



Neptune

Reference Manual

V9.1

Document Revision: 01

Published: January 2024

© 2024 Ribbon Communications Operating Company, Inc. © 2024 ECI Telecom Ltd. All rights reserved.

This is a legal agreement between you, the end user, and ECI Ltd. ("ECI"). BY OPENING THE DOCUMENTATION AND/OR DISK PACKAGE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNOPENED DOCUMENTATION AND/OR DISK PACKAGE AND THE ACCOMPANYING ITEMS (INCLUDING WRITTEN MATERIALS AND BINDERS OR OTHER CONTAINERS), TO THE PLACE FROM WHICH YOU OBTAINED THEM.

All documentation and/or disk and all information and/or data contained in the documentation and/or disk ["ECI's Proprietary"] is ECI's proprietary and is subject to all copyright, patent, and other laws protecting intellectual property, and any international treaty provisions, as well as any specific agreement protecting ECI's rights in the aforesaid information. Any use of ECI's Proprietary for any purposes [included but not limited: published, reproduced, or disclosed to third parties, in whole or in part] other than those for which it was disclosed, without the express prior written permission of ECI, is strictly forbidden.

ECI's Proprietary is provided "AS IS" and may contain flaws, omissions, or typesetting errors. No responsibility and or liability whatsoever are assumed by ECI for you or any other party, for the use thereof, nor for the rights of third parties, nor for any loss or damage whatsoever or howsoever caused, arising directly or indirectly in connection with ECI's Proprietary, which may be affected in any way by the use and/or dissemination thereof. ECI reserves the right, without prior notice or liability, to make changes in equipment design or specifications including any change in and to the ECI's Proprietary.

Any representation(s) in ECI's Proprietary concerning performance of ECI's product(s) are for informational purposes only and are not warranties of product performance or otherwise, either express or implied. No warranty is granted nor liability assumed in relation thereto, unless specifically undertaken in ECI's sales contract or order confirmation. ECI's Proprietary is periodically updated, and changes will be incorporated in subsequent editions. All graphics included in this document are for illustrative purposes only and might not correspond with your specific product version.

The documentation and/or disk and all information contained therein is owned by ECI and is protected by all relevant copyright, patent, and other applicable laws and international treaty provisions. Therefore, you must treat the information contained in the documentation and disk as any other copyrighted material (for example, a book or musical recording).

Other Restrictions. You may not rent, lease, sell, or otherwise dispose of ECI's Proprietary, as applicable.

YOU MAY NOT USE, COPY, MODIFY, OR TRANSFER THE DOCUMENTATION AND/OR DISK OR ANY COPY IN WHOLE OR PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS LICENSE. ALL RIGHTS NOT EXPRESSLY GRANTED ARE RESERVED BY ECI.

All trademarks mentioned herein are the property of their respective holders.

Notwithstanding the generality of the aforementioned, you expressly waive any claim and/or demand regarding liability for indirect, special, incidental, or consequential loss or damage which may arise in respect of ECI's Proprietary contained therein, howsoever caused, even if advised of the possibility of such damages.

The end user hereby undertakes and acknowledges that they read the "Before You Start/Safety Guidelines" instructions (when provided by ECI) and that such instructions were understood by them. ECI shall not be liable to you or to any other party for any loss or damage whatsoever or howsoever caused, arising directly or indirectly in connection with you fulfilling and/or failure to fulfill in whole or in part the "Before You Start/Safety Guidelines" instructions.



NPT-2400, NPT-2300, NPT-2100, NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1100, NPT-1050, NPT-1022, and NPT-1012D are CE2.0 certified/compliant.



NPT-2400, NPT-2300, NPT-2100, NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1100, NPT-1050, NPT-1022, and NPT-1012D are MEF3.0 Carrier Ethernet certified/compliant for E-Line, E-LAN, E-Tree, E-Access, and E-Transit services.



Ribbon's qualification lab is accredited by A2LA for competence in electrical testing according to the International Standard ISO IEC 17025-2017 General Requirements for the Competence of Testing and Calibration Laboratories.\



Ribbon's management applications run on VMWare virtualization hypervisors.

Catalog #: X66500

Drawing #: 417006-2711-127-A00

# Contents

<b>Neptune Reference Manual .....</b>	<b>1</b>
<b>Neptune Reference Manual Revision History .....</b>	<b>2</b>
<b>Introducing Neptune .....</b>	<b>3</b>
NPT Platforms: Tailored to Your Needs .....	5
Implementation Principles .....	8
Neptune Expansion Platforms .....	8
Features and Functions .....	8
Intelligent Edge Service .....	9
<b>NPT-2400 System Architecture .....</b>	<b>11</b>
NPT-2400 Switching Functionality .....	13
NPT-2400 Control Subsystem .....	14
NPT-2400 Communications with External Equipment and Management .....	15
NPT-2400 Timing .....	15
NPT-2400 Cooling Subsystem .....	17
NPT-2400 Power Feed Subsystem .....	18
INF2400A Overview .....	19
ACPS2400A Overview .....	20
<b>NPT-2300 System Architecture .....</b>	<b>22</b>
NPT-2300 Control Subsystem .....	23
NPT-2300 Communications with External Equipment and Management .....	24
NPT-2300 Control and Communication Modules .....	24
NPT-2300 Timing .....	27
NPT-2300 Cooling Subsystem .....	28
NPT-2300 Power Feed Subsystem .....	31
NPT-2300 Switching Cards .....	32
MCIPS3T Switching Card .....	32
MCIPS3T Functional Description .....	35
NPT-2300 Tslot IO Modules .....	37
NPT-2300 Expansion Platforms .....	39
<b>NPT-2100 System Architecture .....</b>	<b>41</b>
NPT-2100 Control Subsystem .....	41
NPT-2100 Communications with External Equipment and Management .....	42
NPT-2100 Timing .....	43
NPT-2100 Cooling Subsystem .....	44

NPT-2100 Power Feed Subsystem .....	45
INF2100A Overview .....	46
ACPS2100A Overview .....	47
NPT-2100 Switching Functionality.....	48
<b>NPT-1800 System Architecture .....</b>	<b>50</b>
NPT-1800 Platform Architecture.....	52
NPT-1800 Platform Design.....	52
Group I Usage Guidelines: CIPS1T Only .....	54
Group II Usage Guidelines: CIPS1T Only .....	57
Card Configuration Guidelines and Example .....	58
Maximum Cards per Platform.....	60
Maximum Ports and Fan-Out per Platform.....	63
NPT-1800 Control Subsystem.....	64
NPT-1800 Communications with External Equipment and Management .....	65
NPT-1800 Controller Cards .....	66
MCP1800 Overview .....	66
MCP1800B Overview .....	69
NPT-1800 Timing Overview.....	69
NPT-1800 Cooling Subsystem .....	70
NPT-1800 Power Feed and Alarm Subsystems .....	75
INF_1800 and INF_1800H Overview .....	75
ECB Overview .....	77
NPT-1800 Switching Cards .....	78
CIPS1T Overview .....	79
CIPS2T Overview .....	82
NPT-1800 Tslot IO Modules .....	85
NPT-1800 Expansion Platforms .....	89
<b>NPT-1300 System Architecture .....</b>	<b>90</b>
NPT-1300 Control Subsystem.....	92
NPT-1300 Communications with External Equipment and Management .....	92
NPT-1300 Control and Communication Modules .....	93
NPT-1300 Timing.....	95
NPT-1300 Cooling Subsystem .....	96
NPT-1300 Power Feed Subsystem .....	99
INF_1300 Overview.....	99
NPT-1300 Switching Cards .....	100
MCIPS1T Switching Card.....	100

---

---

MCIPS1T Functional Description .....	102
NPT-1300 Tslot IO Modules .....	104
NPT-1300 Expansion Platform .....	107
<b>NPT-1250 System Architecture .....</b>	<b>108</b>
NPT-1250 Control Subsystem.....	110
NPT-1250 Communications with External Equipment and Management .....	110
NPT-1250 Timing.....	111
NPT-1250 Cooling Subsystem .....	112
NPT-1250 Power Feed and Alarm Subsystems .....	115
INF_1200 Overview.....	115
AC_PS-1200 Overview .....	116
ECB_1250/1250B Overview.....	116
NPT-1250 Switching Cards .....	117
MCIPS300Fx Family of Switching Cards .....	117
MCIPS300Fx Functional Description .....	119
NPT-1250 Tslot IO Modules .....	121
NPT-1250 Expansion Platforms .....	123
<b>NPT-1200 System Architecture .....</b>	<b>125</b>
NPT-1200 Control Subsystem.....	126
NPT-1200 Communications with External Equipment and Management .....	128
MCP1200 Main Controller Card Overview .....	128
NPT-1200 Timing.....	131
NPT-1200 Cooling Subsystem .....	131
FCU_1200 Overview .....	133
FCU_1200B Overview.....	134
NPT-1200 Power Feed Subsystem.....	136
INF_1200 Power Module Overview.....	136
AC_PS-1200 Power Module Overview .....	137
NPT-1200 Switching Cards .....	137
CPS100 Overview .....	138
CPS100 Functional Description .....	139
CPS320 Overview .....	140
CPS320 Functional Description .....	141
MCIPS320 and MCIPS560 Overview.....	142
MCIPS320 and MCIPS560 Functional Description .....	146
NPT-1200 Tslot IO Modules .....	148
NPT-1200 Expansion Platform .....	152

---

---

<b>NPT-1100 System Architecture .....</b>	<b>154</b>
NPT-1100 Control Subsystem .....	155
NPT-1100 Communication with External Equipment.....	156
NPT-1100 Timing .....	157
NPT-1100 Cooling Subsystem .....	157
NPT-1100 Power Feed Subsystem .....	160
INF-B1UH Overview.....	161
AC_PS-B1UH Overview.....	161
NPT-1100 Traffic and Switching Functionality .....	161
NPT-1100 Tslot IO Modules.....	163
<b>NPT-1050 System Architecture .....</b>	<b>166</b>
NPT-1050 Control Subsystem.....	167
NPT-1050 Communications with External Equipment and Management .....	168
NPT-1050 Timing.....	169
NPT-1050 Cooling Subsystem .....	169
NPT-1050 Power Feed Subsystem .....	172
INF_B1UH Power Module Overview .....	173
AC_PS-B1UH Power Module Overview.....	173
NPT-1050 Switching Cards .....	174
MCPS and MCIPS Control Functionality .....	174
MCPS100 Switching Card .....	175
MCPS100 Functional Description .....	176
MCIPS300 Switching Card.....	179
MCIPS300 Functional Description .....	180
AIM100 Aggregate Interface Module Overview.....	182
AIM300 Aggregate Interface Module Overview.....	183
NPT-1050 Tslot IO Modules .....	184
NPT-1050 Expansion Platform .....	187
<b>NPT-1022 Platform Family System Architecture .....</b>	<b>189</b>
NPT-1022 Platform Family Control Subsystem.....	191
NPT-1022 Platform Family Communication with External Equipment .....	192
NPT-1022 Platform Family Timing.....	192
NPT-1022 Platform Family Cooling Subsystem .....	193
NPT-1022 Platform Family Power Feed Subsystem .....	195
INF-B1U Overview .....	196
INF-B1U-D Overview.....	196

INF_B1UH-24V Overview .....	197
AC_PS-B1U Overview .....	197
NPT-1022 Platform Family Traffic and Switching Functionality.....	198
NPT-1022 Platform Family Tslot IO Modules .....	201
NPT-1022 Platform Family Expansion Platform.....	203
<b>NPT-1012D System Architecture.....</b>	<b>205</b>
NPT-1012D User Interfaces .....	206
NPT-1012D Communication with External Equipment and Management.....	208
NPT-1012D Timing .....	208
<b>IO Modules .....</b>	<b>210</b>
Card and Port Configuration Guidelines.....	210
Multiservice CES Cards .....	210
MSE1_16 Overview.....	215
MSE1_32 Overview.....	216
MSC_2_8 Overview .....	219
DMCES1_4 Overview .....	221
MS1_4 Overview .....	222
MS345_3 Overview .....	225
MS345_24 Overview .....	227
MS16_4MR Overview .....	229
Data Cards .....	231
DHGE_4E and DHGE_4EB Overview .....	239
DHGE_8 Overview .....	243
DHGE_8S Overview.....	245
DHGE_10 Overview .....	247
DHGE_16 Overview .....	249
DHGE_20 Overview .....	251
DHGE_24 Description .....	253
DHXE_2 Overview .....	255
DHXE_4 Overview .....	257
DHXE_4MR Overview .....	259
DHXE_4O Overview .....	260
DHXE_4sec Overview .....	262
DHXE_4MRsec Overview .....	264
DHXE_8 Overview .....	267
DHCE_1 Overview .....	268
DHCE_1C Overview.....	270

---

DHCE_1Q Overview .....	271
DHCE_1QB DHCE_1QC Overview .....	273
DHCE_2Q Overview .....	275
DHCE_2 Overview .....	276
DHCE_2F Overview .....	278
DHCE_2MRF Overview .....	279
DH25_4MR Overview.....	280
DH25_8MR Overview.....	282
DH400_1Q Overview .....	283
Pluggable Transceiver Modules .....	284
Smart SFPs: CES Transceivers .....	286
<b>Expansion Units .....</b>	<b>289</b>
EXT-2U and EXT-2UH Expansion Units.....	289
eEXT-2UH Expansion Unit.....	293
Expansion Unit Common Cards .....	299
INF_E2U Overview.....	299
AC_PS-E2U Overview .....	300
FCU_E2U Overview .....	300
FCU_eE2UH Overview .....	301
ACP2U Overview .....	302
Expansion Unit Traffic Cards .....	303
Optical Base Card Overview .....	305
MXP10 Overview.....	311
DHFE_12 Overview.....	315
DHFX_12 Overview.....	316
DHGE_10_POE Overview .....	317
DMCE1_32 Overview.....	318
EM_10E and EM_10EB Overview .....	319
MSC_2_16E Overview .....	326
Expansion Unit Tributary Protection Cards .....	328
TP32_2 Overview.....	328
TPS345_1 Overview .....	329
TPU345_24_1xx Overview.....	330
<b>Neptune Slot Reassignment and Product Migration .....</b>	<b>332</b>
Platform Replacement.....	332
Card Reassignment.....	332
Moving Cards to a Different Slot .....	333

---

MAC Address Retention .....	333
<b>FlexE Technology .....</b>	<b>334</b>
Understanding FlexE Technology .....	334
FlexE Applications for Transport Networks .....	337
FlexE Benefits .....	339
FlexE in an IP Transport World .....	340
FlexE Channel OAM .....	341
<b>CES Technology .....</b>	<b>342</b>
Smart SFP Solutions .....	342
Use Case: Smart SFP for E1-T1 Traffic .....	345
Use Case: E1-T1 to N x E1-T1 .....	346
CES Migration Applications .....	346
Voice Trunk Migration .....	347
Legacy Service Migration .....	347
Utilities Migration .....	348
Migration Technology .....	349
Standard Emulation Conventions and Interface Support .....	351
CES Protection Mechanisms .....	351
VLAN-Tagged and Double VLAN Classification .....	353
<b>Timing and Synchronization and Clock Recovery .....</b>	<b>354</b>
Adaptive Clock Recovery ACR Overview .....	355
Differential Clock Recovery DCR Overview .....	355
Synchronous Ethernet .....	356
IEEE 1588v2 PTP .....	357
GNSS Receiver Functionality .....	357
G.8275.1-G.8275.2 PTP Implementation .....	358
Hybrid Architecture - Combining SyncE and 1588 .....	359
Synchronization Summary Table .....	360
<b>Segment Routing .....</b>	<b>364</b>
SR Implementation .....	364
Segment Identifiers SID .....	365
SR with BGP .....	368
Topology Independent Loop-Free Alternate FRR TI-LFA .....	369
SR Applications .....	369
SR and LDP Interworking: Ships in the Night .....	371
SR Advantages .....	371

---

<b>IP-MPLS Technology .....</b>	<b>372</b>
Understanding MPLS-TP .....	372
Understanding IP-MPLS.....	375
IP Routing for IP-MPLS .....	376
Understanding IPv4.....	377
Understanding IPv6.....	378
IPv6 Addressing .....	379
Anycast Addresses.....	380
ICMPv6.....	381
Neighbor Discovery .....	381
NDP Tracking .....	382
Understanding Subnetworks .....	382
IPv4 Subnetworks .....	383
IPv6 Subnetworks .....	385
Supporting Multiple IP Addresses .....	385
IP Networking in the Control Plane .....	386
Switching and Routing.....	387
Processing Inbound Packets.....	388
MPLS-TP and IP-MPLS Interworking Models .....	389
Overlay using GRE.....	390
Stitching via Signaling Gateways .....	391
Stitching PE .....	392
Interworking Example.....	393
Integrate Smoothly with Third-Party Elements .....	394
DHCP Relay Agent and Option 82 .....	395
<b>Border Gateway Protocol BGP .....</b>	<b>398</b>
ADD-PATH Support .....	398
AIGP for BGP .....	399
BGP Graceful Restart.....	401
BGP Prefix Independent Convergence: BGP PIC.....	402
BGP Route Aggregation .....	402
ECMP for BGP .....	403
Labeled Unicast: BGP-LU - RFC3107.....	403
Route Reflection .....	404
Virtual Route Reflection: vRR.....	407
<b>Intermediate System to Intermediate System IS-IS.....</b>	<b>409</b>

---

---

IS-IS Level 1 and Level 2 .....	409
IPv6 Support in IS-IS.....	409
IS-IS Support for Segment Routing SR.....	410
SPF and LSP Delay Algorithms for IS-IS .....	410
What is SPF Delay in IS-IS .....	412
What are LSP Generation Timers .....	413
IS-IS SPF and LSP Generation Mechanisms.....	413
IS-IS Graceful Restart .....	414
<b>Label Distribution Protocol LDP .....</b>	<b>415</b>
<b>Open Shortest Path First OSPF .....</b>	<b>416</b>
OSPFv2 for IPv4: RFC 2328 .....	416
OSPFv3 for IPv6: RFC 5340 .....	416
OSPF Support for Segment Routing SR .....	417
SPF and LSA Delay Algorithms for OSPFv2 and OSPFv3 .....	418
What is SPF Delay in OSPF.....	419
What are LSA Generation Timers.....	420
OSPF SPF and LSA Generation Mechanisms .....	421
OSPF Graceful Restart .....	422
<b>Protocol-Independent Multicast PIM .....</b>	<b>423</b>
PIM IPv6 Support .....	424
Multicast Listener Discovery MLD .....	425
<b>Resource Reservation Protocol: RSVP .....</b>	<b>427</b>
RSVP Terminology .....	427
What is an RSVP Session .....	428
Unique LSP Paths in the Network .....	429
RSVP-TE Refresh Reduction .....	432
RSVP-TE Make-Before-Break Mechanism .....	432
RSVP-TE Authentication .....	433
RSVP OAM: Ping and Traceroute .....	433
RSVP-TE Protection.....	434
RSVP-TE Graceful Restart.....	436
RSVP-TE Hello.....	437
<b>Virtual Router Redundancy Protocol VRRP .....</b>	<b>439</b>
<b>Layer 2 VPN: Providing a Full Set of MEF CE3.0 Services.....</b>	<b>442</b>
Ethernet Private Line EPL - Ethernet Virtual Private Line EVPL .....	444
Ethernet Private LAN EPLAN - Ethernet Virtual Private LAN EVPLAN .....	445

---

Multicast Optimized Rooted-MP Services .....	446
IP Multicast Architecture.....	449
IGMP-Aware MP2MP VSI .....	451
<b>Layer 2 Service Card Functionality .....</b>	<b>454</b>
Layer 2 Card Services.....	454
Generic Faming Procedure .....	454
Virtual Concatenation .....	455
Link Capacity Assignment Scheme.....	455
Layer 2 Switching Capabilities .....	455
FDB Quota Provisioning.....	456
Triggers for MSTP .....	456
Port-Based VLANs .....	457
UNI on EoS Ports .....	457
NNI on ETY Ports .....	457
C-VLAN Functionalities .....	457
Access-Controlled Management.....	458
Port Mirroring.....	459
L2CP Flooding Protection .....	459
Additional Features .....	459
<b>Ethernet VPN: EVPN .....</b>	<b>461</b>
What is EVPN.....	461
The EVPN VPLS Solution .....	462
The EVPN VPWS Solution.....	465
EVPN Operation Modes .....	466
Example: EVPN Multi-Homing Mechanism for L2 Domain-Ring Connectivity .....	468
EVPN Route Types .....	469
EVPN Service Interface Types .....	470
EVPN Anycast IRB Mechanism.....	472
<b>Layer 3 VPN .....</b>	<b>473</b>
Example: L3VPN Application.....	473
L3VPN Policies.....	474
6VPE: L3VPN for IPv6 .....	475
HoVPN Architecture .....	476
HoVPN Deployment Scenario .....	477
<b>L2VPN and L3VPN Interworking .....</b>	<b>479</b>
L3VPN PW Extension with PHT.....	479

Integrated Routing and Bridging IRB.....	482
<b>Model-Driven Telemetry: MDT .....</b>	<b>483</b>
Telemetry Modes .....	484
Telemetry Entities .....	485
Telemetry Subscription Methods and Modes .....	486
gRPC and gNMI Framework .....	487
<b>OAM and Performance Monitoring PM.....</b>	<b>489</b>
Ethernet Link OAM - IEEE 802.3-05 .....	490
MPLS-TP Tunnel OAM.....	491
IP-MPLS VPN Service OAM and PM .....	492
TWAMP - RFC 5357.....	493
Link Delay Measurement.....	494
Service OAM CFM - IEEE802.1ag .....	495
CFM-PM Y.1731 .....	497
Throughput RFC 2544.....	498
SLA Y.1564 .....	499
sFlow RFC 3176.....	499
SNMP v2-v3 .....	501
Link Layer Discovery Protocol LLDP .....	502
<b>Ensuring Quality of Experience QoE.....</b>	<b>503</b>
Traffic Management and Performance Overview .....	503
Quality of Service QoS Overview .....	504
Ingress Traffic Management.....	505
Hierarchical Scheduling.....	506
DiffServ Architecture Overview.....	507
Layer 3 Classification .....	508
MPLS TC to DSCP Mapping .....	508
<b>Neptune Protection and Restoration Mechanisms .....</b>	<b>512</b>
LSP Tunnel Restoration .....	513
LDP FRR with Loop-Free Alternatives LFA .....	515
FRR using Local LFA .....	516
FRR using Remote LFA .....	517
Object Tracking .....	518
Tracking Policy Objects .....	519
Using Tracking Policies to Disable Interfaces .....	519
Linear Protection .....	520

PW Redundancy .....	521
Hierarchical VPLS Services .....	523
PW Redundancy for H-VPLS DH Topology .....	526
Multi-Segment PW .....	527
FAT: PW Load Balancing .....	531
Link Aggregation LAG .....	532
Multichassis LAG MC-LAG Protection .....	535
Dual Homing DH .....	536
Link Loss Carry Forward LLCF .....	538
Customer Change Notification CCN .....	540
Resilience and High Availability .....	542
High Availability through Nonstop Forwarding .....	543
Ethernet Ring Protection Switching ERPS PB .....	545
RSTP-MSTP Protection .....	546
Input-Output Protection IOP .....	546
Optical Protection Mechanisms .....	547
Tributary Protection TP Mechanism .....	549
Equipment Protection .....	550
<b>NE Security .....</b>	<b>552</b>
Comprehensive Security Mechanisms .....	552
MACsec 802.1AE .....	553
Port-Based Network Access Control 802.1x .....	554
MAC Authentication Bypass MAB .....	555
TACACS+ .....	556
TACACS+ Authentication Authorization and Accounting .....	557
Firewall Filters .....	558
Filter Evaluation Process .....	558
Management Plane Protection .....	561
Dynamic ARP Inspection DAI .....	562
Enhanced Security Features for Communication Channels .....	563
Secured File Transfer Communication .....	563
Public Key Cryptography Authentication .....	564
OSPF Encryption with HMAC-SHA256 .....	564
<b>Installation and Management .....</b>	<b>565</b>
Zero Touch Provisioning ZTP .....	565
ZTP Generic Workflow .....	566
ZTP Features and Capabilities .....	567

---

Zero Touch Installation ZTI .....	568
LightSOFT NMS Management .....	568
Layered Architecture Maximizes Flexibility.....	570
Easy Data Management.....	570
Graphic User Interface .....	572
GCT to EMS .....	573
Carrier SDN Integration .....	574
EMS-NPT .....	578
Local Craft Terminals.....	581
CLI Configuration Overview .....	582
Command Line Interface .....	582
CLI Hierarchy Display Modes.....	584
Entering Commands.....	584
Supportive Help System.....	585
Command Completion.....	586
<b>Standards and References for the Neptune Product Line .....</b>	<b>588</b>

# Neptune Reference Manual

This document describes the key components of the Neptune platforms, including cards, modules, accessories, and related capabilities. It also provides detailed descriptions for interpreting indicator functions, enabling field personnel to troubleshoot hardware-related problems.

# Neptune Reference Manual Revision History

The following table lists the published revisions of this document, and briefly describes the main changes in each revision.

## Revision History

Revision No.	Pages Changed	Description of Changes
01	N/A	Preliminary

# Introducing Neptune

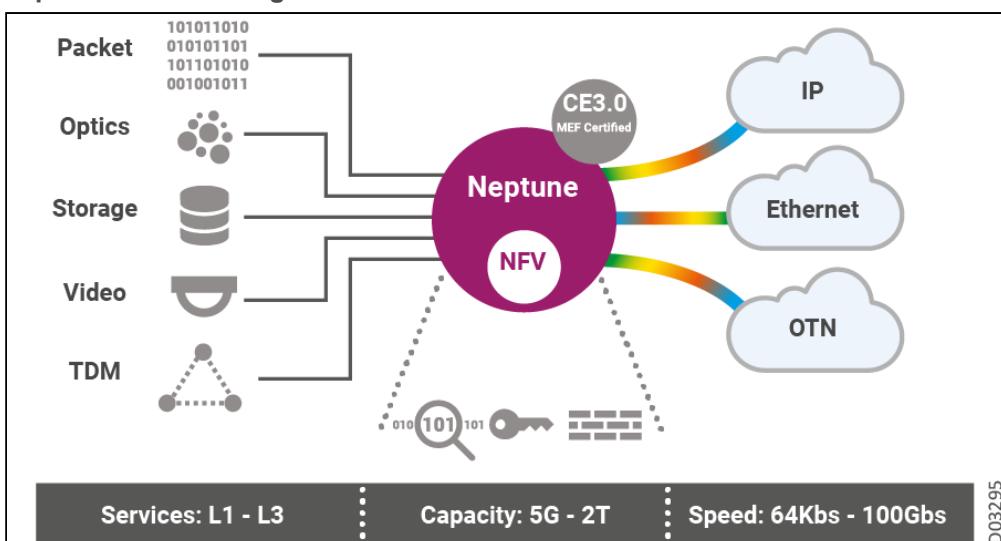
Neptune (NPT) is a family of carrier-class MPLS-based multiservice IP-optical transport platforms, offering best-in-class carrier Ethernet and IP transport solutions for the metro. Neptune streamlines end to end (E2E) metro service delivery by combining:

- Carrier grade service assurance, visibility, and control
- IP efficiency
- Unparalleled L1 to L3 multiservice support.

Neptune features a wide variety of platforms, ranging from 5G to 2T with an in service expansion unit. Neptune offers a powerful, flexible, and efficient E2E solution from the metro access to the metro core, for high-performance L1 to L3 services through convergence of:

- IP
- Elastic MPLS (IP and TP) and segment routing
- Segment Routing
- EVPN
- FlexE
- Ethernet (MEF CE2.0, CE3.0 certified)
- L3VPN and L2VPN services
- Interfaces ranging from 10M to 400G
- WDM
- Wide range of OTN transparent services, including TDM, Ethernet, video, and storage
- Legacy TDM services are supported natively, through Circuit Emulation (CES) or over OTN, with interfaces ranging from PCM to SDH

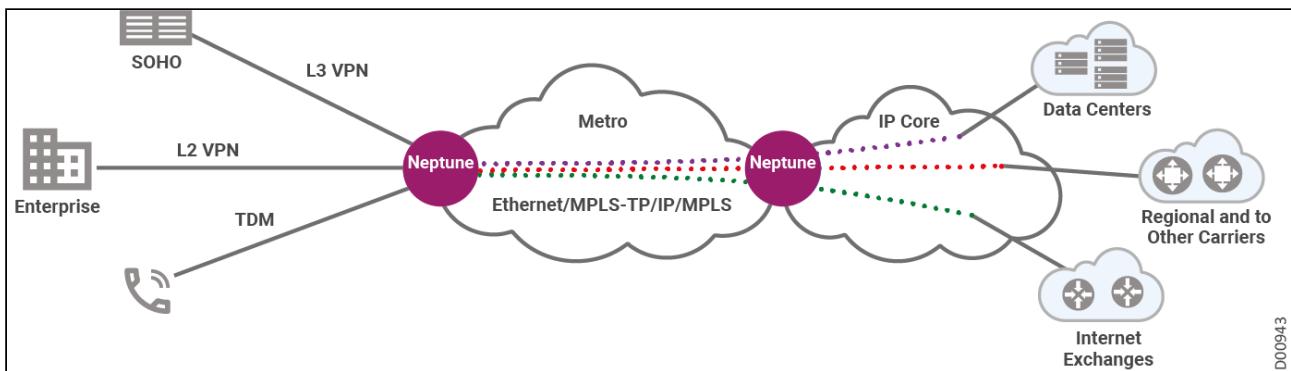
**Neptune Network Diagram**



Neptune's broad set of transport features provides carrier class service availability and scalability, along with IP synchronization support. Consequently, Neptune is well suited for a wide range of applications and networking scenarios, including:

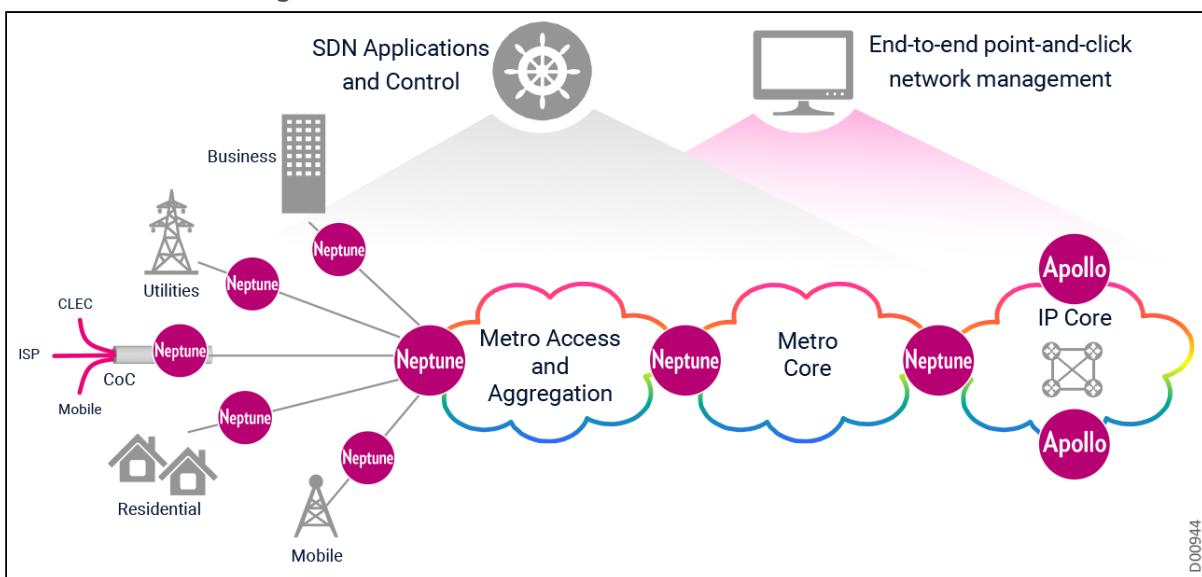
- Multi G mobile backhaul from 2G to LTE A and 5G
- Business and wholesale
- Utilities
- Residential multi-play

## Neptune's Wide Range of Applications and Networking Scenarios



Neptune's flexible traffic-handling architecture offers the most cost-efficient traffic handling in an IP environment while supporting all transport attributes. The result is the lowest TCO throughout the network life cycle, not only over the course of the network transition from TDM-centric to IP-centric, but also when building new carrier Ethernet and IP-based transport networks.

## Seamless Interworking



Neptune is managed by the GUI-based unified multilayer LightSOFT NMS, and is SDN ready for operation with an SDN controller. LightSOFT provides point-and-click service provisioning with configurable per-port QoS, plus hard QoS and Service Level Agreement (SLA) assurances, based on a sophisticated Connection Admission Control (CAC) algorithm. Access to CLI management at the network element (NE) level enables hands-on control at the deepest level, for the most efficient management fine tuning.

Neptune key value propositions include:

- Unmatched multi-service: L1 to L3
  - L3VPN & L2VPN with elastic MPLS and segment routing
  - L1 traffic isolation with FlexE
  - L1 transparent OTN services (storage, video, Ethernet, TDM)
  - TDM: CES from PCM to STM-16
  - Variety of virtual network functions (VNFs)
- Carrier grade service assurance
  - Performance: MPLS-TP based deterministic performance
  - Equipment: Fully redundant
  - Network: Extensive protection and resiliency schemes
  - Control: Separate control and data planes

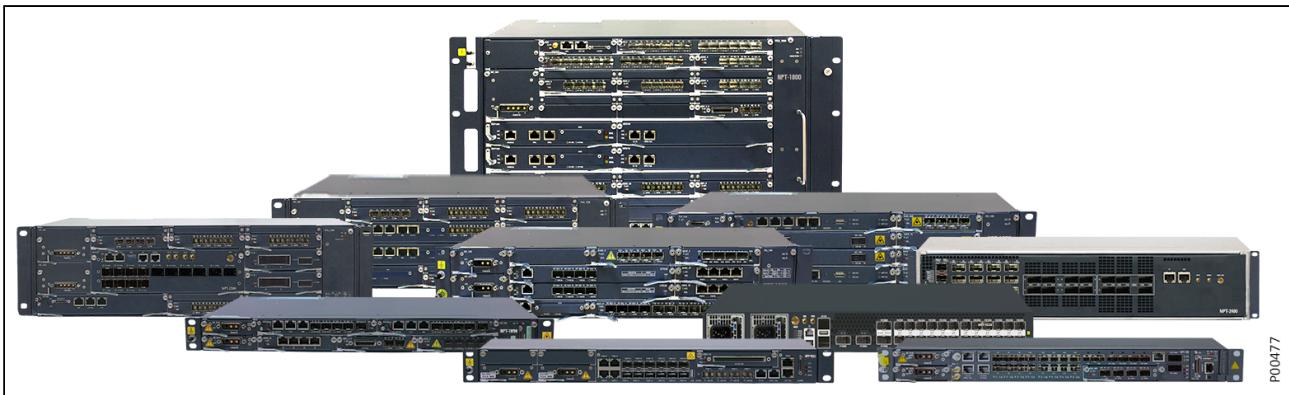
- Management: Automatic RDR (Remote Data Replication)
- E2E from CPE to metro core
  - From 5G to 3T
- Multi-layer visibility and control, through a unified multilayer GUI-based NMS and Muse
- CLI (Command Line Interface), a powerful mechanism to access, configure, and monitor Neptune devices

This section introduces the following features:

- [NPT Platforms: Tailored to Your Needs](#)
- [Implementation Principles](#)
- [Neptune Expansion Platforms](#)
- [Features and Functions](#)
- [Intelligent Edge Service](#)

## NPT Platforms: Tailored to Your Needs

### Neptune Family of Platforms



Neptune provides a comprehensive selection of platforms, offering a range of sizes, configurations, and service level requirements, making them suitable for different deployment scenarios and services.

### Multiservice Edge

The multiservice edge supports a wide range of services delivered from the complete range of fixed and mobile access networks. In some cases, (like business services and mobile), the multiservice edge device is the customer premise equipment (CPE) or the cell site router (CSR). In other cases, the multiservice edge devices will need to be hardened to meet specific environmental constraints, allowing them to be deployed outside the equipment rooms, (for example, in street cabinets or substations). These multiservice edge devices must be agile enough to support a mix of legacy and current services, and flexible enough to support service mix evolution and the addition of new services, with no need for replacing the hardware.

Modular, cost-effective Neptune platforms positioned at the multiservice edge offers the following features:

- Aggregation and grooming
- Elastic IP for multiservice IP transport
- CPEs for business services and mobile
- Combining high density with highly compact size
- Support for current, legacy, and future services

Metro Ethernet routing, tailored to specific service needs, is an essential element in building the next generation multiservice edge. These multiservice edge routers combine support for IP protocols (RIP, BGP, ISIS, OSPF) with support for Layer 3 services (IP VPN, MPLS VPNs, PWE3), while supporting PDH/Async connections and WAN interfacing (POS, ATM). These routers aggregate traffic from the access networks and groom this traffic onto the most appropriate transport technology for transport across the metro network. The

metro transport can be either metro IP or optical transport, depending on the service needs. So the multiservice edge devices must be able to support IP, Ethernet, and optical transport line interfaces.

Due to the diverse nature of the multiservice edge, Neptune provides a range of multiservice edge devices, each optimized to meet the needs of specific business niches and their specific service requirements:

- **NPT-1022/NPT-1022B:** Multiservice IP access, edge, aggregation, and transport. Multiservice 1RU IP transport platform, providing up to 64G switching capacity and a generous fan-out for GE and 10GE interfaces. A powerful, flexible, and efficient end-to-end solution for L2 and L3 services, by converging IP, elastic MPLS, segment routing, Ethernet (MEF CE3.0), and TDM over CES/CEP.
- **NPT-1050:** Multiservice IP edge for aggregation and hub locations in 3G and LTE networks. Fully redundant 1RU multiservice IP transport platform, providing up to 300G switching capacity a port fan out of up to 380G and 100G per slot. Flexible efficient support for L3 and L2 services, with elastic MPLS, segment routing, Ethernet (MEF CE3.0), and TDM over CES/CEP. Ideal for second and third level aggregation and cellular hub locations in 3G and LTE networks.
- **NPT-1100:** Multiservice IP optical transport, optimized for high fan-out metro access/pre-aggregation applications. Multiservice 1RU IP transport platform, providing up to 300G switching capacity and a generous fan-out of up to 582G, for GE, 10GE, and 100GE interfaces. Delivering powerful, flexible, and efficient end-to-end solution for L2 and L3 services, by converging IP, elastic MPLS, segment routing, Ethernet (MEF CE3.0), and TDM over CES/CEP.

### Converged Metro IP Transport

Converged metro IP transport provides an IP transport network optimized for grooming, routing, and backhauling IP traffic from the multiservice edge to the IP core.

Neptune embraces next generation IP transport by combining dynamic router capabilities with the deterministic traffic engineering and service creation capabilities required for the next generation of advanced services. Neptune's support for an IP/MPLS control plane and multi protocol BGP L3VPN services, combined with comprehensive L2 functionality and the deterministic traffic engineering enabled by MPLS-TP and segment routing, make Neptune a versatile and effective solution for this next generation IP transport network.

Neptune's converged metro IP transport platforms offer the following features:

- Optimized for pre-aggregation and aggregation
- Common operating system across the whole portfolio
- Programmable features optimized and instrumented for 5G
- Core gateway for hand-off to the IP core
- Scalable platforms
- Agility to support current, legacy, and future transport needs

The metro network scales significantly. Neptune provides a modular range of platforms ranging from 2RU with 560G capacity, through to a full rack platform with 16Tbps switching capacity:

- **NPT-1200:** Multiservice metro IP pre-aggregation and hub locations in 3G and LTE networks. Fully redundant 2RU multiservice IP transport platform, providing up to 560G switching capacity and 100G per slot. Flexible efficient support for L3 and L2 services, with elastic MPLS, segment routing, Ethernet (MEF CE3.0), and TDM over CES/CEP. Ideal for second and third level aggregation and cellular hub locations in 3G and LTE networks.
- **NPT-1250:** Multiservice metro IP pre-aggregation and 5G backhaul. Fully redundant, 2RU, 5G-enabled platform, providing up to 560G interface switching, 300G processing capacity and 100G interfaces. Flexible efficient support for L3 and L2 services, with elastic MPLS, segment routing, Ethernet (MEF CE3.0), and TDM over CES/CEP. Optimized for 5G transport networks with flexible Ethernet (FlexE), segment routing, and advanced timing/synchronization.
- **NPT-1300:** Multiservice metro IP for high capacity pre-aggregation applications. Fully redundant, 3RU platform providing up to 1Tbs capacity (future upgradable to 2T) with 100G/200G interfaces (future upgradable to 400G). Optimized for high-capacity and high fan-out metro pre-aggregation applications, and delivering L2, L3, and TDM (CES) services. Ideal for IP over DWDM applications, providing 100G coherent interfaces mapped to OTU4, and 200G interfaces mapped to OTUC2.

- **NPT-1800:** Multiservice metro IP for aggregation applications and 5G backhaul. Fully redundant, 8RU platform providing up to 2Tbs capacity with 100G interfaces. Flexible efficient support for L3 and L2 services, with elastic MPLS, segment routing, Ethernet (MEF CE3.0), and TDM over CES/CEP. Optimized for 5G transport networks with flexible Ethernet (FlexE), segment routing, and advanced timing/synchronization.
- **NPT-2100:** High capacity, high density access router providing 800G non-blocking switching capacity and 1G/10G/25G/50G/100G/200G and 400G interfaces in a temperature hardened 1RU form factor, suitable for both outdoor and indoor deployment. Designed for next-generation services and applications, the NPT-2100 supports an extensive set of interfaces for multiple access technologies, such as Ethernet, MPLS, and legacy TDM, making it the ideal solution for deployment at the access edge. With a full set IP/MPLS transport capabilities, the NPT-2100 can efficiently aggregate and route services over the network, meeting their service performance needs (SLAs) on a service by service basis.
- **NPT-2300:** Compact, modular, aggregation router designed to provide aggregation for services, applications, and architectures requiring a high-capacity, high performance multiservice solution. With support for IP/MPLS, MPLS-TP, SR-TE, and IPoDWDM, the NPT-2300 can use the right IP transport technology for each service it provisions. The basic platform configuration provides up to 1.4T capacity at 1000Mpps, and supports 10M/100M, 1G/10G/25G/50G/100G/200G, and 400G interfaces, all in a 3RU form factor. This can be extended to 3T fan-out and 2.4T switching capacity through the addition of service cards.
- **NPT-2400:** High-performance, versatile, metro aggregation router, designed for next generation services and applications. providing 4.8T non-blocking switching capacity and 10G/25G/50G/100G/200G and 400G interfaces in a compact 2RU form factor. The NPT-2400 is optimized for the metro edge, for telecom exchange and data center locations. With a full set of IP/MPLS/MPLS-TP/Segment Routing transport capabilities, the NPT-2400 can efficiently aggregate and route services over the network, meeting their service performance needs (SLAs) on a service by service basis. The NPT-2400 provides an extensive number of coherent interfaces for both 100G/200G and 400G, complying with OpenZR+ technology, and making it an ideal IPoDWDM metro aggregation platform for any telecom provider.

This reference manual describes the shelf layout and system architecture of each platform in the Neptune family. Additional sections describe the I/O cards, transceiver modules, and the data features available through the EMS management system.

**i Note**

Some of the Neptune platforms can optionally be configured with an EXT-2U expansion unit. This modular approach maximizes efficiency while minimizing expense.

For enhanced readability, descriptions of the EXT-2U slot layout are not repeated in each Neptune platform section. The information is provided in [EXT-2U and EXT-2UH Expansion Units](#) and referenced from other sections.

Neptune platforms have been designed to facilitate simple installation and easy maintenance. Hot insertion of cards and modules is allowed to support quick maintenance and repair activities without affecting traffic. The cage design and mechanical practice of all platforms conform to international mechanical standards and specifications.

**i Note**

All installation instructions, technical specifications, restrictions, and safety warnings are provided in the *Neptune Installation and Maintenance Manuals*. See these manuals for specific instructions before beginning any Neptune platform installation.

## Implementation Principles

The Neptune platforms have a fully modular design based on a redundant routing core implemented as a cross-connect matrix surrounded by I/O ports on plug-in I/O cards. The function of the I/O cards is to provide interfaces to the various types of signals that can be transported by the platforms. Internally, all the I/O cards exchange information with the routing core using a proprietary format that does not depend on the characteristics of the external interfaces.

The use of a single proprietary format for all the information flowing through the Neptune results in a highly flexible system that supports a wide range of applications and can easily be expanded to suit virtually any customer need. Moreover, support for new signal formats can be added simply by developing new I/O cards. This protects customer investment in the Neptune platform against obsolescence, and ensures cost-effective upgrade paths.

The Neptune platforms consist of the following main subsystems:

- Traffic processing
- Control and communications
- Timing and synchronization
- Switching/routing core (implemented according to specific platform type)
- Power feed
- Cooling

All the subsystems are modular and implemented as plug-in cards. Except for the traffic interfaces, all the subsystems are fully redundant and/or are implemented as distributed functions. This prevents a single point of failure, thereby ensuring the high availability needed to meet the stringent requirements of telecom operators.

Moreover, Neptune platforms are designed to permit live insertion and hot swapping of cards and modules, and their software can be downloaded from a remote location. In addition to maintenance efficiency, these characteristics enable non-traffic-affecting in-service upgrading and expansion of system capabilities.

## Neptune Expansion Platforms

The Neptune product line includes a set of expansion units, supplemental units that provide a base NPT-XXXX platform with additional traffic and protection capabilities, enhancing scalability and providing the flexibility of additional I/O slots, available to be used as needed.

These platforms are high density modular expansion units for the Neptune's multiservice metro access platform series, supporting the complete range of CES, PCM, optics, and Ethernet services. All traffic processing, packet switching, timing and synchronization, and control and communication functions are performed by the corresponding system in the base unit. The type of traffic delivered by the unit depends on the capabilities and configuration of the base unit. I/O expansion cards are supported in accordance. Integrating this add-on platform into your network configuration is not traffic-affecting.

In addition, the expansion platform has separate sections including:

- **Power feed:** Including local power supply circuits on each card and two power units
- **Cooling fans:** Provided by the FCU unit on the right side of the expansion unit
- **Three Eslots** for installing traffic cards supporting PCM, Ethernet, OTN muxponders, and optical functionality

For more information, see [Expansion Units](#).

## Features and Functions

Neptune platforms support a multitude of features for today's bandwidth-hungry networks, including:

- Transparent support of transmission channels for Fast Ethernet, Gigabit Ethernet (GE), MPLS, IP, SAN (FC), digital video, and more.

- Supporting any service; VPWS, VPLS, IPTV MPLS multicast, 3G/4G/5G mobile backhaul, bandwidth services, and Ethernet leased lines.
- Transport of Ethernet traffic.
- Add and drop of any signal (data, wavelength) at any node using a single platform.
- 10Gbps Add/Drop Multiplexer (ADM) service on a card for GE, 1GFC, 2GFC, OTU1, and STM-16/4/1 services. MXP10's "ADM on a Card" benefits include the ability to route client signals to different locations along the optical ring, as well as per-service selectable protection and drop-and-continue features. The MXP10 can also be used as a multi-rate combiner up to OTU2. The MXP10 combines the cost efficiency of an optical platform with the granularity and flexibility previously available only in SDH networks.
- Comprehensive MPLS Carrier Ethernet capabilities, including use of MPLS technology to carry Ethernet services across the network metro and core.
- Subrate traffic aggregation over optical cards.
- Full compliance with applicable ITU-T and Telcordia standards for optical equipment and safety standards.
- Extremely powerful management that renders the system easy to control, monitor, and maintain.

## Intelligent Edge Service

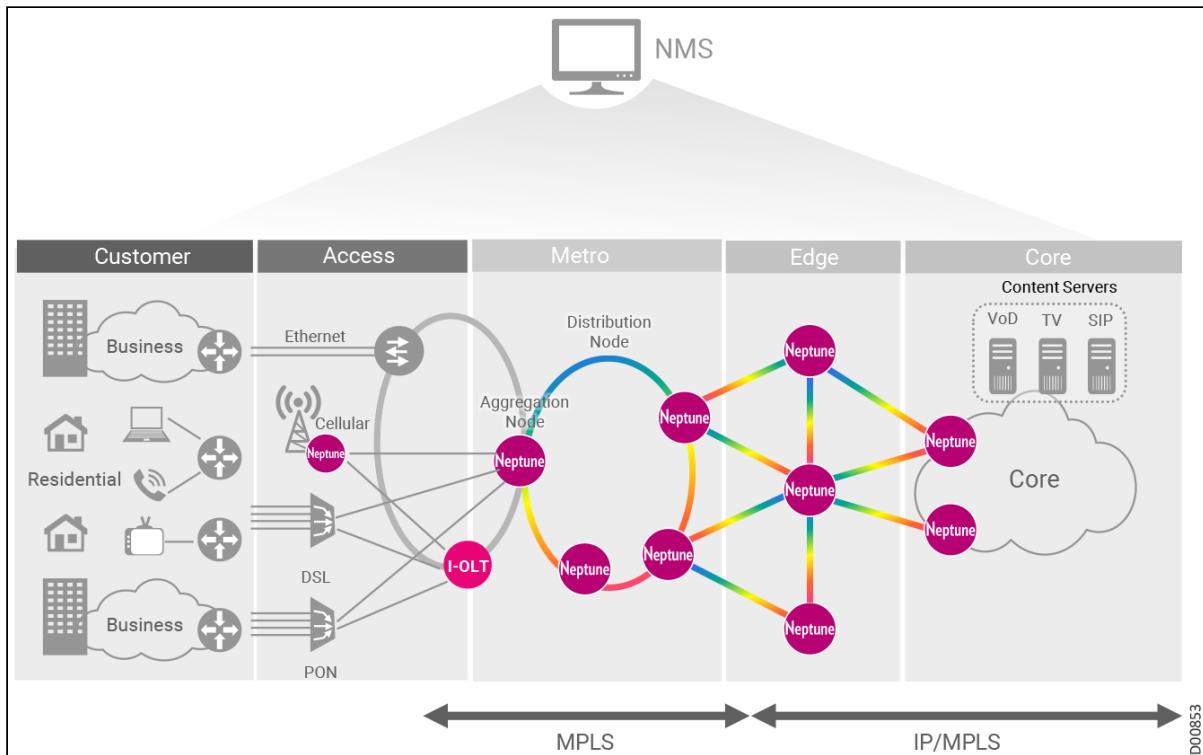
With the mobile data explosion and the proliferation of IP-based services, the shift to IP-based transport networks is only natural. IP-based transport is considered the solution to lowering network cost per bit while cost effectively coping with the huge traffic growth driven mainly by IP traffic.

Metro Ethernet routers are an essential element in building IP-based networks, tailored to the requirements of the network service edge. These multi-function routers combine support for IP protocols (RIP, BGP, ISIS, OSPF) with support for Layer3 services (IP-VPN, MPLS VPNs, PWE3) while supporting PDH connections and WAN interfacing (POS, ATM). These routers are designed for aggregating dedicated access connections, grooming multiple edge devices for the core, comprehensive IP processing, and provisioning of network-based IP services such as VPNs. They can also be used as a platform for mobile IP core traffic.

Neptune's support for IP/MPLS control plane and multi-protocol BGP L3VPN services, combined with comprehensive L2/MPLS-TP functionality, provide a versatile and effective solution for intelligent IP transport network requirements.

Neptune platforms can groom and route traffic onto an IP/MPLS core network. Advanced router features meet the needs of carriers that want to introduce high-margin services across an IP/MPLS backbone.

## E2E Network Management from Access to Core



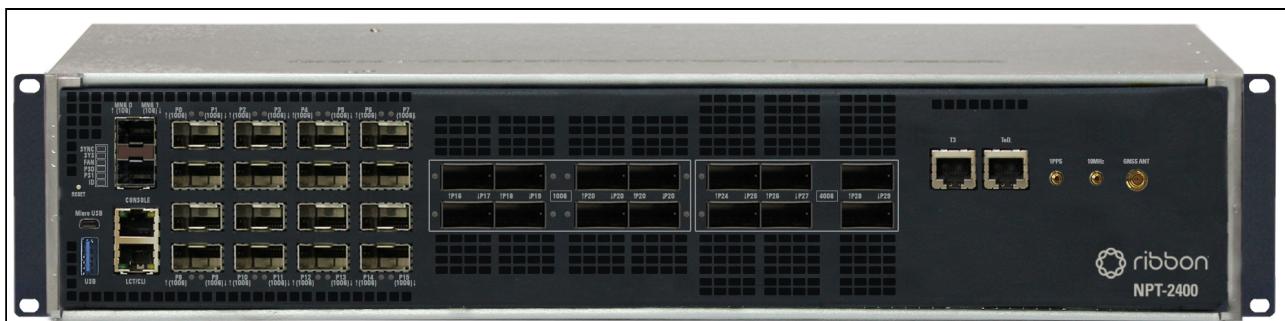
# NPT-2400 System Architecture

The NPT-2400 is high-capacity, high-performance, metro edge aggregation router, designed to provide aggregation and transport for services, applications, and architectures requiring a performance/cost optimized solution.

A 4.8T non-blocking switch capacity, high 100G fan-out, 6 x 400G client/line interfaces, and 2RU form factor mean the NPT-2400 provides the performance and interfaces required at the metro edge aggregation sites in xHaul, broadband backhaul, and Converged Interconnect Networks (CINs). The full set of IP/MPLS/MPLS-TP/Segment Routing transport capabilities provided by Ribbon's IP Wave rNOS allows the NPT-2400 to meet the service performance needs (SLAs) at these aggregation sites, on a service-by-service basis. 5G-specific functionality, such as 5G-specific interfaces and Class C timing, mean the NPT-2400 is ideally suited for aggregation sites in xHaul-specific networks, or in multiservice networks where mobile xHaul and fixed broadband backhaul are supported. Redundant and hot-swappable components, and a high port density design, allow the NPT-2400 to deliver high system reliability and Ethernet switching performance, while network intelligence helps reduce infrastructure and administrative costs.

The NPT-2400 provides an extensive number of coherent, OpenZR+ compliant interfaces for 100G/200G and 400G, providing it with the IPoDWDM and/or IPoOIS capabilities essential in today's metro aggregation network.

## NPT-2400 Front Panel

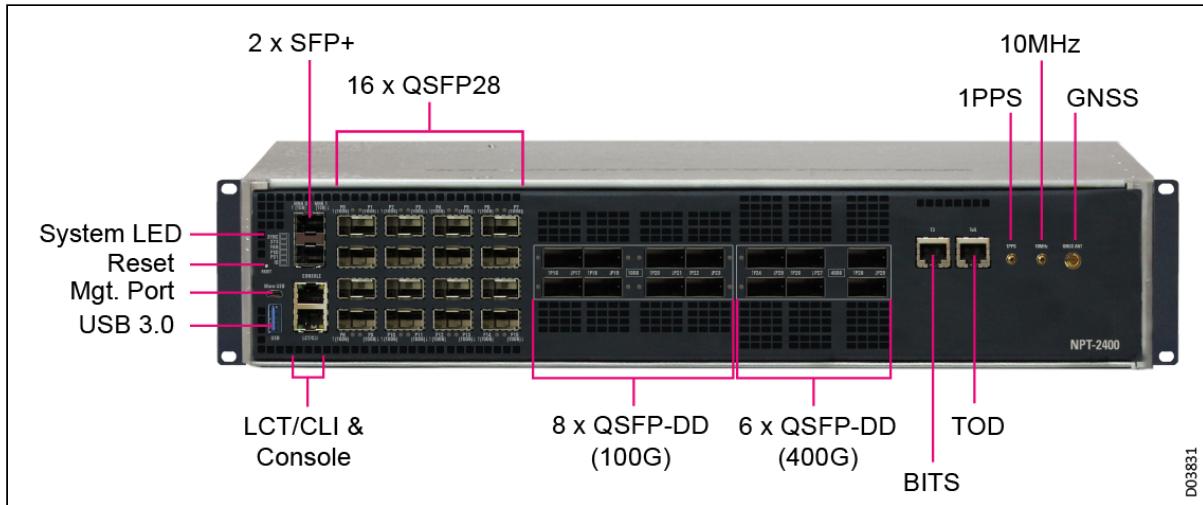


The NPT-2400 can be deployed as either a fully integrated or disaggregated router. This flexibility is achieved through Ribbon's IP Wave rNOS network operating systems (NOS), as well as NPT-2400's full compliance to the standard Open Network Install Environment (ONIE) installation environment, allowing the IP Wave rNOS to be operated on approved, certified, ODM hardware.

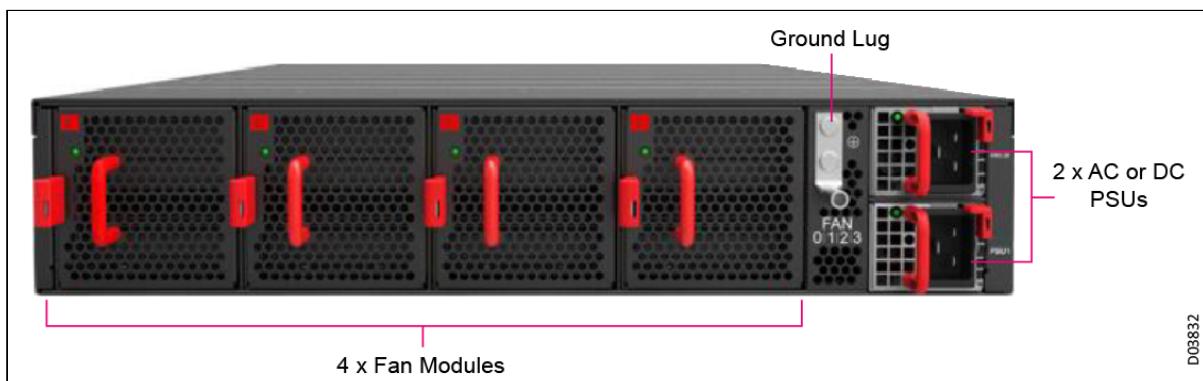
This compact (2U) base platform is housed in a 87.7 mm high, 436 mm wide, and 762 mm deep (3.45 in. x 17.16 in. x 30 in.) equipment cage. All its interfaces are accessible from the front of the unit. The platform includes the following components:

- Native packet-level switching with 4.8T switching capacity and traffic management (packet processing)
- 30 traffic ports
  - 16 x 100G QSFP28
    - 8 ports can be used as breakout ports of 4 x 10G/25G
    - 8 x 100G QSFP-DD (coherent-ready for IPoDWDM)
      - 4 ports can be used as breakout ports of 4 x 10G/25G
    - 6 x 400G QSFP-DD (100G/400G coherent-ready for IPoDWDM)
      - All 6 ports can also be used as breakout ports of 4 x 100G
  - Management interfaces:
    - 1 x GbE (RJ45) LCT/CLI or OOB management port (in V9.2)
    - 1 x USB 2.0 general purpose port (type A)
    - 1 x RS232 console port (RJ45)
    - 1 x Micro USB console port
    - 2 x 10G SFP+ management ports

- 1 system reset switch



- Two power supplies for 1+1 redundancy, hot swappable (2xAC or 2xDC)
  - DC Power supply - 1600W @ -48VDC
  - AC Power supply - 1600W @ 100-240VAC
- 3+1 redundant fan (field replaceable unit) with front to back air flow



- Comprehensive timing and synchronization capabilities:
  - Bits (E1/T1, T3/T4)
  - GNSS built-in receiver
  - 10MHz
  - SyncE ITU-T G.8262.1 compliant
  - IEEE 1588v2 G.8275.1, G.8275.2 (in V9.3)
  - G.8273.2 – Class C compliant
  - 1PPS and ToD
  - Hybrid 1588 and SyncE
  - APTS

This section introduces the following NPT-2400 features:

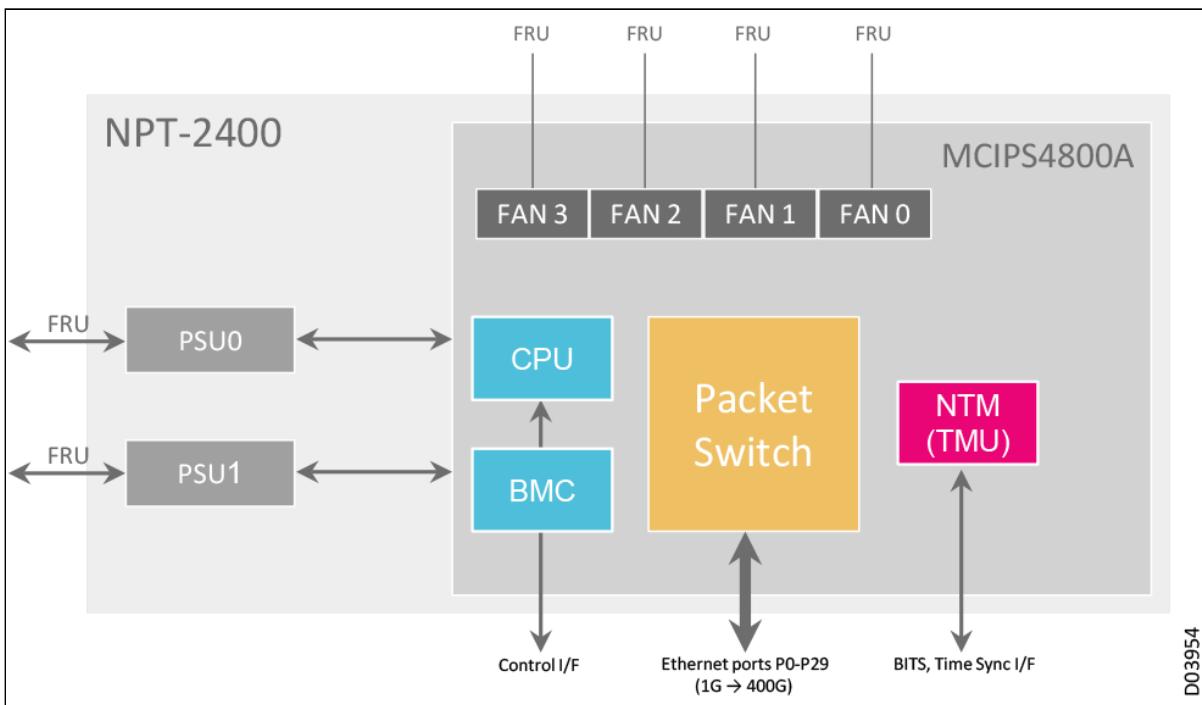
- [NPT-2400 Switching Functionality](#)
- [NPT-2400 Control Subsystem](#)
- [NPT-2400 Communications with External Equipment and Management](#)
- [NPT-2400 Timing](#)
- [NPT-2400 Cooling Subsystem](#)
- [NPT-2400 Power Feed Subsystem](#)

## NPT-2400 Switching Functionality

The NPT-2400's built-in switch provides the following main functions:

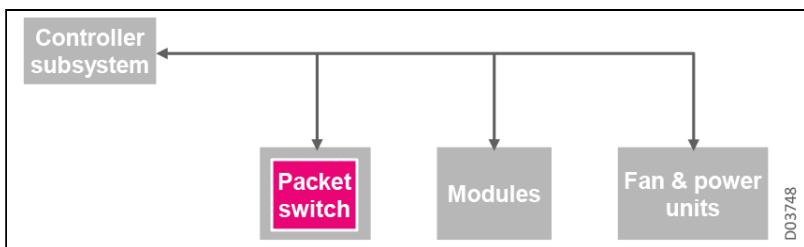
- All Native Ethernet packet switch, supporting native packet-level switching with 4.8T full-duplex packet processor, with a 2000Mps processing rate, providing:
  - Management and internal control
  - User traffic switching
  - Non-blocking data switch fabric up to 4.8T (IMIX)
- OTSOP16 Smart SFP supported in SFP+ 10GE ports
- 5G-ready packet transport, including:
  - Stringent phase synchronization requirement for Class C/D timing accuracy compliance (8273.2)
  - 10G, 25G, 100G, and 400G interfaces
- Comprehensive range of timing and synchronization capabilities (G.781/G.8262 compliant EEC, G.8273.2):
  - GNSS receiver
  - 1PPS and ToD interfaces
  - 10MHz (In/Out)
  - BITS (T3/T4)
  - SyncE
  - IEEE 1588v2 PTP with:
    - OC (primary & secondary), BC
    - One-step TC
    - G.8275.1 and G.8275.2 profiles
    - G8273.2 Class C/D timing accuracy compliance
  - Hybrid 1588 and SyncE
  - APTS
- Traffic management (TM) including:
  - Guaranteed CIR
  - E2E flow control
  - 8 x CoS for differentiated services
- Any-slot-to-any-slot connectivity

## NPT-2400 Block Diagram



## NPT-2400 Control Subsystem

### Control System Block Diagram



The platform control and communication main functions include:

- Internal control and processing
- Network element (NE) software and configuration backup
- Communication with external equipment and management
- Built-in Test (BIT)

### Internal Control and Processing

The NPT-2400 controller provides central control, configuration, alarm, maintenance, and communication functions. The controller can also provide an NE management interface for management stations (EMS/LCT), support MCC, and channel management VLAN processing.

### Software and Configuration Backup

The platform features a large-capacity 128GB SSD that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

## Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

## NPT-2400 Communications with External Equipment and Management

In the Neptune metro access product line, the main controller unit is responsible for communicating with other NEs and management stations.

The main controller unit communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other NEs via the in-band MCC. Communication between other NEs, or between the NEs and the EMS/LCT, can also be via the out-of-band DCN. The controller can connect to the DCN via Ethernet.

### Usage Guidelines

The NPT-2400 supports in-band and DCN management connections for PB and MPLS:

- 20 Mbps shaper for MCC packet to MCP
- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-ISv6, static routes

The NPT-2400 also provides two SFP+ management ports (MNG and AUX MNG) connected directly to the CPU.

## NPT-2400 Timing

The NPT-2400 provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations, such as 1588v2 PTP according to the G.8273.2 standard, at the Class C/D support level.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed from the TMU to all base shelf ports and Tslot cards, minimizing unit types and reducing operation and maintenance costs. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- Internal PLL – ST-3E OCXO

- Bits (E1/T1) - T3/T4
- Built-in GNSS receiver
- 10MHz Coax (In/Out)
- 1PPS Coax (In/Out)
- ToD (RJ45)
- SyncE ITU-T G.8262.1 compliant
- IEEE 1588v2 G.8275.1 profile,
  - T-BC G.8273.2 Class C compliant.
- IEEE G.8275.2 profile (In V9.3)
  - 8273.4 compliant
- APTS support

**i Note:**

BITS (E1/T1) output and 10MHz output are not both available simultaneously; the user must select the frequency output interface type.

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

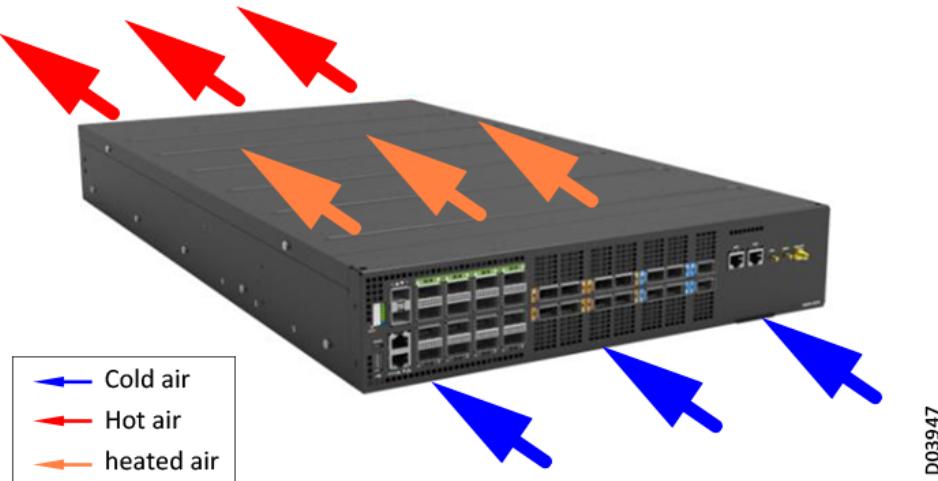
- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization over 10GbE/25GbE/100GbE/400GbE interfaces. Our implementation is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262.1, G.8263, and G.8264.

The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. PTP IEEE 1588v2 is supported in two profiles; full network timing support (G.8275.1 - Class C G.8273.2) and partial network timing support (future, G.8275.2 - Class A/B G.8273.4), providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <10ns (G.8273.2 Class C) timing error per NE. PTP is supported over 10GbE/25GbE/100GbE/400GbE interfaces.

## NPT-2400 Cooling Subsystem

NPT-2400 Air Flow

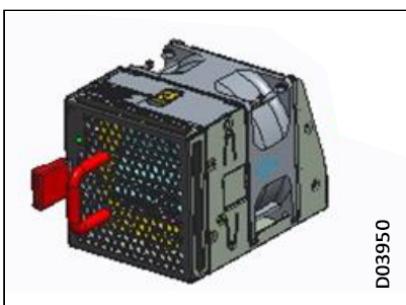


The cooling system is based on the FAN2400A pluggable fan control modules. Each NPT-2400 shelf must have four FAN2400A modules installed in the FCU slots in a 3+1 redundant arrangement. The fans' running speed can be set to speeds ranging from 0-25000RPM. The speed is controlled by the switching card according to the installed cards temperature.

**Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

FAN2400A Module



A LED light on the front panel indicates the status of the FAN2400A modules.

### FAN2400A Status LEDs

Color	Function
OFF	Power feed off or fan modules not present.
Solid Green	Fan modules all working well.
Blinking Yellow	One or more fan modules failed or no fan modules present.

## NPT-2400 Power Feed Subsystem

### Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. Alternatively, two AC power feeds can be used.

### Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-2400 supports the following types of power supply modes.

- -40 - -72 VDC power feed ([INF2400A](#)), configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- 100 - 240 VAC power source ([ACPS2400A](#)), utilizing an external power line connection through a power conversion module to implement AC/DC conversion.

The following flexible power supply configuration options are supported:

- Single DC 1+0
- Dual DC 1+1
- Single AC 1+0
- Dual AC 1+1

A LED light on the NPT-2400 front panel indicates the status of the platform power supply. A LED light on each INF2400A or ACPS2400A module indicates the status of that module.

### Platform Power Status LEDs

Color	Function
OFF	No power or in shutdown mode.
Solid Green	System power good.
Blinking Green	System power good but BMC power fail.
Solid Yellow	System power good but CPU power fail.
Blinking Yellow	System power fail.

## INF2400A Overview

The INF2400A is a DC power-filter module that can be plugged into the platform. Two INF2400A modules are needed for power feeding redundancy. It performs the following functions:

- DC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected
- High-power INF for up to 1600 W

### INF2400A Module



A LED light on the NPT-2400 front panel indicates the status of the platform power supply. A LED light on each INF2400A module indicates the status of that module.

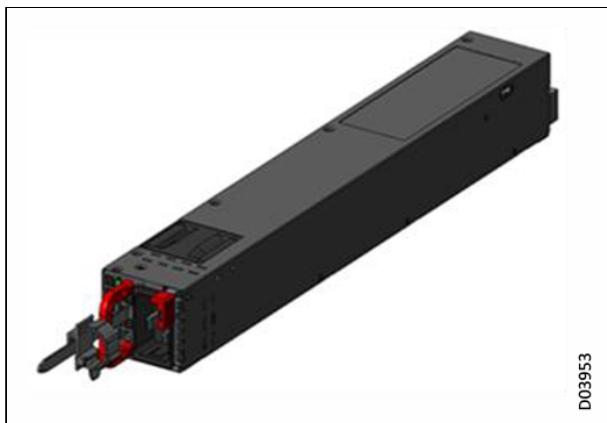
**INF2400A Status LEDs**

<b>Color</b>	<b>Function</b>
OFF	No power to all power modules.
Blinking Red	No power to this module.
Blinking Green	Power present, but only standby output on; poor contact.
Green	Module output on and working well.
Red	Module failure.
Blinking Alternately Red and Green	Warning: Working condition not satisfied. Check voltage, electric current, and temperature.

**ACPS2400A Overview**

The ACPS2400A is a 100-240 VAC power source utilizing an external power line connection through a power conversion module to implement AC/DC conversion. Two ACPS2400A modules must be installed for redundancy. The ACPS2400A performs the following functions:

- AC power input and power supply for all modules in the NPT-2400
- Input filtering function for the entire NPT-2400 platform
- Adjustable output voltage for fans in the NPT-2400
- High-power AC power supply for up to 1600W (65°C (149°F) max working temperature)

**ACPS2400A Module**

A LED light on each ACPS2400A module indicates the status of that module.

**ACPS2400A Status LEDs**

Color	Function
OFF	No power to all power modules.
Blinking Red	No power to this module.
Blinking Green	Power present, but only standby output on; poor contact.
Green	Module output on and working well.
Red	Module failure.
Blinking alternately Red and Green	Warning: Working condition not satisfied. Check voltage, electric current, and temperature.

# NPT-2300 System Architecture

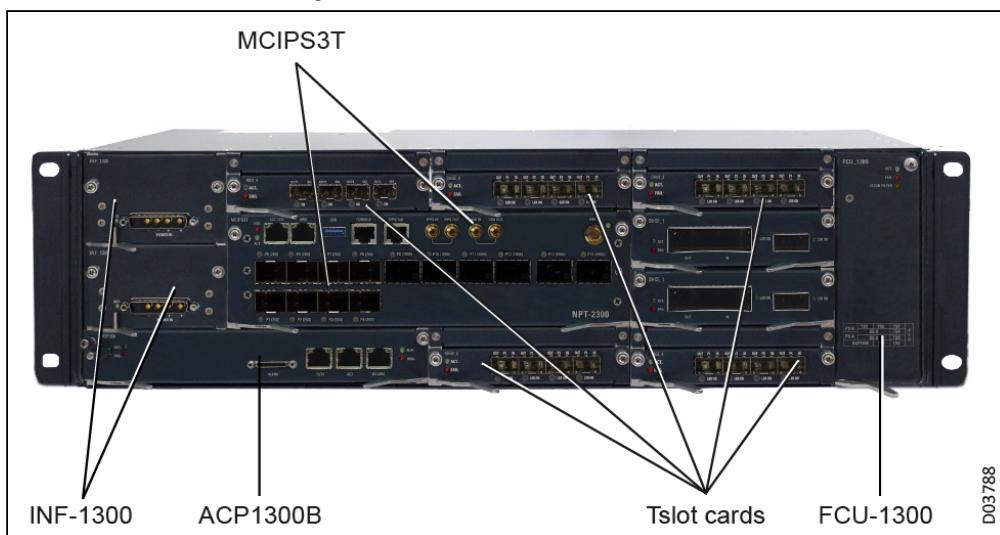
The NPT-2300 is a compact, modular, high-capacity, aggregation router designed to provide aggregation for services, applications, and architectures requiring a high-capacity, high performance multiservice solution. With support for IP/MPLS, MPLS-TP, SR-TE, and IPoDWDM, the NPT-2300 can use the right IP transport technology for each service it provisions. The NPT-2300's modular architecture and unique in-service extensions let you cost effectively scale to meet any service mix.

## NPT-2300 Front Panel



With an extensive set of interfaces for multiple access technologies such as Ethernet, MPLS, and legacy TDM, and redundancy of fans and input power, the NPT-2300 is a perfect fit for networks requiring high capacity, high availability, multiservice access edge and aggregation capabilities. With a full set of IP/MPLS, segment routing, and MPLS-TP transport capabilities, the NPT-2300 efficiently aggregates and routes services over the network, meeting service performance needs (SLAs) on a service by service basis. A full set of optical interfaces, including 400G ZR/ZR+ coherent optical pluggables, allows the NPT-2300 to support both single layer, hop-by-hop IPoDWDM, and multilayer IP and optical transport. Operators can choose which method best meets their needs, or they can run both in a hybrid approach.

## NPT-2300 Front Panel Layout



For a complete list of the modules that can be configured in each NPT-2300 slot, see [NPT-2300 Tslot IO Modules](#).

All cards support live insertion. All cards are connected using a backplane that supports one traffic connector to connect the NPT-2300 and the expansion platform. The NPT-2300 platform provides full 1+1 redundancy in power feeding as well as 1:N redundancy in the fans.

**Note**

Failure of the ACP1300B does not affect any existing traffic on the platform, but card management is affected.

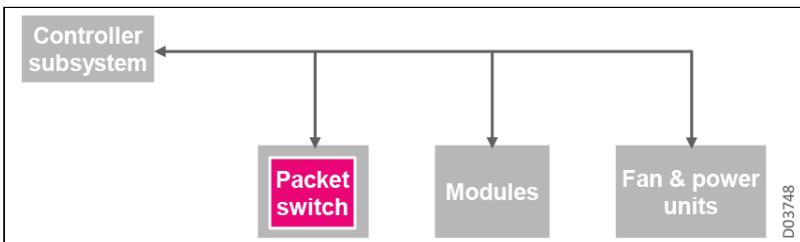
This section introduces the following NPT-2300 features:

- [NPT-2300 Control Subsystem](#)
- [NPT-2300 Communications with External Equipment and Management](#)
- [NPT-2300 Control and Communication Modules](#)
- [NPT-2300 Timing](#)
- [NPT-2300 Cooling Subsystem](#)
- [NPT-2300 Power Feed Subsystem](#)
- [NPT-2300 Switching Cards](#)
- [NPT-2300 Tslot IO Modules](#)
- [NPT-2300 Expansion Platforms](#)

## NPT-2300 Control Subsystem

The main controller is incorporated in the matrix card, from where it controls the entire system via a high-performance CPU, which also processes communication with the EMS/LCT and other equipment. A large capacity NVM stores equipment configuration data and up to two backup software versions. Both online and remote software upgrades are supported. The ACP1300 or ACP1300B card acts as an assistant controller module, since all control interfaces for INF, FCU, and I/O slots are physically connected to the ACP1300/B slot through the platform backplane.

### Controller Subsystem



NPT-2300 control and communication functions include:

- Internal control and processing
- Communication with external equipment and management
- Network element (NE) software and configuration backup
- Built-in Test (BIT)

### Software and Configuration Backup

The platform features a large-capacity on-board storage device that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

### Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

## NPT-2300 Communications with External Equipment and Management

In the Neptune product line, the main controller card is responsible for communicating with other NEs and management stations.

The main controller card communicates with the local EMS and LCT systems via the selected port; MNG, AUX, and LCT ports are all supported options. It communicates with the remote EMS/LCT systems and other PEs via in-band management, enabling NE management through in-band channels.

### Usage Guidelines

The NPT-2300 supports in-band and management communication on the following interfaces:

- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- In-band management processing

The following routing protocols are supported via DCN and in-band:

- IPv4: OSPFv2, IS-IS, static routes
- IPv6: OSPFv3, IS-IS v6, static routes

## NPT-2300 Control and Communication Modules

The ACP1300 and ACP1300B (ACP1300/B) assistant control and communication modules are the supporting processing card of the NPT-2300, integrating functions such as communications and other chassis management functions. ACP1300/B functionality includes:

- Assisting with intra-platform communication:
  - Communication with all modules in power supply slots, fan slot, backplane, Tslots, and Eslots in the NPT-2300 and expansion platform (EXT-2U/2UH), through the backplane (by the CPU)
  - Communication with the main NE controller on the active MCIPS card
  - NE alarm indicators and alarm in/out interfaces
- External timing reference interfaces (T3/T4), which provide the line interface unit for one 2 Mbps and one 2 MHz interface in SDH framing mode; if ACP1300B is used, then also provides one 1.544 Mbps and one 1.5 MHz interface in SONET framing mode

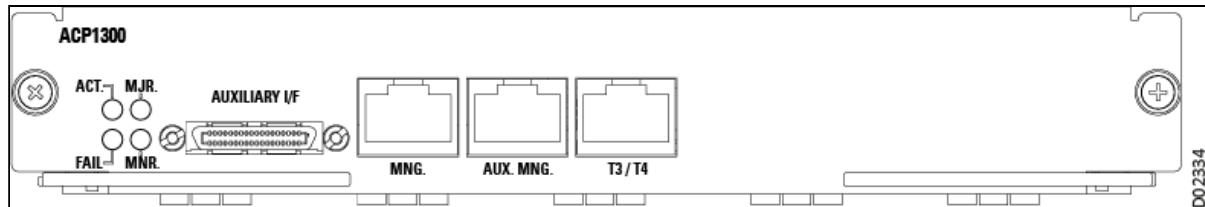
The ACP1300/B supports the following interfaces:

- T3/T4 directly from the front panel
- AUX MNG interface directly from the front panel (out of band DCN interface)
- RS-232, housekeeping and alarms through a concentrated SCSI auxiliary I/F connector on the front panel

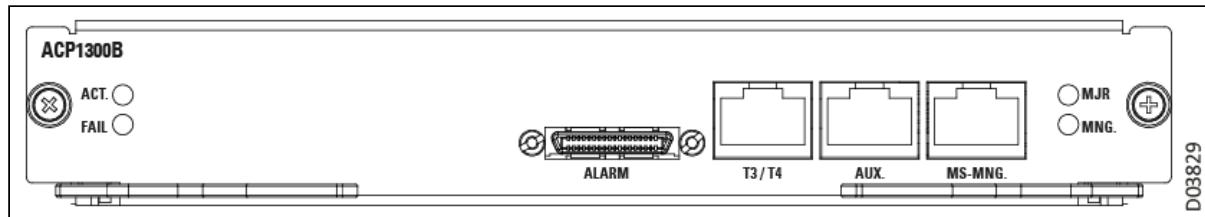
**Note**

Failure of the ACP1300/B does not affect any existing packet traffic on the platform.

Since the NPT-2300 is a front-access platform, all interfaces and LEDs on the ACP1300/B are located on the front panel of the module.

**ACP1300 Front Panel****ACP1300 Front Panel Interfaces**

Marking	Interface Type	Function
AUXILIARY I/F	SCSI-36	A concentrated auxiliary connector for the following interfaces: <ul style="list-style-type: none"> <li>1 x RS-232 interface for debugging or managing external ancillary equipment</li> <li>1 x alarm input and output interface connecting to the RAP</li> </ul>
T3/T4	RJ-45	T3 and T4 timing interfaces (1 x 2MHz/2Mbps)
MNG.	RJ-45	10/100BaseT Ethernet interface for debugging
AUX MNG.	RJ-45	Auxiliary 10/100BaseT Ethernet interface for OOB DCN interface

**ACP1300B Front Panel**

**ACP1300B Front Panel Interfaces**

<b>Marking</b>	<b>Interface Type</b>	<b>Function</b>
ALARM	SCSI-36	A concentrated auxiliary connector for the following interfaces: <ul style="list-style-type: none"> <li>• 1 x RS-232 interface for debugging or managing external ancillary equipment</li> <li>• 1 x alarm input and output interface connecting to the RAP</li> </ul>
T3/T4	RJ-45	T3 and T4 timing interfaces (1 x 2MHz/2Mbps or 1 x 1.5MHz/1.544Mbps)
MS-MNG.	RJ-45	10/100BaseT Ethernet interface for debugging
AUX	RJ-45	Auxiliary 10/100BaseT Ethernet interface for OOB DCN interface

**(i) Note**

An MCP30\_ICP can be used to distribute the concentrated auxiliary connector into dedicated connectors for each function; see the *Neptune Hybrid Reference Manual* for more information.

**ACP1300/B LED Indicators**

Marking	Full Name	Color	Function
- (left LED in MNG and AUX MNG. ports)	Link	Green	Lights when MNG link is on. Off when MNG link is off. Blinks when packets are received or transmitted.
- (right LED in MNG and AUX MNG. ports)	Speed	Orange	Lights when the MNG link is 100 Mbps. Off when the MNG link is 10 Mbps.
ACT.	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates card not running normally.
FAIL	Card fail	Red	Normally off. Lights when card failure detected.
MJR.	System major alarm	Red	Lights when the system has a critical or major alarm.
MNR.	System minor alarm	Yellow	Lights when the highest severity of the NE current alarms is minor or warning. Off when the system has no alarm or the highest severity of the NE current alarms is higher than minor or warning.

**Note**

ACT, FAIL, MJR, and MNR. LEDs are combined to show various failure reasons during the system boot. For details, see the Troubleshooting Using Component Indicators section in the *NPT-2300 Installation, Operation, and Maintenance Manual*.

## NPT-2300 Timing

This platform provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations for functionality and performance.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed from the TMUs to all traffic and matrix cards, minimizing unit types and reducing operation and maintenance costs. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- The system TMU (G.8262.1 eEEC) can support following timing sources:
  - External timing source - T3 (BITS input)
  - 2.048MHz and 2.048Mbit/s in SDH framing mode (ACP1300/B)

- 1.544MHz and 1.544 Mbit/s in SONET framing mode (ACP1300B only)
- 10MHz Interface (DIN1.0/2.3, 50 Ohm)
- E1/T1 interfaces of TDM cards (CES)
- STM-N/OC-n interfaces of TDM cards (CES/CEP)
- Synchronous Ethernet ports of DHxx cards and MCIPS3T card
- PTP clock (recovered clock from PTP)
- Internal timing (ST-3E OCXO)
- Holdover based on ST-3E OCXO
- APTS
- The PTP TMU (IEEE 1588v2 Clock) can support following timing sources.
  - As T-GM or T-BC with APTS
    - Built-in GNSS receiver
    - 1PPS/TOD interface (RS422, balanced)
    - 1PPS and 10MHz interface (DIN1.0/2.3, unbalanced)
    - System clock from T0 (EEC)
    - Holdover based on ST-3E OCXO
  - As T-BC
    - PTP port (any Ethernet port can be defined as PTP port) for both frequency and time/phase synchronization.
    - Sync-E as the frequency synchronization source (Hybrid mode)
    - Holdover based on ST-3E OCXO
- NTP support (NTPv1, NTPv2, NTPv3, and NTPv4)

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using either the Synchronization Status Marker (SSM) bytes in the overhead of the SDH/PDH TDM interface, or the SSM field in the Ethernet Synchronization Message Channel (ESMC) protocol per ITU-T G.8264. The TMU is frequency-locked to this source, providing internal system with the synchronized clock (T0). The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2MHz and 2Mbps. When working with the ACP1300B, 1.5M is also supported. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports enhanced SyncE synchronization, which is fully compatible with the asynchronous nature of traditional Ethernet. Enhanced SyncE is defined in ITU T standards G.8261, G.8262.1, G.8263, and G.8264.

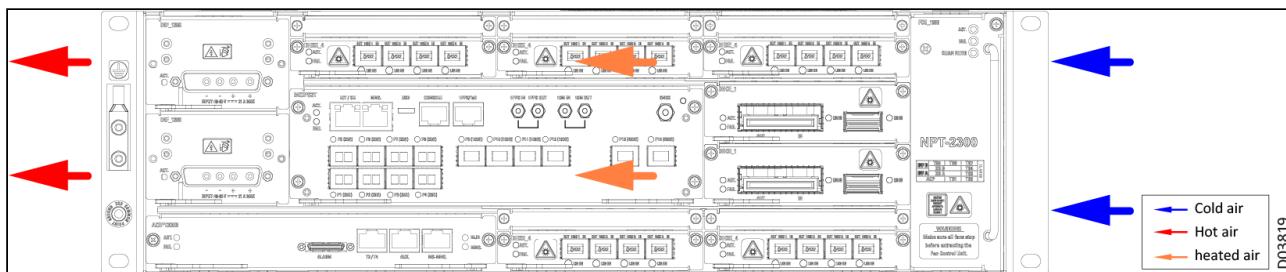
The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. PTP IEEE 1588v2 is supported in two profiles; full network timing support (G.8275.1) and partial network timing support (G.8275.2), providing T-GM and T-BC capabilities. It is possible to support high accuracy PTP mode and achieve <10ns (G.8273.2 Class C) timing error per NE.

## NPT-2300 Cooling Subsystem

The NPT-2300 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components, and cools them.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

## Airflow in the NPT-2300



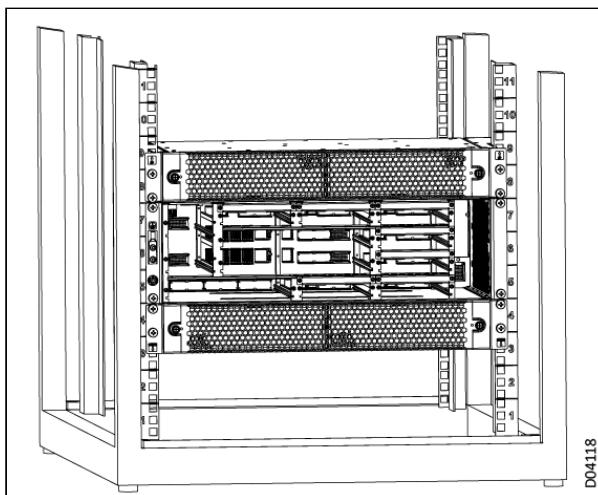
## Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The NPT-2300 platform can be configured together with air baffle units, installed in either a 19" or 23" rack.

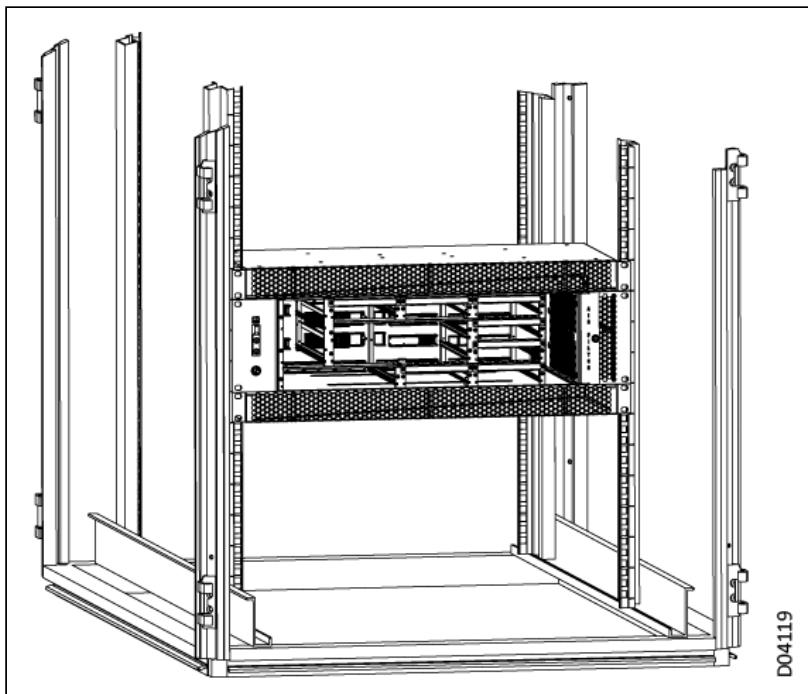
- In the 19" rack, the air baffle unit includes 2 1.5U air-flow boxes; one is located directly *below* the NPT-2300 platform, and one located directly *above* the NPT-2300 platform. The platform and two-part air baffle unit together occupy a total space of 6U height in the rack. The air baffle unit should be installed *before* the NPT-2300 platform; the NPT-2300 platform is then inserted into the gap space between the air-flow boxes. See the *NPT-2300 Installation and Maintenance Manual* for installation procedure details and limitations.

### 3U Height Platform Installed in 19" Rack Between Two Air-Flow Boxes



- In the 23" rack, the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* the NPT-2300 platform, and one located directly *above* the NPT-2300 platform. The platform and two-part air baffle unit together occupy a total space of 5U height in the rack. The air baffle unit should be installed *before* the NPT-2300 platform; the NPT-2300 platform is then inserted into the gap space between the air-flow boxes. See the *NPT-2300 Installation and Maintenance Manual* for installation procedure details and limitations.

### 3U Height Platform Installed in 23" Rack Between Two Air-Flow Boxes

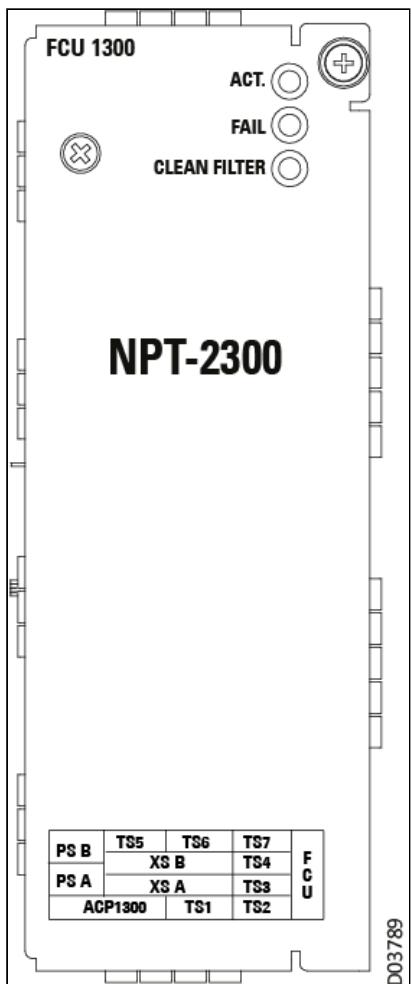


#### FCU Fan Control Module

The NPT-2300 platform is cooled through the FCU\_1300, a pluggable fan control module with six fans. The unit features enhanced PWM (Pulse Width Modulation), which helps optimizing the cooling efficiency and increases the fan operation life. The six fans in the FCU\_1300 are organized at the hardware level into two PWM groups. (The management software does, however, manage the FCU\_1300 as a single group.) By default, fan speed is controlled by SW according to the installed cards temperature, and "force turbo" is supported for maintenance purpose.

**Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

**FCU\_1300 Front Panel****FCU\_1300 Front Panel LEDs**

Marking	Full Name	Color	Function
ACT.	System active	Green	Normally on when the fan unit is powered on. Off indicates a power failure of the fan unit.
FAIL	System fail	Red	Normally off. Lights when a fan failure is detected.
CLEAN FILTER	Filter status indicator	Yellow	Normally off. Lights steadily when the air filter must be cleaned or replaced.

**NPT-2300 Power Feed Subsystem****Description**

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

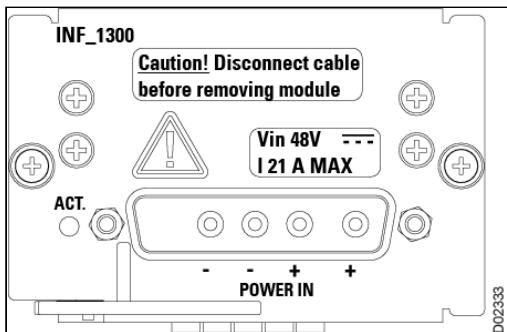
In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. AC power feeding requires the use of a conversion module to implement AC/DC conversion.

## Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-2300 supports two [INF\\_1300](#) power supply cards, supporting 1+1 and 1+0 configuration. The INF\_1300 card is used by both the NPT-1300 and NPT-2300 platforms.

### INF\_1300 Front Panel



## NPT-2300 Switching Cards

The NPT-2300 platform operates with the following matrix card:

- MCIPS3T: Single switching card that provides dual stack packet switching (L2, L3, MPLS-TP, and IP/MPLS). Most convenient for applications that require very high volume of pure packet handling including support for dynamic L2/L3 VPN services. The card also supports 8 x SFP28, 4 x QSFP28, and 2 x QSFP-DD based aggregation interfaces via corresponding ports.

The following sections detail card functionality.

- [MCIPS3T Switching Card](#)
- [MCIPS3T Functional Description](#)

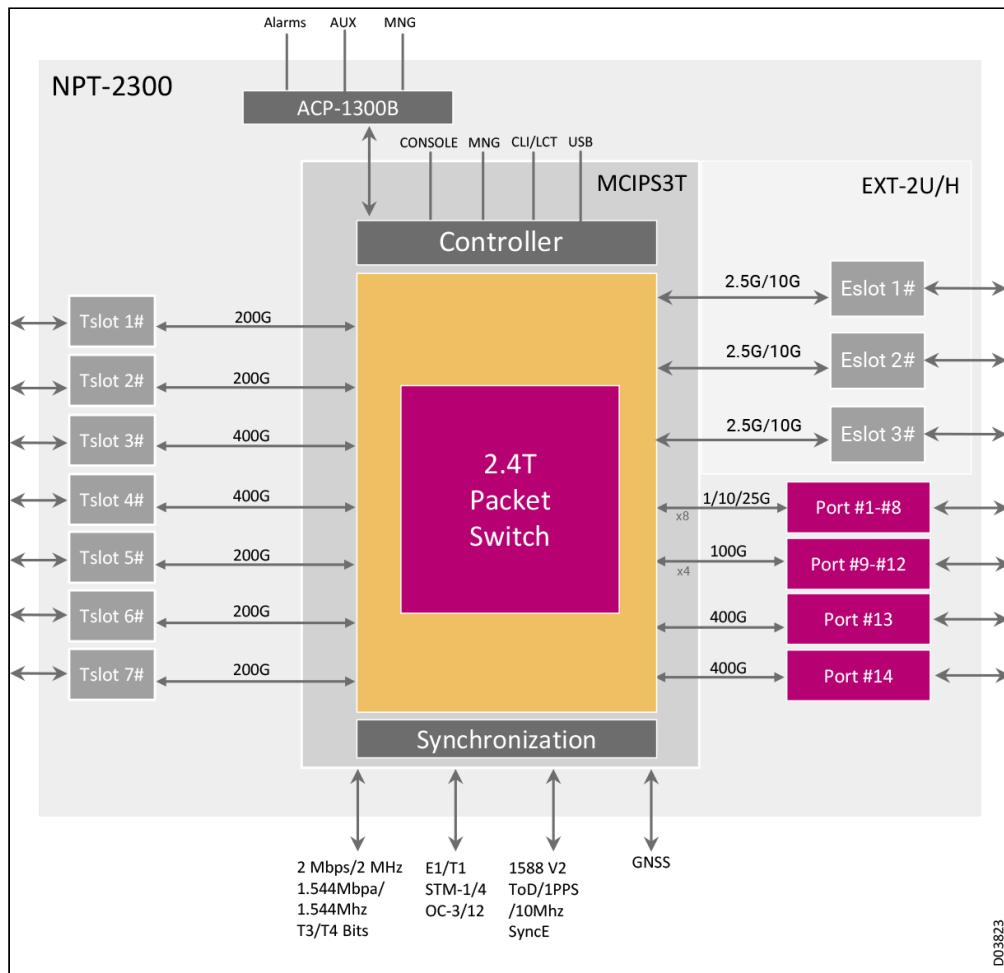
## MCIPS3T Switching Card

The MCIPS3T packet switching card is designed for use in the NPT-2300 metro core platform. The MCIPS3T is a centralized dual stack packet switch with MPLS-TP, IP/MPLS, L2VPN, and L3VPN capabilities, that provides 200G/400G switch capacity per slot (depending on the slot), supporting any-to-any direct data card connectivity. This card includes a main controller processor (MCP), 2.4T switching capacity and 3.23T fan-out, with EEC timing unit, IEEE 1588v2 timing unit, and a variety of aggregate ports (8 x SFP28, 4 x QSFP28, and 2 x QSFP56-DD).

The MCIPS3T module includes three main subsystems:

- **MCP (Main Control Processor)**: Performs all integrated functions like control, communication, and overhead processing with NVM.
- **CPS (Central Packet Switch)**: Performs all NPT-2300 packet switching operations.
- **TMU (Timing Unit)**: Generates and distributes timing and clock signals to all cards installed in the NPT-2300. In addition to its internal timing reference, the TMU can use up to four user-defined timing references.

### MCIPS3T Functional Block Diagram



The MCIPS3T offers a choice of capacity and configuration options, including:

- Ethernet packet switch, supporting native packet level switching with a 2.4T switching capacity and up to 3.23T traffic management (interface fan-out), providing:
  - Non-blocking data switch fabric for Ethernet/MPLS-TP, IP/MPLS, and SR traffic forwarding
  - Management and internal control in addition to user traffic switching
  - Both redundant and non-redundant modes
- Traffic management including:
  - Guaranteed CIR
  - 8 x CoS for differentiated services
  - E2E flow control
- Any slot to any slot connectivity
- On board interfaces:
  - 2 x 400G/100G

- 4 x 100G
- 8 x 25G/10G/1G
- Comprehensive range of timing and synchronization capabilities
  - G.781/G.8262 compliant EEC
  - GNSS, 1PPS ,ToD , 10MHz and Bits interfaces
  - IEEE 1588v2 PTP with OC (primary & secondary), T-GM, T-BC BC, one-step and two-step, and G.8275.1/2 profiles
  - G8273.2 Class C
- High capacity backplane connectivity for 100/200/400GbE interfaces, with up to 5 x 200G and 2 x 400G in a single platform
- IPoDWDM support with 100G/200G/400G coherent OpenZR+ interfaces
- Main control processing unit and built-in NVM
- Supports local management via CLI
- L3 VPN and IP/MPLS features:
  - VRF support:
    - ACL + L3 classification
    - uRPF
    - Multi-VRF networking stack
  - BGP (iBGP & eBGP):
    - AF ipv4
    - AF vpng4
    - Graceful restart
    - BFD support
  - L3VPN extension over static PW (PW-HE)
  - PE-CE protocols:
    - Static
    - eBGP
    - OSPF
  - VRRP
  - IP multicast:
    - IPV4 multicast with PIM and IGMP
  - DHCP:
    - DHCP Relay (to connect hosts to DHCP server via L3 VPN)
    - Multi hop IP-BFD
- NETCONF interface
- Continuous and periodic PM counters
- Syslog report generation support
- Built-in Y.1564 Service Activation Test and loop back with MAC swap

**i Optional Features:**

- MCIPS3T matrix is available in two variants: default switching capacity (1T) and full switching capacity (3T); it is possible to unlock the default capacity limit to utilize full capacity with a software license.
- MCIPS3T is available in two scale variants: default scale and high scale (for ACL rules and FIB routing numbers). Enabling high scale capability is controlled by a license. Users can run services with default scale enabled in the beginning, and purchase a license to enable high scale at a later time, even after services have been provisioned, to scale up the NE performance.

## MCIPS3T Functional Description

### MCIPS3T Front Panel



**MCIPS3T Front Panel Interfaces**

Marking	Interface Type	Function
1PPS IN	DIN 1.0/2.3	1PPS input interface for phase synchronization
10M IN	DIN 1.0/2.3	10MHz Clock Input interface for frequency synchronization
1PPS OUT	DIN 1.0/2.3	1PPS output interface
10M OUT	DIN 1.0/2.3	10MHz Clock Output interface
MNG	RJ-45 connector	1000BaseT Ethernet interface for out-of-band management
ToD	RJ-45 connector	Time synchronization interface (per ITU-T G.703 Section 19.1) Balanced 1PPS and TOD interface (per ITU-T V.11)
GNSS	SMA	The antenna interface of GNSS receiver
USB	USB Type A	USB 2.0 interface, for SW installation
LCT/CLI	RJ-45 connector	10/100/1000Base-T Ethernet interface Local management interface for connecting to an LCT or CLI
CONSOLE	RJ-45 connector	Serial RS-232 communication port for use by technical support personnel (debug, maintenance, etc.).
P1 to P8	SFP+/SFP28	1G/10G/25G ports
P9 to P12	QSFP28	100GbE
P13 to P14	QSFP-DD	400GbE

### MCIPS3T Indicators and Functions

Marking	Full Name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the CIPS1T not downloaded successfully or that the CIPS1T cannot be controlled normally by the MCP1800. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the CIPS1T card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STB.	System standby	Orange	Lights when the card is in standby. Off when the card is active.
GNSS		Green	Off indicates GNSS is not configured. Blinking indicates GNSS is in a learning state; self-survey is not completed. On steadily indicates GNSS is in a normal state; self-survey is completed.

## NPT-2300 Tslot IO Modules

The NPT-2300 has seven Tslots for installing I/O modules. The following table lists the different types of CES and Ethernet I/O modules that can be installed in the NPT-2300, with links to each module listed.

### Note

No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by the NPT-2300.

As of release V9.0.2, which includes fan-out capabilities, the maximum number of supported ports are as follows:

- 4 x 400GE
- 30 x 100GE
- 80 x 25GE
- 80 x 10GE
- 148 x 1GE (178GE with EXT-2UH)

Previous Neptune versions supported the following port maximums:

- 4 x 400GE
- 20 x 100GE
- 64 x 25GE
- 64 x 10GE
- 148 x 1GE (178GE with EXT-2UH)

**NPT-2300 Supported Tslot Modules**

Description	Card	Tslots
CES multiservice module with 32 x E1/T1 interfaces	MSE1_32	TS1-TS2, TS5-TS7
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	MSC_2_8	TS1-TS2, TS5-TS7
CES multiservice module with 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	MS1_4	TS1-TS2, TS5-TS7
CES multiservice module with 3 x DS3 interfaces and 1 x STM-1/OC3 interface	MS345_3	TS1-TS2, TS5-TS7
CES multiservice module with 24 x DS3 interfaces	MS345_24	TS1-TS7
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	DHGE_4EB	TS1-TS2, TS5-TS7
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	DHGE_8S	TS1-TS2, TS5-TS7
Optical 10 x GE module with direct connection to the packet switch	DHGE_10	TS1-TS7
Optical 20 x GbE interface module with direct connection to the packet switch	DHGE_20	TS1-TS7
Optical 4 x 10GE interface module with direct connection to the packet switch	DHXE_4	TS1-TS7
Optical 4 x 10GE/OTU-2 interface module with direct connection to the packet switch with OTN wrapping	DHXE_4O	TS1-TS7
40G MACsec card with: <ul style="list-style-type: none"> <li>• 2 x 10G/OTU-2e (SFP+) ports</li> <li>• 2 x 10G/1GE multi-rate ports</li> </ul> All 4 ports support MACsec capability.	DHXE_4sec	TS1-TS7

Description	Card	Tslots
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces  All 4 ports support MACsec capability.	DHXE_4MRsec	TS1-TS7
Optical 8 x 10GE interface module with direct connection to the packet switch	DHXE_8	TS1-TS7
Optical 100GE combo CFP2 or QSFP28 interface module with direct connection to the packet switch	DHCE_1	TS1-TS7
Optical 100GE QSFP28 interface module with direct connection to the packet switch	DHCE_1Q	TS1-TS7
Optical 100GE QSFP28/QSFP_DD interface module with direct connection to the packet switch	DHCE_1QB/1QC	TS1-TS7
Optical 2 x 100GE interface module (one QSFP28 port and one CFP2 port) with direct connection to the packet switch	DHCE_2	TS1-TS7
Optical 2 x 100/200GE QSFP_DD interface module with direct connection to the packet switch	DHCE_2Q	TS1-TS7
Ethernet I/O card for T-slot with one 400GE port (based on QSFP-DD)	DH400_1Q	TS3-TS4
Ethernet I/O card for T-slot with four 25GE/10GE ports (based on SFP28), rate is configurable between 25GBase-R and 10GBase-R on per card basis. Sync-E supported.	DH25_4MR	TS1-TS7
Ethernet I/O card for T-slot with eight 25GE/10GE/GE ports (based on SFP28), rate is configurable between 25GBase-R, 10GBase-R, and 1000Base-X on per port basis	DH25_8MR	TS1-TS7

## NPT-2300 Expansion Platforms

The traffic capabilities of the Neptune platform can be expanded by installing an expansion unit on top (EXT-2U or EXT-2UH, or eEXT-2UH when base platform is configured with ACP1300B). These are high density modular expansion units for the Neptune multiservice platforms. They support the complete range of CES, PCM, optics and Ethernet services. Integrating these add-on platforms into your network configuration is not traffic-affecting.

These are compact, versatile units that can be used with different base platforms from the Neptune product line. The type of traffic delivered by the unit depends on the type of matrix (PCM or Packet only) installed in the base unit. I/O expansion cards are supported in accordance. The expansion platforms have three

multipurpose slots (ES1 to ES3) for any combination of extractable traffic cards. PCM, Ethernet, OTN muxponders, optical amplifiers, and CES traffic are all handled through cards in these traffic slots.

The following table lists the traffic cards supported in the EXT-2U/2UH/eEXT-2UH units when installed with the platform. For a detailed description of the expansion platform features, functionality, and supported traffic cards, see [EXT-2U and EXT-2UH Expansion Units](#) or [eEXT-2UH Expansion Unit](#).

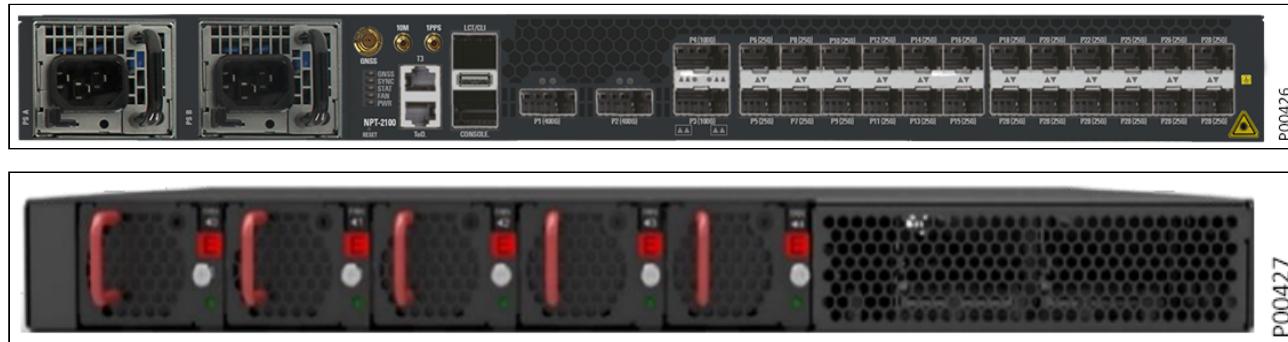
#### **EXT-2U/2UH Supported Cards for NPT-2300**

Card Type	Designation
Multiservice PCM and 1/0 XC card over Ethernet	<a href="#">EM_10E / EM_10EB</a> <ul style="list-style-type: none"> <li>• EM_10EB required for EXT-2UH or eEXT-2UH</li> <li>• Any revision works for EXT-2U</li> </ul>
Optical Base Card (OBC) for optical amplifiers and DCM modules	<a href="#">Optical Base Card</a> <ul style="list-style-type: none"> <li>• OBC with EXT-2U</li> <li>• OBC_B/OBC_C with EXT-2U, EXT-2UH, or eEXT-2UH</li> </ul>
10G card with up to 10 GbE ports; 4 of the ports support POE++	<a href="#">DHGE_10_POE</a> with EXT-2UH or eEXT-2UH
CES multiservice card with 2 x STM-1/OC-3 and 16 x E1/T1 interfaces	<a href="#">MSC_2_16E</a>

# NPT-2100 System Architecture

The NPT-2100 is an access router designed for next generation services and applications. The NPT-2100 is optimized for the access edge, with support for multiple access technologies. It is temperature hardened, with high throughput and a small form factor, and is suitable for both outdoor and indoor deployment.

## NPT-2100 Front and Back Panels



The NPT-2100 supports a full set of optical interfaces, including 400G ZR/ZR+ coherent optical pluggables. This allows the NPT-2100 to support both single layer, hop-by-hop IPoDWDM and multilayer IP and optical transport. Operators can choose which method best meets their needs, or they can run both in a hybrid approach.

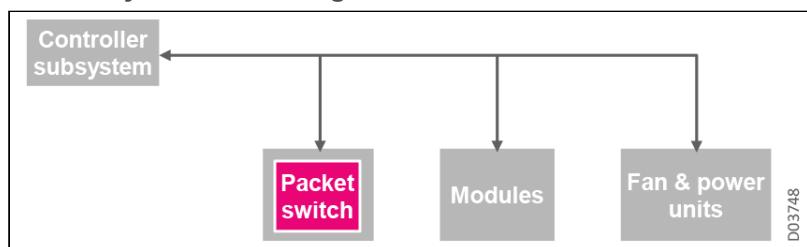
The Open Network Install Environment (ONIE) defines an open “install environment” for modern networking hardware. ONIE enables an open networking hardware ecosystem where end users have a choice among different network operating systems. The NPT-2100 is fully compliant with the standard ONIE installation environment, providing a compelling, open, disaggregated solution that meets the needs of converged multi-access edge and aggregation networks.

This section introduces the following NPT-2100 features:

- NPT-2100 Control Subsystem
- NPT-2100 Communications with External Equipment and Management
- NPT-2100 Timing
- NPT-2100 Cooling Subsystem
- NPT-2100 Power Feed Subsystem
- NPT-2100 Switching Functionality

## NPT-2100 Control Subsystem

### Control System Block Diagram



The platform control and communication main functions include:

- Internal control and processing
- Network element (NE) software and configuration backup
- Communication with external equipment and management
- Built-in Test (BIT)

## Internal Control and Processing

The NPT-2100 controller provides central control, configuration, alarm, maintenance, and communication functions. The controller can also provide an NE management interface for management stations (EMS/LCT), support MCC, and channel management VLAN processing.

## Software and Configuration Backup

The platform features a large-capacity 128GB SSD that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

## Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

# NPT-2100 Communications with External Equipment and Management

In the Neptune metro access product line, the main controller unit is responsible for communicating with other NEs and management stations.

The main controller unit communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other NEs via the in-band MCC. Communication between other NEs, or between the NEs and the EMS/LCT, can also be via the out-of-band DCN. The controller can connect to the DCN via Ethernet.

## Usage Guidelines

The NPT-2100 supports in-band and DCN management connections for PB and MPLS:

- 20 Mbps shaper for MCC packet to MCP
- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-ISv6, static routes

## NPT-2100 Timing

The NPT-2100 provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations, such as 1588v2 PTP according to the G.8273.2 standard, at the Class C/D support level.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed from the TMU to all base shelf ports and Tslot cards, minimizing unit types and reducing operation and maintenance costs. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- BITS (T3) input port
- GNSS input port
- 1PPS input/output port
- 10MHz input/output port
- ToD input port
- SyncE
- 1588v2 - Primary, Secondary, transparent, and boundary clock
- IEEE 1588v2 G.8275.1, G.8275.2 , G.8273.2 Class C
- APTS

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

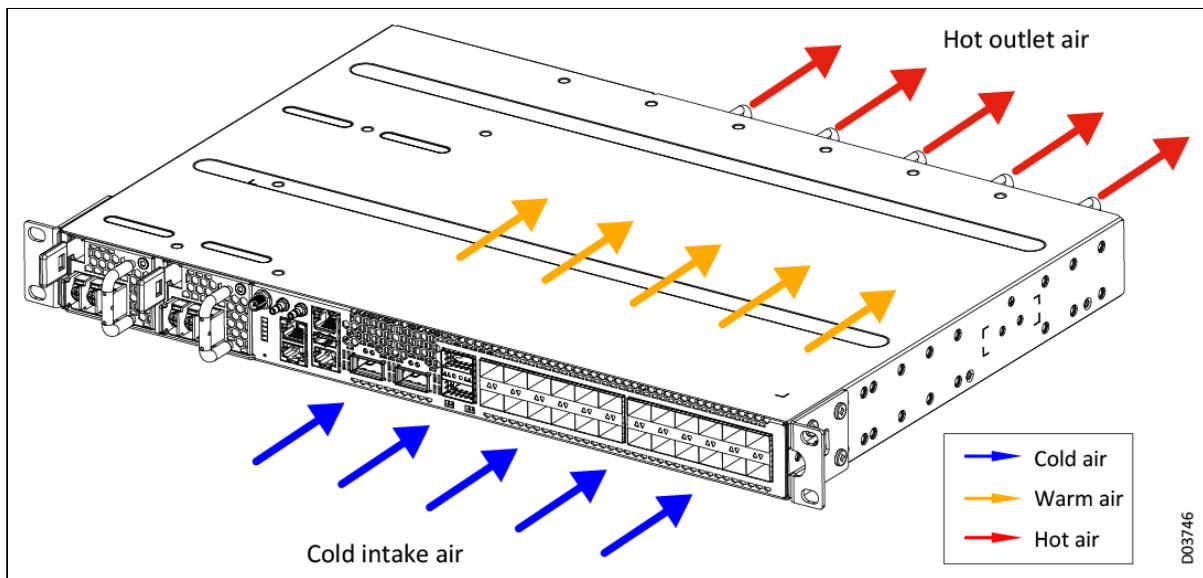
- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization over GbE/10GbE/100GbE interfaces. Our implementation is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262.1, G.8263, and G.8264.

The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. PTP IEEE 1588v2 is supported in two profiles; full network timing support (G.8275.1) and partial network timing support (G.8275.2), providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <10ns (G.8273.2 Class C) timing error per NE. PTP is supported over GbE/10GbE/100GbE interfaces.

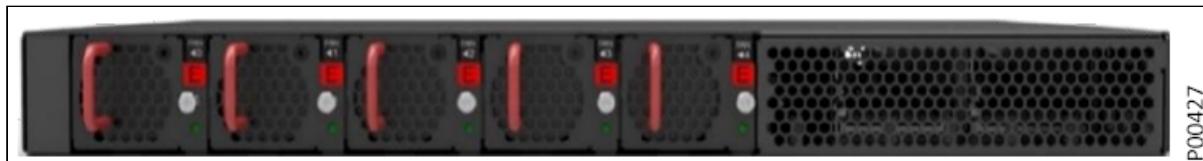
## NPT-2100 Cooling Subsystem

### NPT-2100 Air Flow



The cooling system is based on the FAN2100A pluggable fan control modules. Each NPT-2100 shelf must have five FAN2100A modules installed in the FCU slots, as illustrated in the following view of the platform's back panel.

### Back Panel

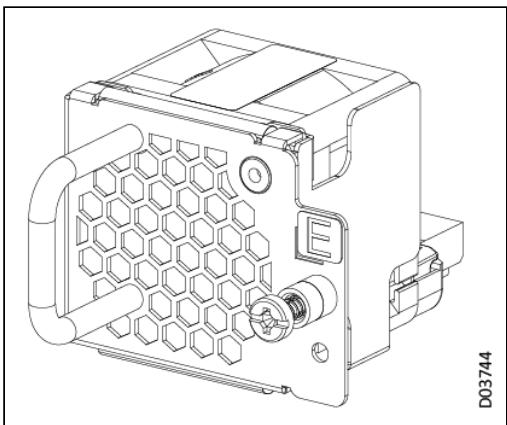


The fans' running speed can be set to speeds ranging from 0-25000RPM. The speed is controlled by the switching card according to the installed cards temperature.

**Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

## FAN2100A Front Panel



A LED light on the front panel indicates the status of the FAN2100A modules.

## FAN2100A Status LEDs

Color	Function
OFF	Power feed off or fan modules not present.
Solid Green	Fan modules all working well.
Blinking Yellow	One or more fan modules failed or no fan modules present.

# NPT-2100 Power Feed Subsystem

## Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. Alternatively, two AC power feeds can be used.

## Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-2100 supports the following types of power supply modes.

- -48 VDC power feed ([INF2100A](#)), configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.

- 100-240 VAC power source ([ACPS2100A](#)), utilizing an external power line connection through a power conversion module to implement AC/DC conversion.

The following flexible power supply configuration options are supported:

- Single DC 1+0
- Dual DC 1+1
- Single AC 1+0
- Dual AC 1+1

A LED light on the NPT-2100 front panel indicates the status of the platform power supply. A LED light on each INF2100A or ACPS2100A module indicates the status of that module.

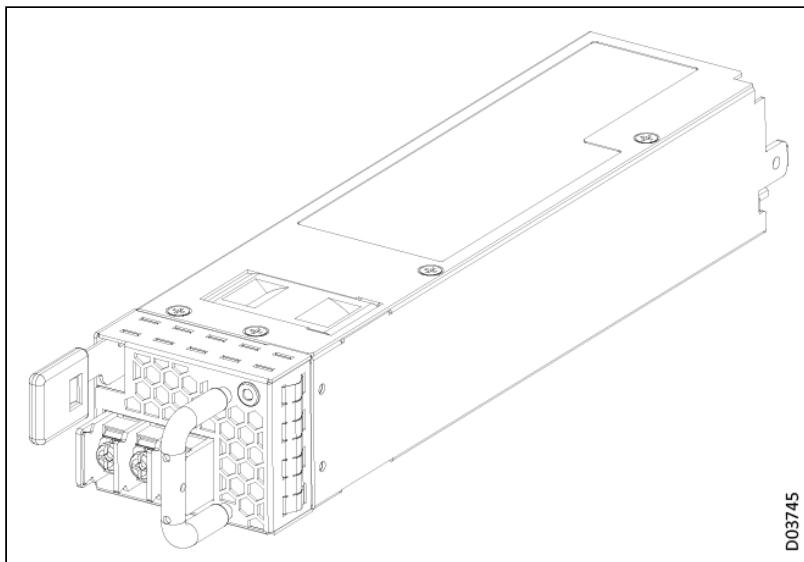
### Platform Power Status LEDs

Color	Function
OFF	No power or in shutdown mode.
Solid Green	System power good.
Blinking Green	System power good but BMC power fail.
Solid Yellow	System power good but CPU power fail.
Blinking Yellow	System power fail.

## INF2100A Overview

The INF2100A is a DC power-filter module that can be plugged into the platform. Two INF2100A modules are needed for power feeding redundancy. It performs the following functions:

- DC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected
- High-power INF for up to 400 W

**INF2100A Module****INF2100A Status LEDs**

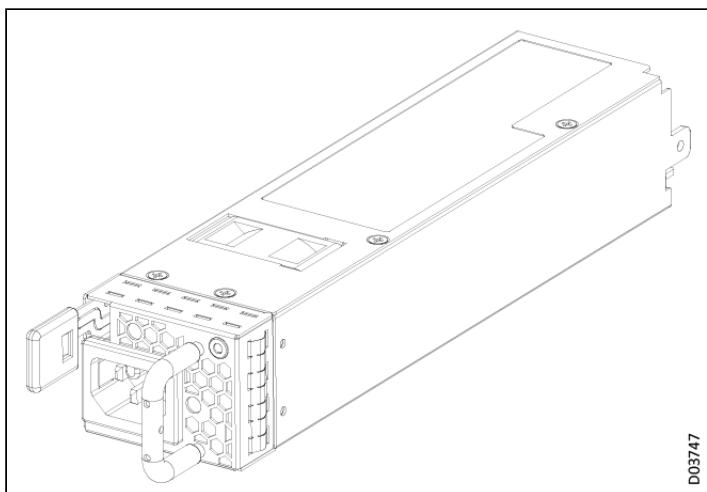
Color	Function
OFF	No power to all power modules.
Blinking Red	No power to this module.
Blinking Green	Power present, but only standby output on; poor contact.
Green	Module output on and working well.
Red	Module failure.
Blinking Alternately Red and Green	Warning: Working condition not satisfied. Check voltage, electric current, and temperature.

**ACPS2100A Overview**

The ACPS2100A is a 100-240 VAC power source utilizing an external power line connection through a power conversion module to implement AC/DC conversion. Two ACPS2100A modules must be installed for redundancy. The ACPS2100A performs the following functions:

- AC power input and power supply for all modules in the NPT-2100
- Input filtering function for the entire NPT-2100 platform
- Adjustable output voltage for fans in the NPT-2100
- High-power AC power supply for up to 400W (65°C (149°F) max working temperature)

### ACPS2100A Module



A LED light on each ACPS2100A module indicates the status of that module.

### ACPS2100A Status LEDs

Color	Function
OFF	No power to all power modules.
Blinking Red	No power to this module.
Blinking Green	Power present, but only standby output on; poor contact.
Green	Module output on and working well.
Red	Module failure.
Blinking alternately Red and Green	Warning: Working condition not satisfied. Check voltage, electric current, and temperature.

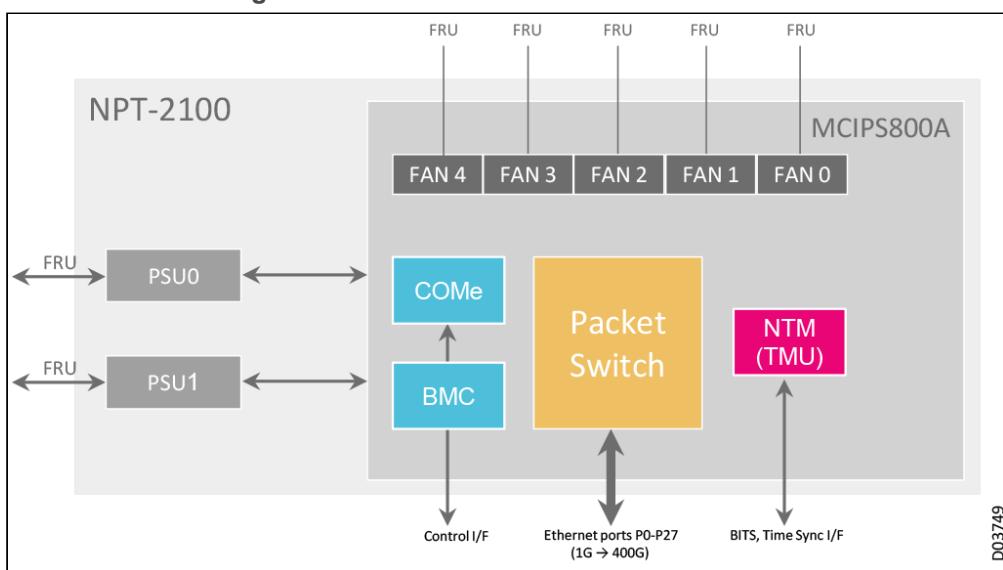
## NPT-2100 Switching Functionality

The NPT-2100's built-in switch provides the following main functions:

- All Native Ethernet packet switch, supporting native packet-level switching with 1.6T switching capacity (port fan-out) and up to 800G traffic management (packet processing), providing:
  - Management and internal control
  - User traffic switching
  - Non-blocking data switch fabric up to 800G (IMIX)
- OTSOP16 Smart SFP supported in SFP+ 10GE ports
- 5G-ready packet transport, including:
  - Stringent phase synchronization requirement for Class C/D timing accuracy compliance (8273.2)
    - 1G, 10G, 25G, 100G, and 400G interfaces
- Comprehensive range of timing and synchronization capabilities (G.781/G.8262 compliant EEC, G.8273.2):

- GNSS receiver
- 1PPS and ToD interfaces
- 10MHz (In/Out)
- BITS (T3)
- SyncE
- APTS
- IEEE 1588v2 PTP with:
  - OC (primary & secondary), BC
  - One-step TC
  - G.8275.1, G.8275.2 profile
  - G8273.2 Class C/D timing accuracy compliance
- Traffic management (TM) including:
  - Guaranteed CIR
  - E2E flow control
  - 8 x CoS for differentiated services
- Any-slot-to-any-slot connectivity

### NPT-2100 Block Diagram



# NPT-1800 System Architecture

The NPT-1800 is a future-proof platform offering ultra-high capacity and fully redundant, converged multiservice IP transport, based on a unique architectural design. This platform is optimized for metro aggregation nodes, supporting the most advanced carrier class Ethernet-based services (L1, L2, MPLS-TP, L2VPN, L3VPN, IP/MPLS, and segment routing) as well as OTN and FlexE support. The NPT-1800 is well positioned to deliver cellular backhaul as well as supporting 3G, 4G, LTE, and 5G networks with enhanced synchronization and timing capabilities based on 1588v2, G.8265.1 (CIPS1T), G.8275.1, and G8273.2 Class C timing accuracy.

## NPT-1800 Front Panel



The NPT-1800 is a carrier-class IP transport dual-stack MPLS-TP/IP-MPLS and L3 routing platform that combines transport network reliability and ease of management with IP and OTN efficiency. As a metro core IP transport platform, the NPT-1800 architecture supports 2TB, and its integrated optics support allows seamless integration with next generation optical networks. NPT-1800 platforms offer the following features:

- 8U-size IP transport aggregation, optimized for cellular hub 3G, 4G, LTE, 5G, and RNC/MSC/SGW locations, as well as service provider hub and core sites
- Support of IP-based applications for optimized packet and CES handling (SAToP, CESoPSN, and CEP)
- High capacity platform, including:
  - High-capacity centralized IP switches (CIPS1T/CIPS2T) supporting 1T/2T IP traffic
  - 800G FlexE traffic switching
  - 23 x I/O slots, 40G/100G capacity per slot
  - 25GbE and 100GbE interfaces
  - IPoDWDM with coherent 100G interfaces
  - E1POP Smart SFP supported in 1000Base-T ports
  - OTSOP16 Smart SFP supported in SFP+\_10GE ports
  - Optional EXT-2U/eEXT-2UH expansion unit with additional 3 slots
- Comprehensive range of timing and synchronization capabilities, compliant with 5G MBH requirements:
  - T3/T4 BITS
  - SyncE
  - IEEE 1588v2 G.8265.1, G.8275.1, Class B (CIPS1T)
  - IEEE 1588v2 G.8275.1 (Class C), G.8275.2 (Class A) (CIPS2T)
  - 1PPS and ToD
  - Hybrid 1588 and SyncE

- APTS (CIPS2T)
- Dynamic BW allocation
- Very high redundancy due to double systems:
  - Two central switch cards with 1588v2 and BITs
  - Two control and IP engine cards
  - Two power supplies
  - Fans and control cards

The NPT-1800's centralized IP switch enables any-to-any data card connectivity, via the DH and FlexE cards. For a complete list of the modules that can be configured in each NPT-1800 slot, see [NPT-1800 Tslot IO modules](#).

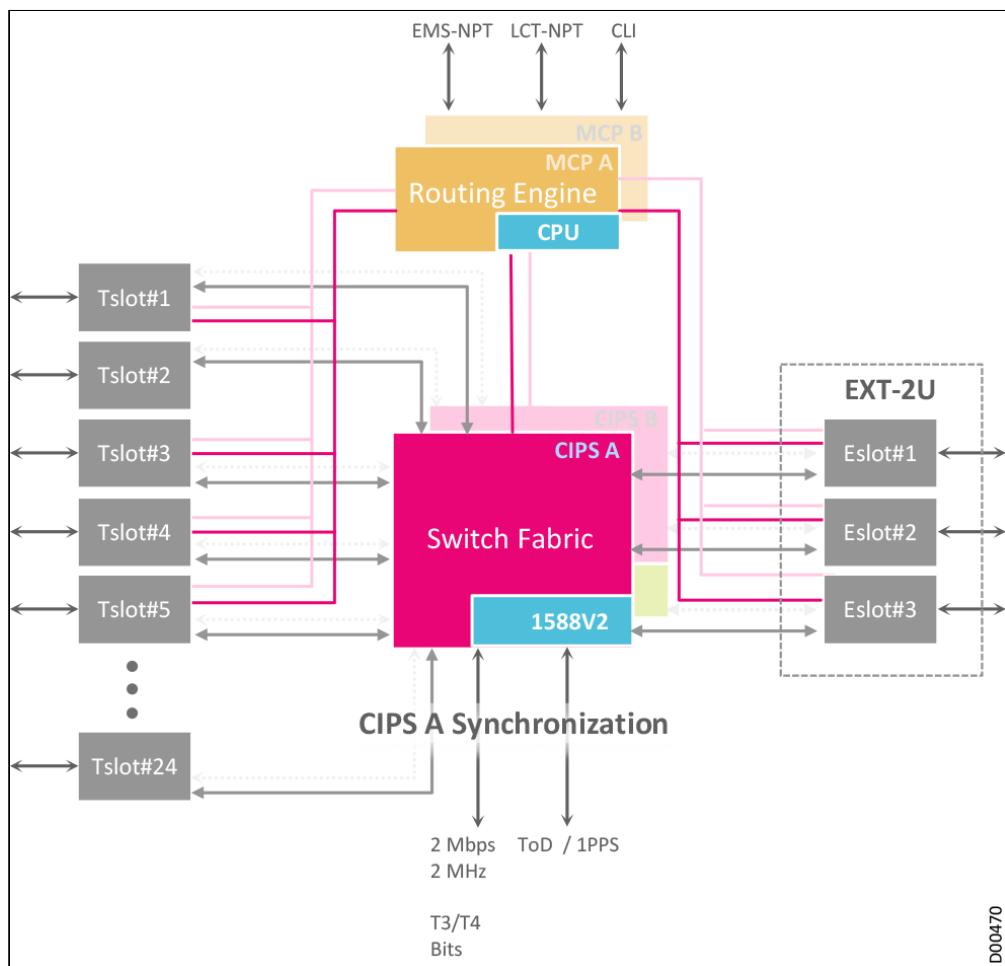
All cards support live insertion. All cards are connected using a backplane that supports one traffic connector to connect the NPT-1800 and the EXT-2U. The NPT-1800 platform provides full 1+1 redundancy in power feeding, IP switching, and the TMU, as well as 1:N redundancy in the fans.

This section introduces the following NPT-1800 features:

- [NPT-1800 Platform Architecture](#)
- [NPT-1800 Platform Design](#)
- [NPT-1800 Control Subsystem](#)
- [NPT-1800 Communications with External Equipment and Management](#)
- [NPT-1800 Controller Cards](#)
- [NPT-1800 Timing Overview](#)
- [NPT-1800 Cooling Subsystem](#)
- [NPT-1800 Power Feed and Alarm Subsystems](#)
- [NPT-1800 Switching Cards](#)
- [NPT-1800 Tslot IO Modules](#)
- [NPT-1800 Expansion Platforms](#)

# NPT-1800 Platform Architecture

## NPT-1800 Architecture



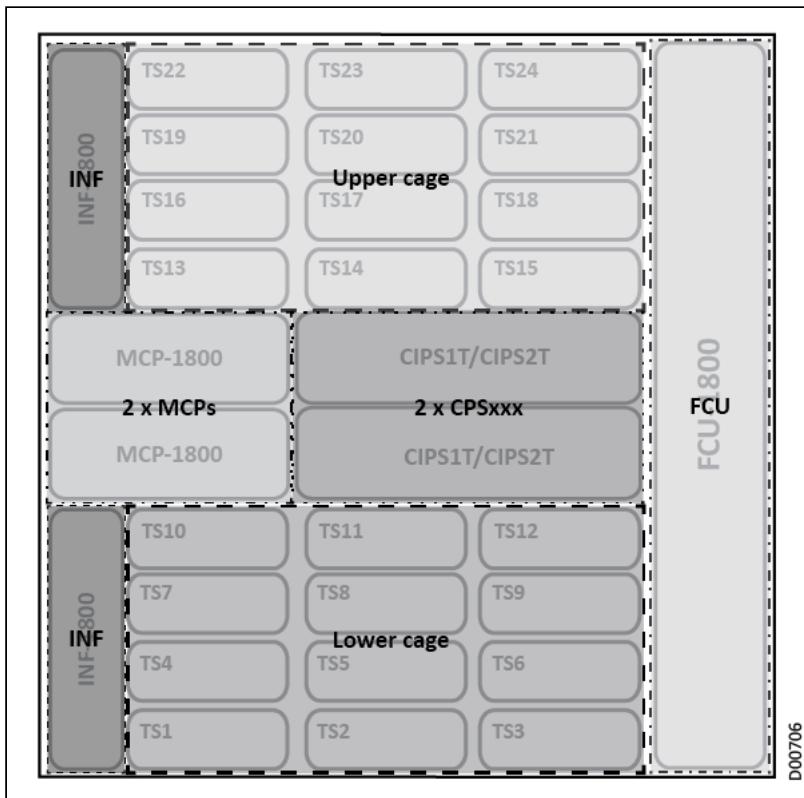
**Notes**

- For IP/MPLS control plane and L3VPN activation, the NPT-1800 must be configured with two MCP1800 cards.
- For PB & MPLS-TP, the NPT-1800 can be configured with one MCP1800 card.

## NPT-1800 Platform Design

NPT-1800 is a small footprint subrack that fits into ETSI, 19", and 23" racks. Its dimensions are 354 mm high, 440 mm wide and 243 mm deep (13.94 in. x 17.32 in. x 9.57 in.). Attaching the optional EXT-2U adds 88.9 mm (3.5 in.) to the height of the basic platform.

## NPT-1800 Cages



The NPT-1800 platform is arranged as follows:

- The right most slot of the platform accommodates the FCU\_1800.
- The middle part of the platform consists of the commons cards cage with four horizontal slots which accommodate:
  - Two CIPS1T/CIPS2T cards (main and protect) main switching cards
  - Two MCP1800 cards (main and protect) main routing engine and controller cards
- The left most slots of the platform house two INF\_1800 modules.
- Two Tslots cages supporting up to 23 I/O modules, organized as follows:
  - **Lower cage:** Tslots 1-12.  
When working with a CIPS1T card, the Tslots are subdivided into two groups:
    - Group I: Tslots 1-6
    - Group II: Tslots 7-12 (with spacer)
  - **Upper cage:** Tslots 13-24.  
When working with a CIPS1T card, the Tslots are subdivided into two groups:
    - Group II: Tslots 13-18 (with spacer)
    - Group I: Tslots 19-24 (excluding Tslot 22, reserved for ECB)

The following sections provide guidelines for card installation and port configuration, for more efficient utilization of NPT-1800 slots and maximum fan-out, including the following sections:

- [Group I Usage Guidelines: CIPS1T Only](#)
- [Group II Usage Guidelines: CIPS1T Only](#)
- [Card Configuration Guidelines and Example](#)
- [Maximum Cards per Platform](#)
- [Maximum Ports and Fan-Out per Platform](#)

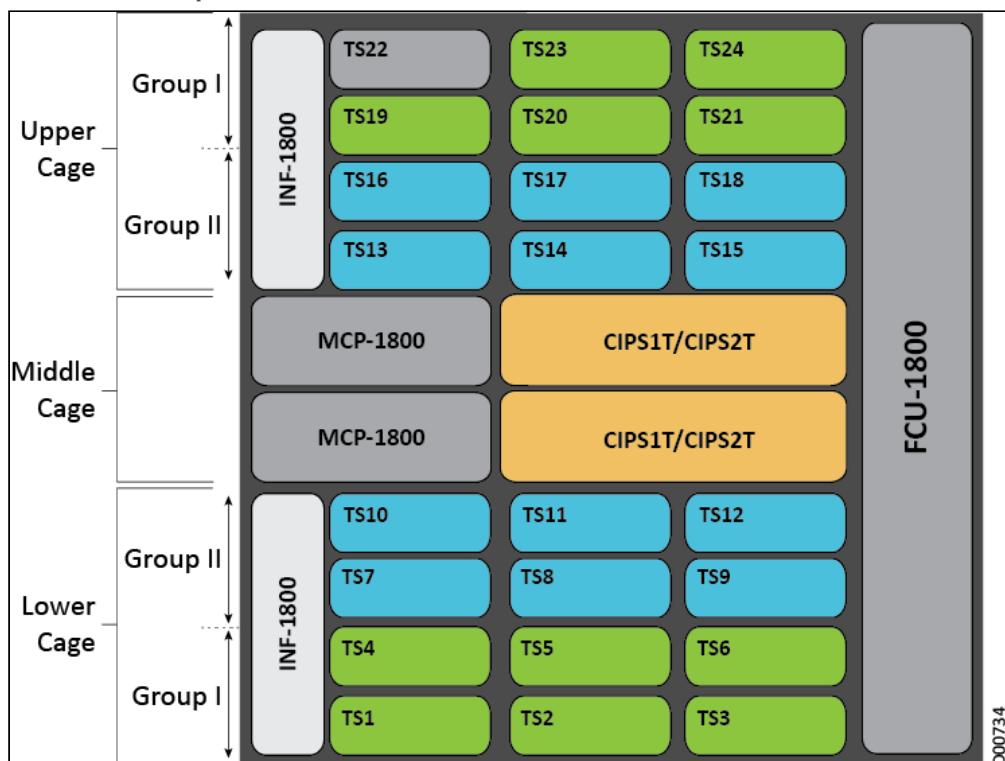
# Group I Usage Guidelines: CIPS1T Only

 **Notes:**

- The Group I/Group II slot organization is only relevant for configuration with the CIPS1T switching card.
  - From V7.6, when high accuracy PTP is enabled, Group I (in both cages) can support a total of 22 x 10GEs in any mixture of card types. If high accuracy PTP is disabled, Group I (in both cages) can support a total of 23 x 10GEs in any mixture of card types.

To maximize Tslot efficiency, throughput, and GE/CES fan-out when working with the CIPS1T card, the NPT-1800 supports dynamic bandwidth allocation in Group I (Tslots 1-6 and Tslots 19-24, excluding Tslot 22, for the ECB). Dynamic bandwidth allocation enables traffic allocation per GE port, per card, as needed, offering efficient utilization for CES cards and GE interfaces. This is generally used for CES and GE based cards (excluding the DHGE\_20 and 10GE cards).

## NPT-1800 Groups



## **Group I Installation Guidelines**

- To utilize the NPT-1800 with the CIPS1T and max. 100GE fan out:
    - For GE ports, use Group I first and then Group II
    - For 10GE ports, if no GE port is required in the NE:
      - a. Use Group I first
      - b. Then use slots TS7-TS9 and TS16-TS18 in Group II
      - c. Finally, use slots TS10-TS15.The reason for this order is simple. We recommend keeping the

The reason for this order is simple. We recommend keeping the higher capacity (100G) slots in reserve, available for use as needed, perhaps when growing capacity demands require migrating to the CIPS2T switch.

- For 10GE ports, if many GE port are to be configured in the NE, then the 10GE ports should use Group II first.

- For CES-based cards, use Group I first, and then (if needed) Group II.
- We recommend populating the Tslots with cards according to the following priority list:
  - a. DHGE\_24: Max. four per cage (two for upper Group I and two for lower Group I)
  - b. DHGE\_16: Max. four per cage (two for upper Group I and two for lower Group I)
  - c. DHGE\_10: Max. eleven per Group I (five for upper Group I and six for lower Group I)
  - d. DHGE\_8: Max. eleven per Group I (five for upper Group I and six for lower Group I)
  - e. DHGE\_4E: Max. eleven per Group I (five for upper Group I and six for lower Group I)
  - f. MSE1\_32: Max. eleven per Group I (five for upper Group I and six for lower Group I)
  - g. MS1\_4: Max. eleven per Group I (five for upper Group I and six for lower Group I)
  - h. MSC\_2\_8: Max. eleven per Group I (five for upper Group I and six for lower Group I)
  - i. DHXE\_4/40: Max. six per Group I
- Try to install the DHGE\_24 and DHGE\_16 cards in the right-side slots (near the FCU\_1800).
- In case of GE SFP-only based configuration, try to install the DHGE\_24 and DHGE\_16 cards first.

There are certain limitations to dynamic bandwidth allocation and mixed card configuration (DHXE\_4 and DHGE\_xx for example). To understand these limitations, the following table summarizes card assignment rules for the Group I slots. Following these rules allows you to achieve maximum fan-out utilization, making maximum use of the port count budget for 10GBE and 1GBE ports.

### Card Assignment Rules for Group I Slots

Card Name	Port Count (out of a total budget of 70/71 GBEs)	Port Count (out of a total budget of 22/23 10GBEs)	Comments
DHXE_4 / DHXE_4O / DHXE_4sec	14	4	
DHGE_24 (SFP/CSFP)	12/24	4/6	
DHGE_16 (SFP/CSFP)	12/16	4/4	
DHGE_10	4/6	1/2	The actual port count with the DHGE_10 can reach up to 110GbEs.
DHGE_8 (SFP/CSFP)	14/8	4/4	We recommend using these cards only after reaching 64 ports with SFP assignments.
DHGE_4E	2	2	
DHGE_4EB	14	4	We recommend using these cards only after reaching 64 ports with SFP assignments.
MSE1_32	4	1	
MSC_2_8 / MS1_4	6	2	

### Group I Utilization Examples

This section provides a few card/port configuration examples to clarify how the Group I usage guidelines would work in practice, in the field.

For example, assume you want to use the maximum of 71 ports (PTP disabled for this example) in the Group I slots, and you are working with DHGE\_24, DHGE\_16, DHGE\_8, and/or DHGE\_4E cards. You can configure 64 ports of these cards utilizing the GbE resources. The remaining 7 ports can be configured by utilizing the unused port budget from the 10GbE port allocation. The last assigned card (a single Tslot card with 4-port count budget taken from the 10GbE port budget) can be configured with a partial port assignment to complete the last 3-port fan-out.

Additional configuration examples include:

- Group I can support up to 110 GEs with the DHGE\_10 card.
- Group I can support up to 71 x GEs (high accuracy PTP disabled) with the following card combination:
  - 2 DHGE\_24 (48 ports CSFP based)
  - 2 x DHGE\_8 (16 ports CSFP based)

- 2 x DHGE\_8 (7 ports SFP based)
- Group I can support up to 70 x GEs (high accuracy PTP enabled), with the following card combination:
  - 2 DHGE\_24 (48 ports CSFP based)
  - 2 x DHGE\_8 (16 ports CSFP based)
  - 2 x DHGE\_8 (6 ports SFP based)

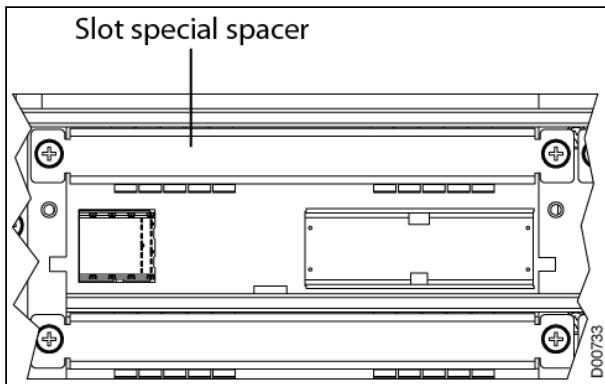
## Group II Usage Guidelines: CIPS1T Only

**Note**

The Group I/Group II slot organization is only relevant for configuration with the CIPS1T switching card.

The 100GE interface cards and high density DHGE\_20 cards require more space than regular Tslot cards. Therefore, the Group II slots (Tslots 7-12 and Tslots 13-18) are slightly larger, to accommodate these cards. Each Group II slot includes an easily-removed spacer, to enable installation of regular Tslot cards as well. You must remove this spacer to configure the slot for 100GE and DHGE\_20 card installation; see the *NPT-1800 Installation and Maintenance Manual* for more details.

### Tslot Spacer (remove for 100GE cards)



### Group II Installation Guidelines

- When working with the CIPS1T, up to 6 x 100GEs can be supported by Group II in Tslots 10-15. Therefore, we recommend populating these Tslots with cards according to the following priority list:
  - DHCE\_1/DHCE\_1C/DHCE\_1Q: Max. six per Group II only
  - DHGE\_20: Max. twelve per Group II only
  - DHXE\_4/4O/4sec: Max. twelve per Group II
  - DHGE\_8S: Up to 4 ports only (no CSFP support in Group II), Max. twelve per Group II
  - MS1\_4: Max. twelve per Group II
  - MSE1\_32: Max. twelve per Group II
  - MS345\_3: Max. twelve per Group II
  - MSC\_2\_8: Max. twelve per Group II
  - DHGE\_10: Max. twelve per Group II
- Up to 18 DHXE\_4/4O/4sec cards can be supported in any Tslot (Group I & Group II).
  - Max: 71 x 10GEs (one/last port will not be active/configured by the management)), for CIPS1T HW revisions preceding Rev G20.
  - Max: 70 x 10GEs (two ports will not be active/configured by the management)), for CIPS1T HW revisions from Rev G20 and above.
- When using multiple DHGE\_20 cards, they should be installed symmetrically between higher and lower slots of Group II.

- When using MSE1\_32 cards, they must be installed next to each other in the NPT-1800 platform to enable the necessary protection cabling.
- Group II does not support DHGE\_4E, DHGE\_24, and DHGE\_16 cards.
- The DHGE\_8 card in Group II supports up to 4 x GE ports only, assigned as DHGE\_8S.

## Card Configuration Guidelines and Example

NPT-1800 is positioned as a metro core platform. Therefore, the most efficient configuration is with a mixture of 100GE and 10GE cards, to optimize NPT-1800 utilization with the most efficient fan-out. For example:

### Card Configuration Guidelines and Example: NPT-1800

Card Configuration	CIPS1T matrix (high accuracy PTP disabled)	CIPS1T matrix (high accuracy PTP enabled)
6 x DHCE_1/DHCE_1C + 12 x DHXE_4/4O	6 x 100GE + 47 x 10GEs	6 x 100GE + 46 x 10GEs
4 x DHCE_1/DHCE_1C + 14 x DHXE_4/4O	4 x 100GE + 55 x 10GEs	4 x 100GE + 54 x 10GEs
2 x DHCE_1/DHCE_1C + 16 x DHXE_4/4O	2 x 100GE + 63 x 10GEs	2 x 100GE + 62 x 10GEs
2 x DHCE_1/DHCE_1C + 12 x DHXE_4/4O + 2 X DHGE_24 + 2 X DHGE_8	2 x 100GE + 47 x 10GE + 64 x GE	2 x 100GE + 46 x 10GE + 64 x GE

To understand these configuration options, consider the following example of how to implement the first configuration option listed.

To configure a combination of

$$6 \times \text{DHCE\_1/DHCE\_1C} + 12 \times \text{DHXE\_4/4O} = 6 \times 100\text{GE} + 47 \times 10\text{GEs}$$

- Place 6 x DHCE\_1/1C in Group II slots TS10 - TS15.
- Place the DHXE\_4/4O cards (24 x 10GE interfaces) in the remaining 6 slots in Group II.
- Port assignment depends on the matrix card revision:
  - For CIPS1T matrix cards (high accuracy PTP disabled), place the additional 6 x DHXE\_4/4O cards in the remaining 23 x 10GE interfaces. This is the maximum allowed for Group I.
  - For CIPS1T matrix cards (high accuracy PTP enabled), place the additional 6 x DHXE\_4/4O cards in 22 x 10GE interfaces. The total configured combination will be 6 x 100GE + 46 x 10GEs.

If a different mixture of interfaces is required, consider the following alternative:

- Each card in Group II can be replaced by a DHGE\_20/DHXE\_4/4O card, thereby increasing the 10GE/1GE fanout at the expense of the 100GE/10GE fan out.
- The 10GE interfaces in Group I can be replaced with GE interfaces (5 x DHXE\_4 to 10 x DHGE\_8).

Due to the dynamic BW assignment capability in Group I, replacing DHXE\_4 or DHGE\_8 (CSFP based) can free space for assigning two CES cards. Removing DHGE\_8 (SFP based) can free space for two MS1\_4, two MCS\_2\_8, or four MCSE1\_32 cards.

**i Notes**

- NPT-1800 max switching utilization with 100GE interface is 1.07T, as illustrated in example 1, when high PTP accuracy is *disabled*.
- NPT-1800 max switching utilization with 100GE interface is 1.06T, as illustrated in example 1, when high PTP accuracy is *enabled*.
- For NPT-1800 with 1T matrix:
  - Number of supported GBE ports is 197, with high accuracy PTP *enabled*.
  - Number of supported GBE ports is 198, with high accuracy PTP *disabled*.
- If DHGE\_8S cards are installed in slots TS5-TS9, TS11-TS18, TS20, or TS21 with the card configured for 100Base-X and/or 10/100/1000Base-T interfaces, CIPS2T can't be assigned.

## Maximum Cards per Platform

Cards per Platform

Card	Max. card Group I (CIPS1T)	Max. card Group II (CIPS1T)	Max. cards per platform (CIPS1T)	Max cards per platform (CIPS2T)	Interface Type	Comments
DHGE_4E	11	---	11	---	4 x 100/1000BaseT	
DHGE_4EB	11	12	23	23	4 x 100/1000BaseT	<ul style="list-style-type: none"> <li>Supports 1 GbE rates only when installed in Tslots TS10-TS15 in NPT-1800 with CIPS1T.</li> <li>Supports 1 GbE rates when installed in all Tslots with CIPS2T.</li> </ul>
DHGE_8	11	--	11	---	8 x 100/1000BaseX (CSFP)	
DHGE_8S	11	12	23	23	8 x 100/1000BaseX (SFP/CSFP) or 4 x 10/100/1000 BaseT	<ul style="list-style-type: none"> <li>Supports 1 GbE rates only when installed in Tslots TS10-TS15 in NPT-1800 with CIPS1T.</li> <li>Supports 1 GbE rates when installed in all Tslots with CIPS2T.</li> </ul>

Card	Max. card Group I (CIPS1T)	Max. card Group II (CIPS1T)	Max. cards per platform (CIPS1T)	Max cards per platform (CIPS2T)	Interface Type	Comments
DHGE_10	11	12	23	18	5/10 x 100/1000Bas eX (SFP/ CSFP) or 5 x 10/100/1000 BaseT	9 in upper cage and 9 in lower cage.
DHGE_16	4	---	4	--	8 x 100/1000Bas eT + 4/8 x 100/1000Bas eX (SFP/ CSFP) or 4 x 100/1000Bas eT	
DHGE_20	---	12	12	12	10/20 x 100/1000Bas eX (SFP/ CSFP) or 10 x 10/100/1000 BaseT	
DHGE_24	4	---	4	---	12/24 x 100/1000Bas eX (SFP/ CSFP) or 12 x 10/100/1000 BaseT	Up to 64 x GEs by DHGE_24.
DHXE_4	11	12	18	23	4 x 10GE (SFP+)	
DHXE_40	11	12	18	23	4 x 10GE/ OTU2e	

Card	Max. card Group I (CIPS1T)	Max. card Group II (CIPS1T)	Max. cards per platform (CIPS1T)	Max cards per platform (CIPS2T)	Interface Type	Comments
DHXE_4sec	11	12	18	23	2 x 10GE (SFP+) 2 x 1GE (multi rate)	
MSC2_8	11	12	23	23	2 x STM-1 + 8 x E1	
MS345_3	11	12	23	23	2 x STM-1 + 8 x E1	
MSE1_32	11	12	23	23	32 x E1	
MS1_4	11	12	23	23	1 x STM-4 or 4 x STM-1	
DHCE_1	---	6	6	12	1 x 100GBase-R / OTU-4	CIPS1T: Tslots #10 to #15 CIPS2T: Tslots #7 to #18
DHCE_1C	---	6	6	12	1 x 100GBase-R / OTU-4	CIPS1T: Tslots #10 to #15 CIPS2T: Tslots #7 to #18
DHCE_1Q / DHCE_1QB	---	6	6	16	1 x 100GBase-R	CIPS1T: Tslots #10 to #15 CIPS2T: Tslots #5 to #18 and TS23-TS24

**i Notes**

- With DHGE\_20 cards in Group II, max GE ports per platform can be up to 180 based on SFP only (any card mixture in Group I and Group II).
- Mixed assignment of SFP/CSFP or ETGBE is allowed as per card population in DHGE\_xx cards.
- For DHGE\_10/20, DHXE\_4O, and DHXE\_4sec, max cards assignment in NPT-1800 with 2T is limited due to power consumption management constraints when configured with INF\_1800. With INF\_1800H these limitations are removed.

## NPT-1800 Hardware Compatibility

To avoid hardware mismatch alarms, use new cards from production only. In case of old cards used, make sure that the following HW revision is available for installation.

**(i) Note: DH cards HW version requirements:**

- DHGE\_4E with HW revision >=C00
- DHGE\_8 with HW revision >=C01
- DHGE\_16 with HW revision >=B00
- DHGE\_24 with HW revision >=C00

## Maximum Ports and Fan-Out per Platform

NPT-1800 platforms allow you to install cards in many different slots, offering useful flexibility in deciding how to arrange your I/O cards and how to assign your ports, up to a predefined maximum number of ports:

### With the CIPS1T:

- Maximum number of interfaces of any kind is 197/198 when high PTP accuracy is enabled/disabled
- Maximum number of GE ports in slots TS7 - TS12 (lower Group II) is 105
- Maximum number of GE ports in slots TS13 - TS18 (upper Group II) is 92/93 when high PTP accuracy is enabled/disabled
- Maximum number of 10GE ports is 71 [high PTP accuracy disabled]
- Maximum number of 10GE ports is 70 [high PTP accuracy enabled]
- Maximum number of 100GE ports is 6

### With the CIPS2T:

- Maximum number of interfaces <=300 (GE/10GE/100GE ports)
- Maximum number of ports in TS1-TS12 (lower cage) <=198
- Maximum number of ports in TS13-TS24 (upper cage) <=198
- Maximum number of 10GE ports is 92
- Maximum number of 100GE ports is 16

**(i) Note**

No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by that platform. The actual number of assigned cards is also limited by power budget management constraints.

## Max Fan-Out per Platform

### Examples of Fan-Out with Common Card Combinations

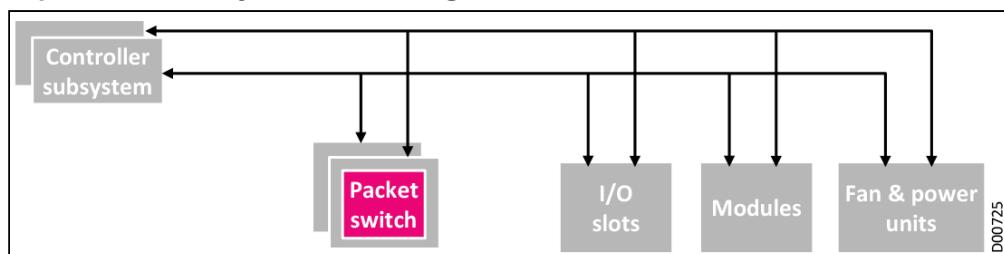
Interface Type	Max. Ports	Configuration Example
E1/T1 (CES)	736	23 x MSE1_32
STM-1/OC-3 (CES)	92	23 x MS1_4
STM-4/OC-12 (CES)	23	23 x MS1_4
10/100/1000BaseT	120	12 x DHGE_20
100BaseFX	240	12 x DHGE_20
1000BaseX	240	12 x DHGE_20
10GE	92	23 x DHXE_4
100GE	16	12 x DHCE_1 + 4 x DHCE_1Q

**Note**

Max fan-out can be achieved through different mixtures of card types and quantities. The max configurations in the preceding table are only examples of some of the options available for reaching max fan out per card per platform.

## NPT-1800 Control Subsystem

### Neptune Control System Block Diagram



The MCP1800 is required for the system to function, since it is responsible for creating virtually a complete standalone native IP system. Moreover, it accommodates one service traffic slot for flexible configuration of virtually any type of Ethernet interfaces. This integrated flexible design ensures a very compact equipment structure and reduces costs, making the NPT-1800 an ideal native choice for the access and metro access layers.

NPT-1800 control and communication functions include:

- Internal control and processing
- Routing engine
- Communication with external equipment and management
- Network element (NE) software and configuration backup

- Built-in Test (BIT)

**Note**

The NPT-1800 supports two controller types; MCP-1800 and MCP-1800B. For simplicity in this section we use the general term MCP-1800; functionality is the same for both cards.

## Software and Configuration Backup

The platform features a large-capacity on-board NVM that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

### Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection
- Protection switch for the main switching card

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

## NPT-1800 Communications with External Equipment and Management

In the Neptune product line, the main controller card is responsible for communicating with other NEs and management stations.

The main controller card communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other PEs via in-band management, enabling NE management through in-band channels.

### Usage Guidelines

The NPT-1800 supports in-band and management communication on the following interfaces:

- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- In-band management processing (40Mbps)

The following routing protocols are supported via DCN and in-band:

- IPv4: OSPFv2, IS-IS, static routes
- IPv6: OSPFv3, IS-IS v6, static routes

## NPT-1800 Controller Cards

The following controller, communication, and L3 forwarding modules in the NPT-1800 are introduced in this section.

- MCP1800
- MCP1800B

## MCP1800 Overview

The MCP1800 is the main processing card of the NPT-1800. It integrates functions such as IP/MPLS control plane, platform control, communications, and MCC. Double redundancy in the NPT-1800 platform can be obtained using a redundant NVM unit in the second redundant controller subsystem, which is updated automatically whenever there is a change in the database.

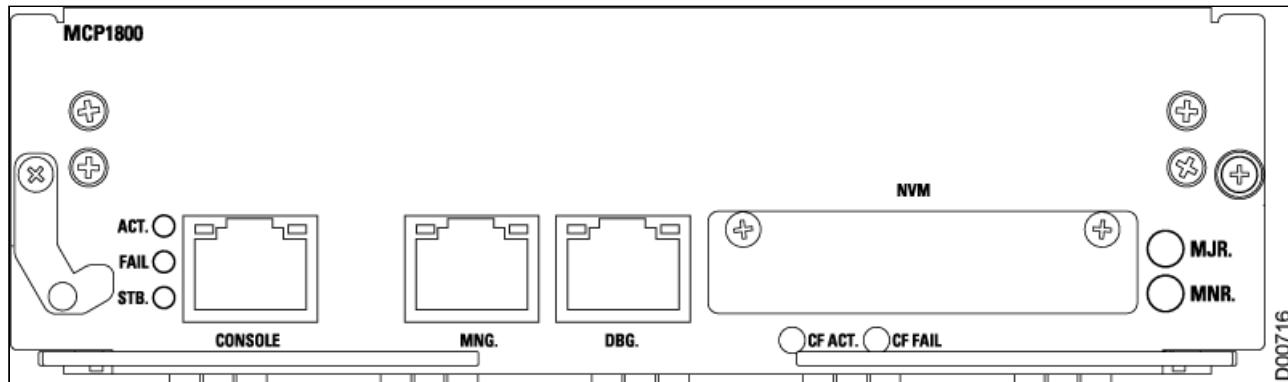
The MCP1800 provides the following control-related functions:

- Communications with and control of all other modules in the NPT-1800 and EXT-2U, via the backplane
- Communications with the EMS-NPT, LCT-NPT, or other NEs via a management interface (MNG), MCC, or VLAN
- Routing engine and handling (IP/MPLS & L3VPN)
- Support of the 8 Gb NonVolatile compact flash (CF) Memory (NVM) card
- Fan control
- Hardware and software controller redundancy
- The MCP1800 supports the following interfaces:
  - MNG
  - Debug (for Technical staff use only)
  - CONSOLE

**(i) Notes**

- For IP/MPLS Control plane and L3VPN activation, the NPT-1800 must be configured with two MCP1800 cards (highly recommended for any application).
- For PB & MPLS-TP only, the NPT-1800 may be configured with one MCP1800 card

### MCP1800 Front Panel



**MCP1800 Front Panel Interfaces**

Marking	Interface type	Function
CONSOLE	RJ-45 connector	Serial RS232 console interface for CLI.
MNG.	RJ-45 connector	10/100/1000BaseT Ethernet interface for management
DBG.	RJ-45 connector	10/100/1000BaseT port for use by technical support personnel (debug, maintenance, etc.).

**MCP1800 LED Indicators and Pushbutton**

Marking	Full name	Color	Function
- (left LED in MNG and AUX MNG. ports)	Link	Green	Lights when MNG link is on. Off when MNG link is off. Blinks when packets are received or transmitted.
- (right LED in MNG and AUX MNG. ports)	Speed	Orange	Lights when the MNG link is 100 Mbps. Off when the MNG link is 10 Mbps.
ACT.	System active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates card not running normally.
FAIL	System fail	Red	Normally off. Lights when card failure detected.
STB.	System standby	Red	Lights when the card is in standby mode.
MJR.	System major alarm	Red	Lights when the system has a critical or major alarm.
MNR.	System minor alarm	Yellow	Lights when the highest severity of the NE current alarms is minor or warning. Off when the system has no alarm or the highest severity of the NE current alarms is higher than minor or warning.
CF ACT.	Compact Flash memory active	Green	Lights when the CF card is present and properly locked. Off when the CF card is not present or not locked. Blinks when the CF card is being written or read.
CF FAIL	Compact Flash memory fail	Red	Normally off. Lights when the CF card is not present, is not locked, or has a failure.

**(i) Note**

ACT, FAIL, MJR, and MNR. LEDs are combined to show various failure reasons during the system boot. For details, see the Troubleshooting Using Component Indicators section in the *NPT-1800 Installation, Operation, and Maintenance Manual*.

## MCP1800B Overview

The MCP1800B is the main processing card of the NPT-1800. It integrates functions such as IP/MPLS control plane, platform control, communications, and MCC. Double redundancy in the NPT-1800 platform can be obtained using a redundant NVM unit in the second redundant controller subsystem, which is updated automatically whenever there is a change in the database.

The MCP1800B is almost identical to the MCP1800 and differs only in the NVM card type, which is micro-SD in the MCP1800B, compared to CF in the MCP1800. The main advantage of the micro-SD memory is a higher Read/Write access speed. All other features and functions of the MCP1800B are the same as described in [MCP1800](#).

## NPT-1800 Timing Overview

This platform provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations for functionality and performance.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed redundantly from the TMUs to all traffic and matrix cards, minimizing unit types and reducing operation and maintenance costs.

The TMU and the internal and external timing paths are fully redundant. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem. In case of hardware failure, the redundant synchronization subsystem takes over the timing control with no traffic disruption.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- 1PPS and ToD interfaces, using external timing input sources
- 2 x 2 MHz/Mbps (T3/T4) external timing input sources
- NTP support (NTPv1, NTPv2, NTPv3, and NTPv4)
- E1/T1 interfaces of CES cards
- STM-1/4 of CES cards
- Local interval clock
- Holdover mode
- SyncE
- 1588v2 - Primary, Secondary, and boundary clock

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization over GbE/10GbE/100GbE and FlexE interfaces. Our implementation is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262.1, G.8263, and G.8264.

The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. PTP is supported over GbE/10GbE/100GbE and FlexE interfaces. IEEE 1588v2 (G.8265.1)

(CIPS1T)/G.8275.1 (CIPS1T and CIPS2T)) is supported in the NPT-1800, providing Boundary Clock (BC) capabilities.

Cellular networks use the 1588 (PTP) standard to transmit accurate timing (frequency and phase) throughout the network. The level of accuracy required depends on the type of network and its capabilities. In 4G networks it was enough to maintain timing accuracy of 1.5µs from RAN to core, with 50ns timing error per NE (Class A). However, in 5G networks the requirements are much higher, and are limited to 130ns, with 10ns timing error per NE (Class C).

The 2T matrix supports PTP IEEE 1588v2 is supported in two profiles; full network timing support (G.8275.1) and partial network timing support (G.8275.2), providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <10ns (G.8273.2 Class C) timing error per NE. The CIPS2T matrix card also supports Assisted Partial Timing Support (APTS), a global navigation satellite system.

The 1T matrix was enhanced in V7.6, and for HW >=G20 it is possible to enable high accuracy PTP mode and achieve <20ns (G.8273.2 Class B) timing error per NE. IEEE 1588v2 (G.8275.1) with G.8273.2 Class C is supported in the platform, providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities.

**i Notes**

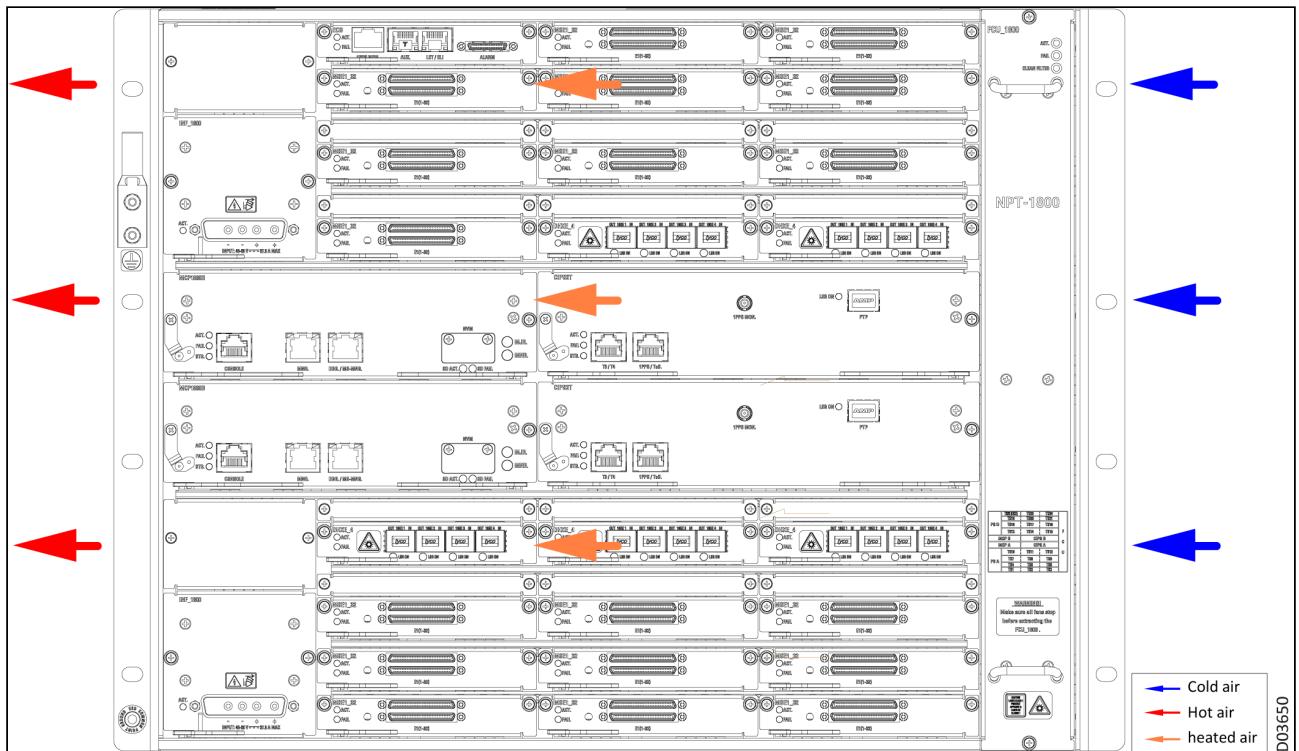
- Some fanout restrictions are applied when using high accuracy PTP enabled in 1T matrices; see [NPT-1800 Platform Design](#).
- For 1T matrices in hardware revisions preceding G20 that are already in the field, we recommend keeping the default mode (high accuracy PTP disabled), as it is backward compatible to the install-base configuration.

## NPT-1800 Cooling Subsystem

The NPT-1800 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components, and cools them.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

## Airflow in the NPT-1800



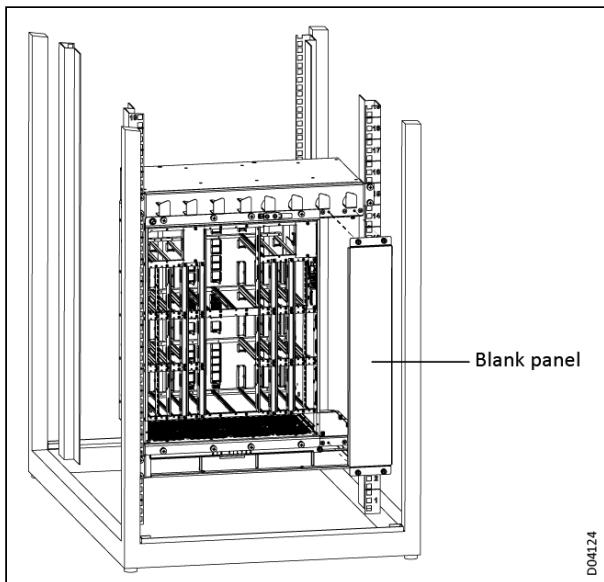
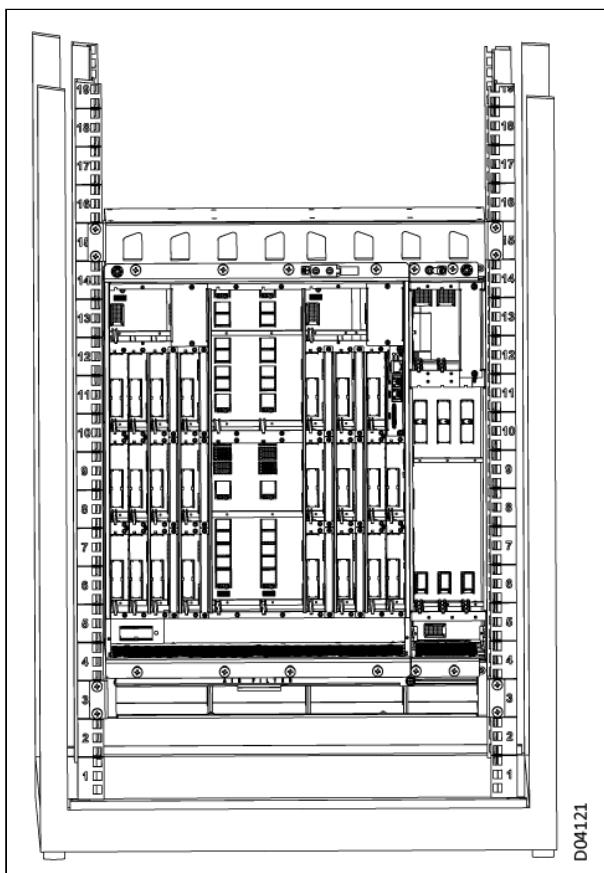
## Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The NPT-1800 platform, with or without an EXT-2U expansion unit, can be installed in a 19" rack together with two air baffle units by using a vertical configuration.

1. If you are using an EXT-2U expansion unit with the NPT-1800 platform, then first install the EXT-2U unit on the NPT-1800 platform.
2. Rotate the NPT-1800 platform 90 degrees to the right. With this orientation, the original top and bottom of the NPT-1800 platform are now on the right and left sides of the platform. The original left and right sides of the platform are now on the top and bottom of the platform.
3. Attach the air baffles above and below the NPT-1800, on the surfaces that were previously the left and right sides of the NPT-1800 platform.
4. Insert the now-rotated and vertically-oriented NPT-1800 platform into the 19" rack. The rotated NPT-1800 platform with air baffle units occupies a total space of 13U height in the rack.

See the *NPT-1800 Installation and Maintenance Manual* for installation procedure details and limitations.

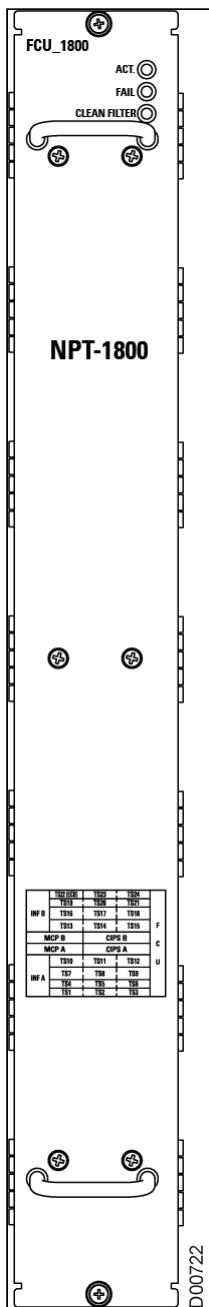
**NPT-1800 Vertical Installation with Air Baffle Units in 19" Rack****NPT-1800 Vertical Installation with Expansion Unit and Air Baffle Units in 19" Rack****FCU Fan Control Module**

The NPT-1800 platform is cooled through the FCU\_1800, a pluggable fan control module with eight fans. The fan speeds can be set at different levels. The speed is controlled by the MCP1800 with PWM signal,

according to the actual temperatures of installed cards and key components. The unit supports 1:N fan redundancy.

 **Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

**FCU\_1800 Front Panel**

### FCU\_1800 Front Panel Indicators

Marking	Item	Functions
ACT.	Green LED	Lights steadily when the card is powered and operating normally.
FAIL	Red LED	Normally off. Lights steadily when a fault is detected.
CLEAN FILTER	Yellow LED	Normally off. Lights steadily when the air filter must be cleaned or replaced.

## NPT-1800 Power Feed and Alarm Subsystems

### Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. AC power feeding requires the use of a conversion module to implement AC/DC conversion.

### Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-1800 is configured with two [INF\\_1800/INF\\_1800H](#) power supply cards for redundancy.

The electrical connection board ([ECB](#)) houses the external alarm connector. This module is integrated in the NPT-1800 platform and is included by default.

## INF\_1800 and INF\_1800H Overview

The INF\_1800 is a DC power filter module for the NPT-1800 platform. Two INF\_1800 modules are needed for power feed redundancy.

The INF\_1800 performs the following functions:

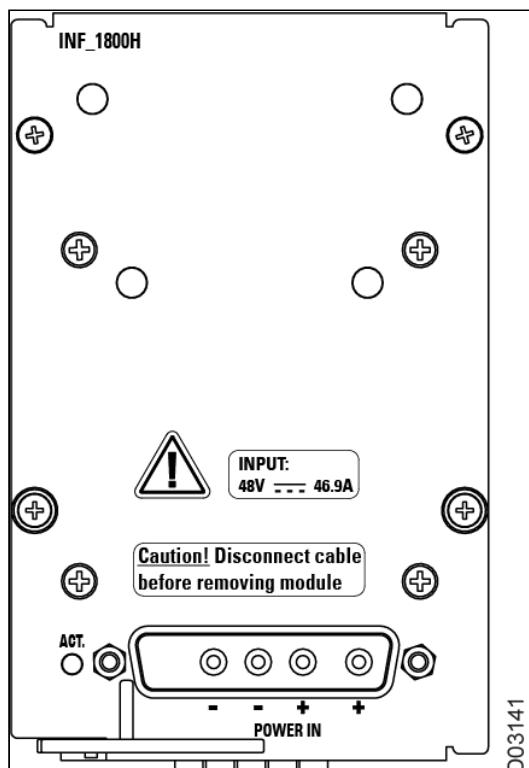
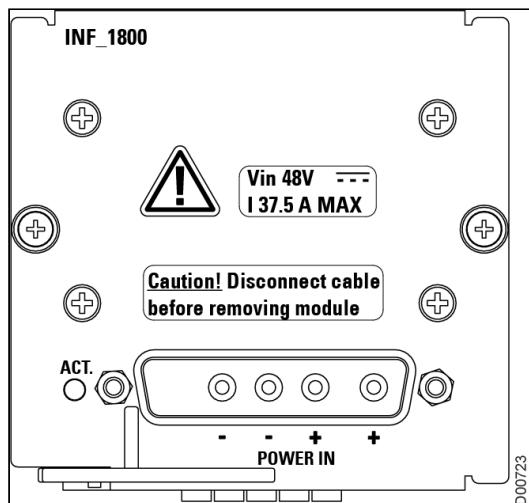
- Single DC power input 5W5-based connector and power supply for all cards and modules in the platform
- Input filtering function for the entire NPT-1800 platform
- Indication of input power loss and detection of under/over voltage
- Shutting down of the power supply when under/over voltage is detected
- Protection micro-switch for safety disconnection cable
- High-power INF for up to 1800 W

The INF\_1800H module provides the same functionality as the INF\_1800 module, and also offers a greater power output of up to 2250W. This greater power output is necessary to fully support the NPT-1800 platform configured with a CIPS2T matrix card running at full scale.

The INF\_1800H is designed with backward compatibility.

- When assigned in V8.0, it is identified as INF\_1800H and provides 2250W.
- When assigned in V7.6MR, it is identified as INF\_1800H and provides 1800W.
- When assigned in earlier versions it is identified as INF\_1800 and provides 1800W.

### INF\_1800 and INF\_1800H Front Panels



### INF\_1800/INF1800H Front Panel Component Functions

Marking	Item	Functions
ACT.	Green LED	Lights steadily when the INF_1800 input supply voltage through the POWER IN connector is in the allowed range.
POWER IN	5W5 D-type connector	Connects DC input power to the first filter in the unit.

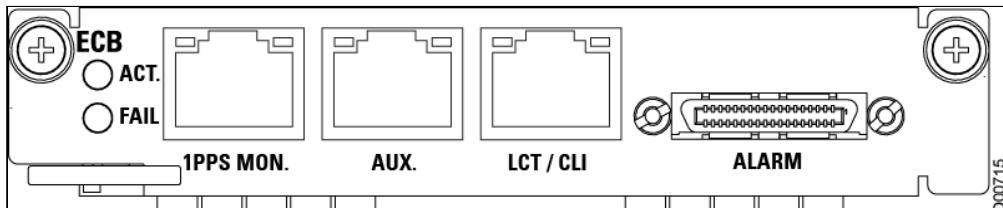
**i Notes**

- The NPT-1800 must be configured for redundancy with two INF\_1800 cards or two INF\_1800H cards.
- A mixture of one INF\_1800 card and one INF\_1800H card is allowed. In this case the platform power consumption support is 1800W.

## ECB Overview

The ECB (Electrical Connection Board) is located in Tslot No. 22. It connects the LCT and CLI for local management configuration and the RJ-45-based connector for 1588V and 2 x 1PPS monitoring.

### ECB Front Panel



### ECB Front Panel Components

Marking	Interface type	Function
1PPS MON.	RJ-45 connector	1588 V2 1PPS monitoring port.
AUX.	RJ-45 connector	Auxiliary 10/100BaseT Ethernet interface for local management and debug.
LCT/CLI	RJ-45 connector	Local management port for connecting an LCT or CLI station.
ALARM	SCSI 36-pin connector	Connects alarm input and output lines via a RAP or directly to the client.
ACT.	Green LED	Indicates that the ECB card is powered and operating normally.
FAIL	Red LED	Lights steadily when a fault is detected in the card.

## NPT-1800 Switching Cards

The NPT-1800's modular architecture enables its outstanding configuration flexibility. The heart of NPT-1800 is a non-blocking switching card. Hardware-based subnet connection protection is provided for all interfaces, with protection switching in less than 50 msec.

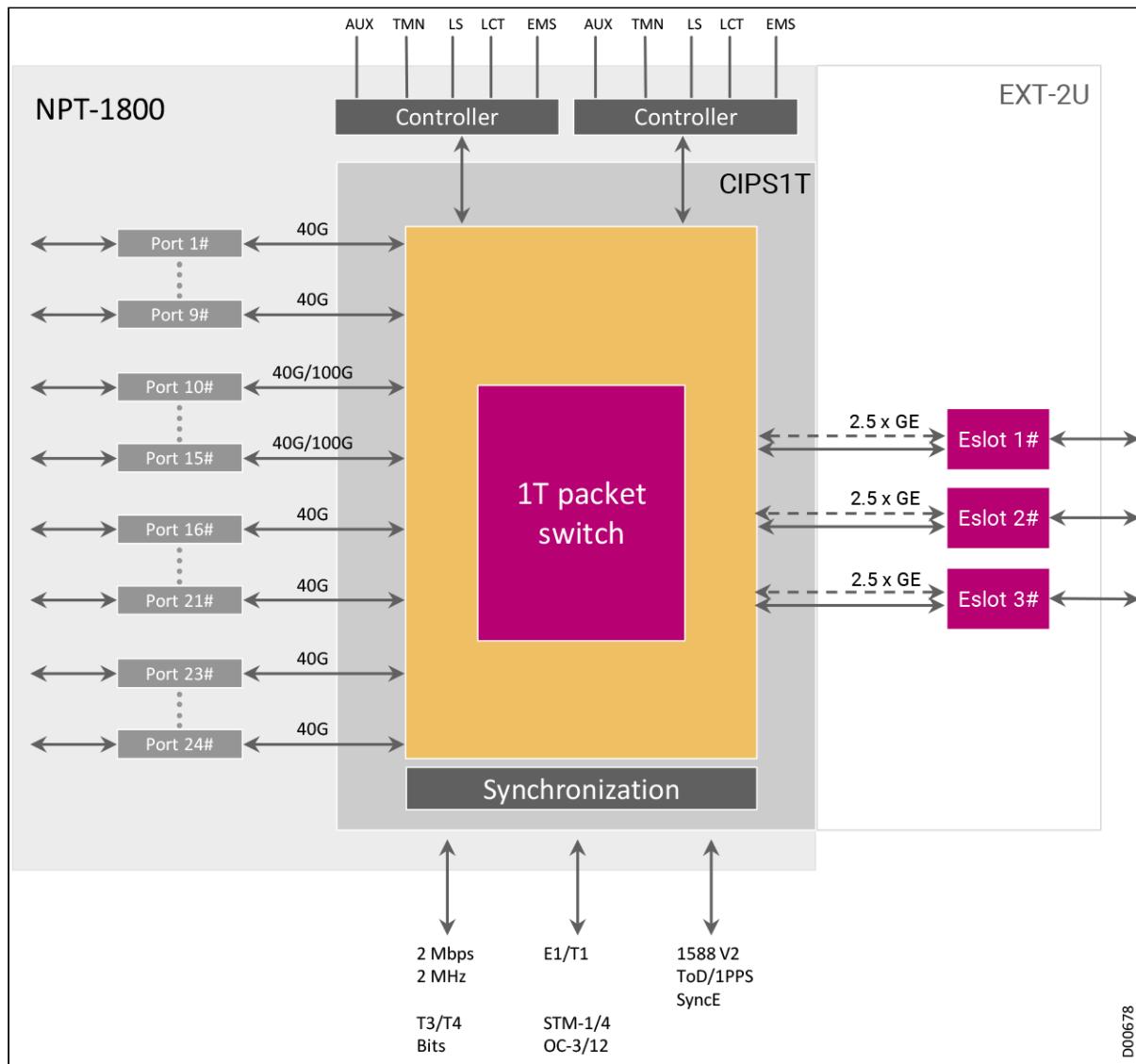
The high-capacity, non-blocking CIPS1T/CIPS2T central switching cards provide dual stack packet switching (L2, L3, MPLS-TP, and IP/MPLS). The CIPS1T/CIPS2T cards provide the main control, communication, timing, and overhead processing functionality. Two matching CIPS1T/CIPS2T cards are required for redundancy.

NPT-1800 platforms support smooth reassignment from CIPS1T to the higher-capacity CIPS2T cards. The following sections detail switching card functionality.

- [CIPS1T Overview](#)
- [CIPS2T Overview](#)

## CIPS1T Overview

### CIPS1T Traffic Flow



The total capacity of a platform using the CIPS1T is more than 1T. The bandwidth is evenly distributed between the platform slots, with 6 slots supporting 40G/100G dynamic capacity allocation and the remaining 17 slots supporting up to 40Gbps. The CIPS1T provides the following main functions:

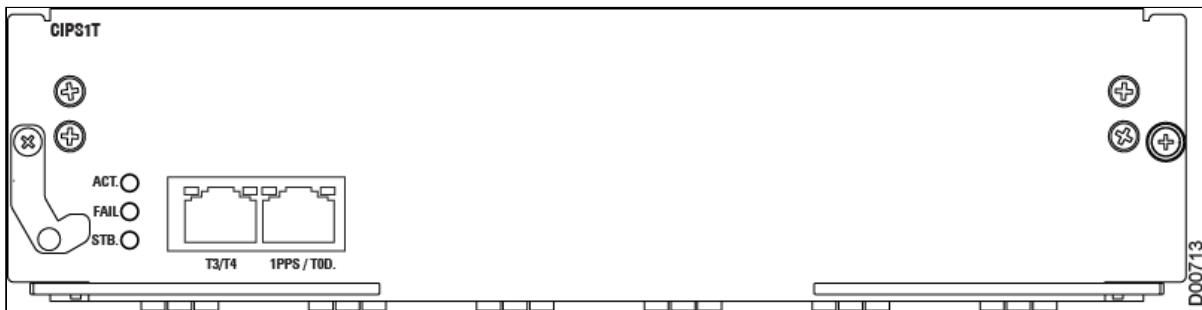
- Packet switching with at least 1T switching and 800G TM, providing non-blocking data switch fabric for Ethernet/MPLS-TP and IP/MPLS traffic forwarding
- Traffic management (TM) including (800G):
  - Guaranteed CIR
  - 8 x CoS for differentiated services
  - E2E flow control
- Any-slot-to-any-slot connectivity
- Comprehensive range of timing and synchronization capabilities G.781/G.8262 compliant EEC
  - 1PPS and ToD interfaces
  - SyncE

- IEEE 1588v2 PTP with:
  - OC (Master & slave), BC
  - One-step TC
  - G.8265.1 profile
  - G.8275.1 profile
  - G8273.2 Class B [CIPS1T with HW revisions from G20 and above]
- Switchover performance less than 50 msec on protection switchover in case of CIPS1T equipment failure (in the data path), plug-out, or manual command
- Supports local management via CLI
- L3 VPN and IP/MPLS features (IPV4 and IPV6):
  - VRF support:
    - ACL + L3 classification
    - uRPF
    - Multi-VRF networking stack
  - BGP (iBGP & eBGP):
    - Graceful restart
    - BFD support
  - L3VPN extension over static PW (PW-HE)
  - PE-CE protocols:
    - Static
    - eBGP
  - VRRP
  - IP multicast:
    - IPV4 multicast with PIM and IGMP
  - DHCP:
    - DHCP Relay (to connect hosts to DHCP server via L3 VPN)
  - Multi hop IP-BFD
- NETCONF interface
- Continuous PM counters
- Syslog report generation support
- Built-in Y.1564 Service Activation Test and loop back with MAC swap

**Notes**

- The NPT-1800 must be configured with two CIPS1T cards.
- From V7.6, NPT-1800 capacity can be upgraded to 2TB using the CIPS2T.

