



## PRODUCT DOCUMENTATION

### *BTI 7000 Series packetVX® Solutions Guide*

**Part Number:** BT7A73DA  
**Document Version:** 01  
**Published:** March 2017  
**Type:** STANDARD

***product release 13.5***



# Contents

---

<b>Preface</b>	<b>xi</b>
<b>1.0 Introduction to the BTI™packetVX®</b>	<b>1-1</b>
1.1 OTU digital wrapper .....	1-2
1.2 BTI™packetVX® modules .....	1-3
1.3 Features of the packetVX portfolio .....	1-5
1.4 Configuration and management .....	1-10
1.5 Ethernet Service fault management .....	1-12
1.6 Applications overview .....	1-13
1.6.1 Provider Bridging and Ethernet Business Services .....	1-13
1.6.2 Ethernet aggregation .....	1-14
1.6.3 Ethernet video applications .....	1-15
1.6.4 4G wireless and WiMAX .....	1-16
<b>2.0 BTI™packetVX® hardware selection and installation</b>	<b>2-1</b>
2.1 BTI™packetVX® portfolio .....	2-2
2.1.1 packetVX specifications .....	2-3
2.1.2 Supported SFPs and XFPs .....	2-4
2.1.3 Shelf support .....	2-5
2.1.4 Considerations for selecting a packetVX module .....	2-6
2.2 packetVX and transceiver installation .....	2-9
2.2.1 BTI 7060 setup .....	2-9
2.2.2 BTI 7030 setup .....	2-10
2.2.3 BTI 7200 setup .....	2-10
2.2.4 Installing packetVX modules .....	2-12
2.2.5 Installing optical transceivers .....	2-16
2.2.6 Installing copper transceivers .....	2-18

### **3.0 Using the command line and other management interfaces** **3-1**

3.1 Overview of management interfaces .....	3-2
3.1.1 Management access and connectivity over IP networks .....	3-4
3.1.2 Provisioning, alarms and events, and upgrading .....	3-6
3.2 Using the Command Line Interface .....	3-7
3.2.1 CLI execution modes and contexts .....	3-7
3.2.2 CLI command help .....	3-10
3.2.3 Command Line completion .....	3-11
3.2.4 Command line editing keys .....	3-12
3.2.5 Controlling output .....	3-12
3.2.6 User sessions .....	3-13
3.3 Using proNX 900 Node Controller .....	3-14
3.4 proNX Service Manager .....	3-15

### **4.0 Basic equipment and switch member configuration** **4-1**

4.1 Create a packetVX equipment entry .....	4-2
4.2 Virtual switches .....	4-3
4.2.1 Create a virtual switch .....	4-3
4.2.2 Add a member to a virtual switch .....	4-4
4.3 Stacking .....	4-7
4.3.1 Stacking operation .....	4-9
4.3.2 Software upgrades and stacking .....	4-10
4.3.3 Sample stacking configuration .....	4-10
4.3.4 Configuring packetVX stacking .....	4-11
4.4 Optical Transport Network .....	4-15
4.4.1 OTU2 .....	4-15
4.4.2 Forward Error Correction and Enhanced Forward Error Correction .....	4-15
4.4.3 Sample OTU2 configuration .....	4-15
4.4.4 Provisioning OTU2 .....	4-16
4.5 GCC .....	4-18
4.5.1 Configuring GCC on OTU2 interfaces .....	4-18

### **5.0 Configuring Ethernet Bridging and STP** **5-1**

5.1 Interfaces and switchports .....	5-2
5.2 Port mirroring .....	5-3
5.3 Link Aggregation .....	5-6
5.3.1 Link Aggregation Group distribution .....	5-8
5.3.2 Link Aggregation and stacking .....	5-9
5.3.3 LACP active and standby links within a LAG .....	5-10
5.3.4 Sample 1+1 LAG configuration .....	5-11
5.3.5 Sample N+N LAG configuration .....	5-14
5.3.6 Sample N+M LAG configuration .....	5-17
5.3.7 Sample LACP misconfiguration .....	5-21
5.4 Link aggregation group provisioning .....	5-26
5.4.1 Displaying LACP system priority and LACP system ID .....	5-26



5.4.2 Setting LACP system priority .....	5-28
5.4.3 Setting LACP port priority .....	5-29
5.4.4 Creating a link aggregation group .....	5-30
5.4.5 Setting the maximum number of links for a LAG .....	5-32
5.4.6 Setting the minimum number of LAG member ports .....	5-33
5.5 Ethernet bridging .....	5-36
5.6 Introduction to Provider Bridging .....	5-37
5.6.1 S-VLAN encapsulation .....	5-38
5.7 Spanning Tree Protocol (STP, RSTP, and MSTP) .....	5-39
5.7.1 MSTP provisioning .....	5-42
5.7.2 Loop Guard .....	5-44
5.7.3 Loop Guard configuration considerations .....	5-45
5.7.4 Configuring packetVX loop guard .....	5-46
5.8 Storm Control .....	5-48
5.8.1 Storm Control on NNI ports .....	5-49
5.8.2 Storm Control on NNI LAGs .....	5-51
5.8.3 Configuring packetVX storm control .....	5-53
5.9 GVRP .....	5-54
5.10 Link Layer Discovery Protocol .....	5-56
5.10.1 LLDP Configuration .....	5-57
5.11 Forwarding database provisioning .....	5-59
5.11.1 Setting the MAC address aging timer .....	5-59
5.11.2 Adding and removing static MAC addresses .....	5-60
5.12 Viewing the configuration of a switch .....	5-62
5.13 Station loopback .....	5-63
5.13.1 Configuring a station loopback .....	5-64

## **6.0 Configuring Ethernet services 6-1**

6.1 UNIs, NNIs and E-NNIs .....	6-3
6.1.1 External Network to Network Interface [E-NNI] .....	6-5
6.1.1.1 Ethernet Access (E-Access) services .....	6-6
6.1.1.2 E-NNI S-VLAN translation .....	6-11
6.1.1.3 E-NNI bandwidth profile .....	6-12
6.1.1.4 E-NNI provisioning specifications .....	6-13
6.1.2 Sample UNI, NNI and E-NNI configurations .....	6-14
6.1.2.1 Sample UNI configuration .....	6-14
6.1.2.2 Sample NNI configuration .....	6-14
6.1.2.3 Sample E-NNI configuration .....	6-15
6.1.3 Private and Virtual Private services .....	6-15
6.2 Ethernet services .....	6-17
6.2.1 Ethernet Private Line (EPLINE) .....	6-18
6.2.2 Ethernet Virtual Private Line (EVPLINE) .....	6-19
6.2.3 Ethernet Private LAN (EPLAN) .....	6-19
6.2.4 Ethernet Virtual Private LAN (EVPLAN) .....	6-20
6.2.5 Ethernet Tree Service (E-TREE) .....	6-21
6.2.6 Mapping untagged packets to a service .....	6-22
6.2.7 Services with untagged-to-tagged translation .....	6-23

6.2.8 L2 Control Packets .....	6-24
6.2.9 Sample Eservices configuration .....	6-25
6.2.10 Ethernet Fault Propagation Shut Down .....	6-26
6.3 Ethernet services provisioning .....	6-28
6.3.1 Define a UNI .....	6-28
6.3.2 Define an NNI .....	6-29
6.3.3 Define an E-NNI and OVC .....	6-30
6.3.4 Provisioning Eservices .....	6-37
6.4 Provisioning profiles .....	6-40
6.4.1 Layer 2 Control Frame Profile provisioning .....	6-40
6.4.2 Tunnel MAC Address Profile provisioning .....	6-43

## **7.0 Configuring Ethernet Services OAM** **7-1**

7.1 Ethernet Service OAM .....	7-2
7.2 Loopbacks and linktrace .....	7-7
7.3 Ethernet Service OAM configuration .....	7-8
7.3.1 Basic configuration using proNX 900 .....	7-8
7.3.2 Provisioning CFM and the CCM interval using the CLI .....	7-9
7.3.3 Basic configuration using the CLI .....	7-10
7.3.4 Viewing the operational state and unavailable seconds (UAS) of an Ethernet service using proNX 900 .....	7-11
7.3.5 Viewing the operational state and unavailable seconds (UAS) of an Ethernet service using the CLI .....	7-11
7.3.6 Viewing the end points of an Eservice using proNX 900 Node Controller .....	7-13
7.3.7 Viewing the endpoints of an Eservice using the CLI .....	7-14
7.3.8 Performing a loopback test using proNX 900 .....	7-16
7.3.9 Performing a loopback test using the CLI .....	7-17
7.3.10 Performing a linktrace test using proNX 900 .....	7-17
7.3.11 Performing a linktrace test using the CLI .....	7-19
7.4 Interoperability considerations with third-party devices .....	7-20
7.5 Advanced procedures — Global settings .....	7-22
7.5.1 Viewing global settings .....	7-22
7.5.2 Changing a MEG name and MEG level .....	7-23
7.5.3 Viewing all MIPs .....	7-24
7.5.4 Disabling MIP auto-creation .....	7-24
7.5.5 Auto-creating MIPs .....	7-25
7.5.6 Changing the MEG ID pad .....	7-27
7.5.7 Disabling the protocol Y.1731 .....	7-27
7.5.8 Enabling the protocol 802.1ag .....	7-28
7.6 Advanced procedures — Eservice settings .....	7-29
7.6.1 Viewing Eservice settings .....	7-29
7.6.2 Disabling or enabling CFMs .....	7-30
7.6.3 Changing the CCM interval .....	7-30
7.6.4 Changing a ME name .....	7-31
7.6.5 Adding a remote MEP ID .....	7-32
7.6.6 Viewing the remote MEPs of an Eservice .....	7-32
7.6.7 Flushing the MEP list .....	7-34
7.6.8 Creating MIPs manually .....	7-34
7.7 Troubleshooting .....	7-36

7.7.1 Number of CCMs sent .....	7-36
7.7.2 Defects .....	7-36

## **8.0 Configuring Quality of Service and Class of Service** **8-1**

8.1 Service Level Agreements .....	8-2
8.2 Packet flow .....	8-4
8.3 Bandwidth profiles and traffic policing .....	8-5
8.3.1 Bandwidth profile rate enforcement .....	8-5
8.3.2 Ingress and egress bandwidth profiles .....	8-6
8.3.2.1 Ingress bandwidth profiles .....	8-6
8.3.2.2 Egress bandwidth profiles .....	8-7
8.3.3 Configuring bandwidth profiles .....	8-8
8.4 Packet classification .....	8-11
8.5 Transmission queuing and scheduling .....	8-13
8.6 CoS on intermediate switches .....	8-17
8.7 Quality of Service configuration .....	8-18
8.7.1 Define a Bandwidth Profile .....	8-18
8.7.2 Define a Class Map .....	8-19
8.7.3 Create a service policy .....	8-21
8.7.4 Applying a bandwidth profile to a UNI or NNI .....	8-22
8.7.5 Applying a bandwidth profile based on an Ethernet Service .....	8-23
8.7.6 Applying a bandwidth profile based on a Class of Service .....	8-24
8.7.7 Creating a Scheduler Profile .....	8-25
8.7.8 Applying a Scheduler Profile to a UNI or NNI .....	8-27
8.7.9 Mapping customer traffic priorities (DSCP/PCP) .....	8-28
8.7.10 Creating a Traffic Class Map Profile .....	8-29
8.7.11 Applying a Traffic Class Map Profile to a UNI/NNI .....	8-30
8.8 SLA monitoring .....	8-32
8.8.1 In-service monitoring .....	8-32
8.8.1.1 Defining an SLA profile .....	8-32
8.8.1.2 Initiating in-service monitoring .....	8-34
8.8.2 On-demand testing .....	8-35
8.8.3 SLA monitoring provisioning .....	8-37
8.8.3.1 Configuring an SLA profile .....	8-37
8.8.3.2 Configuring in-service monitoring .....	8-39
8.8.3.3 Configuring on-demand testing .....	8-41

## **9.0 Configuring flow redirection** **9-1**

9.1 Service maps and service policies .....	9-3
9.2 Applying service policies to service UNIs .....	9-5
9.3 Another application for flow redirection .....	9-7
9.4 Define a class map for flow redirect .....	9-9
9.5 Create a service policy for flow redirect .....	9-11

<b>10.0 Configuring Management VLAN services</b>	<b>10-1</b>
10.1 Managing the BTI 7000 Series: GCC, NMS, Craft, and Management VLAN .....	10-2
10.2 Configuring the Management VLAN service .....	10-5
10.2.1 Basic configuration .....	10-5
10.2.2 MgmtVLAN via UNI ports and C-VLANs .....	10-6
10.3 Configuration flowchart .....	10-9
10.4 Provisioning Management VLANs .....	10-11
10.4.1 Configuring NMS Ethernet to Management VLAN .....	10-11
10.4.2 Configuring Untagged to Tagged Management VLAN .....	10-12
10.4.3 Configuring GCC to Management VLAN Routing .....	10-14
 <b>11.0 Configuring Ethernet Ring Protection Switching (ERPS)</b>	 <b>11-1</b>
11.1 G.8032 operation .....	11-3
11.2 Failure detection .....	11-5
11.3 ERPS Model in the packetVX .....	11-6
11.3.1 Migrating from ERPS Version 1 to Version 2 .....	11-7
11.4 Basic ERPS configuration .....	11-8
11.5 Revertive vs. Non-Revertive operation .....	11-9
11.6 packetVX, BTI 700 Series, and BTI Service Access 800 Series on ERPS rings .....	11-10
11.7 ERPS and Spanning Tree .....	11-11
11.8 Multiple rings .....	11-17
11.8.1 Independent rings .....	11-17
11.8.2 Ladder rings .....	11-17
11.8.2.1 Ladder rings without R-APS virtual channel .....	11-18
11.8.2.2 Ladder ring interoperability with the BTI 700 Series .....	11-19
11.8.3 Managing segmentation between interconnected nodes .....	11-20
11.9 Administrative control of protection switching .....	11-21
11.10 ERPS provisioning .....	11-23
11.10.1 Provision ERPS on a single ring .....	11-23
11.10.2 Provision ERPS on multiple independent rings with a shared node .....	11-26
11.10.3 Provision ERPS on ladder rings .....	11-29
11.10.4 Enable manual protection switching .....	11-33
11.10.5 Disable manual protection switching .....	11-33
11.10.6 Enable forced protection switching .....	11-34
11.10.7 Disable forced protection switching .....	11-35
11.10.8 Modifying ERPS service parameters .....	11-35
11.11 Replacing a packetVX in an ERPS network: non-interconnected nodes .....	11-38
11.11.1 Replace a packetVX in an ERPS network: non-interconnected nodes .....	11-38
11.12 Removing a packetVX in an ERPS network: non-interconnected nodes .....	11-41
11.12.1 Remove a packetVX in an ERPS network: non-interconnected nodes .....	11-41
11.13 Adding a packetVX in an ERPS network: non-interconnected nodes .....	11-43
11.13.1 Add a packetVX in an ERPS network: non-interconnected nodes .....	11-43
 <b>12.0 BTI™packetVX® Security</b>	 <b>12-1</b>
12.1 Adding an access control .....	12-3

12.2 Removing an access control .....	12-4
---------------------------------------	------

## **13.0 Performance management** **13-1**

13.1 Supported performance metrics .....	13-2
13.1.1 Physical PMs supported on packetVX modules .....	13-2
13.1.2 GE port Ethernet (Layer 1) PMs supported on packetVX modules .....	13-2
13.1.3 10 GE (Layer 1) PMs supported on packetVX modules .....	13-3
13.1.4 10GE WAN PHY PMs .....	13-3
13.1.5 10 GE Port OTN (Layer 1) PMs .....	13-5
13.1.6 Ethernet (Layer 2) PMs .....	13-6
13.1.7 Link Aggregation Group PMs supported on packetVX modules .....	13-8
13.1.8 MSTP PMs supported on packetVX modules modules .....	13-9
13.1.9 Ethernet Services PMs supported on packetVX modules .....	13-10
13.1.10 ERPS PMs supported on packetVX modules .....	13-12
13.1.11 Protocol threshold crossing alerts (TCAs) and ranges supported on packetVX modules .....	13-13
13.2 Ethernet service performance monitoring statistics .....	13-15
13.2.1 Display Ethernet Service PM statistics per EVC .....	13-16
13.2.2 Display Ethernet Service PM statistics per CoS .....	13-17
13.2.3 Display Ethernet Service PM Thresholds .....	13-19
13.2.4 Set the Ethernet service PM Threshold per Eservice .....	13-21
13.2.5 Set the Ethernet service PM Threshold per Class of Service .....	13-22
13.2.6 Clear Eservice PMs per EVC .....	13-22
13.2.7 Clear Eservice PMs per CoS .....	13-24
13.3 Displaying and clearing performance monitor counts on packetVX modules .....	13-26
13.3.1 Display performance monitor counts for an Ethernet interface .....	13-26
13.3.2 Display the performance monitor history for an Ethernet interface .....	13-26
13.3.3 Display the performance monitor interval for an Ethernet interface .....	13-27
13.3.4 Display LACP BPDU counts for a LAG .....	13-27
13.3.5 Display MSTP BPDU counts for the CIST .....	13-28
13.3.6 Display MSTP BPDU counts for an MST instance .....	13-29
13.3.7 Display MSTP Topology Change counts for an MST instance .....	13-30
13.3.8 Clear LACP BPDU counts .....	13-31
13.3.9 Clear MSTP BPDU counts for the CIST .....	13-32
13.3.10 Clear MSTP BPDU counts for an MST instance .....	13-33
13.3.11 Clear MSTP Topology Change counts for an MST instance .....	13-34
13.4 Displaying and setting Threshold Crossing Alerts on packetVX modules .....	13-36
13.4.1 Display the performance monitor TCAs for an Ethernet interface .....	13-36
13.4.2 Set the performance monitor threshold for TCAs .....	13-36

## **14.0 Replacing BTI™ packetVX®modules and transceivers** **14-1**

14.1 Replacing packetVX modules .....	14-2
14.2 Replacing optical transceivers .....	14-5
14.3 Replacing copper transceivers .....	14-9

<b>15.0 Alarms and events on BTI™ packetVX® modules</b>	<b>15-1</b>
<b>Appendix A: Using BTI™ proNX 900 to provision and monitor packetVX® modules</b>	<b>A-1</b>
<b>Appendix B: Ethernet services provisioning using the 802.1ad model</b>	<b>B-1</b>
<b>Appendix C: Converting from the 802.1ad model to the Eservices model</b>	<b>C-1</b>

---

# Preface

---

This preface explains who should read this guide, related documentation, and documentation conventions.

