restart the HiProvision Servers.



DASHBOARD SERVERS DATABASE		
		Status
Redundancy status		NotConfigured
* Master on net.tcp://localhost:6001/M8D		Starting
Agent 1 on net.tcp://localhost:6001/BD		Starting
EM1		Started
NC		Started
LOG		Started
ALARM		Started
IM		Started
FTP		Starting
NM1		Started

Figure 328 FTP Server Does Not Start

38.8 Ethernet Service Fails with Multiple Tunnels on Same Link

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

When you have a similar configuration and the problem occurs, contact <https://hirschmann-support.belden.com> for further assistance.

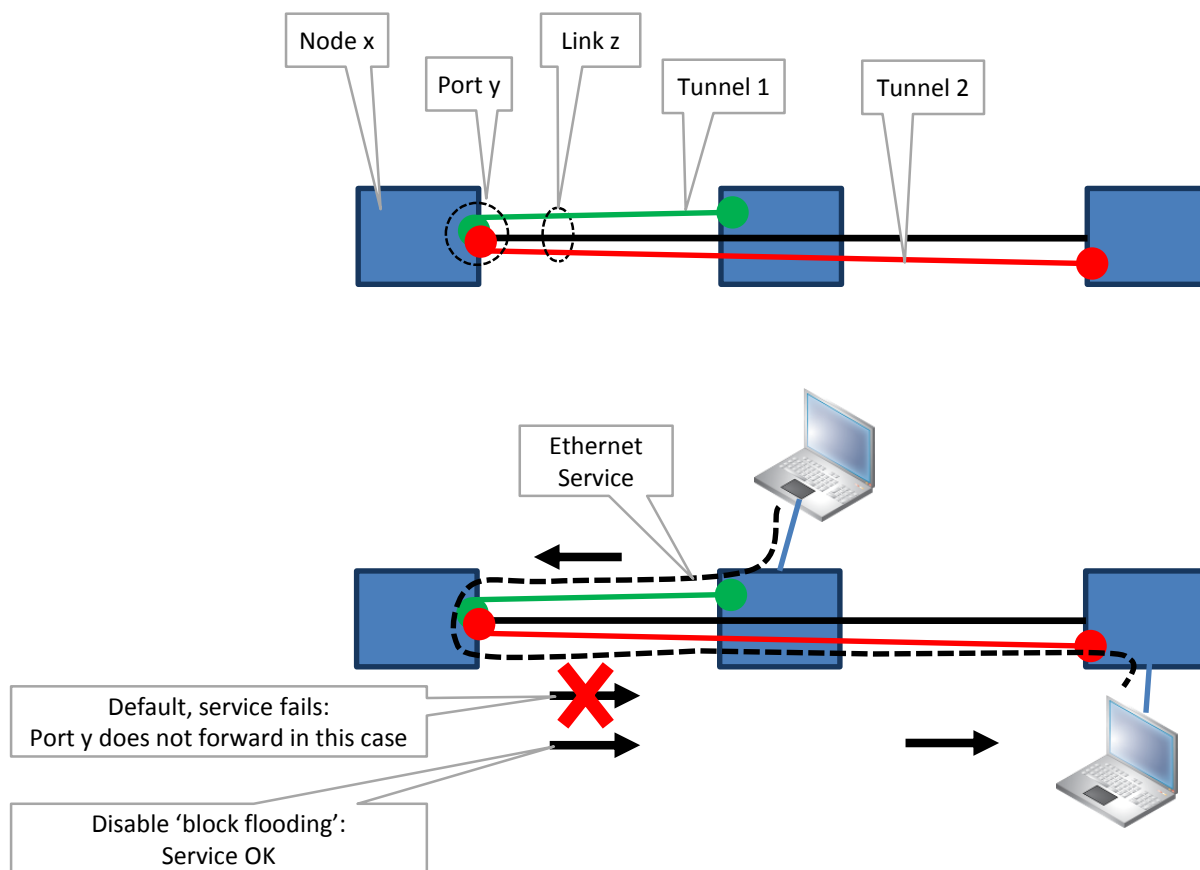


Figure 329 Ethernet Service Fails with Multiple Tunnels on Same Link

38.9 Lost Tree View Structure Due to Older HiProvision Version

In the special case that a user decides to use an older HiProvision version after using a newer one (=not advised!) it is possible that your tree view structure has been lost. To solve this problem, manually clear the user settings via HiProvision User Management, see Ref.[15] in Table 1.