### CIPS1T Front Panel



**CIPS1T Front Panel Interfaces**

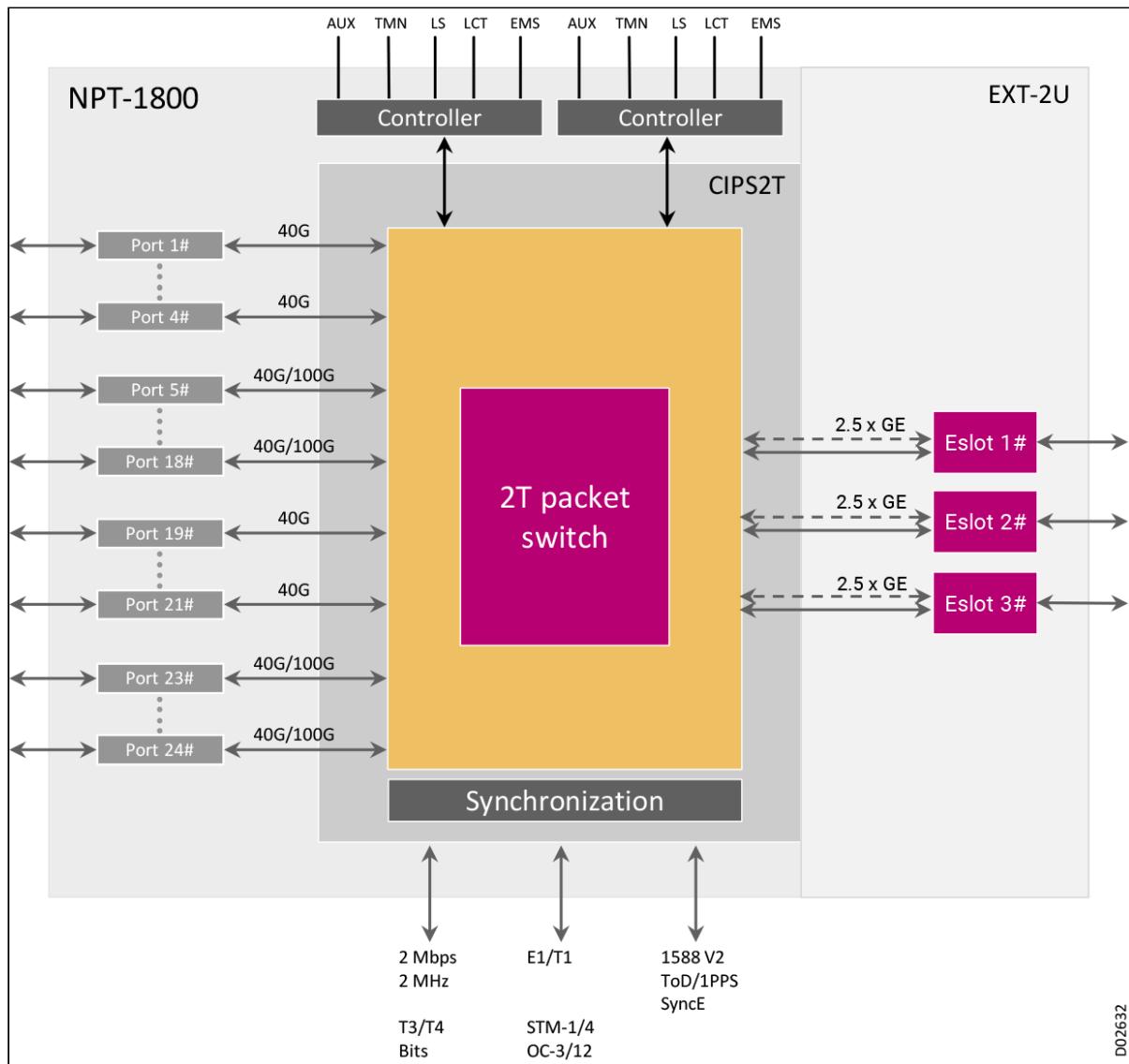
Marking	Interface type	Function
T3/T4	RJ-45 connector	T3 and T4 timing interfaces (one 2 Mbps and one 2 MHz).
1PPS/ToD	RJ-45 connector	1PPS and Time of Day input/output signals supporting Ethernet timing per IEEE 1588v2 standard.

**CIPS1T Indicators and Functions**

Marking	Full name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the CIPS1T not downloaded successfully or that the CIPS1T cannot be controlled normally by the MCP1800. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the CIPS1T card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STB.	System standby	Orange	Lights when the card is in standby. Off when the card is active.

## CIPS2T Overview

### CIPS2T Traffic Flow



The total capacity of a platform using the CIPS2T is 2T. The bandwidth is evenly distributed between the platform slots, with 16 slots supporting 40G/100G dynamic capacity allocation and the remaining 7 slots supporting up to 40Gbps. The CIPS2T provides the following main functions:

- Packet switch with 2T capacity, providing:
  - Management and internal control
  - User traffic switching
  - Non-blocking data switch fabric up to 1880G (IMIX)
  - Up to 800G non-blocking FlexE support (1T-ready FlexE capacity)
  - Up to 1870Mbps x 2 processing rate
- 5G ready packet transport, including:
  - Hard (FlexE) and soft (enhanced VPN and segment routing) network slicing
  - Ultra-low latency support, with deterministic pass-through FlexE channels
  - Stringent phase synchronization requirement for Class C/D timing accuracy compliance (8273.2)
  - 25G interfaces
- Comprehensive range of timing and synchronization capabilities (G.781/G.8262 compliant EEC, G.8273.2):

- SyncE
- 1PPS and ToD interfaces
- APTS
- IEEE 1588v2 PTP with:
  - OC (primary & secondary), BC
  - One-step TC
  - G.8275.1 profile
  - G.8275.2 profile
  - G8273.2 Class C/D timing accuracy compliance (5/10ns)
- Traffic management (TM) including:
  - Guaranteed CIR
  - End-to-end flow control
  - 8 x CoS for differentiated services
- Any-slot-to-any-slot connectivity
- Switchover performance of less than 50msec hit on protection switchover due to CIPS2T equipment failure (in the data path), plug-out, or manual command.
- Supports local management via CLI
- L3 VPN and IP/MPLS features (IPV4 and IPV6):
  - VRF support:
    - ACL + L3 classification
    - uRPF
    - Multi-VRF networking stack
  - BGP (iBGP & eBGP):
    - Graceful restart
    - BFD support
  - L3VPN extension over static PW (PW-HE)
  - PE-CE protocols:
    - Static
    - eBGP
  - VRRP
  - IP multicast:
    - IPV4 multicast with PIM and IGMP
  - DHCP:
    - DHCP Relay (to connect hosts to DHCP server via L3 VPN)
  - Multi hop IP-BFD
- NETCONF interface
- Continuous and periodic PM counters
- Syslog report generation support
- Built-in Y.1564 Service Activation Test and loop back with MAC swap

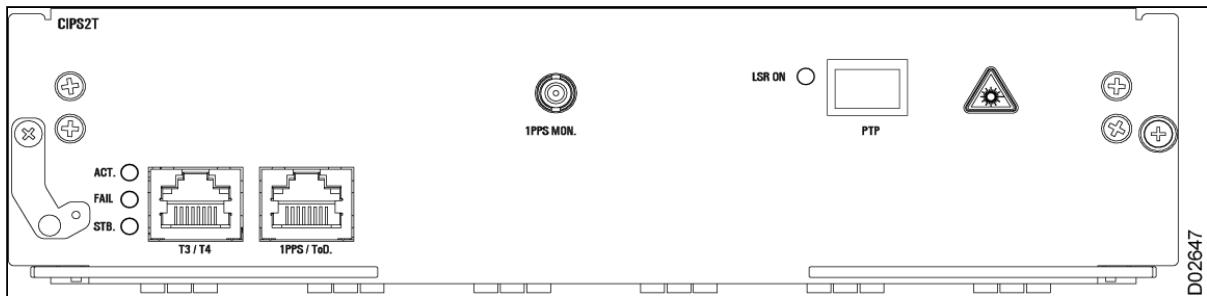
 **Note**

The NPT-1800 must be configured with two CIPS2T cards.

**i Optional Features:**

- CIPS2T matrix is available in two variants: default switching capacity (1T) and full switching capacity (1.88T); it is possible to unlock the default capacity limit to utilize full capacity with a software license.
- CIPS2T is available in two scale variants: default scale and high scale (for ACL rules and FIB routing numbers). Enabling high scale capability is controlled by a license. Users can run services on the NPT-1800 with a CIPS2T with default scale enabled in the beginning, and purchase a license to enable high scale at a later time, even after services have been provisioned, to scale up the NE performance.

### CIPS2T Front Panel



### CIPS2T Front Panel Interfaces

Marking	Interface type	Function
T3/T4	RJ-45 connector	T3 and T4 timing interfaces (one 2 Mbps and one 2 MHz).
1PPS/ToD	RJ-45 connector	1PPS and Time of Day input/output signals supporting Ethernet timing per IEEE 1588v2 standard.
1PPS MON.	Coaxial connector	1588 V2 1PPS monitoring port.
PTP	SFP connector	PTP interface (not in use)

### CIPS2T Indicators and Functions

Marking	Full name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the CIPS1T not downloaded successfully or that the CIPS1T cannot be controlled normally by the MCP1800. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the CIPS1T card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STB.	System standby	Orange	Lights when the card is in standby. Off when the card is active.
LSR ON	Laser on indication	Green	Lights steadily when laser is on.

## NPT-1800 Tslot IO Modules

The NPT-1800 has 23 Tslots for installing I/O modules. The following table lists the different types of CES and Ethernet I/O modules that can be installed in the NPT-1800, with links to each module listed.

 **Note**

No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by that platform; see [Maximum ports per platform](#).

**NPT-1800 Tslot Modules**

Description	Card	With CIPS1T	With CIPS2T
CES multiservice module with 3 x DS3 interfaces and 1 x STM-1/OC3 interface	<a href="#">MS345_3</a>	TS1-TS24, except TS22	TS1-TS24, except TS22
CES multiservice module with 24 x DS3 interfaces	<a href="#">MS345_24</a>	TS1-TS24, except TS22	TS1-TS24, except TS22
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	<a href="#">MSC_2_8</a>	TS1-TS24, except TS22	TS1-TS24, except TS22
CES multiservice module with 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<a href="#">MS1_4</a>	TS1-TS24, except TS22	TS1-TS24, except TS22
CES multiservice module with 32 x E1/T1 interfaces  Note: Protection available through TP32_2 module installed in EXT-2U expansion unit	<a href="#">MSE1_32</a>	TS1-TS24, except TS22	TS1-TS24, except TS22
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4E</a>	TS1-TS6, TS19-TS21, TS23-TS24	N/A
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4EB</a>	TS1-TS24, except TS22	TS1-TS24, except TS22
Optical 8 x GE interface module with direct connection to the packet switch	<a href="#">DHGE_8</a>	TS1-TS6, TS19-TS21, TS23-TS24	N/A
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	<a href="#">DHGE_8S</a>	TS1-TS24, except TS22	TS1-TS24, except TS22
Optical 10 x GE module with direct connection to the packet switch	<a href="#">DHGE_10</a>	TS1-TS24, except TS22	TS1-TS24, except TS22

Description	Card	With CIPS1T	With CIPS2T
Electrical and optical 16 x GE interface module with direct connection to the packet switch	DHGE_16	Tslot pairs: TS1+TS2 <i>or</i> TS2+TS3  TS4+TS5 <i>or</i> TS5+TS6  TS19+TS20 <i>or</i> TS20+TS21  TS23+TS24 (Group I)	N/A
Optical 20 x GE interface module with direct connection to the packet switch	DHGE_20	TS7-TS18	TS7-TS18
Optical 24 x GE interface module with direct connection to the packet switch	DHGE_24	Tslot pairs: TS1+TS2 <i>or</i> TS2+TS3  TS4+TS5 <i>or</i> TS5+TS6  TS19+TS20 <i>or</i> TS20+TS21  TS23+TS24 (Group I)	N/A
Optical 4 x 10GE interface module with direct connection to the packet switch	DHXE_4	TS1-TS24, except TS22	TS1-TS24, except TS22
Optical 4 x 10GE/OTU-2 interface module with direct connection to the packet switch with OTN wrapping	DHXE_40	TS1-TS24, except TS22	TS1-TS24, except TS22

Description	Card	With CIPS1T	With CIPS2T
40G card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces	DHXE_4MR	N/A	TS1-TS24, except TS22
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces  All 4 ports support MACsec capability.	DHXE_4MRsec	TS1-TS24, except TS22	TS1-TS24, except TS22
40G MACsec card with: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 10G/1GE multi-rate ports</li></ul> All 4 ports support MACsec capability.	DHXE_4sec	TS1-TS24, except TS22	TS1-TS24, except TS22
Optical 100GE combo CFP2 or QSFP28 interface module with direct connection to the packet switch	DHCE_1	TS10-TS15	TS7-TS18
Optical 100GE/OTU-4 CFP interface module with direct connection to the packet switch	DHCE_1C	TS10-TS15	TS7-TS18
Optical 100GE QSFP28 interface module with direct connection to the packet switch	DHCE_1Q	TS10-TS15	TS5-TS18, TS23-TS24
Optical 100GE QSFP28/QSFP_DD interface module with direct connection to the packet switch	DHCE_1QB/1QC	TS10-TS15	TS5-TS18, TS23-TS24
200G FlexE card that supports 2 x 100 GbE interfaces, where each interface can be CFP2 or QSFP28	DHCE_2F	N/A	TS7-TS9, TS10-TS12, TS13--TS15, TS16-TS18
100G card that supports up to 4 x 10GE/25GE (based on SFP+), as well as 5G time stamping accuracy	DH25_4MR	N/A	TS5-TS18, TS23-TS24

## NPT-1800 Expansion Platforms

The traffic capabilities of the Neptune platform can be expanded by installing an expansion unit, either the EXT-2U or the eEXT-2UH.

The EXT-2U and eEXT-2UH platforms are high density modular expansion units for the Neptune multiservice platforms. They support the complete range of CES, PCM, optics, and Ethernet services. Integrating these add-on units into your network configuration is not traffic-affecting.

The expansion units are compact and versatile and can be used with different base units from the Neptune product line. The type of traffic delivered by the unit depends on the type of matrix (PCM or Packet only) installed in the base unit. I/O expansion cards are supported in accordance. The expansion units each have three multipurpose slots (ES1 to ES3) for any combination of extractable traffic cards. PCM, Ethernet, OTN muxponders, optical amplifiers, and CES traffic are all handled through cards in these traffic slots; specific interface options are, dependent on the specific platform configuration. For example, adding the eEXT-2UH expansion unit to an NPT-1800 platform that is already using an EXT-2U unit would provide more slots for TP protection cards, doubling the amount of E1 protection available, which is an essential feature for large-scale aggregation sites.

The following table lists the traffic cards supported in the EXT-2UH or eEXT-2UH when installed with the base platform. For a detailed description of the EXT-2UH and eEXT-2UH features, functionality, and supported traffic cards, see [EXT-2U and EXT-2UH Expansion Units](#) or [eEXT-2UH Expansion Unit](#).

### EXT-2U Supported Cards for NPT-1800

Card Type	Designation
Multiservice PCM and 1/0 XC card over Ethernet. (EM_10EB can be used in EXT-2U or eEXT-2UH platforms.)	<a href="#">EM_10E/EM_10EB</a>
10G card with up to 10 GbE ports; 4 of the ports support POE++. (Can be used in eEXT-2UH platforms.)	<a href="#">DHGE_10_POE</a>
CES multiservice card with 2 x STM-1/OC-3 and 16 x E1/T1 interfaces.	<a href="#">MSC_2_16E</a>
Protection card, provides 1:2 protection for MSE1_32 cards installed in base platform. (Can be used in EXT-2U or eEXT-2UH platforms.)	<a href="#">TP32_2</a>
Protection card, provides 1:1 protection for MS345_3 cards installed in base platform	<a href="#">TPS345_1</a>
Optical Base Card (OBC) for optical amplifiers and DCM modules. (OBC, OBC_B, OBC_C) (OBC_B and OBC_C can be used in EXT-2U or eEXT-2UH platforms.)	<a href="#">Optical Base Card (OBC)</a>

# NPT-1300 System Architecture

The NPT-1300 is a highly cost effective metro-aggregation platform, optimized for aggregation layer, cellular hub 3G, 4G, LTE, and RNC/SGW locations, and service provider hub sites. This 3U platform offers extremely high capacity with a small footprint - 920G, upgradable to 3T, with 200G/400G per slot.

The NPT-1300 is ideal for IP over DWDM applications, providing 100G coherent interfaces mapped to OTU4, and even 200G interfaces mapped to OTUC2. *The NPT-1300 provides the lowest cost per bit for a metro aggregation platform.* This fully redundant coherent platform offers a flexible choice of metro technology (enhanced MPLS-TP, IP/MPLS, and segment routing), offering the full range of MEF CE3.0 L2VPN/L3VPN services. Used in many sub network topologies, NPT-1300 can handle a mixture of P2P, hub, and mesh traffic patterns. This combined functionality means that operators benefit from improved network efficiency and significant savings in terms of cost and footprint.

## NPT-1300 Front Panel



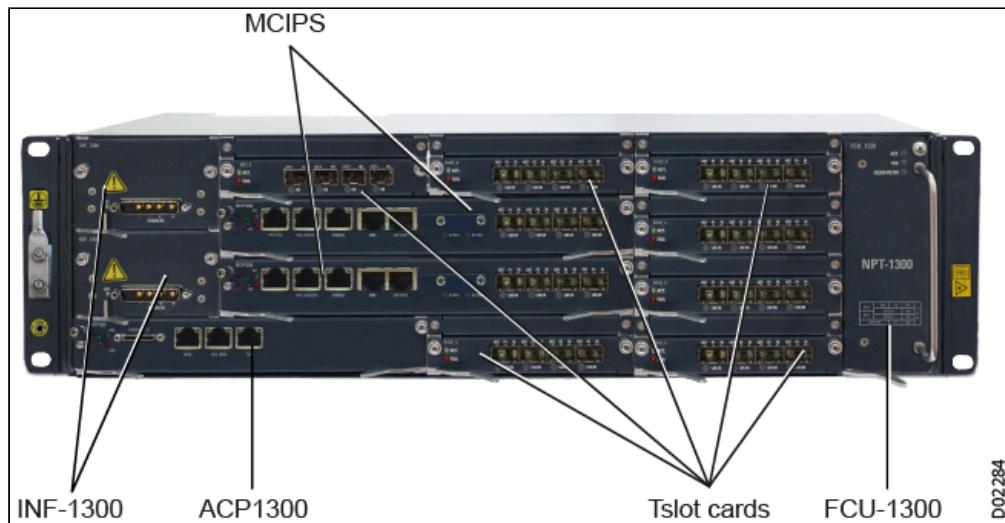
This 3U base platform is housed in a 134 mm high, 440 mm wide, and 243 mm deep (5.28 in. x 17.32 in. x 9.57 in.) equipment cage, with all interfaces accessible from the front of the unit, and fully ruggedized for up to 65°C (149°F) operation in exterior street cabinets. The NPT-1300 provides full redundancy for high resiliency including:

- Two MCIPS1T central packet switches (slots XS A and XS B), providing:
  - IP engine
  - Packet processing capacity of 800G
  - Packet switching capacity of 920G
  - Any-to-any direct data card connectivity
  - 4 SFP+ based 10GE interfaces
  - Shelf controller, supporting:
    - MNG management port
    - Console serial port
    - LCT/CLI Ethernet port
    - NVM (micro SD-based)
- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+ 10GE ports
- Two INF-1300 power supply cards (slots PS A and PS B), support 1+1 and 1+0 configuration
- FCU1300 fan control card (slot FS), with 1:N fan redundancy
- ACP1300 module (slot MS), controls interfaces for all T-slots, PS, FS, alarms, and EXT-2U modules
- 7 I/O card slots (slots TS1-TS7), ready for up to 400G capacity per slot (High-T-slots)
- Comprehensive range of timing and synchronization capabilities (SyncE, 1588v2, G.8275.1, BITS, ToD, and 1pps)
- Backplane connection to optional EXT-2U/EXT-2UH expansion unit, with an additional 3 slots (E-slots)
- System control processor to manage non-traffic-affecting functions

The NPT-1300 is fed from -48 VDC. Two INF-1300 modules can be configured in two power supply module slots for redundant power supply. The NPT-1300 can be installed in 2,200 mm or 2,600 mm ETSI racks or in 19" racks.

Typical power consumption for the NPT-1300 is less than 500 W. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

### NPT-1300 Front Panel Layout



### NPT-1300 Slot Layout

PS B	Tslot 5 (H)	Tslot 6 (H)	Tslot 7 (H)	
	XS B (MCIPS)		Tslot 4 (H)	
PS A	XS A (MCIPS)		Tslot 3 (H)	
	MS (ACP1300)	Tslot 1 (H)	Tslot 2 (H)	FS

For a complete list of the modules that can be configured in each NPT-1300 slot, see [NPT-1300 Tslot IO Modules](#).

All cards support live insertion. All cards are connected using a backplane that supports one traffic connector to connect the NPT-1300 and an expansion unit. The NPT-1300 platform provides full 1+1 redundancy in power feeding, packet switching, and the TMU, as well as 1:N redundancy in the fans.

**Note**

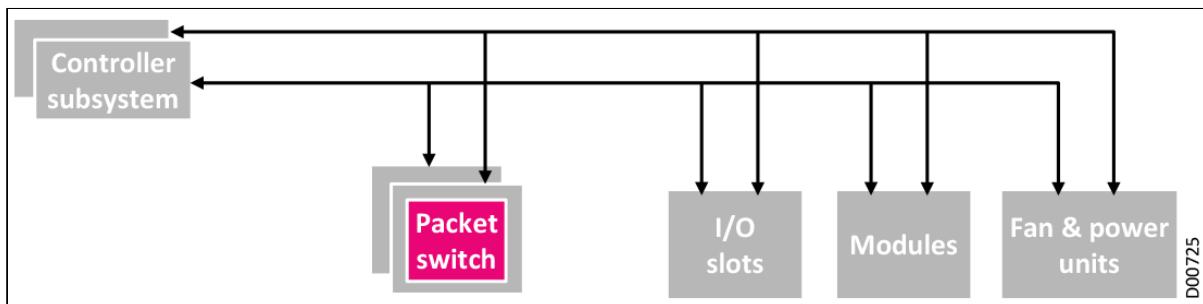
Failure of the ACP1300 does not affect any existing traffic on the platform, but card management is affected.

This section introduces the following NPT-1300 features:

- [NPT-1300 Control Subsystem](#)
- [NPT-1300 Communications with External Equipment and Management](#)
- [NPT-1300 Control and Communication Modules](#)
- [NPT-1300 Timing](#)
- [NPT-1300 Cooling Subsystem](#)
- [NPT-1300 Power Feed Subsystem](#)
- [NPT-1300 Switching Cards](#)
- [NPT-1300 Tslot IO Modules](#)
- [NPT-1300 Expansion Platform](#)

## NPT-1300 Control Subsystem

### Controller Subsystem



NPT-1300 control and communication functions include:

- Internal control and processing
- Communication with external equipment and management
- Network element (NE) software and configuration backup
- Built-in Test (BIT)

### Software and Configuration Backup

The platform features a large-capacity on-board NVM that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

### Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection
- Protection switch for the main switching card

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

## NPT-1300 Communications with External Equipment and Management

In the Neptune product line, the main controller card is responsible for communicating with other NEs and management stations.

The main controller card communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other PEs via in-band management, enabling NE management through in-band channels.

### Usage Guidelines

The NPT-1300 supports in-band and management communication on the following interfaces:

- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- In-band management processing (40Mbps)

The following routing protocols are supported via DCN and in-band:

- IPv4: OSPFv2, IS-IS, static routes
- IPv6: OSPFv3, IS-IS v6, static routes

## NPT-1300 Control and Communication Modules

The ACP1300 and ACP1300B (ACP1300/B) assistant control and communication modules are the supporting processing card of the NPT-1300, integrating functions such as communications and other chassis management functions. ACP1300/B functionality includes:

- Assisting with intra-platform communication:
  - Communication with all modules in power supply slots, fan slot, backplane, Tslots, and Eslots in the NPT-1300 and expansion platform (EXT-2U/2UH), through the backplane (by the CPU)
  - Communication with the main NE controller on the active MCIPS card
  - NE alarm indicators and alarm in/out interfaces
- External timing reference interfaces (T3/T4), which provide the line interface unit for one 2 Mbps T3/T4 interface and one 2 MHz T3/T4 interface

The ACP1300/B supports the following interfaces:

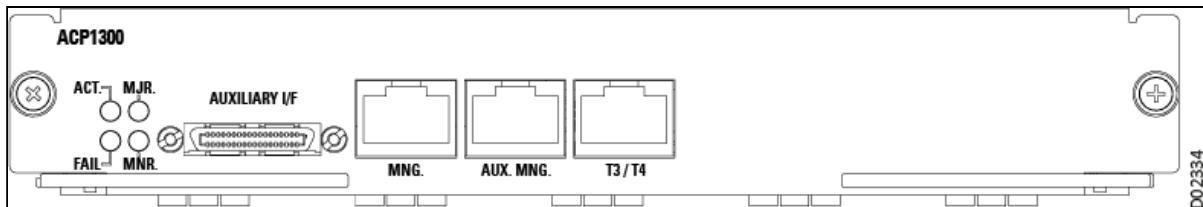
- T3/T4 directly from the front panel
- AUX MNG interface directly from the front panel (out of band DCN interface)
- RS-232, housekeeping and alarms through a concentrated SCSI auxiliary I/F connector on the front panel

**i Note**

Failure of the ACP1300/B does not affect any existing packet traffic on the platform.

Since the NPT-1300 is a front-access platform, all interfaces and LEDs on the ACP1300/B are located on the front panel of the module.

### ACP1300 Front Panel



**ACP1300/B Front Panel Interfaces**

Marking	Interface Type	Function
AUXILIARY I/F	SCSI-36	<p>A concentrated auxiliary connector for the following interfaces:</p> <ul style="list-style-type: none"> <li>• 1 x RS-232 interface for debugging or managing external ancillary equipment</li> <li>• 1 x alarm input and output interface connecting to the RAP</li> </ul>
T3/T4	RJ-45	T3 and T4 timing interfaces (1 x 2MHz/2Mbps)
MNG.	RJ-45	10/100BaseT Ethernet interface for debugging
AUX MNG.	RJ-45	Auxiliary 10/100BaseT Ethernet interface for OOB DCN interface

**i Note**

An MCP30\_ICP can be used to distribute the concentrated auxiliary connector into dedicated connectors for each function; see the Neptune Hybrid Reference Manual for more information.

### ACP1300 LED Indicators

Marking	Full Name	Color	Function
- (left LED in MNG and AUX MNG. ports)	Link	Green	Lights when MNG link is on. Off when MNG link is off. Blinks when packets are received or transmitted.
- (right LED in MNG and AUX MNG. ports)	Speed	Orange	Lights when the MNG link is 100 Mbps. Off when the MNG link is 10 Mbps.
ACT.	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates card not running normally.
FAIL	Card fail	Red	Normally off. Lights when card failure detected.
MJR.	System major alarm	Red	Lights when the system has a critical or major alarm.
MNR.	System minor alarm	Yellow	Lights when the highest severity of the NE current alarms is minor or warning. Off when the system has no alarm or the highest severity of the NE current alarms is higher than minor or warning.



**Note**  
ACT, FAIL, MJR, and MNR. LEDs are combined to show various failure reasons during the system boot. For details, see the Troubleshooting Using Component Indicators section in the *NPT-1300 Installation, Operation, and Maintenance Manual*.

## NPT-1300 Timing

This platform provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations for functionality and performance.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed redundantly from the TMUs to all traffic and matrix cards, minimizing unit types and reducing operation and maintenance costs.

The TMU and the internal and external timing paths are fully redundant. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem. In case of hardware failure, the redundant synchronization subsystem takes over the timing control with no traffic disruption.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- 1PPS and ToD interfaces, using external timing input sources

- 1 x 2MHz/2Mbps (T3/T4) external timing input/output sources, located on the ACP1300 front panel
- NTP support (NTPv1, NTPv2, NTPv3, and NTPv4)
- E1/T1 interfaces of CES cards
- STM-1/4 of CES cards
- Local interval clock
- Holdover mode
- SyncE
- 1588v2 - Primary, Secondary, transparent, and boundary clock

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization, which is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262, G.8263, and G.8264.

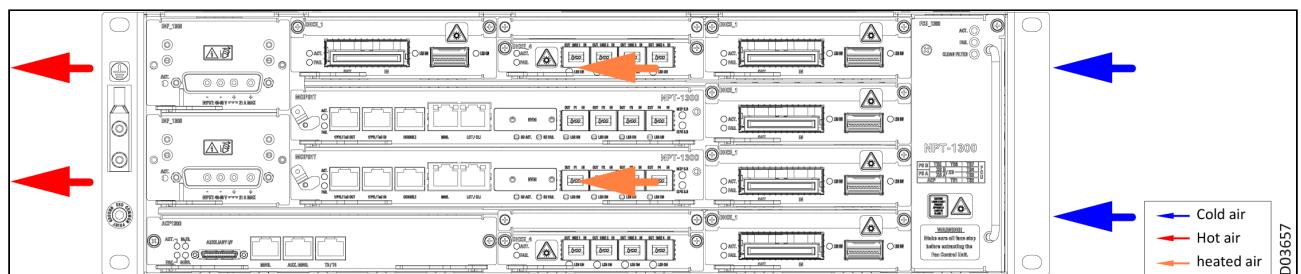
The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. IEEE 1588v2 (G.8265.1/G.8275.1) is supported in the platform, providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <20ns (G.8273.2 Class B) timing error per NE.

## NPT-1300 Cooling Subsystem

The NPT-1300 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components, and cools them.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

### Airflow in the NPT-1300



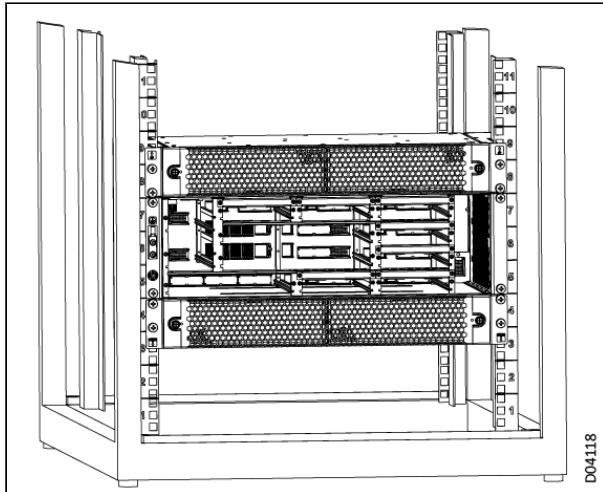
### Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The NPT-1300 platform can be configured together with air baffle units, installed in either a 19" or 23" rack.

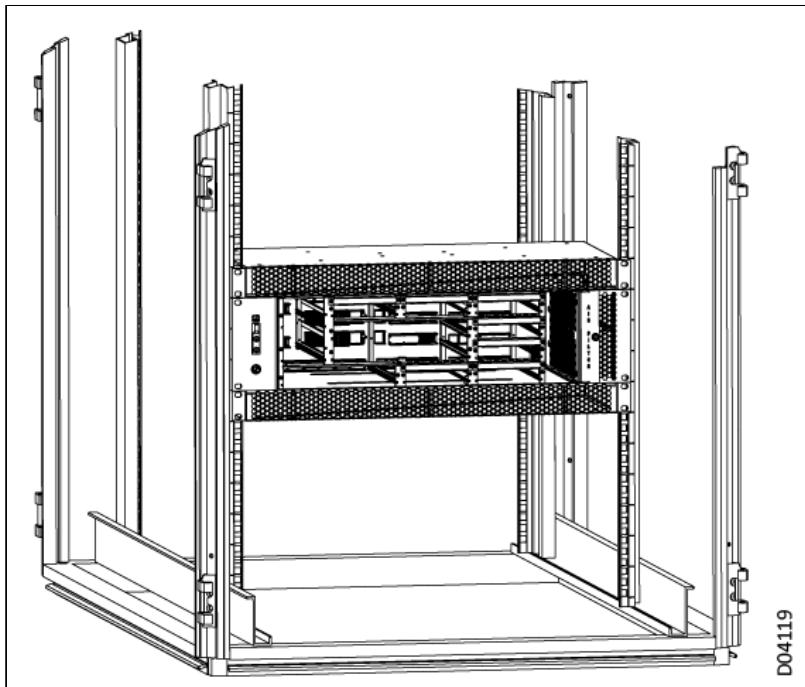
- In the 19" rack, the air baffle unit includes 2 1.5U air-flow boxes; one is located directly *below* the NPT-1300 platform, and one located directly *above* the NPT-1300 platform. The platform and two-part air baffle unit together occupy a total space of 6U height in the rack. The air baffle unit should be installed *before* the NPT-1300 platform; the NPT-1300 platform is then inserted into the gap space between the air-flow boxes. See the *NPT-1300 Installation and Maintenance Manual* for installation procedure details and limitations.

### 3U Height Platform Installed in 19" Rack Between Two Air-Flow Boxes



- In the 23" rack, the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* the NPT-1300 platform, and one located directly *above* the NPT-1300 platform. The platform and two-part air baffle unit together occupy a total space of 5U height in the rack. The air baffle unit should be installed *before* the NPT-1300 platform; the NPT-1300 platform is then inserted into the gap space between the air-flow boxes. See the *NPT-1300 Installation and Maintenance Manual* for installation procedure details and limitations.

### 3U Height Platform Installed in 23" Rack Between Two Air-Flow Boxes



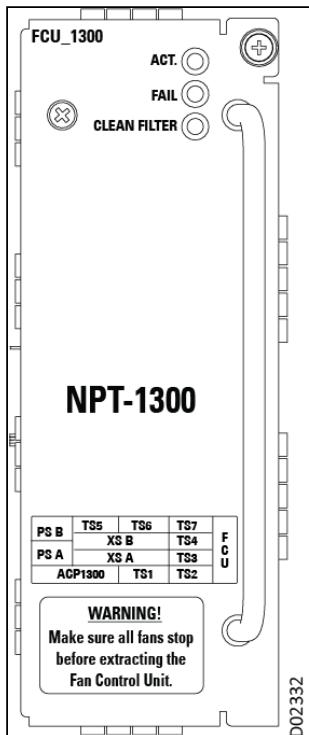
### FCU Fan Control Module

The NPT-1300 platform is cooled through the FCU\_1300, a pluggable fan control module with six fans. The unit features enhanced PWM (Pulse Width Modulation), which helps optimizing the cooling efficiency and increases the fan operation life. The six fans in the FCU\_1300 are organized at the hardware level into two PWM groups. (The management software does, however, manage the FCU\_1300 as a single group.) By default, fan speed is controlled by SW according to the installed cards temperature, and "force turbo" is supported for maintenance purpose.

**i Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

### FCU\_1300 Front Panel



### FCU\_1300 Front Panel LEDs

Marking	Full Name	Color	Function
ACT.	System active	Green	Normally on when the fan unit is powered on. Off indicates a power failure of the fan unit.
FAIL	System fail	Red	Normally off. Lights when a fan failure is detected.
CLEAN FILTER	Filter status indicator	Yellow	Normally off. Lights steadily when the air filter must be cleaned or replaced.

## NPT-1300 Power Feed Subsystem

### Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. AC power feeding requires the use of a conversion module to implement AC/DC conversion.

### Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

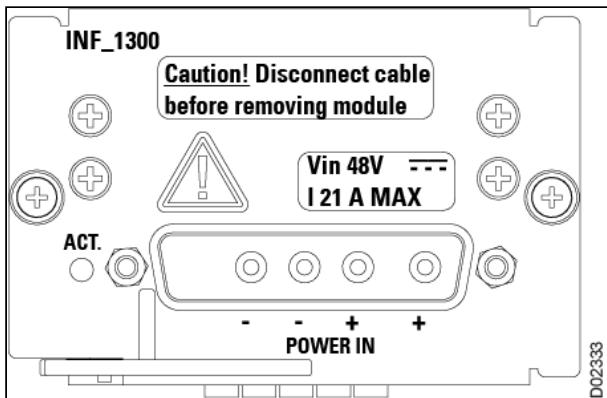
The NPT-1300 supports two [INF\\_1300](#) power supply cards, supporting 1+1 and 1+0 configuration.

## INF\_1300 Overview

The INF\_1300 is a DC power-filter module that can be plugged into the NPT-1300 or NPT-2300 platform. Two INF\_1300 modules are needed for power feeding redundancy. It performs the following functions:

- Single DC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Indication of input power loss and detection of under-/over-voltage
- digital monitoring for input voltage and current
- Shutting down of the power supply when under-/over-voltage is detected
- High-power INF for up to 1000 W

### INF\_1300 Front Panel



## NPT-1300 Switching Cards

The NPT-1300 platform operates with the following matrix card:

- **MCIPS1T**: Single switching card that provides dual stack packet switching (L2, L3, MPLS-TP, and IP/MPLS). Most convenient for applications that require very high volume of pure packet handling including support for dynamic L2/L3 VPN services. The card also supports 4 x 10 GE SFP+ based aggregation interfaces via corresponding ports.

NPT-1300 must be equipped with two matrix cards to support system redundancy. The following sections detail card functionality.

- MCIPS1T Switching Card
- MCIPS1T Functional Description

## MCIPS1T Switching Card

The MCIPS1T is a centralized dual stack packet switch designed for the NPT-1300, with MPLS-TP, IP/MPLS, L2VPN, and L3VPN capabilities, that provides 80/100/200GbE switch capacity per slot, supporting any-to-any direct data card connectivity, for efficient 100GbE connectivity to metro core platforms. This card includes a main controller processor (MCP), 920G central packet switch, EEC timing unit, IEEE 1588v2 timing unit, and 4 x 10GE SFP+ based aggregate ports.

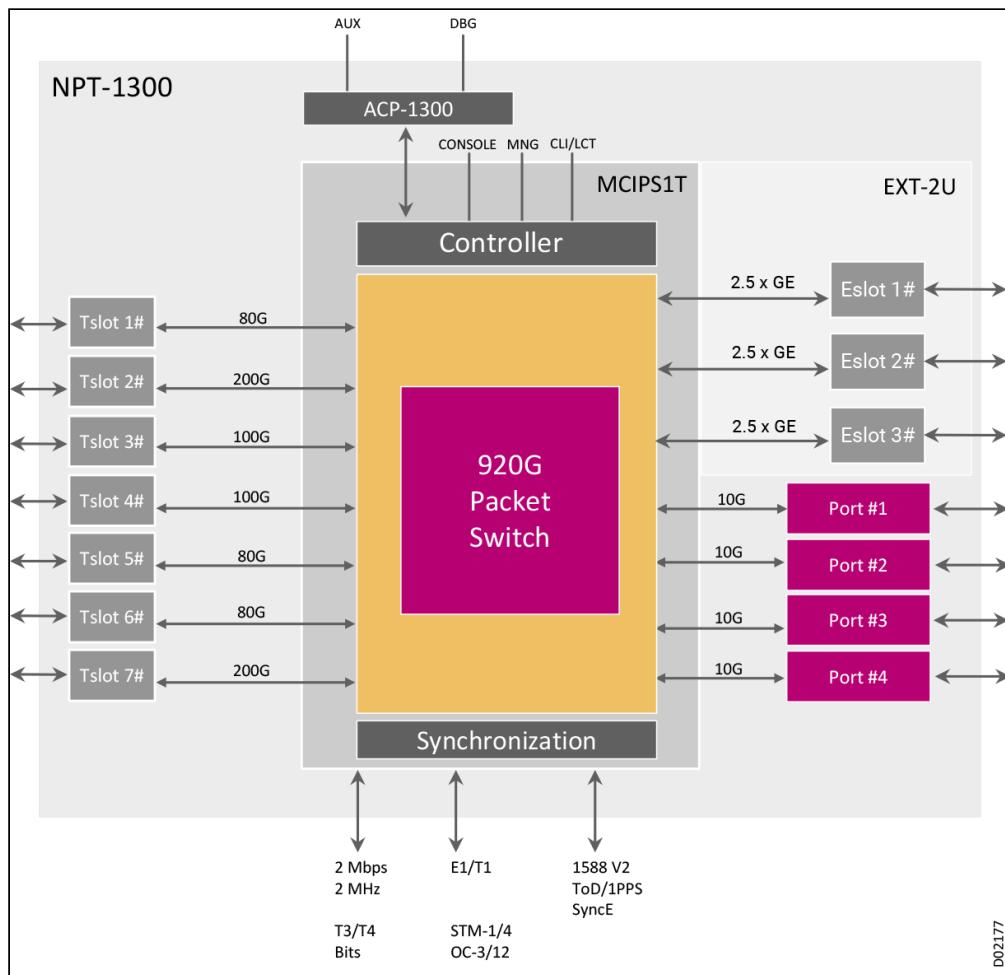
The MCIPS1T module includes three main subsystems:

- **MCP (Main Control Processor)**: Performs all integrated functions like control, communication, and overhead processing with a micro-SD based NVM.
- **CPS (Central Packet Switch)**: Performs all NPT-1300 packet switching operations.
- **TMU (Timing Unit)**: Generates and distributes timing and clock signals to all cards installed in the NPT-1300. In addition to its internal timing reference, the TMU can use up to four user-defined timing references.

The MCIPS1T is a critical NPT-1300 subsystem; therefore, two such cards must be configured in the NPT-1300 for redundancy. Both cards must be of the same type, and running the same software version. The two MCIPS1T modules operate in a primary-secondary configuration:

- At any time, only one card is active and the second is in stand-by.
- Upon failure or removal of the active card, the stand-by becomes active without any disruption in the system operation.

### MCIPS1T Functional Block Diagram



The total capacity of a platform using the MCIPS1T is 920G. The bandwidth is evenly distributed between the platform slots, with each slot accepting up to 80/100/200 Gbps.

The MCIPS1T offers a choice of capacity and configuration options, including:

- Ethernet packet switch, supporting native packet level switching with a 920G switching capacity and up to 800G traffic management (packet processing), providing:
  - Non-blocking data switch fabric for Ethernet/MPLS-TP and IP/MPLS traffic forwarding
  - Management and internal control in addition to user traffic switching
  - Both redundant and non-redundant modes
- Traffic management including:
  - Guaranteed CIR
  - 8 x CoS for differentiated services
  - End-to-end flow control
- Any card installed in any slot
- Any slot to any slot connectivity
- 4 x 10 GbE SFP+ based interfaces with OTN framing for FEC/E FEC
- OTSOP16 Smart SFP supported in SFP+\_10GE ports
- 25G interfaces
- Comprehensive range of timing and synchronization capabilities
  - G.781/G.8262 compliant EEC
  - 1PPS and ToD interfaces
  - IEEE 1588v2 PTP with OC (primary & secondary), BC, One-step TC, and G.8275.1 profile

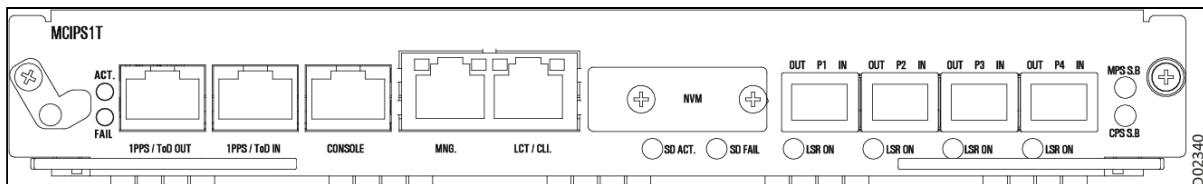
- G8273.2 Class B
- High capacity backplane connectivity for 100/200GBE interfaces, with up to 6 x 100G in a single platform
- Main control processing unit and built-in NVM (micro-SD card)
- Supports local management via CLI
- L3 VPN and IP/MPLS features:
  - VRF support:
    - ACL + L3 classification
    - uRPF
    - Multi-VRF networking stack
  - BGP (iBGP & eBGP):
    - AF ipv4
    - AF vpng4
    - Graceful restart
    - BFD support
  - L3VPN extension over static PW (PW-HE)
  - PE-CE protocols:
    - Static
    - eBGP
  - VRRP
  - IP multicast:
    - IPV4 multicast with PIM and IGMP
  - DHCP:
    - DHCP Relay (to connect hosts to DHCP server via L3 VPN)
    - Multi hop IP-BFD
- NETCONF interface
- Continuous and periodic PM counters
- Syslog report generation support
- Built-in Y.1564 Service Activation Test and loop back with MAC swap
- Switchover performance less than 50 msec on protection switchover due to MCIPS1T equipment failure (in the data path), plug-out, or manual command.

**i Optional Feature:**

MCIPS1T matrix is available in two variants: default switching capacity (500G) and full switching capacity (960G); it is possible to unlock the default capacity limit to utilize full capacity with a software license.

## MCIPS1T Functional Description

### MCIPS1T Front Panel



**MCIPS1T Front Panel Interfaces**

<b>Marking</b>	<b>Interface Type</b>	<b>Function</b>
1PPS/ToD OUT	RJ-45 connector	1PPS and Time of Day output interface per IEEE 1588v2 standard. This is the output of the PTP OC secondary or G.8275.1 T-BC clock.
1PPS/ToD IN	RJ-45 connector	1PPS and Time of Day input interface. This is the input for the grandmaster (T-GM) or T-BC when APTS is enabled.
CONSOLE	RJ-45 connector	Serial RS-232 communication port for use by technical support personnel (debug, maintenance, etc.).
MNG	RJ-45 connector	10/100/1000BaseT Ethernet interface for out-of-band management.
LCT/CLI	RJ-45	Local Management interface for connecting to an LCT or CLI.
P1 to P4	SFP+	4 x SFP+ (10G) ports.

### MCIPS1T Indicators and Functions

Marking	Full Name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the CIPS1T not downloaded successfully or that the CIPS1T cannot be controlled normally by the MCP1800. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the CIPS1T card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STB.	System standby	Orange	Lights when the card is in standby. Off when the card is active.
LSR ON (separate LED for each port)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## NPT-1300 Tslot IO Modules

The NPT-1300 has seven Tslots for installing I/O modules. The following table lists the different types of CES and Ethernet I/O modules that can be installed in the NPT-1300, with links to each module listed.

**i Note**

No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by the NPT-1300:

- 6 x 100GE
- 56 x 10GE
- 140 x 1GE

**NPT-1300 Supported Tslot Modules**

Description	Card	Tslots
CES multiservice module with 3 x DS3 interfaces and 1 x one STM-1/OC3 interface	<a href="#">MS345_3</a>	TS1-TS7
CES multiservice module with 24 x DS3 interfaces	<a href="#">MS345_24</a>	TS1-TS7
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	<a href="#">MSC_2_8</a>	TS1-TS7
CES multiservice module with 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<a href="#">MS1_4</a>	TS1-TS7
CES multiservice module with 32 x E1/T1 interfaces  <b>Note:</b> Protection available through <a href="#">TP32_2</a> module installed in EXT-2U expansion unit	<a href="#">MSE1_32</a>	TS1-TS7
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4E</a>	TS1, TS5, TS6
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4EB</a>	TS1-TS7
Optical 8 x GE interface module with direct connection to the packet switch	<a href="#">DHGE_8</a>	TS1, TS5, TS6
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	<a href="#">DHGE_8S</a>	TS2-TS4, TS7
Optical 10 x GE module with direct connection to the packet switch	<a href="#">DHGE_10</a>	TS1-TS7
Electrical and optical 16 x GE interface module with direct connection to the packet switch	<a href="#">DHGE_16</a>	TS1&TS2, TS6&TS7
Optical 20 x GbE interface module with direct connection to the packet switch	<a href="#">DHGE_20</a>	TS1-TS7
Optical 24 x GE interface module with direct connection to the packet switch	<a href="#">DHGE_24</a>	TS1&TS2, TS6&TS7

Description	Card	Tslots
Optical 2 x 10GE interface module with direct connection to the packet switch	DHXE_2	TS1-TS7
Optical 4 x 10GE interface module with direct connection to the packet switch	DHXE_4	TS1-TS7
Optical 4 x 10GE/OTU-2 interface module with direct connection to the packet switch with OTN wrapping	DHXE_4O	TS1-TS7
40G MACsec card with: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 10G/1GE multi-rate ports</li></ul> All 4 ports support MACsec capability.	DHXE_4sec	TS1-TS7
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces All 4 ports support MACsec capability	DHXE_4MRsec	TS1-TS7
Optical 8 x 10GE interface module with direct connection to the packet switch	DHXE_8	TS1-TS2, TS5-TS7
Optical 100GE/OTU-4 CFP interface module with direct connection to the packet switch	DHCE_1C	TS2-TS4, TS7
Optical 100GE combo CFP2 or QSFP28 interface module with direct connection to the packet switch	DHCE_1	TS2-TS4, TS7
Optical 100GE QSFP28 interface module with direct connection to the packet switch	DHCE_1Q	TS2-TS4, TS7
Optical 100GE QSFP28/QSFP_DD interface module with direct connection to the packet switch	DHCE_1QB/1QC	TS2-TS4, TS7
Optical 2 x 100GE interface module (one QSFP28 port and one CFP2 port) with direct connection to the packet switch	DHCE_2	TS2, TS7
Optical 2 x 200GE QSFP_DD interface module with direct connection to the packet switch	DHCE_2Q	TS2-TS4, TS7

Description	Card	Tslots
100G card that supports up to 4 x 10GE/25GE (based on SFP+), as well as 5G time stamping accuracy	DH25_4MR	TS2, TS3, TS4, TS7

## NPT-1300 Expansion Platform

The traffic capabilities of the Neptune platform can be expanded by installing an expansion unit on top (EXT-2U or EXT-2UH). These are high density modular expansion units for the Neptune multiservice platforms. They support the complete range of CES, PCM, optics and Ethernet services. Integrating these add-on platforms into your network configuration is not traffic-affecting.

The EXT-2U/2UH are compact, versatile units that can be used with different base platforms from the Neptune product line. The type of traffic delivered by the unit depends on the type of matrix (PCM or Packet only) installed in the base unit. I/O expansion cards are supported in accordance. The expansion platforms have three multipurpose slots (ES1 to ES3) for any combination of extractable traffic cards. PCM, Ethernet, OTN muxponders, optical amplifiers, and CES traffic are all handled through cards in these traffic slots.

The following table lists the traffic cards supported in the EXT-2U/2UH when installed on the platform. For a detailed description of the expansion platform features, functionality, and supported traffic cards, see [EXT-2U](#) and [EXT-2UH Expansion Units](#).

### EXT-2U/2UH Supported Cards for NPT-1300

Card Type	Designation
Multiservice PCM and 1/0 XC card over Ethernet	<b>EM_10E / EM_10EB</b> <ul style="list-style-type: none"> <li>EM_10EB required for EXT-2UH</li> <li>Any card works for EXT-2U</li> </ul>
Optical Base Card (OBC) for optical amplifiers and DCM modules	<b>Optical Base Card</b> <ul style="list-style-type: none"> <li>OBC with EXT-2U</li> <li>OBC_B/OBC_C with EXT-2U or EXT-2UH</li> </ul>
10G card with up to 10 GbE ports; 4 of the ports support POE++	DHGE_10_POE
Protection card, provides 1:2 protection for MSE1_32 cards installed in base platform	TP32_2
Protection card, provides 1:1 protection for MS345_3 cards installed in base platform	TPS345_1
CES multiservice card with 2 x STM-1/OC-3 and 16 x E1/T1 interfaces	MSC_2_16E

# NPT-1250 System Architecture

## NPT-1250 Platform



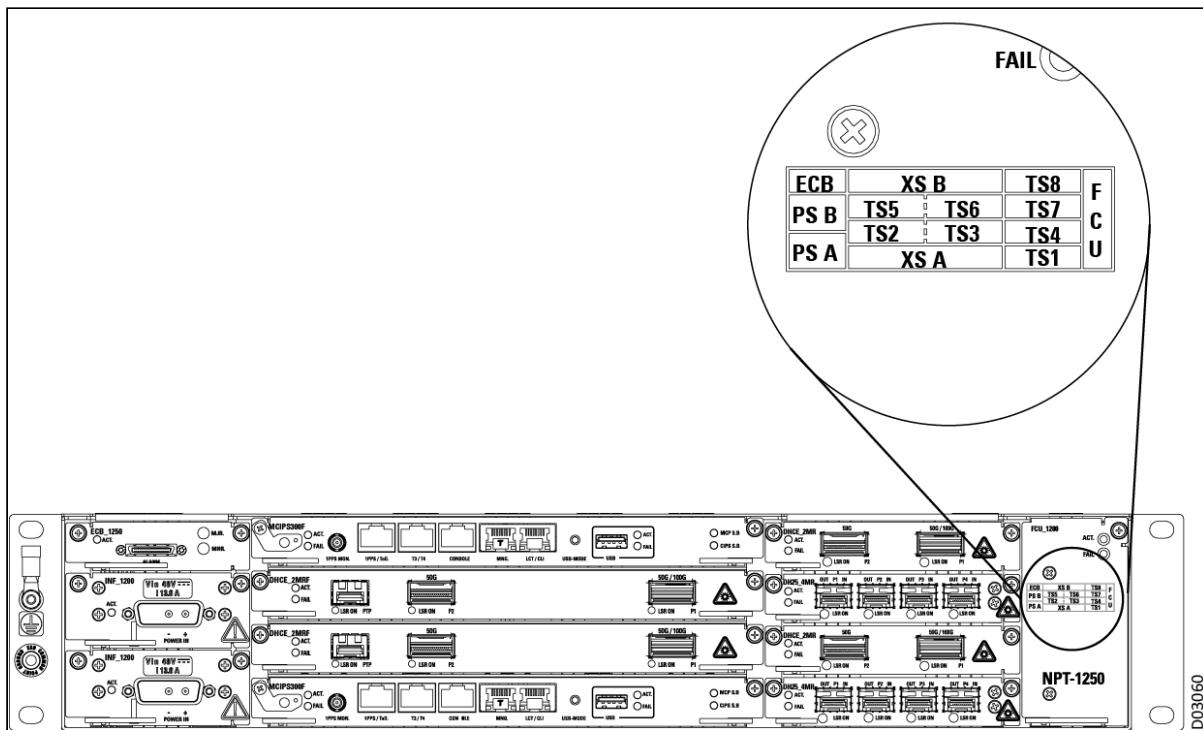
The NPT-1250 is based on a modular architecture, with full redundancy (switch, controller, power, fans) for high resiliency. The platform is designed around a centralized switching card that supports any-to-any direct data card connectivity. Various hardware variations of the MCIPS300F switching card are available, offering different synchronization capabilities, tailored to the site's specific needs and requirements.

The NPT-1250 is a 2U base platform housed in a 88 mm high, 440 mm wide, and 243 mm deep (3.46 in. x 17.32 in. x 9.57 in.) equipment cage with all interfaces accessible from the front of the unit. The platform offers:

- 2U-height packet transport aggregation, optimized for aggregation layer, cellular hub 3G, LTE, 5G RNC/SGW locations, and service provider hub sites
- Packet-based applications for optimized packet and CES handling
- Redundant switching cards for robust provisioning, supporting 300G processing capacity (TM), with packet switching up to 560G, and 200G FlexE.
- Ease of operation and cost reduction with ZTP (zero touch provisioning) and ZTI (zero touch installation).
- 8 I/O card slots, for processing a comprehensive range of traffic interfaces.
  - Up to 4 x 100GE
  - 16 x 25G
  - 32 x 10GE OTN
  - 78 x 100/1000 BaseX (CSFP)
  - 2 x 100G FlexE double-slot cards
- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+\_10GE ports
- Controller function (as part of the MCIPS300F) that provides the following functionalities:
  - Alarm indications and monitoring
  - Management plane and management interfaces
- SDN interfaces (NETCONF/YANG)
- Traffic connector to the (optional) EXT-2UH/eEXT-2UH expansion unit
- Comprehensive range of timing and synchronization capabilities:
  - T3/T4 BITS (MCIPS300F, MCIPS300FH)
  - GNSS built-in receiver (MCIPS300FB, MCIPS300FBH)
  - 10MHz (MCIPS300FB, MCIPS300FBH)
  - SyncE
  - IEEE 1588v2 G.8275.1
  - IEEE 1588v2 G.8275.2 (MCIPS300FH, MCIPS300FBH)
  - G.8273.2 – Class C compliant
  - 1PPS and ToD
  - Hybrid 1588 and SyncE
  - APTS (MCIPS300FB, MCIPS300FBH)
- Power supply, available in two modes:
  - -48 VDC power feed configured in two power supply module slots for external power line connection, with a dual power feed for redundancy

- 110-230 VAC power feed utilizes an external AC power line connection. One AC module can be installed in the NPT-1250

### NPT-1250 Front Panel Layout



The NPT-1250 can be installed in 2,200 mm or 2,600 mm ETSI racks or in 19" racks. Typical power consumption for the NPT-1250 is less than 300 W. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

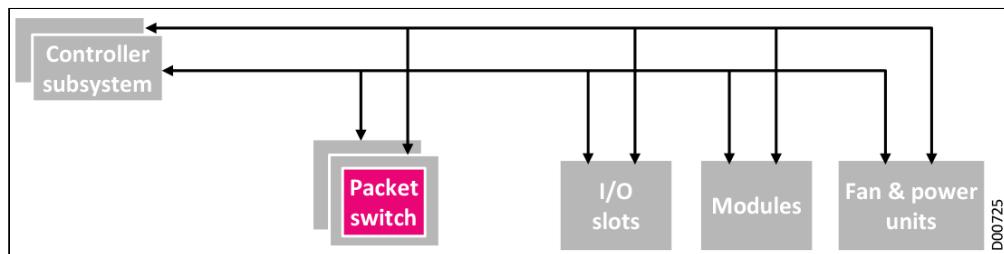
For a complete list of the modules that can be configured in each NPT-1250 slot, see [NPT-1250 Tslot IO Modules](#). All cards support live insertion. All cards are connected using a backplane that supports one traffic connector to connect the NPT-1250 and the EXT-2UH. The NPT-1250 platform provides full 1+1 redundancy in power feeding, packet switching, and the TMU, as well as 1:N redundancy in the fans.

This section introduces the following NPT-1250 features:

- [NPT-1250 Control Subsystem](#)
- [NPT-1250 Communications with External Equipment and Management](#)
- [NPT-1250 Timing](#)
- [NPT-1250 Cooling Subsystem](#)
- [NPT-1250 Power Feed and Alarm Subsystems](#)
- [NPT-1250 Switching Cards](#)
- [NPT-1250 Tslot IO Modules](#)
- [NPT-1250 Expansion Platforms](#)

## NPT-1250 Control Subsystem

### Controller Subsystem



NPT-1250 control and communication functions include:

- Internal control and processing
- Communication with external equipment and management
- Network element (NE) software and configuration backup
- Built-in Test (BIT)

### Software and Configuration Backup

The platform features a large-capacity on-board NVM that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

### Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection
- Protection switch for the main switching card

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

## NPT-1250 Communications with External Equipment and Management

In the Neptune metro access platform product line, the main controller card is responsible for communicating with other NEs and management stations.

The main controller card communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems via the DCN. In-band Management Control Channel (MCC) is supported in the platforms as well, enabling NE management through in-band channels.

### Usage Guidelines

The NPT-1250 supports in-band and management communication on the following interfaces:

- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- In-band management processing (20Mbps)
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-IS v6, static routes

## NPT-1250 Timing

The NPT-1250 was designed as a 5G backhauling platform. As such, it provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations, such as 1588v2 PTP with G.8273.2 Class C support.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed redundantly from the TMUs to all traffic and matrix cards, minimizing unit types and reducing operation and maintenance costs.

The TMU and the internal and external timing paths are fully redundant. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem. In case of hardware failure, the redundant synchronization subsystem takes over the timing control with no traffic disruption.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- 1PPS and ToD interfaces, using external timing input sources
- 1PPS monitoring point
- 2 x 2048K/1544K Hz, E1/T1 (T3/T4) external timing input/output sources (MCIPS300F, MCIPS300FH)
- NTP support (NTPv1, NTPv2, NTPv3, and NTPv4)
- E1/T1 interfaces of CES cards
- STM-1/4 of CES cards
- GNSS built-in receiver (MCIPS300FB, MCIPS300FBH)
- 10MHz (MCIPS300FB, MCIPS300FBH)
- Local interval clock
- Holdover mode
- SyncE
- 1588v2 - Primary, Secondary, transparent, and boundary clock
- Hybrid 1588 and SyncE
- APTS (MCIPS300FB, MCIPS300FBH)

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization over GbE/10GbE/100GbE and FlexE interfaces. Our implementation is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262.1, G.8263, and G.8264.

The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to

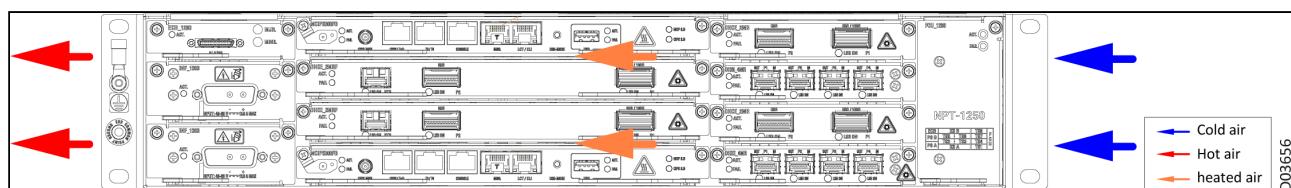
synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. PTP IEEE 1588v2 is supported in two profiles; full network timing support (G.8275.1) and partial network timing support (G.8275.2, MCIPS300FH and MCIPS300FBH), providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <10ns (G.8273.2 Class C) timing error per NE. PTP is supported over GbE/10GbE/100GbE and FlexE interfaces.

## NPT-1250 Cooling Subsystem

The NPT-1250 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components, and cools them.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

### Airflow in the NPT-1250



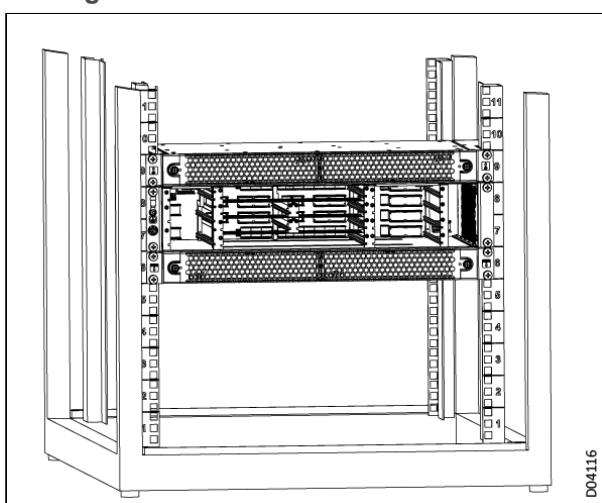
### Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The NPT-1250 platform can be configured together with air baffle units, installed in either a 19" or 23" rack.

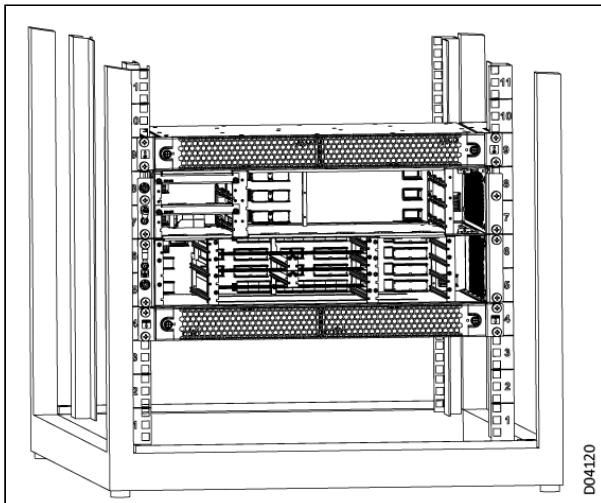
- In the 19" rack, the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* the NPT-1250 platform, and one located directly *above* the NPT-1250 platform. The platform and two-part air baffle unit together occupy a total space of 4U height in the rack. The air baffle unit should be installed *before* the NPT-1250 platform; the NPT-1250 platform is then inserted into the gap space between the air-flow boxes. See the *NPT-1250 Installation and Maintenance Manual* for installation procedure details and limitations.

### 2U Height Platform Installed in 19" Rack Between Two Air-Flow Boxes



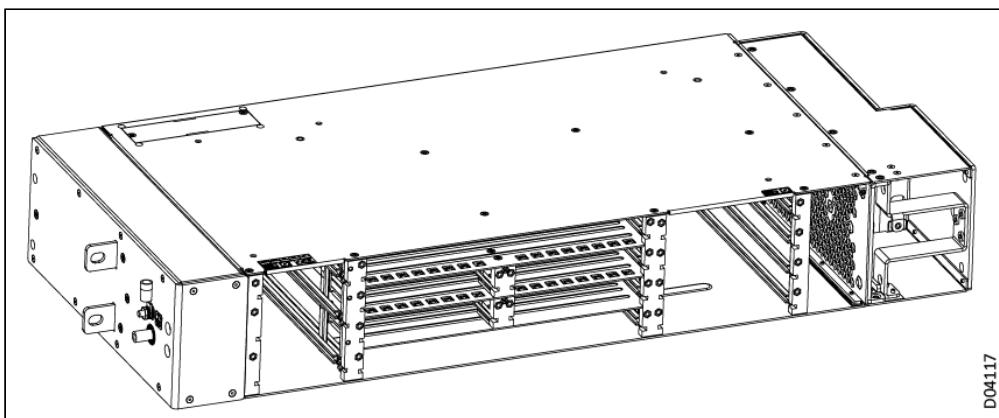
- In the 19" rack, if the NPT-1250 platform is configured with an EXT-2UH expansion unit, the EXT-2UH unit is located directly above the NPT-1250 platform. The air baffle unit is installed in the rack first; one 1U air-flow box is located directly *below* where the NPT-1250 platform will sit, and the second 1U air-flow box is located directly *above* where the EXT-2UH expansion platform will sit. The combined platform and expansion unit are then installed in the rack between the two air-flow boxes. The combination of NPT-1250 platform with EXT-2UH unit and two-part air baffle unit occupies a total space of 6U height in the rack.  
When installing the NPT-1250 platform together with an EXT-2UH expansion unit and air baffles, the internal air filters in the EXT-2UH unit must be removed. External air filters are available; see the *NPT-1250 Installation and Maintenance Manual* for details.

## 2U Height Platform Plus Expansion Unit Installed in 19" Rack Between Two Air-Flow Boxes



- In the 23" rack, the air baffle unit is installed as 2 2U air ducts placed to the right and left sides of the NPT-1250 platform, requiring a total space of 2U height to be available in the rack, since the air ducts don't add anything to the platform height.

## 2U Height Platform Installed with Air Baffle Unit in 23" Rack



- In the 23" rack, if the NPT-1250 platform is configured with an EXT-2UH expansion unit, then a second set of 2U air ducts is installed on either side of the EXT-2UH expansion platform. The combination of NPT-1250 platform with EXT-2UH unit and 2 sets of 2U air ducts requires a total space of 4U height to be available in the rack, since the air ducts don't add anything to the platform height.

## FCU Fan Control Module

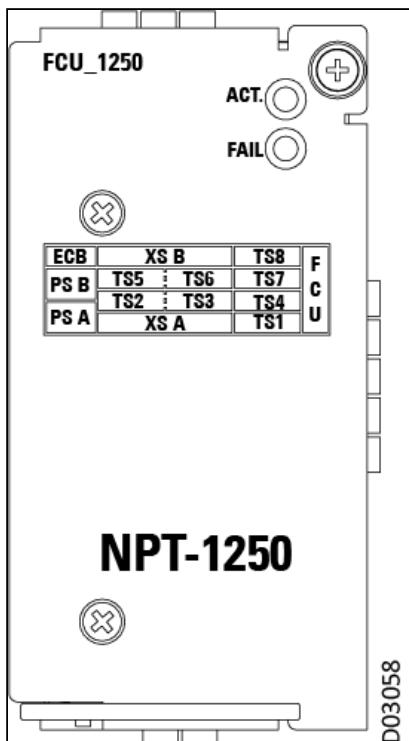
The NPT-1250 platform is cooled through the FCU\_1250, a pluggable fan control module with eight fans. The unit features enhanced PWM (Pulse Width Modulation), which helps optimize fan cooling efficiency and increase fan operation life. PWM technology enables effective cooling at lower fan speeds, thereby

improving fan effectiveness while reducing operating noise in room temperature conditions. By default, fan speed is controlled by SW according to the installed cards temperature, and "force turbo" is supported for maintenance purpose.

**i Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

### FCU\_1250 Front Panel



### FCU\_1250 Front Panel Indicators

Marking	Description	Color	Function
ACT.	System active	Green	Normally on when the fan unit is powered on. Off indicates a power failure of the fan unit.
FAIL	System fail	Red	Normally off. Lights when a fan failure is detected.

# NPT-1250 Power Feed and Alarm Subsystems

## Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. Alternatively, a single AC power feed can be used.

The electrical connection board ([ECB\\_1250](#)) houses the external alarm connector. This module is integrated in the NPT-1250 platform and is included by default.

## Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-1250 offers two power supply modes.

- -48 VDC power feed ([INF\\_1200](#)) configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- 100-240 VAC power source ([AC\\_PS-1200](#)) utilizes an external power line connection through a power conversion module to implement AC/DC conversion.

# INF\_1200 Overview

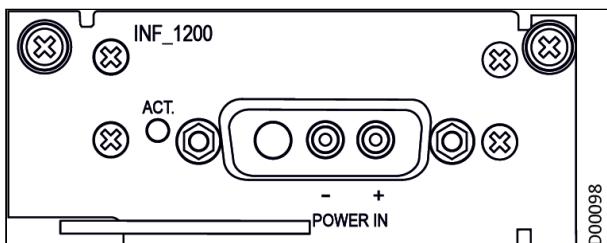
## Description

The INF\_1200 is a DC power-filter module that can be plugged into the NPT-1250 platform. Two INF\_1200 modules are needed for power feeding redundancy.

## Features

- Single DC power input and power supply for all modules in the NPT-1250
- Input filtering function for the entire NPT-1250 platform
- Adjustable output voltage for fans in the NPT-1250
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected
- High-power INF for up to 650W (INF\_1200 HW revision D02 and above)

## INF\_1200 Front Panel



## AC\_PS-1200 Overview

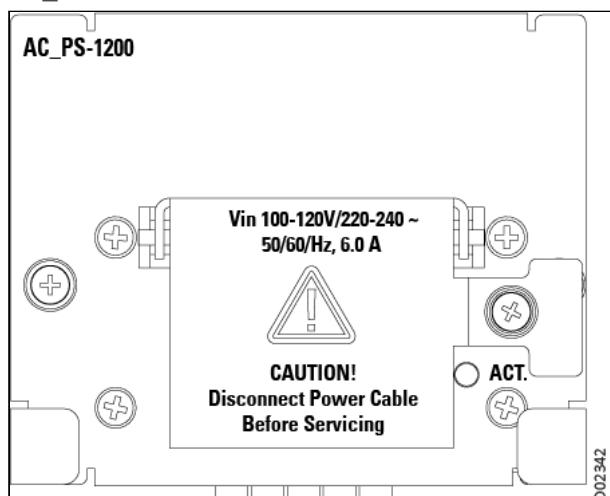
### Description

The AC\_PS-1200 is a 100-240 VAC power source utilizing an external power line connection through a power conversion module to implement AC/DC conversion.

### Features

- Single AC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- High-power AC power supply for up to 420W (100-120 VAC and 45°C (113°F) max working temperature) or 480W (220-240 VAC and 55°C (131°F) max working temperature)

### AC\_PS-1200 Front Panel

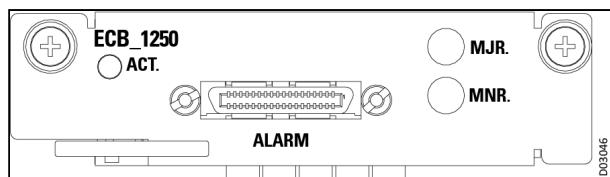


## ECB\_1250/1250B Overview

The electrical connection board ECB\_1250 houses the external alarm connector. This module is integrated in the NPT-1250 platform and is included by default.

The ECB\_1250B is a variant of the ECB\_1250 that supports all functionality of the ECB\_1250 with the addition of a built-in GNSS receiver, and an ANT coaxial interface on the front panel.

### ECB Front Panel



### ECB Front Panel Indicators

Marking	Interface Type	Function
ACT.	Green LED	Indicates that the ECB card is powered and operating normally.
MJR	Red LED	Indicates the NE level alarming status. On if NE has critical or major alarms. Off if NE has no critical/major alarm.
MNR	Yellow LED	Indicates the NE level alarming status. On if NE has minor alarm but without critical/major alarms; highest severity of NE alarms is minor. Off if NE highest alarm severity is not minor.

## NPT-1250 Switching Cards

The NPT-1250 architecture enables its outstanding configuration flexibility. At the heart of the NPT-1250 is a non-blocking switching fabric. The main processing card **MCIPS300F** integrates functions such as control, communications, timing, and overhead processing, in addition to the essential packet switching capabilities. This section introduces the following features:

- [MCIPS300Fx Family of Switching Cards](#)
- [MCIPS300Fx Functional Description](#)

### MCIPS300Fx Family of Switching Cards

The MCIPS300Fx packet switching cards are designed for use in the NPT-1250 platform. MCIPS300Fx switch cards are native Ethernet and FlexE packet switches, supporting native packet-level switching.

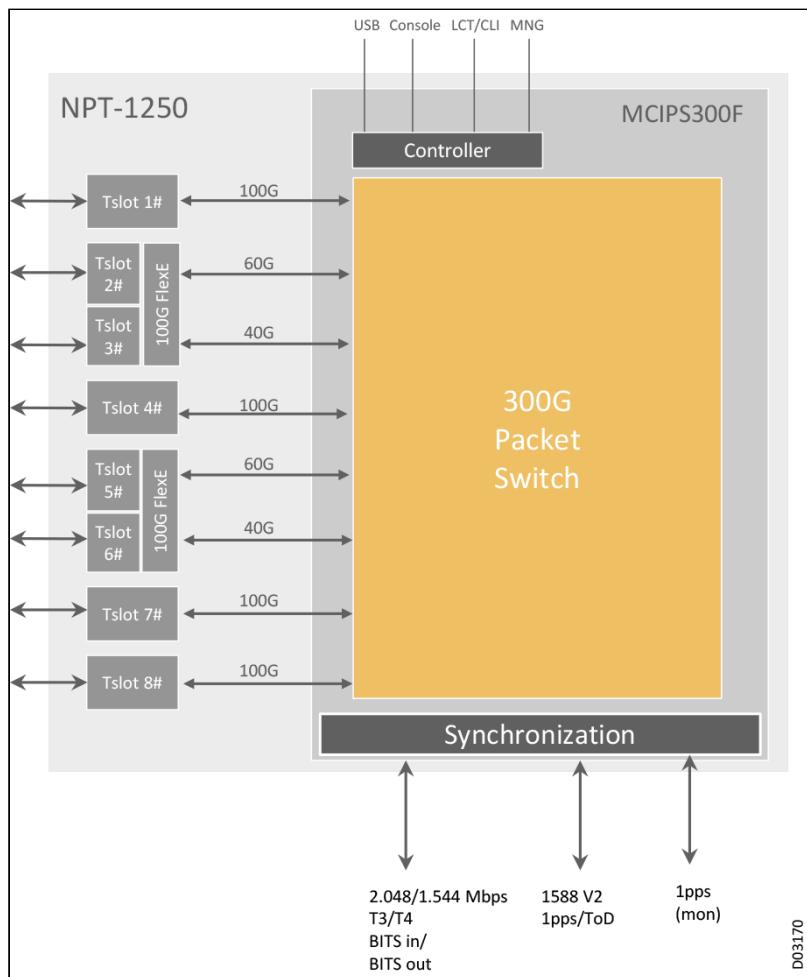
MCIPS300Fx cards represent a family of MCIPS300F cards, including MCIPS300F, MCIPS300FH, MCIPS300FB, and MCIPS300FBH card variants. The different MCIPS300Fx cards variants support the same functionality as the basic MCIPS300F card, with slightly different timing/synchronization support; specific capabilities are identified in the following feature list.

Bandwidth is evenly distributed between the 8 platform slots. 4 slots support 40G/100G dynamic capacity allocation, and the remaining 4 slots support up to 40G per slot for Ethernet or 100G of FlexE per double slot. The MCIPS300Fx cards provide the following main functions:

- All Native Ethernet packet switch, supporting native packet-level switching with:
  - Management and internal control
  - User traffic switching
  - Non-blocking data switch fabric up to 300G processing capacity (IMIX)
  - 560G packet switching (port fan-out) capacity (for Ethernet-only configurations)
  - 200G FlexE
  - Up to 600G fan-out capacity when 200G utilized by FlexE, with up to 400G additional packet switching (port fan-out) available
  - Both redundant and non-redundant modes
- 5G-ready packet transport, including:
  - Hard (FlexE) and soft (enhanced VPN and segment routing) network slicing
  - Ultra-low latency (ULL) support, with deterministic pass-through FlexE channels
  - Stringent phase synchronization requirement for Class C timing accuracy compliance (8273.2)

- 25G interfaces
- Comprehensive range of timing and synchronization capabilities (G.781/G.8262 compliant EEC, G.8273.2):
  - T3/T4 BITS (MCIPS300F, MCIPS300FH)
  - GNSS built-in receiver (MCIPS300FB, MCIPS300FBH)
  - 10MHz (MCIPS300FB, MCIPS300FBH)
  - SyncE
  - 1PPS and ToD
  - Hybrid 1588 and SyncE
  - APTS (MCIPS300FB, MCIPS300FBH)
  - IEEE 1588v2 PTP with:
    - OC (master & slave), BC
    - One-step TC
    - G.8275.1 profile
    - G.8275.2 (MCIPS300FH, MCIPS300FBH)
    - G8273.2 Class C timing accuracy compliance (10ns)
- Traffic management (TM) including:
  - Guaranteed CIR
  - E2E flow control
  - 8 x CoS for differentiated services
- Any-slot-to-any-slot connectivity

### 300G Packet Switching Card



## MCIPS300Fx Functional Description

The MCIPS300Fx card has three main subsystems:

- **Main processing and control:** Performs all integrated functions like control, communication, and overhead processing.
- **Central packet switch:** Performs all the NPT-1250 packet switching operations.
- **TMU:** Generates and distributes timing and clock signals to all the cards installed in the NPT-1250 platform. In addition to its internal timing reference, the TMU can use up to four user-specified reference sources. See Timing for a description of the TMU capabilities.

The MCIPS300Fx card is a critical NPT-1250 subsystem, and therefore, for redundancy purposes, two MCIPS300Fx cards should be installed in any NPT-1250 platform, one on each side of the cards cage. Both cards must be of the same type and configuration and running the same NPT-1250 release version.

When two identical cards are installed in the platform, the cards operate in a primary-secondary configuration:

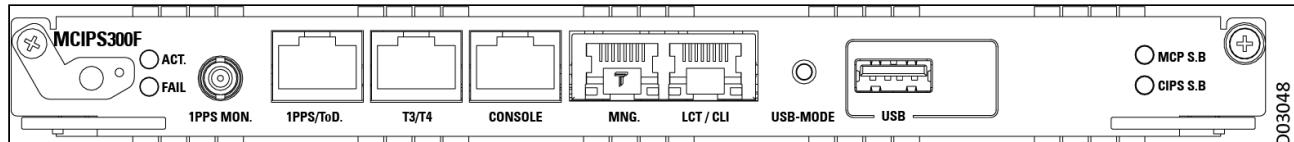
- At any time, only one card is active and the other is in standby.
- Upon failure or removal of the active card, the standby card becomes active without any disruption in system operation.

A MCIPS300Fx card can be inserted and replaced without affecting traffic flow.

**Note**

During an upgrade, a different card version or release can be installed in the platform. With appropriate planning, the upgrade can be non-traffic-affecting.

**MCIPS300F Front Panel**



**MCIPS300F Front Panel Interfaces**

Marking	Interface Type	Function
1PPS MON.	Coaxial connector	1588v2 1PPS monitoring port
1PPS/ToD	RJ-45	1PPS and Time of Day input/output signals supporting Ethernet timing per IEEE 1588v2 standard
T3/T4	RJ-45	T3 and T4 timing interfaces (2048K/1544K Hz, E1/T1)
CONSOLE	RJ-45	Console interface (RS232)
MNG.	RJ-45	10/100/1000BaseT Ethernet interface for management
LCT/CLI	RJ-45	10/100/1000BaseT local management port for connecting an LCT or CLI station
USB	USB 2.0	Maintenance operations and ZTI functionality

**MCIPS300F Indicators and Functions**

Marking	Full Name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the card can't be downloaded successfully or that the card cannot be controlled normally. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the MCIPS300F card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
MCP S.B	MCP system standby	Orange	Lights when the card is in standby. Off when the card is active.
CIPS S.B	CIPS system standby	Orange	Lights when the card is in standby. Off when the card is active.

## NPT-1250 Tslot IO Modules

The NPT-1250 has eight Tslots for installing I/O modules. The following table lists the different types of Ethernet, FlexE, and CES I/O modules that can be installed in the NPT-1250, with links to each module listed.

 **Note**

No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by the NPT-1250:

	Max 1GE ports	Max 10GE ports	Max 25GE ports	Max 100GE ports	Max 100G FlexE ports
With MCIPS300F	78	32	16	4	2

**NPT-1250 Supported Tslot Modules**

Description	Card	Slots in NPT-1250
CES multiservice module with 3 x DS3 interfaces and 1 x STM-1/OC3 interface (future)	<a href="#">MS345_3</a>	TS1-TS8
CES multiservice module with 24 x DS3 interfaces	<a href="#">MS345_24</a>	TS1-TS8
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	<a href="#">MSC_2_8</a>	TS1-TS8
CES multiservice module with 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<a href="#">MS1_4</a>	TS1-TS8
CES multiservice module with 32 x E1/T1 interfaces	<a href="#">MSE1_32</a>	TS1-TS8
Optical 100GE QSFP28 interface module with direct connection to the packet switch	<a href="#">DHCE_1Q</a>	TS1, TS4, TS7, TS8
Optical 100GE QSFP28/QSFP_DD interface module with direct connection to the packet switch	<a href="#">DHCE_1QB/1QC</a>	TS1, TS4, TS7, TS8
Optical 100G FlexE double-slot module with direct connection to the packet switch	<a href="#">DHCE_2MRF</a>	Tslot pairs: TS2+TS3 and TS5+TS6
100G card that supports up to 4 x 10GE/25GE (based on SFP+), as well as 5G time stamping accuracy	<a href="#">DH25_4MR</a>	TS1, TS4, TS7, TS8
40G card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces	<a href="#">DHXE_4MR</a>	TS1-TS8
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces  All 4 ports support MACsec capability	<a href="#">DHXE_4MRsec</a>	TS1-TS8

Description	Card	Slots in NPT-1250
40G MACsec card with: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 10G/1GE multi-rate ports</li></ul> All 4 ports support MACsec capability, as well as 5G time stamping accuracy when installed in NPT-1250	DHXE_4sec	TS1-TS8
Optical 4 x 10GE/OTU-2 interface module with direct connection to the packet switch with OTN wrapping	DHXE_4O	TS1-TS8
Optical 4 x 10GE interface module with direct connection to the packet switch	DHXE_4	TS1-TS8
Optical 2 x 10GE interface module with direct connection to the packet switch	DHXE_2	TS1-TS8
Optical 10 x GE module with direct connection to the packet switch	DHGE_10	TS1-TS8
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	DHGE_8S	TS1-TS8
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	DHGE_4EB	TS1-TS8

## NPT-1250 Expansion Platforms

The traffic capabilities of the NPT-1250 platform can be expanded by configuring the base platform with an EXT-2UH/eEXT-2UH expansion unit.

The EXT-2UH platform is a high density modular expansion unit for the Neptune multiservice platforms. It supports the complete range of CES, PCM, optics, and Ethernet services. The EXT-2UH platform has a high-speed connector enabling 10G connectivity to the base platform, enabling a significant increase in the GbE fan out when configured with the DHGE\_10\_POE cards. Integrating this add-on platform into your network configuration is not traffic-affecting. The EXT-2UH is compact and versatile and can be used with different base units from the Neptune product line. The type of traffic delivered by the unit depends on the type of matrix (PCM or Packet only) installed in the base unit. I/O expansion cards are supported in accordance. The EXT-2UH has three multipurpose slots (ES1 to ES3) for any combination of extractable traffic cards. PCM, Ethernet, OTN muxponders, optical amplifiers, and CES traffic are all handled through cards in these traffic slots.

The eEXT-2UH is an independent 2U platform that provides 3 I/O slots for TP cards, optical amplifiers, PCM services (with EM\_10E), and GbE fan out (with DHGE\_10\_POE). For example, adding the eEXT-2UH expansion unit to an NPT-1800 platform that is already using an EXT-2U unit would provide more slots for TP protection cards, doubling the amount of E1 protection available, which is an essential feature for large-scale aggregation sites.

The following table lists the traffic cards supported in the EXT-2UH or eEXT-2UH when installed with the base platform. For a detailed description of the EXT-2UH and eEXT-2UH features, functionality, and supported traffic cards, see [EXT-2U and EXT-2UH Expansion Units](#) or [eEXT-2UH Expansion Unit](#).

#### EXT-2UH Supported Cards for NPT-1250

Card Type	Designation
Multiservice PCM and 1/0 XC card over Ethernet. (Can be used in both EXT-2UH and eEXT-2UH platforms.)	<a href="#">EM_10EB</a>
Optical Base Card (OBC) for optical amplifiers and DCM modules. (OBC_B, OBC_C) (Can be used in both EXT-2UH and eEXT-2UH platforms.)	<a href="#">Optical Base Card</a>
10G card with up to 10 GbE ports; 4 of the ports support POE+. (Can be used in both EXT-2UH and eEXT-2UH platforms.)	<a href="#">DHGE_10_POE</a>
Protection card, provides 1:2 protection for MSE1_32 cards installed in base platform. (Can be used in both EXT-2UH and eEXT-2UH platforms.)	<a href="#">TP32_2</a>
Protection card, provides 1:1 protection for MS345_3 cards installed in base platform.	<a href="#">TPS345_1</a>
CES multiservice card with 2 x STM-1/OC-3 and 16 x E1/T1 interfaces.	<a href="#">MSC_2_16E</a>

# NPT-1200 System Architecture

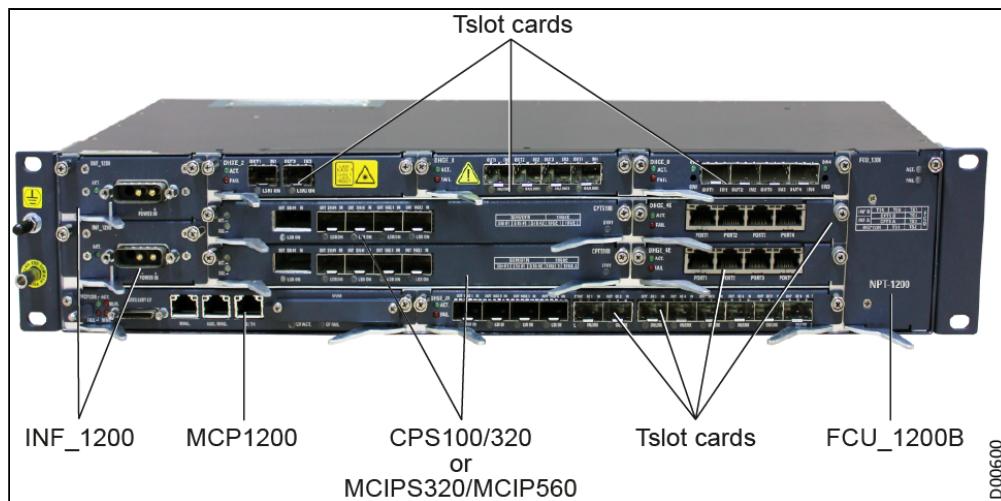
The NPT-1200 is a compact packet platform specially optimized for metro-access and access, RAN cellular networks, service providers, and utilities. This fully modular redundant converged multiservice packet transport platform offers a solution that optimizes packet handling. NPT-1200 integrates advanced Carrier-class Ethernet based services (L1, L2, MPLS-TP, IP/MPLS, and L3VPN) with PCM and optics capabilities into a 2U unit.

The NPT-1200 is a cost-effective choice for second and third level aggregation, geared for cellular hub locations (3G, 4G, LTE, and RNC), providing a unique solution for high capacity access rings, and optimized for popular triple play applications. Used in many sub network topologies, NPT-1200 can handle a mixture of P2P, hub, and mesh traffic patterns. This combined functionality means that operators benefit from improved network efficiency and significant savings in terms of cost and footprint.

The NPT-1200 is designed around a centralized switching card that supports any-to-any direct data card connectivity. The platform can be configured with either CPS100, CPS320, or MCIPS320/560 switching card. The configuration is tailored to the site's specific needs and requirements. The main functional subsystems of the NPT-1200 are:

- **Traffic processing:** I/O cards, and matrix cards for packet switching (CPS/MCIPS)
- **Timing and synchronization:** In the CPS/MCIPS cards
- **Control and communication:** In the MCP1200 and MCIPS320/560
- **Power feed:** Including local power supply circuits on each card and INF\_1200 units
- **Cooling fans:** In the FCU\_1200 unit

## NPT-1200 Platform



The NPT-1200 is a 2U base platform housed in a 88 mm high, 440 mm wide, and 243 mm deep (3.46 in. x 17.32 in. x 9.57 in.) equipment cage with all interfaces accessible from the front of the unit. The platform includes:

- Two slots for redundant switching cards (CPS100/320 or MCIPS320/560, in slots XSA and XSB) for robust provisioning of the following functionalities:
  - Packet processing up to 320G/560G
  - 2/4 SFP+ based 10GbE interfaces on packet switch
  - Comprehensive range of timing and synchronization capabilities (T3/T4, ToD, and 1pps)
- One slot for a controller card (MCP1200, in slot MS) that provides the following functionalities:
  - Alarm indications and monitoring
  - In-band management interfaces (MCC and VLAN)
  - NE management and control
  - T3/T4 synchronization interfaces

- Six I/O card slots (TS1-TS7) with a capacity of 20G/40G per slot. Four slots offer a capacity of 100GE when the platform is configured with the MCIPS560. Ideal for processing a comprehensive range of traffic interfaces, including Ethernet Layer2/MPLS, Layer3, and IP/MPLS.
- Compact flash/SD card (NVM)
- Two power-supply module slots (INF\_1200 or AC\_PS-1200, in slots PSA and PSB)
- Traffic connector to the (optional) EXT-2U expansion unit with additional three slots
- Comprehensive range of timing and synchronization capabilities (SyncE, 1588v2, G.8275.1, BITS, ToD, and 1pps)
- L1, L2, MPLS-TP, IP/MPLS, and L3VPN service support
- Aggregates traffic arriving over Ethernet, PCM low-bitrate interfaces, E1/T1 and STM-1, directly over GbE/10GbE/100GbE
- TDM by CES - SAToP, CESoPSN, and CEP
- Dynamic BW allocation
- Very high redundancy due to double systems:
  - Two central switch cards
  - Two control and IP engine cards (with MCIPS320/560)
  - Two power supplies
  - Fans and control card

The NPT-1200 is fed from -48 VDC. Two INF\_1200 modules can be configured in two power supply module slots for redundant power supply. The AC\_PS-1200 module offers a 100-240 VAC power source option. The NPT-1200 can be installed in 2,200 mm or 2,600 mm ETSI racks or in 19" racks. Typical power consumption for the NPT-1200 is less than 500 W. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

#### NPT-1200 Slot Arrangement



For a complete list of the modules that can be configured in each NPT-1200 slot, see [NPT-1200 Tslot I/O modules](#). All cards support live insertion. All cards are connected using a backplane that supports one traffic connector to connect the NPT-1200 and the EXT-2U. The NPT-1200 platform provides full 1+1 redundancy in power feeding, packet switching, and the TMU, as well as 1:N redundancy in the fans.

This section introduces the following NPT-1200 features:

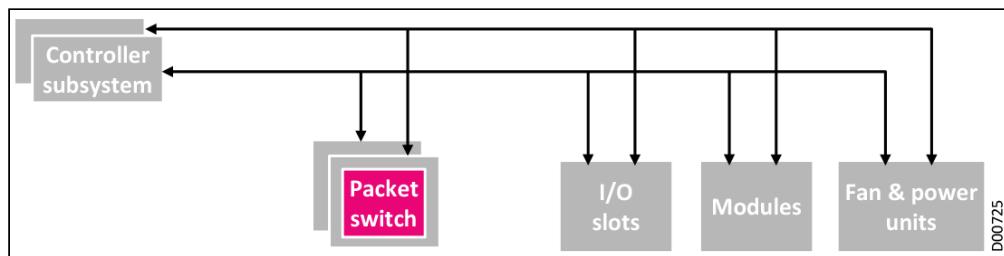
- [NPT-1200 Control Subsystem](#)
- [NPT-1200 Communications with External Equipment and Management](#)
- [MCP1200 Main Controller Card Overview](#)
- [NPT-1200 Timing](#)
- [NPT-1200 Cooling Subsystem](#)
- [NPT-1200 Power Feed Subsystem](#)
- [NPT-1200 Switching Cards](#)
- [NPT-1200 Tslot IO Modules](#)
- [NPT-1200 Expansion Platform](#)

## NPT-1200 Control Subsystem

When the NPT-1200 is configured with a CPS100 or CPS320 switching card, the MCP-1200 main controller card controls the entire NPT-1200 system via a high-performance CPU, which also processes communication with the EMS/LCT and other equipment. A large capacity flash memory stores equipment

configuration data and up to two software versions. Both online and remote software upgrades are supported.

## Controller Subsystem



NPT-1200 control and communication functions include:

- Internal control and processing
- Communication with external equipment and management
- Network element (NE) software and configuration backup
- Built-in Test (BIT)

## Internal Control and Processing

The main controller card provides central control, alarm, maintenance, and communication functions for Neptune NEs. It can also communicate with the control processors of various cards in the extension unit, using a primary-secondary control hierarchy.

The control subsystem is separate from the traffic subsystem. If there is a failure or extraction of the control card, traffic is not impaired.

## Software and Configuration Backup

The platform features a large-capacity on-board NVM that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

## Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection
- Protection switch for the main switching card

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

# NPT-1200 Communications with External Equipment and Management

In the Neptune product line, the main controller card is responsible for communicating with other NEs and management stations.

The main controller card communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other PEs via in-band management, enabling NE management through in-band channels.

## Usage Guidelines

The NPT-1200 (with CPS100/320) supports in-band and management communication channel (MCC) connections for PB and MPLS:

- 4 Mbps policer for PB UNI which connects to external DCN
- 10 Mbps shaper for MCC packet to MCP
- No rate limit for the MNG port rate, up to 100M full duplex
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, static routes
  - IPv6: Over management VLAN, static routes

The NPT-1200 (with MCIPS320/560) supports in-band and management communication on the following interfaces:

- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- In-band management processing (40Mbps)
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-IS v6, static routes

# MCP1200 Main Controller Card Overview

## Description

The MCP1200 card is the main processing card of the NPT-1200. It integrates functions such as control, communications and overhead processing. It provides:

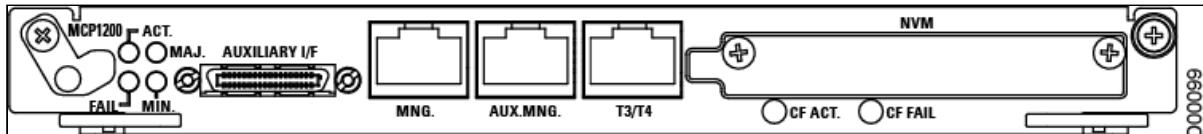
- Control-related functions:
  - Communications with and control of all other modules in the NPT-1200 and EXT-2U through the backplane (by the CPU)
  - Communications with the EMS-NPT, LCT-NPT, or other NEs through a management interface (MNG), or MCC, or VLAN
  - Alarms and maintenance
  - Fan control
- Overhead processing, including overhead byte cross connections, OW interface, and user channel interface
- External timing reference interfaces (T3/T4), which provide the line interface unit for one 2 Mbps T3/T4 interface and one 2 MHz T3/T4 interface

The MCP1200 supports the following interfaces:

- MNG and T3/T4 directly from its front panel
- RS-232, housekeeping, and alarms through a concentrated SCSI auxiliary I/F connector (on the front panel)

**Note**

Failure of the MCP1200 does not affect any existing packet traffic on the platform.

**MCP1200 Front Panel****MCP1200 Front Panel Interfaces**

Marking	Interface Type	Function
AUXILIARY I/F	SCSI-36	A concentrated auxiliary connector for the following interfaces: <ul style="list-style-type: none"> <li>• 1 x RS-232 interface for debugging or managing external ancillary equipment</li> <li>• 1 x alarm input and output interface connecting to the RAP</li> </ul>
T3/T4	RJ-45	T3 and T4 timing interfaces (one 2 Mbps and one 2 MHz)
MNG.	RJ-45	10/100BaseT Ethernet interface for management
AUX MNG.	RJ-45	Auxiliary 10/100BaseT Ethernet interface for local management and debug

**Note**

An MCP30\_ICP can be used to distribute the concentrated auxiliary connector into dedicated connectors for each function.

**MCP1200 LED Indicators and Pushbuttons**

Marking	Full Name	Color	Function
- (left LED in MNG and AUX MNG. ports)	Link	Green	Lights when MNG link is on. Off when MNG link is off. Blinks when packets are received or transmitted.
- (right LED in MNG and AUX MNG. ports)	Speed	Orange	Lights when the MNG link is 100 Mbps. Off when the MNG link is 10 Mbps.
ACT.	System active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates card not running normally.
FAIL	System fail	Red	Normally off. Lights when card failure detected.
MJR.	System major alarm	Red	Lights when the system has a critical or major alarm.
MNR.	System minor alarm	Yellow	Lights when the highest severity of the NE current alarms is minor or warning. Off when the system has no alarm or the highest severity of the NE current alarms is higher than minor or warning.
CF ACT.	Compact Flash memory active	Green	Lights when the CF card is present and properly locked. Off when the CF card is not present or not locked. Blinks when the CF card is being written or read.
CF FAIL	Compact Flash memory fail	Red	Normally off. Lights when the CF card is not present, is not locked, or has a failure.

**Note**

ACT, FAIL, MJR, and MNR. LEDs are combined to show various failure reasons during the system boot. For details, see the Troubleshooting Using Component Indicators section in the *NPT-1200 Installation, Operation, and Maintenance Manual*.

## NPT-1200 Timing

This platform provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations for functionality and performance.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed redundantly from the TMUs to all traffic and matrix cards, minimizing unit types and reducing operation and maintenance costs.

The TMU and the internal and external timing paths are fully redundant. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem. In case of hardware failure, the redundant synchronization subsystem takes over the timing control with no traffic disruption.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- 1PPS and ToD interfaces, using external timing input sources
- 2 x 2 MHz/Mbps (T3) external timing input sources
- NTP support
  - NTPv1, NTPv2, NTPv3, and NTPv4 (with MCIPS320 or MCIPS560)
  - SNTPv4, support for unicast client and unicast server mode only (with CPS100 or CPS320)
- E1/T1 interfaces of CES cards
- STM-1/4 of CES cards
- Local interval clock
- Holdover mode
- SyncE
- 1588v2 - Primary, Secondary, transparent, and boundary clock

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization, which is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262, G.8263, and G.8264.

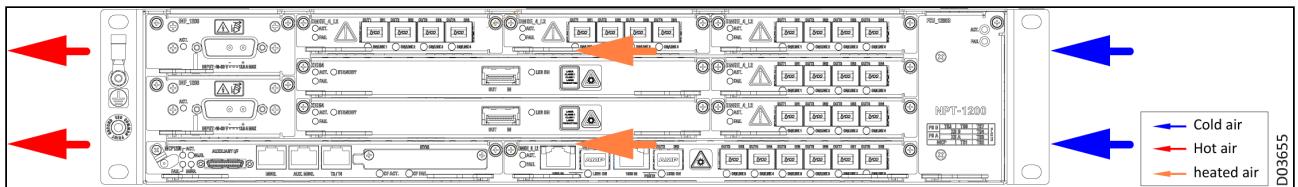
The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. IEEE 1588v2 (G.8265.1/G.8275.1) is supported in the platform, providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <20ns (G.8273.2 Class B) timing error per NE.

## NPT-1200 Cooling Subsystem

The NPT-1200 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components, and cools them.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

### Airflow in the NPT-1200



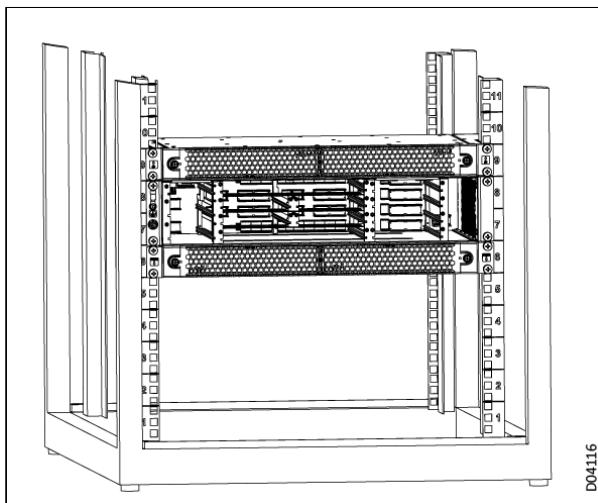
### Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The NPT-1200 platform can be configured together with air baffle units, installed in either a 19" or 23" rack.

- In the 19" rack, the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* the NPT-1200 platform, and one located directly *above* the NPT-1200 platform. The platform and two-part air baffle unit together occupy a total space of 4U height in the rack. The air baffle unit should be installed *before* the NPT-1200 platform; the NPT-1200 platform is then inserted into the gap space between the air-flow boxes. See the *NPT-1200 Installation and Maintenance Manual* for installation procedure details and limitations.

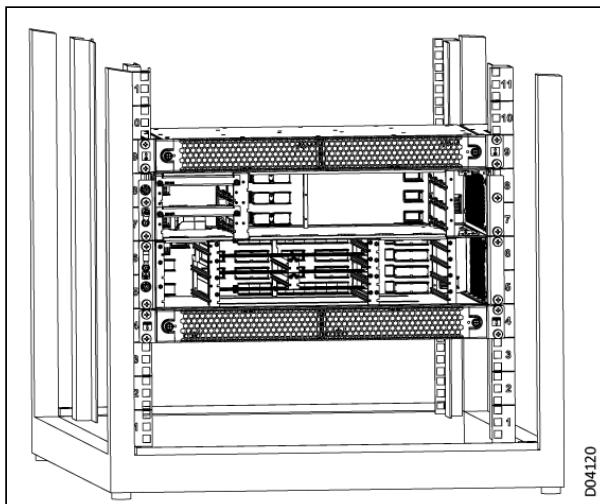
### 2U Height Platform Installed in 19" Rack Between Two Air-Flow Boxes



- In the 19" rack, if the NPT-1200 platform is configured with an EXT-2U expansion unit, the EXT-2U unit is located directly *above* the NPT-1200 platform. The air baffle unit is installed in the rack first; one 1U air-flow box is located directly *below* where the NPT-1200 platform will sit, and the second 1U air-flow box is located directly *above* where the EXT-2U expansion platform will sit. The combined platform and expansion unit are then installed in the rack between the two air-flow boxes. The combination of NPT-1200 platform with EXT-2U unit and two-part air baffle unit occupies a total space of 6U height in the rack.

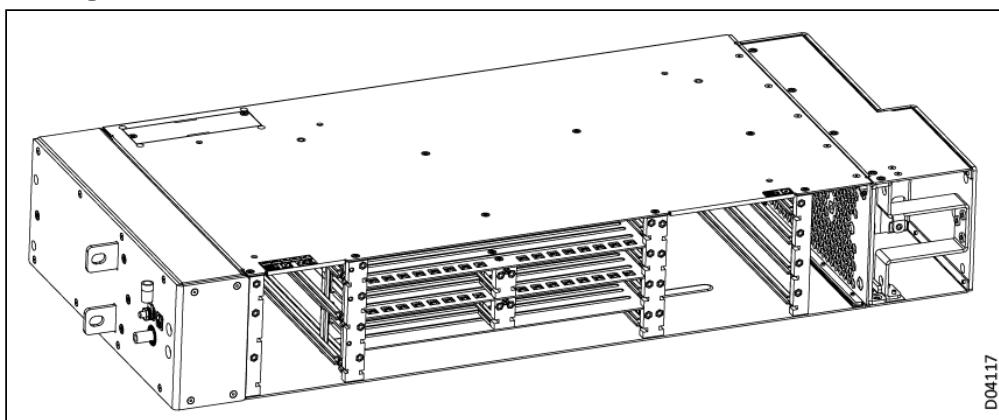
When installing the NPT-1200 platform together with an EXT-2U expansion unit and air baffles, the internal air filters in the EXT-2U unit must be removed. External air filters are available; see the *NPT-1200 Installation and Maintenance Manual* for details.

### 2U Height Platform Plus Expansion Unit Installed in 19" Rack Between Two Air-Flow Boxes



- In the 23" rack, the air baffle unit is installed as 2 2U air ducts placed to the right and left sides of the NPT-1200 platform, requiring a total space of 2U height to be available in the rack, since the air ducts don't add anything to the platform height.

### 2U Height Platform Installed with Air Baffle Unit in 23" Rack



- In the 23" rack, if the NPT-1200 platform is configured with an EXT-2U expansion unit, then a second set of 2U air ducts is installed on either side of the EXT-2U expansion platform. The combination of NPT-1200 platform with EXT-2U unit and 2 sets of 2U air ducts requires a total space of 4U height to be available in the rack, since the air ducts don't add anything to the platform height.

The NPT-1200 platform is cooled through one of the following FCU modules:

- [FCU\\_1200 Overview](#)
- [FCU\\_1200B Overview](#)

## FCU\_1200 Overview

### Description

The FCU\_1200 is a pluggable fan control module with eight fans for cooling the platform

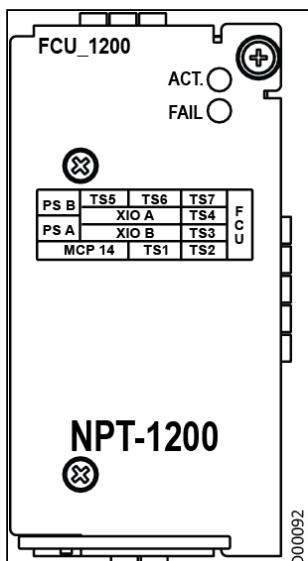
### Features

- 16 different fan speeds
- MCP1200 sets the fan speed to control the temperature in the platform

**Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

### FCU\_1200 Front Panel



### LEDs

Marking	Description	Color	Function
ACT.	System active	Green	Normally on when the fan unit is powered on. Off indicates a power failure of the fan unit.
FAIL	System fail	Red	Normally off. Lights when a fan failure is detected.

## FCU\_1200B Overview

### Description

The FCU\_1200B is a pluggable fan control module with eight fans for cooling the NPT-1200 platform. The unit features enhanced PWM (Pulse Width Modulation), which helps optimize fan cooling efficiency and increase fan operation life. PWM technology enables effective cooling at lower fan speeds, thereby improving fan effectiveness while reducing operating noise in room temperature conditions, compared to fan speed of the FCU\_1200 in same conditions.

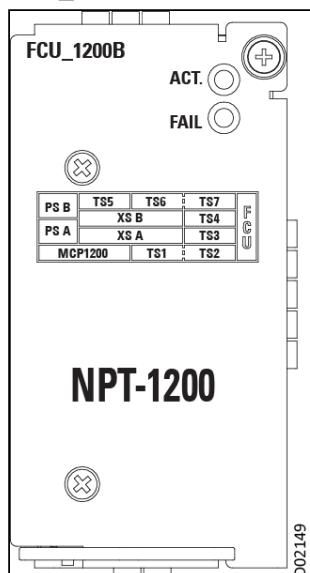
FCU\_1200B is fully backward compatible with [FCU\\_1200](#), so it can replace FCU\_1200 in any version. When FCU\_1200B is installed in NPT-1200 V6.0 or older, it behaves the same as FCU\_1200, with the original 16 levels that can be set for the fan speed control by adjusting the fan power supply voltage. When FCU\_1200B is installed in NPT-1200 V6.1 or higher, PWM is enabled and fan speed control is based on the PWM duty cycle, with the 8 cooling levels.

By default, fan speed is controlled by SW according to the installed cards temperature, and "force turbo" is supported for maintenance purpose.

#### **i Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

### FCU\_1200B Front Panel



### LEDs

Marking	Description	Color	Function
ACT.	System active	Green	Normally on when the fan unit is powered on. Off indicates a power failure of the fan unit.
FAIL	System fail	Red	Normally off. Lights when a fan failure is detected.

# NPT-1200 Power Feed Subsystem

## Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. Alternatively, a single AC power feed can be used.

## Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-1200 offers two power supply modes.

- -48 VDC power feed ([INF\\_1200](#)) configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- 100-240 VAC power source ([AC\\_PS-1200](#)) utilizes an external power line connection through a power conversion module to implement AC/DC conversion.

# INF\_1200 Power Module Overview

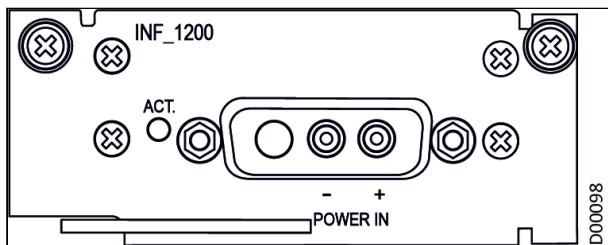
## Description

The INF\_1200 is a DC power-filter module that can be plugged into the NPT-1200 platform. Two INF\_1200 modules are needed for power feeding redundancy. The INF\_1200 module is also used to provide power for the [eEXT-2UH expansion unit](#).

## Features

- Single DC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected
- High-power INF for up to 550 W and 650W (INF\_1200 HW revision D02 and above)

## INF\_1200 Front Panel



## AC\_PS-1200 Power Module Overview

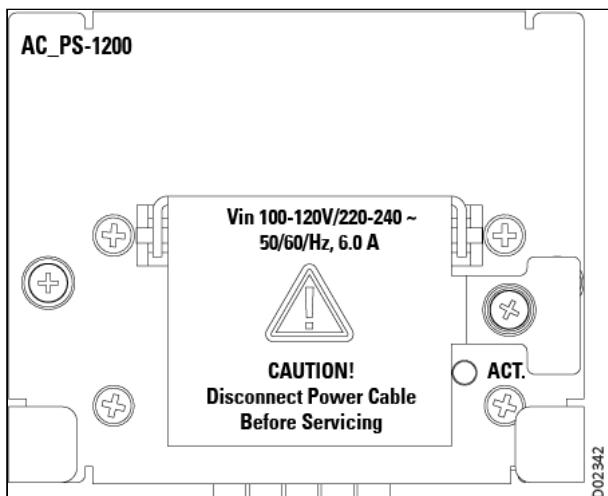
### Description

The AC\_PS-1200 is a 100-240 VAC power source utilizing an external power line connection through a power conversion module to implement AC/DC conversion. The AC\_PS-1200 module is also used to provide power for the [eEXT-2UH expansion unit](#).

### Features

- Single AC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- High-power AC power supply for up to 420W (100-120 VAC and 45°C (113°F) max working temperature) or 480W (220-240 VAC and 55°C (131°F) max working temperature)

### AC\_PS-1200 Front Panel



## NPT-1200 Switching Cards

The NPT-1200 platform operates with different matrix cards, depending on the configuration. The platform must be equipped with two switching cards of the same type to support system redundancy.

- **CPS100:** Central switching card that provides packet switching (L2/MPLS-TP). Two CPS100 cards are required for redundancy. Most convenient for applications that require high volume of pure packet handling. The card also supports 2 x 10 GE SFP+ based aggregation interfaces via corresponding ports.
- **CPS320:** Central switching card that provides packet switching (L2/MPLS-TP). Two CPS320 cards are required for redundancy. Most convenient for applications that require very high volume of pure packet handling. The card also supports 4 x 10 GE SFP+ based aggregation interfaces via corresponding ports.
- **MCIPS320:** Central switching card that provides dual stack packet switching (L2, MPLS-TP, and IP/MPLS). Also provides main control, communication, and overhead processing functionality. Two MCIPS320 cards are required for redundancy. Most convenient for applications that require very high volume of pure packet handling including support for dynamic L2/L3 VPN services. The card also supports 4 x 10 GE SFP+ based aggregation interfaces via corresponding ports.
- **MCIPS560:** Central switching card that provides dual stack packet switching (L2, MPLS-TP, and IP/MPLS). Also provides main control, communication, and overhead processing functionality. Two MCIPS320 cards are required for redundancy. Most convenient for applications that require very high volume of pure packet handling including support for dynamic L2/L3 VPN services. The card also supports 4 x 10 GE SFP+ based aggregation interfaces via corresponding ports.

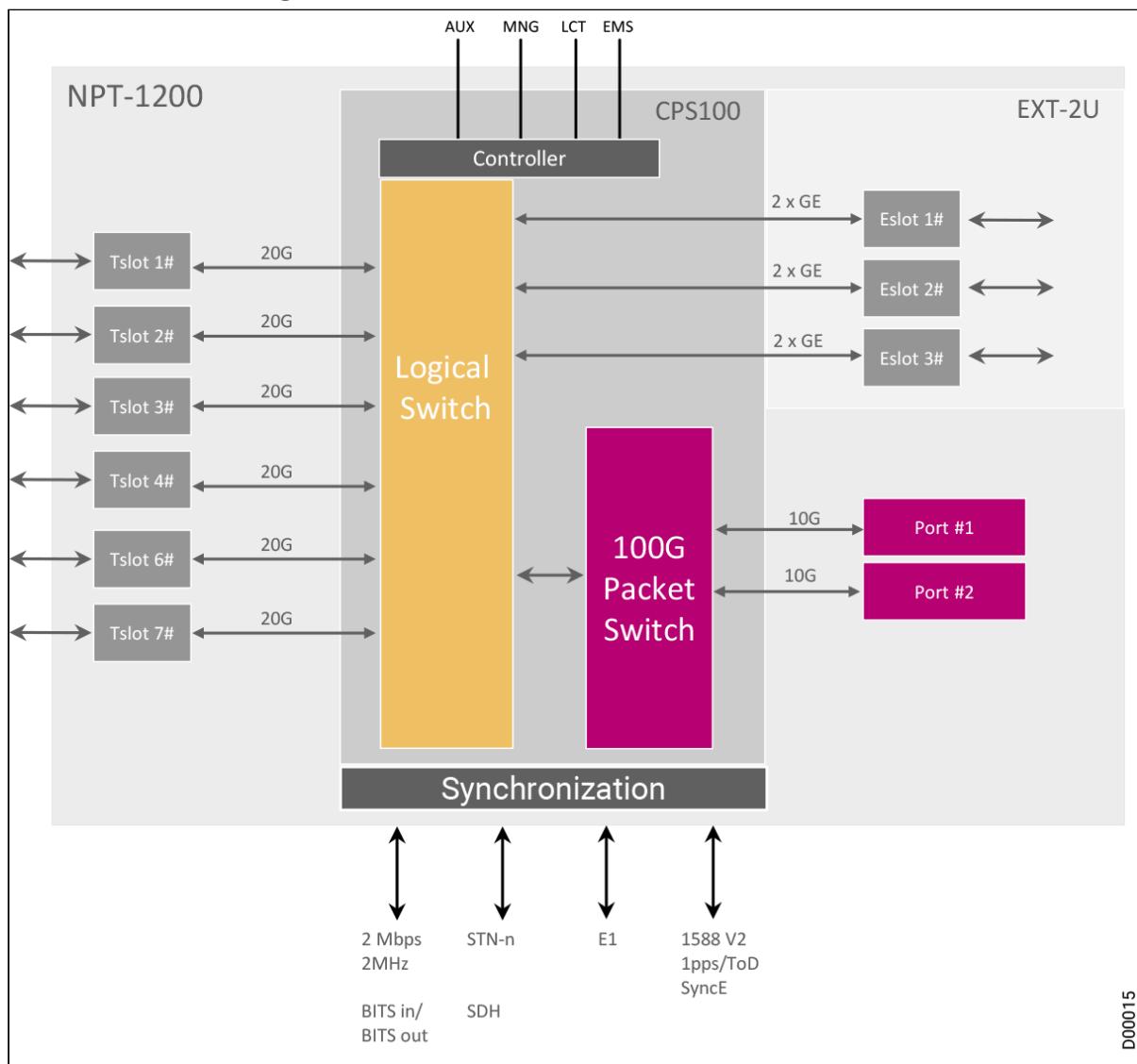
The following sections detail NPT-1200 switching card functionality.

- CPS100 Overview
- CPS100 Functional Description
- CPS320 Overview
- CPS320 Functional Description
- MCIPS320 and MCIPS560 Overview
- MCIPS320 and MCIPS560 Functional Description

## CPS100 Overview

The CPS100 is a powerful, high capacity, non-blocking switching card. It includes a pure switching and a packet switch to support native packet-level switching.

### CPS100 Functional Diagram



The CPS100 is a centralized packet switch that supports any to any direct data card connectivity. This matrix card, designed for use in the NPT-1200 metro access platform series, offers a choice of capacity and configuration options, including:

- All Native Ethernet packet switch, supporting native packet-level switching with a capacity of up to 100G, providing:

- Management and internal control, in addition to user traffic switching
- Non-blocking data switch fabric
- P2P MPLS internal links via the packet switch
- Traffic management including:
  - Guaranteed CIR
  - Eight CoS with differentiated services
  - End-to-end flow control
- Any slot to any slot connectivity
- Any card installed in any slot
- Two SFP+ based 10GE aggregate ports with OTN framing option (OTU-2e FEC/EFEC)
- Comprehensive range of timing and synchronization capabilities (ToD, 1PPS, 1588V2, Primary, Secondary, Transparent, and Boundary Clock)

## CPS100 Functional Description

The CPS100 card has two main subsystems:

- **Central packet switch:** Performs all the NPT-1200 packet switching operations.
- **TMU:** Generates and distributes timing and clock signals to all cards installed in the NPT-1200 platform. In addition to its internal timing reference, the TMU can use up to four user specified reference sources. See Timing for a description of the TMU capabilities.

The CPS100 card is a critical NPT-1200 subsystem, and therefore, for redundancy purposes, two CPS100 cards must be installed in any NPT-1200 platform, one on each side of the cards cage. Both cards must be of the same type and option and running the same NPT-1200 release.

When two identical cards are installed in the platform, the cards operate in a primary-secondary configuration:

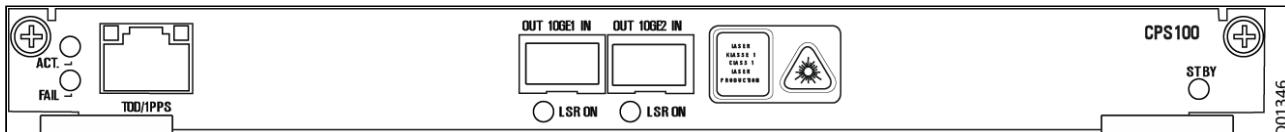
- At any time, only one card is active and the other is in standby mode.
- Upon a failure or removal of the active card, the standby card becomes active without any disruption in the system operation.

A CPS100 card can be inserted and replaced without affecting the traffic flow.

**Note**

During an upgrade, a different card version or release can be installed in the platform. With appropriate planning, the upgrade can be non-traffic affecting.

### CPS100 Front Panel



The CPS100 has an RJ-45 connector marked TOD/1PPS that provides timing and synchronization input/output signals, supporting IEEE 1588v2 standard.

## LEDs

Marking	Full Name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the CPS100 not downloaded successfully or that the CPS100 cannot be controlled normally by the MCP1200. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the CPS100 card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STBY	System standby	Orange	Lights when the card is in standby. Off when the card is active.
LSR ON (separate LED for each port)	Laser on indication	Green	Lights steadily when laser is on.

## CPS320 Overview

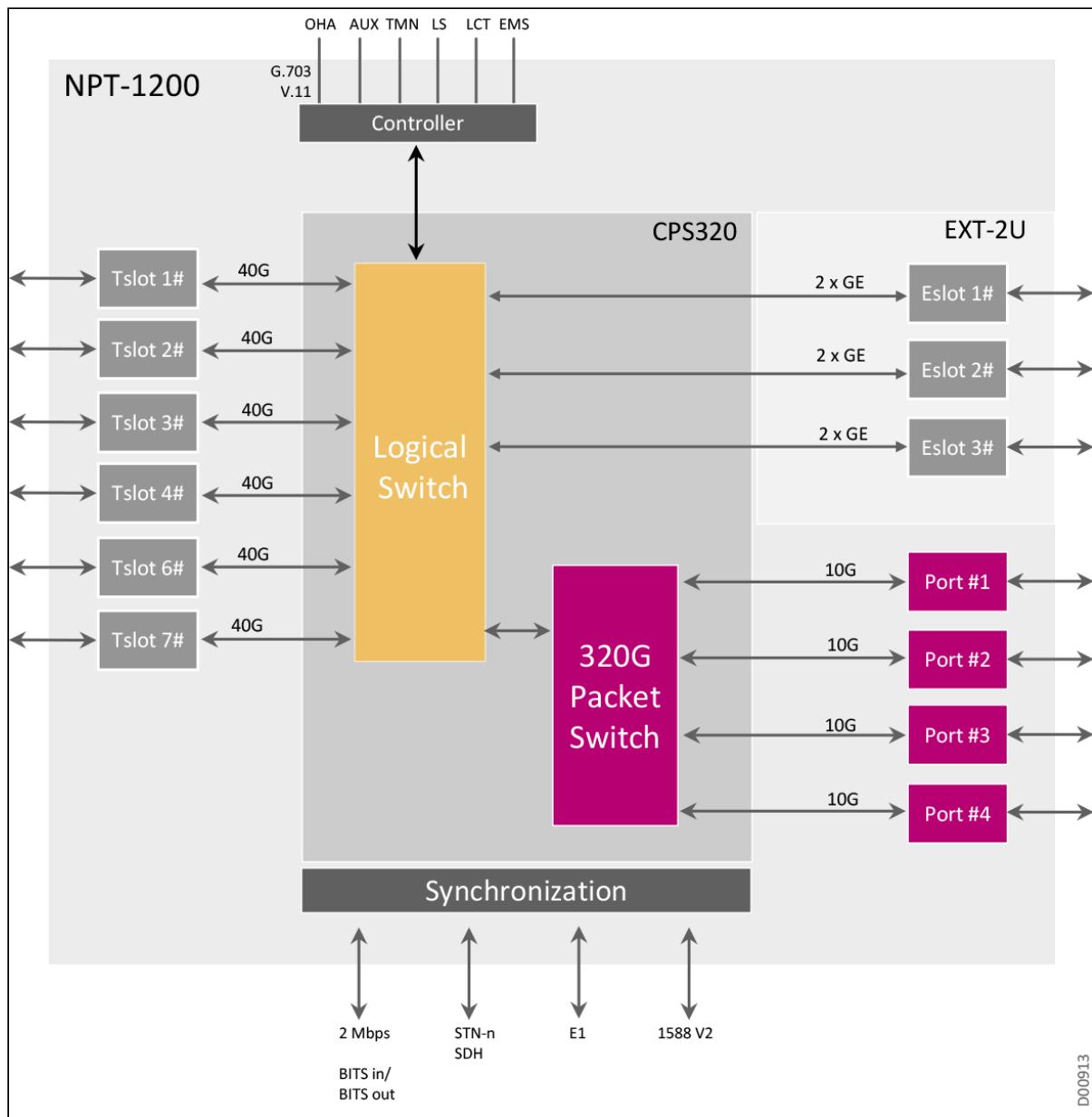
The CPS320 is a centralized packet switch that supports any-to-any direct data card connectivity. This switch card, designed for use in the NPT-1200 metro access platform, offers a choice of capacity and configuration options, including:

- Ethernet packet switch, supporting native packet-level switching with a 320G switching capacity and up to 240G traffic management (MPLS processing), providing
  - Management and internal control, in addition to user traffic switching
  - Non-blocking data switch fabric
  - P2P MPLS internal links via the packet switch
- Traffic management including:
  - Guaranteed CIR
  - Two CoS (within the switch)
  - End-to-end flow control
- Any card installed in any slot
- Any slot to any slot connectivity
- Four SFP+ based 10GE aggregate ports with OTN framing option (OTU-2e FEC/EFEC)
- Comprehensive range of timing and synchronization capabilities (ToD, 1pps)

**① Notes**

- Extended temperature is not supported by the CPS320 switch card.
- Tslot #5 is not used with this matrix.

### Traffic Flow in an NPT-1200 Configured With a CPS320 Matrix Card



## CPS320 Functional Description

The CPS320 card has two main subsystems:

- **Central packet switch:** Performs all the NPT-1200 packet switching operations.
- **TMU:** Generates and distributes timing and clock signals to all cards installed in the NPT-1200 platform. In addition to its internal timing reference, the TMU can use up to four user specified reference sources. See Timing for a description of the TMU capabilities.

The CPS320 card is a critical NPT-1200 subsystem, and therefore, for redundancy purposes, two CPS320 cards must be installed in any NPT-1200 platform for redundancy (non-redundant configuration is supported as well). Both cards must be of the same type and option and running the same NPT-1200 release.

When two identical cards are installed in the platform, the cards operate in a primary-secondary configuration:

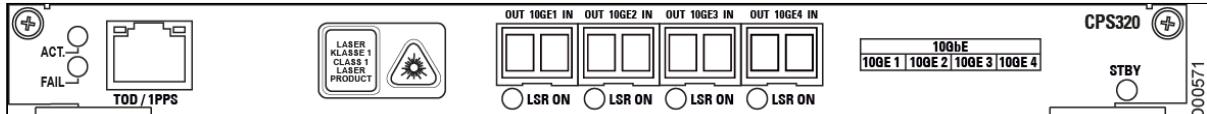
- At any time, only one card is active and the other is in standby mode.
- Upon a failure or removal of the active card, the standby card becomes active without any disruption in the system operation.

A CPS320 card can be inserted and replaced without affecting the traffic flow.

**Note**

During an upgrade, a different card version or release can be installed in the platform. With appropriate planning, the upgrade can be non-traffic affecting.

### CPS320 Front Panel



The CPS320 has an RJ-45 connector marked TOD/1PPS that provides timing and synchronization input/output signals, supporting IEEE 1588v2 standard.

### LEDs

Marking	Description	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the CPS320 not downloaded successfully or that the CPS320 cannot be controlled normally by the MCP1200. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the CPS320 card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STBY	System standby	Orange	Lights when the card is in standby. Off when the card is active.
LSR ON (separate LED for each port)	Laser on indication	Green	Lights steadily when laser is on.

## MCIPS320 and MCIPS560 Overview

MCIPS320/560 are centralized packet switches with IP/MPLS and L3VPN capabilities for the NPT-1200 platform. These cards include a main controller (MCP), 320G/560G central packet switch, EEC timing unit, IEEE 1588v2 timing unit, and four 10GE aggregate ports (SFP+ based). These are the main cards of the NPT-1200 IP/MPLS system. The MCIPS320/560 cards include three main subsystems:

- **MCP (Main Control Processor):** Performs all integrated functions like control, communication, and overhead processing with a micro-SD based NVM.

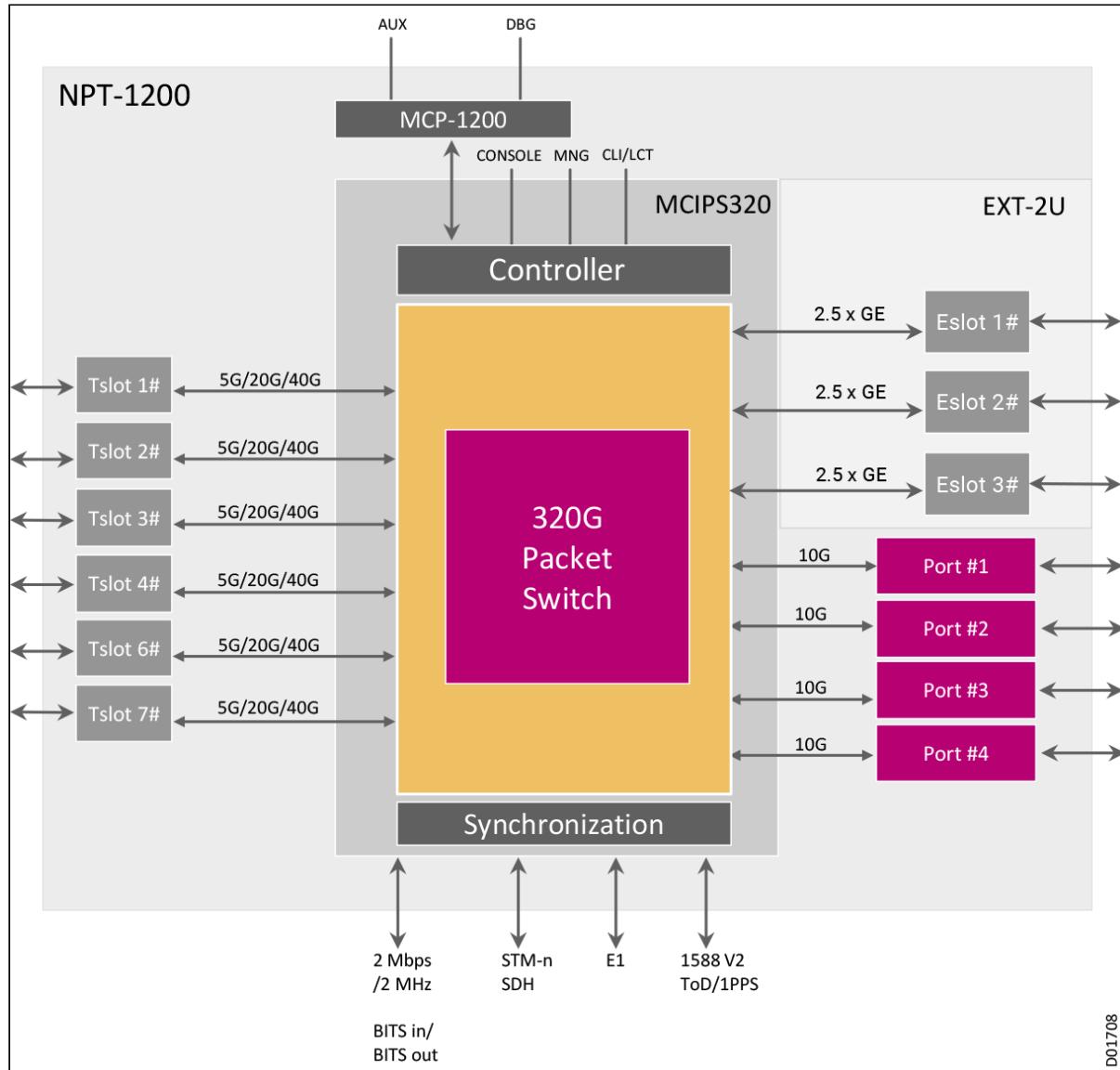
- **CPS (Central Packet Switch):** Performs all NPT-1200 packet switching operations.
- **TMU (Timing Unit):** Generates and distributes timing and clock signals to all cards installed in the NPT-1200. In addition to its internal timing reference, the TMU can use up to four user-defined timing references.

The MCIPS320/560 is a critical NPT-1200 subsystem, therefore, two such cards must be configured in the NPT-1200 for redundancy. Both cards must be of the same type, and running the same software version.

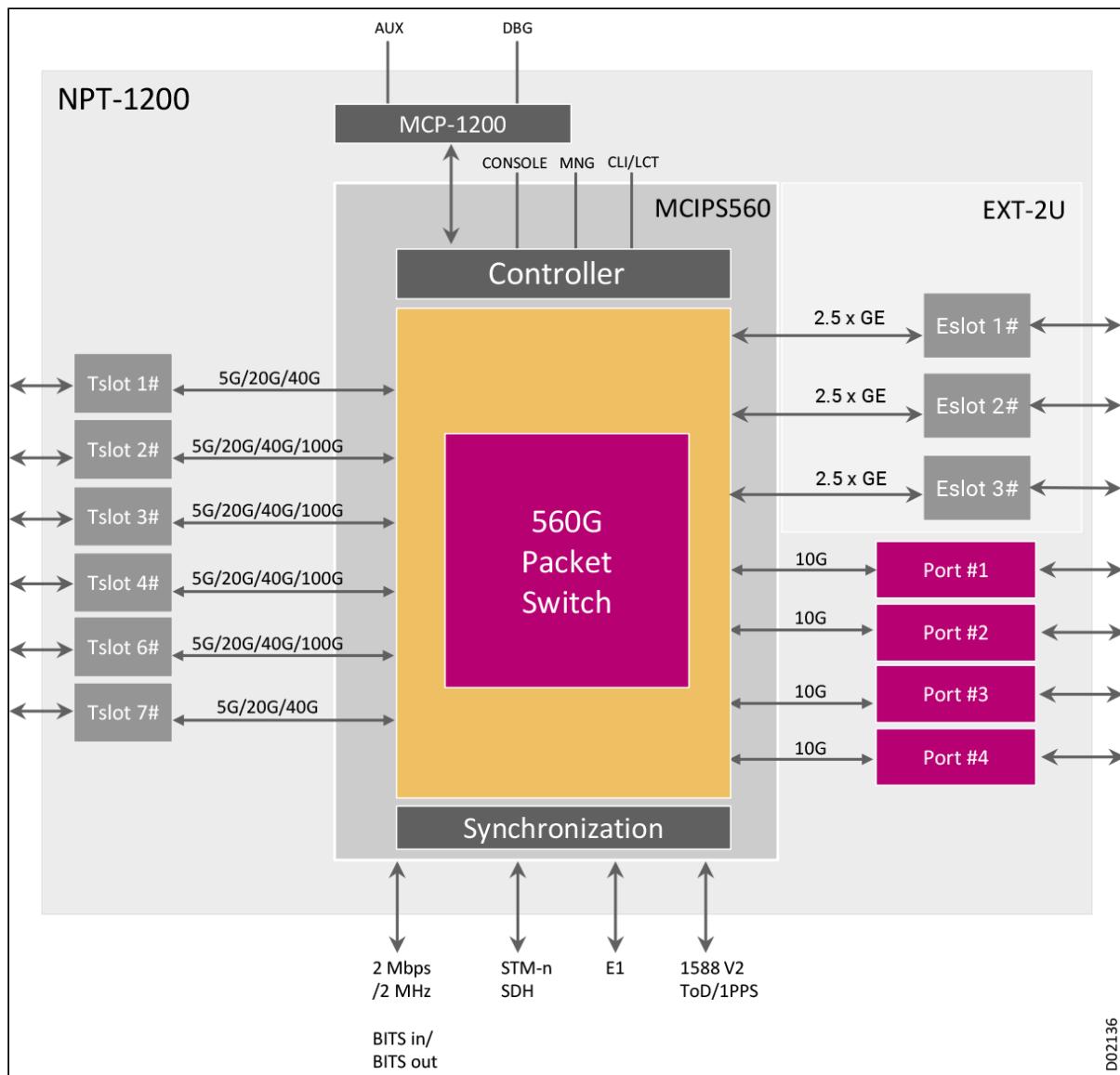
The two MCIPS320/560 operate in a primary-secondary configuration:

- At any time, only one card is active and the second is in stand-by.
- Upon failure or removal of the active card, the stand-by becomes active without any disruption in the system operation.

### MCIPS320 Functional Block Diagram



### MCIPS560 Functional Block Diagram



D02136

The MCIPS320/560 cards have a switching capability of 320/560 Gbps. In addition, they provide four 10GE (SFP+ based) line interface aggregate ports. The SFP+ housing on the card supports 10GE optical transceivers with a pair of LC connectors. In addition to the greater switching capacity, the MCIPS560 differs from the MCIPS320 by enabling 100G capacity to 4 traffic slots (Slots 2, 3 ,4 ,7). Note that Tslot #5 is not used with these matrix cards.

These switching cards, designed for use in the NPT-1200 metro access platform, offer a choice of capacity and configuration options, including:

- Ethernet packet switch, supporting native packet-level switching with a 320G/560G switching capacity and up to 320G/560G traffic management (packet processing), providing:
  - Management and internal control, in addition to user traffic switching
  - Non-blocking data switch fabric for Ethernet/MPLS-TP and IP/MPLS traffic forwarding
- Traffic management including:
  - Guaranteed CIR
  - 8 x CoS for differentiated services
  - E2E flow control
- Any card installed in any slot

- Any slot to any slot connectivity
- Support 1+1 (redundant) configuration for traffic, management, and control
- Main control processing unit and built-in NVM (micro-SD card)
- Four SFP+ based 10GE aggregate ports:
  - Support LAN (10GBase-R) and WAN (10GBase-W)
  - RS FEC and EFEC (I4, I7) support with OTU2e wrapping
  - Support various SFP+ types for different PMDs:
    - Uncolored - OTP10\_SR, LR, ER, ZR, BD;
    - CWDM - OTP10C\_xx
    - DWDM - OTP10D\_xx
    - Support full C-band tunable SFP+ (OTP10T)
  - OTSOP16 Smart SFP supported in SFP+\_10GE ports
- Comprehensive range of timing and synchronization capabilities:
  - G.781/G.8262 compliant EEC
  - 1PPS and ToD interfaces
  - IEEE 1588v2 PTP with:
    - OC (primary & secondary), BC
    - One-step TC
    - G.8275.1 profile
- Supports local management via CLI
- L3 VPN and IP/MPLS features:
  - VRF support:
    - ACL + L3 classification
    - uRPF
    - Multi-VRF networking stack
  - BGP (iBGP & eBGP):
    - AF ipv4
    - AF vpng4
    - Graceful restart
    - BFD support
  - L3VPN extension over static PW (PW-HE)
  - PE-CE protocols:
    - Static
    - eBGP
  - VRRP
  - IP multicast
    - IPV4 multicast with PIM and IGMP
  - DHCP
    - DHCP Relay (to connect hosts to DHCP server via L3 VPN)
    - Multi hop IP-BFD
- NETCONF interface
- Continuous and periodic PM counters
- Syslog report generation support
- Built-in Y.1564 Service Activation Test and loop back with MAC swap

In NPT-1200 platforms equipped with MCIPS320 or MCIPS560 switching cards, the main control and processing (MCP) functions are moved to the MCIPS320/560 modules. In this configuration, the MCP1200 operates as a supporting card. However, MCP1200 installation is still required because all control interfaces of INF, FCU, and I/O slots are physically connected to the MCP1200 slot through the platform's backplane.

**i Optional Feature:**

MCIPS560 matrix is available in two variants: default switching capacity (320G) and full switching capacity (560G); it is possible to unlock the default capacity limit to utilize full capacity with a software license.

## MCIPS320/MCIPS560 Hardware Compatibility

To avoid hardware mismatch alarms, use new cards from production only. In case of old cards used, make sure that the following HW revisions are available for installation.

### **i** Notes

Required hardware revisions in NPT-1200 equipped with MCIPS320/560:

- DHXE\_2 with HW revision >=C00
- DHGE\_4E with HW revision >=C00
- DHGE\_8 with HW revision >=C00
- DHGE\_16 with HW revision >=B00
- DHGE\_24 with HW revision >=C00
- MSC2\_8 with HW revision <=C00

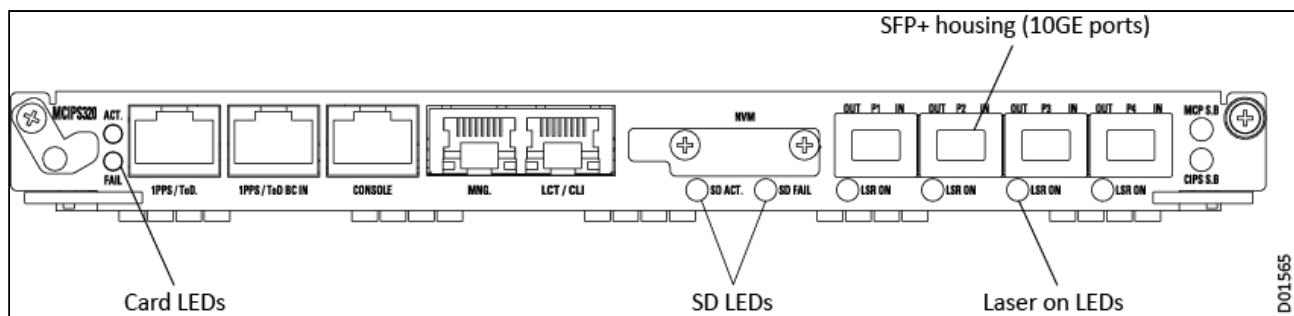
## MCIPS320 and MCIPS560 Functional Description

As described in [MCIPS320/560 Overview](#), the MCIPS320 and MCIPS560 have similar features and functionality, differing only in the switching and forwarding capability. An MCIPS320 or MCIPS560 card can be inserted and replaced without affecting the traffic flow.

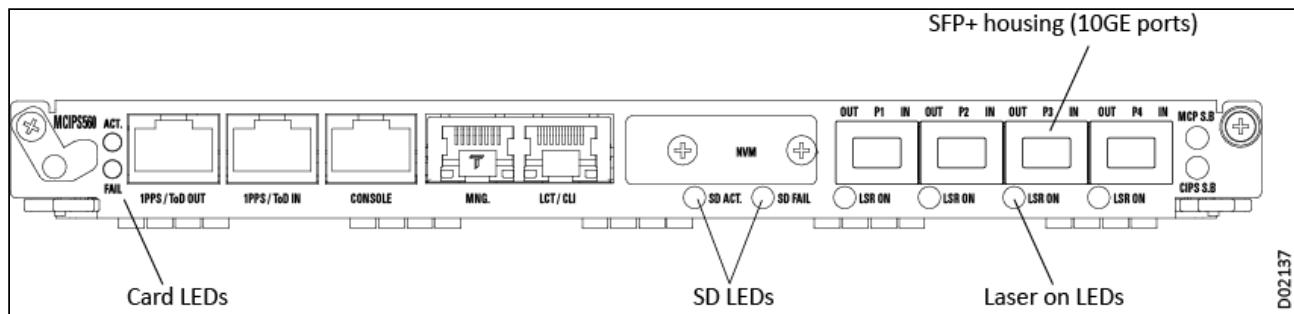
### **i** Note

During an upgrade, a different card version or release can be installed in the platform. With appropriate planning, the upgrade can be non-traffic affecting.

### MCIPS320 Front Panel



### MCIPS560 Front Panel



Both cards have similar components on their front panels with similar functions, listed in the following tables.

**MCIPS320/560 Front Panel Component Functions**

<b>Marking</b>	<b>Interface Type</b>	<b>Function</b>
1PPS/ToD OUT	RJ-45	1PPS/ToD output interface for OC Secondary or T-BC
1PPS/ToD IN	RJ-45	1PPS/ToD input interface grandmaster (T-GBM) or T-BC when APTS is enabled
CONSOLE	RJ-45	Serial RS-232 communication port for use by technical support personnel (debug, maintenance, etc.).
MNG.	RJ-45	10/100/1000BaseT Ethernet interface for out-of-band management.
LCT/CLI	RJ-45	10/100/1000Base-T local management interface for connecting to an LCT or CLI.

**i Note**

An MCP30 ICP can be used to distribute the concentrated auxiliary connector into dedicated connectors for each function.

**MCIPS320/560 LED Indicators**

Marking	Full Name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the MCIPS320/560 not downloaded successfully or that the MCIPS320/560 cannot be controlled normally. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the MCIPS320/560 card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
SD ACT.	NVM card active	Green	Normally on. Off if the micro-SD has a failure.
SD FAIL	NVM card failure	Red	Normally off. Lights when the micro-SD is faulty, such as micro-SD is not inserted.
MCP S.B	Main Control Processor is standby	Orange	On indicates that the MCIPS320/560 is in standby state. Off indicates that the card is active. Fast blinking indicates the card is busy, handling pre-switchover activity.
CIPS S. B	MCIPS320/560 is standby	Orange	On indicates that the MCIPS320/560 is in standby state. Off indicates that the card is active.
LSR ON (separate LED for each 10GE port)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

**NPT-1200 Tslot IO Modules**

The NPT-1200 has seven Tslots for installing I/O modules. The following table lists the different types of CES and Ethernet I/O modules that can be installed in the NPT-1200, with links to each module listed.

**i Note**

No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by the NPT-1200:

	Max 1GE ports	Max 10GE ports	Max 100GE ports
With <b>MCIPS560</b>	60	32	4
With <b>MCIPS320</b>	68	32	N/A
With <b>CPS320</b>	64	32	N/A
With <b>CPS100</b>	48	10	N/A

**NPT-1200 Supported Tslot Modules**

Description	Card	TS#1 to TS#7 with CPS100/CPS320	TS#1 to TS#7 with MCIPS320	TS#1 to TS#7 with MCIPS560
CES multiservice module with STM-1/STM-4 interfaces	<a href="#">DMCES1_4</a>	TS1-TS4, TS6-TS7	N/A	N/A
CES multiservice module with 16 x E1/T1 interfaces	<a href="#">MSE1_16</a>	TS1-TS4, TS6-TS7	N/A	N/A
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	<a href="#">MSC_2_8</a>	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
CES multiservice module for 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<a href="#">MS1_4</a>	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
CES multi-service module with 32 x E1/T1 interfaces	<a href="#">MSE1_32</a>	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4E</a>	TS1-TS4, TS6-TS7	TS1-TS2, TS6-TS7	TS1, TS6
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4EB</a>	N/A	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
Optical 8 x GE interface module with direct connection to the packet switch	<a href="#">DHGE_8</a>	TS1-TS4, TS6-TS7	TS1-TS2, TS6-TS7	TS1, TS6
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	<a href="#">DHGE_8S</a>	N/A	TS3, TS4	TS2-TS4, TS7

Description	Card	TS#1 to TS#7 with CPS100/CPS320	TS#1 to TS#7 with MCIPS320	TS#1 to TS#7 with MCIPS560
Optical 10 x GE module with direct connection to the packet switch	DHGE_10	N/A	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
Electrical and optical 16 x GE interface module with direct connection to the packet switch	DHGE_16	TS1+TS2, TS6+TS7	TS1+TS2, TS6+TS7	TS1+TS2, TS6+TS7
Optical 24 x GE interface module with direct connection to the packet switch	DHGE_24	TS1+TS2, TS6+TS7	TS1+TS2, TS6+TS7	TS1+TS2, TS6+TS7
Optical 2 x 10GE interface module with direct connection to the packet switch	DHXE_2	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
Optical 4 x 10GE interface module with direct connection to the packet switch	DHXE_4	TS1-TS4, TS6-TS7 (not with CPS100)	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
Optical 4 x 10GE/OTU-2 interface module with direct connection to the packet switch with OTN wrapping	DHXE_4O	TS1-TS4, TS6-TS7 (not with CPS100)	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
40G MACsec card with: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 10G/1GE multi-rate ports</li></ul> All 4 ports support MACsec capability.	DHXE_4sec	N/A	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces All 4 ports support MACsec capability	DHXE_4MRsec	N/A	TS1-TS4, TS6-TS7	TS1-TS4, TS6-TS7

Description	Card	TS#1 to TS#7 with CPS100/CPS320	TS#1 to TS#7 with MCIPS320	TS#1 to TS#7 with MCIPS560
Optical 100GE QSFP28 interface module with direct connection to the packet switch	DHCE_1Q	N/A	N/A	TS2-TS4, TS7
Optical 100GE QSFP28/QSFP_DD interface module with direct connection to the packet switch	DHCE_1QB DHCE_1QC	N/A	N/A	TS2-TS4, TS7

**i Notes**

- Failure of the MCP1200 does not affect any existing traffic on the platform.
- The NPT-1200 platform must be configured with identical switching card types.
- The NPT-1200 platform with CPS100 supports max. 48 x GE or max. 10 x 10 GE.
- The NPT-1200 platform with CPS320 supports max. 64 x GE or max. 32 x 10 GE.
- The NPT-1200 platform with MCIPS320 supports max. 68 x GE with 2 x DHGE\_24 + 2 x DHGE\_10 cards.
- The NPT-1200 platform with MCIPS560 supports max. 60 x GE with 6 x DHGE\_10 cards.

## NPT-1200 Expansion Platform

The traffic capabilities of the Neptune platform can be expanded by installing the EXT-2U expansion unit on top.

The EXT-2U platform is a high density modular expansion unit for the Neptune multiservice platforms. It supports the complete range of CES, PCM, optics and Ethernet services. Integrating this add-on platform into your network configuration is not traffic-affecting.

The EXT-2U is compact and versatile and can be used with different base units from the Neptune product line. The type of traffic delivered by the unit depends on the type of matrix (PCM or Packet only) installed in the base unit. I/O expansion cards are supported in accordance.

The EXT-2U has three multipurpose slots (ES1 to ES3) for any combination of extractable traffic cards. PCM, Ethernet, OTN muxponders, optical amplifiers, and CES traffic are all handled through cards in these traffic slots.

The following table lists the traffic cards supported in the EXT-2U when installed on the platform. For a detailed description of the EXT-2U features, functionality, and supported traffic cards refer to the chapter [EXT-2U Expansion Platform](#).

**EXT-2U Supported Traffic Cards for NPT-1200**

<b>Card Type</b>	<b>Designation</b>
Multiservice PCM and 1/0 XC card over Ethernet	<a href="#">EM_10E</a>
Optical Base Card (OBC) for optical amplifiers and DCM modules (OBC, OBC_B, OBC_C)	<a href="#">Optical Base Card (OBC)</a>
CES multiservice card with 2 x STM-1/OC-3 and 16 x E1/T1 interfaces	<a href="#">MSC_2_16E</a>
10G card with up to 10 GbE ports; 4 of the ports support POE++	<a href="#">DHGE_10_POE</a>
Data cards with internal direct connection to the packet switch	<a href="#">DHFE_12</a>
Data cards with internal direct connection to the packet switch	<a href="#">DHFX_12</a>
CES multiservice card for 32 x E1 interfaces.	<a href="#">DMCE1_32</a>
Muxponder card with 12 client ports and a slot for installing an OM_AOC4 optical module.	<a href="#">MXP10</a>

# NPT-1100 System Architecture

The NPT-1100 is a pre-aggregation IP transport platform, designed for mobile backhaul applications (4G/5G) as well as carrier Ethernet applications (such as wholesale carriers, city carriers, CIN for MSOs, and residential voice, video, and data). The NPT-1100 supports elastic MPLS (dual stack MPLS-TP and IP/MPLS) with a large 100G/25G/10G/GE port fan-out, providing colored 100G interfaces, CES/CEP for TDM interfaces supporting 3G migration, and a built-in GNSS receiver interface for timing distribution.

With 300G switching capacity and a port fan-out supporting 582G in a 1RU form factor, the NPT-1100 is ideal for multi-service applications, including a comprehensive and scalable set of Layer 2 and Layer 3 VPN services. The NPT-1100 is well suited for a wide variety of applications and networking scenarios, offering a rich set of robust features built into a small form factor temperature hardened platform, suitable for both outdoor and indoor deployment.

NPT-1100 provides enhanced user platform monitoring by providing a full set of OAM tools, including Dying Gasp signaling capabilities, ensuring effective platform and service management at every stage. The NPT-1100 can be installed easily in a short time using Zero Touch Installation (ZTI). Neptune also supports NFV services and SDN applications, which are compulsory in today's challenging metro environment.

The NPT-1100H platforms are hardware variants of the NPT-1100 platforms, providing the same functionality as the NPT-1100, with the addition of G.8275.2 support.

## NPT-1100 Platform

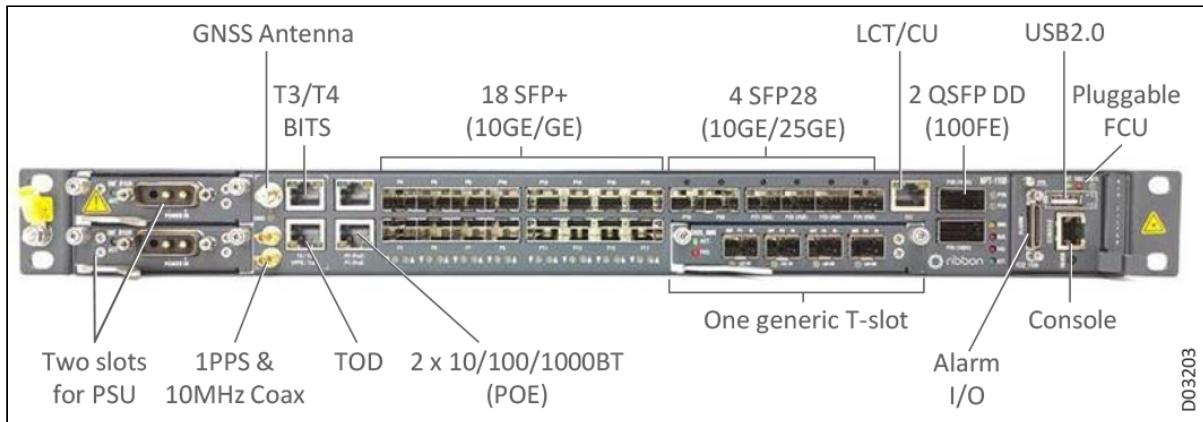


The NPT-1100 is a 1U base platform housed in a 44 mm high, 440 mm wide, and 243 mm deep (1.73 in. x 17.32 in. x 9.57 in.) equipment cage, with all interfaces accessible from the front of the unit. This CE3.0-compliant, carrier Ethernet, IP/MPLS, L3 access and pre-aggregation device supports:

- Up to 582G packet switching (port fan-out)
- 300Gb/s packet processing, implemented through a system-on-a-chip (SoC) architecture
- Base shelf unit fan-out capabilities:
  - 2 x 100G (QSFP-DD, QSFP28)
  - 4 x 25G/10G
  - 18 x 10G/GE
  - 2 x GE Base-T (PoE+)
    - Maximum fan-out capabilities: 3 x 100G, 8 x 25G, 26 x 10G, 30 x GE
- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+\_10GE ports
- Dual-stack MPLS (MPLS-TP and IP/MPLS)
- Wide range of timing support:
  - T3/T4 BITS
  - GNSS built-in receiver
  - 10MHz
  - SyncE
  - IEEE 1588v2 G.8275.1
  - IEEE 1588v2 G.8275.2 (NPT-1100H only)
  - G.8273.2 – Class C compliant
  - 1PPS and ToD
  - Hybrid 1588 and SyncE
  - APTS
- One traffic slot
- Automatic installation using ZTI on USB stick

- SDN interfaces: NETCONF/YANG support
- Temperature hardened, ranging from -40°C to +65°C (-40°F to +149°F )
- Extractable fan and filter units for easy maintenance
- Power supply:
  - Dual DC
  - Single DC
  - Single AC

### NPT-1100 Slot Layout



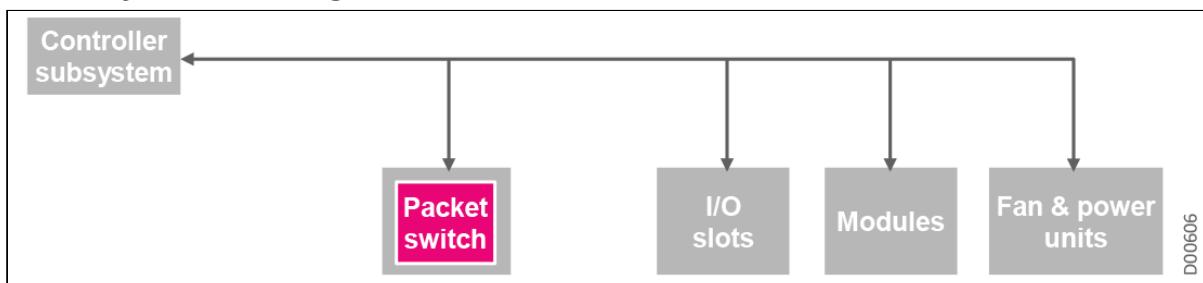
The NPT-1100 can be installed in 2,200 mm or 2,600 mm ETSI racks or in 19" racks. The rugged platform design makes this platform suitable for street cabinet use, withstanding temperatures up to 65°C/149°F. Typical power consumption for the NPT-1100 is less than 250 W. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

This section introduces the following NPT-1100 features:

- [NPT-1100 Control Subsystem](#)
- [NPT-1100 Communication with External Equipment](#)
- [NPT-1100 Timing](#)
- [NPT-1100 Cooling Subsystem](#)
- [NPT-1100 Power Feed Subsystem](#)
- [NPT-1100 Traffic and Switching Functionality](#)
- [NPT-1100 Tslot IO Modules](#)

## NPT-1100 Control Subsystem

### Control System Block Diagram



The platform control and communication main functions include:

- Internal control and processing
- Network element (NE) software and configuration backup

- Communication with external equipment and management
- Built-in Test (BIT)

## Internal Control and Processing

The NPT-1100 controller provides central control, configuration, alarm, maintenance, and communication functions. It can also communicate with the control processors of various cards in the Tslot unit, using a primary-secondary control hierarchy.

The NPT-1100 controller can also provide an NE management interface for management stations (EMS/LCT), support MCC, and channel management VLAN processing.

## Software and Configuration Backup

The platform features a large-capacity on-board NVM that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

## Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection
- Protection switch for the main switching card

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

# NPT-1100 Communication with External Equipment

In the Neptune metro access product line, the main controller unit is responsible for communicating with other NEs and management stations.

The main controller unit communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other NEs via the in-band MCC. Communication between other NEs, or between the NEs and the EMS/LCT, can also be via the out-of-band DCN. The controller can connect to the DCN via Ethernet.

## Usage Guidelines

The NPT-1100 supports in-band and DCN management connections for PB and MPLS:

- 20 Mbps shaper for MCC packet to MCP
- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-ISv6, static routes

## NPT-1100 Timing

The NPT-1100 was designed as a 5G backhauling platform. As such, it provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations, such as 1588v2 PTP according to the G.8273.2 standard, at the Class C/D support level.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed from the TMU to all base shelf ports and Tslot cards, minimizing unit types and reducing operation and maintenance costs. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- GNSS built-in receiver
- 1PPS and ToD interfaces, using external timing input sources
- 1PPS monitoring point
- 2 x 2048K/1544K Hz, E1/T1 (T3/T4) external timing input/output sources
- NTP support (NTPv1, NTPv2, NTPv3, and NTPv4)
- E1/T1 interfaces of CES cards
- STM-1/4 of CES cards
- 10MHz
- APTS
- Local interval clock
- Holdover mode
- SyncE
- 1588v2 - Primary, Secondary, transparent, and boundary clock

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization over GbE/10GbE/100GbE interfaces. Our implementation is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262.1, G.8263, and G.8264.

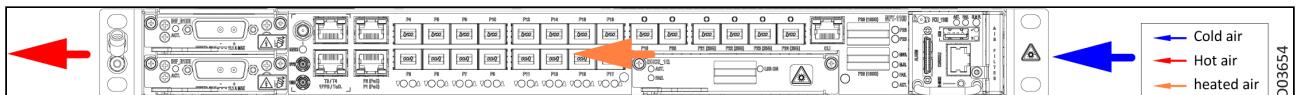
The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. PTP IEEE 1588v2 is supported in two profiles; full network timing support (G.8275.1) and partial network timing support (G.8275.2, NPT-1100H), providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <10ns (G.8273.2 Class C) timing error per NE. PTP is supported over GbE/10GbE/100GbE interfaces.

## NPT-1100 Cooling Subsystem

The NPT-1100 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components, and cools them.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

### Airflow in the NPT-1100



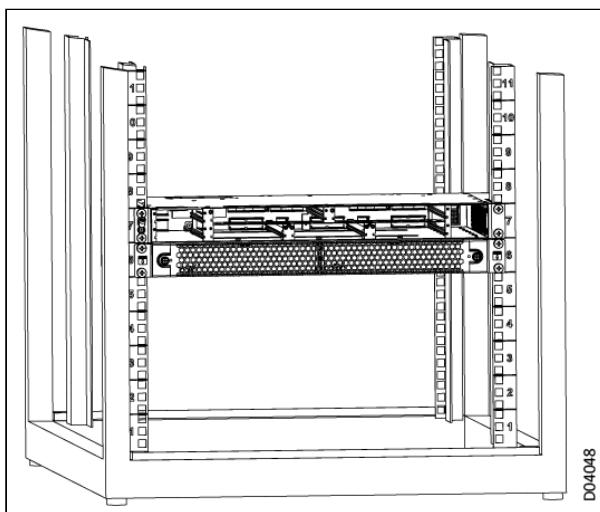
### Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The NPT-1100 platform can be configured together with an air baffle unit, installed in either a 19" or 23" rack.

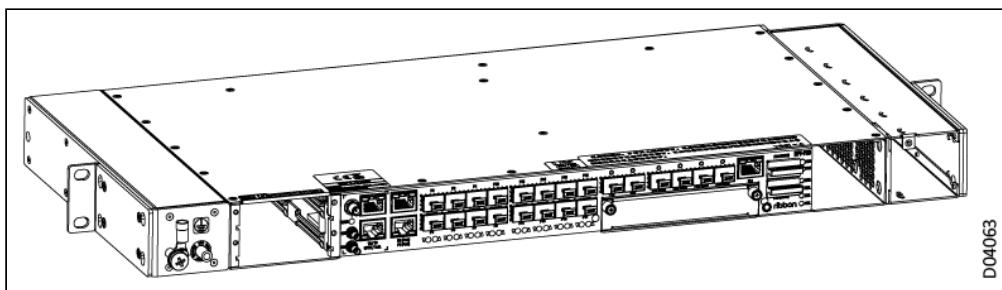
- In the 19" rack, the 1U air baffle unit is located directly below the NPT-1100 platform. The platform and air baffle unit together occupy a total space of 2U height in the rack. The air baffle unit should be installed *before* the NPT-1100 platform; the NPT-1100 platform is then inserted *above* the air baffle unit. Note that a total space of 3U height must be available in the rack for the installation process; see the *NPT-1100 Installation and Maintenance Manual* for the installation procedure details and limitations.

### 1U Height Platform Installed in 19" Rack over Air Baffle Unit



- In the 23" rack, the air baffle unit is installed as 2 1U air ducts placed to the right and left sides of the NPT-1100 platform, requiring a total space of 1U height to be available in the rack, since the air ducts don't add anything to the platform height.

### 1U Height Platform Installed with Air Baffle Unit in 23" Rack



When installing the NPT-1100 platform together with air baffles, the internal air filters in the NPT-1100 platform must be removed. External air filters are available; see the *NPT-1100 Installation and Maintenance Manual* for details.

### FCU Fan Control Unit

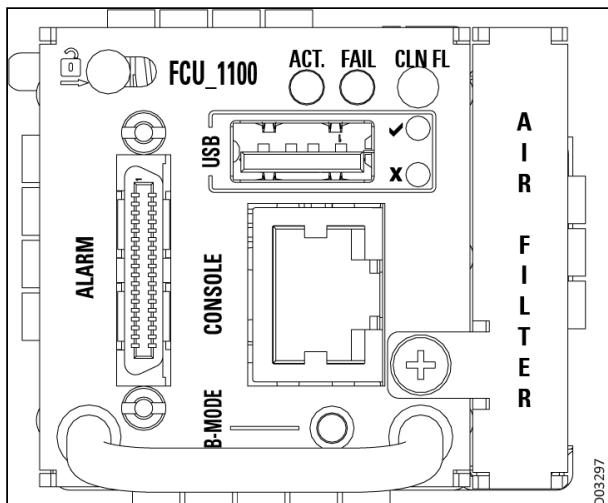
The NPT-1100 platform is cooled using the FCU\_1100, a pluggable fan control module with four fans. The fans' running speed can be set to 16 different levels. The speed is controlled by the switching card according to the installed cards temperature.

In addition the FCU\_1100 includes the ALARM interface connector of the NPT-1100 platform.

**i Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

### FCU\_1100 Front Panel



### FCU\_1100 Front Panel Components

Marking	Full Name	Type	Color	Function
ACT.	System active	LED	Green	Normally on when the fan unit is powered on. Off indicates a power failure of the fan unit.
FAIL	System fail	LED	Red	Normally off. Lights when a fan failure is detected.
ALARM	Alarm connector	SCSI 36-pin connector	-	Alarm input and output interface connecting to the RAP.

## NPT-1100 Power Feed Subsystem

### Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. Alternatively, a single AC power feed can be used.

### Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-1100 supports the following types of power supply modes.

- -48 VDC power feed ([INF-B1UH](#)), configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- Dual input DC power supply ([INF-B1U-D](#)), where only the PSA slot can be assigned.
- 100-240 VAC power source ([AC\\_PS-B1UH](#)), utilizing an external power line connection through a power conversion module to implement AC/DC conversion.

The following flexible power supply configuration options are supported:

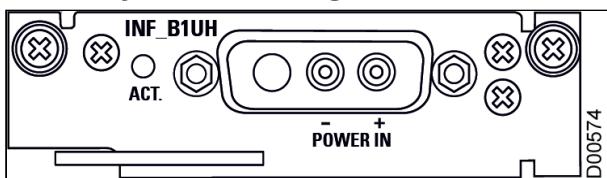
- Single DC 1+0
- Dual DC 1+1 (redundant)
- DC dual feeding
- Single AC 1+0

## INF\_B1UH Overview

The INF\_B1UH is a DC power-filter module that can be plugged into the platform. Two INF\_B1UH modules are needed for power feeding redundancy. It performs the following functions:

- Single DC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected
- High-power INF for up to 450 W

**Control System Block Diagram**

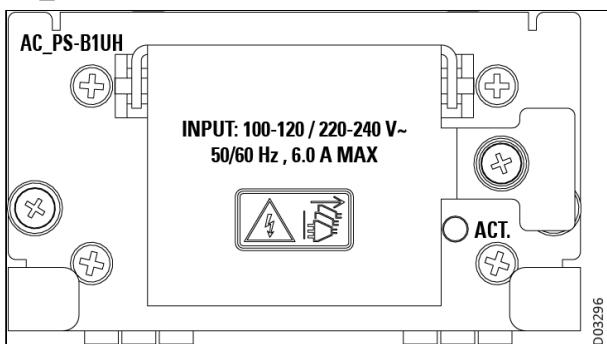


## AC\_PS-B1UH Overview

The AC\_PS-B1UH is a 100-240 VAC power source utilizing an external power line connection through a power conversion module to implement AC/DC conversion. This module occupies two power slots, working in a non-redundant mode. The AC\_PS-B1UH performs the following functions:

- Single AC power input and power supply for all modules in the NPT-1100
- Input filtering function for the entire NPT-1100 platform
- Adjustable output voltage for fans in the NPT-1100
- High-power AC power supply for up to 420W (100-120 VAC and 45°C (113°F) max working temperature) or 480W (220-240 VAC and 55°C (131°F) max working temperature)

**AC\_PS-B1UH Front Panel**



## NPT-1100 Traffic and Switching Functionality

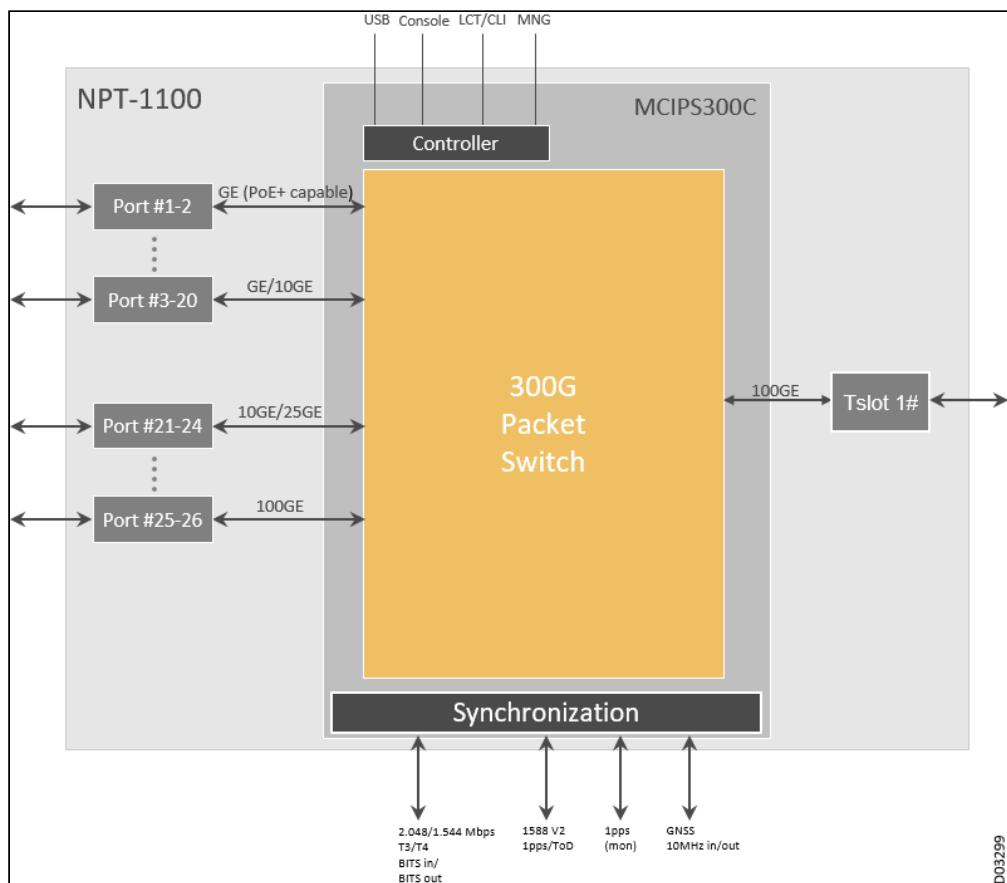
The NPT-1100 is a cost-effective 5G platform optimized for non-redundant access and pre-aggregation IP/MPLS nodes, offering 100GE, 25GE, 10GE, and GE (PoE+) connectivity for MPLS-TP with IP/MPLS. The NPT-1100 works with a native IP/MPLS and MPLS-TP built-in switching mechanism, supporting native packet-level switching, with a switching interface connectivity of 582G. This mechanism provides 300G of non-blocking traffic management throughput, designed to support 5G packet transport requirements.

The NPT-1100's built-in switch provides the following main functions:

- All Native Ethernet packet switch, supporting native packet-level switching with a 582G switching capacity (port fan-out) and up to 300G traffic management (packet processing), providing:

- Management and internal control
- User traffic switching
- Non-blocking data switch fabric up to 300G (IMIX)
- OTSOP16 Smart SFP supported in SFP+\_10GE ports
- 5G-ready packet transport, including:
  - Stringent phase synchronization requirement for Class C/D timing accuracy compliance (8273.2)
  - 100G and 25G interfaces
- Comprehensive range of timing and synchronization capabilities (G.781/G.8262 compliant EEC, G.8273.2):
  - T3/T4 BITS
  - GNSS built-in receiver
  - 1PPS and ToD interfaces
  - 10MHz
  - APTS
  - SyncE
  - IEEE 1588v2 PTP with:
    - OC (primary & secondary), BC
    - One-step TC
    - G.8275.1 profile
    - G.8275.2 profile (NPT-1100H only)
    - G8273.2 Class C/D timing accuracy compliance
- Traffic management (TM) including:
  - Guaranteed CIR
  - E2E flow control
  - 8 x CoS for differentiated services
- Any-slot-to-any-slot connectivity

### 300G Packet Switch



## NPT-1100 Tslot IO Modules

The NPT-1100 has a single Tslot for installing I/O modules. The following table lists the different types of I/O modules that can be installed in the NPT-1100, with links to each module listed.

### *i* Notes

Maximum port fan-out capabilities at the port rate level:

- 3 (2 [base shelf] + 1 [Tslot]) x 100GE
- 8 (4 [base shelf] + 4 [Tslot]) x 25GE
- 26 (22 [base shelf] + 4 [Tslot]) x 10GE
- 30 (20 [base shelf] + 10 [Tslot]) x 1GE
- 32 [Tslot] x E1/T1

	Max 1GE ports	Max 10GE ports	Max 100GE ports
NPT-1100	30	26	3

**NPT-1100 Tslot Modules**

Description	Card
CES multiservice module with 3 x DS3 interfaces and 1 x STM-1/OC3 interface (future)	<a href="#">MS345_3</a>
CES multiservice module with 24 x DS3 interfaces	<a href="#">MS345_24</a>
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	<a href="#">MSC_2_8</a>
CES multiservice module with 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<a href="#">MS1_4</a>
CES multiservice module with 32 x E1/T1 interfaces	<a href="#">MSE1_32</a>
Electrical 4 x GE (SGMII) interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4EB</a>
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	<a href="#">DHGE_8S</a>
Optical 10 x GE module with direct connection to the packet switch	<a href="#">DHGE_10</a>
Optical 4 x 10GE interface module with direct connection to the packet switch	<a href="#">DHXE_4</a>
40G card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces	<a href="#">DHXE_4MR</a>
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces  All 4 ports support MACsec capability	<a href="#">DHXE_4MRsec</a>
In the NPT-1100 this 40G MACsec card supports: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 10GE/1GE ports</li></ul> All 4 ports support MACsec capability.	<a href="#">DHXE_4sec</a>
Optical 4 x 10GE/OTU-2 interface module with direct connection to the packet switch with OTN wrapping	<a href="#">DHXE_4O</a>
100G card that supports up to 4 x 10GE/25GE (based on SFP+), as well as 5G time stamping accuracy	<a href="#">DH25_4MR</a>

Description	Card
Optical 100GE QSFP28 interface module with direct connection to the packet switch	DHCE_1Q
Optical 100GE QSFP28/QSFP_DD interface module with direct connection to the packet switch	DHCE_1QB/1QC

# NPT-1050 System Architecture

## NPT-1050 Platform



NPT-1050 eliminates the boundaries between data and voice communication environments, and paves the way for service provisioning without sacrificing equipment reliability, robustness, and hard QoS (H-QoS). Thus, both operators and service providers benefit from the best of both worlds: the cost-effectiveness and universality of Ethernet and H-QoS, and the scalability and survivability of TDM.

Used in many sub network topologies, NPT-1050 can handle a mixture of P2P, hub, and mesh traffic patterns. This combined functionality means that operators benefit from improved network efficiency and significant savings in terms of cost and footprint.

The NPT-1050 platform:

- Increases the number of Ethernet interfaces, and upgrades from 10M to 10GE and 100GE easily and smoothly.
- Allows you to start as small as necessary and attain ultrahigh expandability in a build-as-you-grow fashion by combining the standard Neptune unit with an expansion unit (EXT-2U/eEXT-2UH).
- Aggregates traffic arriving over Ethernet, PCM low-bitrate interfaces, E1/T1 and STM-1 directly over GbE/10GbE/100GbE.
- Is suitable for indoor and outdoor installations.
- Supports an extended operating temperature range up to 70°C (158°F).

This fully redundant Packet Optical Access (POA) platform offers enhanced MPLS-TP and IP/MPLS data network functionality, providing L1, L2VPN, and L3VPN based services according to the MEF CE3.0 standards. The NPT-1050 includes full traffic and IOP protection and the complete range of Ethernet-based services (CES, MoE, IP, and PoE). TDM support through CES includes SAToP, CESoPSN, and CEP capabilities. The NPT-1050 aggregates traffic arriving over Ethernet, PCM low-bitrate interfaces, E1/T1 and STM-1 directly over GbE/10GbE/100GbE.

The NPT-1050 is designed around a centralized packet switching card that supports any to any direct data card connectivity as well as efficient switching capacity. The platform can be configured with either the MCPS100 switching card (100G packet switch) or the MCIPS300 switching card (300G packet switch).

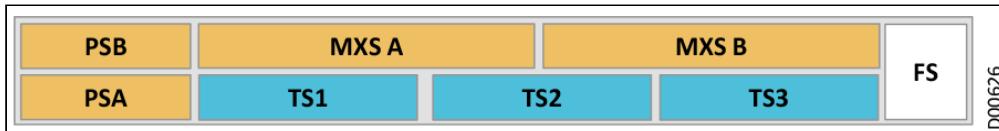
The NPT-1050 is a 1U base platform housed in a 44 mm high, 440 mm wide, and 243 mm deep (1.73 in. x 17.32 in. x 9.57 in.) equipment cage with all interfaces accessible from the front of the unit. The platform includes the following components:

- Two slots (MXS A, MXS B) for redundant packet switching cards for robust provisioning of the following functionalities:
  - With MCPS100 switch:
    - 2 SFP+ based 10GbE interfaces.
    - 2/4 SFP/CSFP-based GE interfaces.
  - With MCIPS300 switch:
    - 4 SFP/SFP+ based 1/10GbE interfaces.
    - Comprehensive range of timing and synchronization capabilities (T3/T4, ToD, and 1pps).
    - In band management interfaces.
- Non redundant mode with a single MCPS100/MCIPS300 matrix and optional AIM100/AIM300 traffic card.
- Three I/O card slots (TS1-TS3), for processing a comprehensive range of traffic interfaces, including Ethernet Layer2/MPLS, Layer3, and IP/MPLS. The Tslots can be configured for up to 100GbE service.

- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+ 10GE ports
- Traffic connector for the (optional) EXT-2U/eEXT-2UH expansion unit.
- Fan unit (FCU\_1050, in slot FS) with alarm indications and monitoring.
- Power supply (PSA, PSB), available in two modes:
  - -48 VDC power feed (INF\_B1UH), configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
  - 100-240 VAC power source (AC\_PS-B1UH) utilizes an external power line connection through a power conversion module to implement AC/DC conversion.

The NPT-1050 can be installed in 2,200 mm or 2,600 mm ETSI racks or in 19" racks. The rugged platform design makes this platform suitable for street cabinet use, withstanding temperatures up to 70°C (158°F). Typical power consumption for the NPT-1050 is less than 250W. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

### NPT-1050 Slot Arrangement



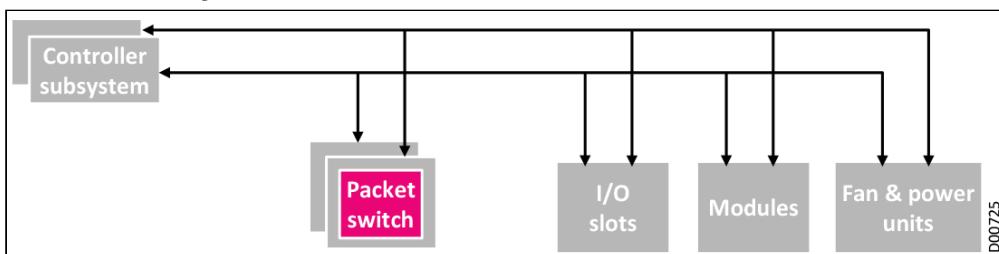
For a complete list of the modules that can be configured in each NPT-1050 slot, see [NPT-1050 Tslot IO Modules](#). All cards support live insertion. All cards are connected using a backplane that supports one traffic connector to connect the NPT-1050 and the EXT-2U. The NPT-1050 platform provides full 1+1 redundancy in power feeding, packet switching, and the TMU, as well as 1:N redundancy in the fans.

This section introduces the following NPT-1050 features:

- [NPT-1050 Control Subsystem](#)
- [NPT-1050 Communications with External Equipment and Management](#)
- [NPT-1050 Timing](#)
- [NPT-1050 Cooling Subsystem](#)
- [NPT-1050 Power Feed Subsystem](#)
- [NPT-1050 Switching Cards](#)
- [NPT-1050 Tslot IO Modules](#)
- [NPT-1050 Expansion Platform](#)

## NPT-1050 Control Subsystem

### Controller Subsystem



NPT-1050 control and communication functions include:

- Internal control and processing
- Communication with external equipment and management
- Network element (NE) software and configuration backup
- Built-in Test (BIT)

### Software and Configuration Backup

The platform features a large-capacity on-board NVM that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

### Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection
- Protection switch for the main switching card

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

## NPT-1050 Communications with External Equipment and Management

In the Neptune metro access platform product line, the main controller card is responsible for communicating with other NEs and management stations.

The main controller card communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems via the DCN. In-band Management Control Channel (MCC) is supported in the platforms as well, enabling NE management through in-band channels.

### Usage Guidelines

The NPT-1050 (with MCPS100) supports in-band and management communication channel (MCC) connections for PB and MPLS:

- 4 Mbps policer for PB UNI which connects to external DCN
- 10 Mbps shaper for MCC packet to MCP
- No rate limit for the MNG port rate, up to 100M full duplex
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, static routes, management VLAN
  - IPv6: Over management VLAN, static routes

The NPT-1050 (with MCIPS300) supports in-band and management communication on the following interfaces:

- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- In-band management processing (20Mbps)
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-IS v6, static routes

## NPT-1050 Timing

This platform provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations for functionality and performance.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed redundantly from the TMUs to all traffic and matrix cards, minimizing unit types and reducing operation and maintenance costs.

The TMU and the internal and external timing paths are fully redundant. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem. In case of hardware failure, the redundant synchronization subsystem takes over the timing control with no traffic disruption.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- 1PPS and ToD interfaces, using external timing input sources
- 2 x 2 MHz/Mbps (T3) external timing input sources
- NTP support
  - NTPv1, NTPv2, NTPv3, and NTPv4 (with MCIPS300)
  - SNTPv4, support for unicast client and unicast server mode only (with MCPS100)
- E1/T1 interfaces of CES cards
- STM-1/4 of CES cards
- Local interval clock
- Holdover mode
- SyncE
- 1588v2 - Primary, Secondary, transparent, and boundary clock

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization, which is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262, G.8263, and G.8264.

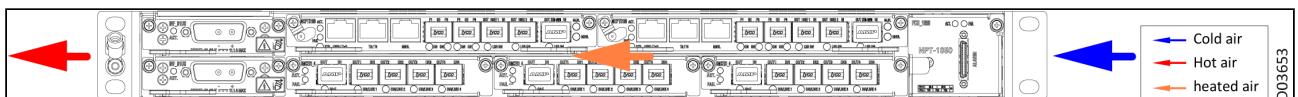
The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. IEEE 1588v2 (G.8265.1/G.8275.1) is supported in the platform, providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <20ns (G.8273.2 Class B) timing error per NE.

## NPT-1050 Cooling Subsystem

The NPT-1050 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components, and cools them.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

## Airflow in the NPT-1050



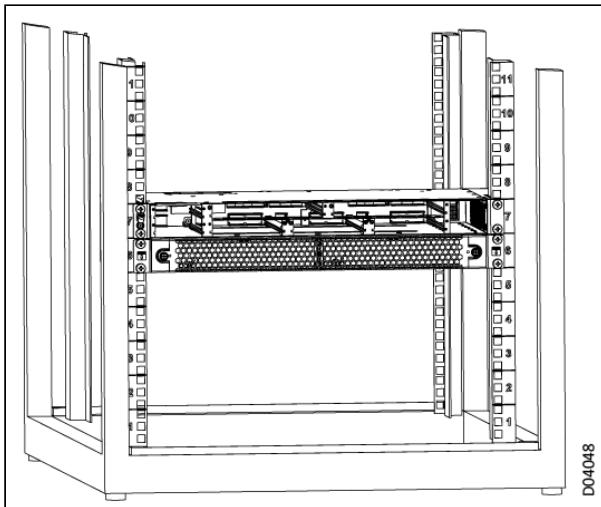
### Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The NPT-1050 platform can be configured together with an air baffle unit, installed in either a 19" or 23" rack.

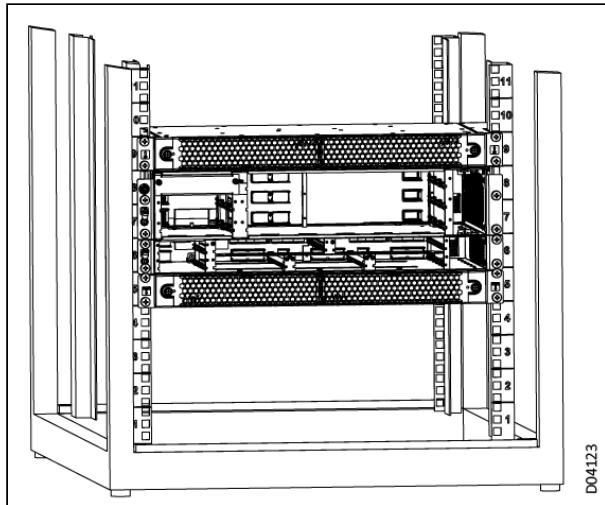
- In the 19" rack, the 1U air baffle unit is located directly below the NPT-1050 platform. The platform and air baffle unit together occupy a total space of 2U height in the rack. The air baffle unit should be installed *before* the NPT-1050 platform; the NPT-1050 platform is then inserted *above* the air baffle unit. Note that a total space of 3U height must be available in the rack for the installation process; see the NPT-1050 Installation and Maintenance Manual for the installation procedure details and limitations.