## Audience

This guide is primarily intended for planning engineers, installers, technicians, and network operation center (NOC) staff.

## Features of the BTI 7000 Series

For detailed information about this release, see the *BTI 7000 Series Release Notes* for this release.

## BTI 7000 Series common equipment

The following table lists the shelves and other common equipment introduced as part of the BTI 7000 Series. For detailed information, see the *BTI 7000 Series Product Guide* and the *BTI 7000 Series Common Equipment Installation Guide*.

### BTI 7000 Series common equipment

Equipment	PEC
BTI 7060	BT7A50AA
BTI 7060 with rear access -48V	BT7A50AR
BTI 7060 Cooling Unit (CU)	BT7A52DA, BT7A52EA
BTI 7060 Main Shelf Interface (MSI)	BT7A53BA, BT7A53BB
BTI 7060 Expansion Shelf Interface (ESI)	BT7A54BA
BTI 7060/BTI 7200 System Control Processor (SCP)	BT7A20CA
BTI 7060 AC Power Assembly Kit	BT7A50BA
BTI 7060 AC Power Module	BT7A58AA

**BTI 7000 Series common equipment (Continued)**

<b>Equipment</b>	<b>PEC</b>
BTI 7060 Filler Panel Kit	BT7A55EA
2U Cover – ANSI	BT7A5070
2U Cover – ETSI	BT7A5071
BTI 7030	BT7A56AA
BTI 7030 Cooling Unit (CU)	BT7A57BA
BTI 7030 Main Shelf Interface (MSI)	BT7A53CA, BT7153CB, BT7A53BB
BTI 7030 System Control Processor (SCP)	BT7A21BA
BTI 7030 AC Power Assembly Kit	BT7A56CA
BTI 7030 AC Power Module	BT7A58BA
1U Cover – ANSI	BT7A5670
1U Cover – ETSI	BT7A5671
BTI 7020	BT7A56BA
BTI 7200	BT7A51AA
BTI 7200 with rear access -48V	BT7A51AR
BTI 7200 Cooling Unit (CU)	BT7A52EA
BTI 7200 Main Shelf Interface (MSI)	BT7A53EA
BTI 7200 Common Communication Module (CCM)	BT7A54EA
BTI 7200 ANSI shelf cover	BT7A5180
BTI 7200 ETSI shelf cover	BT7A5181
BTI 7200 Air Deflector	BT7A59EA
BTI 7200 Installation kit	BT7A5034
BTI 7200 Pack of 5 Mounting Bracket Pairs (7200)	BT7A5035
BTI 7200 Pack of 5 Center Guides	BT7A5036
Single Expansion Shelf Kit (2x 1310 SFP, 1x Dual SM Patch Cord 1.5m)	BP1A58LA-01.5
Single Expansion Shelf Kit (2x 1310 SFP, 1x Dual SM Patch Cord 2m)	BP1A58LA-02

The BTI 7000 Series shelves support a wide range of modules. For the list of modules supported, see the *BTI 7000 Series Product Guide*.

The following table lists the BTI graphical user interface management software suite. For detailed information about each application, refer to the documentation set for the application.

**Management software suite**

<b>proNX Management Suite</b>
proNX Service Manager (PSM)
proNX 900 Node Controller (proNX 900)



## Equipment compliance

The following table provides agency-compliance information for BTI 7000 Series equipment.




Agency	Compliance information
<b>FDA</b>	This equipment is classified by the FDA under IEC 60825, parts 1 and 2, as a Class 1 laser product with a Class 1 hazard rating.
<b>FCC</b>	This equipment complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.
<b>Industry Canada</b>	This Class A digital apparatus complies with Canadian ICES-003.

## Organization of the BTI 7000 Series documentation

The following guides are contained in the BTI 7000 Series documentation suite.

- *BTI 7000 Series Alarm and Troubleshooting Guide*
- *BTI 7000 Series Command Line Interface Reference Guide*
- *BTI 7000 Series Common Equipment Installation Guide*
- *BTI 7000 Series Dynamic Optical Layer Engineering Guideline*
- *BTI 7000 Series Management Communications Channel Solutions Guide*
- *BTI 7000 Series Multiplexing Solutions Guide*
- *BTI 7000 Series Muxponder Solutions Guide*
- *BTI 7000 Series Operations Solutions Guide*
- *BTI 7000 Series Optical Amplifier and DCM Solutions Guide*
- *BTI 7000 Series packetVX Solutions Guide*
- *BTI 7000 Series Product Guide*
- *BTI 7000 Series SNMP Overview Guide*
- *BTI 7000 Series Test and Turn-up Guide*
- *BTI 7000 Series TLI Reference Guide*
- *BTI 7000 Series Transceiver InformationGuide*
- *BTI 7000 Series Transponder Solutions Guide*
- *BTI 7000 Series Upgrade Guide*
- *BTI 7000 Series Release Notes*
- *BTI 7000 Series Quick Installation Notes (various)*

**Documentation conventions**

Convention	Description
<b>Note</b>	Means reader take note. Notes contain helpful suggestions or background information.
 <b>Caution</b>	Means reader be careful. Equipment damage or loss of data can result from your actions.
 <b>Warning</b>	Means reader be careful. Harm to yourself or others can result from your actions.
 <b>Laser Warning</b>	Invisible laser radiation can be emitted from the aperture ports of amplifier circuit packs when no fiber cable is connected. Avoid exposure and do not stare into open apertures to avoid permanent eye damage.

Copyright © 2017 Juniper Networks, Inc. ALL RIGHTS RESERVED.

This product is the property of Juniper Networks, Inc. and its licensors, and is protected by copyright. Any reproduction in whole or in part is strictly prohibited. Juniper, Juniper Networks, BTI, BTI SYSTEMS, packetVX, proNX, and The Network You Need are trademarks or registered trademarks of Juniper Networks, Inc. and/or its subsidiaries in the U.S. and/or other countries.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Copyright 2003-2016 BTI Systems, Inc. All rights reserved.

Copyright 1997-2001 Lumos Technologies Inc. All rights reserved.

Unpublished - All rights reserved under the copyright laws of the United States. This software is furnished under a license and use, duplication, disclosure and all other uses are restricted to the rights specified in the written license between the licensee and Lumos Technologies Inc.

Copyright 1998-2006 NuDesign Team Inc. All rights reserved. Copyright 1982-2001 QNX Software Systems Ltd. All rights reserved.

Copyright 1990-2001 Sleepycat Software. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Redistributions in any form must be accompanied by information on how to obtain complete source code for the DB software and any accompanying software that uses the DB software. The source code must either be included in the distribution or be available for no more than the cost of distribution plus a nominal fee, and must be freely redistributable under reasonable conditions. For an executable file, complete source code means the source code for all modules it contains. It does not include source code for modules or files that typically accompany the major components of the operating system on which the executable file runs. THIS SOFTWARE IS PROVIDED BY SLEEPYCAT SOFTWARE "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ARE DISCLAIMED. IN NO EVENT SHALL SLEEPYCAT SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1990, 1993, 1994, 1995 The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR

CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1995, 1996 The President and Fellows of Harvard University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY HARVARD AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL HARVARD OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1998 The NetBSD Foundation, Inc. All rights reserved.

This code is derived from software contributed to The NetBSD Foundation by Christos Zoulas. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. 3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the NetBSD Foundation, Inc. and its contributors. 4. Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED BY THE NETBSD FOUNDATION, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE FOUNDATION OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 2003 Maxim Sobolev sobomax@FreeBSD.org. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met: 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer. 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution. THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT

SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1995,1996,1997,1998 Lars Fenneberg lf@elemental.net.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg. Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1992 Livingston Enterprises, Inc. Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc. Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

The Regents of the University of Michigan and Merit Network, Inc. 1992, 1993, 1994, 1995. All Rights Reserved. Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation. THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

Copyright 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function. License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work. RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind. These notices must be retained in any copies of any part of this documentation and/or software.

All other product and company names are trademarks or registered trademarks of their respective companies. All of the above-referenced components are not necessarily included in all versions of the product.



# 1.0 Introduction to the BTI™packetVX®

---

The BTI packetVX represents the next stage of development in the BTI 7000 Series product line. The BTI 7000 Series is the industry's most compact, WDM platform, encompassing amplifiers, OADM's, transponders and muxponders, and the packetVX Carrier Ethernet switch.

The BTI 7000 Series, and the packetVX specifically, are designed with a service-provider focus and are NEBS-3 certified. The products support both AC and DC power. Versions that support extended temperature range are available. The BTI 7000 Series supports an OA&M infrastructure, with PM binning and alarming consistent with other CO-based equipment.

All BTI 7000 Series modules support short reach optics, long reach optics, CWDM, and DWDM. All packetVX modules and certain transponder and muxponder modules support OTU2 for increased reliability over extended distances.

## **BTI packetVX application focus**

The packetVX module is designed from the ground up as a Carrier Ethernet switch. Although it is a full-function MAC-layer Ethernet switch, it has been designed with a focus and feature set that is optimized for applications such as Ethernet Business Services, Video Delivery, and Mobile Backhaul.

This section covers the following topics:

- 1.1, "OTU digital wrapper"
- 1.2, "BTI™packetVX® modules"
- 1.4, "Configuration and management"
- 1.5, "Ethernet Service fault management"
- 1.6, "Applications overview"

## 1.1 OTU digital wrapper

---

The BTI 7000 Series platform, including packetVX, support OTU line rates. OTU has advantages over other native formats such as OC192 SONET and 10 GbE.

OTU provides forward error correction (FEC). Roughly six percent of each OTU frame is dedicated to an error correcting code. This provides, roughly, 6dB of coding gain for the OTU signal, resulting in lower error rates and/or greater transport distance. BTI 7000 Series modules that support OTU also support Enhanced Forward Error Correction (EFEC), which provides greater than 8dB of coding gain.

Another benefit of OTU is the bit transparent transport of client signals. OTU can be used to transparently wrap synchronous signals, such as SONET/SDH (and provides pointer adjustment capability to maintain synchrony), and asynchronous signals, such as Ethernet. In the case of Ethernet, transporting it wrapped in OTU enhances fault detection and improves reliability.

Also, due to OTU's forward error correction feature, an accurate bit error rate can be measured. The packetVX can take this signal degrade into account when making topology switching decisions. This capability is not available with 10G LAN PHY.

### OTU2

The BTI 7000 Series supports OTU2 line rates on the 10G Transponders and 10-Port Multiprotocol Muxponders.

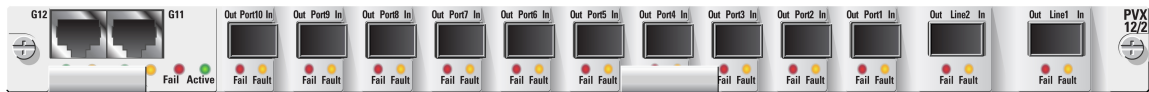
A practical advantage to using OTU2 for all 10G rate signals is simpler optical design. By using a single line rate (OTU2 operates at 10.709 Gb/s) there is a single set of design rules (loss, distance, etc.) for your optical network. This is important in WDM networks where different wavelengths are carrying different types of signals.



## 1.2 BTI™packetVX® modules

There are four members of the packetVX product line: packetVX 12/2, 24/2, 24/4, and 80. These designations indicate the number of Gigabit Ethernet (GbE) interfaces and 10 Gigabit Ethernet (10 GbE) interfaces on each module.

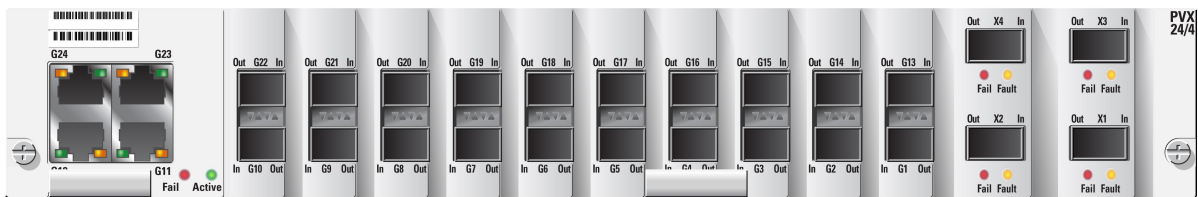
**Figure 1-1 packetVX 12/2**



**Figure 1-2 packetVX 24/2**



**Figure 1-3 packetVX 24/4**



**Figure 1-4 packetVX 80**



### packetVX interfaces

- packetVX 12/2: Double-width (two-slot) module with 12 GbE interfaces and two 10-GbE interfaces.
- packetVX 24/2 and 24/4 are: Double-height/double width (four-slot) modules with 24 GbE interfaces and two or four 10-GbE interfaces, respectively.
- packetVX 80: Double-width (two-slot) module with eight 10-GbE interfaces.

Although it is common to use GbE interfaces as client interfaces and 10-GbE interfaces as line interfaces, the packetVX does not impose these distinctions. All functions and capabilities are available on both interface types. This includes the ability to act as a UNI or NNI, support for link aggregation, performance monitoring, etc.

There are two copper (RJ45) GbE interfaces on the 12/2 packetVX module and four copper GbE interfaces on the 24/2 and 24/4 packetVX modules. There is one copper GbE interface on the packetVX 80, which is reserved for future use. The remaining GbE interfaces (10 and 20, respectively) support Small Form Factor Pluggable (SFPs) optical modules, including copper SFPs, 850nm multimode optics, 1310nm single-mode optics, and CWDM and DWDM optics. Note that the packetVX 80 is not equipped with SFP ports.

The packetVX supports a broad range of XFPs, including 850nm multimode, 1310nm single-mode, CWDM, and DWDM. All 10 GbE interfaces on the packetVX are software selectable between 10G LAN PHY and OTU2 digital wrapper.

---

## 1.3 Features of the packetVX portfolio

---

The packetVX modules provide the following features:

- GbE, 10GbE, and 10/100/1000BASE-T protocols
- G.709 OTN with enhanced FEC
- Provider bridging (IEEE 802.1ad)
- Ethernet services (EPLINE, EVPLINE, EPLAN, EVPLAN, ETREE)
- Quality of Service and Class of Service
- Link aggregation
- Multiple Spanning Tree Protocol (MSTP) which is compatible with RSTP and STP
- Ethernet Ring Protection Switching, Versions 1 and 2 (ITU-T G.8032)
- Ethernet service OAM (ITU-T Y.1731 and IEEE 802.1ag)
- Ethernet service statistics
- Ethernet and optical performance measurements
- Management VLAN
- Support for jumbo frames
- Access Control List (ACL) and Secure Shell (SSH) security
- System architecture that allows traffic to be carried uninterrupted if the System Control Processor (SCP) fails. A cold restart or a reseal of the SCP does not affect traffic.
- Supports a maximum of 32,000 MAC addresses
- proNX 900 Node Controller management support
- proNX Service Manager support
- CLI, SNMP, and Craft GUI management interfaces
- Extended temperature support (-40°C to +65°C)
- Storm Control
- NEBS™ Level 3 certified
- Support for Service Level Agreements ((SLA)
- Link Layer Discovery Protocol (LLDP)
- Stacking

### **VLAN tagging and provider bridging**

The switches supports provider bridging (IEEE 802.1ad). Provider bridging supports the encapsulation of private customer VLANs onto a provider network using stacked tags, or Q-in-Q

tagging, as defined in the IEEE 802.1ad standard. Customers can assign one or more customer VLANs (C-VLAN) to a service provider VLAN (S-VLAN) on any port.

The current provider bridging implementation supports:

- up to 768 individual C-VLAN to S-VLAN mappings (each interface in a LAG requires a separate mapping resource)
- up to 4088 S-VLANs
- Control frame profiles to provide ingress filtering

Provider bridging does not currently support S-VLAN translation.

### **Ethernet services**

- Ethernet Private Line (EPLINE)
- Ethernet Virtual Private Line (EVPLINE)
- Ethernet Private LAN (EPLAN)
- Ethernet Virtual Private LAN (EVPLAN)
- Ethernet Tree (ETREE)

### **Quality of Service and Class of Service**

- 802.1p, DSCP and TOS traffic prioritization
- 8 queues per port, strict priority, round-robin, weighted round-robin and deficit round-robin scheduling
- ingress and egress bandwidth profiles per UNI, EVC, COS

### **Link aggregation**

Link aggregation is an inverse multiplexing technique which uses multiple Ethernet ports in parallel to increase the link capacity beyond the limits of any one port, and to increase the redundancy for higher availability. A group of Ethernets combined in this way is called a Link Aggregation Group (LAG).

The current link aggregation implementation supports:

- up to 27 LAGs
- Eight members per LAG

### **Multiple Spanning Tree Protocol**

Multiple Spanning Tree Protocol (MSTP), part of the IEEE 802.1Q standard, provides the ability to create multiple spanning trees and assign VLANs to a spanning tree that closely reflects its optimal forwarding path. MSTP provides a single Common Spanning Tree Instance (CSTI) that is automatically created and Multiple Spanning Tree Instances (MSTI) that are configured to meet varied forwarding requirements.

The switches currently support up to 16 MSTP instances per switch.

**Ethernet Ring Protection Switching (ITU-T G.8032 Versions 1 and 2)**

Ethernet Ring Protection Switching (ERPS) is a ring-based control protocol that is standardized under ITU-T G.8032/Y1344. The BTI 7000 Series supports the following ERPS features:

- Ring topologies: single, multiple independent instances, ladder
- Switching: forced, manual and clear
- Ring recovery: revertive and non-revertive
- Sub-rings: with and without virtual channels

**Ethernet service OAM**

Ethernet service OAM provides end-to-end service visibility and monitoring of service availability/unavailability through check messaging, as well as loopback and linktrace testing capabilities for problem isolation.

**Ethernet service PM statistics**

The switches support the following Ethernet Service PMs:

- Bandwidth Utilization
- Rx Bytes
- Rx Violate Bytes
- Rx Conform and Exceed Bytes

The switches support the following bins of historical statistics:

- 15 Minutes
- 1 Day
- Un-Timed

The switches support threshold crossing alerts (TCAs) for the following bandwidth utilization policing parameters:

- CIR
- EIR

TCAs can be set or disabled by users. Statistics can be reset and refreshed on demand.

**Ethernet and optical performance measurements**

- GE Port Physical (Layer 0) PMs for SFP transceivers
- 10GbE Port Physical (Layer 0) PMs for XFP transceivers
- Ethernet (Layer 2) PMs
- Link aggregation group PMs
- MSTP PMs

## Management VLAN

The switches support a management VLAN that allows network operators to manage their network elements remotely.