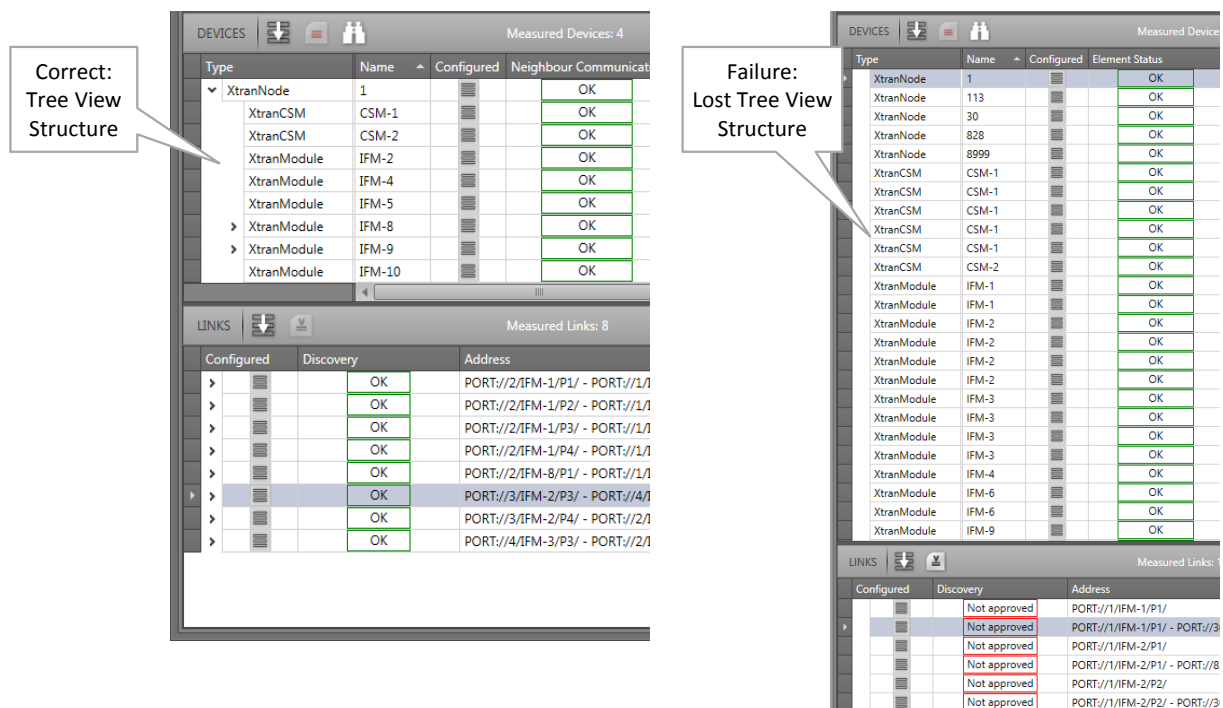


Figure 330 Lost Tree View Structure Due to Older HiProvision Version

38.10 Debugging the Network via Port Mirroring

See §30.

38.11 Health Monitor

If you have problems with a specific node, a service in a node, responsiveness of a node, possible traffic loss is a node, it is always a good idea to verify the Health Monitor (see §15.8).

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

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

39. ABBREVIATIONS

ABR	Area Border Router
ACL	Access Control List
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Boundary Router
BC	Broadcast
BDR	Backup Designated Router

BERT	Bit Error Ratio Tester
BFD	Bi-directional Forwarding Detection
BPDU	Bridge Protocol Data Unit
BWE	Bandwidth Efficiency
CAR IP	Central Alarm Reporter Internet Protocol
CAS	Central Alarm System
CIDR	Classless Inter-Domain Routing
CES	Circuit Emulation Service
CESoPSN	Circuit Emulation Service over Packet Switched Network
CPU	Central Processing Unit
CSM	Central Switching Module
CSV	Comma Separated Values
DCN	Data Communication Network
DHCP	Dynamic Host Control Protocol
DLF	Destination Lookup Failure
DM	Delay Measurement
DR	Designated Router
DUS	Don't Use for Sync
EEC	Ethernet Equipment Clock
ERPS	Ethernet Ring Protection Switching
FCS	Frame Check Sequence
FDV	Frame Delay Variation
ICMP	Internet Control Message Protocol
IFDV	Inter Frame Delay Variation
IP	Internet Protocol
ISP	Internet Service Provider
L2	Layer2
L3VPN	Layer3 Virtual Private Network
LAG	Link Aggregation Group
LAN	Local Area Network
LER	Label Edge Router
LLDP	Link Layer Discovery Protocol (IEEE)
LM	Loss Measurement
LNМ	Large Network Monitor

LPS	Linear Protection Switching
LSA	Link State Advertisements
LSP	Label Switched Path
LSR	Label Switching Router
LT	Line Termination Character
MAC	Media Access Control
MC	Multicast
MPLS-TP	Multiprotocol Label Switching – Transport Profile
MRC	Media Redundancy Clients
MRM	Media Redundancy Manager
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NIC	Network Interface Card
NSM	Node Support Module
NTP	Network Timing Protocol
OSPF	Open Shortest Path First
PD	Powered Device
PRBS	Pseudo Random Bit Sequence
PRC	Primary Reference Clock
PRS	Primary Reference Source
PSE	Power Source Equipment
PSU	Power Supply Unit
PTN	Packet Transport Network
PTP	Precision Time Protocol
QL	Quality Level
QoS	Quality of Service
QRSS	Quasi Random Signal Source
RADIUS	Remote Authentication Dial In User Service
RES	Reserved
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
TRM	Transmit Receive Module
TSoP	Transparent Sonet/SDH over Packet
TTL	Time to Live
UDP	Universal Data Protocol
UM	User Management
UTC	Coordinated Universal Time
VFI	Virtual Forwarding Instance
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network
WTR	Wait to Restore
XFP	10 Gigabit Small Form Factor Pluggable