### 1U Height Platform Installed in 19" Rack over Air Baffle Unit

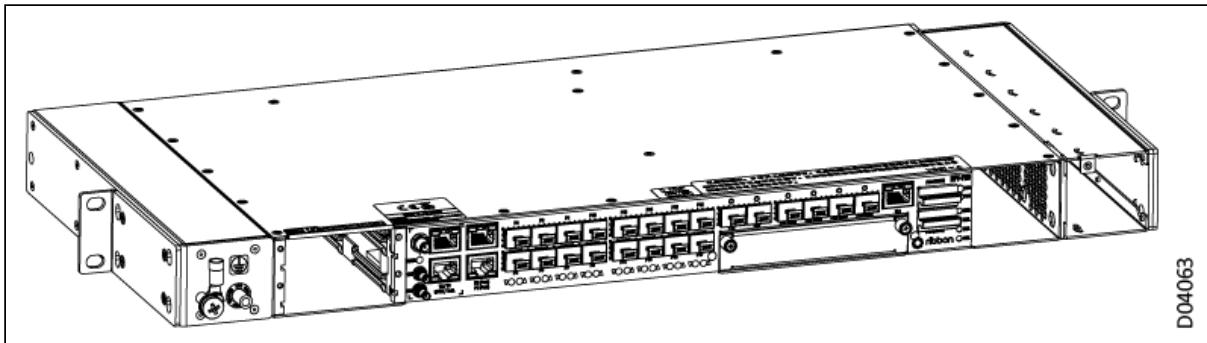


- In the 19" rack, if the NPT-1050 platform is configured with an EXT-2U expansion unit, then the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* where the NPT-1050 platform will be located, and one located directly *above* where the EXT-2U unit will be located.
  - First install the EXT-2U unit on the NPT-1050 platform.
  - Then assemble the air baffle unit (including the 2 air-flow boxes) in the 19" rack.
  - Finally, insert the combined NPT-1050 platform with the EXT-2U expansion unit into the gap between the upper and lower air-flow boxes.

The combination of NPT-1050 platform with EXT-2U expansion unit and 2 air-flow boxes occupies a total space of 5U height in the rack.

**1U Height Platform Plus Expansion Unit Installed in 19" Rack Between Two Air-Flow Boxes**

- In the 23" rack, the air baffle unit is installed as 2 1U air ducts placed to the right and left sides of the NPT-1050 platform, requiring a total space of 1U height to be available in the rack, since the air ducts don't add anything to the platform height.

**1U Height Platform Installed with Air Baffle Unit in 23" Rack**

- In the 23" rack, if the NPT-1050 platform is configured with an EXT-2U expansion unit, then a second set of 2U air ducts is installed on either side of the EXT-2U expansion platform. The combination of NPT-1050 platform with EXT-2U unit and 2 sets of air ducts requires a total space of 3U height to be available in the rack, since the air ducts don't add anything to the platform height.

When installing the NPT-1050 platform together with air baffles in a 19" rack, with or without an EXT-2U expansion unit, the internal air filters in the NPT-1050 platform (and EXT-2U unit, if also installed) must be removed. When installing the platform, with or without an expansion unit, in a 23" rack, only the internal air filter in the NPT-1050 platform must be removed. External air filters are available; see the *NPT-1050 Installation and Maintenance Manual* for details.

**FCU Fan Control Module**

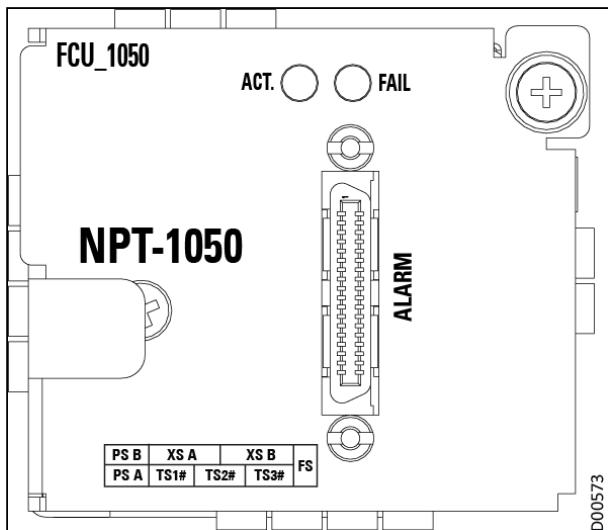
The NPT-1050 platform is cooled through the FCU\_1050, a pluggable fan control module with four fans. The fans' running speed can be set to 16 different levels. The speed is controlled by the MCPS/MCPTS/AIM cards, according to the installed cards temperature.

In addition, the FCU\_1050 includes the ALARM interface connector of the NPT-1050 platform.

**Note:**

Neptune platform configuration includes fan control units (FCUs), cooling units consisting of multiple fans. In case of a problem with the FCU functioning, such as a fan failure, an alarm is triggered. The platform can continue operation for a very short period of time, as long as the maximum ambient temperature does not exceed 40°C (104°F) for short term operation of up to 96 hours, as noted in the NEBS GR-63 Core i4 standard. The exact window of time you have may vary, depending on the operating conditions and the platform configuration, especially the types of cards installed. However, the malfunctioning fan unit must be replaced as soon as possible.

**FCU\_1050 Front Panel**



**FCU\_1050 Front Panel Components**

Marking	Full name	Type	Color	Function
ACT.	System active	LED	Green	Normally on when the fan unit is powered on. Off indicates a power failure of the fan unit.
FAIL	System fail	LED	Red	Normally off. Lights when a fan failure is detected.
ALARM	Alarm connector	SCSI 36-pin connector	-	Alarm input and output interface connecting to the RAP.

## NPT-1050 Power Feed Subsystem

### Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. Alternatively, a single AC power feed can be used.

## Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-1050 offers two power supply modes.

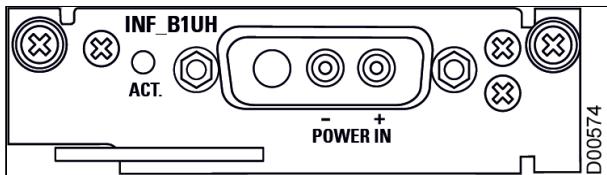
- -48 VDC power feed ([INF\\_B1UH](#)), configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- 100-240 VAC power source ([AC\\_PS-B1UH](#)) utilizes an external power line connection through a power conversion module to implement AC/DC conversion.

## INF\_B1UH Power Module Overview

The INF\_B1UH is a DC power-filter module that can be plugged into the platform. Two INF\_B1UH modules are needed for power feeding redundancy. It performs the following functions:

- Single DC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected
- High-power INF for up to 450 W

### INF\_B1UH Front Panel

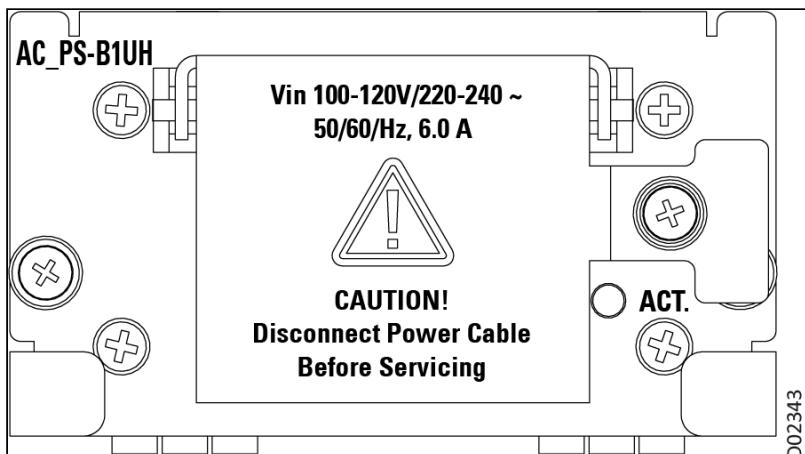


## AC\_PS-B1UH Power Module Overview

The AC\_PS-B1UH is a 100-240 VAC power source utilizing an external power line connection through a power conversion module to implement AC/DC conversion. This module occupies two power slots, working in a non-redundant mode. The AC\_PS-B1UH performs the following functions:

- Single AC power input and power supply for all modules in the NPT-1050
- Input filtering function for the entire NPT-1050 platform
- Adjustable output voltage for fans in the NPT-1050
- High-power AC power supply for up to 420W (100-120 VAC and 45°C (113°F) max working temperature) or 480W (220-240 VAC and 55°C (131°F) max working temperature)

### AC\_PS-B1UH Front Panel



## NPT-1050 Switching Cards

The NPT-1050 architecture enables its outstanding configuration flexibility. At the heart of the NPT-1050 is a non-blocking switching fabric. The main processing card ([MCPS/MCIPS](#)) integrates functions such as control, communications, timing, and overhead processing, in addition to the essential packet switching capabilities.

The NPT-1050 platform operates with different matrix cards, depending on the configuration. The platform must be equipped with two switching cards of the same type to support system redundancy. For a non-redundant configuration, the second switching card slot can be configured with the AIM100/AIM300 card, or left empty. The following switching and control cards and aggregate modules are supported:

- [MCPS100](#): Main controller processor (MCP) and central packet switching card; provides system control and management. This central packet switch supports 100G packet switching, including timing control. The card also supports 4 x GE CSFP based, or 2 x GE SFP based ports, and 2 x 10 GE SFP+ based interfaces.
- [MCIPS300](#): Central switching card that provides dual stack packet switching (L2, L3, MPLS-TP, and IP/MPLS). Also provides main control, communication, and overhead processing functionality. Most convenient for applications that require very high volume of pure packet handling including support for dynamic L2/L3 VPN services. The card also supports multi-rate 4 x 10G/GE SFP+ based aggregation interfaces via corresponding ports.
- [AIM100](#): Aggregate interface module, configured together with a single MCPS100 switching card to provide additional multi-rate 4 x 10G/GE ports in a 1+0 (nonredundant) configuration.
- [AIM300](#): Aggregate interface module, configured together with a single MCIPS300 switching card to provide additional multi-rate 4 x 10G/GE ports in a 1+0 (nonredundant) configuration.

The following sections detail the functionality of the NPT-1050 switching cards.

- [MCPS and MCIPS Control Functionality](#)
- [MCPS100 Switching Card](#)
- [MCPS100 Functional Description](#)
- [MCIPS300 Switching Card](#)
- [MCIPS300 Functional Description](#)
- [AIM100 Aggregate Interface Module Overview](#)
- [AIM300 Aggregate Interface Module Overview](#)

## MCPS and MCIPS Control Functionality

The MCPS/MCIPS modules are the main processing cards of the NPT-1050. These cards integrate functions such as control, communications, and overhead processing, providing:

- Control functions:
  - Communications with and control of all other modules in the NPT-1050 and EXT-2U through the backplane (by the CPU).
  - Communications with the EMS-NPT, LCT-NPT, or other NEs through a management interface (MNG), or MCC, or VLAN.
  - Alarms and maintenance.
  - Fan control.
- External timing reference interfaces (T3/T4), which provide the line interface unit for a single 2 Mbps T3/T4 interface and a single 2 MHz T3/T4 interface. (1.5 MHz and 1.5 Mbps are also available for SONET mode.)

MCPS/MCIPS supports the following interfaces from its front panel:

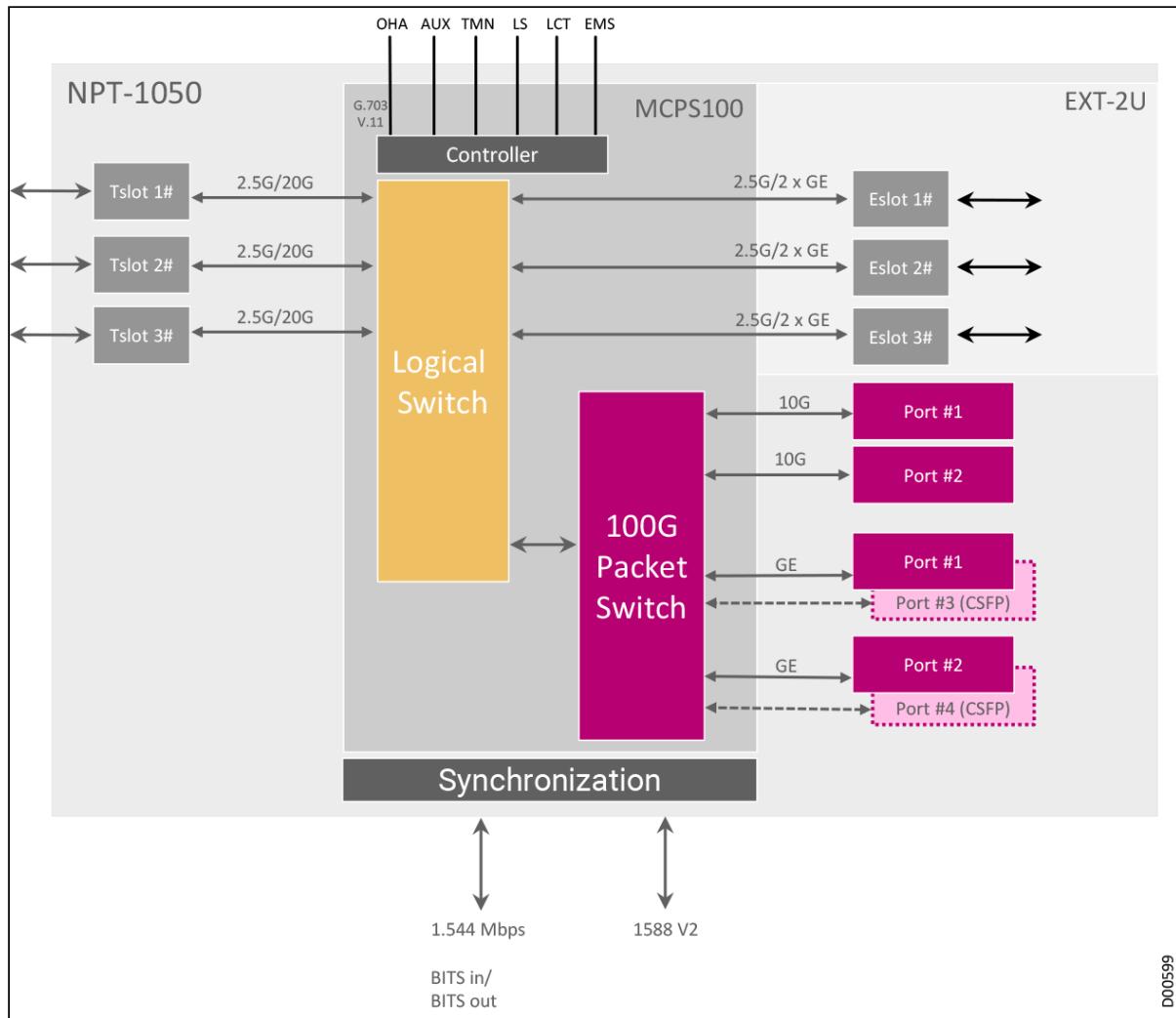
- MNG for management
- T3/T4 for timing
- 1PPS/ToD for timing

## MCPS100 Switching Card

The MCPS100 is a centralized packet switch that supports any to any direct data card connectivity. This matrix card, designed for use in the NPT-1050 metro access platform, offers a choice of capacity and configuration options, including:

- All-Native Ethernet packet switch, supporting native packet-level switching with a 100G switching capacity with up to 72G traffic management (MPLS processing), providing:
  - Management and internal control, in addition to user traffic switching
  - Non-blocking data switch fabric
  - P2P MPLS internal links via the packet switch
  - Both redundant and non-redundant modes
- Traffic management, including:
  - Guaranteed CIR
  - Two CoS (within the switch)
  - End-to-end flow control
- Any card installed in any slot
- Any slot to any slot connectivity
- Aggregate ports:
  - 2x10GE SFP+ based interfaces
  - 4xGECSFP based interfaces
  - 2xGE SFP based interfaces
- Comprehensive range of timing and synchronization capabilities (ToD, 1pps)

### Traffic Flow in an NPT-1050 Configured with an MCPS100 Switching Card



D00599

## MCPS100 Functional Description

The MCPS100 card has three main subsystems:

- **Main processing and control:** Performs all integrated functions like control, communication, and overhead processing.
- **Central packet switch:** Performs all the NPT-1050 packet switching operations.
- **TMU:** Generates and distributes timing and clock signals to all the cards installed in the NPT-1050 platform. In addition to its internal timing reference, the TMU can use up to four user-specified reference sources. See Timing for a description of the TMU capabilities.

The MCPS100 card is a critical NPT-1050 subsystem, and therefore, for redundancy purposes, two MCPS100 cards should be installed in any NPT-1050 platform, one on each side of the cards cage. Both cards must be of the same type and option and running the same NPT-1050 release.

When two identical cards are installed in the platform, the cards operate in a primary-secondary configuration:

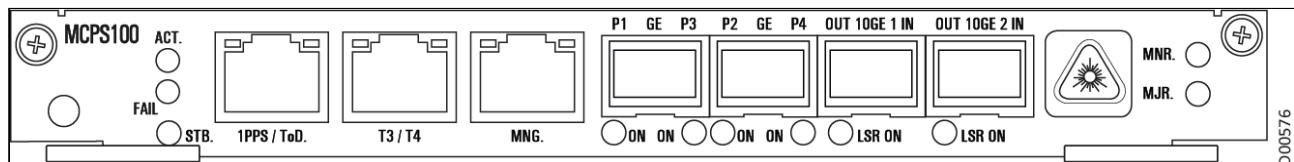
- At any time, only one card is active and the other is in standby.
- Upon failure or removal of the active card, the standby card becomes active without any disruption in system operation.

A MCPS100 card can be inserted and replaced without affecting traffic flow.

**Note**

During an upgrade, a different card version or release can be installed in the platform. With appropriate planning, the upgrade can be non-traffic-affecting.

### MCPS100 Front Panel



**LEDs**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the MCPS100 can't be downloaded successfully or that the MCPS100 cannot be controlled normally. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the MCPS100 card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STBY	System standby	Orange	Lights when the card is in standby. Off when the card is active.
MJR.	System major alarm	Red	Lights when the system has a critical or major alarm.
MNR.	System minor alarm	Yellow	Lights when the highest severity of the NE current alarms is minor or warning. Off when the system has no alarm or the highest severity of the NE current alarms is higher than minor or warning.
LSR ON (separate LED for each 10GE port)	Laser on indication	Green	Lights steadily when laser is on.
ON (separate LED for each GE port, P1 to P4)	Laser on indication	Green	Lights steadily when laser is on.

## Interfaces

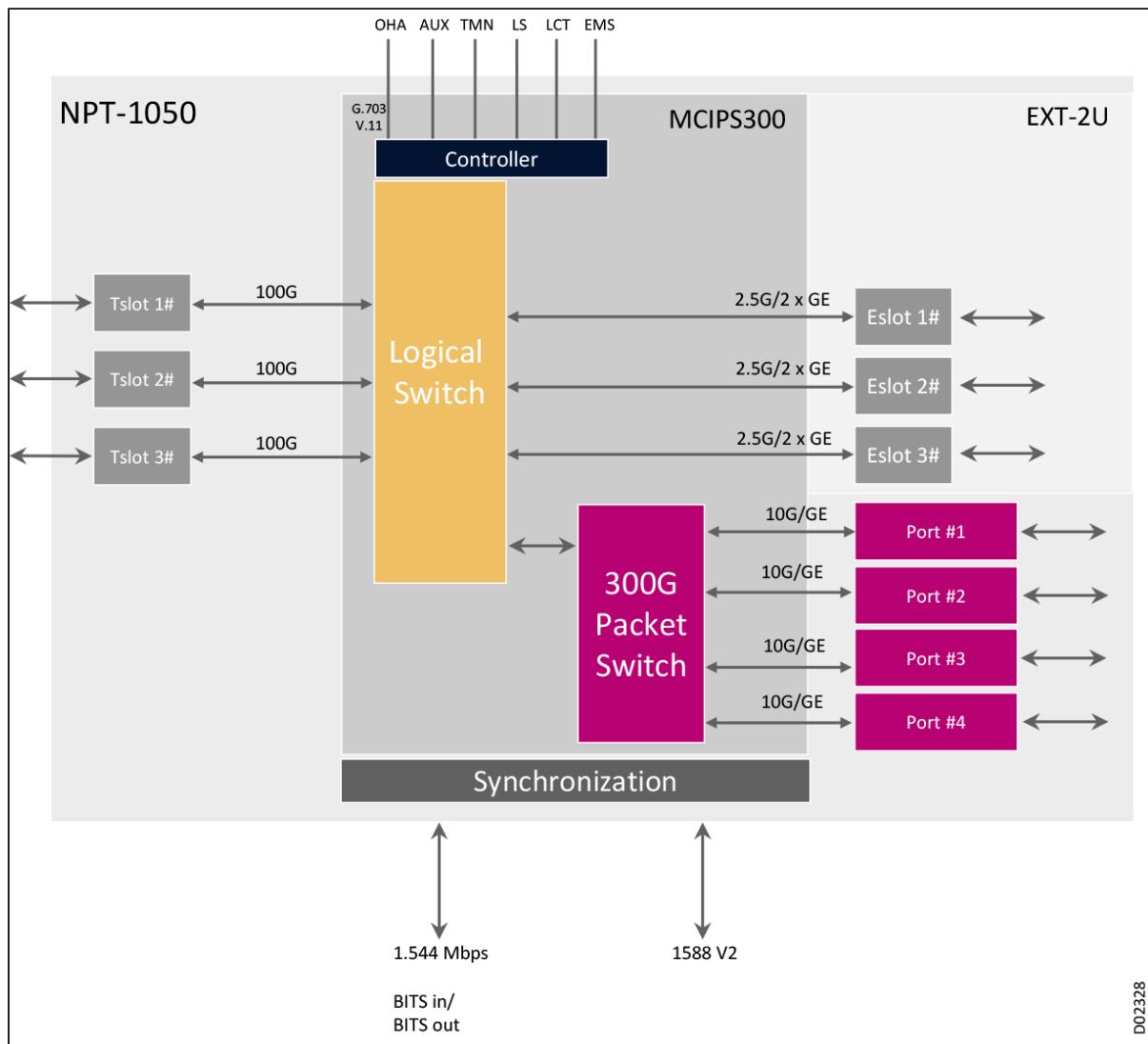
Marking	Interface Type	Function
1PPS/ToD	RJ-45	1PPS and Time of Day input/output signals for supporting Ethernet timing per IEEE 1588v2 standard.
T3/T4	RJ-45	T3 and T4 timing interfaces (one 2 Mbps/1.5 Mbps and one 2 MHz/1.5 MHz).
MNG.	RJ-45	10/100BaseT Ethernet interface for management.

## MCIPS300 Switching Card

The MCIPS300 is a centralized packet switch that supports any to any direct data card connectivity. This matrix card, designed for use in the NPT-1050 metro access platform, offers a choice of capacity and configuration options, including:

- All-Native Ethernet packet switch, supporting native packet-level switching with a 380G switching capacity with up to 300G traffic management (MPLS processing), providing:
  - Management and internal control
  - User traffic switching
  - Non-blocking data switch fabric
  - P2P MPLS internal links via the packet switch
  - Both redundant and non-redundant modes
- Traffic management, supporting guaranteed CIR and DiffServ with 8 CoS
- Any card installed in any slot
- Any slot to any slot connectivity
- Aggregate ports:
  - 4x10GE/GE SFP+ based interfaces
  - Multi-rate support, including 10M/100M/1G/10G
  - Multi-media support, including 10/100/1000Base-T copper interface, 100/1000Base-X optical interface, and 10GBase-R optical interface
  - E1POP Smart SFP supported in 1000Base-T ports
  - OTSOP16 Smart SFP supported in SFP+\_10GE ports
- 25G interfaces through an I/O card in the Tslot
- Comprehensive range of timing and synchronization capabilities (ToD, 1pps)
- Supports MPLS-TP
- Supports IP/MPLS
- High capacity backplane connectivity for 100GE interfaces (up to 3 in a platform)
- Redundant controller with SD flash

### MCIPS300 Traffic Flow



**(i) Optional Feature:**

MCIPS300 matrix is available in two variants: default switching capacity (100G) and full switching capacity (380G); it is possible to unlock the default capacity limit to utilize full capacity with a software license.

## MCIPS300 Functional Description

The MCIPS300 card has three main subsystems:

- Main processing and control:** Performs all integrated functions like control, communication, and overhead processing.
- Central packet switch:** Performs all the NPT-1050 packet switching operations.
- TMU:** Generates and distributes timing and clock signals to all the cards installed in the NPT-1050 platform. In addition to its internal timing reference, the TMU can use up to four user-specified reference sources. See Timing for a description of the TMU capabilities.

The MCIPS300 card is a critical NPT-1050 subsystem, and therefore, for redundancy purposes, two MCIPS300 cards should be installed in any NPT-1050 platform, one on each side of the cards cage. Both cards must be of the same type and configuration and running the same NPT-1050 release version.

When two identical cards are installed in the platform, the cards operate in a primary-secondary configuration:

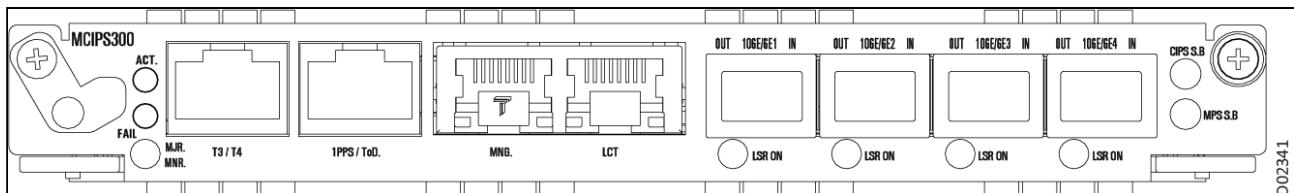
- At any time, only one card is active and the other is in standby.
- Upon failure or removal of the active card, the standby card becomes active without any disruption in system operation.

A MCIPS300 card can be inserted and replaced without affecting traffic flow.

**i Note**

During an upgrade, a different card version or release can be installed in the platform. With appropriate planning, the upgrade can be non-traffic-affecting.

### MCIPS300 Front Panel



### MCIPS300 Front Panel Interfaces

Marking	Interface Type	Function
T3/T4	RJ-45	T3 and T4 timing interfaces (one 2 Mbps/1.5 Mbps and one 2 MHz/1.5 MHz)
1PPS/ToD	RJ-45	1PPS and Time of Day input/output signals supporting Ethernet timing per IEEE 1588v2 standard
MNG.	RJ-45	10/100BaseT Ethernet interface for management.
LCT/CLI	RJ-45	Local management port for connecting an LCT or CLI station
SFP+	SFP+	4 x SFP+ (10G/GE) <ul style="list-style-type: none"> <li>• OTP10/OTP10C/OTP10D/OTP10T_XX for 10GE</li> <li>• OTGBE_XX for optical GE</li> <li>• OTFE_FXSG/LXSG for optical FE</li> <li>• ETGBE for 10/100/1000Base-T</li> </ul>

### MCIPS300 Indicators and Functions

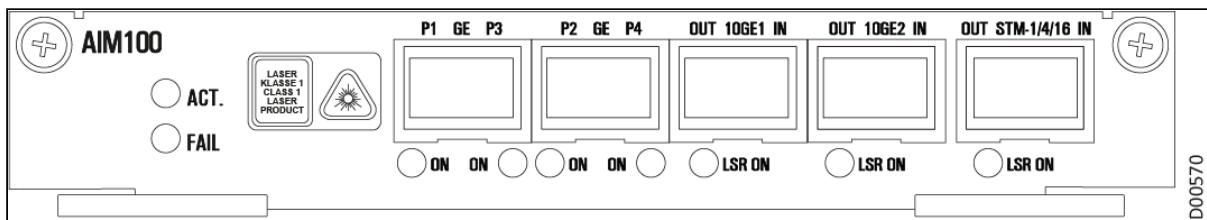
Marking	Full name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the MCPS100 can't be downloaded successfully or that the MCPS100 cannot be controlled normally. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the MCPS100 card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STBY	System standby	Orange	Lights when the card is in standby. Off when the card is active.
MJR.	System major alarm	Red	Lights when the system has a critical or major alarm.
MNR.	System minor alarm	Yellow	Lights when the highest severity of the NE current alarms is minor or warning. Off when the system has no alarm or the highest severity of the NE current alarms is higher than minor or warning.
LSR ON (separate LED for each GE/10GE port)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## AIM100 Aggregate Interface Module Overview

The AIM100 is an aggregate interface module (AIM) for the aggregate (MCPS) slot in a non-redundant configuration. The card enables to achieve the max interfaces with one MCPS card as a non-redundant installation .The AIM100, designed for use in the NPT-1050 metro access platform, offers a choice of configuration options for aggregate ports, including:

- 2 x 10 GE SFP+ based interfaces
- 4 x GE CSFP based interfaces
- 2 x GE SFP based interfaces
- 1 x STM-1/4/16 SFP based interface (not usable if MCPS100 is installed)

## AIM100 Aggregate Interface Module



### LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON (P1 to P4)	Laser on indication (GE ports)	Green	Lights steadily when the corresponding laser is on.
LSR ON	Laser on indication (10GE and STM-1/4/16 ports)	Green	Lights steadily when the corresponding laser is on.

## AIM300 Aggregate Interface Module Overview

The AIM300 is an aggregate interface module (AIM) for the aggregate (MCPS) slot in a non-redundant configuration. The card enables achieving the maximum amount of interfaces when used together with a single MCIPS300 card as a non-redundant installation. The combination of a single MCIPS300 in a 1+0 configuration with an AIM300 module provides the same capacity and fan out as a redundant MCIPS300 configuration, but there is no redundancy for the MCP, TMU, and CIPS modules.



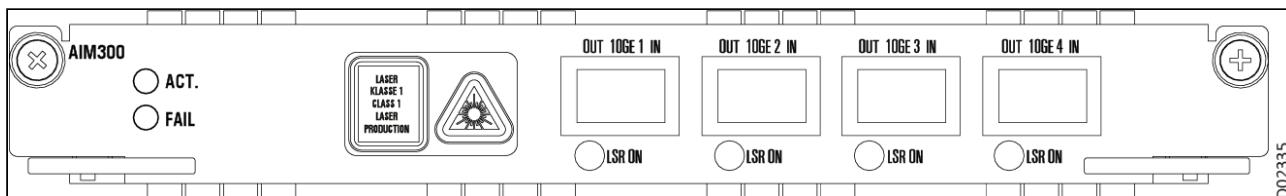
### Tip

When working with a single MICPS300, install the MCIPS300 in the MXSB slot for better cooling.

The AIM300, designed for use in the NPT-1050 metro access platform, offers a choice of configuration option, including:

- 4 x 10G/GE SFP/SFP+ based multi-rate aggregate ports
- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+\_10GE ports

### AIM300 Front Panel



### AIM300 LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P4)	Laser on indication (GE/10GE ports)	Green	Lights steadily when the corresponding laser is on.

## NPT-1050 Tslot IO Modules

The NPT-1050 has three Tslots for installing I/O modules. The following table lists the different types of CES and Ethernet I/O modules that can be installed in the NPT-1050, with links to each module listed.

#### **i** Note

No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by the NPT-1050:

	Max 1GE ports	Max 10GE ports	Max 100GE ports
With <b>MCIPS300</b>	38	20	3
With <b>MCPS100</b>	40	10	N/A

**NPT-1050 Supported Tslot Modules**

Description	Card	TS#1 to TS#3 with MCPS100	TS#1 to TS#3 with MCIPS300
CES multiservice module with 3 x DS3 interfaces and 1 x STM-1/OC3 interface (future)	<a href="#">MS345_3</a>	N/A	TS1-TS3
CES multiservice module with 24 x DS3 interfaces	<a href="#">MS345_24</a>	N/A	TS1-TS3
CES multiservice module with STM-1/STM-4 interfaces	<a href="#">DMCES1_4</a>	TS1-TS3	TS1-TS3
CES multiservice module with 16 x E1/T1 interfaces	<a href="#">MSE1_16</a>	TS1-TS3	N/A
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	<a href="#">MSC_2_8</a>	TS1-TS3	TS1-TS3
CES multiservice module with 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<a href="#">MS1_4</a>	TS1-TS3	TS1-TS3
CES multiservice module with 32 x E1/T1 interfaces	<a href="#">MSE1_32</a>	TS1-TS3	TS1-TS3
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4E</a>	TS1-TS3	N/A
Electrical 4 x GE interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4EB</a>	N/A	TS1-TS3
Optical 8 x GE interface module with direct connection to the packet switch	<a href="#">DHGE_8</a>	TS1-TS3	N/A
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	<a href="#">DHGE_8S</a>	N/A	TS1-TS3

Description	Card	TS#1 to TS#3 with MCPS100	TS#1 to TS#3 with MCIPS300
Optical 10 x GE module with direct connection to the packet switch	DHGE_10	N/A	TS1-TS3
Electrical and optical 16 x GE interface module with direct connection to the packet switch	DHGE_16	TS1+TS2, TS2+TS3	N/A
Optical 24 x GE interface module with direct connection to the packet switch	DHGE_24	TS1+TS2, TS2+TS3	N/A
Optical 2 x 10GE interface module with direct connection to the packet switch	DHXE_2	TS1-TS3	TS1-TS3
Optical 4 x 10GE interface module with direct connection to the packet switch	DHXE_4	N/A	TS1-TS3
Optical 4 x 10GE/OTU-2 interface module with direct connection to the packet switch with OTN wrapping	DHXE_4O	N/A	TS1-TS3
40G MACsec card with: <ul style="list-style-type: none"> <li>• 2 x 10G/OTU-2e (SFP+) ports</li> <li>• 2 x 10G/1GE multi-rate ports</li> </ul> All 4 ports support MACsec capability.	DHXE_4sec	N/A	TS1-TS3
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces  All 4 ports support MACsec capability	DHXE_4MRsec	N/A	TS1-TS3
Optical 100GE QSFP28 interface module with direct connection to the packet switch	DHCE_1Q	N/A	TS1-TS3

Description	Card	TS#1 to TS#3 with MCPS100	TS#1 to TS#3 with MCIPS300
Optical 100GE QSFP28/QSFP_DD interface module with direct connection to the packet switch	DHCE_1QB/1QC	N/A	TS1-TS3
100G card that supports up to 4 x 10GE/25GE (based on SFP+), as well as 5G time stamping accuracy	DH25_4MR	N/A	TS1-TS3

## NPT-1050 Expansion Platform

The traffic capabilities of the Neptune platform can be expanded by configuring the base platform with an EXT-2U or eEXT-2UH expansion unit.

The EXT-2U platform is a high density modular expansion unit for the Neptune multiservice platforms. It supports the complete range of CES, PCM, optics and Ethernet services. Integrating this add-on platform into your network configuration is not traffic-affecting. The EXT-2U is compact and versatile and can be used with different base units from the Neptune product line. The type of traffic delivered by the unit depends on the type of matrix (PCM or Packet only) installed in the base unit. I/O expansion cards are supported in accordance. The EXT-2U has three multipurpose slots (ES1 to ES3) for any combination of extractable traffic cards. PCM, Ethernet, OTN muxponders, optical amplifiers, and CES traffic are all handled through cards in these traffic slots.

The eEXT-2UH is an independent 2U platform that provides 3 I/O slots for TP cards, optical amplifiers, PCM services (with EM\_10E), and GbE fan out (with DHGE\_10\_POE). For example, adding the eEXT-2UH expansion unit to an NPT-1800 platform that is already using an EXT-2U unit would provide more slots for TP protection cards, doubling the amount of E1 protection available, which is an essential feature for large-scale aggregation sites.

The following table list the traffic cards supported in the EXT-2U or eEXT-2UH when installed with the base platform. For a detailed description of the EXT-2U and eEXT-2UH features, functionality, and supported traffic cards, see [EXT-2U Expansion Platform](#) or [eEXT-2UH Expansion Unit](#).

**EXT-2U Supported Traffic Cards for NPT-1050**

<b>Card Type</b>	<b>Card</b>	<b>with MCPS100</b>	<b>with MCIPS300</b>
Multiservice PCM and 1/0 XC card over Ethernet. (EM_10EB can be used in both EXT-2U and eEXT-2UH platforms.)	<a href="#">EM_10E/EM_10EB</a>	E1-E3	E1-E3
Optical Base Card (OBC) for optical amplifiers and DCM modules. (OBC, OBC_B, OBC_C) (OBC_B and OBC_C can be used in both EXT-2U and eEXT-2UH platforms.)	<a href="#">Optical Base Card (OBC)</a>	E1-E3	E1-E3
10G card with up to 10 GbE ports; 4 of the ports support POE++. (Can be used in both EXT-2U and eEXT-2UH platforms.)	<a href="#">DHGE_10_POE</a>	E1-E3	E1-E3
Protection card, provides 1:2 protection for MSE1_32 cards installed in base platform. (Can be used in both EXT-2U and eEXT-2UH platforms.)	<a href="#">TP32_2</a>	E1-E3	E1-E3
Protection card, provides 1:1 protection for MS345_3 cards installed in base platform.	<a href="#">TPS345_1</a>	E1-E3	E1-E3
CES multiservice card with 2 x STM-1/OC-3 and 16 x E1/T1 interfaces.	<a href="#">MSC_2_16E</a>	N/A	E1-E3
Data cards with internal direct connection to the packet switch.	<a href="#">DHFE_12</a>	E1-E3	N/A
Data cards with internal direct connection to the packet switch.	<a href="#">DHFX_12</a>	E1-E3	N/A
CES multiservice card for 32 x E1 interfaces.	<a href="#">DMCE1_32</a>	E1-E3	N/A
Muxponder card with 12 client ports and a slot for installing an MO_AOC4 optical module.	<a href="#">MXP10</a>	E1-E3	N/A

# NPT-1022 Platform Family System Architecture

The NPT-1022 family of platforms (NPT-1022, NPT-1022H, NPT-1022B, and NPT-1022BH) are all extremely compact (1U), high-capacity, 5G-enabled platforms that support flexible and elastic IP and MPLS, Ethernet (MEF CE3.0-compliant), segment routing, and TDM over CES/CEP. NPT-1022 platforms are optimized for access layer node equipment in 5G transport networks.

NPT-1022 platforms all support up to 64G capacity, providing a generous fan-out for 10G/GE interfaces, and optimized for high-capacity CPE and access applications. Neptune streamlines end-to-end metro service delivery by combining carrier-grade service assurance, visibility, and control with packet efficiency and unparalleled multiservice support. Neptune provides a powerful, flexible, and efficient end-to-end metro solution for high-performance L2 and L3 services. It achieves this by converging IP, MPLS, Ethernet, OTN, WDM, and TDM over CES/CEP.

NPT-1022 platforms provide enhanced user platform monitoring by providing a full set of OAM tools, including Dying Gasp signaling capabilities, ensuring effective platform and service management at every stage. NPT-1022 platforms can be installed easily in a short time using Zero Touch Provisioning (ZTP) or Zero Touch Installation (ZTI). Neptune also supports NFV services and SDN applications, which are compulsory in today's challenging metro environment.

With such a rich and robust feature set, the NPT-1022 platforms are well-suited for a wide variety of applications and networking scenarios, including:

- Mobile backhaul, providing a converged access platform, and able to aggregate multiple 3G/4G/LTE/5G base stations
- Triple play, supporting voice, video (IPTV and VoD), and business services
- Utilities, ideal as a sub-station IP GW device and mission critical services carrier
- Business VPN connectivity

## NPT-1022 Front Panel



The NPT-1022 family of platforms offers enhanced data network functionality, including L3 routing and L2 switching, with the full range of MEF CE3.0 services (E-Line, E-LAN, E-Tree, E-Access), PN- and VPN-based Ethernet and IP, MPLS-TP, IP/MPLS, MPLS VPWS, VPLS, L2VPN, L3VPN, LDP for LSP/PW, IPv4 Stack and IPv4 hardware forwarding, OSPF for IPv4, BGP for IPv4, MP-BGP, VRRP, VRF-Lite, multicast, and IPTV, as well as TDM by CES (SAToP, CESoPSN, and CEP) capabilities, in addition to full NETCONF and YANG SDN interface support. Pluggable SFP options include electrical, colored C/DWDM, tunable, non-colored, Compact SFP (CSFP), SFP+, and bidirectional SFPs.

The NPT-1022B platforms provide the same functionality as the NPT-1022, with the following enhancements:

- Built-in GNSS receiver replacing the BITS (T3/4) interface
- Extractable air filter
- Enlarged controller memory to 8G (DDR4)
- F-RAM storage for critical events

The NPT-1022H and NPT-1022BH platforms are hardware variants of the NPT-1022/NPT-1022B platforms, providing the same functionality as the NPT-1022/NPT-1022B, with the addition of G.8275.2 support.

For convenience, we refer to these four platforms (NPT-1022, NPT-1022B, NPT-1022H, NPT-1022BH) platforms as the NPT-1022 family of platforms, except at points where a platform-specific feature is noted.

The NPT-1022 platforms are compact (1U) base platforms housed in a 44 mm high, 440 mm wide, and 266 mm deep (1.73 in. x 17.32 in. x 9.57 in.) equipment cage with all interfaces accessible from the front of the unit. The platform includes the following components:

- Base shelf with the following port fan-out capabilities:
  - 4 x SFP+ 10GE/GE multi-rate ports
  - 4 x RJ45 100/1000 Base-T ports
  - 4 x SFP 1000 Base-X or Base-T ports
  - 8 x SFP 100/1000 Base-X or Base-T ports
- 1 I/O card slot (TS1), providing:
  - Increased port fan-out capacity (additional 10GbE provided by assigning a DHGE\_10 card in the Tslot)
  - Power over Ethernet (PoE+) functionality
- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+\_10GE ports
- Maximum fan-out capabilities:
  - 6 x 10GE
  - 30 x GE, with the following port rates:
    - Ports 1-4, 9-12: 1000M
    - Ports 5-8, 13-20: 100/1000M
- Traffic connector to the (optional) EXT-2U expansion unit
- Comprehensive range of timing and synchronization capabilities, compliant with 5G MBH requirements:
  - T3/T4 BITS (NPT-1022 and NPT-1022H only)
  - GNSS built-in receiver (NPT-1022B and NPT-1022BH only)
  - SyncE
  - IEEE 1588v2 G.8275.1
  - IEEE 1588v2 G.8275.2 (NPT-1022H and NPT-1022BH only)
  - G.8273.2 – Class C compliant
  - 1PPS and ToD
  - Hybrid 1588 and SyncE
  - APTS (NPT-1022B and NPT-1022BH only)
- Console ports
- Flexible input power options:
  - AC/DC in both redundant and non-redundant modes
  - Mixture of AC and DC

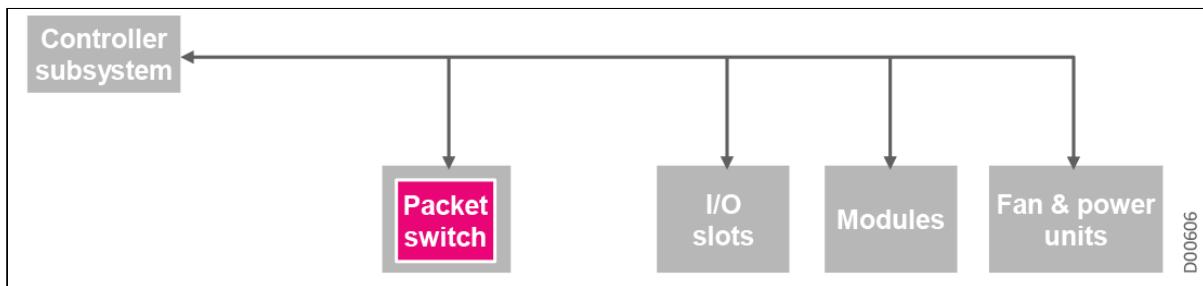
The NPT-1022 platforms can be installed in 2,200 mm or 2,600 mm ETSI racks or in 19" or 23" racks. The rugged platform design also makes this platform suitable for street cabinet use, withstanding temperatures up to 70°C (158°F). Typical power consumption for the NPT-1022 platform family is less than 250W. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

This section introduces the following NPT-1022 family platform features:

- [NPT-1022 Platform Family Control Subsystem](#)
- [NPT-1022 Platform Family Communication with External Equipment](#)
- [NPT-1022 Platform Family Timing](#)
- [NPT-1022 Platform Family Cooling Subsystem](#)
- [NPT-1022 Platform Family Power Feed Subsystem](#)
- [NPT-1022 Platform Family Traffic and Switching Functionality](#)
- [NPT-1022 Platform Family Tslot IO Modules](#)
- [NPT-1022 Platform Family Expansion Platform](#)

# NPT-1022 Platform Family Control Subsystem

**Control System Block Diagram**



The platform control and communication main functions include:

- Internal control and processing
- Network element (NE) software and configuration backup
- Communication with external equipment and management
- Built-in Test (BIT)

## Internal Control and Processing

The NPT-1022 controller provides central control, configuration, alarm, maintenance, and communication functions for NPT-1022. It can also communicate with the control processors of various cards in the extension unit, using a primary-secondary control hierarchy.

The NPT-1022 controller can also provide an NE management interface for management stations (EMS/LCT), support MCC, and channel management VLAN processing.

## Software and Configuration Backup

The platform features a large-capacity on-board NVM that stores a complete backup of the system's software and node configuration. This ensures superior management and control availability.

The main controller card enables easy software upgrades using a remote software procedure operated from the EMS-NPT management station or LCT-NPT craft terminal. The card can store two different software versions simultaneously, and enables a quick switchover between different versions when required.

## Built-in Test

The BIT hardware and its related software assist in the identification of any faulty card or module.

The BIT outputs provide:

- Management reports
- System reset
- Maintenance alarms
- Fault detection
- Protection switch for the main switching card

Dedicated test circuits implement the BIT procedure under the control of an integrated software package. After the platform is switched on, a BIT program is automatically activated for both initialization and normal operation phases. Alarms are sent to the EMS-NPT if any failures are detected by the BIT.

BIT testing covers general tests, including module presence tests and periodic sanity checks of I/O module processors. It performs traffic path tests, card environment tests, data tests, and detects traffic-affecting failures, as well as failures in other system modules.

# NPT-1022 Platform Family Communication with External Equipment

In the Neptune metro access product line, the main controller unit is responsible for communicating with other NEs and management stations.

The main controller unit communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other NEs via the in-band MCC. Communication between other NEs, or between the NEs and the EMS/LCT, can also be via the out-of-band DCN. The controller can connect to the DCN via Ethernet.

## Usage Guidelines

The NPT-1022 supports in-band and DCN management connections for PB and MPLS:

- 20 Mbps shaper for MCC packet to MCP
- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-ISv6, static routes

# NPT-1022 Platform Family Timing

The NPT-1022 platforms were designed as 5G backhauling platforms. As such, they provide high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations, such as 1588v2 PTP according to G.8273.2 standard at Class C support level.

The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed from the TMU to all base shelf ports and Tslot cards, minimizing unit types and reducing operation and maintenance costs. The high-level distributed BIT mechanism ensures top performance and availability of the synchronization subsystem.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously.

- 2 x 2048K/1544K Hz, E1/T1 (T3/T4 BITS) external timing input/output sources (NPT-1022 and NPT-1022H only)
- GNSS built-in receiver (NPT-1022B and NPT-1022BH only)
- SyncE
- 1588v2 - Primary, Secondary, transparent, and boundary clock
- IEEE 1588v2 G.8275.1
- IEEE 1588v2 G.8275.2 (NPT-1022H and NPT-1022BH only)
- G.8273.2 – Class C compliant
- 1PPS and ToD interfaces, using external timing input sources
- 1PPS monitoring point
- Hybrid 1588 and SyncE
- APTS (NPT-1022B and NPT-1022BH only)
- NTP support (NTPv1, NTPv2, NTPv3, and NTPv4)
- E1/T1 interfaces of CES cards
- STM-1/4 of CES cards
- Local interval clock
- Holdover mode

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition

of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT):

- Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.
- The platform provides synchronization outputs for the synchronization of external equipment within the exchange. The synchronization outputs are 2 MHz and 2 Mbps. These outputs can be used to synchronize any peripheral equipment or switch.

The platform supports SyncE synchronization over GbE/10GbE interfaces. Our implementation is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262.1, G.8263, and G.8264.

The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. PTP IEEE 1588v2 is supported in two profiles; full network timing support (G.8275.1) and partial network timing support (G.8275.2, NPT-1022H and NPT-1022BH), providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities. It is possible to support high accuracy PTP mode and achieve <10ns (G.8273.2 Class C) timing error per NE. PTP is supported over GbE/10GbE interfaces.

## NPT-1022 Platform Family Cooling Subsystem

NPT-1022 platforms include fan units for cooling purposes. The ventilation system pumps the cold air using the equipment fans. The cold air flows over the cards and components and cools them. In NPT-1022B and NPT-1022BH platforms, the extractable air filter is installed in a dedicated air filter slot.

The routes of cold and hot air in the system are schematically shown in the following figure. Cold air flow is marked blue; hot flow is marked red; air flow through the platforms is marked orange.

### Airflow in NPT-1022

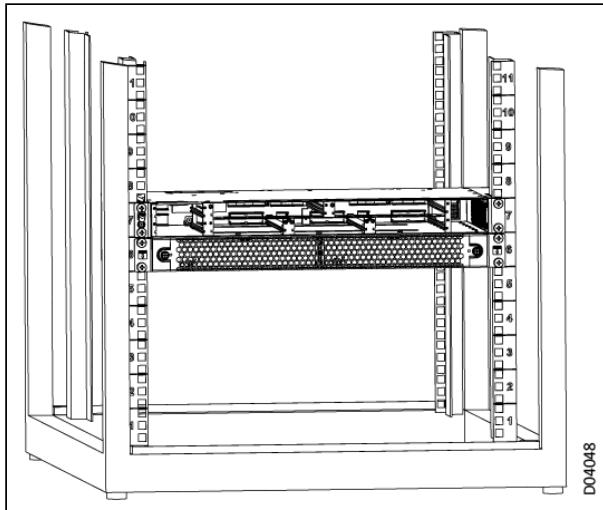


### Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

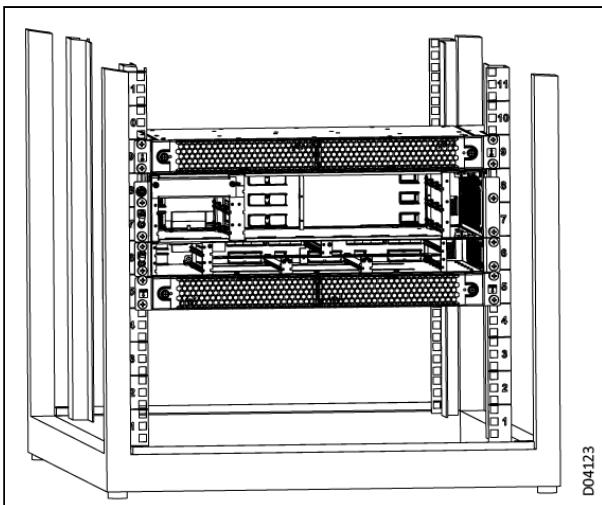
The NPT-1022x platforms can be configured together with an air baffle unit, installed in either a 19" or 23" rack.

- In the 19" rack, the 1U air baffle unit is located directly below the NPT-1022x platform. The platform and air baffle unit together occupy a total space of 2U height in the rack. The air baffle unit should be installed *before* the NPT-1022x platform; the NPT-1022x platform is then inserted *above* the air baffle unit. Note that a total space of 3U height must be available in the rack for the installation process; see the *NPT-1022 Installation and Maintenance Manual* for the installation procedure details and limitations.

**1U Height Platform Installed in 19" Rack over Air Baffle Unit**

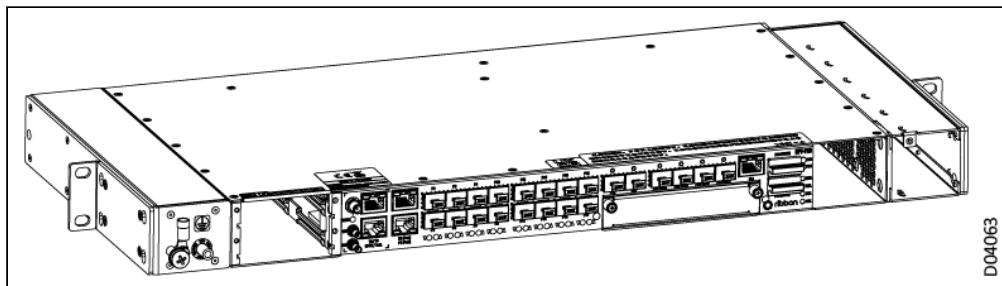
- In the 19" rack, if the NPT-1022x platform is configured with an EXT-2U expansion unit, then the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* where the NPT-1022x platform will be located, and one located directly *above* where the EXT-2U unit will be located.
  - First install the EXT-2U unit on the NPT-1022x platform.
  - Then assemble the air baffle unit (including the 2 air-flow boxes) in the 19" rack.
  - Finally, insert the combined NPT-1022x platform with the EXT-2U expansion unit into the gap between the upper and lower air-flow boxes.

The combination of NPT-1022x platform with EXT-2U expansion unit and 2 air-flow boxes occupies a total space of 5U height in the rack.

**1U Height Platform Plus Expansion Unit Installed in 19" Rack Between Two Air-Flow Boxes**

- In the 23" rack, the air baffle unit is installed as 2 1U air ducts placed to the right and left sides of the NPT-1022x platform, requiring a total space of 1U height to be available in the rack, since the air ducts don't add anything to the platform height.

### 1U Height Platform Installed with Air Baffle Unit in 23" Rack



- In the 23" rack, if the NPT-1022x platform is configured with an EXT-2U expansion unit, then a second set of 2U air ducts is installed on either side of the EXT-2U expansion platform. The combination of NPT-1022x platform with EXT-2U unit and 2 sets of air ducts requires a total space of 3U height to be available in the rack, since the air ducts don't add anything to the platform height.

In a 19" rack, when installing the NPT-1022B/BH platform together with air baffles, or installing any NPT-1022x platform together with an EXT-2U expansion unit and air baffles, the internal air filters in the NPT-1022B/BH platform (and EXT-2U unit, if installed) must be removed. When installing the NPT-1022B/BH, with or without an expansion unit, in a 23" rack, only the internal air filter in the NPT-1022B/BH platform must be removed. External air filters are available; see the *NPT-1022 Installation and Maintenance Manual* for details.

## NPT-1022 Platform Family Power Feed Subsystem

### Description

The platform features a distributed power feed subsystem. This distributed power concept assures system upgrading and efficient heat distribution. It also makes sure maximum reliability of the power feed interface.

In the platform, two INF power feed modules serve as a redundant interconnection device between the platform cards and the -48 VDC power sources. The main purpose of this unit is to decouple the noise generated/received from the DC power source lines. Each INF power feed module has an external power input. The filter is connected to a power input to distribute the -48 VDC battery plant input to all cards via fully redundant power buses. Alternatively, a single AC power feed can be used, or a mixture of 1 AC module and 1 DC module. Each card of the platform generates its own local voltage using high-quality DC/DC converters. AC power feeding requires the use of a conversion module to implement AC/DC conversion.

### Features

- Reverse polarity protection
- Overvoltage alarm and protection
- Undervoltage alarm and protection
- Redundancy between INF units
- Hot swapping
- Power-fail detection and 10 msec holdup
- Lightning-strike protection
- Redundant fan power supply with adjustable voltages

The NPT-1022 platforms support the following types of power supply modes.

- Single input -48 VDC power feed ([INF-B1U](#)), configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- Dual input DC power supply ([INF-B1U-D](#)), where only the PSA slot can be assigned.
- Single input 24V DC power supply ([INF\\_B1UH-24V](#)). Both PS slots can be assigned.
- Single input AC to DC converter for 100-240 VAC power source ([AC\\_PS-B1U](#)), utilizing an external power line connection through a power conversion module to implement AC/DC conversion. Only the PSA slot can be assigned.

The following flexible power supply configuration options are supported:

- Single DC 1+0
- Dual DC 1+1 (redundant)
- DC dual feeding
- Single AC 1+0
- Dual AC 1+1 (redundant)
- Mixture of AC and DC (redundant)

## INF-B1U Overview

### Supported Platforms

- NPT-1022/B

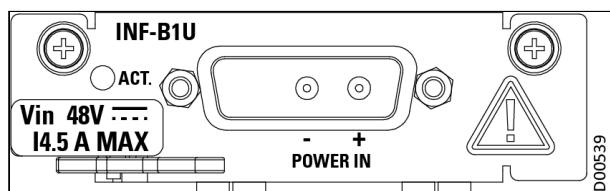
### Description

The INF-B1U is a -48 VDC power-filter module. Two INF-B1U modules are needed for power feeding redundancy.

### Features

- High-power INF for up to 250 W
- Single DC power input and power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected

### INF-B1U Front Panel



## INF-B1U-D Overview

### Supported Platforms

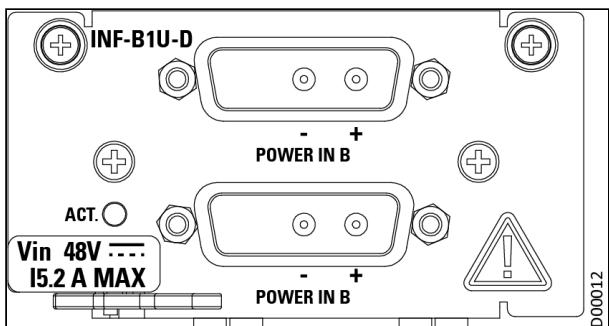
- NPT-1022/B

### Description

The INF-B1U-D is a DC power-filter module. It performs the following functions:

- Dual DC power input and power supply for all modules in the platform
- Input filtering for the entire platform
- Adjustable output voltage for platform fans
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage is detected

### INF-B1U-D Front Panel



## INF\_B1UH-24V Overview

### Supported Platforms

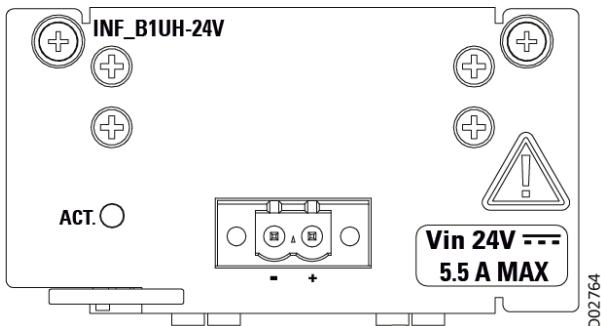
- NPT-1022/B

### Description

The INF\_B1UH-24V is a 24 VDC power-filter module. Two INF\_B1UH-24V modules are needed for power feeding redundancy. It performs the following functions:

- Feed power supply for all modules in the platform
- Input filtering function for the entire platform
- Adjustable output voltage for fans in the platform
- Support of fan power loss alarm and LED display
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply in the event of under-/over-voltage
- Single DC power input: 20 VDC to 32 VDC
- Supplies up to 110W power

### INF\_B1UH-24V Power-Filter Module



## AC\_PS-B1U Overview

### Supported platforms

- NPT-1022/B

### Description

AC\_PS-B1U is a pluggable module and works if plugged into the NPT-1022 platforms only.

**Note**

AC\_PS-B1U cannot work in standalone mode.

## Features

- Converts AC power to DC power
- Filters input for the entire platform
- Supplies adjustable output voltage for the fans
- Supplies up to 150 W power, with an AC input range of 100-240 VAC

## NPT-1022 Platform Family Traffic and Switching Functionality

The NPT-1022 platform architecture enables its outstanding configuration flexibility. At the heart of the NPT-1022 is a built-in non-blocking switching fabric, integrating functions such as control, communications, timing, and overhead processing, in addition to the essential packet switching capabilities. The NPT-1022 provides a full IP/MPLS system, including controller, central packet processor (PP and TM), SyncE timing unit, PTP timing unit, 16 built-in GE ports (12xSFP and 4xRJ45), 4 built-in 10GE/GE SFP+ ports, control and management interfaces, LED indicators, etc.

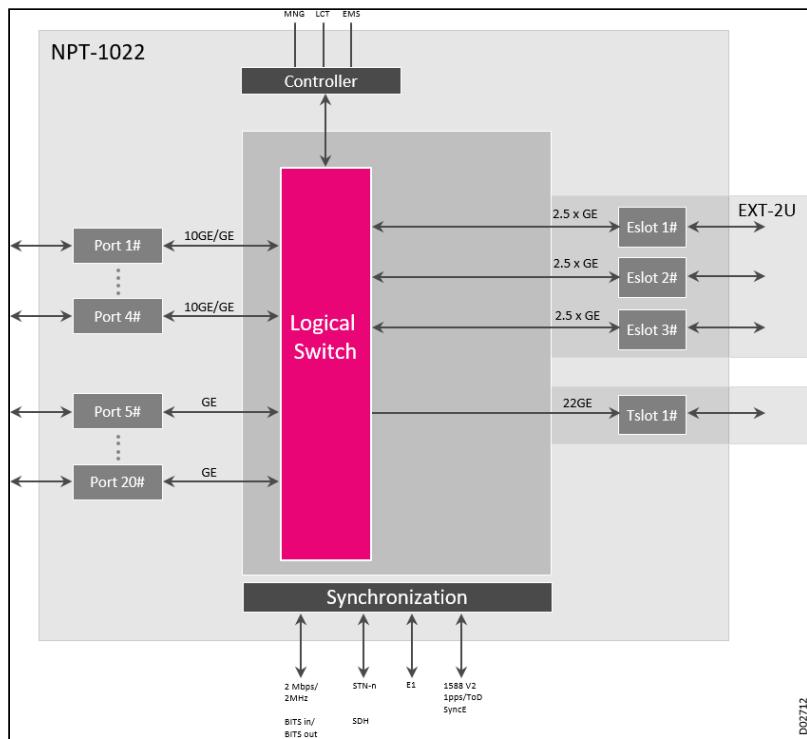
The NPT-1022 switching fabric has three main subsystems:

- **Main processing and control:** Performs all integrated functions like control, communication, and overhead processing.
- **Central packet switch:** Performs all the NPT-1022 packet switching operations.
- **TMU:** Generates and distributes timing and clock signals to all the cards installed in the NPT-1022 platform. In addition to its internal timing reference, the TMU can use up to four user-specified reference sources; see [NPT-1022 Platform Family Timing](#) for more information.

The NPT-1022 metro access platform offers a choice of capacity and configuration options, including:

- All-Native Ethernet packet switch, supporting native packet-level switching with 78G switching capacity (port fan-out) with up to 64G traffic management (MPLS processing), providing:
  - Management and internal control
  - User traffic switching
  - Non-blocking data switch fabric
  - P2P MPLS internal links via the packet switch
- Traffic management, supporting guaranteed CIR and DiffServ with 8 CoS
- Supports 1 Tslot
- Aggregate ports:
  - 16 GE ports (12xSFP and 4xRJ45)
  - 4 10GE/GE ports (4xSFP+)
  - E1POP Smart SFP supported in 1000Base-T ports
  - OTSOP16 Smart SFP supported in SFP+\_10GE ports
- Comprehensive range of timing and synchronization capabilities (ToD, 1PPS, T3/T4 (NPT-1022/H only), and GNSS (NPT-1022B/BH only))
- Supports MPLS-TP
- Supports IP/MPLS
- Built-in NVM card

## NPT-1022 System Architecture



**NPT-1022 Front Panel Interfaces**

<b>Marking</b>	<b>Interface Type</b>	<b>Function</b>
T3/T4 (NPT-1022/H)	RJ-45	T3 and T4 timing interfaces (one 2 Mbps/1.5 Mbps and one 2 MHz/1.5 MHz)
GNSS (NPT-1022B/BH)	COAX	GNSS receiver
1PPS/ToD	RJ-45	1PPS and Time of Day input/output signals supporting Ethernet timing per IEEE 1588v2 standard
Console	RJ-45	Serial RS-232 console interface for CLI
LCT/CLI	RJ-45	10/100/1000Base-T Ethernet interface as local management port for connecting an LCT or CLI station
USB port	USB	USB interface for Zero Touch Installation (ZTI) application
PORt 1 - PORT 4	SFP+	4 x SFP+ (10G/GE)
PORt 5 - PORT 8	RJ-45	4 x RJ45
PORt 9 - PORT 20	SFP	12 x SFP (GE)

**NPT-1022 Indicators and Functions**

Marking	Full Name	Color	Function
ACT.	System active	Green	Off indicates no power supply. On steadily indicates the MCIPS60/B can't be downloaded successfully or that the MCIPS60/B cannot be controlled normally. Blinking with a frequency (1 sec ON and 1 sec OFF) indicates the MCIPS60/B card is running normally and is active.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
STBY	System standby	Orange	Lights when the card is in standby. Off when the card is active.
MJR.	System major alarm	Red	Lights when the system has a critical or major alarm.
MNR.	System minor alarm	Yellow	Lights when the highest severity of the NE current alarms is minor or warning. Off when the system has no alarm or the highest severity of the NE current alarms is higher than minor or warning.
USB MODE	USB mode indicator		
LSR ON (separate LED for each 10GE port)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).
ON (separate LED for each GE port, P1 to P4)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

**NPT-1022 Platform Family Tslot IO Modules**

The NPT-1022 has a single Tslot for installing I/O modules. The following table lists the different types of CES and Ethernet I/O modules that can be installed in the NPT-1022, with links to each module listed.

**i Notes**

- No matter how many cards are installed into the platform slots, you cannot configure more than the maximum number of ports supported by the NPT-1022:
  - 6 x 10GE
  - 30 x 1GE
- The maximum bandwidth per Tslot in the NPT-1022 is [2x10G+2x1G], so for multi-rate DHxxx I/O cards (such as the DHXE\_4sec), only two ports can work at 10GE.

**NPT-1022 Tslot Modules**

Description	Card
CES multiservice module with 3 x DS3 interfaces and 1 x STM-1/OC3 interface (future)	<a href="#">MS345_3</a>
CES multiservice module with 24 x DS3 interfaces	<a href="#">MS345_24</a>
CES multiservice module with 2 x OC3/STM-1 and 8 x E1/T1 interfaces	<a href="#">MSC_2_8</a>
CES multiservice module with 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<a href="#">MS1_4</a>
CES multiservice module with 32 x E1/T1 interfaces	<a href="#">MSE1_32</a>
Electrical 4 x GE (SGMII) interface module with direct connection to the packet switch with PoE+ capabilities	<a href="#">DHGE_4EB</a>
Logical version of DHGE_8, supporting up to 4 SFP ports (no CSFP support) with direct connection to the packet switch	<a href="#">DHGE_8S</a>
Optical 10 x GE module with direct connection to the packet switch	<a href="#">DHGE_10</a>
Optical 2 x 10GE interface module with direct connection to the packet switch	<a href="#">DHXE_2</a>
40G card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces	<a href="#">DHXE_4MR</a>
40G MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces All 4 ports support MACsec capability	<a href="#">DHXE_4MRsec</a>
In the NPT-1022 this 40G MACsec card supports: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 1GE ports</li></ul> All 4 ports support MACsec capability.	<a href="#">DHXE_4sec</a>

## NPT-1022 Platform Family Expansion Platform

The traffic capabilities of the Neptune platform can be expanded by installing the EXT-2U expansion unit on top.

The EXT-2U platform is a high density modular expansion unit for the Neptune multiservice platforms. It supports the complete range of CES, PCM, optics and Ethernet services. Integrating this add-on platform into your network configuration is not traffic-affecting.

The EXT-2U is compact and versatile and can be used with different base units from the Neptune product line. The type of traffic delivered by the unit depends on the type of matrix (PCM or Packet only) installed in the base unit. I/O expansion cards are supported in accordance.

The EXT-2U has three multipurpose slots (ES1 to ES3) for any combination of extractable traffic cards. PCM, Ethernet, OTN muxponders, optical amplifiers, and CES traffic are all handled through cards in these traffic slots.

The following table lists the traffic cards supported in the EXT-2U when installed on the platform. For a detailed description of the EXT-2U features, functionality, and supported traffic cards refer to the chapter [EXT-2U Expansion Platform](#).

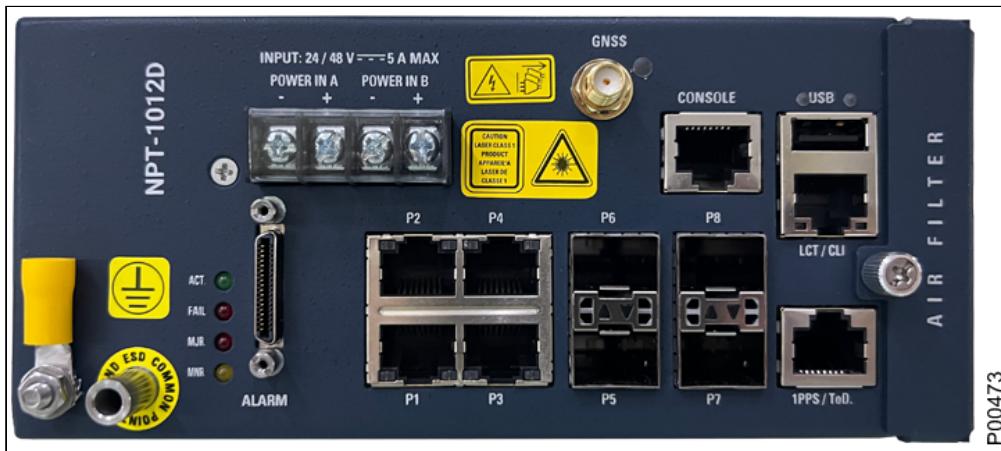
#### **EXT-2U Supported Traffic Cards for NPT-1022**

Card Type	Designation
Multiservice PCM and 1/0 XC card over Ethernet	<a href="#">EM_10E</a>
10G card with up to 10 GbE ports; 4 of the ports support POE++	<a href="#">DHGE_10_POE</a>
CES multiservice card with 2 x STM-1/OC-3 and 16 x E1/T1 interfaces	<a href="#">MSC_2_16E</a>
Optical Base Card (OBC) for optical amplifiers and DCM modules (OBC, OBC_B, OBC_C)	<a href="#">Optical Base Card (OBC)</a>

# NPT-1012D System Architecture

The NPT-1012D is an extremely compact hardened DIN-rail switch. This IP/MPLS based multiservice packet transport platform is an edge device with up to 32G switching capacity. With a rich and robust feature set, NPT-1012D is well suited for a wide variety of applications and networking scenarios. NPT-1012D is optimized for critical infrastructure applications, where the advanced IP/MPLS traffic engineering tools and features must extend to remote locations (interior and exterior), with strict environmental and size requirements.

## NPT-1012D Front Panel



This compact DIN-rail platform is housed in an equipment cage with all interfaces accessible from the front of the unit. NPT-1012D traffic interfaces are housed on a single board system, supporting:

- Traffic processing through 8 ports, divided between:
  - 4 x 10/100/1000BaseT electrical ports with ETGBE
  - 4 x 100/1000 FX/GE optical (SFP/SFP+) ports
- Comprehensive timing and synchronization capabilities, including:
  - GNSS built-in receiver
  - SyncE
  - 1588v2 (G.265.1, G.8275.1, G.8275.2)
  - G.8273.2 – Class C compliant
  - 1PPS and ToD
  - Hybrid 1588 + SyncE
  - APTS (Assisted Partial Timing Support (global navigation satellite system))
- Native packet switching (Ethernet and MPLS-TP)
- Full range of MEF CE3.0 services (E-Line, E-LAN, E-Tree, E-Access)
- VPN- and eVPN-based Ethernet and IP, MPLS-TP, IP/MPLS, MPLS VPWS, VPLS, L2VPN, and L3VPN
- Wide range of protection options (ERP, MSTP, Linear 1:1, PWR, MS-PW)
- Wide range of security options, including RADIUS, SFTP, SSHv2, IEE802.1x authentication, and L2/L3 ACL
- DC power supply, a -48 VDC power feed providing two connectors for external power line connection, with a dual power feed for redundancy

The NPT-1012D can be installed in rail mode in a street cabinet. The rugged platform design makes this platform suitable for street cabinet use, withstanding temperatures from -25°C (-13°F) up to +65°C (158°F).

This section introduces the following features:

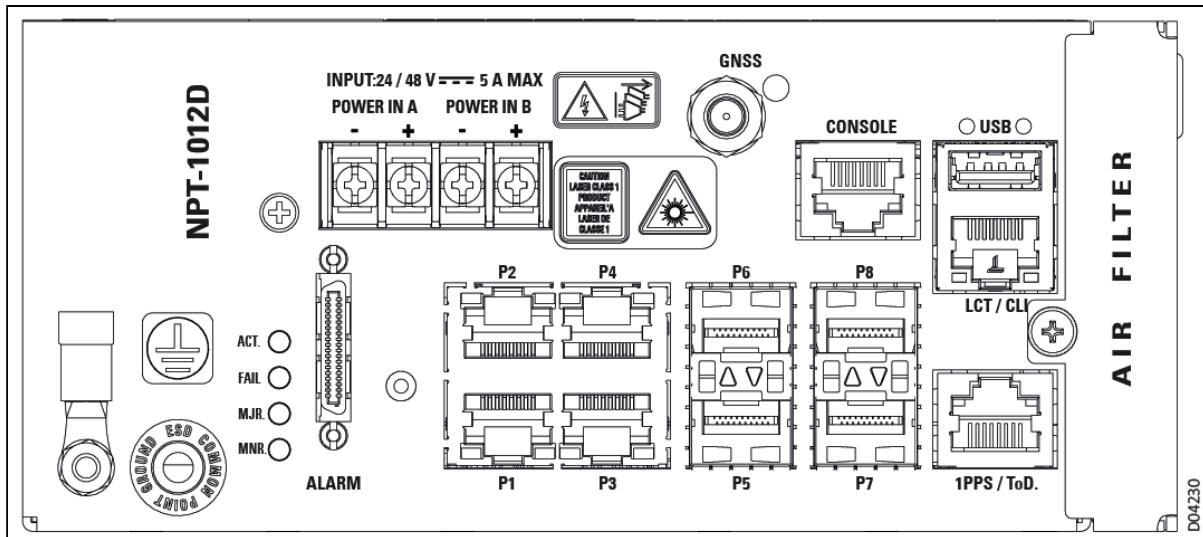
- [NPT-1012D User Interfaces](#)
- [NPT-1012D Communication with External Equipment and Management](#)
- [NPT-1012D Timing](#)

## NPT-1012D User Interfaces

NPT-1012D supports the following interfaces:

- 4 x 100/1000BaseT electrical ports
- 4 x 1/10G optical (SFP+) ports
- 1PPS/TOD timing
- MNG management ports

### NPT-1012D Front Panel



**NPT-1012D Front Panel Interfaces**

Marking	Interface Type	Function
POWER IN A	D-type, 3-pins	DC power input connector, source A
POWER IN B	D-type, 3-pins	DC power input connector, source B
ALARMS	D-type, 15-pins	Alarm input and output interface connector
PORT 1 to PORT 4	RJ-45	100/1000BaseT interfaces
PORT 5 to PORT 8	SFP housing	SFP+ housing for 1/10G L2 interface (multi-rate)
1PPS/ToD	RJ-45	1PPS and Time of Day input/output signals supporting Ethernet timing per IEEE 1588v2 standard
Console	RJ-45	10/100BaseT Ethernet interface for management
LCT/CLI ports	RJ-45 USB	2 local management port options
GNSS	Antenna	GNSS interface

**NPT-1012D LED Indicators and Functions**

Marking	Full Name	Color	Function
ACT.	System active	Green	Normally blinks with the frequency of 0.5 Hz. Off or lights when the platform is not running normally.
FAIL	System fail	Red	Normally off. Lights when a card failure is detected.
MJR.	System Major alarm	Red	Lights when the system has a Critical or Major alarm.
MNR.	System Minor alarm	Orange	Lights when the system has a Minor or Warning alarm (and no Critical or Major alarm).

**Note**

ACT, FAIL, MJR, and MNR LEDs are combined to show various failure reasons during the system boot. For details, see the *Troubleshooting Using Component Indicators* section in the *NPT-1012D Installation, Operation, and Maintenance Manual*.

The four SFP housings on the NPT-1012D support four types of SFP module:

- GE SFP optical transceivers with a pair of LC optical connectors
- Electrical GE SFP electrical transceivers with a RJ-45 connectors
- Bidirectional GE SFP optical transceivers with one LC optical connector (bidirectional GE Tx/Rx over a single fiber using two different lambdas)
- Colored GE SFP optical transceivers with a pair of LC optical connectors (colored C/DWDM SFP)

## NPT-1012D Communication with External Equipment and Management

In the Neptune metro access product line, the main controller unit is responsible for communicating with other NEs and management stations.

The main controller unit communicates with the local EMS and LCT systems via the Ethernet interface. It communicates with the remote EMS/LCT systems and other NEs via the in-band MCC. Communication between other NEs, or between the NEs and the EMS/LCT, can also be via the out-of-band DCN. The controller can connect to the DCN via Ethernet.

### Usage Guidelines

The NPT-1012D supports in-band and DCN management connections for PB and MPLS:

- 20 Mbps shaper for MCC packet to MCP
- IPv4 and/or IPv6 LIF over Ethernet port
- IPv4 and/or IPv6 IRB LIF
- IPv4 and/or IPv6 PHT LIF
- IPv4 and/or IPv6 network-bridging to management VRF
- The following routing protocols are supported via DCN and in-band:
  - IPv4: OSPFv2, IS-IS, static routes
  - IPv6: OSPFv3, IS-ISv6, static routes

## NPT-1012D Timing

This platform provides high-quality system timing to all traffic modules and functions in compliance with applicable ITU-T recommendations for functionality and performance. The main component in the synchronization subsystem is the timing and synchronization unit (TMU). Timing is distributed redundantly from the TMUs to all traffic and matrix cards, minimizing unit types and reducing operation and maintenance costs.

To support reliable timing, the platform provides multiple synchronization reference options. Up to four timing references can be monitored simultaneously:

- GNSS built-in receiver
- SyncE
- 1588v2 (G.265.1, G.8275.1, G.8275.2) - Primary, Secondary, transparent, and boundary clocks
- G.8273.2 – Class C compliant
- 1PPS and ToD interfaces, using external timing input sources
- Hybrid 1588 + SyncE
- APTS (Assisted Partial Timing Support (global navigation satellite system))

In these platforms, any timing signal can be selected as a reference source. The TMU provides direct control over the source selection (received from the system software) and the frequency control loop. The definition of the synchronization source depends on the source quality and synchronization mode of the network timing topology (set by the EMS-NPT or LCT-NPT).

Synchronization references are classified at any given time according to a predefined priority and prevailing signal quality. The synchronization subsystem synchronizes to the best available timing source using the Synchronization Status Marker (SSM) protocol. The TMU is frequency-locked to this source, providing internal system. The platform is synchronized to this central timing source.

The platform supports SyncE synchronization, which is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU T standards G.8261, G.8262, G.8263, and G.8264.

The IEEE 1588 Precision Time Protocol (PTP) provides a standard method for high precision synchronization of network connected clocks. PTP is a time transfer protocol enabling secondary clocks to synchronize to a known primary clock, ensuring that multiple devices operate using the same time base. The protocol operates in primary/secondary configuration using UDP packets over IP or multicast packets over Ethernet. IEEE 1588v2 (G.8265.1/G.8275.1) is supported in the platform, providing Ordinary Clock (OC) and Boundary Clock (BC) capabilities.

# IO Modules

Neptune offers a wide range of I/O modules. This section provides a detailed description of the Tslot and Eslot cards and transceiver modules available for the Neptune platforms. The modules available for the Neptune platforms are organized into the following main categories:

- Multiservice CES Cards: Supporting TDM transport over PSNs.
- Data cards: Supporting electrical/optical GE, 10 GE/OTU2, and 100 GE/OTU4 interfaces.
- Smart SFPs: Supporting CES technology through smart SFP modules

This section includes the following topics:

- [Card and Port Configuration Guidelines](#)
- [Multiservice CES Cards](#)
- [Data Cards](#)
- [Pluggable Transceiver Modules](#)

## Card and Port Configuration Guidelines

When configuring a platform, you first install I/O cards into platform slots, and then configure and activate the ports on those cards. There is usually a maximum number of ports that can be activated on a platform, depending on the port and switching card configuration.

In many cases, a data card *could* physically be installed in many (or all) slots in the platform, but that does *not* mean you can activate every port on every card in the platform. You are limited by the maximum number of ports defined for that platform/switch/card combination.

Neptune platforms allow you to install cards in many different slots, offering useful flexibility in deciding how to arrange your I/O cards and how to assign your ports. You may choose to install more cards and configure fewer ports on each card, or to install fewer cards and configure more ports on each card, depending on your network considerations, such as hardware resiliency preferences.

Each I/O card description includes a table listing:

- Which platforms can be configured with the specific card
- Into which slots in the platform the specific card can be installed, including multiple option rows if the platform offers different switching card options that affect the card installation guidelines
- Maximum number of ports that can be configured on all cards of this type installed in this platform

## Multiservice CES Cards

Even though Ethernet has a compelling value proposition and carriers roll out broadband packet based services, not all companies can generate a business case for abandoning their investments in legacy infrastructure such as PBXs, ATM switches, and radio networks. Operators cannot ignore profitable revenues gained from traditional TDM services and equipment still dominating the current transport networks. They would naturally prefer to extend the capabilities and profitability of those networks with the ability to carry TDM traffic over PSNs such as Ethernet.

Neptune platforms enable CES and CEP emulation, providing TDM transport over PSNs for backhaul applications offering a wide range of new broadband data services. These boost the advantages inherent in packet based networks, including flexibility, simplicity, and cost effectiveness. Neptune platforms support:

- CESoPSN and SAToP for E1/T1 interfaces with encapsulation support for CES over MPLS TP (CESoMPLS) and CES over Ethernet (CESoETH)
- CESoPSN and SAToP for STM-1/4 channelized and OC-3/12 interfaces with encapsulation support for CES over MPLS TP (CESoMPLS) and CES over Ethernet (CESoETH)
- CEP service based on VC-3, VC-4, VC4-4c, CEP service based on STS-1, STS-3c, STS-12c

At the hub or BSC/RNC sites, the Neptune functions as a carrier class multiservice aggregator, optimizing cellular backhaul by multiplexing various TDM services into a single ChSTM-n. STM-1/OC-3 support includes channelized STM-1/OC-3 with up to 63 x VC 12 channels for SDH or 84 VT1.5 channels for SONET.

For more information about our CES solution, see [CES Technology](#). For more information about timing and synchronization, see [Timing Synchronization and Clock Recovery](#).

Neptune platforms offer the following CES service modules, supporting TDM transport over PSNs.

**Neptune Multiservice CES E1/T1 and STM-1/OC-3 Cards per Platform**

Platform	MSE1_16 16 x E1/T1 interfaces	MSE1_32 32 x E1/T1 interfaces	TMSE1_8 Up to 8 x E1/T1 interfaces and IEEE 1588v2 timing support	DMCE1_32 32 x E1 ports plus GE combo port	MSC_2_8 2 x OC3/ STM-1 and 8 x E1/T1 interfaces	MSC_2_16E 2 x STM-1/ OC-3 and 16 x E1/T1 interfaces  Card for the expansion platform (EXT-2U or EXT-2UH)
NPT-1022		Yes			Yes	Yes
NPT-1050	Yes	Yes		Yes	Yes	Yes (only with MCIPS300)
NPT-1100		Yes			Yes	
NPT-1200	Yes (excluding XIO64, XIO16_4, MCIPS320, and MCIPS560)	Yes (excluding XIO64, XIO16_4, MCIPS320, and MCIPS560)		Yes (with CPS100, CPS320, CPTS100, or CPTS320)	Yes (excluding XIO64, XIO16_4, MCIPS320, and MCIPS560)	Yes (only with MCIPS)
NPT-1250		Yes			Yes	Yes
NPT-1300		Yes			Yes	Yes
NPT-1800		Yes			Yes	Yes
NPT-2100						
NPT-2300		Yes			Yes	Yes

Platform	MSE1_16 16 x E1/T1 interfaces	MSE1_32 32 x E1/T1 interfaces	TMSE1_8 Up to 8 x E1/T1 interfaces and IEEE 1588v2 timing support	DMCE1_32 32 x E1 ports plus GE combo port	MSC_2_8 2 x OC3/ STM-1 and 8 x E1/T1 interfaces	MSC_2_16E 2 x STM-1/ OC-3 and 16 x E1/T1 interfaces  Card for the expansion platform (EXT-2U or EXT-2UH)
EXT- 2U EXT- 2UH eEXT- -2UH		Protection available with TPS32_2 module for appropriate base platforms				Installed in EXT-2U or EXT-2UH with appropriate base platforms

### Neptune Multiservice CES STM-1/OC-3 /STM-4/OC-12 Cards per Platform

Platform	<b>DMCES1_4</b> 4 x STM-1 or 1 x STM-4 interfaces plus GE combo port	<b>MS1_4</b> 4 x OC3/STM-1 and 1 x OC12/STM-4 interfaces	<b>MS345_3</b> 3 x DS3 interfaces and 1 x OC3 interface	<b>MS345_24</b> 24 x DS3 interfaces	<b>MS16_4MR</b> Multi-Rate 4 x OC3/12/48 CES interfaces
NPT-1022		Yes	Yes	Yes	Yes
NPT-1050	Yes (only with MCPTS100, MCPS100)	Yes	Yes (only with MCIPS300)	Yes	Yes
NPT-1100		Yes	Yes	Yes	Yes
NPT-1200	Yes (only with CPTS320, CPS320, CPTS100, CPS100)	Yes (excluding XIO64, XIO16_4, MCIPS320, MCIPS560)			
NPT-1250		Yes	Yes	Yes	Yes
NPT-1300		Yes	Yes	Yes	Yes
NPT-1800		Yes	Yes	Yes	Yes
NPT-2100					
NPT-2300		Yes	Yes	Yes	Yes
EXT-2U EXT-2UH eEXT-2UH			Protection available with TPS345_1 module for appropriate base platforms		

This section introduces the following CES cards:

- MSE1\_16 Overview
- MSE1\_32 Overview
- MSC\_2\_8 Overview
- DMCES1\_4 Overview
- MS1\_4 Overview
- MS345\_3 Overview
- MS345\_24 Overview
- MS16\_4MR Overview

## MSE1\_16 Overview

### Supported Platforms

- NPT-1021
- NPT-1050 (not with MCIPS300)
- NPT-1200 (not with MCIPS320/560)

### Description

The MSE1\_16 is a CES multiservice card that provides CES for E1/T1 interfaces.

### Features

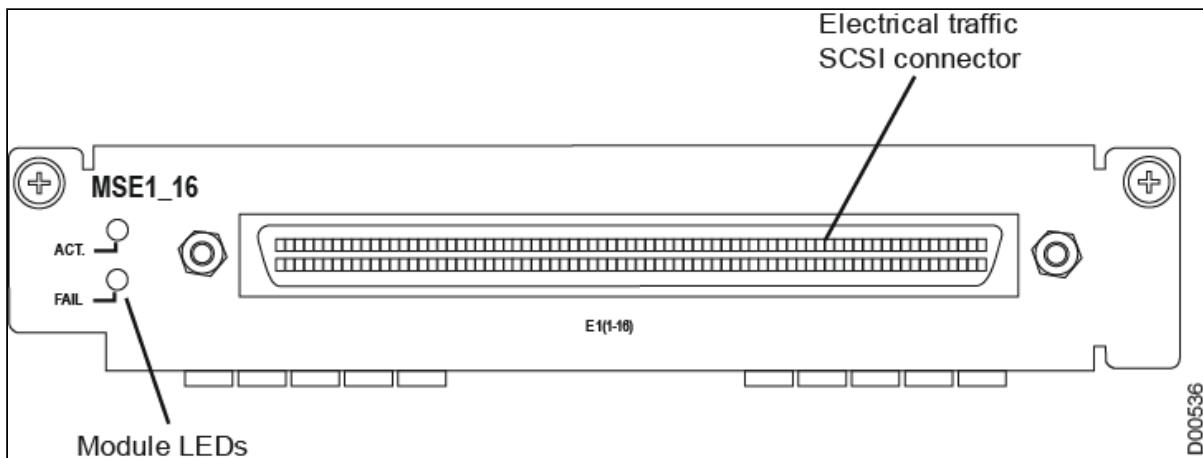
- 16 x E1/T1 interfaces supported.
- Physical connection towards customer E1/T1 interfaces is by a SCSI 100-pin socket connector on the front panel of the card.
- Connectivity to the packet network is by direct 1.25G SGMII connection to the central packet switch on CPS card through the backplane.
- SAToP and CESoPSN standards supported.
- Adaptive and differential clock recovery for CES services is in accordance with ITU-T G.8261.

CEP (RFC-4842) is supported on the 2 x STM-1/OC-3 interfaces for VC-4, STS-1, STS-3c. A mixture of channelized VC-4 (E1 CES) and VC-4 clear channel (VC-4 CEP) is supported on per VC-4 basis.

### Max. MSE1\_16 Modules and E1/T1 Interfaces per Platform

Platform	Max. MSE1_16 Modules	Max. E1/T1 Interfaces	Installed into Slots
NPT-1021	1	16	TS1
NPT-1050 (not with MCIPS300)	3	48	TS1-TS3
NPT-1200 (not with MCIPS320/560)	6	96	TS1-TS4, TS6-TS7

### MSE1\_16 Front Panel



### LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.

## MSE1\_32 Overview

### Supported Platforms

- NPT-1021
- NPT-1022/B
- NPT-1050
- NPT-1100
- NPT-1200
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

### Description

The MSE1\_32 is a CES multiservice card that provides CES for E1/T1 balanced interfaces. An MSE1\_32 card configured in NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms together with an expansion unit can be protected as follows:

- **1:1 protection group:** Provides protection for one MSE1\_32 card by a second MSE1\_32 card, through an associated TP32\_2 card installed in the expansion unit. The second (protecting) card is kept in standby mode; traffic is switched to the protecting card if this is triggered, for example, by a hardware failure or user request for a forced switch. Traffic can be switched back to the original protected card after that card recovers and returns to a normal state if switching is revertive.
- **1:2 protection group:** Provides protection for two MSE1\_32 cards by a third MSE1\_32 card, through an associated TP32\_2 card installed in the expansion unit. The third (protecting) card is kept in

standby mode; traffic is switched to the protecting card if this is triggered, for example, by a hardware failure or user request for a forced switch. Traffic is switched back to the original protected card after that card recovers and returns to a normal state.

Protection switch time is <50ms for card reset, card extraction, and user-requested commands.

## Features

- 32 x E1/T1 balanced interfaces supported
- Physical connection towards customer E1/T1 interfaces is by 2 x SCSI 68-pin socket connectors on the front panel
- Connectivity to the packet network is made by direct 1.25G SGMII connection to the central packet switch on CPS card through the backplane
- CES services:
  - CESoETH and CESoMPLS mode
  - SAToP and CESoPSN
- Clock recovery for CES services:
  - Adaptive and differential clock recovery as per ITU-T G.8261
  - 32 clock domains
- PM counters support per channel
- Alarm support per channel

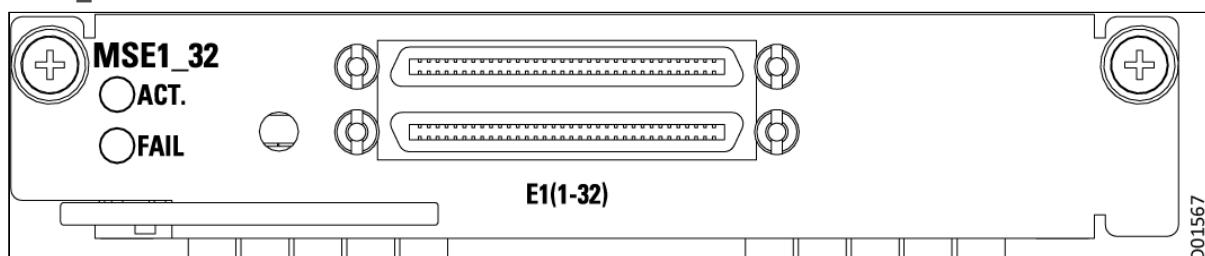
## Usage Guidelines

- Two external xDDF-21 units are required to connect 32 x E1/T1 unbalanced interfaces to the MSE1\_32.
- When MSE1\_32 cards are not connected to TP32\_2 cards, they can be installed in any slot as listed in the following table. However, when MSE1\_32 cards are connected to TP32\_2 cards in a protection configuration, due to the cabling requirements:
  - The MSE1\_32 cards participating in the protection instance must be installed next to each other.
  - The MSE1\_32 cards participating in the protection instance must be installed in slots close to the EXT-2U/2UH expansion units.
  - No other cards can be installed between the MSE1\_32 cards participating in the protection instance and the corresponding TP32\_2 cards.
  - The cable guide and cable slack tray accessories must also be installed.

## Modules/Interfaces per Platform

**MSE1\_32 Modules and E1/T1 Interfaces per Platform**

Platform	Max. MSE1_32 modules	Max. E1/T1 Interfaces	Max. <i>protected</i> E1/T1 Interfaces When Configured with TP32_2	Installed into Slots
NPT-1021	1	32	N/A	TS1
NPT-1022	1	32	N/A	TS1
NPT-1050	3	96	N/A	TS1-TS3
NPT-1100	1	32	N/A	TS1
NPT-1200	6	192	N/A	TS1-TS4, TS6-TS7
NPT-1250	8	256	N/A	TS1-TS8
NPT-1300	7	224	192	TS1-TS7
NPT-1800	23	736	192	TS1-TS24, except TS22
NPT-2300	5	160	192	TS1-TS2, TS5-TS7

**MSE1\_32 Front Panel**

### MSE1\_32 Front Panel LED Indicators LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.

## MSC\_2\_8 Overview

### Supported Platforms

- NPT-1021
- NPT-1022/B
- NPT-1050
- NPT-1100
- NPT-1200
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

### Description

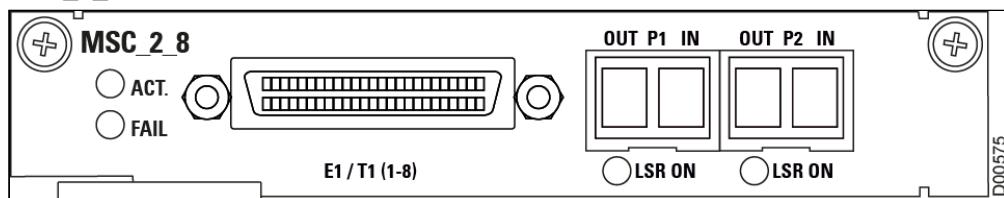
The MSC\_2\_8 is a CES multiservice card that provides CES for E1/T1 and STM-1/OC-3 interfaces.

### Features

- 8 x E1/T1 interfaces supported. Physical connection towards customer E1/T1 interfaces is by a 36-pin SCSI socket connector on the front panel.
- 2 x STM-1/OC-3 interfaces supported. 2 x SFP sockets enable physical connection to the card.
- Connectivity to the packet network is made by direct 1.25G SGMII connection to central packet switch on CPS card through the backplane.
- SAToP and CESoPSN standards supported.
- CEP (RFC-4842) is supported on the 2 x STM-1/OC-3 interfaces for VC-4, STS-1, and STS-3c.
- A mixture of channelized VC-4 (E1 CES) and VC-4 clear channel (VC-4 CEP) is supported on a per VC-4 basis.
- The card supports MSP1+1 protection in the following modes:
  - MSP1+1 protection between two STM-1/OC-3 ports (intra-card).
  - MSP1+1 protection between STM-1/OC3 ports (cross-card).
  - STM-1/OC-3 ports are either protected or non-protected; mixed configurations (partial protection) are not supported.
  - Both unidirectional and bidirectional MSP1+1 protection between ports on MS1\_4 and MSC\_2\_8 cards (intra-card) in NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1100, NPT-1050, and NPT-1022 platforms
  - Both unidirectional and bidirectional MSP1+1 protection between ports on MS1\_4 and MSC\_2\_8 cards (cross-card) in NPT-1800, NPT-1250, and NPT-1050 platforms
  - Both revertive and non-revertive modes are supported for bidirectional MSP1+1. For unidirectional MSP1+1, only non-revertive mode supported
- Clock recovery for CES Services:
  - Adaptive and differential clock recovery as per ITU-T G.8261.
  - For the STM-1/OC-3 interfaces, each E1/DS1 channel has an independent clock domain in Differential or Adaptive clock recovery.

**MSC\_2\_8 Modules and STM-1/OC-3 and E1/T1 Interfaces per Platform**

Platform	Max. MSC_2_8 modules	Max. STM-1/OC-3 Interfaces	Max. E1/T1 Interfaces	Installed into Slots
NPT-1021	1	2	8	TS1
NPT-1022	1	2	8	TS1
NPT-1050	3	6	24	TS1-TS3
NPT-1100	1	2	8	TS1
NPT-1200	6	12	48	TS1-TS4, TS6-TS7
NPT-1250	8	16	64	TS1-TS8
NPT-1300	7	14	56	TS1-TS7
NPT-1800	23	46	184	TS1-TS24, except TS22
NPT-2300	5	10	40	TS1-TS2, TS5-TS7

**MSC\_2\_8 Front Panel****LEDs**

Marking	Description	Color	Function
FAIL	Card fail	Red	Normally off. Lights steadily when card failure is detected.
ACT.	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicate the card is not running normally.
LSR ON (separate LED for each port P1, P2)	Laser on	Green	Lights steadily when laser is on.

## DMCES1\_4 Overview

### Supported Platforms

- NPT-1021
- NPT-1050
- NPT-1200 (not with MCIPS320/560)

### Description

The DMCES1\_4 is a CES multiservice card that provides CES for channelized STM-1 or STM-4 interfaces.

### Features

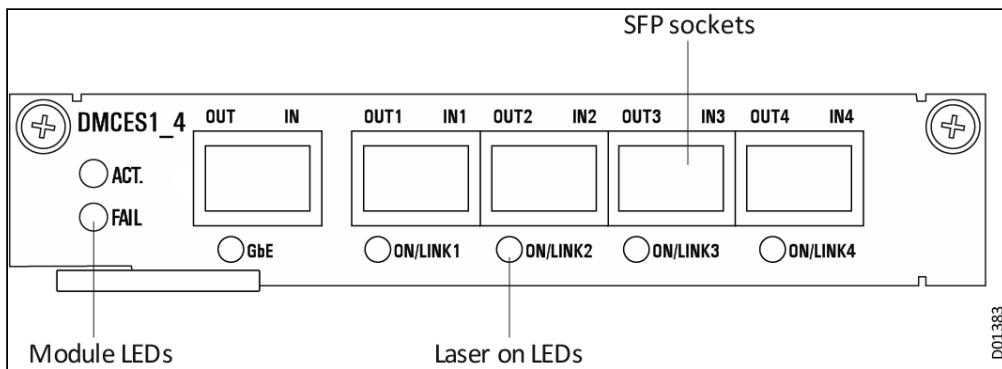
- Supports either:
  - 4 x Channelized STM-1 interfaces  
OR
  - 1 x STM-4 interface
- Physical connection towards the customer STM-1 or STM-4 signals is by SFP. There are 4 x SFP sockets; each port can be configured to support an STM-1 interface. Port No. 1 can be configured to support channelized STM-4; when this is the case the remaining ports are disabled.
- Up to 252 E1 CES services are supported
- SAToP and CESoPSN standards supported
- Connectivity to the packet network is by one of the following:
  - Direct 1.25G SGMII connection to central packet switch on CPS cards through the backplane.
  - Connection to 3rd party device (router/switch) through SFP based GbE port on the front panel, working in standalone mode with CESoETH and CESoIP/UDP encapsulation.

**Note**

The GbE port is not required by the platforms supported. Connection to this port is made through the backplane.

### DMCES1\_4 modules and STM-1/STM-4 Interfaces per Platform

Platform	Max. DMCES1_4 Modules	Max. STM-1/STM-4 Interfaces	Installed into Slots
NPT-1021	1	4/1	TS1
NPT-1050	3	12/3	TS1-TS3
NPT-1200 (not with MCIPS320/560)	6	24/4	TS1-TS4, TS6-TS7

**DMCES1\_4 Front Panel****LEDs**

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON/LINK1 to LSR ON/LINK4	Laser on indication	Green	Lights steadily when the corresponding laser is on.
GbE	Laser on indication	Green	Lights steadily when the GbE port laser is on.

**MS1\_4 Overview****Supported Platforms**

- NPT-1021
- NPT-1022/B
- NPT-1050
- NPT-1100
- NPT-1200
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

**Description**

The MS1\_4 is a CES multiservice card that supports up to 4 xSTM-1 interfaces, or a single STM-4 interface.

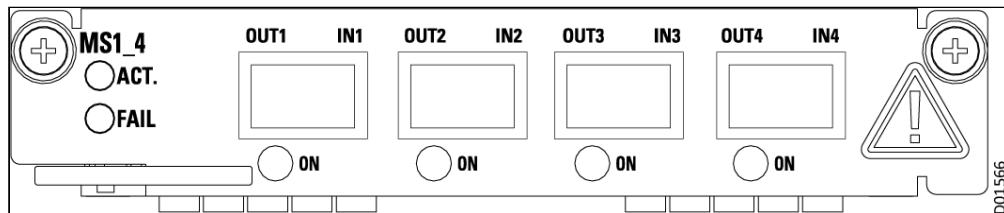
**Features**

- Supports either:
  - 4 x STM-1 interfaces
  - OR
  - 1 x STM-4 interface

- Physical connection towards the customer STM-1 or STM-4 signals is by SFP. There are 4 x SFP housing slots. Port No. 1 can be configured to support channelized STM-4; when this is the case the reaming ports are disabled
- Up to 252 E1 CES services are supported
- CES services:
  - STM-1 channelized to 63 x VC-12 (E1) interfaces
  - STM-4 channelized to 256 x VC-12 (E1) interfaces
  - OC-3 channelized to 84 x VT-15 (DS1) interfaces
  - OC-12 channelized to 336 x VT-15 (DS1) interfaces
- CESoETH and CESoMPLS emulation formats supported
- SAToP and CESoPSN standards supported
- Clock recovery for CES services:
  - Adaptive and differential clock recovery as per ITU-T G.8261
  - For the STM-1/OC-3 interfaces, each E1/DS1 channel has an independent clock domain in Differential or Adaptive clock recovery
- CEP Services (RFC-4842):
  - CEP service based on VC-3, VC-4, VC4-4c
  - CEP service based on STS-1, STS-3c, STS-12c
- MSP1+1 protection in the following modes:
  - MSP1+1 protection between two STM-1/OC-3 ports (intra-card)
  - MSP1+1 protection between STM-1/OC3 ports (cross-card)
  - STM-1/OC-3 and STM-4/OC-12 ports are either protected or unprotected; mixed configurations (partial protection) are not supported
  - Both unidirectional and bidirectional MSP1+1 protection between ports on MS1\_4 and MSC\_2\_8 cards (intra-card) in NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1100, NPT-1050, and NPT-1022 platforms
  - Both unidirectional and bidirectional MSP1+1 protection between ports on MS1\_4 and MSC\_2\_8 cards (cross-card) in NPT-1800, NPT-1250, and NPT-1050 platforms
  - Both revertive and non-revertive modes are supported for bidirectional MSP1+1. For unidirectional MSP1+1, only non-revertive mode supported

**MS1\_4 modules and STM-1/OC-3 Interfaces per Platform**

Platform	Max. MS1_4 modules	Max. STM-1 / OC-3 Interfaces	Installed into Slots
NPT-1021	1	4	TS1
NPT-1022	1	4	TS1
NPT-1050	3	12	TS1-TS3
NPT-1100	1	4	TS1
NPT-1200	6	24	TS1-TS4, TS6-TS7
NPT-1250	8	32	TS1-TS8
NPT-1300	7	28	TS1-TS7
NPT-1800	23	92	TS1-TS24, except TS22
NPT-2300	5	20	TS1-TS2, TS5-TS7

**MS1\_4 Front Panel**

## LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (separate LED for each port P1 to P4)	Laser on	Green	Lights steadily when laser is on.

## MS345\_3 Overview

### Supported Platforms

- NPT-1022/B
- NPT-1050
- NPT-1100
- NPT-1250
- NPT-1300
- NPT-1800

### Description

The MS345\_3 is a CES multiservice module with 3 x DS3 interfaces and 1 x STM-1/OC3 interface. Each DS3 interface can be configured to M13/CBIT framed mode. If configured in unframed mode:

- From DS3 TDM interfaces towards PSN, DS3 is mapped to STS-1. The STS-1 is then transported over the packet network through CEP technology, as per RFC4842.
- From PSN towards DS3 TDM interfaces, STS-1 CEP service is terminated. The STS-1 is then de-mapped to DS3.

An MS345\_3 card configured in NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms together with an EXT-2U expansion unit can be protected with a 1:1 protection group. One MS345\_3 card is protected by a second MS345\_3 card through an associated [TPS345\\_1](#) card installed in the EXT-2U expansion unit. The second (protecting) card is kept in standby mode; traffic is switched to the protecting card if this is triggered, for example, by a hardware failure or user request for a forced switch. Traffic can be switched back to the original protected card after that card recovers and returns to a normal state if switching is revertive. The MS345\_3 also supports cross-card protection for the OC-3 port. Protection switch time is <50ms for card reset, card extraction, and user-requested commands.

### Features

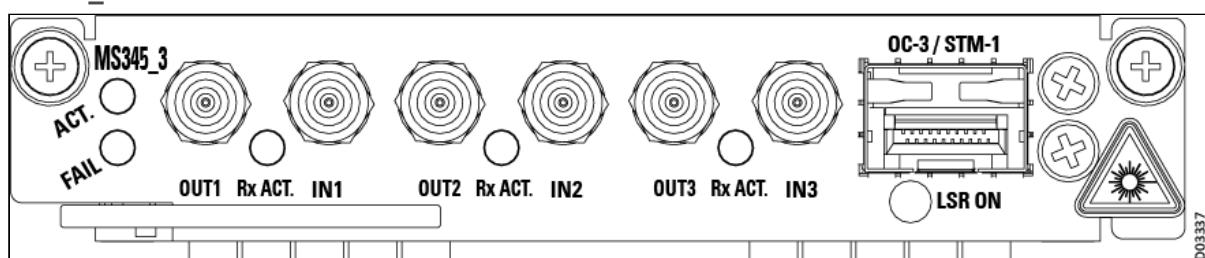
- Supports either:
  - 3 x DS3 interfaces, where each DS3 can be configured to a different frame format:
    - Unframed
    - Standard M13
    - C-bit parity format
  - A single STM-1/OC3 interface
- Supported services include:
  - Transparent DS3 over packet via STS-1 CEP, with up to 3 x DS3/STS-1 CEP
  - Channelized DS3, where each DS3 can be channelized to 28 DS1 CES, up to 84 DS1 CES services per card
- SAToP and CESoPSN service types

- CESoETH and CESoMPLS emulation formats
- Timing modes:
  - DS1 CES (system timing, loop timing, PSN (ACR, DCR) timing)
  - DS3 STS-1 CEP (system timing)
- DS3 line alarms
- Performance Monitoring (PM)

#### MS345\_3 Modules and DS3 Interfaces per Platform

Platform	Max. MS345_3 modules	Max. DS3 Interfaces	Installed into Slots
NPT-1022	1	3	TS1
NPT-1050	3	9	TS1-TS3
NPT-1100	1	3	TS1
NPT-1250	8	24	TS1-TS8
NPT-1300	7	21	TS1-TS7
NPT-1800	23	69	TS1-TS21, TS23-TS24

#### MS345\_3 Front Panel



### MS345\_3 Front Panel LED Indicators and Ports

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected for OC-3/STM-1 port.
LSR ON	Indicates active laser	Green	Indicates laser in use for OC-3/STM-1 port.
Rx ACT (3)	Indicates active traffic reception	Green	One Active Reception indicator for each DS3 port.
OUT1/IN1 OUT2/IN2 OUT3/IN3	Output and Input DS3 traffic ports	N/A	N/A

## MS345\_24 Overview

### Supported Platforms

- NPT-1022/B
- NPT-1050
- NPT-1100
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

### Description

The MS345\_24 is a CES multiservice module with 24 x DS3 interfaces, with dual 10G connectivity to the matrix cards. Each DS3 interface can be configured to M13/CBIT framed mode (future). If configured in unframed mode:

- From DS3 TDM interfaces towards PSN, DS3 is mapped to STS-1. The STS-1 is then transported over the packet network through CEP technology, as per RFC4842.
- From PSN towards DS3 TDM interfaces, STS-1 CEP service is terminated. The STS-1 is then de-mapped to DS3.

An MS345\_24 card configured in NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms together with an external TPU box can be protected with a 1:1 protection group. One MS345\_24 card is protected by a second MS345\_24 card through an associated [TPU345\\_24\\_1xx](#) card installed in a patch panel box at the side of the platform. The second (protecting) card is kept in standby mode; traffic is switched to the protecting card if this is triggered, for example, by a hardware failure or user request for a forced switch. Traffic can be switched back to the original protected card after that card recovers and returns to a normal state if switching is revertive. Protection switch time is <50ms for card reset, card extraction, and user-requested commands.

### Features

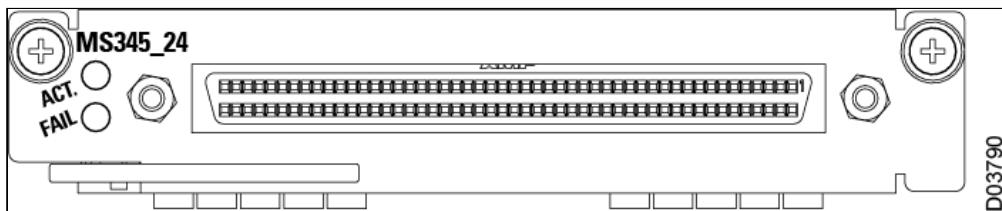
- Supports either:

- 24 x DS3 interfaces, where each DS3 can be configured to a different frame format:
  - Unframed
  - Standard M13 (future)
  - C-bit parity format (future)
- Supported services include:
  - Transparent DS3 over packet via STS-1 CEP, with up to 24 x DS3/STS-1 CEP
  - Channelized DS3, where each DS3 can be channelized to 28 DS1 CES, up to 84 DS1 CES services per card (future)
  - SAToP and CESoPSN service types
  - CESoETH and CESoMPLS emulation formats
- Timing modes:
  - DS1 CES (system timing, loop timing, PSN (ACR, DCR) timing)
  - DS3 STS-1 CEP (system timing)
- DS3 line alarms
- Performance Monitoring (PM)

#### **MS345\_24 Modules and DS3 Interfaces per Platform**

Platform	Max. MS345_24 modules	Max. DS3 Interfaces	Installed into Slots
NPT-1022	1	24	TS1
NPT-1050	3	72	TS1-TS3
NPT-1100	1	24	TS1
NPT-1250	8	192	TS1-TS8
NPT-1300	7	168	TS1-TS7
NPT-1800	23	552	TS1-TS21, TS23-TS24
NPT-2300	7	168	TS1-TS7

#### **MS345\_24 Front Panel**



### MS345\_24 Front Panel LED Indicators and Ports

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected for OC-3/STM-1 port.

## MS16\_4MR Overview

### Supported Platforms

- NPT-1022/B
- NPT-1050
- NPT-1100
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

### Description

The MS16\_4MR is a CES multiservice module with 4 x multi-rate (OC-3/12/48) interfaces, with dual 10G connectivity to the matrix cards. Both intra-card and cross-card linear MS (Line) protection is supported, both unidirectional and bidirectional.

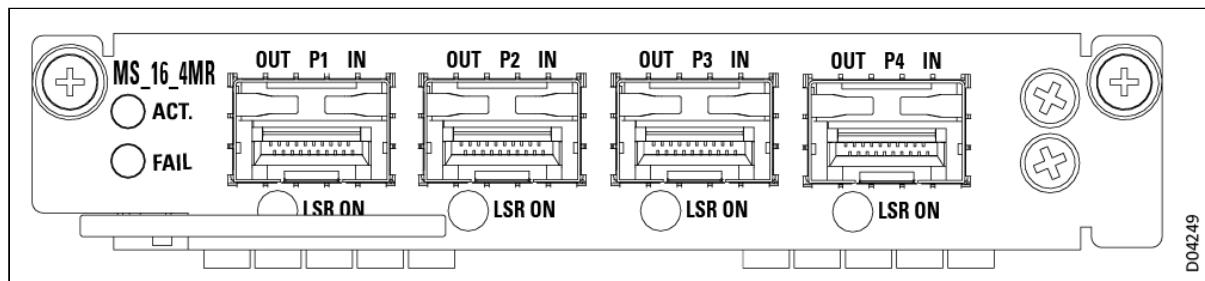
### Features

The MS16\_4MR supports the following features:

- CEP services, through multi-rate SFP interfaces, in any combination of:
  - STS-1 (of OC-3/12/48)
  - STS-3c (of OC-3/12/48)
  - STS-12c (of OC-12/48)
  - STS-48c (of OC-48)
- Unchannelized CEP support
- Channelized SAToP and CESoPSN support (future)
- Encapsulation
  - Ethernet (CESoETH)
  - MPLS (CESoMPLS)
- Linear MSP 1+1 protection - intra-card and cross-card
  - Unidirectional
  - Bidirectional
- Timing
  - 2 reference clocks
  - EPAR for CEP clock recovery mechanism

**MS16\_4MR Modules and Interfaces per Platform**

Platform	Max. MS16_4MR modules	Max. STS-48 Interfaces	Max. STS-12 Interfaces	Max. STS-3 Interfaces	Max. STS-1 Interfaces	Installed into Slots
NPT-102 2/B	1	4	16	64	192	TS1
NPT-105 0	3	12	48	192	576	TS1-TS3
NPT-110 0	1	4	16	64	192	TS1
NPT-125 0	8	32	128	512	1536	TS1-TS8
NPT-130 0	7	28	112	448	1344	TS1-TS7
NPT-180 0	23	92	368	1472	4416	TS1-TS21, TS23-TS24
NPT-230 0	7	28	112	448	1344	TS1-TS7

**MS16\_4MR Front Panel**

### **MS16\_4MR Front Panel LED Indicators and Ports**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected for OC-3 port.
LSR ON (P1-P4)	Laser on indicator	Green	One indicator for each port

## **Data Cards**

The DH cardset, used in the Neptune metro access platforms, includes a broad range of data cards. The data cards in Neptune platforms provide options for packet services with Ethernet, L2, MPLS, L3, IP/MPLS, and FlexE technologies. The following table lists the data cards available, providing a brief description and indicating the platforms on which each card can be installed.

All optical data cards are equipped with transceiver sockets to house various pluggables. For a full list of supported pluggables, please refer to the Neptune System Specifications.

**Neptune Data Cards per Platform (part 1)**

Data cards		NPT-1 022	NPT-1050	NPT-1100
DHFE_12	Ethernet I/O card that supports 12x FE 100/1000BaseT ports on an Eslot card with internal direct connection to the packet switch			
			Yes (not with MCIPS300)	
DHGE_4E	Ethernet I/O card that supports 4 x 10/100/1000BaseT onboard ports with PoE+ capabilities			
			Yes (not with MCIPS300)	
DHGE_4EB	Ethernet I/O card that supports 4 x 10/100/1000BaseT onboard ports with PoE+ capabilities			
			Yes (with MCIPS300 only)	Yes
DHGE_8/ DHGE_8B	Ethernet I/O card that supports 8 x GE (CSFP-based) or 4 x GE (SFP-based) ports, in any mixture of ports			
			Yes (not with MCIPS)	
DHGE_8S	Ethernet I/O card that supports 4 x GE (SFP-based) ports			
			Yes (with MCIPS300 only)	Yes
DHGE_10	Ethernet I/O card that supports 10 x GE (CSFP-based) or 5 x GE (SFP-based) ports, in any mixture of ports			
			Yes (with MCIPS300 only)	Yes

Data cards		NPT-1 022	NPT-1050	NPT-1100
DHGE_10_ POE	Ethernet I/O card with up to 10 GbE ports; 4 of the ports support POE++ on an Eslot card with internal direct connection to the packet switch		Yes	Yes
DHGE_16	Double-slot Ethernet I/O card that supports 8 x 10/100/1000BaseT, 8 x GE (CSFP-based), or 4 x GE (SFP-based) LAN/WAN ports, in any mixture of ports		Yes (not with MCIPS)	
DHGE_24	Double-slot Ethernet I/O card that supports 24 x GE (CSFP-based), or 12 x GE (SFP-based) ports, in any mixture of ports		Yes (not with MCIPS)	
DHXE_2	Ethernet I/O card that supports 2 x 10GbE (SFP+) ports		Yes	Yes
DHXE_4	Ethernet I/O card that supports 4 x 10GbE/1GbE (SFP+) ports		Yes (with MCIPS300 only)	Yes
DHXE_4MR	Ethernet I/O card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces		Yes	Yes
DHXE_4MR sec	Ethernet I/O MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces  All 4 ports support MACsec capability		Yes	Yes
DHXE_40	Ethernet I/O card that supports 4 x 10GbE (SFP+) OTN wrapping (OTU2/2e) ports		Yes	Yes

Data cards		NPT-1 022	NPT-1050	NPT-1100
			Yes (with MCIPS300 only)	Yes
DHXE_4sec	Ethernet I/O card with MACsec capability, that supports: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 10G/1GE multi-rate ports</li></ul> All 4 ports support MACsec capability			
	Yes	Yes (with MCIPS300 only)	Yes	
DHCE_1Q	Ethernet I/O card that supports 1 x 100 GbE (QSFP28) pluggable			
		Yes (with MCIPS300 only)	Yes	
DHCE_1QB /1QC	Ethernet I/O card that supports 1 x 100 GbE (QSFP28/QSFP_DD) pluggable			
		Yes (with MCIPS300 only)	Yes	
DH25_4MR	Ethernet I/O card that supports up to 4 x 10GE/25GE (based on SFP+), with 5G time stamping accuracy			
		Yes (with MCIPS300 only)	Yes	

## Neptune Data Cards per Platform (part 2)

Data cards	NPT-1200	NPT-1250	NPT-300	NPT-1800	NPT-2300	EXT-2U EXT-2UH eEXT-2UH
DHFX_12	Ethernet I/O data card that supports 12x10/100FX ports on an Eslot card with internal direct connection to the packet switch					
	Yes (not with MCIPS)					Installed in <b>EXT-2U</b> with appropriate base platforms
DHFE_12	Ethernet I/O data card that supports 12xFE 100/1000BaseT ports on an Eslot card with internal direct connection to the packet switch					
	Yes (not with MCIPS)					Installed in <b>EXT-2U</b> with appropriate base platforms
DHGE_4E	Ethernet I/O card that supports 4 x 10/100/1000BaseT onboard ports with PoE+ capabilities					
	Yes (with MCIPS only)		Yes	Yes (with CIPS1T only)		
DHGE_4EB	Ethernet I/O card that supports 4 x 10/100/1000BaseT onboard ports with PoE+ capabilities					
	Yes (with MCIPS only)	Yes	Yes	Yes		
DHGE_8 / DHGE_8B	Ethernet I/O card that supports 8 x GE (CSFP-based) or 4 x GE (SFP-based) ports, in any mixture of ports					
	Yes		Yes	Yes (with CIPS1T only)		
DHGE_8S	Ethernet I/O card that supports 4 x GE (SFP-based) ports					
	Yes (with MCIPS only)	Yes	Yes	Yes		

Data cards	NPT-1200	NPT-1250	NPT-1300	NPT-1800	NPT-2300	EXT-2U EXT-2UH eEXT-2UH
DHGE_10	Ethernet I/O card that supports 10 x GE (CSFP-based) or 5 x GE (SFP-based) ports, in any mixture of ports					
	Yes (with MCIPS only)	Yes	Yes	Yes	Yes	
DHGE_10_POE	Ethernet I/O card with up to 10 GbE ports; 4 of the ports support POE++ on an Eslot card with internal direct connection to the packet switch					
	Yes (EXT-2U, with MCIPS only)	Yes (EXT-2UH)		Yes (EXT-2UH)	Yes	Installed in <b>EXT-2U</b> , <b>EXT-2UH</b> , or <b>eEXT-2UH</b> with appropriate base platforms
DHGE_16	Double-slot Ethernet I/O card that supports 8 x 10/100/1000BaseT, 8 x GE (CSFP-based), or 4 x GE (SFP-based) LAN/WAN ports, in any mixture of ports					
	Yes		Yes	Yes (with CIPS1T only)		
DHGE_20	Ethernet I/O card that supports 20 x GE (CSFP-based), or 10 x GE (SFP-based) ports, in any mixture of ports					
			Yes	Yes	Yes	
DHGE_24	Double-slot Ethernet I/O card that supports 24 x GE (CSFP-based), or 12 x GE (SFP-based) ports, in any mixture of ports					
	Yes		Yes (16 ports only)	Yes (with CIPS1T only)		
DHXE_2	Ethernet I/O card that supports 2 x 10GbE (SFP+) ports					
	Yes	Yes	Yes			
DHXE_4	Ethernet I/O card that supports 4 x 10GbE/1GbE (SFP+) ports					
	Yes (with 320/560 only)	Yes	Yes	Yes	Yes	

Data cards	NPT-1200	NPT-1250	NPT-1300	NPT-1800	NPT-2300	EXT-2U EXT-2UH eEXT-2UH
DHXE_4 MR	Ethernet I/O card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces					
		Yes		Yes (with CIPS2T only)		
DHXE_4 MRsec	Ethernet I/O MACsec card that supports up to 4 x 10GE/1GBE (based on SFP+), as well as 5G time stamping accuracy for 10G interfaces All 4 ports support MACsec capability					
	Yes	Yes	Yes	Yes	Yes	
DHXE_4 O	Ethernet I/O card that supports 4 x 10GbE (SFP+) OTN wrapping (OTU2/2e) ports					
	Yes (with CPTS320/CPS320 and MCIPS only)	Yes	Yes	Yes	Yes	
DHXE_4 sec	Ethernet I/O card with MACsec capability, that supports: <ul style="list-style-type: none"><li>• 2 x 10G/OTU-2e (SFP+) ports</li><li>• 2 x 10G/1GE multi-rate ports</li></ul> All 4 ports support MACsec capability					
	Yes (with MCIPS only)	Yes	Yes	Yes	Yes	
DHXE_8	Ethernet I/O card that supports 8 x 10GbE/1GbE (SFP+) ports					
			Yes		Yes	
DHCE_1	Ethernet I/O card that supports 1 x 100 GbE (QSFP28/CFP2) pluggable short, medium, and long reach (coherent) port					
			Yes	Yes	Yes	
DHCE_1 C	Ethernet I/O card that supports 1 x 100 GbE (CFP) pluggable long-reach (coherent) port (OTU-4)					

Data cards	NPT-1200	NPT-1250	NPT-1300	NPT-1800	NPT-2300	EXT-2U EXT-2UH eEXT-2UH
			Yes	Yes		
DHCE_1 Q	Ethernet I/O card that supports 1 x 100 GbE (QSFP28) pluggable					
	Yes (with MCIPS560 only)	Yes	Yes	Yes	Yes	
DHCE_1 QB/1QC	Ethernet I/O card that supports 1 x 100 GbE (QSFP28/QSFP_DD) pluggable					
	Yes (with MCIPS560 only)	Yes	Yes	Yes	Yes	
DH400_1 Q	Ethernet I/O card for T-slot with one 400GE port (based on QSFP-DD)					
					Yes	
DHCE_2	Ethernet I/O card that supports: <ul style="list-style-type: none"><li>• 2 x 100 GbE over one QSFP28 and one CFP2</li><li>• 2 x 100 GbE mapped to OTUC2 over one CFP2</li></ul>					
			Yes		Yes	
DHCE_2 Q	200G/400G Ethernet I/O card with 2 x 100GE/200GE QSFP_DD interfaces with direct connection to the packet switch					
			Yes		Yes	
DH25_4 MR	Ethernet I/O card that supports up to 4 x 10GE/25GE (based on SFP+), with 5G time stamping accuracy					
		Yes	Yes	Yes (with CIPS2T only)	Yes	
DH25_8 MR	Ethernet I/O card for T-slot with eight 25GE/10GE/GE ports (based on SFP28), rate is configurable between 25GBase-R, 10GBase-R, and 1000Base-X on per port basis					

Data cards	NPT-1200	NPT-1250	NPT-1300	NPT-1800	NPT-2300	EXT-2U EXT-2UH eEXT-2UH
					Yes	
<b>FlexE cards</b>						
DHCE_2F	Ethernet I/O FlexE card that supports 2 x 100 GbE interfaces, where each interface can be CFP2 or QSFP28/QSFP_DD					
				Yes (with CIPS2T only)		
DHCE_2MRF	Ethernet I/O FlexE card that supports 1 x 100 GbE (based on QSFP28/QSFP_DD)					
		Yes				

This section introduces the following data cards:

- [DHGE\\_4E and DHGE\\_4EB Overview](#)
- [DHGE\\_8 Overview](#)
- [DHGE\\_8S Overview](#)
- [DHGE\\_10 Overview](#)
- [DHGE\\_16 Overview](#)
- [DHGE\\_20 Overview](#)
- [DHGE\\_24 Description](#)
- [DHXE\\_2 Overview](#)
- [DHXE\\_4 Overview](#)
- [DHXE\\_4MR Overview](#)
- [DHXE\\_4O Overview](#)
- [DHXE\\_4sec Overview](#)
- [DHXE\\_4MRsec Overview](#)
- [DHXE\\_8 Overview](#)
- [DHCE\\_1 Overview](#)
- [DHCE\\_1C Overview](#)
- [DHCE\\_1Q Overview](#)
- [DHCE\\_1QB DHCE\\_1QC Overview](#)
- [DHCE\\_2Q Overview](#)
- [DHCE\\_2 Overview](#)
- [DHCE\\_2F Overview](#)
- [DHCE\\_2MRF Overview](#)
- [DH25\\_4MR Overview](#)
- [DH25\\_8MR Overview](#)
- [DH400\\_1Q Overview](#)

## DHGE\_4E and DHGE\_4EB Overview

### Supported Platforms

- NPT-1021
- NPT-1022/B
- NPT-1050
- NPT-1100
- NPT-1200
- NPT-1250
- NPT-1300
- NPT-1800

### Description

The DHGE\_4E/DHGE\_4EB are data hybrid cards that support up to 4 x 10/100/1000BaseT ports connected to the packet switch. The cards have similar capabilities but differ with regards to backplane connectivity; the DHGE\_4EB supports standard 4 x SGMII interfaces.

### Features

- 4 x 10/100/1000BaseT ports with RJ-45 connectors
- PoE+ functionality

**Modules/Interfaces per Platform**

<b>Platform</b>	<b>Max. DHGE_4E modules</b>	<b>Max. DHGE_4EB modules</b>	<b>Max. 10/100/ 1000BaseT Interfaces</b>	<b>DHGE_4E Installed into Slots</b>	<b>DHGE_4EB Installed into Slots</b>
NPT-1021	1	N/A	4/4	TS1	N/A
NPT-1022/B	N/A	1	-/4 (10BaseT not supported)	N/A	TS1
NPT-1050 (with MCPS100)	3	N/A	12/-	TS1-TS3	N/A
NPT-1050 (with MCIPS300)	N/A	3	-/12 (only 1000BaseT supported)	N/A	TS1-TS3
NPT-1100	N/A	1	4	N/A	TS1
NPT-1200 (with CPS100/320 )	6	N/A	24/24	TS1-TS4, TS6-TS7	N/A
NPT-1200 (with MCIPS320)	4	6	16/24 (Only 100/1000BaseT is supported)	TS1-TS2, TS6-TS7	TS1-TS4, TS6-TS7
NPT-1200 (with MCIPS560)	2	6	8/24 (10BaseT is not supported) (Only 1000BaseT supported in slots 2,3,4,7)	TS1, TS6 100/1000Base T	TS1, TS6 100/1000Base T  TS2-TS4, TS7 1000BaseT only
NPT-1250	N/A	8	32 (10BaseT is not supported) (Only 1000BaseT supported in slots 1,4,7,8)	N/A	TS1-TS8

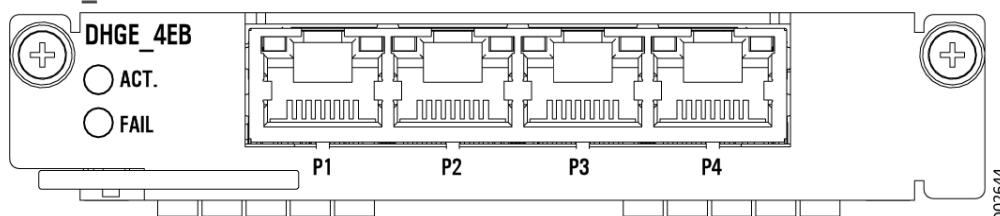
Platform	Max. DHGE_4E modules	Max. DHGE_4EB modules	Max. 10/100/ 1000BaseT Interfaces	DHGE_4E Installed into Slots	DHGE_4EB Installed into Slots
NPT-1300	3	7	12/28 (10BaseT is not supported)  (Only 1000BaseT supported in slots 2,3,4,7)	TS1, TS5, TS6	TS1-TS7
NPT-1800 (with CIPS1T)	11	23	44/71 [high accuracy PTP disabled]  44/70 [high accuracy PTP enabled]  (10BaseT is not supported)  (Only 1000BaseT supported in slots 10-15)	TS1-TS6, TS19-TS21, TS23-TS24	TS1-TS24, except TS22
NPT-1800 (with CIPS2T)	N/A	23	-/92 (10BaseT is not supported)  (Only 1000BaseT supported in slots 5-18 and 23, 24)	N/A	TS1-TS24, except TS22

### Usage Guidelines

- When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform.
- PoE+ configuration:
  - When the DHGE\_4E/4EB is configured with PoE, the main power feeding voltage must be less than 58 VDC and greater than 40V.
  - The DHGE\_4E/4EB card MAX power consumption for PoE is 62 W; any mixture of PD devices is allowed up to 62W.

Cabling for the DHGE\_4E/4EB module is directly from the front panel. The DHGE\_4E card has an essentially identical panel layout.

### DHGE\_4EB Front Panel



**LEDs**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Off indicates no power supply. On steadily indicates the module was not downloaded successfully or the module cannot be controlled normally by the MCP1200. Blinking indicates the module is running normally.
FAIL	Module fail	Red	Normally off. Lights when module failure detected.
- (left LED in the P1 to P4 RJ-45)	Link/Active (P1 to P4 10/100/1000BaseT interface)	Green	Lights when the link is OK. Blinks when packets are received or transmitted.
- (right LED in the P1 to P4 RJ-45)	Speed (P1 to P4 FE 10/100/1000BaseT interface)	Orange	Off when the speed is 10/100 Mbps. Lights steadily when the speed is 1000 Mbps.

## DHGE\_8 Overview

### Supported Platforms

- NPT-1021
- NPT-1050 (with MCPS100)
- NPT-1200
- NPT-1300
- NPT-1800 (with CIPS1T)

### Description

The DHGE\_8 is a data hybrid card that supports up to 8 x GbE/FX ports connected to the packet switch.

### Features

- 4 x physical sockets for installation of SFP, CSFP, or ETGBE transceivers:
  - CSFP enables two bidirectional 100/1000Base-X ports, with a total of 8 ports per card (Port1 ~ Port8)
  - SFP enables a single 1000Base-X/100Base-FX/1000Base-T port, with a total of 4 ports per card (Port1 ~ Port4)
  - ETGBE enables 10/100/1000BaseT
  - E1POP Smart SFP supported in 1000Base-T ports

**Modules/Interfaces per Platform**

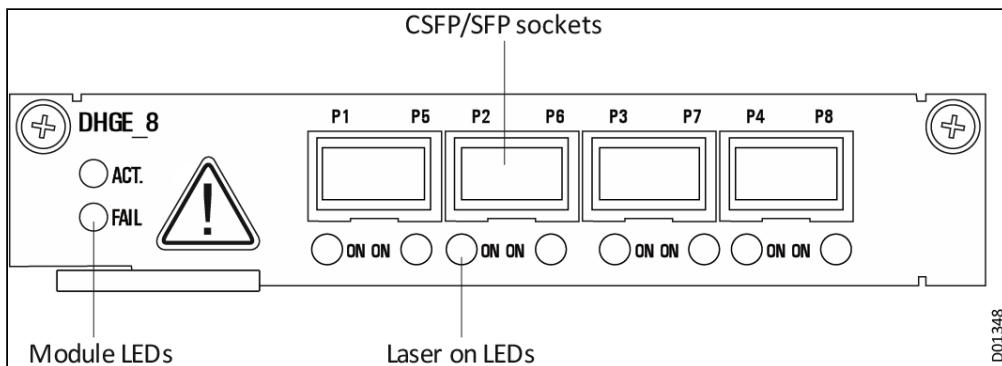
Platform	Max. DHGE_8 modules	Max. 100/1000Base-X Interfaces	Max. 10/100/1000BaseT (electrical)	Installed into Slots
NPT-1021	1	4	4	TS1
NPT-1050 (with MCPS100)	3	24	12	TS1-TS3
NPT-1200 (with CPS100/320)	6	48	24	TS1-TS4, TS6-TS7
NPT-1200 (with MCIPS320)	4	32	16 (10BaseT is not supported)	TS1, TS2, TS6, TS7
NPT-1200 (with MCIPS560)	2	16	8 (10BaseT is not supported)	TS1, TS6
NPT-1300	3	24	12 (10BaseT is not supported)	TS1, TS5, TS6
NPT-1800 (with CIPS1T)	11	64	32 (10BaseT is not supported)	TS1-TS6, TS19-TS21, TS23-TS24

**Usage Guidelines**

- Support for dense 100Base-X with CTFE\_xx transceivers.
- When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform.

**Card View**

- The card ports are grouped in pairs: P1~P5, P2~P6, P3~P7, and P4~P8
- Each pair represents a socket. Each socket can contain either an SFP or CSFP transceiver

**DHGE\_8 Front Panel****LEDs**

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON (P1 to P8)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHGE\_8S Overview

**Supported Platforms**

- NPT-1021
- NPT-1022/B
- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with MCIPS320/MCIPS560)
- NPT-1250
- NPT-1300
- NPT-1800

**Description**

The DHGE\_8S supports GE/FX (SFP) ports. This card is a logical card type with same physical card type as DHGE\_8.

**Features**

- 4 x GE/FX (SFP) or ETGE ports
- Supports only SFP transceivers (optical and electrical)

**DHGE\_8S Modules and GE Interfaces per Platform**

Platform	Max. DHGE_8S modules	Max. 100/1000Base-X Interfaces	Max. 10/100/1000BaseT (electrical)	Installed into Slots
NPT-1021	1	4	4	TS1
NPT-1022/B	1	4	4 (10BaseT is not supported)	TS1
NPT-1050 (with MCIPS300)	3	12 (1000BaseX only)	12 (1000BaseT only)	TS1-TS3
NPT-1100	1	4	4	TS1
NPT-1200 (with MCIPS320)	2	8	8 (10BaseT is not supported)	TS3, TS4
NPT-1200 (with MCIPS560)	4	16 (1000BaseX only)	16 (1000BaseT only)	TS2-TS4, TS7
NPT-1250	8	32 (1000BaseX only in TS1, TS4, TS7, TS8)	32 (10BaseT is not supported) (TS1, TS4, TS7, TS8 support 1000BaseT only)	TS1-TS8
NPT-1300	4	16 (1000BaseX only)	16 (1000BaseT only)	TS2-TS4, TS7
NPT-1800 (with CIPS1T)	23	71 [high accuracy PTP disabled] 70 [high accuracy PTP enabled] (TS10-TS15 support 1000BaseX only)	71 [high accuracy PTP disabled] 70 [high accuracy PTP enabled] (10BaseT is not supported) (TS10-TS15 support 1000BaseX or 1000BaseT only)	TS1-TS24, except TS22

Platform	Max. DHGE_8S modules	Max. 100/1000Base-X Interfaces	Max. 10/100/1000BaseT (electrical)	Installed into Slots
NPT-1800 (with CIPS2T)	23	92	92 (10BaseT is not supported) (Only 1000BaseT supported in TS5-TS18, TS23, and TS24)	TS1-TS24, except TS22

### Usage Guidelines

- When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform.
- The physical specifications of the DHGE\_8S card are identical to the DHGE\_8 card - same physical front panel, cabling, and LED indicators as described in [DHGE\\_8](#), without the CSFP support.

## DHGE\_10 Overview

### Supported Platforms

- NPT-1022/B
- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with MCIPS320/MCIPS560)
- NPT-1250
- NPT-1300
- NPT-1800

### Description

The DHGE\_10 is a data hybrid card that supports up to 10 x GE/OTFX ports connected to the packet switch.

### Features

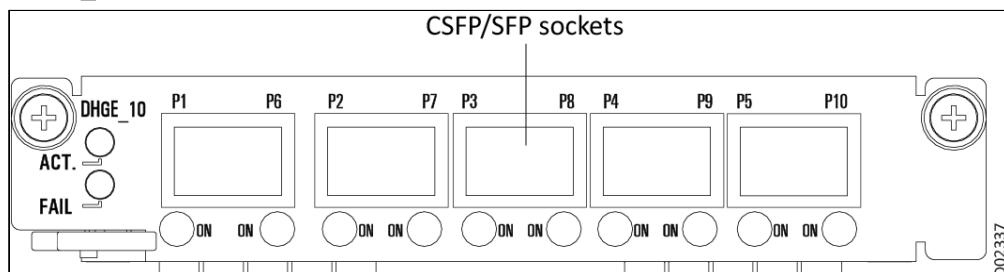
- 5 X physical sockets for installation of either SFP or CSFP transceivers:
  - CSFP enables two bidirectional 100/1000Base-X ports , for a total of 10 ports per card.
  - SFP enables a single 1000Base-X/100Base-FX/1000Base-T port, for a total of 5 ports per card.
  - ETGBE enables 10/100/1000 Base-T.
  - E1POP Smart SFP supported in 1000Base-T ports.
- MPLS support with appropriate licensing.
- Supports 1588v2 primary, secondary, and transparent modes.
- Sync-E support with configurable Tx clock between T0 and PTP clock
  - Two timing sources can be selected per card
  - Sync-E (Tx only) supported for electrical ports with ETGBE\_SE

**Max DHGE\_10 modules and Interfaces per Platform**

Platform	Max. DHGE_10 modules	Max.100/1000Base-X Interfaces	Max. 10/100/1000BaseT (electrical with ETGE)	Installed into Slots
NPT-1022/B	1	10	5	TS1
NPT-1050 (with MCIPS300)	3	30	15	TS1-TS3
NPT-1100	1	10	5	TS1
NPT-1200 (MCIPS320/ MCIPS560)	6	60	30	TS1-TS4, TS6-TS7
NPT-1250	8	78	40	TS1-TS8
NPT-1300	7	70	35	TS1-TS7
NPT-1800 (CIPS1T/ CIPS2T)	23/18  (Number of assigned cards in 2T is limited due to power consumption management constraints)	198/180	115/90	TS1-TS24 except TS22

**Usage Guidelines**

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

**DHGE\_10 Front Panel**

- Card ports are grouped in pairs: P1 and P6, P2 and P7, P3 and P8, P4 and P9, and P5 and P10
- Each pair represents a socket. Each socket can contain either an SFP or CSFP transceiver, supporting one 1000Base-X/100Base-FX/1000Base-T port (for SFP) or two bidirectional 100/1000Base-X ports (for CSFP)

The Laser On LED indicators are arranged in two groups, one on each side of the card. The table near each group identifies the corresponding LED for each port.

### LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR. ON (1 to 10)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHGE\_16 Overview

### Supported Platforms

- NPT-1050 (with MCPS100)
- NPT-1200
- NPT-1300
- NPT-1800 (with CIPS1T)

### Description

The DHGE\_16 is a double-slot data hybrid card that supports up to 8 x 10/100/1000BaseT and 8 x GbE/FX ports connected to the packet switch.

### Features

- 4 x physical sockets for installation of either SFP or CSFP transceivers:
  - CSFP enables two bidirectional 100/1000Base-X ports, with a total of 8 ports per card.
  - SFP enables a single 1000Base-X/100Base-FX/1000Base-T port, for a total of 4 ports per card.
- 8 x 10/100/1000Base-T ports with RJ45 connectors.
- E1POP Smart SFP supported in 1000Base-T ports.
- MPLS support with appropriate licensing.
- Supports 1588v2 primary, secondary, and transparent modes.

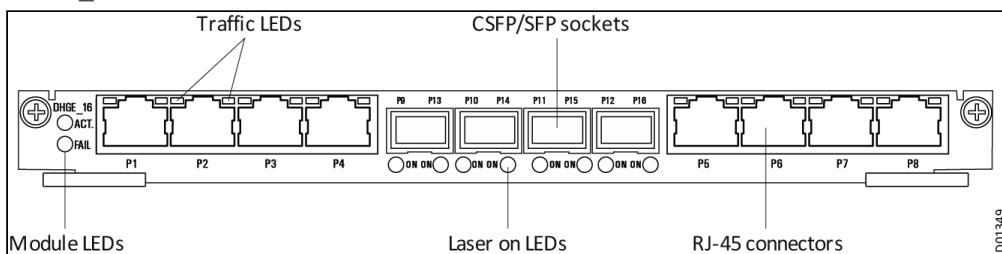
**Max DHGE\_16 modules and Interfaces per Platform**

Platform	Max. DHGE_16 modules	Max.1000Base-X Interfaces	Max 100BaseX Interfaces	Max. 10/100/1000BaseT (electrical) Interfaces	Installed into Slots
NPT-1050 (only with MCPS100)	1	8	8	12	Tslot pairs: TS2+TS3
NPT-1200	2	16	16	24 (10BaseT is not supported with MCIPS320/560)	Tslot pairs: TS1+TS2 and TS6+TS7
NPT-1300	2	16	16	24 (10BaseT is not supported)	Tslot pairs: TS1+TS2 and TS6+TS7
NPT-1800 (with CIPS1T)	4	32	32	48 (10BaseT is not supported)	Tslot pairs: TS1+TS2 or TS2+TS3  TS4+TS5 or TS5+TS6  TS19+TS20 or TS20+TS21  TS23+TS24 (Group I)

**Usage Guidelines**

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

### DHGE\_16 Front Panel



- The module occupies a double slot in the Tslot module space. A spacer between the slot pairs must be removed; see the Operation, and Maintenance Manuals for further information.
- Ports P1 to P8 are RJ-45 connectors for 8 x 10/100/1000BaseT electrical interfaces.
- Ports P9 to P16 are grouped in pairs: P9~P13, P10~P14, P11~P15, and P12~P16. Each pair represents a socket. Each socket can contain either an SFP or CSFP transceiver. SFPs support one 1000Base-X/100Base-FX port, and CSFPs support two bidirectional 100/1000Base-X ports.

### LEDs

Marking	Full Name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
- (left LED in the P9 to P16 RJ-45)	Link/Active (P1 to P8 interface)	Green	Lights when the link is OK. Blinks when packets are received or transmitted.
- (right LED in the P9 to P16 RJ-45)	Speed (P1 to P8 interface)	Orange	Off when the speed is 10/100 Mbps. Lights steadily when the speed is 1000 Mbps.
ON (P1 to P8)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHGE\_20 Overview

### Supported Platforms

- NPT-1300
- NPT-1800

### Description

The DHGE\_20 is a data hybrid card for high-capacity slots that supports 10/20 x GE/FX ports connected to the packet switch.

### Features

- 10 x physical sockets for installation of either SFP or CSFP transceivers:
  - CSFP enables two bidirectional 100/1000Base-X ports, for a total of 20 ports per card.
  - SFP enables a single 1000Base-X/100Base-FX/1000Base-T port, for a total of 10 ports per card.
- 10/100/1000Base-T interfaces are fully supported.
- E1POP Smart SFP supported in 1000Base-T ports.
- MPLS support with appropriate licensing.
- Supports 1588v2 primary, secondary, and transparent modes.

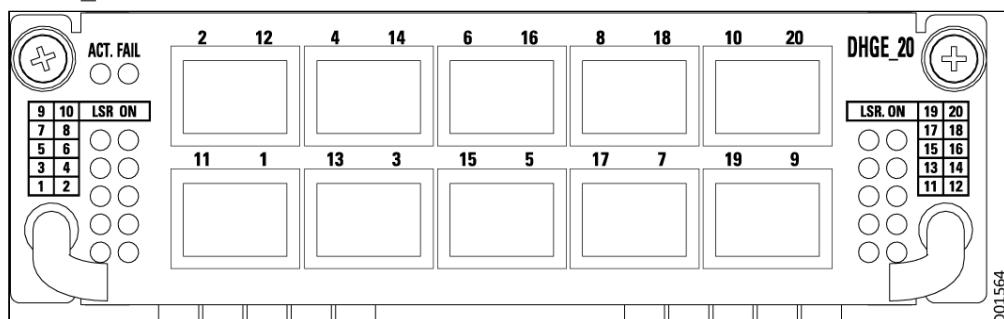
#### Max DHGE\_20 modules and Interfaces per Platform

Platform	Max. DHGE_20 modules	Max. 100/1000Base-X Interfaces	Max. 10/100/1000BaseT (electrical with ETGE) Interfaces	Installed into Slots
NPT-1300	7	140	70	TS1-TS7
NPT-1800 (CIPS1T/ CIPS2T)	12	197/240	120	TS7-TS18

#### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

#### DHGE\_20 Front Panel



- Card ports are grouped in pairs: P1 and P11, P2 and P12, P3 and P13, and so on, to P10 and P20.
- Each pair represents a socket. Each socket can contain either an SFP or CSFP transceiver.
- The Laser On LED indicators are arranged in two groups, one on each side of the card. The table near each group identifies the corresponding LED for each port.

**LEDs**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (1 to 20)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHGE\_24 Description

**Supported Platforms**

- NPT-1050 (with MCPS100)
- NPT-1200
- NPT-1300
- NPT-1800 (with CIPS1T)

**Description**

The DHGE\_24 is a double-slot data hybrid card that supports up to 24 x GbE/FX ports connected to the packet switch.

**Features**

- 12 x physical sockets for installation of either SFP or CSFP transceivers:
  - CSFP enables two bidirectional 100Base-FX/1000Base-X ports, for a total of 24 ports per card.
  - SFP enables a single 1000Base-X/100Base-FX/1000Base-T port, for a total of 12 ports per card.
- E1POP Smart SFP supported in 1000Base-T ports.

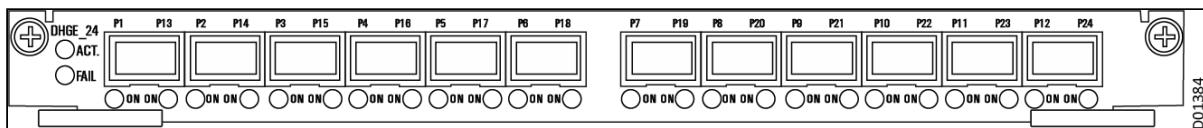
**Max DHGE\_24 modules and Interfaces per Platform**

Platform	Max. DHGE_24 modules	Max. 100/1000Base-X Interfaces	Max. 10/100/1000BaseT (electrical) Interfaces	Installed into Slots
NPT-1050 (with MCPS100)	1	24	12	Tslot pairs: TS2+TS3
NPT-1200 (with CPS100, CPS320, MCIPS320)	2	48	24 (10BaseT is not supported with MCIPS320)	Tslot pairs: TS1+TS2 and TS6+TS7
NPT-1200 (with MCIPS560)	2	32	24 (10BaseT is not supported)	Tslot pairs: TS1+TS2 and TS6+TS7
NPT-1300	2	32	24 (10BaseT is not supported)	Tslot pairs: TS1+TS2 and TS6+TS7
NPT-1800 (with CIPS1T)	4	64	48 (10BaseT is not supported)	Tslot pairs: TS1+TS2 <i>or</i> TS2+TS3  TS4+TS5 <i>or</i> TS5+TS6  TS19+TS20 <i>or</i> TS20+TS21  TS23+TS24 (Group I)

**Usage Guidelines**

- When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform.
- When DHGE\_24 is assigned in TS1-2 or TS6-7 in NPT-1200 with MCIPS560 or NPT-1300, only 16 ports can be activated; P17-P24 cannot be used.

## DHGE\_24 Front Panel



The card ports are grouped in pairs: P1~P13, P2~P14, P3~P15, and so on, to P12~P24. Each pair represents a socket, with each socket containing either an SFP or CSFP transceiver. The module occupies a double slot in the Tslot module space. A spacer between the slot pairs must be removed; see the Operation and Maintenance Manuals for further information.

### LEDs

Marking	Full Name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON (P1 to P24)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHXE\_2 Overview

### Supported Platforms

- NPT-1022/B
- NPT-1050
- NPT-1200
- NPT-1250
- NPT-1300

### Description

The DHXE\_2 is a data hybrid card with 2 x 10GbE ports connected to the packet switch.

### Features

- 2 x 10GbE ports
- Each 10GBE interface can be configured as 10GBase-R, 10GBase-W, or 10GBase-R over OTU2e
- OTSOP16 Smart SFP supported in SFP+\_10GE ports
- Support for FEC and EFEC (I4, I7) with OTU2e wrapping

### Max DHXE\_2 Modules and Interfaces per Platform

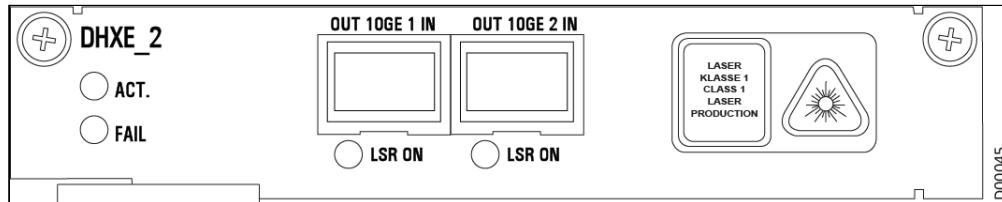
Platform	Max. DHXE_2 modules	Max. 10GE Interfaces	Installed into Slots
NPT-1022/B	1	2	TS1
NPT-1050	3	6	TS1-TS3
NPT-1200 (with CPS100)	3	6	TS1-TS4, TS6-TS7
NPT-1200 (with CPS320 and MCIPS320)	6	12	TS1-TS4, TS6-TS7
NPT-1200 (with MCIPS560)	6	12	TS1-TS4, TS6-TS7
NPT-1250	8	16	TS1-TS8
NPT-1300	7	14	TS1-TS7

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DHXE\_2 module is directly from the front panel with two SFP+ transceivers. The card has two SFP housing slots for SFP+ transceivers.

### DHXE\_2 Front Panel



**LEDs**

<b>Marking</b>	<b>Full name</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 and P2)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHXE\_4 Overview

**Supported Platforms**

- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with CPS320, MCIPS320/560)
- NPT-1250
- NPT-1300
- NPT-1800

**Description**

The DHXE\_4 is a data hybrid multi-rate card supporting up to 4 x 10GbE/1GbE ports connected to the packet switch. 1G/10G multi-rate support is available as of v8.1. E1POP Smart SFPs are supported in 1000Base-T ports. OTSOP16 Smart SFPs are supported in SFP+\_10GE ports.

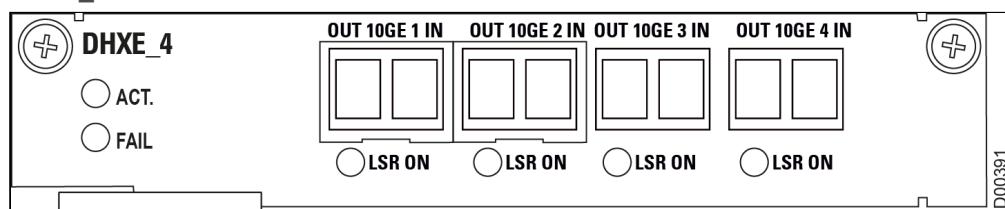
**Max DHXE\_4 Modules and Interfaces per Platform**

Platform	Max. DHXE_4 modules	Max. 10GE Interfaces	Installed into Slots
NPT-1050 (with MCIPS300)	3	12	TS1-TS3
NPT-1100	1	4	TS1
NPT-1200 (with CPS320, MCIPS320/560)	6	24	TS1-TS4, TS6-TS7
NPT-1250	8	32	TS1-TS8
NPT-1300	7	28	TS1-TS7
NPT-1800 (with CIPS1T)	18	71 [High accuracy PTP disabled] 70 [High accuracy PTP enabled]	TS1-TS24, except TS22
NPT-1800 (with CIPS2T)	23	92	TS1-TS24, except TS22

**Usage Guidelines**

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and Port Configuration Guidelines](#).

The cabling of the DHXE\_4 module is directly from the front panel with four SFP+ transceivers. The card has four SFP housing slots for SFP+ transceivers.

**DHXE\_4 Front Panel**

## LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P4)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHXE\_4MR Overview

### Supported Platforms

- NPT-1022/B
- NPT-1100
- NPT-1250
- NPT-1800 (with CIPS2T only)

### Description

The DHXE\_4MR is a 40G multi-rate card that supports up to 4 x 1GE/10GBE, configurable per port (based on SFP/SFP+). OTSOP16 Smart SFP is supported in SFP+\_10GE ports. This card provides 5G time stamping accuracy (G.8273.2 Class C) for 10G interfaces, supporting both 1588 and Sync-E. Two recovered clocks from 4 ports can be selected as the timing source.

### Max DHXE\_4MR Cards and Interfaces per Platform

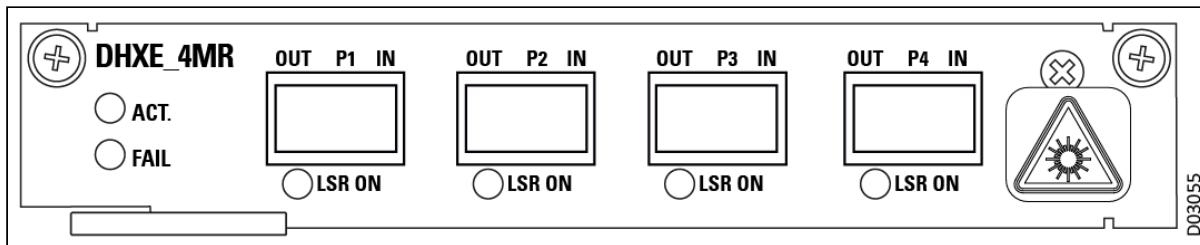
Platform	Max. DHXE_4MR Cards	Max. 1/10GE Interfaces	Inserted into Slots
NPT-1022/B	1	4/2	TS1
NPT-1100	1	4/4	TS1
NPT-1250	8	32	TS1-TS8
NPT-1800 (with CIPS2T only)	23	92/92	TS1-TS24, except TS22

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DHXE\_4MR module is directly from the front panel with four SFP/SFP+ transceivers. The card has four SFP housing slots for SFP/SFP+ transceivers.

### DHXE\_4MR Front Panel



### LEDs

Marking	Full Name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P4)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHXE\_4O Overview

### Supported Platforms

- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with CPTS320/CPS320 and MCIPS only)
- NPT-1250
- NPT-1300
- NPT-1800

### Description

The DHXE\_4O is a data hybrid card with 10GbE/OUT2e ports connected to the packet switch.

### Features

- 4 x 10GbE/OUT2e ports. Each port can be configured as 10GBase-R, 10GBase-W, or 10GBase-R over OTU2e
- OTSOP16 Smart SFP supported in SFP+\_10GE ports
- Support for OTN wrapping
- Support for FEC and EFEC (I4, I7) with OTU2e wrapping

### Max DHXE\_4O Modules and Interfaces per Platform

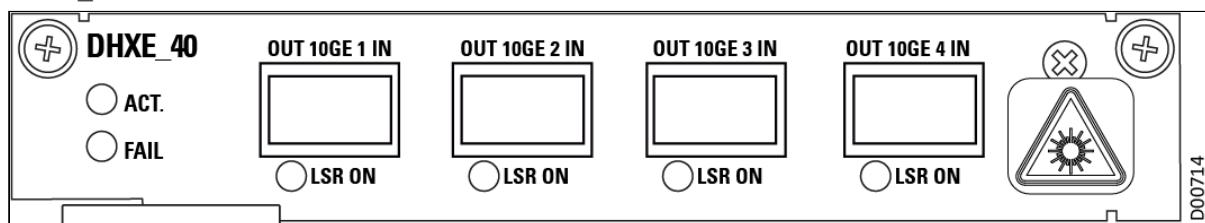
Platform	Max. DHXE_4O Modules	Max. 10GE Interfaces	Installed into Slots
NPT-1050 (with MCIPS300)	3	12	TS1-TS3
NPT-1100	1	4	TS1
NPT-1200 (with CPS320, MCIPS320, or MCIPS560)	6	24	TS1-TS4, TS6-TS7
NPT-1250	8	32	TS1-TS8
NPT-1300	7	28	TS1-TS7
NPT-1800 (with CIPS1T)	18	71 [High accuracy PTP disabled] 70 [High accuracy PTP enabled]	TS1-TS24, except TS22
NPT-1800 (with CIPS2T)	16 (with INF_1800) 23 (with INF_1800H)	64 92	TS1-TS24, except TS22

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DHXE\_4O module is directly from the front panel with four SFP+ transceivers. The card has four positions for installing SFP+ transceivers.

### DHXE\_4O Front Panel



**LEDs**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P4)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHXE\_4sec Overview

**Supported Platforms**

- NPT-1022/B
- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with MCIPS320/MCIPS560)
- NPT-1250
- NPT-1300
- NPT-1800

**Description**

The DHXE\_4sec is a 40G data hybrid card with MACsec capability connected to a packet switch.

**Features**

- 2 x 10G/OTU-2e (SFP+) ports (P3 and P4)
- 2 x 10G/1GE multi-rate ports (P1 and P2)
- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+\_10GE ports

All 4 ports support MACsec capability, providing network-wide L2 traffic port-to-port encryption, as per the IEEE 802.1AE standard. The strong cipher implementation is based on GCM-AES-256.

5G timing accuracy (G.8273.2 Class C) is supported when it is installed in NPT-1022, NPT-1050 (with MCIPS300), NPT-1250, and NPT-1800 (with CIPS2T) platforms.

As of V8.1, 1588 PTP (G.8273.2 Class B) is supported when it is installed on NPT-1800 (with CIPS1T), NPT-1300, and NPT-1200 (with MCIPS320/560) platforms.

i **Note:**

PTP for the DHXE\_4sec port and PTP for the DHGE\_4E/8/16/24 port cannot be enabled simultaneously.

- If there is PTP enabled on DHXE\_4sec port, then PTP cannot be enabled on a DHGE\_4E/8/16/24 port
- If there is PTP enabled on a DHGE\_4E/8/16/24 port, then PTP cannot be enabled on a DHXE\_4sec port

The DHXE\_4sec timing functions are as follows:

- SyncE clock per port
- Two timing reference clocks from four ports



**Optional Feature:**

DHXE\_4sec requires a software license to activate 1G/10G encryption; MACsec activation is license-controlled per port.

#### Max DHXE\_4sec Modules and Interfaces per Platform

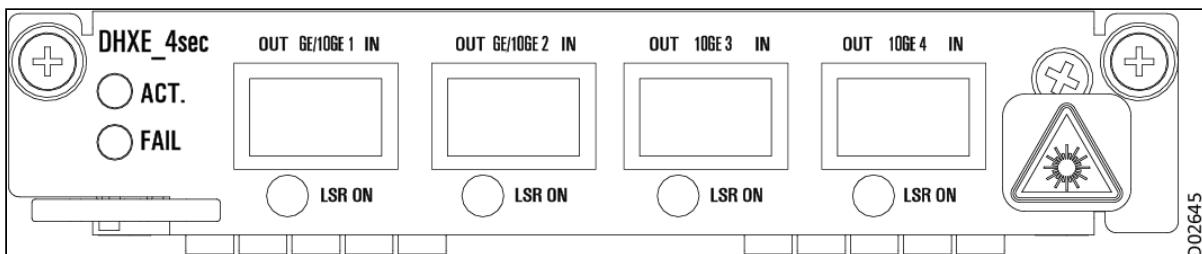
Platform	Max. DHXE_4sec modules	Max. GE Interfaces	Max. 10GE Interfaces	Installed into Slots
NPT-1022/B	1	2	2	TS1
NPT-1050 (with MCIPS300)	3	6	12	TS1-TS3
NPT-1100	1	2	2	TS1
NPT-1200 (with MCIPS320 / MCIPS560)	6	12	24	TS1-TS4, TS6- TS7
NPT-1250	8	16	32	TS1-TS8
NPT-1300	7	14	28	TS1-TS7
NPT-1800 (with CIPS1T)	18	36	71 [High accuracy PTP disabled] 70 [High accuracy PTP enabled]	TS1-TS24, except TS22
NPT-1800 (with CIPS2T)	18 (with INF_1800) 23 (with INF_1800H)	36 46	72 92	TS1-TS24, except TS22

#### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DHXE\_4sec module is directly from the front panel with four SFP+ transceivers. The card has four SFP sockets for installing SFP+ transceivers.

### DHXE\_4sec Front Panel



### LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P4)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHXE\_4MRsec Overview

### Supported Platforms

- NPT-1022/B
- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with MCIPS320/MCIPS560)
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

### Description

The DHXE\_4MRsec is a 40G data hybrid card with MACsec capability connected to a packet switch.

### Features

- 4 x 10G/1GE multi-rate ports (P1-P4)
- E1POP Smart SFP supported in 1000Base-T ports
- OTSOP16 Smart SFP supported in SFP+\_10GE ports

All 4 ports support MACsec capability, providing network-wide L2 traffic port-to-port encryption, as per the IEEE 802.1AE standard. The strong cipher implementation is based on GCM-AES-256.

5G timing accuracy (G.8273.2 Class C) is supported when it is installed in NPT-1022, NPT-1250, NPT-1800 (with CIPS2T), and NPT-2300 platforms.

1588 PTP (G.8273.2 Class B) is supported when it is installed on NPT-1800 (with CIPS1T), NPT-1300, NPT-1200 (with MCIPS320/560), and NPT-1050 (with MCIPS300) platforms.

**i Note:**

PTP for the DHXE\_4MRsec port and PTP for the DHGE\_4E/8/16/24 port cannot be enabled simultaneously.

- If there is PTP enabled on DHXE\_4MRsec port, then PTP cannot be enabled on a DHGE\_4E/8/16/24 port
- If there is PTP enabled on a DHGE\_4E/8/16/24 port, then PTP cannot be enabled on a DHXE\_4MRsec port

The DHXE\_4MRsec timing functions are as follows:

- SyncE clock per port
- Two timing reference clocks from four ports

**i Optional Feature:**

DHXE\_4MRsec requires a software license to activate 1G/10G encryption; MACsec activation is license-controlled per port.

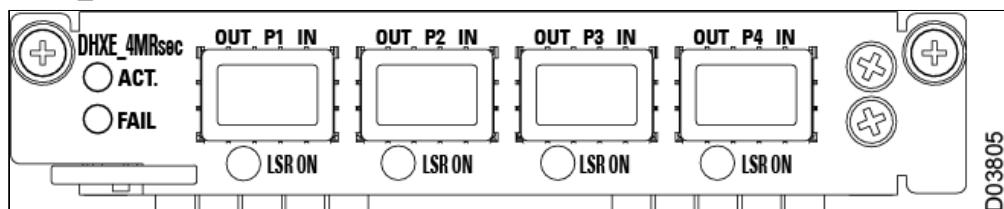
**Max DHXE\_4sec Modules and Interfaces per Platform**

Platform	Max. DHXE_4MRsec modules	Max. GE Interfaces	Max. 10GE Interfaces	Installed into Slots
NPT-1022/B	1	4	4	TS1
NPT-1050 (with MCIPS300)	3	12	12	TS1-TS3
NPT-1100	1	4	4	TS1
NPT-1200 (with MCIPS320 / MCIPS560)	6	24	24	TS1-TS4, TS6- TS7
NPT-1250	8	32	32	TS1-TS8
NPT-1300	7	28	28	TS1-TS7
NPT-1800 (with CIPS1T)	18	71 [High accuracy PTP disabled] 70 [High accuracy PTP enabled]	71 [High accuracy PTP disabled] 70 [High accuracy PTP enabled]	TS1-TS24, except TS22
NPT-1800 (with CIPS2T)	18 (with INF_1800) 23 (with INF_1800H)	72 92	72 92	TS1-TS24, except TS22
NPT-2300	7	28	28	TS1-TS7

**Usage Guidelines**

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DHXE\_4MRsec module is directly from the front panel with four SFP+ transceivers. The card has four SFP sockets for installing SFP+ transceivers.

**DHXE\_4MRsec Front Panel**

**LEDs**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P4)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHXE\_8 Overview

**Supported Platforms**

- NPT-1300

**Description**

The DHXE\_8 is a data hybrid multi-rate card that supports up to 8 x 10GbE/1GbE ports connected to a packet switch. 1G/10G multi-rate support is available as of v8.1. E1POP Smart SFPs are supported in 1000Base-T ports. OTSOP16 Smart SFPs are supported in SFP+\_10GE ports. Sync-E and 1588 Class B are supported.

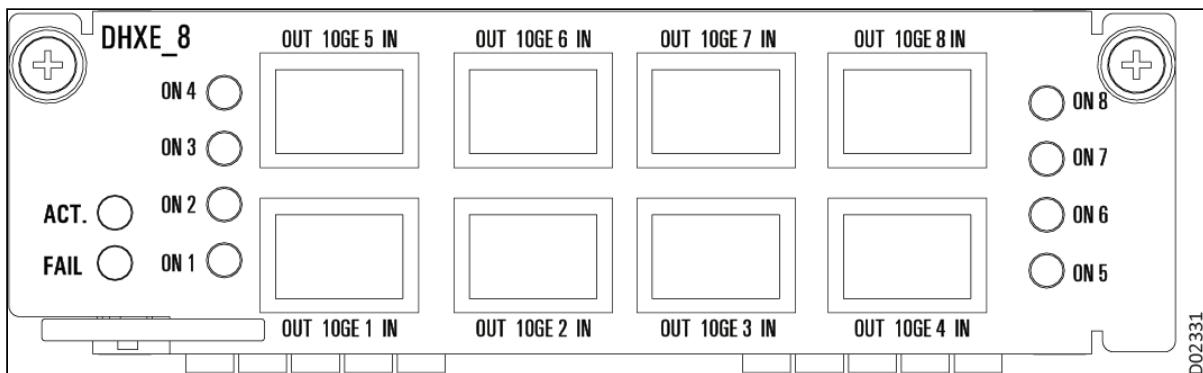
**Max DHXE\_8 modules and Interfaces per Platform**

<b>Platform</b>	<b>Max. DHXE_8 modules</b>	<b>Max. 10GE Interfaces</b>	<b>Installed in these Slots</b>
NPT-1300	5	40	TS1-TS2, TS5-TS7

**Usage Guidelines**

- When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).
- When the DHXE\_8 is installed in all 5 available slots in the NPT-1300, a total of 56 x 10GE interfaces can be configured in the platform, including 8 x 10GE on the MCIPS1T matrix cards and installing two DHXE\_4 cards in slots TS3 and TS4.

The cabling of the DHXE\_8 module is directly from the front panel with eight SFP+ transceivers. The card has eight SFP sockets for installing SFP+ transceivers.

**DHXE\_8 Front Panel****LEDs**

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON (P1 to P8)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

**DHCE\_1 Overview****Supported Platforms**

- NPT-1300
- NPT-1800
- NPT-2300

**Description**

The DHCE\_1 is a 100G Ethernet multiservice interface card, designed for access and intra office configurations, connected to a packet switch.

**Features**

- Sockets for:
  - 1 x CFP2 transceiver  
or
  - 1 x QSFP28 transceiver, supporting SR4, CWDM4, LR4, ER4, and ZR4
- Connects directly to the packet switch with 100G based connections
- Supports 100GBase-R and 100GBase-R with OTU4 mapping
- Supports OTU4 colored and tunable CFP2 with coherent-based technology
- Supports terminal/facility loopback as well as CL91 FEC

### Max DHCE\_1 Cards and Interfaces per Platform

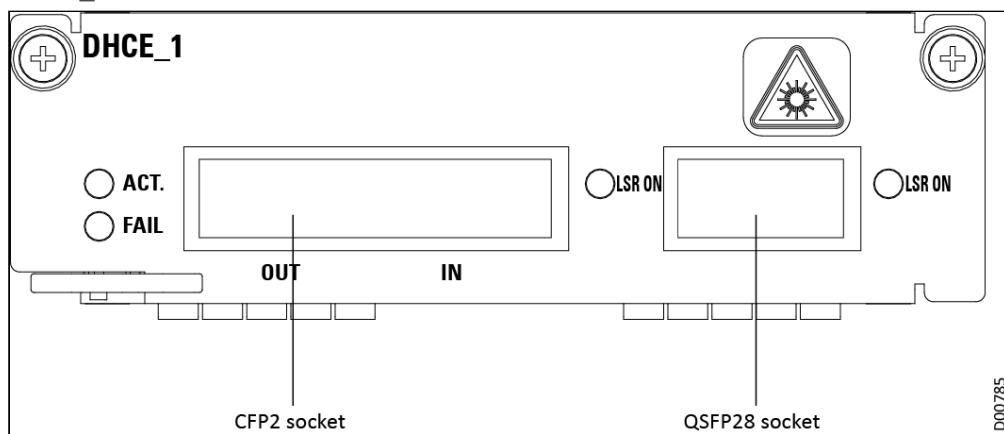
Platform	Max. DHCE_1 Cards	Max. 100GE Interfaces	Installed into Slots
NPT-1300	4	4	TS2-TS4, TS7
NPT-1800 (with CIPS1T)	6	6	TS10-TS15 (Group II)
NPT-1800 (with CIPS2T)	12	12	TS7-TS18
NPT-2300	7	7	TS1-TS7

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The card has two sockets for installing either a CFP2 or QSFP28 transceiver. Only one transceivers can be configured at a time.

### DHCE\_1 Front Panel



### LEDs

Marking	Description	Color	Function
Lights steadily when the corresponding QSFP28 laser is on.	Sample text for column 2	Sample text for column 3	
LSR ON (CFP2 port)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHCE\_1C Overview

### Supported Platforms

- NPT-1300
- NPT-1800

### Description

The DHCE\_1C is an Ethernet multiservice interface card with a 100G/OTU-4 port. The card is designed for metro and metro core network configurations. This card supports 100G long distance interfaces for 80km and longer, based on CFP modules.

### Features

- 1 x CFP port, with a single CFP socket.
- Connected directly to the packet switch with 100G-based connections.
- Supports OTU-4 colored and tunable CFPs with coherent-based technology.
- Supports terminal/facility loopback.

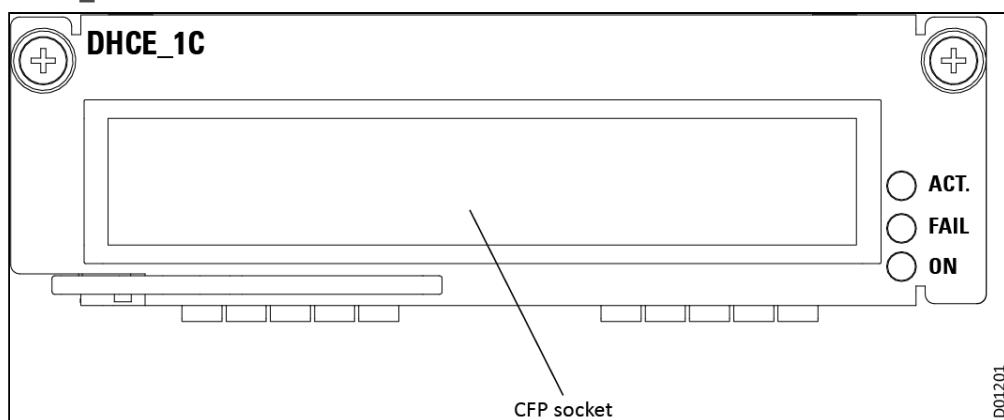
### Max DHCE\_1C Cards and Interfaces per Platform

Platform	Max. DHCE_1C Cards	Max. 100GE Interfaces	Installed into Slots
NPT-1300	4	4	TS2-TS4, TS7
NPT-1800 (with CIPS1T)	6	6	TS10-TS15 (Group II)
NPT-1800 (with CIPS2T)	12	12	TS7-TS18

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

### DHCE\_1C Front Panel



**LEDs**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHCE\_1Q Overview

**Supported Platforms**

- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with MCIPS560)
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

**Description**

The DHCE\_1Q is a 100G Ethernet multiservice interface card. It is designed with QSFP28 interfaces suited for intra-office, access, and non-amplified links up to 80km.

**Features**

- 1 x QSFP28 socket
- Supports 100GBase-SR4, CWDM4, LR4, and ER4
- Supports CL91 RS FEC
- Connected directly to the packet switch with 100G based connections

### Max DHCE\_1Q Cards and Interfaces per Platform

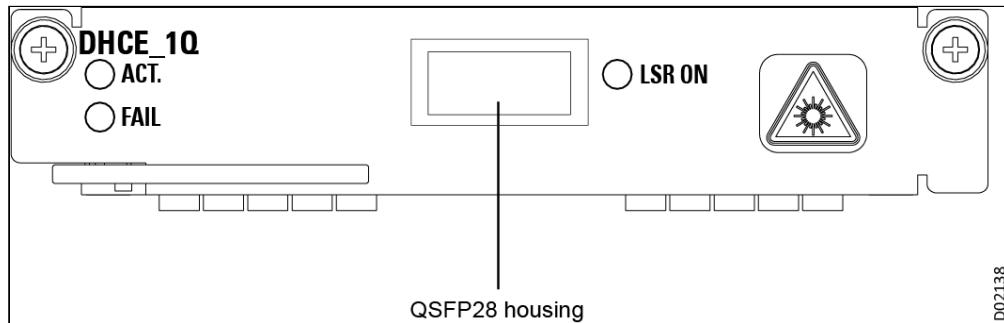
Platform	Max. DHCE_1Q cards	Max. 100GE interfaces	Installed into slots
NPT-1050 (with MCIPS300)	3	3	TS1-TS3
NPT-1100	1	1	TS1
NPT-1200 (with MCIPS560)	4	4	TS2-TS4, TS7
NPT-1250	4	4	TS1, TS4, TS7, TS8
NPT-1300	4	4	TS2-TS4, TS7
NPT-1800 (with CIPS1T)	6	6	TS10-TS15 (Group II)
NPT-1800 (with CIPS2T)	16	16	TS5-TS18, TS23-TS24
NPT-2300	7	7	TS1-TS7

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DHCE\_1Q card is directly from the front panel with a QSFP28 transceiver.

### DHCE\_1Q Front Panel



**LEDs**

<b>Marking</b>	<b>Description</b>	<b>Color</b>	<b>Function</b>
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHCE\_1QB DHCE\_1QC Overview

**Supported Platforms**

- NPT-1050 (with MCIPS300)
- NPT-1100
- NPT-1200 (with MCIPS560)
- NPT-1250
- NPT-1300
- NPT-1800
- NPT-2300

**Description**

The DHCE\_1QB and DHCE\_1QC are 100G Ethernet interface cards. These cards work with QSFP28 and QSFP-DD interfaces suited for intra office, access and non-amplified links up to 80km, as well as metro and regional amplified links. The DHCE\_1QC is an updated version of the DHCE\_1QB; the information on this page applies to both cards.

**Features**

- 1 x QSFP28/QSFP-DD socket
- Supports all QSFP28 transceivers that DHCE\_1Q supports:
  - OTR100Q28\_XX
  - OTR100Q28I\_XX
- Supports 100Gbps coherent QSFP-DD modules, supporting Open ZR+, with C-band tunable laser (OTR100Q28DD\_CZZR, OTR400Q56DD\_CZZR) or fixed wavelength (OTR100Q28DD\_C37ZR)
- Connected directly to the packet switch with 100G based connections

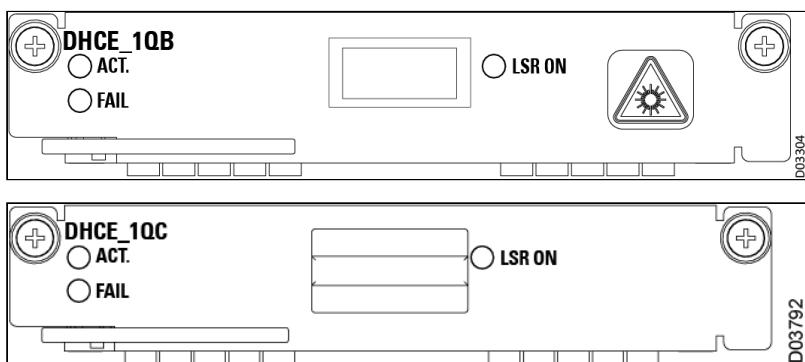
### Max DHCE\_1QB Cards and Interfaces per Platform

Platform	Max. DHCE_1QB/1QC Cards	Max. 100GE Interfaces	Installed into Slots
NPT-1050 (with MCIPS300)	3	3	TS1-TS3
NPT-1100	1	1	TS1
NPT-1200 (with MCIPS560)	4	4	TS2-TS4, TS7
NPT-1250	4	4	TS1, TS4, TS7-TS8
NPT-1300	4	4	TS2-TS4, TS7
NPT-1800 (with CIPS1T)	6	6	TS10-TS15 (Group II)
NPT-1800 (with CIPS2T)	16	16	TS5-TS18, TS23-TS24
NPT-2300	7	7	TS1-TS7

### Usage Guidelines

- When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).
- The 100G QSFP-DD coherent module has high power consumption. Therefore, the maximum ambient temperature that the Neptune platform can support is reduced when such a module is installed in the DHCE\_1QB or DHCE\_1QC card.

### DHCE\_1QB and DHCE\_1QC Cards



The cabling of the DHCE\_1QB/1QC cards is directly from the front panel.

## LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHCE\_2Q Overview

### Supported Platforms

- NPT-1300
- NPT-2300

### Description

The DHCE\_2Q is a 200G Ethernet multiservice interface card. It is designed with 2 x 200G/100G (QSFP-DD) ports on the front panel, suited for intra-office, access, and non-amplified links up to 80km, as well as metro and regional amplified links. 200G interface support is considered for future versions.

### Features

- 2 x QSFP-DD sockets, enabling each card to support:
  - 2 x 100G
  - Supports fan-out options with break-out cables (in NPT-2300 only) for lower rates of 25G/10G
  - Backward compatible with QSFP28
- Supports 100Gbps coherent QSFP-DD modules, supporting Open ZR+, with C-band tunable laser (OTR100Q28DD\_CZTR, OTR400Q56DD\_CZTR) or fixed wavelength (OTR100Q28DD\_C37ZR)
- Supports 100GBase-SR4, CWDM4, LR4, ER4, and ZR4
- Supports CL91 RS-528 FEC for 100G configuration
- Supports CL74 FC FEC, RS-528 FEC for 25g-4x, CL74 FC FEC, RS-528 FEC
- Connected directly to the packet switch with 100G based connections

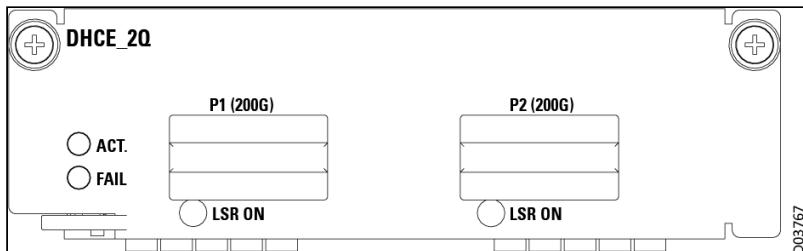
### Max DHCE\_2Q Cards and Interfaces per Platform

Platform	Max. DHCE_2Q cards	Max. 200G/100G interfaces	Installed into slots
NPT-1300	4	6 x 100G	TS2-TS4, TS7
NPT-2300	7	14 x 100G	TS1-TS7

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

### DHCE\_2Q Front Panel



The cabling of the DHCE\_2Q card is directly from the front panel with a QSFP-DD transceiver.

### LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHCE\_2 Overview

### Supported Platforms

- NPT-1300
- NPT-2300

### Description

The DHCE\_2 is a 200G Ethernet multiservice interface card with two transceiver ports.

### Features

- Transceiver ports are connected directly to the central switch with 100G based connections:
  - 1 x CFP2 socket, supporting coherent 100G OTU4 or 200G OTUC2
  - 1 x QSFP28 socket, supporting SR4, CWDM4, LR4, ER4, and ZR4
- 2 x 100GE logical interfaces can be mapped to two ODU4s and then multiplexed to OTUC2, enabling transmission of 200G capacity over a single fiber pair or single wavelength. When OTUC2 (muxponder mode) is used, the QSFP28 port is disabled. Enabling 2x100G into a single wavelength requires licensing per transceiver (OTR200P2\_CF).
- When DHCE\_2 is assigned in TS3 or TS4, only the 1st 100G port (P1) can be activated with MCIPS1T. (Such assignment is useful for future use once a higher capacity matrix is available.)
- Sync-E supported; Tx timing depends on NPU Serdes Tx clock.

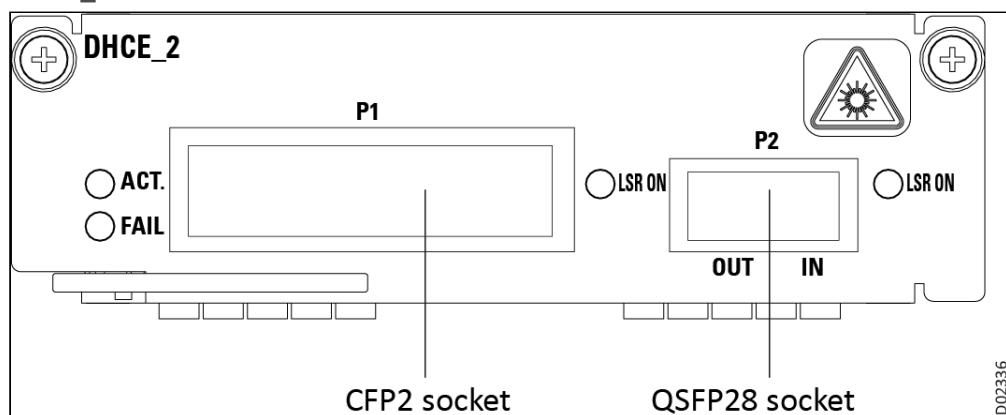
### Max DHCE\_2 Cards and Interfaces per Platform

Platform	Max. DHCE_2 Cards	Max. 100GE Interfaces	Inserted into Slots
NPT-1300	4	6	TS2-TS4 and TS7 (TS3 and TS4 support 100G only on P1 port)
NPT-2300	7	14	TS1-TS7

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

### DHCE\_2 Front Panel



The cabling of the DHCE\_2 module is directly from the front panel. The card has two housing slots for housing a CFP2 or a QSFP28 transceiver.

### LEDs

Marking	Full Name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (separate LED for each port)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DHCE\_2F Overview

### Supported Platforms

- NPT-1800 (with CIPS2T only)

### Description

The DHCE\_2F is a triple slot 200G FlexE card that supports 2 x 100 GbE FlexE combo ports (CFP2 or QSFP28), with OTGBE for OSC port.

### Features

- Transceiver ports are connected directly to the central switch with 100G based connections:
  - 2 x CFP2 sockets, supporting coherent OTU4 (future)
  - 2 x QSFP28/QSFP\_DD sockets, supporting SR4, CWDM4, LR4, ER4, and ZR4
- MCC support on FlexE shim and OSC port.
- Full FlexE support (shim, group, port, channel, and OAM), with multi-rate MAC from FlexE FPGA and Interlaken channel support.
- Timing features include:
  - PTP/SyncE support on FlexE shim
  - PTP/SyncE support on OSC port
  - Port Tx timing for SyncE (T0 only)
  - Timing reference clock
- Terminal/facility loopback

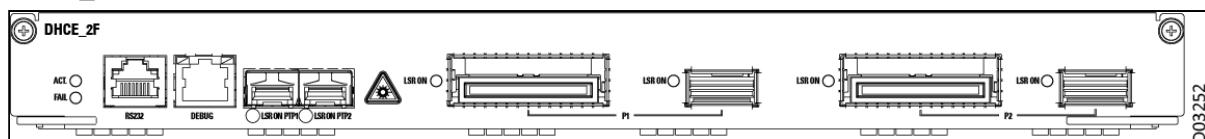
### Max DHCE\_2F Cards and Interfaces per Platform

Platform	Max. DHCE_2F Cards	Max. 100GE Interfaces	Inserted into Slots
NPT-1800 (with CIPS2T only)	4	8	TS7-TS9, TS10-TS12, TS13-TS15, TS16-TS18

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

### DHCE\_2F Front Panel



The cabling of the DHCE\_2F module is directly from the front panel. The card has two housing slots for housing a CFP2 or a QSFP28/QSFP\_DD transceiver.

## LEDs

Marking	Full name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (CFP2 port)	Laser on indication (100GE ports)	Green	Lights steadily when the corresponding CFP2 laser is on.
LSR ON (QSFP28 port)	Laser on indication (100GE ports)	Green	Lights steadily when the corresponding QSFP28 laser is on.

## DHCE\_2MRF Overview

### Supported Platforms

- NPT-1250

### Description

The DHCE\_2MRF is a 100G FlexE double-slot card that supports 1 x 100 GbE (based on QSFP28/QSFP\_DD) or 2 x 50 GbE ports (future).

### Features

Transceiver ports are connected directly to the central switch with 100G based connections (2 x QSFP28 sockets).

### Max DHCE\_2MRF Cards and Interfaces per Platform

Platform	Max. DHCE_2MRF cards	Max. 100GE interfaces	Inserted into slots
NPT-1250	2	2	TS2&TS3 and TS5&TS6

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

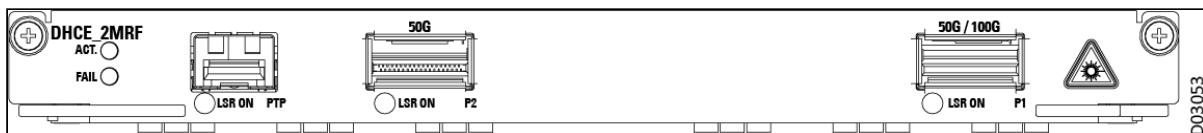
DHCE\_2MRF ports support **one 100G** interface or **two 50G** interfaces, configurable.

- If Port1 is configured as 100G interface, then Port2 is unavailable.
- Port2 can only be configured as 50G interface.  
If Port2 is enabled as 50G interface,  
then Port1 must also be configured as 50G interface as well.

The cabling of the DHCE\_2MRF module is directly from the front panel. The card has two housing slots for housing 2 x QSFP28 transceivers. P1 can also accept QSFP\_DD transceivers. In the current release only

the P1 port is operational, supporting 100G of FlexE. The card is also equipped with a GbE SFP socket for out-of-band 1588 PTP transmission (future option).

### DHCE\_2MRF Front Panel



### LEDs

Marking	Full name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (PTP)	Laser on indication (PTP port)	Green	Lights steadily when the corresponding SFP laser is on.
LSR ON (QSFP28/QSFP_DD port)	Laser on indication (100GE ports)	Green	Lights steadily when the corresponding QSFP28 laser is on.

## DH25\_4MR Overview

### Supported Platforms

- NPT-1050 (with MCIPS300 only)
- NPT-1100
- NPT-1250
- NPT-1300
- NPT-1800 (with CIPS2T only)

### Description

The DH25\_4MR is a 100G card that supports up to 4 x 10GE/25GE (based on SFP+/SFP28). The port rate is configurable per card; either all ports on a card are 10G (logical card type DHXE\_4B, SFP+ transceivers) or all ports on a card are 25G (logical card type DH25\_4, SFP28 transceivers). Multi-rate transceivers can be assigned for either 10G or 25G. OTSOP16 Smart SFP is supported in SFP+\_10GE ports. The card can support 5G timing accuracy (G.8273.2 Class C) when it is installed in NPT-1250 and NPT-1800 with CIPS2T matrix. When configured with SyncE, two recovered clocks from 4 ports can be selected as the timing source.