## Jumbo frames

The switches support jumbo frames of up to 9600 bytes.

## ACL and SSH security

- Access Control Lists (ACLs) filter ingress traffic. The switches support up to 256 ACLs per switch.
- Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network, such as the Internet. The switches support up to 50 simultaneous SSH sessions.

## Management interfaces

The switches support the following management interfaces:

- Command Line Interface (CLI) interface
- proNX 900 Node Controller
- proNX Service Manager
- SNMP

The **Command Line Interface (CLI)** supports a comprehensive and interactive set of commands to provision, monitor, and administer switch modules.

The **proNX 900 Node Controller** provides a graphical user interface to provision, operate, monitor, and troubleshoot switches. This interface provides a representational view of the physical configuration of each shelf in the BTI 7000 Series network and the modules in each shelf.

The **proNX Service Manager** provides proactive, service-centric management of network resources to simplify network operations, from visualization and activation of services to troubleshooting and supporting end customers.

The **Simple Network Management Protocol (SNMP)** implementation supports SNMPv1 and SNMPv2c, for messaging and authentication of community strings.

## Extended temperature support

The switches can be deployed in extended temperature environments ranging from -40°C to +65°C (-4°F to +150°F). For more information, refer to Application Note BTI-APN002-2011 *Engineering considerations for packetVX in -40C to +65C applications*.

**Storm Control**

The packetVX provides Layer-2 storm protection to maintain network performance during periods of excessive traffic. Storm Control is supported on configured NNI ports, on a per-port basis, and on NNI LAGs.

**SLA monitoring**

The BTI 7000 Series provides SLA support in two ways: In-service monitoring and on-demand testing.

**Link Layer Discover Protocol (LLDP)**

The BTI packetVX supports LLDP, as specified in the IEEE 802.1AB standard for "Station and Media Access Control Connectivity Discovery." LLDP is a Link Layer protocol that provides network devices the ability to advertise their identity, capabilities, and neighbors to other network devices on an IEEE 802 local area network. For information on how LLDP is implemented on the packetVX refer to [5.10, "Link Layer Discovery Protocol"](#).

**Stacking**

The packetVX provides equipment redundancy by stacking two PVX modules. The 12/2 and 24/4 PVX stacking is through one or more 10 gigabit Ethernet interfaces to expand bandwidth to the stacking ports and provide a non-blocking bridge between two stacked modules. Multiple interfaces on the stacking port balances the traffic across the interfaces, which allows more data bandwidth between switches and minimizes the risk for blocking. The packetVX 80 stacking is via the backplane on the BTI 7200. Hence, packetVX 80 stacking is not supported on the BTI 7060.

For more information about stacking refer to [4.3, "Stacking"](#).

## 1.4 Configuration and management

---

SNMP or CLI are required to manage BTI 7000 Series network elements equipped with packetVX modules. A subset of TL1 capabilities are provided for packetVX modules, including equipment inventory and alarms.

The proNX 900 Node Controller (proNX 900) and proNX Service Manager (PSM) can be used to configure, manage, and monitor BTI 7000 Series, in which packetVX modules are installed:

- proNX 900: Manages the system per component
- PSM: Manages all components as a system

The BTI 7000 Series supports an IP transport facility for network management. The System Control Processor (SCP) implements an IP control plane with distributed forwarding on all modules. Interfaces to the management network include the following:

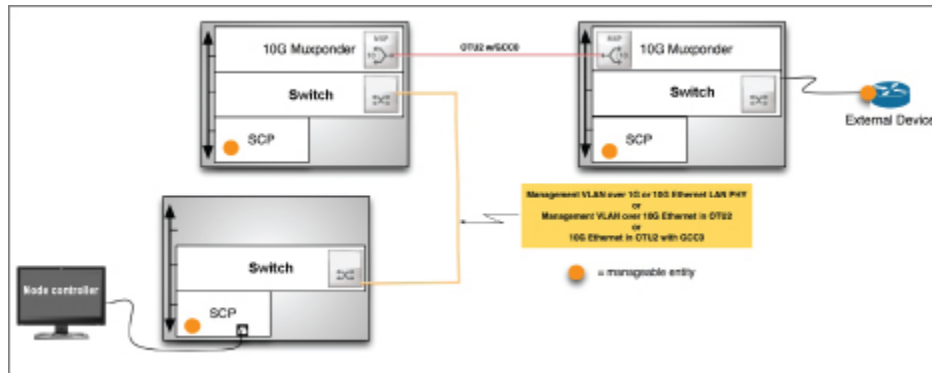
- The external management Ethernet connection on each system
- The management VLANs between packetVX modules in the bridged network
- The GCC0 (General Communications Channel) on OTU2 interfaces

The management VLAN capability allows the network administrator to define an S-VLAN on the bridged network for management traffic—both BTI 7000 Series system management and management of external devices. The packetVX treats the management VLAN as an IP interface into the management subsystem. It will respond to ARP messages on this channel and also act as an IP forwarder/router for packets addressed to it.

The OTU2 GCC0 is also an interface on the management network. Each OTU2 frame contains a 2-byte GCC0 field. All BTI 7000 Series modules, including the packetVX, allow the GCC0 to be used as an out-of-band management channel. Management packets that enter the BTI 7000 Series chassis from different interfaces (management Ethernet, OSC, etc.) can be routed from chassis to chassis over the GCC0 channel. This provides a secure channel that does not interfere with user data.

This set of capabilities provides network management connectivity for a broad range of network configurations. The following figure shows some of the possible management connections. In this figure, the proNX 900-based network management station on the left can manage any of the systems with an orange dot (the external device might require a different network manager, which could be on the same network as the proNX 900-based system). Each module has an IP forwarder, with forwarding tables that can be populated manually or, more commonly, by OSPF running on each SCP. The management packets can traverse Ethernets in the management VLAN and OTU2 links in the GCC0 channel.



**Figure 1-5 Network management infrastructure**

## 1.5 Ethernet Service fault management

---

The packetVX supports Y.1731 Connectivity Fault Management (CFM). CFM discovers the end points of configured Ethernet services and periodically verifies connectivity between the UNIs that compose the service. If a connectivity failure is detected, the packetVX systems will record that as part of the status for the service and will, if appropriate, report an event to the network management system. CFM also provides the ability to perform a loopback from end-to-end on a service (similar to a PING) and also to trace the path of a service in order to assist in diagnosis of a fault.

## 1.6 Applications overview

The BTI packetVX provides an innovative approach for the rapid delivery of new Ethernet-based services. It provides carrier-grade GbE service aggregation onto 10 Gb/s linear and ring topologies, coupling packet switching functionality with wavelength-division multiplexing (WDM).

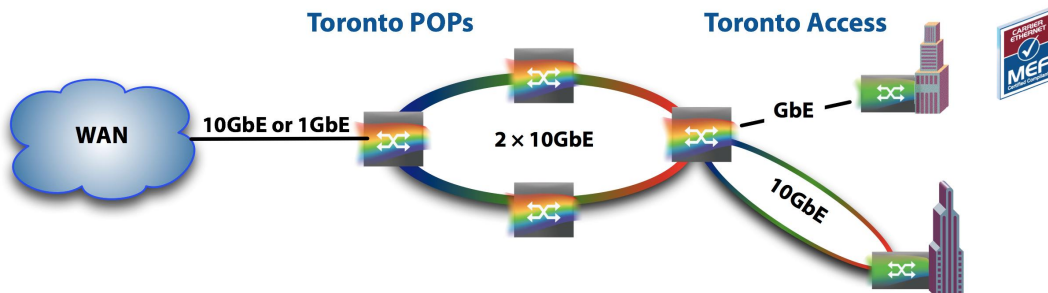
The packetVX provides point-to-point and ring protection for increased service availability. Innovative service provisioning capabilities dramatically simplify the operation, management, and provisioning of residential, video, and Ethernet business services.

### 1.6.1 Provider Bridging and Ethernet Business Services

The BTI packetVX module is an 802.1ad-compatible Provider Bridge that has been designed around the concept of Ethernet as a service.

The packetVX module provides Ethernet Line and Ethernet LAN services as defined by the Metro Ethernet Forum (MEF). The Ethernet Service is a basic building block of the packetVX configuration. It supports Ethernet business services (Eservices), as shown in the following figure:

**Figure 1-6 Ethernet business services**



The packetVX module supports the following features for Eservices:

- MEF 6 and 10 for ELine, ELAN, and ETree services (MEF 9 and MEF 14 certified)
- 802.1ad Q-in-Q tagging
- Per-port and per VLAN rate limiting with granularity of 1 Mb/s.
- CoS on a per-ingress-port, per-EVC, or per-ingress-VLAN basis
- Access control lists (ACLs) to filter ingress traffic on source MAC, destination MAC, source IP, and destination IP

When the packetVX is configured, an Eservice is defined, its type (for example, Ethernet Virtual Private Line) and S-VLAN are specified, and the UNI (or UNIs) is attached to the service. For example:

```
//First define the UNI
BTI7000:sw1(config)# uni gigabitEthernet 1/1/11
```

```

uni GigE 1/1/11 created.
BTI7000:sw1(config-uni GigE 1/1/11)# exit
//Now define and configure the Ethernet Service
BTI7000:sw1(config)# eservice Customer1 type EPLAN
Ethernet Service "Customer1" created.
BTI7000:sw1(config-eservice)# s-vlan 10
BTI7000:sw1(config-eservice)# uni gigabitEthernet 1/1/11
UNI E-Service "GigE 1/1/11-Customer1" created.
BTI7000:sw1(config-uni-eservice)# exit
BTI7000:sw1(config-eservice)# exit

```

With most systems, it is necessary to configure the bridge to implement an Eservice. With packetVX, the user configures the Eservice and the system configures a logical bridge to implement it.

The packetVX module includes traffic management and quality of service capabilities. Traffic policing can be performed on each UNI at the UNI level, at the EVC level, or at the Class-of-service (CoS) level. CoS can be assigned based on a number of attributes, such as input port, Eservice, 802.1p priority, and IP markings, such as ToS and DSCP. Each egress (NNI) port supports eight class-of-service queues. Traffic shaping parameters and scheduling discipline can be specified for each CoS queue on each port.

## 1.6.2 Ethernet aggregation

The packetVX module supports the following Ethernet aggregation applications:

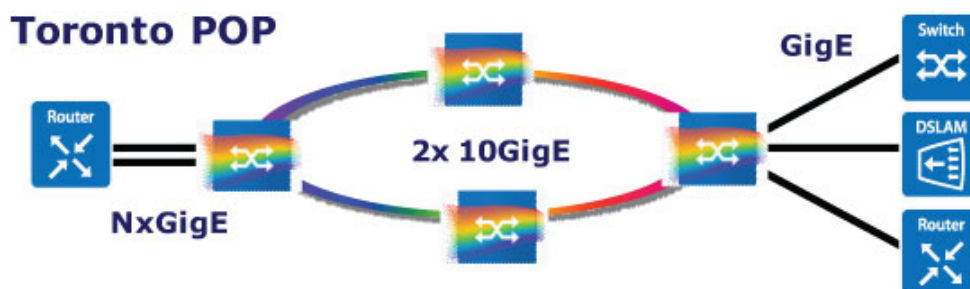
- Simple Ethernet aggregation
- Wholesale access aggregation
- Cable Modem Termination System (CMTS) backhaul

### Scenario 1 - Simple Ethernet aggregation

This simple Ethernet aggregation scenario shows the following:

- Up to four 10-GbE ports to support the migration to GbE access
- high fan-in density with up to 24 1-GbE ports per module
- Bandwidth when and where it is needed to address traffic unpredictability
- Two 10-GbE-port hand off to enable high-density GbE aggregation

**Figure 1-7 Simple Ethernet aggregation**

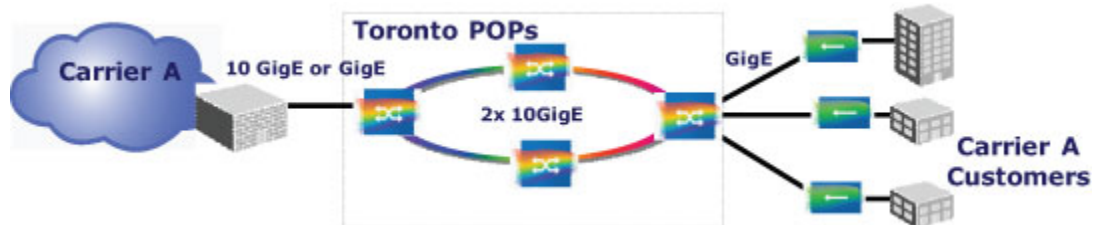


## Scenario 2 - Wholesale access aggregation

This wholesale access aggregation scenario shows the following:

- 802.1ad Q-in-Q tagging with single-tagging or double-tagging on any port
- Tunnel Layer 2 control protocols, as required, for service transparency
- Low frame delay and delay variation
- No packet reordering
- Optical and Ethernet performance measurements

**Figure 1-8 Wholesale access aggregation**

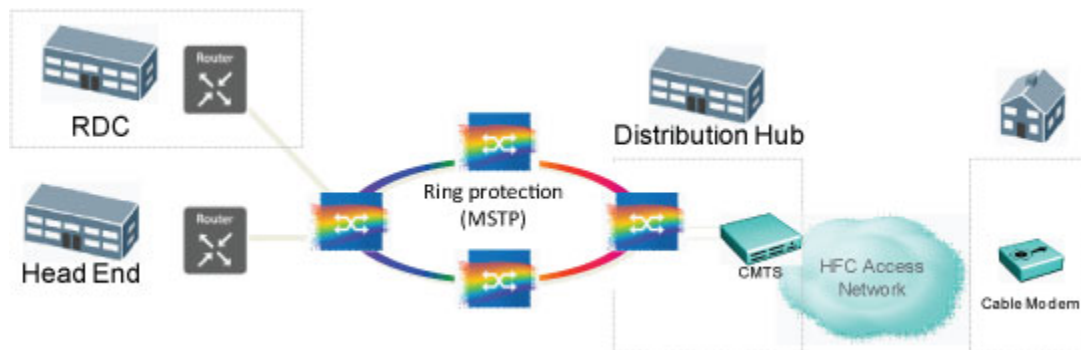


## Scenario 3 - Cable Modem Termination System (CMTS) backhaul

The switch supports the following features for CMTS backhaul:

- 802.1ad Q-in-Q tagging with single-tagging or double-tagging on any port
- Access control lists (ACLs) to filter ingress traffic on SMAC, DMAC, SIP, and DIP

**Figure 1-9 CMTS backhaul**



## 1.6.3 Ethernet video applications

The packetVX module supports the following Ethernet video applications:

- Broadcast video
- Video on Demand (VoD)

## Scenario 1 - Broadcast video

This broadcast video scenario shows the following:

- Up to four 10-GbE ports to support thousands of broadcast video streams
- Optimized network bandwidth with Ethernet aggregation at the network edge
- Delay, delay-variation and packet loss minimized
- No packet reordering
- All traffic arriving at an ingress port is guaranteed to be transmitted out of the egress port at the other end of the connection

**Figure 1-10 Broadcast video**

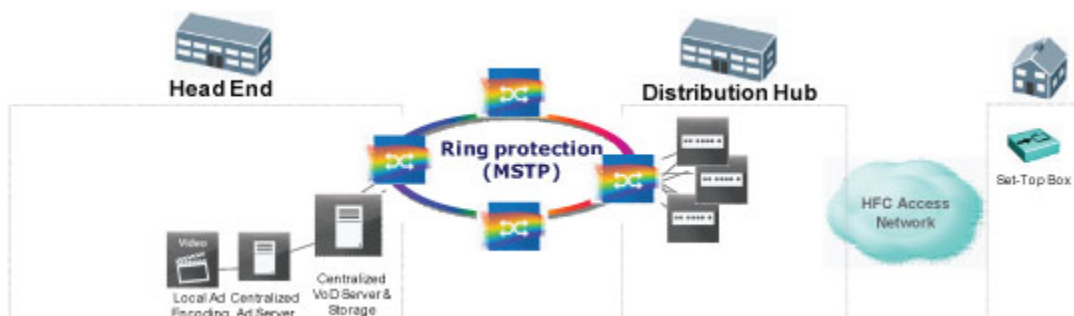


## Scenario 2 -Video on Demand

This video on demand scenario shows the following:

- Up to 4 10GE ports to support the migration to High Definition
- High fan-in density with up to 24 GbE ports per switch
- Bandwidth when and where it is needed to address unpredictability of VoD
- LAG for subtending devices at head end or distribution hub
- MSTP ring protection

**Figure 1-11 Video on Demand**



## 1.6.4 4G wireless and WiMAX

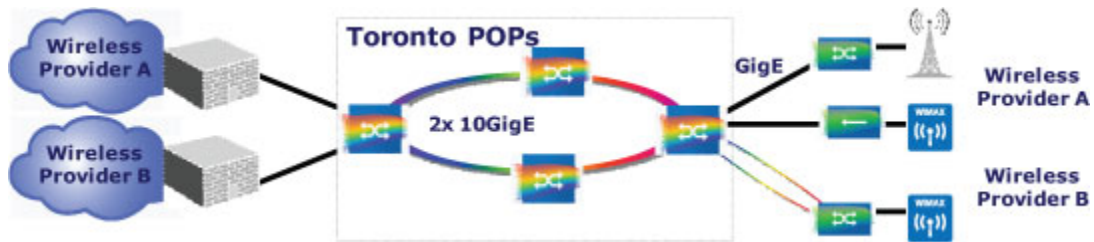
The packetVX module supports 4G wireless and WiMAX applications.

### Scenario 1 - 4G wireless and WiMAX

This 4G wireless and WiMAX scenario shows the following:

- network capacity enables migration to 4G networks (Gbps per antenna)
- 802.1ad Q-in-Q tagging to accommodate and separate wireless service providers
- low frame delay, delay variation and guaranteed delivery of voice
- suitable for deployment in outside plant modules

**Figure 1-12 4G wireless and WiMAX**







## 2.0 BTI™packetVX® hardware selection and installation

---

This section describes the family of BTI packetVX modules, providing guidance on how to select a particular module for a specific application and detailed specifications for each switch.

This section also describes the procedures for installing a system equipped with packetVX modules. Specific tasks include shelf setup, and module and transceiver installation.