### Max DH25\_4MR Cards and Interfaces per Platform

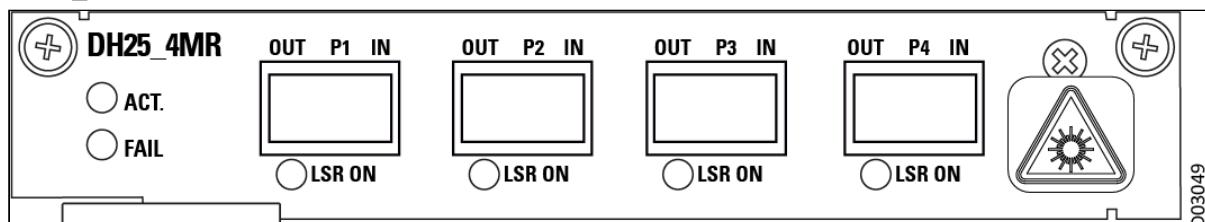
Platform	Max. DH25_4MR Cards	Max. 10/25GE Interfaces	Inserted into Slots
NPT-1050 (MCIPS300 only)	3	12/12	TS1-TS3
NPT-1100	1	4/4	TS1
NPT-1250	4	16/16	TS1, TS4, TS7, TS8
NPT-1300	4	16/16	TS2, TS3, TS4, TS7
NPT-1800 (CIPS2T only)	16	64/64	TS5-TS18, TS23-TS24

#### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DH25\_4MR module is directly from the front panel. The card has four housing slots for housing SFP+ or SFP28 transceivers.

#### DH25\_4MR Front Panel



#### LEDs

Marking	Full name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P4)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DH25\_8MR Overview

### Supported Platforms

- NPT-2300

### Description

The DH25\_8MR is a 200G card that supports up to 8 x 25G/10GE/1GE. The port rate is configurable per port. When a port is working in GE mode, only 1000Base-X or 1000Base-T can be supported. Up to two ports can be defined as timing sources at the same time.

### Max DH25\_8MR Cards and Interfaces per Platform

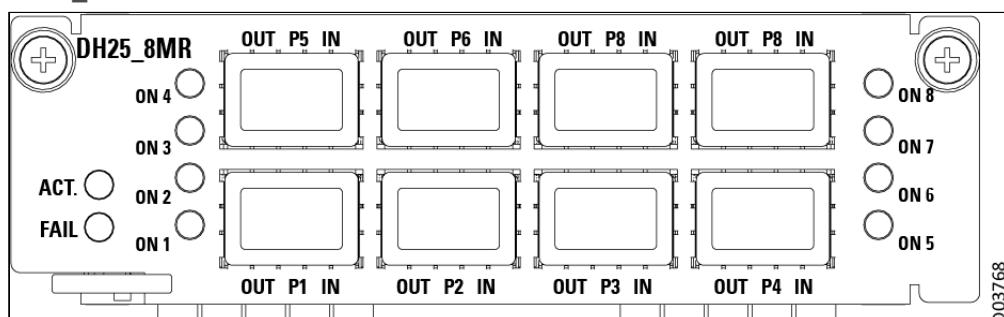
Platform	Max. DH25_8MR Cards	Max. 10/25GE Interfaces	Inserted into Slots
NPT-2300	7	56	TS1-TS7

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DH25\_8MR module is directly from the front panel. The card has eight housing slots for housing SFP+ or SFP28 transceivers.

### DH25\_8MR Front Panel



### LEDs

Marking	Full name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
LSR ON (P1 to P8)	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DH400\_1Q Overview

### Supported Platforms

- NPT-2300

### Description

The DH400\_1Q is a 400G Ethernet multiservice interface card. It is designed with QSFP-DD interfaces suited for intra-office, access, and non-amplified links up to 40km with 400G, and up to 80km for 100G, as well as metro and regional amplified links.

### Features

- 1 x QSFP-DD socket, supporting:
  - 1 x 400G, including coherent 400G ZR+ transceivers
  - Supports lower rates of 100G
  - Supports fan-out options with break-out cables for 4 x 100G
  - Backward compatible with QSFP28
- Configuration options include:
  - QSFP-DD 400G coherent for 400G Base-R over OZR (QSFP56DD, OTR400Q56DD\_CTZR) with CL119 RS-544 FEC
  - QSFP-DD 400 regular for 400G Base-R
  - QSFP28 100G coherent for 100G Base-R over OZR with CL91 RS-544 FEC
  - QSFP28 100G regular for 100G Base-R
  - Support breakout 4 x 100G (OTR400Q56DD\_DR4/LR1/PFR4) with CL91 RS-544 FEC
- Connected directly to the packet switch with 400G based connections

### Max DH400\_1Q Cards and Interfaces per Platform

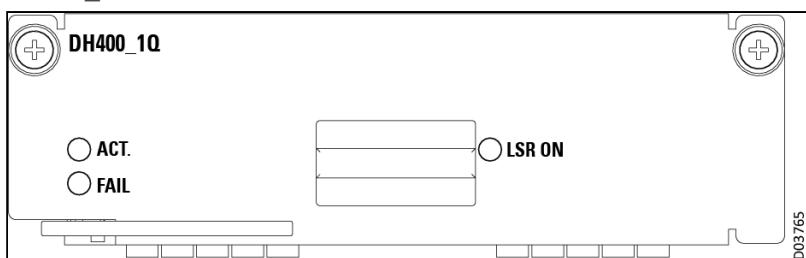
Platform	Max. DH400_1Q cards	Max. 400GE interfaces	Installed into slots
NPT-2300	2	2	TS3, TS4

### Usage Guidelines

When configuring cards in a platform, you cannot enable more than the maximum number of ports defined for that platform/card combination, no matter how many cards are physically installed in the platform; see [Card and port configuration guidelines](#).

The cabling of the DH400\_1Q card is directly from the front panel with a QSFP-DD transceiver.

### DH400\_1Q Front Panel



## LEDs

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ON	Link active	Green	Lights steadily when the corresponding port link status is UP (operational).

## Pluggable Transceiver Modules

SFP, SFP+, CSFP, CTFE, XFP, CFP, CFP-2, QSFP28, and QSFP\_DD are all varieties of modular optical transceivers with a small footprint and low power consumption.

- SFP transceivers operate at rates of up to 2.7 Gbps, with either electrical or optical ports, including both colored and noncolored interfaces (C/DWDM).
- XFP transceivers operate at rates of up to 10.7 Gbps.
- SFP+ transceivers provide 10GbE.
- CFP transceivers provide 100GbE connectivity.
- CFP-2 transceivers provide 100G/200G connectivity in a relatively small form factor.
- QSFP28/QSFP\_DD transceivers provide 100GbE connectivity in a small form factor similar in size to the legacy SFPs, enabling higher density and lower power consumption.

Neptune supports tunable transceivers for all 10/100GbE, 200G, and 400G metro service cards.

The Compact Small Form Factor Pluggable (CSFP) optical transceiver is a bidirectional single fiber optical module designed for high density platforms. This module supports a new technology which combines two single fiber duplex/ bidirectional transmissions in SFP form factor. It doubles the port density of current equipment and line cards. Moreover, The CSFP supports very low power consumption and complies with green environmental technology. The CSFP can work with bidirectional SFPs as well as regular unidirectional SFPs (with a Y-cable). CSFP transceivers are available in 2 rates:

- CTGbE for GbE interfaces
- CTFE for FX interfaces (supported as of V7.0)

The transceiver modules are used for the entire spectrum of interfaces, including intraoffice, short, and long ranges, and the interchangeable transceiver components are utilized throughout the product line. The standardized modular design of the transceiver components facilitates network maintenance and upgrades. Instead of replacing an entire circuit board, a single module can be removed or replaced, a considerable cost savings.

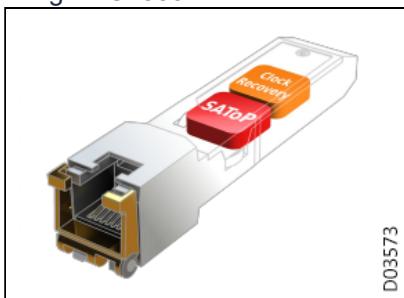
## Various Types of SFPs



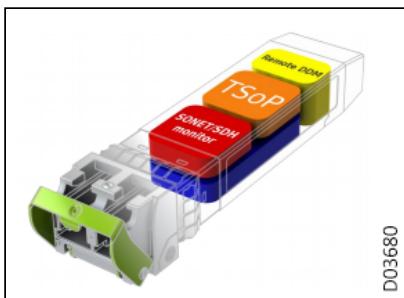
Neptune platforms also support Smart SFP transceiver solutions. Smart SFP transceivers include sophisticated functionality built in to the transceiver. Smart SFPs bring simplicity to your network. Because network functions are integrated into the transceivers, Smart SFPs can replace several devices in your network, decreasing the overall number of devices used in your network and thereby simplifying your network. A simpler network can be managed more efficiently, lowering overall power consumption and carbon footprint, and reducing your OPEX. Smart SFPs are a zero-footprint solution; simply replacing the existing transceivers lowers the CAPEX while enhancing network performance.

Neptune platforms offer a choice of [CES Transceivers](#), smart SFP transceivers that allow TDM services to be transported over Ethernet and IP/MPLS transport networks. Migrating the network from legacy TDM technology to packet has become as simple as replacing a regular transceiver with a Smart SFP. Plug a Smart SFP transceiver into your router or switch to transport TDM traffic (converted into a packet stream) across a PSN; see [Smart SFP Solutions](#).

- TPoP (Transparent PDH over Packet) Smart SFPs convert E1 or T1 (DS1) traffic to a packet stream, using RFC4553 SAToP TDM over packet pseudowire technology.



- TSOP (Transparent SDH/SONET over Packet) Smart SFPs provide a standard SFP interface and can be assigned to any 10GBE port. These transceivers support encapsulation of CESoETH and CESoMPLS.



For detailed information about the transceiver options available with Neptune platforms, please refer to the [Neptune System Specifications](#).

**Note:**

All optical modules used in Neptune systems must be certified with IEC 62368-1/EN 62368-1, IEC 60825, and CDRH registered authorized safety certifications.

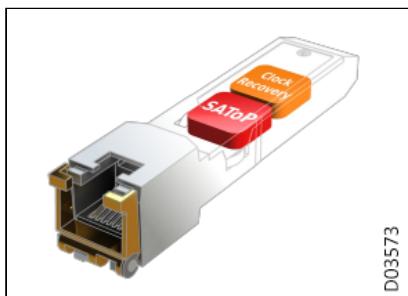
## Smart SFPs: CES Transceivers

### Description

Smart SFP transceivers allow TDM services to be transported over Ethernet and IP/MPLS transport networks. Migrating the network from legacy TDM technology to packet has become as simple as replacing a regular transceiver with a Smart SFP. Plug a Smart SFP transceiver into your router or switch to transport TDM traffic (converted into a packet stream) across a PSN.

- E1POP/T1POP

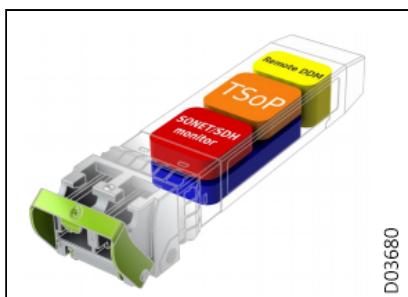
### E1POP/T1POP



- OTSOP16

The Transparent SONET/SDH over Packet (TSoP) Smart SFPs convert STM-1/OC-3, STM-4/OC-12, and OC-48/STM-16 TDM traffic to a packet stream.

### OTSOP16



**Supported Cards and Platforms**

<b>Modules</b>	<b>E1POP/T1POP in GE ports</b>	<b>OTSOP in 10GE ports</b>
<b>Cards</b> (when used in the relevant platforms)		
DHXE_2		Yes (P1, P2)
DHXE_4	Yes (P1-P4)	Yes (P1-P4)
DHXE_4sec	Yes (P1-P4)	Yes (P1-P4)
DHXE_4MR	Yes (P1-P2)	Yes (P1-P4)
DHXE_4O		Yes (P1-P4)
DHXE_8	Yes (P1-P8)	Yes (P1-P8)
DH25_4MR		Yes (P1-P4)
DHGE_8	Yes (P1-P4)	
DHGE_10	Yes (P1-P5)	
DHGE_10_POE	Yes (P1-P6)	
DHGE_16	Yes (P9-P12)	
DHGE_20	Yes (P1-P10)	
DHGE_24	Yes (P1-P12)	
<b>Platforms</b> (when used in switching cards in the platform)		
NPT-1022/B	Yes (P1-P4, P9-P20)	Yes (P1-P4)
NPT-1050, in switching cards: • MCIPS300 • AIM300	Yes (P1-P4)	Yes (P1-P4)
NPT-1100	Yes (P3-P20)	Yes (P3-P24)

Modules	E1POP/T1POP in GE ports	OTSOP in 10GE ports
NPT-1200 in switching cards: • MCIPS560 • MCIPS320		Yes (P1-P4)
NPT-1300, in switching card MCIPS1T		Yes (P1-P4)
NPT-2100	Yes (P4-P27)	

# Expansion Units

The Neptune product line includes a set of expansion units, supplemental units that provide a base NPT-XXXX platform with additional traffic and protection capabilities, enhancing scalability and providing the flexibility of additional I/O slots, available to be used as needed.

These platforms are high density modular expansion units for the Neptune's multiservice metro access platform series, supporting the complete range of CES, PCM, optics, and Ethernet services. All traffic processing, packet switching, timing and synchronization, and control and communication functions are performed by the corresponding system in the base unit. The type of traffic delivered by the unit depends on the capabilities and configuration of the base unit. I/O expansion cards are supported in accordance. Integrating this add-on platform into your network configuration is not traffic-affecting.

## Notes

- These expansion units can be combined with the many of the Neptune platforms. For easier reading, the expansion slot layout is not repeated in the sections describing each of those base platforms. The reader is simply referred back to the slot layout description in this section.
- The EXT-2U and EXT-2UH platforms share the same design principles and layout; the description here applies to both, unless noted otherwise. The main difference is that the EXT-2UH platform has a *high-speed connector enabling 10G connectivity* to the base platform, enabling a significant increase in the GbE fan out when configured with the DHGE\_10\_POE cards. A table at the end of the EXT-2U and EXT-2UH page indicates which platform combinations are available.
- The eEXT-2UH platform is similar to the other expansion platforms, except that it *does not require direct backplane connectivity* to the base platform, and therefore does not have to be installed directly above the base platform in the equipment racks.

This section introduces the following expansion units:

- [EXT-2U and EXT-2UH Expansion Units](#)
- [eEXT-2UH Expansion Unit](#)
- [Expansion Unit Common Cards](#)
- [Expansion Unit Traffic Cards](#)
- [Expansion Unit Tributary Protection Cards](#)

## EXT-2U and EXT-2UH Expansion Units

The EXT-2U and EXT-2UH platforms are high density modular expansion units for the Neptune's multiservice metro access platform series. These platforms support the complete range of CES, PCM, optics, and Ethernet services. All traffic processing, packet switching, timing and synchronization, and control and communication functions are performed by the corresponding system in the base unit on which the expansion unit is installed. The type of traffic delivered by the unit depends on the capabilities and configuration of the base unit. I/O expansion cards are supported in accordance. Integrating this add-on platform into your network configuration is not traffic-affecting.

The modules used in the EXT-2U and EXT-2UH expansion units are described in the following sections:

**Notes**

- These expansion units can be combined with the many of the Neptune platforms. For easier reading, the expansion slot layout is not repeated in the sections describing each of those base platforms. The reader is simply referred back to the slot layout description in this section.
- The EXT-2U and EXT-2UH platforms share the same design principles and layout; the description here applies to both, unless noted otherwise. The main difference is that the EXT-2UH platform has a high-speed connector enabling 10G connectivity to the base platform, enabling a significant increase in the GbE fan out when configured with the DHGE\_10\_POE cards. A table at the end of this page indicates which platform combinations are available.

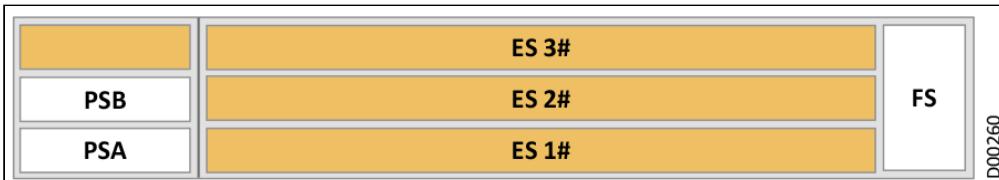
### EXT-2U Expansion Unit



The EXT-2U/2UH expansion units are housed in a 88.9 mm high, 440 mm wide, and 243 mm deep (3.5 in. x 17.32 in. x 9.57 in.) equipment cage with all interfaces accessible from the front of the unit. Each expansion unit includes its own independent power supply and fan unit, for additional reliability and security. The platform includes the following components:

- **Three multipurpose slots** (ES1 to ES3) for any combination of extractable traffic cards, including optical base cards (OBC), intelligent PCM base cards, tributary protection cards, GE/FE Ethernet cards, and CES cards. Each slot has dual connectivity to the base platform in order to support matrix card (CIPS/MCIPS) redundancy.
- **Two slots for INF power supply units.** There are two units for system redundancy.
- **One FCU fan unit** consisting of multiple separate fans to support cooling system redundancy.
- **Traffic connectivity to the base platform** is as follows:
  - **1/2.5G** connectivity per traffic slot for the EXT-2U
  - **1/2.5/10G** connectivity per traffic slot for the EXT-2UH

### EXT-2U/2UH Slot Layout



## EXT-2U and EXT-2UH Platform Compatibility

Platform	EXT-2U	EXT-2UH
NPT-1021	Yes	No
NPT-1022/B	Yes	No
NPT-1050	Yes	No
NPT-1200	Yes	No
NPT-1250	No	Yes (10G connectivity supported)
NPT-1300	Yes	Yes (10G connectivity not supported with MCIPS1T)
NPT-1800	Yes	No
NPT-2300	Yes	Yes

Typical power consumption for the EXT-2U/2UH is less than 150 W. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

### Notes

- With the NPT-1021 (10 Gbps mode), each slot in the EXT-2U has a capacity of up to 1 x GE; the total capacity of the EXT-2U is 3 x GE.
- With the NPT-1021 (60 Gbps mode), each slot in the EXT-2U has a capacity of up to 2 x GE; the total capacity of the EXT-2U is 6 x GE.

## Front-to-Back Airflow

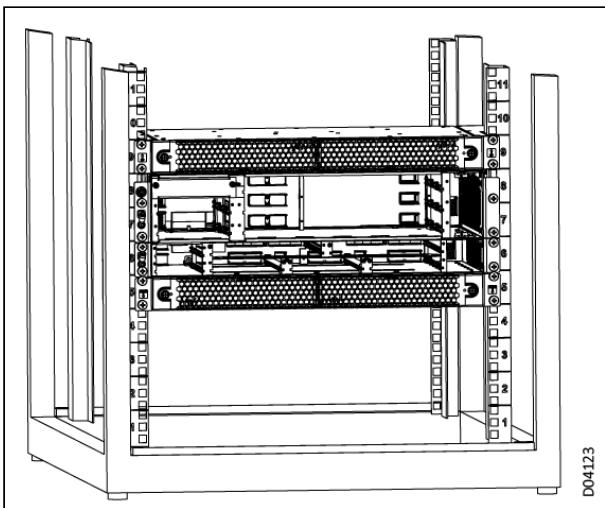
Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The EXT-2U/H expansion platform can be configured together with air baffle units, installed in either a 19" or 23" rack.

- In the 19" rack, if a platform is configured with an EXT-2U or EXT-2UH expansion unit, the expansion unit is located directly above the platform. In this configuration, the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* where the platform will be located, and one located directly *above* where the expansion unit will be located.
  - First the expansion unit is installed on the base platform.
  - Then assemble the air baffle unit (including the 2 air-flow boxes) in the 19" rack.
  - Finally, insert the combined platform and expansion unit into the gap between the upper and lower air flow boxes.

The combination of base platform and expansion unit plus 2 air-flow boxes occupies a total space of 5U or 6U, depending on the height of the base platform.

## **1U Height Platform Plus Expansion Unit Installed in 19" Rack Between Two Air-Flow Boxes**



- In the 23" rack, if the platform is configured with an EXT-2U or EXT-2UH expansion unit, then a second set of 2U air ducts is installed on either side of the EXT-2U/H expansion platform. The combination of base platform with expansion unit and 2 sets of air ducts occupies a total space of 3U or 4U, depending on the height of the base platform, since the air ducts don't add anything to the platform height.

When installing air baffle units in a 19" rack, the internal air filters in the EXT-2U/H expansion unit must be removed. External air filters are available; see the *Neptune Installation and Maintenance Manual* for details.

## Expansion Platform Cards and Slots

The following table lists the modules supported in the EXT-2U/2UH units. The specific card options available may depend on the base platform.

**EXT-2U and EXT-2UH Cards and Slots**

Card	EXT-2U slots	EXT-2UH slots
INF_E2U	PSA and PSB	PSA and PSB
AC_PS-E2U	PSA	N/A
FCU_E2U	FS	FS
EM_10E	ES#1, ES#2, ES#3	N/A
EM_10EB	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
DHFE_12	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
DHFX_12	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
DHGE_10_POE	ES#1, ES#2, ES#3 (2.5G connectivity)	ES#1, ES#2, ES#3 (10G connectivity)
DMCE1_32	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
MXP10	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
OBC	ES#1, ES#2, ES#3	N/A
OBC_B	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
TP32_2	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
TPS345_1	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3
MSC_2_16E	ES#1, ES#2, ES#3	ES#1, ES#2, ES#3

**Note**

For a table listing which extension cards can be used with which base platforms, see [Expansion Unit Traffic Cards](#).

## eEXT-2UH Expansion Unit

The eEXT-2UH platforms are high density modular expansion units for Neptune's multiservice metro access platform series. These expansion units provide a base NPT-XXXX platform with additional traffic and

protection capabilities, enhancing scalability and providing the flexibility of additional I/O slots, available to be used as needed.

The eEXT-2UH is an independent 2U platform that provides 3 I/O slots for TP cards, optical amplifiers, PCM services (with EM\_10E), and GbE fan out (with DHGE\_10\_POE). For example, adding the eEXT-2UH expansion unit to an NPT-1800 platform that is already using an EXT-2U unit would provide more slots for TP protection cards, doubling the amount of E1 protection available, which is an essential feature for large-scale aggregation sites.

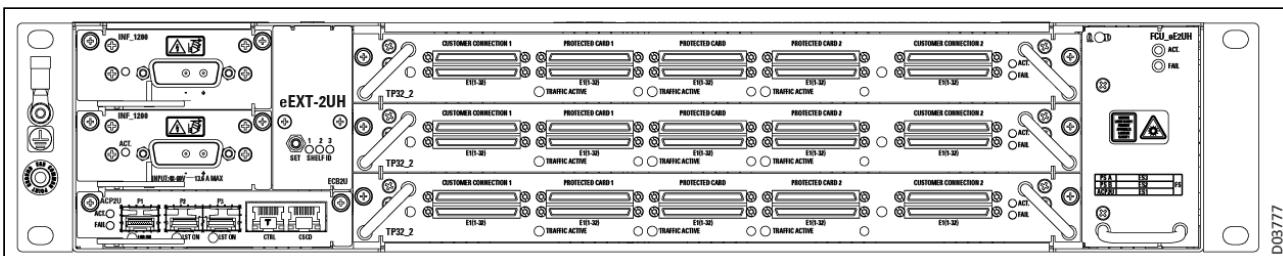
All control functionality is handled by the ACP2U card, in conjunction with the MCP unit in the corresponding base platform. Integrating this add-on platform into your network configuration is not traffic-affecting.

## Platform Layout

### Notes

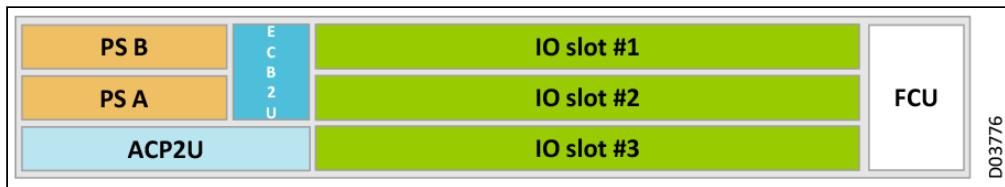
- These expansion units are used in conjunction with a base Neptune platforms. For easier reading, the expansion slot layout is not repeated in the sections describing the base platforms. The reader is simply referred back to this expansion slot layout description.
- The eEXT-2UH platform is similar to the EXT-2UH expansion platform, except that it *does not require direct backplane connectivity* to the base platform, and therefore does not have to be installed directly above the base platform in the equipment racks.

## eEXT-2UH Expansion Unit



The eEXT-2UH expansion units are housed in a 88 mm high, 440 mm wide, and 243 mm deep (3.46 in. x 17.32 in. x 9.57 in.) equipment cage with all interfaces accessible from the front of the unit. Each expansion unit includes its own independent power supply and fan unit, for additional reliability and security. The platform includes the following components:

- **Three multipurpose slots** (ES1 to ES3) for any combination of extractable traffic cards, including optical base cards (OBC\_B), tributary protection cards (TP32\_2), GbE POE cards (DHGE\_10\_POE), and PCM base cards (EM\_10E).
- **Two slots for power supply units.** There are two power supply options:
  - DC power supply (redundant)
  - AC power supply
- **One FCU fan unit** consisting of multiple separate fans to support cooling system redundancy.
- **One ACP2U control card**, works on conjunction with the MCP controller card on the base platform to manage the expansion unit.

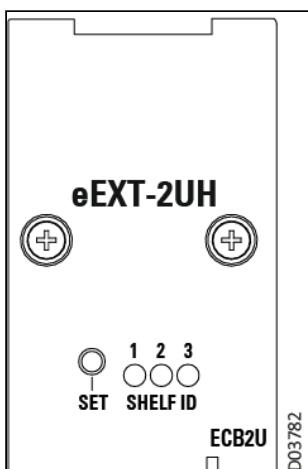
**EXT-2U/2UH Slot Layout****eEXT-2UH Platform Compatibility**

Platform	Card options
NPT-2300 with ACP1300B	OBC_B/C DHGE_10_POE EM_10EB
NPT-1800	TP32_2 OBC_B/C DHGE_10_POE EM_10EB
NPT-1250	TP32_2 OBC_B/C DHGE_10_POE EM_10EB
NPT-1050	TP32_2 OBC_B/C DHGE_10_POE EM_10EB

Typical power consumption for the eEXT-2UH is about 112 W with components installed. Power consumption is monitored through the management software. For more information about power consumption requirements, see the *Neptune Installation and Maintenance Manual* and the *Neptune System Specifications*.

Up to 3 eEXT-2UH platforms can be added to a Neptune base platform. When multiple expansion platforms are added to one base platform, the expansion platforms are uniquely identified through the platform ID LED displayed on the front panel (future).

### Shelf ID LEDs



### Platform Components

The following table lists the modules supported in the eEXT-2UH units. The specific card options available may depend on the base platform.

#### eEXT-2UH Cards and Slots

Card	eEXT-2UH Slots
INF_1200	PSA and PSB
AC_PS-1200	PSA and PSB
ACP2U	ACP
FCU_eE2UH	FS
TP32_2	ES#1, ES#2, ES#3
OBC_B/C	ES#1, ES#2, ES#3
DHGE_10_POE	ES#1, ES#2, ES#3
EM_10EB	ES#1, ES#2, ES#3

The eEXT-2UH offers two power supply modes.

- -48 VDC power feed ([INF\\_1200](#)) configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- 100-240 VAC power source ([AC\\_PS-1200](#)) utilizes an external power line connection through a power conversion module to implement AC/DC conversion.

These power modules are also used in the NPT-1200 platform; the module descriptions are provided there and not repeated in this section.

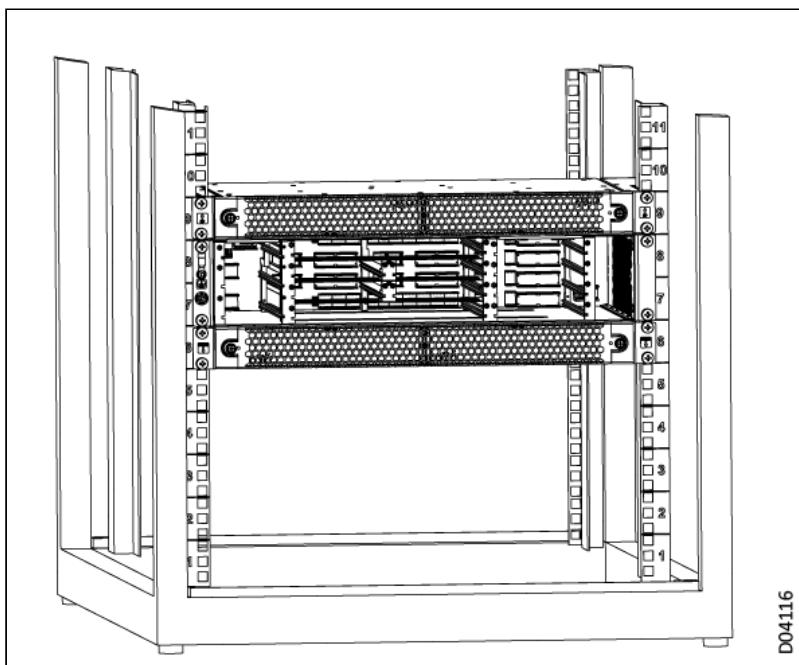
#### Front-to-Back Airflow

Neptune platforms can be installed with air baffle units that provide front-to-back airflow for cooling. The air baffle design is for server racks and other computer equipment typically used, for example, in a data center. This configuration conserves energy and lowers cooling costs by managing airflow.

The eEXT-2UH expansion unit is used together with a Neptune base platform. The 2 objects - the base platform and the expansion unit - are installed separately in the rack. The eEXT-2UH is therefore configured together with its own air baffle unit, installed in either a 19" or 23" rack.

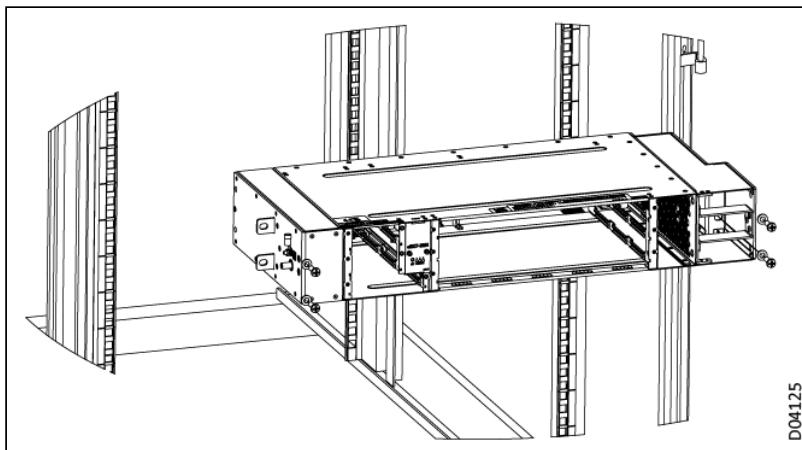
- In the 19" rack, the air baffle unit includes 2 1U air-flow boxes; one is located directly *below* the eEXT-2UH expansion unit, and one located directly *above* the eEXT-2UH expansion unit. The expansion unit and two-part air baffle unit together occupy a total space of 4U height in the rack. The air baffle unit should be installed *before* the eEXT-2UH expansion unit; the eEXT-2UH expansion unit is then inserted into the gap space between the air-flow boxes. The internal air filters in the eEXT-2UH unit must be removed. See the *Neptune Installation and Maintenance Manuals* for installation procedure details and limitations.

#### 2U Height Platform Installed in 19" Rack Between Two Air-Flow Boxes



- In the 23" rack, the air baffle unit is installed as 2 2U air ducts placed to the right and left sides of the eEXT-2UH expansion unit, requiring a total space of 2U height to be available in the rack, since the air ducts don't add anything to the platform height.

## 2U Height Platform Installed with Air Baffle Unit in 23" Rack



### Management Port Protection

Management of the traffic ports on the eEXT-2UH expansion platform (and the traffic protection provided through those ports) is dependent on the connection to the base platform through the management (MNG) port. Of course, safety mechanisms are built into the platform design, and the possibility of a double failure is very low (with both the MNG port disconnected and a TP switchover in place). Nevertheless, for greater security, the eEXT-2UH provides a mechanism for MNG 1+1 protection.

Two management interfaces are available in redundant systems. For example, when working with the NPT-1800 base platform in redundant mode, two MCP cards (MCP-A and MCP-B) are configured in the platform, each providing a management port. These two ports are in the same VLAN, with the same BC domain. They are therefore actually working in a 1+1 mode, and either management port can be used to manage the attached eEXT-2UH platform.

In a typical configuration, the MNG port on MCP-A is connected to the CTRL port of the ACP2U card in the eEXT-2UH platform, and the MNG port on MCP-B is connected to the CSCD (cascading) port of the ACP2U. This configuration can be used to provide two different protection implementation options:

- 1:1 protection optimized for a single eEXT-2UH platform.  
With this option, the ACP2U card software treats the CTRL and CSCL interfaces as a single 1:1 protection group, where the CSCD port is configured as the protection control interface.
  - If both ports are "up", the card blocks one of the ports.
  - If one port is down, the other port is unblocked and active.
- 1:1 MNG protection for one or multiple eEXT-2UH platforms (future).  
If multiple eEXT-2UH platforms are used together in a daisy-chain arrangement, the MNG port on the second MCP-B card is connected to the CSCD port on the ACP2U card in the "last" platform in the daisy-chain. This connection topology provides ring protection for the management port.
  - Only one MNG port can be operational at any time; when both MNG ports are connected, one port must be blocked to prevent an Ethernet loop.
  - To prevent a broadcast storm, the MNG port of the standby MCP card must be blocked during MCP1800 card startup as a standby. The standby card port can only be unblocked by the APS controller on the active MCP card.
  - To prevent a Layer 2 ETH loop, the user must not connect both management ports to the same L2 switch (or the same L2 BC domain).

### Management Port Usage Guidelines

- The MS-MNG connectivity between the Neptune base platforms and the eEXT-2UH expansion units must be point-to-point (P2P). The same L2 domain cannot be shared between different Neptune NEs. This means that the MS-MNG management interfaces (whether from dedicated MS-MNG ports or from a reuse of LCT ports) from different Neptune base platforms **cannot** be connected to the same LAN and then connected to the eEXT-2UH platform.

- For NPT-1050 or NPT-1250 base platforms, when the LCT interface is defined as MS-MNG to manage the eEXT-2UH platform, (the CLI command `ms-mng-if-over-lct` is **enabled**), the following usage guidelines are applicable:
  - When the base platform is configured with redundant MCIPS modules, 2 LCT ports are available for use. You can use 1 port to connect the eEXT-2UH platform, and the other port for the regular LCT/CLI interface.
  - When the base platform is configured with a single MCIPS module, the 1 LCT port available is used to connect the eEXT-2UH platform. You can use the cascading (CSCD) port on the ACP2U module for the LCT/CLI interface.
  - You are **never** allowed to connect LCT interfaces of different Neptune platforms to a LAN (L2 Switch), and then connect to a laptop/PC, when MS-MNG is enabled over LCT. The reason is that with this configuration, LCT and MS-MNG are enabled through the same port, so connecting the LCT interfaces to the L2 domain effectively connects MS-MNG to the same L2 domain, which results in a MAC/IP conflict.

## Expansion Unit Common Cards

Each expansion unit has its own power-feeding modules. One type of power module must be configured in the expansion unit for the platform to work; the expansion unit is always shipped with a power module installed. Power modules can be replaced in the field. In addition, expansion units feature a fan unit that is shipped with the platform. These modules are described in the following sections:

- [INF\\_E2U Overview](#)
- [AC\\_PS-E2U Overview](#)
- [FCU\\_E2U Overview](#)
- [FCU\\_eE2UH Overview](#)
- [ACP2U Overview](#)

The eEXT-2UH offers two power supply modes.

- 48 VDC power feed ([INF\\_1200](#)) configured in two power supply module slots for external power line connection, with a dual power feed for redundancy.
- 100-240 VAC power source ([AC\\_PS-1200](#)) utilizes an external power line connection through a power conversion module to implement AC/DC conversion.

These power modules are also used in the NPT-1200 platform; the module descriptions are provided there and not repeated in this section.

## INF\_E2U Overview

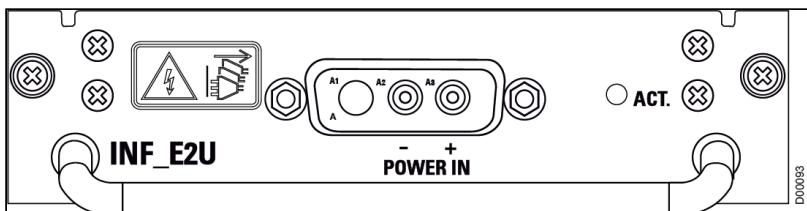
### Description

The INF\_E2U is a DC power-filter module that can be plugged into the expansion platform (EXT-2U or EXT-2UH). Two INF\_E2U modules are needed for power feeding redundancy.

### Features

- Single DC power input and power supply for all modules in the expansion platform
- Input filtering function for the entire expansion platform
- Adjustable output voltage for fans in the expansion platform
- Indication of input power loss and detection of under-/over-voltage
- Shutting down of the power supply when under-/over-voltage detected
- Supplies up to 503 W of power

### INF\_E2U Front Panel



## AC\_PS-E2U Overview

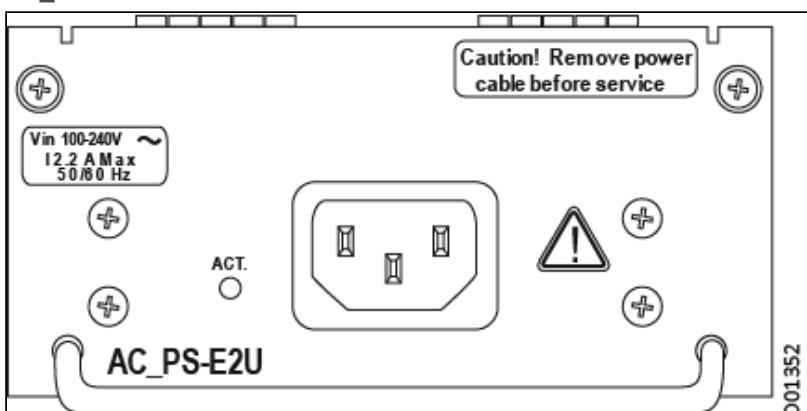
### Description

The AC\_PS-E2U is an AC power module that can be plugged into the EXT-2U platform.

### Features

- Converts AC power to DC power for the EXT-2U
- Filters input for the entire EXT-2U platform
- Supplies adjustable output voltage for fans in the EXT-2U
- Supplies up to 180 W of power, with an AC input range of 100-240 VAC

### AC\_PS-E2U Front Panel



**Note**

When using the MPoE\_12G with PoE+ functionality with AC\_PS-E2U feeding, check the power consumption calculation. Only one card of this type is allowed.

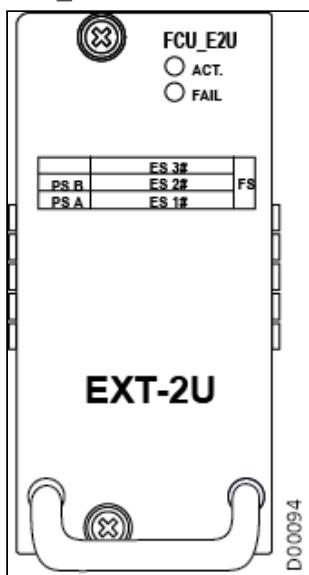
## FCU\_E2U Overview

### Description

The FCU\_E2U is a pluggable fan control module with four fans for cooling the expansion platform (EXT-2U or EXT-2UH).

### Features

- The fans' running speed can be low, medium, or turbo
- It is controlled by the MCP card in the base platform according to the environmental temperature and fan failure status

**FCU\_E2U Front Panel****FCU\_E2U Front Panel LEDs**

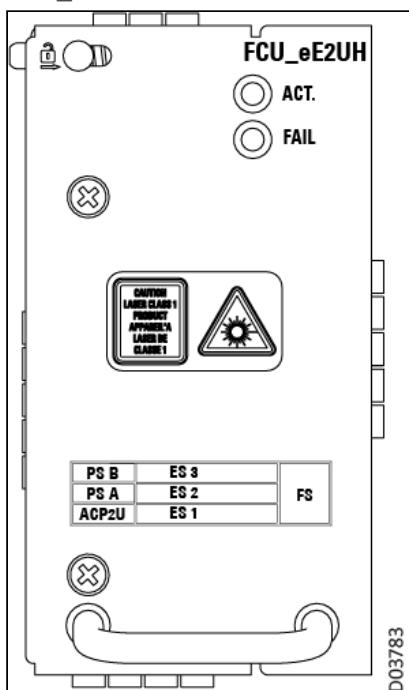
Marking	Full name	Color	Function
ACT.	System active	Green	Normally On. Off indicates the module is not running normally.
FAIL	System fail	Red	Normally off. Lights when module failure detected.

**FCU\_eE2UH Overview****Description**

The FCU\_eE2UH is a pluggable fan control module that includes eight fans for cooling the eEXT-2UH expansion platform.

**Features**

- The fans' running speed can be low, medium, or turbo
- It is controlled by the ACP2U card in the expansion platform according to the environmental temperature and fan failure status

**FCU\_eE2UH****FCU\_eE2UH Front Panel LEDs**

Marking	Full name	Color	Function
ACT.	System active	Green	Normally On. Off indicates the module is not running normally.
FAIL	System fail	Red	Normally off. Lights when module failure detected.

## ACP2U Overview

The ACP2U is the controller card for the eEXT-2UH expansion platform. The ACP2U card acts as the assistant / supporting controller card of MCP controller in the Neptune base shelf with which the expansion platform is working.

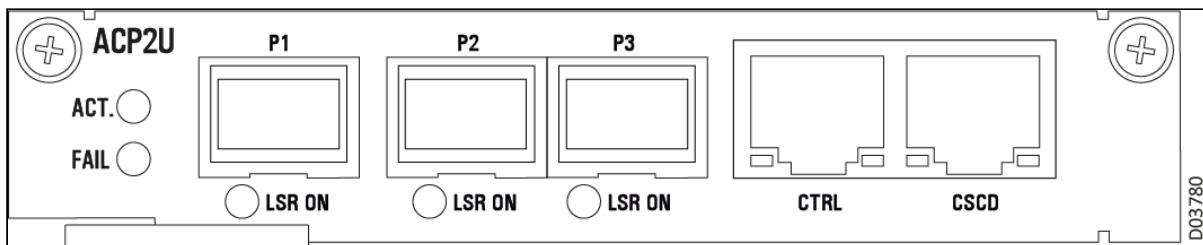
ACP2U functionality includes intra-platform and inter-platform communication:

- Internal communication with all modules in power supply slots, fan slot, and Eslots in the eEXT-2UH
- External communication with the main NE controller on the active MCP card in the base platform, through two RJ45 ports providing 10/100/1000Base-T interfaces:
  - One for the control interface uplink
  - One offering a cascading interface downlink, to connect multiple expansion platforms in a daisy-chain arrangement
  - The two ports (CTRL and CSCD) can work together in a 1:1 protection mode when connected to a base platform in redundant mode, with two controller cards. The CTRL and CSCD ports are each connected to a MNG port on one of the controller cards; see Management Port Protection in [eEXT-2UH Expansion Unit](#).

- Three SFP+ ports for 1G/10G connectivity to the base platform, with one-to-one mapping to the three I/O slots. The MCP in the base platform actually controls the slots in the eEXT-2UH platform, working through the ACP2U acting as an agent to control each slot
- Alarm indicators

All interfaces and LEDs on the ACP2U are located on the front panel of the module.

### ACP2U Front Panel



### ACP2U Front Panel Interfaces

Marking	Interface Type	Function
CTRL	RJ-45	Control interface to base platform
CSCD	RJ-45	Cascading interface to additional eEXT-2UH platform
P1/P2/P3	SFP+	1G/10G connectivity to base platform, corresponding to 3 Eslots

### ACP2U LED Indicators

Marking	Color	Function
LSR ON	Green	Lights when laser is on.
ACT.	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates card not running normally.
FAIL	Red	Normally off. Lights steadily when card failure detected. Flashing if ACP2U can't reach MCP in base platform.

## Expansion Unit Traffic Cards

The expansion platforms have three expansion slots (ES1 to ES3) to accommodate traffic cards. Expansion cards support hot insertion and can be added at any time to any installed and operational Neptune NE. The following table lists the various traffic cards that can be installed in the expansion units when configured with a Neptune base platform. The specific card options available may depend on the base platform configuration.

**Expansion Unit Traffic Cards per Platform**

Card	Description	NPT-1022	NPT-1050	NPT-1200	NPT-1250	NPT-1300	NPT-1800
Optical Base Card (OBC)	Optical amplifiers base card: <ul style="list-style-type: none"><li>• OBC can be used with EXT-2U only</li><li>• OBC_B can be used with either EXT-2U or EXT-2UH</li></ul>						
			Yes	Yes	Yes (OBC_B in EXT-2UH only)	Yes	Yes
MX P10	Muxponder card with 2 x 10G line ports and 12 client ports and a slot for installing an MO_AOC4 optical module (additional 4 client ports).						
			Yes (not with MCIPS300)	Yes (not with MCIPS320/560)			
DH FE_12	2G data card that supports 12xFE 100/1000BaseT ports on an Eslot card with internal direct connection to the packet switch.						
			Yes (not with MCIPS300)	Yes (not with MCIPS320/560)			
DH FX_12	2G data card that supports 12x10/100FX ports on an Eslot card with internal direct connection to the packet switch.						
			Yes (not with MCIPS300)	Yes (not with MCIPS320/560)			
DH GE_10_POE	10G card with up to 10 GbE ports; 4 of the ports support POE++ on an Eslot card with internal direct connection to the packet switch. <ul style="list-style-type: none"><li>• 1G/2.5G backplane connectivity with EXT-2U</li><li>• 1G/2.5G/10G backplane connectivity with EXT-2UH</li></ul>						

Card	Description	NPT-1022	NPT-1050	NPT-1200	NPT-1250	NPT-1300	NPT-1800
		Yes (EXT-2U only)	Yes (EXT-2U only)	Yes (EXT-2U with MCIPS only)	Yes (EXT-2UH only)	Yes (EXT-2U/ 2UH)	
DM CE1 _32	CES multiservice card for 32 x E1 interfaces.						
			Yes (not with MCIPS300)	Yes (not with MCIPS320/5 60)			
MS C_2 16 E	CES multiservice card for the expansion platform (EXT-2U or EXT-2UH) with 2 x STM-1/ OC-3 and 16 x E1/T1 interfaces						
		Yes (EXT-2U only)	Yes (EXT-2U only with MCIPS only)	Yes (EXT-2U with MCIPS only)	Yes (EXT-2UH only)	Yes (EXT-2U/ 2UH)	Yes (EXT-2U only)
EM _10 E / EM _10 EB	Multiservice access card that supports 64 Kbps, N x 64 Kbps PCM interfaces, and DXC1/0 functionality. <ul style="list-style-type: none"> <li>• EM_10E can be used with EXT-2U only</li> <li>• EM_10EB can be used with either EXT-2U or EXT-2UH</li> </ul>						
		Yes	Yes	Yes	Yes (EXT-2UH only)	Yes	Yes

## Optical Base Card Overview

### Supported Platforms

- OBC/OBC\_B card in EXT-2U:
  - NPT-1020
  - NPT-1022/B
  - NPT-1050
  - NPT-1200
  - NPT-1300
  - NPT-1800
- OBC\_B card in EXT-2UH:
  - NPT-1250
  - NPT-1300
- OBC\_B/C card in eEXT-2UH:

- NPT-1050
- NPT-1250
- NPT-1800
- NPT-2300 (with ACP1300B)

## Description

Neptune optical base cards (OBC, OBC\_B, and OBC\_C, referred to as OBCx) can be inserted in the Eslots of the expansion units. The OBC and OBC\_B cards can be used with the EXT-2U; the OBC\_B can also be used with the EXT-2UH, and the OBC\_B and OBC\_C cards can be used in the eEXT-2UH. Up to three OBCx cards can be installed in each expansion platform. The OBCx cards have high modularity for flexible configuration.

Each OBCx has three sub-slots: two for installing optical amplifier modules, and a smaller one for installing a DCM module. The OBCx and its modules support live insertion.

**i Note:**

The OBC\_B and OBC\_C cards are re-engineered versions of the OBC. When the OBC\_B or OBC\_C is installed in platforms running versions previous to V8.1, it is identified as OBC in the management software.

The following optical amplifier modules are available:

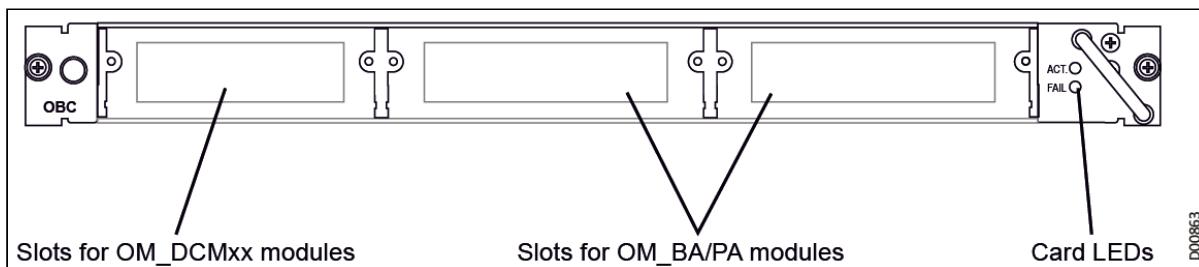
- **OM\_BA**: Single channel booster amplifier with constant output power
- **OM\_PA**: Single channel pre-amplifier with constant output power of -12 dBm
- **OM\_ILA**: DWDM amplifier in the C-band range configurable as Booster, Preamplifier, and In-line amplifier
- **OM\_DCMxx**: Micro dispersion compensation module used to correct excessive dispersion on long fibers
- **OM\_LVM**: DWDM amplifier in the C-band range for in line applications with midstage for DCF

Each of these amplifiers can be installed in any of the wider slots in the OBCx without limitations. The amplifiers support full management capabilities.

## Features

- Automatic power control (APC) based on changes in the network.  
Optical amplifiers automatically set their gain to the appropriate level as needed for network conditions such as fiber aging.

## OBC Front Panel



The smaller (left-most) slot of the OBCx supports installation of an **OM\_DCMxx** module (xx designates the dispersion compensation distance in km). The module is available for distances of 40, 80, and 100 km. The preceding figure illustrates the OBC card front panel; the OBC\_B and OBC\_C front panels are equivalent.

## LEDs

Marking	Full name	Color	Function
ACT.	Card active	Green	Normally blinks with a frequency of 0.5 Hz. Off or on steadily, indicate the card is not running normally.
FAIL	Card fail	Red	Normally off. Lights steadily when a failure is detected in the card.

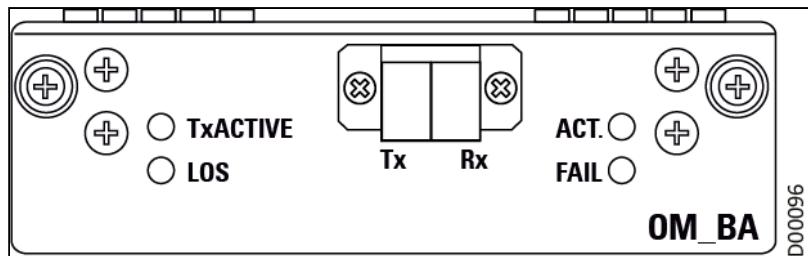
## OM\_BA Overview

### Description

The OM\_BA is a single channel booster amplifier module with constant output power.

The OM\_BA can be installed in the [Optical base card \(OBC\)](#) wide sub-slots. Up to two modules can be installed in each OBC, totaling six modules in an expansion platform.

### OM\_BA Front Panel



The module has two LC connectors: Rx (input), and Tx (output), protected by a spring-loaded cover.

## LEDs

Marking	Full Name	Color	Functions
Tx Active	Transmit active	Green	Lights when the module's output power is at a normal level.
LOS	Loss of signal	Red	Normally off. The indicator lights red when the stage input signal is missing or is too low for normal operation.
ACT.	Module active	Green	Lights when the module is powered and operating normally.
FAIL	Module fail	Red	Lights when a general fault condition is detected.

## OM\_PA Overview

### Description

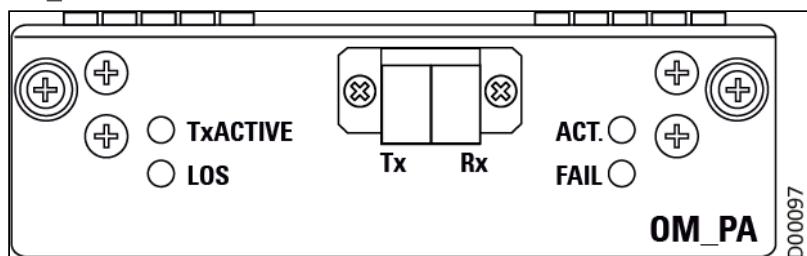
The OM\_PA is a single channel amplifier working in Channel 35 of the C-band. The amplifier works in a constant power mode and provides a power output of -12 dBm. The OM\_PA can be installed in the [Optical base card \(OBC\)](#) wide sub-slots. Up to two modules can be installed in each OBC, totaling six modules in an expansion platform.

### Features

The module can be connected in two link applications:

- Receives optical signals from an SFP/XFP transmitter and the preamplifier connected before the receiver. In this mode the module is capable of delivering signals between 80 to 120 Km.
- Includes a booster amplifier after the SFP/XFP transmitter and the preamplifier connected before the receiver. In this option the total power budget enables the amplifier to deliver signals between 120 km to 180 km.

### OM\_PA Front Panel



The module has two LC connectors: Rx (input), and Tx (output), protected by a spring-loaded cover.

### LEDs

Indicator	Functions
Tx Active	Green indicator, lights when the module's output power is at a normal level.
LOS	Loss of signal indicator, which is normally off. The indicator lights red when the stage input signal is missing or is too low for normal operation.
AC	Green indicator, lights when the card is powered and running normally.
FL	Red indicator, lights when a general fault condition is detected.

## OM\_ILA Overview

### Description

The OM\_ILA is a DWDM amplifier working in the C-band for links up to 44/88 channels.

### Features

- Fixed 21 dB gain EDFA based DWDM amplifier
- For links of up to 500 km, with up to 88 channels

- Operation as a preamplifier, booster, or inline amplifier
- Output power of 16 dBm with a gain of 21 dB
- Minimum input power of -24 dBm
- Monitoring and alarms
- Support for DWDM filters (Mux/DeMux or OADM) in a separate Artemis platform

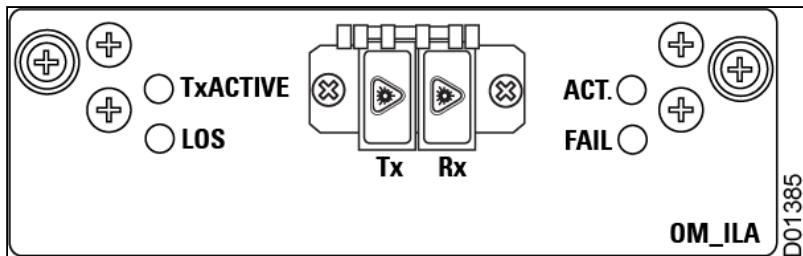
**i Note**

The module is configured by AGC in the EMS-NPT.

### Usage Guidelines

- Install in [Optical base card \(OBC\)](#) wide sub-slots
- Up to two modules can be installed in each OBC
- Maximum of six modules in an expansion platform

### OM\_ILA Front Panel



The module has two LC connectors: Rx (input), and Tx (output), protected by a spring-loaded cover.

### OM\_ILA Front Panel LED Indicators

Indicator	Functions
Tx Active	Green indicator, lights when the module's output power is at a normal level.
LOS	Loss of signal indicator, which is normally off. The indicator lights red when the stage input signal is missing or is too low for normal operation.
AC	Green indicator, lights when the card is powered and running normally.
FL	Red indicator, lights when a general fault condition is detected.

## OM\_DCMxx Overview

### Description

The OM\_DCMxx is a micro dispersion compensation module used to correct excessive dispersion on long fibers.

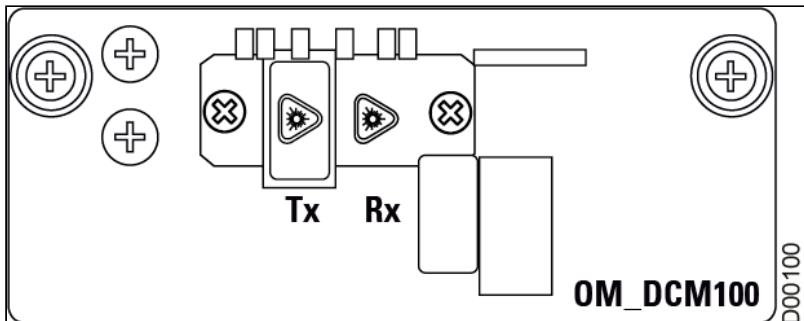
### Features

The OM\_DCMxx is available for several distance ranges: 40, 80, and 100 km (xx in the module name designates the distance in km).

### Usage Guidelines

- The OM\_DCMxx is installed in the [Optical base card \(OBC\)](#) narrow sub-slot
- One module can be installed in the OBC
- Maximum three modules in an expansion platform

### OM\_DCMxx Front Panel



The module has two LC connectors: Rx (input), and Tx (output), protected by a spring-loaded cover.

## OM\_LVM Overview

### Description

The OM\_LVM is a DWDM two stage VGA amplifier working in the C-band for links up to 44/88 DWDM channels.

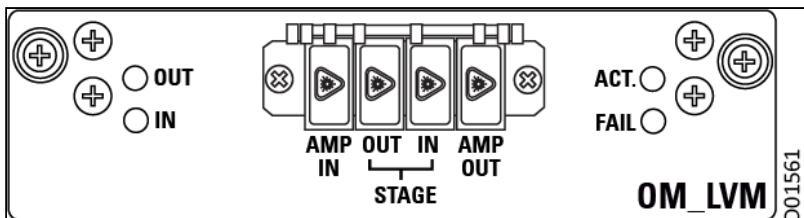
### Features

- Operates as a preamplifier, booster, or inline amplifier
- Output power of 20.5 dBm with a variable gain of 15 to 30 dB0
- Variable gain EDFA with mid-stage access (MSA)
- Minimum input power of -28 dBm
- Monitoring and alarms
- Support for DWDM filters (Mux/DeMux or OADM) in a separate Artemis platform

### Usage Guidelines

- Installed in the [optical base card](#) wide sub-slots
- Up to two modules can be installed in each OBC
- Maximum six modules in an expansion platform

### OM\_LVM Front Panel



## LEDs

Indicator	Functions
OUT	Green indicator, lights when the EDFA output power is at a normal level.
IN	Red indicator, lights when the EDFA input power is missing or is too low for normal operation.
ACT	Green indicator, lights when the card is powered and running normally.
FAIL	Red indicator, lights when a general fault condition is detected.

## Interfaces

The module has four LC connectors, protected by a spring-loaded cover:

- AMP IN - input to the first amplifier stage
- IN (STAGE) - input to the mid-stage
- OUT (STAGE) - output from the mid-stage
- AMP OUT - output from the second amplifier stage

## MXP10 Overview

### Supported Platforms

- NPT-1021
- NPT-1050
- NPT-1200

### Description

The MXP10 is a muxponder base card supporting up to 16 (CSFP) client ports, which are multiplexed into G.709 multiplexing structure and sent via two OTU-2/2e line interfaces.

The MXP10 can also be configured to operate as a transponder where it can map any 10 GE/STM-64/FC-800/FC-1200 signal into an OTU2/2e line.

The card has integrated cross-connect capabilities, providing more efficient utilization of the lambda. Any of the signals can be added or dropped at each site, while the rest of the traffic continues on to the next site. Broadcast TV services can be dropped and continued (duplicated), eliminating the need for external equipment to provide this functionality. For more information, see:

- [OM\\_AOC4 Overview](#)
- [MXP10 Applications](#)

### Features

- 12 CSFP-based client ports
- 4 additional client ports can be installed by installing an OA\_AOC4 module in the card's Tslot
- Client ports are software configurable and support GE, FC/FC2/FC4, STM-1, STM-4, STM-16, OTU-1 services or HD-SDI signal
- Two independent SFP+ based OTU-2/2e line ports
- Can be used as a multi-rate combiner up to OTU-2/2e
- Can be used as a multi OTU-1 transponder - up to 5
- Can operate as two separate muxponders with sets of eight clients multiplexed into one OTU-2 line
- Can operate as 5 separate 2.5G muxponders with up to 5 clients multiplexed into OUT-1 line

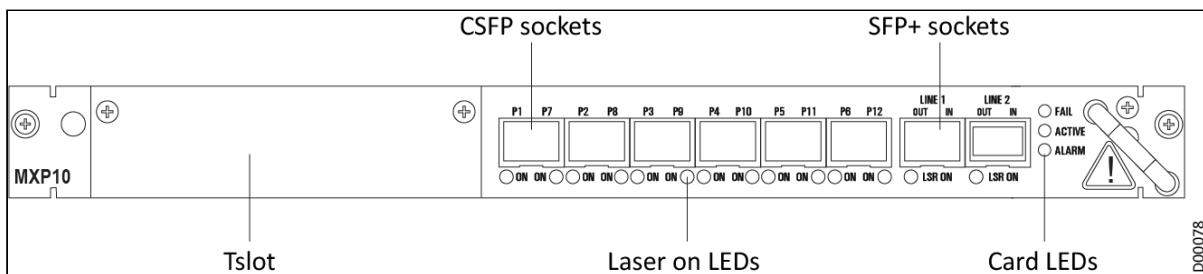
- Regeneration mode is supported for OTU-2 (single) and OUT-1 (up to 5)
- Any mix of functionality is supported as long occupied resources do not exceed MXP10 OTN capacity of 40G
- Per port HW protection
- Supports G.709 FEC for OUT-1 and G.709 FEC and EFEC (I.4 and I.7) for OTU-2 and ignore-FEC modes towards the line
- Supports Subnetwork Connection Protection (SNCP) mechanisms
- Complies with ITU-T standards for 50 GHz and 100 GHz multichannel spacing (DWDM)
- Support two GCC channels one for each OTU-2 interface, to allow management over OTN interface
- Supports in-service module insertion and removal without any effect on other active ports
- Supports interoperability with Apollo AoC cards

### Usage Guidelines

- Installed in the Eslots of expansion platforms
- Maximum of three MXP10 cards can be installed in an expansion platform

Hardware protection is supported, using a pair of MXP10 cards, configured in slots ES1 and ES2 of the expansion platform. In protection mode, each service is connected to both MXP10 cards by splitters/ couplers. In case a traffic or equipment failure occurs, it will trigger a switch to the protection card.

### MXP10 Front Panel



The cabling of the MXP10 card is directly from the front panel. It includes 6 housings for installing CSFP client transceivers; the positions are gathered in pairs: P1 and P7, P2 and P8, P3 and P9, P4 and P10, P5 and P11, and P6 and P12. Each pair can house one CSFP. Each CSFP supports two configurable ports, totaling 12 client ports on the base card. In addition, the MXP10 has two positions for installing SFP transceivers that serve the line ports.

**LEDs**

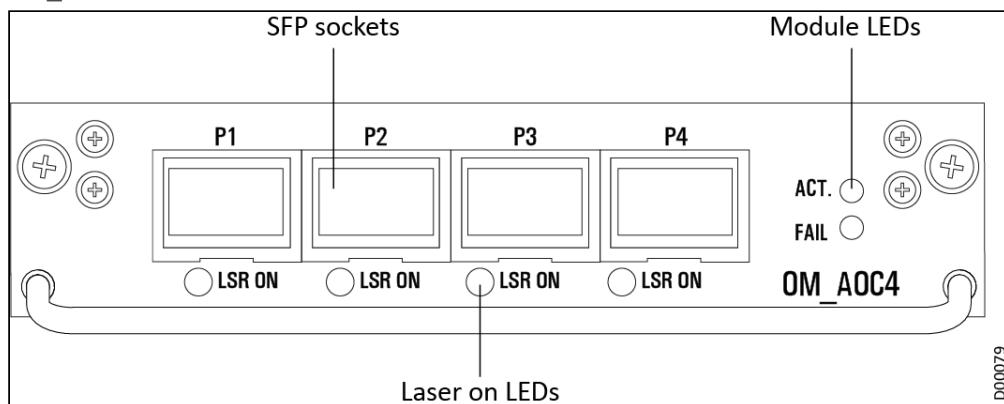
Marking	Full Name	Color	Function
ACT.	Card active	Green	Normally blinks with a frequency of 0.5 Hz. Off or on steadily, indicate the card is not running normally.
FAIL	Card fail	Red	Normally off. Lights steadily when a failure is detected in the card.
ALARM	Card alarm	Red	Normally off. Lights steadily when an alarm is detected in the card.
ON (P1 to P12)	Laser on indication (ports P1 to P12)	Green	Lights steadily when the corresponding laser is on.
LSR ON (LINE 1 and LINE 2)	Laser on indication (ports LINE 1 and LINE 2)	Green	Lights steadily when the corresponding laser is on.

**OM\_AOC4 Overview****Description**

The OM\_AOC4 is an optical ADM on a card module for insertion in the MXP10 card. It increases the MXP10 capacity with 4 client ports.

**Features**

- Each client port can be configured to operate as one of the following interfaces:
  - STM-1/STM-4/STM-16
  - GE
  - FC1/2/4/8
  - HD-SDI
  - ODU-1
- When operating in the base card, each port supports the same functionality as the client ports incorporated on the [MXP10](#).

**OM\_AOC4 Front Panel****LEDs**

Marking	Full Name	Color	Functions
ACT.	Module active	Green	Lights when the module is powered and operating normally.
FAIL	Module fail	Red	Lights when a general fault condition is detected.
LSR ON (P1 to P4)	Laser on indication (ports P1 to P4)	Green	Lights steadily when the corresponding laser is on.

## MXP10 Applications

**Applications**

- One 10 GE transponder, which can be:
  - STM64/OC192 to OTU2
  - 10 GE to OTU2e or OTU2f
  - FC-1200 to OTU2e or OTU2f
  - FC-800 to OTU2
- One 10 GE regenerator, which can be:
  - OTU2 regenerator
  - OTU2e regenerator
  - OTU2f regenerator
- Can support AoC10 applications, including:
  - Two OTU2, SFP+ based, interfaces
  - Up to 16 client interfaces with a max. capacity of 20 G, which can be:
    - STM-1/OC-3
    - STM-4/OC-12
    - STM-16/OC-48
    - OTU1
    - GE
    - FC-100/200/400
    - HDSDI1485/HDSDI3G
    - Video270
- MXP10 can support TRP25/REG25/AoC25 applications:

- Up to 5 x OTU1 transponders/combiners
- Supported client interfaces:
  - STM-1/OC-3
  - STM-4/OC-12
  - STM-16/OC-48
  - GE
  - FC-100/200
  - Video270

**Note**

The MXP10 is not supported in NPT-1800, NPT-1300, NPT-1200 with MCIPS320/MCIPS560, NPT-1050 with MCIPS300, and NPT-1022.

## DHFE\_12 Overview

### Supported Platforms

- NPT-1021
- NPT-1050 (with MCPS100 only)
- NPT-1200 (with CPS100/320 only)

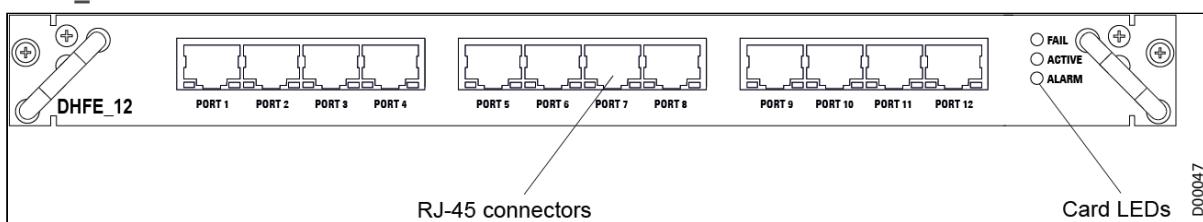
### Description

The DHFE\_12 is a data hybrid card that supports up to 12 x FE ports with connection to the packet switch.

### Usage Guidelines

- Installed in the Eslots of expansion platforms
- Maximum of three cards can be installed in an expansion platform
- When installed in an NPT-1021, can support up to 8 x FE ports
- When installed in an NPT-1021 with a CPS50 card, can support up to 12 x FE ports
- When installed in an NPT-1200 (with CPS100) or NPT-1050, the base unit max GE or 10G fan out is decreased by 16 ports, or by single 10G interface, respectively
- The FE ports of DHFE\_12 can't work at line speed; users should control traffic over FE port to be no more than 90% of total bandwidth

### DHFE\_12 Front Panel



The cabling of the DHFE\_12 module is directly from the front panel with RJ-45 based connectors.

## LEDs

Marking	Full Name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ALARM	Module alarm	Red	Normally off. Lights steadily when an alarm is detected in the card.

## DHFX\_12 Overview

### Supported Platforms

- NPT-1021
- NPT-1050 (with MCPS100 only)
- NPT-1200 (with CPS100/320 only)

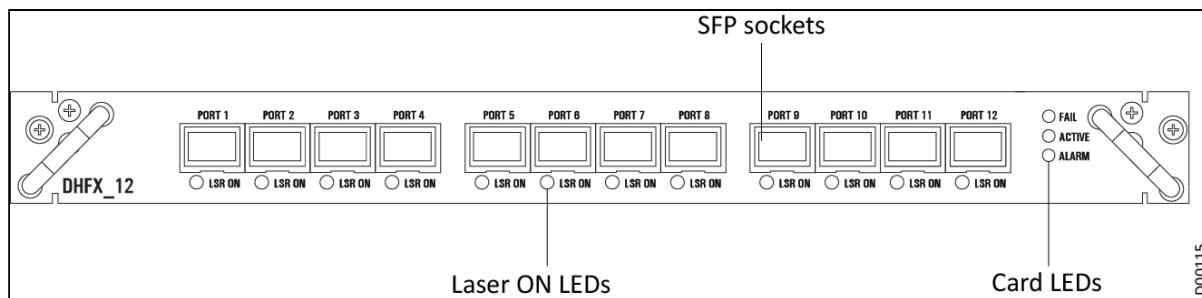
### Description

The DHFX\_12 is a data hybrid card that supports up to 12 x 100Base-FX ports with connection to the packet switch.

### Usage Guidelines

- Installed in the Eslots of expansion platforms
- Maximum of three cards can be installed in an expansion platform
- When installed in an NPT-1021, can support up to 8 x 100Base-FX ports
- When installed in an NPT-1021 with a CPS50 card, can support up to 12 x 100Base-FX ports
- When installed in an NPT-1200 (with CPS100) or NPT-1050, the base unit max GE or 10G fan out is decreased by 16 ports or by single 10G interface respectively
- The FX ports of DHFX\_12 can't work at line speed; users should control traffic over FX port to be no more than 90% of total bandwidth

### DHFX\_12 Front View



The cabling of the DHFX\_12 module is directly from the front panel with SFP sockets.

**LEDs**

Marking	Full Name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ALARM	Module alarm	Red	Normally off. Lights steadily when an alarm is detected in the card.
LSR ON (P1 to P12)	Laser on FX indication (ports)	Green	Lights steadily when the corresponding laser is on.

## DHGE\_10\_POE Overview

**Supported Platforms**

- In EXT-2U:
  - NPT-1022/B
  - NPT-1050
  - NPT-1200 (with IP switch)
  - NPT-1300
- In EXT-2UH:
  - NPT-1250
  - NPT-1300
- In eEXT-2UH:
  - NPT-1050
  - NPT-1250
  - NPT-1800
  - NPT-2300

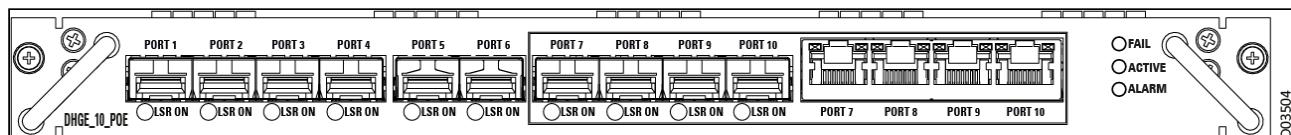
**Description**

The DHGE\_10\_POE is a data hybrid card that supports up to 10 GbE ports; 4 of the ports support POE++.

**Usage Guidelines**

- Installed in the Eslots of the expansion platforms
- Maximum of three cards can be installed in the expansion platform
- 14 physical ports are on the card. Up to 10 ports can be used as follows:
  - P1-P6: 6 x SFP (1000Base-X, 100Base-X, 1000Base-T with ETGBE, 10/100/1000Base-T with ETGBE)
  - P7-P10: 4 combo ports, configured as either:
    - RJ45 (10/100/1000Base-T) with POE functionality  
or
    - SFP (1000Base-X, 100Base-X)

### DHGE\_10\_POE Front Panel



### LEDs

Marking	Full Name	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ALARM	Module alarm	Red	Normally off. Lights steadily when an alarm is detected in the card.
LSR ON	Link active indicator	Green	Lights steadily when the corresponding port link status is UP (operational).

## DMCE1\_32 Overview

### Supported Platforms

- NPT-1021
- NPT-1050 (not with MCIPS300)
- NPT-1200 (not with MCIPS320/MCIPS560)

### Description

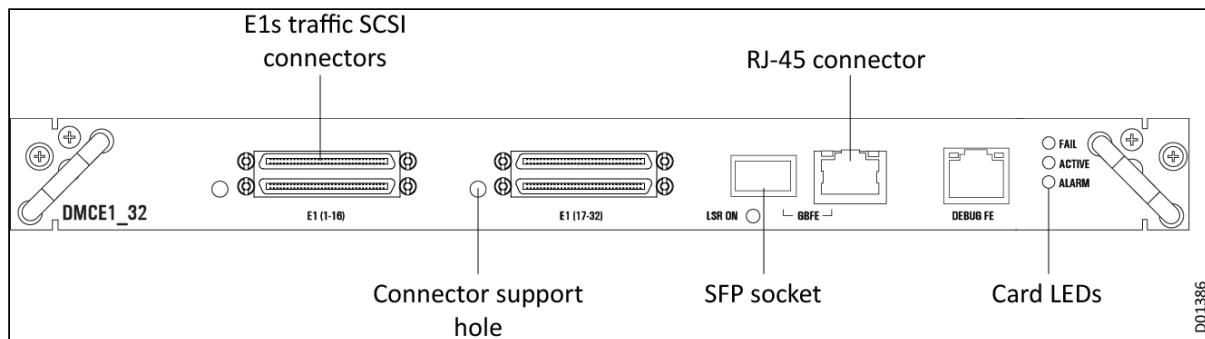
The DMCE1\_32 is a CES multiservice card that provides CES for E1 interfaces.

### Features

- 32 x E1 interfaces supported
- Physical connection towards customer E1 interfaces by 2 x SCSI 68-pin socket connector on the card front panel
- Connectivity to the packet network is made through one of the following options:
  - Direct 1.25G SGMII connection to the packet switch on CPS cards through the backplane
  - Connection to 3rd party device (router/switch) through the combo GE port on the front panel, working in standalone mode with CESoETH and CESoIP/UDP encapsulation
- SAToP and CESoPSN standards supported
- Adaptive and differential clock recovery for CES services is in accordance with ITU-T G.8261

### Usage Guidelines

- Installed in the Eslots of expansion platforms
- Maximum of three cards can be installed in an expansion platform

**DMCE1\_32 Front Panel**

Connectivity to the packet network is made through backplane connection (to the packet switch), or combo GE port on front panel.

**LEDs**

Marking	Full Name	Color	Function
FAIL	Card fail	Red	Normally off. Lights steadily when card failure is detected.
ACTIVE	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicate the card is not running normally.
ALARM	Alarm detected	Red	Normally off. Lights steadily when an alarm is detected.
GE/FE port (left LED in the RJ-45 connector)	Link and Rx/Tx	Green	Lights when the link is OK. Blinks when packets are received or transmitted.
GE/FE port (right LED in the RJ-45 connector)	Speed/laser on	Orange	Acts as speed indication when the port works in the electrical mode. Off when the speed is 10/100Mbps. Lights steadily when the speed is 1000 Mbps. Acts as laser-on indication when the port works in the optical mode Lights when the laser is on. Off when the laser is off.
LSR ON ( slot)	Laser on	Green	Lights steadily when laser is on.

**EM\_10E and EM\_10EB Overview****Supported Platforms**

- NPT-1021
- NPT-1022/B
- NPT-1050
- NPT-1200
- NPT-1250 (EXT-2UH or eEXT-2UH with EM\_10EB only)
- NPT-1300 (EXT-2U, or EXT-2UH with EM\_10EB)
- NPT-1800
- NPT-2300 (with ACP1300B, eEXT-2UH with EM\_10EB only)

### Description

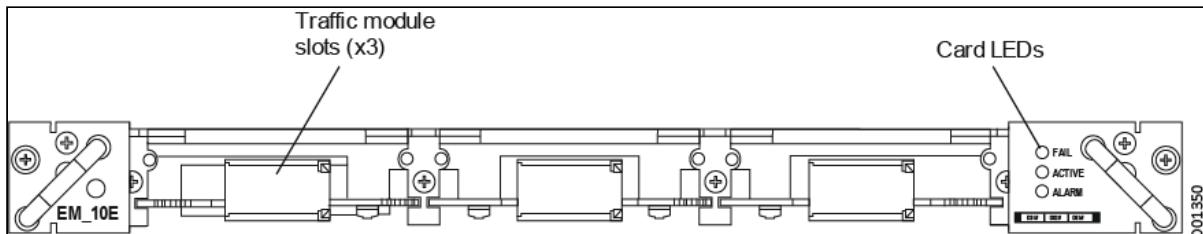
The EM\_10E/EM\_10EB are multiservice access cards that provide CES functionality for PCM services. The EM\_10E/10EB introduce various 64 Kbps, N x 64 Kbps PCM interfaces, and DXC1/0 functionality. They provide mappers for up to 16 E1s, and a DXC1/0 with a total capacity of 589 DS-0 x 589 DS-0. There are three module slots, each of which accommodates traffic bandwidth of six E1s per slot. Through the configuration of different types of traffic modules, the EM\_10E/10EB can provide up to 24 channels of different types of PCM interfaces, such as FXO, FXS, 2W, 4W, 6W, E&M, V.24, V.35, V.11, Omni, V.36, RS-422, RS-449 C37.94, and codirectional 64 Kbps interfaces. A maximum of three EM\_10E/10EB cards can be installed in one EXT-2U, EXT-2UH, or eEXT-2UH expansion platform.

The EXT-2UH supports the EM\_10EB with base platforms NPT-1250 or NPT-1300. The eEXT-2UH supports the EM\_10EB with base platforms NPT-1050, NPT-1250, NPT-1800, or NPT-2300 with ACP1300B.

**i Note:**

The EM\_10EB card was previously identified in the documentation as the EM\_10E RevF module.

### EM\_10E Front View



The EM\_10E/10EB base cards have no external interfaces. Each traffic module for the EM\_10E/10EB has its own external interfaces on its front panel.

### LEDs

Marking	Full Name	Color	Function
FAIL	Card fail	Red	Normally off. Lights steadily when card failure is detected.
ACTIVE	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily, indicate the card is not running normally.
ALARM	Alarm detected	Red	Normally off. Lights steadily when an alarm is detected.

Three traffic module slots are available in an EM\_10E/10EB card to accommodate the various types of PCM traffic modules.

The following EM\_10E/10EB/SM\_10E traffic modules are supported:

- [SM\\_FXO\\_8E Overview](#): Traffic module for eight FXO interfaces.
- [SM\\_FXS\\_8E Overview](#): Traffic module for eight FXS or FXD interfaces. Each interface can be set to FXS or FXD independently.
- [SM\\_EM\\_24W\\_6E Overview](#): Traffic module for six 24W E&M interfaces. Each interface can be set to 2W, 4W, 6W, 2WE&M, or 4WE&M independently.
- [SM\\_V24E Overview](#): Traffic module for V.24 interfaces (RS232) that supports three modes: Transparent (eight channels), Asynchronous with controls (four channels), and Synchronous with controls (two channels). Both point-to-point and point-to-multipoint services are supported.
- [SM\\_V35\\_V11 Overview](#): Traffic module for two V.35/V.11/V.24/V.36/RS-422/RS-449 (64 Kbps only) compatible interfaces with full controls. Each interface can independently be configured as V.35 or V.11/X.24 or V.24 64 Kbps.
- [SM\\_CODIR\\_4E Overview](#): Traffic module for four codirectional 64 Kbps (G.703) interfaces.
- [SM\\_IO18 Overview](#): Traffic module for 18 input/output configurable ports (dry contacts) for utilities teleprotection interfaces.
- [SM\\_C37.94S/SM\\_C37.94D](#): Traffic module for two teleprotection (IEEE C37.94) interfaces. Includes support for two SFP-based interfaces.

Each EM\_10E/10EB traffic module can be inserted into any of the three module slots in the EM\_10E/10EB. All EM\_10E/10EB traffic modules support live insertion.

EM\_10E/10EB modules support up to 16 x E1/DS1 CES services for any sub-card, supporting flexible 64k timeslot cross-connections between 16 x E1/DS1 interfaces and the timeslot in sub-card.

EM\_10E/10EB CES services support the following features:

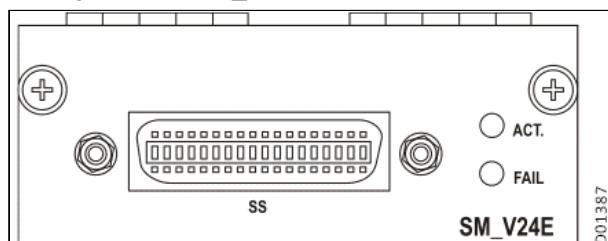
- Unframed for SAToP service, or framed for CESoPSN service
- CESoETH or CESoMPLS mode
- Configurable Tx timing mode between system timing, loop timing, and PSN timing

EM\_10E/10EB modules provide hitless switching with 1+1 transport layer protection, supporting:

- Hitless switching to any EM\_10 sub-module services
- Ensuring no packet losses during packet switching
- Equal latency for main and protection paths

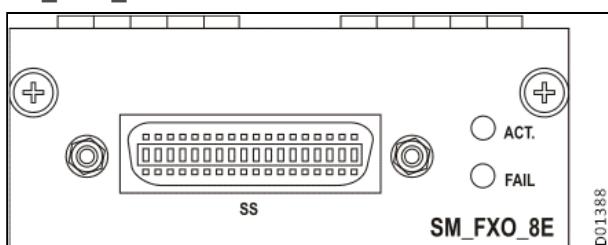
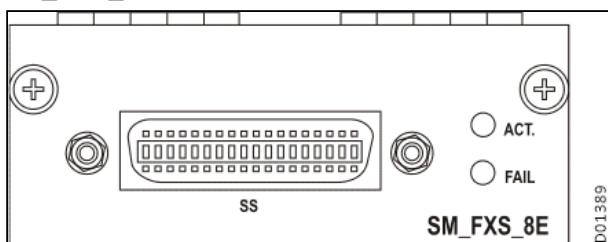
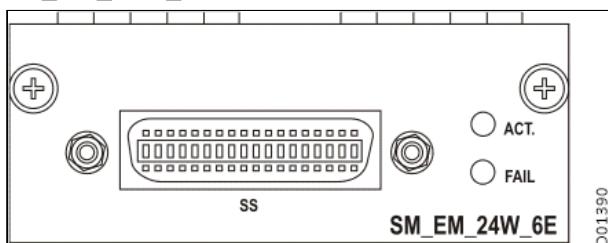
Each module provides corresponding traffic interfaces through a SCSI-36 connector on its front panel. The cabling of these interfaces can be directly via the SCSI-36 connector, or via the corresponding ICP that connects the SCSI-36 connector through a special cable.

#### Example of an EM\_10 Traffic Module



**EM\_10E/10EB/SM\_10E Traffic Module Front Panel LED Indicators**

Marking	Full Name	Color	Function
ACT	Module active	Green	Normally on. Off indicates no power supply.
FAIL	Module fail	Red	Normally off. Lights when module failure is detected.

**SM\_FXO\_8E Overview****SM\_FXO\_8E Front Panel****SM\_FXS\_8E Overview****SM\_FXS\_8E Front Panel****SM\_EM\_24W\_6E Overview****SM\_EM\_24W\_6E Front Panel**

## SM\_V24E Overview

SM\_V24E is a traffic module with V.24 interfaces (RS232) for the EM\_10E. V.24 is low bit rate data interface also known as RS232. It supports three types of the module:

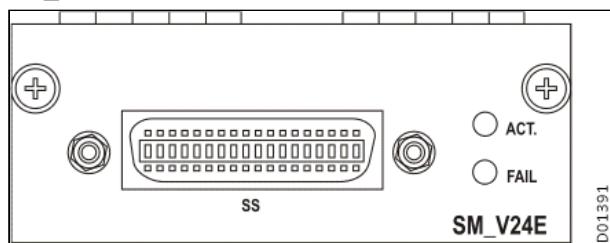
- Transparent mode with eight channels
- Asynchronous mode with controls has four channels
- Synchronous mode with controls has two channels

The SM\_V24E supports a wide range of bit rates in two grades (low and high) and three operating modes as described in the following table.

**SM\_V24E (RS232) Supported Bit Rates and Modes (V.24 attribute setting)**

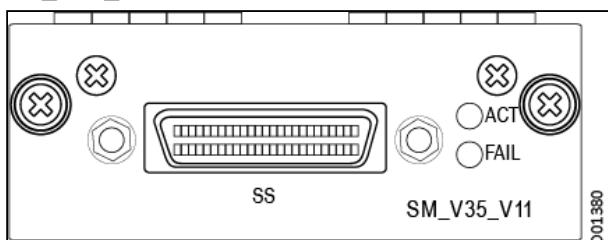
Rate Grade	Mode	TC Mode	Band Rate (bps)	Operation Mode	Rate Adaptation
	Transparent (8 channels)	Sampling	---	---	---
		TC	50-19200	---	---
Low	Async. with control	---	600-38400	Duplex	V110/HCM
	Sync with control	---	600-38400	Duplex	V110/HCM
High	Transparent (8 channels)	Sampling	---	---	---
		TC	0-19200	---	---
	Async. with control	---	57600	Duplex	HCM
	Sync with control	---	56000, 64000	Duplex	V110/HCM

**SM\_V24E Front Panel**



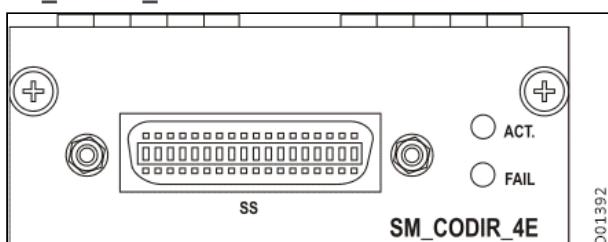
## SM\_V35\_V11 Overview

SM\_V35\_V11 Front Panel



## SM\_CODIR\_4E Overview

SM\_CODIR\_4E Front Panel

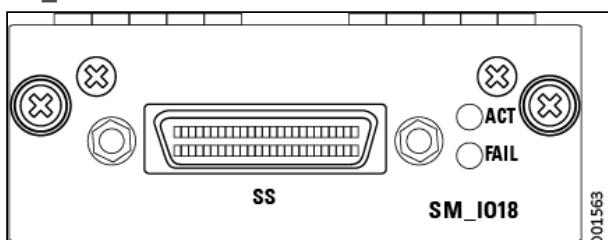


## SM\_IO18 Overview

The SM\_IO18 is a sub module of the SM\_10E/EM\_10E, which provides 18 dry contact ports and is used for substation alarm monitoring and control. Each port can be defined as input or output by configuration:

- Input port
  - Port name and severity is configurable
  - Monitor type is configurable between alarm and event
- Output
  - Support manual control
  - Support automatic control by associating an input port.

SM\_IO18 Front Panel



The main functions supported by the SM\_IO18 include:

- 18 input/output dry contact ports
- The dry contact port can be defined as input or output on per port basis
- Used for substation alarm monitoring and control

Neptune platforms' dry contact fan-out capacity has been expanded with the SM\_IO18 to support up to 162 per platform.

SM\_IO18 modules support binary input/output commands over the transmission layer in order to provide corresponding relay actions (Local to Remote). The following modes are supported:

- Single to Single
- Multiple to Single
- Multiple to Multiple

## SM\_C37.94S-SM\_C37.94D Overview

SM\_C37.94S/D sub modules provide two teleprotection interfaces per IEEE C37.94 for the EM\_10E. The interfaces enable transparent communications between different vendors' teleprotection equipment and multiplexer devices, using multimode optical fibers.

In general, teleprotection equipment is employed to control and protect different system elements in electricity distribution lines.

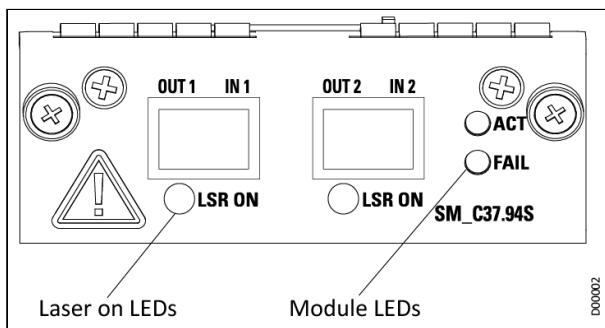
Traditionally, the interface between teleprotection equipment and multiplexers in high-voltage environments at electric utilities was copper-based. This media transfers the critical information to the network operation center. These high-speed, low-energy signal interfaces are vulnerable to intra-substation electromagnetic and frequency interference (EMI and RFI), signal ground loops, and ground potential rise, which considerably reduce the reliability of communications during electrical faults.

The optimal solution is based on optical fibers. Optical fibers don't have ground paths and are immune to noise interference, which eliminates data errors common to electrical connections.

### **i** Notes

- SM\_C37.94S supports two SFP based C37.94 interfaces (OTR2M\_MM and OTR2M\_SM, which should be ordered separately).
- The SM\_C37.94D submodule works with two C37.94D oversampling interfaces (OTR2MD) based on DC-coupling SFPs, designed for non-standard low bound rate optical interfaces.

### SM\_C37.94S Front Panel



**SM\_C37.94S/94D Front Panel LED Indicators**

Marking	Full name	Color	Function
FAIL	Module fail	Red	Normally off. Lights steadily when card failure is detected.
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicate the card is not running normally.
LSR ON	Laser on	Green	Lights steadily when the corresponding laser is on.

**MSC\_2\_16E Overview****Supported Platforms**

- In the EXT-2U:
  - NPT-1022
  - NPT-1050 (with IP switch)
  - NPT-1200 (with IP switch)
  - NPT-1300
  - NPT-1800
- In the EXT-2UH:
  - NPT-1250
  - NPT-1300
  - NPT-2300

**Description**

The MSC\_2\_16E is a CES multiservice card for the expansion platform (EXT-2U or EXT-2UH) with the following interface options:

- 2 x (STM-1/OC-3) interfaces  
*and*
- 16 x (E1/T1) interfaces

The MSC\_2\_16E can be installed in any E-slot of EXT-2U or EXT-2UH expansion platforms.

The MSC\_2\_16E supports cross-card protection between Eslot1 and Eslot2.

**Features**

- Unstructured E1/DS1 service (SAToP - RFC4553)
- Channelized E1/DS1 service (CESoPSN - RFC5086)
- Both CESoETH and CESoMPLS encapsulation
- Up to 142 E1 services or 184 DS1 services
- Both adaptive clock recovery (ACR) and differential clock recovery (DCR), with system and loop timing
- SDH/SONET Circuit Emulation over Packet (CEP) as per RFC4842, to enable VC-4/STS-1/STS-3c transparent transport over packet switched network
- CES 1+1 hitless protection
- Intra-card MSP1+1 protection for STM-1/OC-3 ports
- Cross-card MSP1+1 protection for STM-1/OC-3 ports on two MSC\_2\_16E cards located in ES1 and ES2

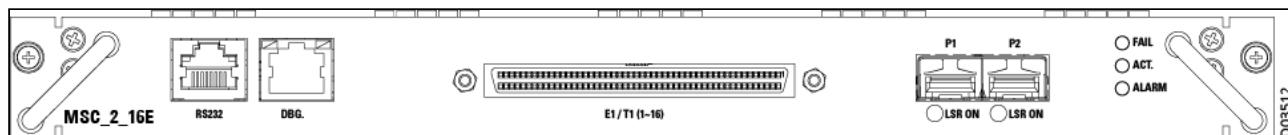
- Both unidirectional and bidirectional MSP1+1 protection between ports on MSC\_2\_16E cards (cross-card and intra-card) in NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1050, and NPT-1022 platforms
- Both revertive and non-revertive modes are supported for bidirectional MSP1+1. For unidirectional MSP1+1, only non-revertive mode supported
- Connectivity to the packet network through direct 1.25G SGMII connection to central packet switch on CPS cards through the backplane

**i Notes**

- The GbE port is not required by the supported platforms. Connection to this port is via the backplane.
- If you require this card for your Neptune V8.1 implementation, contact your customer service representative to verify availability.

#### MSC\_2\_16E Modules and STM-1/STM-4 Interfaces per Platform

Platform	Max. MSC_2_16E Modules	Max. STM-1/STM-4 Interfaces	Installed into Slots
NPT-1021	3	12/3	ES1-ES3 (EXT-2U)
NPT-1022	3	12/3	ES1-ES3 (EXT-2U)
NPT-1050 (with IP switch)	3	12/3	ES1-ES3 (EXT-2U)
NPT-1200 (with IP switch)	3	12/3	ES1-ES3 (EXT-2U)
NPT-1250	3	12/3	ES1-ES3 (EXT-2UH)
NPT-1300	3	12/3	ES1-ES3 (EXT-2U or EXT-2UH)
NPT-1800	3	12/3	ES1-ES3 (EXT-2U)
NPT-2300	3	12/3	ES1-ES3 (EXT-2UH)

**MSC\_2\_16E Front Panel****LEDs**

Marking	Description	Color	Function
ACT.	Module active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicates the card is not running normally.
FAIL	Module fail	Red	Normally off. Lights steadily when a fault is detected.
ALARM	Module alarm	Red	Normally off. Lights steadily when an alarm is detected in the card.
LSR ON (2)	Laser on indication	Green	Lights steadily when the corresponding laser is on. Separate LED for each port.

## Expansion Unit Tributary Protection Cards

Neptune platforms support Tributary Protection (TP) by protection cards, installed in the expansion platforms. This provides protection for tributary card failures, such as card power-off, card out, BIT fail, and so on.

The protection scheme can be either 1:1 or 1:2. Protection is configured by defining a Protection Group (PG), as follows:

- Protecting card: Only one tributary card can be selected as the protecting card. This card should have no existing trails. The protecting card can be located in any slot.
- Protected cards: One (1:1) or two (1:2) tributary card(s) can be selected as protected cards. A protected card can have existing trails. This means that TP can be configured for a card that is already carrying traffic, without removing existing traffic.
- Associate the protecting card and protected cards.

Neptune (IP) currently provides the following protection cards:

- [TP32\\_2 Overview](#)
- [TPS345\\_1 Overview](#)
- [TPU345\\_24\\_1xx Overview](#)

## TP32\_2 Overview

The TP32\_2, installed in the expansion platform, provides 1:1 or 1:2 protection for 32 x E1 interfaces on MSE1\_32 cards installed in the corresponding base unit (NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms). Latched relays are used to redirect the traffic connections between customer connections and internal connections, so that a redirecting cable is not required when a switch is triggered for the protected card. Warm reset is supported; traffic is not affected when the software is restarted.

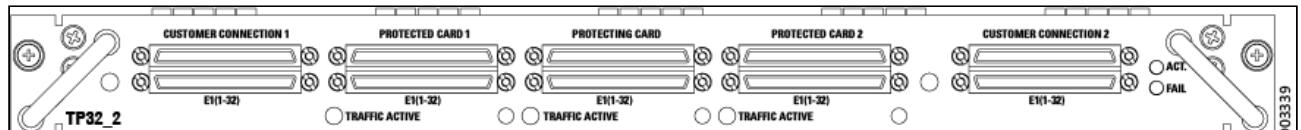
The TP32\_2 provides the following connectors on the front panel:

- **Protected Card 1:** One SCSI connector for connecting to protected MSE1\_32 card #1

- **Protected Card 2:** One SCSI connector for connecting to protected MSE1\_32 card #2
- **Protecting Card:** One SCSI connector for connecting to the protecting MSE1\_32 card
- **Customer Connection 1 and Customer Connection 2:** Two SCSI connectors for external customer E1 connections

The TP32\_2 card provides bidirectional redirection for traffic, based upon instructions from the APS controller. By default, traffic from customer connection #1 is directed to protected card #1, and traffic from customer connection #2 is directed to protected card #2. Traffic of either customer connection can be redirected to the protecting card.

### TP32\_2 Front Panel



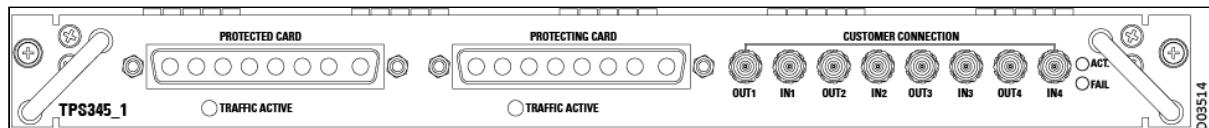
### TP32\_2 Front Panel LED Indicators

Marking	Full Name	Color	Function
ACT.	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily Indicate the card is not running normally.
FAIL	Card fail	Red	Normally off. Lights steadily when card failure is detected.
TRAFFIC ACTIVE (3)	Traffic active	Green	Lights steadily when traffic is being transferred in the corresponding module.

## TPS345\_1 Overview

The TPS345\_1, installed in the expansion platform, provides 1:1 protection for the DS3 interfaces on MS345\_3 cards installed in the corresponding base unit (NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms). Latched relays are used to redirect the traffic connections between customer connections and internal connections, so that a redirecting cable is not required when a switch is triggered for the protected card. Warm reset is supported; traffic is not affected when the software is restarted.

### TPS345\_1 Front Panel

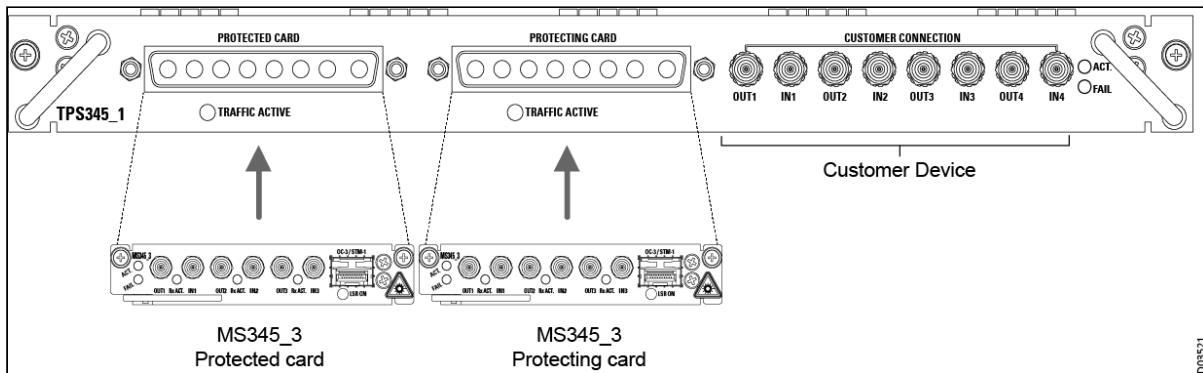


The TPS345\_1 provides the following connectors on the front panel:

- **Protected Card:** One set of DS3 connectors for connecting to protected MS345\_3 card
- **Protecting Card:** One set of DS3 connectors for connecting to the protecting MS345\_3 card
- **Customer Connection 1 through Customer Connection 4:** Four E3/DS3 connectors for external customer connections

The TPS345\_1 card provides 4 E3/DS3 interface pairs. Since protection for the MS345\_3 card only involves 3 E3/DS3 interfaces, the fourth interface pair is by default left idle, and ports 1 - 3 are used for protection. The TPS345\_1 card provides bidirectional redirection for traffic, based upon instructions from the APS controller. Card configuration for both the protected and the protecting card must match.

### TPS345\_1 Protection Mechanism



### TPS345\_1 Front Panel LED Indicators

Marking	Full Name	Color	Function
ACT.	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily Indicate the card is not running normally.
FAIL	Card fail	Red	Normally off. Lights steadily when card failure is detected.
TRAFFIC ACTIVE (2)	Traffic active	Green	Lights steadily when traffic is being transferred in the corresponding module.

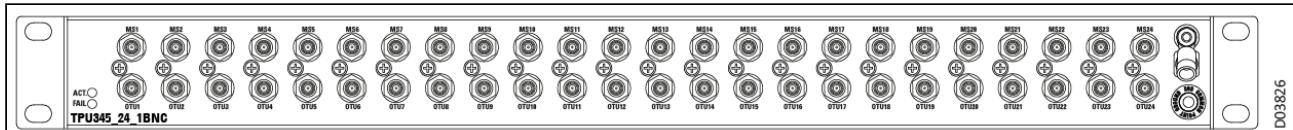
## TPU345\_24\_1xx Overview

The TPU345\_24\_1xx card, installed directly in the platform rack, works together with MS345\_24 cards installed in the corresponding base unit (NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms).

The front panel of the TPU345\_24\_1xx card has 24 pairs of coaxial E3/DS3 connectors for external customer interfaces. The TPU345\_24\_1 card is available in two versions:

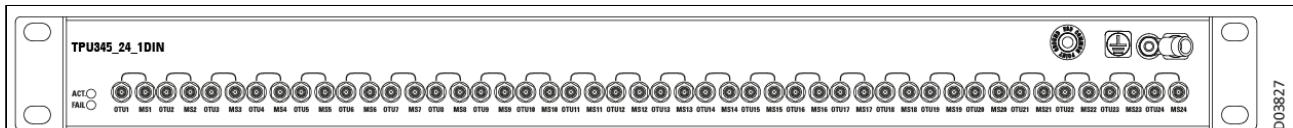
- TPU345\_24\_1BNC, usually for North American users

### TPU345\_24\_1BNC Front Panel



- TPU345\_24\_1DIN, usually for European users

### TPU345\_24\_1DIN Front Panel



Both versions of the TPU345\_24\_1xx card have 2 SCSI100 connectors on the back panel for connections to the corresponding MS345\_24 cards. The TPU345\_24\_1xx card is connected to one or two MS345\_24 cards in the base platform, through two jumper cables to the two SCSI100 ports on the back of the TPU345\_24\_1xx card, one cable to each MS345\_24 card. These connections enable the following features:

- The MS345\_24 card is very dense, with no space for the necessary transformers. Therefore, the TPU345\_24\_1xx card serves as a patch panel, providing the transformers necessary for the MS345\_24 card. The TPU345\_24\_1xx card is controlled by the MS345\_24 card.
- The TPU345\_24\_1xx card can be used to provide 1:1 protection by connecting two MS345\_24 cards to the TPU345\_24\_1xx card, configured as follows:
  - **Protected Card:** One SCSI100 connector on the back of the TPU345\_24\_1xx unit, for a cable connecting to the *protected* MS345\_24 card
  - **Protecting Card:** One SCSI100 connector on the back of the TPU345\_24\_1xx unit, for a cable connecting to the *protecting* MS345\_24 card

Card configuration for both the protected and the protecting card must match.

### TPU345\_24\_1 Card Panels



### TPU345\_24\_1xx Front Panel LED Indicators

Marking	Full Name	Color	Function
ACT.	Card active	Green	Normally blinks with the frequency of 0.5 Hz. Off or on steadily indicate the card is not running normally.
FAIL	Card fail	Red	Normally off. Lights steadily when card failure is detected.

# Neptune Slot Reassignment and Product Migration

The Neptune product line provides procedures for simplifying network maintenance and upgrade. These procedures are supported by the EMS-NPT with a user friendly GUI. This section lists some of the reassignment and replacement options available using simple migration procedures. For specific instructions, see the *EMS-NPT User Guide*.

The procedures include:

- Platform Replacement
- Card Reassignment
- Moving Cards to a Different Slot
- MAC Address Retention

## Platform Replacement

The platform replacement procedure is very important for network maintenance and upgrade. It allows the customer to migrate existing platforms to a new one with more capacity and functionalities. The Neptune product line enables platform replacement through a unified migration process.

The current version supports the following replacements:

- BG-20 to NPT-1020
- BG-30 to NPT-1200
- BG-64 to NPT-1200
- NPT-1050 with MCPS100 to NPT-1050 with MCIPS300
- NPT-1200 with CPS100/CPS320 to NPT-1200 with MCIPS320
- NPT-1200 with CPS320 to NPT-1300
- NPT-1200 with CPS100/CPS320 to NPT-1800
- NPT-1200 with CPS100/CPS320 to NPT-1200 with MCIPS560

## Card Reassignment

Card reassignment is card migration method that changes the logical card assignment in a slot with no need to reconfigure the card ports. There is no need to delete ports, interfaces, or services relevant to the card. Port mapping and configuration conversion are completed automatically from the original card type to the new card type.

A simple "edit" operation logically changes the expected equipment type within a slot to the new (and compatible) one. Unlike an "assign" or "unassign" procedure, reassignment can be completed without deleting existing traffic and configurations. All traffic is recovered automatically, as long as the actual equipment is compatible with the new equipment type after reassignment.

The following card reassessments are supported:

- CPTS100 to CPS100
- CPTS320 to CPS320
- CPS100 to CPS320
- DHXE\_2 to DHXE\_4 (in NPT-1200 with CPS320)
- CIPS1T to CIPS2T

**i Notes**

- Reassignment is based on the expected card type; it's not determined by the actual card type in the slot and its status.
- Reassignment can only be completed successfully if the new card contains all the functionality of original card, i.e., the new card type is compatible with original card type in terms of port types and quantity.
- The following DHxxx cards can be configured in the NPT-1800 platform with the CIPS1T matrix, but are not supported when the platform is configured with the CIPS2T matrix card, which does not support QSGMII interfaces.
  - DHGE\_4E
  - DHGE\_8
  - DHGE\_16
  - DHGE\_24
- CIPS1T can't be reassigned to CIPS2T if the PHY type of TS5-TS9, TS11-TS18, TS20, or TS21 in DHGE\_8S is 100Base-X and 10/100/1000Base-T.

## Moving Cards to a Different Slot

The Neptune product line supports a "move slot" operation that allows the customer to change location of a card between platform slots through the EMS system. This operation allows the customer, for example, to free slots for a double-slot card, or change a card location to facilitate cabling in the platform.

**i Note**

For help with slot or card reassignments and product replacement or upgrades, contact customer support.

## MAC Address Retention

The MAC address of all CES cards is determined by the base MAC embedded into the card hardware. If a platform is replaced, the source MAC address also changes. If the MAC address changes, then the peer MAC setting for all CESoETH services at remote sites must be updated accordingly. Of course, all these peer MAC updates can become problematic if they have to be completed manually. Therefore, Neptune offers an option to retain the base MAC of the original platform even after it is replaced, rather than requiring the MAC address to change to match the new base MAC of the new platform. The original base MAC value is programmed into the new platform through a system file that contains the original and new base MAC numbers, implemented either through a Windows-based file creation tool or through a CLI command; see [Neptune CLI User Guide](#).

# FlexE Technology

The Optical Internetworking Forum (OIF) is an industry group uniting representatives of the data and optical worlds, in an effort to accelerate deployment of interoperable, cost-effective, and robust optical internetworks and their associated technologies. OIF has developed a standardized Flexible Ethernet (FlexE) Implementation Agreement, defining a cost-effective carrier-grade interface technology. This section introduces FlexE technology, and the advantages it provides for transport networks.

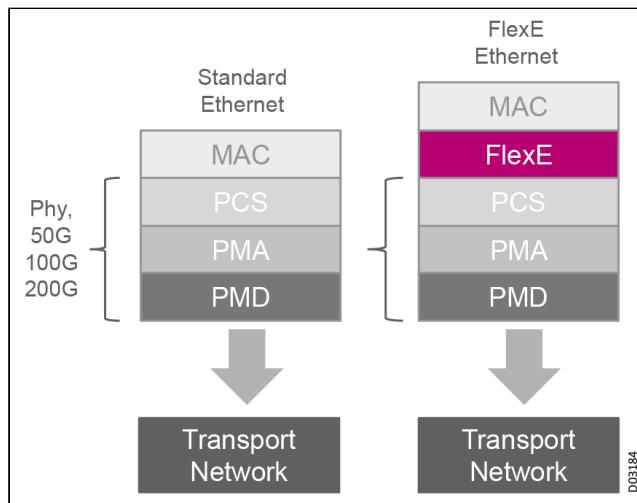
This section introduces the following FlexE concepts:

- [Understanding FlexE Technology](#)
- [FlexE Applications for Transport Networks](#)
- [FlexE Benefits](#)
- [FlexE in an IP Transport World](#)
- [FlexE Channel OAM](#)

## Understanding FlexE Technology

OIF has developed a standardized Flexible Ethernet (FlexE) Implementation Agreement, defining a cost-effective carrier-grade interface technology that provides a *generic mechanism* for supporting a variety of Ethernet MAC rates that may or may not correspond to any existing Ethernet PHY rate. This includes MAC rates that are both greater than, (through bonding), and less than, (through sub-rate and channelization), the Ethernet PHY rates used to carry FlexE. FlexE 2.1 augments FlexE 2.0 by providing support for FlexE groups composed of Mx50G Ethernet PHYs on top of the 100G, 200G, and 400G PHYs.

### Adding a FlexE Shim Layer

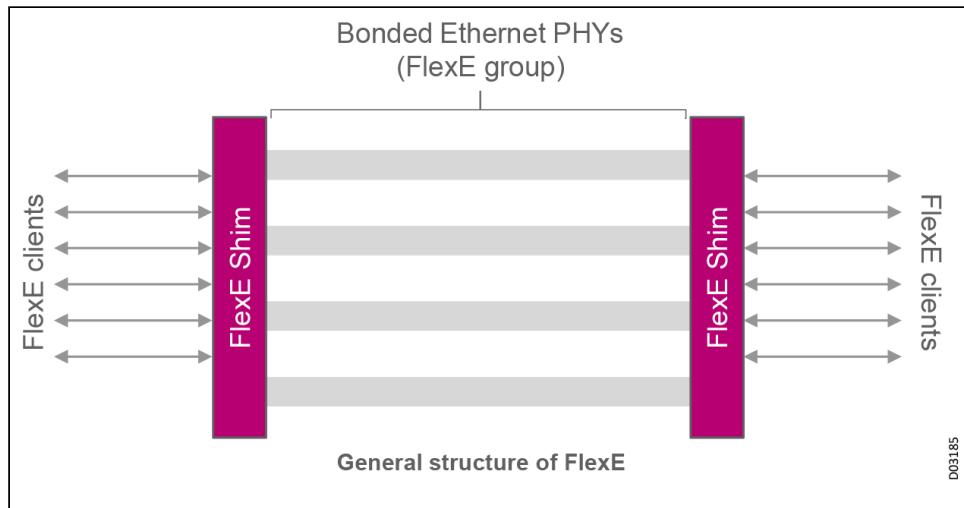


The general capabilities supported by the FlexE implementation agreement are:

- **Bonding** of Ethernet PHYs (for example, supporting a 200G MAC over two bonded 100GBASE-R PHYs)
- **Sub-rates** of Ethernet PHYs (for example, supporting a 50G MAC over a 100GBASE-R PHY)
- 5G-granularity **channelization** within a PHY or a group of bonded PHYs (for example, support a 150G and two 25G MACs over two bonded 100GBASE-R PHYs)

Note that **hybrids** are also possible. For example, a sub-rate of a group of bonded PHYs, such as a 250G MAC over three bonded 100GBASE-R PHYs.

## Hybrid FlexE Implementation



The FlexE design is based on a client/group architecture, in which multiple FlexE clients can be mapped to a single FlexE transmission group for bonding, channelization, sub-rating, and other functions.

A **FlexE group** (bundle) consists of from 1 to m bonded Ethernet PHYs. FlexE groups may consist of 50GBASE-R PHYs, 100GBASE-R PHYs, 200GBASE-R PHYs, or 400GBASE-R PHYs. All PHYs within a single group must operate at the same rate, as illustrated in the following figure.

## FlexE Use Case



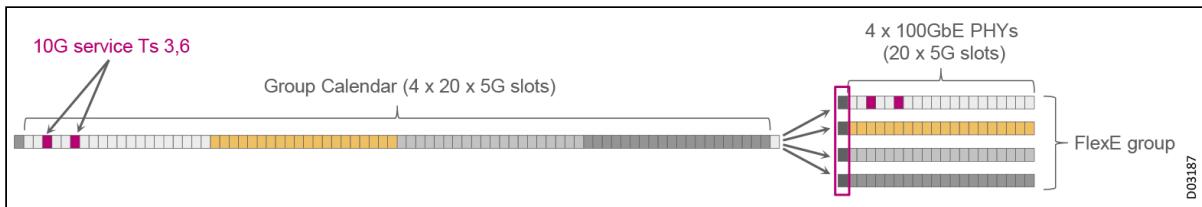
To understand the FlexE architecture, we introduce the following terms:

- A **FlexE instance** is a unit of information carried across each PHY of the FlexE group. A FlexE instance is configured with either 50G or 100G of capacity, able to carry FlexE client data, together with its associated overhead. A 50G FlexE instance is only carried over a 50GBASE-R PHY. A 100GBASE-R PHY carries a single 100G FlexE instance. A 200GBASE-R PHY carries two 100G FlexE instances, and a 400GBASE-R PHY carries four 100G FlexE instances.
- A **FlexE client** is an Ethernet flow based on a MAC data rate that may or may not correspond to any Ethernet PHY rate. The FlexE client represents the aggregated capacity to which we can map the service. The FlexE client MAC rates supported by FlexE groups are mapped to Nx5G rates.
- The **FlexE shim** is the layer that maps or demaps the FlexE clients carried over a FlexE group. The FlexE mux refers to the transmit direction, which maps FlexE clients over the FlexE group. The FlexE DeMux refers to the receive direction, which demaps the FlexE clients from the FlexE group.

The FlexE shim layer is the key to FlexE implementation. Each FlexE client is presented to the FlexE shim as a 64B/66B encoded bit-stream [according to 802.3]. Details of how to create the bit stream are application-specific, but the end result should appear to the FlexE shim as having been created from an Ethernet MAC operating at a rate of 10, 40, or Mx25G (or a subset of these rates, such as Mx25G).

The shim layer partitions each 100G PHY in a FlexE into a group, called a **sub-calendar**, of 20-slot data channels, providing 5G bandwidth per slot. The **FlexE slot** defines the granularity to which we can map the service. Ethernet frames of FlexE clients are partitioned into 64B/66B blocks, which are distributed to multiple PHYs of a FlexE group, based on slots through the FlexE shim layer. The **group calendar** is the overall TDM bitstream that is used as the server to carry FlexE clients. The following figure illustrates how a 10G service is mapped to a FlexE client which is composed of 2x5G sub-calendar slots, in a 400G group calendar that is mapped into a 4x100G FlexE group.

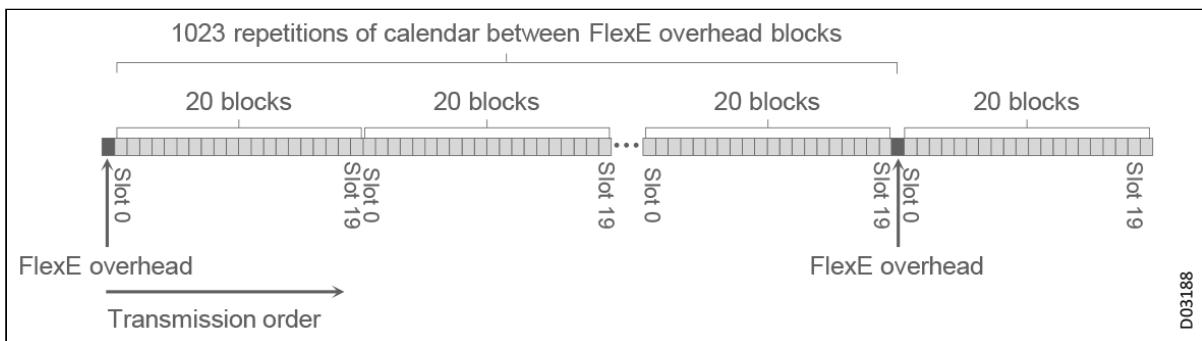
## Group Calendar Carrying FlexE Clients



The FlexE port is the actual PHY which is used as the network port, following IEEE standards (50G, 100G, 200G, 400G, or any other future IEEE rate).

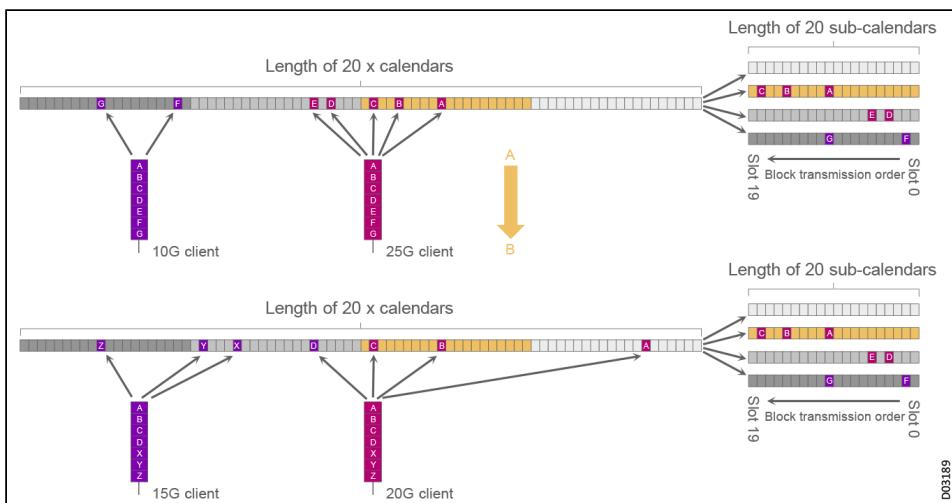
A FlexE client can theoretically support multiple rates through different combinations of these 5G slots. The calendar mechanism enables the FlexE shim to map and carry multiple FlexE clients with different rates within a FlexE group, allocating bandwidth as needed to these clients, by mapping each client to one or more slots.

## Logical Calendar Units of 20 Blocks Each



FlexE provides dynamic bandwidth adjustment for clients by allowing modification of the slot/calendar configurations. This is done by maintaining two types of calendar configurations (A and B configurations). These calendar configurations can be switched dynamically to adjust bandwidth and FlexE client slot allocation.

## Dynamic Calendar Switching

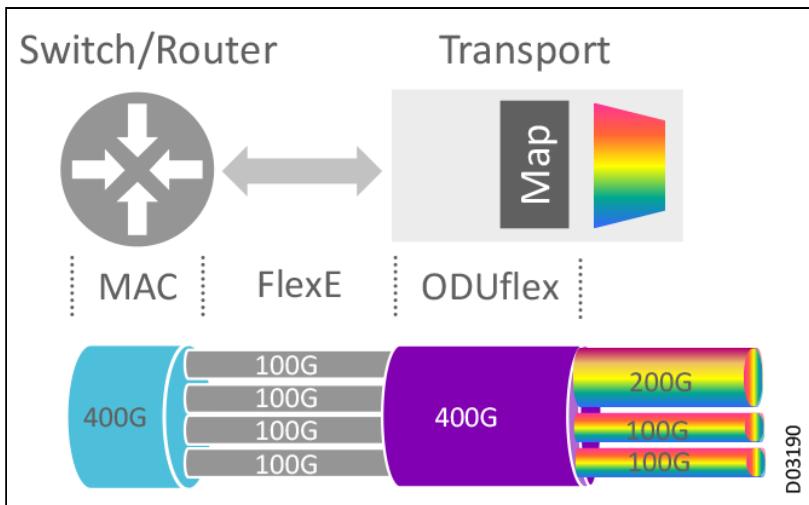


## FlexE Applications for Transport Networks

FlexE offers advantages for transport networking, whether or not the network itself is explicitly working with FlexE. This is a critical point when working with existing/brownfield networks that must continue to utilize their current infrastructure, but are in various stages of preparation for the transition to 5G technology. This can be seen in three different scenarios.

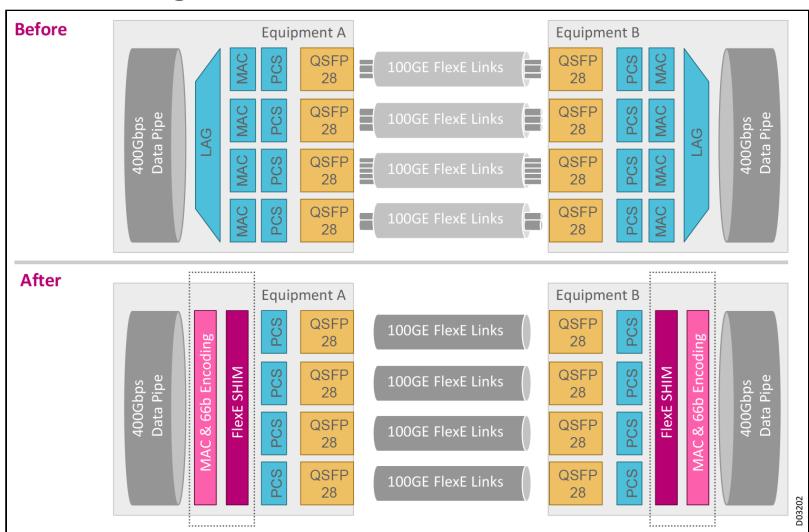
### FlexE Unaware

#### FlexE

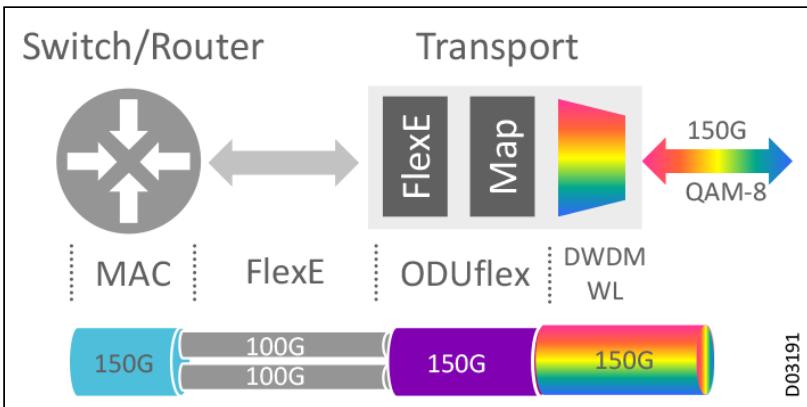
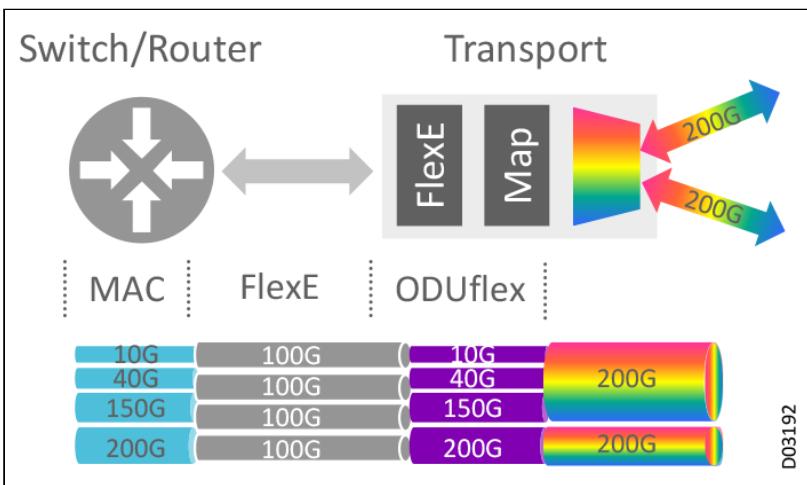


FlexE bonding is a more efficient alternative to LAG or ECMP implementations, that are inefficient due to the necessary hashing algorithms. As illustrated by the following figure, efficient bonding means that the bandwidth of each link is utilized completely.

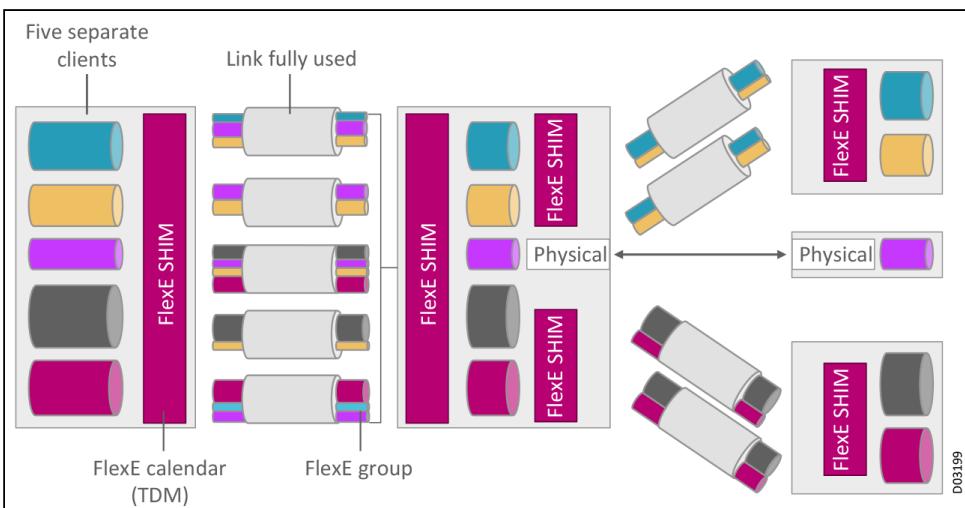
### FlexE Bonding



### FlexE Aware

**FlexE Aware****FlexE Full Termination****FlexE Full Termination**

Channelization is a much more efficient alternative for traffic segregation compared to the capabilities offered by VPNs, VLANs, or LSPs. As illustrated by the following figure, efficient channelization means that the links are fully utilized, because the clients are organized into the most efficient groupings possible.

**Channelization**

## FlexE Benefits

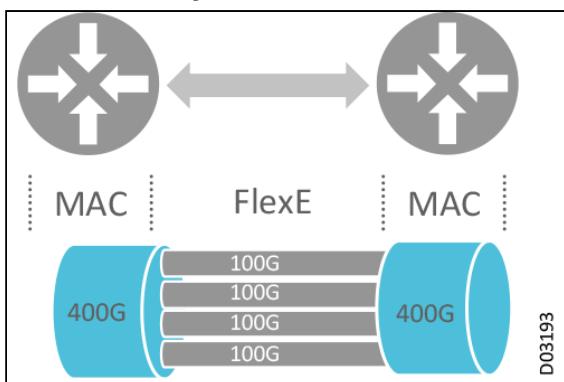
FlexE technology offers more than just efficient bandwidth usage. The technology provides additional benefits for many different transport network components.

### DC Connectivity

FlexE offers advantages for router-to-router DC connectivity, including:

- Fast introduction of new rates
- Improved LAG performance
- Interface readability, enabling the interface to keep working after a line failure
- Flexible multi-link gearbox (MLG)

### DC Connectivity

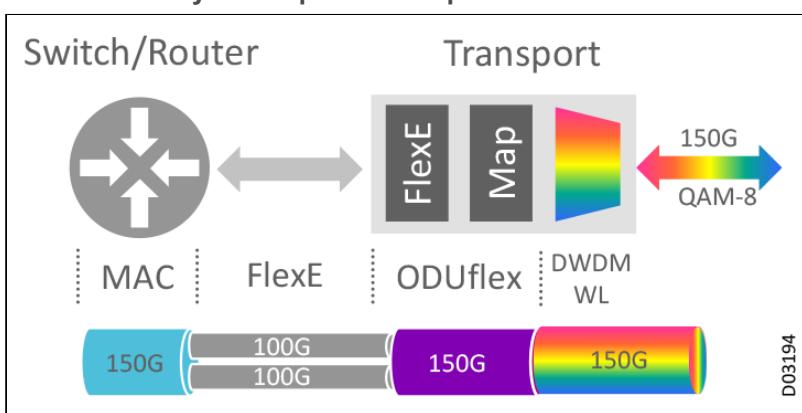


### DC Connectivity over Optical Transport

FlexE offers advantages for router-to-transport DCI connectivity, including:

- Matching transport bandwidth rates - 150G, 300G, and higher rates in the future
- Enable per wavelength, for greater performance optimization
- Interface readability, enabling the interface to keep working after a lane failure
- Channelized hand-off from router to transport

### DC Connectivity over Optical Transport

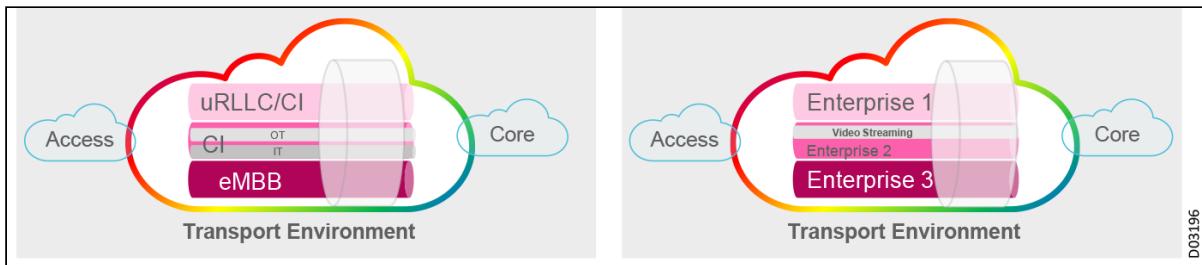


### Traffic Isolation with Guaranteed Capacity

FlexE architecture provides service providers with the ability to segregate each FlexE port in the network into several FlexE clients. Each FlexE client will have its own guaranteed BW totally isolated from the other FlexE clients that are mapped to different FlexE slots in the TDM bit stream calendar, ensuring they are

independent on the forwarding plane. This method is much easier to implement than applying sophisticated traffic engineering techniques.

### Traffic Isolation

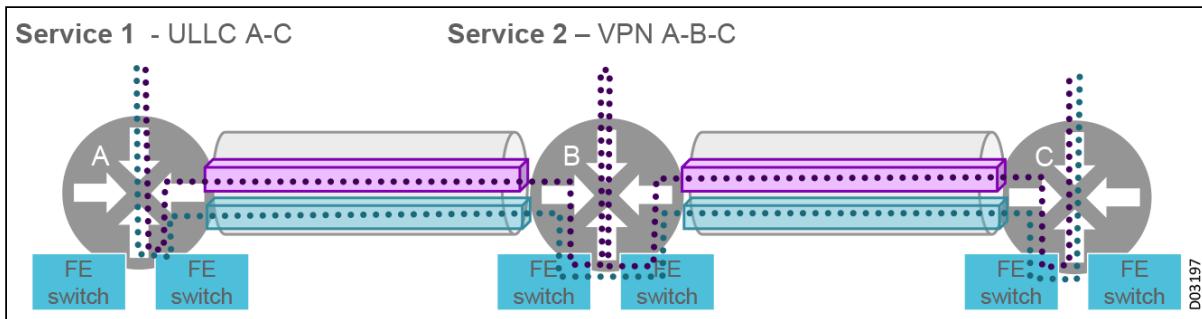


### Low Latency

FlexE uses a mapping approach, mapping traffic into the bitstream calendar, based on TDM, instead of being based on packet classification and packet processing into packet buffers and queues. FlexE offers a simple, efficient design that reduces pass-through latency in a FlexE cross-connect operation to the minimum.

These latency values are an obvious advantage, especially when compared to values of a few tens of  $\mu$ s for traffic flow with OTN networks, and even in packet devices, especially during periods of congestion or burst traffic. In any given scenario, FlexE channels provides a deterministic latency that is near the minimum needed to deliver the bandwidth.

### Reducing Pass-through Latency



## FlexE in an IP Transport World

OIF has accomplished a great deal with FlexE. A consortium of companies, all working together for everyone's benefit, has hammered out an excellent technology, flexible, robust, offering many advantages for NG networks.

- Working with efficient, flexible size Ethernet instead of LAG functionality, with innate hashing inefficiencies and network state explosion. [LAG is considered about 80% efficient.]
- FlexE offers the ability to use 50/100/200/400GE PMDs (or any future PMDs) without requiring development of new IEEE standards for new Ethernet rates. This allows operators to decouple PMD development from the other network layers.
- FlexE enables a better match between actual router rates with transport rates (150G, 250G, etc.).
- Network slicing with services segregation, guaranteed BW, and low latency.

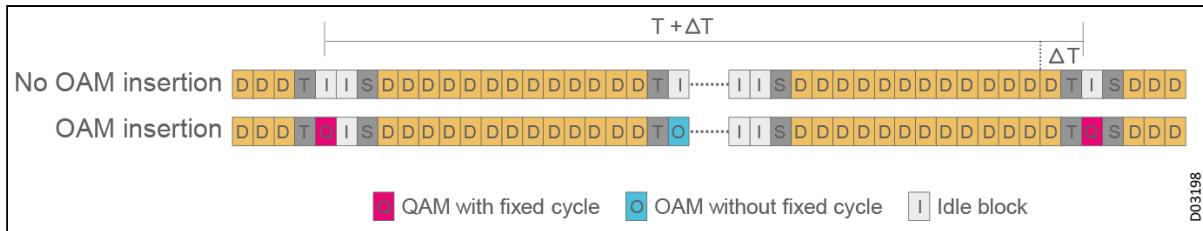
This is a good fit for DCI and point to point applications, but lacks the basic carrier grade requirements that are the basis for any IP/packet network. While FlexE does provide support for the network slicing ability that is an essential element in 5G networks, it's missing essential elements such as multi-link end-to-end services, and protection through end to end FlexE client OAM, capabilities that are critical for 5G implementations. This is why we offer a comprehensive 5G transport solution, which is based on FlexE enhancements according to G.mtn and G.8312 transport standards.

## FlexE Channel OAM

Transport technologies, such as SONET/SDH, OTN, MPLS-TP, and traffic engineering extensions of IP protocols, are used in the telecom world to deliver carrier grade services. These technologies rely on OAM tools to provide sub-50ms protection and end to end service monitoring. G.8312 enhances FlexE capabilities by defining a method for insertion of path layer OAM, to enable APS (automatic path protection) and end to end OAM for every FlexE client.

FlexE channel layer OAM is located between the FlexE customer data and the FlexE group link layer, enabling customer data access/recovery, addition/deletion of OAM information, data flow cross-connection, and channel protection. FlexE channel OAM is inserted/extracted while client services are unaware of the process. The FlexE channel OAM is based on an idle block replacement mechanism.

## FlexE Channel OAM



## **FlexE OAM Features**

The following OAM features, based on ITU-T G.MTN G.8310/8312, are implemented:

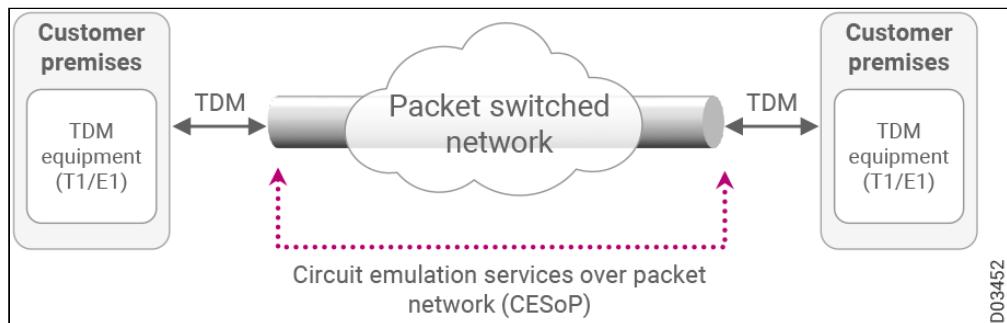
- BAS: Code block for basic OAM messages sent periodically, including connectivity check (CC), BIP check, RDI, REI, CS\_LF, CS\_RF function; interval period is configurable between 16K Blocks (default), 32K Blocks, 64K Blocks, and 512K Blocks.
  - APS: Automatic protection switching message block for automatic protection switching.
  - CV: Connectivity verification code block for connectivity verification; on-demand OAM.
  - CS: Customer signal indicating code block for indicating customer signal type.
  - 2DMM: Bidirectional delay measurement code block for sending two-way delay measurement messages; on-demand OAM.
  - 2DMR: Bidirectional delay response code block for responding to a two-way delay measurement message.

FlexE OAM also includes the following Alarms and PM counters:

- Channel alarms: LOC, RDI, CS\_LF, CS\_RF, CS\_UNEQ, TIM, SF, SD, Period-Mismatch, LF, RF
  - Channel PM counters: BIP error counter, REI counter, CRC errored blocks, statistics of various OAM blocks

# CES Technology

## CES Over Packet Network



TDM data may be transported over IP, MPLS, or Ethernet networks, by configuring the encapsulation methods and the services that transport the encapsulated packets. Different techniques are used to translate TDM timing aspects to the relevant recovery mechanisms at the far end. The emulated network also provides the OAM functions necessary to deliver the reliable TDM service experience over an emulated network.

Neptune platforms support traditional CES emulation, providing TDM transport over PSNs for backhaul applications offering a wide range of new broadband data services. These boost the advantages inherent in packet based networks, including flexibility, simplicity, and cost effectiveness.

Neptune platforms also offer an elegant end-to-end CES services solution, implemented through Smart SFPs that facilitate the efficient transformation of legacy networks to Ethernet and IP/MPLS transport. Migrating your network from legacy TDM technology to packet has become as simple as replacing a regular transceiver with a Smart SFP. Just plug a Smart SFP transceiver into your router or switch to transport TDM traffic (converted into a packet stream) across a PSN.

This section introduces the CES solutions provided by Neptune platforms, including the following:

- Smart SFP Solutions
- CES Migration Applications
- Migration Technology
- CES Protection Mechanisms
- VLAN-Tagged and Double VLAN Classification

## Smart SFP Solutions

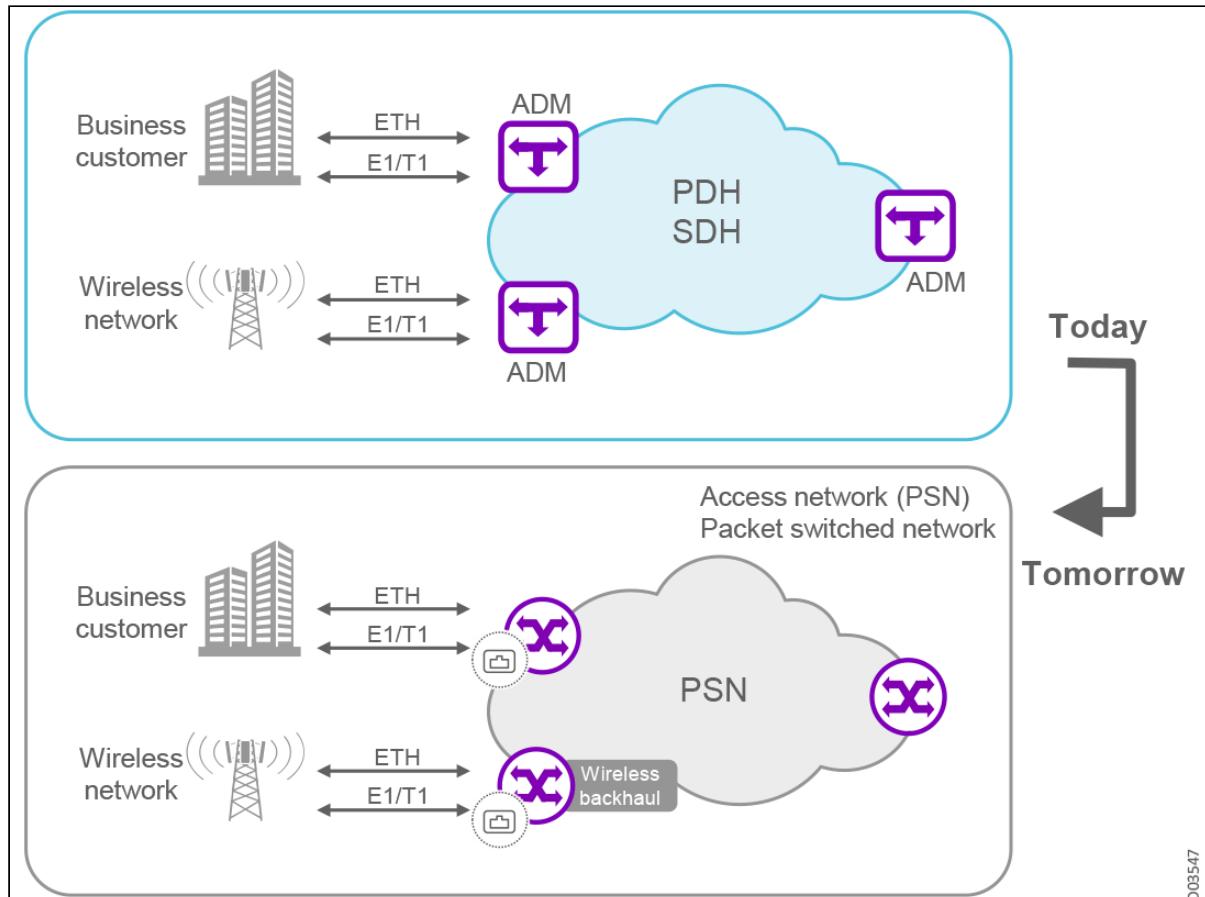
Legacy SDH and SONET networks, traditionally used for transmission of voice and data signals, still operate worldwide. These legacy networks use time-division multiplexing (TDM), which ensures that a constant stream of data travels on the network. Lower bit-rate streams of information are combined (multiplexed) into higher bit-rate streams to take advantage of the bandwidth available.

Today most services are packet-based, presenting Ethernet LAN interfaces to the WAN transport network, with the WAN using IP/MPLS to route these services across the WAN. However, a large number of the legacy TDM-based services still remain, with SDH/SONET still being used to transport these services. Operators of these networks are starting to face some critical issues:

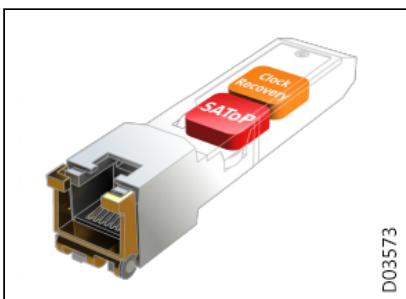
- SDH/SONET equipment has been in the network for a very long time, 20 years or more, and is starting to fail
- SDH/SONET components and products are becoming End of Life
- An ever-decreasing number of people who understand how to operate SDH/SONET equipment
- The customers who are still using TDM services do not want to or cannot migrate to an equivalent packet service

Smart SFP (small form-factor pluggable) transceivers are designed to allow TDM services to be transported over Ethernet and IP/MPLS transport networks. Migrating the network from legacy TDM technology to packet has become as simple as replacing a regular transceiver with a Smart SFP. Just plug a Smart SFP transceiver into your router or switch to transport TDM traffic (converted into a packet stream) across a PSN.

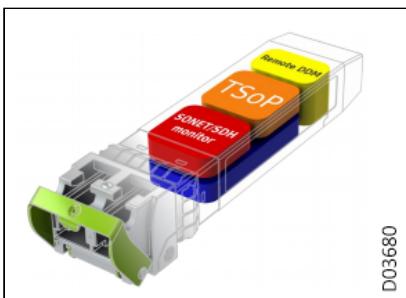
### Smart SFPs Simplify Migration to Tomorrow



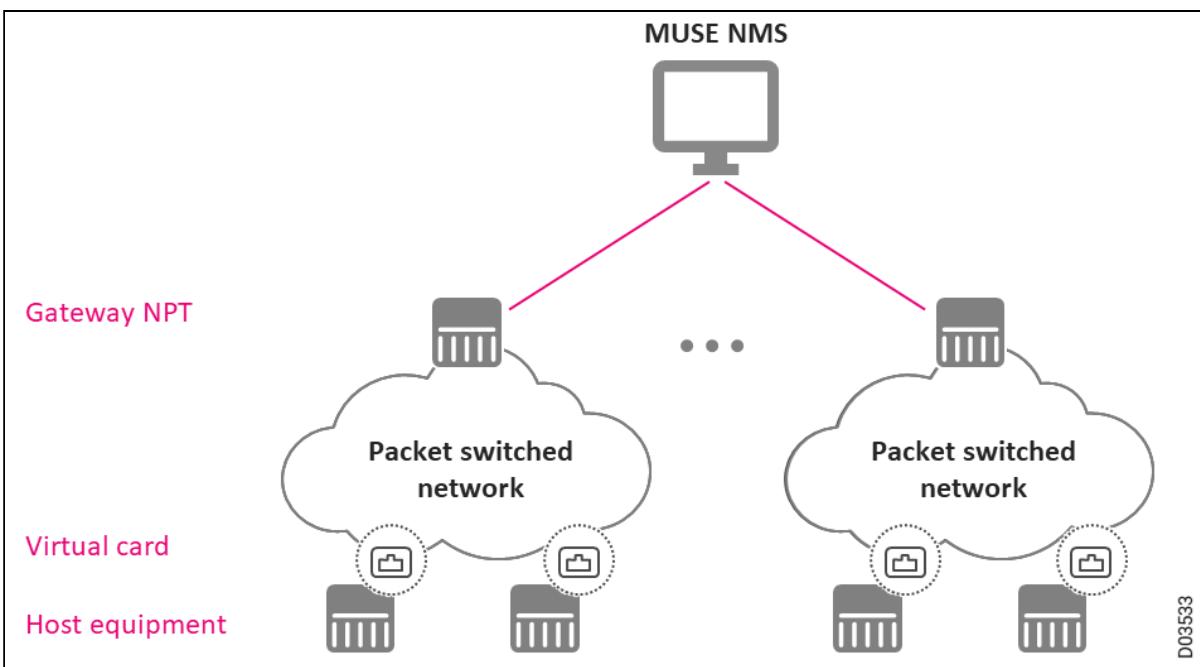
TPoP (Transparent PDH over Packet) Smart SFPs convert E1 or T1 (DS1) traffic to a packet stream, using RFC4553 SAToP TDM over packet pseudowire technology. Designed in conformance with the Small Form Factor Pluggable 20-pin Multi-Source Agreement (MSA), Smart SFPs can be used in any free SFP slot in a router or a switch to transport PDH traffic across a packet network. Smart SFPs are plug-and-play devices which can be used without any provisioning, and simplify configuration and service turn-up of E1/T1 connections across a packet network. Integration of TPoP functionality within an SFP module greatly reduces system and network complexity, offers a lower carbon footprint, and provides significant savings in CAPEX and OPEX. TPoP capabilities are complemented with a Gigabit Ethernet system interface. Smart SFPs provide a standard RJ45 interface and are designed to operate within the standard industrial temperature range (-40°C to 85°C, -40°F to 185°F). Optionally, an API is available to facilitate integration into existing equipment and management systems. This management interface allows configuration and helps to monitor relevant parameters.

**TPoP Smart SFP**

The Transparent SONET/SDH over Packet (TSoP) Smart SFPs convert STM-1/OC-3, STM-4/OC-12, and OC-48/STM-16 TDM traffic to a packet stream, providing a standard SFP interface. TSoP SFPs can be assigned to any 10GbE port. These transceivers support encapsulation of CESoETH and CESoMPLS.

**TSOP Smart SFP**

Choose the appropriate Smart SFP transceiver based on the type of legacy TDM traffic, PDH or SDH. These pluggable modules convert TDM-format (E1/T1 or STM) digital signals into data packets. Packets are transferred via the Ethernet port on the SFP's host device, through one or more PSNs. The process is reversed at the other end. Smart SFPs enable end-to-end CES services across networks that include both our own and third-party equipment. The CES service termination points can be on anyone's equipment, since the smart SFPs that actually create the end-to-end CES service are pluggable into any appropriate device.

**Smart SFP Solution Architecture**

Smart SFPs bring simplicity to your network. Because network functions are integrated into the transceivers, Smart SFPs can replace several devices in your network, decreasing the overall number of devices used in your network and thereby simplifying your network. A simpler network can be managed more efficiently, lowering overall power consumption and carbon footprint, and reducing your OPEX. Smart SFPs are a zero-footprint solution; simply replacing the existing transceivers lowers the CAPEX while enhancing network performance. Integrated solutions from Ribbon using smart SFPs provide:

- Intelligent system functions embedded inside the transceiver
- Network functionality providing:
  - Service Assurance
  - Network Migration
  - Network Timing

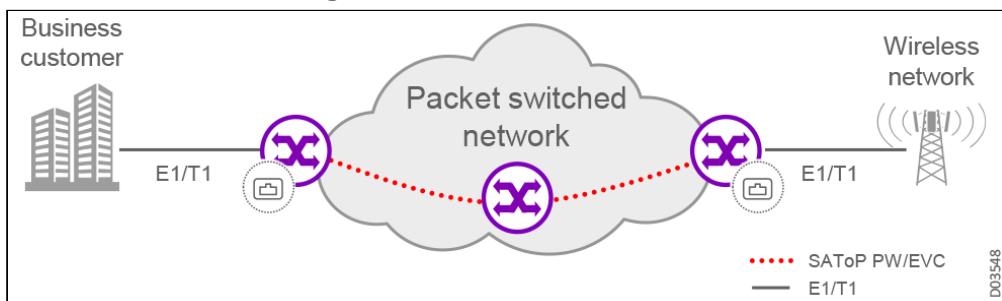
This section introduces the following use cases:

- Use Case: Smart SFP for E1-T1 Traffic
- Use Case: E1-T1 to N x E1-T1

## Use Case: Smart SFP for E1-T1 Traffic

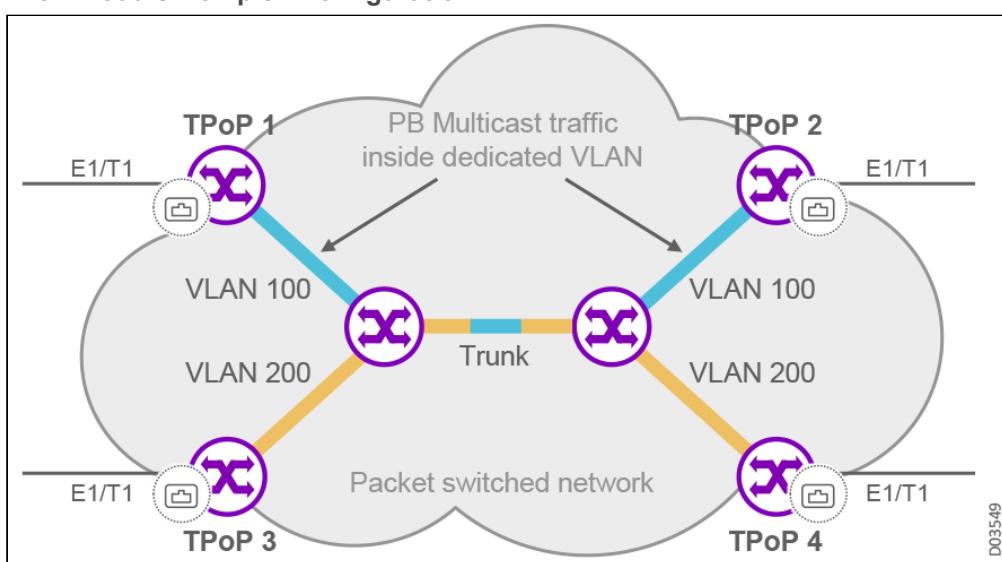
The following figure illustrates a simple configuration based on the TPoP (Transparent PDH over Packet) Smart SFP. E1/T1 traffic from a PDH network on one side is encapsulated by a TPoP module. The traffic packets are sent across the packet switched network. At the other side they are decapsulated and forwarded by the peer TPoP module to the second PDH network. Each TPoP Smart SFP provides complete encapsulation and decapsulation functions, enabling a bi-directional link across the packet switched network.

### TPoP Module Basic Configuration



In this basic configuration, a CES Provider Bridge (PB) point-to-point (P2P) service segment is created at each end. A Layer 2 VPN service segment (such as a PB P2P) is created over the PSN section.

### TPoP Module Complex Configuration

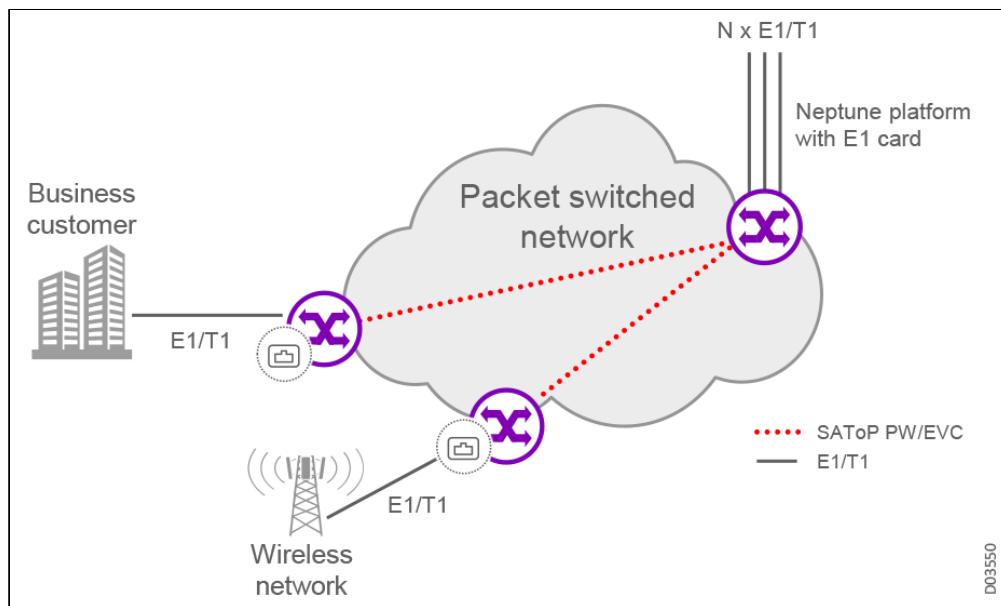


In this more-realistic configuration, a CES PB P2P service segment is created at each end. A L2VPN service segment (such as a PB multi-point-to-multi-point (MP2MP) is created over the PSN section.

The TPoP Smart SFP can transport a Gigabit Ethernet through a 20-pin electrical interface. TPoP Smart SFP provides an E1 (2.048Mbps-120Ω) or T1 (1.544Mbps-100Ω) balanced interface (through an RJ45 port) to transport an E1/T1 (aka DS1) signal across an Ethernet network, using the SAToP (RFC4553) protocol.

## Use Case: E1-T1 to N x E1-T1

E1/T1 to N x E1/T1



In this typical configuration, a CES PB P2P service segment is created at each of the starting (E1/T1) ends. Multiple CES PB P2P services are created in the N x E1/T1 SAToP card end. And an L2VPN service segment is created over the PSN section in the middle.

## CES Migration Applications

Operators have an urgent need to retire their SDH/SONET networks and migrate their legacy TDM services onto a modern packet network. This packet network must support the full range of services currently supported on the SDH/SONET network; the packet network must offer equivalent, or better, performance than the existing SDH/SONET network. The migration itself should be “invisible” to the end users, with no service disruption.

Fortunately, Neptune platforms offer well established, field proven processes to make this migration seamless and risk-free. We have the technology to support TDM services on the packet network in a manner which is, as is required, at least equivalent to, if not better than, the legacy SDH/SONET network. Once migrated, the new network must have the flexibility to allow the customers to easily migrate their services from legacy TDM services to new packet services as and when they upgrade their applications. The new network must also give the service provider the ability to offer differentiated services and provide the agility to dynamically react to changing conditions.

This section describes the three primary CES migrations being performed today.

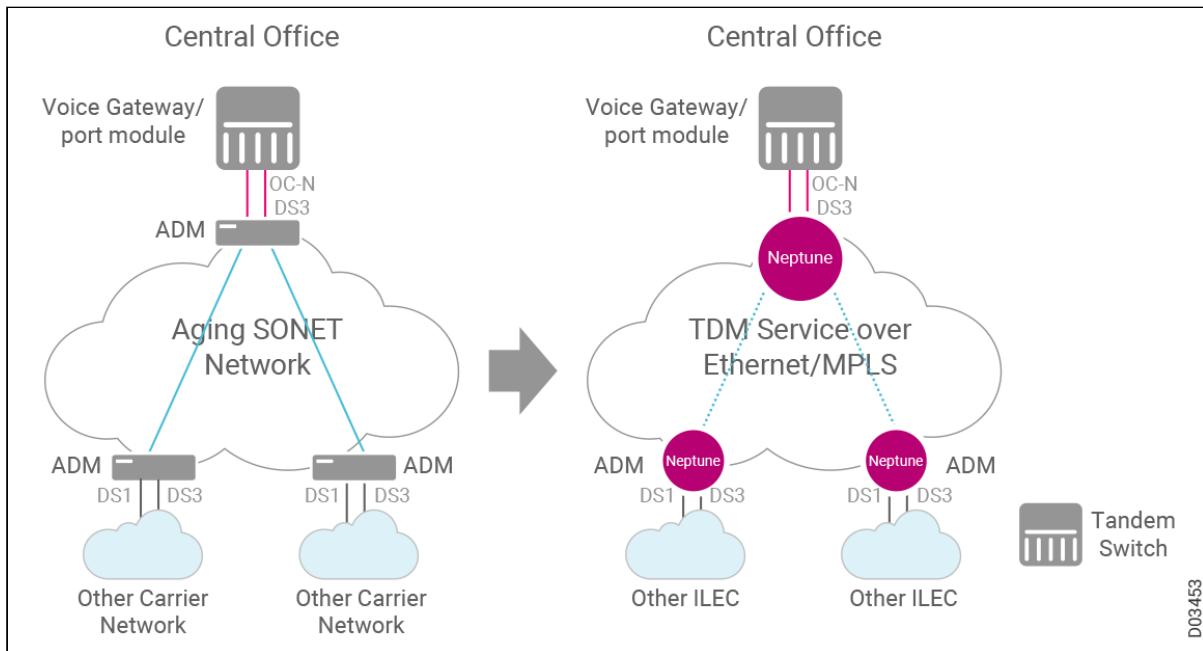
- Voice Trunk Migration
- Legacy Service Migration
- Utilities Migration

## Voice Trunk Migration

Traditional "voice" telephone calls were the first applications handled in the original SDH/SONET networks, based on the gold-standard of TDM technology. Now these classic SDH/SONET trunk technologies must be migrated to the current packet networks. This includes the ability to:

- Interconnect voice switches
- Eliminate PDH/SONET NEs
- Leverage Ethernet and MPLS efficiency
- Provide equivalent or better availability, resilience, and OAM than the legacy SDH/SONET network

### Voice Trunk Migration



The new IP/MPLS network uses standards-based circuit emulation (CES) approaches (SAToP and CESoPSN) to enable it to support all of the functionality required to provide voice trunks:

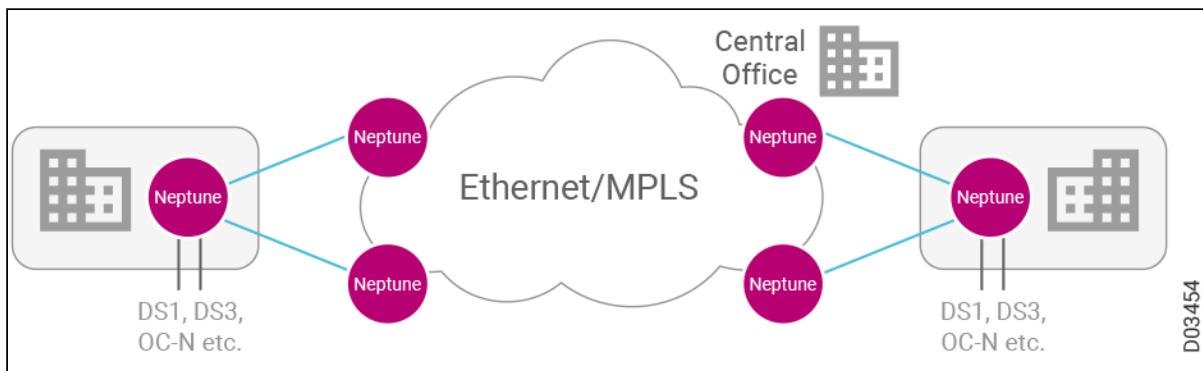
- DS1/DS3 hand-off to other suppliers
- OC-N hand-off to the voice gateway
- 50ms protection switching
- 10ms failure detection
- Voice-grade QoS

Where required, deterministic packet transport protocols such as Segment Routing (SR), MPLS-TP, or RSVP-TE can be used. This new network is fully interoperable with existing IP routing and DWDM networks.

## Legacy Service Migration

Historically, many enterprises leased SDH/SONET connectivity from service providers to transport their TDM traffic. But over the last couple of decades, Ethernet and PSN have become the ubiquitous WAN technologies. The cost per bit of Ethernet connectivity has dropped dramatically; the footprint and power consumption of Ethernet and PSN hardware has been dramatically reduced as well. Migrating these TDM services so they can be transported over a PSN will dramatically reduce the costs enterprises are paying for leasing their connectivity.

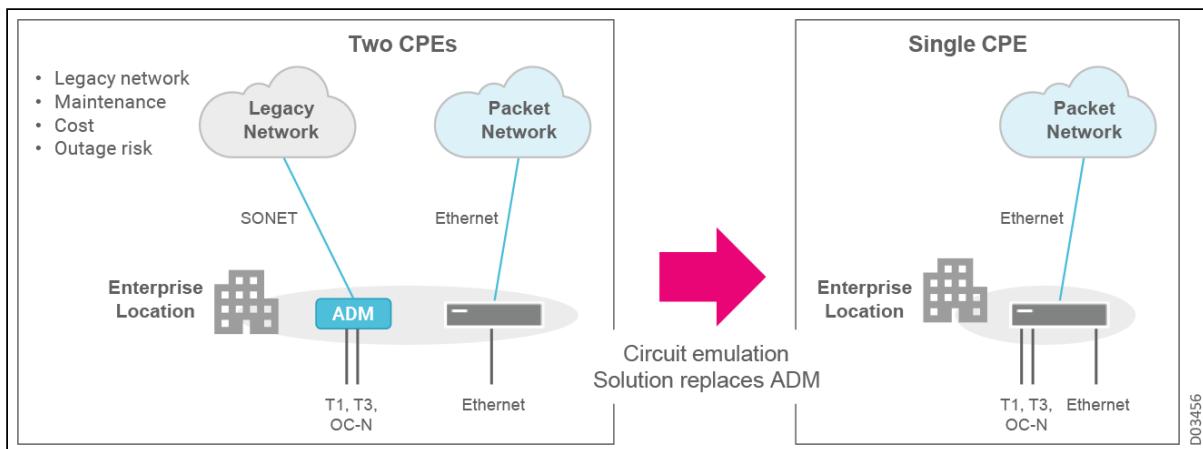
### TDM Services over a Packet Network



The packet network uses circuit emulation to provide enterprises with a reliable platform for supporting their legacy SDH/SONET services. Direct DS1, DS3, and OC-3/12 interfaces allow existing services to be connected directly to this packet network. Where the service requires high availability, the packet network supports a number of resilience options, providing the same level of service resilience as provided by the legacy SDH/SONET network:

- G.8032v1: Recommended for access protection
- MC-LAG (Multi-Chassis Link Aggregation Group): Allows the traffic to be shared over multiple chassis, as well as providing redundancy in the event one of the chassis fail
- LDP (Label Distribution Protocol): Used to provide end to end protection

### Simplifying your Network with Circuit Emulation

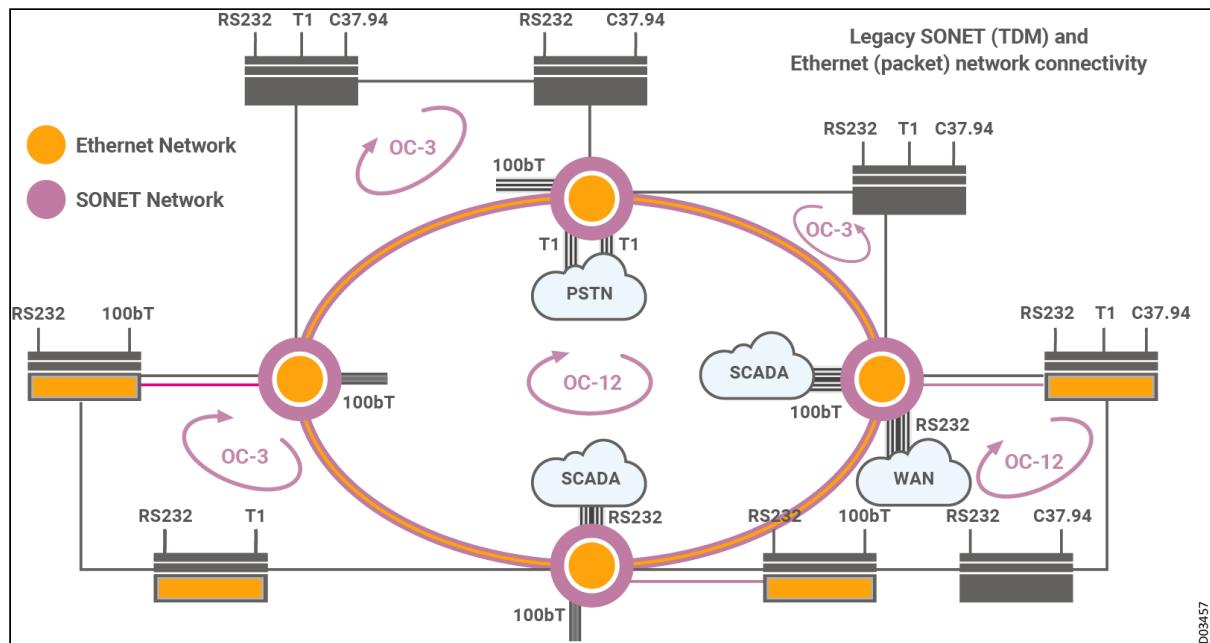


## Utilities Migration

The following figures illustrate migration from a legacy TDM/Ethernet utilities network to a modern dual-stack packet network.

In the **legacy network**, specialized SDH/SONET equipment is designed to carry SCADA and other TDM traffic, including T1, RS232, and C37.94 tele-protection traffic. At interconnection points, ports on the SDH/SONET equipment are reserved to route traffic between rings. A packet network carries Ethernet traffic for the IT services.

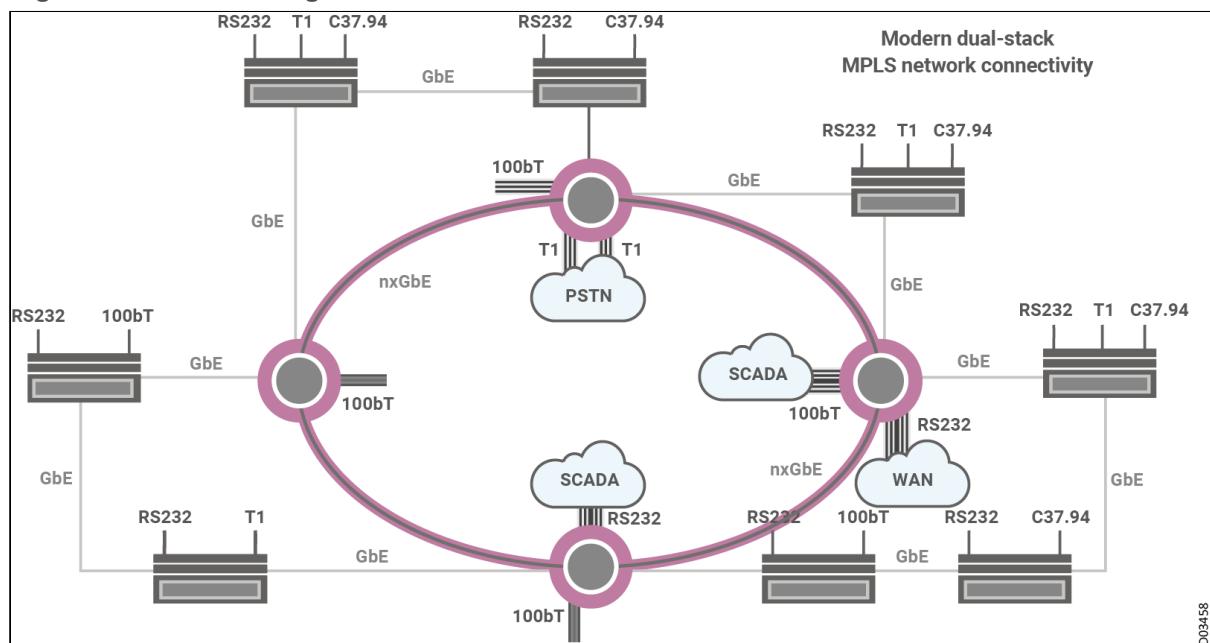
## Legacy Network Configuration



D03457

In the **migrated network**, the two separate networks are converged onto a single packet network (utilities may optionally choose to keep separate physical devices for their IT and OT networks). The MPLS packet network provides guaranteed deterministic performance, meeting the strict protection and latency requirements required for tele-protection and TDM traffic.

## Migrated Network Configuration



D03458

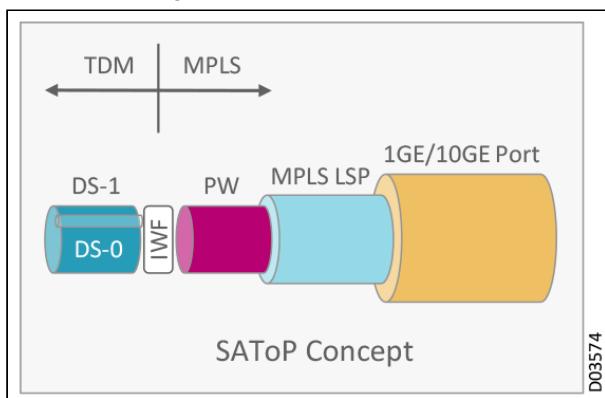
## Migration Technology

Circuit emulation (CES) technology is used to allow legacy SDH/SONET services to be mapped onto the packet network. Different circuit emulation standards are designed to cater for different operational scenarios. This section introduces some of those technology standards.

**IETF RFC 4553**

SAToP - Structure-Agnostic TDM over Packet

- Maps complete DS1s and DS3s into pseudo wires
- Maintains all the framing structure
- Agnostic to payload – voice, video, data
- Bulk transport over MPLS networks
  - SONET ADM replacement
  - DCS replacement
  - Private line replacement
  - Lease line cost avoidance
  - Voice trunking

**SAToP Concept****IETF RFC 5085**

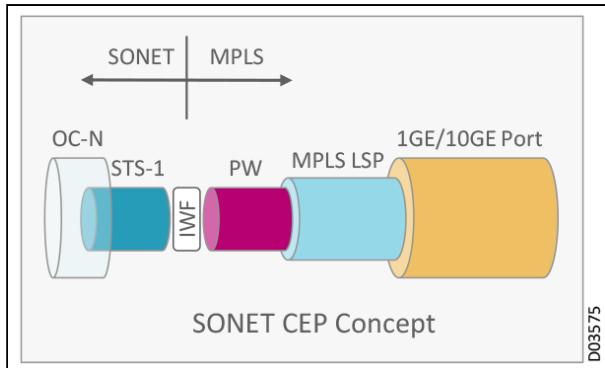
CESoPSN - Structure-Aware TDM Circuit Emulation Service over Packet Switched Network

- Provides individual DS0 visibility
- Needed for 1/0 DCS replacement

**IETF RFC 4842**

CEP - SDH/SONET Circuit Emulation over Packet

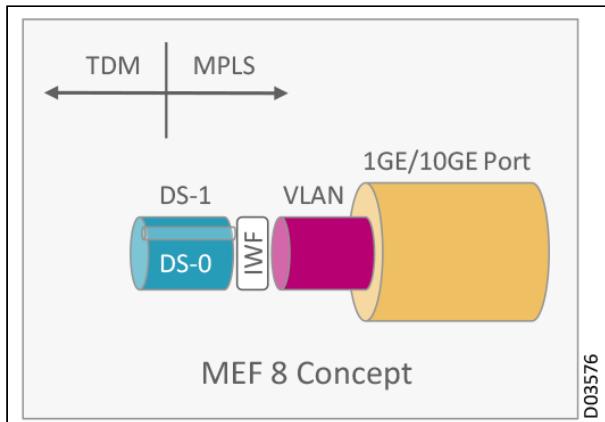
- Emulates SDH/SONET path structures
- STS, VT1.5, VT11, etc.
- SDH/SONET path payload agnostic

**SONET CEP Concept****MEF 8**

## PDH over Metro Ethernet

- DS0, DS1, DS3 (E3 / E1) over Ethernet
- Structure agnostic (DS1, E1, DS3, E3) [like SAToP]
- Structure-aware mode ( n x 64kbps aware) [like CESoPSN]
- Basic mode (no SONET path over Ethernet)

## MEF 8 Concept



## MEF 3

- Circuit Emulation Service Definitions

## Standard Emulation Conventions and Interface Support

Neptune platforms support the standard emulation conventions that have been developed, appropriate for all types of networks, including:

- Circuit Emulation over Ethernet
  - MEF 3 and MEF 8
  - PBB and E-Line conventions
- Circuit Emulation over Pseudo-Wire
  - PWE3 conventions: MPLS-LDP, MPLS-RSVP-TE, MPLS-TP
  - Structure Agnostic CES: SAToP
  - Structure-Aware CES: CESoPSN

This includes:

- CESoPSN and SAToP for E1/T1 interfaces, with encapsulation support for CES over MPLS-TP (CESoMPLS) and CES over Ethernet (CESoETH)
- CESoPSN and SAToP for STM-1/4 channelized and OC-3/12 interfaces, with encapsulation support for CES over MPLS-TP (CESoMPLS) and CES over Ethernet (CESoETH)
- CEP service based on VC-3, VC-4, VC4-4c
- CEP service based on STS-1, STS-3c, STS-12c
- CES service based on DS1, DS3, and OC-n (OC-3 - OC-48)

For example, at the hub or BSC/RNC sites, Neptune functions as a carrier class multiservice aggregator, optimizing cellular backhaul by multiplexing various TDM services into a single ChSTM-n. STM-1/OC-3 support includes channelized STM-1/OC-3 with up to 63 x VC-12 channels for SDH or 84 VT1.5 channels for SONET.

## CES Protection Mechanisms

Neptune's CES solutions enjoy the same standard of protection as the other solutions in the Neptune product line; see [Neptune Protection and Restoration Mechanisms](#). This section describes a few of the Neptune protection mechanisms.

## MSP 1+1 Protection

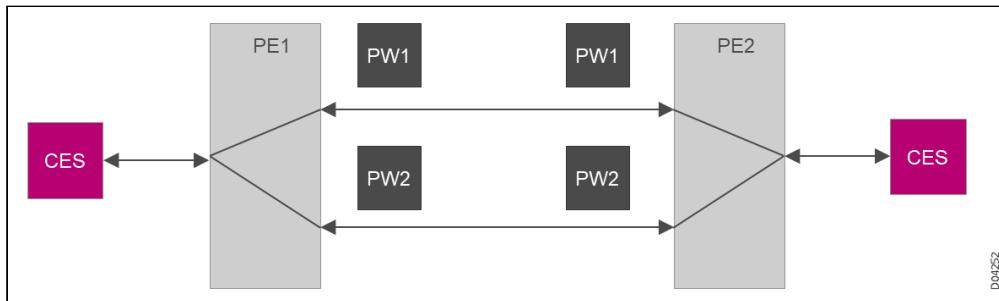
Neptune platforms support MSP 1+1 protection at the port level for STM-n/OC-n ports. Protection can be either bidirectional or unidirectional, available in both SDH and SONET modes, for both revertive and non-revertive configurations.

- Cross-card protection is available with MSC\_2\_8 and MS1\_4 cards when used in NPT-1800, NPT-1250, and NPT-1050 platforms.
- Intra-card protection is available with MSC\_2\_8 and MS1\_4 cards when used in NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1100, NPT-1050, and NPT-1022 platforms.
- Cross-card protection is available with MSC\_2\_16E cards when used in NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1050, and NPT-1022 platforms.
- Intra-card protection is available with MSC\_2\_16E cards when used in NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1050, and NPT-1022 platforms.
- Cross-card protection is available with MS16\_4MR cards when used in NPT-2300, NPT-1800, NPT-1300, NPT-1250, NPT-1200, and NPT-1050 platforms.
- Intra-card protection is available with MS16\_4MR cards when used in NPT-2300, NPT-1800, NPT-1300, NPT-1250, NPT-1200, NPT-1100, NPT-1050, and NPT-1022 platforms.

## PW 1+1 Protection

Neptune platforms support CES protection through pseudowires (PW), configured in a 1+1 arrangement. As illustrated in the following figure, 2 PWs are established between a pair of NEs, providing non-traffic affecting protection to the CES service. Traffic is transmitted and received on both PWs simultaneously. If one PW fails, traffic flow is automatically taken from the other PW. So as long as the CES traffic can be transported through either one of the PWs, the traffic flows normally.

### CES PW 1+1 Protection



### 1:1/1:N Tributary Protection (TP)

Neptune platforms support 1:1/1:N protection at the card level for DS1/DS3 ports.

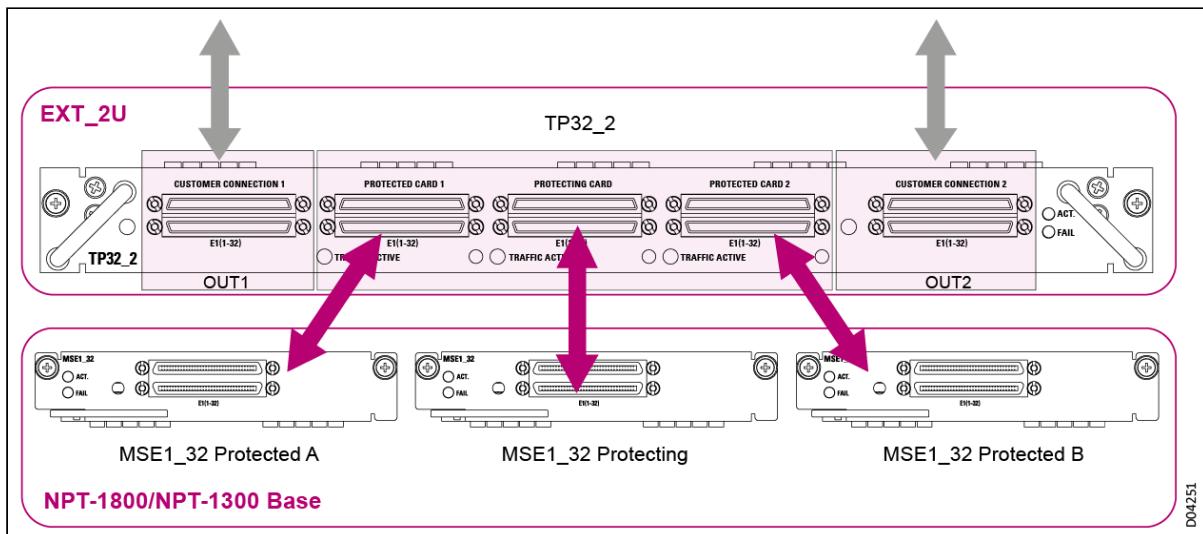
- E1/T1 CES card 1:N protection
- E3/DS3 CES card 1:1 protection

For example, Neptune platforms support Tributary Protection (TP) by protection cards installed in EXT-2U/2UH expansion units. This provides protection for tributary card failures, such as card power-off, card out, BIT fail, and so on. Protection can be either bidirectional or unidirectional, available in both SDH and SONET modes, for both revertive and non-revertive configurations. The protection scheme can be either 1:1 or 1:2. Protection is configured by defining a Protection Group (PG), as follows:

- Protecting card: Only one tributary card can be selected as the protecting card. This card should have no existing trails. The protecting card can be located in any slot.
- Protected cards: One (1:1) or two (1:2) tributary card(s) can be selected as protected cards. A protected card can have existing trails. This means that TP can be configured for a card that is already carrying traffic, without removing existing traffic.
- Associate the protecting card and protected cards.

For example, the TP32\_2, installed in the expansion platform, provides 1:1 or 1:2 protection for 32 x E1 interfaces on MSE1\_32 cards installed in the corresponding base unit (NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms). Latched relays are used to redirect the traffic connections between customer connections and internal connections, so that a redirecting cable is not required when a switch is triggered for the protected card. Warm reset is supported; traffic is not affected when the software is restarted.

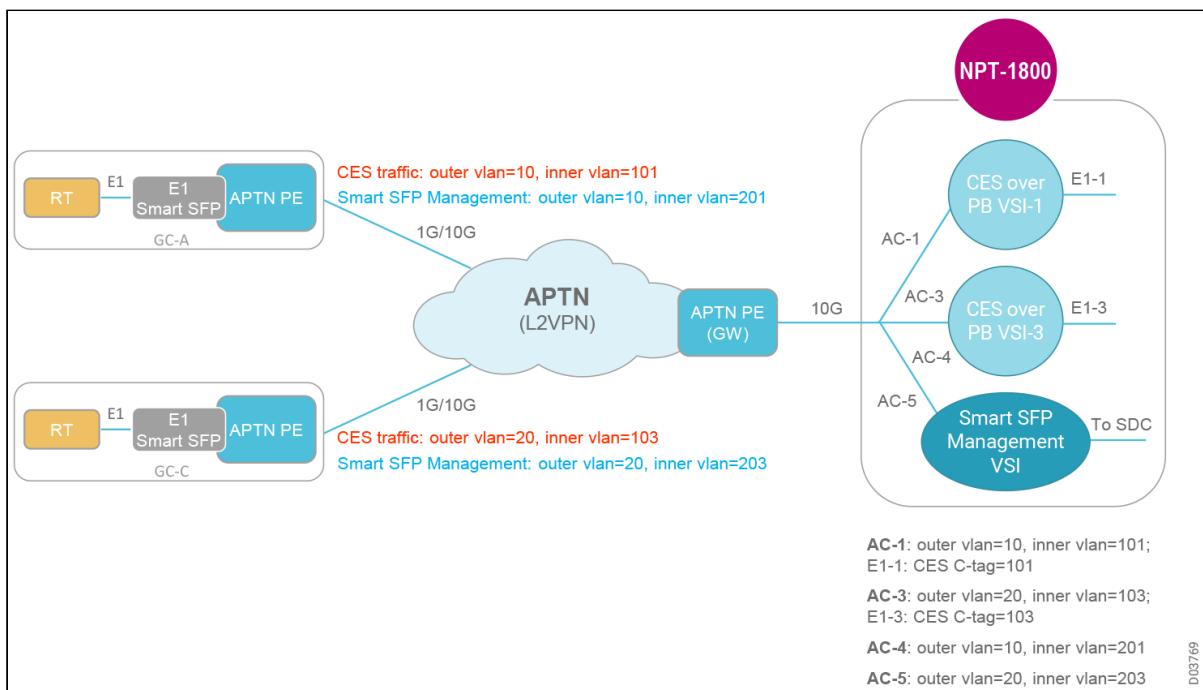
### MSE1\_32 CES Card 1:2 Protection



The TPS345\_1 provides 1:1 protection for MS345\_3 cards installed in the corresponding base unit (NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms). The protection mechanism is similar; customer connections are available for external customer devices, as well as 2 connectors for 2 MS345\_3 cards, one to be protected and one to do the protecting.

## VLAN-Tagged and Double VLAN Classification

### Double-VLAN Classification

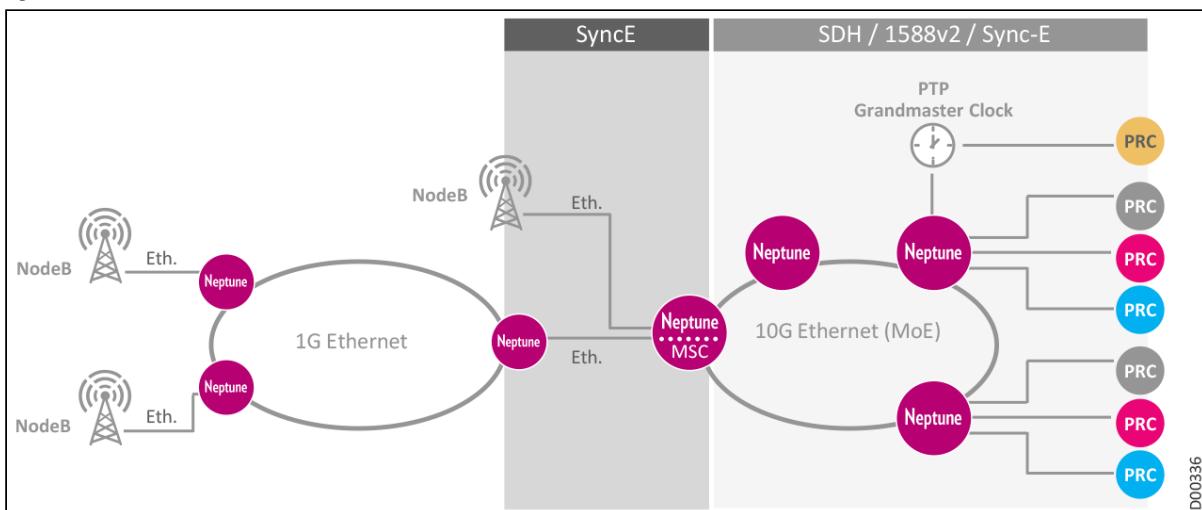


# Timing and Synchronization and Clock Recovery

Network synchronization is an important feature, essential to providing excellent performance and quality of service for subscribers. Synchronization is essential for TDM components and mobile backhaul applications. Base stations in wireless networks must be synchronized to a common clock for smooth call handoff between adjacent cells. Until recently, it has not been possible to work with Ethernet protocols, which are by nature asynchronous, in wireless networks for which synchronization is essential. Migrated networks must be able to provide the same timing and synchronization capabilities that SDH/SONET provided, with timing from an internal or external clock source, and timing distribution achieved with SyncE and/or 1588v2.

Neptune platforms in 3G, 4G, LTE, and 5G backhauling networks are able to support intelligent combinations of SyncE and 1588v2 synchronization mechanisms, providing the most efficient solution for synchronizing NodeBs connected via Ethernet interfaces, depending on the network configuration and infrastructure.

## Synchronization in MBH Networks



To synchronize both ends of a TDM circuit across packet based networks, clock recovery mechanisms such as Adaptive Timing or Differential Timing, designed to tolerate Frame Delay, Frame Delay Variation, and Frame Loss, must be used at the receiving end of the CESoPSN/SAToP connection.

*Differential Timing*, which is a more costly solution, requires a reference clock signal at all ends. Differential timing is very reliable, being less affected by network delay, Packet Delay Variations (PDVs), or packet loss.

*Adaptive Timing* is used when a remote site doesn't have access to a primary reference clock, in which case the receiving system recovers the clock based solely on incoming packets. In this case the TDM service performance is strongly dependent upon the characteristics of the carrier Ethernet network, such as Frame Delay, Frame Delay Variation, and Frame Loss Ratio.

The Neptune product line supports SAToP service termination from physical E1/T1 interfaces and can also aggregate multiple E1s into STM-1 and STM-4 interfaces and T1s into OC-3 and OC-12 interfaces. Every E1/T1 is mapped into a PW. Each PW is mapped to the relevant service using a dedicated VLAN ID. Payload size depends on the service type. For E1, the payload size is 256 bytes and for T1, payload size is 192 bytes.

The CES modules support two timing modes per CES service, as follows:

- **Differential Clock Recovery (DCR):** The original clock is recovered for each circuit using network-wide synchronization and marking the clock difference between each payload and the reference network clock.

- **Adaptive Clock Recovery (ACR):** The E1/T1 clock is generated from the packet network. Each E1/T1 service has its own logical jitter buffer and PLL to align the TDM frames to the E1/T1 timing.

When groomed to SDH interfaces, the individual E1 timing is independent of the SDH interface synchronization. In fact, each VC-12 within the STM-n interface carries an E1 with its own independent timing.

This section introduces the following features:

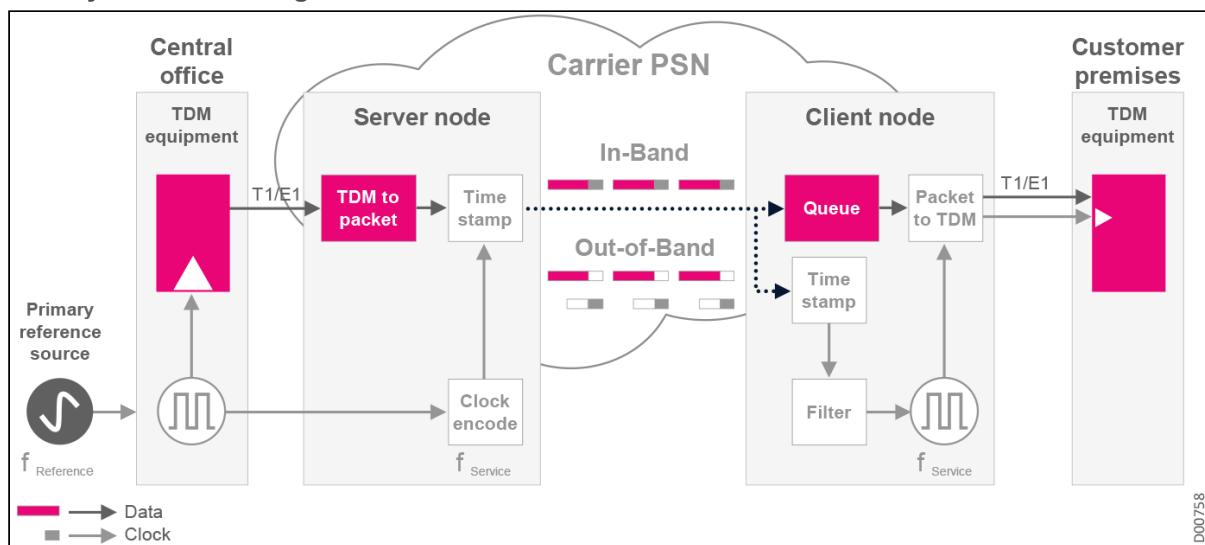
- Adaptive Clock Recovery ACR Overview
- Differential Clock Recovery DCR Overview
- Synchronous Ethernet
- IEEE 1588v2 PTP
- GNSS Receiver Functionality
- G.8275.1-G.8275.2 PTP Implementation
- Hybrid Architecture - Combining SyncE and 1588
- Synchronization Summary Table

## Adaptive Clock Recovery ACR Overview

Adaptive Clock Recovery (ACR) was developed to transfer a rough time-base between the transmitter and the receiver that was adequate to ensure that jitter buffers did not overflow/underflow because of a frequency offset between the Transmitter and the Receiver. It is essentially a recovered clock based on the average cell/packet size. This method is not suitable for 3G if Cell Delay Variation is not within tight bound. The figure that follows explains the principle behind ACR. Digital Service clock is derived from the Reference Clock. This derived clock is fed to the TDM equipment as well as the clock encoder. Clock encoder is a device that time-stamp the network bound frames. The interface between the TDM world and the PSN world is a server node (commonly known as Inter Work Function (IWF), that performs appropriate signaling between TDM streams and Packet streams).

At the server node TDM stream is Packetized and time-stamped and transmitted on the network port. Transmission of Timing information can be either In-band or Out-of-band. Choice of In-band or Out-of-band depends on the quality of synchronization desired at the intermediate nodes in the PSN.

**ACR System Block Diagram**

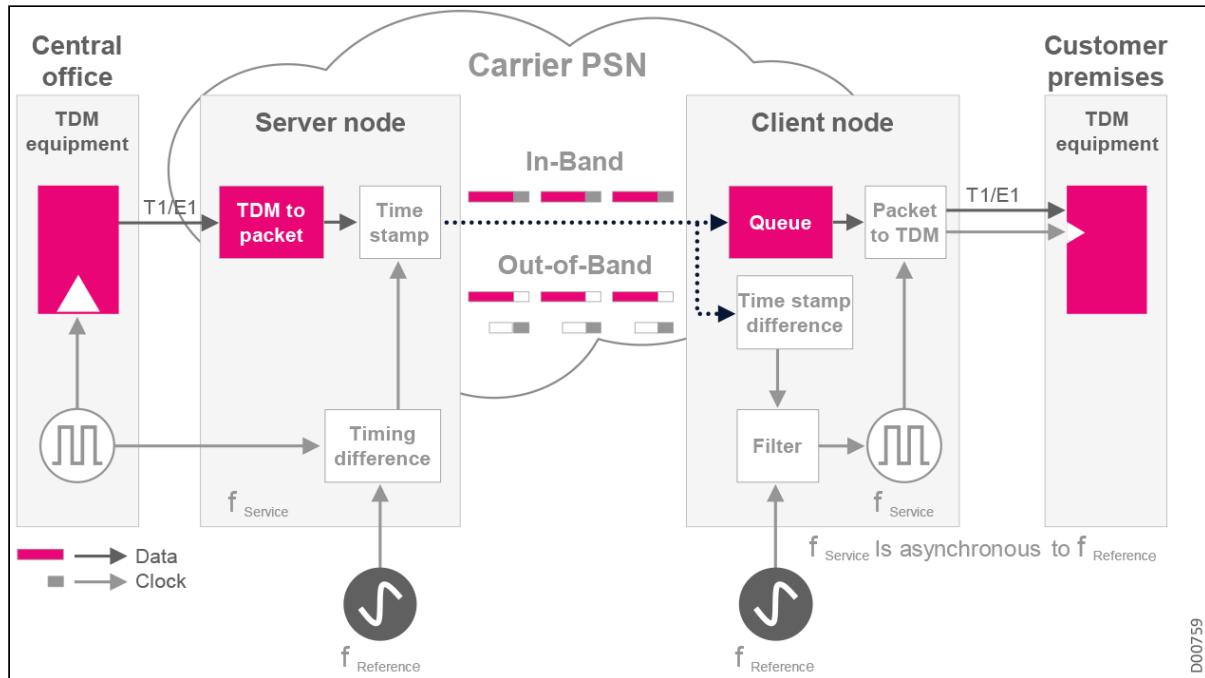


## Differential Clock Recovery DCR Overview

Differential Clock Recovery (DCR) is a useful technique if Reference clock is available at both server and client sides. Refer the figure below. Possible means of distributing a reference clock:

- Central Office clock (if reference clock equipment is located in the CO)
- SDH/SONET clock (e.g. if network uses Packet or Ethernet over SDH/SONET)
- GPS clock

### DCR in the Network



## Synchronous Ethernet

Synchronous Ethernet (SyncE) is a powerful physical layer approach to frequency synchronization that provides an elegant effective solution to the lack of synchronization in traditional Ethernet. SyncE is based on the well-established SDH/SONET synchronization model extended for Ethernet-based networks. SyncE uses the physical layer interface to pass timing from node to node, as done in SDH/SONET networks.

Neptune data cards support SyncE synchronization, which is fully compatible with the asynchronous nature of traditional Ethernet. SyncE is defined in ITU-T standards G.8261, G.8262.1, and G.8264.

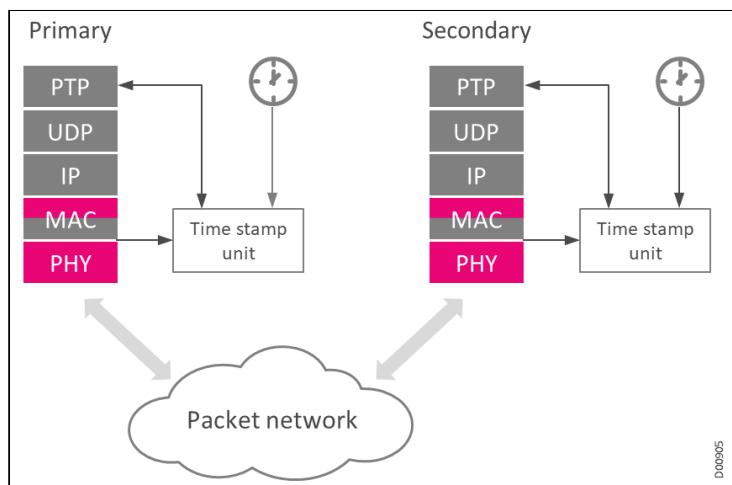
SyncE makes it possible for mobile operators to incorporate Ethernet in their network infrastructure. SyncE clocks, as defined in G.8262.1, are compatible with the clocks used in current synchronous networks. As a result, forward-looking network synchronization designs can remain consistent with existing network synchronization implementations.

In a typical use case, optical 1/10/100GE (ETY/MoE) and FlexE ports support SyncE on the Tx and Rx directions for SDH/SONET clock to all service interfaces. These capabilities enable use of an efficient Ethernet infrastructure for the mobile backhauling network.

Because not all links on the network may be SyncE-capable or support synchronization distribution at the physical layer, IEEE 1588-2008 PTPv2 may also be used for frequency distribution.

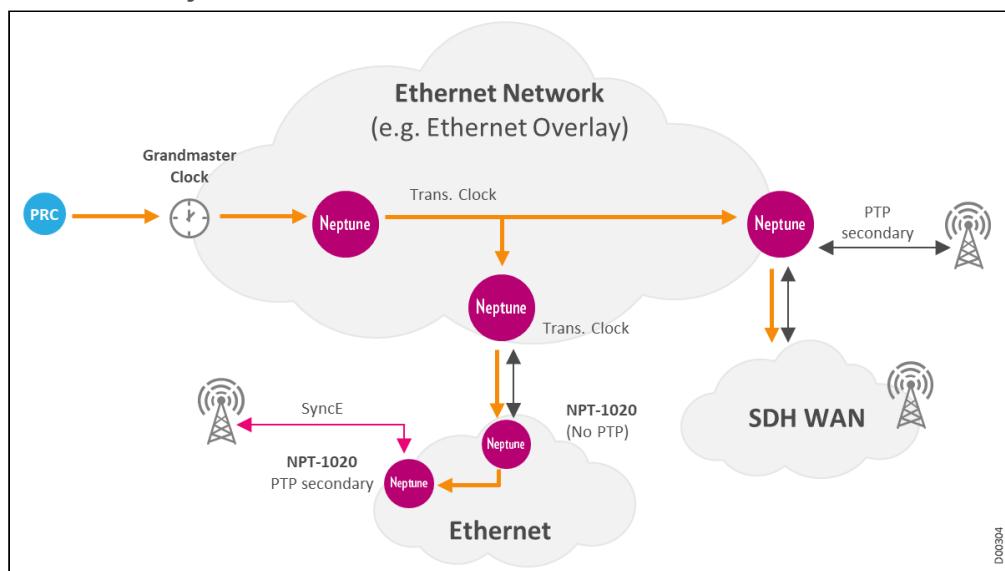
## IEEE 1588v2 PTP

**PTP Protocol Stack**



PTP is an application layer protocol that is implemented over UDP/IPv4/Ethernet, as illustrated in the previous figure. PTP is based on IP/Ethernet transmission between a grandmaster and its associated secondaries. Neptune data cards support IEEE1588v2 functionality, including PTP primary, boundary, transparent, and secondary clocks.

**IEEE 1588v2 Synchronization**



### 1588 Synchronization over Encrypted Up-links

Neptune platforms support 1588 synchronization over up-links encrypted with L2 encryption (MACsec cards).

## GNSS Receiver Functionality

**Global Navigation Satellite System (GNSS)** refers to a group of orbiting satellites providing signals from space that transmit positioning and timing data to a network of ground control stations and receivers. The receivers then use this data to determine location, by calculating ground positions through an adapted version of trilateration.. By definition, GNSS provides global coverage. Examples of GNSS include Europe's [Galileo](#), the USA's NAVSTAR Global Positioning System (GPS), Russia's Global'naya Navigatsionnaya Sputnikovaya Sistema (GLONASS), and China's BeiDou Navigation Satellite System.

GNSS performance is assessed using four criteria:

- **Accuracy:** The difference between a receiver's measured and real position, speed or time
- **Integrity:** A system's capacity to provide a threshold of confidence and, in the event of an anomaly in the positioning data, an alarm
- **Continuity:** A system's ability to function without interruption
- **Availability:** The percentage of time a signal fulfills these accuracy, integrity and continuity criteria.

This performance can be improved by regional satellite-based augmentation systems (SBAS), such as the European Geostationary Navigation Overlay Service (EGNOS). EGNOS improves the accuracy and reliability of GPS information by correcting signal measurement errors and by providing information about the integrity of its signals.

GNSS provides geo-spatial positioning to many devices autonomously, allowing electronic devices with the appropriate receivers to determine their precise location on the surface of the Earth. When connected to an external antenna, the GNSS module can acquire satellite signals and track up to 32 GNSS satellites, computing location, speed, heading, and time, and providing an accurate 1PPS signal, a stable 10MHz frequency output, and an accurate time-of-day (ToD). The antenna must have as large an unobstructed view as possible of the sky. For proper timing, the receiver should lock onto a minimum of four satellites.

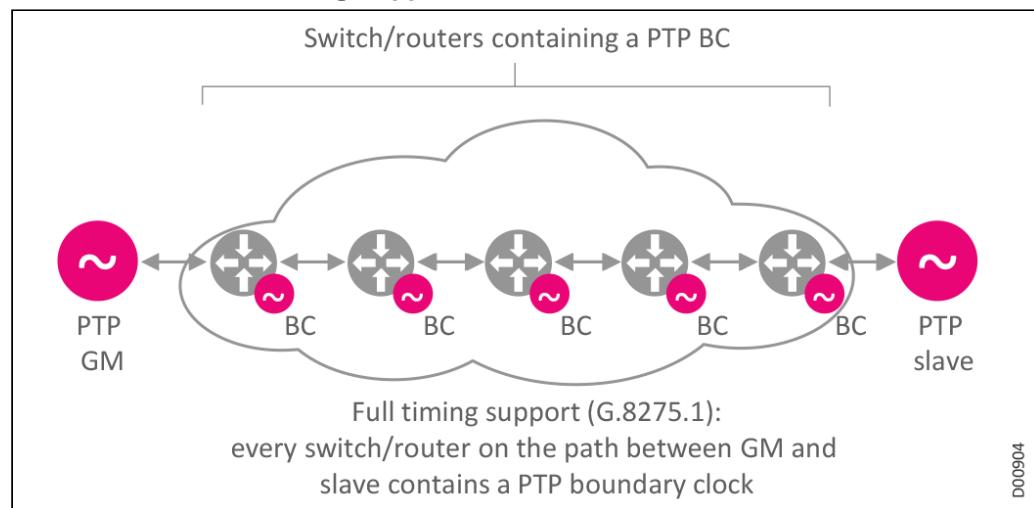
NPT-1022B/BH, NPT-1100/H, NPT-1250 (with MCIPS300FB/FBH and ECB\_1250B), NPT-2100, NPT-2300, and NPT-2400 platforms include a GNSS receiver sub-card built into the controller, receiving 1PPS/ToD from the satellites via the GNSS interface. The GNSS interface provides synchronization sources (1PPS & ToD) for T-GM and T-BC APTs.

## G.8275.1-G.8275.2 PTP Implementation

Mobile applications and location- based services require very accurate phase/time synchronization. For example, the new LTE-Advanced standard requires base station clocks to be in phase with accuracy in the range of 500 nanoseconds. This is essential to be able to efficiently operate eICIC and CoMP, and ensure 911-service in North America. This clock accuracy is difficult to achieve without on-path support, with backhaul networks participating actively in timing distribution. The exacting requirements led to the development of the PTP telecom profiles ITU-T G.8275.1 and G.8275.2, defining telecom profiles facilitating end-to-end frequency and phase synchronization across packet-based networks with on-path support.

ITU T G.8275.1, *Precision time protocol (PTP) telecom profile for phase/time synchronization with full timing support from the network*, provides the technical details necessary to implement IEEE 1588 PTP. The profile specifies the functions necessary to ensure network element (NE) interoperability and enable end-to-end delivery of accurate phase/time synchronization across packet based networks.

### ITU-T G.8275.1: Full Timing Support

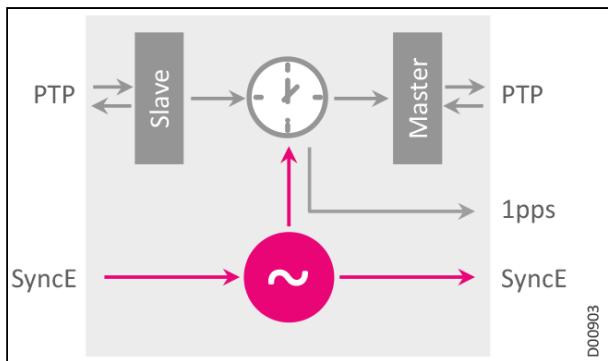


A BC may be configured with multiple network connections, and can therefore serve to accurately bridge synchronization between network segments. BCs improve the accuracy of clock synchronization by filtering network jitter and deliver better scale on the master.

G.8275.2 is a PTP profile for use in telecom networks where phase or time-of-day synchronization is required. It differs from G.8275.1 in that it defines a situation of *partial* timing support from the network. This means that the nodes using G.8275.2 do not have to be directly connected, since not every device in the network participates in the PTP protocol. G.8275.2 is used in mobile cellular systems that require accurate synchronization of time and phase, such as 4G mobile telecommunications technology. G.8275.2 uses PTP over IPv4 and IPv6 in unicast mode.

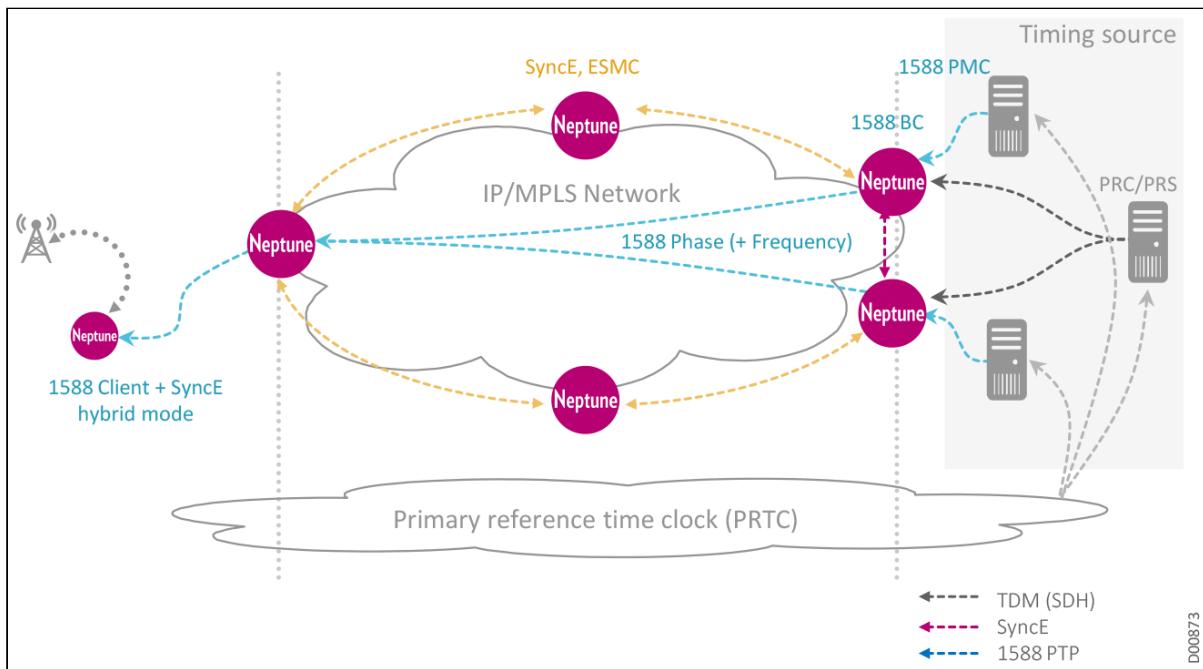
## Hybrid Architecture - Combining SyncE and 1588

### Hybrid Synchronization Solution



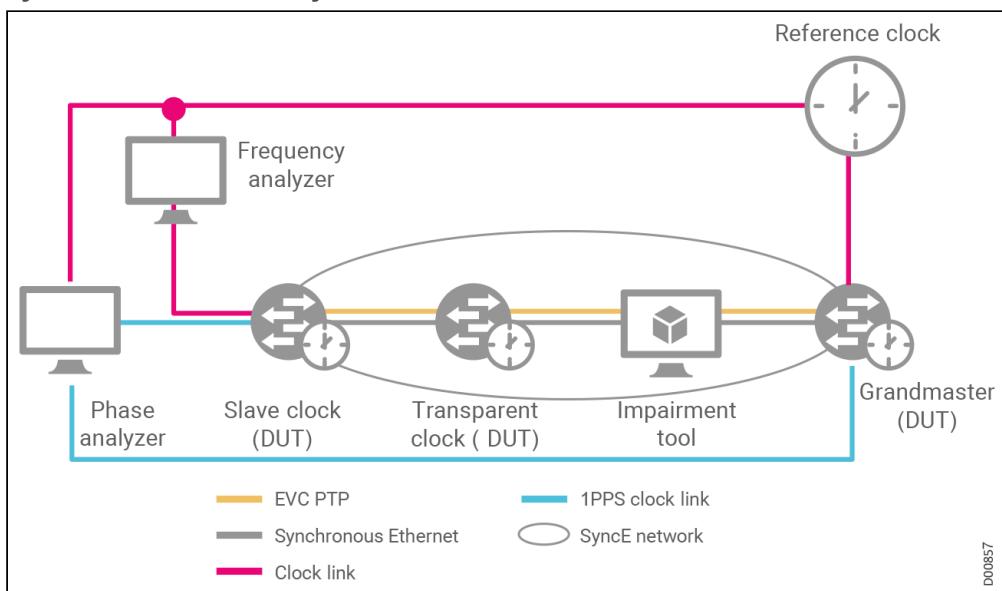
Neptune solutions support a combination of SyncE and 1588v2 in a hybrid synchronization architecture, aiming to improve the stability and accuracy of the phase and frequency synchronization delivered to the client for deployments such as Time Division Duplex (TDD)-LTE eNodeBs. In this architecture, the packet network infrastructure is frequency synchronized by SyncE. The phase signal is delivered by 1588-2008 PTPv2.

### Hybrid SyncE/PTP Architecture



The frequency source for the mobile backhaul network is the Primary Reference Clock (PRC), which can be based on a free-running atomic clock (typically Cesium), a global navigation satellite system (GNSS) receiver that derives frequency from signals received from one or more satellite systems, or a combination of both.

#### Hybrid Mode: PTP and SyncE



## Synchronization Summary Table

SyncE and PTP are supported over GbE/10GbE/100GbE and FlexE interfaces. The following table summarizes the synchronization and timing functionality supported by each of the Neptune platforms, when configured with the appropriate data cards. For a detailed specification of the card and platform combinations that support each type of timing and synchronization, see the *Neptune System Specification*.

**Neptune Timing and Synchronization Support**

Timing Interface	T3/T4 (BITS)	G N S S	10 M Hz	Sy nc E	1588v2 (PTP) G.8265.1	1588v2 (PTP) G.8275.1	1588v2 (PTP) G.8275.2	PTP class level	1PPS + ToD	Hybrid 1588 + SyncE	A P T S
NPT-1010	--	--	--	Yes	Yes	--	--	Class A	Yes	--	--
NPT-1010D	--	--	--	Yes	Yes	Yes	--	Class B	Yes	Yes	--
NPT-1012D (future)	--	Yes	--	Yes	Yes	Yes	Yes	Class C	Yes	Yes	Yes
NPT-1021	Yes	--	--	Yes	Yes	--	--	Class A	Yes	--	--
NPT-1022	Yes	--	--	Yes	--	Yes	--	Class C	Yes	Yes	Yes
NPT-1022H	Yes	--	--	Yes	--	Yes	Yes	Class C	Yes	Yes	Yes
NPT-1022B	--	Yes	--	Yes	--	Yes	--	Class C	Yes	Yes	Yes
NPT-1022BH	--	Yes	--	Yes	--	Yes	Yes	Class C	Yes	Yes	Yes
NPT-1050 (MCPS 100)	Yes	--	--	Yes	Yes	Yes	--	Class A	Yes	Yes	--
NPT-1050 (MCIPS 300)	Yes	--	--	Yes	Yes	Yes	--	Class B	Yes	Yes	--
NPT-1100	Yes	Yes	Yes	Yes	--	Yes	--	Class C	Yes	Yes	Yes
NPT-1100H	Yes	Yes	Yes	Yes	--	Yes	Yes	Class C	Yes	Yes	Yes

Timing Interface	T3/T4 (BITS)	G N S S	10 M Hz	Sy nc E	1588v2 (PTP) G.8265.1	1588v2 (PTP) G.8275.1	1588v2 (PTP) G.8275.2	PTP class level	1PPS + ToD	Hybrid 1588 + SyncE	A P T S
NPT-1200 (CPS100/ CPS320)	Yes	--	--	Yes	Yes	Yes	--	Class A	Yes	Yes	--
NPT-1200 (MCIPS / MCIPS 560)	Yes	--	--	Yes	Yes	Yes	--	Class B	Yes	Yes	--
NPT-1250 (MCIPS 300F)	Yes	--	--	Yes	--	Yes	--	Class C	Yes	Yes	--
NPT-1250 (MCIPS 300FH)	Yes	--	--	Yes	--	Yes	Yes	Class C	Yes	Yes	--
NPT-1250 (MCIPS 300FB)	--	Yes	Yes	Yes	--	Yes	--	Class C	Yes	Yes	Yes
NPT-1250 (MCIPS 300FBH )	--	Yes	Yes	Yes	--	Yes	Yes	Class C	Yes	Yes	Yes
NPT-1300	Yes	--	--	Yes	Yes	Yes	--	Class B	Yes	Yes	--
NPT-1800 (CIPS1T)	Yes	--	--	Yes	Yes	Yes	--	Class B	Yes	Yes	--

Timing Interface	T3/T4 (BITS)	G N S S	10 M Hz	Sy nc E	1588v 2 (PTP) G.826 5.1	1588v 2 (PTP) G.827 5.1	1588v2 (PTP) G.8275. 2	PTP class level	1PPS + ToD	Hybrid 1588 + SyncE	A P T S
NPT-1800 (CIPS2T)	Yes	--	--	Yes	--	Yes	Yes	Class C	Yes	Yes	Yes
NPT-2100	T3 only	Yes	Yes	Yes	--	Yes	Yes	Class C	Yes	Yes	Yes
NPT-2300	Yes	Yes	Yes	Yes	--	Yes	Yes	Class C	Yes	Yes	Yes

# Segment Routing

**Source routing** is defined as the ability for a node to specify a specific unicast-forwarding path that a particular packet should traverse, in situations where the specified path is different from the standard shortest path. It should be possible to implement this specified path using IGP-based MPLS tunnels, without a need to add any other signaling protocol for tunneling services (L3VPN, L2VPN) from ingress PE to egress PE, with or without an explicit path, and without requiring a specific forwarding plane or control plane state in the intermediate nodes.

**Segment Routing (SR)** allows the user to specify a path from ingress to egress, using a forwarding path that is completely abstract from the classic shortest path identified through IGP.

In the SR domain, nodes and links are assigned Segment Identifiers (SDIDs), which are advertised into the domain by each SR router using extensions to IS-IS/OSPF protocols. These SDIDs allow an ingress node to select a path through the network, using either a single SID to represent the destination node, or using a series of SDIDs, called a *segment list*, which specifies a particular path through the network that an SR tunnel should traverse.

SDIDs or segment lists can be encoded as one or more MPLS labels. SR does not require use of LDP and/or RSVP-TE transport signaling control plane. No state is maintained in the interim nodes of the network with the exception of the ingress SR router. This allows SR to scale significantly better than RSVP-TE, while providing most of the same functions. SR offers:

- IGP-based MPLS tunnels to L2VPN and L3VPN services with no need to add any other transport signaling protocol.
- Fast-Reroute (FRR) capability using a pre-computed backup path that can provide full coverage without any topology dependencies.
- Source routing based on a combination of loose and/or strict hops. SR allows for centralized or distributed traffic engineering models with most of the capabilities of RSVP-TE, including Admin-Groups and Shared Risk Link Groups, without requiring an associated midpoint state.

While SR enables building the forwarding paths across the network, some abstract intelligence is required to instruct ingress routers which paths to use through the network, for which services. An external traffic-engineering controller may deliver this intelligence.

This section introduces the following features:

- [SR Implementation](#)
- [Segment Identifiers SID](#)
- [SR with BGP](#)
- [Topology Independent Loop-Free Alternate FRR TI-LFA](#)
- [SR Applications](#)
- [SR and LDP Interworking: Ships in the Night](#)
- [SR Advantages](#)

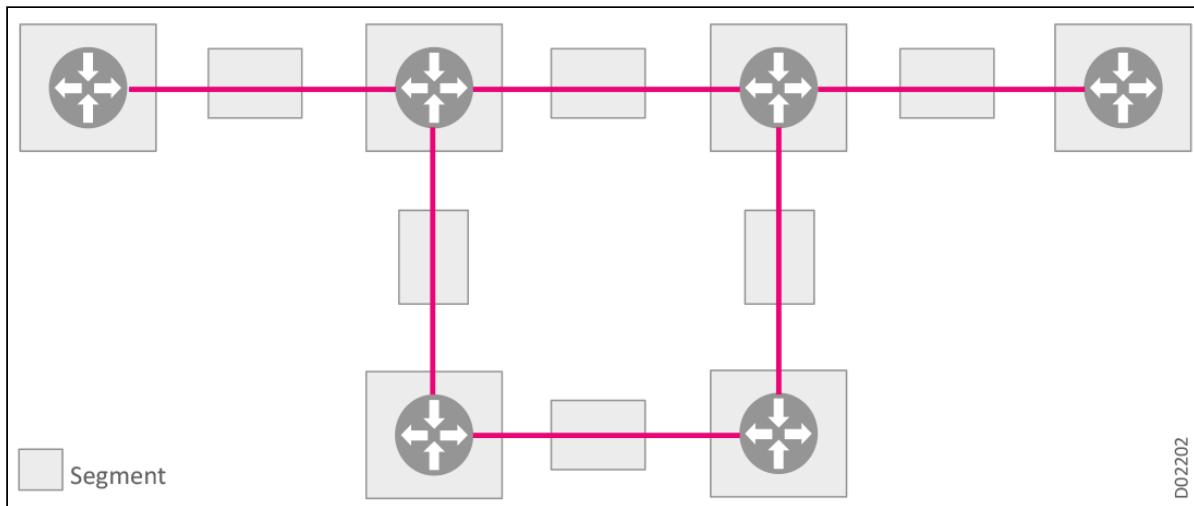
## SR Implementation

SR provides a tunneling mechanism that enables source routing in IP/MPLS networks. An SR path (SR tunnel) is encoded as a sequential list of sub-paths called **segments**, which are advertised to the SR domain using extensions to link-state routing protocols such as IS-IS or OSPF.

An SR tunnel can contain:

- A single segment, in the form of an MPLS label that represents the destination node
- A list of segments, where the list represents the set of segments that a given tunnel must traverse, in the form of an ordered list of hops represented as a stack of labels, with no change to the MPLS data plane

## SR Domain



MPLS is used to instantiate SR tunnels; no change is required for the MPLS forwarding plane. SR uses extensions to the link-state IGP to propagate SIDs in the form of MPLS labels. When SR is instantiated over the MPLS data plane, the following actions apply:

- A list of segments is represented as a stack of labels.
- The active segment is the top label.
- The CONTINUE operation is implemented as an MPLS swap operation.
- The NEXT operation is implemented as an MPLS pop operation.
- The PUSH operation is implemented as an MPLS push operation.

No LDP control plane is required, although you can utilize LDP in conjunction with SR; because the LDP label spaces do not overlap, they do not affect each other.

## Segment Identifiers SID

Each SID is a 32-bit entity with the MPLS label encoded as the 20 right-most bits of the segment. In an SR domain, different types of SIDs are defined, depending on the type of node and link requirements, to enable efficient SR implementations.

### Prefix-SID

A Prefix-SID is globally unique within the IGP/SR domain. The SID value is allocated from a unique pool called the SR Global Block (SRGB). A Prefix-SID is allocated in the form of an index in the SRGB.

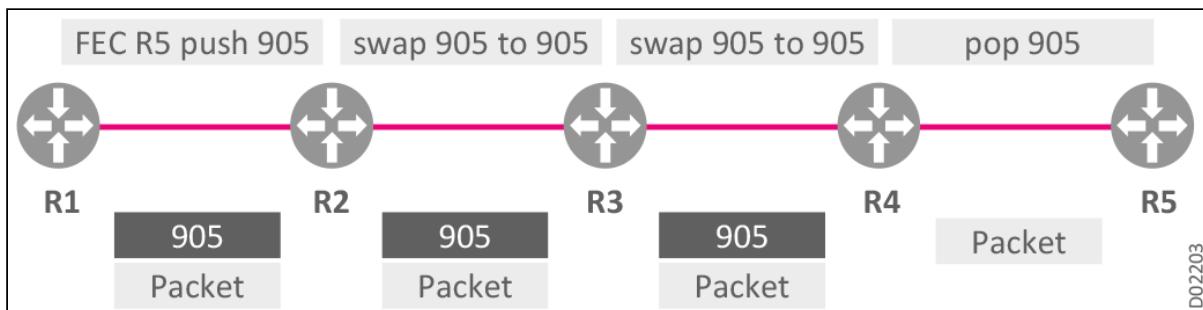
In an MPLS network, the SRGB is a set of labels reserved specifically for SR use. A Prefix-SID is actually a MPLS label allocated from the SRGB MPLS label pool, where the label value is simply the Prefix-SID index combined with the SRGB base. The Prefix-SID represents the Equal Cost Multi-Path (ECMP)-aware shortest-path route to the related prefix and is typically a multi-hop path.

### Node-SID

A Node-SID is a special type of Prefix-SID, used to identify a particular router (node segment) in the domain. An N flag indicates this is a Node-SID. This flag is set to 1 in the Prefix-SID sub-TLV that IS-IS or OSPF uses to advertise the SID. Because the Node-SID is also a Prefix-SID, it also represents the ECMP-aware shortest-path route to the related prefix, typically a multi-hop path. When an SR router advertises its Node-SID to the SR domain, all routers in the domain install the node segment in the data-plane.

### Example: Working within the same SRGB

### SR Tunnel with a Single SRGB



In this example, all the participating routers are included within an SRGB that begins with 900. Router R5 advertises a Node-SID as an index 5 to the SR domain. When Router R1 wants to forward a SR tunnel-encapsulated packet towards Router R5, it PUSHES the node segment label {905 = 900 + 5} on the top of packet and forwards the packet using its shortest-path towards Router R5. Routers R2 and R3 each implement a SWAP action in the data plane.

In this example, Router R4 also implements a SWAP action. R4 may also implement a POP action if the egress router has the P flag set to 0 in its advertised Prefix-SID Sub-TLV. This behavior is analogous to Penultimate Hop Popping (PHP) in MPLS.

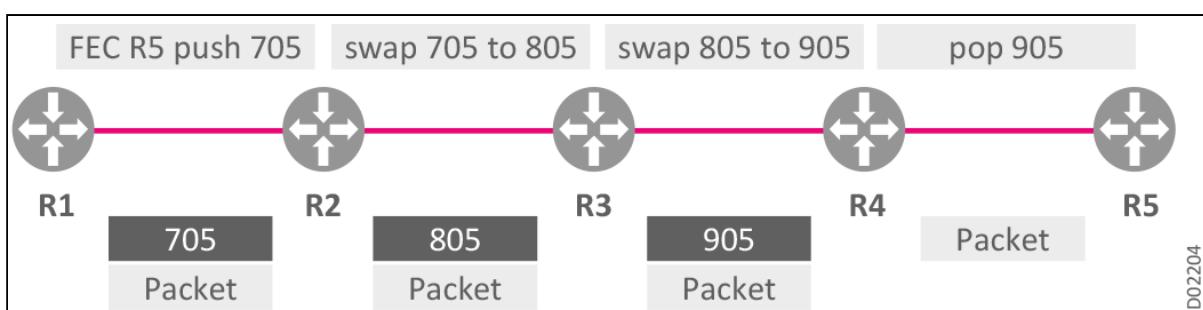
### Example: Working with different SRGBs

The following figure illustrates an SR tunnel with the Node-SID indicating different SRGBs for the various intra-tunnel routers. Router R2's SRGB begins with 700, Router R3's SRGB begins with 800, and Router R4's SRGB begins with 900.

As a result, Routers R2, R3, and R4 execute operations on the packet directed to R5 as follows:

- R2 swaps from 705 to 805
- R3 swaps from 805 to 905
- R4 pops 905

### SR Tunnel with Different SRGBs



### Adjacency-SID

An Adjacency Segment (Adj-SID) is a segment that identifies an adjacency to another router, where the other router is known in the IGP, and the link connecting the two routers is specified. The value of an Adj-SID is local to the router that advertises it. Since every SR router in the domain can potentially use the same segment (label) space, therefore only the advertising router can install an Adj-SID in the LFIB for forwarding decisions.

For example, a packet injected anywhere within the SR domain with a segment list {SN, SNL}, where SN is the Node-SID of node N and SNL is an Adj-SID attached by node N to its adjacency over link L, will be forwarded along the shortest-path to N and then be switched by N towards link L, without any IP shortest-path consideration.

An Adj-SID enforces the switching of the packet from a node towards a defined interface. This is a key element to theoretically prove that any path can be expressed as a list of segments. Therefore, for an effective implementation, a node should allocate one Adj-SIDs for each of its adjacencies.

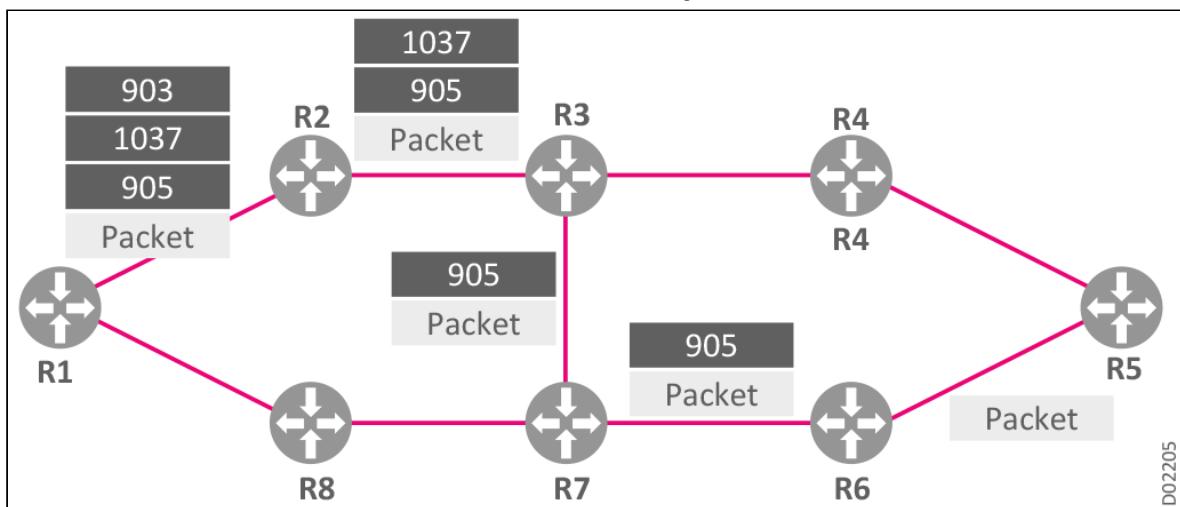
Adj-SIDs can be used to define a source-routed explicit hop-by-hop path from ingress to egress. However, constructing lists using only Adj-SIDs can potentially create a deep segment list depth (in the case of an MPLS data plane, deep label stack). An alternative method is to combine Node-SIDs and Adj-SIDs to identify ECMP paths to the next specified Node-SID in the segment list, and to enforce only the use of a particular link from that node as relevant.

#### Example: SR tunnel based on a combination of Node-SID and Adj-SID

The following figure illustrates a network example in which Router R1 must configure an SR tunnel to Router R5, with the constraint that the tunnel must pass through the R3-to-R7 link and avoid the R3-to-R4 link. Router R1 therefore imposes the segment list {903, 1037, 905} as follows:

- Node-SID for R3
- Adj-SID for link R3-to-R7 - local for R3
- Node-SID for R5

#### SR Tunnel Based on Combination of Node-SID and Adj-SID



#### Anycast-SID

An "Anycast Segment" or "Anycast SID" enforces the ECMP-aware shortest-path forwarding towards the closest node of the anycast set. This is useful when implementing protection mechanisms.

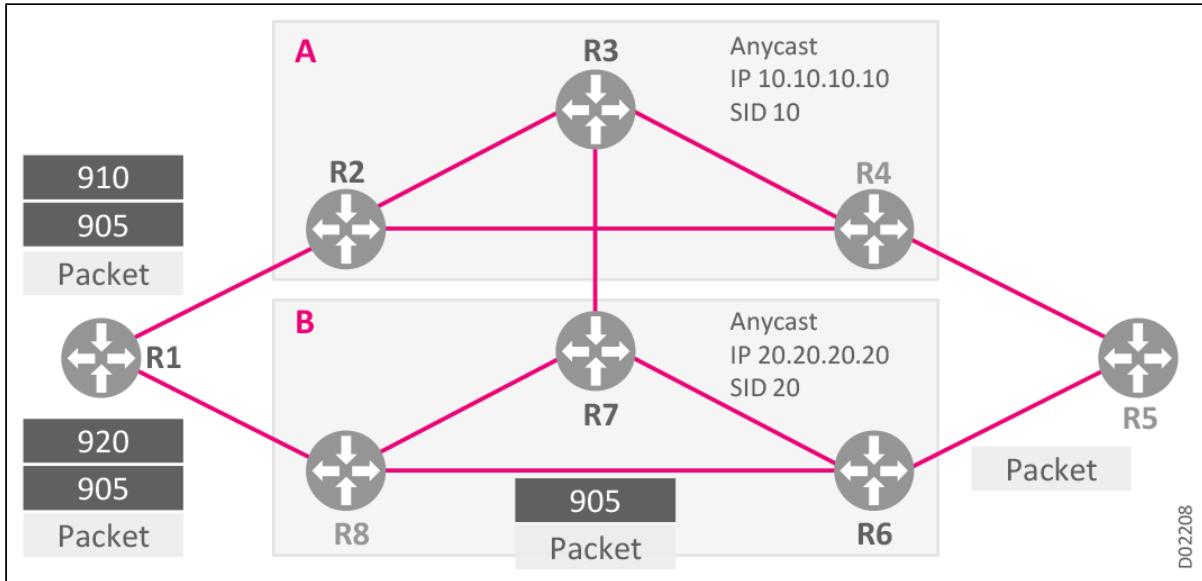
An Anycast SID cannot reference a particular node. Within an anycast group, all routers will advertise the same prefix with the same SID value. Since an anycast prefix may be owned by more than one router, it cannot be advertised as a Node-SID.

#### Example: Anycast SID usage

The following figure illustrates a network example with two groups of transit devices.

- Group A consists of devices {R2, R3, R4}. They are all provisioned with the anycast address 10.10.10.10, SID 10.
- Group B consists of devices {R8, R7, R6}. They are all provisioned with the anycast address 20.20.20.20, SID 20.

### Anycast SID Example



## SR with BGP

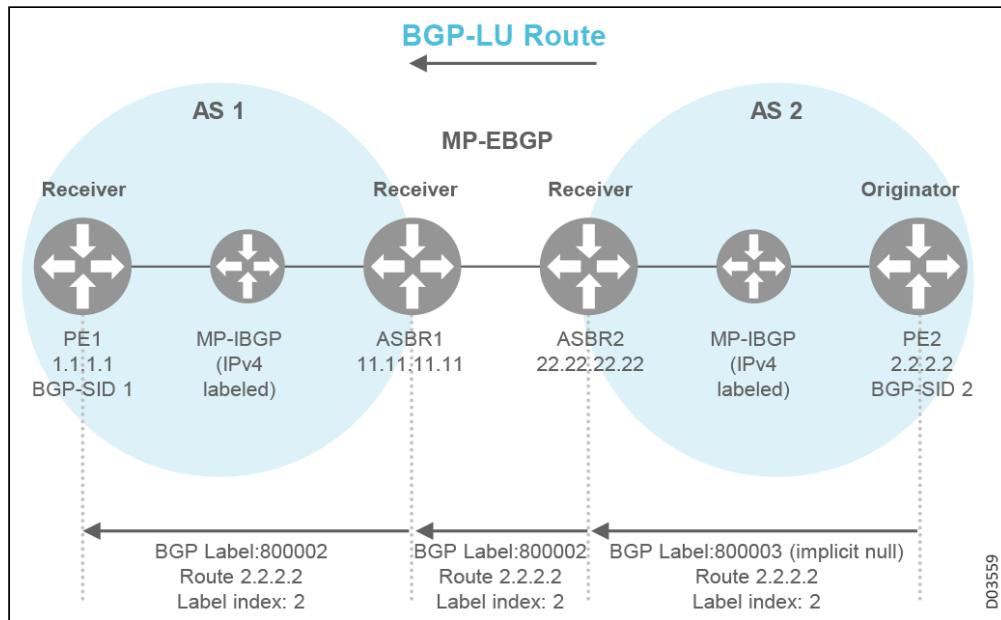
IETF has released [draft-ietf-idr-bgp-prefix-sid-27](#), part of <https://www.rfc-editor.org/info/rfc8669>, describing the SR prefix segment identifier extensions to use when working with BGP.

Segments are identified through a **Segment Identifier (SID)**. An "SR domain" is defined as a single administrative domain for global SID assignment. It may be comprised of a single Autonomous System (AS), or composed of multiple ASs under consolidated global SID administration. Typically, the ingress node of the SR domain prepends an SR header containing SIDs to an incoming packet. When segment routing is applied to the *MPLS data plane*, the SID consists of a label. (Segment routing can also be applied to an *IPv6 data plane* (SRv6), using an IPv6 routing header containing a stack of SR SIDs encoded as IPv6 addresses).

Segments associated with a BGP Prefix are called **BGP Prefix Segments**. These segments are identified with a **BGP-Prefix SID**. A BGP Prefix-SID is always a global SID ([[RFC8402](#)]) within the SR domain. The BGP Prefix-SID identifies the instruction to follow when forwarding the packet over the best path computed by BGP to the related prefix. BGP must know the Segment Routing Global Block (SRGB); the BGP-Prefix SID is an offset value from the SRGB, and is also known as the Label Index.

A BGP Prefix-SID will be global across autonomous systems (AS) when the interconnected ASs are part of the same SR domain. Alternatively, when interconnecting ASs, the ASBRs of each domain will have to handle the advertisement of unique SIDs.

### BGP Prefix SID: Example



In this example:

- PE2 is the originator of the BGP-LU route (2.2.2.2). The BGP-PREFIX-SID attribute is set to 2.
  - ASBR2 receives BGP LU with a PREFIX SID attribute and an implicit null.
  - ASBR2 uses an MP-EBGP to advertise calculated label 800002 for this route to ASBR1.
  - ASBR1 assigns label 800002 to this route and changes the next-hop address to its own address. It then advertises this label to PE1.
  - PE1 is the ingress router of this LSP. The BGP-LU outgoing label is 800002 and the next-hop is ASBR1.
- Next-hop resolution to ASBR1 may be done by any available LSP based on the local policy on PE1.

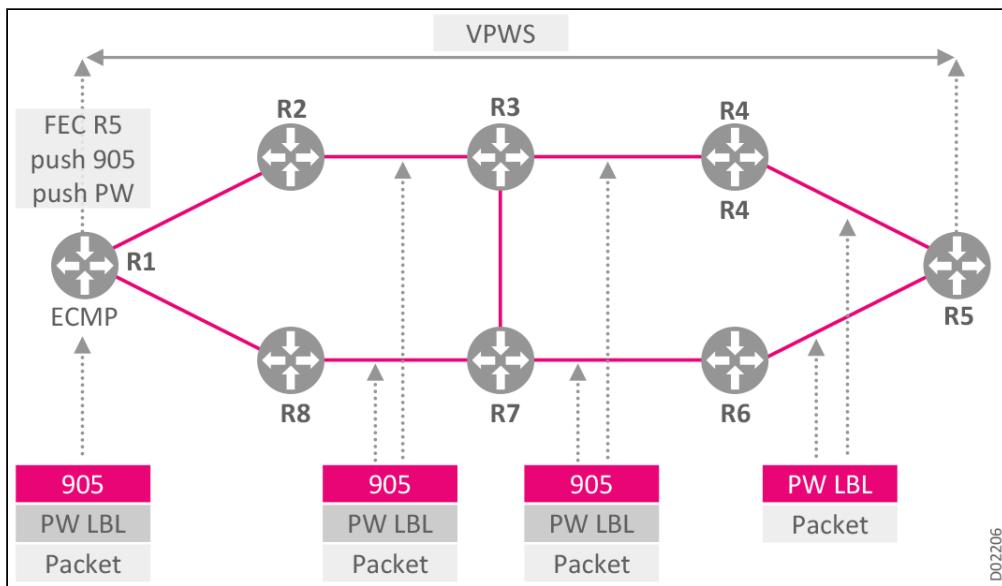
## Topology Independent Loop-Free Alternate FRR TI-LFA

Topology Independent Loop-free Alternate (TI-LFA) Fast Re-route (FRR) is aimed at providing protection for node and adjacency segments within the Segment Routing (SR) framework. This Fast Re-route (FRR) behavior builds on proven IP-FRR concepts, including LFAs, remote LFAs (RLFA), and remote LFAs with directed forwarding (DLFA). TI-LFA extends these concepts to provide guaranteed coverage in any IGP network. A key aspect of TI-LFA is the FRR path selection approach, establishing protection over post-convergence paths from the point of local repair, dramatically reducing the operational need to control the tie-breaks among various FRR options. TI-LFA provides:

- Protection upon local link, node, or SRLG failure
  - Simple to operate and understand
  - Automatically computed by the router's IGP process (ISIS and OSPF)
  - 100% coverage across any topology
  - Predictable (backup = postconvergence)
- Optimum backup path
  - Leverages the post-convergence path, planned to carry the traffic
  - Avoid any intermediate flap via alternate path
  - Incremental deployment
  - Also protects LDP and IP traffic

## SR Applications

### L2VPN using SR Tunnels

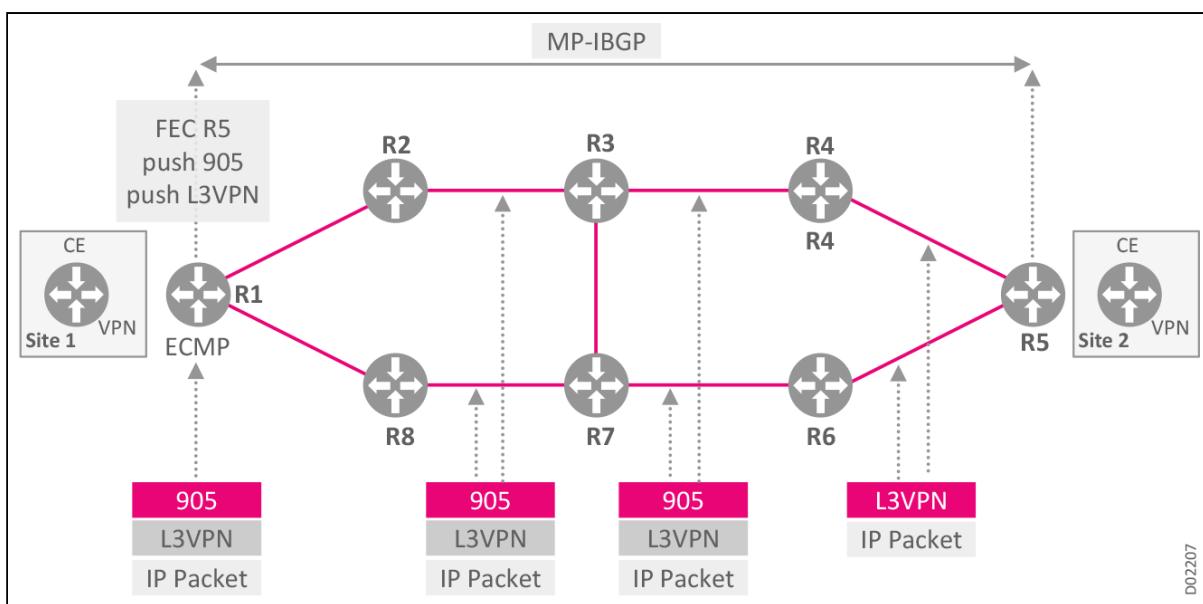
**VPWS**

In this example, R1 and R5 are PE routers and endpoints for an L2VPN (VPWS) service. These routers are working with targeted LDP for service label exchange. R1 and R5 are also SR routers. Note that in this example, all of the SR routers in the domain use a single consistent SRGB beginning with 900.

The SR routers in the domain install a PUSH entry and a swap entry for the advertised prefix/label 905 in the LFIB. For L2 traffic from R1 to R5:

- R1 pushes on packet label 905 and uses its shortest IGP path to reach R5.
- R1 also pushes the L2VPN service label (PW LBL) received from the R5-targeted LDP.

Multiple SR tunnels (SR-TE) may be running between service endpoints. LDP tunnels may also exist between the service endpoints. In all these cases, the choice of service tunnels is a local matter decided at the head-end.

**L3VPN using SR Tunnels****L3VPN Service**

D02207

In this example, R1 and R5 are PE routers and endpoints for an L3VPN service. These routers are working with MP-BGP for service label exchange. R1 and R5 are also SR routers. Note that in this example, all of the SR routers in the domain use a single consistent SRGB beginning with 900.

The SR routers in the domain install a PUSH entry and a swap entry for the advertised prefix/label 905 in the LFIB. For IP traffic from R1 to R5:

- R1 pushes on packet label 905 and uses its shortest IGP path to reach R5.
- R1 also pushes the BGP service label (L3VPN) received from the R5 MP-IBGP session.

A preference policy must be defined for multiple tunnels between the L3VPN endpoints.

## SR and LDP Interworking: Ships in the Night

SR and LDP can both be present and co-exist on all network elements. If multiple MPLS control plane protocols (i.e., both LDP and SR) install forwarding entries into the MPLS data-plane, those entries must be unique in order to function as 'ships in the night'.

Preference for LDP or SR for service tunnels is a local matter, defined at the head-end. By default, if both LDP and SR propose an MPLS entry for the same IP prefix, then the LDP route is selected. A local policy can be defined on a router to enable preference for the SR-provided MPLS entry. There is no requirement that all routers use the same policy.

When SR is only present in parts of the network, LDP and SR can be interworked to provide an end-to-end tunnel through the use of an SR Mapping Server (SRMS).

## SR Advantages

SR has evolved into a fundamental architecture for modern IP networks, positioned by the industry as 'the de-facto SDN network architecture'. SR provides significant advantages for modern IP networks, including:

- **Sophisticated combination of simplicity and functionality:** solving unsolved problems
  - Implemented through lightweight extensions to core IP control-plane protocols (BGP, ISIS, OSPF, PCEP)
  - Elimination of unnecessary protocols (LDP, RSVP-TE)
  - End-to-end policies through domains both external and internal to the SP, avoiding issues of disjointedness and low-latency
  - Application controls the network, without the complexity and performance-impact of PBR/DPI
  - SRTE algorithm, either local to the router or defined for the centralized PCE
  - On-demand SR next-hop
  - Intelligent automation, including:
    - Automatic local protection, per prefix, for any topology, within less than 50msec (TI-LFA)
    - Automatic uloop avoidance
    - Automatic traffic matrix
- **Smooth scaling capabilities**
  - No SR-TE midpoint states
  - No SR-TE head-end configuration (on-demand SR next-hop)
  - Binding SID for compressed SID list length
  - Seamless deployment
    - SR/LDP interworking
    - SR/RSVP-TE interworking (binding SID)
    - Ships-in-the-night co-existence
    - SW upgrades enable reuse of existing HW platforms
- **Decoupling data and control planes**
  - Architecture designed to natively accommodate decoupled data and control planes

# IP-MPLS Technology

This section introduces IP/MPLS technology, including the following sections:

- Understanding MPLS-TP
- Understanding IP-MPLS
- IP Routing for IP-MPLS
- Understanding IPv4
- Understanding IPv6
- Understanding Subnetworks
- Supporting Multiple IP Addresses
- IP Networking in the Control Plane
- Switching and Routing
- Processing Inbound Packets
- MPLS-TP and IP-MPLS Interworking Models
- DHCP Relay Agent and Option 82

## Understanding MPLS-TP

**Ethernet service**, the preeminent LAN technology, is now becoming the dominant service for the metro domain (WAN) as well. Consumers require guaranteed service delivery of the appropriate quality, expecting operators to provide differentiated services with comprehensive carrier class capabilities, from access to core.

**MultiProtocol Label Switching (MPLS)** is a mechanism for transporting data using a connection-oriented approach. Standardized by the IETF, MPLS is a scalable protocol-agnostic mechanism designed to carry both circuit and packet traffic over virtual circuits known as LSPs. MPLS fits into the category of packet-switched networks, falling in between the traditional OSI definitions of the Data Link Layer (Layer2) and the Network Layer (Layer3). MPLS makes packet-forwarding decisions based on the contents of the label without examining the packet itself.

MPLS provides a unified data-carrying service for circuit-like packet-switching client data. MPLS can be used to carry many different kinds of traffic, including IP packets, native ATM, and Ethernet frames. MPLS has gradually been replacing traditional transport technologies, such as frame relay and ATM, mostly because it is better aligned with current and future technology needs.

**MPLS Transport Profile (MPLS-TP)** is an MPLS profile defined under the auspices of the IETF and ITU-T. The MPLS-TP standard defines a list of features most relevant for transport networks, and to support packet transport services with a degree of predictability similar to that found in traditional transport networks.

MPLS-TP is a connection-oriented packet-switched (CO-PS) application for Layer2 transport network technology that incorporates elements of both MPLS and PW architectures, such as the MPLS forwarding paradigm and PW Emulation Edge to Edge (PWE3) client mapping. MPLS-TP is based on the same architectural principles of layered networking used in transport network technologies like SDH, SONET, and OTN. MPLS-TP extends IP/MPLS beyond the core network into the metro network, providing reliable packet-switching transport between these networks. MPLS-TP simplifies MPLS by eliminating elements of MPLS that are not necessary in a transport-oriented network.

MPLS-TP is a low-cost Layer 2 technology that provides QoS, end-to-end OAM, and protection switching. Additional mechanisms supporting critical transport functionality were added, including supplemental OAM, resiliency, bidirectional LSPs, protection schemes, and control/management features that enable maximum synergy with existing optical transport network operations and management paradigms.

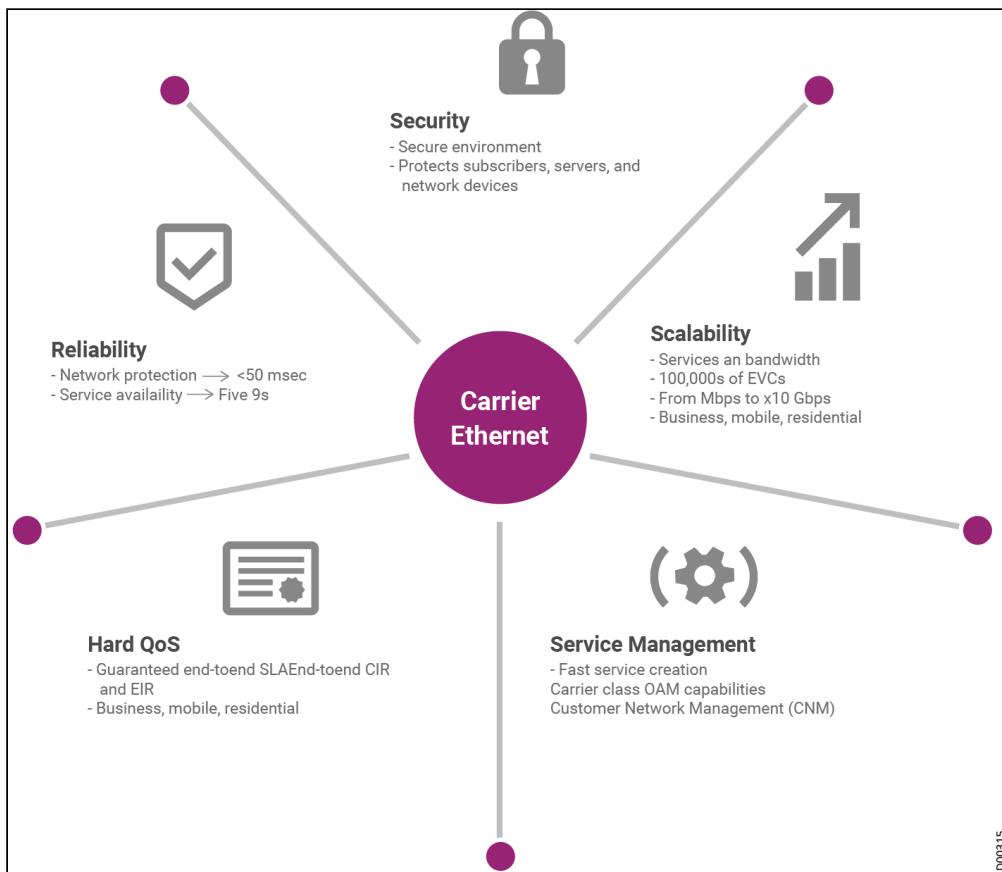
The MPLS-TP protocol enables more affordable end-to-end MPLS deployments by streamlining operations models and consolidating/simplifying network topologies. For example, one of the key elements is eliminating the costs associated with distributed control plane functionality being integrated into each node across an MPLS-based network. This is accomplished through the use of a more affordable transport-oriented static

configuration through a transport-grade NMS, helping operators reduce their OPEX significantly and get networks ready to offer true NG service convergence.

MPLS-TP as a transport layer for metro Carrier Ethernet services, rather than using Ethernet as both transport and service layers, enhances the Ethernet service, enabling it to meet a complete carrier class standard. MPLS-TP addresses all key attributes defined by MEF for Carrier Ethernet:

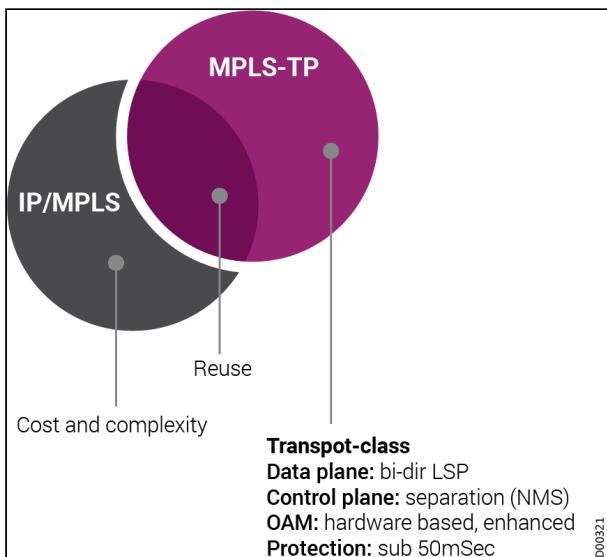
- **Hard Quality of Service (QoS)**, with guaranteed end-to-end Service Level Agreements (SLAs) for business, mobile, and residential users that enables efficient differentiated services, allowing service providers (SPs) to tailor the level of service and performance to the requirements of their customers (real-time, mission-critical, BE, etc.), as well as assuring the necessary network resources for Committed Information Rate (CIR) and Extended Information Rate (EIR).
- **Reliability**, with a robust, resilient network that can provide uninterrupted service across each path. This includes network protection of less than 50msec, meeting a five 9s standard of end-to-end service availability.
- **Scalability** of both services and bandwidth, ranging from megabits to hundreds of gigabytes with variable granularity and hundreds of thousands of flows supporting controlled scalability for both the number of elements and the number of services on the network.
- **End to End Service Management** through a single comprehensive Network Management System (NMS) that provisions, monitors, and controls many network layers simultaneously. Advancement in the management of converged networks takes advantage of the "condensed" transport layer for provisioning and troubleshooting while presenting operators with tiered physical and technology views that are familiar and easy to navigate. The comprehensive NMS simplifies operations by allowing customers and member companies to monitor and/or control well-defined and secure resource domains with partitioning down to the port.
- **Security**, with a safe environment that protects subscribers, servers, and network devices, blocking malicious users, Denial of Service (DoS), and other types of attacks. Use of provider network constraints, as well as complete traffic segregation, ensures the highest level of security and privacy for even the most sensitive data transmissions.

## Carrier Class Ethernet Requirements



MPLS-TP is both a subset and an extension of MPLS, already widely used in core networks. It bridges the gap between packet and transport worlds by combining the efficiency of packet networks with the reliability, carrier-grade features, and OAM tools traditionally found in SDH/SONET transport networks. MPLS-TP builds upon existing MPLS forwarding and MPLS-based pseudowires, extending these features with in-band active and reactive OAM enhancements, deterministic path protection, and a network management-based static provisioning option.

### Relationship of MPLS-TP to IP/MPLS



As part of MPLS, MPLS-TP falls under the umbrella of the IETF standards (relevant standards are listed in the System Specifications). MPLS-TP is supported across product lines, enabling end-to-end QoS assurance across network domains.

## Understanding IP-MPLS

**MultiProtocol Label Switching (MPLS)** is a mechanism for transporting data using a connection-oriented approach. MPLS is a routing technique that directs network packets from one node to the next based on labels rather than network addresses. While network addresses identify the destination nodes (endpoints), labels identify the nodes along an established path between the endpoints. In an MPLS network, labels are assigned to data packets. Packet-forwarding decisions are based on the label contents, with no need to examine the packet contents. You can create end-to-end circuits across any type of transport medium. It is called *Multiprotocol* because it supports multiple protocols like Internet Protocol (IP), Asynchronous Transport Mode (ATM), and Frame Relay protocols. Network packet forwarding is based on the label present on the packet; that's why it is called Label Switching.

Standardized by the IETF, MPLS is a scalable protocol-agnostic mechanism designed to carry both circuit and packet traffic over virtual circuits known as LSPs. MPLS fits into the category of packet switched networks, falling in between the traditional OSI definitions of the Data Link Layer (Layer 2) and the Network Layer (Layer 3), and thus is often referred to as a *layer 2.5* protocol.

MPLS can be used to carry many different kinds of traffic, including IP packets (**IP/MPLS**), as well as native ATM, E1/T1, Frame Relay, DSL, Synchronous Optical Networking (SONET), and Ethernet frames. MPLS was created in the late 1990s as a more efficient alternative to traditional Internet Protocol (IP) routing, which requires each router to independently determine a packet's next hop by inspecting the packet's destination IP address before consulting its own routing table. This process consumes time and hardware resources, potentially resulting in degraded performance for real-time applications, such as voice and video. In an MPLS network, the first router to receive a packet determines the packet's entire route upfront, the identity of which is quickly conveyed to subsequent routers using a label in the packet header.

MPLS also has very attractive features such as VPNs at both Layer 2 and 3 levels. The beauty of IP/MPLS is that companies can extend a LAN across vast distances, thereby connecting remote offices as if they were conjoined. Similarly, they could support VPNs at Layer 3 by connecting remote offices, third parties, and partners using address routing, regardless of the private address scheme used by each entity. For example, one office could use private address space of 172.16.10.x and another remote office could be assigned the same, but with MPLS, they could both communicate without having to readdress their respective IP schemes.

MPLS works in conjunction with the **Internet Protocol (IP)** and its routing protocols, usually **Interior Gateway Protocols (IGPs)**. MPLS LSPs provide dynamic, transparent virtual networks that offer:

- Traffic engineering
- Ability to transport Layer 3 (IP) VPNs with overlapping address spaces
- Support for Layer 2 pseudowires using PseudoWire Emulation Edge-to-Edge (PWE3)

These virtual networks are capable of transporting a variety of transport payloads (IPv4, IPv6, ATM, Frame Relay, etc.). MPLS-capable devices are referred to as LSRs. The paths an LSR knows can either be defined using explicit hop-by-hop configuration, or dynamically routed by a constrained shortest path first (CSPF) algorithm, or configured as a loose route that avoids a particular IP address or that is partly explicit and partly dynamic.

In a pure IP network, the shortest path to a destination is chosen even when the path becomes congested. In an IP network with MPLS Traffic Engineering and CSPF routing, constraints such as the RSVP bandwidth of the traversed links can also be considered, which means the shortest path with *available bandwidth* will be chosen. MPLS Traffic Engineering relies upon the use of TE extensions to Open Shortest Path First (OSPF) or Intermediate System To Intermediate System (IS-IS) and RSVP. Users can also define their own constraints by specifying link attributes and special requirements for tunnels to route (or not to route) over links with certain attributes.

MPLS can exist in both an **IPv4** and an **IPv6** environment, using the appropriate routing protocols. Currently, the main application of MPLS is implementing traffic engineering and Layer 3 / Layer 2 “service provider type” VPNs over IP networks.

## IP Routing for IP-MPLS

IP/MPLS networks implement IP routing through a network architecture composed of hosts, routers, and the interfaces used to communicate between them. This section provides a general overview of the basic elements of IP routing.

*IP interfaces* are logical channels for sending and receiving IP packets within IP networks. IP interfaces can be explicitly associated with one or more IP address. The IP address of an interface is 'owned' by the associated node, where each host and each router in the network must 'own' at least one IP address.

*Hosts* are connected to one or more networks via IP interfaces. A host handles both remote and locally-generated IP packets. These packets are received, processed, and transmitted based on its routing table. The RIB is populated by local and static routes.

*Routers* are connected to multiple networks via IP interfaces. A router forwards IPv4 packets based on its FIB, and runs routing protocols to populate its RIB.

The IP stack is the software component that handles the network and transport layers of the protocol stack. The IP stack also includes the socket interface, facing towards the upper level protocols and applications in the protocol stack, as well as the interface drivers, facing towards the media elements. The network and transport layers include the following elements:

- Network layer
  - Interfaces
  - IP forwarding (enabled/disabled)
  - Routing instances
  - Routing information base (RIB)
  - IP 'helper protocol' layer (ARP, IPCP)
- Transport layer
  - UDP
  - TCP

In IP networks, a *route* defines the path used to reach a specific location, identified by a packet prefix. This is indicated through a contiguous bit-string within the address. The *route metric* is a logical concept that defines which route is given preference out of a group of routes all leading to the same location. For example, the route metric might specify that the preferred path is the one with the shortest number of hops.

A *local route* defines the path to a directly-connected subnet or node. The local route is associated with the subnets of numbered interfaces, or with P2P interfaces. By contrast, a *remote route* defines how to reach a 'remote' location, accessible only through another (Next Hop) router. Next-hop routers maybe either *local next hop*, meaning a next hop router that is directly connected to this node via one of the node interfaces, or *remote next hop*, meaning a next hop router that is *not* directly connected to this node, and is only reachable via some other local next hop.

A *routing policy* defines an organized set of control plane rules and associated actions. For example, a routing policy might define the redistribution of routes between different routing protocols. Specific protocols are configured with specific routing policies defining their export and import actions. A routing policy *rule* can include multiple parameters for a route, such as the destination, the protocol on which the route is based, relevant tags, etc. A policy *action* is the action that is applied, such as accept, reject, tag, etc. For example, a tag assigned by a routing policy in one node is distributed with that route and may be used by a routing policy in another node.

Neptune platforms support use of 31-bit prefixes on IPv4 P2P links, as per RFC 3021, enabling the operator to conserve IP address space and improve numbering efficiency.

## Understanding IPv4

IPv4 is the common name for Version 4 of the Internet Protocol, the version that is currently the most commonly used in networks. IPv4 was the primary version deployed for general use through ARPANET in 1983. IPv4 addresses are 32-bit integers, usually expressed in dotted-decimal format, with four numbers separated by periods, such as 192.168.123.132. It uniquely identifies a host (computer or other device, such as a printer or router) on a TCP/IP network.

A TCP/IP wide area network (WAN) is essentially a collection of networks. The routers that pass packets of data between these networks work on an efficient, need-to-know basis. The routers don't need to know the exact location of a packet's specific host destination. They only need to know what network the host is a member of, using information stored in their route table to determine how to get the packet to the destination host's network. After the packet is delivered to the destination's network, the packet is delivered to the appropriate host.

Therefore, an IPv4 address (192.168.123.132) is divided into the following parts.

- Network address: Identifies the network (192.168.123.0 in our example)
- Host address: Identifies the host device in this network (0.0.0.132 in our example). For each host device in the network, the network address is the same, but the host part must be unique to each machine.
- Subnet number: This part of IPv4 is optional. Local networks that include massive numbers of hosts are divided into [subnetworks](#); the subnet numbers are assigned accordingly. The subnet mask is used by the TCP/IP protocol to determine whether a host is on the local subnet or on a remote network; see [Understanding Subnetworks](#) for more information.

IPv4 addresses can be used for unicast, broadcast, and multicast addressing. IPv4 uses the Post Address Resolution Protocol to map the MAC address. IPv4 security permits encryption to keep up privacy and security.

IPv4 routes most of today's internet traffic. A 32-bit address space limits the number of unique hosts to 2<sup>32</sup>, which is nearly 4.3 billion IPv4 addresses for the world to use (4,294,967,296, to be exact). However, in today's world of ultra-connected computer networks, where every stationary and mobile device now has an IP address, it turns out that 4.3 billion of them isn't nearly enough.

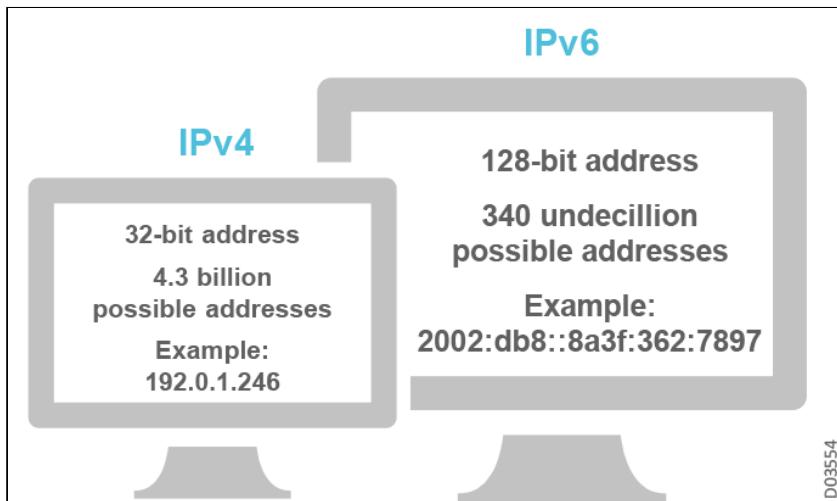
In 2011, the Internet Assigned Numbers Authority (IANA), the global coordinator of IP addressing, ran out of free IPv4 address space to allocate to regional registries. IANA then recovered additional unused IPv4 address blocks from the regional registries and created a recovered address pool. In 2014, IANA announced that it was redistributing the last addresses in the recovered address pool. When it's tapped, there will be no more IPv4 addresses left.

Besides running out of address space, the IPv4 addressing system has some additional downsides:

- About 18 million addresses were set aside for private addressing, drawn from a range known as RFC 1918. Most organizations use private addresses on internal networks. However, devices on these local networks have no direct path to the public internet. To access the public internet, devices with private addresses require a complex and resource-intensive workaround called network address translation (NAT).
- Historically, North America received the largest subset of IPv4 address allocations. As a result, entities in Asia-Pacific and elsewhere, where internet use has exploded, have had to purchase large chunks of IP space on the gray market. This has resulted in the breaking of contiguous ranges of IP addresses, making it more complicated to route internet traffic.

For all these reasons, the internet is gradually transitioning to IPv6. IPv6 moves internet addressing from 32 bits to a 128-bit address space, with both letters and numbers in the identifiers. For example, while an IPv4 address would look similar to `192.168.1.2`, an IPv6 address would look similar to `2001:0578:0123:4567:89AB:CDEF:0123:4567`. IPv6 has 2128 uniquely identifying addresses, which is about 340 undecillion, or 340 billion billion billion.

### IPv4 Addressing vs. IPv6 Addressing



IPv6 offers some obvious advantages, the primary one being that it's a lot more space. With IPv6, a single network can have more IPv6 addresses than the entire IPv4 address space. For more information, see [Understanding IPv6](#).

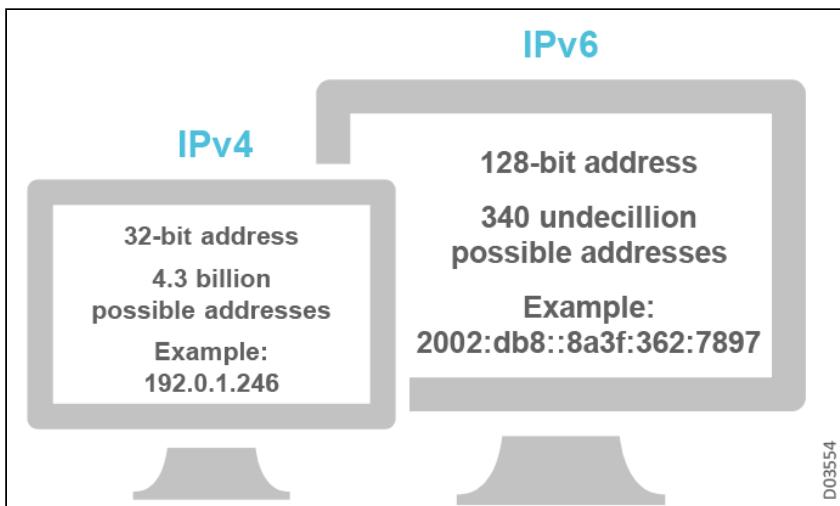
## Understanding IPv6

Internet Protocol version 6 (IPv6) was developed by the Internet Engineering Task Force to deal with the long-anticipated problem of IPv4 address exhaustion.

Every device on the Internet is assigned a unique IP address for identification and location definition. IPv4 addressing is based on a 32-bit header, providing approximately 4.3 billion possible addresses. This is a legitimately large number, and at the time that IPv4 was designed it seemed to supply many more addresses than anyone would ever need.

However, in today's world, internet addresses are not only needed for government, academia, and enterprise users. In today's Internet of Things, soon every single car and refrigerator will need its own IP address! For this reason, IPv6 is based on 128-bit addresses, allowing  $2^{128}$  raised to the power of 128, or approximately  $3.4 \times 10^{38}$  addresses! This is *79 trillion trillion times the number of possible IPv4 addresses!* and will hopefully suffice.

## IPv4 Addressing vs. IPv6 Addressing



IPv6 provides other technical benefits in addition to a larger addressing space. In particular, it permits hierarchical address allocation methods that facilitate route aggregation across the Internet, and thus limit expansion of routing tables. The use of multicast addressing is expanded and simplified, and provides additional optimization for service delivery. Device mobility, security, and configuration aspects have all been taken into consideration in the design of the protocol.

This section introduces the following IPv6 features:

- IPv6 Addressing
- Anycast Addresses
- ICMPv6
- Neighbor Discovery
- NDP Tracking

## IPv6 Addressing

Similar to the address format of IPv4, addresses in IPv6 are represented by 4 digit hexadecimal numbers separated by colon (:) characters. For example:

**2001:0db8:0000:130F:0000:0000:087C:140B**

Abbreviations are possible. For example, leading zeros in a contiguous block could be represented by (::). (Only leading zeros are omitted; trailing zeros cannot be omitted.) The double-colon abbreviation can be used once in an address. Prefix representation is based on CIDR notation, in which an address or routing prefix is written with a suffix indicating the number of bits of the prefix. In IPv4 it would look something like this: 192.168.2.0/24. In IPv6 it would look something like this: 2001:db8::/32.

Loopback address representation is available. Similar to 127.0.0.1 in IPv4, 0:0:0:0:0:0:1 (which is conveniently written as ::1) is used to identify self. Unspecified addresses are represented by 0:0:0:0:0:0:0, written as ::. This is used as a placeholder when no address is available.

IPv6 addresses are assigned to interfaces, with interfaces expected to have multiple addresses (unlike IPv4). The following types of IPv6 addresses are supported:

- Unicast: Address of a single interface. One-to-one delivery to a single interface. The following versions are defined:
  - Global Unicast: Addresses for generic use of IPv6, structured as a hierarchy to keep the aggregation.
  - Unique-Local: Addresses for local communications and inter-site VPNs, not routable on the internet.
  - Link-Local: Addresses for the mandatory address for communication between two IPv6 devices, similar to ARP but at Layer 3. These are automatically assigned by the router as soon as IPv6 is

enabled. These addresses are also used for next-hop calculation in routing protocols. The scope of these addresses is limited and only link-specific. The remaining 54 bits could be zero (0) or any manually-configured value.

- **Multicast:** Address of a set of interfaces, providing one-to-many delivery to all interfaces in the set. Multicast addresses have a prefix FF00::/8 (1111 1111). The second octet defines the lifetime (temporary or permanent) and scope (node, link, site, organization, or global) of the multicast address. IPv6 multicast addresses can be mapped to Ethernet addresses, using a standard 33:33 prefix: 33:33:<last 32 bits of the IPv6 multicast address>.
- **Anycast:** Address of a set of interfaces, providing one-to-one-of-many delivery to a single interface in the set that is closest. Anycast allows a source node to transmit IP datagrams to a single destination node out of a group of destination nodes with same subnet id, based on the routing metrics. Only routers respond to anycast addresses, processing the packets based on the network prefix. Routers configured to respond to anycast packets will automatically do so when they receive a packet sent to the anycast address.

Note that for each unicast and anycast address configured, there is a corresponding solicited-node multicast address. This is used in place of ARP and DAD, and also used in neighbor solicitation messages. This is a unique type of multicast address with a link-local scope. A solicited-node multicast address consists of the prefix + the lower 24 bits of the unicast address: FF02::1:FF:. IPv6 does not support broadcast addresses.

For more information, see <http://www.iana.org/assignments/ipv6-multicast-addresses>, or *IP Version 6 Addressing Architecture* (RFC 4291) and the subsequent updates.

Neptune platforms support usage of 127-bit IPv6 prefixes on inter-router links, as per RFC 6164.

## Anycast Addresses

Anycast addressing allows a source node to transmit IP datagrams to a single destination node out of a group of destination nodes with same subnet id, based on the routing metrics. An IPv6 anycast (AC) address is an IPv6 address assigned to multiple interfaces, where these interfaces typically belong to different nodes (hosts/routers). The AC address is allocated from the unicast address space, and is thus indistinguishable from unicast addresses. Routing to AC destinations is achieved by distant routers, assuming they have multiple routes to same destination. Packets are forwarded to the closest interface where the AC address is located, where 'closest' means smallest routing protocol distance.

AC is designed for stateless and short-lived services. In these services, the network topology typically remains unchanged during a session, therefore the session between a client and specific server can be completed without disruption. For example:

- **Domain Name Systems (DNS) services**

The Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. DNS functions as a database managing Resource Records (RR) of various types, including IPv4 and IPv6. DNS is an IP application that uses either UDP or TCP on top of IPv4 or IPv6.

DNS services are provided by geographically dispersed DNS servers. A DNS server is used to store translations of domain names to IP addresses. The client would send a query for a domain name, and the server would send the respective IP address in reply. Transactions between client and server are well-suited for AC addressing, because they are stateless, short-lived, and use UDP. Being connectionless, UDP makes a server change go unnoticed by the clients. Therefore DNS servers often share an AC address, wherein client queries are routed to closest (routing-wise) DNS server.

- **Content Delivery Network (CDN) services**

CDN servers are typically globally distributed over multiple data centers. A CDN server stores internet content of various types, such as text and images. The client would send an HTTP request, and the server would send the internet content in reply. Transactions between client and server are suited for AC addressing, because they are stateless and short-lived, however they use TCP. Being connection oriented, a server change would break the TCP sessions, and they would need to be recreated with the new server. This disadvantage is tolerable, owing to the nature of the transactions as described.

here. Therefore CDN servers often share an AC address, wherein client HTTP requests are routed to closest (routing-wise) CDN server.

AC addressing offers many advantages:

- **Faster service:** Forwarding client requests to closest (routing-wise) server cuts resolution time.
- **Higher service uptime:** When a route to server is down, it is no longer used by routers. Thereafter, requests are automatically routed to another server.
- **Load balancing:** Distributing requests among multiple servers based on shortest routing distance provides load balancing.
- **Better resistance against DDoS attacks:** Large scale Distributed Denial of Service (DDoS) attacks are executed from multiple locations. When the target is AC, attack volume gets distributed, because each server is attacked by "nearby" clients only.
- **Maintainability:** Servers can be deployed globally with same IP address, thus eliminating the need to allocate and maintain a separate IP address per server.

## ICMPv6

Internet Control Message Protocol (ICMP) version 6, defined in RFC 2463 to support IPv6, is a modification of ICMP for IPv4. The message types are similar, but version 6 utilizes different types and codes:

- Destination unreachable (type 1)
- Packet too big (type 2)
- Time exceeded (type 3)
- Parameter problem (type 4)
- Echo request/reply (type 128 and 129)

ICMPv6 messages include the following fields:

- Type: identifies the message or action needed.
- Code: a type-specific sub-identifier. For example, Destination Unreachable can mean no route, port unreachable, administratively prohibited, etc. The code field is used to identify these sub-types.
- Checksum: computed over the entire ICMPv6 message, and prepended with a pseudo-header containing a single-octet.
- Next Header: in IPv6 has a value of 58, indicating ICMP.

## Neighbor Discovery

Neighbor discovery for ICMPv6 indicates reachability of neighbors, handling tasks and functions such as those addressed by Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) redirection and router discovery, as well as the Router Discovery and Router Redirect protocols used in IPv4. Hosts use it to discover routers and for autoconfiguration of addresses. Neighbor discovery is also an effective mechanism for Duplicate Address Detection (DAD).

NDP, however, has been improved compared to its IPv4 predecessors. NDP covers different kinds of network communication such as router solicitation, router advertisement, and neighbor solicitation or advertisement. These kinds of processes help to route data along network trajectories using individual nodes. In general, systems like NDP help to make data transmission more efficient and consistent across multiple networks and processes.

Neighbor discovery uses ICMPv6 messages, originated from nodes on link-local, with a hop limit of 255. These messages include an IPv6 header, ICMPv6 header, neighbor discovery header, and neighbor discovery options. Five ICMPv6 neighbor discovery messages are defined:

- Router solicitation (RS) (type 133)
- Router advertisement (RA) (type 134)
- Neighbor solicitation (type 135)
- Neighbor advertisement (type 136)
- Redirect (type 137)

For example, router solicitations (RS) are sent by booting nodes to request router advertisements (RA) for configuring the interfaces. Routers send periodic RAs to the all-nodes multicast address. The process is similar for neighbor solicitation and advertisement. A set of multicast neighbor solicitations and advertisements is used for duplicated address detection (DAD). Routers send redirect messages to signal the rerouting of a packet to a better router.

The larger address space supports autoconfiguration by enabling use of link-layer addresses inside the address space, allowing autoconfiguration with 'no collisions' and offering 'plug and play' capabilities as well. A larger address space also enables renumbering, through a combination of autoconfiguration and use of multiple addresses.

## NDP Tracking

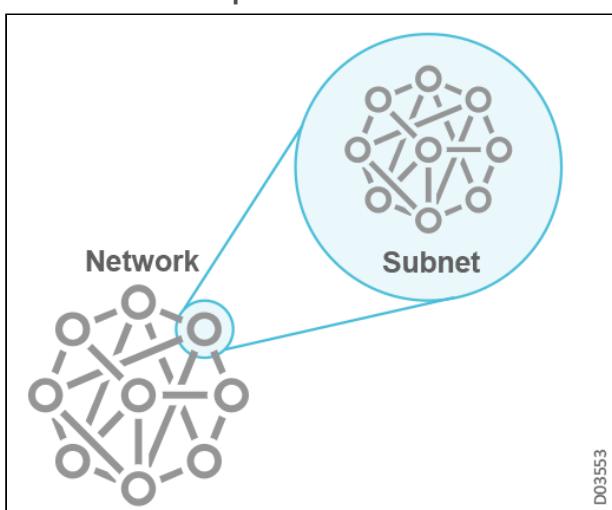
NDP tracking affects advertising and redistribution of prefixes to routing protocols, either IGP or BGP. NDP Tracking operation is generally as follows:

- The NPT IP interface is configured with an IPv6 destination address to track.
- NPT periodically sends NDP Neighbor Solicitation messages over the IP interface to the destination address, and expects to receive NDP Neighbor Advertisement messages in reply.
- If there are no replies after some configurable time period threshold, the NPT withdraws the prefix containing the IPv6 address of the destination from all routing protocols to which it was advertised or redistributed.

NDP tracking can be enabled for any AC/UC adjacent destinations, either hosts or routers. NDP tracking for target applications is better suited than IP Ping tracking, because it ensures that replies are received from a local (adjacent) server, with which the router shares a link/LAN. In comparison, with IP Ping tracking, the replier could be a distant (non-adjacent) server, thus preventing detection of a local server failure.

## Understanding Subnetworks

### Subnetwork Example

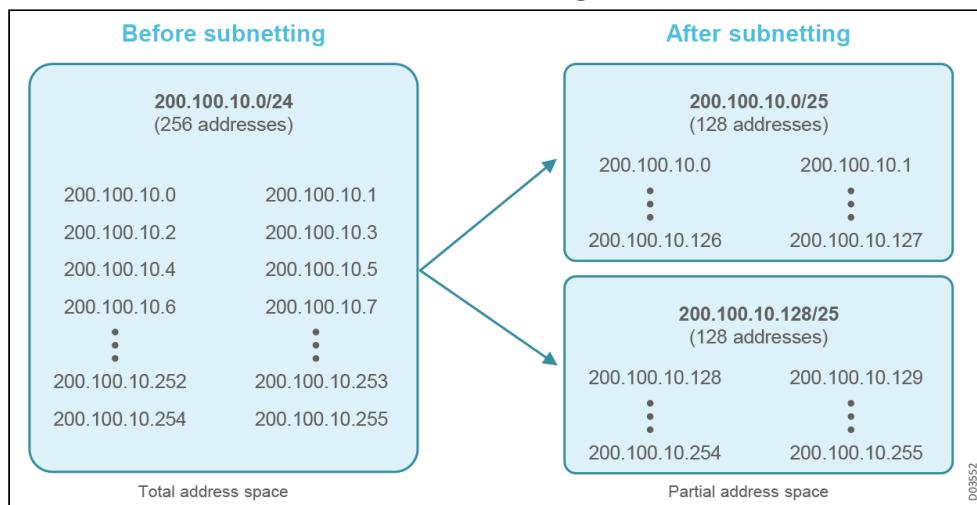


Every IP address has two main parts: the network number (routing prefix) and the rest field (host identifier), identifying the specific host or network interface. The first part indicates the network to which the address belongs. The second part specifies the device within that network. The subnetwork part is appended at the end of the network-host address.

The routing prefix may be expressed in Classless Inter-Domain Routing (CIDR) notation. It counts the number of bits in the prefix and appends that number to the address after a slash (/) character separator. For example, 198.51.100.0/24 is the prefix of the IPv4 network starting at the given address, with 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing. Addresses in the

range 198.51.100.0 to 198.51.100.255 belong to this network, with 198.51.100.255 as the subnet broadcast address. This notation is used for both IPv4 and IPv6. So the IPv4 network 192.0.0.0 with the subnet mask 255.255.255.0 is written as 192.0.0.0/24, and the IPv6 notation 2001:db8::/32 designates the address 2001:db8:: and its network prefix consisting of the most significant 32 bits.

## 256 Network Addresses Subdivided into 2 Logical Subnets of 128 Addresses Each



Given an IPv4 source address, its associated subnet mask, and the destination address, a router can determine whether the destination is on a locally connected network or a remote network. The subnet mask of the destination is not needed, and is generally not known to a router. When the routing prefixes of the source address and the destination address differ, traffic is exchanged between subnetworks through routers. Subnetworks allow the networks to process traffic more efficiently. For example, take a network ID 192.168.123.0, with a host address 0.0.0.132. When a packet arrives on the 192.168.123.0 subnet (from a local subnet or a remote network), with a destination address of 192.168.123.132, the router receives it from the network and forwards it to the appropriate destination. A router serves as a logical or physical boundary between the subnets. Note that for IPv6, on-link determination is different in detail and requires the [Neighbor Discovery Protocol \(NDP\)](#).

The benefits of subnetting an existing network vary with each deployment scenario. In the address allocation architecture of the Internet using CIDR and in large organizations, it is necessary to allocate address space efficiently. Subnetting may also enhance routing efficiency, or offer advantages in network management when subnetworks are administratively controlled by different entities in a larger organization. Subnets may be arranged logically in a hierarchical architecture, partitioning an organization's network address space into a tree-like routing structure, or other structures such as meshes.

This section introduces the following topics:

- [IPv4 Subnetworks](#)
- [IPv6 Subnetworks](#)

## IPv4 Subnetworks

For IPv4, a network may also be characterized by its subnet mask or netmask. This is a bitmask that, when applied by a bitwise AND operation to any IP address in the network, yields the routing prefix. Subnet masks are also expressed in dot-decimal notation like an IP address. For example, the prefix 198.51.100.0/24 would have the subnet mask 255.255.255.0.

An IPv4 subnet mask consists of 32 bits; it is a sequence of ones (1) followed by a block of zeros (0). The ones indicate bits in the address used for the network prefix and the trailing block of zeros designates that part as being the host identifier. The following example shows the separation of the network prefix and the host identifier from an address (192.0.2.130) and its associated /24 subnet mask (255.255.255.0). The operation is visualized in a table using binary address formats.

### Parts of an IPv4 Address

	<b>Binary Form</b>	<b>Dot-Decimal Notation</b>
IP address	11000000.00000000.0000010.10000 010	192.0.2.130
Subnet mask	11111111.11111111.11111111.0000000 0	255.255.255.0
Network prefix	11000000.00000000.0000010.00000 000	192.0.2.0
Host identifier	00000000.00000000.00000000.10000 010	0.0.0.130

The result of the bitwise AND operation of the IP address and the subnet mask is the network prefix 192.0.2.0. The host part, which is 130, is derived by the bitwise AND operation of the address and the one's complement of the subnet mask.

**Subnetting** is the process of designating some high-order bits from the host part as part of the network prefix and adjusting the subnet mask appropriately. This divides a network into smaller subnets. The following table modifies the preceding example by moving 2 bits from the host part to the network prefix, thereby forming four smaller subnets, each one quarter of the previous size.

### Subnetting

	<b>Binary Form</b>	<b>Dot-Decimal Notation</b>
IP address	11000000.00000000.0000010.10000 010	192.0.2.130
Subnet mask	11111111.11111111.11111111.1100000 0	255.255.255.192
Network prefix	11000000.00000000.0000010.10000 000	192.0.2.128
Host part	00000000.00000000.00000000.00000 010	0.0.0.2

For example, suppose an IP packet is addressed to the IP address 192.0.2.15. The network is identified by "192.0.2" (or to be technically precise, 192.0.2.0/24). Network routers forward the packet to a host on the network indicated by "192.0.2." Once the packet arrives at that network, a router within the network consults its routing table. Using its subnet mask of 255.255.255.0, the router sees the device address "15" (the rest of the IP address indicates the network and can be ignored), and calculates which subnet the packet should go to. It forwards the packet to the router or [switch](#) responsible for delivering packets within that subnet, and the packet arrives at IP address 192.0.2.15.

## IPv6 Subnetworks

The design of the IPv6 address space differs significantly from IPv4. The primary reason for subnetting in IPv4 is to improve efficiency in the utilization of the relatively small address space available, particularly to enterprises. No such limitations exist in IPv6, as the large address space available, even to end-users, is not a limiting factor.

As in IPv4, subnetting in IPv6 is based on the concepts of variable-length subnet masking (VLSM) and the Classless Inter-Domain Routing methodology. It is used to route traffic between the global allocation spaces and within customer networks between subnets and the Internet at large.

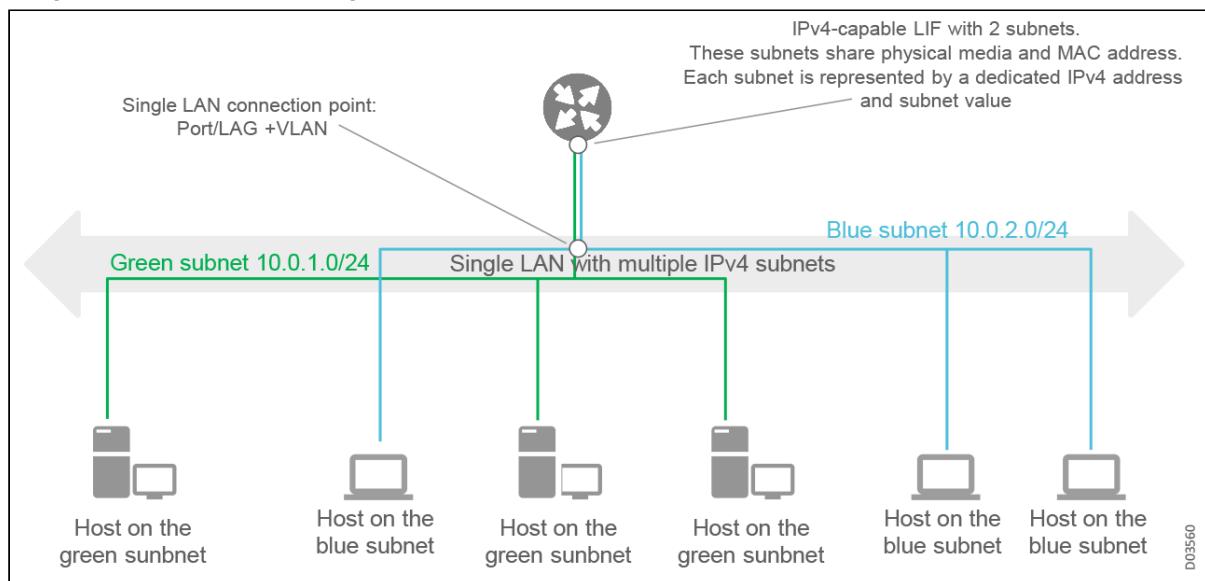
A compliant IPv6 subnet always uses addresses with 64 bits in the host identifier. Given the address size of 128 bits, it therefore has a /64 routing prefix. Although it is technically possible to use smaller subnets, they are impractical for local area networks based on Ethernet technology, because 64 bits are required for stateless address autoconfiguration. The Internet Engineering Task Force recommends the use of /127 subnets for point-to-point links, which have only two hosts.

IPv6 does not implement special address formats for broadcast traffic or network numbers, and thus all addresses in a subnet are acceptable for host addressing. The all-zeroes address is reserved as the subnet-router anycast address.

## Supporting Multiple IP Addresses

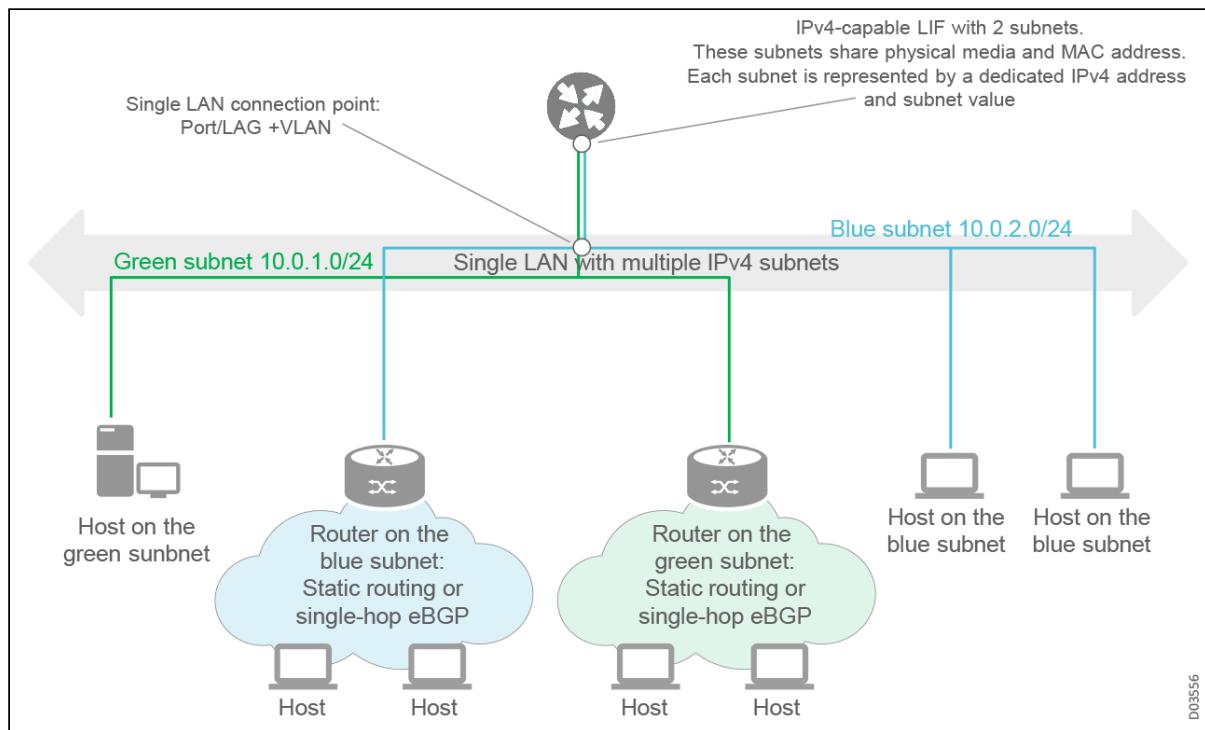
Mobile service providers frequently assign IPv4 addresses from different subnets to different functionalities within the same base station. As a result, the customer-facing IPv4 interface to which such a base station is connected (directly or via some L2 switching media) has to be configured with multiple IPv4 addresses - one for each subnet supported by the base station.

### Simple Use Case with Multiple IPv4 Addresses



In a more complicated scenario, some of the hosts on the LAN (in the lower half of the following diagram) may actually be routers running some protocol with the router in the upper half of the diagram. In this example, you can configure static routing with single-hop eBGP in each of the multiple subnets.

## Configure Static Routing with Single-hop eBGP



Note that multiple IPv4 addresses and IPv6 addresses can be configured on the same interface; they do not interact in any way.

## IP Networking in the Control Plane

The control plane, the data (forwarding) plane, and the management plane are the three basic components of a telecommunications architecture. The data plane carries the network's traffic. The control plane provides configuration, support, and administrative services for the data plane, enabling its efficient functioning. The management plane, which carries administrative traffic, is considered a subset of the control plane.

The control plane is the part of the router architecture that is concerned with drawing the network topology, or the information in a routing table that defines what to do with incoming packets. In most cases, the routing table contains a list of destination addresses and the outgoing interface(s) associated with them. Control plane logic also can define certain packets to be discarded, as well as preferential treatment of certain packets for which a high QoS is defined by such mechanisms as DiffServ.

The control plane is where forwarding/routing decisions are made. Switches and routers have to decide where to send frames (L2) and packets (L3). The switches and routers that run the network run as discrete components, but since they are in a network, they have to exchange information such as host reachability, status, and so on with their neighbors. The route controller exchanges the topology information with other routers and constructs a routing table based on a routing protocol, such as OSPF or BGP.

The control plane is the part of a network that is responsible for routing and carries signaling traffic. Intelligent routing provides the ability to select the most appropriate path. Signaling provides the ability to create, delete, and maintain end-to-end connections. Through signaling, the control plane sets up and releases connections, and restores a connection in case of failure.

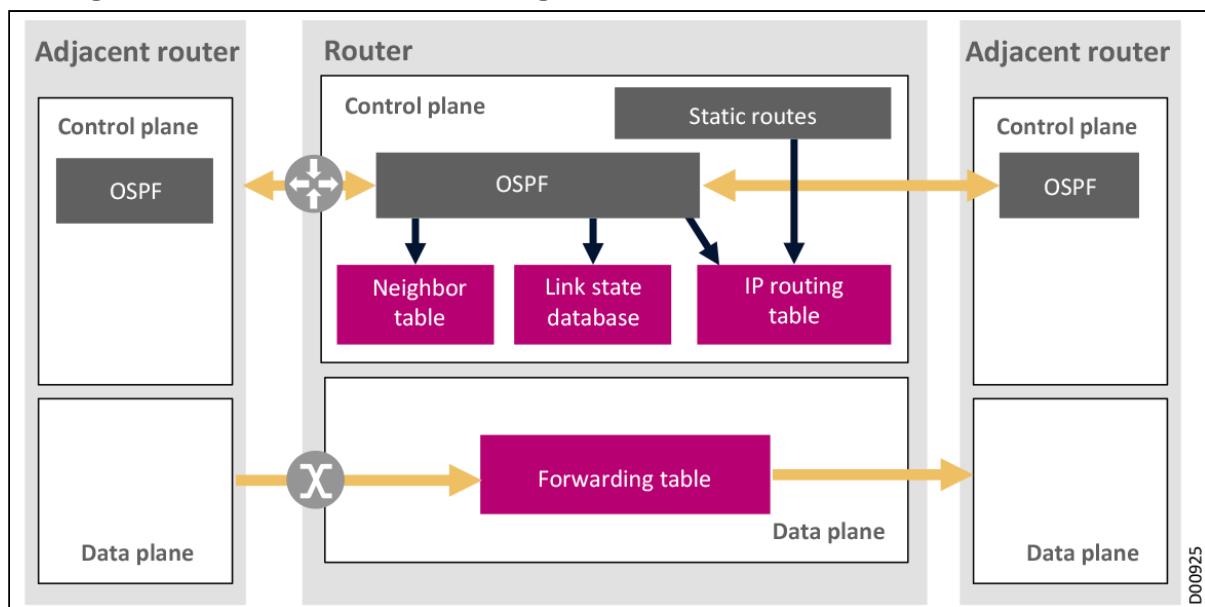
For example, in the control plane you set up IP networking and routing (routing protocols, route preferences, static routers, etc.) and connect hosts and switches/routers together. Each switch/router figures out what is directly connected to it, and then tells its neighbor what it can reach and how it can reach it. The switches/routers also learn how to reach hosts and networks not directly attached to it. Once all of the routers/switches have a coherent picture - shared via the control plane - the network is converged.

## Switching and Routing

Switching (packet forwarding) is performed in the data (forwarding) plane. Routing (exchange of routing information) is performed in the control plane. The information collected through routing protocols (for example) is used to build topology or routing databases. The routing protocols identify the best paths from the protocol-specific data structures and insert these paths in the routing table. The routing table might contain recursive information and is thus not suitable for fast packet forwarding. The routers use two mechanisms to speed up packet forwarding:

- They can cache the results of routing table lookup for recently used destinations
- They can pre-compute the actual forwarding data for every destination and store them in a forwarding table that can be used directly by the data plane

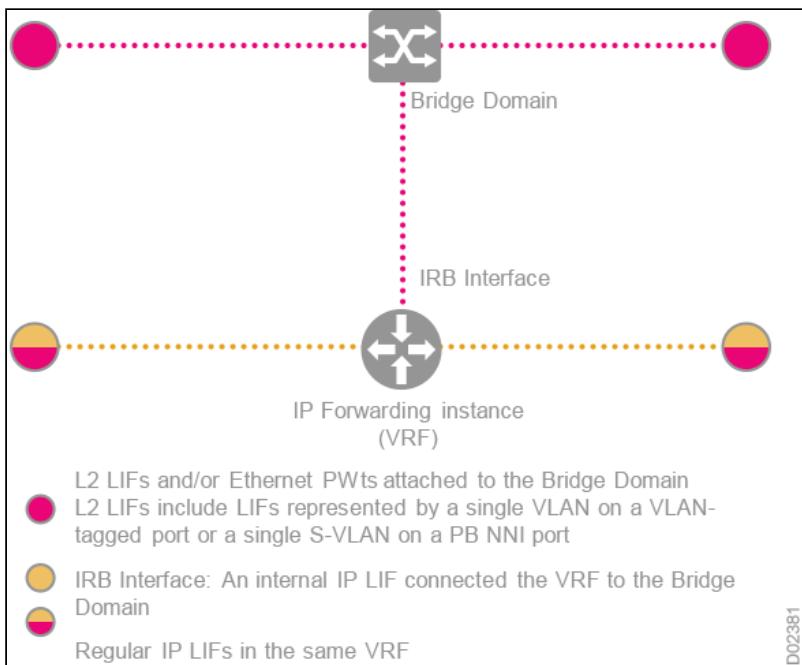
### Routing in the Control Plane and Switching in the Data Plane



### IRB: Integrated Switching and Routing

An Integrated Routing and Bridging (IRB) interface connects management traffic between routed IP IP/MPLS domains with devices on legacy PB domains that are using management VLAN for in-band management.

### Integrated Routing and Switching Functionalities



By default, an IRB LIF belongs to the global/default VRF. However, you can configure an IRB LIF to belong to a specific VRF.

The IRB LIF can also be used as a bridge domain on an MP2MP VSI. In this domain, you can:

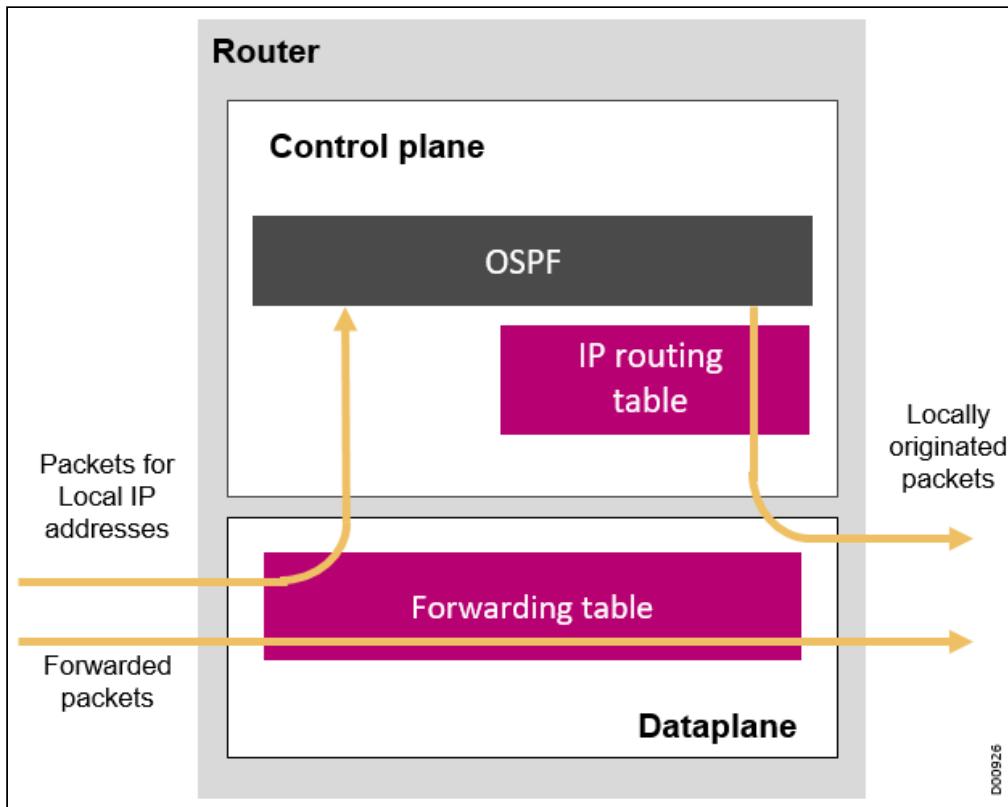
- Attach L2 LIFs on VLAN-tagged Ethernet ports or LAGs. The VLANs can be either ingress or egress, and the L2 LIFs must be associated with a single VLAN on the supporting port/LAG.
- Connect Ethernet PWs (such as an MP2MP VSI) to remote peers. The PWs can be static or signaled, and can be set up as pairs using PW redundancy.
- Associate attachment circuits and PWs with specific split horizon groups.

You can configure an IRB LIF to carry traffic from IPv4, IPv6, or both protocols. To configure IPv6 support through the Neptune CLI, use the command family `inet6`. When you set up an IPv6-capable IRB LIF, it is automatically assigned a link-local unicast address. The interface ID for this address is derived from the system MAC address. It can also be configured with up to 4 globally unique IPv6 addresses, and you can configure some of these addresses explicitly as **anycast**. You can also enable IPv6 router advertisements.

## Processing Inbound Packets

In most router implementations, the data plane receives and processes all inbound packets, selectively forwarding packets destined for the router (such as routing protocol updates) or packets that need special processing (such as IP datagrams with IP options or IP datagrams that have exceeded their TTL) to the control plane.

### Typical Packet Flow in a Router

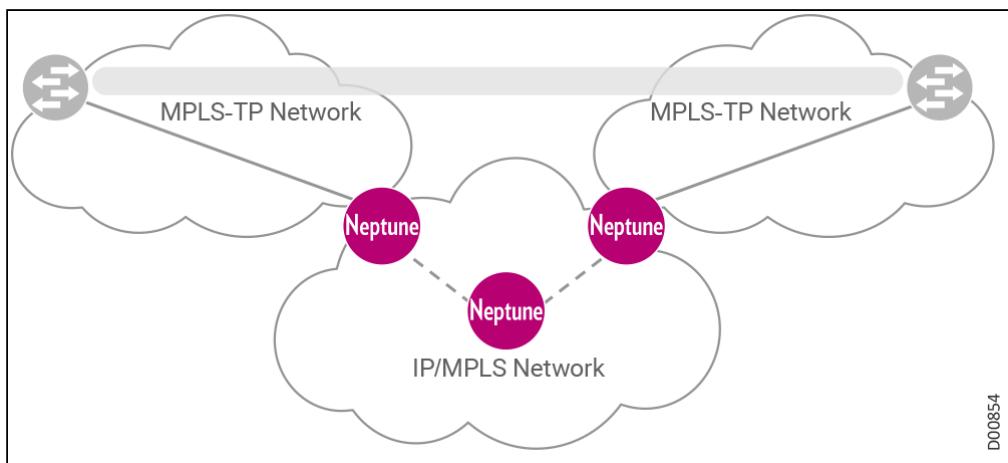


## MPLS-TP and IP-MPLS Interworking Models

Our MPLS end-to-end solution relies on a smooth MPLS-TP to IP/MPLS internetwork implementation, based on a combination of overlay and stitching models.

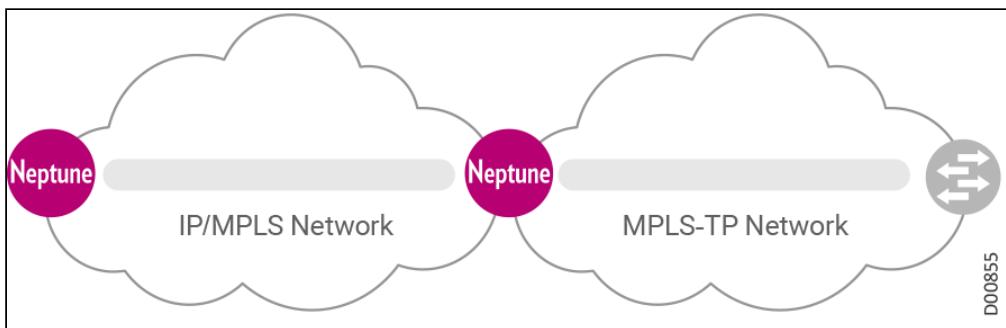
### Overlay

#### Overlay Model



### Stitching

## Stitching Model



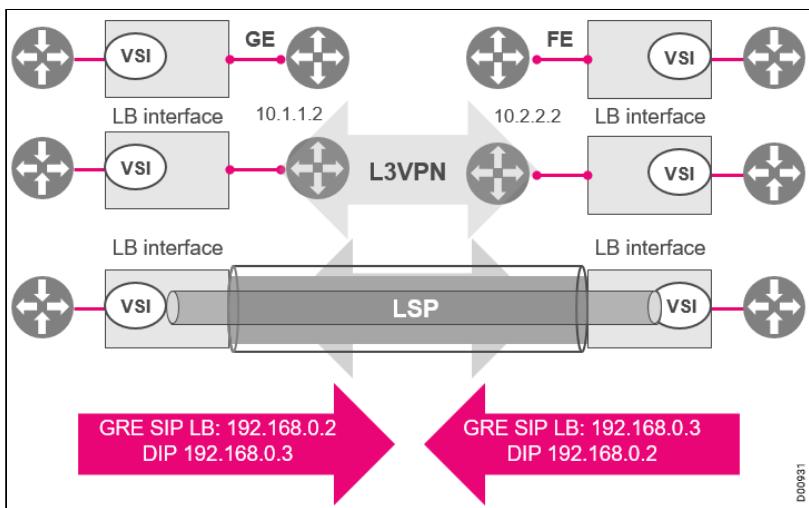
This section introduces the following features:

- Overlay using GRE
- Stitching via Signaling Gateways
- Stitching PE
- Interworking Example
- Integrate Smoothly with Third-Party Elements

## Overlay using GRE

MPLS over Generic Routing Encapsulation (GRE) provides a mechanism for tunneling MPLS packets over a non-MPLS network. This feature utilizes MPLS over generic routing encapsulation (MPLSoGRE) to encapsulate MPLS packets inside IP tunnels. Encapsulating MPLS packets inside IP tunnels creates a virtual P2P link across non-MPLS networks.

### Generic Routing Encapsulation



Advantages of the GRE overlay method include:

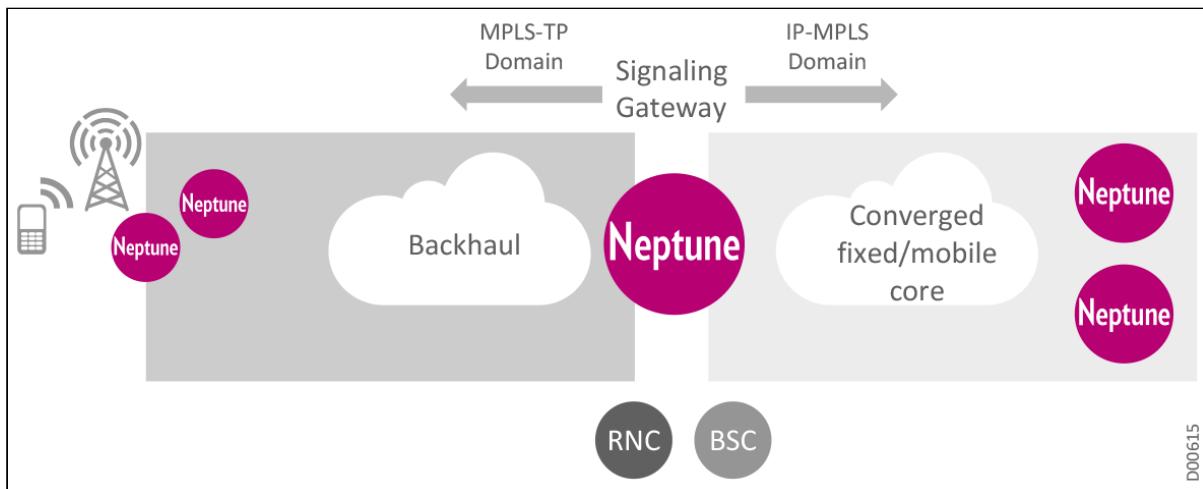
- Simplicity
- Preserve all MPLS-TP features end-to-end through the IP cloud
- Simplify operational activity by the IP cloud (simple L3VPN configuration)
- Encase multiple protocols over a single IP protocol backbone
- Carrier network becomes transparent
- Allow L2VPNs MPLS-based across wide networks

## Stitching via Signaling Gateways

A pseudowire (PW) is a virtual 'wire' that emulates a P2P connection over a packet switching network (PSN). The PW emulates the operation of a 'transparent wire' carrying a service, such as ATM, Frame Relay, Ethernet, or TDM, over an MPLS or IP packet network. The PW is a logical connection that is intended to provide only the minimum necessary functionality to emulate the 'wire' with the required degree of faithfulness for the given service definition.

Signaling gateways (SGW) are used to tie PW segments together into a single connection (*stitching*) at a given point. This functionality is implemented within a single platform located at the border of two network domains. The two domains may both be static, both dynamic, or one static and one dynamic. Network interworking enables LSP and service stitching, interaction between the data planes, and end-to-end OAM.

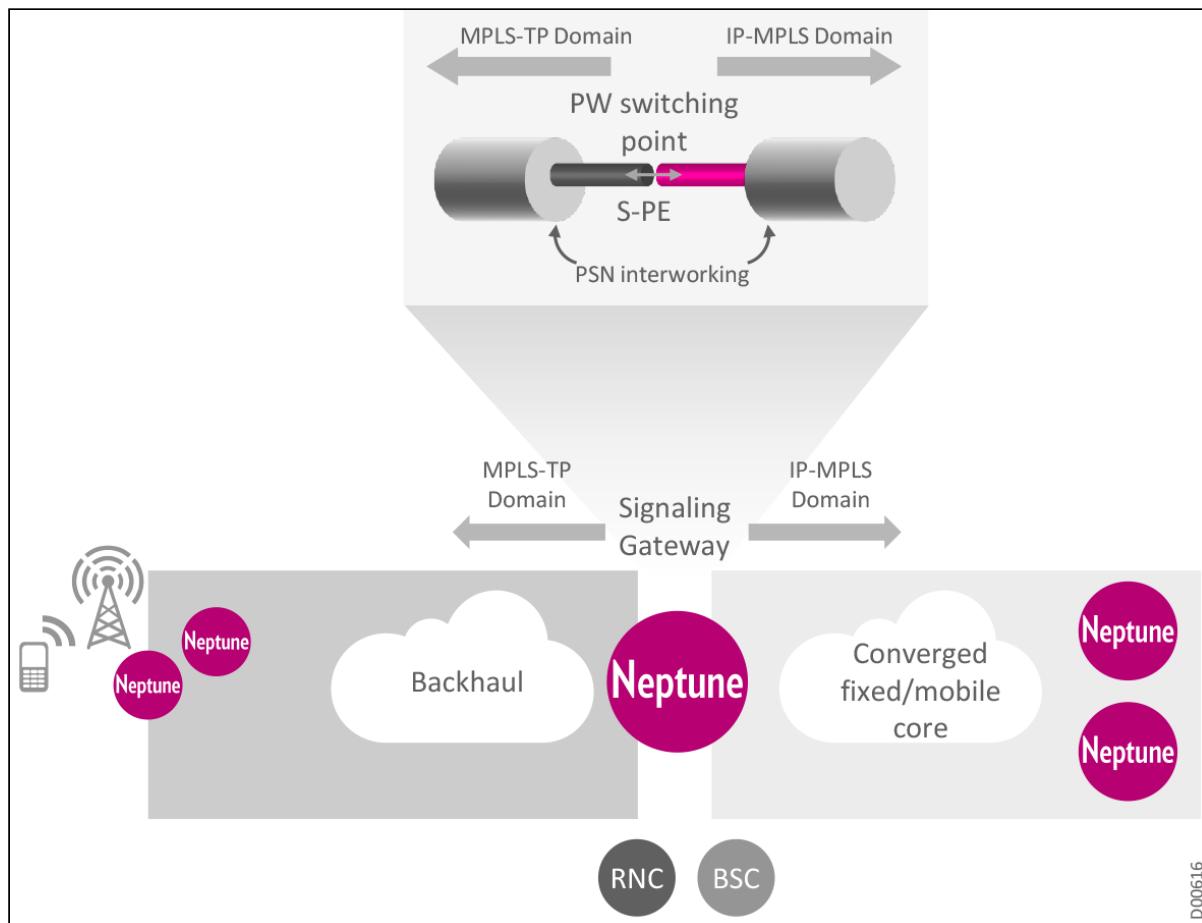
### Signaling Gateway Concept



MPLS-TP and IP/MPLS domains can be connected through SGWs. In PW-based backhaul, this is implemented through multisegment PWs (MS-PWs), including:

- Static MPLS-TP segments
- Dynamic IP/MPLS segments
- Gateway interconnections or "stitches" of both types of segments

## PW Switching Point



D00616

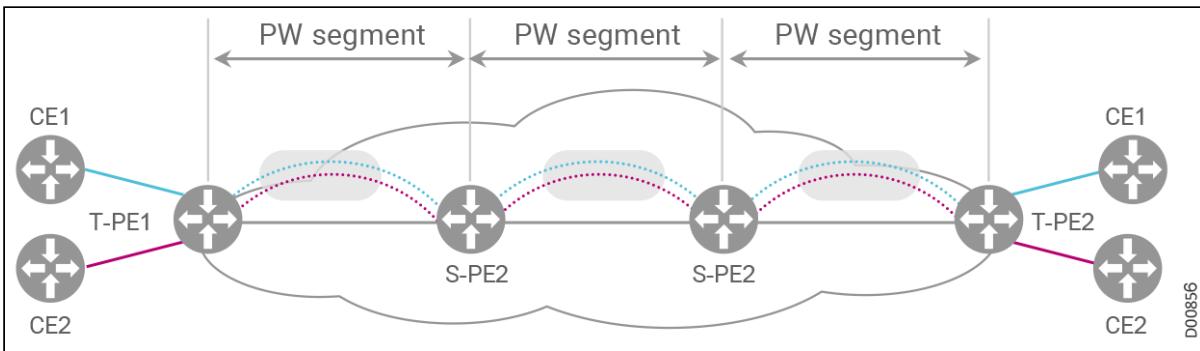
## Stitching PE

An L2VPN multisegment pseudowire (MS-PW) is a set of two or more PW segments that function as a single PW, as illustrated in the following figure. MS-PWs can span multiple cores or autonomous systems of the same or different carrier networks.

The routers participating in the PW segments are identified as follows:

- Switching provider edge (S-PE) routers, which are located at the switching points connecting the tunnels of the participating PW segments. The S-PE routers can switch the control and data planes of the preceding and succeeding PW segments.
- Terminating provider edge (T-PE) routers, which are located at the MS-PW endpoints.

### Stitching PE

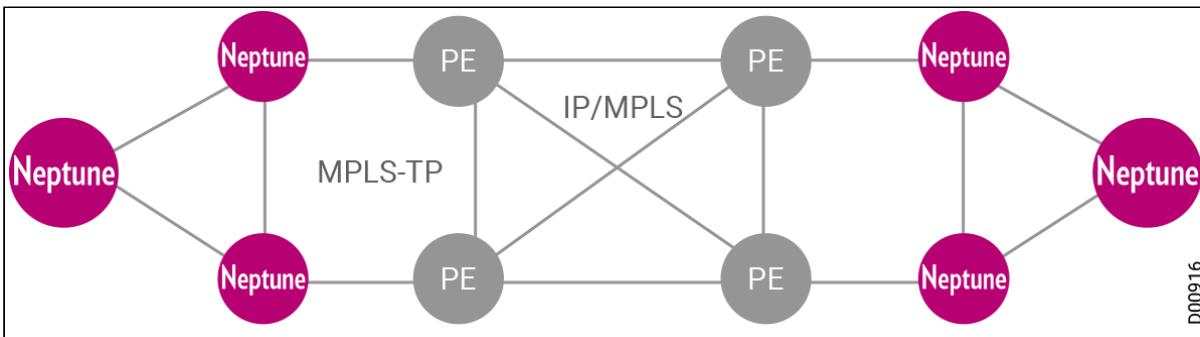


Advantages of the stitching PE method include:

- Simplify network view
- Reduce complexity in network operation
- Full service end-to-end OAM solution including both MPLS-TP and IP networks
- End-to-end service protection across different region/network domains

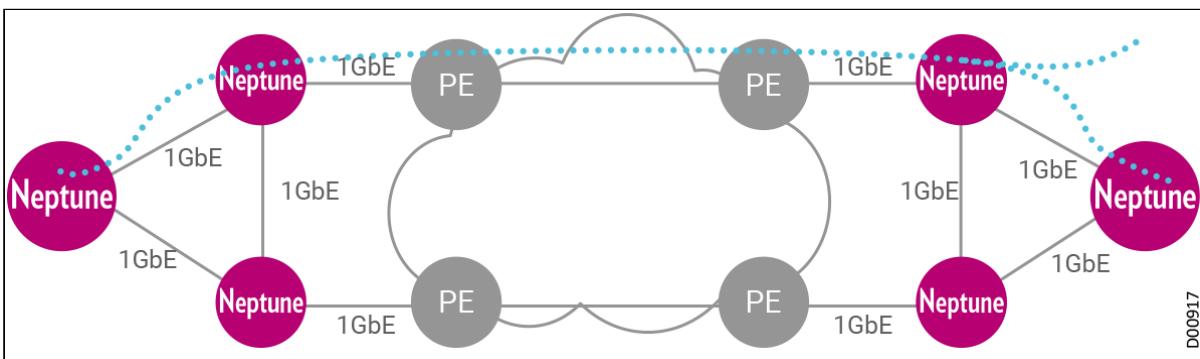
## Interworking Example

### Physical Network Topology



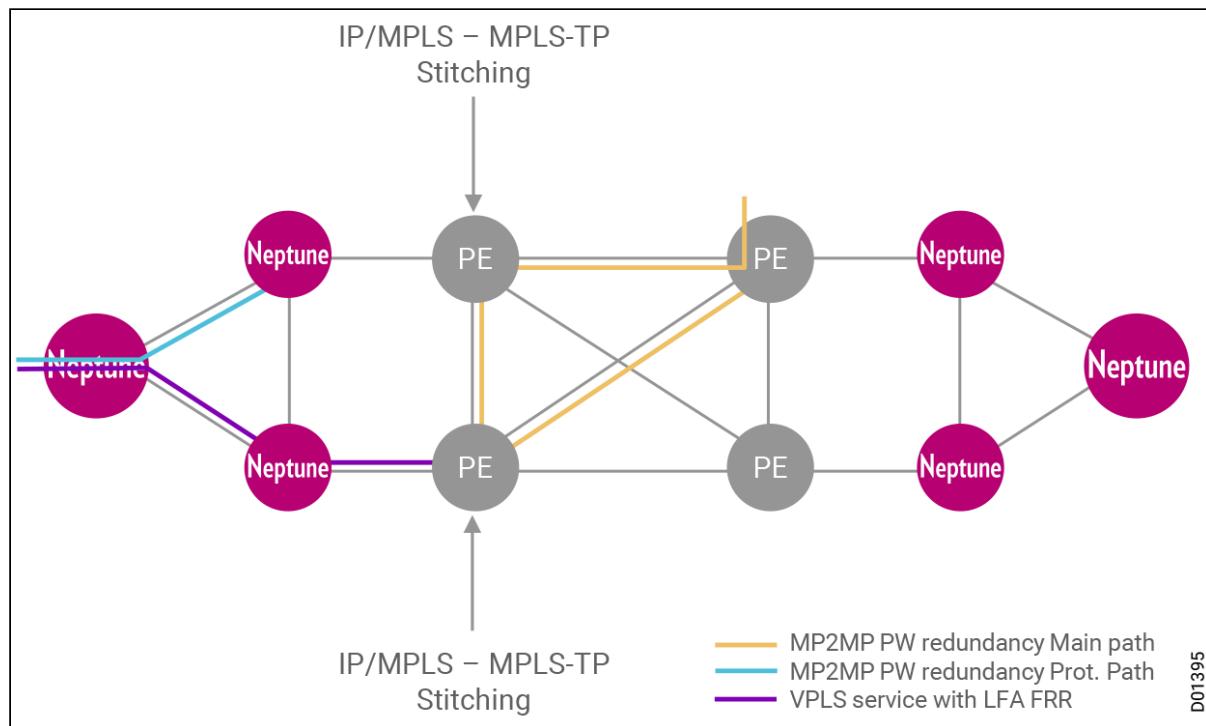
One possible solution for this network, based on the overlay model, is illustrated in the following figure. In this solution, protected service traffic runs ETE through an overlay using GRE.

### Overlay Model Solution



A second possible solution for this network, based on the stitching model, is illustrated in the following figure. In this solution, protected service traffic runs ETE, transmitted through stitching PEs. Services in this model are implemented over MS-PWPs, using PW-R at the access layer and VPLS using FRR.

### Stitching Model Solution

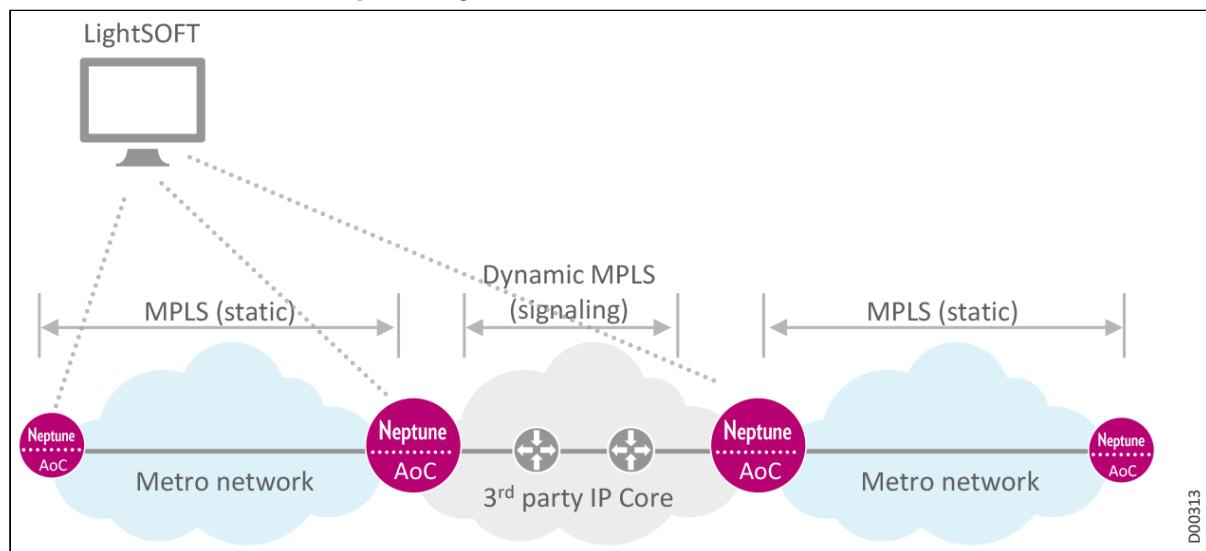


### Integrate Smoothly with Third-Party Elements

Telecommunications networks today are complex entities, usually incorporating elements from a wide range of sources, including third-party equipment. Our data cards support smooth integration and interworking with networks based on third-party equipment.

Neptune data cards support the E-LSP tunnel infrastructure currently most popular with SPs. The data cards integrate smoothly with third-party PB access networks, providing fully compliant support for MSTP/RSTP (IEEE802.1D) on all Ethernet port types (UNI, E-NNI, I-NNI) as well as ERP (ITU-TG.8032) on EoS I-NNI ports.

### Smooth E2E Network Interoperability



## DHCP Relay Agent and Option 82

Dynamic Host Configuration Protocol (DHCP) enables dynamic transmission of configuration information between hosts on a TCP/IP network. Servers utilizing DHCP are able to automatically assign an IP address to a computer. There are more than one billion computers in the world, and each individual computer needs its own IP address whenever it's online. The DHCP protocol automatically assigns and keeps tabs of IP addresses and any "subnetworks" that require them. The IP addresses are selected from a pre-defined range of numbers allocated for a specific network.

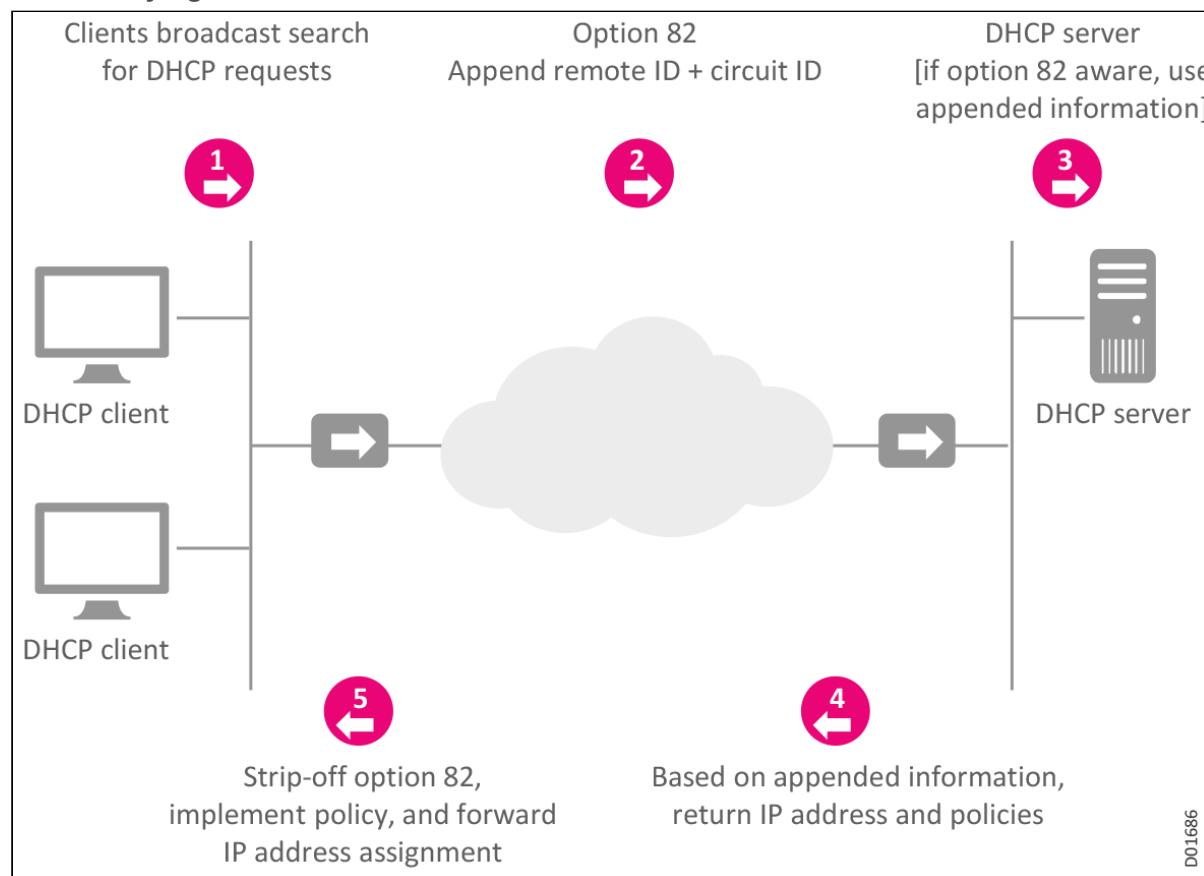
DHCP is implemented through a system of DHCP clients, servers, and relay agents. The following figure illustrates what happens when a DHCP client requests an IP address from a DHCP server. The **client**, Host A, sends a **DHCPDISCOVER** broadcast message to locate a DHCP server. A **relay agent** forwards these packets between DHCP clients and servers. In response, a **DHCP server** offers configuration parameters (such as IP address, MAC address, domain name, etc.) to the client in a **DHCPOFFER** unicast message.

Dynamic address assignment provides significant benefits for many network applications, such as IP-TV, business applications, and other contexts that benefit from L3VPN and hosting configurations.

Neptune PEs act as DHCP **relay agents**.

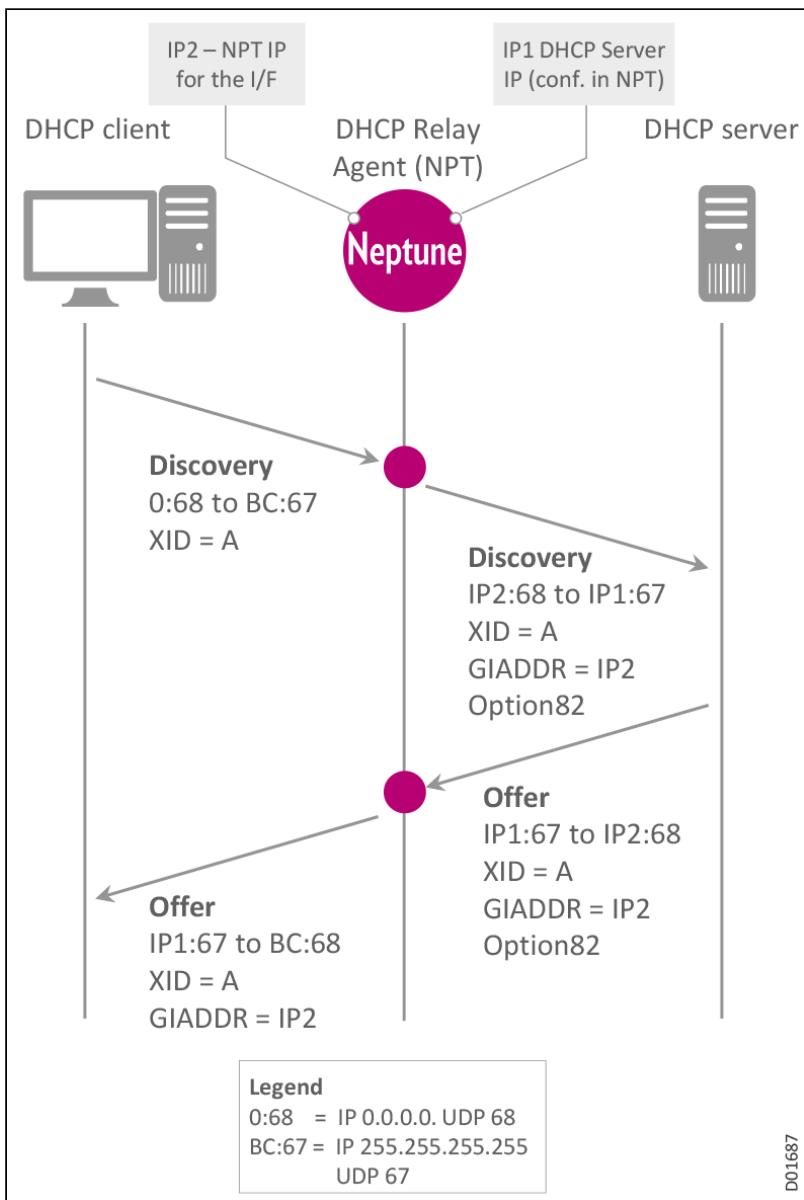
- The PE traps broadcast DHCP messages generated by the IP hosts (clients). The PE then adds itself as the relay agent (`giaddr`), optionally adds local information (option 82), and sends unicast messages to remote preconfigured DHCP servers.
- The PE also traps unicast messages received from DHCP servers, removes local information, and sends unicast or broadcast messages to the client.

### DHCP Relay Agents



**DHCP option 82** provides additional security when DHCP is used to allocate network addresses. Option 82 enables the controller to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.

## DHCP Option 82



## DHCP Relay for IPv6

**DHCPv6** is an updated version of DHCP, designed for IPv6. DHCPv6 supports the new addressing mode used in IPv6, and can also be used for renumbering. The DHCP process is same as in IPv4:

- The client first detects the presence of routers on the link.
- If found, it then examines router advertisements to determine if DHCP can be used.
- If no router is found or if DHCP can be used, then a DHCP Solicit message is sent to the All-DHCP-Agents multicast address, using the link-local address as the source address.

DHCPv6 supports IPv6 addressing and configuration requirements. For example, it supports "prefix delegation", not just "address assignment". While IPv6 does provide stateless autoconfiguration for addresses, DHCPv6 is necessary to configure 'other-configuration' information, such as DNS servers, domain search lists, etc. Stateless configuration is also a 'one-size-fits-all' approach, unable to assign addresses selectively, and policies cannot be enforced for client-allowed addresses.

DHCPv6 is not simply a patch built over the original DHCP. DHCPv6 offers a clean, efficient design, including:

- New optimized packet format (no BOOTP legacy)
- 16-bit option space, 16-bit option lengths
- Encapsulation, where some messages/options encapsulate others
- Client may obtain many addresses (not just one)
- Client and server use DUID (DHCP Unique IDentifier)
- Relay agent always involved, unless server allows otherwise
- Client has link-local address so can communicate on-link
- Link-local multicasting used (client to relay/server)
- Server to client or relay to client communication via link-local unicast

The DHCP Unique Identifier (DUID) is used by client and server to identify themselves. The DUID should remain stable and unique for the long term. Three types of DUID are defined in RFC 3315:

- Link-layer address plus time (DUID-LLT)
- Vendor-assigned unique ID based on Enterprise ID (DUID-EN)
- Link-layer address (DUID-LL)

# Border Gateway Protocol BGP

BGP is a standardized protocol designed to exchange routing and reachability information between autonomous systems (AS) on the Internet. The protocol is often classified as a path vector protocol but is sometimes also classed as a distance-vector routing protocol. BGP makes routing decisions based on paths, network policies, or rule-sets configured by a network administrator. BGP is also involved in making core routing decisions. Changes in topology trigger incremental updates, with new routes updated and lost routes withdrawn.

BGP neighbors, called peers, are established by manual configuration between neighbor-routers to create a TCP session on port 179. A BGP speaker sends keep-alive messages every 60 seconds to maintain the connection. Among routing protocols, BGP is unique in using TCP as its transport protocol.

The current version of BGP is version 4 (BGP4), defined in RFC 4271 and based on RFC 1771. The major enhancement was support for Classless Inter-Domain Routing (CIDR) and use of route aggregation to decrease the size of routing tables.

BGP may be used for routing within an AS. In this application it is referred to as Interior Border Gateway Protocol, Internal BGP, or iBGP. The internet application of the protocol may be referred to as Exterior Border Gateway Protocol, External BGP, or eBGP.

Standard BGP supports IPv4 unicast prefixes. Neptune also supports Multi-protocol Extensions for BGP (MP-BGP) that are needed for IPv6 and L3VPN implementation. MP-BGP supports different addresses:

- IPv4 unicast
- IPv4 multicast
- IPv6 unicast
- IPv6 multicast

MP-BGP is also used for MPLS VPN to exchange the VPN labels. For each different type of address, MP-BGP uses a different address family.

A BGP peer retains routing information from a neighboring peer when it goes down for a certain length of time. When it comes back up and the router receives refreshed routing information, it compares the new information with that retained. The router can thus preserve the routing state of BGP even during short peer outages.

This introduction to BGP includes the following sections:

- ADD-PATH Support
- AIGP for BGP
- BGP Graceful Restart
- BGP Prefix Independent Convergence: BGP PIC
- BGP Route Aggregation
- ECMP for BGP
- Labeled Unicast: BGP-LU - RFC3107
- Route Reflection
- Virtual Route Reflection: vRR

## ADD-PATH Support

BGP specification RFC 4271 defines an Update-Send Process to advertise the routes chosen by the Decision Process to other BGP speakers. No provisions are made to allow advertisement of multiple paths for the same address prefix or Network Layer Reachability Information (NLRI). In fact, a route with the same NLRI as a previously-advertised route implicitly replaces the previous advertisement.

ADD-PATH support for BGP (RFC 7911) utilizes a BGP extension that allows advertisement of multiple paths for the same address prefix without the new paths implicitly replacing any previous ones. This is accomplished by identifying each path with a Path Identifier in addition to the address prefix.

Availability of the additional paths can help reduce or eliminate persistent route oscillations (RFC 3345). It can also help with optimal routing and routing convergence in a network by providing potential alternate or backup paths, respectively.

With ADD-PATH capabilities, the PEs request ADD-PATH from the RR. The PEs use the best-external option towards the RR. The RRs use the second-best option towards each other and towards the PEs.

## AIGP for BGP

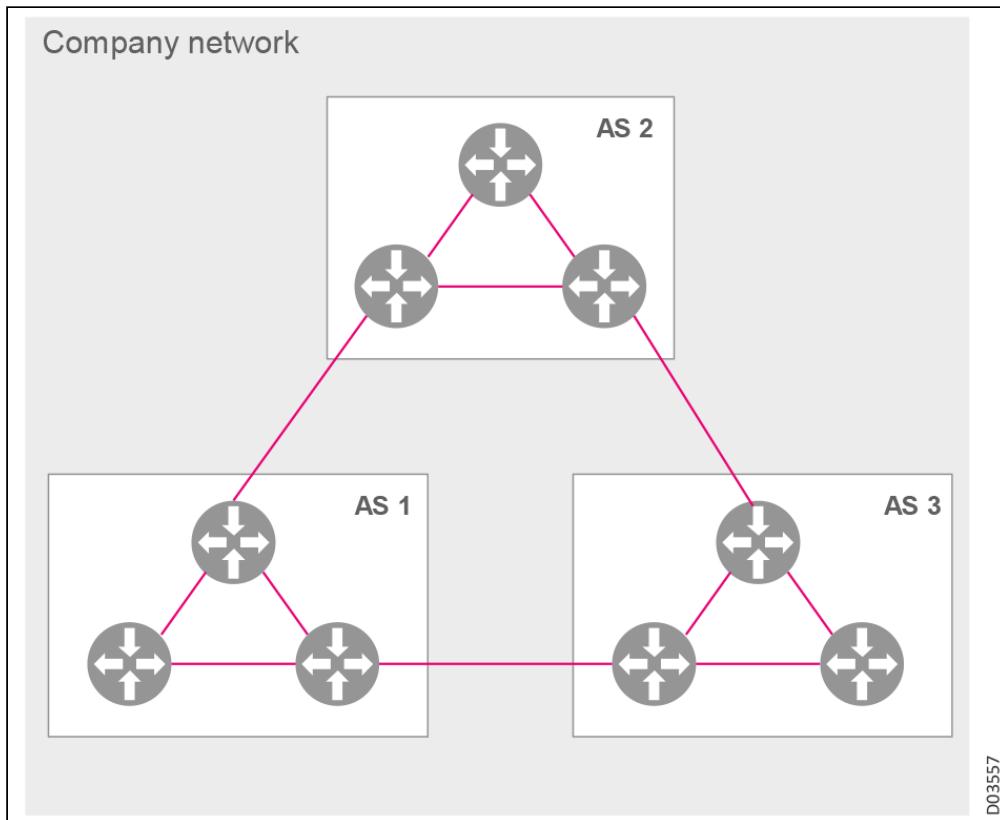
There are many routing protocols that have been designed to run within a single administrative domain, exchanging [routing table](#) information between gateways (typically [routers](#)) *within* an [autonomous system](#) (for example, a system of corporate local area networks). This routing information can then be used to route [network-layer protocols](#) like [IP](#). These are known collectively as "Interior Gateway Protocols" (IGPs). Specific examples of IGPs include [Open Shortest Path First: OSPF](#) and [Intermediate System to Intermediate System: IS-IS](#).

Typically, each link is assigned a particular "metric" value. The path between two nodes can then be assigned a "distance", which is the sum of the metrics of all the links that belong to that path. An IGP selects the "shortest" (minimal distance) path between any two nodes, perhaps subject to the constraint that if the IGP provides multiple "areas", it may prefer the shortest path totally contained within an area, rather than a path that traverses more than one area. Typically, the network administration has some routing policy that can be approximated by selecting shortest paths in this way.

By contrast, exterior gateway protocols (EGPs) are used to exchange routing information *between* autonomous systems; EGPs rely on IGPs to resolve routes *within* an autonomous system. BGP, as opposed to the IGPs, was designed to run over an arbitrarily large number of administrative domains ("autonomous systems" or "ASs"), with limited coordination among the various administrations. BGP does not make its path-selection decisions based on a metric; there is no such thing as an "inter-AS metric", for two basic reasons:

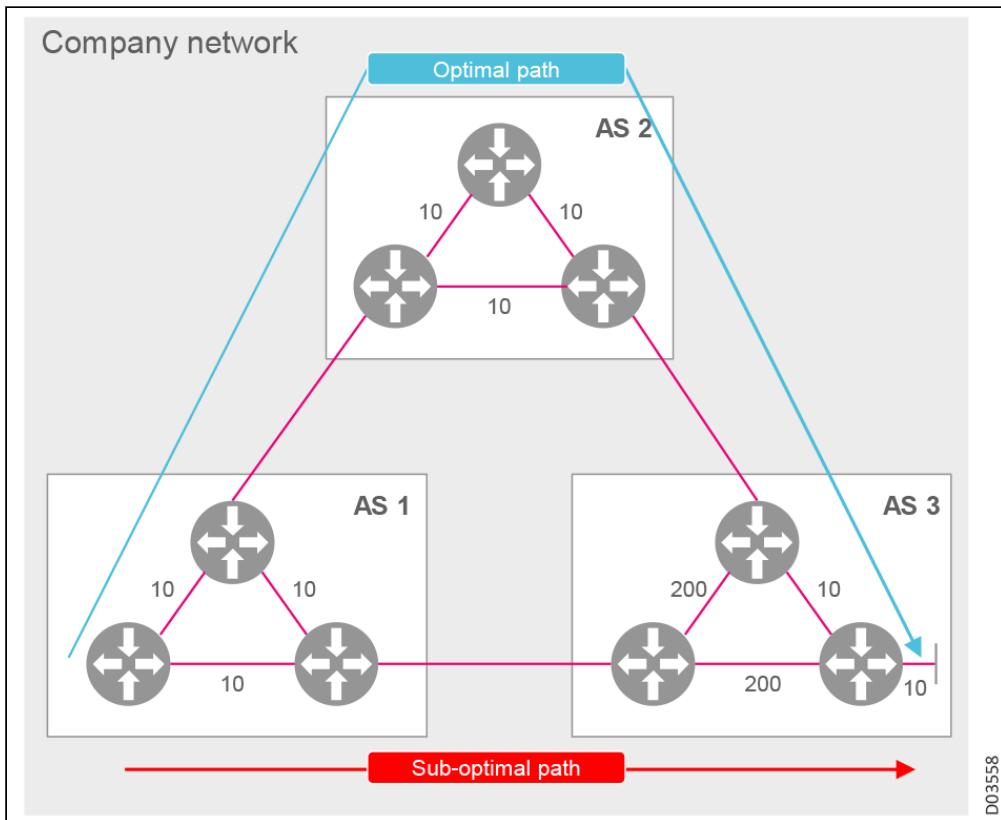
- The distance between two nodes in a common administrative domain may change at any time due to events occurring in that domain. These changes are not propagated around the Internet unless they actually cause the border routers of the domain to select routes with different BGP attributes for some set of address prefixes. This accords with a fundamental principle of scaling, that changes with only local significance must not have global effects. If local changes in distance were always propagated around the Internet, this principle would be violated.
- A basic principle of inter-domain routing is that the different administrative domains may have their own policies, which do not have to be revealed to other domains and which certainly do not have to be agreed to by other domains. Yet, the use of an inter-AS metric in the Internet would have exactly these effects.

### Network Organized into Multiple Areas



A network with multiple IGPs and BGP in between, instead of a single IGP, introduces a potential problem. BGP selects a path using the best path selection algorithm, which isn't based on a "lowest metric" as IGPs do. What happens is that your router will sometimes select sub-optimal paths in your network, as illustrated in the following figure. The routers in this example don't have any inside metric information about the other ASs. AS 1 has no way of knowing that somewhere inside AS 3, there are some very slow, congested links. In this example, the "long" way around is actually much faster.

### Potential to Select Sub-Optimal Path



In these types of networks, it can be useful to allow BGP to make its decisions, based on the IGP metric, allowing BGP to choose the shortest end-to-end path between two nodes, even if the nodes are in two different ASes within the same administrative domain. There are, in fact, some implementations that already do something like this, using BGP's MULTI\_EXIT\_DISC (MED) attribute to carry a value based on IGP metrics. However, that doesn't really provide IGP-like shortest path routing, as the BGP decision process gives higher priority to other factors, such as the AS\_PATH length.

[RFC 7311](#) defines a new non-transitive BGP attribute called the "**Accumulated IGP Metric Attribute**", or "AIGP attribute", and specifies the procedures for using it. BGP routers advertise this AIGP metric to neighbors in other ASes. This allows BGP routers to select the best path based on the end-to-end IGP metric.

AIGP impacts the BGP best-route decision process. The AIGP attribute preference rule is applied after the local-preference rule. The AIGP metric is used as a tie-breaker factor, before other important attributes like the AS path length or MED. The BGP best-route decision process also impacts the way the interior cost rule is applied if the resolving next hop has an AIGP attribute. Without AIGP enabled, the interior cost of a route is based on the calculation of the metric to the next hop for the route. **With AIGP enabled, the resolving AIGP distance is added to the interior cost.**

The AIGP attribute is particularly useful in networks that use tunneling to deliver a packet to its BGP next hop (i.e., using BGP LU in a multi-AS /multi-IGP domain). Targeted applications for AIGP include:

- Multi-IGP Domain networks using BGP LU for inter-IGP domain MPLS communication
- Multi-BGP AS networks using BGP LU for inter-AS MPLS communication

## BGP Graceful Restart

Graceful restart is an optional capability added to BGP to minimize route flapping when BGP peers restart, or if the TCP connection between BGP peers goes down. Graceful restart allows a BGP peer to retain the

routing information from a neighboring peer when it goes down, for a certain period of time. This allows the device to preserve the routing state of BGP during short peer outages.

We support Graceful Restart in accordance with [RFC 4724: BGP Graceful Restart](#) and [RFC 4781: Graceful Restart Mechanism for BGP with MPLS](#).

## BGP Prefix Independent Convergence: BGP PIC

As a path vector protocol, BGP propagates reachability serially. Therefore, BGP convergence speed is limited by the time required to serially propagate reachability information from the point of failure to the device that must re-converge. BGP speakers exchange reachability information about prefixes. For labeled address families, an edge router also assigns local labels to prefixes and associates the local label with each advertised prefix, such as L3VPN or 6PE, using the BGP-LU technique.

In modern networks, it is not uncommon to have a prefix reachable via multiple edge routers. Another common and widely deployed scenario is L3VPN with multi-homed VPN sites, with unique Route Distinguishers. It is advantageous to utilize the commonality among paths used by NLRI to significantly improve convergence in case of topology modifications.

BGP Prefix Independent Convergence (PIC) is a method which allows traffic to be restored to a pre-calculated alternative equal-cost primary path or backup path, within a time period that does not depend on the number of BGP prefixes. The technique relies on internal router behavior that is completely transparent to the operator and can be incrementally deployed and enabled with zero operator intervention.

BGP PIC decreases the data plane convergence time by installing an alternate path. There are two flavors:

- **BGP PIC Core:** Decreases convergence time when a **core router** fails and your IGP has to find a new best path to your PE router.
- **BGP PIC Edge:** Decreases convergence time when a **PE router** fails and BGP has to switch to a different PE router.

Links and nodes in the core or edge of the network can be recovered within less than a second; in most cases in under 100ms. The exact timing depends on IGP convergence, so either IGP should be fine-tuned or IGP FRR can be used. BGP PIC can essentially be thought of as a BGP Fast Reroute mechanism, which relies on IGP convergence for the failure detection.

## BGP Route Aggregation

Route Aggregation (RA) (aka BGP Route Summarization) is a method that helps minimize the size of the routing tables in an IP network by consolidating a selected group of multiple routes into a single route advertisement. This approach is in contrast to non-aggregation routing, in which every routing table contains a unique entry for each route. Note that the aggregation methodology does not help reduce the size of the routing-table on the router that does the aggregation. However, once you configure an export policy that only advertises the aggregate route, without all the contributing routes, you then benefit from the efficiency of the aggregation for the rest of the routers receiving updates. RA reduces the size of the global routing table, decreasing router workload and saving network bandwidth.

An aggregate route becomes active when it has one or more contributing routes. A contributing route is an active route that is a more specific match for the aggregate destination. For example, for the aggregate destination 192.168.0.0/16, routes to 192.168.192.0/19 and 192.168.67.0/24 are contributing routes, but routes to 192.168.0.0/8 and 192.168.0.0/16 are not. A route can only contribute to a single aggregate route. However, an active aggregate route can recursively contribute to a less-specific matching aggregate route. For example, an aggregate route to the destination 192.168.0.0/16 can contribute to an aggregate route to 192.168.0.0/13.

BGP allows the aggregation of specific routes into one aggregate route through the use of an aggregate-address address mask. In our implementation, the aggregate route configuration is stored in a BGP instance `afi-safi`. The aggregate route state is stored in `bgp-local-rib` and `neighbor-adj-rib-out`. A policy is defined to prevent advertisement of aggregate and contributing routes to remote VRFs.

When an aggregate route becomes active, it is installed in the routing table with the following information:

- Reject next hop — If a more-specific packet does not match a more-specific route, the packet is rejected and an ICMP unreachable message is sent to the packet's originator.
- Metric value, as configured with the aggregate statement.
- Preference value that results from the policy filter on the primary contributor, if a filter is specified.
- AS path, as configured in the aggregate statement, if any. Otherwise, the path is computed by aggregating the paths of all contributing routes.
- Community as configured in the aggregate statement, if any is specified.

The benefits of route aggregation in terms of efficiency are obvious - multiple BGP routes are aggregated into a single route, reducing the number of routes that must be advertised between BGP speakers in the global VRF and reducing the number of routes advertised in the L3VPN.

However, it must be noted that the increased efficiency of the smaller routing tables comes at a price. For example, when you reduce the amount of detailed information being stored at each point, it leads to a corresponding reduction in granularity for policy control. Once a more-detailed set of information has been collapsed into a more-general piece of information for all members of a specific equivalence class of destinations, the same policies will apply to all destinations and paths in that equivalence class.

Nevertheless, BGP Route Aggregation can be very useful in the following contexts:

- Aggregate route for address families: IPv4 Unicast and IPv6 Unicast
- Aggregate route for:
  - Internal and External BGP neighbors in global VRF
  - Towards eBGP neighbor of L3VPN VRF
  - Towards L3VPN remote VRF

## ECMP for BGP

The basic BGP implementation selects only one best path as candidate for FIB installation. BGP then advertises only this one best path. As a result, failure recovery is very slow. This one best path ends up being congested while the other possible paths are rarely used. The commonly-used solution to this issue is to use Equal Cost Multiple Paths (ECMP) for BGP.

ECMP is a routing strategy where next-hop packet forwarding to a single destination can occur over multiple "best paths" which tie for top place in routing metric calculations. Multi-path routing can be used in conjunction with most routing protocols, because it is a per-hop decision limited to a single router. It can substantially increase bandwidth by load-balancing traffic over multiple paths.

With ECMP, when running a single BGP session over multiple links using loopback addresses and eBGP multi-hop, static routes are configured via the multiple links. Load sharing/balancing is accomplished over the multiple links using ECMP for native IP traffic, when eBGP is used as the PE-CE protocol.

When running a separate BGP session over each of the equal cost links, multiple paths are received for each prefix. If the maximum number of paths is configured, and all received paths have the same cost, then all these paths enter the FIB and load balancing happens.

This method consumes more memory and CPU time, but has the advantage that each link may be connected to a different router, working with multiple neighbors (sessions) per VRF/dual homing. ECMP over multiple links in a non-global VRF is also supported, providing protection and load balancing, as well as increasing bandwidth of flows from PE to CE or CE-site.

## Labeled Unicast: BGP-LU - RFC3107

When BGP is used to distribute a particular route, it can also be used to distribute an MPLS label that is mapped to that route. The BGP Labeled Unicast (BGP-LU) multiprotocol extension is used to distribute an MPLS label that is mapped to a particular route. The label mapping information for a particular route is piggybacked in the same GP update message that is used to distribute the route itself.

It can also be used to advertise an MPLS transport path between IGP regions and Autonomous Systems. Also, BGP-LU can help to solve the inter-domain traffic-engineering problem. BGP-LU can be deployed in large-scale networks together with MPLS and Segment Routing.

BGP-LU is widely implemented in the industry, field proven, interoperable with many vendors. It's considered the corner stone of "Seamless MPLS". Using BGP's ability to carry label information, RFC3107 builds on the Multi-Protocol BGP extension MP\_REACH\_NLRI attribute using AFI 1 (IPv4) with SAFI 4 (NLRI with MPLS labels) to indicate the presence of a label, thus making it possible to "piggy-back" MPLS label mapping information for a particular prefix.

BGP-LU provides a way to create end-to-end connectivity and enable inter-region (PE to PE) communication for regions which do not share IGP routing information. It provides:

- A mechanism to create H-LSP, spanning across different IGP/LDP domains ("stitched LSP")
- A mechanism to maintain scalable network topologies / service architecture, such as MP-BGP Inter-AS or single BGP AS over multiple IGP AS.

BGP-LU supports use-cases such as:

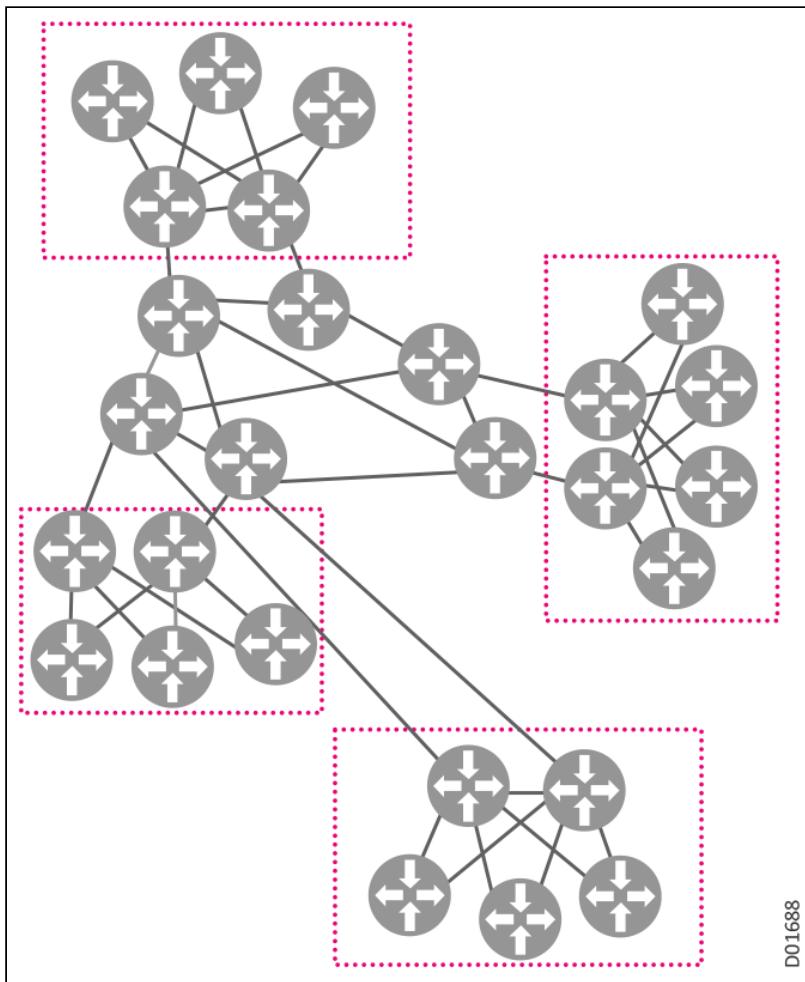
- Inter-AS Option C
- Multi-AS IGP Single BGP AS
- H-LSP support

## Route Reflection

Networks are typically organized into a hierarchical structure, in which edge routers send traffic through hub aggregators to the core routers. This naturally hierarchical structure enables a simple scaling approach that offers significant benefits for BGP networks. Rather than implementing an iBGP full mesh configuration for each router, routers can simply 'learn' the routes used by the router that is located one level 'up' in the network, who reflects those routes back. In a typical route reflection (RFC-4456) implementation:

- Edge routers are the route reflection clients of the hub aggregators.
- Hub aggregators are the route reflection clients of the core routers.
- Core routers at the highest level of the hierarchy maintain the full iBGP mesh topology.

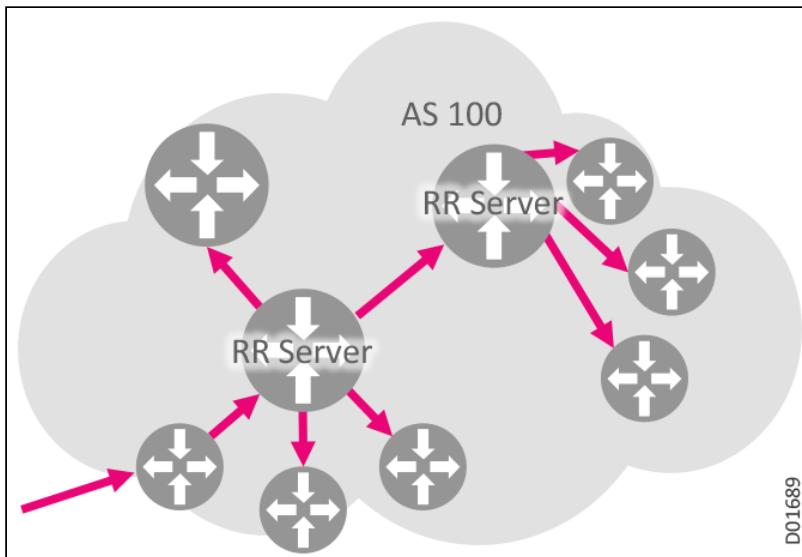
### Typical Network Hierarchy



D01688

Routers that are not located at the central core or 'high' point of the network don't have to maintain a full mesh iBGP configuration. A router can simply be a client of a route reflection server. The route reflection server 'reflects' the best paths between any one of its clients and all other clients (and non-clients). Route reflectors are typically used in a hierarchical topology, and are therefore themselves deployed hierarchically. The router reflector server may *have* its own clients and may also *be* a client of another route reflector server.

### Route Reflector Server that is Also a Client of Another Route Reflector



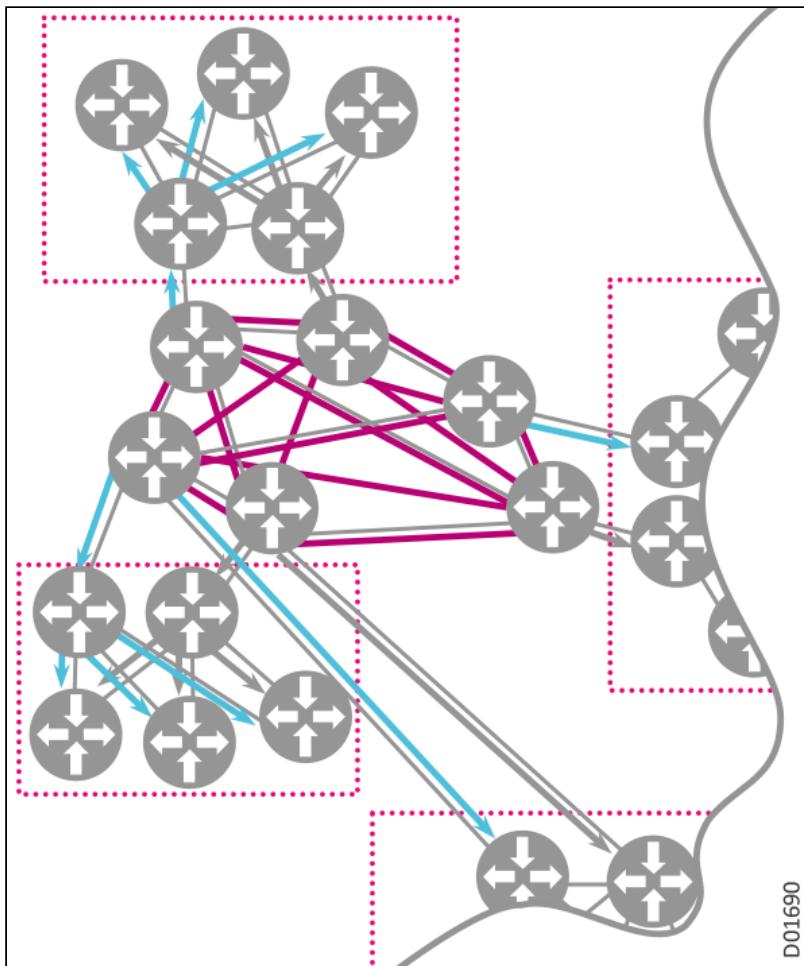
Route reflectors do not reflect or provide best-path analyses between non-clients. Traffic between two non-clients must rely on standard iBGP behavior.

Each route reflection server and its downstream clients form a cluster. Clusters are identified by a unique number. If each router reflection server is in its own cluster, then the cluster number can simply be the router ID number. Each router reflection sever adds its cluster ID to a list of clusters used when advertising a path. To prevent infinite looping, route reflector servers do not 'learn' paths that include their own cluster ID in the list.

A typical route reflection topology, with built-in redundancy, is constructed based on the following guidelines:

- Each edge device is a client of *two* upstream hub aggregators.
- Hub aggregators are route reflection *servers* for edge routers.
- Hub aggregators are *clients* of the core routers.
- Core routers are route reflection *servers* for hub aggregators.
- Core routers are the highest level of the hierarchy and have knowledge of the full iBGP mesh topology of the network.

### Typical Route Reflector Topology with Built-in Redundancy



A route reflection topology offers multiple path options to the participating servers and clients. Each route reflection server 'learns' the available path options from its clients. The server then chooses a single best path and reflects that path back to its clients. Each route reflection client ends up 'learning' a single path for each route in the network. The route reflection servers also advertise the best client paths to non-clients in the network. NEs that are not aware that they are clients simply follow standard iBGP rules.

Another route reflection option is introduced in [Virtual Route Reflection: vRR](#).

## Virtual Route Reflection: vRR

Standard Route Reflection (RR) provided an excellent mechanism for BGP peering scaling, solving NxN full-mesh BGP interconnection issues, and distributing BGP routes to PEs. Traditionally, dedicated routers were used to provide the BGP RR functionality within the network. However, RR built on classic platforms targeted data plane forwarding rather than control plane processing. This method can reduce robustness while increasing route convergence times. The approach is fundamentally inflexible and unnecessarily expensive.

The trend in RR is to move in a new direction. There is a growing need for:

- More control plane memory
- Smaller footprint devices
- Out-of-path topologies
- Detaching RIB from FIB, to speed up convergence
- Leveraging commodity hardware
- Virtualization

- Innovation through software
- Elimination of hardware limitations

The industry is, therefore, moving towards virtual Route Reflection (vRR), which offers innovation through software, eliminating hardware limitations, and allowing network operators to leverage their commodity hardware. vRR can run on commodity x86 hardware using VM Image/VMware, ESXI, KVM, Citrix XenServer, Microsoft Hyper-V, and more.

vRR advantages include:

- Scalability (64 bit OS)
- Performance (with multi-core support)
- Requiring less infrastructure space
- Addressing control plane memory requirements
- Deploying out of path topologies for better convergence

For example, vRR implementations that are based on out-of-path topologies offer many benefits, such as:

- Reduction of BGP memory footprint in the MPLS core
- Reduction of control plane CPU footprint in the MPLS core
- Remove impact the core has on routing convergence
- Drastically reduce day-to-day operational contact with the core
- Remove impact of backbone flaps on route reflector CPU
- Run the latest routing features without impacting core forwarding
- Keep maintenance to the core at an absolute minimum
- Avoid unnecessary upgrades in the MPLS core to support routing enhancements which are relevant only for BGP

Neptune's Virtual BGP Route Reflector (vRR) implementation is, in fact, a virtualization of the same control plane functions available in the Neptune platforms, provided to the end-customer as a containerized application, and allowing for flexible deployment models ranging from dedicated servers to cloud data center hosts.

# Intermediate System to Intermediate System IS-IS

IS-IS is an interior gateway protocol (IGP) that uses link state information for the nodes to discover and establish adjacencies, and thereby determine the availability of routes. Nodes also distribute and synchronize link state databases through a reliable flooding mechanism. IS-IS runs directly on Layer 2, distributing routing information between routers belonging to a single Autonomous System (AS). Each router in the AS eventually learns the same link state database. IS-IS uses an SPF (Shortest Path First) algorithm, such as Dijkstra's, to compute the best path and define a complete set of 'shortest-path tree' routes through the network. Shortest path selection guarantees loop-free routing.

The International Organization for Standards (ISO) developed IS-IS as part of the Open Systems Interconnection (OSI) protocol suite. The ISO originally developed IS-IS to route data in an ISO Connectionless Network Protocol (CLNP) network (ISO10589 or RFC 1142) and afterwards was adapted for IP Routing in addition to CLNP (RFC1195) as integrated or dual IS-IS. IS-IS is generally the IGP of choice for large service providers.

This section introduces the following IS-IS features:

- IS-IS Level 1 and Level 2
- IPv6 Support in IS-IS
- IS-IS Support for Segment Routing SR
- SPF and LSP Delay Algorithms for IS-IS
- IS-IS Graceful Restart

## IS-IS Level 1 and Level 2

In IS-IS, a single AS can be divided into smaller groups, called areas. Routing between areas is organized hierarchically, allowing one domain to be administratively divided into many smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area; when the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs. No IS-IS area functions strictly as a backbone.

Level 1 routers share intra-area routing information. Level 2 routers share inter-area information about IP addresses available within each area. Uniquely, IS-IS routers can act as both Level 1 and Level 2 routers, sharing intra-area routes with other Level 1 routers and inter-area routes with other Level 2 routers.

The propagation of link-state updates is determined by the level boundaries. All routers within a level maintain a complete link-state database of all other routers in the same level. Each router then uses the Dijkstra algorithm to determine the shortest path from the local router to other routers in the link-state database.

Multiple IS-IS instances can coexist within a router, where each IS-IS instance can support either a single Level 1 or Level 2 area, or one of each. By default, all IS-IS instances automatically support Level 1 and Level 2 routing. When multiple instances of IS-IS are being run, an interface can be associated with only one instance (process). Instances may not share an interface.

## IPv6 Support in IS-IS

Since IS-IS runs directly on the data-link layer (Layer 2), from the IS-IS perspective there is nothing different or special about configuring it for an IPv6 environment. The only thing to do differently is to use an IPv6 address instead of or in addition to an IPv4 address.

To provide IPv6 unicast routing, the following changes are required:

- New TLV for IPv6 to describe IPv6 routes (RFC5308):

- TLV 236: IPv6 reachability is equivalent to IPv4 internal reachability TLV and IPv4 external reachability TLV
- TLV 232: IPv6 interface addresses
- IPv6 NLPID (0x8E) advertised by IPv6-enabled routers
- Supporting only wide metric
- Supporting a single topology when adding IPv6:
  - When both IPv4 and IPv6 protocols are supported on IS-IS, all L3 LIFs have both IPv4 and IPv6 with the same metric
- Supporting a dual-stack solution via introduction of Multi-Topology for IPv6 and introduction of new TLVs as defined in RFC5120:
  - TLV 222: MT Intermediate Systems once supporting IPv4 user MT
  - TLV 237: Multi-Topology Reachable IPv6 Prefixes, an extension of TLV 236
  - When both IPv4 and IPv6 protocols are supported on IS-IS, L3 LIFs can have one of the following:
    - IPv4 only
    - IPv6 only
    - Both IPv4 and IPv6 with the same metric
  - When only IPv6 is supported on IS-IS, L3 LIFs can have IPv6 only
- Supporting transition from Single-Topology to Multi-Topology to prevent back holes via transition option

## IS-IS Support for Segment Routing SR

Segment routing can be used to add the concept of abstract segments to IS-IS routing protocols. Abstract segments make it possible to add the ability to perform shortest-path routing and source-routing. An abstract segment can represent the local prefix of a node, a specific adjacency of the node (interface or next-hop), a service context, or a specific explicit path over the network. For each segment, the IGP advertises an identifier referred to as a Segment ID (SID).

When a segment routing is used in the MPLS data plane, the SID is a standard MPLS label. When forwarding a packet using segment routing, the router pushes one or more MPLS labels.

### IS-IS Segment Routing Extensions

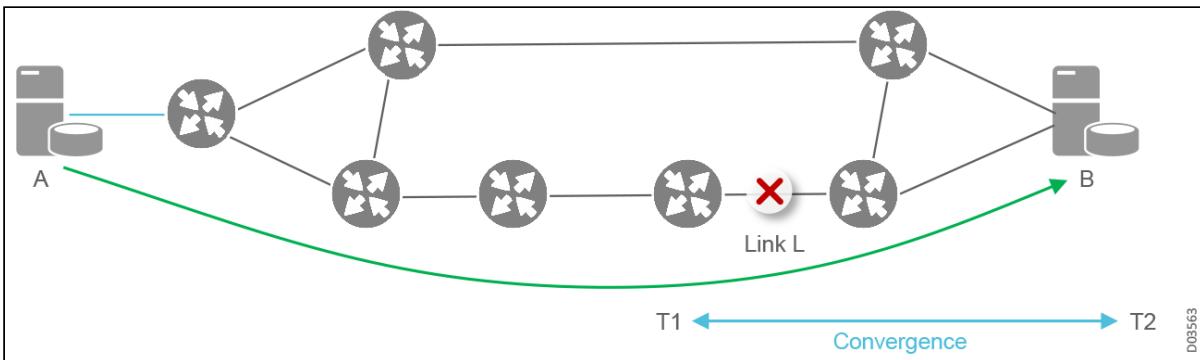
New TLV/sub-TLVs are defined in RFC 8667 (*IS-IS Extensions for Segment Routing*) and are supported in the IS-IS implementation of segment routing. This includes:

- The prefix SID sub-TLV
- The adjacency SID sub-TLV
- The SID/Label Binding TLV
- SR capabilities sub-TLV

## SPF and LSP Delay Algorithms for IS-IS

For a network to *converge*, all routers in the network must collect from each other and agree on all the network topology information. This information must be consistent, reflecting the current state of the network, and free of routing loops or any other kinds of corruption.

### Fast Convergence



Convergence involves the following stages:

- **Event detection**, including considerations such as:
  - How fast can we detect a change in topology (through the hardware or through IGP protocol timer expiration)?
  - Do we use BFD on the interface to speed up defect detection?
- **Event propagation**, including considerations such as:
  - Once a problem is detected, how fast can we inform others?
  - When there is a change, the LSP must be flooded as fast as possible by the neighbor
  - We must flood the LSP that triggers SPF before SPF execution
- **Event processing**, including the following steps:
  - Run SPF (Dijkstra algorithm) to recalculate routes *only* if there have been topology changes (nodes or links), in order to re-compute SPT and the RIB table values
  - Run a partial route calculation (PRC) *only* if an IP prefix has changed. We can keep the SPT, and just update the RIB table entries for the nodes whose prefixes have changed.
- **Update RIB/FIB**, selecting the best routes from the local IGP LSDB, sets of static routes, and BGP decisions
- **IGP convergence status**, where historically IGP convergence would be on the order of 10-30s, focusing on stability rather than speed.

Emphasizing stability over speed sometimes led to undesired consequences. For example, in some contexts, with fast reroute techniques, traffic restoration may be completed well before network convergence! In any case, today speed is an essential factor; convergence must be in the range of milliseconds rather than seconds, with no compromise on stability or scalability.

Network interface speeds are growing rapidly. It's common to see very-high-bandwidth links between two devices, especially in core networks. Consider the failure of such a trunk for only two seconds. Imagine how much information would be lost during the failure before the network is once again fully converged. Default routing protocol timers are not 'good enough' for networks with high-speed interfaces that need such levels of convergence speed. Networks require faster failure detection, faster event reporting and table calculations, and faster times for the forwarding engine to react to topology changes and adjust its tables.

*Fast convergence* describes a quick convergence time, meaning the time required by all the routers in the network to flood and incorporate the relevant network topology information. By fast convergence we usually mean sub-second convergence time. However, if dealing with unstable networks, this approach can backfire. **The trick is to react more quickly to initial events, but in situations of constant churn, to slow down convergence time enough to avoid collapse.** This means that in stable periods, with rare triggers, actions are processed promptly. But as stability decreases, and trigger frequency increases, a mechanism must be built in to delay processing of the related actions.