- 2.1, “BTI™packetVX® portfolio”
- 2.2, “packetVX and transceiver installation”

## 2.1 BTI™ packetVX® portfolio

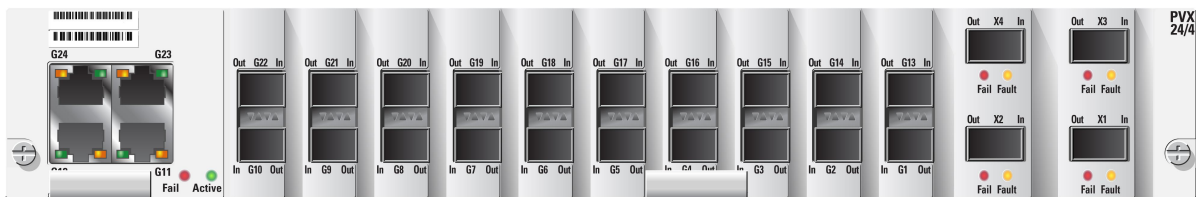
The BTI packetVX modules provide an innovative approach for rapid delivery of new Ethernet-based services. Integrated into a BTI 7000 Series platform, the packetVX modules provide Ethernet service aggregation onto 10Gb/s Ethernet rings, coupling packet switching functionality with WDM. Managed as a module within the platform, the packet service delivery capabilities dramatically simplify operations, management, and provisioning of residential, video and Ethernet business services using a converged network approach.

The following figures show the modules offered in the BTI 7000 Series packetVX portfolio.

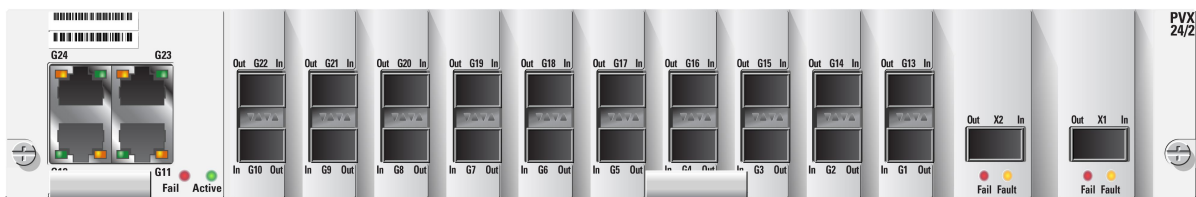
**Figure 2-1 packetVX 80 (BT7A81GA)**



**Figure 2-2 packetVX 24/4 (BT7A81CA)**



**Figure 2-3 packetVX 24/2 (BT7A81BA)**



**Figure 2-4 packetVX 12/2 (BT7A81AA)**



All packetVX modules support the same features and functionality, differing only in the number of GbE and 10-GbE ports. For detailed information, see [2.1.1, “packetVX specifications”](#).

## 2.1.1 packetVX specifications

Specification	packetVX 80 (BT7A81GA)	packetVX 24/4 (BT7A81CA)	packetVX 24/ 2 (BT7A81BA)	packetVX 12/ 2 (BT7A81AA)
Dimensions (slots wide x slots high)	2 x 1	2 x 2	2 x 2	2 x 1
RJ45 ports <sup>1</sup>	0	4	4	2
SFP ports	None	20	20	10
XFP ports	8	4	2	2
10/100/1000BT -- RJ45	No <sup>2</sup>	Yes	Yes	Yes
10/100/1000BT -- copper SFP	No	Yes	Yes	Yes
100FX -- optical SFP	No	Yes	Yes	Yes
Gigabit Ethernet -- optical SFP	No	Yes	Yes	Yes
10 Gigabit Ethernet LAN PHY -- optical XFP	Yes	Yes	Yes	Yes
ITU-T G.709 OTU2 with G.975 FEC -- optical XFP	Yes	Yes	Yes	Yes
ITU-T G.709 OTU2 with enhanced FEC -- optical XFP	Yes	Yes	Yes	Yes
10 Gigabit Ethernet WAN PHY <sup>3</sup> -- optical XFP	Yes	No	No	No
Switching Capacity (Gbps)	160	64	44	32
Forwarding Rate 64-byte packets (Mpps)	95	95	65	47
Number of MAC addresses <sup>4</sup>	32,000	32,000	32,000	32,000
Number of S-VLANs (4091- 4095 are reserved for internal operation) <sup>5</sup>	4090	4090	4090	4090
Number of C-VLAN map table entries <sup>6</sup>	768	768	768	768
<sup>7</sup>				
Ethernet Virtual Circuit (EVC) <sup>8</sup>	500	500	500	500
Number of static unicast entries	256	256	256	256
Jumbo frame size (bytes)	9600	9600	9600	9600
Maximum number of link aggregation groups	8	27	27	27
Number of members in a link aggregation group	8	8	8	8
Number of MSTP instances	16	16	16	16
Number of L2 control frame profiles	154	154	154	154
Egress queues per port	8	8	8	8
Ingress policers	256	768	768	768

Specification	packetVX 80 (BT7A81GA)	packetVX 24/4 (BT7A81CA)	packetVX 24/ 2 (BT7A81BA)	packetVX 12/ 2 (BT7A81AA)
Egress policers	64	64	64	64
Local Maintenance End-points (MEPs)	768	768	768	768
Remote Maintenance End-points (MEPs)	768	768	768	768
Maintenance Intermediate points (MIPs)	1536	1536	1536	1536
Maximum number of nodes per ERPS ring	16	16	16	16
Maximum number of management VLANs	1	1	1	1
Number of ACLs	256	256	256	256
Maximum number of modules per network element	10	10	10	10
One-way latency for a 64 byte packet (micro-seconds)	5	5	5	5
One-way latency for a 1518 byte packet (micro-seconds)	20	20	20	20
Operating Temperature	-5 to +50C	-5 to +50C	-5 to +50C	-5 to +50C
Operating Temperature (with engineering restrictions)	-40 to +65C	-40 to +65C	-40 to +65C	-40 to +65C
Maximum power consumption (Watts)	50	70	65	50

<sup>1</sup>When SLA is enabled, the maximum number of RJ45 ports is 2.

<sup>2</sup>The RJ45 port is reserved for future use.

<sup>3</sup>10GE WAN PHY allows the port to be connected directly to SONET/SDH equipment such as an add/drop multiplexer or a transponder, without intervening equipment. The Ethernet signal is encapsulated within an OC192/STM64 frame, which can then be transported across the SONET/SDH network. However, because the encapsulation requires additional information to be inserted, the effective data rate is reduced to just under 9.3 Gbps.

<sup>4</sup>MAC addresses age out, automatically, in five minutes when traffic is not seen from that MAC address.

<sup>5</sup>This is without spanning tree protocol (RSTP) enabled on the UNI port. When RSTP is enabled on UNIs that are supporting virtual services, the maximum number of EVCs per network is 1000.

<sup>6</sup>This is without spanning tree protocol (RSTP) enabled on the UNI port. When RSTP is enabled, the maximum number of C-VLAN map table entries is 200.

<sup>7</sup>There can be a maximum of 400 EVCs per UNI.

<sup>8</sup>There can be up to 500 dynamically signaled EVCs per network element. All other EVCs must be statically configured.

## 2.1.2 Supported SFPs and XFPs

The following table lists the SFPs and XFPs supported on packetVX modules.

Type	Description	PEC
SFP	10/100/1000BT Copper	BP3AD3ES

Type	Description	PEC
	850nm SX	BP3AD1SS
	SFP: 4G 850nm SX	BP3AD2SS
	<b>Note</b> Introduced in Release 7.1.2.	
	1310nm SR	BP3AM1MS
	1310nm IR	BP3AM1MI
	Bidirectional 1310nm TX/1550nm RX	BP3AM5MB
	Bidirectional 1550nm TX/1310nm RX	BP3AM5LB
	CWDM 23dB	BP3AM1CJ-xx [xx = 01 to 16]
	CWDM LR	BP3AM1CL-xx [xx=01 to 16]
	DWDM ER	BP3AM1DE-xx [xx = 01 to 32]
	DWDM XR	BP3AM1DX-xx [xx = 01 to 32]
<b>XFP</b>	850nm	BP3AM4SS
	1310nm SR	BP3AM4MS
	1550nm IR	BP3AM4LI
	C-band Tunable DWDM LR	BP3AM4TL
	CWDM LR	BP3AM4CL-xx [xx = 01 to 08]
	DWDM LR	BP3AM4DL-xx [xx = 01 to 32]

### XFP Cold Reboot

packetVX , transponder, and muxponder modules support an XFP cold reboot on only 10G ports. An XFP cold reboot may be performed provided one of the following conditions exist:

- The associated port is manually put out of service (OOS-MA).
- There is no provisioned port against it.

To perform an XFP cold reboot use the **reset** command from Ethernet interface configuration mode.

## 2.1.3 Shelf support

The packetVX modules are supported in BTI 7060 and BTI 7200 main and expansion shelves.

The BTI 7030 supports only the packet 12/2 as it has only two active slots. A packetVX 12/2 can also be equipped in a Netstender 2060 shelf provided that the System Control Processor and cooling unit have been properly upgraded.

The following table summarizes the shelf support options for the modules.

Shelf	packetVX 80	packetVX 24/4	packetVX 24/2	packetVX 12/2
BTI 7060 (BT7A50AA)	Yes	Yes	Yes	Yes
BTI 7030 (BT7A56AA)	No	No	No	Yes

Shelf	packetVX 80	packetVX 24/4	packetVX 24/2	packetVX 12/2
BTI 7200 (BT7A51AA)	Yes	Yes	Yes	Yes
<b>Note</b> This shelf supports BTI software releases 8.1 and later.				

## 2.1.4 Considerations for selecting a packetVX module

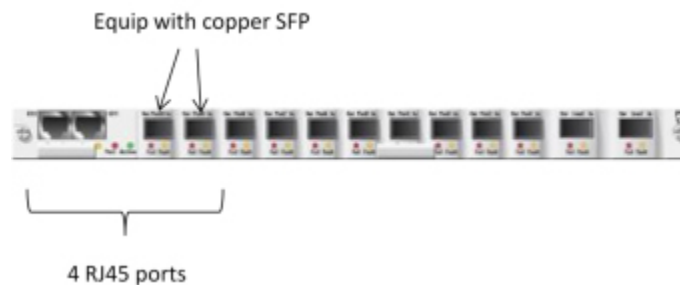
Selecting a packetVX module for a specific application is a matter of determining the required number of GbE and 10-GbE ports.

### GbE ports

If more than 12 GbE ports are required, a packetVX 24/2 or packetVX 24/4 module is required.

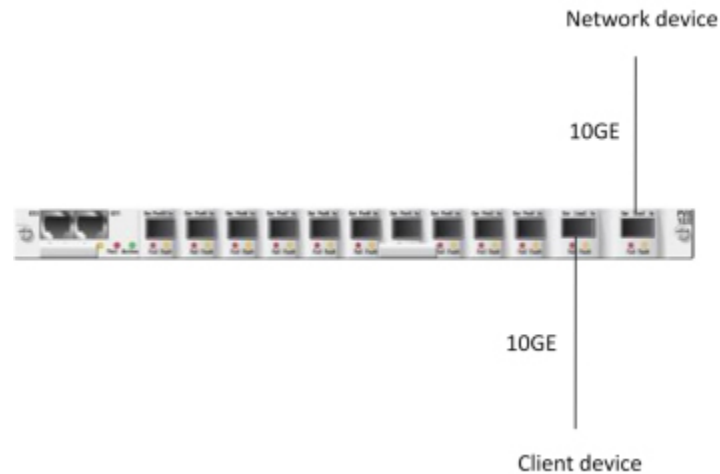
SFP ports on a packetVX module support optical or copper (electrical) SFPs. Therefore, if an application requires four RJ45 ports, a packetVX 12/2 module equipped with two copper SFPs may be a suitable alternative.

**Figure 2-5 packetVX 12/2 equipped with two copper SFPs to provide four RJ45 ports**

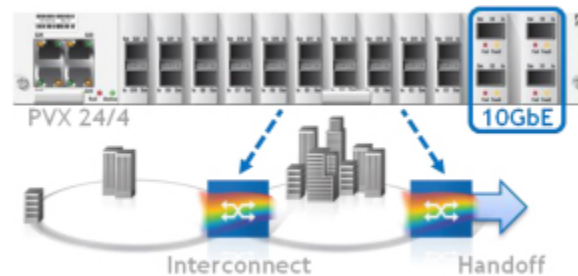


### 10-GbE ports

The 10-GbE ports on a packetVX module can be used as client or line ports, i.e., there are no restrictions between client and line.

**Figure 2-6 packetVX 12/2 with one 10-GbE client and one 10-GbE line**

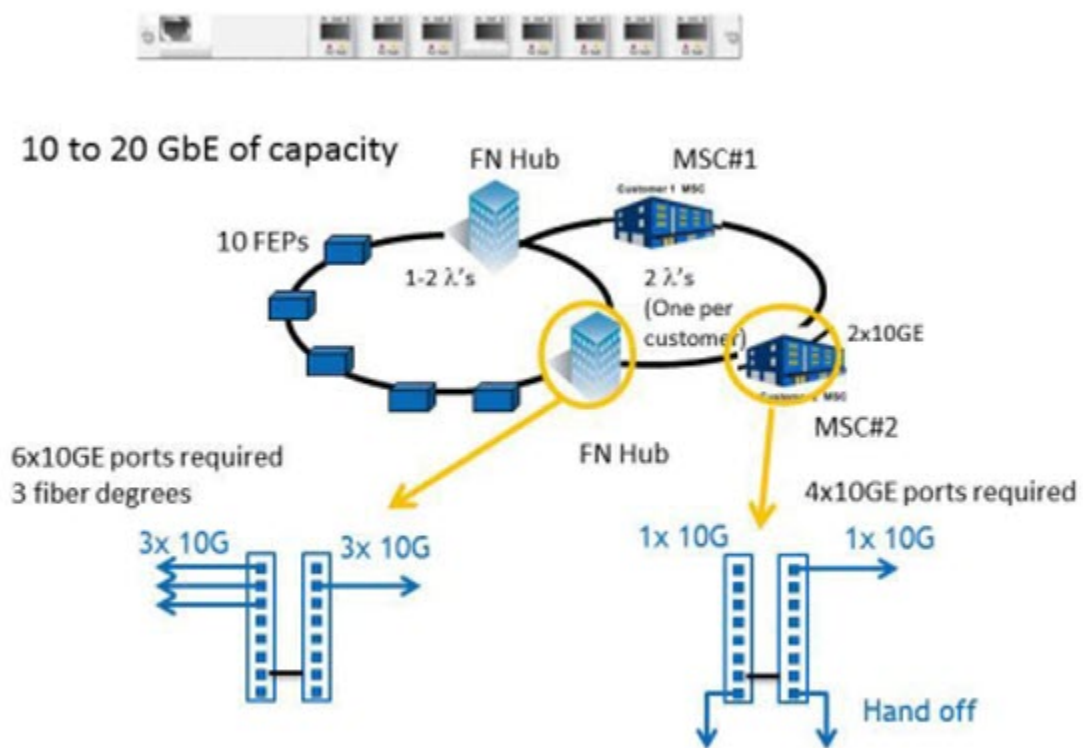
In ring applications, two 10-GbE ports at access sites are usually sufficient. At hub sites, four 10-GbE ports may be necessary in order to handoff at 10 GbE. Four 10-GbE ports may also be necessary at sites where two 10-GbE rings need to be interconnected.

**Figure 2-7 packetVX 24/4 used for ring interconnect and 10-GbE handoff**

In ring applications, you use the packetVX 80 to interconnect more than two 10G rings. Use the packetVX 80 where:

- Node level redundancy is required with high capacity.
- Ring capacity is expected to grow, rapidly, from 10G to 20G or 40G.
- WAN PHY interface is needed

Figure 2-8 packetVX 80





## 2.2 packetVX and transceiver installation

### 2.2.1 BTI 7060 setup

The default configuration of a BTI 7060 is six slots. To accommodate a packetVX module, slot dividers need to be removed. In a main shelf (shelf equipped with an SCP and MSI), the slot dividers must not be removed between slots 5 and 6. In an expansion shelf (shelf equipped with an ESI) all slot dividers can be removed. See the *Common Equipment Installation Guide* for information about removing slot dividers. The following figures show various configurations of the BTI 7060 shelf.

**Figure 2-9 BTI 7060 default configuration**



Power	Cooling	1	Service Slot	2	Service Slot
		3	Service Slot	4	Service Slot
	Shelf I/P	5	Shelf Controller	6	Service Slot

**Figure 2-10 BTI 7060 designed to accommodate a packetVX 12/2 module and a packetVX 80**



Power	Cooling	1 Service Slot	
		3 Service Slot	4 Service Slot
	Shelf I/P	5 Shelf Controller	6 Service Slot

Power	Cooling	1	Service Slot	2	Service Slot
		3	Service Slot		
	Shelf I/F	5	Shelf Controller	6	Service Slot

Power	Cooling	1	Service Slot	
		3	Service Slot	
	Shelf I/F	5	Shelf Controller	6

**Figure 2-11 BTI 7060 designed to accommodate a packetVX or 24/2 or 24/4 module**



Power	Cooling	1 Service Slot	
	Shelf I/F	5 Shelf Controller	6 Service Slot

**Note** When a slot divider is removed from a BTI 7060, the resulting slot is referred to by the lowest slot number. For example, if the slot divider is removed between slots 1 and 2, the resulting slot is referred to as slot 1.

2.2.2 BTI 7030 setup

The default configuration of a BTI 7030 is two slots. The slot divider between slots 1 and 2 must be removed to accommodate a packetVX 12/2 module. The following figures show various configurations of the BTI 7030 shelf.

Figure 2-12 BTI 7030 default configuration



Figure 2-13 BTI 7030 designed to accommodate a packetVX 12/2 module



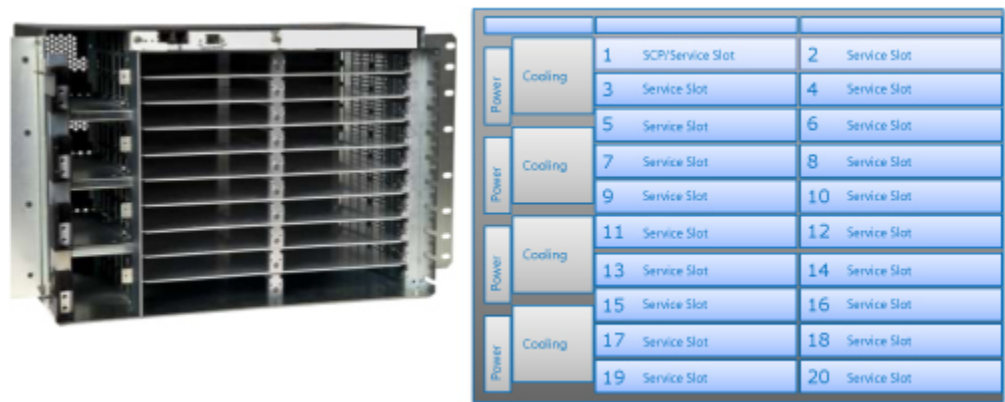
**Note** When a slot divider is removed from a BTI 7030, the resulting slot is referred to by the lower slot number. For example, if the slot divider is removed between slots 1 and 2, the resulting slot is referred to as slot 1.