This section introduces the following delay mechanisms:

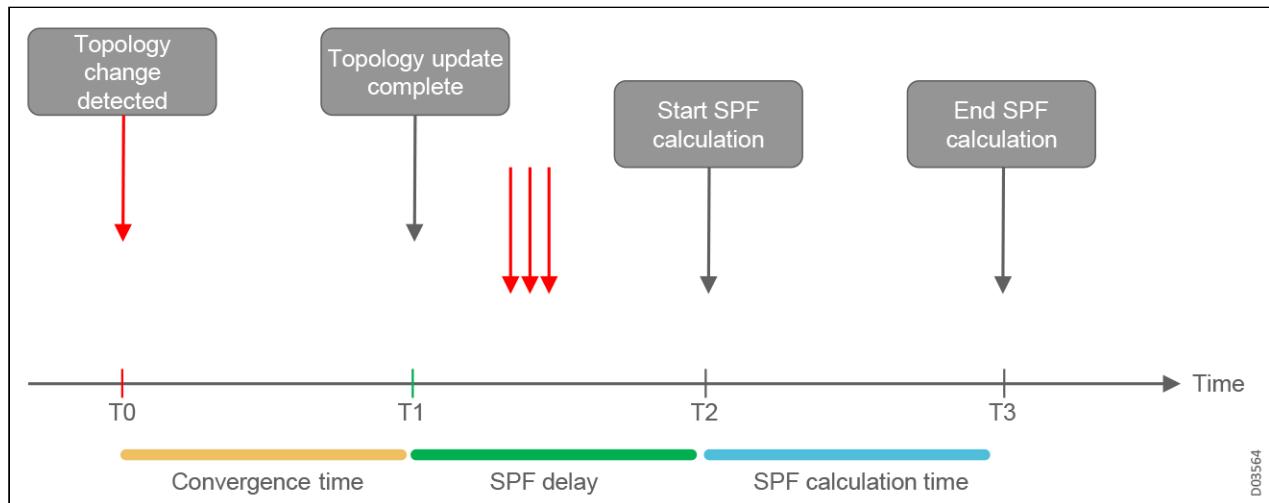
- What is SPF Delay in IS-IS
- What are LSP Generation Timers

- IS-IS SPF and LSP Generation Mechanisms

## What is SPF Delay in IS-IS

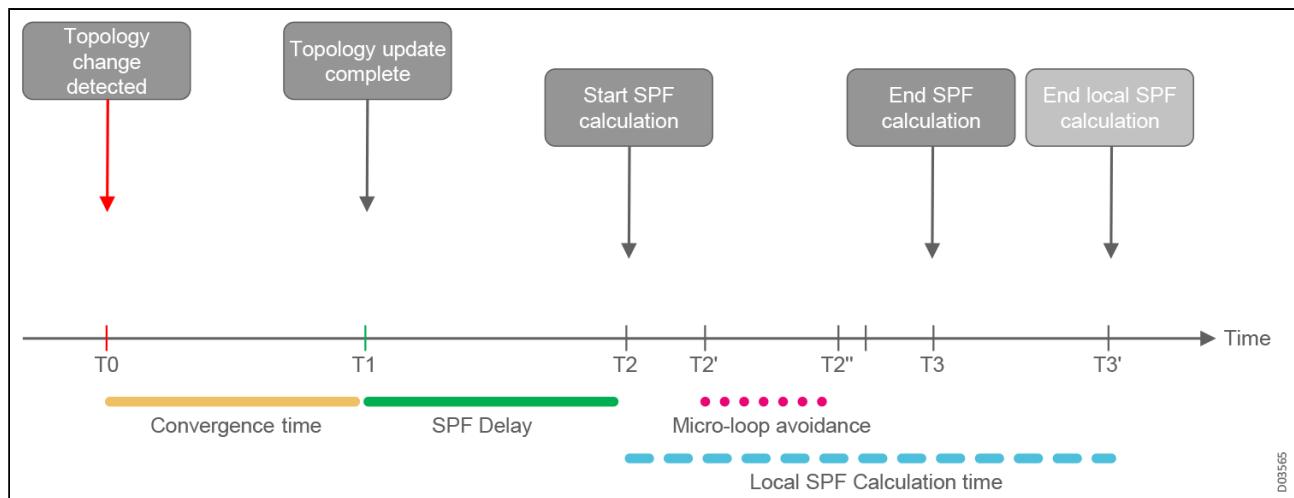
SPF delay is the delay time between the first IGP event triggering a new routing table computation, and the actual start of that routing table computation. SPF delay can be a good thing - the parameter is often associated with a damping mechanism to slow down reaction times by incrementing the delay timer setting when the IGP becomes unstable. As illustrated in the following figure, you don't want to start a new set of SPF calculations before the topology update has been completed. When there are many topology change events, inserting an SPF delay period slows down SPF calculations to avoid system collapse

### SPF Delay



RFC 8405 defines a back-off algorithm to use for SPF delay. RFC8333 defines an additional mechanism to delay local convergence, compared to the network-wide convergence, when traffic is protected by FRR or administrative deactivation. This helps avoid local micro loops, as illustrated in the following figure.

### Local SPF Calculation



In this example, a topology change is detected at T0. The topology update is completed at T1. The initial convergence time is the time period between T0 and T1. An SPF delay factor is added, so the new SPF calculations are only started at T2. The main SPF calculation is completed at T3. If there is also a **local** link down, that local SPF calculation is delayed through use of a micro-loop delay-timer, and is only completed at time T3'.

## What are LSP Generation Timers

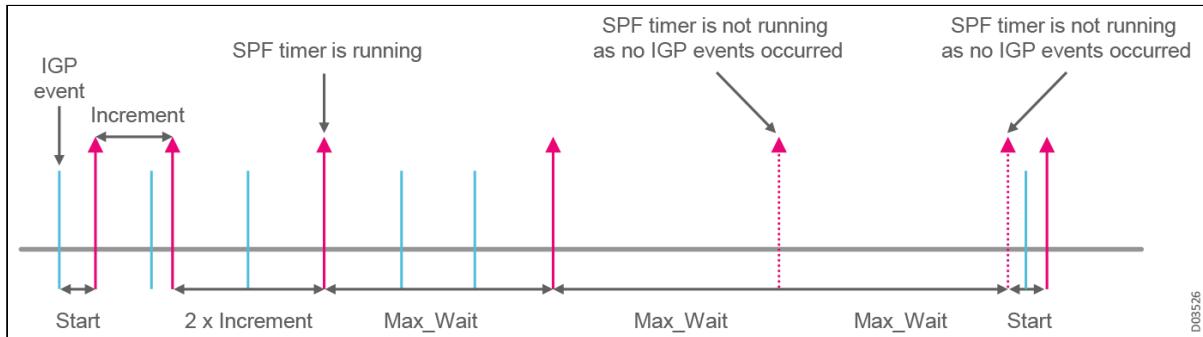
LSPs are Link State PDUs (Protocol Data Units), used by IS-IS protocols. The collected link state PDUs of all routers and networks form the IS-IS protocol's link state database. If there is a change in the LSP database, the system must complete a new SPF calculation. Neptune platforms provide a built-in delay mechanism, with values configure for **initial wait time**, **minimum/maximum wait time**, and an **exponential increment value**, for maximum efficiency in times of network stability and instability.

Similarly, if there is a change in the local LSP values, the system must generate a new LSP and flood the network with the new values. Again, a built-in delay mechanism, with values configure for initial wait time, minimum/maximum wait time, and an exponential increment value, enables maximum efficiency in times of network stability and instability.

For example, suppose the network was stable for a relatively long time. Then an LSP-triggering event occurs. The router delays SPF computations for the **start parameter** (initial wait time) amount of milliseconds, and also increases the **next** wait-time value by the **increment-parameter** number of milliseconds. Next, if another event occurs *after* the start-wait window expires, the event would be held for processing until the **increment-parameter** window of milliseconds expires. At the same time, the **next** wait-time value would be doubled, set to **2\*increment**.

Every time an event occurs *during the current wait-time window*, the processing is delayed until the current wait-time expires *and the next* wait-time interval is doubled. The wait-time grows exponentially until it reaches the **max\_wait** value. After this, for every event received during the current wait-time window, the next wait-time interval remains equal to the constant **max\_wait** value. This ensures that exponential wait-time growth is limited by a ceiling value. If there are no events for the duration of **2\*max\_wait** milliseconds, the hold-time window is reset back to the **start** value, assuming the network has returned to a stable condition. A typical sequence is illustrated in the following figure.

### LSP Generation Timers



The first event triggers an SPF to be run in **start** milliseconds. At the same time, the next wait interval is set to **increment** milliseconds. Since there is an event during the second wait interval, the third wait interval is set to **2\*increment**. There is another event during the third window, and this should presumably set the fourth window to **4\*increment**. However, in this example this would exceed the **max\_wait** value. Therefore, the fourth wait-time interval is simply set to **max\_wait** milliseconds. There are more events during the fourth interval, but since the maximum wait-time value has been reached, the fifth interval is still set to **max\_wait** milliseconds. Since there are no events during the fifth and sixth intervals, the hold-time is reset to **start** milliseconds again.

## IS-IS SPF and LSP Generation Mechanisms

IS-IS fast convergence is an extended feature of IS-IS, implemented to efficiently speed up route convergence. It includes the following features.

### Incremental SPF (I-SPF)

Incremental SPF (I-SPF) recalculates only the routes of the changed nodes rather than the routes of all nodes when the network topology changes, which speeds up the calculation of routes. In ISO 10589, the Dijkstra algorithm was adopted to calculate routes. When a node changes on the network, the algorithm recalculates all routes. The calculation requires a long time to complete and consumes a significant amount of CPU resources, reducing convergence speed.

I-SPF improves the algorithm. Except for the first time the algorithm is run, *only the nodes that have changed* (rather than all nodes in the network) are included in the calculation. The shortest-path tables (SPT) generated using I-SPF are the same as those generated using the previous algorithm. This significantly decreases CPU usage and speeds up network convergence.

### Partial Route Calculation (PRC)

Partial route calculation (PRC) calculates only those routes which have changed when the network topology changes. Similar to I-SPF, PRC calculates only routes that have changed. For improved efficiency, PRC updates routes based on the SPT calculated by I-SPF.

In route calculation, a leaf represents a route, and a node represents a device. If the SPT changes after I-SPF calculation, PRC re-calculates all the leaves *only on the changed node*. PRC updates only the routes of these changed nodes, which consumes less CPU resources. PRC based on the I-SPF further improves network convergence performance, replacing the original SPF algorithm.

### Link State PDUs (LSP) Fast Flooding

When an IS-IS device receives new LSPs from other devices, it updates the LSPs in the LSDB, periodically flooding the updated LSPs based on a timer. Therefore, the synchronization of all LSDBs is slow.

With LSP fast flooding, when the router receives LSPs that can trigger route calculation or route update, it floods these LSPs *before* route calculation occurs, which speeds up network convergence and LSDB synchronization throughout the entire network.

### Intelligent Timer

Even when the route calculation algorithm is improved, the long *interval* for triggering route calculations also affects convergence speed. A millisecond-level timer can shorten the interval. However, frequent network changes also consume too much CPU resources. The SPF intelligent timer addresses these problems.

In most cases, an IS-IS network running normally is stable. Frequent changes on a network are rather rare, and IS-IS does not calculate routes frequently. Therefore, a short period (within milliseconds) can be configured as a 'fixed' first interval for route calculation. If an event that triggers the timer occurs before the set timer expires, the next timeout period of the timer increases. If the network topology changes frequently, the interval set by the SPF intelligent timer increases with the calculation times to reduce CPU consumption.

The LSP generation intelligent timer is similar to the SPF intelligent timer. When the LSP generation intelligent timer expires, the system generates a new LSP based on the current topology. The original mechanism uses a timer with fixed intervals, which results in slow convergence and high CPU consumption. Therefore, the LSP generation timer is also designed as an intelligent timer, so it can respond to emergencies (for example, the interface goes up or down) quickly and speed up network convergence. In addition, when the network changes frequently, the interval for the intelligent timer becomes longer to reduce CPU consumption.

## IS-IS Graceful Restart

IS-IS Graceful Restart is a feature in IS-IS that allows a device (IS) to remain on the forwarding path of the network while the router restarts IS-IS. Graceful restart can also be used for unplanned restarts of IS-IS, such as when a router unexpectedly restarts.

When an IS device wishes to restart IS-IS, it sends out a Hello message with the Restart Request bit set to its direct neighbors, to alert them that it intends to restart gracefully. Neighboring ISs act as helpers to the restarting IS by keeping that router on the forwarding path as if it were still fully adjacent.

We support Graceful Restart in accordance with [RFC 5306: Restart Signaling for IS-IS](#).

# Label Distribution Protocol LDP

LDP is a protocol in which MPLS routers exchange label mapping information. Two routers with an established session are called LDP peers and the exchange of information is bi-directional. LDP is used to build and maintain LSP databases that are used to forward traffic through MPLS networks. Label Switching Routers (LSRs) preserve the label mappings of an LDP tunnel while the signaling LDP routers restart, thus preserving the state of LDP tunnels during short outages.

Within a given AS, LDP is typically enabled on all intra-AS interfaces. LDP can be used to set up unidirectional MP2P LSPs with IPv4-prefix FECs as destinations, following the paths to these prefixes that have been computed by the IGP, including ECMP. Inbound and outbound label binding filtering can be used to define the subset of all IPv4 prefixes for which these LSPs are defined.

In this context, tunnel LSPs are LSPs with IP-prefix FECs for /32 IPv4 FECs representing LSP IDs. A full mesh of tunnel LSPs can be configured and maintained without user intervention, once the initial configuration of the routers has been completed. These LSPs can now be used by L2/L3VPNs.

LDP reacts to topology changes according to the IGP. For example, assume a topology change is detected. (Note that topology changes may be detected at the physical layer (fast), using 1-hop IPv4 BFD (fast), or by the IGP itself (slow).) The IGP reacts to topology change by flooding the link state change across the AS until all Link State Databases are re-synchronized. This may take some time, depending on the size of the AS and complexity of the topology. Routes are updated and new routes computed and installed in the RIB. The actual computation time can be quite fast. The LDP follows the changes in the RIB and makes the corresponding changes as needed; existing LSPs are re-routed, new LSPs are set up, and total recovery time is defined by the time it takes the IGP to re-converge. LDP also supports Fast ReRoute (FRR) based on IP loop-free alternatives (LFA).

# Open Shortest Path First OSPF

Open Shortest Path First (OSPF) is an IETF standard routing protocol for Internet Protocol (IP) networks. OSPF uses a link state routing (LSR) algorithm and falls into the group of interior gateway protocols (IGPs), operating within a single autonomous system (AS). OSPF is generally the IGP of choice for most enterprise network administrators.

This section introduces the following OSPF features:

- OSPFv2 for IPv4: RFC 2328
- OSPFv3 for IPv6: RFC 5340
- OSPF Support for Segment Routing SR
- SPF and LSA Delay Algorithms for OSPFv2 and OSPFv3
- OSPF Graceful Restart

## OSPFv2 for IPv4: RFC 2328

OSPF Version 2 was defined in RFC 2328 (1998) for IPv4. With OSPF, the nodes discover and establish adjacencies. Nodes also distribute and synchronize link state databases through a reliable flooding mechanism, with designated routers (DR) identifying the selected path for multiple routers on a multi-access network segment. Each router in the AS eventually learns the same link state database. Each router then runs a Shortest Path First (SPF) algorithm to define a complete set of 'shortest path tree' routes through the network with itself as the root. Shortest path selection guarantees loop free routing. OSPF supports the Classless Inter-Domain Routing (CIDR) addressing model.

Protocol messages include the standard Hello, DBD, LSReq, LSU, and LSAck. Supported interface types include P2P, Broadcast (BC), Virtual, NBMA, and P2MP. The Hello protocol is used for dynamic neighbor discovery, and subsequent LSDB synchronization for becoming (fully) adjacent. The local states (interfaces and neighbors) of routers and networks are distributed via LSAs, which are flooded throughout the AS.

OSPF maintains a two-level hierarchy among the areas, where packets going from one area to another must traverse through the backbone area, using virtual links if necessary. In OSPF, boundaries are within area border routers. Areas are numbered (area 0, area 1, etc.), and SPF algorithms are executed per area. Links must be in the same area at both ends to form an adjacency. Several types of areas perform summarization with different granularity. An OSPF router remains on the forwarding path of the network while restarting OSPF. The amount of LSA flooding and consecutive updating that consequently occurs is minimized.

## OSPFv3 for IPv6: RFC 5340

OSPF updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008). OSPFv3 runs over IPv6 and supports distribution of IPv6 prefixes. It is based on OSPFv2, retaining the fundamental mechanisms of flooding, DR election, area support, and SPF calculations, but enhanced to support IPv6 addresses and prefixes. OSPFv3 coordinates with OSPFv2 using a ships-in-the-night approach, meaning these protocols do not exchange information or pay attention to each other, and can run simultaneously and independently.

OSPFv3 differs from OSPFv2 in the following significant ways:

- **OSPFv3 runs per link, not per subnet:** The OSPFv2 terms *network* and *subnet* are replaced by the term *link* (LIF). OSPFv3 interfaces connect to a link rather than to IP subnets. This means that an OSPFv3 LIF can support multiple subnets (IPv6 prefixes). Since the IP subnet no longer uniquely identifies a LIF, a LIF is now uniquely identified by a dedicated and persistent Interface ID. This differs from OSPFv2, where numbered LIFs are globally identified by the IP interface address. Moreover, now there is no need to share subnets (IPv6 prefix) to form an adjacency, as neighboring routers communicate using link-local IPv6 addresses. This flexibility enhances network mobility.
- **Addressing:** OSPFv3 packet headers do not contain IPv6 addresses; instead the address is part of the payload, carried by the LSAs. Moreover, Router and Network LSAs no longer contain IPv6 prefixes, instead carrying only topology (connectivity) information. Prefixes carried by LSAs are expressed as [prefix, prefix length] instead of [address, mask]. A router is always identified by

Router ID, in contrast to OSPFv2 routers which are identified by IP interface address on the broadcast LIF. The Router ID, Area ID, and Link State ID remained 32 bits. They are no longer (IPv6) addresses.

- **Extension of flooding scope options:** There are now 3 flooding scopes for LSA flooding, explicitly coded in the LS type field. AS and Area define the same scope as in OSPFv2. The new scope category is Link-Local (LL), in which LSA is only flooded on the local link and no further.
- **Multiple instances per LIF:** It is possible to run multiple OSPFv3 instances per LIF. This is accomplished using the Instance ID field on the OSPFv3 header, and enables support of multiple IGP domains (AS) or multiple address families per LIF.
- **Options field:** The Options field on Hello and DBD packets has been expanded to 24 bits. Two new Options bits have been defined, the R-bit (V6-bit). Resetting them would indicate that the advertiser would not forward transit IP (IPv6) traffic. This could be used by hosts that want to participate in the routing protocol without forwarding transit traffic.
- **Use of link-local (LL) addresses:** OSPFv3 packets have LL addresses as the source IP (SIP); these are unicast addresses within the range FE80/10, and are typically auto-assigned based on the MAC address of the interface. LL addresses as the destination IP (DIP) are used to reach neighboring nodes attached to the same link. OSPFv3 packets on virtual links have global-scope DIP rather than LL, since LL addresses are limited to local link. Routers will not forward packets with LL SIP and/or DIP; such packets are instead trapped to the control plane.
- **Authentication:** Authentication has been removed from OSPFv3, which now relies on IPv6 IPsec. IPsec uses IPv6 Authentication and Encapsulating Security Payload (ESP) headers to provide authentication and encryption. An alternative approach is to use the OSPFv3 Authentication Trailer as described in RFC 7168.
- **Unknown LSA handling is explicitly specified:** Handling of unknowns is explicitly specified on the LSA. It is coded in the LS type field of the LSA, to either discard the LSA or store and flood the LSA.
- **New LSAs:** OSPFv3 defines a new LSA called Link LSA. It has a link-local flooding scope and lists the router's IPv6 prefixes assigned to the link. It also advertises the router's Options bits, to undergo logical OR by the DR with the Options bits of all adjacent neighbors on the link, and be advertised via the Network LSA. Link LSAs are not generated for OSPFv3 virtual links. OSPFv3 further defines another new LSA called Intra-Area Prefix LSA, which carries all the router's IPv6 prefixes, rather than be advertised via the router LSA (OSPFv2 stub networks) or the network LSA (OSPFv2 Transit networks).

## OSPF Support for Segment Routing SR

Segment routing can be used to add the concept of abstract segments to OSPF routing protocols. Abstract segments make it possible to add the ability to perform shortest-path routing and source-routing. An abstract segment can represent the local prefix of a node, a specific adjacency of the node (interface or next-hop), a service context, or a specific explicit path over the network. For each segment, the IGP advertises an identifier referred to as a Segment ID (SID).

When a segment routing is used in the MPLS data plane, the SID is a standard MPLS label. When forwarding a packet using segment routing, the router pushes one or more MPLS labels.

### OSPF Segment Routing Extensions

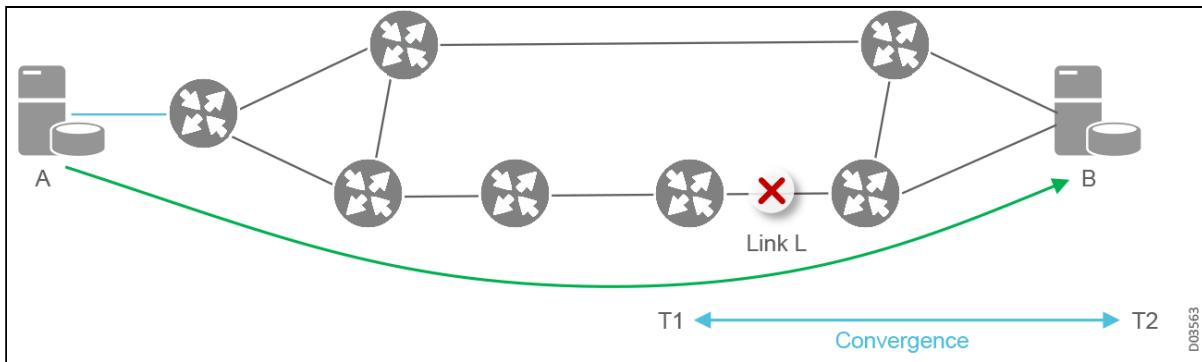
New TLV/sub-TLVs are defined in RFC 8667 (*OSPF Extensions for Segment Routing*) and are supported in the OSPF implementation of segment routing. This includes:

- The prefix SID sub-TLV
- The adjacency SID sub-TLV
- The SID/Label Binding TLV
- SR capabilities sub-TLV

## SPF and LSA Delay Algorithms for OSPFv2 and OSPFv3

For a network to *converge*, all routers in the network must collect from each other and agree on all the network topology information. This information must be consistent, reflecting the current state of the network, and free of routing loops or any other kinds of corruption.

### Fast Convergence



Convergence involves the following stages:

- **Event detection**, including considerations such as:
  - How fast can we detect a change in topology (through the hardware or through IGP protocol timer expiration)?
  - Do we use BFD on the interface to speed up defect detection?
- **Event propagation**, including considerations such as:
  - Once a problem is detected, how fast can we inform others?
  - When there is a change, the LSP must be flooded as fast as possible by the neighbor
  - We must flood the LSP that triggers SPF *before* SPF execution
- **Event processing**, including the following steps:
  - Run SPF (Dijkstra algorithm) to recalculate routes *only* if there have been topology changes (nodes or links), in order to re-compute SPT and the RIB table values
  - Run a partial route calculation (PRC) *only* if an IP prefix has changed. We can keep the SPT, and just update the RIB table entries for the nodes whose prefixes have changed.
- **Update RIB/FIB**, selecting the best routes from the local IGP LSDB, sets of static routes, and BGP decisions
- **IGP convergence status**, where historically IGP convergence would be on the order of 10-30s, focusing on stability rather than speed.

Emphasizing stability over speed sometimes led to undesired consequences. For example, in some contexts, with fast reroute techniques, traffic restoration may be completed well before network convergence! In any case, today speed is an essential factor; convergence must be in the range of milliseconds rather than seconds, with no compromise on stability or scalability.

Network interface speeds are growing rapidly. It's common to see very-high-bandwidth links between two devices, especially in core networks. Consider the failure of such a trunk for only two seconds. Imagine how much information would be lost during the failure before the network is once again fully converged. Default routing protocol timers are not 'good enough' for networks with high-speed interfaces that need such levels of convergence speed. Networks require faster failure detection, faster event reporting and table calculations, and faster times for the forwarding engine to react to topology changes and adjust its tables.

*Fast convergence* describes a quick convergence time, meaning the time required by all the routers in the network to flood and incorporate the relevant network topology information. By fast convergence we usually mean sub-second convergence time. However, if dealing with unstable networks, this approach can backfire. **The trick is to react more quickly to initial events, but in situations of constant churn, to slow down convergence time enough to avoid collapse.** This means that in stable periods, with rare triggers, actions

are processed promptly. But as stability decreases, and trigger frequency increases, a mechanism must be built in to delay processing of the related actions.

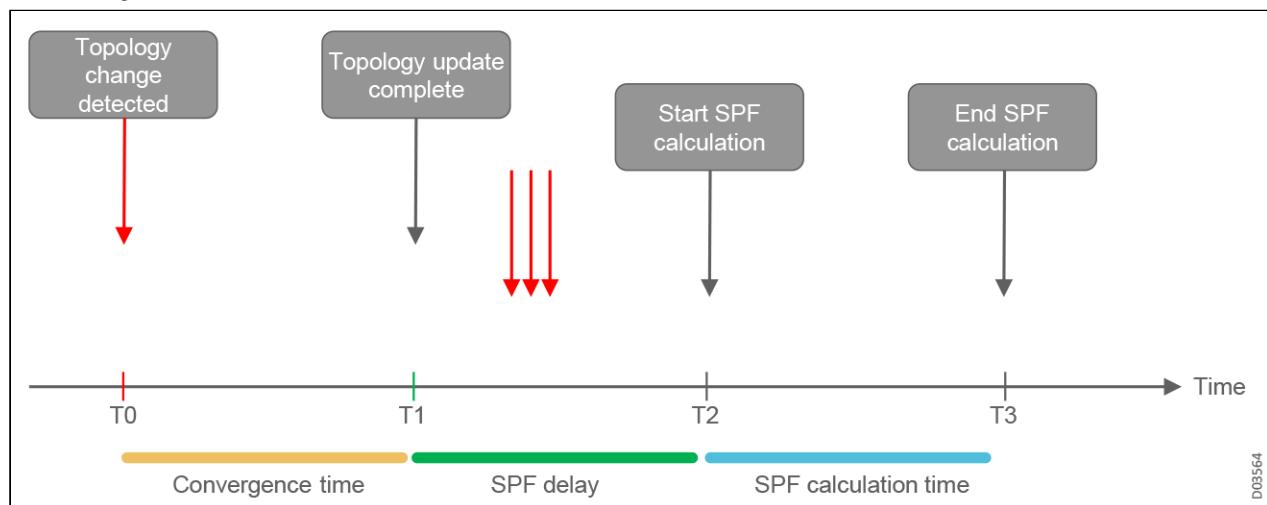
This section introduces the following delay mechanisms:

- What is SPF Delay in OSPF
- What are LSA Generation Timers
- OSPF SPF and LSA Generation Mechanisms

## What is SPF Delay in OSPF

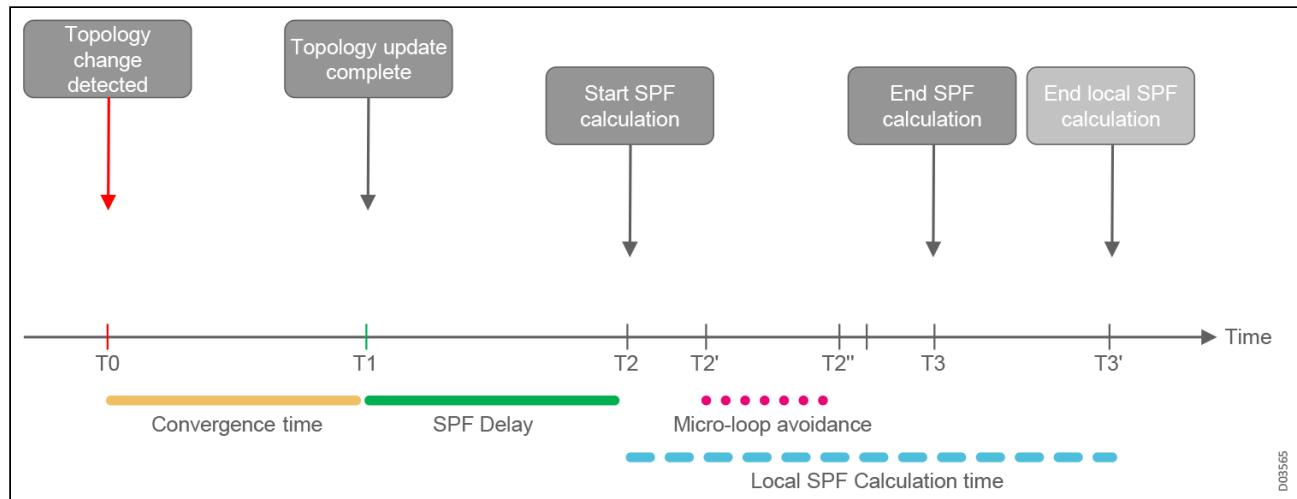
SPF delay is the delay time between the first IGP event triggering a new routing table computation, and the actual start of that routing table computation. SPF delay can be a good thing - the parameter is often associated with a damping mechanism to slow down reaction times by incrementing the delay timer setting when the IGP becomes unstable. As illustrated in the following figure, you don't want to start a new set of SPF calculations before the topology update has been completed. When there are many topology change events, inserting an SPF delay period slows down SPF calculations to avoid system collapse

### SPF Delay



RFC 8405 defines a back-off algorithm to use for SPF delay. RFC8333 defines an additional mechanism to delay local convergence, compared to the network-wide convergence, when traffic is protected by FRR or administrative deactivation. This helps avoid local micro loops, as illustrated in the following figure.

### Local SPF Calculation



In this example, a topology change is detected at  $T_0$ . The topology update is completed at  $T_1$ . The initial convergence time is the time period between  $T_0$  and  $T_1$ . An SPF delay factor is added, so the new SPF calculations are only started at  $T_2$ . The main SPF calculation is completed at  $T_3$ . If there is also a **local** link down, that local SPF calculation is delayed through use of a micro-loop delay-timer, and is only completed at time  $T_3'$ .

## What are LSA Generation Timers

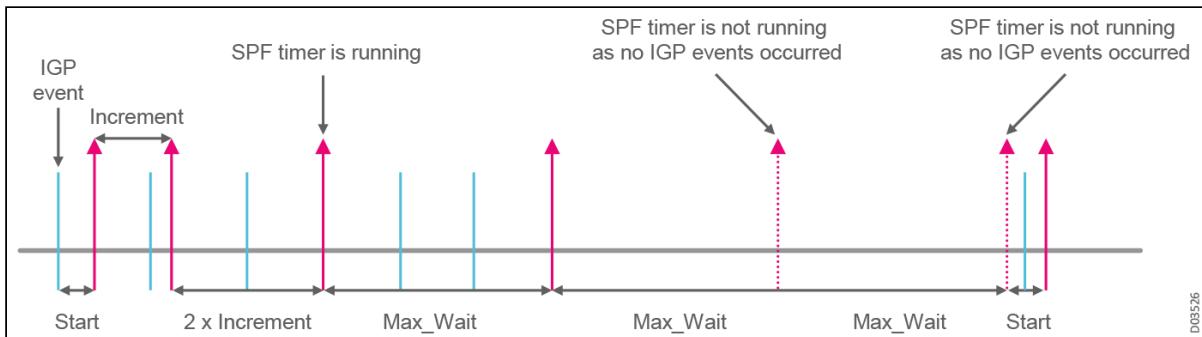
LSAs are Link State Advertisements, used by OSPFv2 and OSPFv3 protocols. The collected link state advertisements of all routers and networks form the OSPFv2/v3 protocols' link state database. If there is a change in the LSA database, the system must complete a new SPF calculation. Neptune platforms provide a built-in delay mechanism, with values configure for **initial wait time**, **minimum/maximum wait time**, and an **exponential increment value**, for maximum efficiency in times of network stability and instability.

Similarly, if there is a change in the local LSA values, the system must generate a new LSA and flood the network with the new values. Again, a built-in delay mechanism, with values configure for initial wait time, minimum/maximum wait time, and an exponential increment value, enables maximum efficiency in times of network stability and instability.

For example, suppose the network was stable for a relatively long time. Then an LSA-triggering event occurs. The router delays SPF computations for the **start parameter** (initial wait time) amount of milliseconds, and also increases the **next** wait-time value by the **increment-parameter** number of milliseconds. Next, if another event occurs *after* the start-wait window expires, the event would be held for processing until the **increment-parameter** window of milliseconds expires. At the same time, the **next** wait-time value would be doubled, set to **2\*increment**.

Every time an event occurs *during the current wait-time window*, the processing is delayed until the current wait-time expires *and* the **next** wait-time interval is doubled. The wait-time grows exponentially until it reaches the **max\_wait** value. After this, for every event received during the current wait-time window, the next wait-time interval remains equal to the constant **max\_wait** value. This ensures that exponential wait-time growth is limited by a ceiling value. If there are no events for the duration of **2\*max\_wait** milliseconds, the hold-time window is reset back to the **start** value, assuming the network has returned to a stable condition. A typical sequence is illustrated in the following figure.

## LSA Generation Timers



The first event triggers an SPF to be run in **start** milliseconds. At the same time, the next wait interval is set to **increment** milliseconds. Since there is an event during the second wait interval, the third wait interval is set to **2\*increment**. There is another event during the third window, and this should presumably set the fourth window to **4\*increment**. However, in this example this would exceed the **max\_wait** value. Therefore, the fourth wait-time interval is simply set to **max\_wait** milliseconds. There are more events during the fourth interval, but since the maximum wait-time value has been reached, the fifth interval is still set to **max\_wait** milliseconds. Since there are no events during the firth and sixth intervals, the hold-time is reset to **start** milliseconds again.

## OSPF SPF and LSA Generation Mechanisms

OSPF fast convergence is an extended feature in OSPFv2 and OSPFv3, implemented to efficiently speed up route convergence. It includes the following features.

### Partial Route Calculation (PRC)

When a node changes on the network, if the router has to recalculate all routes, the calculation generally takes a long time and consumes too many CPU resources, which affects the convergence speed.

Partial route calculation (PRC) calculates only those routes which have changed when the network topology changes. In PRC, a leaf represents a route, and a node represents a router. Either an SPT or a leaf change causes a route change. The SPT change is irrelevant to the leaf change. PRC processes routing information as follows:

- If the SPT changes, PRC processes the routing information of all leaves on a changed node.
- If the SPT remains unchanged, PRC does not process the routing information on any node.
- If a leaf changes, PRC processes the routing information on that leaf only.
- If a leaf remains unchanged, PRC does not process the routing information on any leaf.

### Intelligent Timer

Even when the route calculation algorithm is improved, the long *interval* for triggering route calculations also affects convergence speed. A millisecond-level timer can shorten the interval. However, frequent network changes also consume too much CPU resources. The OSPF intelligent timer addresses these problems.

On an unstable network, routes are calculated frequently, which consumes a great number of CPU resources. In addition, LSPs that describe the unstable topology are generated and transmitted on the unstable network. Frequently processing such LSPs affects the rapid and stable operation of the entire network. To speed up route convergence on the entire network, the OSPF intelligent timer controls route calculation, LSA generation, and LSA receiving.

The OSPF intelligent timer works as follows:

- On a network where routes are calculated repeatedly, the OSPF intelligent timer dynamically adjusts the route calculation based on user's configuration and the exponential backoff technology. The number of route calculation times and the CPU resource consumption are decreased. Routes are calculated after the network topology stabilizes.

- On an unstable network, if a router generates or receives LSAs due to frequent topology changes, the OSPF intelligent timer can dynamically adjust the interval. No LSAs are generated or processed within a specified interval, which prevents invalid LSAs from being generated and advertised on the entire network.

## OSPF Graceful Restart

OSPF Graceful Restart is a feature in OSPF that allows an OSPF router to remain on the forwarding path of the network while it restarts OSPF. Graceful restart can also be used for unplanned restarts of OSPF, such as when a router unexpectedly restarts.

When a router wishes to restart OSPF, it sends out a link-local opaque LSA (Type 9), called a grace-LSA. The Grace-LSA announces to the router's direct neighbors that it intends to restart gracefully. Neighboring OSPF routers act as helpers to the restarting router by keeping the router on the forwarding path as if the restarting router were still fully adjacent.

We support Graceful Restart in accordance with [RFC 3623: Graceful OSPF Restart](#).

# Protocol-Independent Multicast PIM

Protocol Independent Multicast (PIM) is a family of multicast routing protocols for IP networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the internet. It is called *protocol-independent* because the PIM protocols do not include their own topology discovery mechanism. Instead they use routing information supplied by other routing protocols.

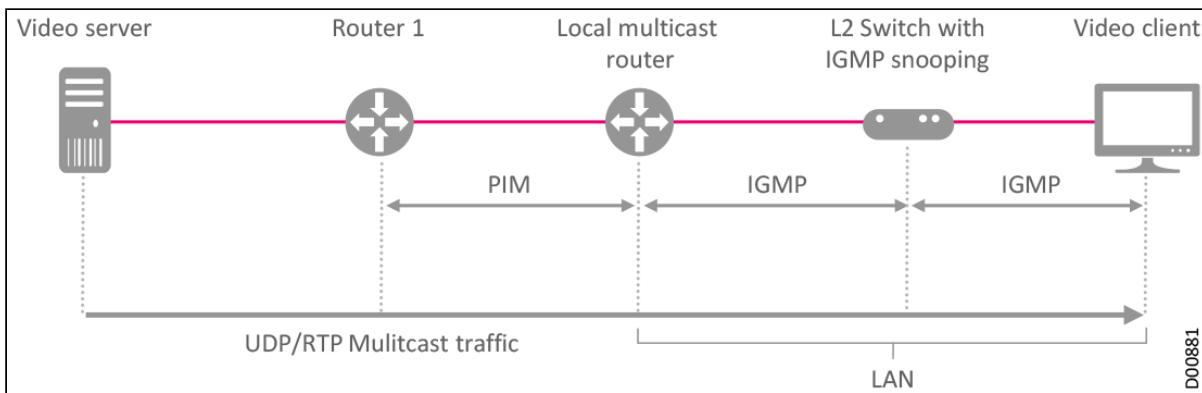
PIM provides IP multicast forwarding by leveraging static routes or unicast routing tables generated by any unicast routing protocol, such as OSPF, IS-IS, or BGP. Independent of the unicast routing protocols running on the device, multicast routing can be implemented as long as the corresponding multicast routing entries are created through unicast routes.

PIM uses reverse path forwarding (RPF) to implement multicast forwarding. When a multicast packet arrives on an interface of the device, it is subject to an RPF check. If the RPF check succeeds, the device creates the corresponding routing entry and forwards the packet; if the RPF check fails, the device discards the packet. PIM can also be used by a router to notify an upstream router that it wishes to receive or stop receiving multicast traffic for a given group ( $G$ ).

Different PIM strategies can be chosen, depending on the network configuration and whether the multicast tree is considered *sparse* or *dense*. The PIM protocol family includes four variants:

- **PIM Sparse Mode (PIM-SM)** is generally appropriate when the receivers are sparsely situated. A join & prune approach is an effective technique when working in sparse mode. PIM-SM explicitly builds unidirectional shared trees rooted at a single rendezvous point (RP) per group, and optionally creates shortest-path trees per source. The multicast forwarding path is the shared-based tree, and multicast traffic is forwarded only to receivers that ask for it via join and prune messages. PIM-SM generally scales fairly well for wide-area usage. PIM-SM is also known as Any Source Multicast (ASM). The complete service description is in RFC 1112.
- **PIM Dense Mode (PIM-DM)** uses dense multicast routing. This mode is generally appropriate when the receivers are densely situated and most of the routers are participating in the multicast forwarding. The multicast forwarding path is a source tree. This is a forwarding tree where the multicast source serves as the 'root' and the multicast group members serve as the 'leaves'. Because the source tree is the shortest path from the multicast source to the receivers, it is also called shortest path tree (SPT). A flood & prune approach is an effective technique for building the SPT when working in dense mode. PIM-DM implicitly builds SPTs by flooding multicast traffic domain wide, and then pruning back branches of the tree where no receivers are present. PIM-DM is straightforward to implement but generally has poor scaling properties. The first multicast routing protocol, DVMRP, used dense-mode multicast routing; see the PIM Internet Standard RFC 3973.
- **Bidirectional PIM** explicitly builds shared bi-directional trees. It never builds a shortest path tree, so there may be longer end-to-end delays than PIM-SM. Nevertheless, this protocol scales well because it needs no source-specific state; see Bidirectional PIM Internet Standard RFC 5015.
- **PIM Source-Specific Multicast (PIM-SSM)** builds trees that are rooted in just one source, offering a more secure and scalable model for a limited amount of applications (usually broadcasting of content). In SSM, an IP datagram is transmitted by a source  $S$  to an SSM destination address  $G$ . Receivers can receive this datagram by subscribing to channel  $(S,G)$ ; see informational RFC 3569. PIM-SM is commonly used in IPTV systems for routing multicast streams between VLANs, subnets, or local area networks. PIM-SSM is also known as Source Specific Multicast (SSM). It is technically a subset of PIM-SM, not a separate protocol.

### Multicast Network Architecture with PIM



This section introduces the following topics:

- [PIM IPv6 Support](#)
- [Multicast Listener Discovery MLD](#)

## PIM IPv6 Support

PIM-SM for IPv6 (PIM-SMv6) provides efficient communication between members of sparsely distributed groups—the type of groups that are most common in wide-area inter-networks. PIM-SMv6 helps geographically dispersed network nodes to conserve bandwidth and reduce traffic by simultaneously delivering a single stream of information to multiple locations.

PIM-SMv6 uses the IPv6 multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, with mechanisms to adapt to changing network conditions. PIM-SMv6 uses a topology gathering approach to populate a multicast routing table with routes.

The following table highlights some of the differences between IPv4 multicast and IPv6 multicast.

### IPv4 Multicast vs. IPv6 Multicast

IP Service	IPv4 Solution	IPv6 Solution
Address range	32-bit, Class D	128-bit
MC address structure	IPv4 structure	IPv6 structure
MC group address	224.0.0.0/4	FF00::/8
SSM range (default)	232.0.0.0/8	FF3x::/32
Routing	PIM (family: inet)	PIM (family: inet, inet6)
	IS-IS (family: iso, inet)	IS-IS (family: iso, inet, inet6)
	OSPFv2 (family: inet)	OSPFv3 (family: inet6)
	BGP-4 with IPv4 AFI and multicast SAFI	BGP-4 with v6 AFI and multicast SAFI
Forwarding	PIM-SM (ASM and SSM) (family: inet)	PIM-SM (ASM and SSM) (family: inet, inet6)
Group membership	IGMPv2 (ASM model)	MLD1 (ASM model)
	IGMPv3 (ASM+SSM)	MLD2 (ASM+SSM)
Domain control	Border/Boundary (optional)	Scope Identifier

## Multicast Listener Discovery MLD

Multicast Listener Discovery (MLD), used in IPv6, is functionally equivalent to IGMP in IPv4. Messages are transported over ICMPv6.

MLD uses link-local source addresses, and utilizes the "Router Alert" option in the header (RFC 2711). MLDv2 also provides SSM support.



### Tip

Note the slight confusion in version numbering:

- MLDv1 (RFC2710) is similar to IGMPv2 (RFC2236)
- MLDv2 (draft-vida-mld-v2-07) is similar to IGMPv3 (RFC3376), and also provides SSM support.

Typical uses of MLD include joining a group and sending group-specific queries. Other MLD operations include:

- General Query (Type 130), which is sent to learn of listeners on the attached link. A General Query sets the Multicast Address Field to zero, and is by default sent every 125 seconds (configurable).
- Leave/DONE messages. A DONE (Type 132) message is sent by the last host to leave. The router responds with a Group-Specific Query. The router uses the last-member-query response interval (default=1 sec) for each query. The query is sent twice. If no reports occur in response then entry is removed (default 2 sec).

# Resource Reservation Protocol: RSVP

The Resource Reservation Protocol (RSVP) is a [transport layer protocol](#) designed to reserve resources across a network using the integrated services model. RSVP operates over either IPv4 or IPv6, and provides receiver-initiated setup of resource reservations for multicast or unicast data flows. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, etc.) of the packet streams they want to receive.

RSVP-TE is used to establish MPLS transport LSPs when there are traffic engineering requirements. RSVP-TE generally allows the establishment of MPLS label switched paths (LSPs), taking into consideration network constraint parameters such as available bandwidth and explicit hops. RSVP-TE allows the use of source routing where the ingress router determines the complete path through the network. The ingress router can use a Constrained Shortest Path First (CSPF) calculator to determine a path to the destination.

The CSPF algorithm is an advanced form of the shortest-path-first (SPF) algorithm used in OSPF and IS-IS route computations. CSPF is used in computing paths for LSPs that are subject to multiple constraints. When computing paths for LSPs, CSPF considers not only the topology of the network, but also the attributes of the LSP and the links, and it attempts to minimize congestion by intelligently balancing the network load. While SPF calculates the best path to a destination according to a basic set of links metrics, CSPF can calculate the best path to a destination according to the basic set of link metrics plus additional relevant constraints such as bandwidth, delay, and affinity, thereby ensuring that any QoS and Shared Risk Link Group (SRLG) requirements are met. The resulting path is then used to establish the LSP. RSVP-TE can be used on both IPv4 and IPv6.

This section introduces RSVP-TE, and includes the following:

- [RSVP Terminology](#)
- [What is an RSVP Session](#)
- [Unique LSP Paths in the Network](#)
- [RSVP-TE Refresh Reduction](#)
- [RSVP-TE Make-Before-Break Mechanism](#)
- [RSVP-TE Authentication](#)
- [RSVP OAM: Ping and Traceroute](#)
- [RSVP-TE Protection](#)
- [RSVP-TE Graceful Restart](#)
- [RSVP-TE Hello](#)

## RSVP Terminology

To understand what RSVP is and how it works, you must first understand the terminology.

### RSVP Messages

RSVP messages are sent over IP. The following types of messages are the most commonly used:

- **PATH:** Sent by the headend router requesting the resources. This message is forwarded through the network from the headend router towards the tailend router.
- **RESV:** Sent by the tailend router in response to the PATH message received, confirming the resource reservation. This message travels from the tailend towards the headend router.
- **Error Messages:** PathErr (PATH Error) and ResvErr (RESV Error) messages are sent in the event of unavailability of the requested resource.
- **Tear Messages:** PathTear and ResvTear messages are used to clear the PATH and/or RESV states from the network.

### What is an LSP?

An **LSP** is a label switched path, (a type of logical tunnel), running through an MPLS network. LSPs are configured by the network management system, or by a signaling protocol such as LDP, BGP, or RSVP-TE. A network can include multiple RSVP-TE LSPs; each one is uniquely identified by its Source IP, Destination IP,

and Tunnel-ID. These three identifying parameters are encoded in the SESSION object of the PATH message during initial setup of an LSP path.

The **LSP-Path** is the actual MPLS connection from the Headend to the Tailend router. It is identified by the LSP-ID field encoded in the SENDER\_TEMPLATE. The LSP-Path is a logical entity containing a list of IP hops, providing an end-to-end representation of the RSVP sessions along each hop. When an LSP is associated with a path, the path in effect regulates the LSP, controlling which route it must take. An LSP can be associated with multiple LSP-Paths, such as an Active and Standby LSP-Path.

### What is an RSVP-TE Tunnel?

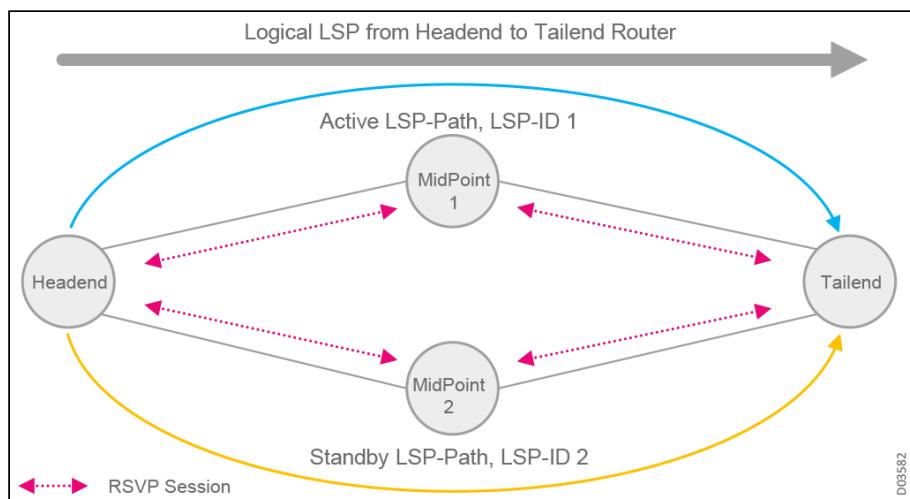
A Traffic Engineered (TE) tunnel is a container of TE LSPs instantiated between the tunnel ingress and the tunnel destination. A TE tunnel can instantiate one or more RSVP-TE LSPs, where each TE LSP is defined with a preference value, and the LSP with the highest preference is considered the primary LSP. The LSP with the next-highest preference is considered the secondary (hot-standby) LSP. All other participating LSPs are considered cold-standby. Hot and cold standby LSPs are described in RSVP-TE Protection.

## What is an RSVP Session

An RSVP session is an MPLS label cross-connect. In each MPLS router, one RSVP session associates one ingress label and one egress label of the same LSP-Path. An RSVP session for an LSP contains:

- **A Pair of Labels:** An ingress label distributed to the upstream router and an egress label received from the downstream router.
- **A Pair of State Blocks:** The Path State Block (PSB) maintains the relationship with the upstream router by constantly receiving PATH messages refreshing the session. The RESV State Block (RSB) maintains a relationship with the downstream router by constantly receiving RESV messages refreshing the session.
- **A Pair of Messages:** The Original PATH and RESV messages used to establish the RSVP sessions are stored in the router to validate the subsequent refreshing of PATH and RESV messages.

### RSVP Session



- The blue arrow just above the network diagram represents an E2E MPLS tunnel, running from the headend to the tailend.
- The green and orange arrows are two LSP-PATHS, one active and one standby, each identified through a unique LSP-ID.
- Both of these LSP-PATHS are part of the same blue MPLS tunnel running between the headend and the tailend.
- The pink arrows indicate the RSVP session between each router, configured on a hop-by-hop basis.

RSVP-TE signaled LSP-Paths are explicit-route LSP paths. An explicit routing object (ERO) contains all the interface IP addresses that the LSP-Path must pass through to reach its destination. When signaling the LSP-Path, an RSVP-TE PATH message follows the route specified by the ERO. The ERO can be strictly or loosely defined.

A typical RSVP session involves the following sequence of events:

1. A potential sender starts sending RSVP PATH messages to the session address.
2. A receiver, wanting to join the session, registers itself if necessary. For example, a receiver in a multicast application would register itself with IGMP. The receiver receives the PATH messages.
3. When the PATH message reaches the outbound router, resource reservation begins. The outbound router sends a RESV message upstream to the inbound router. Each router along the path receives the RESV message and sends it upstream, following the path of the original PATH message. When the inbound router receives the RESV message, the unidirectional network path is established.
4. The sender receives the RESV message and then starts sending application data.
5. The established path remains open as long as the RSVP session is active. The session is maintained by the transmission of additional PATH and RESV messages that report the session state every 30 seconds. If a router doesn't receive the maintenance messages for three minutes, it terminates the RSVP session and reroutes the LSP through another active router.

This sequence of events may not be strictly synchronized. For example, receivers can register themselves before receiving PATH messages from the sender, and application data can flow before the sender receives RESV messages. An application data that is delivered before the actual reservation contained in the RESV message is typically treated as best-effort, non-real-time traffic with no CoS guarantee.

## Unique LSP Paths in the Network

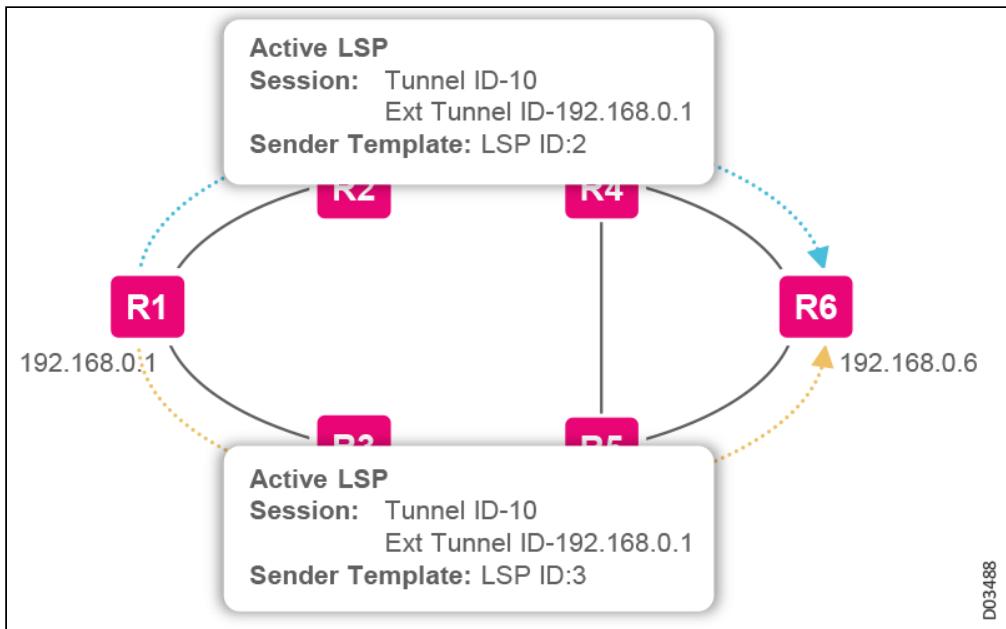
In the RSVP domain, an LSP is identified by the tunnel ID (which is usually a number) and by the Extend Tunnel ID (which is usually the IP of the Headend router), fields which are present in the SESSION Object. All LSPs that belong to the same LSP have the same SESSION object. Therefore, they have the same tunnel ID and Extended Tunnel ID.

There are two objects required to uniquely identify an LSP path within an LSP:

- **Tunnel-ID:** This is shared by all LSP paths belonging to the same LSP. It is part of the SESSION object.
- **LSP-ID:** Each individual LSP path has its own LSP ID. The LSP ID is located in the SENDER\_TEMPLATE object.

If the LSP path uses MPLS FRR (one-to-one/path protection) backup, two sets of RSVP sessions belong to the same LSP path. One set **belongs to the original protecting LSP path**, and the other belongs to the protection LSP. Both LSP paths will have the same tunnel ID, but the LSP ID will be different in the SENDER\_TEMPLATE object.

## Active and Standby LSP Paths



D03488

## Setting Up an LSP Path

Before signaling the LSP path, the Headend router runs a Constrained SPF. Assuming it is able to find a path, it will come with a list of IP addresses (EROs) through which the path will be signaled. Then, it sends a PATH message towards the Tailend router, asking to reserve the necessary resources and to be allocated labels. This PATH message is propagated down the network all the way to the Tailend router. All the intermediate hops look at that PATH message and store the resource requested (if available) and then forward it downstream towards the Tailend router. The RSVP PATH message has the source IP of the Headend and the destination IP of the Tailend router. The RSVP PATH message functions as a label request in the MPLS TE domain.

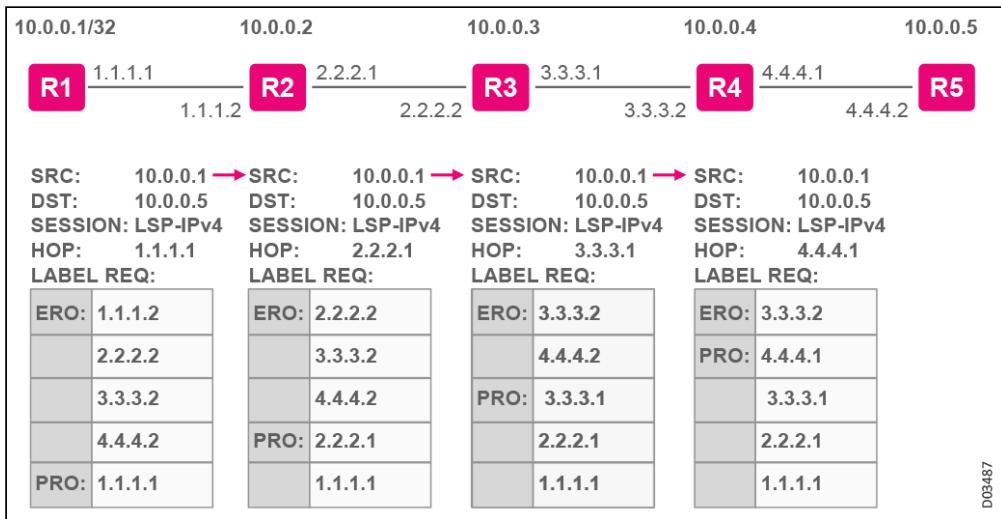
When the Tailend router receives the PATH message, it allocates a label and distributes it to the upstream router via a RESV message. Since RSVP-TE is unidirectional, the Tailend router doesn't need to reserve any resources. Each LSR along the path doesn't start resource reservation and label distribution toward the Headend router until it receives a label from the downstream router (Ordered Control). The LSR performs this process in every hop of the LSP toward the Headend router. After the entire process is finished, the Headend router has an egress label for this LSP path. Each LSR router along the route has one ingress label and one egress label in the RSVP session. The Tailend router has one ingress label. All required resources (for example, bandwidth) are reserved along the path.

The following figure illustrates a typical example of a PATH message being sent from a Headend router (R1) to a Tailend router (R5). The source and destination IPs of the PATH message are the IPs of the Headend and Tailend routers. The PATH message has a Router Alert Option, which informs the intermediate hops to intercept the PATH message and pass it to the local RSVP process, even though the destination IP address is not a local IP.

Notice that in this process:

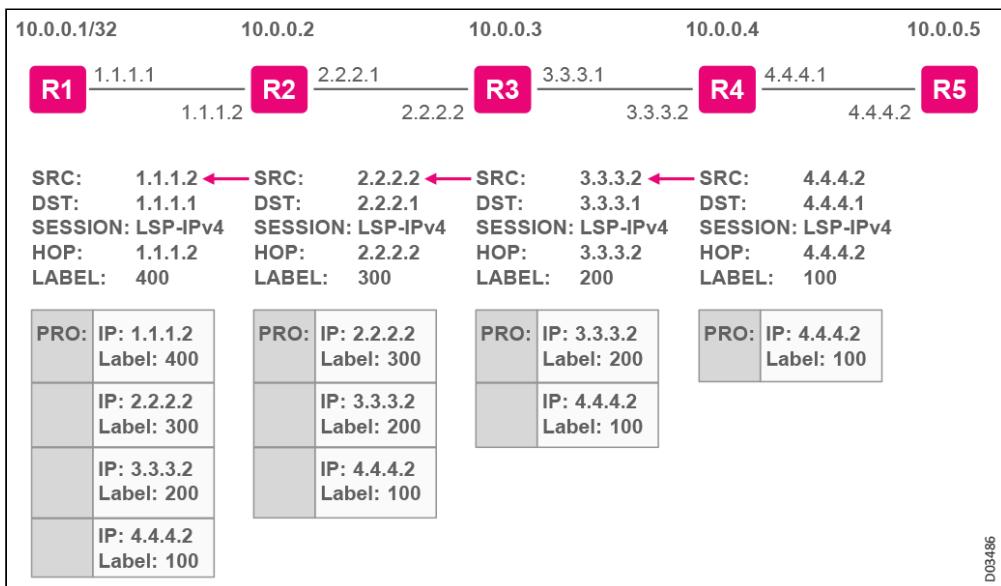
- The HOP field changes at every hop, indicating the outgoing interface IP.
- The ERO list shrinks as it gets closer to the Tailend router.
- The increasing RRO list captures the outgoing interface IP address.

### PATH Message Example



After receiving the PATH message, the Tailend router signals the RESV message back to the Headend, including the label assigned.

### RESV Message Example



The RROs in the RESV messages contain both the IPv4 sub-object and the LABEL sub-object. The IPv4 sub-object contains the router's local egress interface IP address for the message. The LABEL sub-object also contains the label generated and distributed by the local router. RRO information from the RESV messages is used to calculate MPLS FRR paths.

### LSP Optimization

LSP optimization refers to periodic re-optimization of an LSP that is *already set up*. For example, if there is a change in a network topology, then an existing path might become suboptimal; a subsequent re-computation might be able to determine a better path. This feature is applicable only on LSPs for which constrained-path computation is enabled (locally-computed). Re-computation attempts are only applied if a periodic re-optimization timer has expired, to avoid the churning effect of constant re-computation.

If the new computed path for an LSP has a better metric than the current path, an attempt is made to re-signal that LSP using the make-before-break mechanism. If the attempt to re-signal an LSP fails, the LSP will continue to use the existing path and a re-signal will be attempted the next time the timer expires.

## RSVP-TE Refresh Reduction

RSVP-TE is a *soft state protocol*, meaning signaling messages must be exchanged periodically between two peering routers to maintain the path. If the exchanges of signaling messages stops, RSVP adjacency times out after a pre-configured timer period (*Refresh timer*) expires. This means that once the LSP-PATH has been established, it must be constantly refreshed to keep the operational state up. This is achieved by sending a constant PATH and RESV messages (default every 30 seconds). If a router doesn't receive the maintenance messages for (default) three minutes, it terminates the RSVP session and reroutes the LSP through another active router.

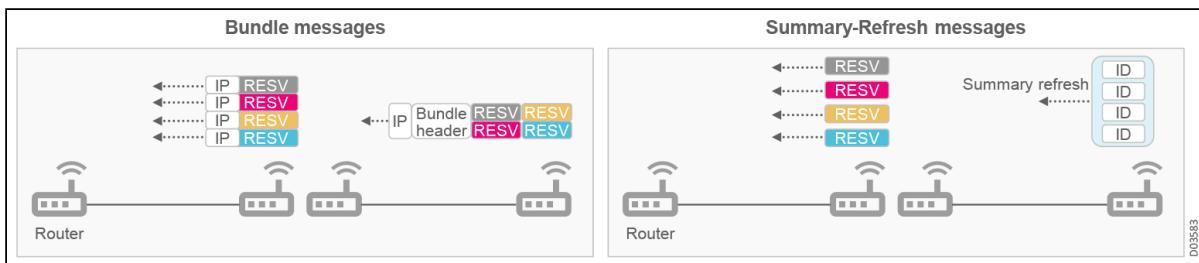
There are two issues with this method:

- **Scalability:** The increasing overhead generated by periodic transmission and processing of refresh messages, as the number of RSVP sessions increases
- **Reliability and Latency:** The reliability and latency problem stems from the loss of non-refresh or one-time RSVP messages, such as PathTear or PathErr. The time to recover from such a loss is usually tied to the refresh interval and keepalive timer values that were configured.

Refresh reduction is a method of handling these issues, using a series of messaging techniques to reduce the amount of information transmitted at every refresh interval:

- Message bundling
- Message ID
- Reliable delivery of RSVP message (ACK,NACK)
- Summary refresh

### Refresh Reduction Messaging Techniques



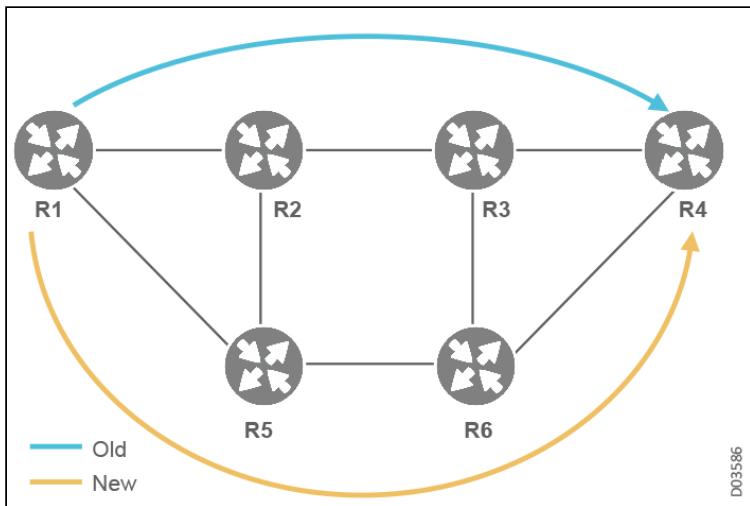
Refresh reduction is enabled through setting of the refresh reduction bit in the RSVP common header. It is only significant between RSVP neighbors.

## RSVP-TE Make-Before-Break Mechanism

The make-before-break (MBB) mechanism prevents traffic loss during a traffic switchover between two LSPs in an RSVP-TE tunnel. This mechanism improves MPLS TE tunnel reliability.

For example, an update to the network topology may enable creation of a better path than the existing one, a feature known as LSP Optimization, described in [Unique LSP Paths in the Network](#). Any change in bandwidth or path attributes causes an LSP in an MPLS TE tunnel to be reestablished using the new attributes, and causes traffic to switch from the previous LSP to the newly established LSP.

### Make-Before-Break (MBB) Mechanism



In this example:

- R1 is an ingress node for an LSP running from R1, through R2 and R3, to the destination in R4 (ERO).
- The trigger for optimization is new, more efficient calculated path running from R1, through R5 and R6, to the same R4 destination node.
- The new path is signaled with the **same tunnel ID** and a **new LSP ID**.
- Once the new path (R1-R5-R6-R4) is successfully established, only then is the original LSP (R1-R2-R3-R4) torn down.

MBB is also used when a failure on a protected tunnel occurs. When the head of the tunnel is notified of the protection tunnel failure, it recalculates a new path (LSP) and signals it. Only *after* the new LSP is signaled successfully does it switch traffic to the new signaled LSP. Make-before-break can be configured on both primary and secondary (hot-standby) LSPs.

## RSVP-TE Authentication

RSVP MD5 authentication provides hop-by-hop security against message spoofing and replay attacks. Authentication is configured per RSVP-TE enabled interface, and done on per-hop basis. This means that every pair of adjacent nodes must have the same authentication key.

Configuration of the authentication-key is also allowed per instance for bypass tunnels only. When the 'point of local repair' (PLR) transmits PATH messages to the merge point (MP), it will use the instance key for authentication.

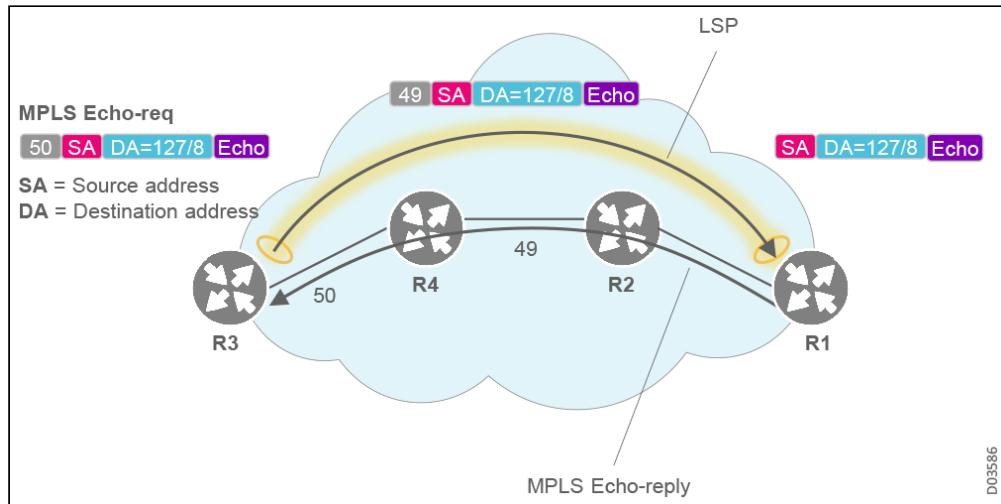
When authentication is configured, RSVP embeds an integrity object within the RSVP messages sent between peers. The integrity object includes a key ID unique to the sender, a message sequence number, and keyed message digest (the hashed result of the key). These attributes enable verification of both packet content and sender.

## RSVP OAM: Ping and Traceroute

Ping messages are used to check bi-directional reachability of a specified IP address. Traceroute messages are used to provide information about the actual path to a specified IP address. RSVP-TE LSP Ping and Traceroute implementations utilize IPv4 or IPv6 UDP packets with port 3503, using MPLS **echo-requests** or **echo-replies**. The Neptune implementation is aligned with the current RFC 8029 standard, with backward-compatibility with RFC 4379.

The MPLS echo-request uses the same label stack as that used by the LSP. The IP header destination address field of the echo request is a 127/8 address. The MPLS echo-reply source IP address is the routable address of the replier. The *destination* IP address is copied from the echo-request's *source* address. These two complementary address headers are illustrated in the following figure.

### MPLS Echo-Request



## RSVP-TE Protection

There are several commonly-used methods for protecting an RSVP tunnel against link and node failures along the tunnel's path. The term *fast reroute* (FRR) describes methods that use pre-signaled backup paths to reroute the tunnel's path around a failure quickly (10s of milliseconds). There is no signaling at the time of the reroute, which means the reroute process is fast. If a link or node fails, FRR rapidly switches traffic to a backup path, minimizing traffic loss. In a typical network, every tunnel head defines and signals whether it wants LSP protection (FRR) or not, and if so, which type: Detour (1:1) or Facility (bypass), described in RFC 4090.

- **Facility (N:1):** In Facility backup protection, (aka Bypass), a single bypass tunnel will back up a set of main LSPs traversing between the 'point of local repair' (PLR) and a common node downstream of the potential failure. Bypass tunnels are pre-provisioned by management to protect against failures of particular links and nodes in the network. When a protected tunnel is set up, a node may select one of the pre-provisioned bypass tunnels to use as a backup path around the downstream link or node. The same bypass tunnel can be used to protect multiple protected tunnels.
- **Detour (1:1):** In Detour FRR, as a protected tunnel is being set up, each node along the path automatically creates a detour tunnel that avoids the next downstream node and that is used as a backup path for the protected tunnel. This requires no pre-provisioning of backup paths, so less management effort is required. However, each detour tunnel is used only by a single protected tunnel, so this scheme typically requires more resources to be reserved for the infrequently used backup paths.

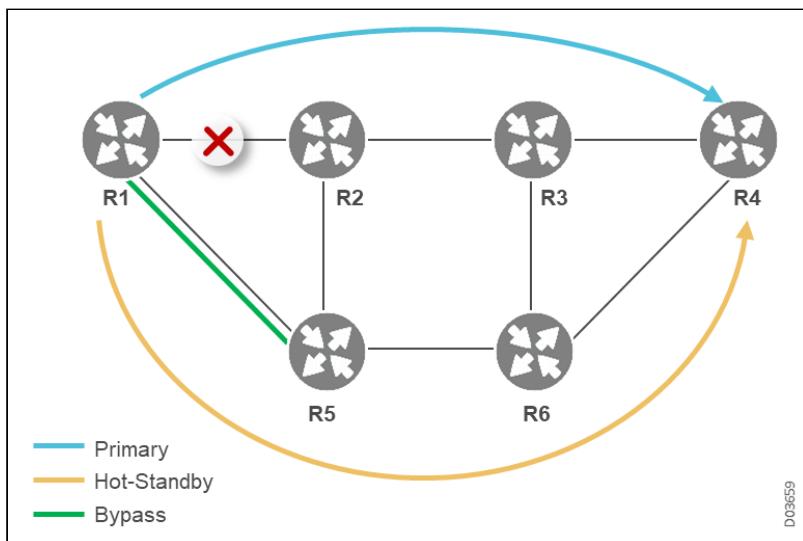
The nodes on the protected tunnel that are linked by a bypass or detour tunnel are referred to as the Point of Local Repair (PLR) and Merge Point (MP) nodes. A single node can act as both MP (for an upstream backup) and PLR (for a downstream backup) for the same protected tunnel. Any node but the egress can act as a PLR. Any node but the ingress can act as an MP.

### Facility Fast Reroute (FRR)

Facility (FRR) is a mechanism for protecting MPLS TE LSPs from link and node failures by locally repairing the LSPs at the point of failure (PLR), allowing data to continue to flow on them while their headend routers attempt to establish new end-to-end LSPs to replace them. FRR locally repairs the protected LSPs by rerouting them over **bypass tunnels** that bypass failed links or node.

- **Link Protection:** Bypass tunnels that bypass only a single link of the LSP's path provide link protection. They protect LSPs if a link along their path fails by rerouting the LSP's traffic to the next hop (bypassing the failed link). These are referred to as next-hop (NHOP) bypass tunnels. This single bypass LSP protects all the LSPs crossing the that link. Protecting an N number of LSPs crossing a link through the use of a single LSP improves the scalability aspect. Link protection is applied by default for all facility protected LSPs.
- **Node Protection:** FRR provides node protection only for those LSPs that desire node protection. These LSPs are explicitly configured with node protection since this is not the default setting. Bypass tunnels that bypass next-hop nodes along LSP paths are called next-next-hop (NNHOP) backup tunnels because they terminate at the node following the next-hop node of the LSP paths, thereby bypassing the next-hop node. They protect LSPs if a node along their path fails by enabling the node upstream of the failure to reroute the LSPs and their traffic *around* the failed node to the next-next hop. NNHOP Bypass tunnels also provide protection from link failures, because they bypass the failed link and the node.
- **Bandwidth Protection:** NHOP and NNHOP bypass tunnels can be used to provide bandwidth protection for protected LSPs. These protected LSPs are explicitly configured with bandwidth protection since this is not the default setting. Bandwidth protection may also be configured for NHOP or NNHOP bypass tunnels. This informs the PLR of the amount of backup bandwidth a particular backup tunnel can protect. When a PLR maps protected LSPs to backup tunnels, bandwidth protection ensures that an LSP uses a given bypass tunnel only if there is sufficient backup bandwidth.

### Bypass Tunnels



### Path Protection

RSVP-TE supports end-to-end path protection through configuration of primary and secondary LSPs for RSVP-TE tunnel. This type of protection is also known as “global repair”. RSVP-TE provides two types of secondary LSPs:

- **Hot Standby:** The secondary path is precomputed and pre-established, with the necessary resources reserved on both LSPs.
- **Cold Standby:** The secondary path is precomputed on the Headend, but not pre-established (not signaled); the resources are not held in reserve on the secondary LSPs.

Hot standby is more resource consuming; even when main path is up, we hold in reserve the resources that might be needed on the secondary path. By comparison, Cold standby only reserves resources after the active path fails.

Cold standby is typically used in path protected tunnels with 3 or more LSPs in the tunnel, configured as follows:

- The **Primary LSP** is the active LSP
- The **Secondary LSP** is a Hot standby (signaled and installed)
- The the third LSP is a Cold standby, and will only be signaled once the primary fails. At that point it turns into the Secondary LSP of the (former) Hot standby

### Backup Tunnel Selection

When an LSP is signaled, each node along the LSP path that provides FRR protection for the LSP selects a backup tunnel for the LSP to use if the link to the next hop fails, or if the next hop itself fails. By having the node select the backup tunnel for an LSP before a failure occurs, the LSP can be rerouted onto the backup tunnel quickly if there is a failure.

Auto-tunnel refers to the mechanism for automatically creating backup LSPs for signaled main LSPs with a protection flag enabled. Auto-created bypass tunnels enable a router to dynamically build bypass tunnels when they are needed.

## RSVP-TE Graceful Restart

The RSVP-TE Graceful Restart feature enables non-stop forwarding (NSF) in any case where the RSVP-TE process restarts, such as Active to Standby MCP, stateful switchover SSO, or if a failure occurs.

A restarting RSVP-TE process identifies that the forwarding plane states are working properly, and uses the help of its RSVP-TE helper peers to recover its previously successfully signaled PSB and RSB states. The helper RSVP peers first send the PATH messages of the working LSPs to the Restarting Peer node, which recovers its PATH states and sends PATH messages downstream towards its helper RSVP peers. The helper nodes, in turn, respond with RESV messages, which enable the Restarter to recover its LSP RESV states. Stale RSVP states that have not managed to recover during the Recovery time are deleted from the Restarter data plane.

Both restarting and helper RSVP-TE nodes can be LSP Headend, intermediate LSR, or Tailend LSR nodes. Using standard RSVP-TE Graceful Restart tools, an FRR Merging point cannot get the help of a helper PLR.

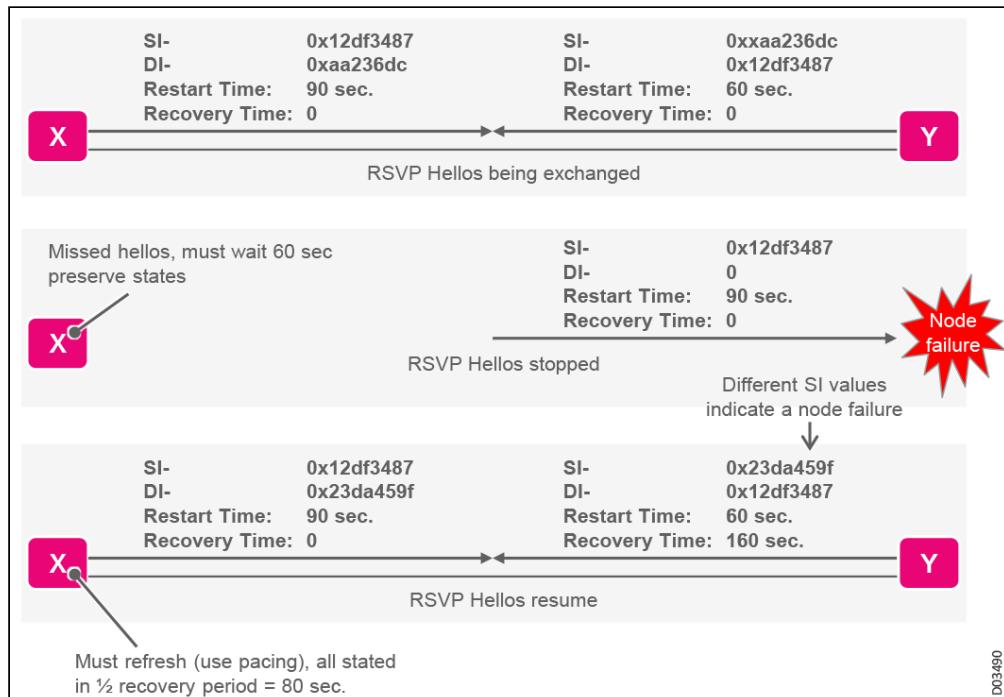
The RSVP-TE Graceful Restart **standard** mechanism includes the following key capabilities:

- RSVP Hello and Restart Capability Object, described in [RSVP-TE Hello](#).
- A new PATH message Recovery label object, which enables the upstream helper inform the downstream restarter of the label it used for the specified LSP via the PATH message Refresh.

RSVP-TE Graceful Restart relies on RSVP Hello adjacency, in which RSVP nodes learn about each other's expected Restart time and Recovery time during the RSVP restarting process. Each RSVP node tells his neighbor that it supports RSVP-TE Restarter. Using the Restart Capability Object, each node informs its peer about how long it should wait for its restarting peer RSVP node to recover, in case the Hello session has timed out. While restarting, it tells the peer how long it will take the restarted node to recover its control plane.

In the following diagram , nodes X and Y establish Hello adjacency and learn how long each of the peer routers expects its neighbor to wait (Restart time) for its recovery once Hello adjacency is lost. When a helper node learns about a restarting neighbor (via a new Source Instance) in the Hello Ack object, and learns the recovery time in the Restart\_Cap Object, it will immediately start helping the restarter to recover its PATH and RESV states. In the diagram, X learns that Y has restarted by receiving a Hello request with a new source instance number. X also learns that Y recovery time takes 160 seconds, which means that X must send Y all the PATH messages within 80 seconds. The helper must resend all PATH refresh messages including Recovery Label objects during the first half of the recovery time (since the restarting node must also send the PATH messages downstream and receive RESV messages from downstream helper nodes).

## Steps Prior to Recovery



As for the Headend restarter node, it recovers the locally originated LSPs PSB using a saved RRO and the related first hop label (received from downstream node) and sends that path downstream.

If the restarter Hello Request message includes a zero recovery time, this means that no forwarding states survived the restart, and all LSPs shared with the restarter node will be dropped and re-signaled.

The helper node must send all the PATH messages with a Recovery Label downstream to the Restarter LSR node. The helper node must then wait for an upstream restarter node to send it a PATH messages before it sends back the RESV refresh messages. This case covers an upstream restarter node that is not an LSP Headend.

If the Restarter is a Headend node, it can use the RFC5063 capability object to ask the downstream helper to send it a Recovery Path object. However, this feature is not supported by MSW in this version and therefore, an LSP Headend Restarter must keep each of the Headend LSPs RRO object in non-volatile memory and recover this information after RSVP-TE process restarts. Then, it must send the PATH message for the Headend LSP as soon as possible.

## RSVP-TE Hello

RSVP Hello was first defined in [RFC3209: Extensions to RSVP for LSP Tunnels](#) in order to enable the detection of peer failure when the neighbor node is not reachable. Later definitions of RSVP-Hello in [RFC3473](#) and [RFC5063](#) provide the major RSVP Hello mechanism for serving RSVP Graceful Restart.

Fundamentally, RSVP PATH and RESV messages can be exchanged even if Hello adjacency was not created. RSVP node Hello adjacency with a peer is only created if a Hello Request message with the local source IP address and destination IP address of the peer **it sent to the RSVP Peer** is answered with a Hello Ack message. **This Hello Ack message should have a non-zero SRC\_Instance and a DST\_Instance equal to the SRC\_Instance sent in the Hello Request.** Every RSVP node sends its own Hello Requests and the adjacency is only created when a valid Hello Ack is received as described above. RSVP-TE peers normally send each other Hello requests and expect Hello Acks from the peer.

The node then periodically sends a Hello Request message to the specific peer every Hello interval, making sure that the same Instance numbers are exchanged between the two neighbors. Hello adjacency is

considered lost if three consecutive Hello Requests have not been answered unless other RSVP packets are received, in which case the Hello timer is reset. Link connectivity failure is detected when the link Hello adjacency is lost but can also be detected by other measures such as single hop BFD, if enabled, or when IGP adjacency is lost. However, RSVP-TE node adjacency failure is only detected if all Hello connections, in case of multiple interfaces between the nodes, are lost. Under multiple unnumbered interfaces (when supported) only a single Hello session between the two neighbors using Router ID IP addresses as RSVP Hello Source and Destination accordingly.

An RSVP-TE link adjacency loss impacts the PSB/RSBs generated over this link. RSVP node Hello adjacency loss impacts all the PSB/RSB states established between the neighboring nodes. A node receiving Hello Ack with a SRC\_Instance that is different from the previously known SRC\_Instance learns that the peer node restarted. This is independent of whether adjacency was lost. The change in the Hello message SRC\_Instance number is nevertheless insufficient for NSF Graceful Restart recovery support. To RFC3473 added the Restart Cap Object to the RSVP Hello message.

A node that supports Graceful Restart Restarter mode uses the Hello Restart\_Cap Object for two purposes:

- To declare to its peer that it supports NSF Control plane recovery by indicating a non-zero restart time, which indicates the time it will take the restarter to restart its RSVP-TE process. A 0xffffffff value indicates that the node supports NSR and doesn't need state recovery help from the peer.
- To declare to its peer how long it will take it to recover as a restarting node. When restarting, after RSVP-TE process recovers, the restarting node sends the Hello Request Restart\_Cap object with Recovery time which is greater than 0. If the restarting node sets a Zero Recovery time, this means that no forwarding states survived the restart event and therefore, all RSVP LSPs states (PATH and RESV) stated between the two nodes will be removed.

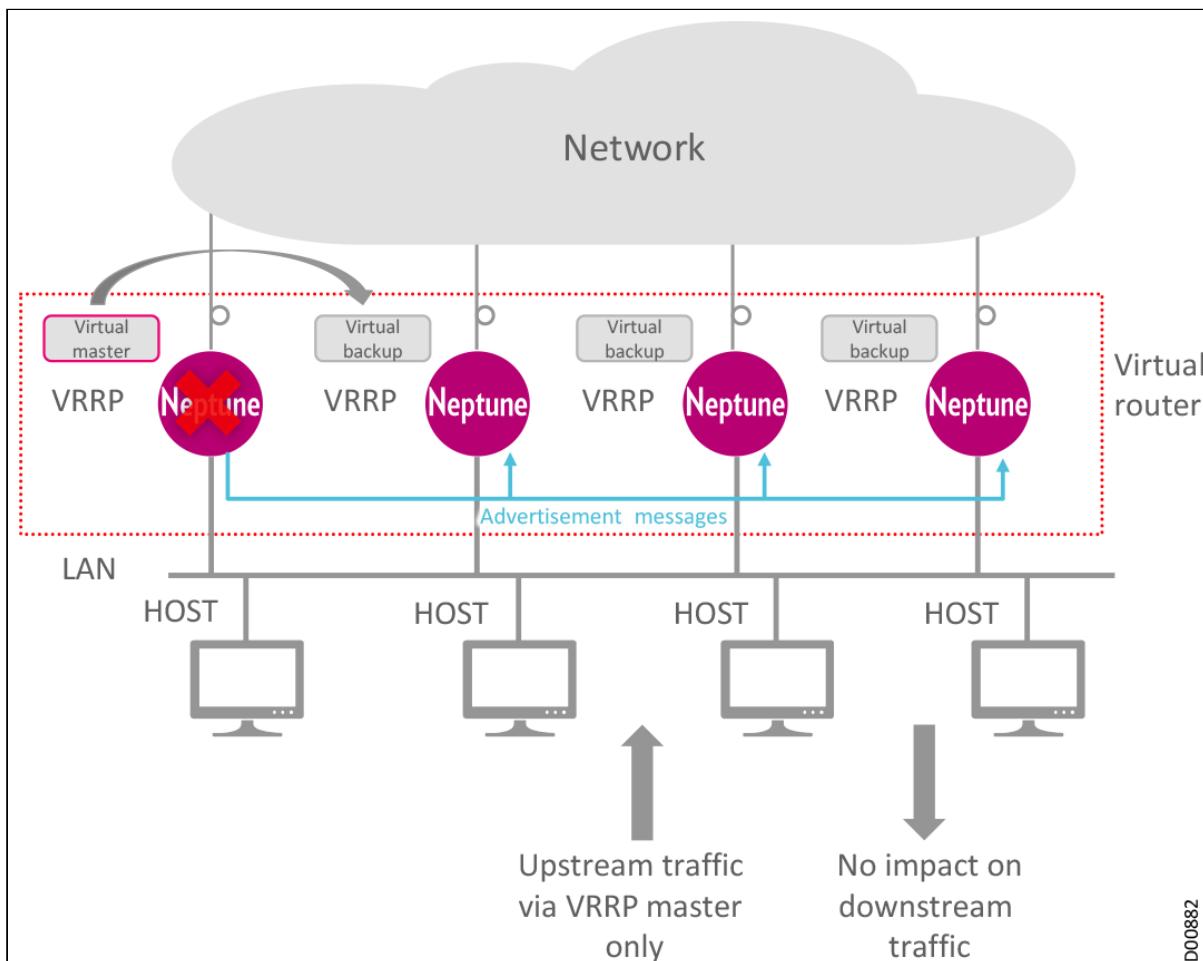
The helper peer that receives the Hello Request from a peer with a Restart-Cap whose recovery time is greater than 0, sends PATH/RESV refresh messages as needed. For more details on the state recovery process, see [RSVP-TE Graceful Restart](#).

Additional Hello extensions are defined in [RFC5063](#) to enable recover Path state blocks in Head-end node. The Hello message Capability object was defined to enable a head-end LSR to request the last PATH message from the downstream node, which sends the RecoveryPath message. For more details, see [RSVP-TE Graceful Restart](#).

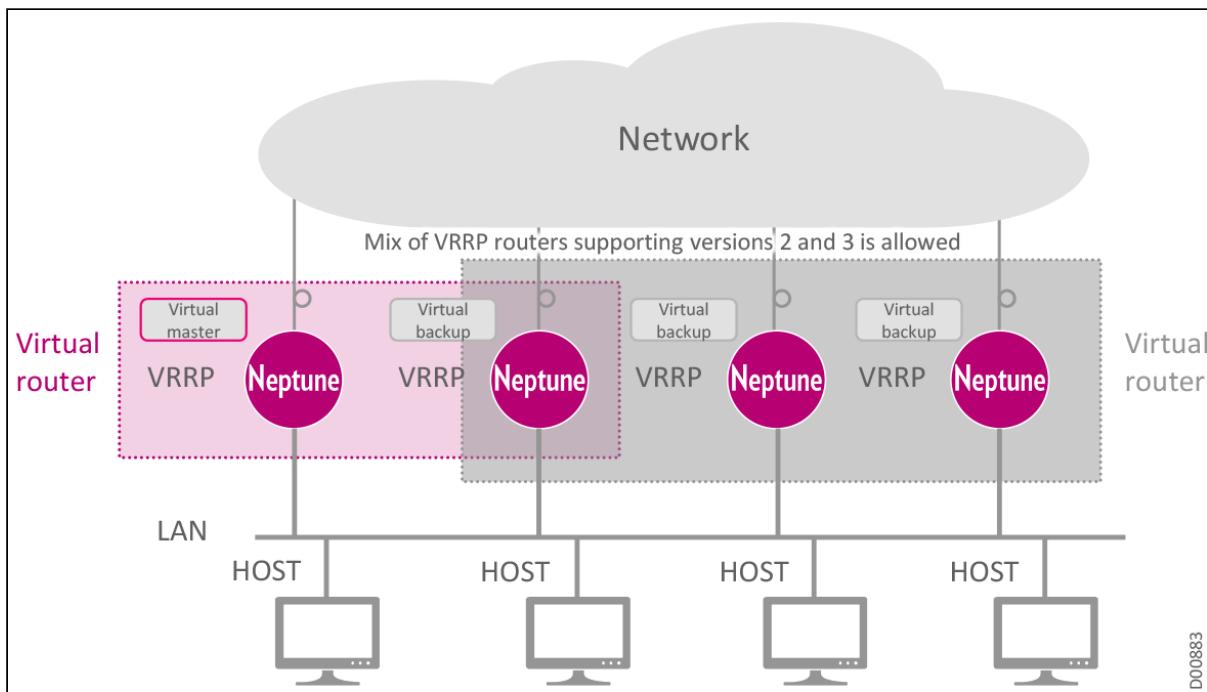
# Virtual Router Redundancy Protocol VRRP

The Virtual Router Redundancy Protocol (VRRP), defined in IETF RFP 5798, is a networking protocol that defines a method for automatic assignment of available IP routers to participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP subnetwork.

## VRRP Operational Scenarios - Basic Configuration

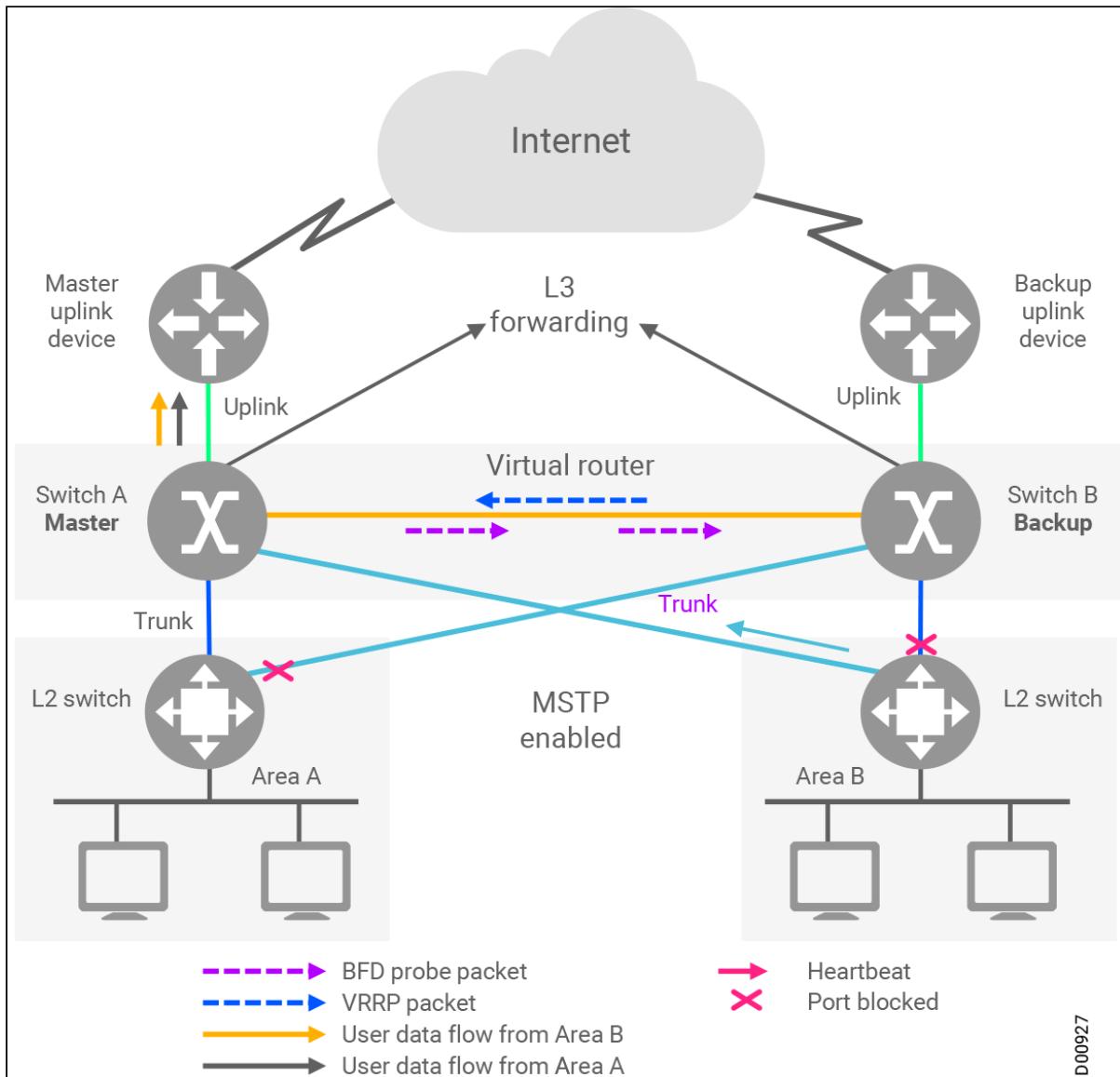


The default gateway for a participating host is assigned to a virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The selection process provides dynamic fail-over for the forwarding responsibility, should the master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

**VRRP Operational Scenarios - Mix of v2 and v3**

Neptune's VRRP implementation incorporates BFD to shorten the time needed to detect a failure of the master router. The master and backup routers use BFD as part of their communication system.

### VRRP Operational Scenarios - Configuring BFD for VRRP



# Layer 2 VPN: Providing a Full Set of MEF CE3.0 Services

A Layer 2 Virtual Private Network (L2VPN) is a method that Internet service providers use to subdivide their network between different customers, allowing each customer to transmit data over a separate IP network. This is often sold as a service to businesses. Layer 2 VPNs use MPLS labels to transport data. Communication occurs between routers that are known as Provider Edge routers (PEs), as they sit on the edge of the provider's network, next to the customer's network.

Internet providers who already have an existing Layer 2 network (such as ATM or Frame Relay) may choose to use these VPNs instead of a Layer 3 VPN, allowing them to have a single infrastructure for both IP and legacy services. Two methodologies are typically used: BGP-based and LDP-based. Both methods use a standard MPLS header to encapsulate data. They simply differ in their signaling protocols.

- **BGP-based:** Border Gateway Protocol (BGP) is used for communication between PE routers about their customer connections. Each router connects to a central cloud, using BGP. This means that when new customers are added (usually to new routers), the existing routers will communicate with each other, via BGP, and automatically add the new customers to the service.
- **LDP-based:** Label Distribution Protocol (LDP) is used for communication between PE routers. (This method is also known as a Layer 2 circuit.) With this method, every LDP-speaking router will exchange FECs (forwarding equivalence classes) and establish LSPs with every other LDP-speaking router on the network (or alternatively, when LDP is tunneled over RSVP-TE, the router connects only to the other PE router). The LDP-based L2VPN defines new TLVs and parameters for LDP to assist with VPN signaling.

The Metro Ethernet Forum (MEF) has defined a comprehensive set of L2VPN carrier class transport solutions for emerging Ethernet-based applications, including:

- Triple play
- Business connectivity (enterprise and SMB)
- Ethernet-based mobile aggregation
- DSLAM transport and aggregation

These services are technology-agnostic, and can be offered over IP/MPLS, MPLS-TP, Ethernet, or any combination of technologies. The range of data-centric services defined by the MEF standards includes:

- **Ethernet Line (E-Line)** for P2P connectivity, used to create Ethernet private line services, Ethernet-based internet access services, and P2P Ethernet VPNs. These include:
  - **Ethernet Private Line (EPL):** P2P Ethernet connection that uses dedicated bandwidth, providing a fully managed, highly transparent transport service for Ethernet. EPL provides an extremely reliable and secure service, as would be expected from a private line.
  - **Ethernet Virtual Private Line (EVPL):** P2P connectivity over shared bandwidth. Service can be multiplexed at the user-to-network interface (UNI) level.

E-Line services may be implemented, for example, through an MPLS-based Virtual PseudoWire Service (**VPWS**). This implementation provides P2P connectivity over MPLS PW, sharing the same tunnel on the same locations and benefiting from MPLS end-to-end hard QoS (H-QoS) and carrier class capabilities.

- **Ethernet LAN (E-LAN)** for multipoint-to-multipoint (MP2MP) (any-to-any) connectivity, designed for multipoint Ethernet VPNs and native Ethernet Transparent LAN Services (TLS). These include:
  - **Ethernet Private LAN (EPLAN):** Multipoint connectivity over dedicated bandwidth, where each subscriber site is connected to multiple sites using dedicated resources (so different customers' Ethernet frames are not multiplexed together).
  - **Ethernet Virtual Private LAN (EVPLAN):** Multipoint connectivity over shared bandwidth, where each subscriber site is connected to multiple sites using shared resources. This is a highly cost-effective service, as it can leverage shared transmission bandwidth in the network.

E-LAN services may be implemented, for example, through an MPLS-based **VPLS**. This implementation provides multipoint connectivity over MPLS PW, sharing the same tunnel, and enables

delivery of any-to-any connectivity that expands a business LAN across the WAN. VPLS enables SPs to expand their L2VPN service offerings to enterprise customers. VPLS provides the operational cost benefits of Ethernet with the end-to-end QoS of MPLS.

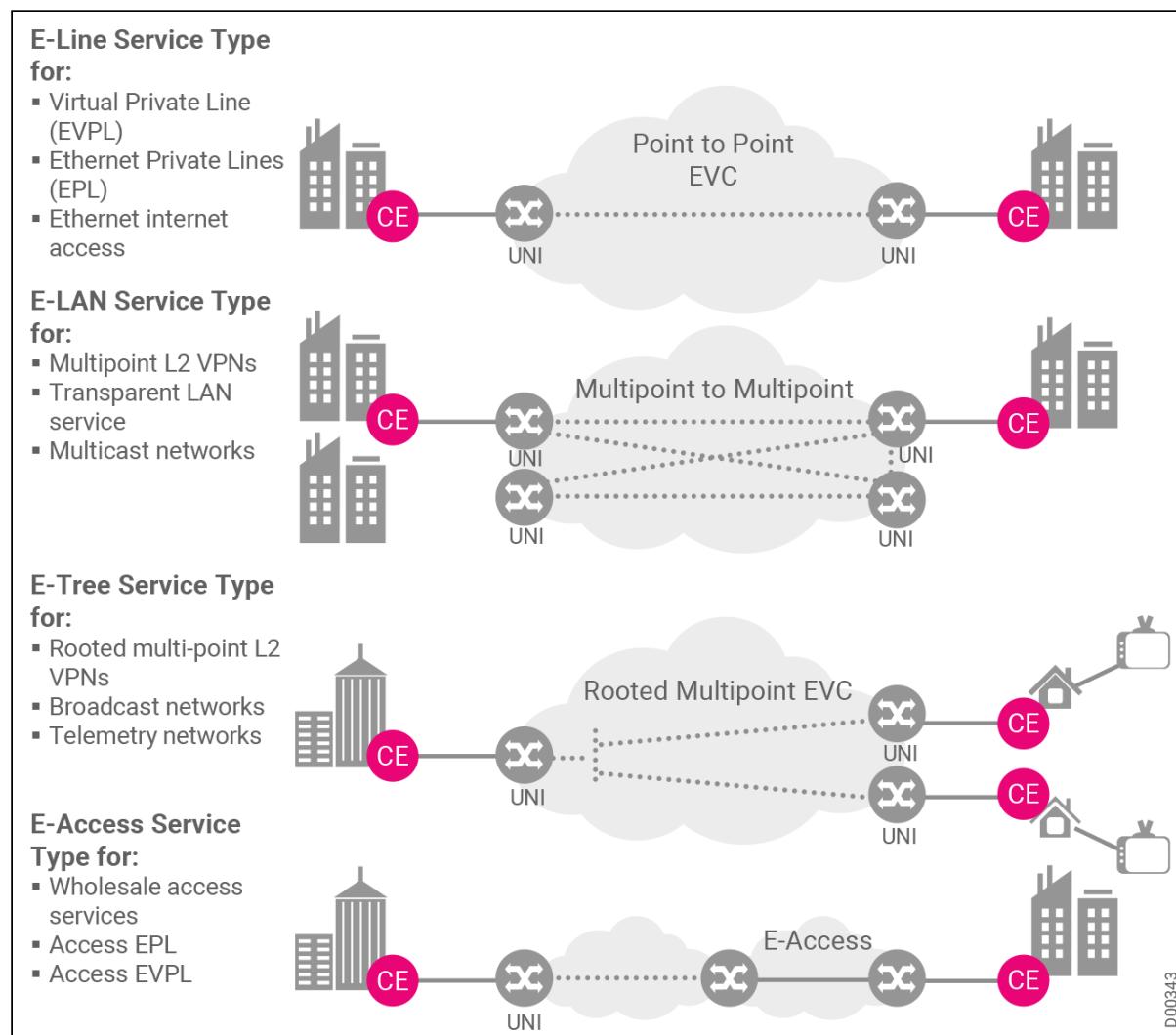
Classic VPLS service creates a full mesh between all network nodes and, under certain circumstances, this may not be the most efficient use of network resources. With H-VPLS, full mesh is created only between hub nodes using Split Horizon Groups (SHGs). Spoke nodes are only connected to their hubs, without SHGs. This efficient approach improves MP2MP service scaling and allows less powerful devices such as access switches to be used as spoke nodes, since it removes the burden of unnecessary connections.

- **E-Tree (Rooted-Multipoint)** for point-to-multipoint (P2MP) multicast tree connectivity, designed for BTV/IPTV services. These include:
  - **Ethernet Private Tree (EP-Tree):** In its simplest form, an E-Tree service type provides a single root for multiple leaf UNIs. Each leaf UNI only exchanges data with the root UNI. This service is useful and enables very efficient bandwidth use for BTV or IPTV applications, such as multicast/broadcast packet video. With this approach, different copies of the packet need to be sent only to roots that are not sharing the same branch of the tree.
  - **Ethernet Virtual Private Tree (EVP-Tree):** An EVP-Tree is an E-Tree service that provides rooted-multipoint connectivity across a shared infrastructure supporting statistical multiplexing and over-subscription. EVP-Tree is used for hub and spoke architectures in which multiple remote offices require access to a single headquarters, or multiple customers require access to an internet SP's point of presence (POP).

E-Tree services may be implemented, for example, through an **MPLS Rooted-P2MP Multicast Tree** that provides an MPLS drop-and-continue multicast tree on a shared P2MP multicast tree tunnel, supporting multiple Digital TV (DTV)/IPTV services as part of a full triple play solution. LightSOFT provides full support for classic E-Tree functionality as of the current release.

- **E-Access (Ethernet Access)** for Ethernet services between UNI and E-NNI endpoints, based on corresponding Operator Virtual Connection (OVC) associated endpoints. Ethernet services defined within the scope of this specification use a P2P OVC which associates at least one OVC endpoint as an E-NNI and at least one OVC endpoint as a UNI. These services are typically Ethernet access services offered by an Ethernet Access Provider. The Ethernet Access Provider operates the access network used to reach SP out-of-franchise subscriber locations as part of providing end-to-end service to subscribers.

## MEF Definitions for Ethernet Services



The Neptune product line supports the full set of MEF services, including end-to-end QoS, C-VLAN translation, flow control, and Differentiated Services Code Point (DSCP) classification.

This section includes the following sections:

- Ethernet Private Line EPL - Ethernet Virtual Private Line EVPL
- Ethernet Private LAN EPLAN - Ethernet Virtual Private LAN EVPLAN
- Multicast Optimized Rooted-MP Services
- IP Multicast Architecture
- IGMP-Aware MP2MP VSI

## Ethernet Private Line EPL - Ethernet Virtual Private Line EVPL

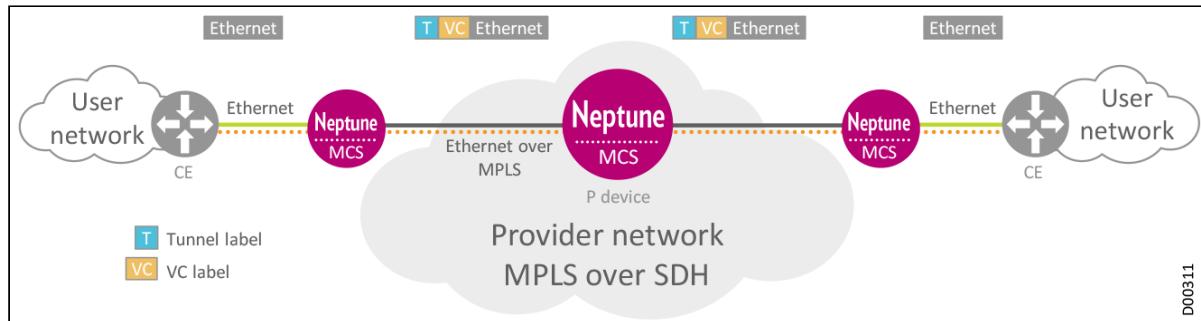
VPWS forms a **P2P Ethernet service** between two sites belonging to the same customer. P2P services can be dedicated per customer or shared through statistical multiplexing between customers.

VPWS uses P2P tunnels originating at the source PE devices, traveling through Transit Ps, and terminating at the destination PE. The term PseudoWire (PW) encapsulation is used to refer to transporting P2P Ethernet traffic over an MPLS tunnel.

As illustrated in the following figure, the **Source PE** pushes two MPLS labels into each customer's Ethernet packet as it enters the tunnel. The inner MPLS label is the **VC label**, and represents the VPN to which the packet belongs. The VC label serves as a demultiplexer field, allowing aggregation of multiple VPNs into a single tunnel and thereby providing a scalable tunneling solution rather than a dedicated tunnel per VPN. The outer MPLS label is the **Tunnel label**, and represents the tunnel to which the packet is mapped.

The **Transit P** provider devices simply swap the MPLS labels from the incoming port to the outgoing port. The **Destination PE** terminates the tunnel and identifies the packet VPN based on the VC label. The Destination PE then removes (pops) the two MPLS labels and forwards the packet to the customer equipment (CE) port(s).

#### P2P MPLS Tunnel Example

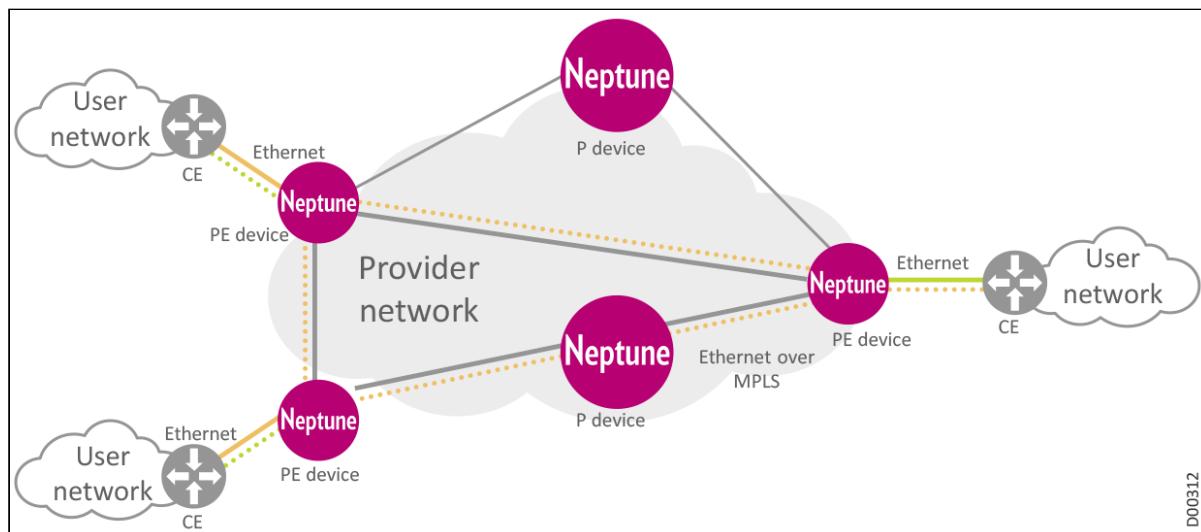


## Ethernet Private LAN EPLAN - Ethernet Virtual Private LAN EVPLAN

VPLSs and TLSs provide connectivity between geographically dispersed customer Ethernet sites across the SP network, creating a virtual LAN network. The interconnected customer sites form a Layer2 VPN.

VPLS service can be configured for MP2MP services (VPLS full mesh), hub and spoke services (VPLS partial mesh), and statistical multiplexing between various virtual LAN customer VPNs.

#### VPLS Service Example



Sites that belong to the same MPLS VPN expect their packets to be forwarded to the correct destinations. This is accomplished through the following means:

- Establishing a full mesh of MPLS LSPs or tunnels between the PE sites.
- MAC address learning on a per-site basis at the PE devices.

- MPLS tunneling of customer Ethernet traffic over PWs while it is forwarded across the provider network.
- Packet replication onto MPLS tunnels at the PE devices, for multicast-/broadcast-type traffic and for flooding unknown unicast traffic.

## Multicast Optimized Rooted-MP Services

Neptune platforms provide E-Tree services with maximum efficiency at minimum cost. Metro network optimization is achieved by an efficient MPLS P2MP multicast tree carrying IPTV services concurrently with hub and spoke ("Star VPLS") connectivity for other triple play services such as VoD, VoIP, and HSI.

The P2MP tunnels carry multicast content such as IPTV in a triple play network, but P2MP tunnels are not enough on their own. Two other functionalities complete the triple play solution:

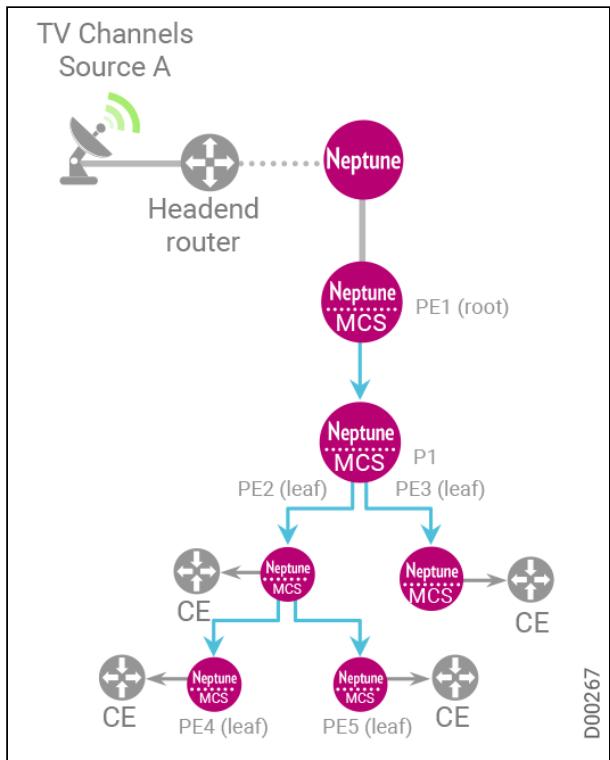
- Star VPLS
- IGMP snooping

The triple play service delivery network architecture includes the following components:

- **End-to-end MPLS carrier class capabilities.** MPLS capabilities assure the QoS of IPTV service delivery over dedicated P2MP tunnels (MPLS multicast tree).
- **Multiple distributed PE service edges (leaf PE).** Leaf PEs terminate the IPTV downstream traffic arriving over P2MP tunnels and apply IGMP snooping, policing, and traffic engineering on upstream traffic. This gives SPs the ability to scale their IPTV network.
- **Efficient IPTV multicast distribution.** IPTV distribution utilizes an efficient drop-and-continue methodology, using an MPLS P2MP multicast tree to deliver IPTV content across the metro aggregation network. This allows SPs to optimize bandwidth utilization over the metro aggregation network. It also enables simple scaling capabilities as IPTV service demands increase.
- **IGMP snooping** at the PE leaf service edges allows the PE device to deliver only the IPTV channels requested by the user, further improving bandwidth consumption over the Ethernet access ports and enabling easy scalability as the number of IPTV channels grows.
- **Star VPLS topology** to carry the VoIP, VoD, and HSI P2P services. The star VPLS is built over the aggregation network from the root PE (aggregator) device that connects the edge router/BRAS to the leaf PE that connects the IPDSLAM/MSAN. This star VPLS also carries the bidirectional IPTV control traffic that is either sent by the router downstream (IGMP query), or sent by the subscriber set-top-box (STB) upstream at channel zapping events (IGMP join/leave requests).
- **End-to-end interoperability** with the DSLAM/MSAN and MSER, implemented either by the Ethernet or the MPLS layer. The P2MP multicast tree continues from the PIM-SM multicast tree over the core network.

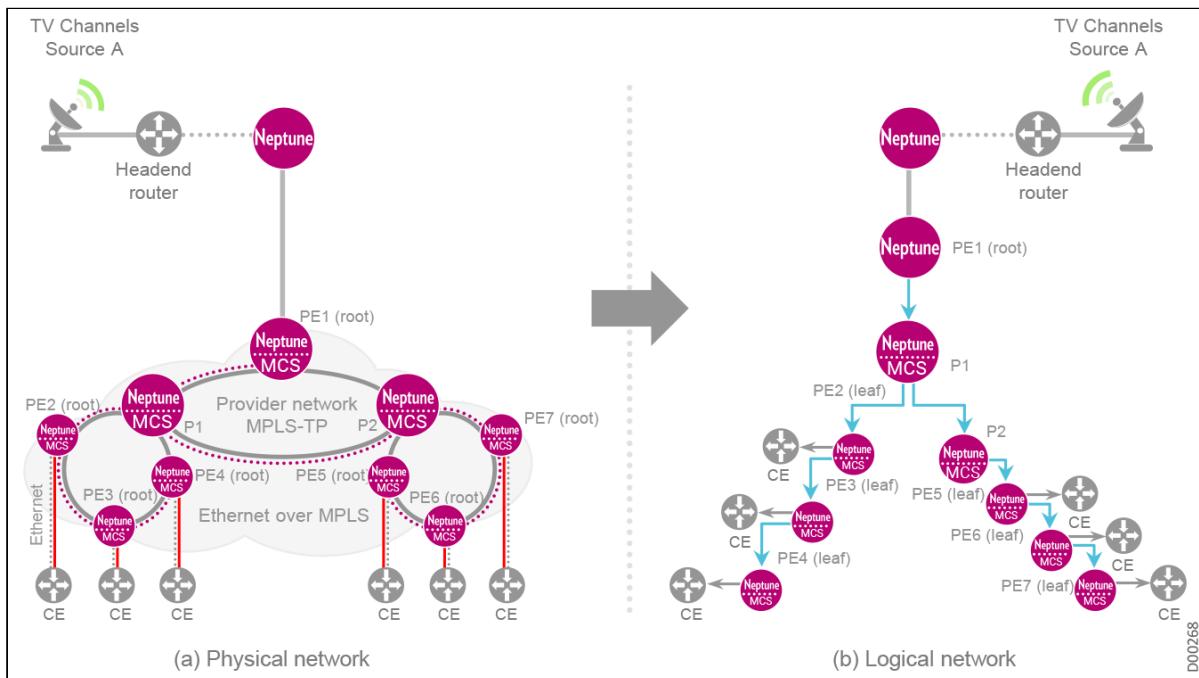
A **P2MP** tunnel originates at the source PE and terminates at multiple destination PEs. This tunnel has a tree-and-branch structure, where packet replication occurs only at branching points along the tree. This scheme achieves high multicast efficiency since **only one copy of each packet ever traverses an MPLS P2MP tunnel**. The Neptune can act as both a transit P and as a destination PE within the same P2MP tunnel, in which case it can be referred to as a **Transit PE** rather than a Transit P.

### P2MP Multicast Tunnel Example



The following figure illustrates a second example of a P2MP multicast tree arranged over a multi-ring topology network. The multicast tunnel paths are illustrated in both a physical layout and a logical presentation. In this example, PE1 is the source PE (root); P1 and P2 are transit Ps; PE2, PE3, PE5, and PE6 are transit leaf PEs; and PE4 and PE7 are destination leaf PEs.

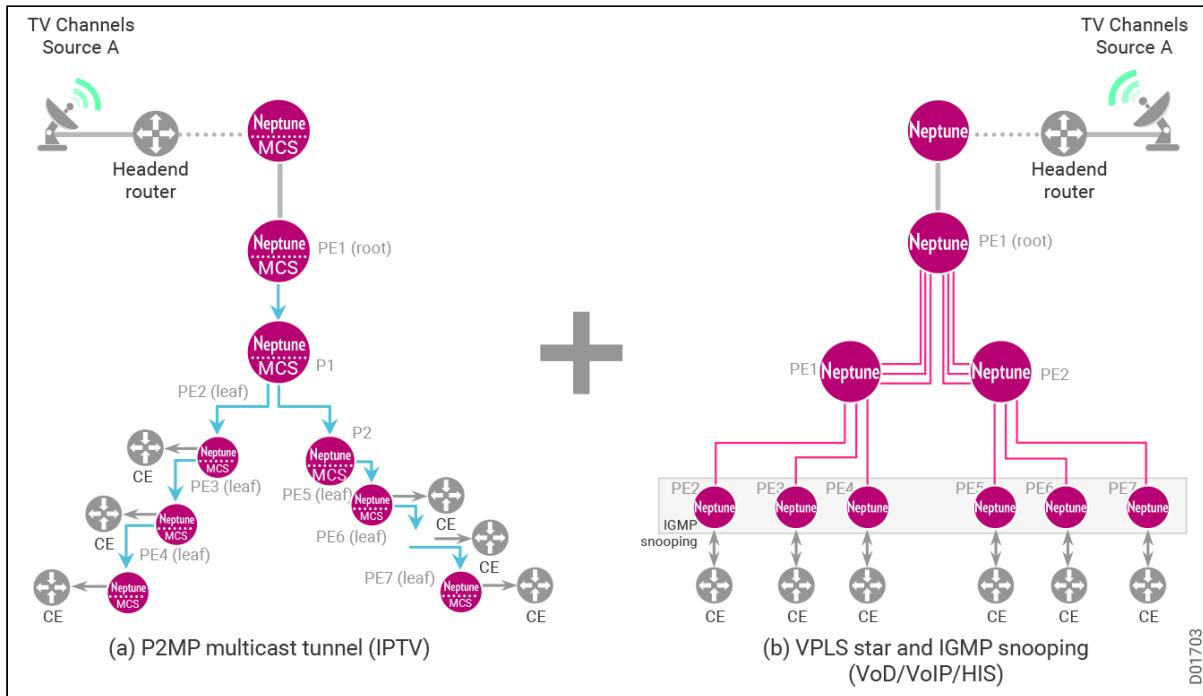
### P2MP Multicast Tunnel Example - Physical and Logical Networks



The full triple play solution, incorporating P2MP multicast tunnels, star VPLS, and IGMP snooping, is illustrated in the following figure. The P2MP multicast tunnels carry IPTV content in an efficient drop-and-

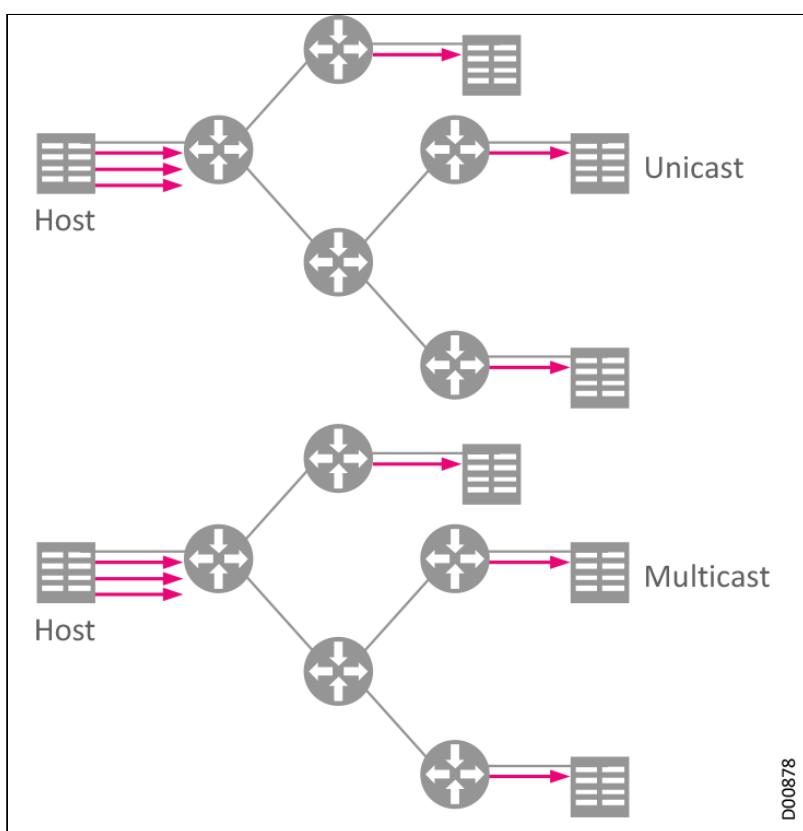
continue manner from the TV channel source, headend router, and MSER, through the root PE (PE1) to all endpoint leaf PEs. The VPLS star carries all other P2P triple play services, such as VoIP, VoD, and HSI. The VPLS star also carries the IGMP messages both upstream (request/leave messages from the customer) and downstream (query messages from the router). IGMP snooping is performed at the endpoint leaf PEs to deliver only the IPTV channels requested by the user. This allows scalability in the number of channels, as well as freeing up bandwidth for other triple play services.

### Triple Play Network Solution for IPTV VoD and HSI Services



## IP Multicast Architecture

### Unicast vs. Multicast

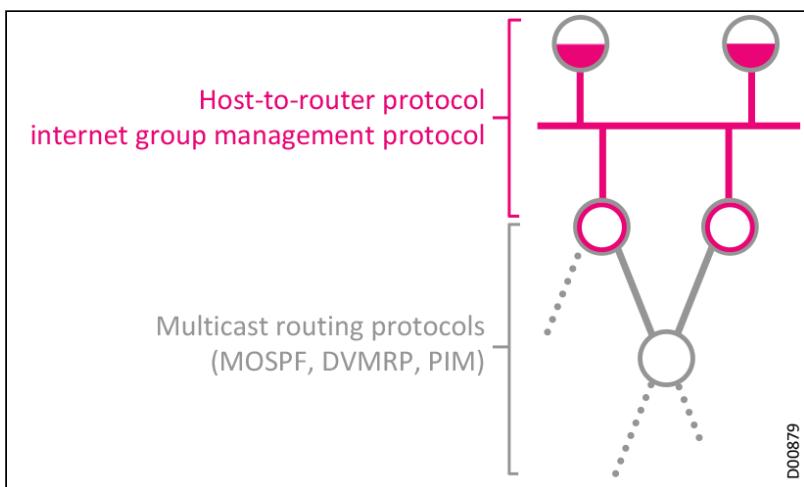


In an IP multicast architecture, the hosts communicate with the routers through the **Internet Group Management Protocol (IGMP)**. IGMP runs between the routers and local hosts on the IP/MPLS network.

Hosts may join or leave the multicast group by sending IGMP requests to the multicast router:

- The **Join** request is used to register the channel in the IGMP proxy entities all the way up to the IGMP router.
- The router, residing at the head of the multicast tree, queries the IGMP multicast tree entities all the way back down to the local hosts for multicast group membership.
- The hosts respond with membership reports.
- The routers distribute transmission packets to their destinations using a multicast routing protocol such as PIM.
- PIM and IGMP integration is usually implemented according to the interaction guidelines defined in RFC5168.

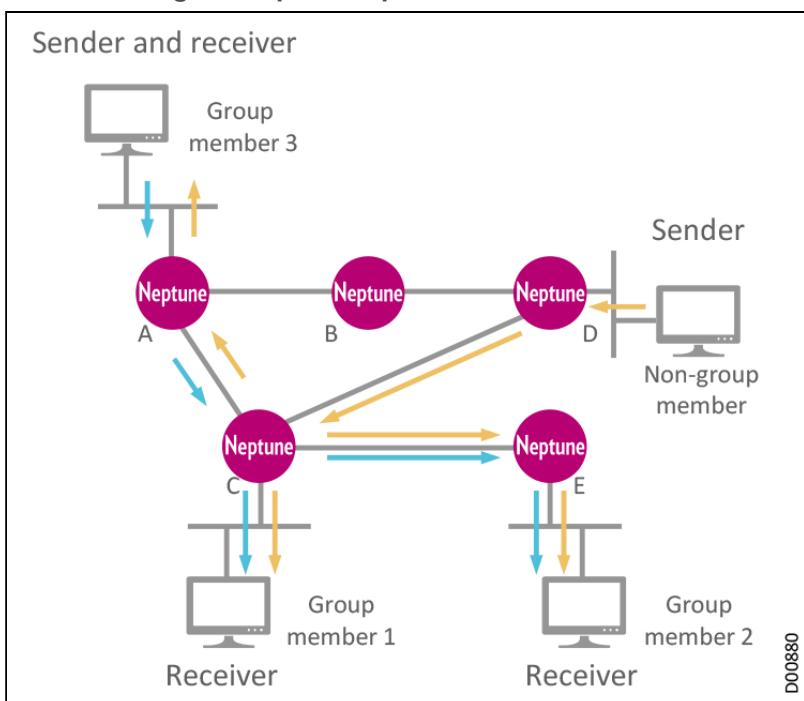
## IP Multicast Architecture



IP multicasting utilizes a group concept:

- In order to receive group data, the receiver must be a group member.
- When sending data to a group address, all members receive that data transmission.
- The destination IP address for a group transmission doesn't directly indicate where to forward the packet.
- Packets are forwarded based on multicast distribution trees.
- Users create distribution trees that control the path that IP multicast traffic takes through the network in order to deliver traffic to all receivers.
- The distribution tree is constructed at service creation.

## IP Multicasting - Group Concept



Based on how the receivers treat the multicast sources, there are two multicast models:

- **ASM (any-source multicast) model:** In the ASM model, any sender can be a multicast source sending multicast information to a multicast group. Receivers can join a multicast group identified by a group

address and obtain multicast information addressed to that multicast group. In this model, receivers are not aware of the location of the multicast source in advance. However, they can join or leave the multicast group at any time. The multicast routing protocols mentioned previously are used mainly for the ASM model. In ASM, receivers cannot specify the multicast sources they are interested in; instead, they passively receive multicast streams from all multicast sources.

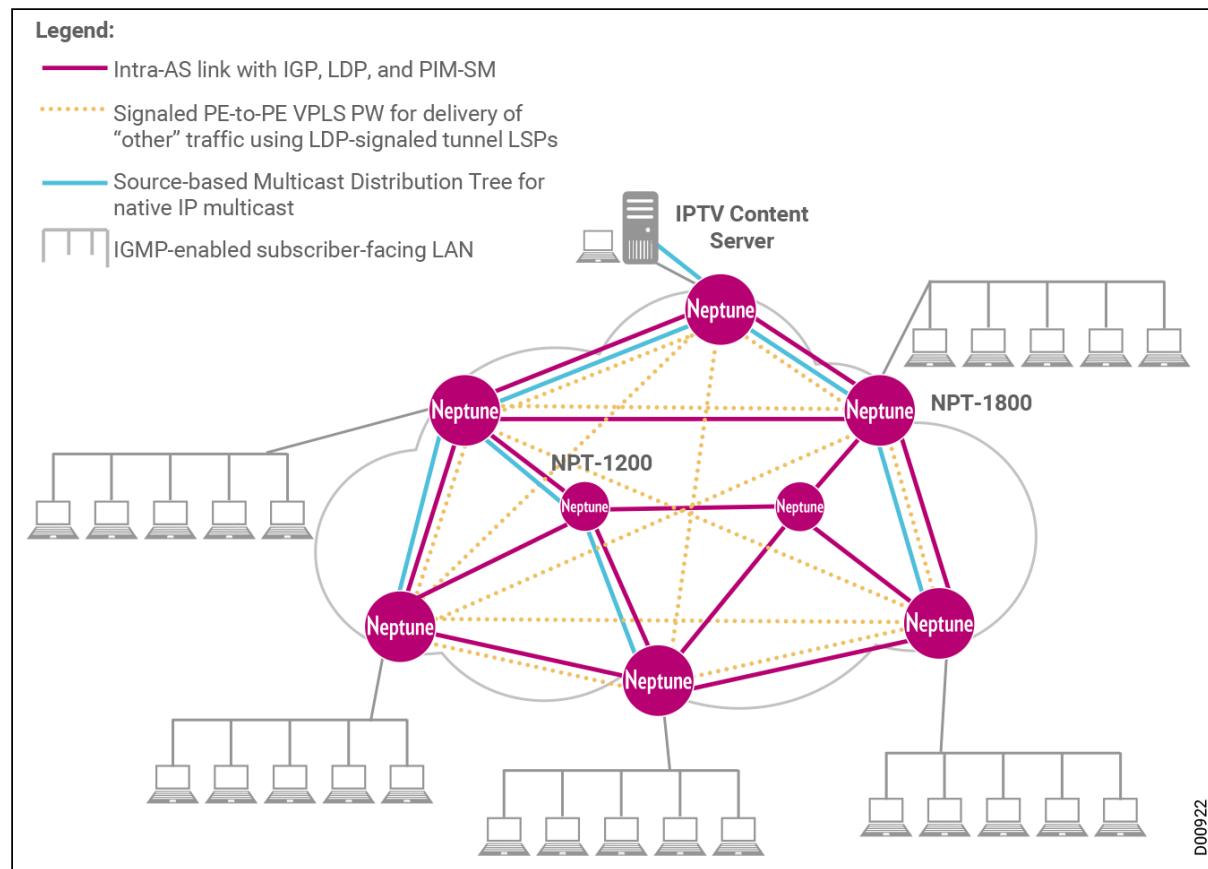
- **SSM** (source-specific multicast) model: In a real-world context, users may only be interested in the multicast data from certain specific multicast sources. The SSM model provides a transmission service that allows users to specify the multicast sources in which they are interested at the client side. Unlike the ASM model, the SSM model allows hosts to specify the multicast sources. In the SSM model, the multicast address range is different from that of the ASM model. Dedicated multicast forwarding paths between receivers and the specified multicast sources are established through PIM-SM. With this model, receivers know exactly where a multicast source is located.

## IGMP-Aware MP2MP VSI

IPTV services are in demand, but they can be complicated to implement. This section describes a typical IPTV network scenario, and highlights the efficient solutions provided by Neptune networks.

IPTV services typically combine elements of both unicast and multicast traffic. The unicast and non-routable multicast or broadcast traffic is carried on the same interface (DHCP, VoD, etc.). Limiting the service to a source-specific multicast (SSM) configuration resolves privacy issues, since different content providers use different source addresses. Subscribers are managed using IGMPv3, and distribution is limited to a single IP/MPLS domain. IGP provides full mesh IP connectivity and external route distribution as needed, and LDP provides full mesh MPLS connectivity between PE nodes. The data plane supports native IP forwarding for SSM, with strict RPF to eliminate loops. The control plane supports native IP multicast through PIM-SM in SSM mode.

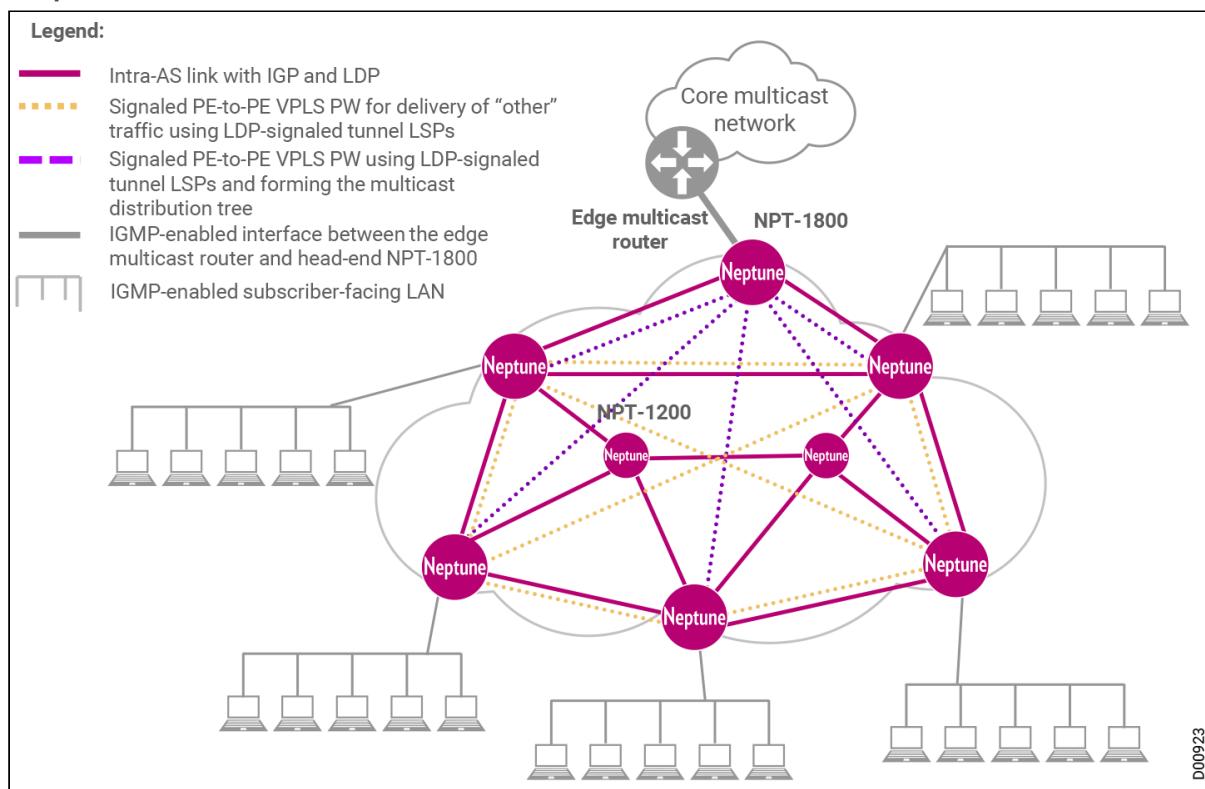
### IPTV Solution



IGMP-aware MP2MP VSIs augment the network elements illustrated in the preceding figure by combining multicast and unicast traffic on the same interfaces, and reducing multicast traffic towards subscribers at the domain edge. This approach uses standard VPLS mechanisms for intra-domain delivery. Multicast delivery is implemented through ingress replication across a full mesh of PWs, filtered based on subscriber requests to eliminate unnecessary traffic. These elements are highlighted in the following figure.

On the management plane, this approach is implemented through an enhanced VSI configuration that includes enabling IGMP proxy functionality. Upstream (host) and downstream (router) AC (link) and peer (node) must be explicitly configured as IGMP-aware, and assigned their own IP addresses and subnet masks. On the control plane, IGMP proxy is implemented through configuring one instance per VSI, including the corresponding upstream and downstream node and interface parameters. IGMP queries and responses are handled at the control plane level. On the data plane, traffic received from an IGMP-aware AC or peer is separated and handled according to its type (IGMP traffic, non-IGMP routable IP multicast, or other MP2MP VSI traffic).

### Simple Network Reference Model for IGMP-Aware VSI



This diagram shows an IP/MPLS domain representing a single AS with GP (IS-IS or OSPF) running on all intra-AS links. An MP2MP L2VPN service (VPLS) is set up between some PEs, with a full mesh of PWs set up between all VSIs representing this service in each of the affected NEs using tLDP.

An edge multicast router is connected to one of the PEs of an MP2MP L2VPN (VPLS) service. Multiple subscribers to this content are connected to other PEs participating in this VPLS instance via access LANs. Each subscriber indicates its interest in one or more IPTV channels using IGMPv3, with each IPTV channel mapped to exactly one SSM Multicast Channel.

The VSI representing the VPLS service in question in each of the affected PEs is marked as IGMP-aware. Its relevant ACs are marked as Upstream or Downstream. Each PW that connects the VSI that is directly connected through the edge multicast router to a VSI that is directly connected to a subscriber LAN is treated as an Upstream interface in the former and as a Downstream interface in the latter. An IGMP Proxy instance is associated with this VSI and treats its Downstream and Upstream ACs and PWs as if they were Upstream and Downstream.

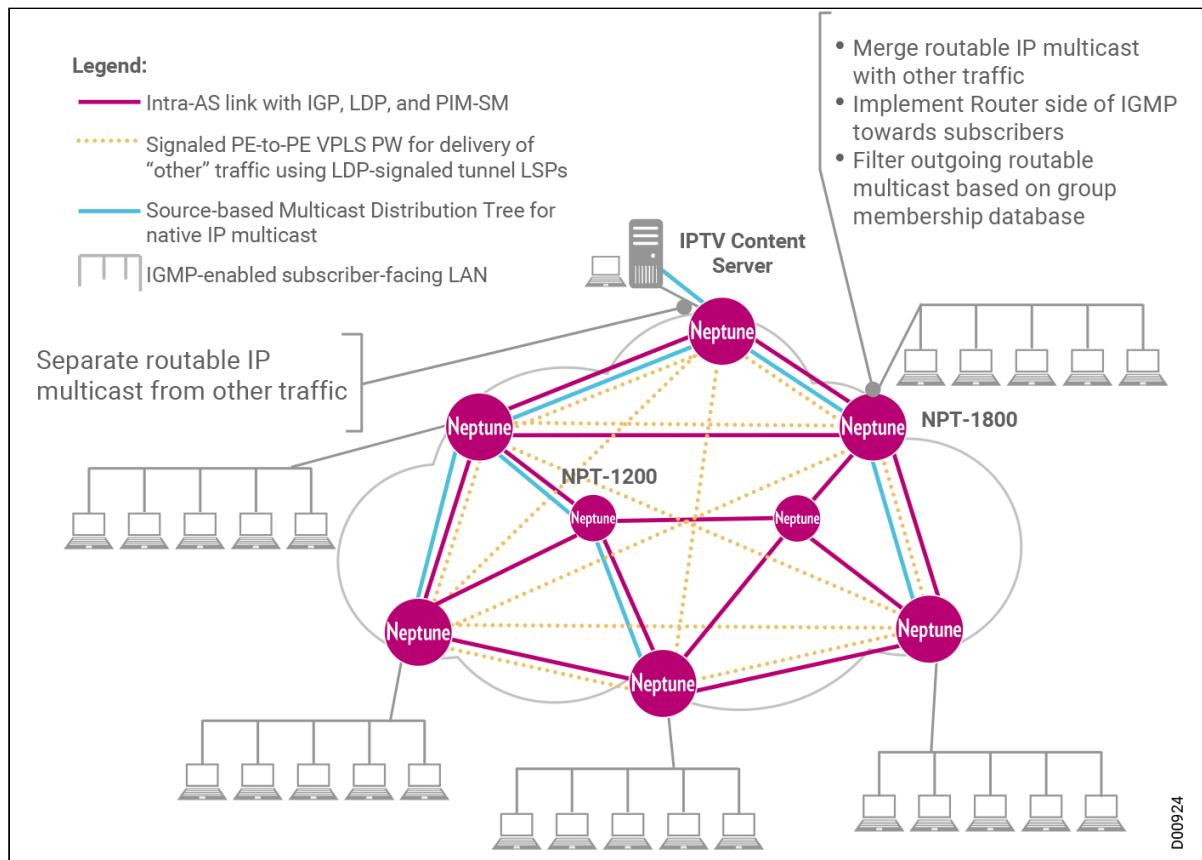
When an Ethernet frame is received from the Upstream AC or PW associated with an IGMP-aware VSI, it is checked to see whether it belongs to one of the following traffic types:

- IGMP packets. These are identified by Ethertype being IPv4 and IP protocol number being IGMP. The IGMP packets are trapped to the IGMP Proxy instance for processing.
- Routable IP multicast packets. These are identified by Ethertype being IP, IP protocol number being *different* from IGMP, and Destination IP address being a routable IP multicast address. The routable IP multicast packets undergo normal VPLS flooding, subject to additional filtering based on the contents of the Group Membership DB built by the corresponding IGMP Proxy instance.
- All other packets. These frames receive normal VSI forwarding in accordance with the L2 FIB of the VSI created by the normal MAC Learning process.

With this network model, these rules result in the following handling of routable multicast traffic transmitted by the IPTV Content Server:

- Unicast traffic will be forwarded as if in the normal MP2MP VSI. For example:
  - Unicast traffic generated by triple play services (such as VoIP, internet access, or VoD traffic)
  - Fast delivery of the baseline picture after selecting a new IPTV channel by the subscriber
- Each routable IP multicast packet received from the server by the directly-connected PE would be forwarded (using ingress replication) to all PEs connected to the subscriber LANs that have requested the corresponding Multicast Channel.
- The PE that is directly connected to the subscriber LANs will forward each routable IP multicast packet received from its single Upstream PW to all subscriber LANs where subscribers have requested this channel. The packet will not be sent to the LANs where nobody has requested the channel.

### Focus on IGMP Awareness



# Layer 2 Service Card Functionality

Ethernet Layer 2 cards provide many L2 service features, some of which are introduced in the following sections:

- Layer 2 Card Services
- Generic Faming Procedure
- Virtual Concatenation
- Link Capacity Assignment Scheme
- Layer 2 Switching Capabilities
- FDB Quota Provisioning
- Triggers for MSTP
- Port-Based VLANs
- UNI on EoS Ports
- NNI on ETY Ports
- C-VLAN Functionalities
- Access-Controlled Management
- Port Mirroring
- L2CP Flooding Protection
- Additional Features

## Layer 2 Card Services

Neptune Layer 2 cards support the following services:

- **Transparent LAN Service (TLS)** - connects multiple ports belonging to the same customers over shared SDH bandwidth, with user-defined grades of service.
- **Virtual Leased Line (VLL)** - connects two external ports over shared SDH bandwidth.
- **Dedicated VLL** - VLL service over SDH capacity dedicated only to a single customer. Provides zero packet loss, virtually no delay, and zero delay variation.
- **Guaranteed VLL** - VLL with zero frame loss rate and bounded delay and delay variation.
- **ISP connectivity** - a single port configured as an ISP port connected to multiple customer ports (up to a maximum of 4096).
- **Ethernet Private Line (EPL)** - support provisioning to provide EPL services point-to-point (P2P) interconnection between two Ethernet UNI over dedicated EoS trails.

Multiple types of services can be provisioned on one port, where each service is policed independently at the ingress. This imposes a strict limit on the input rate, separately for each service.

The customer can mark frames destined for different services based on port 802.1Q and 802.1p tag.

## Generic Faming Procedure

GFP, defined in ITU-T Rec. G.7041, is a protocol for mapping data packets into a synchronous transport system like SDH. GFP requires a fixed amount of overhead for encapsulation that is independent of the data packets. This allows deterministic matching of bandwidth between the Ethernet flow and the virtually concatenated SDH stream.

To cater for all mapping requirements, two mapping modes are defined for GFP:

- Frame mapped - used for connections where efficiency and flexibility are essential and reasonable latency can be tolerated
- Transparent mapped - enables the transport of block-coded client signals (like Fiber Channel, ESCON, or FICON) that require very low transmission latency

Neptune Layer 2 service cards support the GFP-F (frame-based) mode.

## Virtual Concatenation

VCAT, defined in ITU-T Rec. G.707, is a technique used to give SDH additional flexibility in transporting client signals requiring a bandwidth that does not match the bandwidth granularity of SDH networks.

The approach used by VCAT is to combine the bandwidth available on an arbitrary number of SDH containers (configured as a virtual concatenated group - VCG) in a way that creates a single logical channel capable of carrying a single byte-synchronous data stream.

With virtual concatenation, the individual containers are transported over the SDH network independently and then recombined to restore the original payload signal at the endpoint of the transmission path.

Differential delay due to the different path of each VC is compensated at the end of the path as part of regrouping the VCs of a VCG.

Virtual concatenation has the following benefits:

- **Scalability** - allows bandwidth to be selected in VC-4, VC-3, or VC-12 increments, as required, to match the required payload data rate.
- **Efficiency** - the resulting signals are easily routed through the SDH network, making more efficient use of available bandwidth on existing networks.
- **Compatibility** - virtual concatenation requires only the end nodes to be aware of the containers being virtually concatenated, making the signals transparent to the core NEs.

The fine bandwidth management made possible by VCAT is particularly effective for the efficient transport of data services that inherently comprise variable bitrates. For example, consider the transport of a partially filled GE signal. Although the nominal bandwidth is 1 Gbps, often the instantaneous rate is only 200 Mbps to 300 Mbps. Thus, continuous allocation to this GE signal of a bandwidth equal to the peak value (1 Gbps), as done in pure transport applications, wastes on average 70% of the network bandwidth. With VCAT, an optimal bandwidth close to the average bandwidth requirements is selected, for example, a bandwidth of 300 Mbps. To handle the peak bandwidth requirements, ingress buffers are used to shape the peak traffic to match the provisioned bandwidth.

## Link Capacity Assignment Scheme

LCAS, defined in ITU-T Rec. G.7042, enables dynamic changes in the amount of bandwidth used for a virtual concatenation channel. Signaling messages are exchanged within the SDH overhead to change the number of members included in the VCG. The number of members can either be reduced or increased, and the resulting bandwidth change is applied without loss of data.

Neptune Layer 2 cards support the dynamic bandwidth adjustment provided by LCAS functionality. Dynamic bandwidth adjustment allows the increasing or decreasing of the bandwidth of a VCG link. Typical scenarios where this capability is used include:

- Automatic removal of failed members temporarily from an active VCG and transferring traffic only via the remaining operational members. When the failure condition is fixed, the Layer 2 card set adds the members back into the group. This is also useful for traffic protection.
- Adjusting the link bandwidth to the bandwidth required by an application. If the bandwidth allocation is only for the average amount of traffic and not the full peak bandwidth, and the average bandwidth usage changes overtime, the allocation can be modified to reflect this change.

## Layer 2 Switching Capabilities

The Neptune Layer 2 cards incorporate a Layer 2 Provider Bridge Ethernet switch that supports VLANs and double tagging per IEEE 802.1Q and 802.1p. QoS is controlled by four CoS, together with strict priority queuing and full buffer allocation per QoS.

To provide prioritized/differentiated services, the client's traffic is policed and classified as follows:

- The rate of the flow at the ingress is limited according to a configured Committed Information Rate (CIR) and Committed Burst Size (CBS).

- Each packet is classified according to one of four CoS by marking it with a configured 802.1Q and a user priority (802.1p).

Client's flows are policed to conform to the specific Service Level Agreement (SLA). 128 policers are available on each module that can be allocated to each of the module ports.

The Weighed Random Early Discard (WRED) technique used to smooth traffic pattern under congestion conditions supports the policing procedure as follows:

- When traffic exceeds the module capabilities, it must discard packets. Any TCP client detecting discarded packets will reduce its transmission rate to half. After packets are no longer discarded, the rate will slowly be increased as long as there is no packet loss.
- If the module would discard packets only during congestion conditions, traffic volume would suffer from the sawtooth syndrome: after a series of packets are discarded, all the clients would drop their rate to half, resulting in partial utilization of the network. Together they will again increase the rate until the network is congested again.

WRED prevents this behavior by discarding a small part of the packets before its buffers are full. As a result, only a small number of TCP clients decrease their rate and traffic utilization does not drop.

Neptune Layer 2 cards support WRED, and its characteristics are separately configurable for each of the four priority classes of the internal Ethernet switch.

## FDB Quota Provisioning

Ethernet frames are forwarded according to their Destination MAC address and VLAN ID. The forwarding information is stored in a filtering data base (FDB) (routing table). The size of this database is limited; therefore, to free space for new addresses, the entries are automatically removed after a configurable aging time. If the address and VID of a packet don't match any entry in the table, the packet is flooded (sent to all output ports).

A MAC address storm from a VPN can occupy all free resources of the address table. In the absence of free resources, packets with new addresses are not learned. This causes the addresses to be flooded and overload the egress ports.

The FDB quota provisioning minimizes this effect by letting the operator to set a limited amount of entries (MAC addresses) per VPN (S-VLAN) and block any client port that exceeds the limit. Although in Neptune Layer 2 cards any client can exceed their quota, they, since FDB quota violation, reduce the aging time to minimum to free the FDB from the new entries and block the interfering client port to prevent it from continuing to overload the FDB.

## Triggers for MSTP

MSTP prevents the creation of loops and enables the protection of Ethernet traffic by the ring topologies used in SDH networks.

Link bandwidth reduction as a result of failures in VC members of a VCG can in turn cause service degradation performance. In such cases the MSTP is activated to change the network topology and overcome the failure. Neptune Layer 2 cards have a set of link capacity-related parameters that are used as triggers for MSTP:

- No members provisioned on the Tx direction
- No members provisioned on the Rx direction
- Partial Loss of Capacity (PLCr) on the receive side
- Partial Loss of Capacity (PLCt) on the transmit side
- Total Loss of Capacity (TLCr) on the receive side
- Total Loss of Capacity (TLCr) on the transmit side
- Link Fail Detection (LFD)
- Remote Defect Indication (RDI) on at least one member in the VCG (only for VCAT mode)

The threshold values of the TLCr and PLCr can be set by the user.

## Port-Based VLANs

Client frames can enter the provider's network tagged or untagged. A client that provides tagged frames attaches his CVLAN (Client VLAN ID) and priority bits to the Ethernet frames. The provider uses this information to identify the client and decide how to handle the traffic within his network.

In many cases the provider is not allowed to change the client tagging because the client needs it to continue the traffic handling at the far end. To enable traffic handling, the provider attaches his SVLAN (Service Provider VLAN) containing VLAN ID (VID) and CoS bits at the ingress port, and removes them at the egress.

### Attach/Detach VLAN

Neptune Layer 2 cards enable the provider to add a VLAN tag to incoming untagged frames. This VLAN is named PVID and is maintained throughout the network. The PVID enables the operator to identify different clients arriving from different ports, even after being multiplexed in point-to-multipoint (P2MP) configurations. The PVID is detached from the frames that are outgoing from the same port which was configured to attach and detach PVID.

## UNI on EoS Ports

The Neptune Layer 2 cards enable serving client traffic arriving through EoS ports as if they were received from ETY ports. This enables the provider to give the client "port extension" services. For example, a client that is far from the providers' Neptune Layer 2 card location uses a Neptune Layer 1 card to map his Ethernet traffic over SDH, and reaches the provider via the SDH network. This traffic is directed to a Layer 2 card EoS port. The traffic is demapped and enters the card. It is then handled as regular traffic that enters the card via a regular ETY port.

## NNI on ETY Ports

Neptune Layer 2 cards enable configuring the ETY port as NNI. Traffic in such ports use QinQ where the S-VLAN of the Neptune Layer 2 cards network is maintained and transmitted towards the client equipment.

## C-VLAN Functionalities

### C-VLAN Translation

This unique feature enables the merging of two different customer VLANs from different locations. Due to the VLAN translation at the edge of the provider network, two different VLANs that are in different places can be merged into one VLAN, or an external S-VLAN of another provider can be mapped to an internal S-VLAN.

Only one C-VLAN translation per UNI port per VSI is supported. C-VLAN translation is bidirectional.

### C-VLAN Bundling

VLAN bundling carries the traffic of multiple VLANs. Multiple customer C-VLANs can map through a single Ethernet service on the UNI. All-to-one bundling is a special case whereby all customer VLANs map to a single Ethernet service at the UNI.

### Ingress/Egress C-VLAN Filtering

Ingress/egress C-VLAN filtering is a means of filtering out unrequired traffic on a port. When VLAN filtering is enabled, packets are only accepted or transmitted into a port if they match the VLAN configuration of that port. Based on whether the port is on the ingress list of the VLAN associated with a frame, the port determines whether the frame can be processed.

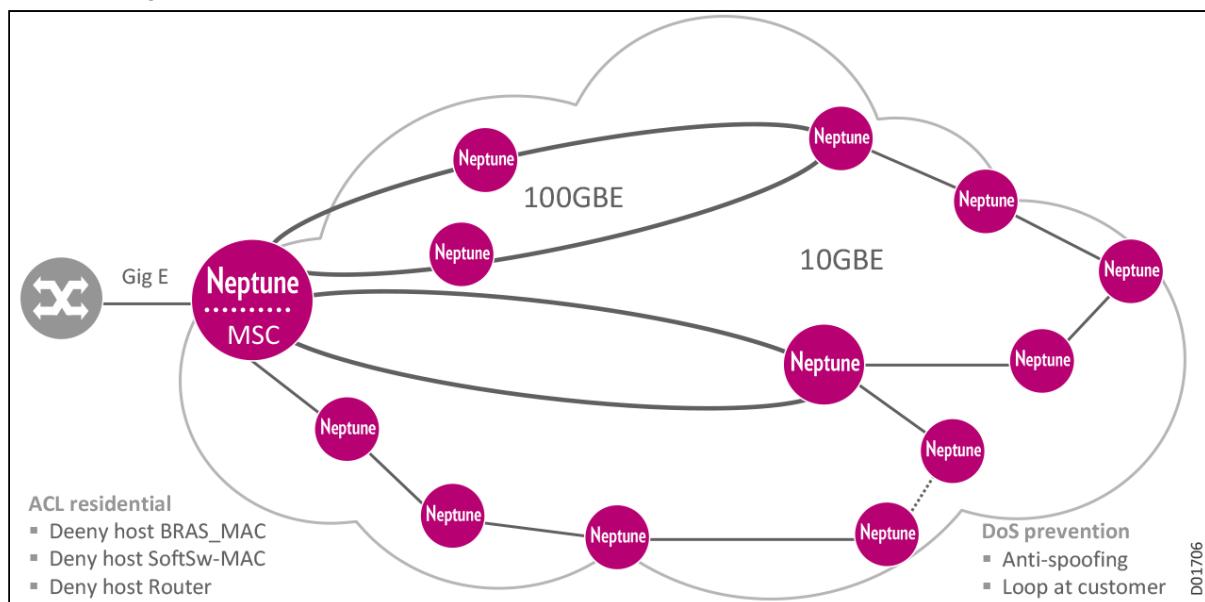
# Access-Controlled Management

Intelligent management access controls are needed at the customer edge to keep unauthorized users from accessing the provider's network. Preventing denial of service attacks involves deciding whether to accept, discard, or monitor certain traffic.

## Access Control List

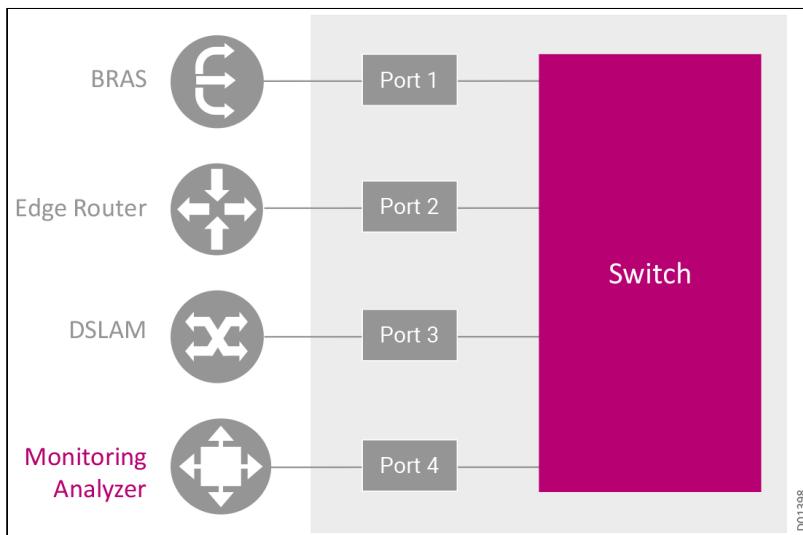
The **Access Control List (ACL)** is a list of permissions attached to an object. The list specifies who or what is allowed to access the object and what operations are allowed to be performed on the object. In a typical ACL, each entry in the list specifies a subject and an operation. One of the most important implementations is to protect routers from various risks, both accidental and malicious. Infrastructure protection ACLs should be deployed at network ingress points.

## ACL Description



## Port Mirroring

### Port Mirroring Description



## L2CP Flooding Protection

The Neptune product line provides protection against Layer 2 Control Protocol (L2CP) flooding sent by malicious users. Protection is implemented by limiting the number of L2CP frames which can be received from Neptune ports through the combined application of the following techniques:

- BPDU Blocking
- CFM
- IGMP Policing
- Link OAM
- Tunnel OAM

### L2CP Processing Overview

This section provides an overview of the L2CP processing.

- For a given L2 Control Protocol or OAM there are four possibilities for processing:
  - Pass to an EVC for tunneling
  - Peer at the UNI
  - Peer and pass to an EVC for tunneling
  - Discard at the UNI
- The requirements of L2CP processing on UNI port are defined in MEF20:
  - Pass to EVC
  - No pass to EVC (Filter)
- Filter means the L2CP or OAM frames could be either peered or discarded, depending on the service type

Neptune's platform functionality covers L2CP processing requirements in MEF CE3.0.

## Additional Features

Additional supported features include:

- **Autonegotiation** - supported by ETY ports to select common transmission parameters with the customer's equipment connected. The port capable of transmission at various rates (10/100 Mbps or 10/100/1000 Mbps) and mode (full duplex) exchanges data with the connected device. The two

devices then choose the best possible mode of operation that is shared by both, where higher speed is preferred over lower speed.

- **Store and Forwarding** - mechanism used to check the integrity of the frame at the ingress port. The frame's source and destination address and CRC are checked. Only error-free frames are forwarded, and frames with errors are dropped.
- **Layer 2 Control Protocol Handling** - Ethernet ports handle some specific MAC addresses in a special way to provide predicted efficient behavior of the network. As opposed to a standard service frame that is transported untouched from side to side, these special frames should be treated differently. For example, PAUSE frames have their meaning only within the local link and therefore should be discarded immediately upon reception. Other MAC addresses are configurable to be discarded or forwarded transparently.

# Ethernet VPN: EVPN

Ethernet VPN (EVPN) is an advanced solution for providing Ethernet services over IP/MPLS networks, both VPLS and VPWS.

As opposed to the current VPLS architectures, EVPN enables control-plane based MAC learning in the network. PEs participating in EVPN instances learn customer MAC routes in the control-plane, using MP-BGP advertisements. Control-plane MAC learning offers a number of benefits that allow EVPN to address known VPLS shortcomings, such as support for multi-homing with per-flow load balancing, and avoidance of unnecessary flooding over the MPLS network to multiple PEs participating in the P2MP/MP2MP L2VPN.

EVPN VPWS service is a BGP control plane solution for point-to-point (P2P) services. It implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. EVPN VPWS service is able to forward traffic from one network to another without MAC lookup; the MPLS label associated with the per-EVPN instance (EVI) Ethernet A-D route can be used to forward user traffic to the destination AC. Using EVPN for VPWS eliminates the need for signaling single-segment and multi-segment PWs for P2P Ethernet services.

This section introduces EVPN, including the following:

- [What is EVPN](#)
- [The EVPN VPLS Solution](#)
- [The EVPN VPWS Solution](#)
- [EVPN Operation Modes](#)
- [Example: EVPN Multi-Homing Mechanism for L2 Domain-Ring Connectivity](#)
- [EVPN Route Types](#)
- [EVPN Service Interface Types](#)
- [EVPN Anycast IRB Mechanism](#)

## What is EVPN

EVPN is the next-generation technology for providing MP2MP (VPLS) and P2P (VPWS) L2VPN Ethernet services on top of IP/MPLS provider cores. It is optimized for carrying unicast IP traffic for both IPv4 and IPv6. Current Neptune platforms support EVPN for MP2MP Ethernet services; P2P will be supported in a future release.

While operators have traditionally used VPLS technology to provide MP2MP L2VPN services, they have encountered some critical operational issues in doing so. EVPN technology resolves these issues by:

- **Facilitating an All-Active mode of operation for multi-homed CEs**

With EVPN, the traffic between a multi-homed CE and the provider core can be load-balanced across multiple physical PE-CE links and multiple paths through the IP/MPLS core. The previous technology (VPLS) is restricted to a Single-Active mode of operation in these scenarios.

- **Dramatically reducing the amount of customer traffic that has to be flooded across the provider core**

Flooding of unknown unicast traffic across the provider core can be completely suppressed. Even flooding of necessary ARP/DN packets is dramatically reduced using an ANP/ND Proxy.

- **Supporting fast failover** in the following cases:
  - One of the PEs to which a multi-homed customer site has been attached fails.
  - The Ethernet link that connects one of the PEs to a multi-homed customer site fails.

- **Providing effective mechanisms for handling MAC mobility**, and thereby resolving a major problem in the DC/DCI environment, where MAC addresses represent virtual machines and can move from one DC location to another one.

Neptune platforms support MPLS LSPs (EVPN-MPLS) as a tunneling mechanism for EVPN services. EVPN technology provides effective redundancy mechanisms for inter-subnet forwarding of unicast IP traffic, which

do not involve resource-consuming protocols like VRRP. As such, it can serve multiple applications, including mobile backhaul applications for one or more mobile operators. Having proven effective for intra-DC and inter-MEC connectivity, and with excellent synergy with the 5G Mobile Edge Computing (MEC), EVPN-MPLS is the natural choice for Layer 2 connectivity among the 5G mobile backhauling solutions.

## EVPN Terminology

To understand what an EVPN is and how it works, you must first understand the terminology:

- **EVI:** An EVPN instance (EVI) is a routing and forwarding VPN instance configured on all PEs participating in that instance. EVIs are assigned import/export Route Targets (RTs). EVIs serve the same role as a VRF, but for EVPNs. They are also known as MAC-VRFs.
- **ES:** An Ethernet Segment (ES) is a set of Ethernet links that connects a multi-homed device. If a multi-homed device or network is connected to two or more PEs through a set of Ethernet links, then that set of links is referred to as an *Ethernet segment*. The Ethernet segment route is also referred to as Route Type 4. This route is used for designated forwarder (DF) election for BUM traffic.
- **ESI:** Ethernet segments are assigned a unique non-zero identifier, called an Ethernet segment identifier (ESI). An ESI uniquely represents each Ethernet segment across the network. The same ESI value is configured on all links participating in the same Ethernet segment.
- **DF Election:** Used to prevent forwarding loops of broadcast, unknown-unicast, and multicast (BUM) traffic. Only a single router in an MH setup is allowed to de-capsulate BUM traffic from the EVPN network and forward it to the CE/CEs of a given Ethernet Segment.
- **Aliasing:** Used for load balancing traffic to all the connected routers for a given Ethernet segment, using the Route Type 1 EAD/EVI route. This is done irrespective of the router where the hosts are actually learned.
- **Mass Withdrawal:** This is used for fast convergence during access failure scenarios using the Route Type 1 EAD/ES route, by withdrawing a particular route.
- **Ethernet Tag:** An EVPN instance consists of one or more broadcast domains. An Ethernet tag identifies a specific broadcast domain, such as a VLAN. The **Ethernet Tag ID** is a 32-bit field identifying the specific broadcast domain.

## The EVPN VPLS Solution

Prior to the introduction of EVPN, MP2MP L2VPN services were provided using the VPLS technology as defined in RFC 4762 [STD-7].

With this technology:

- Each such service instance is locally represented by a VSI in each affected PE.
- VSI residing in different PEs are connected by Ethernet PWs.
- In the “flat” VPLS model, a full mesh of PWs connected each VSI with other VSIs.
- In the Hierarchical VPLS model, only partial mesh of PWs is required.
- A VSI can be connected to one or more CE via appropriate ACs.
- Each VSI performs native L2 switching and MAC learning between its ACs and PWs.

As deployment of MP2MP L2VPN services that used VPLS technology have grown in scale, operators have encountered several major operational issues:

- Only S-A Multihoming (MH) of customer sites to Provider Edge (PE) devices can be supported. As a consequence, additional bandwidth between the customer site and multiple PEs to which it is attached cannot be utilized.
- Changes in the service topology may result in flooding of unknown unicast traffic with prolonged impact on the overall service availability.
- Mobility of the customer end stations may result in prolonged loss of connectivity. This problem is especially relevant in the DC environments where the customer end stations representing virtual machines can move between different geographical locations.

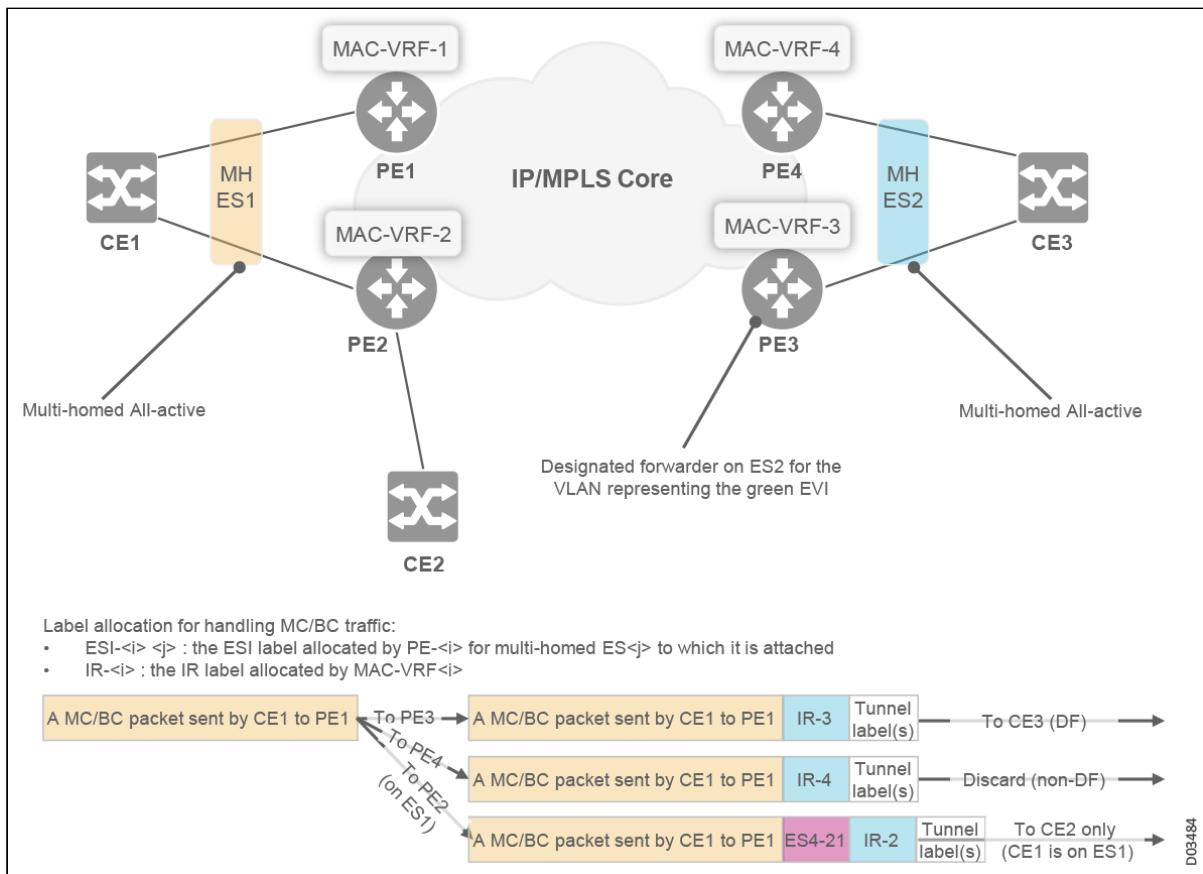
EVPN technology addresses these issues by optimizing the L2VPN services it provides for carrying unicast IPv4 or IPv6 customer traffic and eliminating native MAC learning from Source MAC addresses of Ethernet frames received from remote PEs.

The EVPN solution:

- **Relies on various control protocols** employed by IP hosts within the customer sites to learn {MAC, IP} pairs that can be reached via a specific AC. Examples of these protocols include: ARP for IPv4 and NDP for IPv6, DHCP. Other implementations rely both on the "native" local DP learning and on control protocols, and future implementations will use both.
- **Disables native MAC learning** from Source MAC addresses of Ethernet frames received from remote PEs (native MAC learning from Source MAC addresses of Ethernet frames received from local ACs is still enabled). Instead, reachability of MAC and IP addresses (learned from the CP protocols listed above) is advertised in MP-BGP using a dedicated AFI/SAFI – L2VPN/EVPN. Acceptance of this information by the remote PEs is controlled by Route Targets similar to how distribution of the VPN routing information is controlled in IP VPN (see [RFC 4364](#)).
- **Reduces flooding of BUM traffic** in the core network providing the underlay for the EVPN services by using the following mechanisms:
  - **Proxy ARP**: When remote PEs learn about reachability of a certain {MAC, IP} pair, they can install this pair in their local ARP (for IPv4) or ND (for IPv6) cache, so that they could locally respond to ARP or Neighbor Solicitation requests for the corresponding IP address with the corresponding MAC address.
  - **Suppression of unknown unicast flooding**: Source MAC addresses of packets received from the remote PEs is not natively learned, therefore flooding them across the core is not needed.
  - **EVPN-IRB with Anycast IP and MAC addresses**: If an EVI connects multiple hosts to two or more "first mile" routers acting as the default Next Hop for these hosts, protection of upstream traffic generated by these hosts can be provided by configuring the interfaces of these routers connected to the EVI with the same IP and MAC addresses. This eliminates the need for VRRP and therefore, flooding of VRRP Advertisement messages (non-routable IP multicast).
  - **Supports A-A Multi-homing**: If a certain customer MAC address can be reached via multiple ACs (in different PEs), and if the CE at the other end of these ACs is capable of simultaneously receiving traffic from any of them, then the following can be achieved:
    - **FIB Stability**: If the same MAC address has been locally learned and advertised by multiple PEs where the EVPN-based L2VPN service is represented, all remote PEs will accept one of these advertisements using the BGP route selection process.
    - **Load Balancing**: Remote PE can send the traffic with this Destination MAC address to each of the PEs for which this MAC address is locally reachable without causing any problems.
    - **Fast Failover**: When one of the ACs mentioned above fails, the PE to which it belongs only have to announce this failure once in order to trigger forwarding the customer traffic with all DMAC addresses that have been reachable via this AC to the other PEs, i.e., the failover time will not depend on the number of MAC addresses affected by the failure.
- **Solves the MAC Mobility problem**: When the previously learned customer MAC address moves to another location so that it is now reachable via another AC attached to another PE, it is possible to advertise its new reachability information with an explicit indication of being new, so that all affected PEs immediately update their FIBs and start forwarding to the new PE.
- **Can use different Provider tunneling mechanisms** for delivery of multi-destination traffic to remote PEs. In cases where the amount of this traffic is negligible (due to flooding suppression measures), ingress replication (IR) can be used as such tunneling. IR uses a single downstream-allocated label per BT in each MAC-VRF to identify the scope of flooding of received multi-destination frames:
  - It is allocated by per BT per egress MAC-VRF.
  - It is used as the EVPN application label in the EVPN encapsulation of multi-destination frames sent to this BT in this MAC-VRF by all ingress PEs.
  - Supports interconnect of multiple EVI (each representing a single IP subnet with multiple IP hosts in it) via a single BGP/MPLS IP VPN instance.
  - It is implemented by an abstraction called EVPN-IRB that is instantiated by multiple IRB LIFs in each PE where both one of the EVIs and the IP-VPN service are represented. Each such IRB LIF:
    - Is contained in IP-VRF locally representing interconnecting IP-VPN service instance
    - Uses MAC-VRF locally representing some EVI as its BD

- All IRB LIFs that use MAC-VRFs of the same EVI can be assigned with the same anycast IP and MAC addresses. Such an arrangement is possible only with EVPN-based services (anycast MAC addresses cannot work with VPLS).
- **Provides the same level of protection for upstream traffic** generated by the hosts attached to the EVI as would be provided by VRRP, however, without deployment of multiple resource-consuming VRRP instances.
- **Eliminates Ethernet loops** by combining the following mechanisms:
  - **Strict Split Horizon**: An EVPN-encapsulated Ethernet frame (received from a remote PE that has imposed EVPN encapsulation on it) is never forwarded to another remote PE. This eliminates Ethernet loops across the provider core network.
  - **DF Filtering**: All PEs connected to the same Multi-Homed Ethernet Segment (MH ES) learn about each other and elect one of them as the DF. The default FD election scheme elects a DF per MH ES per EVI. Only the elected DF is responsible for sending multi-destination traffic received from the remote PEs to the ES. Non-DF PEs discard such traffic, thus preventing the situation when the same multi-destination frame is sent into the same customer L2 domain more than once.
  - **ESI Label Filtering**: Each PE that is attached to a certain MH ES, allocates an ESI label for this ES. With ingress replication, each ingress PE that is assigned to a certain MH ES includes the ESI label allocated by the egress PE attached to the same MH ES in the EVPN encapsulation of multi-destination Ethernet frames it sends to this PE. Handling of this label in the DP prevents forwarding the packet with this label exposed to the MH ES for which it has been allocated. As a consequence, a multi-destination frame received from a MH ES will never be forwarded back to the same ES.

### EVPN Encapsulation



## The EVPN VPWS Solution

EVPN VPWS service is a BGP control plane solution for point-to-point (P2P) services. It implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. EVPN VPWS service is able to forward traffic from one network to another without MAC lookup; the MPLS label associated with the per-EVPN instance (EVI) Ethernet A-D route can be used to forward user traffic to the destination AC. Using EVPN for VPWS eliminates the need for signaling single-segment and multi-segment PWs for P2P Ethernet services.

EVPN VPWS is implemented according to RFC 8214, supporting the following:

- Load balancing: Single home and multi-home all active and port-active load balancing modes with VPWS.
- VLAN-based service interfaces, including:
  - A VPWS instance identifier corresponds only to a *single* VLAN on a specific interface.
  - VID translation on the disposition PE (the egress PE)
- VLAN-Bundle service interfaces, including:
  - A VPWS service instance identifier corresponds to *multiple* VLANs on a specific interface ("EVPL" alternative)
  - VLAN translation *not* allowed
  - VLAN-Aware bundles work the same as VLAN-Bundles in VPWS, according to standard
- Must support "local" and "remote" service identifiers on the PE routers for identifying the endpoints of the EVPN-VPWS service.
  - Local ID: The *local* identifier of the AC, sent *to* the remote PE in the per-EVI Ethernet A-D route advertisement
  - Remote ID: The *remote* PE identifier of the AC, expected to be received *from* the remote PE in the per-EVI Ethernet A-D route advertisement.

This means that the PE devices on each side of the network advertise their service identifiers, and receive the identifiers from their remote neighbors. One's local ID must match one's remote ID, and vice versa.

- The same VPWS service identifier (local and remote) may be configured on both PEs.
- In multi-home CE topologies, all PEs attached to the same ES must have the same VPWS service identifier values.
- The endpoints must be auto-discovered using BGP-based EVPN signaling, to exchange the service identifier labels.
  - Per-EVI Ethernet A-D route is used to signal VPWS services
  - The ESI field is set to the customer ES.
  - The 32-bit Ethernet Tag ID field must be set to the VPWS service instance identifier value.
  - The pair of PEs instantiating the VPWS service instance will advertise a per-EVI Ethernet A-D route with its service VPWS service instance identifier and will each be configured with the other PE's VPWS service instance identifier
- An EVPN instance (EVI) must not be configured with both VPWS service instances and standard EVPN multipoint services. Multiple EVPN-VPWS services can be set in the same EVI.
- Must support the *EVPN Layer 2 Attributes Extended Community*, to be included with the per-EVI Ethernet A-D routes.
- Failures handling:
  - Single-homed: Withdrawal of per-EVI Ethernet A-D route in an event of a link/port failure of a given single-home Ethernet segment.
  - Multi-Homed: Mass withdrawal technique. In multi-home configurations, the withdrawal is done on the per-ES Ethernet A-D route. In multi-homed CE topology, the Ethernet A-D per-EVI route must not be used for traffic forwarding by a remote PE until it also receives the associated set of Ethernet A-D per-ES routes (RFC 7432).
- Flow Aware Transport (FAT) Labels (RFC 6391) in EVPN VPWS service ("both-static" mode only)
- Connecting an EVPN VPWS to a PHT, so PHT state is affected by VPWS states change. Supports PHT with EVPN-VPWS in single homing, port-active multi-homing, and active-active multi-homing.

- Yang Data Model for EVPN (RFC 8466)

EVPN-VPWS uses the following Route Types:

- Route Type 1 - "Ethernet Auto-Discovery (AD) Route": *Per-EVI* Ethernet A-D route to signal VPWS service identifier and MPLS Label, and *Per-ESI* Ethernet A-D route to signal the multi-homing ES, if there is one.
- Route Type 4 - "Ethernet Segment Route": Allows PEs with same ESI to discover each other; used for Designated Forwarder (DF) Election.

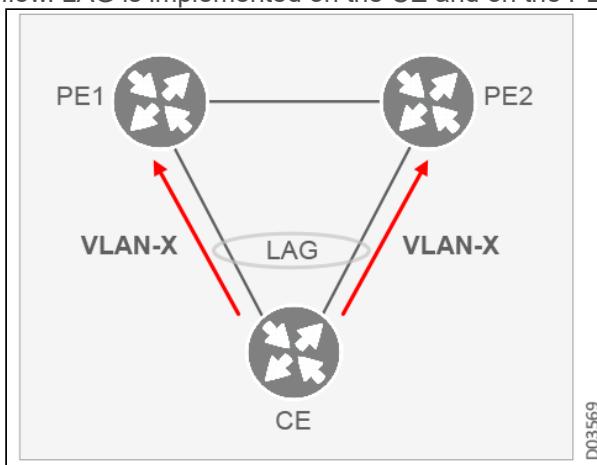
For a single-homed CE, in an advertised per-EVI Ethernet A-D route, the ESI field is set to zero and the Ethernet Tag ID is set to the VPWS service instance identifier that identifies the EVPL or EPL service.

For a multihomed CE, in an advertised per-EVI Ethernet A-D route, the ESI field is set to the CE's ESI and the Ethernet Tag ID is set to the VPWS service instance identifier, which has the same value on all PEs attached to that ES. This allows an ingress PE in a multihoming All-Active scenario to perform flow-based load-balancing of traffic flows to all of the PEs attached to that ES. In all cases, traffic follows the transport paths, which may be asymmetric.

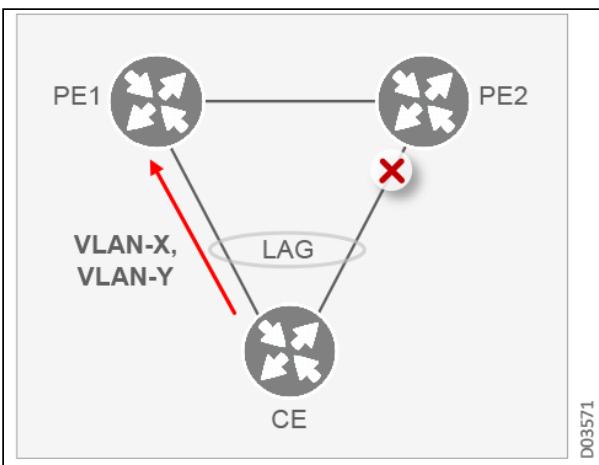
## EVPN Operation Modes

EVPNs work with one of the following operation modes:

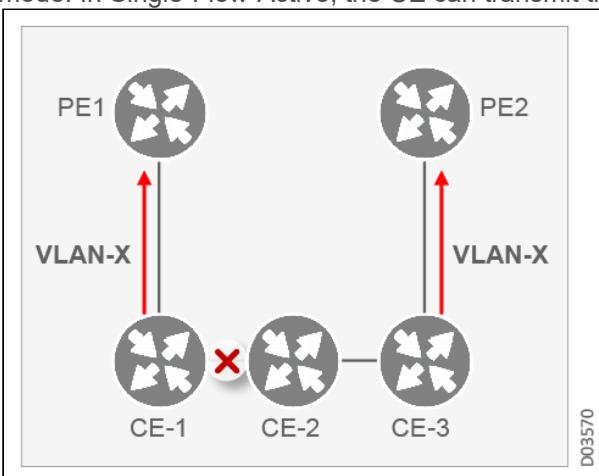
- **Single-Homing:** A customer edge (CE) device is connected to a single provider edge (PE) device. Single-Homing is the simplest mode of operation. It does not involve any Ethernet segments, so there is no ESI configuration.
- **Multi-Homing:** When a CE device is connected to more than one PE device. The CE device and its connection to each PE is an *Ethernet Segment*. Each Ethernet Segment is identified by an Ethernet segment identifier. Multi-homing ensures redundant connectivity. There are various types of multi-homing modes:
- **Active-Active (All-Active) (A-A):** When all PE routers attached to an Ethernet segment are allowed to forward traffic to and from the Ethernet segment, then the Ethernet segment is defined as operating in Active-Active (All-Active) redundancy mode. In All-Active mode, the CE performs load-balancing per flow. LAG is implemented on the CE and on the PEs.



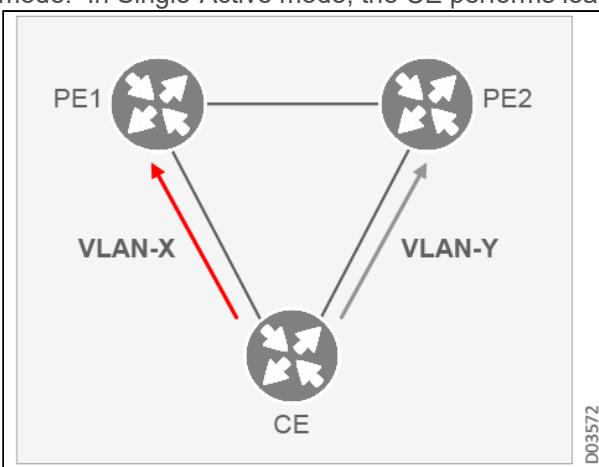
- **Port-Active (P-A):** When only a single PE is allowed to forward traffic to/from that Ethernet segment for all members of that Ethernet Segment, then the Ethernet segment is defined as operating in Port-Active redundancy mode. In Port-Active mode, the CE performs load balancing per-port. (The port on the standby PE is blocked.) LAG is implemented on the CE and on the PEs. Non-primary PEs signal "distribution off" via LACP.



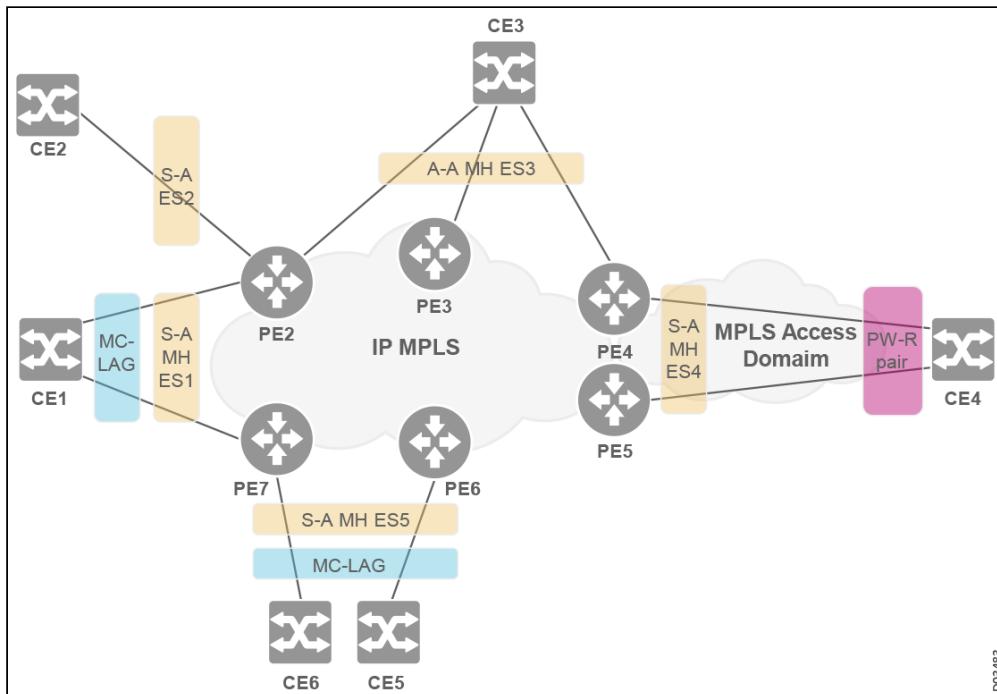
- **Single-Flow-Active (SFA):** When all PEs routers attached to an Ethernet segment are allowed to forward traffic to/from that Ethernet segment, while relying on the CE network connected to the PEs to prevent loops, then the Ethernet segment is defined as operating in Single-Flow-Active redundancy mode. In Single-Flow-Active, the CE can transmit traffic in both directions.



- **Single-Active (S-A):** When only a single PE is allowed to forward traffic to/from that Ethernet segment for a given VLAN, then the Ethernet segment is defined as operating in Single-Active redundancy mode. In Single-Active mode, the CE performs load balancing per-VLAN.



### Active-Active (A-A) and Single-Active (S-A) Operation Modes

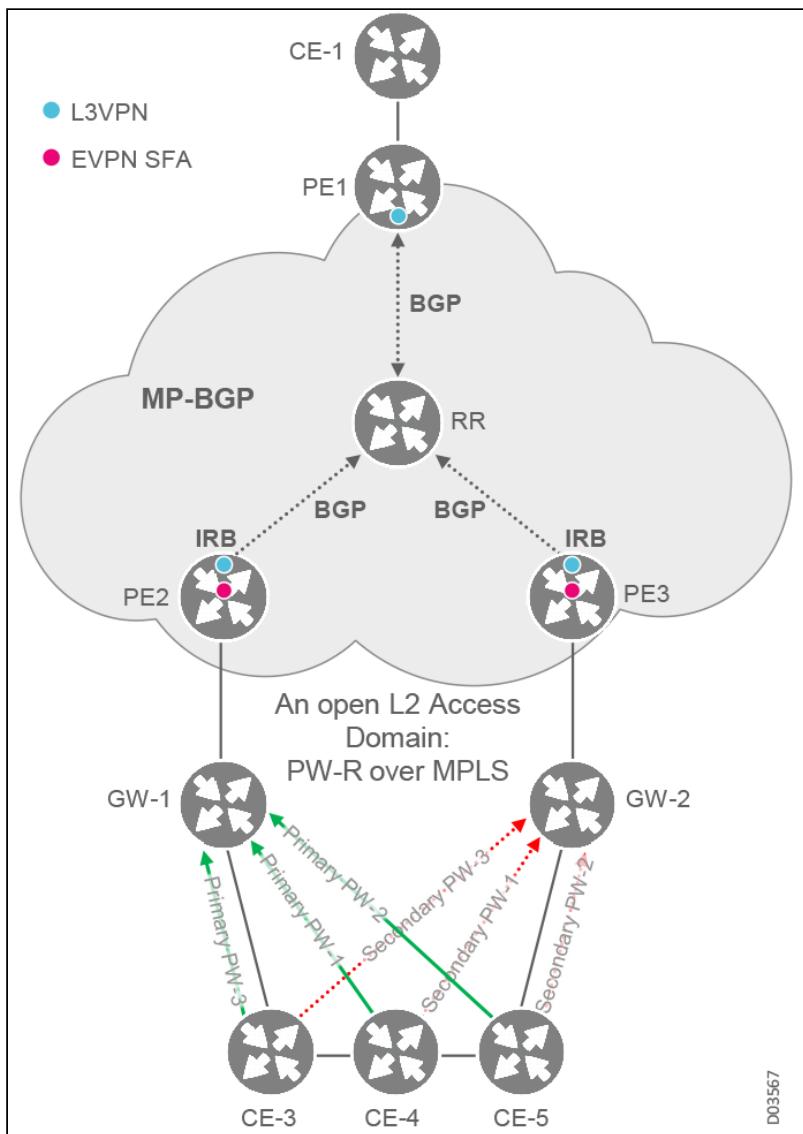


## Example: EVPN Multi-Homing Mechanism for L2 Domain-Ring Connectivity

The following figure illustrates a multi-homing configuration in single-flow active mode. This configuration provides an efficient EVPN-based solution for DH connectivity of the L2 domain access network, offering the following advantages:

- Minimal flooding over the IP/MPLS network, since there is control plane BGP-based MAC/IP learning, with ARP/ND proxy and suppression capabilities
- The EVPN PEs detect local MAC move events, which are then rapidly reflected in the EVPN/L3VPN network through EVPN advertisements
- The EVPN network “aligns” with the L2 gateway protocols' loop prevention mechanisms; working PEs are not selected independently, but according to the traffic flows arriving on the local ACs
- More resilient, scalable, and easier to maintain
- Typically implemented with IRBs on the PE GWs, providing inter-subnet routing
- Interoperable with MPLS-TP and IP/MPLS-based L2 access domain networks

### A Multi-Homing Configuration in Single-Flow Active Mode



This network configuration enables efficient service convergence, with full resilience from both sides:

- Implementing Object Tracking on the EVPN PEs enables detection and handling of “core isolation” of a primary PE in the IP/MPLS network. The system may track prefixes or interfaces in global or non-global VRFs. Once a prefix is unreachable, or the interface is down, the appropriate reaction is implemented based on the relevant policy.
- Failures in the L2 access network are recognized by the Secondary PE once traffic reaches the local AC, and the EVPN network transitions accordingly.

For example, a common action is an AC/interface shutdown. This causes the L2 access domain to converge accordingly, after which the EVPN network converges as well. In cases of MPLS-TP in the L2 access domain network, both gateways of the TP network enable a flag to signal a PW switchover after recognizing that the AC is down.

## EVPN Route Types

The following table lists the types of routes that can be configured with EVPN. Neptune platforms support route types 1, 2, 3, and 4.

### EVPN Route Types

Route Type	Scope	Name	Description
1	ESI	Ethernet Auto-Discovery (AD) Route per ES	Used for advertising split-horizon label (“ESI-label”) and to enable fast convergence (mass withdrawal)
1	EVI/BD	Ethernet Auto-Discovery (AD) Route per EVI	Used for advertising the EVPN aliasing label (distinct label for each EVI or BD)
2	EVI/BD	MAC/IP Advertisement Route	Used for advertising a service label for reachability of a MAC address and MAC/IP pair binding
3	BD	Inclusive Multicast Ethernet Tag Route	Advertises the “BUM Label” – used by remote PEs when transmitting BUM traffic
4	ESI	Ethernet Segment Route	Allows PEs with same ESI value to discover each other, used for Designated Forwarder (DF) Election
5	EVI/BD	IP Prefix Route	Used for advertising L3 prefix information
6	BD	Selective Multicast Ethernet Tag Route	Used for advertising IGMP/MLD Membership messages (IGMP Proxy) Reduces IGMP/MLD Group Membership flooding Prevents sending MCAST traffic to EVPN PEs with no MCAST receivers
7	ESI	Multicast Join Sync Route	Used for synchronizing IGMP/MLD Group Membership states between PEs connected to common ESI
8	ESI	Multicast Leave Sync Route	Used for synchronizing IGMP/MLD Group Membership states between PEs connected to common ESI

### EVPN Service Interface Types

The following table lists the types of interfaces that can be configured with EVPN.

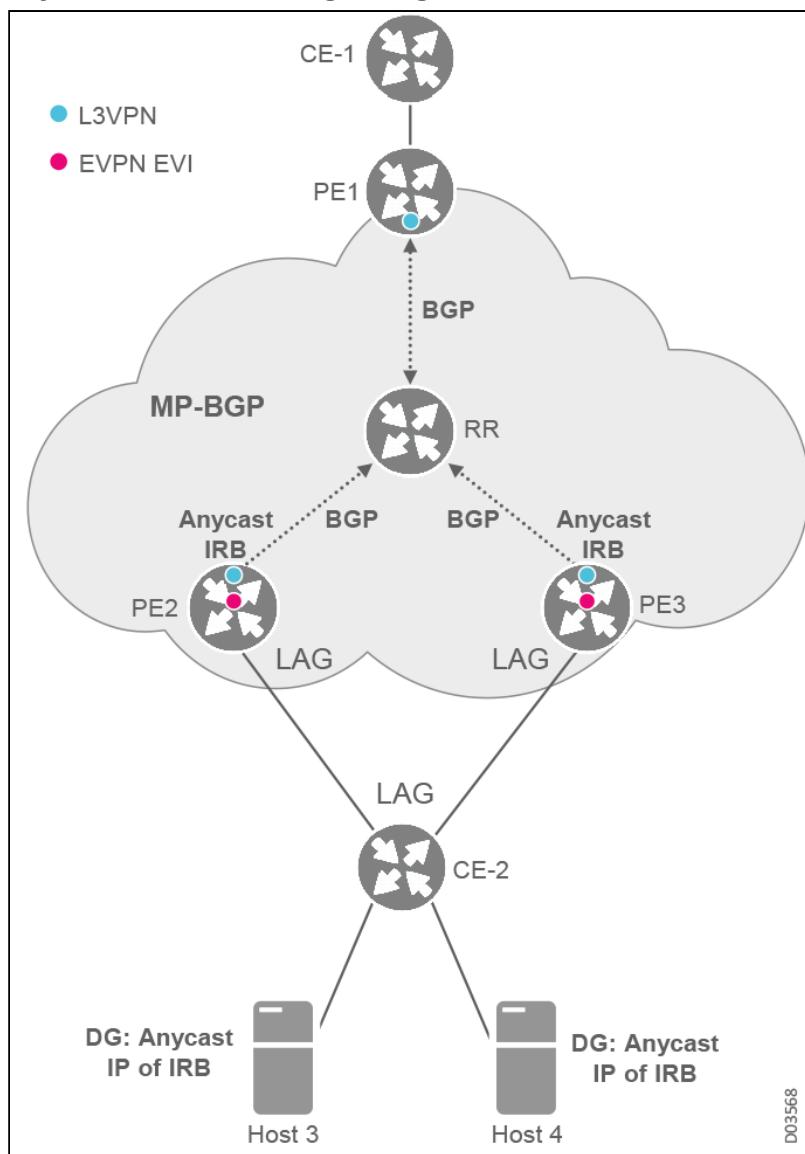
**EVPN Interface Types**

	VLAN-Based Service	VLAN Bundle Service	VLAN-Aware Bundle Service	Port-Based Service	Port-Based VLAN-Aware Service
Broadcast Domains (VLANs)	Single	Multiple	Multiple	Multiple	Multiple
Bridge Table (MAC Table)	Single	Single	One per VLAN	Single	One per VLAN
MAC Addresses	Can overlap between VLANs	Unique for all VLANs	Can overlap between VLANs	Unique for all VLANs	Can overlap between VLANs
VLAN to MAC-VRF (EVI) Mapping	one-to-one	many-to-one	many-to-one	many-to-one	many-to-one
Ethernet TAG ID	0 Single bridge table per EVI.	0 Single bridge table per EVI.	VID or normalized TAG ID (Normalized VID)	0 Single bridge table per EVI.	VID
VID Translation	Egress Translation at the PE. Only one bridge table that corresponds to one VLAN.	Not Supported according to standard. IRB not supported as well.	Supported Because there's a bridge table per VLAN, and because CE-VID may be different, translation may be required for end-to-end communication.	Not Supported	Not Supported
Corresponding Service Type in L2VPN T-LDP based VSI	Bridge Domain – one VLAN per bridge domain VSI.	VPLS with multiple VLANs allowed, in a single VSI, with a single MAC table	Doesn't exist. It's like having multiple bridge domains under a single VSI.	EPL/All-to-one-bundling of the interface in a single VSI.	Doesn't exist. It's like having a different MAC table for each VLAN under the same VSI.

## EVPN Anycast IRB Mechanism

The following figure illustrates an anycast IRB multi-homing configuration in active-active mode. This configuration provides an efficient EVPN-based solution for MH connectivity. With the IRB interfaces included inside the EVPN service, the multi-homing devices function as gateways that handle inter-subnet routing. In the following figure, you can see that CE2 balances between each PE the traffic load coming from hosts over its LAG. The PEs route the incoming traffic over the L3VPN in which the IRBs participate. IRBs are configured with the same IP address and virtual MAC address; there is no need for VRRP.

**Anycast IRB Multi-Homing Configuration in Active-Active Mode**



D03568

# Layer 3 VPN

A Virtual Private Network (VPN) extends a private network across a public network, such as the internet. It enables a computer or network-enabled device to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security, and management policies of the private network.

A VPN connection across the internet is similar to a wide area network (WAN) link between websites. From a user perspective, the extended network resources are accessed in the same way as resources available within the private network.

One major limitation of traditional VPNs is that they do not tend to support or connect broadcast domains. Therefore communication, software, and networking, which are based on Layer2 and broadcast packets, (such as NetBIOS used in Windows networking), may not be fully supported or work exactly as they would on a real LAN. Variants on VPN, such as Virtual Private LAN Service (VPLS), and Layer 2 tunneling protocols, are designed to overcome this limitation.

Layer 3 VPN utilizes Layer 3 VRF (VPN/virtual routing and forwarding) to segment routing tables for each 'customer' utilizing the service. The customer peers with the service provider router and the two exchange routes, which are placed into a routing table specific to that customer.

Multiprotocol BGP (MP-BGP) is required in the cloud to utilize the service, which increases complexity of design and implementation. L3 VPNs are typically not deployed on utility networks due to their complexity; however, L3 VPNs could be used to route traffic between corporate or data center locations.

Implementation of the Layer 3 VPN requires appropriate settings of import and export policies. The VRF BGP filters incoming routes according the supported VPN address family (IPv4-unicast). It drops all incoming routes that do not belong to this address family.

Default configuration of the VRF export policy allows VRF to redistribute all VRF routes into the global routing instance (called also VRF-0 or default routing instance). Global BGP allows export of all VPN-IPv4 address family routes to all internal BGP peers.

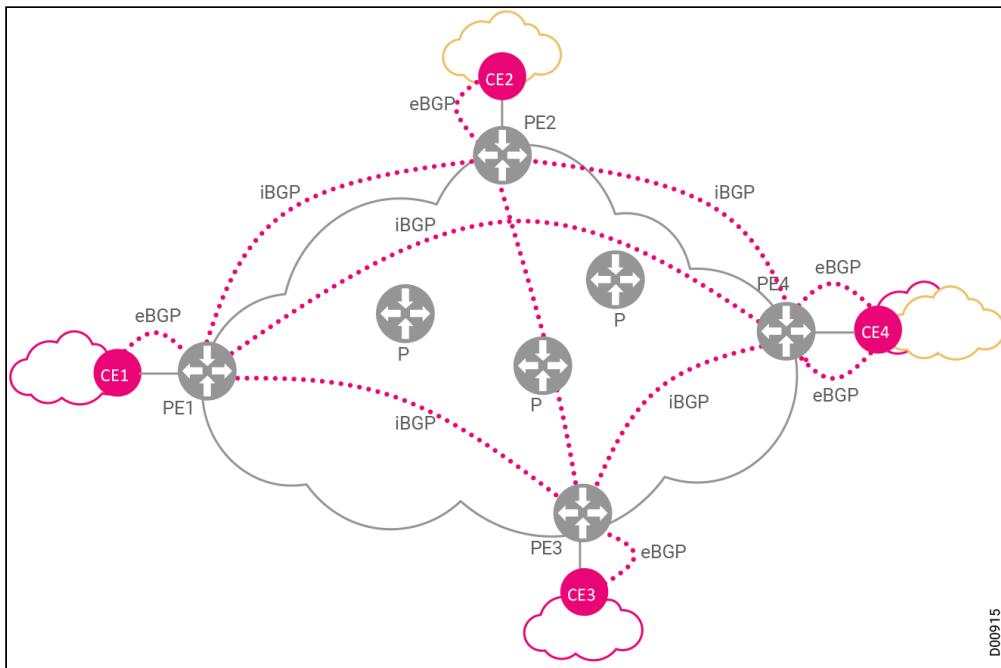
This section includes the following topics:

- Example: L3VPN Application
- L3VPN Policies
- 6VPE: L3VPN for IPv6
- HoVPN Architecture
- HoVPN Deployment Scenario

## Example: L3VPN Application

Neptune platforms implement BGP/MPLS IP VPN according to RFC4364, supporting customer VPNs by dedicating for each VPN its own VRF table. Neptune supports exchanges of route information either through static configuration or using eBGP.

### L3VPN Network Configuration Example



One VPN is in sites 2 and 4. The other VPN is in sites 1, 3, and 4. Provider Edge router 4 (PE4) has two VRFs. It establishes one eBGP within each VRF. PE4 learns routing and reachability information for the two VPNs from site 4. Using the *VPN-IPv4 address family*, it advertises the routes to all its iBGP peers.

According to the labels and the Route Target associated with the route, PE2 eBGP selects only the routes that were learned from the orange VPN, to be informed to CE2. In a similar way, eBGP of PE3 and PE4 select only the routes that were learned from the blue VPN, to be informed to CE3 and CE4.

eBGP PE1, PE2, and PE3 perform the same activities for the routing and reachability information learned from CE1, CE2, and CE3. The traffic that should traverse the service provider's network does it via LDP LSPs.

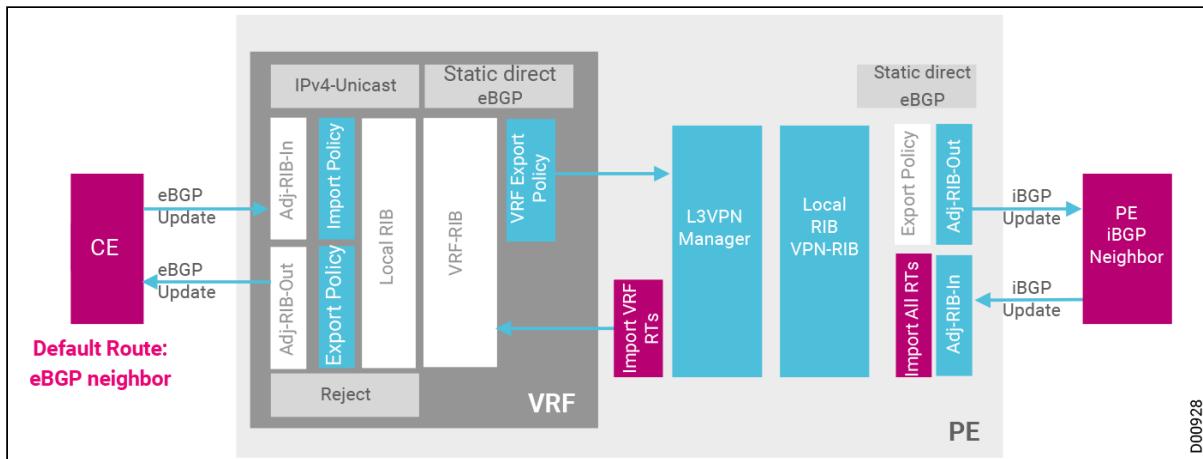
## L3VPN Policies

### L3VPN Import and Export Policies

L3VPN implementation requires appropriate configuration of import and export policies.

- **VRF BGP import policy:** The VRF BGP filters incoming routes according to the supported VPN address family (IPv4-unicast). It drops all incoming routes that do not belong to this address family.
- **VRF export policy:** Default configuration of the VRF export policy allows VRF to redistribute all VRF routes into the global routing instance (called VRF-0 or default routing instance).
- **Global BGP export policy:** Global BGP allows export of all VPN-IPv4 address family routes to all internal BGP peers.

### L3VPN Import/Export Policies



The global routing instance filters incoming VPN-IPv4 address family routes according all import RTs that are configured on the PE. Further, the routes are redistributed to each VRF according its import RTs.

- **VRF BGP export policy:** When the CE (VRF BGP peer) configures a default route toward its PE neighbor, default BGP export policy blocks redistribution of its routes towards the CE.

### L3VPN with ECMP

Equal Cost Multiple Paths (ECMP) over multiple links in a non-global VRF is supported, providing protection and load balancing, as well as increasing bandwidth of flows from PE to CE or CE-site. In a typical scenario, operators would configure native IP ECMP for IPv4 or IPv6 address families in VRFn use cases as follows:

- ECMP between any combination of two equal-cost routes with local next hops (from Static Route, BGP or OSPF)
- No ECMP between one local and one remote next hop
- No ECMP between two remote next hops
- BGP PIC and ECMP are both enabled

## 6VPE: L3VPN for IPv6

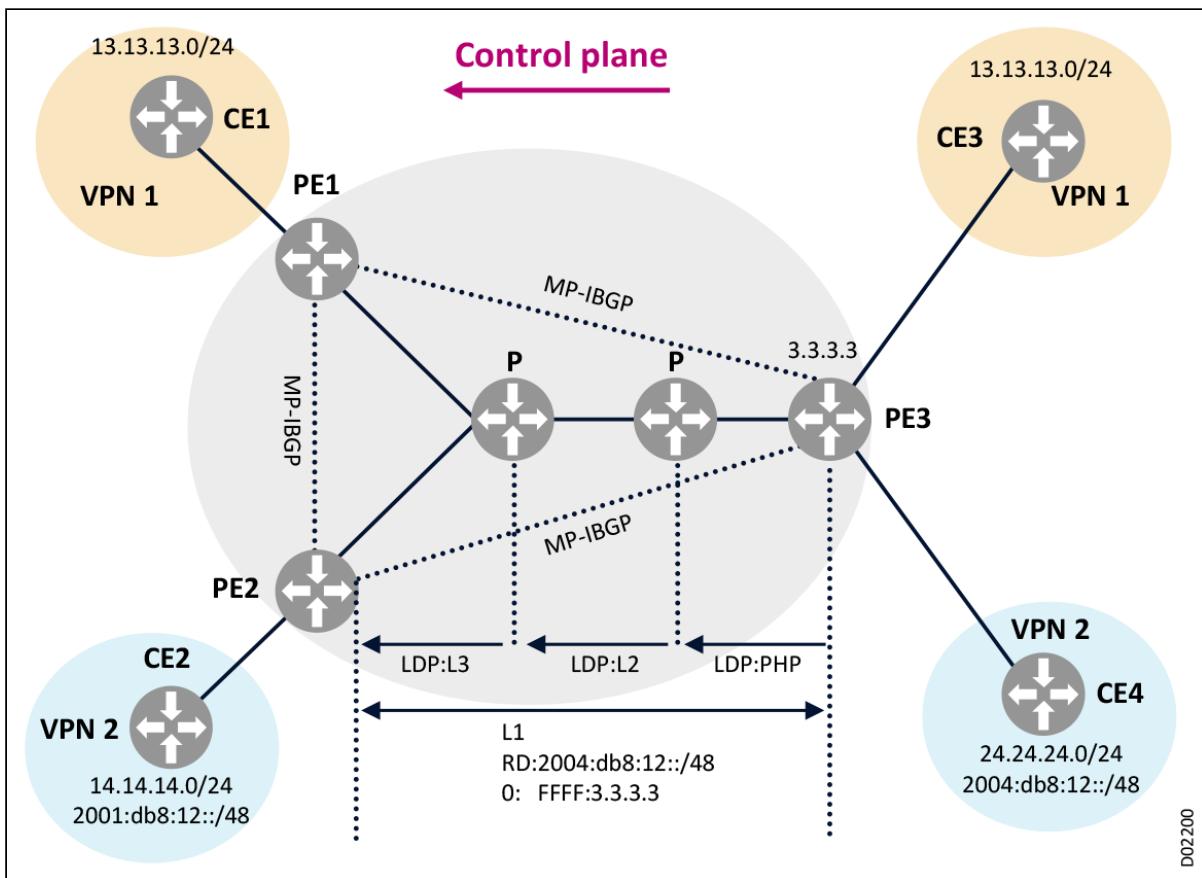
6VPE is the name for IPv6 L3VPN as defined in RFC 4659. 6VPE is the equivalent of IPv4 BGP/MPLS L3VPN, redefined and standardized for IPv6. 6VPE allows networks to carry IPv6 customer traffic without affecting the MPLS backbone, which can remain IPv4. 6VPE can work smoothly with VPnv4, with zero impact on P/PE routers that don't have VPnv6 sites.

Each IPv6 VPN has its own address space. This is accomplished by the addition of a new **VPnv6 address-family**, which prepends a Route Distinguisher (RD) to the IPv6 address. A VPnv6 address is a 24-byte quantity that begins with a 8-byte RD, followed by a 16-byte **IPv6 address**. When a site supports both IPv4 and IPv6, the same RD can be used for advertising both IPv4 and IPv6 addresses. **MP-BGP** is used to advertise IPv6 VPN routes. IPv6 VPN traffic is transported using IPv4 tunneling. The next-hop network address is the IPv4-mapped IPv6 address of the advertising PE.

IPv6 L3VPN is typically configured per PE. Network operators generally complete the following process:

- Create a VRF and associate it with the IPv6 interface connecting to the site.
- Configure a Route Distinguisher for the VRF, and configure a set of import and export Route Targets.
- Configure PE-CE protocols.
- Configure iBGP sessions to the PE routers in the AS.
- Enable the VPN-IPV6 address family on those iBGP sessions.

### IPv6 L3VPN Solution



If the IPv6 L3VPN solution is implemented at the data plane level, then the IPv6 user traffic is encapsulated with an MPLS header, similar to IPv4 user packets. For hybrid VPNs, the same application label (L1) may be allocated for both IPv4 and IPv6 routes related to the same VRF. Both flows usually use the same LSP path.

## HoVPN Architecture

Hierarchy of Virtual Private Networks (HoVPN) is a multi-layer VPN architecture that deploys PE functions on multiple PE devices. In this architecture, the functions of a single PE are distributed among multiple PEs. Playing different roles, these PEs form a hierarchical architecture, handling the functions of a centralized PE. For this reason, the solution is also called a Hierarchy of PE (HoPE).

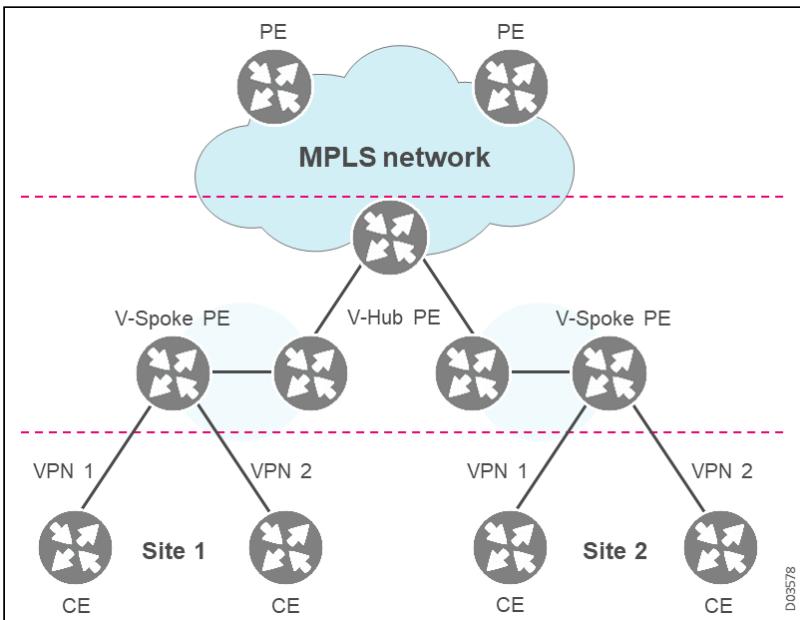
HoVPN technology solves a known scalability problem of VPNs. The main problem is that the any-to-any connectivity among all customer-sites of the VPN requires each PE router that serves such sites to hold all the routes of the VPN and to maintain tunnels to all other PEs.

With HoVPN, the Service Provider (SP) can reduce the number of routers that actually have to hold all the VPN route and tunnel data. The other PE routers can hold a smaller number of routes, and simply forward some of the ingress traffic to one of the PEs that hold more detailed routes.

HoVPN is based on the Virtual Hub and Spoke technology defined in [RFC 7024](#). It divides PEs into the following categories.

- **Regular IP VPN PE:** This PE advertises routes it has learned from the locally attached customer site, and learns "routes of interest" from other PEs.
- **Virtual-Hub PE (V-Hub):** This PE may or may not be attached to any customer site. The IP-VRF of a V-Hub holds all specific VPN routes and advertises the default route towards V-Spokes.
- **Virtual-Spoke PE (V-Spoke):** This PE advertises routes it has learned from the locally attached customer site but only learns the default routes advertised by V-Hubs.

### HoVPN Architecture Including both HoVPN PEs and Common PEs



Either MP-IBGP or MP-EBGP can run between the V-Hubs and the V-Spokes connected to it. When MP-IBGP runs between V-Hubs and V-Spokes, the V-Hub acts as the RR for multiple V-Spokes, to reflect routes between the V-Spokes.

## HoVPN Deployment Scenario

In a network with a very high number VPN sites and the PEs to which they are attached, any-to-any connectivity between the VPN sites would require each PE router connected to any of these sites to hold all the routes of that VPN. This would require the following:

- The RIB and FIB of each VRF locally representing such a service would have to hold a large number of routes
- Each PE where the service is represented would set up an LSP to every other PE where that service is represented.

Addressing these scale requirements is problematic for low-end PEs, such as access nodes (cell-site routers) in Mobile Backhaul (MBH) applications. And the situation doesn't improve - MBH for 4G and 5G mobile networks require even greater complexity to enable X2 services that require any-to-any connectivity between all the base stations.

HoVPN simplifies implementation when any-to-any L3VPN services are provided over an IP/MPLS network with a multi-level hierarchical structure. Services can be deployed using HoVPN to relax scalability requirements on the low-end PEs, both from the perspective of the number of routes they hold, and from the perspective of the number of LSPs for which they act as head-ends. HoVPN support is based on virtual hub-and-spoke configurations in BGP/MPLS VPNs, with the Area Border Routers (ABRs) of each access domain acting as virtual hubs for the access nodes in the same access domain as their virtual spokes.

The following figure illustrates a configuration that includes multiple hierarchy levels within a typical MBH network, where the access nodes (such as AN-111) in a given access domain establish tunnels only to other access nodes and to the ABR located within their own access domain, but not to any other router in the MBH network. In addition, such an access node receives only the routes advertised by other access nodes within its own access domain, as well as the default routes advertised by ABRs within its access domain.

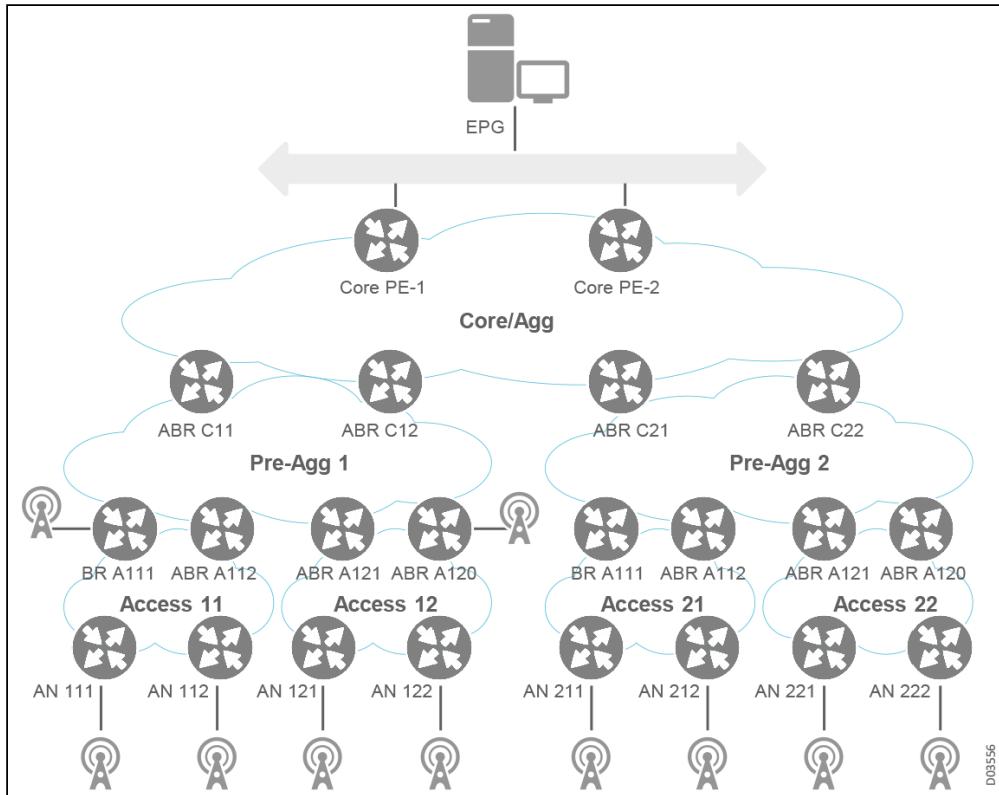
Therefore, any traffic from the access node destined for the pre-aggregation PEs, for the core/aggregation PEs, or for access nodes in other access domains is forwarded to one of the ABRs. The ABRs of the access domain maintain all the routes of the VPN.

The user defines the ABRs of the access domain as *Virtual Hubs* and defines the access nodes as *Virtual Spokes*, where each Virtual Spoke is associated with one of the Virtual Hubs. Furthermore, each Virtual Hub and all its Virtual Spokes share a unique RT value. The Virtual Hub uses that value as an Export RT pattern. The Virtual Spokes use it as an Import RT pattern. With the assistance of an enhanced VRF export policy, the Virtual Hub is directed to advertise its default route message with the unique Export RT pattern. So, the default route is accepted only by the associated Virtual Spokes and ignored by all other VRFs (i.e., other virtual Hubs/Spokes in the same L3VPN service, and VRFs in same service that were not defined as either Virtual Hubs or Spokes).

**Notes:**

- HoVPN technology is not always required or justified in all network contexts. It's generally only configured if a given L3VPN service has an appropriate topology.
- Access nodes (that do not serve as "Virtual Hubs") are not required to have any specific capabilities to implement HoVPN. The configuration necessary utilizes the already existing parameters.

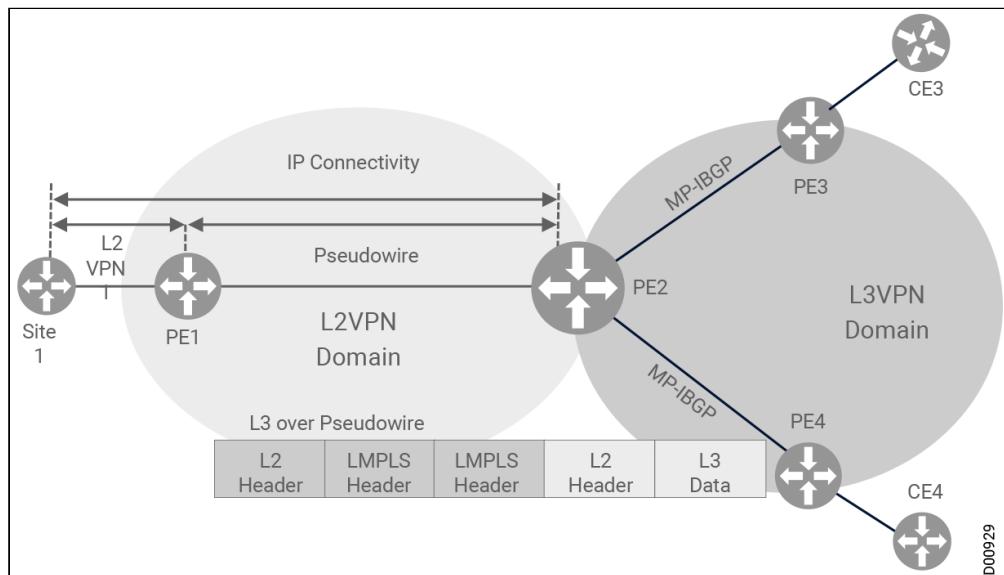
### Multiple Hierarchy Levels within a Typical MBH Network



With HoVPN, access nodes within a specific access domain receive and install only the routes relevant for them, from other nodes in the same access domain; they don't have to waste any space or time on information relevant only to access nodes located in other access domains. They also receive default routes from the Area Border Routers (ABRs) of the containing access domain; any traffic that is destined for the core PEs or for access nodes in the other domains is sent to one of the ABRs. The ABRs of the access domain receive, resolve, and install all the routes of the service.

# L2VPN and L3VPN Interworking

## Pseudowire Headend Termination (PHT)



Incorporating PHT technology into your network provides many benefits, including:

- Seamless MPLS end-to-end transport architecture
- Flexible service edge placement with virtual PHT interface
- Feature parity as regular L3 interface
- CE-PE routing over MPLS transport network with no need for a direct L3 link
- CE-PE virtual link protected by the MPLS transport network, making it:
  - Controlled
  - Visible
  - Reliable
  - SLA and QoS-capable

This section includes the following topics:

- [L3VPN PW Extension with PHT](#)
- [Integrated Routing and Bridging IRB](#)

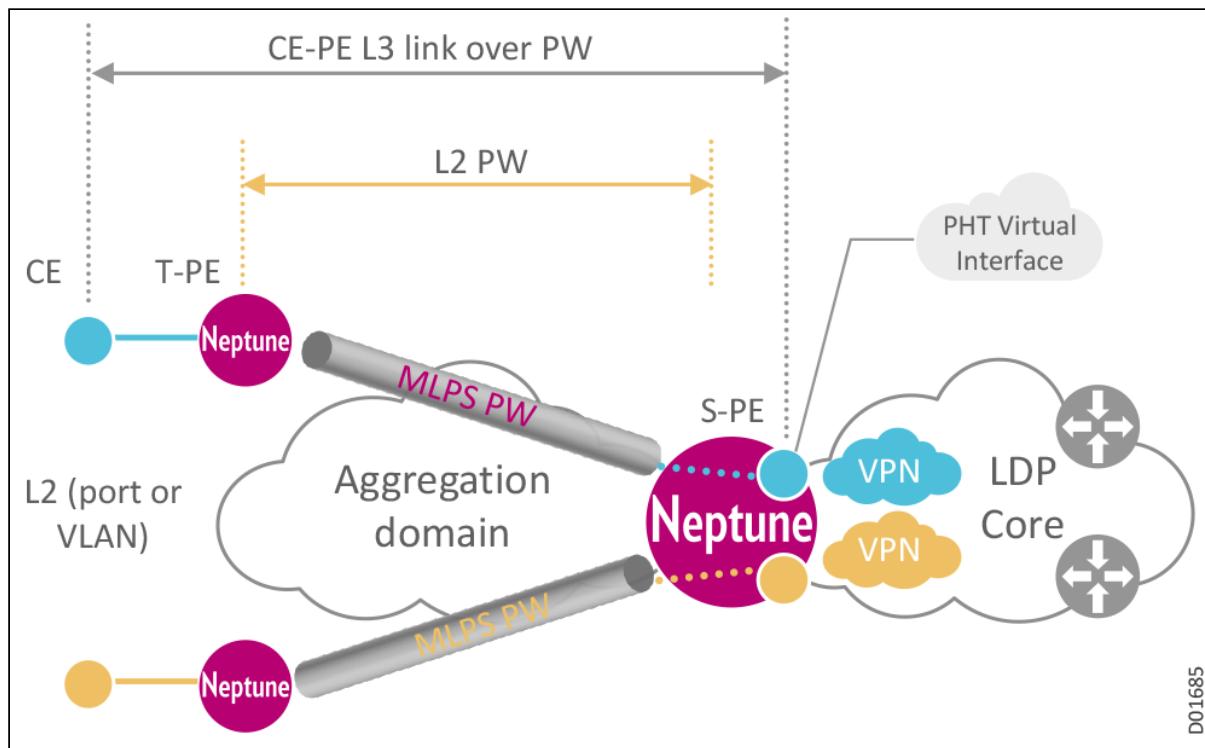
## L3VPN PW Extension with PHT

PWs are simple, manageable lightweight tunnels that enable payloads to be transparently carried across IP/MPLS packet-switched networks, providing an easy and scalable mechanism for tunneling customer traffic into a common IP/MPLS network infrastructure.

Access PWs, located between access and edge nodes, offer a simple mechanism for returning customer traffic into core networks, terminating into a Layer2 or Layer3 (VRF or global) domain.

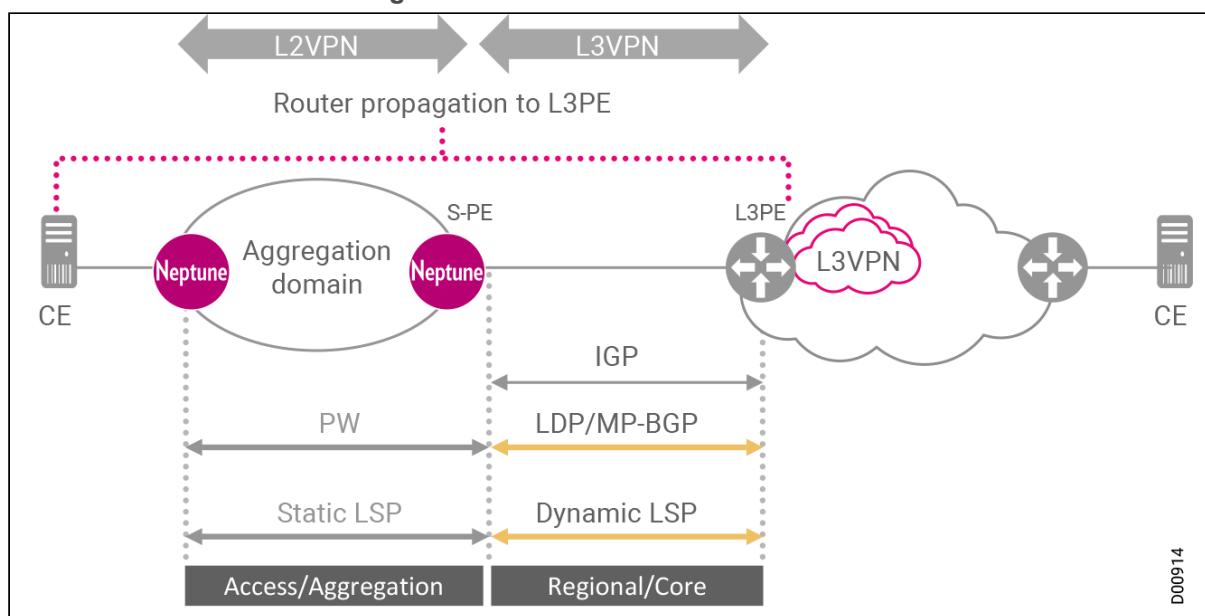
The L3 routing domain between CPE and S-PE is **extended** transparently over the MPLS-TP access infrastructure. The S-PE terminates the MPLS-TP LSP/PWE from the access/aggregation region and participates in L3VPN forwarding with IP/MPLS core L3PEs using conventional LDP/MP-BGP mechanisms.

### Extending the L3 Routing Domain



The following figure illustrates an L2VPN/L3VPN **interworking** configuration, implemented using L3VPN PW extensions with PHT over MPLS-TP access.

### L2VPN and L3VPN Interworking with PHT



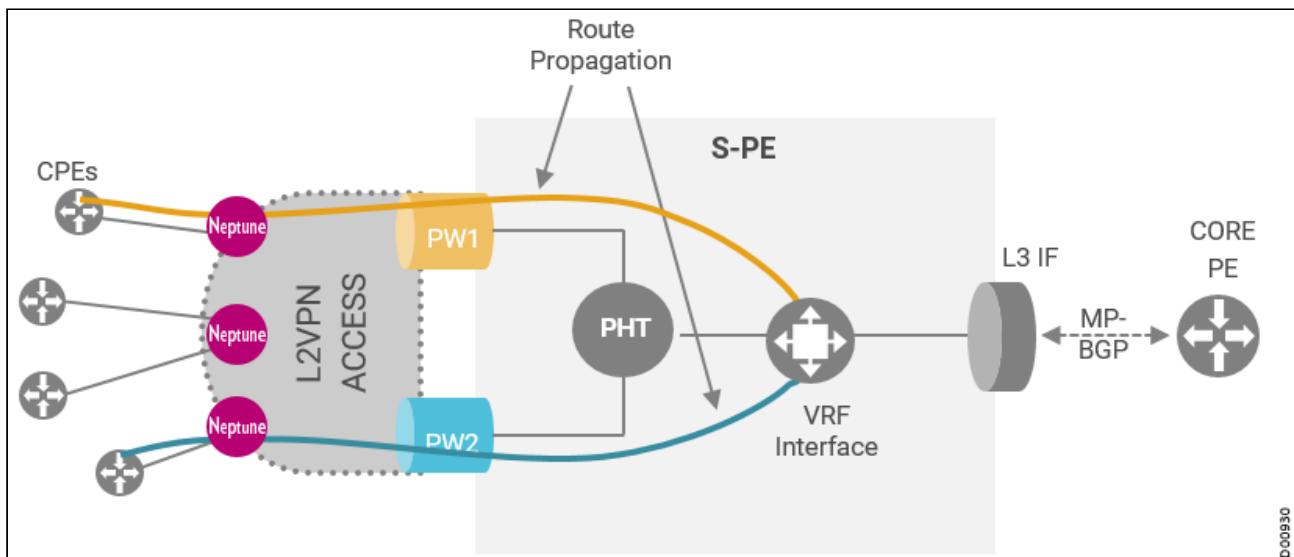
In this network, we see MPLS PWs configured between access and edge Neptune nodes. Each PW carries a single service or bundle of services (service per VLAN or multiple VLANs). (In this type of network, H-VPLS can be used to increase scalability.) The S-PE is peering with the L3PE. iBGP is used within the AS, and eBGP is used towards the ASBR in a different AS. (This actually poses more strain on S-PE.) The S-PE utilizes a L3 virtual interface, created to represent traffic from/to a given PW, while terminating that traffic in a VRF.

At this point, FHRP, QoS, ACL, and PBR can be applied. The PE-CE routing information is exchanged either via IGP or through static routing.

Smooth L2/L3 interworking through PHT offers many benefits, including:

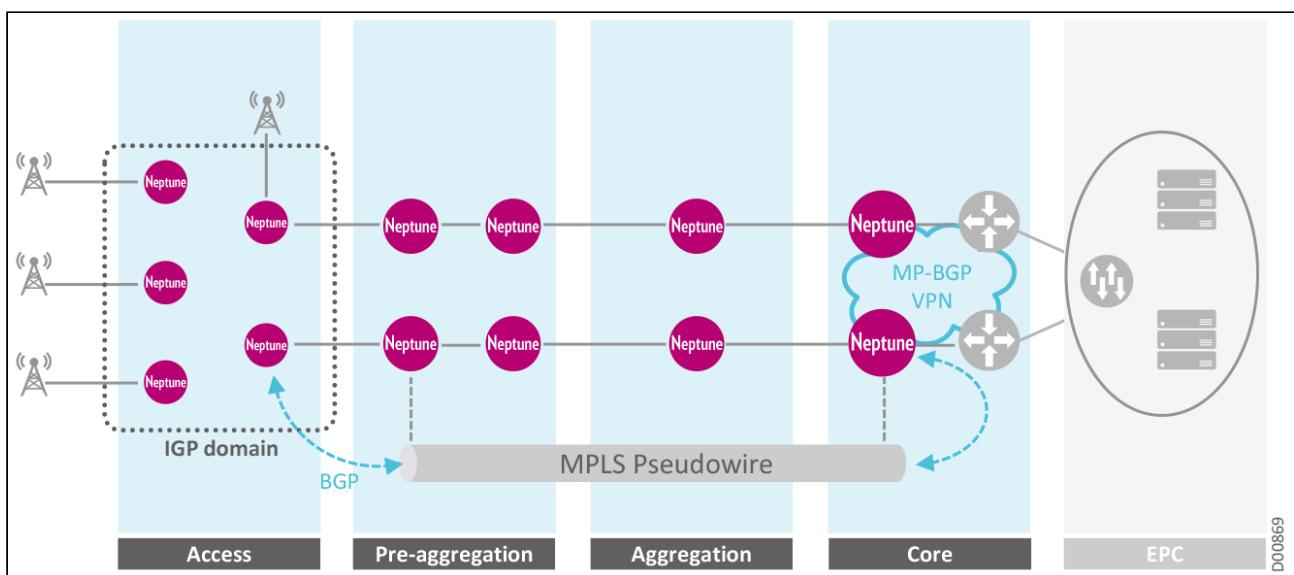
- Simpler resiliency between L3 PEs and the aggregating network
- SDH/SONET-like OAM and resiliency with MPLS-TP
- Eliminates operationally cumbersome VLAN hand-off
- Simpler service delivery with centralized universal edge
- Enables flexible edge placement
- Cost-effective access solution
- Simpler migration path to IP/MPLS services

### L3VPN Extension into Access



An excellent use case example would be using this configuration for an LTE MBH network. This approach solves the network scaling issue by creating an additional layer of abstraction between the access and core aggregation domains. This eliminates the need for signaling protocols within the access and aggregation network. The underlying network infrastructure is utilized as a service over which the LTE transport L3VPN is established.

### LTE MBH Solution



## Integrated Routing and Bridging IRB

**Integrated Routing and Bridging (IRB)** allows the routed and bridged interfaces to communicate with each other. IRB is a router feature that allows network operators to create a connection between a bridged domain and a routed domain.

For a VLAN to span a router, the router must be able to forward frames from one interface to another while maintaining the VLAN header. If a network protocol is configured on a router interface (IP), the VLAN header will not be maintained, which terminates the VLAN. When configuring IRB, we use a switching instance *attached* to a bridge domain, thus providing the bridged interfaces a connection to the routed world.

When IRB is configured:

- If traffic that is destined for a host in the bridge group comes in on a routed interface (IP address configured), then the traffic is first routed to the switching instance. The packet is then forwarded to the bridging engine, which forwards it through a bridged interface. The forwarding is based on the destination MAC address.
- If a packet that is destined for a host in a routed network comes in on a bridged interface, then the traffic first goes to the switching instance, and then sent to the routing engine before it sends it out through the routed interface.

# Model-Driven Telemetry: MDT

Model-Driven Telemetry (MDT) is a new approach for network monitoring, in which data is continuously streamed from network devices using a push model, with efficient, incremental updates. A next-generation intelligent OAM system, telemetry is becoming the leading technology in network monitoring, offering greater advantages over traditional methods, such as SNMP and CLI.

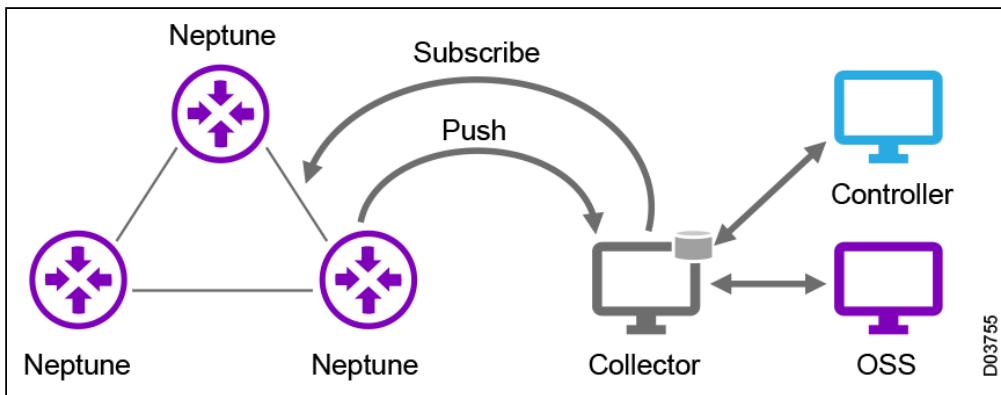
Conventional data collection technologies chiefly employ the pull mode to periodically query multiple device indicators, including interface rate, memory usage, and optical power. With query messages sent every five minutes, network issues arising between the queries may go undetected due to the delay. In addition to data inaccuracy, the SNMP polling method also causes excessive CPU usage and may hamper routine operations.

With MDT, data can be collected from remote wired or wireless devices faster and more efficiently, providing a greater degree of visibility and flexibility. Streaming telemetry replaces the need for the periodic polling of network elements; instead, a continuous request for information to be delivered to a subscriber is established upon the network element using the push mode. This approach provides near real-time access to operational statistics, while having very little impact on the device's ordinary functions and performance. Operators can subscribe to the specific data items they need, using the OpenConfig telemetry YANG model as the common interface. Multiple subscriptions can be active simultaneously so that different groups of parameters can be monitored with different rules and/or frequency. The requested data items are often implemented through standard-based YANG data models.

Telemetry functions as a closed-loop automatic OAM system and consists of the following stages:

1. The Telemetry collector must first subscribe to stream data. Depending on the Telemetry mode, either the network device or the collector initiates the streaming session.
2. The device sends the collected data to the collector based on the selected data subscription method.
3. The controller analyzes the data stored in the collector for network optimization. It then delivers the improved network configurations back to the device.
4. After the new settings are implemented, the device reports new collected data to the collector. This data is checked by the controller against the optimization analysis previously carried out. The process is complete once optimization has been reached.

## The Telemetry Lifecycle



Neptune supports MDT based on Open Config YANG models and gNMI/gRPC transport. OpenConfig provides a vendor-neutral data model used to configure and manage network devices, and assist in transitioning from a pull model to a push model, with subscriptions and update streaming. While OpenConfig handles the state of the devices, the actual data streaming is done using the gRPC Network Management Interface (gNMI) protocol, which provides the mechanism to retrieve and view operational data as well as manipulate configurations of network devices (also known as gNMI targets). A list of the YANG modules currently supported by Neptune can be obtained from Ribbon's documentation portal.

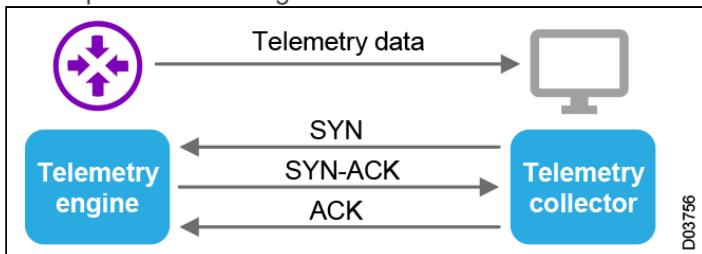
This section introduces model-driven telemetry, including:

- Telemetry Modes
- Telemetry Entities
- Telemetry Subscription Methods and Modes
- gRPC and gNMI Framework

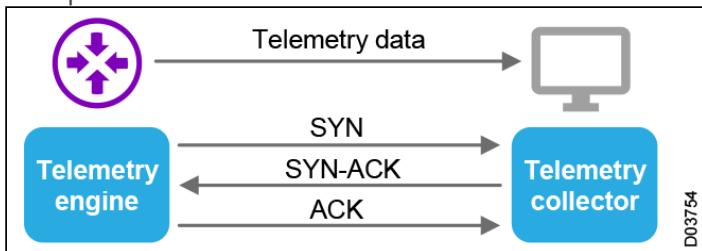
## Telemetry Modes

Model-driven telemetry doesn't involve a polling mechanism. Alternatively, the data is proactively and periodically pushed off the device at any of the following modes of operation:

- **Dial-in:** In a dial-in mode, the Telemetry collector initiates a session with the network device (Telemetry engine) and subscribes to stream data. The collected data is dynamically configured by the collector and delivered back to the device. In the event of connection loss, the device will cancel the subscription and no longer send collected data to the collector.



- **Dial-out:** In a dial-out mode, the network device (Telemetry engine) initiates a session with the Telemetry collector based on the subscription. The collected data is configured using commands on the device. Dial-out is the default mode of operation. When a session ends, the device continually attempts to re-establish a new session with the destination every 30 seconds.



### **i Note**

The Neptune product line currently supports the dial-out mode only.

During the establishment of a TCP protocol connection between the client and the server, the initiator side uses the three-way (or 3-step) handshake. In dial-in, the initiator is the client (Telemetry collector) whereas in Dial-out, the initiator is the server (Telemetry engine).

TCP 3-way handshake includes:

1. **SYN:** The active open is performed by the client/server sending a SYN to the server/client. The client/server sets the segment's sequence number to a random value (A).
2. **SYN-ACK:** In response, the server/client replies with a SYN-ACK. The acknowledgment number is set to the received sequence number incremented by 1 (A+1). The sequence number chosen by the server/client for the packet is another random number (B).
3. **ACK:** Finally, the client/server sends an ACK back to the server/client. The sequence number is set to the received acknowledgment value (A+1). The acknowledgment number is set to the received sequence number incremented by 1 (B+1).

### Dial-Out Configuration Workflow

1. Create a destination-group, specifying the collector's address, port, encoding, and transport to be used by the route to send out telemetry data.
2. Create a sensor-group, specifying the list of YANG models to be streamed.
3. Create a subscription, associating a sensor-group with the streaming interval as well as with the destination-group.

## Telemetry Entities

To enable telemetry streaming, you must first configure the following entities:

- **Sensor groups:** A sensor group specifies a list of YANG models to be streamed. You can define up to 8 sensor groups per NE.

Each sensor group consists of:

- A sensor group ID (a string)
- 16 sensor paths

Each YANG model in a sensor group is represented by a **sensor path**. The sensor path describes a YANG path or a subset of data definitions in a YANG data model within a container.

In a YANG model, the sensor path can be specified to end at any level in the container hierarchy.

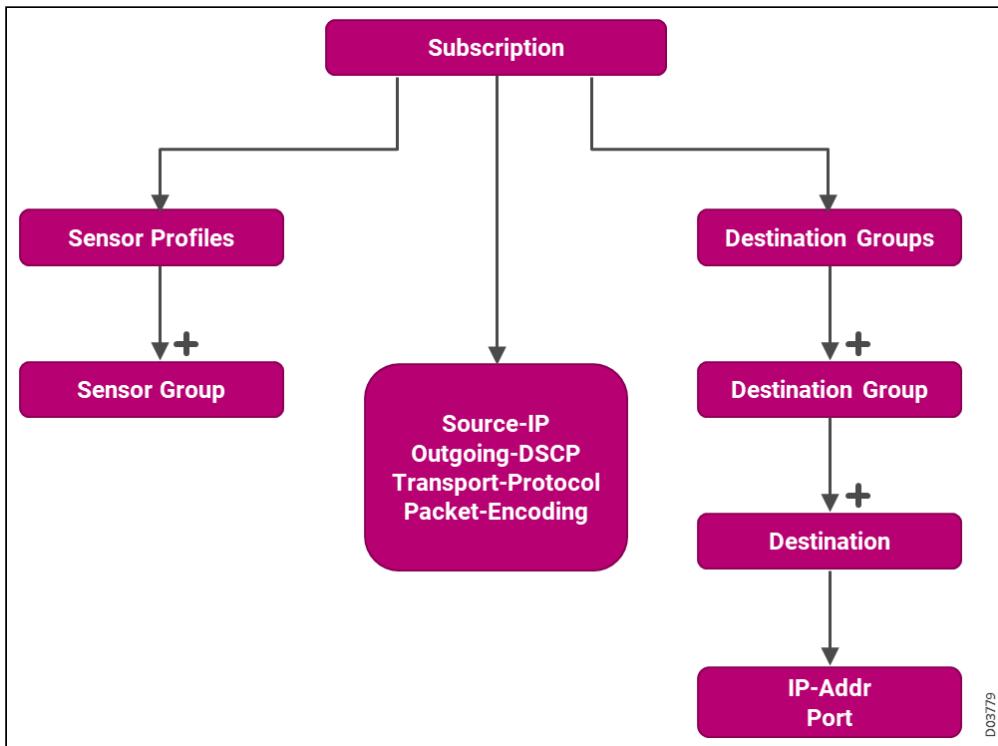
- **Destination groups:** The destination group specifies the destination address, port, encoding, and transport used by the router to send out telemetry data. You can define up to 8 destination groups per NE. Each destination group consists of:

- A destination group ID
- 8 destinations: Each destination comprising a set of IP (IPV4 or IPV6) destinations and a port number

- **Subscription groups:** The subscription group sets the number of sessions between the NE and the telemetry collector. It associates a destination group with a sensor group and selects the streaming method. Multiple destination groups and sensor groups must be supported in a single subscription group. A source interface in the subscription group specifies the interface to be used for establishing the session to stream data to the destination. If both the VRF and the source interface are configured, the source interface must be in the same VRF as the one specified under the destination group for the session to be established.

Once the configuration is complete, the NE internally uses **gNMI API Subscribe** to create a session between the device and the collector. If the subscription mode is **STREAM**, the device pushes the telemetry information to its destination collector.

## Relationships Between Telemetry Entities



## Telemetry Subscription Methods and Modes

### Subscription Methods

There are two subscription methods for telemetry streaming:

- **Cadence-Driven Telemetry:** Data is streamed according to a set **sample-interval** attribute, ranging from 1000 to 604,800,000 milliseconds.
- **Event-Based Telemetry:** Data is streamed according to an occurring event/threshold crossing event. To set the subscription to Event-Driven telemetry, you should configure the **sample-interval** attribute to 0.

#### **i** Note

Separating the sensor paths into different subscriptions enhances the efficiency of the router to retrieve operational data at scale. Hence, the subscription of a certain sensor group can be enabled with the Cadence-Driven method, while another subscription can be enabled with the Event-Based method.

### Subscription Modes

Telemetry includes the following subscription modes:

- **STREAM:** The device pushes the information to the collector.
- **Once:** The data is returned immediately and only once for all the specified paths.
- **POLL:** The data is returned from the device when polled with the current values for all the specified paths.

**Note**

The Neptune product line currently supports the **STREAM** mode only.

## gRPC and gNMI Framework

Telemetry organizes data based on YANG models, encodes data in JSON or Google Protocol Buffers (GPB) format, and transmits data through the Google Remote Procedure Call (gRPC) protocol. This improves data collection efficiency and facilitates intelligent interconnection.

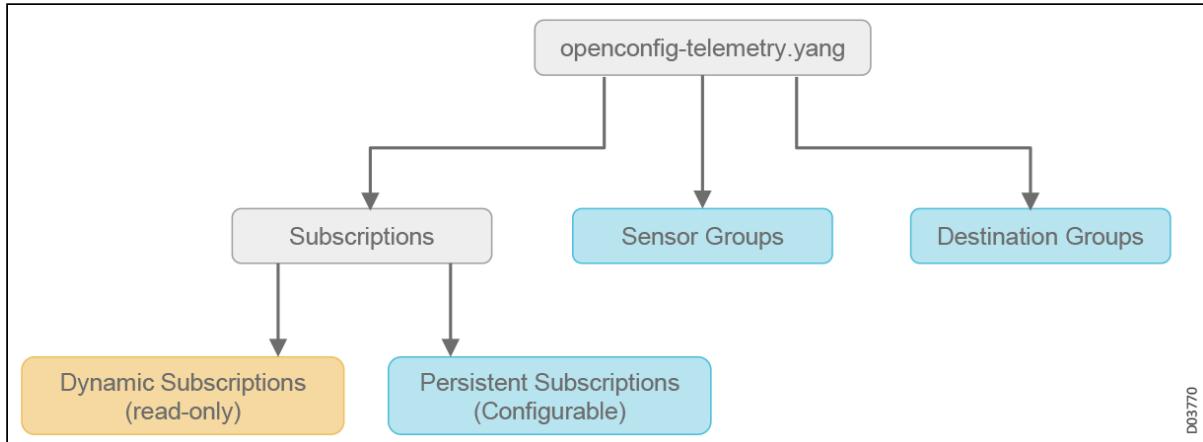
### OpenConfig

OpenConfig is a group of network operators sharing the common goal of migrating networks toward a more dynamic, programmable infrastructure by adopting modern networking principles such as declarative configuration and model-driven management and operations. OpenConfig supports vendor-neutral data models for configuration and monitoring of the network, as well as assisting in moving from a pull model to a push model, with subscriptions and update streaming.

The **openconfig-telemetry.yang** module is used in the Telemetry solution to configure a dial-out subscription and to monitor both Dial-out and Dial-in subscriptions. The dial-in subscriptions are configured through other interfaces.

The YANG model defines Dial-out (persistent) and Dial-in (dynamic) subscriptions. While persistent subscriptions are configurable, the dynamic aren't.

### OpenConfig Telemetry YANG Model



A list of the YANG modules currently supported by Neptune can be obtained from Ribbon's documentation portal.

### gRPC

gRPC is a modern open-source high performance Remote Procedure Call (RPC) framework that can run in any environment. Initially created by Google, gRPC efficiently connects services in and across data centers with pluggable support for load balancing, tracing, health checking, and authentication. It is also applicable to the "last mile" of computing as it is used with mobile applications and browsers to backend services. gRPC leverages the standard HTTP/2 as its transport layer and uses Protobuf as its interface description language.

### gRPC Network Management Interface (gNMI)

The gRPC Network Management Interface (gNMI) is a protocol for configuration, manipulation, and state retrieval. Built on top of the gRPC, gNMI provides the mechanism to install, manipulate, and delete the configuration of network devices, as well as to view operational data.

# OAM and Performance Monitoring PM

Business critical applications rely heavily on network services. The smallest change in network usage can impact network performance and reliability, which directly affects the cost of maintaining network services and ability to conduct key business operations. Therefore, monitoring networks is essential to prevent and detect faults and improve overall network reliability.

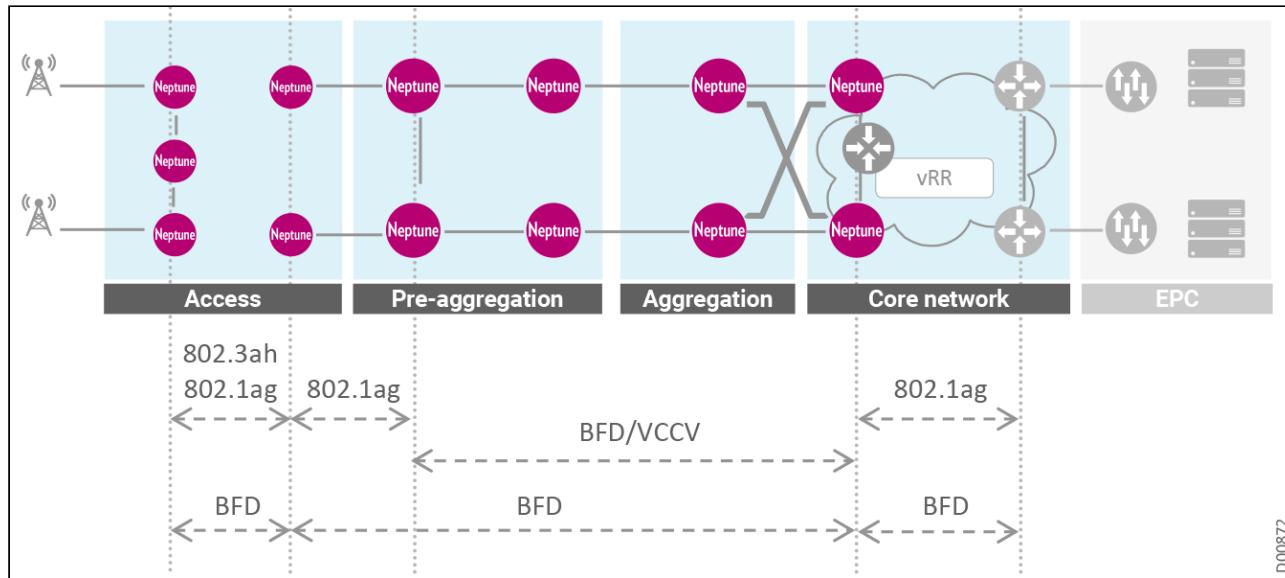
Since modern converged networks carry different kinds of traffic, a means of measuring traffic characteristics is therefore important. For a service provider selling premium services, measuring and analyzing traffic characteristics is crucial. For businesses that are building new network infrastructure or IT solutions, capacity planning for new networks is based on historic and projected traffic usage patterns. So measuring traffic characteristics and usage becomes central to capacity planning. It is clear that there is an acute need for traffic monitoring technologies for both enterprises and service providers.

Operations, Administration, and Maintenance (OAM) functions provide mechanisms for monitoring a physical or logical connection. OAM provides network operators the ability to monitor the health of the network and quickly determine the location of faults. Our platforms provide full end-to-end OAM for efficient fault localization, including:

- **Performance Monitoring** tools and other internal card implementations, enabling efficient tracking, storage, and analysis of the potentially huge amounts of historical PM data produced by large numbers of large-scale SDH/SONET and data objects, a valuable capability for network operators monitoring heavy traffic.
- **Ethernet link OAM**, based on IEEE802.3-05 (formerly 802.3ah), featuring remote failure indication, remote loopback control, and link monitoring that includes diagnostic information.
- **MPLS service OAM and PM**
  - **Virtual Circuit Connectivity Verification (VCCV) PW OAM**: Including PW ping and BFD failure detection
  - **MPLS-TP tunnel OAM**, based on RFC5860 and ITU-T 8113.2 Generic Alert Labels (GAL), providing continuous end-to-end tunnel connectivity verification as well as monitoring of endpoints and PWs running over the tunnel, through BFD support for MPLS TP in bidirectional tunnels.
  - **MPLS-TP fault management (FM)**, based on RFC 6427. Fault OAM messages are generated by intermediate nodes where a client LSP is switched and sent downstream towards the end point of the LSP.
- **IP/MPLS VPN service OAM and PM**
  - **IP and VRF** mechanisms, including:
    - **Ping**, to check bi-directional reachability of a specified IP address
    - **Traceroute**, to provide information about the actual path to a specified IP address
  - **BFD**, providing a continuity check mechanism for failure detection
- **TWAMP**, based on RFC 5357, an open protocol for measuring network performance (one-way and round-trip) between any two devices supporting the TWAMP protocol.
- **Link Delay Measurement**, measuring the time elapsed between the moment that a packet leaves the network of one provider and the moment that the packet arrives at its destination. Link delay measurement is a key factor in effective OAM.
- **Service OAM**, including Connectivity Fault Management (CFM) based on IEEE802.1ag, enabling end-to-end network OAM for Ethernet networks.
- **CFM-PM**, based on Y.1731, enabling measurement and collection of Ethernet service performance measurements that provide objective data regarding delay and synthetic loss.
- **Throughput testing**, based on RFC2544, including packet generator and analyzer which enable RFC2544 testing between two access ports for any end-to-end service. This provides an on-demand service OAM mechanism to measure service performance.
- **Service Level Agreement (SLA)**, based on Y.1564, including its Ethernet-based service testing method for QoS and network performance. This standard defines procedures to test service turn-up, installation, and troubleshooting of Ethernet-based services, in order to achieve assured and verified committed SLA performance.

- **sFlow**, based on RFC 3176, is a packet sampling technology that can be implemented in a broad range of networking devices, from Layer 2 switches to high-end core routers, providing unprecedented visibility into network usage and active routes of even today's high-speed and complex networks.
- **SNMP**, used for performance monitoring and management of network devices.
- **LLDP**, based on 802.1AB, facilitates identification of stations connected by IEEE 802 LANs/MANs, their points of interconnection, and access points for management protocols.

### E2E OAM Model for a Mobile Backhaul Network



This section includes the following OAM features:

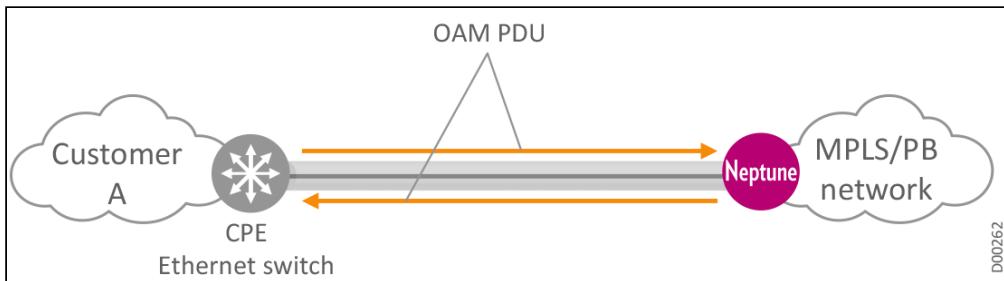
- Ethernet Link OAM - IEEE 802.3-05
- MPLS-TP Tunnel OAM
- IP-MPLS VPN Service OAM and PM
- TWAMP - RFC 5357
- Link Delay Measurement
- Service OAM CFM - IEEE802.1ag
- CFM-PM Y.1731
- Throughput RFC 2544
- SLA Y.1564
- sFlow RFC 3176
- SNMP v2-v3
- Link Layer Discovery Protocol LLDP

## Ethernet Link OAM - IEEE 802.3-05

OAM can be enabled on any full-duplex P2P or emulated P2P Ethernet link. OAM information is carried in Slow Protocol frames called OAM Protocol Data Units (OAM PDUs). Maximal rate of OAM PDU frames is 10frames per second. OAM mechanisms are supported for all ETY UNI and NNI ports according to IEEE802.3 2005 (formerly 802.3ah).

When the card acts as a PE to a Customer Edge CE, OAM is based on IEEE 802.3-05 standard Ethernet Link OAM (formerly 802.3ah). It provides connectivity check for link monitoring. Loopback operates on peer remote equipment. Reports about link-down conditions are sent to peers. Discovery process for peer capabilities is also supported.

### Ethernet Link OAM - IEEE 802.3-05



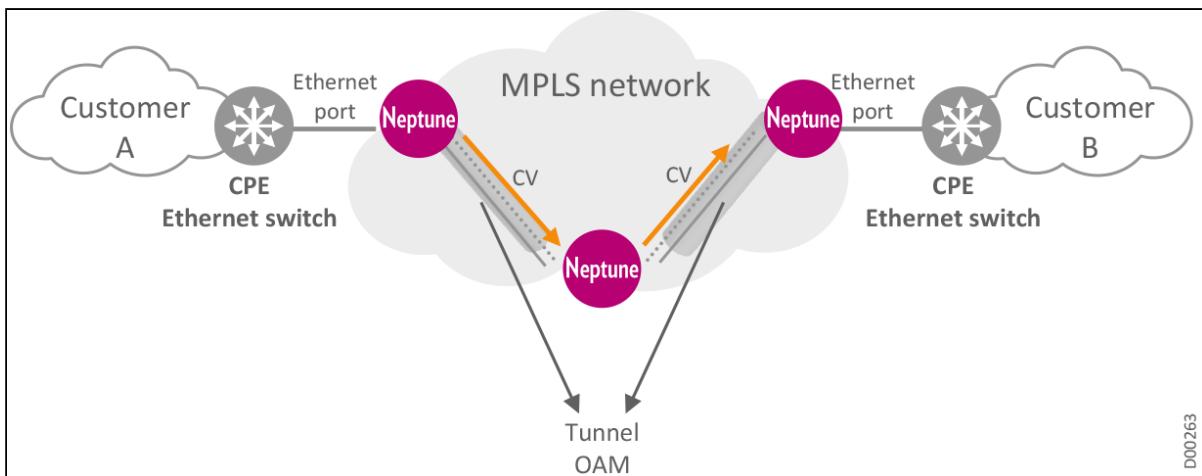
## MPLS-TP Tunnel OAM

MPLS-TP tunnel OAM, based on **RFC5860** and **ITU-T 8113.2 Generic Alert Labels (GAL)**, provides continuous end-to-end tunnel connectivity verification as well as monitoring of endpoints and PWs running over the tunnel.

MPLS-TP tunnel OAM for bidirectional tunnels is based on **Bidirectional Fault Detection (BFD)**, a simple Hello protocol used to verify connectivity between systems. A pair of systems transmits BFD packets periodically over each path between the two systems.

If a system stops receiving BFD packets for some preconfigured period of time, a component in that particular bidirectional path to the neighboring system is assumed to have failed.

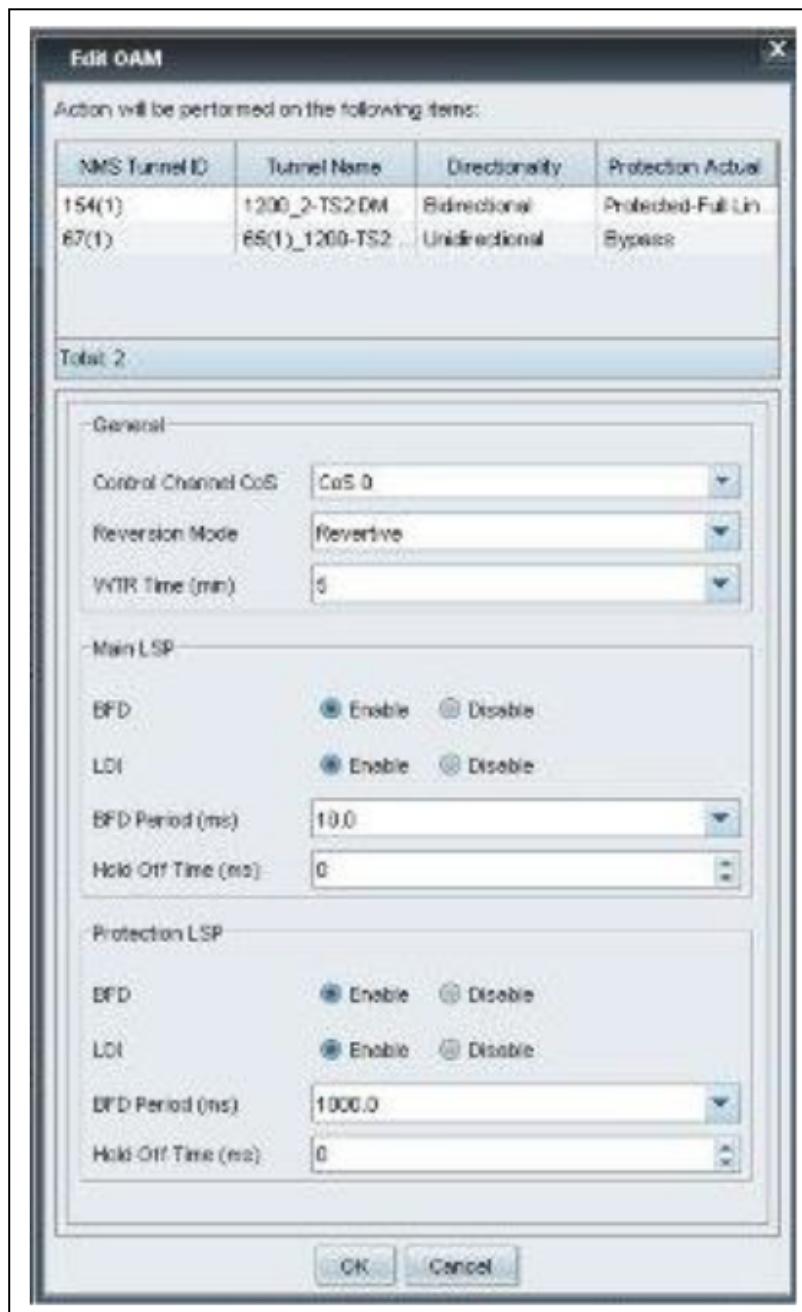
### Tunnel OAM



BFD provides proactive end-to-end tunnel CC (Continuity Check), CV (Connectivity Verification), and Remote Defect Indication (RDI):

- Continuity Check (CC): Continuously monitors the integrity of the continuity of the path. In addition to failure indication, detection of Loss of Continuity may trigger the switch over to a backup LSP.
- Connectivity Verification (CV): Monitors the integrity of routing of the path between sink and source for any connectivity issues, continuously or on-demand. Detection of unintended continuity blocks the traffic received from the misconnected transport path.
- Remote Defect Indication (RDI): Enables an End Point to report to its peer a fault or defect condition that it detects on a path.

## Edit OAM



## IP-MPLS VPN Service OAM and PM

OAM and PM mechanisms for IP/MPLS VPN service is supported, including:

- **Ping**, to check bi-directional reachability of a specified IP address.
- **Traceroute**, to provide information about the actual path to a specified IP address.
- **Bidirectional Forwarding Detection (BFD)** is a network protocol used to detect faults between two forwarding engines connected by a link, thereby providing a continuity check mechanism for failure detection. BFD provides low-overhead fault detection even on physical media that doesn't support failure detection of any kind, such as Ethernet, virtual circuits, tunnels, and MPLS LSPs.

## IP-BFD Setup Tab



## TWAMP - RFC 5357

Measuring the performance of IP networks through the use of standard protocols has always been a challenge. The inventors of IP provided some tools, such as Internet Control Messaging Protocol (ICMP) Ping, Traceroute and User Datagram Protocol (UDP) Echo, as part of the TCP/IP suite of protocols. However, these tools were designed for simple IP network troubleshooting, and are not suitable for OAM performance measurements.

Accurate measurement of transmission metrics between devices is the foundation of effective OAM. The IETF initially produced RFC4656, defining the one-way active measurement protocol (OWAMP) for measuring one-way metrics between network devices. OWAMP could also be used bi-directionally to measure one-way metrics in both directions between two network elements. However, that would not enable meaningful measurements for round-trip or two-way transmissions.

The IETF's IP Performance Metrics working group has therefore developed RFC5357, specifying a two-way active measurement protocol (TWAMP), based on the OWAMP, to add two-way or round-trip measurement capabilities. TWAMP is an open protocol for measuring network performance (one-way and round-trip) between any two devices supporting the TWAMP protocol. TWAMP employs time stamps applied at the echo destination (reflector) to enable greater accuracy, since processing delays can be taken into account. With TWAMP, enterprise IT managers can effectively measure the complete IP performance of underlying transport through cooperation between network elements that have already been deployed.

The TWAMP protocol includes the following components: test endpoints, two inter-related protocols, (TWAMP-control, TWAMP-test), and two modes (Full, Light).

- TWAMP endpoints are assigned clearly defined roles, responsible for starting a monitoring session and exchanging packets.
  - The session-sender node is responsible for generating test traffic and processing the returned traffic in order to measure performance.
  - The reflector node returns test traffic received from the sender node.
- TWAMP can be configured for two different modes: Full and Light. While each mode has its advantages, both measure critical KPI's, including loss, latency, jitter, duplicates, out of order scenarios, and more.
  - Full mode test is designed to work in a client-server relationship, where the control of the test may be managed by separate devices from the devices that will be sending and receiving the test traffic. During a full-mode TWAMP session, the session is established between the sender and responder through a control channel within a control session that negotiates communication between devices.

- TWAMP Light mode is designed to help implement the TWAMP standard across entities that act as active responders to TWAMP controllers within the network, thereby enabling the measurement of two-way IP performance from anywhere within that network. In a light-mode TWAMP session, no negotiation occurs between the endpoint and the client.
- TWAMP works with two different protocol models, Control and Test.
  - The TWAMP-Control protocol is used to set up performance measurements. The control client initiates all requested test sessions with a start sessions message, and the server acknowledges. When necessary, the control client sends a message to stop all test sessions.
  - The TWAMP-Test protocol is used to send and receive performance measurement probes. The session sender and the session reflector exchange test packets according to the TWAMP-Test protocol for each active session. On receiving a TWAMP-Test packet, the session reflector only reflects a measurement packet and does not collect packet statistics in TWAMP.

Through the use and deployment of TWAMP, operators can avoid the costly deployment of performance management systems with proprietary protocols while effectively measuring the IP performance of their network at all locations.

Neptune platforms can function as server and session reflectors.

## Link Delay Measurement

Network performance is measured by analyzing various performance metrics, usually using a two-way active measurement protocol ([TWAMP](#)).

Two of the parameters that determine network performance between two providers are:

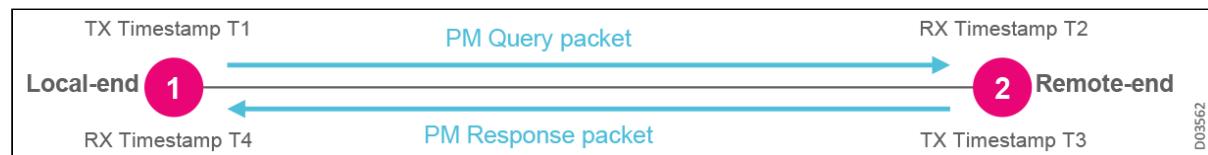
- Bandwidth: The number of bits that can be transferred between two providers per unit of time.
- Delay: The time elapsed between the moment that a packet leaves the network of one provider and the moment that the packet arrives at its destination. Link delay measurement is a key factor in effective OAM.

This information can be used to make intelligent path-selection decisions based on network performance. TE mechanisms help ensure compliance with Service Level Agreements (SLAs). The metrics make it possible to optimize network LSPs, improving path selection since dynamic link delay data can be analyzed together with other path cost data. These decisions must be made carefully, balancing the relevant network data and service requirements. For example, you could have a network where traffic across the core network is "cheaper" in terms of classic transmission costs, but would involve a longer link delay time. Alternatively, there may be an access "shortcut" path available, with lower latency but a greater transmission "expense". Intelligent traffic optimization would be able to take both these factors into account and provision the traffic routes accordingly. So if you are providing service for a business where ultra-low latency is crucial, packets may be transmitted across the (more expensive) access "shortcut", providing transport services optimized for that business.

Neptune platforms support link delay measurement advertisements based on RFC 6374. Link delay parameters may include minimum, average, maximum, and variance values. The minimum link delay values are used as a metric for SR-TE (through tunnels or Flex-Algo). Link delay can be calculated per port or LAG. The delay measurement (DM) parameter is part of the MPLS LIF interface configuration; only one LIF per port or LAG is used for DM.

Neptune platforms provide two-way link-delay measurements, calculated as illustrated in the following figure.

### Two-Way Link-Delay Measurements



The query-response steps are as follows:

- The local-end router sends a PM query packet periodically to the remote-end side; transmission is as soon as the T1 timestamp is applied to the packet.
- The remote-end router applies the T2 time-stamp on packet as soon as it is received.
- The remote-end router time-stamps the packet again (T3) just before sending the packet back to the local-end router.
- The local-end router time-stamps the packet (T4) as soon as the packet is received.

Given the 4 timestamp values (T1, T2, T3, and T4), two-way delay is simply the time needed to travel from local-end 1 to remote-end 2 (T2-T1), plus the time needed to travel back from remote-end 2 back to local-end 1 (T4-T3).

$$\text{Two-way delay} = (T2 - T1) + (T4 - T3)$$

One-way delay can be calculated based on the two-way delay value divided by 2. Link delay can be calculated per port or LAG; only one LIF per port or LAG is used for DM.

Neptune platforms support link delay measurement advertisements when MPLS-TE is enabled, for the following attributes:

- **Advertising interval** defines the periodic advertising interval period (default 120 seconds)
- **Threshold** defines the threshold change percentage at which point a change should be advertised (default 10%)
- **Minimum** lower bound defines the maximum value that can be set for the minimum delay value (default 1000 µsec)

Delay measurement advertisement is applicable only for unidirectional minimum and maximum link delays.

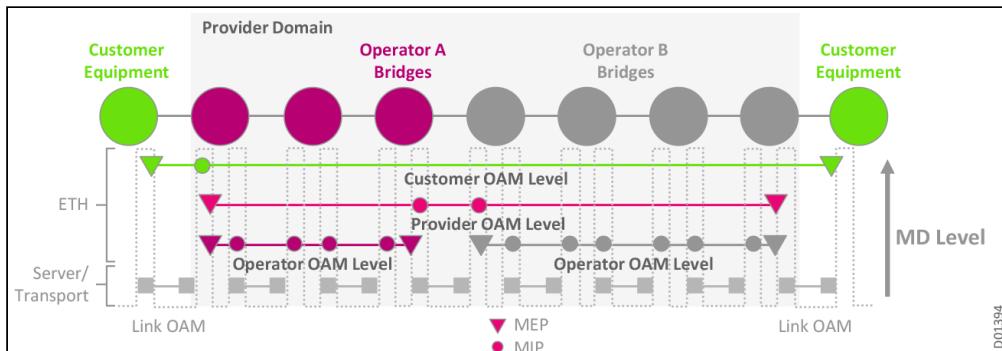
At the end of each periodic interval, if the change in a measured value for a link, compared to the previous advertised value, is greater than the configured threshold value AND greater than the configured minimum value, then the delay values are updated. Each IGP instance supporting MPLS-TE and link delay measurement is notified about the new changes; the changes are then advertised immediately to all relevant links. If the changes are not greater than the thresholds that were configured, the IGP instances report the last advertised delay measurement at the LSP/LSA refresh time. Protocol-specific implementation details are provided in the [IS-IS Support for Delay Measurement Advertisement](#) and [IS-IS Support for Delay Measurement Advertisement](#).

## Service OAM CFM - IEEE802.1ag

Connectivity Fault Management IEEE802.1ag (CFM) is the OAM mechanism for Ethernet services. CFM is used to monitor connectivity in Ethernet networks that encompass multiple administrative domains. CFM is a joint effort of IEEE, ITU-T, and MEF, designed to help SPs achieve end-to-end network OAM for multidomain networks. CFM facilitates detection of continuity loss or incorrect network connections, connectivity verification, and fault isolation.

CFM defines proactive and diagnostic fault localization procedures for P2P and MP services that span one or more links end-to-end within an Ethernet network. CFM enables detection, verification, localization, and notification of different defect conditions and enables SPs to manage each customer service instance on an individual basis.

## Multidomain Ethernet Service OAM



As illustrated in the preceding figure, CFM descriptions utilize a specific terminology:

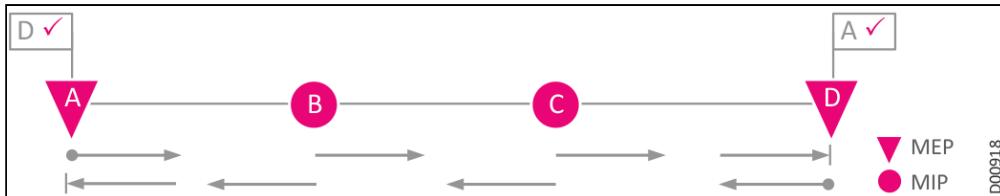
- **Maintenance Entity (ME):** an entity that requires management. May also be referred to as a **Maintenance Point (MP)**.
- **Maintenance Association (MA):** a set of MEs that satisfy the following conditions:
  - MEs in a single MA existing in the same administrative domain and at the same ME level.
  - MEs in a single MA belonging to the same SP VLAN (S-VLAN).
- **MA Endpoint (MEP):** an ME located at the edges or ends of an MA. Each MA must include two MEPs, one at each end, in the administrative domain boundaries. An MEP generates and receives OAM frames.
- **MA Intermediate Point (MIP):** an ME located at intermediate points along the end-to-end path of an MA. A MIP does not initiate OAM frames; it reacts and responds to OAM frames that were generated by the MEPs.

Note that the more generic term **MP** may be used when a description refers to either a **MEP** or a **MIP**.

Ethernet service OAM includes the following fault management techniques:

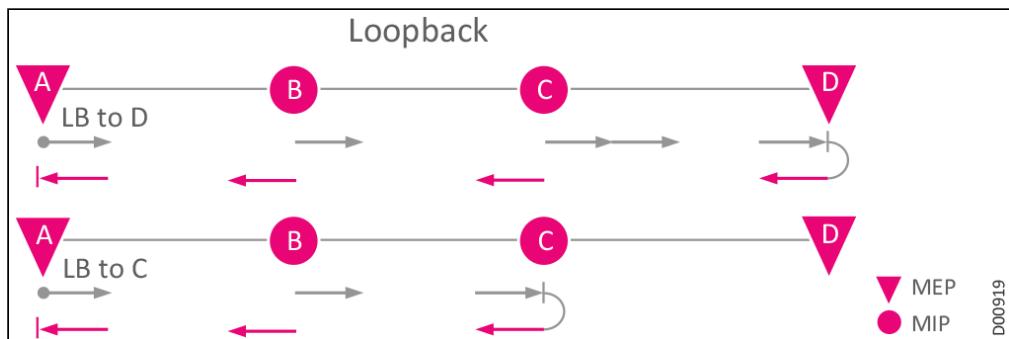
- **Continuity Check:** A simple, reliable, and effective tool for fault detection. These multicast transmissions are transmitted regularly and automatically by each MEP, providing a constant network 'heartbeat' that verifies transmission integrity. If a MEP misses three consecutive 'heartbeats' of transmission from another MEP, the network is immediately alerted to a connectivity problem.

### Continuity Check Functionality



- **Loopback:** A request/response protocol similar to the classic IP Ping tool. MEPs send Loopback Messages (LBMs) to verify connectivity with another MP (MEP or MIP) within a specific MA. The target MP generates a Loopback Reply Message (LBR) in response. LBMs and LBRs are used to verify bidirectional connectivity, and are initiated by operator command.

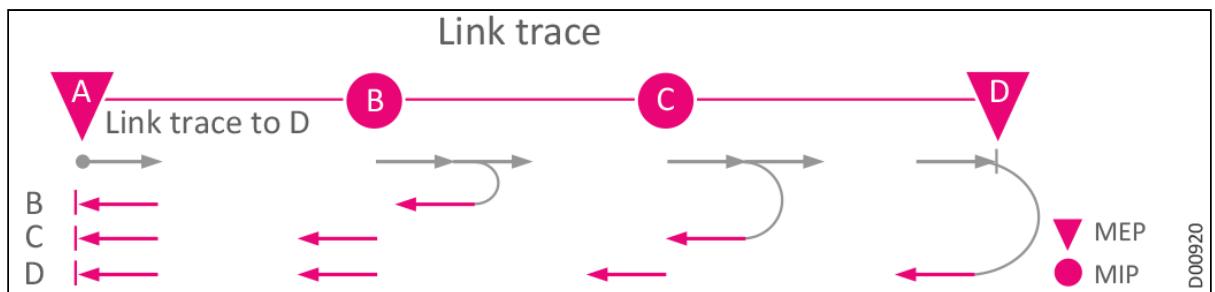
### Loopback



- **Link Trace:** Another request/response protocol similar to the classic IP Traceroute tool. Link trace may be used to trace the path to a target MP (MEP or MIP) and for fault isolation. MEPs send multicast Link Trace Messages (LTMs) within a specific MA to identify adjacency relationships with remote MPs at the same administrative level. When an MP receives an LTM, it completes one of the following actions:

- If the NE is aware of the target MP destination MAC address in the LTM frame and associates that address with a single egress port, the current MP generates a unicast Link Trace Reply (LTR) to the initiating MEP and forwards the LTM to the target MEP destination MAC address.
- Otherwise the LTM frame is relayed unchanged to all egress ports associated with the MA except for the port from which the message was received.

### Link Trace



- **CFM Alarm Management:** Various types of CFM alarms can be received at the service level when Alarms functionality is enabled for an MA.

## CFM-PM Y.1731

The **Y.1731** standard defines Ethernet PM mechanisms for measuring Ethernet service performance (**P2P**, **P2MP** and **MP2MP** services), performed between pairs of MEPs belonging to the same MA. Each pair includes a **Sender MEP** that generates messages, and a **Responder MEP** that replies to them. On MP service MEGs, CFM-PM can be applied to any subset of the pairs of MEPs.

The CFM-PM mechanism covers the following SLA parameters:

- **Frame Delay (FD):** The round trip time that a frame spends on the way to the remote endpoint and back again (2-way trip). FD time includes travel time only. The time that the packet is delayed within the remote MEP is excluded.
- **Frame Delay Variation (FDV):** The difference (delta) between the current FD value and the previous FD value. This measurement also excludes the time that the packet is delayed within the remote MEP.
- **Frame Loss (FL):** The number of frames lost during transmission from the local MEP to the remote MEP, or during the return transmission. FL measurements are based on synthetic traffic.
- **Availability:** The amount of time (in seconds) that service was available between a pair of MEPs belonging to the same MA.

To measure SLA parameters, synthetic frames are periodically generated by a local MEP towards a remote MEP along the same path as the service frames. The remote MEP replies with synthetic loss reply frames, which are then used by the local MEP for calculating performance.

CFM-PM quality standards can be tailored to the type of service through user-defined profiles. Settings for transmission period, frame size and minimum performance threshold can be configured by the user.

CFM-PM (Y.1731) performance management operations are configured through the **Performance Management** windows. The selected service name appears at the top of the window. For example, you would configure a DM session through the **Set DM Session** pane, used to define a new DM session or to reconfigure an existing DM session.

### Set DM Session Pane

The screenshot shows the 'Set DM Session' pane. It includes fields for 'DM Period' (set to 1000) and 'DM FrameSize' (set to 1500). Below these are tables for 'DM Session Parameters' and 'DM Session MEPs'. The 'DM Session MEPs' table lists two entries:

Role	MEP ID	LE Name	MAC Address	Status	DM Period	DM FrameSize
Sender	8190	NE_2-TS1:DMGE_4_L2-200	00:00:02:08:1A:00	Disabled	1000	1500
Respon...	8189	NE_1-TS1:DMGE_4_L2-100	00:00:01:08:1A:00	Disabled	1000	1500

At the bottom, there are buttons for 'Select Sender', 'Select Responder', 'Clear', and checkboxes for 'Auto Select Roots', 'Auto Select Leaves', and 'Auto Select all Unselected MEPs'. A 'Session Operations' section contains 'Apply', 'Enable', and 'Disable' buttons.

## Throughput RFC 2544

Customer SLAs dictate performance criteria requirements, usually regarding verifiable network availability and mean-time-to-repair values. Generally, Ethernet performance criteria can be difficult to prove; demonstrating performance availability, transmission delay, link burstability, and service integrity cannot be accomplished accurately through PING commands alone.

IETF's RFC 2544 standard (*Benchmarking Methodology for Network Interconnect Devices*) outlines the tests required to measure and prove performance criteria for carrier Ethernet networks. The standard provides an out-of-service benchmarking methodology to evaluate the performance of network devices using throughput, back-to-back, frame loss and latency tests, with each test validating a specific part of an SLA. The methodology defines the frame size, test duration and number of test iterations. Once completed, these tests provide performance metrics of the Ethernet network under test.

The **throughput** test defines the maximum amount of data, measured in number of frames per second, that can be transmitted from source to destination without any error. This test involves starting at a maximum frame rate and then comparing the number of transmitted and received frames. Should frame loss occur, the transmission rate is divided by two and the test is restarted. If during this trial there is no frame loss, then the transmission rate is increased by half of the difference from the previous trial. This methodology is known as the half/doubling method. This trial-and-error methodology is repeated until the highest rate at which there is no frame loss is found.

The throughput test must be performed for each frame size. The test time during which frames are transmitted must be at least 60seconds. Each throughput test result is recorded in a report, using frames per second (f/s or fps) or bits per second (bit/s or bps) as the measurement unit.

## SLA Y.1564

ITU's Y.1564 standard (*Ethernet service activation test methodology*) defines a test methodology used to assess the proper configuration and performance of an Ethernet network delivering Ethernet-based services. This out-of-service test methodology was created to standardize Ethernet-based service performance measurement, enabling verification of SLA compliance.

What makes this standard unique is that it allows for complete validation of Ethernet SLA in one test, including:

- Ensuring that the network complies with SLA requirements by ensuring that a service meets its **key performance indicators (KPI)** at different rates, within the committed range.
- Ensuring that all services carried by the network meet their KPI objectives at their **maximum committed rate**, validating that under maximum load the network devices and paths are able to service all the traffic as designed.
- Confirming that network elements can properly carry all services while under a significant load **extended over a significant period of time** (sometime referred to as a soaking test).

Y.1564 supports current service provider offerings, which typically consist of multi-services. Y.1564 allows them to simultaneously test all services and measure if they qualify to the committed SLA attributes. On top of that it also validate the different QoS mechanisms provisioned in the network to prioritize the different service types - allowing service providers faster deployment (as the need for repeated tests is eliminated) and easier service and network troubleshooting.

Y.1564 allows for very high flexibility in simulating testing scenarios that are very close to the real active network traffic. It defines test streams (or "flows") with service attributes aligned with MEF10.2 definitions. These test flows can be classified using various mechanisms such as 802.1qVLAN, 802.1ad, DSCP, and CoS profiles. Services are defined at the UNI level with different frame and bandwidth profiles, such as the service's MTU or frame size, CIR, and EIR settings, with up to five different frame sizes in single test.

## sFlow RFC 3176

sFlow is a packet sampling technology that can be implemented in a broad range of networking devices, from Layer 2 switches to high-end core routers. Due to the introduction of high-speed networks, packet sampling has become widely recognized as the most scalable, accurate, and comprehensive solution for network monitoring. By providing unprecedented visibility into network usage and active routes of even today's high-speed and complex networks, sFlow provides the data required to effectively control and manage network usage, ensuring that network services provide a competitive advantage.

Several different technologies have been employed to monitor network traffic, such as sFlow, NetFlow, Remote Network MONitoring (RMON I and II), and SMON (a set of MIB extensions to RMON). Although both sFlow and NetFlow are used for traffic monitoring, sFlow has many benefits over NetFlow.

- **Support for all network layers:** sFlow is an industry standard (RFC 3176), which can be used across multiple platforms supporting diverse protocols. The generic format of the sFlow packet allows it to work on all layers of the network stack from Layer 2 to Layer 7, installed on both switches and routers. NetFlow works only on IP routers on Layers 3 and 4 of the network stack. Although some recent extensions have been released to support Layer 2 in NetFlow version 9, support for switching technology is mostly incomplete.
- **Superior processor and resource utilization:** The superior sampling technology used by sFlow reduces processor load on routers and switches and provides an accurate representation of the network traffic for monitoring, accounting, billing, network planning, and traffic engineering. Since NetFlow caches information in the router and sometimes also forwards packets in software, it imposes a much higher load on processor and memory resources. Sorting algorithms implemented on the

NetFlow cache to match each packet to its NetFlow flow also significantly increase processor utilization rates. For example, CPU utilization could go as high as 70% in some routers for larger numbers of flows. Because of NetFlow's higher processor and memory resource requirements, it cannot be used for higher speed interfaces. Other applications on the router also suffer when NetFlow is enabled because of the resources (memory, CPU, CAM entries, and so on). In addition, NetFlow suffers from inaccuracies when there is a high load on the processors.

- **Real-time monitoring:** sFlow provides accurate statistics in real time, essential to prevent security attacks such as Denial of Service (DoS) and meet QoS guarantees. It is also useful to determine historic network load for trending and network planning. Since sFlow does not cache and aggregate flow data or spend time processing data inside the router, the statistics are provided real time. However, NetFlow does not separate processing of data from its export and therefore is not working in real time.
- **Standards-based:** sFlow is a standard defined in RFC 3176. The [sFlow.org](#) consortium that develops the sFlow standard includes most of the leading network equipment and network traffic analysis vendors. Most packet-processing ASICs support the sFlow standards. NetFlow, on the other hand, is a proprietary, single-vendor technology. One vendor alone decides on its future enhancements. Although there have been recent efforts to include NetFlow specifications within a standard called IP Flow Information Export (IPFIX), which emphasizes the exporting of flow information, IPFIX suffers from poor vendor adoption and still has most of the deficiencies of NetFlow.
- **Ease of configuration:** sFlow has superior configuration capabilities and can be configured through SNMP. Sampling rates can be set on every interface. NetFlow, on the other hand, does not support sampling on most versions. Version 9 supports sampling, but only allows a global sampling rate to be set. sFlow is a cheaper technology to develop, since it is supported in ASICs and processed outside the router or switch, and these savings are passed on to customers.

Traditional technologies such as NetFlow have focused on analyzing each packet and embedding traffic monitoring inside routers. This methodology impacts the performance of the router (especially at high traffic speeds) and leads to inaccurate results. sFlow samples packets, but separates traffic analysis from traffic sampling. While the sampling logic is embedded inside the network element (for example, the router or switch), traffic analysis is actually performed on a separate machine (typically a server). This allows for both larger scale and real-time responsiveness.

sFlow data can be used for effective:

- Detecting, diagnosing, and fixing network problems  
The first hint of a network problem is often found in abnormal traffic patterns. sFlow makes these abnormal traffic patterns visible, with sufficient detail to enable rapid identification, diagnosis and correction.
- Real-time congestion management  
sFlow can be used to instantly highlight congested links, identifying the source of the traffic and the associated application level conversations. sFlow provides the necessary information to determine effective controls, such as which traffic to rate control or prioritize or where to provision more bandwidth.
- Security and audit trail analysis  
Because attacks and security threats usually come from unknown sources, effective security monitoring requires complete network surveillance, with alerts to suspicious activity, to immediately identify unauthorized network activity and trace the sources of denial-of-service attacks. When sFlow is used to build a detailed traffic history, a baseline of normal behavior is established, from which anomalies can quickly be detected and suspicious activity identified.
- Usage accounting for billing and charge-back
- Route profiling and peering optimization
- Trending and capacity planning

sFlow has become an industry standard for providing a network-wide view of usage and active routes, with interoperable implementations provided by a wide range of network equipment and software application vendors. sFlow provides a scalable technique for measuring network traffic, collecting, storing, and analyzing traffic data. This enables tens of thousands of interfaces to be monitored from a single location.

sFlow provides a scalable methodology, enabling it to monitor links of speeds up to 10Gb/s and beyond without impacting the performance of core internet routers and switches, and without adding significant network load. Since it is a low-cost solution, sFlow has been implemented on a wide range of devices, from simple L2 work-group switches to high-end core routers, without requiring additional memory and CPU.

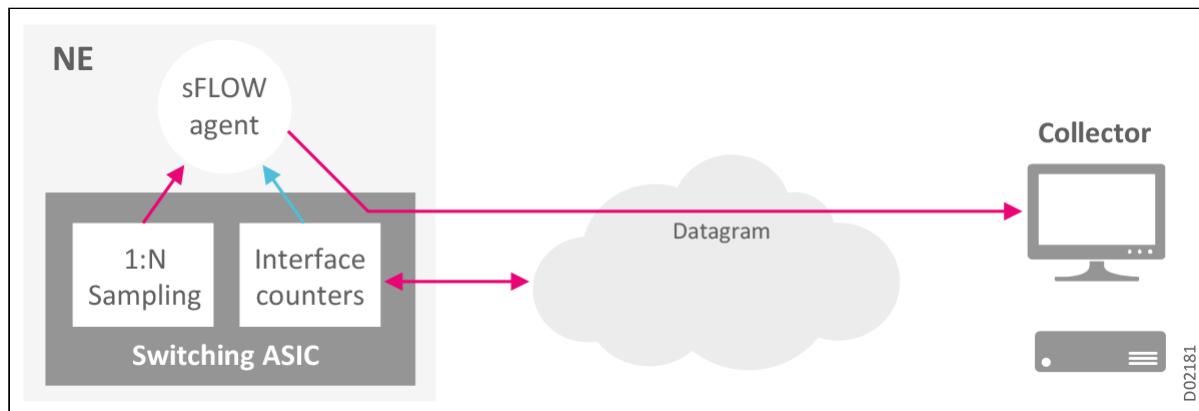
The sFlow monitoring system consists of an sFlow Agent (embedded in a switch or router) and a central sFlow Collector.

- The sFlow Agent is a software process that runs as part of the network management software within the network element. sFlow Agents in routers and switches throughout the network continuously capture traffic and statistics from the devices and send a stream of sFlow Datagrams to a central sFlow Collector.
- sFlow Datagrams are combinations of statistics and flow samples collected by the sFlow Agents. Datagrams require very little processing. Data is packaged into sFlow Datagrams, which are immediately sent on the network. This minimizes the load on sFlow Agents' memory and processor.
- The sFlow Collector software analyzes the Datagrams received from each sFlow Agent and presents a real-time, network-wide view of traffic flows.

The following figure illustrates how the sFlow Agent and Collector work together to collect the necessary data:

1. The sFlow instances associated with individual data sources perform packet flow and counter sampling.
2. The packet flow sampling instance is configured with a sampling rate, and a packet flow record is generated.
3. The counter sampling instance is configured with a sampling interval, and a counter record is generated.
4. The sFlow Agent collects counter records and packet flow records and sends them in the form of Datagrams to sFlow Collectors.

### sFlow Agent and Collector



Neptune supports sFlow sampling per interface on a single port or LAG. The sFlow sampling interval is configured per sFlow instance. The maximum total packet sampling rate is configured per device. Users can define up to 3 separate sFlow sampling profiles, including:

- Sampling probability (0.000-100.000 @0.001%)
- Packet truncation option (truncate after the first 64/128/192 Bytes, or don't truncate). Note that the control plane may further truncate the packet based on other configuration settings.

## SNMP v2-v3

Simple Network Management Protocol (SNMP) is used for monitoring and management of network devices. Neptune platforms support the following versions of SNMP:

- Simple Network Management Protocol version 2 (SNMPv2)

- Simple Network Management Protocol version 3 (SNMPv3)

Neptune platforms support polling of statistics counters via the SNMP protocol; please refer to the *Neptune MIB Reference Manual* for the relevant object definitions.

### **SNMP Notifications**

A key feature of SNMP is the ability to generate notifications from an SNMP agent; these notifications can be generated as traps. Traps are messages alerting the SNMP management server to a condition occurrence or KPI violation on the network. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighboring router, or other significant events.

Neptune platforms can alert the upper layer management systems upon a state change of the routing protocols or environmental events, via SNMP notification traps. Examples of such SNMP trap notifications include:

- LDP session state change
- BGP session state change
- IGP adjacency state change
- Temperature TCA crossing
- Routing table overflow condition

## **Link Layer Discovery Protocol LLDP**

The Link Layer Discovery Protocol (LLDP - 802.1AB) standard defines a protocol and management elements suitable for advertising information to stations attached to the same 802 LAN, in order to populate the physical topology and device discovery management information databases. LLDP facilitates identification of stations connected by IEEE 802 LANs/MANs, their points of interconnection, and access points for management protocols.

LLDP is a one-way protocol with periodic retransmissions out each port (30 sec default). Frames are sent to a Layer-2 BPDU address that isn't forwarded by bridges. The frames contain formatted records (TLVs), including:

- Mandatory Chassis-ID and Port-ID TLVs to identify stations
- Mandatory Time-to-live information for aging purposes
- Optionally includes additional device describing TLVs such as the management address and system name
- Optionally includes Organization Specific TLVs (defined by the organizations themselves, such as IEEE 802.1, IEEE 802.3, TIA, etc.)
- Mandatory End-of-PDU TLV to consistently mark the end of processing

Participants populate mandatory and other optional Local MIBs as needed, and advertise to the far end. Receivers hold received records in Remote MIBs and age appropriately. Management entities and other applications may make decisions based upon received data. All advertised information ages together. Multiple different LLDP advertisements on same port are not allowed.

LLDP is highly useful for:

- Topology discovery
- Network troubleshooting
- Network management automation

# Ensuring Quality of Experience QoE

Quality of Experience (QoE) for a network operator or service provider must include a wide range of aspects, including traffic management, performance, quality of service (QoS), hierarchical scheduling, and a sophisticated DiffServ architecture. These aspects are introduced in this section.

- Traffic Management and Performance Overview
- Quality of Service QoS Overview
- Ingress Traffic Management
- Hierarchical Scheduling
- DiffServ Architecture Overview

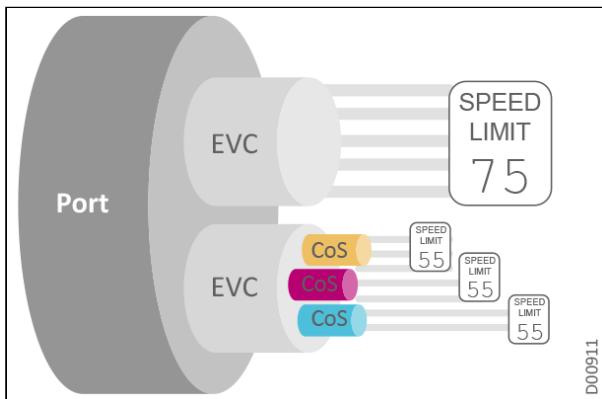
## Traffic Management and Performance Overview

Intelligent TM enables reliable provision of different SLA levels. For example, policer profiles encapsulating the bandwidth parameters defined for Ethernet services are one of the tools used by TM, allowing greater flexibility when managing different customer scenarios. Bandwidth allocations and traffic priority can be configured per ingress or egress UNI ports, as well as per port, per EVC, and per CoS.

The Neptune supports three types of queue scheduling mode, with each port handling up to eight CoS queues:

- **Strict Priority:** Higher priority queues are entitled to utilize all the bandwidth allocated to that port. Packets of lower priority are only transmitted when the higher priority queue is empty.
- **Weighted Round Robin (WRR):** Packets in all queues are sent in order based on the weighted value of each queue.
- **Enhanced (Strict Priority + WRR [SPQ]):** The port's eight queues are organized into two groups, based on the CoS delimiter configured by the user. Strict Priority mode is applied to scheduling decisions between queues in the higher priority group and queues in the lower priority group. WRR mode is applied to scheduling decisions between queues within the same priority group. Enhanced mode is configurable on PB based ports. MPLS ports are automatically set to Enhanced mode.

### Traffic Management with Policer Profiles



Some of the TM tools utilized by the Neptune platforms include:

- **Classification:** A method for categorizing network traffic CoS upon ingress and marking packets upon egress. Neptune platforms support classification based on C-VLAN as well as Differentiated Services (DiffServ) Code Point (DSCP for IPv4 and IPv6), implemented on ingress and egress for both IP and non-IP traffic. DSCP implementation enables TM that skillfully incorporates DSCP capabilities wherever DSCP is in use.
- **Policing:** TM in the Neptune utilizes two-rate three-color policing to achieve a notable combination of efficiency and flexibility, supporting CIR, EIR, Committed Burst Size (CBS), and Excess Burst Size (EBS) traffic categories. Intelligent bandwidth management enables profile enhancement capabilities

that improve handling of 'bursty' traffic as well. Bandwidth management profiles are extended based on MEF5 standards. Policing is implemented on both the ingress and egress sides, allowing greater flexibility when managing different customer scenarios.

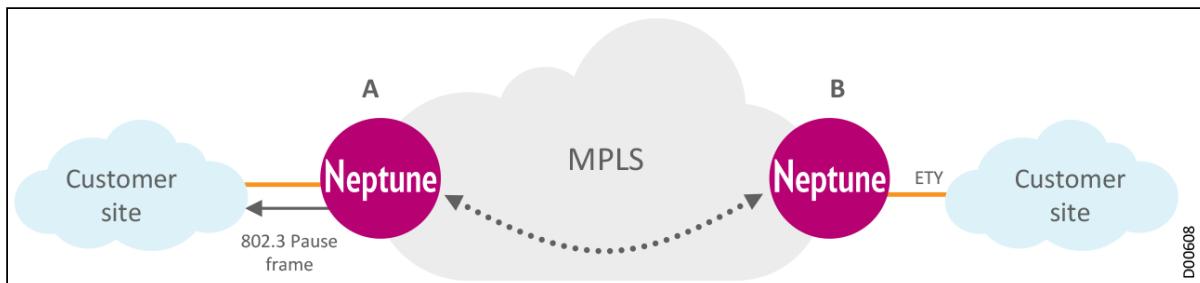
- **Strict TM:** QoS is implemented on a per-flow basis, with SPQ between two CoS groups, high and low. This service ensures that each traffic queue receives its guaranteed bandwidth and other resources while simultaneously allocating extra available bandwidth fairly among the queues. The TE manager implements buffer management (WRED), scheduling (WFQ), shaping, and counting on a three-level hierarchy per port, per class, and per tunnel.
- **DiffServ TM:** QoS is implemented on a per-port basis. This method bypasses the hierarchical approach of Strict TM. DiffServ TM improves scalability by dividing traffic into a small number of classes, and allocating resources on a per-class basis.

#### Tip

Neptune platforms allow you to configure both TM models within a single port, increasing the service options available to network operators. Some of the port LSPs can be configured with Strict TM, and other LSPs in the same port can be configured with DiffServ TM.

- **Flow control with frame buffering** (802.3x) reduces traffic congestion. When the input buffer memory on an Ethernet port is nearly full, the data card sends a 'Pause' packet back to the traffic source, requesting a halt in packet transmission for a specified time period. After the period has passed, traffic transmission is resumed. This approach gives the overloaded input buffer a little 'breathing room' while the card clears out the input data and sends it on its way. The following figure illustrates an NE sending a 'Pause' packet to the link partner.

#### Pause Frame Example



## Quality of Service QoS Overview

MPLS, together with Connection Admission Control (CAC) and Traffic Engineering (MPLS-TE), support guaranteed end-to-end SLAs for business, mobile, and residential users. This level of QoS enables efficient differentiated services (DiffServ), allowing service providers to tailor the level of service and performance to the requirements of their customers (real-time, mission-critical, best-effort, etc.), as well as assuring the necessary network resources for CIR and EIR. Built-in TM capabilities support the following QoS mechanisms:

- **Hierarchical QoS** enables fine tuning of traffic flow based on a structured approach and a finer granularity of traffic categorization.
- **Eight CoS levels** per port used for service differentiation, maximizing SLA diversity and optimizing packet handling throughout the network. Each CoS can be assigned a scheduling priority.
- **Auto Queuing**, with 64K queue traffic manager, for true end-to-end bandwidth guarantees per MPLS tunnel.
- **Auto WRED** mechanism for TCP-friendly congestion management. Optional manual WRED, where user can configure WRED curves and assign them per CoS on both MPLS and non-MPLS ports.
- **Auto Shaping** that provides rate limiting and burst smoothing. Optional manual shaping, where user can configure committed and excess rate limits per CoS on non-MPLS ports.

- **Auto Weighted Fair Queuing (WFQ) scheduling** mechanism, ensuring that bandwidth is distributed fairly between individual queues. Optional manual scheduling, where user can configure weight per CoS per switch.

## Ingress Traffic Management

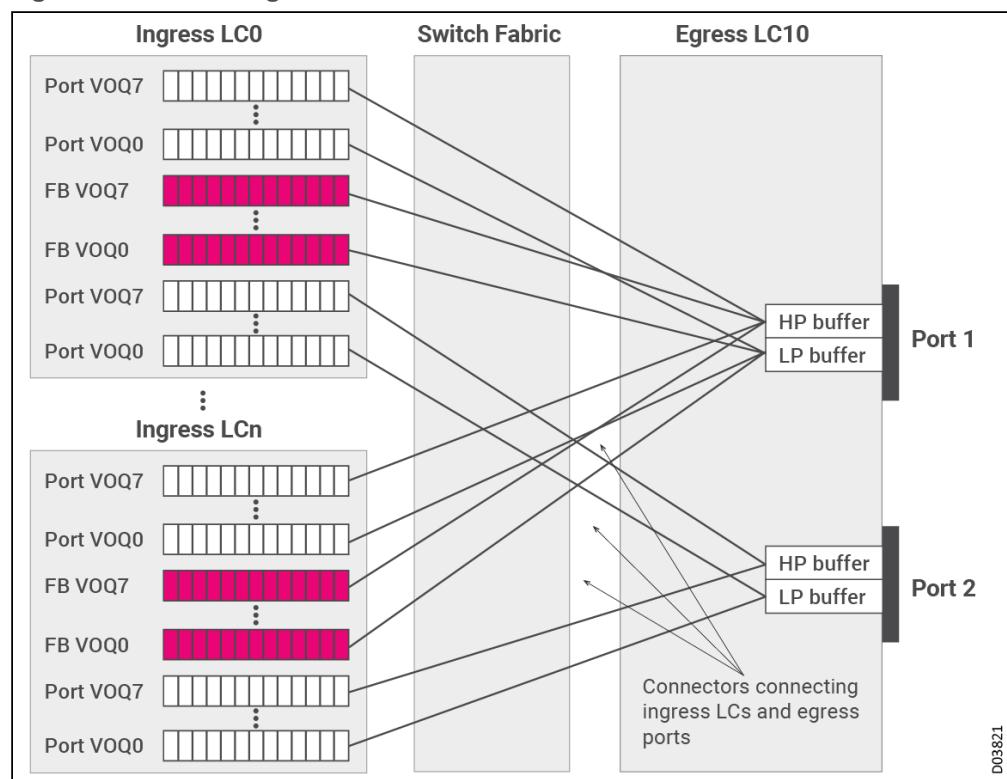
The ingress TM model relies on packet queuing in Virtual Output Queues (VOQs) at the ingress line card (LC). In this model, buffering takes place at the ingress network processing unit (NPU) of each LC.

Each ingress LC supports 8 CoS VOQs per physical port. You assign a flow block (FB) per egress logical interface (LIF) to ensure bandwidth for each specific LIF, in which case the ingress LC also sets 8 CoS VOQs per FB.

Each CoS is assigned a priority, based on the CoS delimiter per NE. Neptune schedules packets from CoS VOQs according to the defined priority, as described in the following table:

Priority	CoS VOQs
High Priority (HP)	CoS 6 and CoS 7
Low Priority (LP)	CoS 0 through CoS 5

### Ingress Traffic Management Model



As the preceding figure illustrates, every ingress LC (LC1 to LCn) has 8 Port VOQs for each outgoing port (Port1 and Port2) on the single egress line card LC10. In this example, the user also assigned an FB to the egress LIF (for example, defined FB1000 for the LIF on LC10 Port1). In this case, every ingress LC also has 8 VOQs for this FB.

To transmit packets:

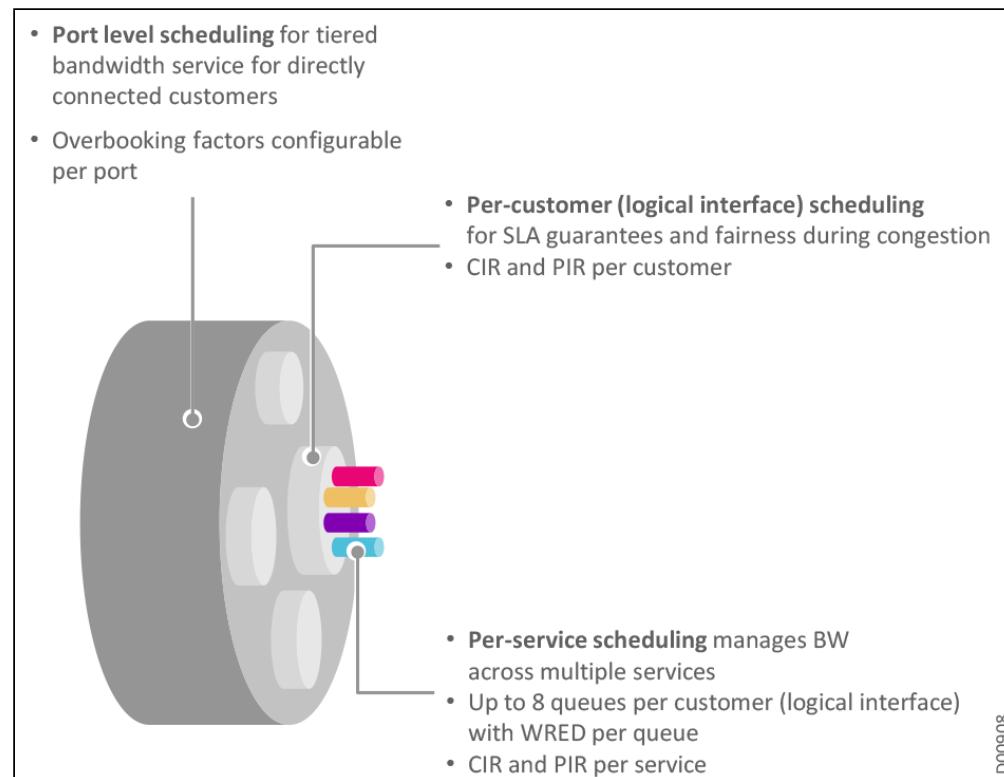
1. When a packet arrives at an ingress LC (for example, on LC0), it is assigned (classified) to one of the 8 CoS options (for example, CoS0). In addition:
  - a. The forwarding lookup on the ingress line card points to the egress port (for example, Port1 of LC10).
  - b. Based on the CoS and egress port, the packet is enqueued to the VOQ0 that sends traffic to LC10 Port1.
  - c. When the forwarding lookup points to a LIF to which you assigned an FB (for example, FB1000 on LC10 Port1), the packet is enqueued to the VOQ0 of that FB.
2. Once egress bandwidth is available, the HP or LP egress buffer on the LC10 port that is ready to receive the packets sends permission (*a grant*) to the HP or LP ingress VOQs respectively, via the connectors, providing that grant was requested from these VOQs.
3. The ingress VOQs respond to this grant by transmitting the packets via the switch fabric to the LC10 port.

The VOQ model thus operates on the principle of storing excess packets in buffers at ingress until bandwidth becomes available. This is a more efficient model, since depending on the congestion that builds up and the configured threshold values, packets begin to drop at the ingress itself, instead of having to travel all the way to the egress port and then getting dropped.

## Hierarchical Scheduling

Neptune supports a mix of latency-sensitive, loss-sensitive, and best effort service flows for thousands of triple play subscribers. This requires a QoS mechanism that can classify thousands of network flows and direct them to the appropriate queues and schedulers on each customer interface. To meet this need, Neptune utilizes a dedicated DiffServ classification and queuing mechanism for each of its thousands of subscribers.

### Hierarchical Scheduling: Per Port, Per Customer, Per Service

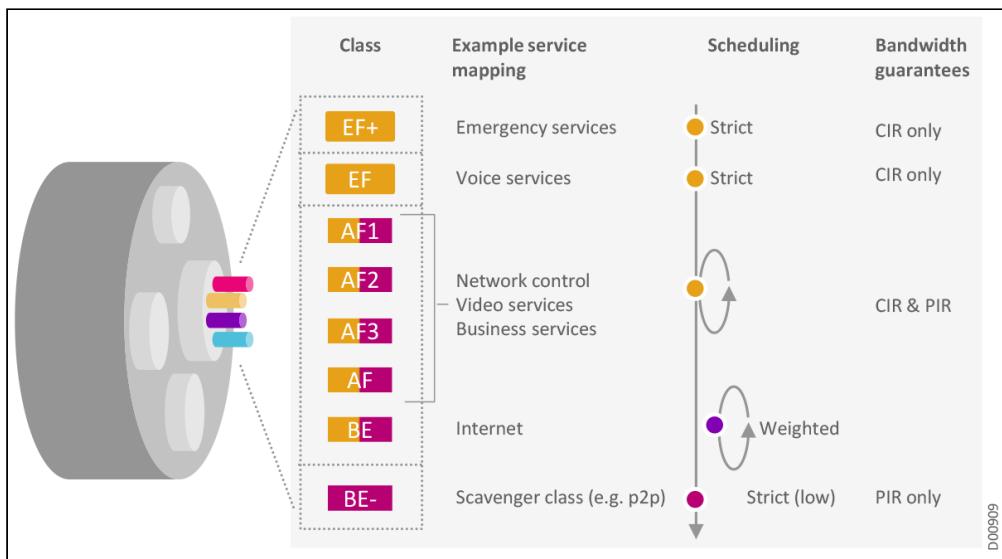


Commonly used DiffServ classification methods define how to prioritize and weight the classes that share a link. But they offer no real guarantees that traffic belonging to a specific class receives its required

throughput. This is not enough for SPs, who are not interested in clever traffic priority assignments. SPs need to know that a service that is guaranteed to be delivered will in fact be delivered as expected.

Therefore, the **Neptune H-QoS model improves on DiffServ techniques by offering guaranteed throughput with separate bandwidth profiles per customer**, including CIR scheduling with frame delivery obligations per SLA, EIR/PIR with excess frame delivery allowed, not subject to SLA, and Committed/Excess Burst Size (CBS/EBS) for CIR/EIR.

### Bandwidth Management Per Customer



Neptune supports **all MEF TM models**, including port-based, port/VLAN-based, and port/VLAN/CoS-based.

## DiffServ Architecture Overview

Traditionally, enterprise grade Ethernet switches have focused on best effort Ethernet connectivity rather than stringent SLA-bound services. As SPs move to offering more services over their Ethernet-based residential networks, service resiliency becomes a critical factor in ensuring subscriber QoE.

With the stringent requirements of Carrier Ethernet in mind, the Neptune was designed to provide high availability that exceeds the five 9s standard. Neptune platforms are based on a carrier class design that includes a completely nonblocking switch fabric as well as fully redundant common components. To minimize network outages and improve service resiliency, the Neptune delivers advanced features such as hitless card insertion and removal, hitless software upgrade, and nonstop forwarding.

The differentiated service (DiffServ) concept is a well-known priority-marking scheme used in IP packet networks, based on a set of forwarding behaviors called Per-Hop Behavior (PHB). These behaviors are in turn organized into a PHB Scheduling Classes (PSC) framework and are associated with relative priority markings, called DiffServ Code Points (DSCP), carried in the IP header. These PHBs in essence represent the underlying QoS mechanism or packet forwarding treatment within a node. Neptune platforms apply the IETF DiffServ Architecture (RFC 2475) across all network layers, utilizing classification mechanisms like MPLS Traffic Class (TC) bits, IP DSCP, and IEEE 802.1p for implementing the DiffServ PHBs in use.

In a transport network, congestion can occur anywhere. However, congestion is more likely where statistical estimates of peak demand are conservative (that is, under-provisioned), which happens more often on the design of access and aggregation bandwidth links. Congestion due to instantaneous ingress bandwidth to a node exceeding egress bandwidth (assuming the node can process all ingress bandwidth) therefore requires all nodes to be able to implement DiffServ scheduling functions. The result is that the under-provisioning is unfairly distributed among the services transported. This redistribution with DiffServ can result in over-

provisioning for higher quality services (such as voice over IP [VoIP] and video) and differing levels of under-provisioning for other services. This is in line with the functional requirements defined by standards bodies, such as the NGMN and Broadband Forum TR-221 specification for mobile backhaul, and TR-101 for Ethernet-based aggregation networks for residential and business services.

This section introduces the following features:

- Layer 3 Classification
- MPLS TC to DSCP Mapping

## Layer 3 Classification

Classification rules are similar to firewall filters. They have an order and are processed in a sequential manner. Classification results in the application of a service profile to the packet.

Layer 3 (IP) packets are traditionally classified through one of the following methods:

- **ToS/DiffServ Classification:** Examines the IPv4 terms of service (ToS) or the DSCP field in an IP header to provide per-hop classification.
- **Multifield Classification:** Examines multiple fields in an IP header, usually those that identify an IP flow. This method provides for a more flow-based classification.

DiffServ is a well-known service model that relies on routers using markers and multifield classifiers at the edge of a network to map packets to a small set of traffic behaviors in the core. Network-wide context is provided to packets by routers setting a packet's DSCP field. Based upon the contents of the DSCP field, core routers provide per-hop QoS for the traffic.

The DSCP field is 8 bits long, but only the first 6 bits are currently used. The DSCP field replaces the ToS field.

There are three classes of traffic defined by DiffServ:

- **Best Effort (BE):** Applied to all normal, best effort traffic traversing the network. This traffic has no service expectations. It therefore receives the lowest priority and service within the core. Best effort traffic receives a DSCP code of 000000.
- **Expedited Forwarding (EF):** Designed for traffic that requires low loss, low latency, and low jitter, such as real-time video or voice. Edge routers usually police to limit the rate of EF traffic before it enters the core. To prevent traffic delays in the core, core routers service EF packets at a rate that exceeds the aggregate expected arrival rate of the traffic. The DSCP code for EF is 101110.
- **Assured Forwarding (AF):** To allow for flexibility when sharing resources, the AF class is actually a group of traffic classes for several different levels of service. The class defines the level of service provided by specifying the availability of relative bandwidth and packet drop characteristics. DSCP defines two classification elements:
  - **Service class:** Used to select a queue.
  - **Drop precedence:** Weights RED-like behavior by specifying three drop probabilities: low, medium, and high.

Because AF uses drop precedence, DiffServ routers use an independent RED-like scheduler to keep flow congestion to a minimum, while allowing for short-term burstiness in the flow.

## MPLS TC to DSCP Mapping

The traffic classification, marking, and DiffServ PHB behaviors considered in the system architecture, which are depicted in the following table, are targeted to fit the deployment of residential, business, and mobile services. Traffic across all three services is divided into the following categories:

- Expedited forwarding (EF)
- Assured forwarding (AF)
- Best effort (BE)

### DSCP/DiffServ PHB Mapping

DSCP	DiffServ PHB	Ethernet P-bits
46	EF	7
36	AF42	5
26	AF31	3
46	EF	7
34	AF41	4
28	AF32	3
18	AF21	2
10	AF11	1
0	BE	0

Traffic marked as expedited forwarding (EF) is grouped in a single class serviced with priority treatment to satisfy stringent latency and delay variation requirements. The EF PHB defines a scheduling logic able to guarantee an upper limit to the per hop delay variation caused by packets from non-EF services. This category includes residential voice and business real time traffic, mobile network timing synchronization (1588 PTP), and mobile signaling and conversation traffic (GSM Abis, UMTS Iub control plane and voice user plane, LTE S1-c, X2-c, and the LTE guaranteed bit rate (GBR) user plane).

Traffic marked as assured forwarding (AF) is divided over multiple classes. Each class is guaranteed a predefined amount of bandwidth, thus establishing relative priorities while maintaining fairness among classes and somewhat limiting the amount of latency traffic in each class may experience. Neptune platforms support five AF classes, two of which are reserved for network traffic, control, and management, and the remaining three are dedicated to traffic from residential and business services, such as residential TV and video distribution, and business TelePresence and mission-critical applications.

The third category, best effort (BE), encompasses all traffic that can be transmitted only after all other classes have been served within their fair share. This is traffic that is neither time nor delay sensitive and includes residential H.323 signaling interface (HSI), business best effort, mobile background, and video-quality experience control traffic.

For Ethernet UNI interfaces, upstream traffic classification is based on IP DSCP or 802.1P CoS markings. The ingress QoS service policy will match on these markings and map them to the corresponding DSCP and/or MPLS TC value, depending on the access NNI being Ethernet or MPLS-based. In the downstream direction, IP DSCP markings are preserved and may be used for queuing and scheduling at the UNI as well as for restoring 802.1P CoS values.

Specifically to mobile services, SDH UNI interfaces transported via CEoP pseudowires require all traffic to be classified as real-time with EF PHB. The ingress QoS service policy matches all traffic inbound to the interface, and applies an MPLS TC value of 5. No egress service policy is required for SDH UNI interfaces.

For an access NNI and in upstream direction, classification is based on IP DSCP or Ethernet ToS markings. The ingress QoS service policy will match on these markings, which are retained when forwarding toward the

core. In the downstream direction, IP DSCP or MPLS TC markings are preserved and can be used for queuing and scheduling toward the access NNI.

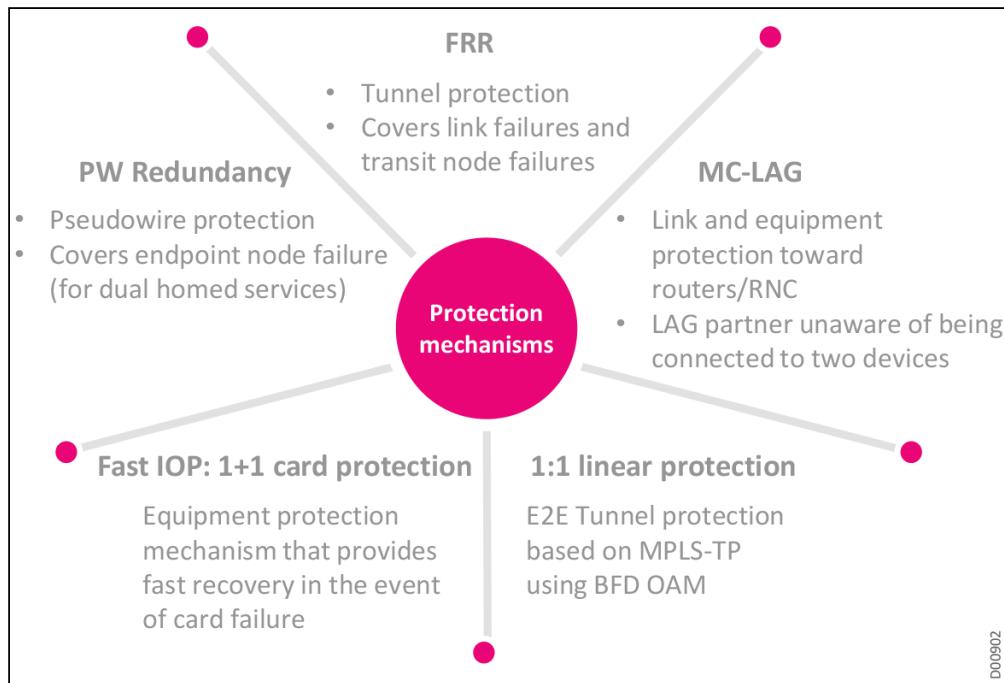
All the remaining core, aggregation, and access network traffic classification is based on MPLS TC or IP DSCP. RFC 5127 'Aggregation of DiffServ Classes' (2008) is an informational RFC which proposes to aggregate or map the twelve DiffServ classes of service into four aggregate classes of service. The following table, extracted from RFC 5127, introduces a recommendation for the inter-layer CoS alignment or mapping to the MPLS TC field (formerly known as EXP bits) of the MPLS label transporting the IP packet.

**RFC 5127 DiffServ Mapping to MPLS TC**

<b>4 Classes of Service Aggregate</b>	<b>Service Class Name</b>	<b>PHB</b>	<b>DSCP</b>	<b>MPLS TC</b>
<b>Network control</b>	Network control	CS6	110000	110
	Telephony	EF	101110 (46)	
	Signaling	CS5	101000 (40)	
	Multimedia conferencing	AF41	100010 (34)	
<b>Real-time</b>		AF42	100100 (36)	100
		AF43	100110 (38)	
	Real-time interactive	CS4	100000 (32)	
	Broadcast video	CS3	011000 (24)	
	Multimedia streaming	AF31	011010 (26)	010 (2)
		AF32	011100 (28)	011 (3)
		AF33	011110 (30)	
	Low-latency data	AF21	010010 (18)	010 (2)
<b>Assured elastic</b>		AF22	010100 (20)	011 (3)
		AF23	010110 (22)	
	OAM	CS2	010000 (16)	010 (2)
	High-throughput data	AF11	001010 (10)	010 (2)
		AF12	001100 (12)	011 (3)
		AF13	001110 (14)	
<b>Elastic</b>	Standard	DF	000000 (0)	000 (0)
	Low-priority data	CS1	001000 (8)	001 (1)

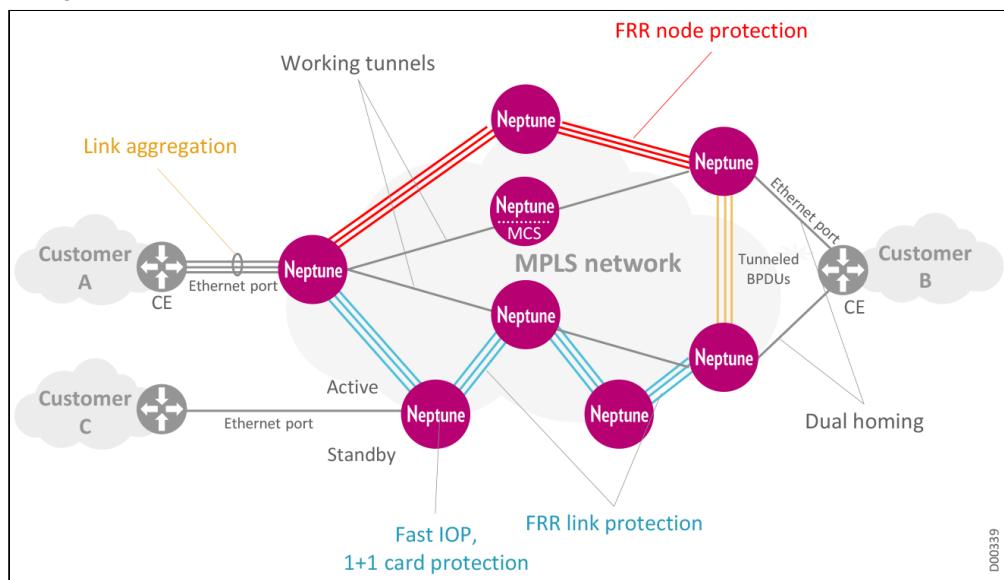
# Neptune Protection and Restoration Mechanisms

## Neptune Protection Mechanisms



The following figure shows an MPLS network that incorporates an end-to-end combination of protection schemes to provide protection at every point. Protection mechanisms incorporated into the figure include sub-50msec FRR link and node protection described in the following sections, as well as Link Aggregation LAG, Dual-homed device protection in H-VPLS networks, and Fast IOP: 1+1 card protection.

## Comprehensive MPLS Protection



Neptune platforms provide protection at every network level. Network operators can choose from a range of **Network-level**, **IP/MPLS**, **MPLS-TP**, **PB**, and **equipment** protection schemes, creating a protective structure tailored to their specific network configuration and functionality.

This section introduces the following features:

- LSP Tunnel Restoration
- LDP FRR with Loop-Free Alternatives LFA
- Object Tracking
- Linear Protection
- PW Redundancy
- Hierarchical VPLS Services
- PW Redundancy for H-VPLS DH Topology
- Multi-Segment PW
- FAT: PW Load Balancing
- Link Aggregation LAG
- Multichassis LAG MC-LAG Protection
- Dual Homing DH
- Link Loss Carry Forward LLCF
- Customer Change Notification CCN
- Resilience and High Availability
- High Availability through Nonstop Forwarding
- Ethernet Ring Protection Switching ERPS PB
- RSTP-MSTP Protection
- Input-Output Protection IOP
- Optical Protection Mechanisms
- Tributary Protection TP Mechanism
- Equipment Protection

CES protection mechanisms are described in the section that focuses on [CES technology](#).

## LSP Tunnel Restoration

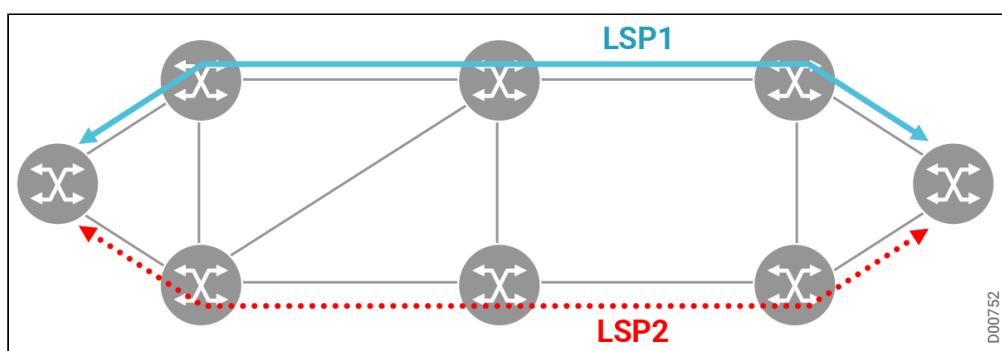
Automatic network restoration capabilities provide valuable protection against multiple failures, assuring network availability over time with efficient hitless restoration. Dynamic restoration capabilities make sure that there is always an alternative route available as soon as it is needed, even if multiple failure cycles are triggered.

In our equipment, dynamic restoration capabilities are supported for bidirectional tunnels. Both protected and unprotected tunnels can be restored. When an automatic switch to protection is triggered, LightSOFT restores the failed LSP and downloads the restoration route to the network. As soon as the failed link is fixed, LightSOFT reverts the restored LSP back to the originally provisioned LSP and downloads the restored (original) route to the network.

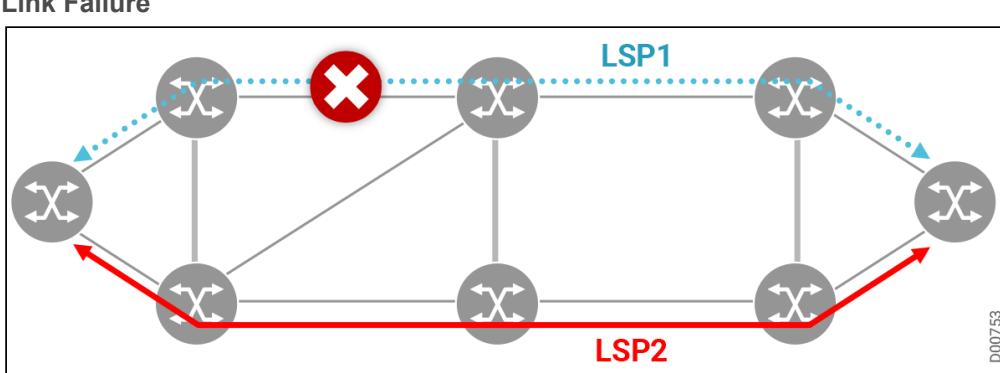
The following sequence shows a typical example of this restoration process.

- 

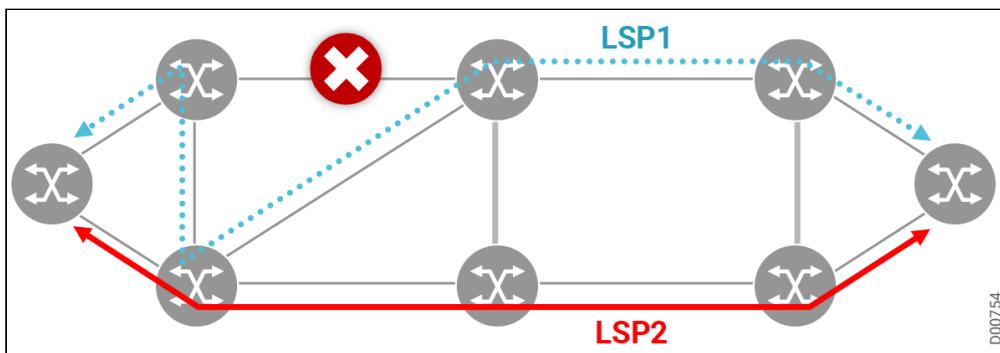
**Traffic Transmitted Over LSP1**



- Link Failure



- Restore Traffic to Original LSP1



If multiple link failures are detected in the original LSP, LightSOFT dynamically restores the relevant tunnels by configuring alternative routes, working link by link and taking all active failures into account when performing restoration. As the participating links are repaired, LightSOFT reverts the tunnels where possible to the original links.

Network restoration is a dynamic, flexible feature that intelligently chooses the most efficient route, based on the current network status, correlating all affected tunnels and identifying the most efficient route for the current network functional topology.

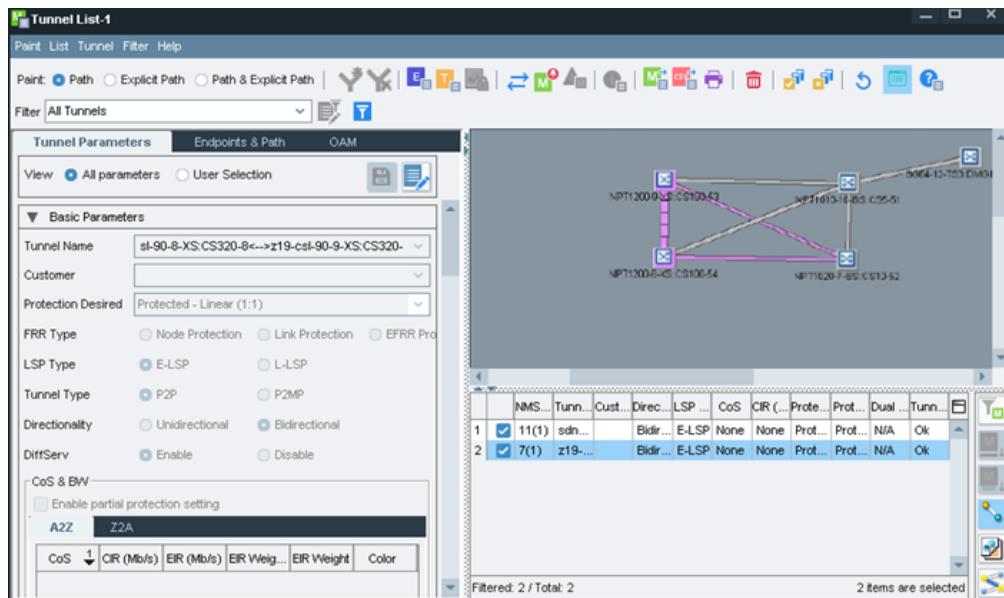
As link failures are fixed, LightSOFT efficiently reverts the affected tunnels, correlating the tunnels and repaired links and completing either full or partial reversions.

Automatic network restoration can be configured for protected and unprotected tunnels, for either one or both main and protection paths.

Operators can choose how they prefer to optimize resource usage, either maximizing disjoint route selection or focusing on resource sharing to minimize resource utilization. Network restoration provides protection from multiple network failures, since new LSP paths are dynamically prepared and ready for use *before* they are needed.

You can view the tunnel status in the **Tunnel List** window. In the event of a failure, a dotted line indicates the original path of the tunnel and a solid line of the same color indicates the active (restoration) path.

## Tunnel Restoration



### In the Tunnel List:

- **Restoration Status:** Indicates whether the restoration attempt was successful.
- **Restoration:** Indicates whether restoration is enabled on this tunnel.
- **Number of Retries:** The maximum number of restoration attempts LightSOFT performed to find available resources in the event of a failure.

You can exclude one or more links from **LSP Restoration**. If a link is excluded, it will not be used in LSP restoration, unless the Ring ID of the link is the same as the provisioned path of the main or protected LSP that is failed.

Fragments of tunnels left over in NEs, which were temporarily left unmanaged when the feature rerouted the tunnel away from them, are automatically cleaned up by LightSOFT once these NEs are managed again.

The attribute indicating whether a tunnel is protected by restoration is preserved in cases when the tunnel must be deleted from the LightSOFT database and acquired bottom-up (as long as at least one of the tunnel endpoints is a Neptune NE).

## LDP FRR with Loop-Free Alternatives LFA

IP Fast Reroute (FRR) is a mechanism that enables a router that detects a failure in an adjacent link or node (or both) to rapidly switch traffic towards a pre-defined loop-free alternative (LFA) path. This LFA path is used for traffic until the router installs a new primary next hop again, as computed for the changed network topology. The goal of LFA FRR is to reduce failure reaction time to 50 milliseconds by using a pre-computed alternate next hop, in the event that the currently selected primary next hop fails, so that the alternate can be rapidly put into use when a failure is detected.

This feature addresses the fast convergence requirement by detecting, computing, updating, or enabling prefix independent pre-computed alternate loop-free paths at the time of failure. IGP pre-computes a backup path per IGP prefix. IGP selects one and only one backup path per primary path. The routing information base (RIB) table installs the best path and download path protection information to the forwarding information base (FIB) table by providing correct annotation for protected and protecting paths. FIB pre-installs the backup path in the data plane. Upon link or node failure, the routing protocol detects the failure and all the backup paths of the impacted prefixes are enabled in a prefix-independent manner.

LDP FRR provides an effective technique for fast local repair of link and node failures in an IP/MPLS domain, represented by a single AS. LDP must be enabled on all intra-AS links, using local and remote loop-free

alternate (LFA) next hops. LDP FRR provides fast protection for all types of traffic using LSPs set up by LDP, including L2VPN and L3VPN traffic.

LDP FRR provides sub-50ms traffic recovery following an IGP adjacency failure, for L2/L3VPN traffic using LDP LSPs. 1-hop IPv4 BFD can be configured as a trigger for LDP FRR. Neptune's LDP FRR implementation is based on IP FRR using loop-free alternates (IP-LFA). This implementation can be used with both OSPFv2 and IS-IS protocols. Users can configure the LFA selection preferences:

- LFA per destination prefix (default)
- LFA per failed adjacency
- LFA for both link and node protection (default link)
- LFA from the same ECMP group

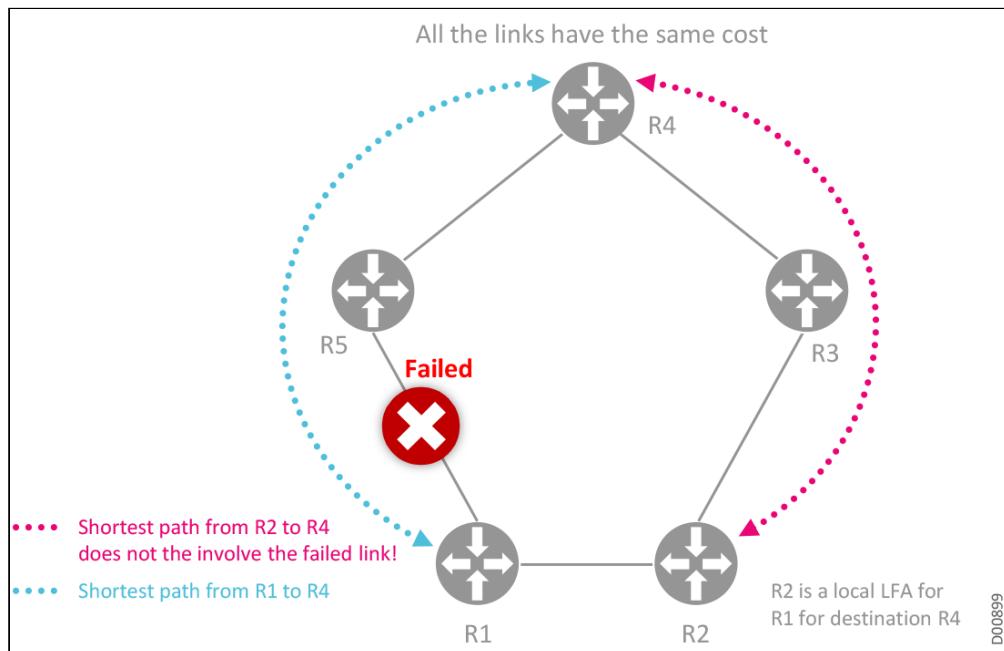
LDP FRR is configured in flat topologies that include a single IS-IS or OSPF area, where all relevant interfaces are P2P. IP and LDP FRR are implemented using the 'not-via' technique described in RFC 6981, and with maximally redundant trees (MRT), as described in draft-ietf-rtgwg-mrt-frr-architecture and draft-ietf-rtgwg-mrt-frr-algorithm.

This section introduces the following features:

- FRR using Local LFA
- FRR using Remote LFA

## FRR using Local LFA

### FRR Using Local LFA



The network illustrated in this example is a single AS. From the IGP perspective, this is either a single IS-IS Level2 domain, or a single OSPF area. All the intra-AS links are P2P, and IP FRR using local LFA is enabled. LDP and LDP FRR are enabled on all intra-AS links.

Through **normal IGP** processing, R1 learns that R2 and R5 are both adjacent. An AS topology graph is built, and R1 computes the shortest path from itself to R4. There is exactly one such path, and the next hop for this path is R5. R5 is therefore defined in the RIB as the next hop for destination R4.

Through **normal LDP** processing, label bindings for an R4 destination are received from the adjacencies. LDP looks in the RIB and sees that R5 is the next hop to R4, so its label binding is *installed* in the RIB. R2 is not the next hop to R4, so its label binding for R4 is *retained*.

With **extended IGP** processing that supports IP FRR, R1 tries to find a local loop-free alternate (LFA) to R5 for destination R4. R2 is the only local alternate, and it is confirmed to be loop-free, so R2 is selected as the local LFA for R4.

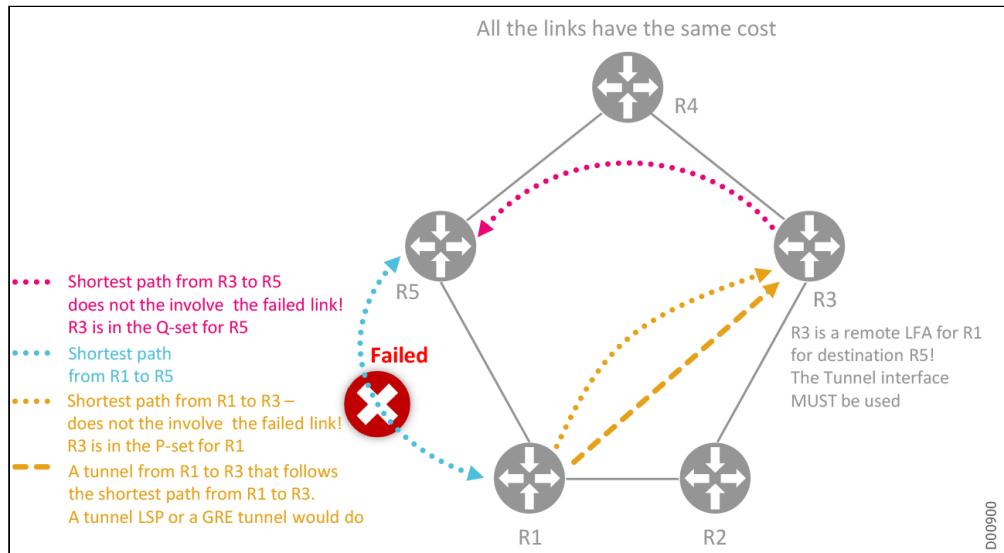
When the **IGP adjacency between R1 and R5 fails**, extended IGP installs the retained LFA R2 as the next hop for destination R4 in the RIB. When LDP is notified of the change in the RIB, R2 is now defined as the next hop for destination R4, and the retained label-to-FEC binding received from R2 is installed, accomplishing fast LDP rerouting.

In the interim, basic IGP processing continues. The changes in the link state are flooded. LSDB in all the routers in the AS are re-synchronized. New shortest paths are computed, and the new next hops to all destinations are entered in the RIB and FIB. In the PLR these decisions override the LFA selection.

Extended IGP processing begins looking for a new LFA. Basic LDP processing continues. The LDP notices the changes in the RIB, and label-to-FEC bindings from the newly entered next hops are entered in the LFIB. In the PLR these decisions override the LFA selection.

## FRR using Remote LFA

### FRR using Remote LFA



The network illustrated in this example is a single AS. From the IGP perspective, this is either a single IS-IS Level2 domain, or a single OSPF area. All the intra-AS links are P2P, and IP FRR using local and remote LFA is enabled. LDP and LDP FRR are enabled on all intra-AS links.

Through **normal IGP** processing, R1 learns that R2 and R5 are both adjacent. An AS topology graph is built, and R1 computes the shortest path from itself to R4. There is exactly one such path, and the next hop for this path is R5. R5 is therefore defined in the RIB as the next hop for destination R4.

Through **normal LDP** processing, R1 learns that R2 and R5 are both adjacent. R1 then receives label-to-FEC bindings for the FEC representing R4 from R2 and R5.

With **extended IGP** processing that supports IP FRR, R1 tries to find a local LFA for R5, leading to destination R4. R2 is the only local alternate. However, it is not loop-free, so no local LFA is available for this destination.

Therefore, IGP in R1 tries to identify a remote LFA for R5. First it computes a P-set for the failed adjacency. These are the NEs that R1 can reach without using failed resources, and includes {R2, R3}. R1 then computes a Q-set for the failed adjacency. These are the NEs that can reach R5 without using failed resources, and includes {R3, R4}. Since R3 is in both the P-set and the Q-set, R3 is selected as the remote LFA for R5.

LDP has already set up a tunnel LSP to R3. This is an unnumbered P2P interface, through which IP packets to be transmitted are encapsulated into MPLS with a suitable label. LDP retains the route to R5 using this interface as the next hop for future use.

Extended LDP processing is notified about the selection of R3 as a remote LFA, and if necessary sets up an indirect (targeted) LDP session to R3, and requests label-to-FEC bindings for R5 via this session. These bindings are associated with the LSP from R1 to R3 as the next hop, even though this LSP is not the best next hop in the RIB.

When IGP adjacency between R1 and R5 fails, extended IGP installs the LDP-instantiated LSP to R3 as the next hop for destination R5 in the RIB. LDP is notified about the change in the RIB, installs the LDP-instantiated LSP to R3 in the RIB as the next hop for destination R5, and the retained label-to-FEC binding received from R3 is installed, accomplishing fast LDP rerouting.

In the interim, basic IGP processing continues. The changes in the link state are flooded. LSDB in all the routers in the AS are re-synchronized. New shortest paths are computed, and the new next hops to all destinations are entered in the RIB and FIB. In the PLR these decisions override the LFA selection.

Extended IGP processing begins looking for a new LFA. Basic LDP processing continues. The LDP notices the changes in the RIB, and label-to-FEC bindings from the newly entered next hops are entered in the LFIB. In the PLR these decisions override the LFA selection.

## Object Tracking

Object tracking is a mechanism to *track one object*, and to then *take an action on another object* (where the second object may have no relationship to the tracked object), based on changes to the properties of the original object being tracked. Each tracked object is identified by a unique name. The tracking process periodically polls the tracked object and reports any changes to its state, in terms of its being up or down, either immediately or after a delay period, as configured by the user.

Multiple objects can also be tracked by maintaining all the objects in a list, using a flexible method for combining the subset of included objects, using Boolean logic. This functionality includes:

- Boolean **AND**: When a tracked list has been assigned a Boolean AND function, the tracked object can only be in an "up" state if **each object** defined within the list subset is in an up state. Only then can the tracked object also be in an up state.
- Boolean **OR**: When a tracked list has been assigned a Boolean OR function, the tracked object can only be in an "up" state if **at least one object** defined within the list subset is in an up state. Only then can the tracked object also be in an up state.

Simplified Object Tracking is one application of object tracking, used for handling core isolation scenarios that were previously defined for PHT LIFs, but with the following changes:

- **Support for the following types of named, simple Track objects:**
  - Port and/or Logical Interface: The tracked property is the Operational Status of the interface.
  - IP Host in a specific VRF (default/global or specific): The tracked property is the existence of an exact active route in the RIB of the VRF in question.
  - IP Prefix in a specific VRF (default/global or specific): The tracked property is the existence of a covering active route in the RIB of the VRF in question.
- **Support for composite named Track objects as lists of simple Track objects:**
  - The number of simple Track objects is limited.
  - The tracked property can be either logical OR or logical AND of the tracked properties of all simple Track objects in the list.
- **Support for the following actions that can be triggered by transitions of a single or composite Track object from TRUE to FALSE and vice versa:**
  - Administrative disabling/enabling of an interface
  - Withdrawal/insertion of a specified static route in a specified RIB

This section includes the following:

- [Tracking Policy Objects](#)

- Using Tracking Policies to Disable Interfaces

## Tracking Policy Objects

You can configure new named objects called tracking policy. Each tracking policy object includes the following attributes:

- **Name** (key): A unique ASCII string
- **Description**: Free text, sufficiently long. It may be left empty.
- **Two stabilization intervals** (in seconds):
  - **Down**: For transition from UP to DOWN state
  - **Up**: For transition from DOWN to UP state
- **Initial weight** (integer): If not specified explicitly, the sum of the weights of entries in the two lists below (list of tracked interfaces and list of tracked prefixes) is used. Alternatively, a positive integer value may be specified by the user.
- **Two lists**, of which at least one must not be empty:
  - **List of tracked interfaces**, defined in pairs {interface name, interface weight (optional)}
    - Empty by default
    - Up to 4 members
    - The default weight for each pair is 1. May be set to another positive integer by the user.
    - A tracked interface affects the policy if it is not in its UP operational state.
  - **List of tracked prefixes**, defined in sets of 4 attributes {IP prefix, VRF name (optional), network tracking mode (optional) , prefix weight (optional)}:
    - Empty by default
    - Up to 4 members
    - If VRF name is not specified, the prefix is looked up in the RIB of the global/default VRF. Otherwise, it is looked up in the RIB of the corresponding VRF.
    - Only active routes in the RIB are looked up. Inactive routes are ignored.
    - If network tracking mode is not specified, an exact match of the route destination for the tracked prefix is looked up. Otherwise, any route with a covering destination is looked up.
    - The default weight for each set of attributes is 1. May be set to another positive integer by the user.
    - A tracked prefix affects the policy if its lookup did not yield any result.

## Using Tracking Policies to Disable Interfaces

The tracking policy settings and values can be used to disable interfaces, as follows:

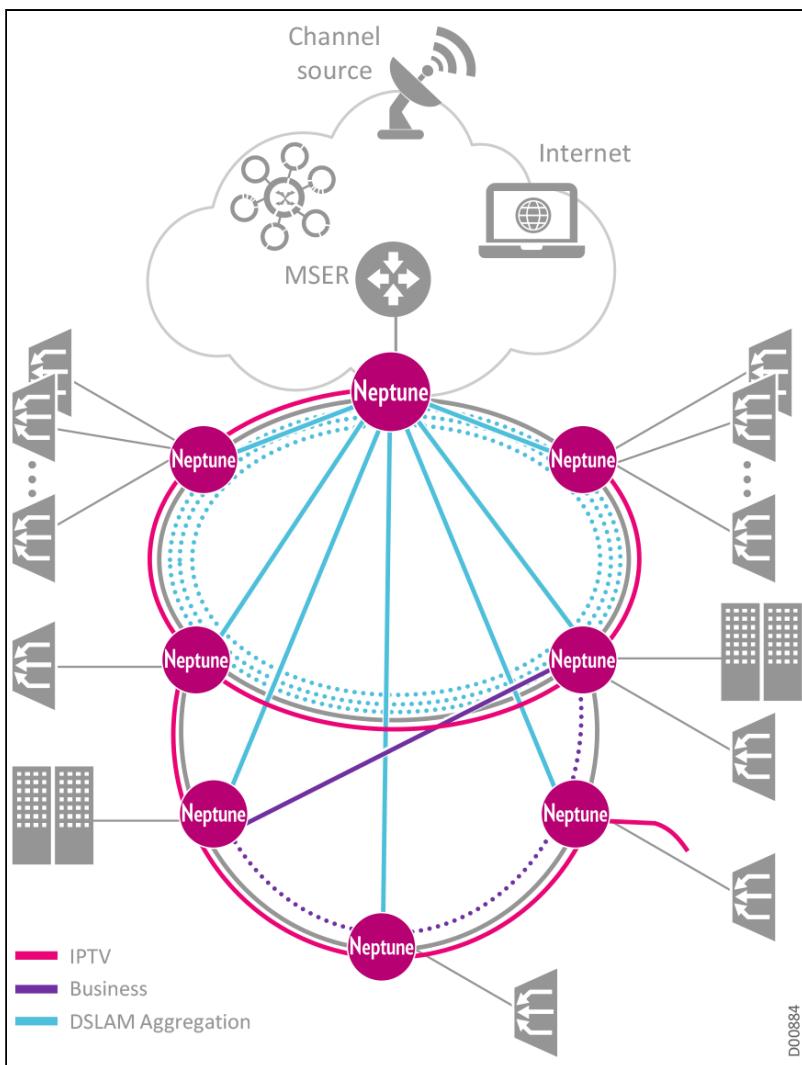
- All interfaces (both port interfaces and logical interfaces) may be optionally configured with a reference (by name) to a specific tracking policy object.
  - Loopback interfaces may be an exception.
  - Multiple interfaces may refer to the same tracking policy object, so that any changes to this object are done once and affect all interfaces referring to it.
  - If such a reference is not defined, the interface behaves as usual
  - If the reference is defined:
    - As long as the policy is UP or stabilizing for DOWN, the user-defined administrative state of the interface applies.
    - Once the policy becomes DOWN or stabilizing for UP, the interface is treated as if it were administratively disabled regardless of the user-specified administrative state.
- The port interface of the LAG is represented (as always) by its Master port.
- Administrative disabling of an interface has the following effects (regardless of whether it comes from the user configuration or from the tracking mechanism):
  - The interface and all its dependencies are reported as DOWN to the DSWP and to the Linux IP stack.
  - For port interfaces that use optical media, disabling results in laser shutdown.
    - For LAG port interfaces, laser is shut down on all LAG members.

- For electrical Ethernet port interfaces, disabling results in shutdown of the port PHY.
- For PHT LIFs, disabling includes signaling of the PW status.

## Linear Protection

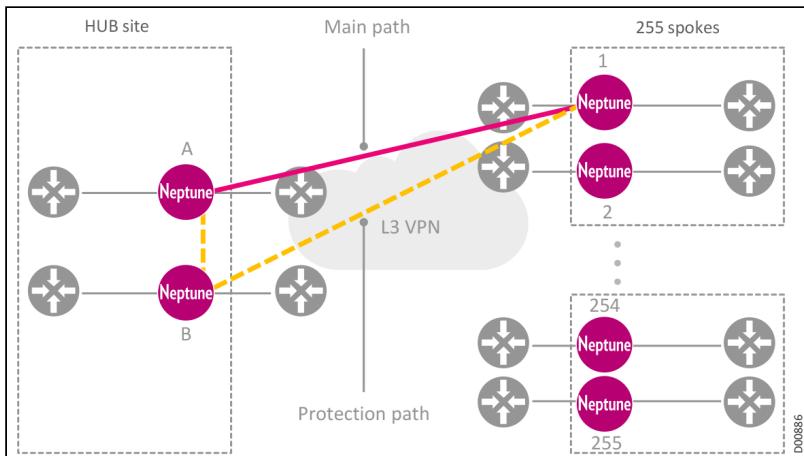
LightSOFT provides end-to-end linear protection for bidirectional E-LSP tunnels, as described in the MPLS-TP Survivability Framework (RFC6372). The goal of 1:1 linear protection is to provide protection switching triggered by data plane OAM, similar to SDH/SONET protection, without depending on signaling or the control plane. With this bidirectional 1:1 protection, traffic is transmitted only via one LSP - main or protection - but never both. In case of an LSP failure, the traffic is automatically switched to the standby LSP.

### Linear Protection for Various Services



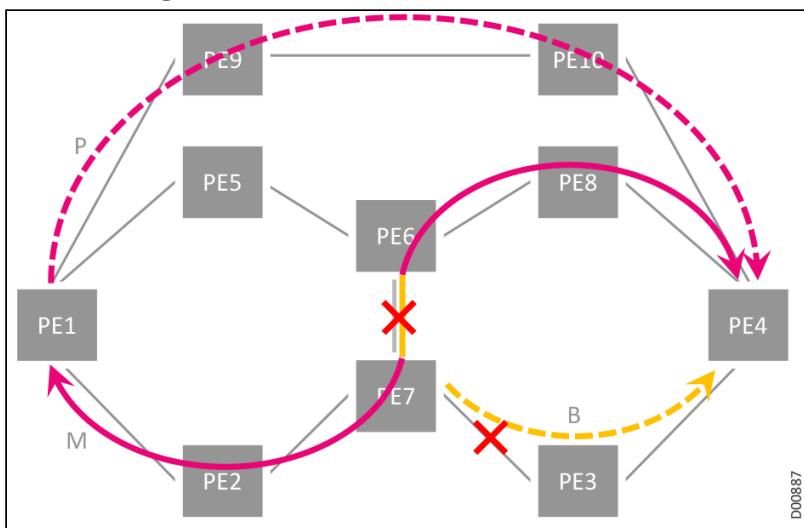
1:1 linear protection provides a solution for MPLS-TP services over IP-MPLS core. The customer configures a tunnel in overlay mode (see [Overlay using GRE](#)) and the in-band OAM signals the end points when there is a failure in the third party core segment.

### MPLS-TP Services Crossing the IP-MPLS Core



Another use of 1:1 linear protection, when combined with FRR, is to restore service even after a second fiber cut. In this scenario, FRR protects against the first fiber cut or node failure, and if a second failure occurs, the head-end switches to the predefined protection LSP.

### Protection Against Two Failures



Our 1:1 linear protection implementation on Neptune platforms includes:

- Protection for bidirectional co-routed E-LSPs
- Protection State Coordination (PSC) protocol to synchronize both ends of a tunnel
- Protection triggers include:
  - Local faults (server indication), including:
    - Link failures
    - LDI indication from intermediate points to the end-point
  - End to End Connectivity Check (CC)
    - Using BFD OAM mechanism per LSP

## PW Redundancy

A pseudowire (PW) is a virtual 'wire' that emulates a P2P connection over a packet switching network (PSN). The PW emulates the operation of a 'transparent wire' carrying a service, such as ATM, Frame Relay, Ethernet, or TDM, over an MPLS or IP packet network. The PW is a logical connection that is intended to

provide only the minimum necessary functionality to emulate the 'wire' with the required degree of faithfulness for the given service definition.

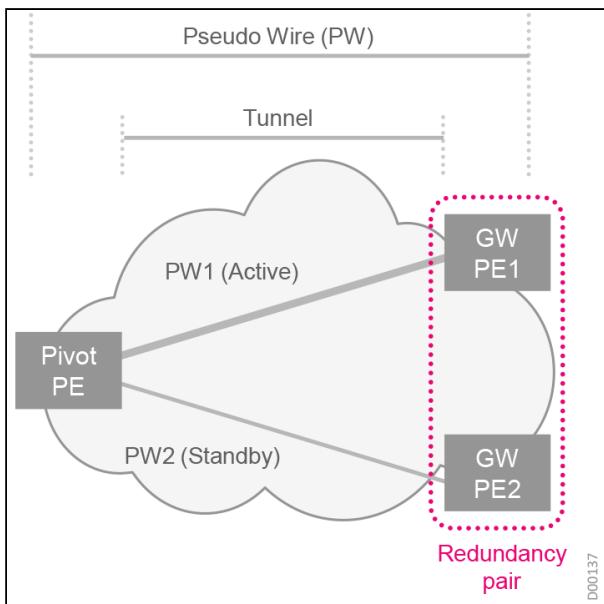
PW redundancy (PW-R) enables networks to provide protection on the PW level in addition to the other existing layers of protection. PW-R is based on configuring pairs of PWs, where one is configured as the primary (active) and the other as secondary (standby).

- Both PWs originate in a **pivot node** and connect to gateway nodes.
- The pivot node normally transmits traffic out of the active PW.
- If there is a failure on the active PW, the node 'pivots' and transmits traffic out of the standby PW.

**Note**

The nodes that are linked to a pivot PE node are referred to as **gateways**. Two gateways that connect to the same pivot node and serve as destinations for two redundant PWs are referred to as a **redundancy pair**.

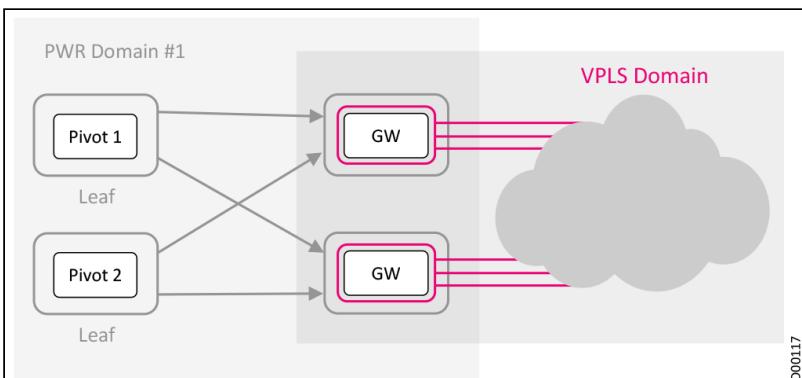
### Generalized PE Dual-Homing Topology



Our equipment offers multiple layers of protection options. Protection option selection and configurations can be tailored to specific network preferences. For example, PWs run over MPLS tunnels.

- If the tunnel is protected, for example through LP protection, then the PW-R hold-off timer should be configured to a high enough value to allow time to handle protection at the tunnel level.
- If tunnel traffic is either restored or diverted to the protection tunnel within the time limit set by the hold-off timer, then no PW redundancy switchover will be needed.
- Alternatively, if the underlying tunnel is not protected, then a failure of the transport layer tunnel will be handled by the PW at the service layer. In this case, the hold-off timer setting would be much smaller.

## Sharing Gateways Between Domains



PW-R is supported on selected data cards for MoE, MoF, and IC-MoE ports over bidirectional E-LSP tunnels. A Bidirectional Forwarding Detection (BFD) protocol monitors the status of the tunnels and PEs.

To provision PW redundancy in LightSOFT, define a PW redundancy domain (PW-R domain) that includes one or more pivot PEs and two PEs that will serve as gateways. LightSOFT automatically configures the redundancy pairs of PWs into sets of primary and secondary PWs.

PW-R is also implemented automatically by LightSOFT as part of [MC-LAG protection](#). LightSOFT automatically detects the redundant pair of ports participating in the MC-LAG. The LAG service automatically determines which is the primary PW and which the secondary.

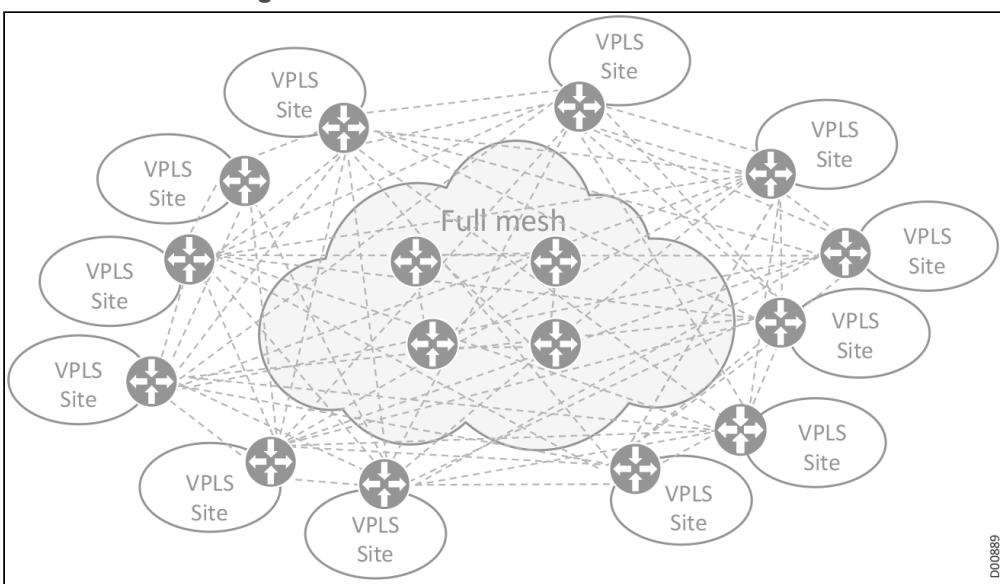
You may optionally choose to manually configure the primary and secondary PWs.

### PW Status Propagation

Neptune platforms provide efficient PW implementations including PW status propagation, as described in RFC4447 and RFC6310. PW status messages are sent in-band through PW OAM messages that carry the PW status for a particular PW. The PW status is monitored and propagated as relevant. An awareness of the PW status enables more efficient switching decisions, based on real-time knowledge of the PW's actual status.

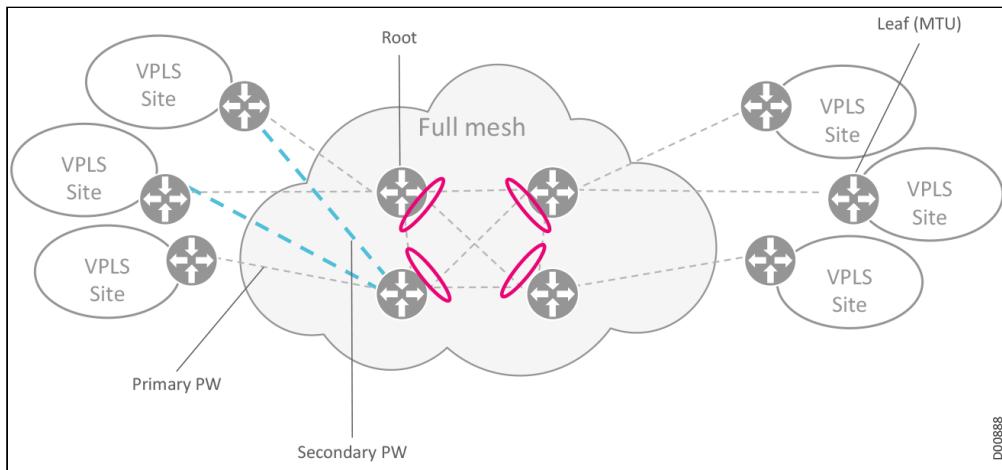
## Hierarchical VPLS Services

### VPLS Network Configuration



With H-VPLS, the network is split into hierarchical VPLS domains. Leaf nodes are connected only to their roots, and full mesh is only created between root nodes within each domain.

### Typical H-VPLS Topology



H-VPLS enables connections between VPLS domains.

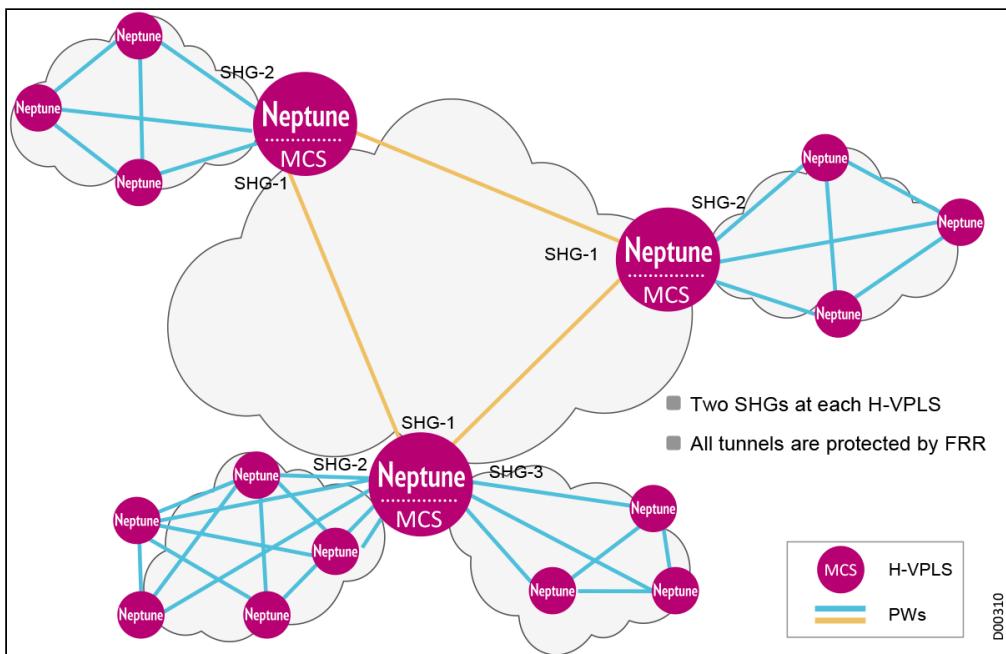
H-VPLS defines a hierarchy of VPLS domains and allows MPLS-level connectivity between them, providing VPLS network scalability, hierarchical partitioning and interoperability.

- LightSOFT platforms support static H-VPLS over MoE interfaces, based on IETF standard RFC4762.
- LightSOFT platforms also support an enhanced H-VPLS feature enabling definitions of multiple SHGs with traffic switching between these groups.
- LightSOFT H-VPLS implementation supports both two-tier H-VPLS (root and leaf) and multidomain H-VPLS.

The following figure illustrates an example of a network where the gateway supports multiple H-VPLS domains:

- Within each domain, member nodes are connected in a full mesh VPLS.
- Each domain is connected to other NEs using H-VPLS.
- Multiple domains are connected through each gateway NE.

### Multiple H-VPLS Domains



H-VPLS also enables dual homing for multiple access/metro rings connected to a core ring.

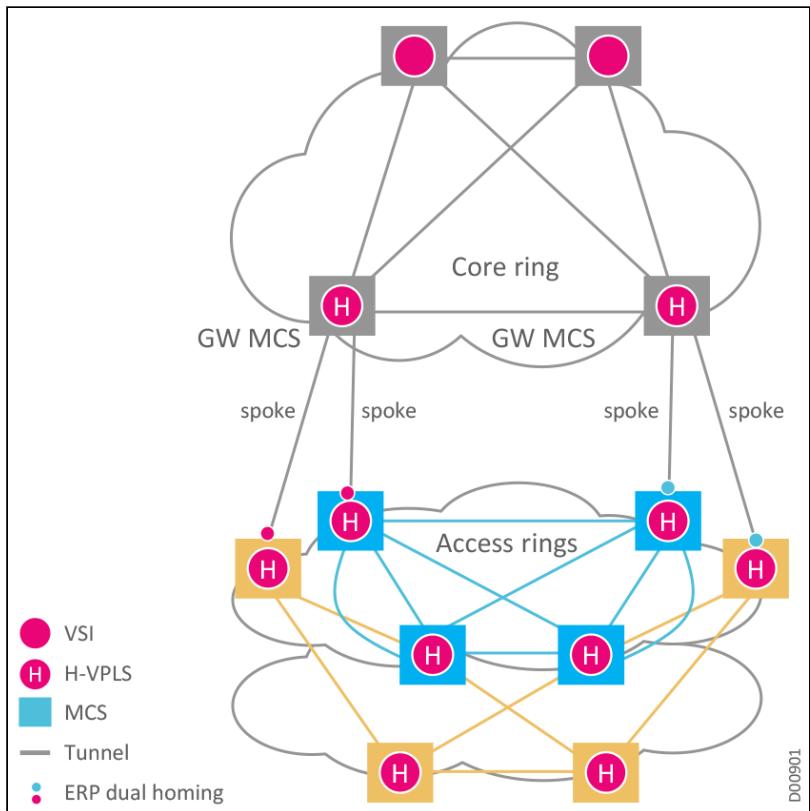
#### Example: Dual Homing for Multiple MPLS Access Rings

Neptune data cards support dual-homed device protection for H-VPLS networks. Dual-homed protection for H-VPLS networks enables dual homing for multiple MPLS access rings connected to a core ring. Typical configurations include full mesh within each access ring and spokes reaching from each ring towards gateway nodes in the core ring. The access rings may be either open or closed.

Intelligent use of CCN enhances network resiliency and enables more effective use of dual-homed device protection in H-VPLS networks. In some H-VPLS dual homing topologies, when there is a need for CCN to cross VPLS domains, **CCN forwarding** can be enabled on the relevant NEs.

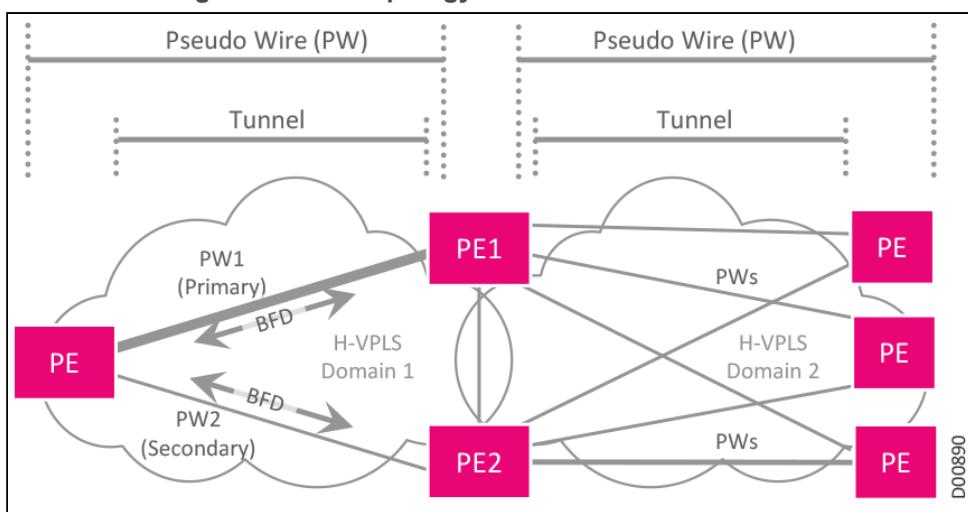
Redundant connectivity is enabled through use of **ERP** (see [Ethernet ring protection switching \(ERPS\)](#)) in the access gateway nodes. Configuring ERP between the two local gateways prevents creation of loops in the network.

### H-VPLS with Dual Homing for Access Rings



## PW Redundancy for H-VPLS DH Topology

### PE Dual-Homing to H-VPLS Topology



In this H-VPLS network, the dual-homed PE has configured spoke PWs to H-VPLS gateways PE1 and PE2. One of the PEs is currently active, linked to the PE via the primary PW. The primary PW is given priority by the EMS and is responsible for forwarding traffic to the peer H-VPLS domain. Failure of an H-VPLS gateway PE generates an OAM defect, which in turn triggers the dual-homed PE to select a new primary PW. A hold-off timer can be used to mask temporary server layer faults.

Another option to trigger PW redundancy is by using PW status from the gateway PE. The end to end PW is traversing two H-VPLS domains and tunnel OAM is maintained over each domain. Hence, in case of a failure in Domain #2 which is not recovered by the tunnel protection, the gateway PE will mark the PW as down and generate a defect status message towards the pivot node that will trigger a PWR switch.

A PW switchover requires an FDB flush at PE1, PE2, and the far H-VPLS domain. This is achieved by the transmission of CCN messages between data cards that indicate for which PE(s) the FDB entries should be deleted (see Configuring CCN).

PW Redundancy can also be used for load balancing between the H-VPLS gateways. By configuring some PEs with the primary PWs toward PE1 (where PE1 becomes the default H-VPLS gateway), and other PEs with primary PWs toward PE2, the traffic load can be reasonably balanced between the two gateway PEs.

**Note**

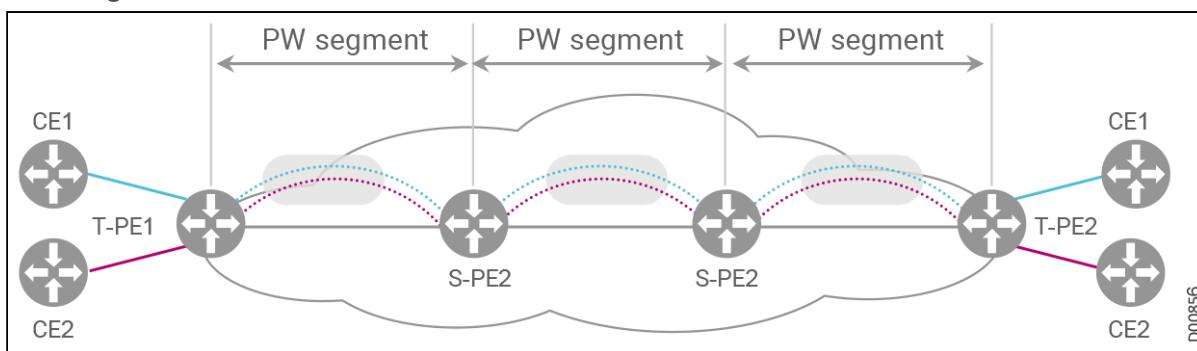
In dual-homing to H-VPLS topology, BFD must be used to monitor the status of the remote PE and the status of the transport layer, in order for the pivot PE to select the appropriate PW. BFD should therefore be enabled on the tunnel carrying the PW (see Configuring MPLS-TP Linear Protection).

## Multi-Segment PW

An L2VPN multi-segment pseudowire (MS-PW) is a set of two or more PW segments that function as a single PW, as illustrated in the following figure.

- Some routers participating in the PW segments are identified as switching provider edge (S-PE) routers, which are located at the switching points connecting the tunnels of the participating PW segments.
- Some routers participating in the PW segments are identified as terminating provider edge (T-PE) routers, which are located at the MS-PW endpoints.
- The S-PE routers can switch the control and data planes of the preceding and succeeding PW segments.
- MS-PWs can span multiple cores or autonomous systems of the same or different carrier networks.