2.2.3 BTI 7200 setup

The default configuration of a BTI 7200 is 20 slots. To accommodate a packetVX module, slot dividers need to be removed. In a main shelf (shelf equipped with an SCP), the slot dividers must not be removed between slots 1 and 2. In an expansion shelf, all slot dividers can be removed. See the *Common Equipment Installation Guide* for information about removing slot dividers. The following figures show some configurations of the BTI 7200 shelf.

**Note** BTI 7200 supports only BTI software releases 8.0 and later.

Figure 2-14 BTI 7200 default configuration: 20 service slots, 7 RU

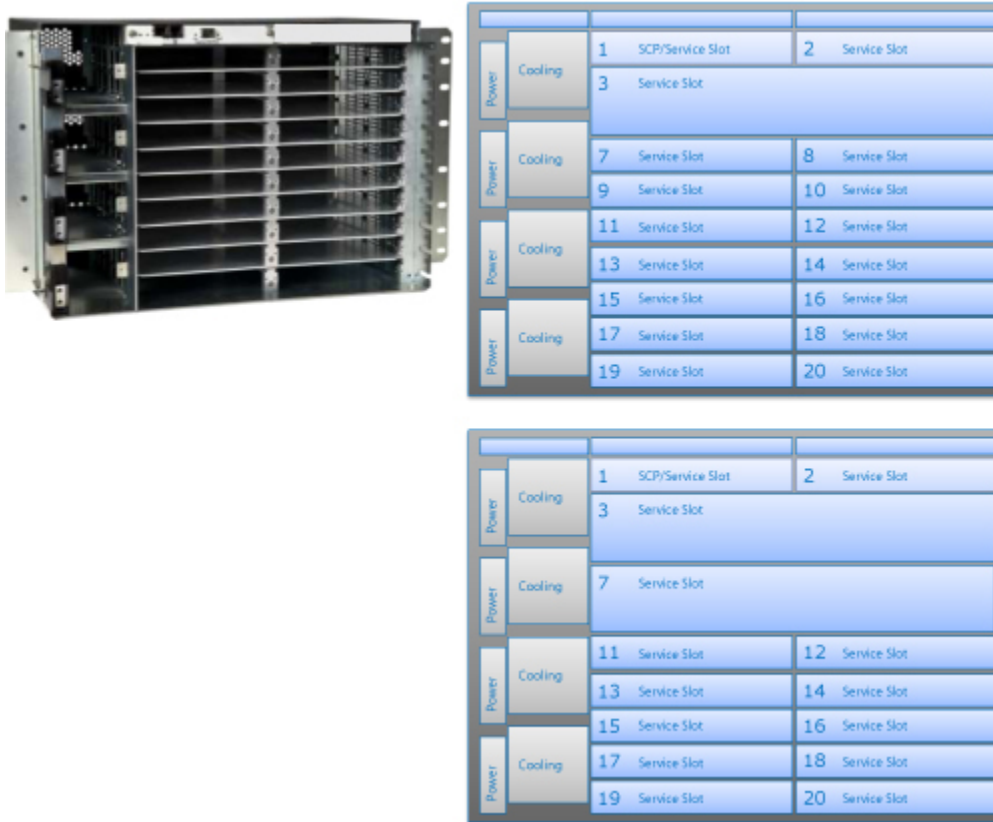


**Figure 2-15 BTI 7200 configured to accommodate two packetVX 24/2 or 24/4 modules and a packetVX 12/2 module**



**Figure 2-16 BTI 7200 configured to accommodate a packetVX 12/2 module**



**Figure 2-17 BTI 7200 configured to accommodate a packetVX 24/2 or 24/4 module**

**Note** When a slot divider is removed from a BTI 7200, the resulting slot is referred to by the lowest slot number. For example, if the slot divider is removed between slots 3 and 4, the resulting slot is referred to as slot 3.

## 2.2.4 Installing packetVX modules

Use this procedure to install a packetVX module.

### What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- packetVX module
- SFP or XFP transceivers
- Isopropyl alcohol and lint-free pads
- 1.25 mm HUXcleaner (recommended). Use ordering code BP1A5034.

## Prerequisites

- If installing a packetVX 12/2 or packetVX 80 module, ensure that a double-width slot is available for it.
- If installing a packetVX 24/2 or 24/4 module, ensure that a double-width, double-height slot is available for it.

## Considerations for installing a double-height packetVX module in a BTI 7200 shelf

Double-height packetVX modules (24/2 - BT7A81BA or 24/4 - BT7A81CA) that are new, or that have previously been used in BTI 7060 shelf running R7.x, must have their software upgraded to R8.1 or later to be fully compatible with the BTI 7200 shelf.

To upgrade a packetVX module's software, use one of the following methods:

- Install the packetVX module into one of slots 5, 7, 11, 15, or 17 in the BTI 7200 shelf. By installing into one of these slots, the module's software is automatically upgraded to R8.1, and the module can then be provisioned. If you install the module into any other BTI 7200 slot (3, 9, or 13), the software is not upgraded and the module cannot be provisioned.
- If the packetVX module is being re-deployed from a BTI 7060 shelf, leave the packetVX module in the BTI 7060 shelf, and upgrade the BTI 7060 shelf to R8.1 or later. The packetVX module is upgraded to R8.1 or later as part of the shelf upgrade.

Once a packetVX module is upgraded to Release 8.1 or later, it can be installed in any slot in the BTI 7200 shelf (except for slot 1 in a master shelf, which is reserved for the SCP).

## Installation procedure

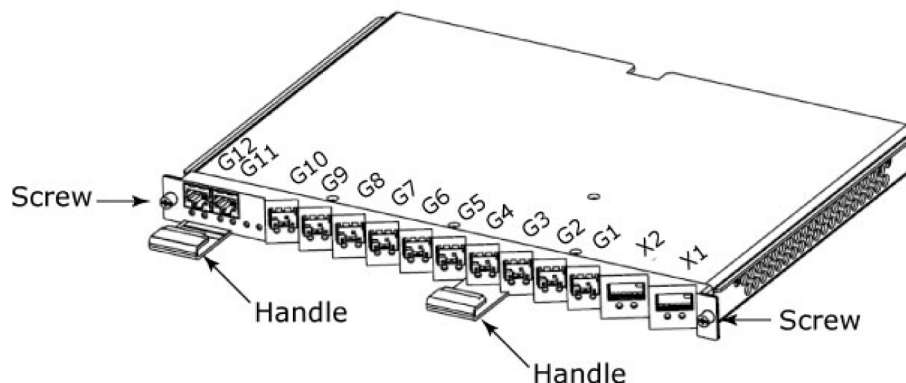


### Caution

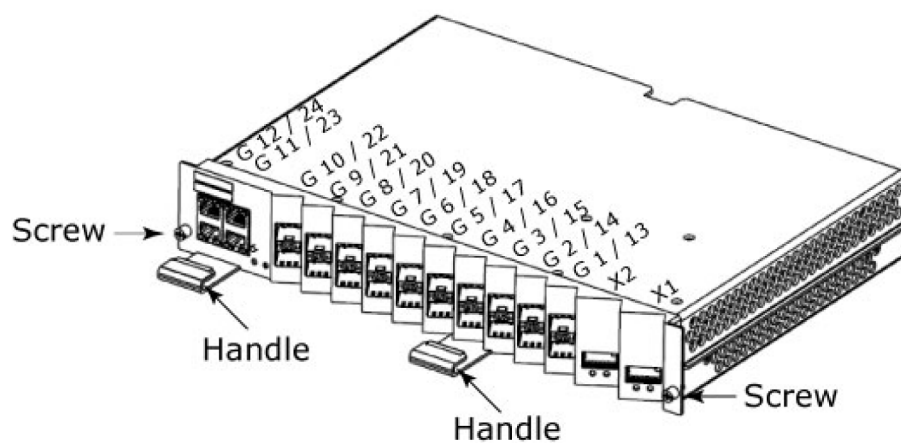
Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

The following figures show the key mechanical features of the packetVX modules.

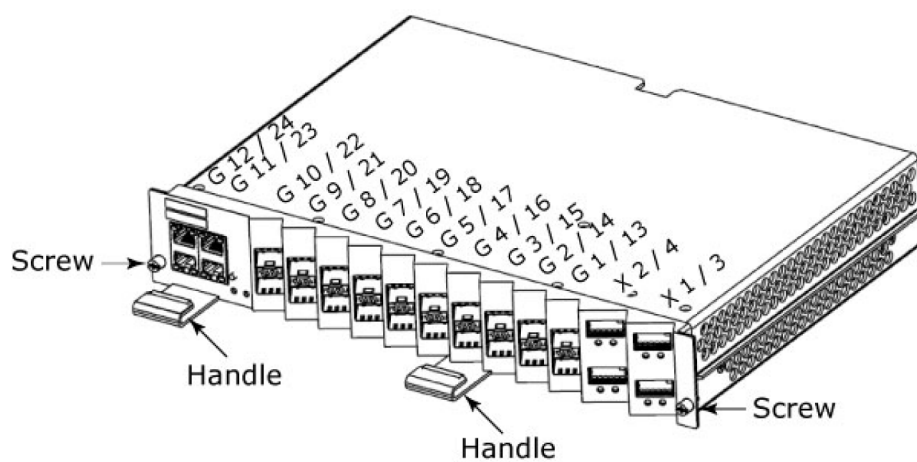
**Figure 2-18 Key features of the packetVX 12/2 module**



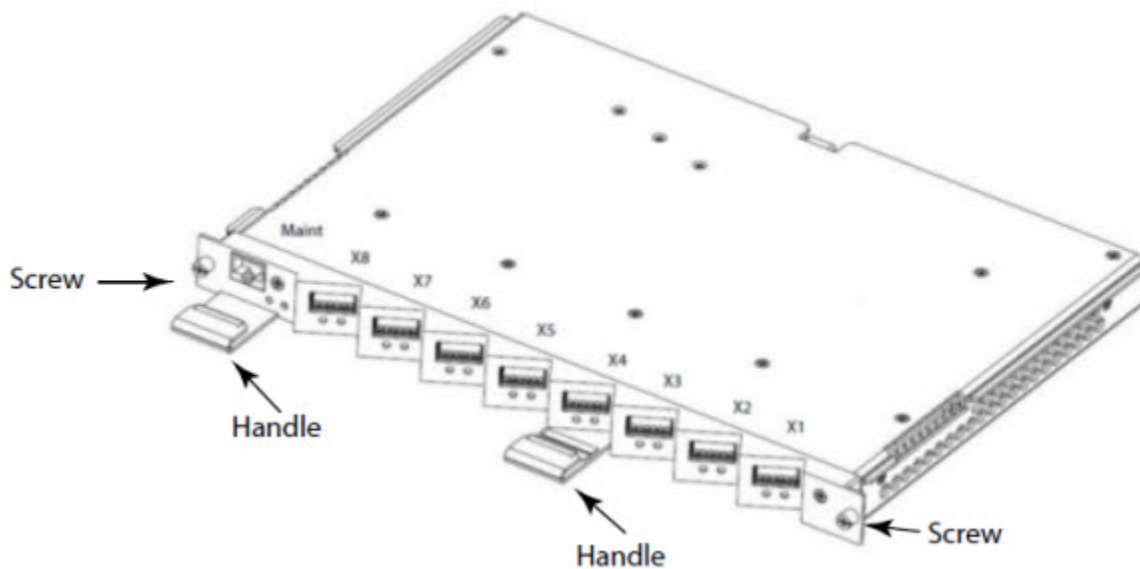
**Figure 2-19 Key features of the packetVX 24/2 module**



**Figure 2-20 Key features of the packetVX 24/4 module**



**Figure 2-21 Key features of the packetVX 80 module**



Use this procedure to install a packetVX module:

**Step 1 Insert the module**

- a) Align the module to the slot in which it is being inserted.
- b) Carefully push the module straight into the slot.
- c) Push with sufficient pressure until the LEDs come on.

**Step 2 Attach the Faceplate Screws**

- a) Facing the front of the shelf, align the module with its mounting holes.
- b) Using a slot-head or Phillips screwdriver, carefully tighten the two faceplate screws.
- c) Partially tighten the first screw.
- d) Partially tighten the other screw.
- e) Fully tighten the first screw.
- f) Fully tighten the other screw.

**Caution** Tighten with no more than 4.7 in-lbs of torque.

**Step 3 Insert the SFP or XFP Transceivers**

See [2.2.5, “Installing optical transceivers”](#) or [2.2.6, “Installing copper transceivers”](#) to insert the SFPs or XFPs into the module, and then return to this procedure.

**Step 4 Replace the Cables**

If any cables were moved to install the module, replace the cables to their original locations.



You have successfully completed this procedure.

## 2.2.5 Installing optical transceivers

Use this procedure to install optical small form factor (SFP) or 10 Gb/s (XFP) transceivers.

### What you need

- Electrostatic discharge (ESD) wrist strap
- SFP or XFP transceiver
- Isopropyl alcohol and lint-free pads

### Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.



#### Caution

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).



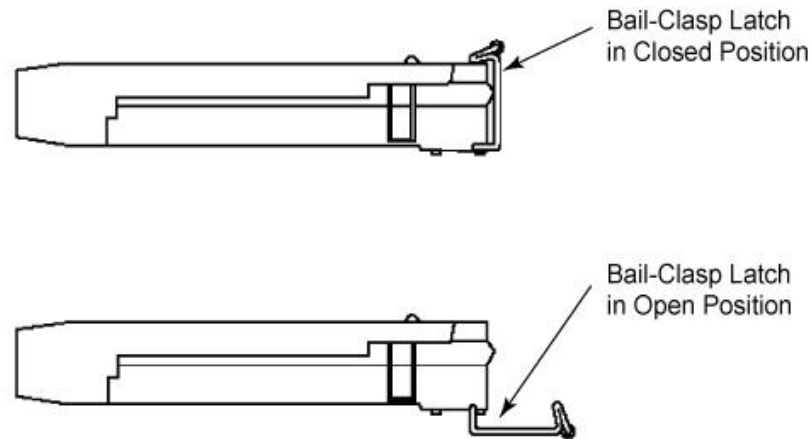
#### Laser

Invisible laser radiation can be emitted from the aperture ports of various modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures to avoid permanent eye damage.

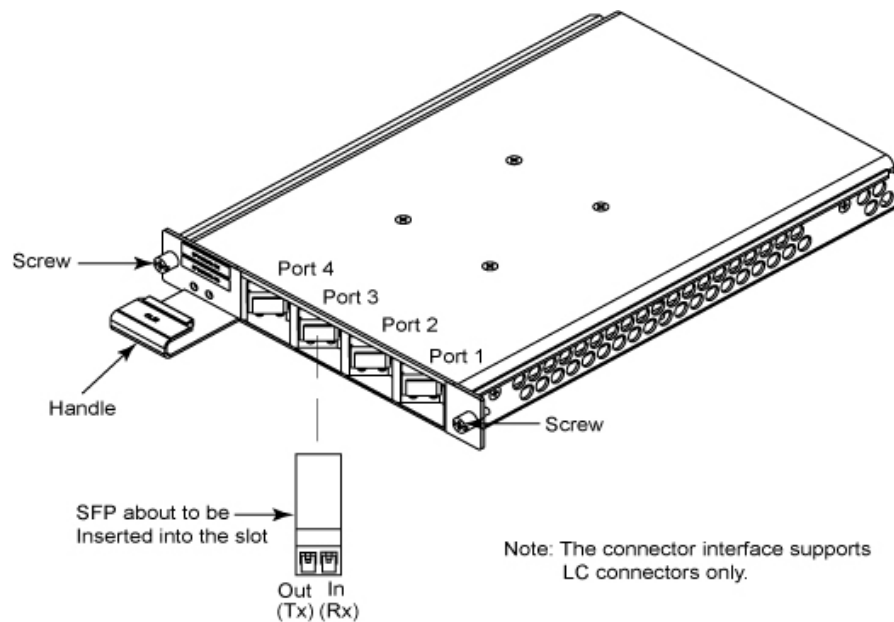
### Transceiver key features

The following figure shows a typical SFP transceiver with a bail-clasp latch.



**Figure 2-22 SFP transceiver with a bail-clasp latch**

The following figure shows a transceiver about to be inserted into its slot.

**Figure 2-23 Transceiver insertion in a generic module**

## Installation procedure

### Step 1 Insert the Transceiver

**Note** Never insert a transceiver that already has a fiber connected to it. Always fully insert the transceiver first, and then connect the fiber to it.

- a) Hold the transceiver so that the optical connectors face you. On an SFP, the product label is visible. On an XFP, the product label is not visible.
- b) Ensure that the latch is in the closed position.

- c) Align the transceiver to the port in which it is being inserted.
- d) Carefully slide the transceiver straight into the port until it clicks.
  - If the red Fail LED turns on, there is a transceiver fault. To clear the fault, refer to the *Alarm and Troubleshooting Guide*.
  - If the yellow LOS LED turns on, there is no valid modulated signal connected to the transceiver. This condition clears once a valid modulated signal is connected.
- e) Remove the plastic protective cover, if fitted.

## Step 2 Clean the Ends of the Fiber Optic Cables

Use lint-free pads with isopropyl alcohol to clean the ends of the fiber optic cables.

## Step 3 Connect the Input and Output Optical Cables

<b>Note</b>	Before connecting the optical cables to the transceiver, ensure that both the optical cable connectors and the transceiver optical surfaces are clean and that there is no residue on the optical surfaces.
-------------	---

<b>Note</b>	The input, or receiver, is on the right side of the transceiver. The output, or transmitter, is on the left side of the transceiver.
-------------	--

- a) Ensure that the latch of the transceiver is in the closed position.
- b) Carefully slide the bottom of the male optical connector along the bottom of the transceiver opening.
- c) Gently push the male optical connector into the transceiver until a distinctive click is heard. Then continue exerting pressure on the connector to ensure a good connection is achieved.

<b>Note</b>	A Loss of Signal (LOS) alarm can occur when no coherent modulated signal is connected to the transceiver. To clear an LOS alarm, see the <i>Alarm and Troubleshooting Guide</i> .
-------------	---

<b>Important</b>	XFPs and DWDM SFPs take about 90 seconds to reach a stable operating temperature. As a result, the REPLUNITFAIL (XFP or SFP Failure) alarm is disabled for 95 seconds after the transceiver is seated. If there is a hardware fault, the REPLUNITFAIL alarm is raised after the 95-second time delay. For more information, see the <i>Alarm and Troubleshooting Guide</i> .
------------------	--

You have successfully completed this procedure.

## 2.2.6 Installing copper transceivers

Use this procedure to install a copper small form factor (SFP) transceiver with an RJ45 connector.

### What you need

- Electrostatic discharge (ESD) wrist strap

- Copper SFP transceiver

### Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.



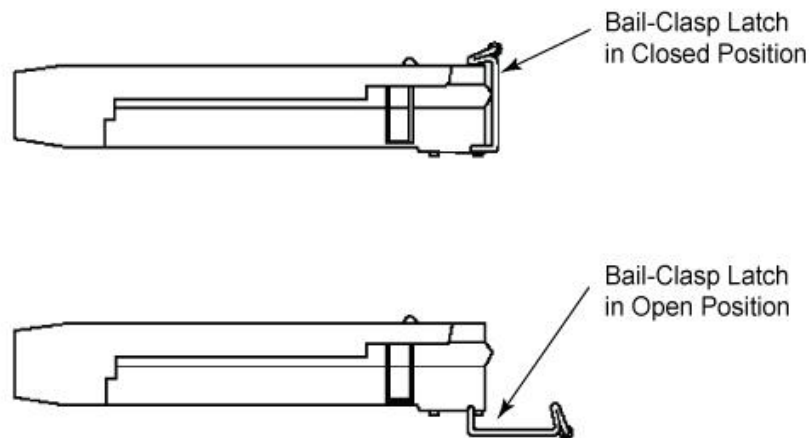
**Caution**

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

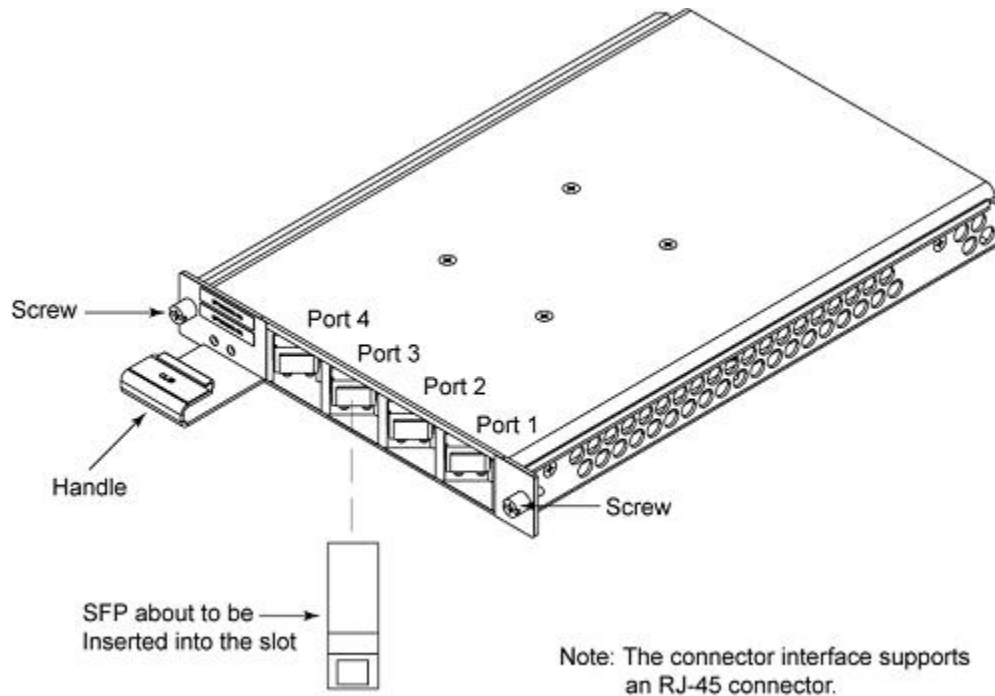
### Transceiver key features

The following figure shows a typical SFP transceiver with a bail-clasp latch.

**Figure 2-24 SFP transceiver with a bail-clasp latch**



The following figure shows a transceiver about to be inserted into its slot.

**Figure 2-25 Transceiver insertion in a generic module**

### Installation procedure

**Note** The maximum cable length (CAT5 UTP) is 100 m.

Follow these steps to install a copper SFP transceiver:

#### Step 1 Insert the Transceiver

**Note** Never insert a transceiver that already has a CAT5 cable connected to it. Always fully insert the transceiver first, and then connect the CAT5 cable to it.

- a) Hold the transceiver so that the electrical RJ45 connector faces you. On an SFP, the product label is visible.
- b) Ensure that the latch is in the closed position.
- c) Align the transceiver to the port in which it is being inserted.
- d) Carefully slide the transceiver straight into the port until it clicks.
  - If the red Fail LED turns on, there is a transceiver fault. To clear the fault, refer to the *Alarm and Troubleshooting Guide*.
- e) Remove the plastic protective cover, if fitted.

#### Step 2 Connect an RJ45 cable to each copper SFP transceiver.

Connect an RJ45 cable to each copper SFP transceiver as follows:

- a)** Ensure that the latch of the SFP transceiver is in the closed position
- b)** Push the RJ45 connector into the SFP transceiver until a distinctive click is heard.

**Note** A Link Down alarm can occur when no signal is connected to the transceiver. To clear a Link Down alarm, refer to the *Alarm and Troubleshooting Guide*.

You have successfully completed this procedure.



## 3.0 Using the command line and other management interfaces

---

This section provides a basic overview of how to manage a BTI 7000 Series™ network element equipped with a packetVX® module, as well as, more detailed information about using the command line interface.

- [3.1, “Overview of management interfaces”](#)
- [3.2, “Using the Command Line Interface”](#)
- [3.3, “Using proNX 900 Node Controller”](#)
- [3.4, “proNX Service Manager”](#)

## 3.1 Overview of management interfaces

---

See the following for more information:

- *BTI 7000 Series Command Line Interface Reference Guide*
- *SNMP Overview Guide*
- *TL1 Reference Guide*
- packetvx-bridge.my (SNMP MIB)

### proNX Management Suite

The proNX Management Suite includes the proNX 900 Node Controller, proNX Service Manager, and proNX 9000 Network Manager, which are used to manage BTI 7000 Series network elements using a graphical user interface (GUI).

<b>Note</b>	proNX 9000 Network Manager was replaced with proNX Service Manager beginning with BTI 7000 Series Release 9.1.
-------------	--

### proNX 900 Node Controller

The proNX 900 Node Controller is a local craft terminal for on-site or remote monitoring and control of individual network elements. The graphical interface provides the following:

- Nodal-level FCAPS with alarm monitoring and diagnostic capabilities
- Automated element inventory/discovery features to simplify provisioning
- Physical and protocol layer performance monitoring
- Point-and-click provisioning

### proNX Service Manager

The proNX Service Manager provides proactive, service-centric management of network resources using tools closely aligned with service providers' own business processes. It is designed to simplify network operations from visualization and activation of services to troubleshooting and supporting end customers.

PSM can be installed in a standalone configuration for new installations, or in a co-resident configuration, when installed with an existing proNX 9000.

PSM is Java-based, and uses a client/server architecture.

For more information refer to PSM documentation.

### proNX 9000 Network Manager

The proNX 9000 Network Manager enables end-to-end monitoring of Ethernet services running over packetVX networks. In addition, the proNX 9000 Network Manager provides such functions as:

- Network-wide topology view



- Network-wide alarms
- Configuration
- Scheduled PMs/Statistics collection
- Network-wide inventory/logs
- Scheduled NE database backups
- Scheduled NE software check and download
- User administration

### 3.1.1 Management access and connectivity over IP networks

BTI 7000 Series network elements can be managed using TCP/IP protocols. In addition, transfers of software files or configuration databases can be performed using FTP. The TCP/UDP ports for these protocols are listed the following table.

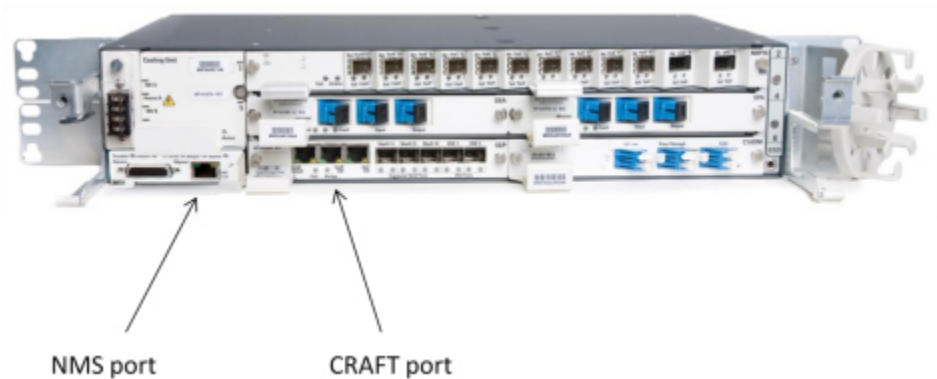
**Table 3-1 Management access ports**

Port number	Service	Configurable	Closeable	Service can be stopped	Usage
161	SNMP	No	No	No	SNMP management, proNX 900
3022	SSH - TL1	No	No	No	SSH mode TL1 protocol over an encrypted link
3082	TL1 ( proNX 900)	No	No	No	proNX 900 TL1 interface (exclusive to proNX 900)
3083	Telnet - TL1 (user)	No	No	No	TL1 ASCII user interface
3084	Telnet - CLI	No	No	No	CLI user interface
8022	SSH - CLI	No	No	No	SSH CLI
20, 21	FTP client	No	NA	NA	System upgrades (outbound only)
162	SNMP traps	Yes	NA	NA	SNMP alarm reporting (outbound only)

#### Direct Access

Direct access to the BTI 7000 Series is provided through the NMS and CRAFT Ethernet ports. The NMS port is on the MSI and the CRAFT port is on the SCP.

Figure 3-1 Location of NMS and CRAFT Ethernet ports



The following table lists the default IP address for BTI 7000 Series network elements.

<b>Note</b> These values may be changed by the network operator.			
Type	IP Address	Mask	Default Gateway
NMS	10.0.0.1	255.0.0.0	0.0.0.0
Craft	192.168.17.1	255.255.255.0	N/A

The following is an example of how to change the IP address on the NMS port using CLI commands:

```
interface mgmteth
ip 172.16.1.254/24
system
gateway 172.16.1.1
```

Remote access

Remote access to a BTI 7000 Series network element equipped with a packetVX module can be provided using any of the following methods:

- Optical Supervisory Channel (OSC), available when OSC ports are equipped and enabled on SCP
- General communications Channel (GCC), available when OTU2 are enabled on 10GbE ports. See the *MCC Solutions Guide* for more information.

**Note**    The packetVX 80 does not support GCC.

- Management VLAN, available when configured on packetVX modules. See [Chapter 10, “Configuring Management VLAN services”](#) for more information.

## 3.1.2 Provisioning, alarms and events, and upgrading

### Provisioning modules

The BTI 7000 Series stores all provisioning information in a non-volatile database on the system control processor (SCP). It supports provisioning and pre-provisioning of all modules. A module need not be present within the shelf to be provisioned. Furthermore, if a module is removed from the shelf and replaced, the new module will not need to be provisioned again.

### Alarms and events

The BTI 7000 Series is designed to report packetVX module faults to users and surveillance systems. Fault reporting is enabled by default. When a fault occurs, the network element sends SNMP traps and TL1 autonomous reports to connected management systems. Active faults can be queried via CLI, SNMP, or TL1. For more information, see the *Alarm and Troubleshooting Guide*.

### Software upgrades

The BTI 7000 Series supports a multistage software upgrade process that consists of separate steps for loading, invoking, and committing software. A single binary image includes all the software for all modules that may be equipped within a shelf; for example, packetVX modules, muxponders, transponders, amplifiers, etc. This simplifies the loading of software onto the system, as only a single file needs to be transferred.

Once the new software load is invoked, the system automatically upgrades and restarts all modules, including the SCP. After all modules have restarted, the user can commit or cancel the upgrade. Committing the upgrade will make it permanent. Canceling the upgrade will cause the system to roll-back to the earlier software version. For more information, see the *BTI 7000 Series Upgrade Guide*.

## 3.2 Using the Command Line Interface

---

The Command Line Interface (CLI) is a text-only mechanism for interacting with packetVX modules. CLI provides an easy-to-use interface for provisioning the system and displaying the system configuration. It is especially useful when a large set of commands has to be entered. It also contains additional provisioning and display commands which may not be available in other management interfaces.

### Accessing the CLI

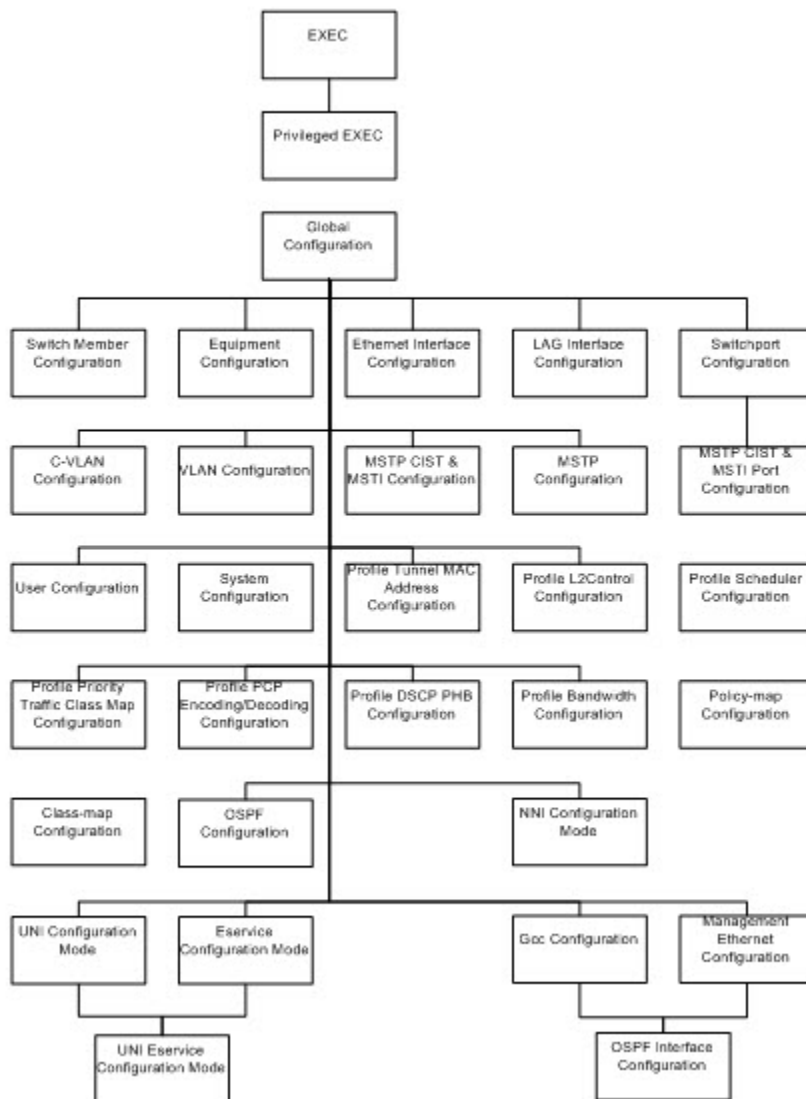
The following command examples demonstrate how a user can start a CLI session using Telnet on port 3084 or SSH on port 8022.

```
tester@ma-tester-lx:~$ Telnet 10.128.3.6 3084
Trying 10.128.3.6...
Connected to 10.128.3.6.
Escape character is '^]'.
NOTICE:This is a private computer system. Unauthorized access or use may lead
to prosecution.
Username: admin
Password: *****
BTI7000>

tester@ma-tester-lx:~$ ssh admin@10.128.3.6 -p 8022
The authenticity of host '[10.128.3.6]:8022 ([10.128.3.6]:8022)' can't be
established.
DSA key fingerprint is 16:70:ea:2a:2f:03:60:3c:ee:11:73:5e:8c:36:f0:7e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.128.3.6]:8022' (DSA) to the list of known
hosts.
This is a private computer system. Unauthorized access or use may lead to
prosecution.
admin@10.128.3.6's password:
BTI7000>
```

### 3.2.1 CLI execution modes and contexts

The CLI is organized into a hierarchical collection of execution modes and contexts. The command set is divided according to the user privilege levels and is accessible from the various execution modes and contexts. Some of the modes are designated as being context-specific, meaning that the user must set a context for which other commands executed in that mode will apply.

**Figure 3-2 CLI command modes**

For example, the Interface Configuration Mode is a context-specific mode containing commands, some of which support provisioning of the individual parameters on a per-interface basis. Rather than entering the interface type name for the targeted facility interface on each command for each parameter, the user simply enters a command to set the interface type name for the targeted interface, thereby establishing a context in which all future parameter-based commands will apply. The context remains in effect until the user exits the context via an explicit command.

In the following example, a UNI interface is created and a UNI interface mode is entered. All commands in this mode will apply to the current UNI.

```
BTI7000:sw1(config)# uni gigabitEthernet 1/1/4
UNI Gige 1/1/4 created.
BTI7000:sw1(config-uni Gige 1/1/4)# ! UNI interface context entered
```

If at this point the user enters an Ethernet Service command, the current UNI is assigned to the Ethernet Service and a UNI Ethernet Service mode is entered.

```
BTI7000:sw1(config-uni GigE 1/1/4)# eservice my_test_2
SW:1, E-Service: my_test_2, UNI GigE 1/1/4 created.
BTI7000:sw1(config-uni-eservice)# ! UNI Eservice context entered
```

To return to the configuration mode, the user must enter the `exit` command twice. The first instance will return the system to the UNI interface mode; the second instance will return to the configuration mode. The `exit` command will return from different modes and submodes in the order in which they were entered.

```
BTI7000:sw1(config-uni-eservice)# exit ! exit the UNI Eservice context
BTI7000:sw1(config-uni GigE 1/1/4)# exit ! exit the UNI interface context
BTI7000:sw1(config)#
```

The CLI has two primary modes and many submodes, each with access to a different command set. Each mode and submode is identified by a different command prompt. The two primary modes are User Exec or just User mode and Privileged Exec or Privileged mode.