### Multi-Segment PW



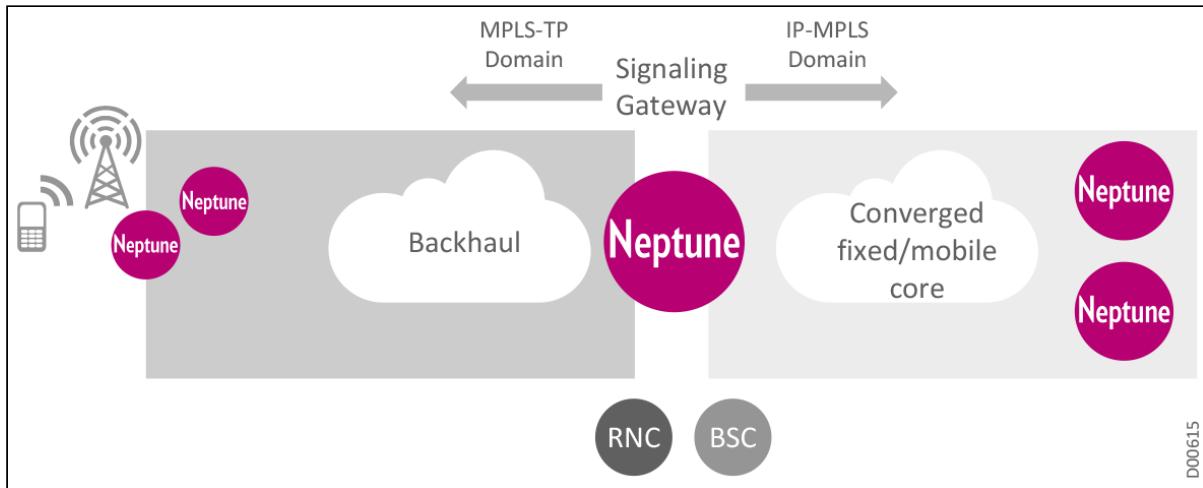
- MS-PW service enables a hierarchical network structure for data networks, similar to H-VPLS capabilities.
- MS-PW functionality improves scalability, facilitates multi-operator deployments and facilitates use of different control plane techniques in different domains.

These are valuable capabilities in network configurations that must typically be able to integrate static PW segments in the access domains and signaled PW segments in the IP/MPLS core.

- Signaling gateways (SGW) are used to tie PW segments together into a single connection (*stitching*) at a given point.
- This functionality is implemented within a single platform located at the border of two network domains. The two domains may both be static, both dynamic, or one static and one dynamic.

- Network interworking enables LSP and service stitching, interaction between the data planes and end-to-end OAM.

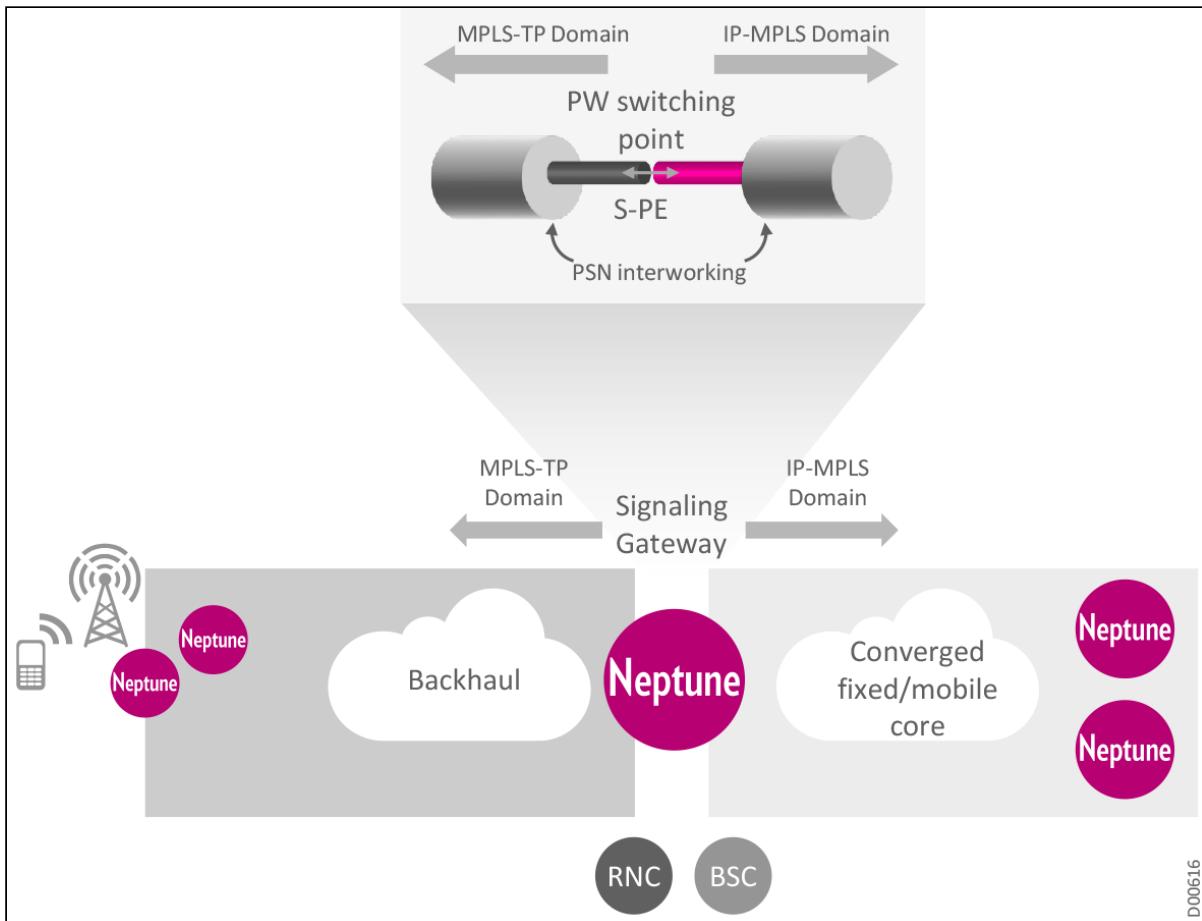
### Signaling Gateway Connecting PW Segments



MPLS-TP and IP/MPLS domains can be connected through SGWs. In PW-based backhaul, this is implemented through multi-segment PWs (MS-PWs), including:

- Static MPLS-TP segments
- Dynamic IP/MPLS segments
- Gateway interconnections or "stitches" of both types of segments

### Focus on the PW Switching Point within the Gateway



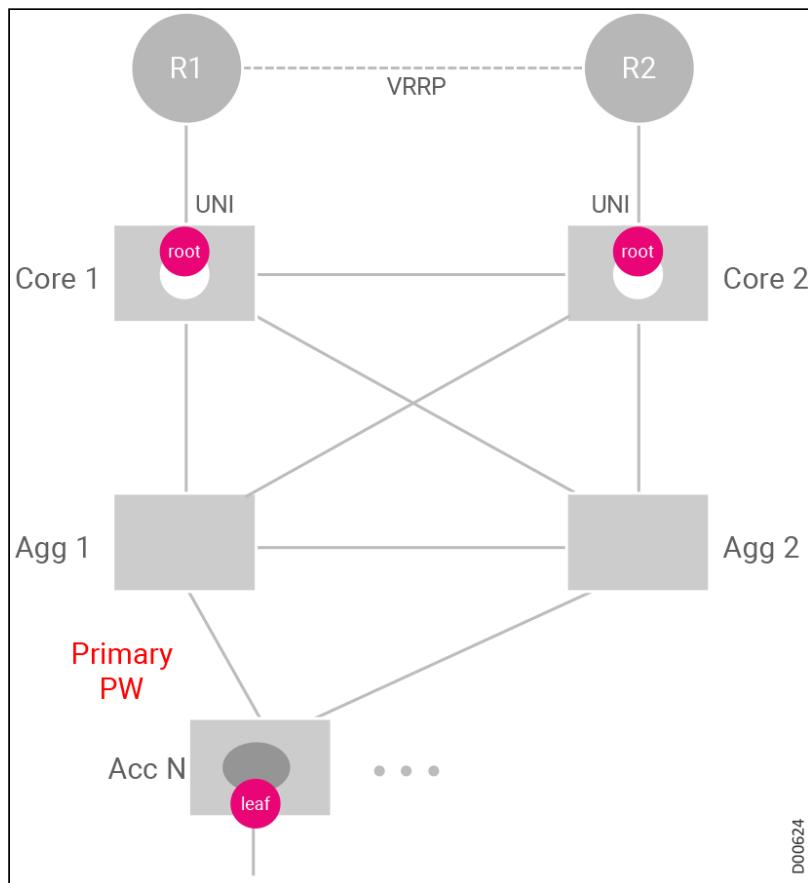
### Example: VPLS with MS-PW and PW Redundancy

VPLS networks configured with a combination of MS-PW and PW-R offer an efficient service solution for complex network operation. The PW-R enables fast protection switching in a loop-free topology, providing multi-failure protection, including aggregation node failure.

**Note**

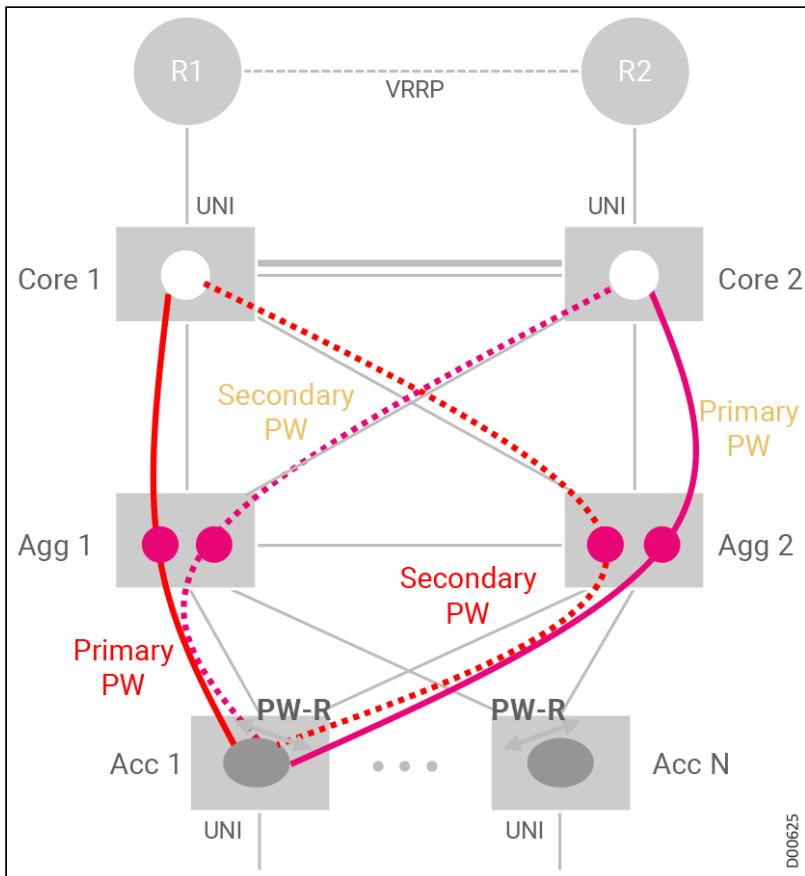
This network solution model is based on RFC 6073 and RFC 6718, using PW-R in a linear protection scheme.

### Basic VPLS Service Configuration



Within this network, the network operator can configure multiple MS-PW path segments, running between the core, aggregation, and access nodes. The network operator can also define corresponding PW redundancy pairs for these PW segments.

### MS-PW with PW Redundancy



Bidirectional E-LSP tunnels carry each PW segment. BFD is used to monitor the LSP operational status. MPLS-TP 1:1 linear protection is provided to protect against multiple link failures.

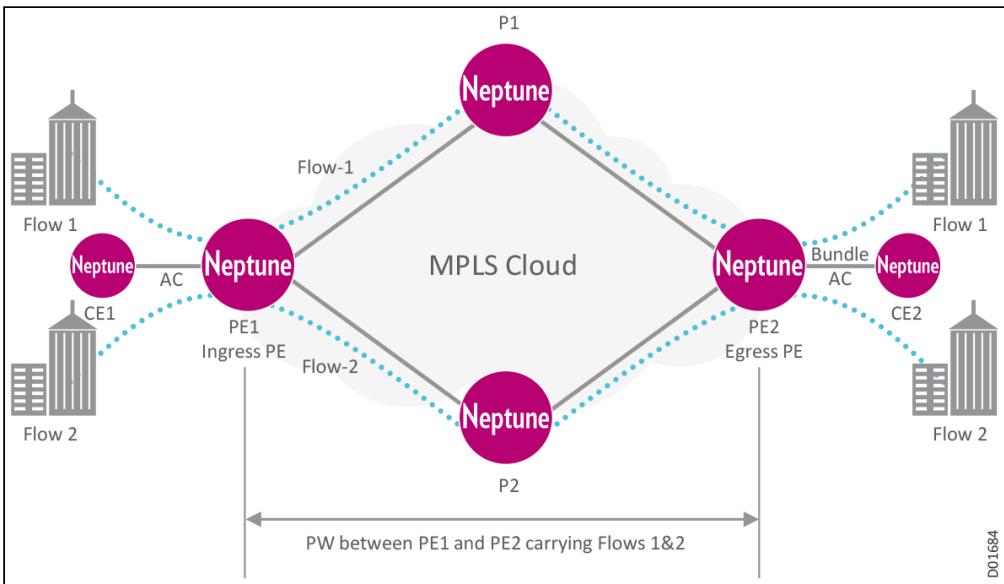
This model provides robust, efficient protection for link and node failures. For example, the first layer of protection covers link failures, based on MPLS-TP 1:1 linear protection and LSP BFD. The second layer of protection covers aggregation node failure, based on PW-R and end-to-end PW VCCV (BFD). An alternative implementation would use LSP OAM per PW segment and propagation of the segment status, using PW status messages at the S-PE.

## FAT: PW Load Balancing

Routers usually balance their traffic load based on the "common denominator" label, the lowest label in the label stack. This is the label shared by all flows on a given PW, where 'flow' refers to the sequence of packets that share the same source and destination PEs. While this is a logical approach, it can lead to uneven or asymmetrical load balancing, depending on the PW traffic patterns.

Flow-Aware Transport Pseudowires (FAT PW) make it possible to identify individual flows within a PW. With this information, routers can manage these flows to balance the traffic load more intelligently. FAT PWs are used to balance traffic in the core through utilization of equal cost multi-paths (ECMPs). A **flow label** is created based on indivisible packet flows entering a PW. This flow label is inserted as the lowest label in the packet's label stack. Routers can then check the flow label and distribute traffic flows in a more balanced pattern across ECMPs or link-bundled paths in the core. The following figure illustrates a FAT PW with two flows distributed over ECMPs and bundle links.

### FAT PW with 2 Flows



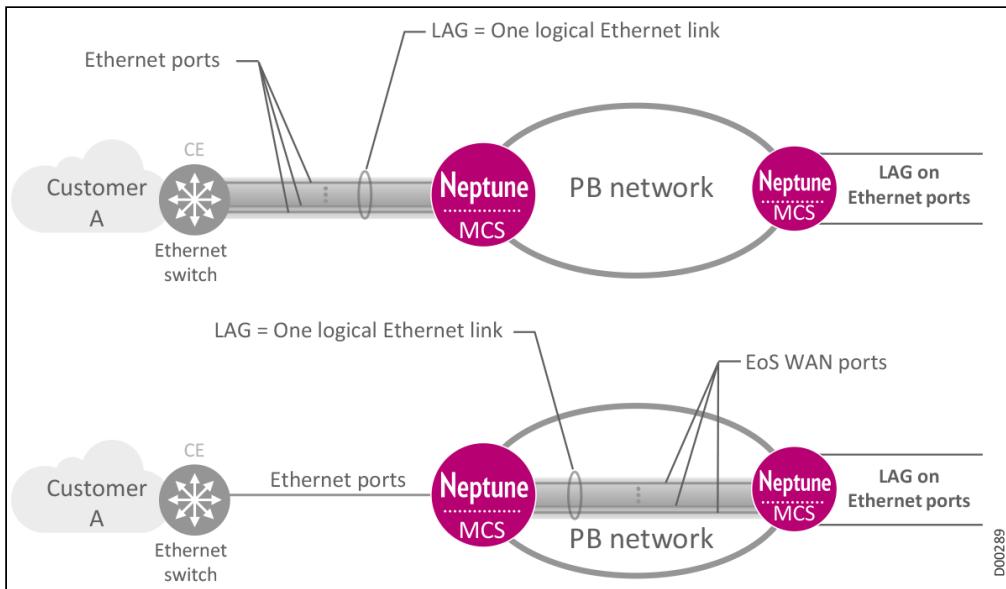
An additional 'flow label' with the flow information of the corresponding virtual circuit (VC) is added to the stack, providing a unique identifier that distinguishes the flow within the PW. The VC is derived from source and destination MAC and IP addresses. The flow label also contains the end of label stack (EOS) bit, set and inserted after the VC label and before the control word (if any). The ingress PE calculates and forwards the flow label. The FAT PW configuration enables the flow label. The egress PE discards the flow label since it is no longer relevant.

## Link Aggregation LAG

Ethernet link aggregation (LAG) protection is based on standard Ethernet link aggregation schemes (**IEEE 802.3ad**). Link aggregation is available for Ethernet, MPLS-TP and MoE WAN ports. In LAG protection schemes, a single logical link is composed of up to eight physical links. When one (or more) physical links fails, it is simply removed until recovered. The network continues to function correctly without the failed link, since the links for the LAG as a whole are still functioning.

Network operators can configure a **LAG Link Down** threshold, defining up to how many links can go down and the whole LAG will still be considered operational, and at what point a LAG is considered to have failed even if still a few links are functional. Some data cards support link aggregation based on IP (IPv4/IPv6) or MAC address hashing, depending on the packet header data. This capability enables superior load balancing and enhanced TM efficiency.

## LAG: Link Aggregation Examples



## LAG Configuration Options

Neptune supports link aggregation groups (LAG) used for two types of purposes:

- **Load Balancing** divides the traffic load between up to 32 equivalent Ethernet ports, enabling higher bandwidth connectivity. Participating ports should all be working at the same port speed; mixing different rate ports in the same LAG is not allowed. Services can only be defined on the LAG master port, which serves as the service endpoint. The LAG multilink behaves like a single link for service provisioning. Traffic distribution is based on hashing the MAC or IP address (IPv4 and IPv6).

Neptune platforms support **IP packet payload-based load-balancing for MPLS encapsulated traffic**. The platform hardware identifies the packet header type (either IPv4/IPv6 or MPLS) and hashes the relevant header fields accordingly. A hash algorithm for next-hop address selection creates an optimal traffic distribution, thus balancing the traffic load across LAG links.

Neptune platforms in the NPT-2xxx series also support **load balancing of IPv4 or IPv6 packets using GPRS Tunneling Protocol (GTP) tunnel endpoint identifier (TE-ID)** field hash calculations. GTP is a tunnel control and management protocol. Wireless networks use GTP tunnels to deliver mobile data. GTP includes a complete set of procedures and protocols for signaling, data transfer, and tunnel control and management. GTP offers a comprehensive approach to creating, deleting, and modifying tunnels, as well as a tunneling mechanism to provide a service for carrying user data packets over the network.

GTP load balancing enables using the tunnel endpoint identifier (TE-ID), unique for each traffic flow, to compute load balancing (or hashing) of traffic in tunnels between ports. Using the TE-ID ensures that load balancing occurs even if the other parameters (such as source or destination address or port, or router ID) don't have unique values, thus achieving a greater distribution of traffic over equal-cost links, allowing efficient distribution of traffic in mobile networks, and providing increased reliability and availability for the network.

Using GTP TE-ID based load balancing rather than LAG round-robin offers the following advantages:

- It does not cause packet disordering
- It is applicable to both ECMP and LAG
- It is supported for all traffic paths, L2 or L3 or MPLS (local handoff or transit)

NPT-2xxx series platforms automatically choose the GTP TE-ID load balancing option. If there is no GTP TE-ID field present, then the hardware automatically falls back to the IP packet-payload based load-balancing scheme.

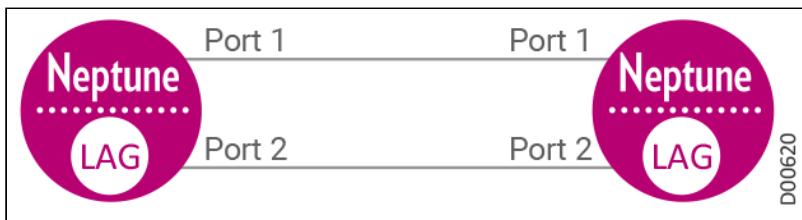
If LAG is used in the context of dual homing protection, ETH I-NNI and MoE ports can be used and the LAG master ports must be connected before slave ports. LAG can be configured for any leg of any protection mechanism (such as ERP or BPDU tunneling). Only the LAG master link is used for service management purposes; slave links are ignored.

There is a limitation regarding PE insertion as this can't be done into an MoE LAG link. The user must first delete the slave links from LightSOFT, perform the insert, and recreate the links.

For information about LAG configuration in a BPDU tunneling network topology, see [Creating Internetwork Dual Homing](#).

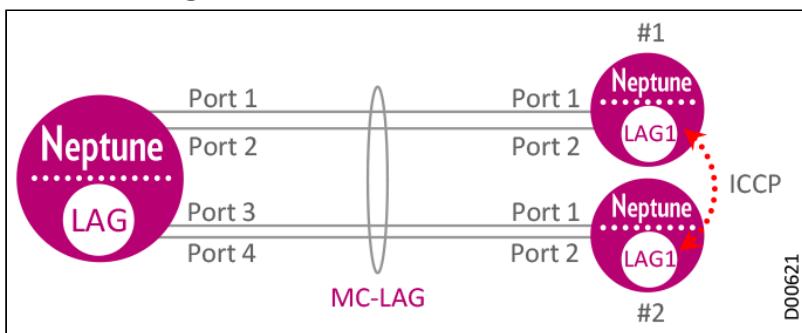
- **Protection (1:1)** provides protection at the service level (similar to MS Linear protection on the SDH/SONET level). LAG 1:1 sends all the traffic through the primary port. If that port fails, then all traffic is shifted to the secondary port. Compatible equipment currently supports protection LAG on ETH ports only.

### LAG Configuration



With LAG protection, the participating ports may both be located on a single card, or located on different cards within the same NE (inter-card LAG (IC-LAG)), or located on different cards installed in two different NE (multi-chassis LAC (MC-LAG)). Participating ports are configured as master ports and share the same LAG identification key. Each port must be provided with the global PE ID of the second corresponding partner port.

### MC-LAG Configuration



When working with multiple ports, the member ports are organized into active and standby port groups, providing both node and link protection as well as load sharing between ports in the active group. MC-LAG can be integrated with other MPLS-TP protection mechanisms, supporting service interworking towards the network either through PW redundancy or as a CCN trigger, as relevant. For example, MC-LAG can be configured in the Ethernet segment and PW-R in the MPLS segment.

### Micro-BFD

Micro-BFD refers to running bidirectional forwarding detection (BFD) over the individual links in a LAG, to monitor the bidirectional health status of the Ethernet links that make up the LAG. Neptune supports BFD on LAG interfaces (RFC 7130). Network operators can configure an independent, asynchronous mode BFD session on every LAG member link in a LAG bundle. This is known as a *micro-BFD* session per link.

- Each micro-BFD session uses its own unique local discriminator values, maintains its own set of state variables, and has its own state machine. The general BFD session parameters, configured at the global level for a protocol or application, also apply to the micro-BFD sessions.
- A LAG member cannot be made operational within the LAG until the micro-BFD session is fully established.
  - Micro-BFD sessions must be established between both endpoints of a link before the link can be operationally up.
  - If the micro-BFD session fails, the associated Ethernet link becomes operationally down and is taken out of service from the perspective of the LAG.
  - If LACP is not enabled for the LAG, then if the Ethernet port is up, the system attempts to re-establish the micro-BFD session with the far end of the link once LACP reaches distributing state.
- If a link is not active for forwarding from the perspective of a LAG, ARP can still be performed across the link. For example, when a link is being brought up, and its micro-BFD session is not yet established, ARP can still be performed for the MAC address at the far end of the link, even though the link is not yet part of the LAG.
- Micro-BFD packets bypass ingress and egress sub-interface/interface ACLs, but received micro-BFD packets can be matched by ACL filters for filtering and logging.
- State changes of each micro-BFD session should be reported as an event.

## Multichassis LAG MC-LAG Protection

MPLS tunnels in the transport layer provide connectivity between the PEs or CEs, including protection against failure of a transport entity, whether link or intermediate node.

However, the transport layer cannot provide protection against failure of an edge node, where the service end point is located. A redundant service end point is required, forming a dual (or multi) homing topology. PW redundancy is the standard mechanism for such a topology.

PW protection is implemented through the use of PW pairs, with one PW active and the second PW kept on standby in case of need. PW status messages are signaled between PW endpoints, with the standby PW activated as needed.

P2MP services, consisting of a hub with multiple spokes, require a high level of resiliency. When dual hubs are used, PW redundancy enables hot-standby connectivity between each spoke and the currently active hub. This dual homing assures traffic flow by preventing single points of failure (SPoFs).

### MC-LAG Table

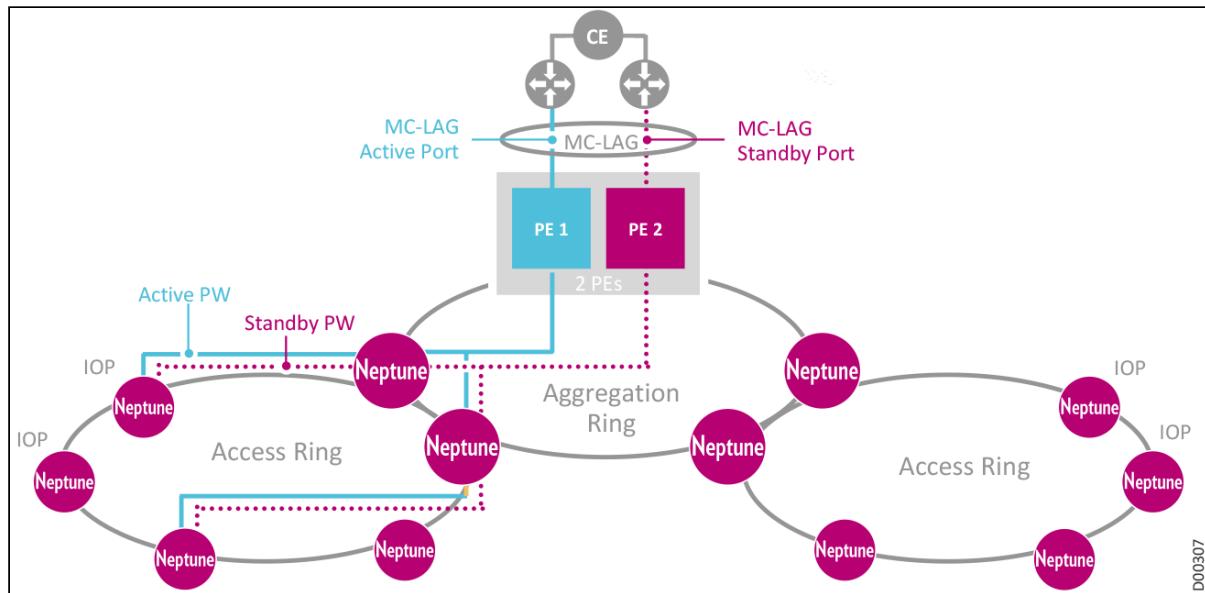
MC-LAG Table					
MC-LAG ID	Port1	Port2	Add PW	MC-LAG Trigger Enabling	
1	Sec: 1800-77:TS23:DHGE_...	Pri: 1800-48:TS23:DH...	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

PW redundancy is coordinated with MC-LAG to connect the two hubs with customer edge (CE) devices, where each hub is based on a data card located on a different device.

**PW protection interworks with MC-LAG for complete end-to-end protection, providing protection from access nodes to core termination nodes.**

In the following redundant configuration example, Ethernet links from the CE to data cards on two different hubs are aggregated using MC-LAG.

## MC-LAG and PW Redundancy

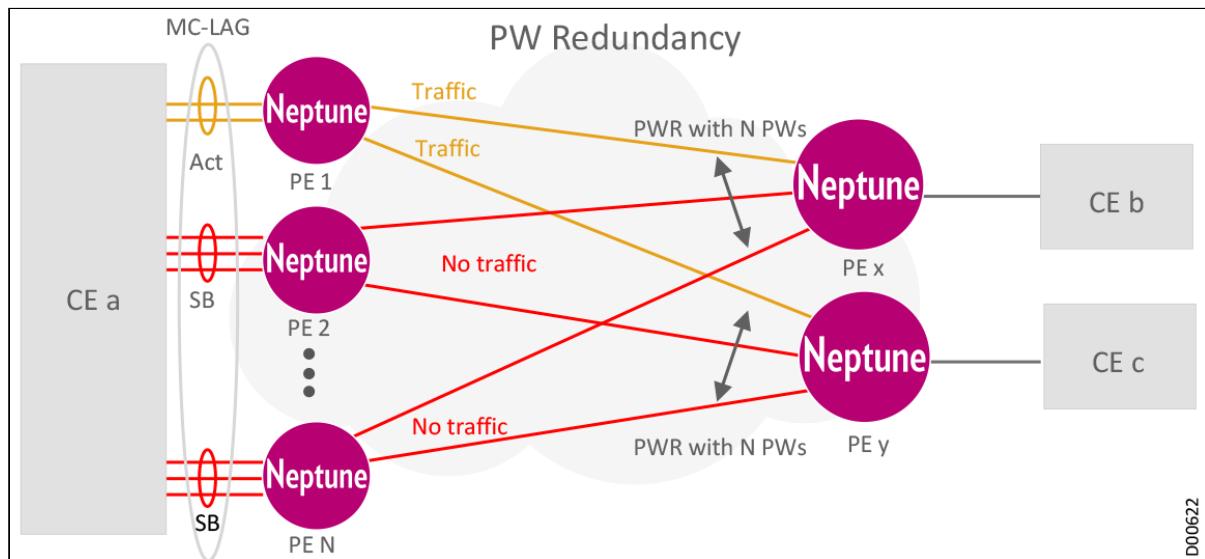


Note that both IP and MAC address hashing is supported on the LAG as well as MC-LAG on the data cards. In addition, the standby link can be disabled to force the LAG partner to forward traffic on the alternate link.

The MC-LAG and PW protection mechanisms utilize standardized implementation based on **IEEE 802.3ad/802.1AX**. The platforms also support the **multichassis link aggregation control protocol (mLACP)**, which defines the redundancy implementation. mLACP functionality extends 802.3ad/802.1AX LACP.

### Example: MC-LAG with PW-R

#### MC-LAG with PW Redundancy Example



## Dual Homing DH

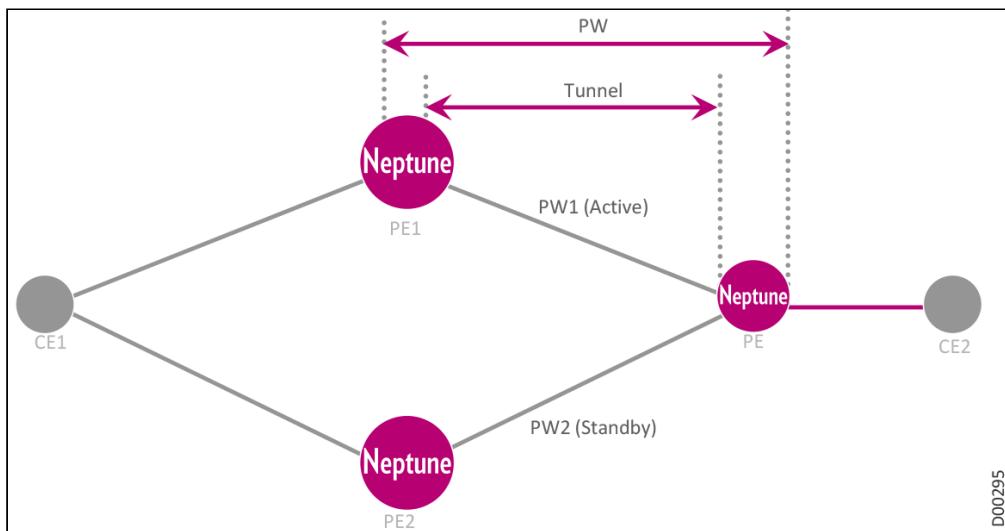
Dual homing (DH) provides a useful protection mechanism that can be applied in many different network contexts. This section describes two typical network examples.

### Single Dual-Homed CE Topology

In single dual-homed CE topology, a CE (CE1) is dual homed to two PEs (PE1, PE2). This topology includes the following features:

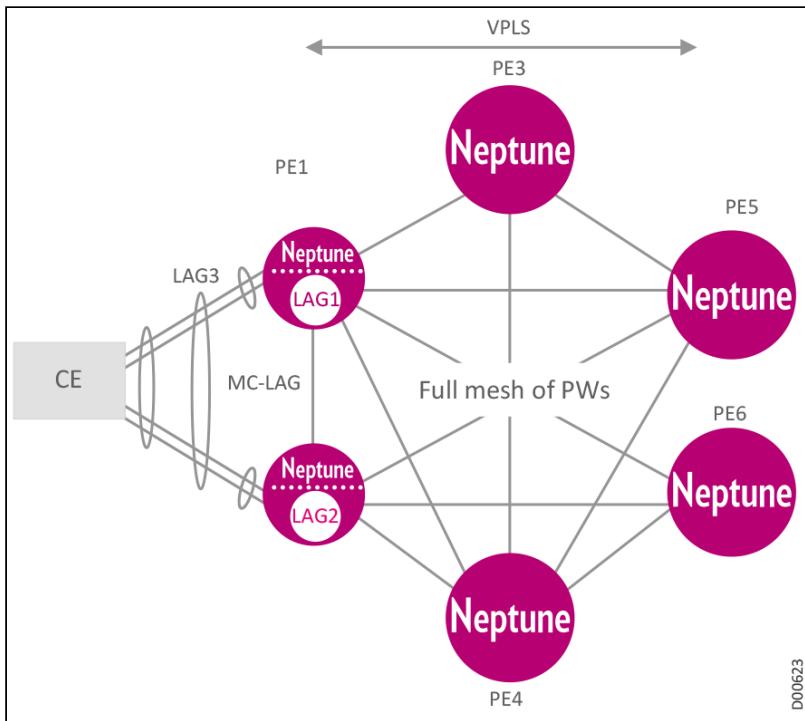
- Service between CE1 and CE2 can be either P2P, P2MP, or MP2MP.
- Protection against failure of the service endpoint port (CE1-PE1 or CE1-PE2) is provided through a dual homing protocol (MC-LAG) implemented between CE1 and the two PEs. An interworking function between the MC-LAG protocol and PW Redundancy ensures that one active PW is always connected to the active service port.
- Protection against failure of one of the PEs attached to the dual homed CE (PE1 or PE2). MPLS-TP tunnel OAM (BFD protocol) is used between PE1-PE2 to monitor the status of each PE. PE failure is identified by BFD and reported to MC-LAG and PW redundancy for proper actions.
- Protection for the transport layer (excluding failure of the service end point PE) is provided through FRR or 1:1 linear LSP protection. Such a failure does not affect the choice of active PW. Failures in the transport network do not propagate to the attached CE.

#### Single Dual-Homed CE Topology



#### Dual-Homing to a VPLS Network

### Dual Homing to VPLS Network

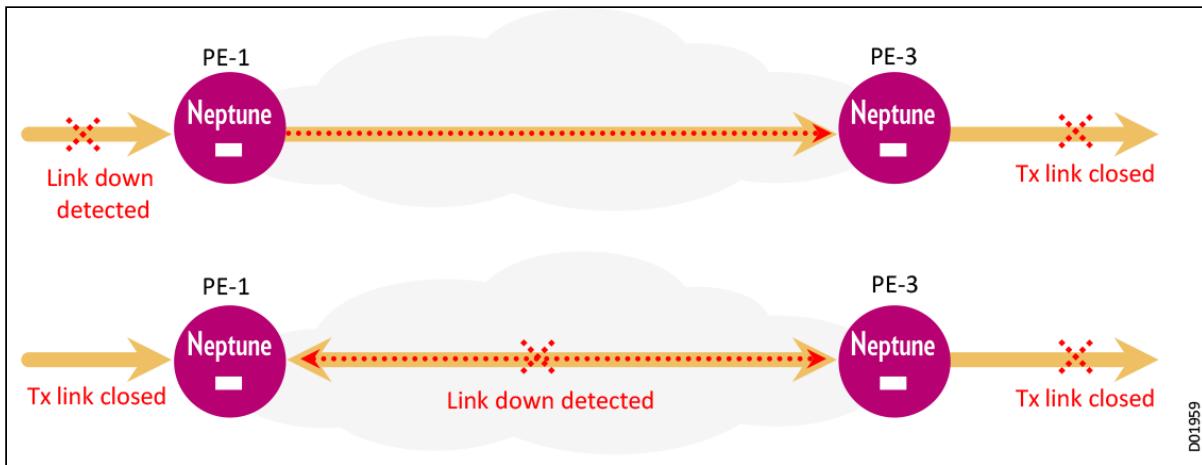


## Link Loss Carry Forward LLCF

Link Loss Carry Forward (LLCF) is a method for ensuring traffic flow continuity with minimal disruption even if a link goes down. LLCF assists in troubleshooting remote connections and provides an early indication of failing links in router interconnections. The basic approach is similar to that of Client Signal Fail (CSF)/Trail Signal Fail (TSF) solutions in pure SDH/SONET networks, where the port status is transferred end-to-end through Layer1 network connections.

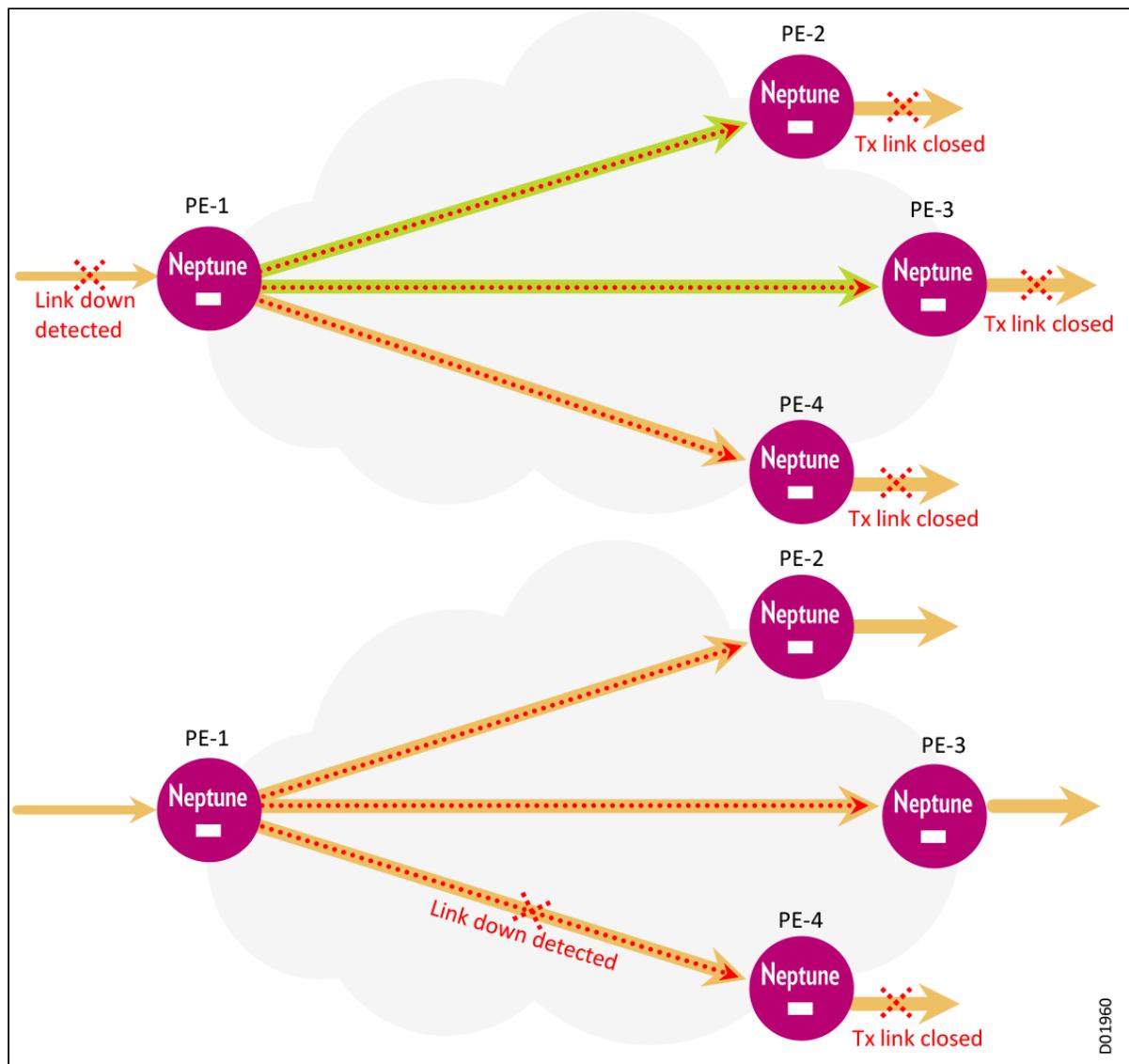
LLCF, implemented in MXP10 cards, enables efficient protection and troubleshooting functionality for P2P and P2MP services. Bidirectional LLCF is supported by configuring two independent LLCF connections between the same endpoints, one in each direction. In this case, port failures on one side of the service are always reflected at the other end of the service. This is particularly useful for router interconnection, which requires fast detection of Loss of Connectivity between the routers. LLCF is usually enabled or disabled during CFM configuration.

### LLCF in P2P Configuration



The platform data cards implement LLCF using standard CFM to transport the port status from the LLCF trigger to the LLCF client. Continuity check messages are used to send the port status end-to-end. The client port status is changed within 50msec of a change in the trigger port. LLCF in P2MP hub and spoke configurations may reflect links down at two different levels: on the link coming in to the hub node, or on any of the links between the hub node and the spokes. This is illustrated in the following figure.

### LLCF in Hub and Spoke Configuration



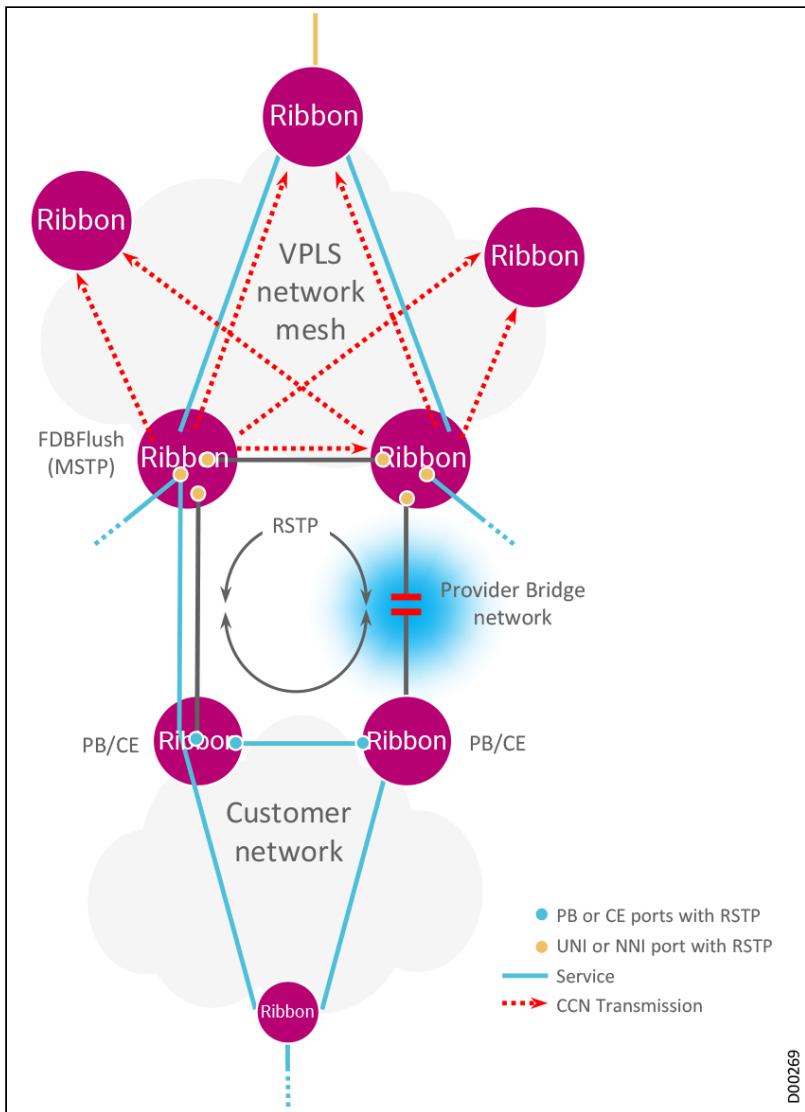
## Customer Change Notification CCN

Communication networks are dynamic entities. On a macro long-term level, networks are constantly growing and evolving over time. On a micro immediate level, networks are constantly reconfiguring their path and tunnel configurations in response to changing network traffic conditions and equipment status. Dynamic networks must be agile, able to react in real time to changes in network status.

A common approach is to handle dynamic network status changes using an LDP MAC Withdraw mechanism. Neptune data cards offer a more effective approach by providing CCN capabilities. Topology changes, such as a temporary link down triggering an RSTP/MSTP recovery action, automatically trigger messages notifying remote PEs of changes in the network topology. Change notification messages are distributed to all VPLS peers.

Intelligent configuration rules make sure that data is transmitted responsibly, without confusion from unnecessary multiple notification messages and without affecting uninvolved traffic. Neptune data cards support selective FDB flush, whereby CCN messages trigger a selective flush of only specific FDB entries whose source was the PE that originally triggered the topology change.

## CCN Functionality



D00269

## CCN Forwarding

In some H-VPLS dual homing topologies, when there is a need for CCN to cross VPLS domains, CCN forwarding can now be enabled on the relevant NEs.

CCN forwarding enhances message transfer capabilities, while keeping the networks efficiency and protection. CCN messages are transmitted from PEs that detect a network topology change to update their local and remote PE peers based on the recipient PE IDs.

In simple network topologies the PE CCN message initiator "knows" the peer IDs residing in the same domain. When the peer PEs are part of an H-VPLS topology or, in other cases, part of a Dual-Homed H-VPLS topology, located in two different domains, the initiator is not aware on their ID, because of the hierachal structure of the network.

By configuring the relevant PEs in the network for CCN forwarding to Enabled, messages can traverse between the domains and deliver the required messages to the peer PEs.

## Resilience and High Availability

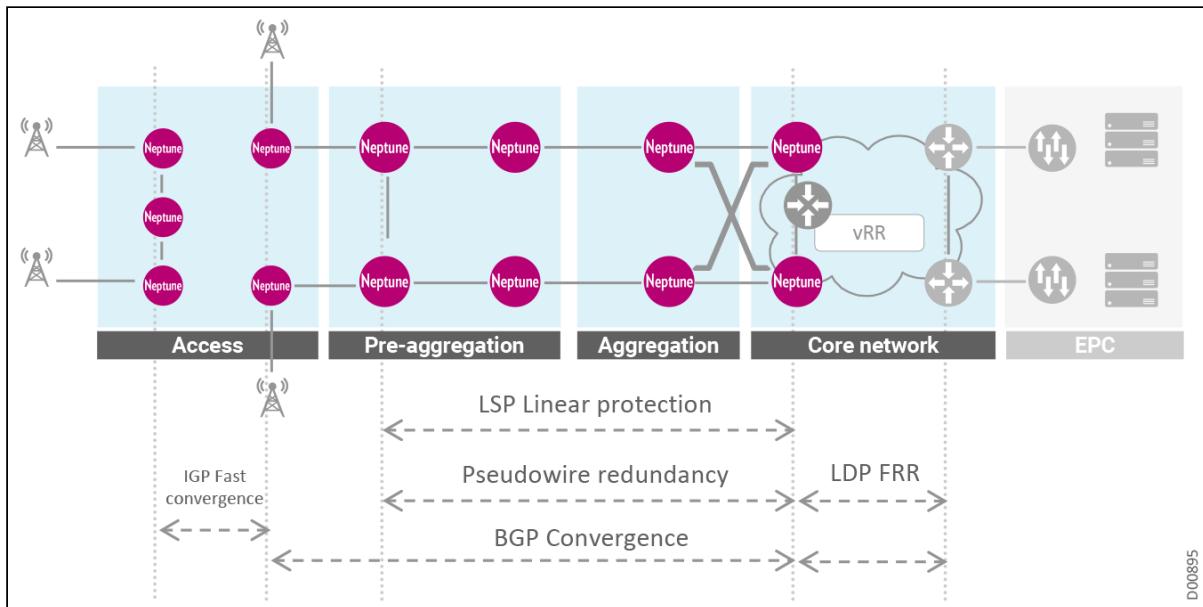
Network protection and resiliency are critical to telecom network functionality. Neptune platforms provide a comprehensive set of end-to-end protection and restoration mechanisms for every aspect of your network configuration, based on the complete range of technologies.

Neptune platforms utilize independent control and data planes and support nonstop forwarding, to minimize traffic outage in case of control plane failover. All dynamic protocols implemented in the solution support graceful recovery to allow routing instance restart in case of node/control plane failure.

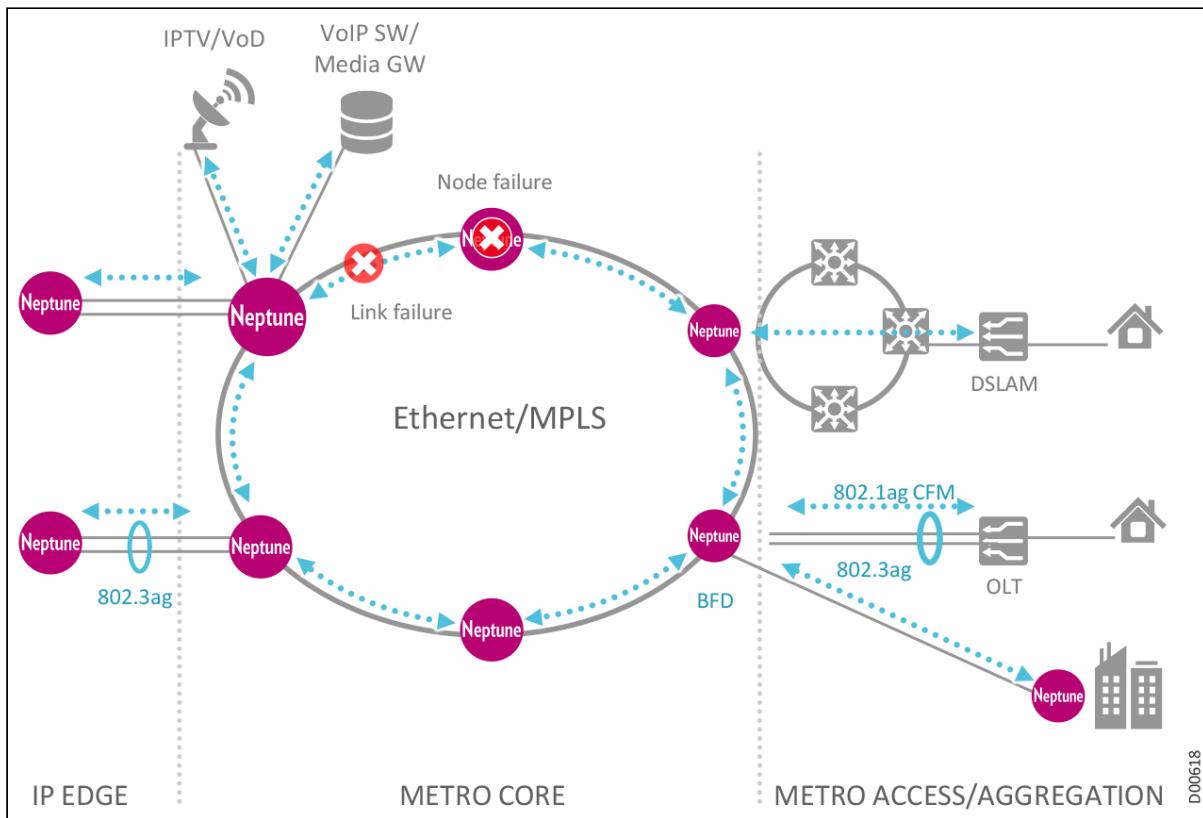
The MPLS VPN services between the access and core aggregation layers implement the following mechanisms for improving network availability:

- For UNI connections at the access layer:
  - Ethernet Link Aggregation (LAG) protection, based on standard Ethernet link aggregation schemes (IEEE 802.3ad), can be employed, with Link Aggregation Control Protocol (LACP)
- Node protection
  - Multichassis Link Aggregation Control Protocol (mLACP) port-bundles are utilized; mLACP functionality extends 802.3ad/802.1AX LACP
- MPLS connection layer: Infrastructure LSPs (dynamic and static) can be protected, utilizing either:
  - LDP-FRR (based on IP LFA, IETF RFCs 5286, 5714, and 6571)
  - Linear Protection (RFC 6372) allowing for:
    - Protection for bidirectional co-routed E LSPs
    - Protection State Coordination (PSC) protocol to synchronize both ends of a tunnel. Protection triggers include:
      - Local faults (server indication)
      - Link failures
      - LDI indication from intermediate points to the end point
      - BFD OAM mechanisms per LSP
- MPLS Pseudowire layer:
  - Pseudowire Redundancy (RFC 6718)
  - Pseudowire Status Propagation as described in RFC4447 and RFC6310  
PW status messages are sent in-band through PW OAM messages that carry the PW status for a particular PW. The PW status is monitored and propagated as relevant. An awareness of the PW status enables more efficient switching decisions, based on real-time knowledge of the PW's actual status.
- IP layer: BFD rapid failure detection and IS-IS/OSPF extensions for fast IGP (sub-second) convergence

## Protection Mechanisms



## Carrier Class Network Resiliency

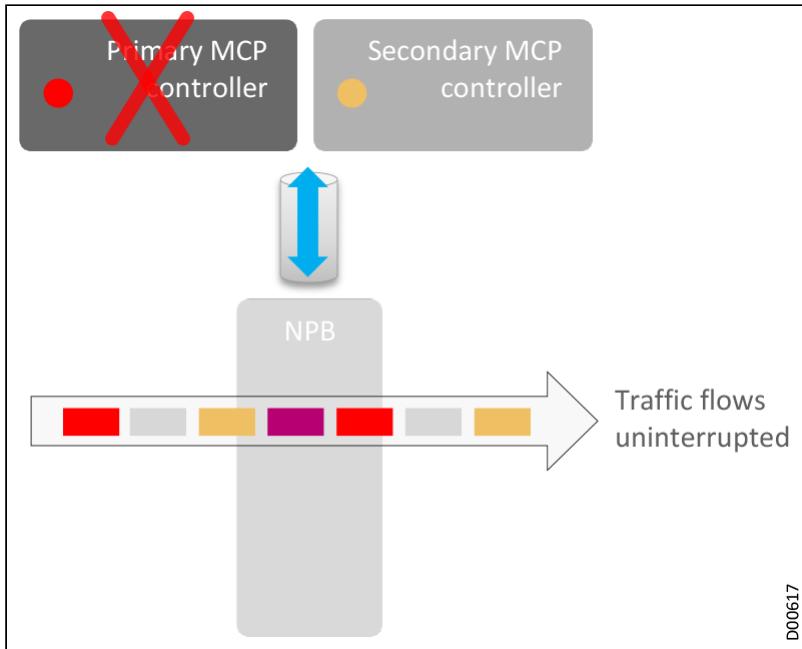


## High Availability through Nonstop Forwarding

To ensure completely uninterrupted traffic flow and a five 9s standard of high availability, Neptune platforms utilize independent control and data planes with full central components and link redundancy, multi-layer hardware support for fast failovers, optimized architecture for hitless maintenance functions, and automatic

synchronization for graceful restarts in dynamic network topologies. Neptune meets the highest standards of reliability and availability with redundant hardware, failure isolation, parallel recovery capabilities, and live software upgrades.

### Uninterrupted Traffic Flow



Every system component is fully in-service upgradable with no interruption of existing services. This includes adding lines to an existing line card, adding or replacing line cards, protecting fabric, pluggable optics, and a power supply. Configuration changes required for expansion do not impact existing services. Cards and other shared buses and common components can be taken in and out of service without impacting system functionality. The only traffic affected during a hot swap is that carried by the card being removed. Card insertion creates no errors on active traffic passing through the other components.

All systems, including processor cards, are optionally fully redundant. The fabric protection with automatic synchronization enables graceful recovery and restart within a dynamic network topology. Supported protocols include:

- **Border Gateway Protocol (BGP):** A BGP peer retains routing information from a neighboring peer when it goes down for a certain length of time. When it comes back up and the router receives refreshed routing information, it compares the new information with that retained. The router can thus preserve the routing state of BGP even during short peer outages.
- **Open Shortest Path First (OSPF):** An OSPF router remains on the forwarding path of the network while restarting OSPF. The amount of LSA flooding and consecutive updating that consequently occurs is minimized.
- **Intermediate System to Intermediate System (IS-IS):** An IS-IS router remains on the forwarding path of the network while restarting the protocol. The amount of LSP flooding and consecutive updating that consequently occurs is minimized.
- **Label Distribution Protocol (LDP):** Label Switching Routers (LSRs) preserve the label mappings of an LDP tunnel while the signaling LDP routers restart, thus preserving the state of LDP tunnels during short outages.

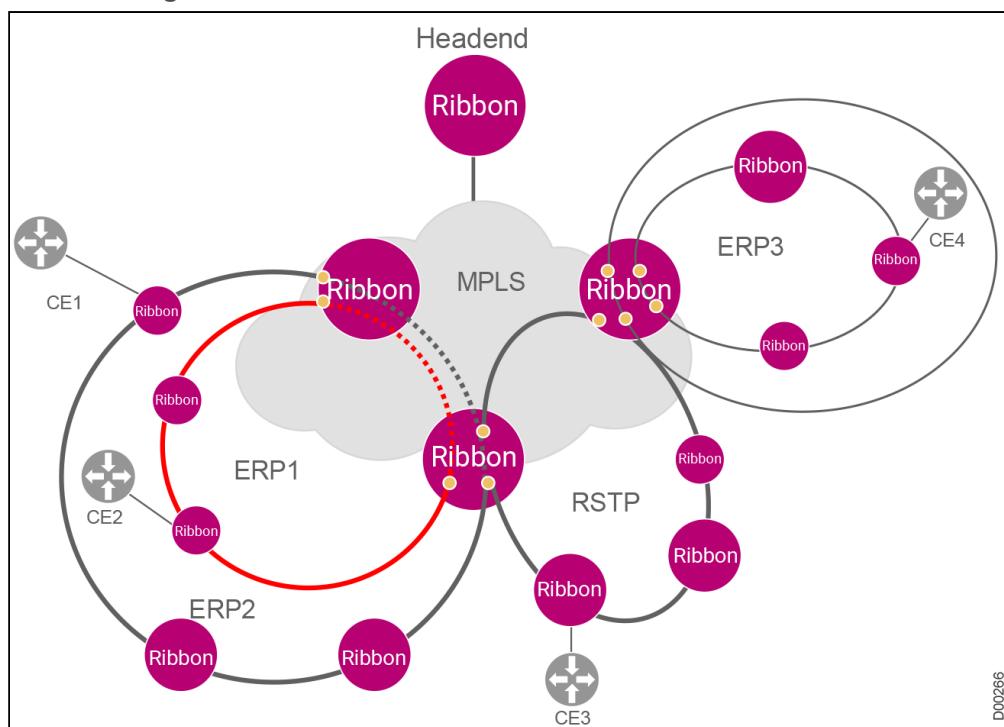
Neptune ensures highest availability by providing multiple methods of minimizing downtime and interruptions on the system and the network.

## Ethernet Ring Protection Switching ERPS PB

Ethernet Ring Protection Switching (ERPS) is an enhanced protection mechanism for Ethernet networks, defined by ITU-T G.8032 V1 standard. It supports improved resiliency, manageability, and reliability of metro Ethernet networks, offering switching to protection time in less than 50msec. The standard has the ability to protect against both link and equipment faults.

Each node in the ring protection network has two ring ports (East and West) and a number of local ports. One link in the ring is designated as the Ring Protection Link (RPL) and used only for redundancy. One node, connected to the RPL, is selected as the RPL owner, and is responsible to block traffic on the RPL in normal operation (idle state) and unblock it when a failure is detected (protection state).

### Ethernet Ring Protection



When the failed link recovers, the nodes adjacent to the recovered link transmit a R-APS No Request (NR) message, indicating they have no local request. When the RPL owner receives the R-APS message it starts a Wait to Restore (WTR) timer. Once the WTR expires, the RPL owner blocks the RPL and transmits a R-APS (NR, RB) No Request, Root Blocked message. The nodes receiving the message perform a selective FDB flush for the relevant port and unblock their previously blocked port. The ring returns to normal operation (idle state).

Neptune data cards support G.8032 V1 ERP in addition to RSTP protection, providing a valuable service for customer applications by enabling sub-50msec protection for Ethernet rings, adding an important level of protection for customer applications.

While MPLS networks provide carrier class sub-50msec protection, PB networks have not yet reached that level of protection. Current xSTP technology cannot provide sub-50msec protection. Yet most data network configurations include PB rings, typically in the access level. With G.8032 support, network operators are able to benefit from carrier class sub-50msec protection over their entire data network configuration, including both the MPLS and the PB rings.

Our Ethernet ring protection provides standard compliant protection for I-NNI ports and also for E-NNI ports, added as of V7.6, for IP/MPLS platforms. Protection is implemented per port for multiple rings. Up to 16 instances can be defined per card. Protection is provided across product lines, implemented through data cards in the Neptune, XDM, and BroadGate platforms.

## RSTP-MSTP Protection

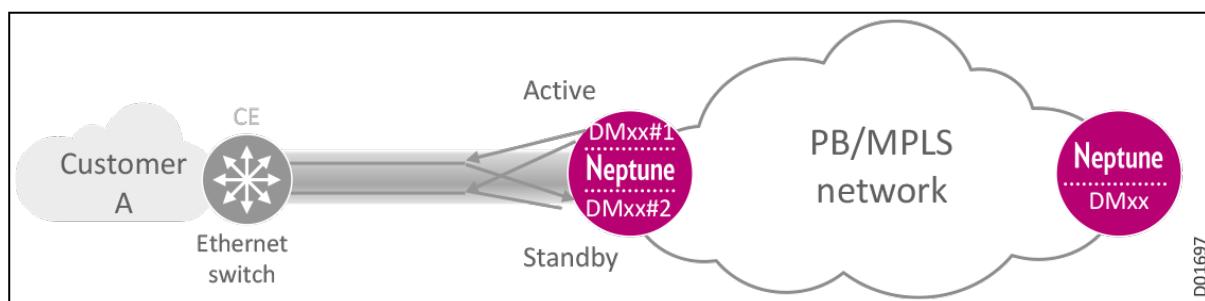
Neptune platforms offer complete RSTP 802.1D-2004 compliance and interoperability, supporting RSTP on UNI, I-NNI, and E-NNI ports. Neptune platforms also provide the ability to close access RSTP/MSTP rings over MPLS networks. This is accomplished through the data cards, which are able to participate in the access RSTP/MSTP ring and also forward the BPDUs over the relevant MPLS networks.

Neptune platforms provide intelligent efficient responses to RSTP/MSTP ring topology changes through the use of [CCN messages](#), which enable flushing of remote PEs on the core MPLS network as a result of topology changes in the remote access RSTP/MSTP rings.

## Input-Output Protection IOP

### Fast IOP: 1:1 Card Protection

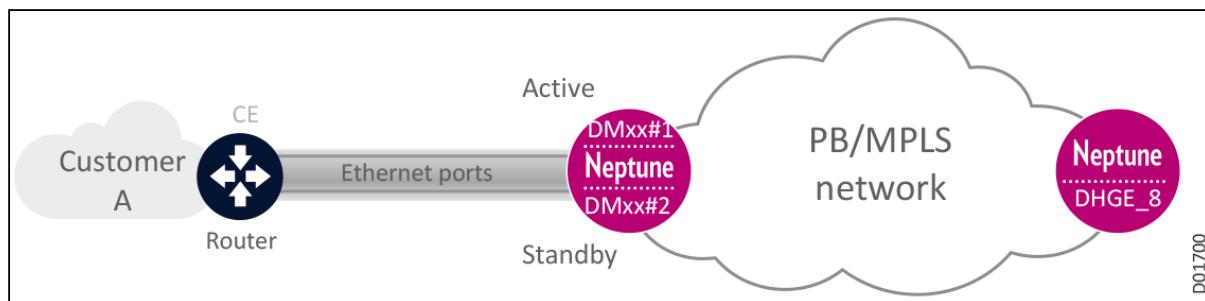
#### Fast IOP Protection



#### Enhanced IOP (eIOP)

Neptune data cards (such as DMGE\_4\_L2/DMGE\_8\_L2/DMXE\_48\_L2 and DMXE\_22\_L2) support Enhanced IOP (eIOP) functionality, with switchover triggered by link failures (LOS) in addition to the standard node failure triggers. Adding LOS as an IOP trigger enhances IOP functionality, freeing up a port on each participating card for carrying additional traffic. This is explained in the following example.

#### Enhanced IOP Example



With traditional Fast IOP, a link failure between DM #1 and the router would result in traffic loss, since DM #2 remains designated as standby. This means that the router would not be able to find any route available for traffic. To prevent this loss of traffic, the links are configured over splitter/coupler cables that link both cards to the router ports (see illustrated in the figure Fast IOP Protection).

DM cards resolve this problem through the use of eIOP, by adding LOS as an IOP trigger on selected LAN ports. With eIOP, a failure on the link to the active DM card triggers an IOP switchover. DM #2 becomes active and activates transmissions on the LAN ports. The router detects this link is now up and sets/advertisess a new traffic route. Traffic is restored.

With eIOP, the splitter/coupler cable is no longer required. A regular fiber cable can be used between the DM cards and the router, as illustrated in the preceding figure. This frees a port on each DM card to carry additional traffic.

# Optical Protection Mechanisms

Protection is of the utmost importance in the high-capacity traffic transmitted through WDM systems. Neptune features a variety of optical protection options, enabling network operators to choose the protection scheme most useful for their network configuration.

## Network Protection

The MXP10 card can be used to protect P2P services against network failures (fiber cuts) with OCH 1+1. In this mode, a single user interface can connect to a single client port, while the traffic is transmitted from two line interfaces on the same MXP10 card.

## Full Equipment Protection

The MXP10 as a multi-rate combiner for standard P2P service supports OCH 1+1 with full equipment protection.

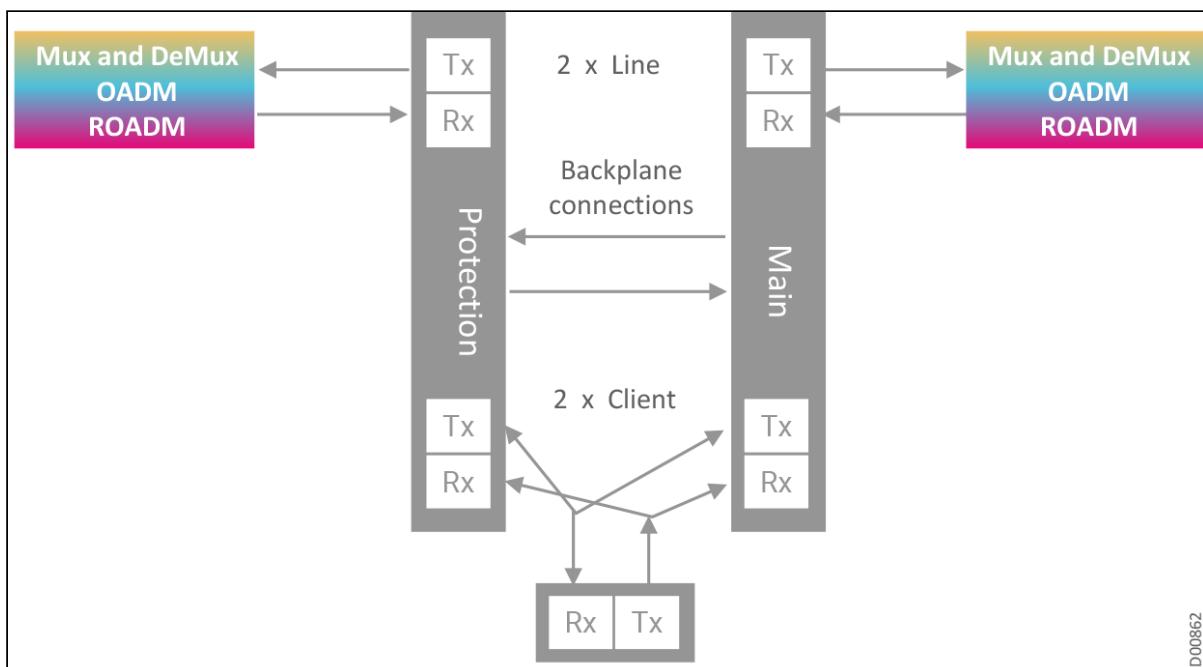
The MXP10 offers the option of arranging double line aggregates on separate cards with two clients connected to a single client interface. This configuration requires card installation in adjacent slots and a splitter/coupler or Y-fiber to connect the client interfaces.

## OCH Protection

Neptune provides port protection very similar to its path protection mechanism. By using double transponder/combiner cards, a dual-traffic path goes around the ring and is received by both the main and the protection transponder/combiner. Both perform continuous PM to ensure channel integrity.

If PM on the main transponder/combiner does not indicate a problem, a message is sent through the backplane to the protection transponder/combiner for it to shut down its laser to the client, thereby ensuring transmission to the client from only one transponder/combiner (the main). Protection switching to the protection transponder/combiner occurs automatically when a failure is detected by the main transponder/combiner.

## OCH 1+1 Port Protection



OCH port protection is currently the most popular optical protection method for the optical layer. The mechanism transports each optical channel in two directions, clockwise and counterclockwise. The shortest path is defined as the main or working channel; the longer path as the protection channel.

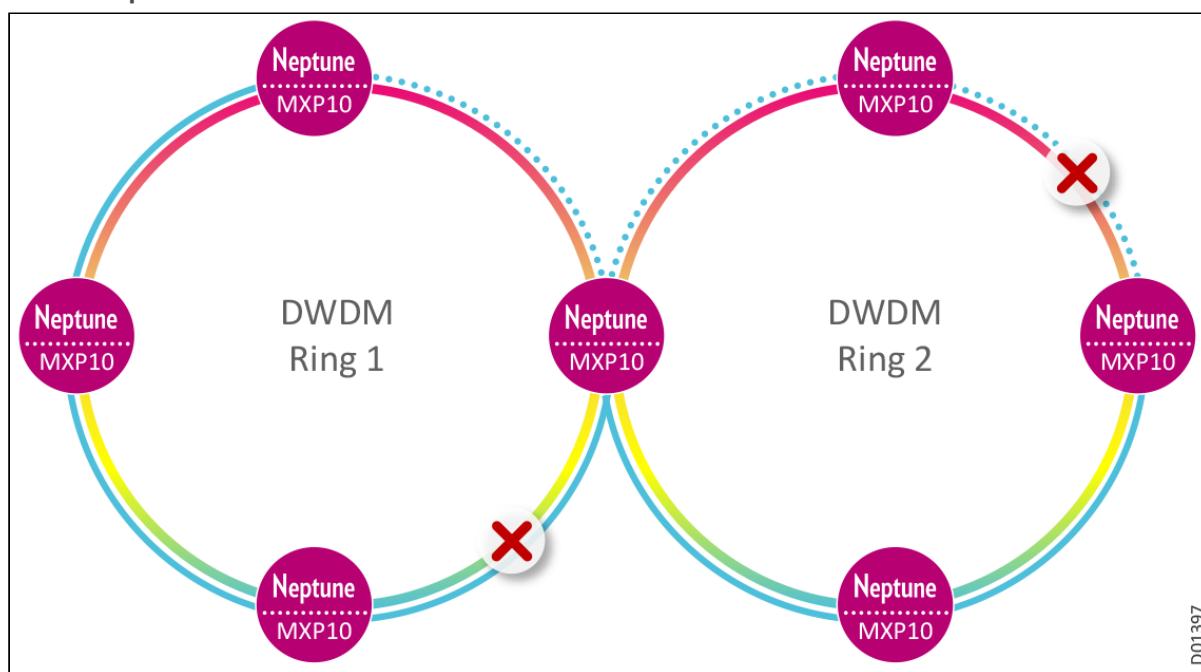
The main benefit of OCH port protection is its ability to separately choose the shortest path as the working path for each client port. There are no dedicated working and protection fibers. Each fiber carries traffic with both working and protection signals in a single direction.

The OCH 1+1 port protection scheme provides separate protection for each client port. For SDH/SONET, GbE, and 10G, protection switching is based on PM parameters. Switching criteria can be Loss of Signal (LOS), Loss of Frame (LOF), or Degraded Signal (SD). The switch-to-protection mode is automatic when a malfunction is detected in a single channel. This is very convenient as users can choose the client ports to be protected, as well as choosing the main or protection paths. Switch-to-protection time in the OCH1+1 port protection scheme is less than 50msec.

### Optical DRI Protection

When used in ring applications, the MXP10 supports optical DRI protection. (Note that inter-ring traffic is through client ports.)

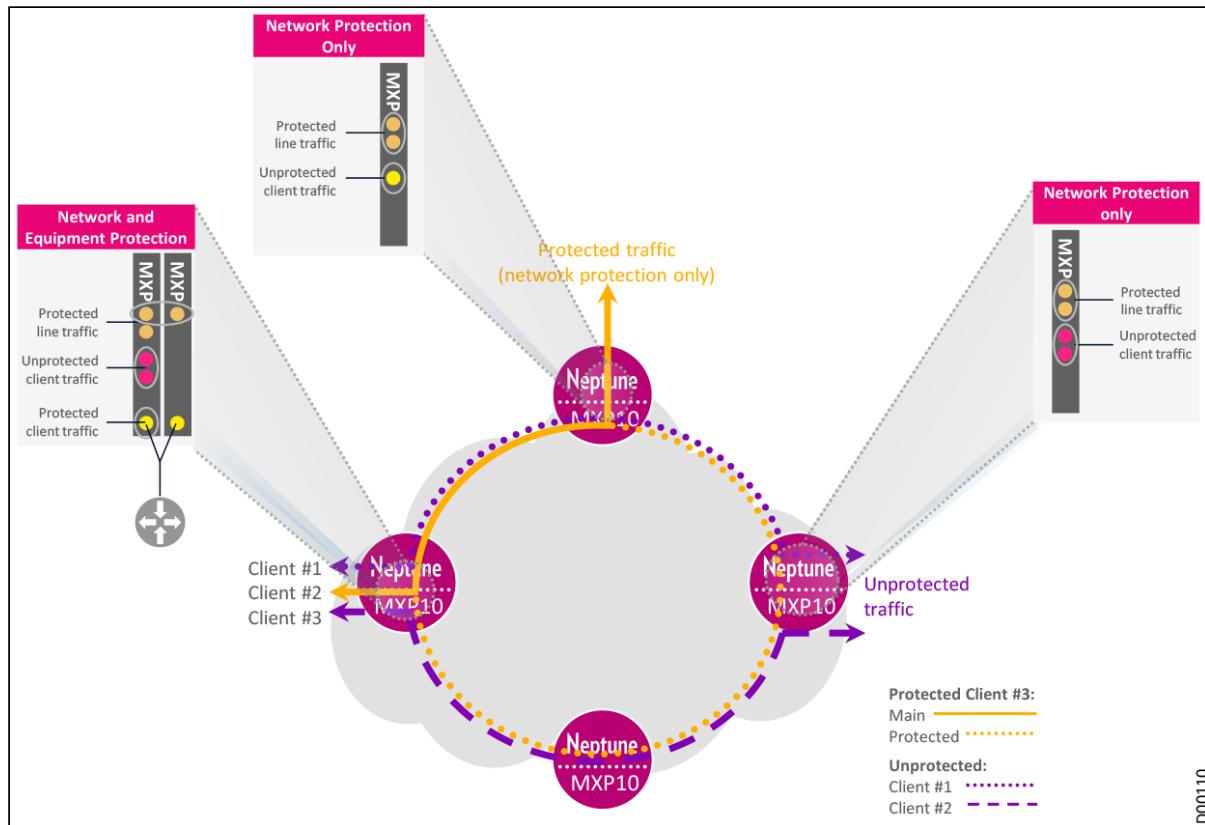
#### MXP10: Optical DRI Protection



### Mixed Protection Schemes

When used in ring applications, the MXP10 supports a mixture of network and/or equipment protection schemes.

### MXP10: Protection Mixture



With the MXP10, you may choose any combination of protected network traffic, unprotected traffic, fully protected traffic including client port protection, and so on. Dual homing from access to ring is also supported.

## Tributary Protection TP Mechanism

Neptune platforms support Tributary Protection (TP) by protection cards, installed in the expansion units (EXT-2U or EXT-2UH). This provides protection for tributary card failures, such as card power-off, card out, BIT fail, and so on. The protection scheme can be either 1:1 or 1:2. Protection is configured by defining a Protection Group (PG), as follows:

- Protecting card: Only one tributary card can be selected as the protecting card. This card should have no existing trails. The protecting card can be located in any slot.
- Protected cards: One (1:1) or two (1:2) tributary card(s) can be selected as protected cards. A protected card can have existing trails. This means that TP can be configured for a card that is already carrying traffic, without removing existing traffic.
- Associate the protecting card and protected cards.

For example, the **TP32\_2**, installed in the expansion platform, provides 1:1 or 1:2 protection for 32 x E1 interfaces on MSE1\_32 cards installed in the corresponding base unit (NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms). Latched relays are used to redirect the traffic connections between customer connections and internal connections, so that a redirecting cable is not required when a switch is triggered for the protected card. Warm reset is supported; traffic is not affected when the software is restarted.

The TP32\_2 provides the following connectors on the front panel:

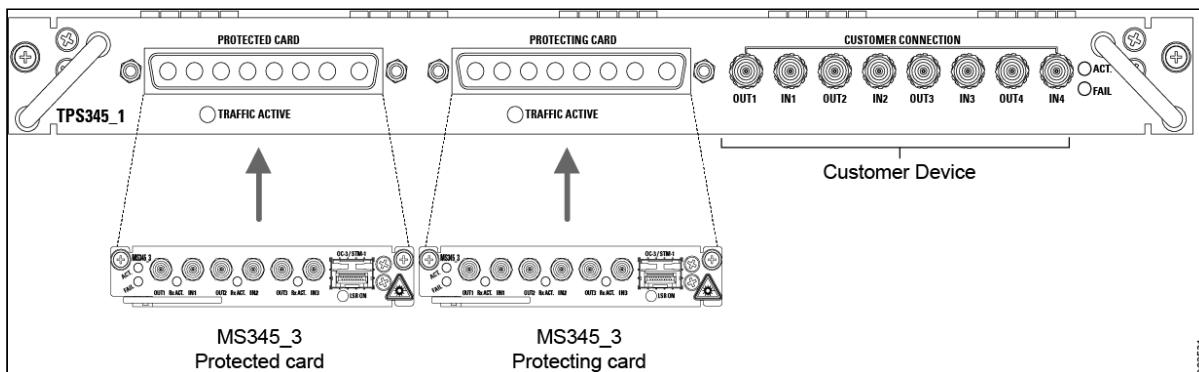
- **Protected Card 1:** One SCSI connector for connecting to protected MSE1\_32 card #1
- **Protected Card 2:** One SCSI connector for connecting to protected MSE1\_32 card #2
- **Protecting Card:** One SCSI connector for connecting to the protecting MSE1\_32 card

- **Customer Connection 1 and Customer Connection 2:** Two SCSI connectors for external customer E1 connections

The TP32\_2 card provides bidirectional redirection for traffic, based upon instructions from the APS controller. By default, traffic from customer connection #1 is directed to protected card #1, and traffic from customer connection #2 is directed to protected card #2. Traffic of either customer connection can be redirected to the protecting card.

The **TPS345\_1** provides 1:1 protection for MS345\_3 cards installed in the corresponding base unit (NPT-1050, NPT-1250, NPT-1300, or NPT-1800 platforms). The protection mechanism is similar; customer connections are available for external customer devices, as well as 2 connectors for 2 MS345\_3 cards, one to be protected and one to do the protecting.

### TPS345\_1 Protection Mechanism



Similarly, the **TPU345\_24\_1xx** cards provide 1:1 protection for the MS345\_24 cards installed in the corresponding base unit. The protection mechanism is similar; customer connections are available for external customer devices, as well as 2 connectors for 2 MS345\_24 cards, one to be protected and one to do the protecting.

## Equipment Protection

Neptune's high-level reliability is achieved through comprehensive equipment redundancy on all units (common units, traffic units, I/O cards, and network connections). Automatic protection switching is initiated by a robust internal BIT diagnostic system.

### Common Units

Neptune provides 1+1 and 1:1 protection of the power supply, central switches, and fan units.

### Traffic Unit (I/O card) Hardware Protection

Data cards also offer 1:1 hardware protection. Optical interfaces are duplicated using splitter/coupler devices (Y-fibers or dedicated splitter modules) and electrical interfaces are protected using an external switch.

### Cross-Card MSP 1+1 Protection

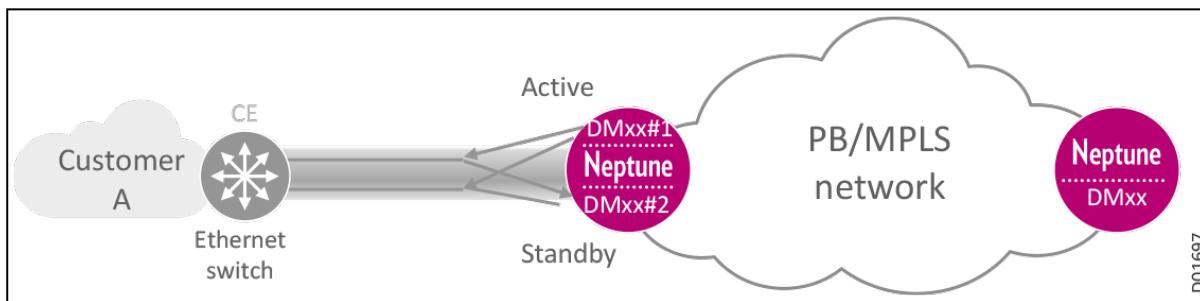
CES cards can be configured to provide cross-card MSP 1+1 protection in under 50 ms. For example, in the NPT-2300, you can install two MS1\_4 cards, to provide MSP 1+1 protection for either 4 x STM-1/OC-3 or 1 x STM-4/OC-12 interfaces. Cross-card protection is available through MSC\_2\_8, MS1\_4, MS345\_3, and MSC\_2\_16E cards.

### Fast IOP: 1:1 Card Protection

Fast IOP offers the reliability of 1:1 card protection. The protection card is kept on hot standby, ready to step in immediately, with no delay required for card synchronization. All tables, including FIB, RSTP, etc., are kept updated between the active and standby cards. Fast IOP can be used in both revertive and non-revertive mode. Card protection is based on BIT, card plug-out, and manual switching through the management

system. In Fast IOP for optical links, the links are connected with Y-fiber splitters and couplers. In Fast IOP for electrical links, the links are connected through switches.

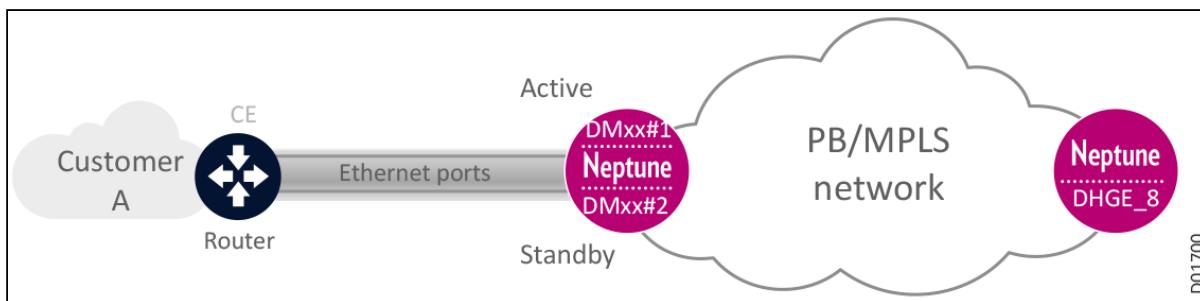
### Fast IOP Protection



### Enhanced IOP (eIOP)

Neptune data cards (such as DMGE\_4\_L2/DMGE\_8\_L2/DMXE\_48\_L2 and DMXE\_22\_L2) support Enhanced IOP (eIOP) functionality, with switchover triggered by link failures (LOS) in addition to the standard node failure triggers. Adding LOS as an IOP trigger enhances IOP functionality, freeing up a port on each participating card for carrying additional traffic. This is explained in the following example.

### Enhanced IOP Example



With traditional Fast IOP, a link failure between DM #1 and the router would result in traffic loss, since DM #2 remains designated as standby. This means that the router would not be able to find any route available for traffic. To prevent this loss of traffic, the links are configured over splitter/coupler cables that link both cards to the router ports (see illustrated in the figure Fast IOP: 1+1 Card Protection).

DM cards resolve this problem through the use of eIOP, by adding LOS as an IOP trigger on selected LAN ports. With eIOP, a failure on the link to the active DM card triggers an IOP switchover. DM #2 becomes active and activates transmissions on the LAN ports. The router detects this link is now up and sets/advertisises a new traffic route. Traffic is restored.

With eIOP, the splitter/coupler cable is no longer required. A regular fiber cable can be used between the DM cards and the router, as illustrated in the preceding figure. This frees a port on each DM card to carry additional traffic.

# NE Security

Comprehensive security mechanisms protect both the complete transport network and individual clients within the network. We are committed to incorporating powerful, advanced security technology and methodology across the full range of our product offering.

The current Neptune release includes a strong set of security features, with additional key security enhancements now in development, to be implemented in upcoming releases. The main security functions are implemented through the following functionality:

- Kerberos, Radius, and TACACS+ clients (authentication, and two levels of authorization - viewer and administrator)
- SSH V2.0 and SFTP
- SW integrity based on SHA-2
- Public key authentication for NEs
- MD5 authentication for control plane and routing protocol (OSPF, IS-IS, LDP)
- Role based access control (RBAC) for CLI users

The EMS system can be upgraded to apply enhanced security settings to the EMS and to selected NEs managed by the EMS. Communication channels between entities with enhanced security settings are secured and information sent via SSH2 protocol.

For more information about the security features built into our platforms, see the *Neptune Security General Description*.

This section introduces the following topics:

- Comprehensive Security Mechanisms
- MACsec 802.1AE
- Port-Based Network Access Control 802.1x
- MAC Authentication Bypass MAB
- TACACS+
- Firewall Filters
- Dynamic ARP Inspection DAI
- Enhanced Security Features for Communication Channels
- Secured File Transfer Communication
- Public Key Cryptography Authentication
- OSPF Encryption with HMAC-SHA256

## Comprehensive Security Mechanisms

Comprehensive security mechanisms protect both the complete transport network and individual clients within the network. Neptune platforms support the following security mechanisms:

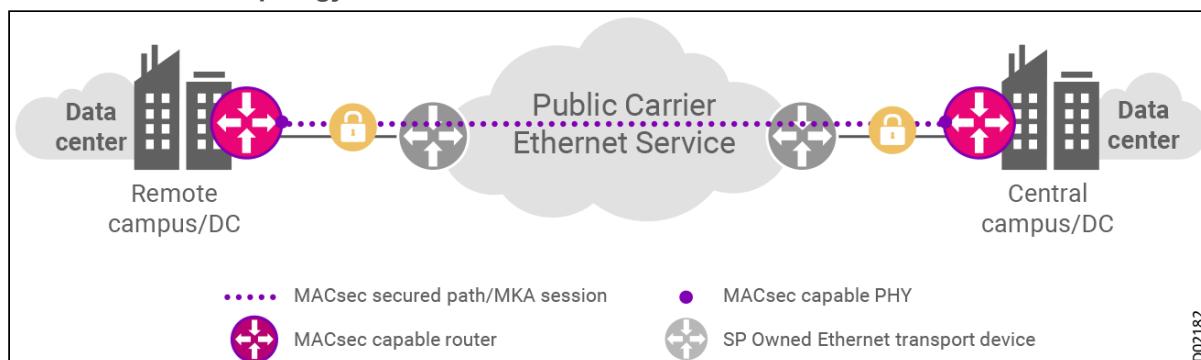
- **Broadcast Storm Control (BSC):** Depending on the network traffic patterns, extremely heavy levels of broadcast traffic (called a 'broadcast storm') may consume such a huge amount of network resources that the network becomes overloaded and unable to transport regular traffic. This is typically the situation in a DoS attack. The data cards support BSC in which broadcast traffic transmission is halted if the incoming broadcast traffic exceeds a configurable threshold value. While this action does not solve the problem at the broadcast flooding source, BSC does limit the risk of network overload, enabling the network to continue to function and giving network operators an opportunity to pinpoint and resolve the source of the problem. BSC can be configured separately for each service.
- **Access Control List (ACL):** The ACL is a list of objects and their associated permissions. These object permissions specify who or what is allowed to access that object and what operations are permitted. Additional ACL implementations include, for example, defining a list of restricted IP addresses from which the user can access a specific device, or a list of IP addresses that the user is allowed to access within the network. In a typical ACL, each entry in the list specifies a subject and an operation. One of the most important ACL applications is to protect routers from various risks, both

accidental and malicious. Infrastructure protection ACLs should be deployed at network ingress points.

- **VPN security** is provided for both QinQ and MPLS architectures. Users are protected from attacks or loss of data privacy to other users through comprehensive filtering and segregation per client. Protection from other users may be defined through VLAN segregation per client. Once a packet has been classified to a specific VPN, the contents of that packet are not visible to any other VPN. This protects the packet from sniffing or snooping.
- **Layer 2 Control Protocol (L2CP) flooding protection:** Neptune platforms protect against L2CP flooding sent by malicious users. Protection is implemented by limiting the number of L2CP frames which may be received from data ports through a combination of BPDU blocking, CFM, IGMP policing, and link and tunnel OAM rate limiters.
- **MAC flooding protection:** Another typical DoS that may be attempted by malicious users is MAC flooding. In our equipment, MAC addresses are learned through Forwarding Information Base (FIB) tables which are optimized for fast lookup of destination addresses. The data cards work with an FIB quota system to forestall MAC DoS attacks by limiting the number of MAC addresses available for each VPN.
- **MACsec (802.1AE):** 802.1AE is the IEEE MAC security standard (known as MACsec) which defines connectionless data confidentiality and integrity for media access independent protocols; see [MACsec \(802.1AE\)](#).
- **Port-based network access control (802.1x):** 802.1x is an IEEE standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols, providing an authentication mechanism for devices wishing to attach to a LAN, see [Port-based network access control \(802.1x\)](#).
- **Dynamic ARP Inspection (DAI):** A method of protection against address resolution protocol (ARP) spoofing attacks. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. See [Dynamic ARP Inspection \(DAI\)](#).

## MACsec 802.1AE

MACsec 802.1AE Topology Model



Neptune's network-wide MACsec solution is based on IEEE 802.1AE hop-by-hop Layer 2 encryption, providing port to port (including ports that are part of a LAG group) data confidentiality and integrity based on a GCM-AES-256 strong cipher, managed peer to peer through the MACsec Key Agreement (MKA). MKA is a protocol for discovering MACsec peers and negotiating keys.

The root key in the MACsec Key Agreement (MKA) key hierarchy is the Connectivity Association Key (CAK), and is identified by a CAK Name (CKN). The MKA derives two further keys from the CAK using the AES cipher in CMAC mode (AES-CMAC-256). SAKs should be generated by MKA using the CAK with a random number generated (RNG). Unlike the CAK, which is a long-term master key, the SAK is a transient key that is periodically refreshed.

Our MACsec solution can also operate over Ethernet networks with MACsec support only in the end points. This is accomplished through the hardware, thereby providing line-rate throughput.

The MACsec header frame format is similar to Ethernet frames, with an additional 32 bytes including 2 fields:

- Security Tag, an extension of the EtherType
- Message authentication code (ICV)

All fields following the Source Address (SA) and Destination Address (DA) bytes are encrypted, including the MPLS labels.

Neptune provides MACsec functionality through the DHXE\_4sec/4MRsec cards, 40G packet cards with MACsec capability built-in.

- The DHXE\_4sec provides 4 ports:
  - 2 x 10G/OTU-2 (SFP+)
  - 2 x 10G / 1GE (multi-rate)
- The DHXE\_4MRsec provides 4 ports:
  - 4 x 10G / 1GE (multi-rate)

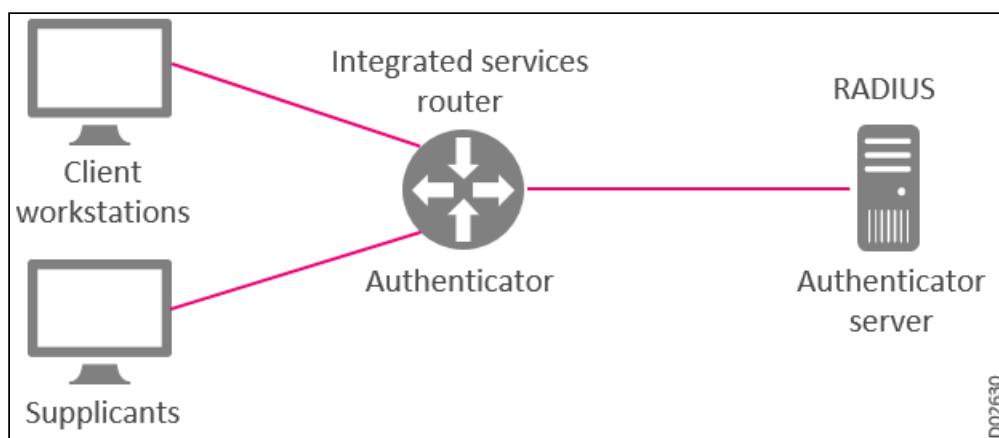
## Port-Based Network Access Control 802.1x

Neptune platforms provide enhanced security by implementing port authentication based on the IEEE 802.1x standard. This standard provides a standardized security authentication process for access to Ethernet networks, including LANs and Wireless LANs (WALNs).

802.1x is an IEEE standard for port-based network access control (PNAC). It is part of the IEEE 802.1 group of networking protocols, providing an authentication mechanism for devices wishing to attach to a LAN. IEEE 802.1x port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network.

The IEEE 802.1x provides almost unlimited scalability with minimal administration overhead. The user's access authentication is made at the network edge, at the port level. This guarantees that no unauthorized access is made, and all user access is made through a centralized authentication server.

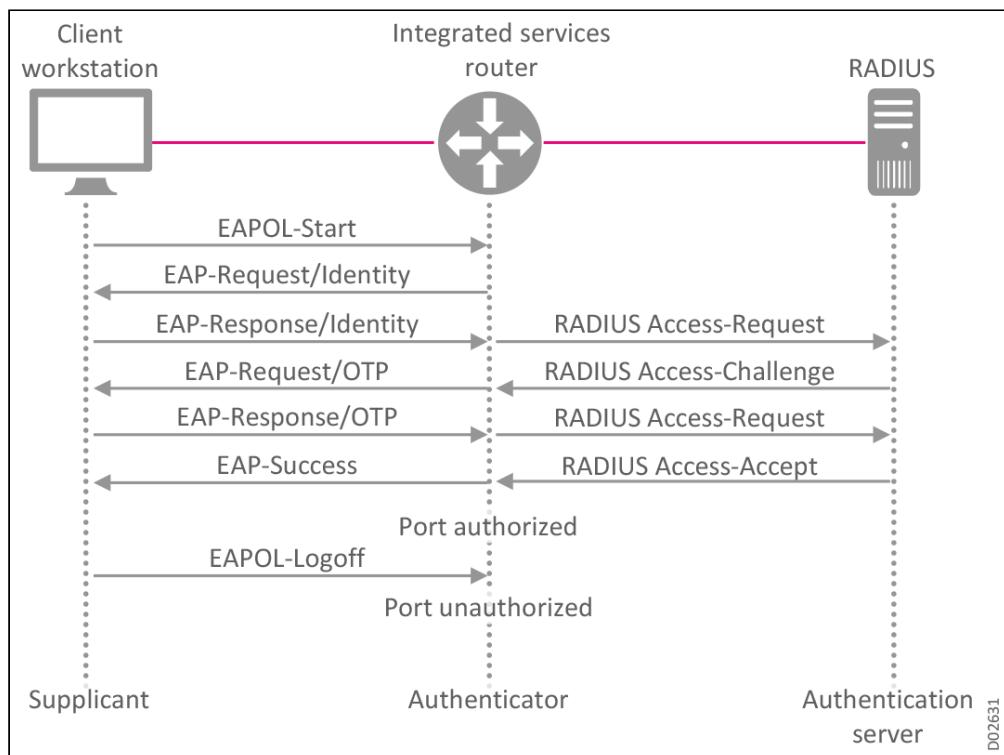
### 802.1x Device Roles



- **Supplicant:** The network access device requesting LAN services. This is the device (workstation) that requests access to the LAN and switch services and responds to requests from the router. The workstation must be running IEEE 802.1x-compliant client software such as that offered in the Microsoft Windows XP operating system. (The supplicant is sometimes called the client.)
- **Authenticator:** The network access point that has 802.1x authentication enabled. This includes LAN switch ports and Wireless Access Points (WAP). This is the router that controls the physical access to the network based on the authentication status of the supplicant. The router acts as an intermediary between the supplicant and the authentication server, requesting identity information from the supplicant, verifying that information with the authentication server, and relaying a response to the supplicant. The router includes the RADIUS client, which is responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

- **Authentication server:** The server device that performs the actual authentication of the supplicant, allowing or denying access to the network based on username/password. The 802.1x defines a Remote Authentication Dial In Server (RADIUS) as the required server. The authentication server validates the identity of the supplicant and notifies the router whether or not the supplicant is authorized to access the LAN and switch services.
- **Extensible Authentication Protocol (EAP):** The protocol that is used between the client and the authenticator. The 802.1x protocol specifies encapsulation methods for transmitting EAP messages so they can be carried over different media types.
- **Port Access Entry (PAE):** The 802.1x "logical" device of the client and authenticator that exchange EAP messages.

### 802.1x Authentication Procedure



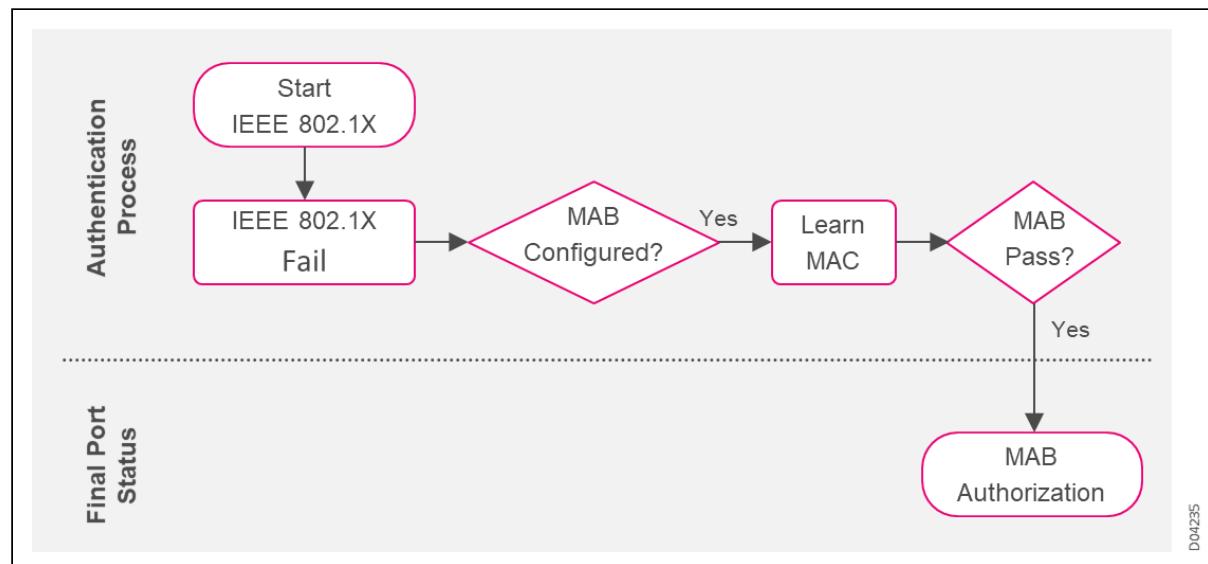
## MAC Authentication Bypass MAB

MAC Authentication Bypass (MAB) uses the MAC address of a device to determine the level of network access to be provided. MAB offers visibility and identity-based access control at the network edge for endpoints, mainly for those that do not support IEEE 802.1X. With the appropriate design and well-chosen components, you can meet the needs of your security policy while reducing the impact on your infrastructure and end users.

MAB is not a secure authentication method, but it is an access control technique that allows port-based access control by using an endpoint's MAC address. An interface with MAB authentication configured can be dynamically enabled or disabled based on the connected endpoint's MAC address.

MAB is typically used as a fallback to 802.1x. For endpoints that don't support IEEE 802.1X, such as printers and IP phones, MAB provides visibility and identity-based access control at the network edge. MAB can't check anything besides the endpoint's MAC address. Therefore, it does not offer secure authentication because MAC addresses are easy to spoof.

### MAB as Fallback Mechanism for Non-IEEE 802.1X Endpoints



D04235

If MAB is enabled on a port that does not have 802.1X enabled, then MAB authentication is performed automatically when the port status moves from down to up.

## TACACS+

Terminal Access Controller Access-Control System (TACACS) refers to a family of related protocols handling remote authentication and related services for networked access control, working through a centralized server. The original TACACS protocol, which dates back to 1984, was used for communicating with an authentication server, common in older UNIX networks such as ARPANET. TACACS was originally designed as a means to automate authentication – allowing someone who was already logged into one host in the network to connect to another on the same network without needing to re-authenticate.

TACACS is defined in RFC 8907, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. The server would determine whether to accept or deny the authentication request and send back a response. The routing node would then allow access or not, based upon the response. In this way, the process of making the decision is "opened up" and the algorithms and data used to make the decision are under the complete control of whomever is running the TACACS daemon.

Terminal Access Controller Access-Control System Plus (TACACS+) is a protocol that was released as an open standard beginning in 1993. Although derived from TACACS, TACACS+ is a separate protocol that handles [authentication, authorization, and accounting \(AAA\) services](#). TACACS+ and RADIUS have generally replaced TACACS in more recently built or updated networks.

TACACS+ uses TCP (while RADIUS operates over UDP). Since TCP is a connection-oriented protocol, TACACS+ has to implement transmission control. RADIUS, however, does not have to detect and correct transmission errors like packet loss, timeout etc. since it rides on UDP which is connectionless. RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore, it is vulnerable to different types of attacks. TACACS+ encrypts all the information listed here, and therefore does not have the vulnerabilities present in the RADIUS protocol. TACACS+ encrypts the full content of each packet. Moreover, it provides granular control (command by command authorization).

TACACS+ implementations work with the following terminology:

- **TACACS+:** Terminal Access Controller Access-Control System Plus

- **Client:** The client is any device which initiates TACACS+ protocol requests to mediate access, mainly for the Device Administration use case.
- **Server:** The server receives TACACS+ protocol requests, and replies according to its business model, in accordance with the flows defined in the specification.
- **Connection:** TACACS+ uses TCP for its transport. TCP Server port 49 is allocated by IANA for TACACS+ traffic.
- **Session:** A TACACS+ session is a single authentication sequence, a single authorization exchange, or a single accounting exchange. An accounting and authorization session will consist of a single pair of packets (the request and its reply). An authentication session may involve an arbitrary number of packets being exchanged. The session is an operational concept that is maintained between the TACACS+ client and server. It does not necessarily correspond to a given user or user action.

## TACACS+ Authentication Authorization and Accounting

TACACS+ is generally used for device administration: authenticating access to network devices, providing central authorization of operations, and auditing of those operations. The TACACS+ protocol allows for arbitrary length and content authentication exchanges, to support alternative authentication mechanisms. It is extensible to provide for site customization and future development features, and it uses TCP to ensure reliable delivery. The protocol allows the TACACS+ client to request fine-grained access control and allows the server to respond to each component of that request. The separation of authentication, authorization and accounting is a key element of the design of TACACS+ protocol. Essentially, this separation turns TACACS+ into a suite of three protocols.

### Authentication

In the TACACS+ protocol, authentication is the action of determining the user's identity and if that user is allowed access. There are three types of packets in authentication:

1. Authentication\_START
2. Authentication\_CONTINUE
3. Authentication\_REPLY

Each authentication flow begins with a START packet from the client. The server responds either with a request for more information (GETDATA, GETUSER, or GETPASS) or a termination message (PASS, FAIL, ERROR, or RESTART). If the server requests more information then authentication continues with the client sending a CONTINUE packet with the requested information. If the information being requested by the server from the client is sensitive, that is flagged and the content is treated accordingly.

### Authorization

In the TACACS+ protocol, authorization is the action of determining what a user is allowed to do. Authorization does not merely provide yes or no answers; it can also customize a service for the particular user. In the current implementation, the user's role is defined in the server, and returned to the client to determine the user's permissions. There are two types of packets in authorization:

1. Authorization\_REQUEST
2. Authorization\_REPLY

In the TACACS+ protocol an authorization is always a single pair of messages: a REQUEST from the client followed by a REPLY from the server. The authorization REQUEST message contains a fixed set of fields that indicate how the user was authenticated and a variable set of arguments that describe the services and options for which authorization is requested. The REPLY contains a variable set of response arguments (argument-value pairs) that can restrict or modify the client's actions.

### Accounting

Accounting is typically the third action after authentication and authorization, responsible for recording what a user is doing, and/or has done. Accounting in TACACS+ can serve two purposes. It may be used as an auditing tool for security services, and it may also be used to account for services used, such as in a billing environment. To this end, TACACS+ supports three types of accounting records.

- Start records indicate that a service is about to begin.

- Stop records indicate that a service has just terminated.
- Update records are intermediate notices that indicate that a service is still being performed.

TACACS+ accounting records contain all the information used in the authorization records, and also contain accounting-specific information such as start and stop times (when appropriate) and resource usage information. There are two types of packets in accounting:

1. Accounting\_REQUEST
2. Accounting\_REPLY

## Firewall Filters

Firewall filters allow you to filter traffic destined for, or traversing through, a Neptune device. Firewall filters are used for a variety of reasons:

- Protect NE management plane from denial-of-services attacks
- Create access control lists (ACL)
- Redirect packets to an alternate next hop
- Filters traffic based on a condition-match/action pairs for efficient implementation of protocol policies

You filter packets based on their content, and then apply actions to the packet, such as rejecting, accepting, or redirecting the packet. Firewall filters can be applied per logical interface or globally for all interfaces. Basic firewall filters provide basic packet filtering based only on the source IP address. Extended firewall filters allow filtering not only on the source address, but also on the destination IP addresses, protocol type, and source and destination port numbers.

All firewall filters consist of terms, match conditions, and actions:

- **Match condition:** Condition a packet must match before an action can be applied to it. You can match against the specific contents of a packet, such as the IP source or destination field, TCP flags, or ICMP packet type.
- **Action:** What happens to the packet if a match condition is met. You can configure the firewall filter to accept, reject, discard, or redirect the packet. Once an action is applied, evaluation of the filter ends.
- **Action modifier:** A modification to an action. Counting a packet is an action modifier.
- **Term:** Set of match conditions and actions. You can have multiple terms per firewall filter.

This section includes the following:

- Filter Evaluation Process
- Management Plane Protection

## Filter Evaluation Process

Firewall filters work with sets of *match conditions*, *actions*, and *action modifiers* that are grouped into *terms*. A single firewall filter can have more than one term. Terms of a filter are evaluated in the order in which they are configured.

Firewall filters evaluate each packet against the terms of a filter. As a packet passes through the filter, the packet is evaluated against the first term of the filter. If the packet matches the conditions in the term, the filter applies the action associated with the term.

If the action is to accept, reject, discard, or redirect the packet, the evaluation of the packet ends and the action is implemented. If a counter is specified in a term, that counter increments for every packet that matches the term. If the packet is to be sampled, it is. Counted and sampled packets cannot be accepted.

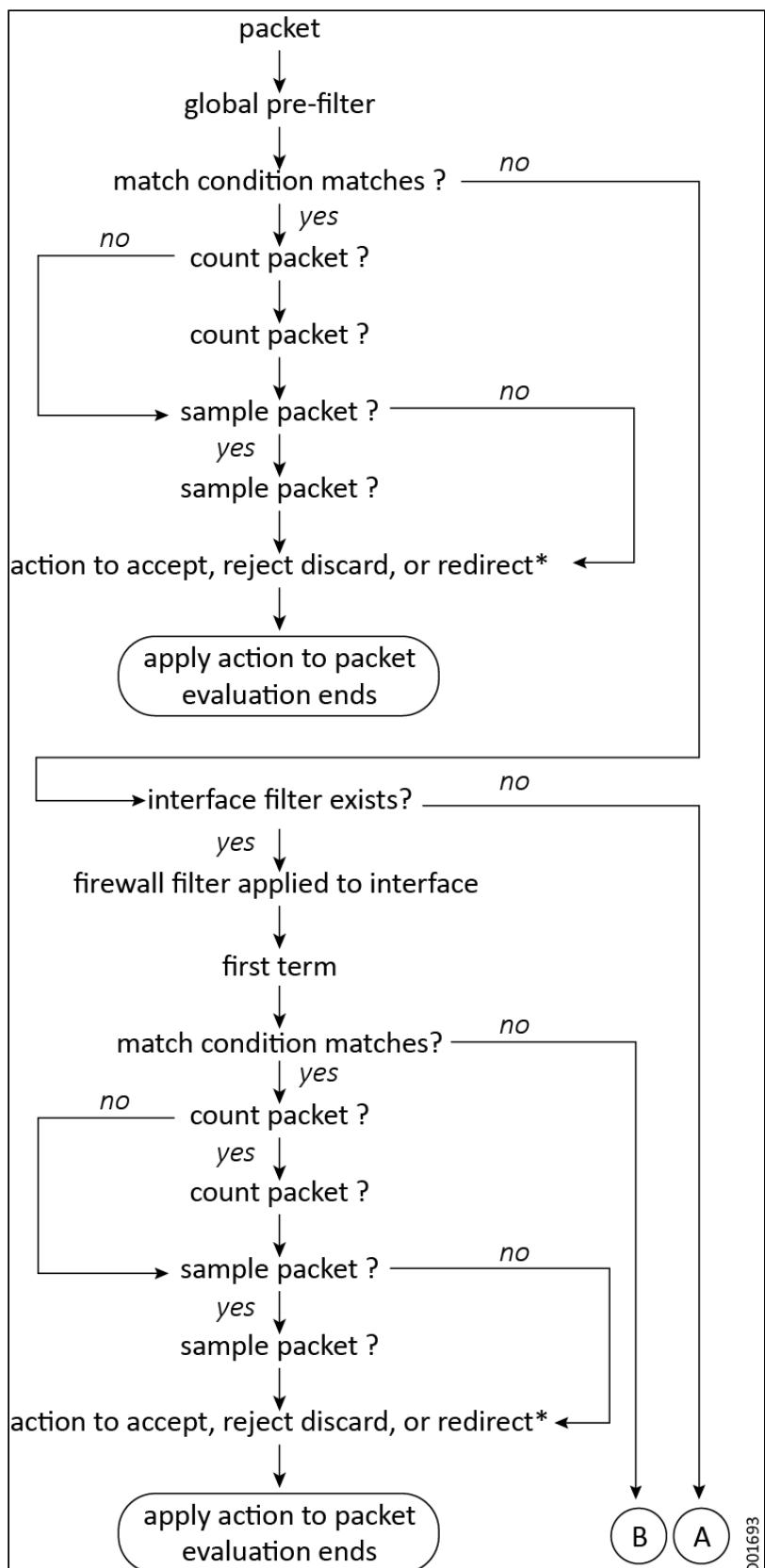
If the packet does not match the conditions in a term, the packet is evaluated against the next term in the filter. Evaluation continues until the packet matches a condition and a specified action is applied (i.e., reject, accept, discard, redirect). If the packet passes through an interface-specific filter without matching any conditions, the packet is dropped without an error message; that is, the packet is discarded.

Only one firewall filter can be applied to an interface. You can also apply global filters that filter packets either before or after the interface-specific filter. If no interface-specific firewall filters are configured, all packets are accepted by the logical interface unless overridden by a global firewall filter.

The following figures illustrate how firewall filters are evaluated. This example assumes that both a global pre-filter and interface-specific post-filter exist. If global filters do not exist, the interface filter processes packets as shown and if no match is found, the packet is discarded.

 **Note**

In the illustration, the action for sampled and counted packets - marked with an asterisk (\*) - cannot be Accept. The figure assumes the use of implicit-discard-disable. If not, the evaluation will never continue beyond the pre-filter stage.

**Filter Evaluation Process**D01633  
B A

## Management Plane Protection

Management plane protection mechanism is typically used to harden security for management traffic directed to the Neptune platform, by setting a firewall for the IP packets. IP filter parameters are configurable, and include options for both IPv4 and IPv6 attributes. You can also disable the configured IP filter.

The IP filter can include one or more *terms*, where each term includes the following attributes:

- **Match** conditions, including:
  - The source/destination IP addresses
  - The source/destination TCP/UDP ports
  - The protocols (user-specified port/name, or according to a predefined list of protocols; see table at the end of this page)
  - The ingress IP LIFs
- **Action**, either `accept` or `discard`. After a discard action is selected, you can also select a `log` action.

This filter is configured for the global VRF only. After the filter (ACL) for the packets to CPU has been configured, each ingress packet to the IP stack in the CPU is evaluated through one of the following approaches:

- **Term by term:** If matched by at least one term, the IP filter will perform the action for that packet; the filter does not continue checking the remaining/reserved terms in the filter.
- If **multiple fields** are configured in the match conditions of a term, *all* the configured fields must be matched. For example, if the source IP address and the source TCP ports are configured, the packets will be matched only when *both* source IP and source TCP ports are matched.

This ACL doesn't affect the following traffic types:

- Packets to the LCT interface
- Internal communication packets (CBUS, etc.) to the internal IP interfaces

The new ACL affects management traffic only. It neither damages management connectivity nor does it drop signaling packets.

### Port and Protocol Options

Destination Port Number	Protocols	Management-related Application
23	TCP	Telnet
22	TCP	SSH/SFTP
21	TCP	FTP
6337	TCP	CORBA(non-SSL)
6338	TCP	CORBA(SSL)
830	TCP	NETCONF
161	UDP	SNMP
8001	UDP	UDP
7	TCP	Echo
2002	TCP	LCT Socket
5179	TCP	BGP alarm server
60021	TCP	FTP
60023	TCP	SFTP
4189	TCP	PCEP
49	TCP	TACACS+
50021	TCP	FTP port at LCT side
50023	TCP	sFTP port at LCT side

## Dynamic ARP Inspection DAI

Dynamic ARP Inspection (DAI) is a method of protection against address resolution protocol (ARP) spoofing attacks. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

ARP enables IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. Spoofing attacks occur because ARP allows a response from a host even when an ARP request is

not actually received. After an attack occurs, all traffic from the device under attack first flows through the attacker's system and then flows to the router, switch, or host. An ARP spoofing attack affects the devices connected to your Layer 2 network by sending false information to the ARP caches of the devices connected to the subnet. Sending false information to an ARP cache is known as *ARP cache poisoning*.

DAI ensures that only valid ARP requests and responses are relayed. NPT checks each ARP packet received against the binding table. If no IP-MAC entry in the table corresponds to the information in the ARP packet, DAI drops the ARP packet and the local ARP cache is not updated with the information in that packet. DAI also drops ARP packets when the IP address in the packet is invalid. ARP probe packets are not subjected to dynamic ARP inspection; NPT always forwards such packets.

## Enhanced Security Features for Communication Channels

The EMS can be upgraded to apply enhanced security settings to the EMS, and to selected NEs managed by the EMS. Communication channels between entities with enhanced security settings are secured and information is sent via SSH2 protocol. Security features include:

- **Access control:** Ensure resources are accessed in an authorized manner, incorporating the following control mechanisms:
  - **Management association access control:** Limit access rights related to the right to establish an association.
  - **Management notification access control:** Ensure notifications are only disclosed to the entities authorized to receive them.
  - **Managed resource access control:** Limitations related to resource access.
- **Accountability:** Supported by the non-repudiation services, binding the individual (or entity) to the operation performed. These services provide means to prove that the exchange of data was really made. Another option to support accountability is by appropriate combination of authentication, access control, and audit trail services.
- **Activity logging:** Provide log files recording management information such as events that have occurred or operations that have been completed, or attempted, by or on various resources. Log file data also provides important information regarding lost or modified records.
- **Confidentiality:** Protection of confidentiality, through services such as access control for stored data and data confidentiality for communicated data. Data confidentiality may also be required for certain types of stored data like passwords. Confidentiality services provide protection against unauthorized disclosure of exchanged data.
- **Data integrity:** Security services that support data integrity include access control and data integrity for stored and communicated data. These services provide a means of ensuring the correctness of exchanged data, protection against modification, deletion, creation, and reply of exchanged data.
- **Identification and authentication:** Delivering proof of object identity, including user authentication, peer entity authentication, and data origin authentication.
- **Security alarm reporting:** Provide information regarding operational condition pertaining to security.
- **Security auditing:** Ensure compliance with security audit requirements.

## Secured File Transfer Communication

The SSH File Transfer Protocol (also known as Secure FTP or SFTP) is a computing network protocol for accessing and managing files on remote file systems. SFTP also allows file transfers between hosts. Unlike standard FTP, SFTP encrypts both commands and data, preventing passwords and sensitive information from being transmitted in the clear over a network. SFTP clients are usually programs that use SSH to access, manage, and transfer files. SFTP clients are functionally similar to FTP clients, but they use different protocols. Consequently, you cannot use standard FTP clients to connect to SFTP servers, nor can you use clients that support only SFTP to connect to FTP servers. EMS-NPT also supports secured communication through CORBA.

These protocols are supported by the Neptune software systems, to transfer files (usually embedded files) in highly secure manner. For example, data is transferred from the NE to the EMS-NPT level either through CORBA with SSH or through a CMIP-like protocol with SSH, depending on the type of platform. Data is transferred from the EMS-NPT level to the NMS level (LightSOFT) through a CORBA MTNM interface secured with TLS.

## Public Key Cryptography Authentication

The unique public key enables to protect the managed NE under the EMS-NPT.

SSH uses public-key cryptography to authenticate the EMS-NPT and allow it to authenticate the NE. The public key is placed on all NEs that must allow access to the EMS-NPT for the matching private key (the EMS-NPT keeps the private key secret). While authentication is based on the private key, the key itself is never transferred through the network during authentication. SSH only verifies if the same NE offering the public key also owns the matching private key.

In Public key authentication, the NE holds a list of client user keys. Each user has its own key in the list, and the SSH-2 protocol makes the validation according to this list.

EMS-NPT also holds a list of all NEs with their keys and authenticates the NE user using this list (authorized users).

The unique public key enables to protect the managed NE under the EMS-NPT.

SSH uses public-key cryptography to authenticate the EMS-NPT and allow it to authenticate the NE. The public key is placed on all NEs that must allow access to the EMS-NPT for the matching private key (the EMS-NPT keeps the private key secret). While authentication is based on the private key, the key itself is never transferred through the network during authentication. SSH only verifies if the same NE offering the public key also owns the matching private key.

In Public key authentication, the NE holds a list of client user keys. Each user has its own key in the list, and the SSH-2 protocol makes the validation according to this list.

EMS-NPT also holds a list of all NEs with their keys and authenticates the NE user using this list (authorized users).

## OSPF Encryption with HMAC-SHA256

Neptune introduces an additional dimension to network security, using message authentication for the OSPF protocol to route the MCC between NEs.

Mechanisms that provide such integrity check based on a secret key are usually called "message authentication codes" (MAC). Typically, message authentication codes are used between two parties that share a secret key to validate information transmitted between these parties.

The user can configure the OSPPF security by selecting one of the following modes:

- **None** - meaning, there is no authentication to a party that joins the network. This is the default mode.
- **Simple** - a party that wants to join the network must first be authenticated by entering a password.
- **HMAC-SHA256 based encrypted OSPF** - keyed-Hash Message Authentication Code in conjunction with SHA256 algorithm hashing function. The OSPF information is encrypted with a 256-bit key. These algorithms are used as the basis for data origin authentication and integrity check based on a secret key. There are two options available in this mode:
  - Key ID, configurable from the EMS-NPT, is a number from 0 to 255 that identifies the authentication key.
  - Key, configurable from the EMS-NPT, the length of the key is 32 characters.

# Installation and Management

Zero touch provisioning (ZTP) simplifies installation of new NEs in the network. The only work required in the field is the actual mechanical installation of the physical equipment into place. NE provisioning within the management system requires no further manual intervention.

Once installation is complete, Neptune platforms are managed either through the Muse SDN applications suite, or by the LightSOFT multidimensional NMS, together with the relevant EMS and LCT systems. An intuitive user-friendly GUI makes new services easy to deploy and supervise. Neptune platforms also support a fully functional CLI capable of configuring, monitoring, troubleshooting, and debugging any configurable and measurable parameter, using a transaction-based mechanism. CLI can be run in multiple sessions, and supports multiple users.

This section introduces the Neptune installation and management systems.

- Zero Touch Provisioning ZTP
- Zero Touch Installation ZTI
- LightSOFT NMS Management
- Carrier SDN Integration
- EMS-NPT
- Local Craft Terminals
- CLI Configuration Overview

For more information about our management suite, see the *End to End Management Suite General Description*, and the Muse, EMS-NPT, LCT-NPT, and CLI user manuals.

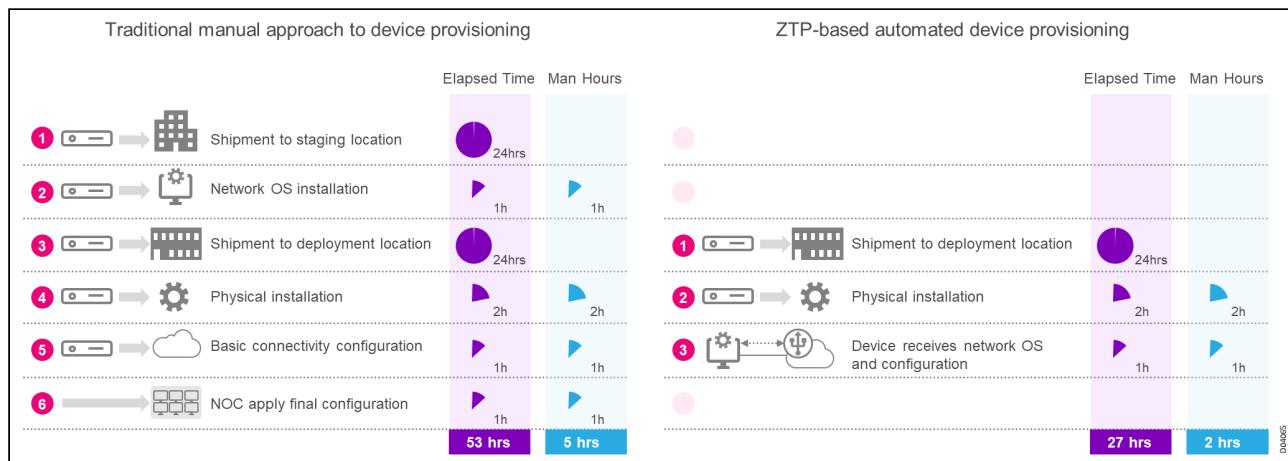
## Zero Touch Provisioning ZTP

### Note

From Neptune V9.0.2, [Zero Touch Installation \(ZTI\)](#) is no longer supported. From V9.0.2 and onward, automatic installation is implemented through Zero Touch Provisioning (ZTP).

Traditional approaches to device provisioning are labor intensive, time consuming, and prone to human error. They are not appropriate for the rapid pace and diversity of today's network deployments, and often require complex planning and co-ordination across multiple teams, functions, and organizations. Automated life-cycle technologies make it simpler and more cost effective for operators to build and expand their networks, enabling greater velocity by making initial provisioning, upgrading, and replacement of network devices more efficient.

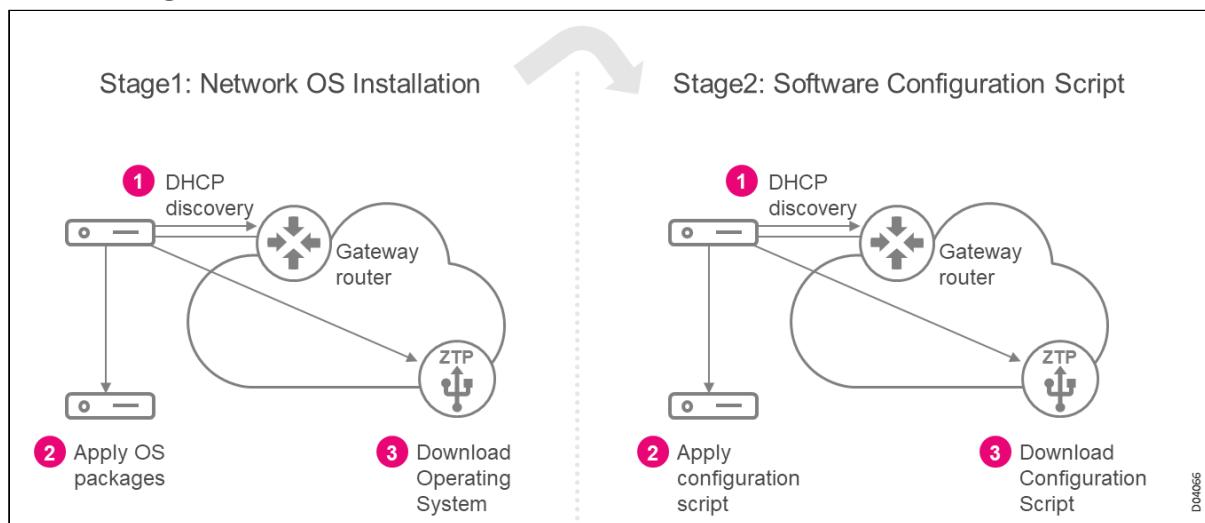
## ZTP Automated Provisioning



Zero-Touch Provisioning (ZTP) is an automatic process for deploying a NOS and base configuration for a device, so the device can enter in production without any human manipulation. The ZTP process is started automatically the first time a device is turned on and connected to the existing network infrastructure. The ZTP solution enables dynamic automated provisioning of devices, following a 2-stage process:

1. Network OS Installation
2. Software Configuration Script

## Two ZTP Stages



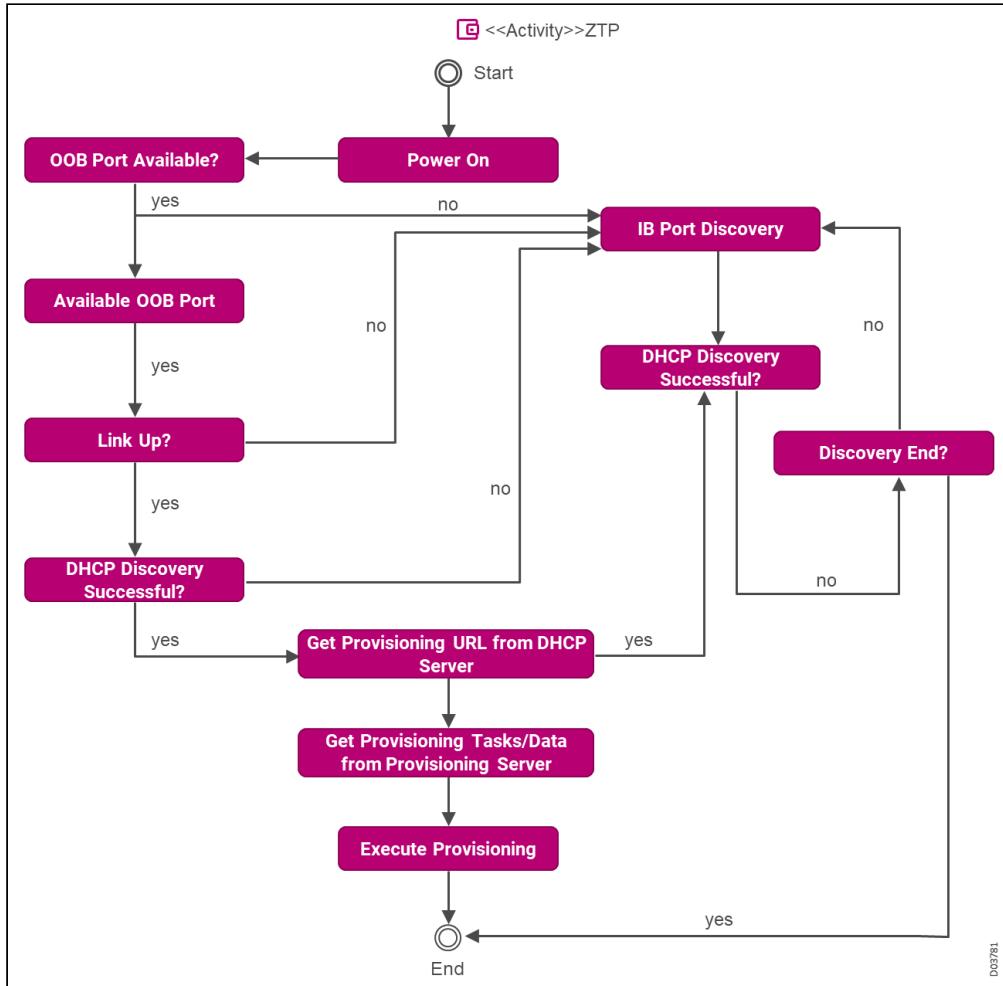
## ZTP Generic Workflow

The ZTP generic workflow is as follows, illustrated in the flow chart below:

1. The NE is powered on.
2. The out-of-band MNG port is checked for link connectivity.
3. The NE sends a DHCP discovery request to the DHCP server, using the out-of-band management port.
4. If the OOB trial failed, the in-band ports are checked for a link.
5. If DHCP discovery is unsuccessful, the NE reattempts it using the in-band management ports.
6. After DHCP discovery is successful, the DHCP server returns an IPv4 or IPv6 FTP or HTTP URL of a file server from which the NE can retrieve provisioning information.

7. The NE downloads the provisioning information and performs auto-provisioning, according to the specifications in the files.
8. After the NE is successfully provisioned, it automatically reboots and becomes operational.

## ZTP Workflow



## ZTP Features and Capabilities

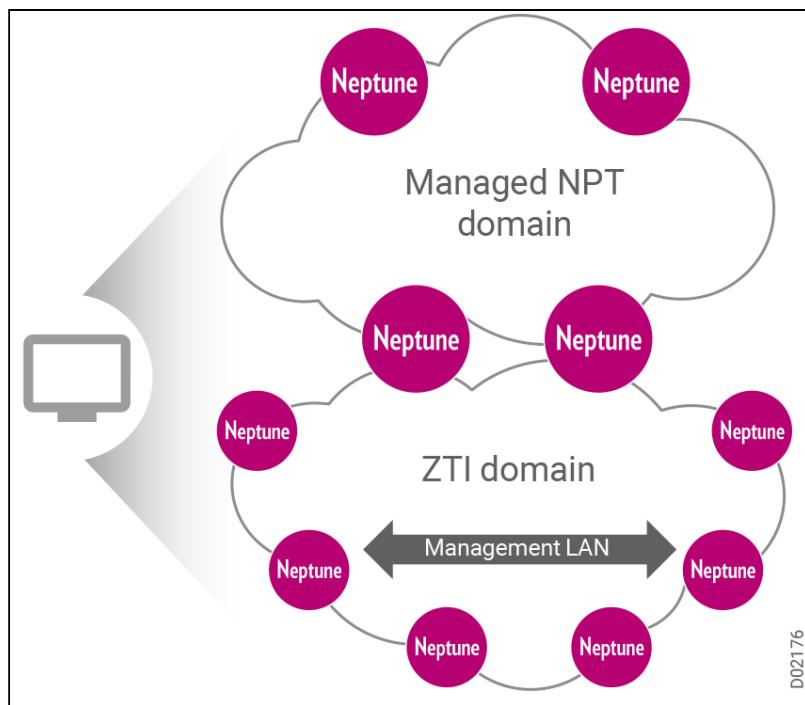
Neptune's ZTP implementation provides the following features and capabilities:

- Manual control commands for ZTP (Enable/Disable/Pause/Resume/Status, etc.)
- DHCPv4/v6 client and server options
- Configure SYSLOG, NTP, static route, etc., based on the DHCP server options
- Provisioning tasks from Provisioning Server via HTTP, HTTPS, TFTP, FTP, and SCP protocols
- Execute provisioning tasks:
  - Software upgrade/downgrade
  - Configuration file import
  - Script (shell/python) execution
- Support ZTP in redundant MCP/RCP system (HA)
- Support logging of ZTP procedure to console, local logs, and SYSLOG
- Support LED indicators for different stages of ZTP
- Support sending “adopt-me” messages to management systems

## Zero Touch Installation ZTI

Zero touch installation (ZTI) simplifies installation of new NEs in the network. The only work required in the field is the actual mechanical installation of the physical equipment into place. NE provisioning within the management system requires no further manual intervention. When ZTI is completed, the NE and its links are visible in the management system. The NE is fully managed; the EMS can download any pre-defined configuration settings or obtain configuration settings from the NVM (early integration mode).

### Zero Touch Installation



## LightSOFT NMS Management

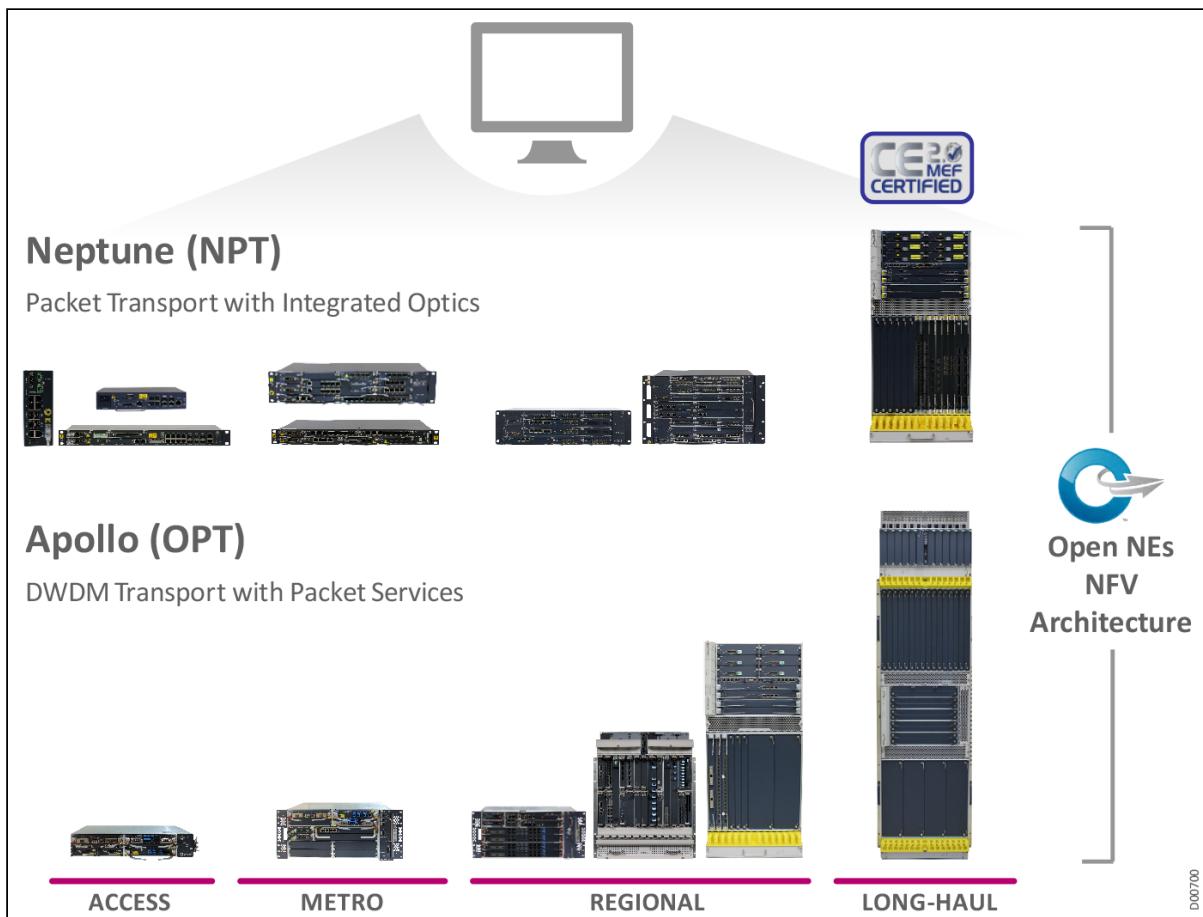
Our powerful network management suite, LightSOFT, is a unified NMS that provisions, monitors, and controls all NEs and layers. Multiple transmission technologies are controlled: each is represented as a layer (Ethernet/MPLS, OTN, optics, and SDH/SONET) in addition to the physical layer (fibers, copper, etc.). This approach enables you to manage multiple technology layers independently of the physical layer.

End-to-end tunnels, services, and trails are supported across the products, allowing services to be set that start, for example, at the Neptune and terminate at an XDM or Apollo. LightSOFT also supports top-down service and tunnel provisioning, reducing the time needed to provision new services.

Multidimensional LightSOFT manages our complete family of EMSs and enables you to assume full control of all equipment in your network, including:

- Neptune family of All-Native transport platforms for the metro
- Apollo family of NG transport platforms
- XDM family of multiservice transport platforms for the metro aggregation and metro core
- BroadGate family of multiservice transport for the metro access
- Multivendor networks

## One Management System



LightSOFT offers on-demand service provisioning, pinpoint bandwidth allocation, and dramatic reductions in equipment and operating costs that multiple management systems often require. It does this by providing complete network management from a single platform, including configuration, fault management, performance management, administrative procedures, maintenance operations, and security control. Within one integrated management system, LightSOFT's network manager enables you to fully control all your NEs regardless of their manufacturer, and view the complete network at a glance. Multiple operators can simultaneously configure the network without any conflicts.

Network provisioning, particularly in the data era, has become very complex. For example, tunnels must be pre-provisioned with various protection schemes. Service configuration requires setting multiple parameters for each service. LightSOFT offers a number of powerful automation tools to ease the provisioning process, thereby saving valuable OPEX for service providers. More services can be created in the same amount of time, which is directly reflected in revenues. Automation tools include automatic creation of tunnels per network or per service, automatic creation of bypass tunnels, reusable templates, automatic configuration of the tunnels needed for mesh topologies, and more.

LightSOFT's comprehensive, end-to-end perspective supports comprehensive definition of MPLS tunnels, Ethernet services, and SDH/SONET and optical trails, for primary and protection paths. LightSOFT supports all types of trails and links (MoT, MoE, EoS, ETY, SDH/SONET, optical), protection schemes, and user constraints. Simply point and click to connect any two endpoints, even in the most complex topology. LightSOFT provides powerful trail reconstruction options to reconcile discrepancies between different layers, as well as batch traffic management capabilities. LightSOFT provides smoothly integrated management for packet, optical, and MSPP-based platforms.

This section introduces the following features:

- Layered Architecture Maximizes Flexibility
- Easy Data Management
- Graphic User Interface
- GCT to EMS

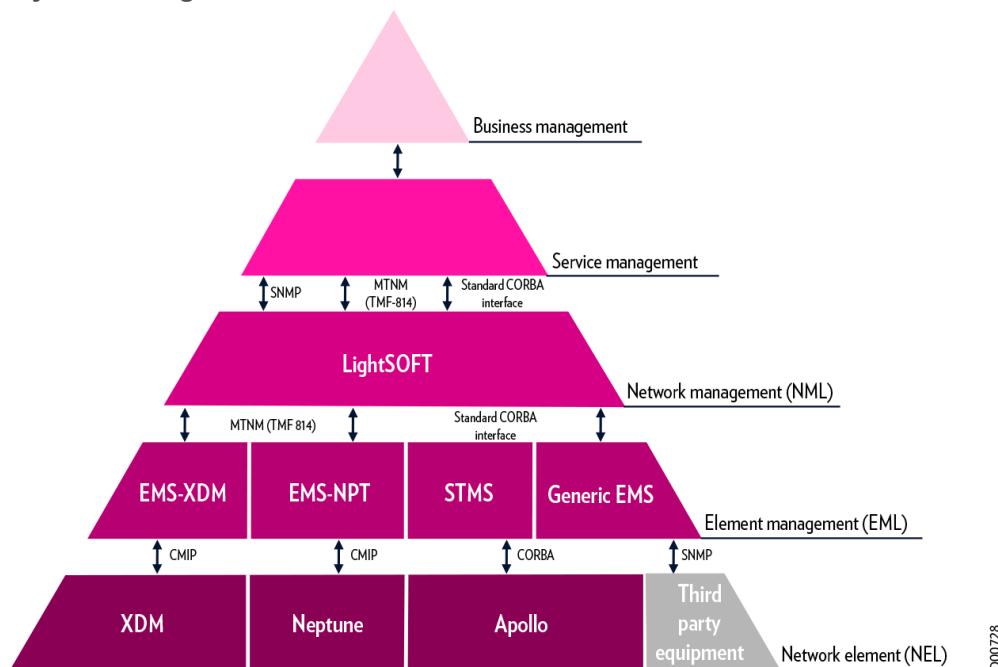
## Layered Architecture Maximizes Flexibility

Our management concept is based on a layered architecture in accordance with the **ITU-TM.3010** standard for compliant layer architecture.

Separate layers make up the management structure as follows:

- The lowest level, the **Network Element Layer (NEL)**, constitutes the embedded agent software of the NEs.
- The second layer, the **Element Management Layer (EML)**, controls many individual NEs.
- The third layer, the **Network Management Layer (NML)**, controls the main network management functions.

**Layered Management Structure**



LightSOFT functions at the NML, while a variety of different **Element Management Systems (EMSs)** are controlled through the LightSOFT umbrella function at the EML. Each EMS is tailored to a specific type of NE.

A **Northbound Interface (NBI)** connects either the EMS or LightSOFT to your **Operations Support System (OSS)**.

At the NEL, the Neptune features the local craft terminal (LCT) system, providing fast easy connectivity to the NE and enabling access to configuration and management functions through a user-friendly GUI as well as an efficient CLI.

## Easy Data Management

Packet-based transport networks are paving their way into the metro, resulting in thousands of packet-based NEs that need to be managed. An effective network management system provides its users with powerful, easy-to-use provisioning, monitoring, and fault management features, giving network operators an overall

view of network performance, enabling quick, efficient service provisioning, and isolating faults rapidly. This is done by means of sophisticated alarm handling windows, fault management tools, and maintenance operations. LightSOFT's easy data management suite features a service-centric approach, enabling operators to quickly identify exactly which services are being affected by a particular alarm, and vice versa. Troubleshooting and maintenance operations should all be available directly from the services menu.

While some of these features are known and implemented in SDH/SONET-based transport networks, LightSOFT, our state-of-the-art multi-layer multi-technology NMS, goes beyond this and extends these valuable skills to data networks. The result is a familiar look-and-feel and ease of management for both TDM-based and packet transport networks. The benefits of this approach are numerous, resulting in substantial direct and indirect OPEX savings.

LightSOFT's data management suite tackles all of the day to day aspects of packet transport management, including service provisioning, performance management, and fault management. Moreover, its field-proven scalable architecture ensures management of thousands of NEs in a cost-effective pay-as-you-grow model.

LightSOFT offers easy service provisioning, reducing service turn-up time. This shortens the time-to-market for revenues and eliminates mistakes that could lead to lengthy and costly troubleshooting time and consequent loss of revenue and credibility. Easy service provisioning is based on the following sophisticated features:

- Data Layer Abstraction: At the heart of our management approach lays the multi-layer multitechnology concept, tailored to transport networks that rely on multiple technologies (data, TDM, optics). LightSOFT helps network operators focus on the particular layer of interest by graphically separating the various layers. For example, the data layer view displays the Ethernet technology layer with data logical elements (LEs) only, providing a simple, intuitive, and easy-to-grasp view.
- Inserting and Removing Provider Edge (PE) Nodes: One issue that can be an endless source of errors and loss of service is any change in the network that calls for insertion or removal of a PE node. With one simple mouse-click, LightSOFT's powerful insert-and-remove-PE node function initiates a completely automatic reconfiguration and recalculation of tunnels and services traversing the link associated with that PE node. In this way, human error and exhausting manual reconfiguration are avoided.
- Point-and-Click MPLS-TP Tunnel/Service Configuration: With LightSOFT, point-and-click is not merely a catchy phrase. Simply select the endpoints and the associated tunnels and services are automatically selected as well. The ease of implementing P2P, P2MP, MP2MP, HVPLS, and CES yields tangible OPEX savings. The services can be auto-provisioned over a combination of MPLS and Provider Bridge (PB) networks. For example, even complex MP2MP services are activated in 2-3 minutes (instead of the typically required 10-15 minutes with the CLI scheme).
- IP/MPLS L2VPN/L3VPN Service Management: LightSOFT makes it simple to manage IP/MPLS L2/L3VPN services, offering point-and-click convenience for configuring, monitoring, and viewing them in a network-wide view. IP/MPLS management includes the full set of L2/L3VPN services over IP/MPLS.
- Automated Provisioning: With the operator in mind, LightSOFT provides a set of easy-to-use automation tools that make provisioning across complex networks a simple and scalable task. New PEs and links are configured automatically with a system preference default feature. This saves time and trouble when provisioning, as there is no need to re-create the list of all the relevant configuration parameters each time. Automatic provisioning features include automatic tunnel creation over complex topologies and automatic bypass tunnel assignment.

## Automatic Tunnel Creator



LightSOFT offers the important advantage of resource optimization, since LightSOFT's sophisticated pathfinding algorithm can be programmed to account for criteria such as shared risk link group (SRLG), link cost, length, and minimum hops.

For example, link cost is an important parameter for automatic pathfinding. The system-wide default is configurable, thereby minimizing the need to change this value manually in every link. You can also set the link cost value to 0, for situations where the user wishes this criterion to carry no weight. The operator benefits from a built-in optimization tool, improving pathfinding calibration and enabling more efficient workflow, by eliminating the need for cumbersome offline planning and optimization tools.

LightSOFT's northbound interface (NBI) was developed according to MTNM (also known as TMF-814), the leading industry standard and based on CORBA. It is rich in functionality and allows LightSOFT to be integrated under any OSS for alarms, and equipment and service inventory retrieval. The single point of integration and standards-based approach means that any new equipment or version deployed under LightSOFT does not require additional integration efforts.

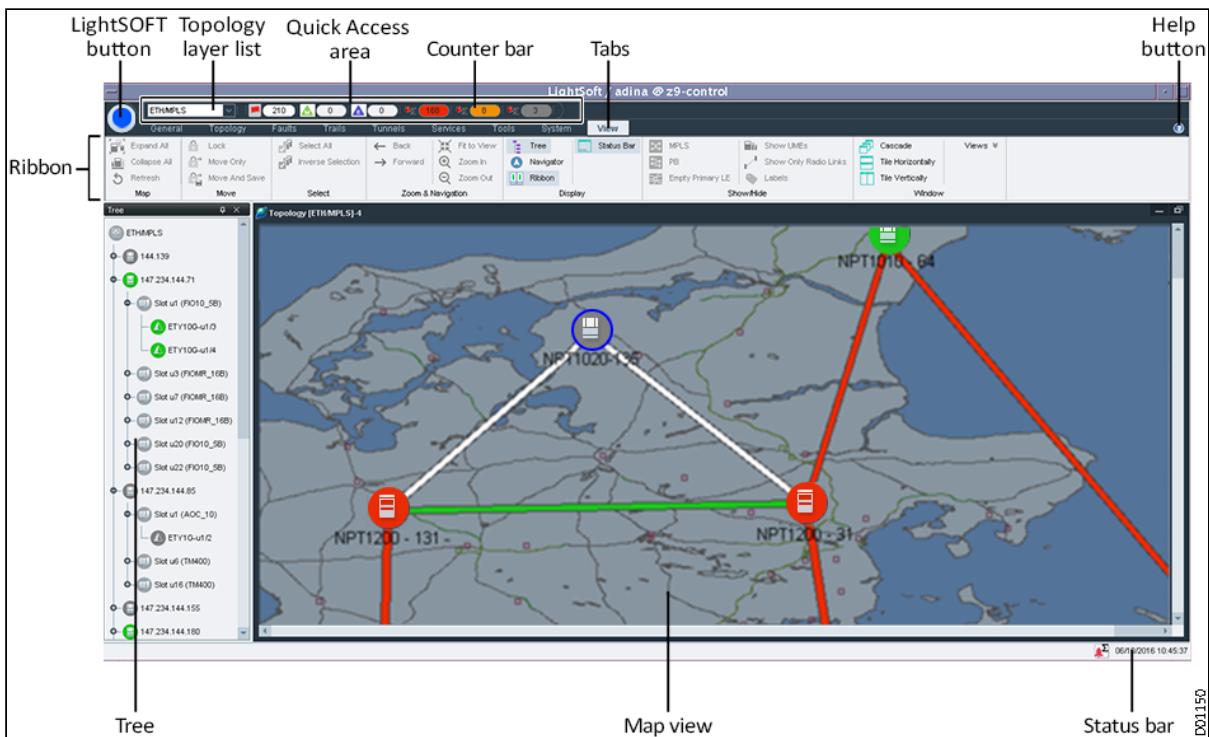
## Inconsistent Services Notification



## Graphic User Interface

The LightSOFT GUI provides a powerful yet easy-to-use tool for managing your network. It combines security, configuration, maintenance, and performance management tools with fault handling, E2E trail definition, and fail-safe database backups for uninterrupted and reliable network operation. LightSOFT's powerful tools and capabilities are easily accessed through the main window.

## LightSOFT Main Window

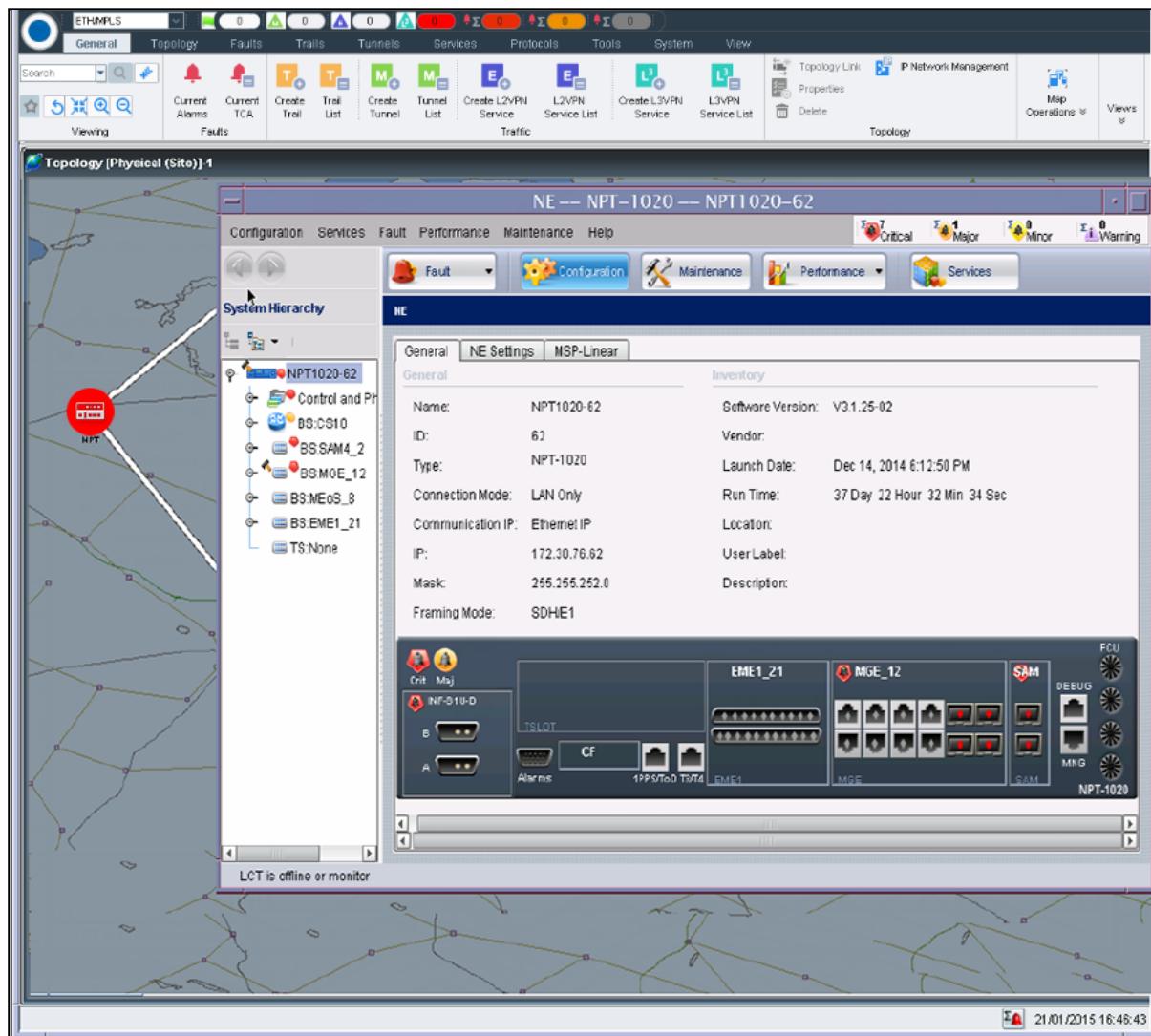


## GCT to EMS

You can use the GCT to easily access functions performed at the EMS level without actually launching it, including:

- Setting, changing, and propagating NE attributes
- Configuring platforms and cards
- Changing alarm severities
- Setting NE timing sources
- Activating performance management functions on NEs
- Performing maintenance functions on NEs or their objects

### GCT Example (LightSOFT to EMS-NPT)



## Carrier SDN Integration

Multivendor software-defined networking (SDN) control integration is enabled through use of PCEP, BGP-LS, and NETCONF/YANG interfaces.

We support the RFC4741 NETCONF Configuration Protocol, an IETF protocol for managing network devices. NETCONF operations are realized on top of a Remote Procedure Call (RPC) layer, using XML encoding for both the configuration data and the protocol messages. The NETCONF protocol has been implemented in network devices such as routers, switches, and OTN platforms by major equipment vendors. One particular strength of NETCONF is its support for robust configuration change transactions involving a number of devices.

Neptune platforms can be deployed as part of an SDN solution, supporting unified service automation and network optimization across IP, MPLS, Ethernet, and optical transport layers.

### NETCONF

The Network Configuration protocol (NETCONF) is an IETF network management protocol published in RFC 4741 (2006) and revised in RFC6241 (2011). NETCONF has gained strong industry support and is being adopted by major network equipment providers as the primary candidate for provisioning network functions.

Using protocols like NETCONF and data models such as YANG, SDN controllers can provision services across vendor and technology domains because they have a standardized method to provision different network functions, using a consistent set of data models.

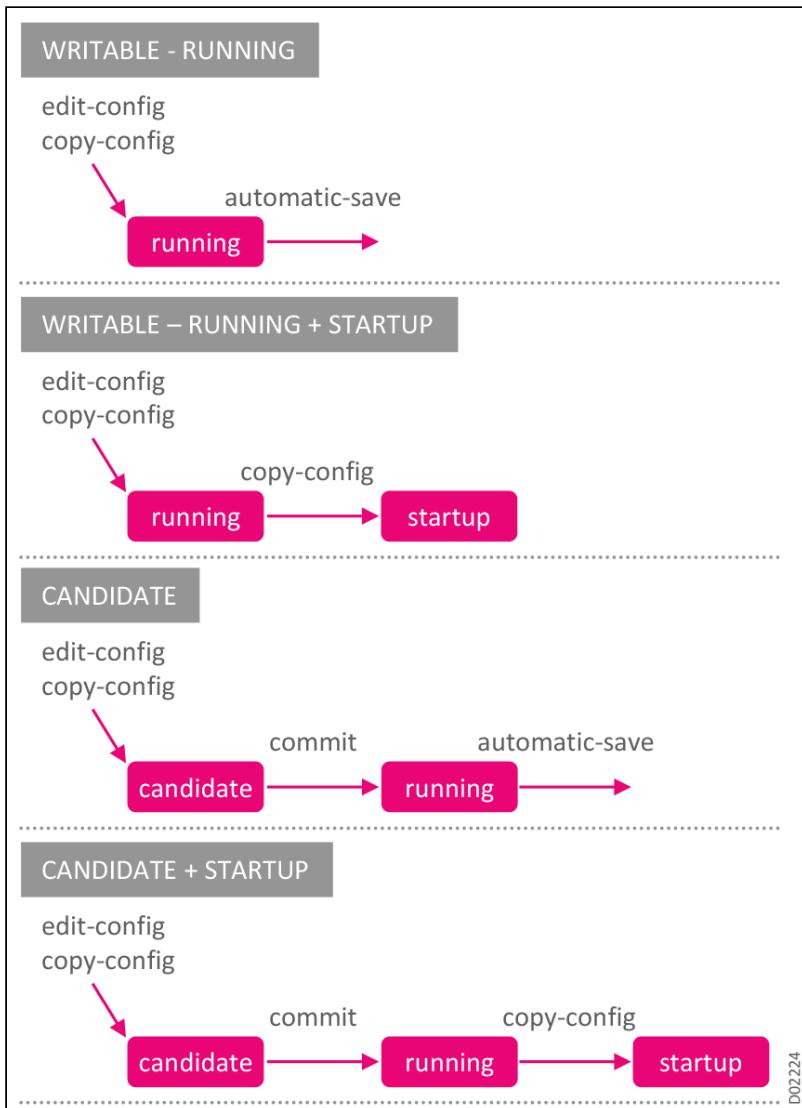
NETCONF is specifically not meant to *replace* SNMP, but rather to provide significant improvements in the area of configuration management, by offering Seamless integration with existing and future OSS/BSS environments. The loosely-coupled and modular architecture leverages open APIs and standard protocols, enabling orchestration across multi-domain and multi-layer for centralized policy and services across the entire network. NETCONF provides universal mechanisms to install, manipulate, and delete network device configurations. Operations are realized on top of a simple Remote Procedure Call (RPC) layer. The NETCONF protocol uses XML based data encoding for the configuration data as well as the protocol messages.

NETCONF is designed to be a replacement for CLI-based programming interfaces, such as Perl + Expect over Secure Shell (SSH). NETCONF is usually transported over the SSH protocol using the "NETCONF" sub-system, and in many ways it mimics the native proprietary CLI over SSH interface available in a device. However, it uses structured schema-driven data and provides detailed structured error return information, which CLI cannot provide.

NETCONF is based on **ACID** to define a transaction:

- **Atomicity:** Transactions are like a bulk operation, where the whole set either takes or it fails.
- **Consistency:** Transactions can be implemented simultaneously. They are not order-dependent as with CLI. If this cannot be done, the implication is that the system is not transactional.
- **Independence:** Parallel transactions are independent. They do not conflict, and always appear to be in-sequence.
- **Durability:** Committed data is not expected to be withdrawn.

## NETCONF Datastores



All NETCONF devices must allow the configuration data to be locked, edited, saved, and unlocked. In addition, all modifications to the configuration data must be saved in non-volatile storage. A typical example from RFC 4741 illustrates this approach. The following code sample adds an interface named "Ethernet0/0" to the running configuration, replacing any previous interface with that name.

```

<rpc message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <edit-config>
    <target>
      <running/>
    </target>
    <config
      xmlns:xc="urn:ietf:params:xml:ns:netconf:base:1.0">
      <top xmlns="http://example.com/schema/1.2/config">
        <interface xc:operation="replace">
          <name>Ethernet0/0</name>
          <mtu>1500</mtu>
          <address>
            <name>192.0.2.4</name>
            <prefix-length>24</prefix-length>
          </address>
        </interface>
      </top>
    </config>
  </edit-config>
</rpc>

<rpc-reply message-id="101"
  xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <ok/>
</rpc-reply>

```

NETCONF provides operators with a standardized, regimented, yet flexible means to manipulate network device configuration, using XML with an applied structure that can be validated effectively.

YANG (Yet Another Next Generation) data modeling language is used to model configuration and state data. The YANG modeling language was defined in RFC 6020 by IETF through the NETCONF Data Modeling Language Working Group (NETMOD). YANG extensions allow codeless, intuitive, GUI-based modeling and provisioning. This enables operators to provide higher level abstraction for orchestrating and automating devices and network services.

YANG is tree-structured rather than object-oriented. Configuration data is organized into a tree hierarchy, and the data can be of complex types such as lists and unions. The definitions are contained in modules, where one module can augment the tree within another module. YANG also differentiates between configuration and operational data. YANG differs from previous network management data model languages by its strong support of constraints and data validation rules. Strong revision rules are defined for modules.

A simple YANG coding example is illustrated in the following figure.

```

module acme-system {
    namespace
        "http://acme.example.com/system";
    prefix "acme";
    organization "ACME Inc.";
    contact "joe@acme.example.com";
    description
        "The ACME system.";
    revision 2007-11-05 {
        description "Initial revision.";
    }
    container system {
        leaf host-name {
            type string;
        }
        leaf-list domain-search {
            type string;
        }
        list interface {
            key "name";
            leaf name {
                type string;
            }
            leaf type {
                type enumeration {
                    enum ethernet;
                    enum atm;
                }
            }
            leaf mtu {
                type int32;
            }
            must "ifType != 'ethernet' or " +
                "(ifType == 'ethernet' and " +
                "mtu == 1500)" {
            }
        }
    }
}

```

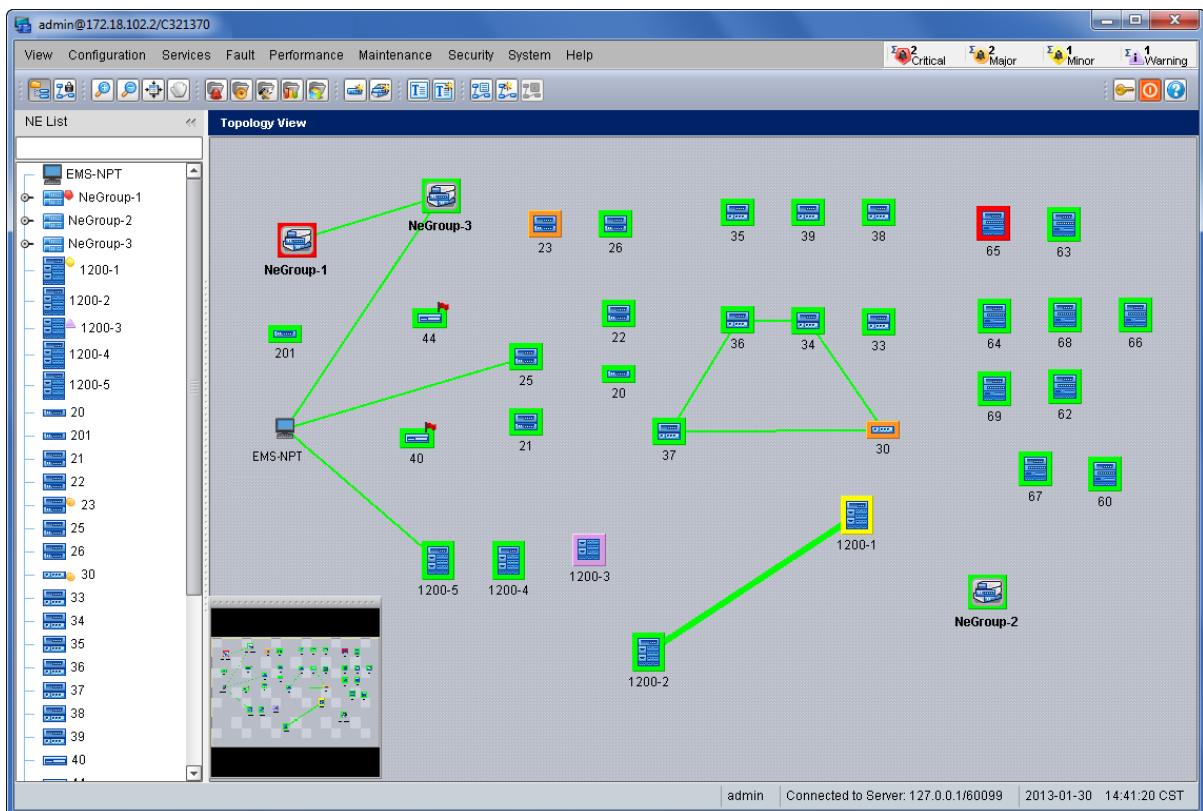
NETCONF/YANG's ambition is to enable universal multi-vendor R/W element and service management, thereby supporting a truly open standard programmability architecture. A list of the YANG modules currently supported by Neptune can be obtained from Ribbon's documentation portal.

## EMS-NPT

The EMS-NPT provides full-feature support for Neptune and BroadGate platforms. It functions at the element management layer (EML) in our network management scheme based on the TMN scheme. EMS-NPT has been designed as an open system in compliance with the CORBA MTNM standard, allowing it to be integrated smoothly and operate under a third party NMS TMN umbrella system.

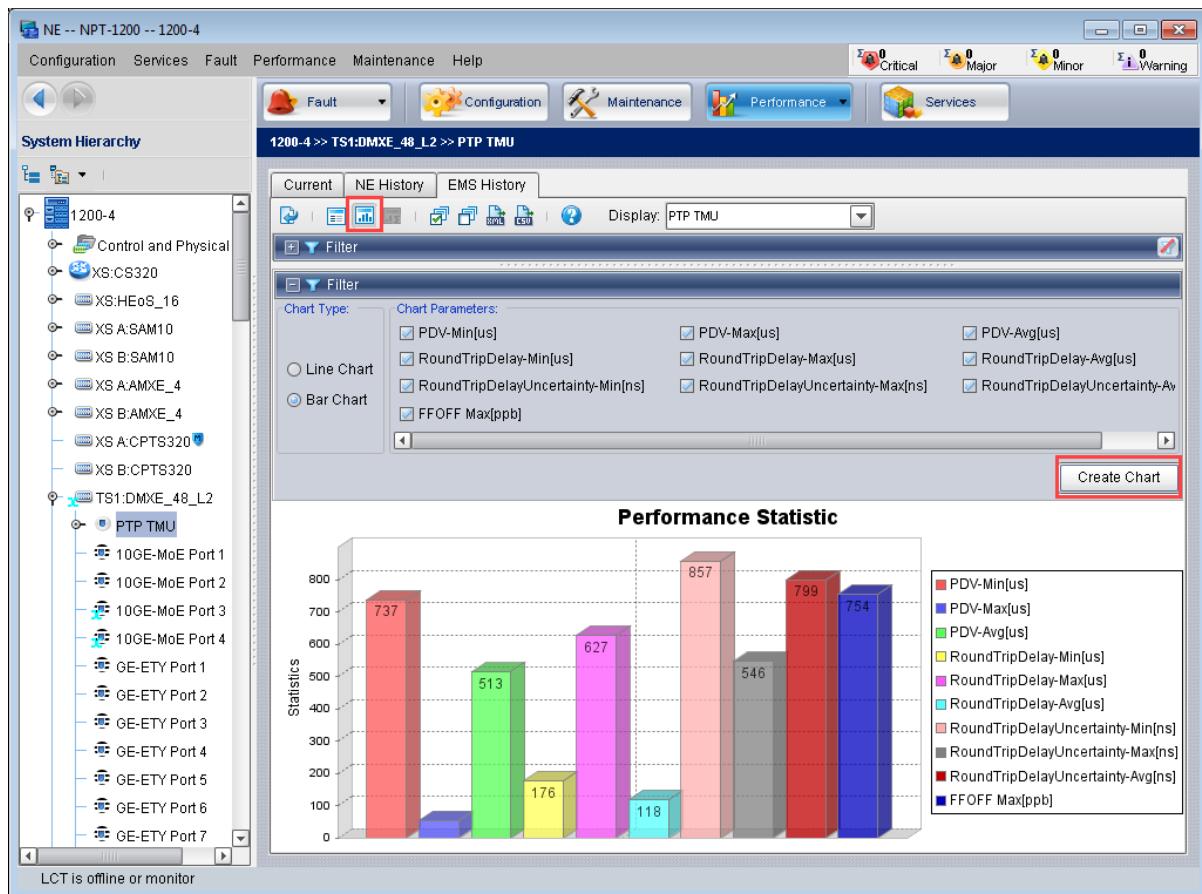
Element management in EMS-NPT provides a state-of-the-art GUI, with superior user experience, carrier grade in both functionality and scalability. EMS-NPT is based on Java together with a relational database, allowing it to run on multiple platforms (e.g., Microsoft Windows, SUN Solaris, VMWare Virtualized Servers, Linux) and support multiple operators concurrently.

## EMS-NPT Main Window



EMS-NPT applications provide a complete set of FE utilities ( pingne , logoutuser , changeneid , etc.) to help field engineers monitor and troubleshoot basic network operations. For more information, see the [EMS-NPT User Guide](#).

## View Performance History



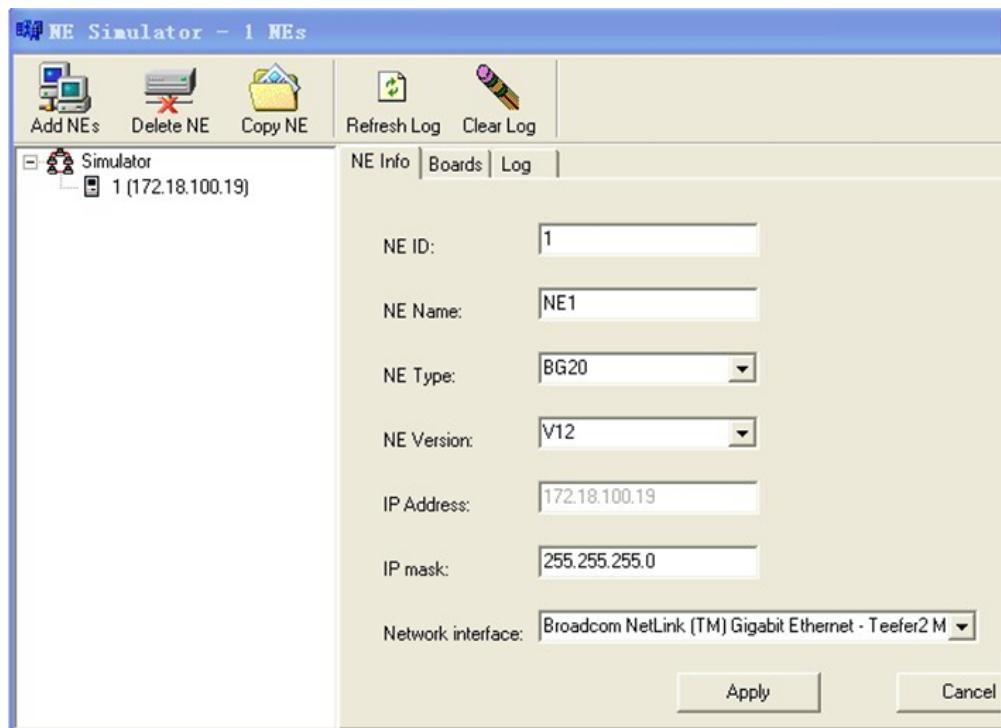
## EMS-NPT Features

The EMS-NPT supports an extended set of sophisticated features, including:

- Network configuration and management
- Software downloads and upgrades
- Service configuration and management
- User-friendly GUI simplifies card and sub-card slot assignments
- Moving cards between slots without deleting existing traffic and configuration
- Performance monitoring and fault management
- Hourly exports of historical PM counters, in XML and CSV format
- Robust security, including:
  - Data for sensitive ports is securely encrypted
  - Sensitive data is only stored in encrypted method files
  - Sensitive data within code is also encrypted
  - Passwords automatically expire after a set period
- Smooth NE migration, for example:
  - Between type of NEs
  - Between types of matrixes

## NE Simulator

## NE Simulator



## Local Craft Terminals

We offer a powerful suite of Local Craft Terminals (LCTs), PC-based installation, maintenance, commissioning, and configuration tools for field technicians. LCTs provide rapid direct connection to deployed NEs using a standard serial interface. Each type of NE managed by LightSOFT utilizes a specific application, such as LCT-NPT.

For smaller networks with fewer platforms, LCTs can be used as an economical standalone EMS that includes a current alarm window, NE database backup and restore capabilities, and current PM and TCA configuration.

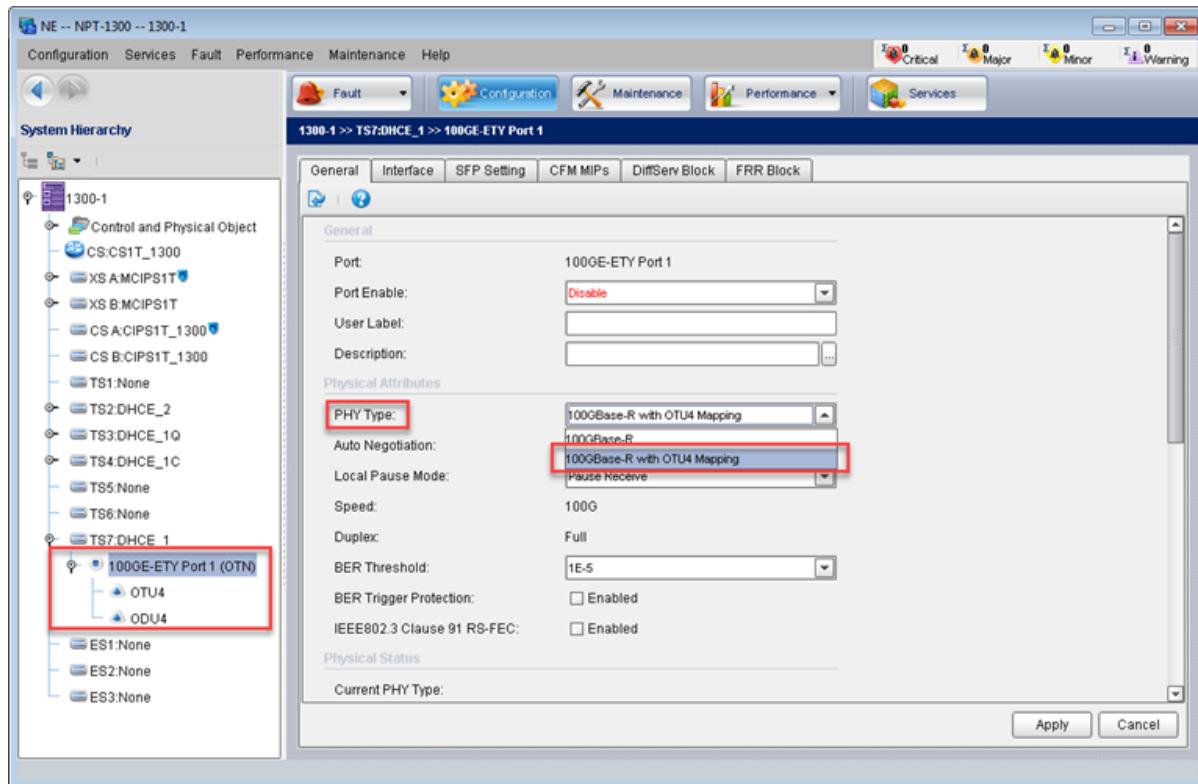
### LCT-NPT

The LCT-NPT is the PC-based platform field tool. The easy-to-use GUI provides direct connection to deployed NEs using an Ethernet interface.

The LCT-NPT supports all site functionalities: installation, NE commissioning (including slot assignment, IP routing, and DCC ports configuration), port and XC provisioning, and troubleshooting. The LCT-NPT also supports alarm and event management, inventory, PM, security management, system administration, and log management.

The system provides you with a clear view and control of NE internals, cards and objects, status, and configuration. Access from the LCT is password-protected. The intuitive Java-based interface is simple to use and runs on Windows platforms.

## Platform View as Displayed in the LCT-NPT



## CLI Configuration Overview

Our platforms support a fully functional CLI capable of configuring, monitoring, troubleshooting, and debugging any configurable and measurable parameter. CLI uses a transaction-based mechanism. CLI can be run in multiple sessions, and supports multiple users. For example, if you enter configuration mode while other users are editing the configuration, the CLI displays a list of users who are editing the configuration and the amount of time they have been idle. This section introduces the following features:

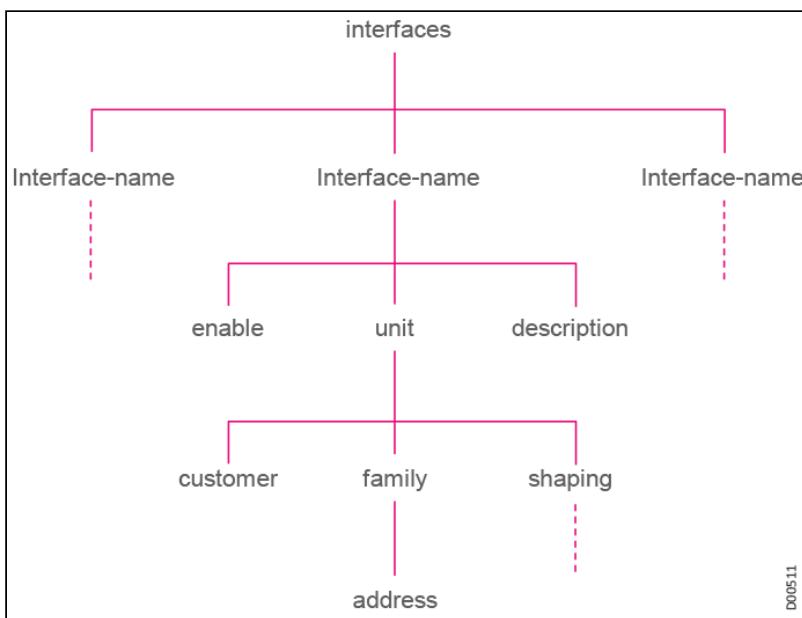
- Command Line Interface
- CLI Hierarchy Display Modes
- Entering Commands
- Supportive Help System
- Command Completion

## Command Line Interface

CLI is the primary device management interface, whether a user is logged in from a console or from a remote location via Telnet or a secure shell. CLI starts automatically when you log into the device, either from the console or via Telnet or SSH. The intuitive text-based command interface features:

- Operation and configuration modes
- Hierarchical command and configuration structure
- Context-sensitive help
- Command completion

## CLI Commands

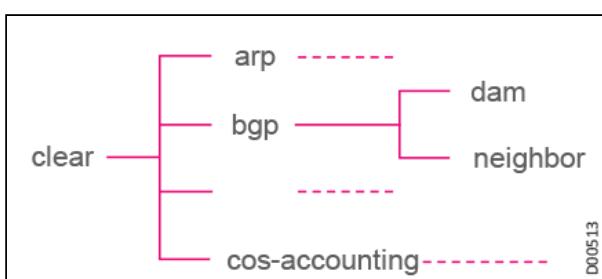


CLI operates in two modes:

- **Operation:**

Initial login is in operation mode. Use operation mode commands to view, monitor, and troubleshoot the system as it is running. Commands are organized into a hierarchical structure. Commands with similar functions are grouped together under a common command name and start with the same word.

The following figure illustrates the command structure. For example, all commands that reset statistics or connections begin with `clear`.



- **Configuration:**

In configuration mode, you create and edit the configuration of the device, such as interfaces, routing protocols, routing policy, and CoS parameters. Configuration changes are not implemented until the user *commits* them, at which time the changes are pushed out to the hardware.

The configuration statements are also organized into a hierarchical structure. Because the configuration is structured, you view the configuration statement and determine the command you would use to set, edit, or delete the statement.

For example, the command to configure a Gigabit Ethernet interface with an IP address is  
**set interfaces ge-ts1/0 unit 0 family inet address 172.18.1.154/24**

When you display the configuration, it displays as:

```

interfaces {
    ge-ts1/0 {
        unit 0 {
            family inet {
                address 172.18.1.154/24;
            }
        }
    }
}
  
```

```

        }
    }
}
```

The structure of the command statements also allow you to edit and delete parts of the statements at different levels. For example, to delete only the IP address from the previous configuration, you type:

```
delete interfaces ge-ts1/0 unit 0 family inet address 172.18.1.154/24
```

To delete the entire configuration for interface ge-ts1/0, you type:

```
delete interfaces ge-ts1/0
```

CLI is also used to load NE configuration files and/or XML files. Initial NE installation or NE expansion is faster and easier when loading an NE configuration generated by a planning tool.

Most of the debug, output, and show commands are very similar to JunOS CLI, which purposely makes the 24x7 first line support of the product very familiar.

## CLI Hierarchy Display Modes

The CLI command structure can be displayed in two different modes:

- **Hierarchy display mode**, where the command is listed in an indented hierarchical 'tree' structure, with command sub-structures indicated through a combination of curly brackets ({} ) and indentations. For example, the following code chunk illustrates the output of a show interfaces command in hierarchical mode:

```

ge-u1/3 {
    ethernet-options {
        mac-filtering enabled;
        default-c-vlan-priority 0;
        ingress-untagged-handling forward;
        max-frame-size 1540;
        link-oam-options {
            enable disabled;
            local-mode disabled;
            passive-peer-only disabled;
            remote-loopback disabled;
        } // end link-oam-options
    } // end ethernet-options
} // end object configuration
```

- **Flat display mode**, where the command is displayed as a series of set configuration command lines with the options set to the current configuration. For example, the following code chunk illustrates the output of the same show interfaces command, listed in flat mode:

```

set ge-u1/3 ethernet-options mac-filtering enabled
set ge-u1/3 ethernet-options default-c-vlan-priority 0
set ge-u1/3 ethernet-options ingress-untagged-handling forward
set ge-u1/3 ethernet-options max-frame-size 1540
set ge-u1/3 ethernet-options link-oam-options enable disabled
set ge-u1/3 ethernet-options link-oam-options local-mode disabled
set ge-u1/3 ethernet-options link-oam-options passive-peer-only disabled
set ge-u1/3 ethernet-options link-oam-options remote-loopback disabled
```

## Entering Commands

To enter a command, type the command at the prompt and then press **Enter**.

If you type a command or option that is not valid, CLI responds with an error message. The error message you receive depends on where you typed the invalid command. In all cases, the CLI points to the term it does not understand, using the caret symbol (^).

```
user@host> clear route
          ^ syntax error, expecting <command>.
```

CLI may display commands that are available and could potentially be used to correct the syntax error.

```
[edit]
user@host# load myconfig-file      <Enter>
          ^ syntax error, expecting 'merge',
'override', or 'replace'.
```

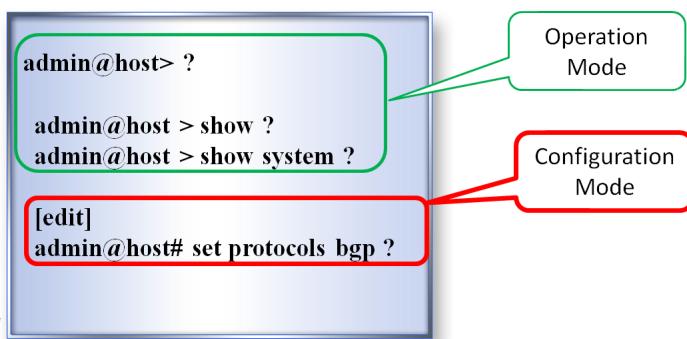
The CLI supports several keyboard commands that you can use to move the cursor on the command line, edit the commands you have typed, or repeat previously typed commands, such as CTRL-W to erase words, or CTRL-A/CTRL-E to go to the beginning or end of the line. Many of the commands are the same movement and editing commands as used in the UNIX-based editor, EMACS.

## Supportive Help System

### Context Sensitive Help

CLI features context-sensitive help throughout the command structure. Help displays a list of options available at the current hierarchy and a description of each option.

To access help, type ?. You do not need to press Enter after you type the question mark. The system responds with a list of valid possibilities that are relevant within the current command context, such as a list of commands that could be entered or a list of the options relevant for the command you are currently typing. Context sensitive help is relevant for both operation and configuration modes.



For example:

- If you type ? at the CLI prompt, help displays the commands and options that are currently available, followed by the CLI prompt.

```
admin@host> ?

Possible completions:
  clear           Clear information in the system
  configure       Enter configuration mode
  file            Perform file operations
  ftp             Open a ftp connection to another host
  help            Provide help information
  monitor         Real-time debugging
  Ping            Ping a remote target
  quit            Exit the management session
  request         Make system-level requests
  reset           reset
  restore          Restore an interface determined to have excess
                  bit errors
```

- If you type ? after entering a complete command name or option, help displays the options available for that command or option, followed by a re-typing of the command or option you typed. If the option is a variable, help displays the range of values you can type for that variable.

user@host> **set ?**

Possible completions:

cli	Set cli control flags
date	Set system date and time
led	Set LED related options
logging	Set logging options

- If you type ? in the middle of a command or option name, help displays possible completions, then displays what you typed.

user@host> **show i?**

Possible completions:

interfaces	Show information about interfaces
isis	Show information about IS-IS

user@host> **show i**

## Reference Help

CLI features reference help for configuration mode commands. Reference help is available from both the operation and configuration modes. Type **help command**, where **command** is the configuration command for which you want reference help and press **Enter**. Reference information for the configuration command is displayed.

## Hierarchy Help

In configuration mode, you can display the complete configuration statement for your current hierarchy level. To display hierarchy help, type **help hierarchy** and press **Enter**.

The complete hierarchy statement for the current level displays. If you enter this command at the top hierarchy level, all possible configuration statements for the device display.

## Command Completion

To complete a command or option you have partially typed, press **Tab** or **Space**. If the letters begin a uniquely identifiable option or command, the complete word displays. If the letters do not uniquely match any command or option, a list of possible completions displays. Command completion also applies to file names and user names.



### Tip

If the option is a user-defined text variable (such as a name), you cannot type **Space** to command complete the variable. Type **Tab** instead.

## Example

```
user@host# del<Tab> ete in<Tab> terfaces ge<Tab>
^
'ge' is ambiguous.
Possible completions:
<interface> Configure an interface
  ge-ts1/0
  ge-ts2/3
[edit]
user@host# delete interfaces ge
```

**Tip**

You can change the CLI environmental settings to only complete commands when you type **Tab** (i.e., not complete when you type **Space**).

# Standards and References for the Neptune Product Line

For a detailed list of the standards and reference documents that relate to the Neptune product line, refer to **Neptune Standards and References** in the *Neptune System Specifications*.