### User Exec mode

This is the first mode a user has access to after logging in to the system. This mode allows the user to execute only the basic commands, such as show the system status and provisioning. The system cannot be configured or restarted from this mode. The user mode is identified by the `>` prompt:

```
BTI7000>
```

### Privileged Exec mode

This mode allows users to restart the system and enter a configuration mode. It also allows all the commands available in User mode. The user mode enable command tells the system that the user wants to enter Privileged mode. The disable command will exit Privileged mode. Privileged mode and all its submodes are identified by the `#` at the end of the prompt:

```
BTI7000> enable ! Enter privileged EXEC mode
BTI7000# disable ! Exit from the privileged EXEC mode
BTI7000>
```

### Configuration mode and Privileged mode

This mode allows users to modify the running system configuration. To enter Configuration mode, enter the command `configure terminal` from Privileged mode. Configuration mode is identified by the `(config)#` prompt:

```
BTI7000# configure terminal ! Enter configuration mode
BTI7000(config)#
```

Like Configuration mode, Privileged mode has several submodes. Each submode has its own prompt. To enter these submodes you must first enter configuration mode using the `configure terminal` command.

The `exit` command is available in Configuration mode and all the submodes. It will leave the current mode and return to the previous mode.

The `end` command will return to the privileged exec mode from Configuration mode or any of the submodes.

Each submode has a different command set associated with it.

### Examples

```
BTI7000> enable ! Enter privileged EXEC mode
BTI7000# configure terminal ! Enter configuration mode
BTI7000(config)# virtual-switch 1 ! Set virtual-switch mode
```

The following example shows how creating a UNI interface enters a UNI interface submode. In this context, the user can set parameters for the interface, without specifying the interface:

```
BTI7000:sw1(config)# uni gigabitEthernet 1/1/3
UNI GigE 1/1/3 created.
BTI7000:sw1(config-uni GigE 1/1/3)# ! UNI interface context entered
Question mark ( ? )
Command Line and Management Interfaces Page 3-5
! Set bandwidth profile
BTI7000:sw1(config-uni GigE 1/1/3)# set ingress profile bandwidth bandwidth_
1
BTI7000:sw1(config-uni GigE 1/1/3)#
```

The `show` command will show the current context, which is `uni gigabitEthernet 1/1/3`:

```
BTI7000:sw1(config-uni GigE 1/1/3)# show
Uni GigE 1/1/3:
Virtual Switch is 1
Admin Status is enabled, Operational Status is notPresent
invalid(0) duplex, 1000Mb/s
Max frame size is 1522, Maximum service frame size is 1522
Service type is unspecified
Number of Ethernet services is 0
C-PVID is 0
Port type is Multiple Ethernet Virtual Connection (UNI)
Default Priority is 0
useDEI is disabled
Trust Incoming PCP is enabled
Trust Incoming DSCP is enabled
Profiles:
Control Frame: "DEFAULT_UNI_PROFILE"
Scheduler: "DEFAULT_SCHEDULER_PROFILE"
Priority Traffic Class Map: "DEFAULT_PRIORITY_TC_MAP_PROFILE"
PCP Encoding/Decoding: "DEFAULT_8P0D_PROFILE"
Ingress Bandwidth: "bandwidth_1"
BTI7000:sw1(config-uni GigE 1/1/3)#
```

## 3.2.2 CLI command help

Use the `?` command to access CLI command help, which lists all commands available for the current command mode. This command is available to all users.



```
BTI7000> ?
disable - Disable privileged EXEC mode
enable - Enable privileged EXEC mode
end - Exit from the EXEC
help - Ask for help
logout - Exit from the Exec
password - Change password
ping - Ping a remote node
set - Change System Variables
show - Show running system information
t11 - Switch to TL1
virtual-switch - Specify a virtual switch
BTI7000>
```

<b>Note</b>	The command ? is context sensitive and entering it at any mode shows the available commands at that mode. It can also be used in the middle of a command to show possible completion options.
-------------	---

### 3.2.3 Command Line completion

Command line completion makes the CLI much more user friendly. It saves extra typing and helps when one cannot remember a command's syntax.

If you type only the beginning of a command and press Tab, the CLI will complete the keyword for you. If CLI does not complete the keyword, type a few more letters and the CLI will fill in the best completion.

If the system does not understand a command, it repeats the entire command line and places a caret (^) under the point at which it run into trouble.

If you know the command's syntax, there is no need to complete the command. If enough letters are entered and the input is not ambiguous, the CLI will execute the command.

### 3.2.4 Command line editing keys

The CLI provides a number of keyboard shortcuts that let you edit the line you are typing. The following table lists the available command-line editing keys.

Key	Command
Tab	Tries to finish the current command (command completion)
↑	Moves back through the history of commands
↓	Moves forward through the history of commands
←	Moves the cursor to the left
→	Moves the cursor to the right
Ctrl+A	Returns the cursor to the beginning of the current line
Ctrl+B	Moves the cursor back one character (equivalent to the left-arrow key)
Ctrl+D	Deletes the character the cursor point to
Ctrl+E	Moves the cursor to the end of the line
Ctrl+F	Moves the cursor forward one character (equivalent to the right-arrow key)
Ctrl+K	Deletes all characters from the current cursor position to the end of the line
Ctrl+N	Goes to the next command in the session history (equivalent to the ↓ key)
Ctrl+P	Goes to the previous command in the session history (equivalent to the ↑ key)
Ctrl+T	Switches character left of the cursor with the character left of it
Ctrl+R	Redisplays the current line
Ctrl+U	Clears the line
Ctrl+W	Deletes the word to the left of the cursor
Ctrl+X	Deletes from the cursor position to the beginning of the line
Ctrl+Z	Exits the current configuration mode and returns to the previous configuration mode

### 3.2.5 Controlling output

The CLI supports a MORE facility to control the output when a large amount of data is displayed. If you run a command that has more than one page of output, the CLI will pause after each page with a `-MORE-` prompt. The output is then suspended until the user types in one of the following:

`<space>` which displays the next screen worth of data, or remaining output

`Q` or `q` which stops the display and terminates the command

Using the `set pagination` command, you can turn off or on an automatic pause of lengthy output. The pausing can be disabled using the `set pagination off` command. To turn pagination back on, enter the command `set pagination on`.

The number of lines displayed is determined by the screen size values that are sent in by the Telnet or SSH client. The number of lines that will be displayed for each screen of a `more` display will be the screen size less 1 line for the `-MORE-` prompt.

## Comments in command lines

CLI commands can contain comments in the command line. The CLI will ignore anything after a `!` character until the end of the line.

## 3.2.6 User sessions

The CLI allows up to 50 user sessions to be opened simultaneously. There is no restriction on the number of sessions a user can have.

By default, user sessions will timeout after 15 minutes of inactivity. The timeout can be reset with the `timeout` command by a super user in configuration mode.

```
BTI7000(config)# user admin
BTI7000(config-user)#
BTI7000(config-user)# timeout ?
<timeout> - Timeout value 5-60
BTI7000(config-user)# timeout 30
BTI7000(config-user)#
```

The `no timeout` command sets the timeout to null.

The command `show users active` displays all users currently logged into the system and their IP addresses:

```
BTI7000# show users active
Id  UserName  Remote IP    Elapsed Time  Expire In
---  -
0   admin    172.26.1.63  00:18:19     never
1   admin    172.26.1.63  00:00:06     never
```

```
BTI7000#
[11:41:12 Sun Jan 17 2010] User "admin" successfully logged in
```

```
BTI7000# show users active
Id  UserName  Remote IP    Elapsed Time  Expire In
---  -
0   admin    172.26.1.63  00:19:00     never
1   admin    172.26.1.63  00:00:47     never
2   admin    172.26.1.84  00:00:08     never
```

```
BTI7000#
```

## 3.3 Using proNX 900 Node Controller

---

The proNX 900 Node Controller provides a graphical user interface to provision, operate, monitor, and troubleshoot packetVX modules. This interface provides a representational view of the physical configuration of each shelf in the system, the network, and the modules in each shelf. For detailed information about using the proNX 900 Node Controller, see the *proNX 900 Node Controller Online Help*.

The proNX 900 is accessible from a Windows-based PC with a network connection to a BTI 7000 Series interface, a Solaris workstation, or a MAC OS X operating system.

<b>Note</b>	The proNX 900 is supported only over LAN connections to the BTI 7000 Series equipment.
-------------	--

## 3.4 proNX Service Manager

---

proNX Service Manager provides proactive, service-centric management of network resources (including BTI Systems full line of network elements as well as select third-party equipment) using tools closely aligned with service providers' own business processes. It is designed to simplify network operations from visualization and activation of services to troubleshooting and supporting end customers.

PSM is Java-based, and uses a client/server architecture.

### Client

The PSM client is a Java-based Graphical User Interface (GUI) that communicates with the PSM server using an HTTP-based protocol. The GUI runs on the desktop / laptop of the technician or NOC staff.

### Server

The PSM server component communicates with the network elements using SNMP. The PSM server runs over the WideCast OS on x86-64 servers from vendors such as Oracle, HP, Dell, or IBM.

The number of clients and nodes supported is determined by the hardware, and a calculator is available to determine the correct hardware for specific deployments.

The proNX Service Manager server has the following components:

- One or more Java-based processes (depending on the performance requirements of the platform)
- MySQL Database
- WideCast OS

### WideCast OS

WideCast OS is a Just Enough OS (JEOS), based on Redhat Fedora that is fully tested with proNX components software. This offering partitions the file system appropriately, removes unnecessary services from Fedora, installs the latest security patches and automates the installation process. Process management on WideCast OS is performed by Monit, an open source utility for managing and monitoring processes, files, directories, and file systems.

<b>Note</b>	The net-snmp Linux implementation shipped with WideCast OS allows the proNX Service Manager to manage the host workstation via SNMP. In essence, the PSM can manage itself and generate alarms about its own resources if there are error conditions.
-------------	---

### Support for RADIUS server

WideCast OS provides a local instance of a RADIUS (Remote Authentication Dial-In User Service) server implementation. When PSM is installed, the PSM server is configured by default to use RADIUS to provide authentication and authorization mechanisms for access to PSM features.

For more information about using PSM refer to the *proNX Service Manager User Guide*.

## 4.0 Basic equipment and switch member configuration

---

This section provides the provisioning procedures required to set up a BTI<sup>™</sup> packetVX<sup>®</sup>™ switch.

The MEF-based provisioning model incorporates Ethernet services, UNIs, NNIs and E-NNIs. The traditional IEEE 802.1ad Provider Bridge provisioning model uses interfaces and switchports, and requires manual provisioning of VLANs. The switch still supports the traditional IEEE provisioning model; however, the MEF-based model greatly simplifies switch provisioning.

<b>Note</b>	BTI strongly recommends using the MEF Ethernet services provisioning model for all provisioning in provider bridge mode.
-------------	--

## 4.1 Create a packetVX equipment entry

---

This procedure explains how to create a packetVX equipment entry.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- None

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Create provisioning information for a packetVX module

To create provisioning information for a packetVX module, enter the following command:

```
equipment <location> [pec <type>]
```

For example, the command string might be

```
equipment 1/1 PEC BT7A81AA
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-eqpt PVX-1/1)#
```

You have successfully completed this procedure.



## 4.2 Virtual switches

The BTI 7000 Series allows you to create multiple virtual switches within one network element. Virtual switches are software implemented logical concepts that allow up to two packetVX modules to be configured as a single switch. Each virtual switch is configured independently.

To provision a packetVX module, there has to be at least one virtual switch defined. Once a virtual switch is created, members representing hardware equipment can be added to it. Each virtual switch may have up to two packetVX modules assigned to it as member(s).

If you enter the `virtual-switch <switch-id>` command while in User or Privileged modes, you will enter the corresponding virtual switch mode. If a virtual switch does not exist, an error is displayed.

To create a virtual switch, you have to be in configuration mode. If the `virtual-switch <switch-id>` command is entered while in Configuration mode and the virtual switch does not exist, it is created.

```
BTI7000> virtual-switch 3 ! virtual switch 3 does not exist
% Virtual Switch 3 not created
BTI7000>enable
BTI7000# virtual-switch 3 ! virtual switch 3 does not exist
% Virtual Switch 3 not created
BTI7000#conf t ! enter configuration mode
BTI7000(config)# vi 3 ! create virtual switch 3
BTI7000:sw3(config)# ! the prompt reflects that the system
! is in a virtual switch submenu
```

At this point, you can add member modules and provision the newly created virtual switch.

You can remove a virtual switch while in Configuration mode with the `no virtual-switch` command:

```
BTI7000(config)# no virtual-switch 3
BTI7000(config)#
```

<b>Note</b>	Members and associated Eservices must be removed from a virtual switch before you can remove the switch.
-------------	--

### 4.2.1 Create a virtual switch

This procedure explains how to create a virtual switch to which a packetVX module can be associated.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- None

The CLI can be accessed using Telnet or SSH. Telnet is available using port 3084. SSH is available using port 8022.

To use SSH via Linux:

```
tester@site-575 ~ $ ssh admin@10.1.200.112 -p 8022 The authenticity of host
'[10.1.200.112]:8022 ([10.1.200.112]:8022)' can't be established.
DSA key fingerprint is 71:da:4e:81:7c:65:15:3c:d2:72:ac:7a:80:64:57:4a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.1.200.112]:8022' (DSA) to the list of known
hosts.
This is a private computer system. Unauthorized access or use may lead to
prosecution.
```

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000 (config)#
```

### Step 3 Create a virtual switch

To create a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

You have successfully completed this procedure.

## 4.2.2 Add a member to a virtual switch

This procedure explains how to add apacketVX as a member of a virtual switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- A virtual switch must be provisioned.

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Add the packetVX as a member of the virtual switch**

To add the packetVX as a member of the virtual switch, enter the following command:

```
member <location>
```

where <location> is the location of the packetVX

For example, the command string might be

```
member 1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-member 1/1)#
```

**Step 5 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

You have successfully completed this procedure.

## 4.3 Stacking

---

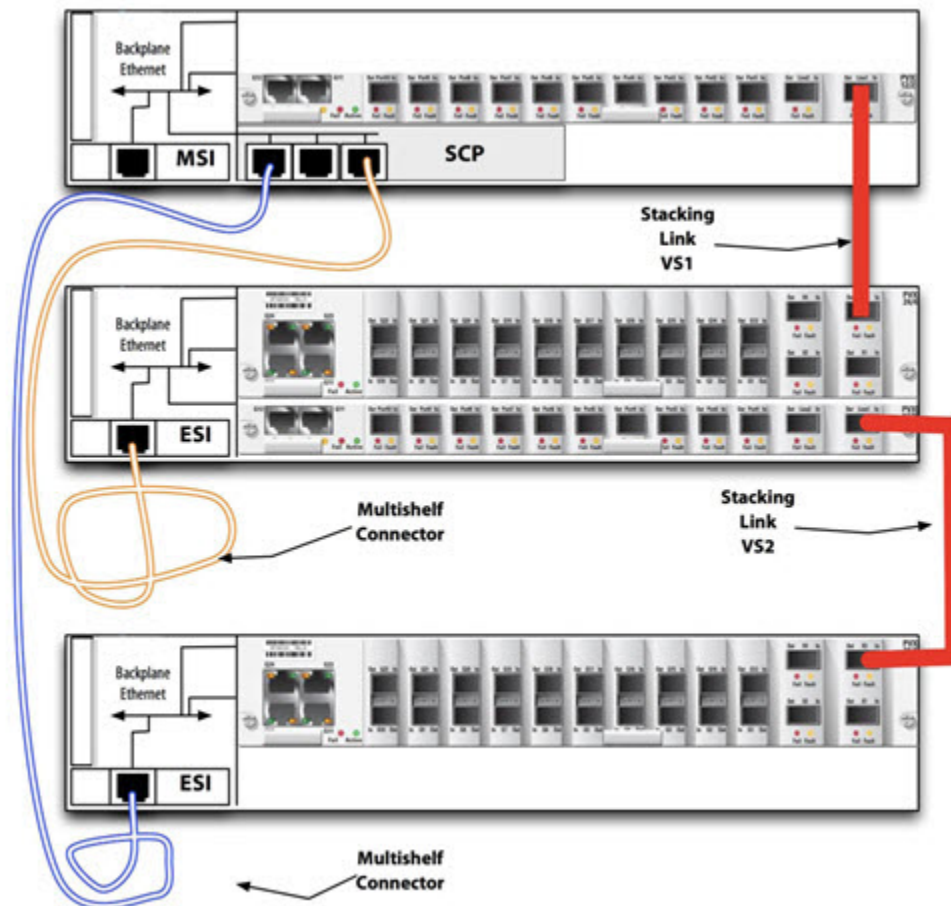
The packetVX provides equipment redundancy by stacking two packetVX modules, through one or more 10 gigabit Ethernet interfaces to expand bandwidth to the stacking ports and provide a non-blocking bridge between two stacked modules. Multiple interfaces on the stacking port balances the traffic across the interfaces, which allows more data bandwidth between switches and minimizes the risk for blocking.

A stack is created by adding two members to a virtual switch. The packetVX modules must be in the same extended chassis group; however, they do not have to be in the same physical chassis. The stacking rules are different between the packetVX 12/2, 24/2 and 24/4 modules, and the packetVX 80 module. Following are the stacking guidelines:

### **Stacking guidelines: packetVX 12/2, 24/2 and 24/4 modules**

- Any combination of these modules and ports may be part of a stack.
- Stacking on these modules is accomplished from the faceplate ports.
- These modules must be controlled by the same System Control Processor.

The following figure shows two sets of stacked packetVX modules spread across three chassis in an extended chassis group.

**Figure 4-1 packetVX 12/2 and 24/4 module stacks in an extended chassis****Stacking guidelines: packetVX 80 module**

- A packetVX 80 module supports stacking on only the BTI 7200.
- This module can be stacked with only another packetVX 80 .
- The difference with stacking on the packetVX 80 is that the stacking is accomplished through the connections on the backplane, rather than through external XFP ports, configured manually. For example, if two packetVX 80 modules are configured as members of a virtual switch, these five interfaces are automatically stacked.
- Up to four pairs of packetVX 80 modules may be stacked per 7200 chassis, based on the following lower and higher slot pairing requirements:

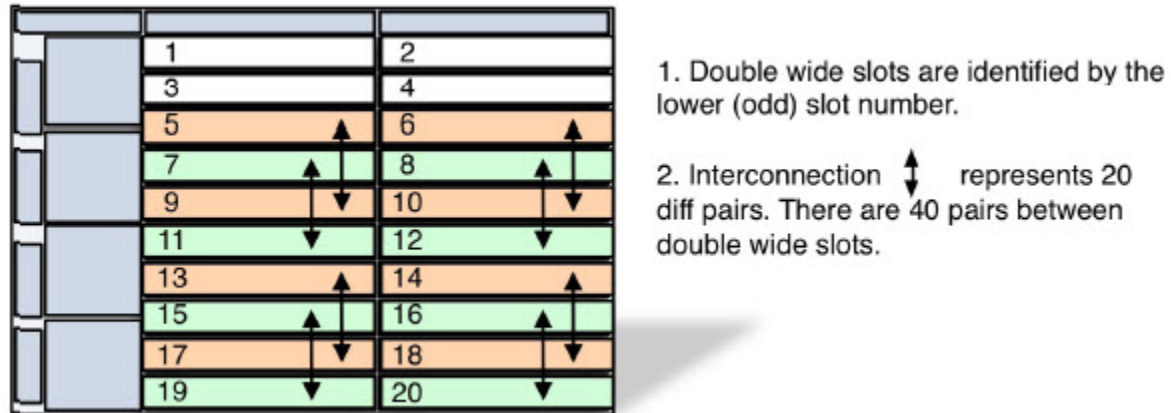
**Table 4-1 packetVX 80 slot pairs**

Lower slots	Higher slots
5-6	9-10
7-8	11-12

**Table 4-1 packetVX 80 slot pairs (Continued)**

Lower slots	Higher slots
13-14	17-18
15-16	19-20

The following figure shows how the slots are organized on the BTI 7200:

**Figure 4-2 BTI 7200 backplane slots**

## Redundancy

The equipment redundancy created by stacking switches includes the following:

- **Control and Management plane redundancy:** Each switch chooses the role of primary or secondary. All control protocols (e.g., MSTP, G.8032, etc.) operate on the primary. The secondary stays synchronized with the primary so that it can take over if the primary fails.
- **Data Plane redundancy:** By configuring Link Aggregation groups to include members on both modules (often referred to as Cross-Card LAG), a UNI or NNI can remain operational when a switch fails or is restarted.

**Note** After adding stacking links, it can take up to two seconds to stabilize the switchover. During this time you should not perform provisioning tasks on the stack; otherwise, you run the risk that the provisioning may fail. If provisioning fails, you can retry provisioning.

### 4.3.1 Stacking operation

One of the switches in the stack is designated the **primary** and the other the **secondary**. Initially, the primary is the first member added to the virtual switch, but the modules change roles when necessary.

All control and management protocols operate on the primary switch. The primary and secondary switches continually communicate across the backplane Ethernet and across the stacking link to keep their databases synchronized so that the secondary switch can take over operation quickly if the primary switch fails (warm standby). If the secondary module fails or is

removed, the primary switch will continue to operate normally although the interfaces on the secondary switch will not be accessible. Link aggregation groups that are defined across the switches will continue to operate with a reduced number of links.

If, however, the primary switch fails, the secondary switch will detect this and assume the role of the primary switch. The interfaces on the (previously) primary switch will not be accessible. Support for all control and management functions will be taken up by the new primary switch. This role is not revertive—when the failed switch recovers it will become the secondary switch.

**Important    Replacing or redeploying a stacked packetVX module**

You cannot remove a packetVX module from a stacking configuration and re-deploy it somewhere else in the network unless the remaining packetVX module is rebooted. Otherwise, two NEs may end up with the same MAC address which can affect network operation.

The reseating of a packetVX module in a stacking configuration does not require reboot of the other packetVX module.

## 4.3.2 Software upgrades and stacking

When a software upgrade is invoked on the system, the new software version is downloaded to each stacked packetVX module. The secondary switch immediately reinitializes with the new software version and resynchronizes its database with the primary switch. After five minutes (ensuring enough time for the secondary switch to reinitialize and then resynchronize with the primary switch), the primary switch reinitializes with the new software version. The secondary switch becomes the primary switch when it detects that the primary switch is reinitializing, and, when the former primary switch reinitializes it becomes the secondary switch.

### Hitless upgrades

**Note** Near hitless software upgrades are supported in BTI software Releases 10.3.0 and later. Upgrades prior to Release 10.3.0 require simultaneous reboot on both packetVX modules. Before you upgrade, refer to the procedures described in the technical note BTI-TIB006-2012 ISSUE 001: "PVX ERPS Configuration Issue after Software Upgrade to 9.2 or later" included in the *BTI 7000 Series Upgrade Guide for Release 10.3.0*.

## 4.3.3 Sample stacking configuration

The stacking configuration examples in this section represent the procedures required for stacking the packetVX 12/2, 24/2 and 24/4 modules. Stacking for the packetVX 80 module is accomplished automatically, as described in the topic [4.3, “Stacking”](#).

First, create equipment entries in the main shelf and the expansion shelf, and then add them to a single virtual switch. For example:

```
BTI7000(config)# equipment 1/1 PEC BT7A81AA
BTI7000(config-eqpt PVX-1/1)# exit
BTI7000(config)# equipment 11/1 PEC BT7A81CA
BTI7000(config-eqpt PVX-11/1)# exit
BTI7000(config)# virtual-switch 1 ! select or create VS 1
```



```
BTI7000:sw1(config)# member 1/1 ! add member shelf 1 / slot 1
BTI7000:sw1(config-member 1/1)# exit ! leave member config mode
BTI7000:sw1(config)# member 11/1 ! add member shelf 11 / slot 1
BTI7000:sw1(config-member 11/1)# exit ! leave member config mode
BTI7000:sw1(config)#
```

Next, define the stacking ports on each switch. For example:

```
BTI7000:sw1(config)# interface stackingport teng 1/1/2
BTI7000:sw1(config-if TenGigE 1/1/1)# exit
BTI7000:sw1(config)# interface stackingport teng 11/1/2
BTI7000:sw1(config-if TenGigE 11/1/1)# exit
```

This defines 10G interface number 2 on each switch as the stacking port. The status of the virtual switch can be displayed:

```
BTI7000:sw4(config)# show virtual-switch 1 brief
Member Stacking
VS BridgeMode Tunnel MAC Address Profile Location State
--
1 provider DEFAULT_TMA_PROFILE 1/1 primary
11/1 secondary
```

### 4.3.4 Configuring packetVX stacking

This procedure explains how to add packetVX equipment to a virtual switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- A virtual switch must be provisioned.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Create provisioning information for the first packetVX module

To create provisioning information for a packetVX module, enter the following command:

```
equipment <location> [pec <type>]
```

For example, the command string might be

```
equipment 1/1 PEC BT7A81AA
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-eqpt PVX-1/1)#
```

#### **Step 4 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### **Step 5 Create provisioning information for the other packetVX module**

To create provisioning information for a packetVX module, enter the following command:

```
equipment <location> [pec <type>]
```

For example, the command string might be

```
equipment 11/1 PEC BT7A81AA
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-eqpt PVX-11/1)#
```

#### **Step 6 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### **Step 7 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### **Step 8 Add the first packetVX as a member of the virtual switch**

To add the packetVX as a member of the virtual switch, enter the following command:

```
member <location>
```

where <location> is the location of the packetVX

For example, the command string might be

```
member 1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-member 1/1)#
```

#### **Step 9 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### **Step 10 Add the other packetVX as a member of the virtual switch**

To add the packetVX as a member of the virtual switch, enter the following command:

```
member <location>
```

where <location> is the location of the packetVX

For example, the command string might be

```
member 11/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-member 11/1)#
```

#### **Step 11 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### **Step 12 Define the stacking port on the first packetVX**

Define the stacking port on the first packetVX, enter the following command:

```
interface stackingport <interface-type> <interface-id>
```

where <interface-type> is the interface type, and <interface-id> is the shelf/slot/port of the interface.

For example, the command string might be

```
interface stackingport tenGigabitEthernet 1/1/2
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-if TenGigE 1/1/2)#
```

#### **Step 13 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### **Step 14 Define the stacking port on the other packetVX**

Define the stacking port on the other packetVX, enter the following command:

```
interface stackingport <interface-type> <interface-id>
```

where <interface-type> is the interface type, and <interface-id> is the shelf/slot/port of the interface.

For example, the command string might be

```
interface stackingport tengigabitEthernet 11/1/2
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-if TenGigE 11/1/2)#
```

#### **Step 15 Follow this procedure if you configure more than one stacking link**

Verify that each pair of stacking links is in service before configuring the next stacking link pair:

```
show interfaces <interface-type> <interface-id> brief
```

You have successfully completed this procedure.

## 4.4 Optical Transport Network

### 4.4.1 OTU2

The OTU2 protocol operating over the Optical Transport Network (OTN) has a line rate of approximately 10.7 Gb/s and is designed to transport OC192, STM64, or 10Gb/s WAN. OTU2 can be over-clocked (non standard) to carry signals faster than OC192/STM64 (9.953 Gb/s), such as 10 GbE LAN PHY coming from IP/Ethernet switches and routers at full line rate (10.3 Gb/s).

### 4.4.2 Forward Error Correction and Enhanced Forward Error Correction

The switch offers encapsulation within a G.709 OTN digital wrapper, providing reach extension capabilities with Forward Error Correction (FEC) as well as Enhanced Forward Error Correction (EFEC).

An established technology frequently used in long-haul networks, FEC enables proactive detection and correction of errors in an optical link. FEC is implemented by adding redundant information using a predetermined algorithm. That is, the receiver can accept a lower-quality signal and correct many errors by using the additional information provided in each frame by the Forward Error Correction.

G.709 FEC uses the standardized Reed Solomon code RS(255/239). This provides approximately 6 dB of coding gain. The FEC is approximately 6¼% of the frame.

The packetVX also supports an Enhanced FEC (EFEC) capability corresponding to ITU-T G.975.1 appendix I.4. EFEC provides 1- to 2-dB of additional gain (over standard FEC) with the same amount of frame overhead. A 10G port that is configured for OTU2 line mapping can also be configured for EFEC as an alternative to the standard G.709 FEC.

### 4.4.3 Sample OTU2 configuration

In this sample configuration, OTU2 is provisioned as a line protocol without enabling GCC.

First, access the Privileged EXEC mode and then enter Administration Configuration mode. For example:

```
BTI7000> enable
BTI7000# configure terminal
BTI7000(config)#
```

Next, select an existing virtual switch. For example:

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)#
```

Now, create a 10G NNI<sup>9</sup> and change the interface line mapping to OTU2 (from the default 10G LAN PHY). For example:

```
BTI7000:sw1(config)# nni ten 1/1/1
BTI7000:sw1(config)# exit
```

<sup>9</sup> Creating an NNI creates both an interface and a switchport. See 6.1, “UNIs, NNIs and E-NNIs” for more information.

```
BTI7000:sw1(config)# interface ten 1/1/1
BTI7000:sw1(config)# shutdown
BTI7000:sw1(config-if TenGigE 1/1/1)# line-mapping otu2-gfp1
BTI7000:sw1(config-if TenGigE 1/1/1)# no shutdown
BTI7000:sw1(config-if TenGigE 1/1/1)# exit
BTI7000:sw1(config)#
```

#### 4.4.4 Provisioning OTU2

Use this procedure to provision OTU2 as a line protocol without enabling GCC.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

##### Prerequisites

- Use the Craft interface on the SCP to perform initial equipment deployment.
- Make sure the equipment, virtual switch, and members are already provisioned.

##### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

##### Step 2 Access the Global Configuration mode

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

##### Step 3 Create a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows

```
BTI7000:sw1(config)#
```

##### Step 4 Create the 10 GbE NNI interface

To create the 10 GbE NNI interface, enter the following command:

```
BTI7000:sw1(config)# nni ten 1/1/1
BTI7000:sw1(config)# exit
```

**Step 5 Change the line mapping of the 10 GbE interface from default "10GE LAN PHY" to "OTU2 GFP"**

To change the line mapping of the 10 GbE interface, enter the following command:

```
BTI7000:sw1(config)# interface ten 1/1/1
BTI7000:sw1(config)# shutdown
BTI7000:sw1(config-if TenGigE 1/1/1)# line-mapping otu2-gfp1
```

**Step 6 Optionally, change from the default Forward Error Correction (FEC) to Enhanced Forward Error Correction (EFEC)**

To change FEC to EFEC, enter the following command:

```
BTI7000:sw1(config-if TenGigE 1/1/1)# error-correction efec
BTI7000:sw1(config-if TenGigE 1/1/1)# no shutdown
```

**Step 7 Exit the configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-uni gig 1/1/1)# exit
```

**Step 8 Repeat steps 1 to 7 for each node or port participating in the network**

You have successfully completed this procedure.

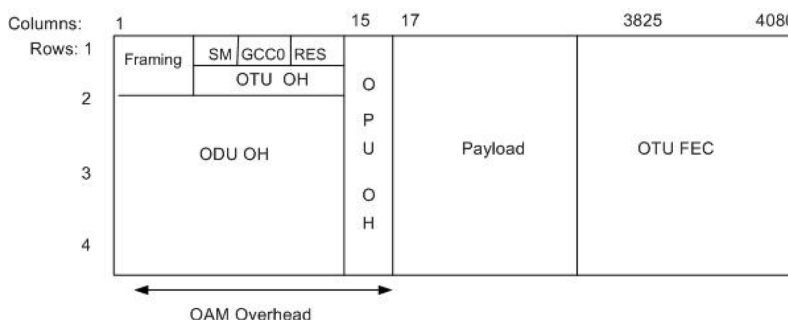
## 4.5 GCC

The switch uses the general communications channel (defined in ITU-T standard G.709-2003) to form an IP-based network for management communications. Service Providers can use the GCC for out-of-band management of their networks without impacting customer bandwidth or using another wavelength on their fibers. By using the GCC0 bytes defined in the OTU2 overhead, the switch forms a 1.3 Mb/s channel for management traffic.

**Note** GCC is not supported on the packetVX 80 module.

The following figure shows the parts of the G.709 OTN frame.

**Figure 4-3 GCC in the OTN OTU2 frame structure**



### 4.5.1 Configuring GCC on OTU2 interfaces

Use this procedure to configure an out-of-band management communications channel for the switch. BTI recommends using OSPF for the GCC interfaces. Before you can use OSPF for the GCC interfaces, it must be enabled. Alternatively, you can use static routing. For information about using static routing, see the route static command in the *BTI 7000 Series packetVX Command Line Reference Guide*.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- Use the CRAFT interface on the SCP to perform initial equipment deployment.
- Make sure the equipment, virtual switch, and members are already provisioned.
- The packetVX 80 does not support GCC.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```



**Step 2 Access the Global Configuration mode**

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Create a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Provision OSPF**

To provision OSPF, enter the following command:

```
BTI7000:sw1(config)# ospf area-id default
```

**Step 5 Set OSPF redistribution**

To set OSPF redistribution, enter the following command:

```
BTI7000:sw1(config-ospf)# redistribution stat
```

**Step 6 Create the GCC interfaces**

To create the GCC interfaces, enter the following command:

```
BTI7000:sw1(config)# interface gcc tenGigabitEthernet 1/1/1
```

**Step 7 Exit configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-ospf)# exit
```

**Step 8 Set the interface to OSPF**

To set the interface to OSPF, enter the following command:

```
BTI7000:sw1(config-gcc TenGigE 1/1~)# ospf
```

```
BTI7000:sw1(config-ospf-if)#
```

**Step 9 View the OSPF settings**

To view the OSPF settings configured, enter one of the following commands:

- BTI7000:sw1(config)# show ospf

```
Admin State: IS-NR, AINS
Area Id: 0.0.20.208
Router ID: 10.1.200.122
Redistribute: stat
Area Type: default
```

- BTI7000:sw1(config)# show interface tengigabit 1/1/1

```
TenGigE 1/1/1
State is IS-NR,
fiber type is none, wavelength is 1310
Line Mapping is otu2-gfp1
Error Correction is efec
Circuit ID is 1
MTU 1522 bytes
MAC Address is 00-14-d0-00-1b-de
Flow control configured as auto, Flow control status is off
Full-duplex, 10000Mb/s
loopback is off
phyPmMon is disabled
AINS Timer is 00:00
Signal Degrade BERT is none
OPR threshold (Min: -14.9, Max: 0.9)
OPT threshold (Min: -6.5, Max: -0.5)
SES Level is 0
Media Rate is auto negotiated
```

- BTI7000:sw1(config)# show interface gcc tengigabit 1/1/1

```
if-name State Rate IP OSPF
```

```
-----
----
```

```
gcc 1/1/1 IS-NR full unnumbered
yes
```

- BTI7000:sw1(config)# sh route

```
Admin
IP Address/Prefix Dist Cost Next Hop Protocol
Type Age PR
Product Release 7.2.1 STANDARD 6-67
Provisioning
```

```
-----
-----
```

```
0.0.0.0/0 0 0 10.1.1.1 other
indirect 00:00:00 Y
10.0.0.0/8 110 10 IP-NMS ospf
direct 00:09:52 N
10.0.0.0/8 0 0 IP-NMS connected
direct 00:00:00 Y
10.1.200.121/32 0 0 IP-1/1/1 connected
direct 00:00:00 Y
127.0.0.0/8 0 0 IP-LOOPBACK connected
direct 00:00:00 Y
```

```
192.168.17.0/24 110 20 IP-1/1/1 ospf
indirect 00:00:06 N
192.168.17.0/24 0 0 IP-CRAFT connected
direct 00:00:00 Y
200.200.200.0/24 0 0 10.1.200.122 static
indirect 00:00:00 Y
224.0.0.0/24 0 0 127.0.0.1 other
indirect 00:00:00 Y
```

**Step 10 Repeat steps 1 to 9 for each node or port participating in the network**

You have successfully completed this procedure.



## 5.0 Configuring Ethernet Bridging and STP

---

The capabilities of the BTI™ packetVX® module are organized around Ethernet Services (Eservices).

Eservices are built on top of an 802.1ad<sup>10</sup> Provider Bridge. In most cases, using the Eservices configuration model will reduce or eliminate the need to deal with provider bridging and the various protocols associated with it, such as spanning tree and GVRP. Nonetheless, having a basic understanding of provider bridging and the important control protocols is useful in designing, configuring, and troubleshooting the network.

This section covers the following topics:

- 5.1, “Interfaces and switchports”
- 5.2, “Port mirroring”
- 5.3, “Link Aggregation ”
- 5.4, “Link aggregation group provisioning”
- 5.5, “Ethernet bridging”
- 5.6, “Introduction to Provider Bridging”
- 5.7, “Spanning Tree Protocol (STP, RSTP, and MSTP)”
- 5.8, “Storm Control”
- 5.9, “GVRP”
- 5.10, “Link Layer Discovery Protocol”
- 5.11, “Forwarding database provisioning”
- 5.12, “Viewing the configuration of a switch”

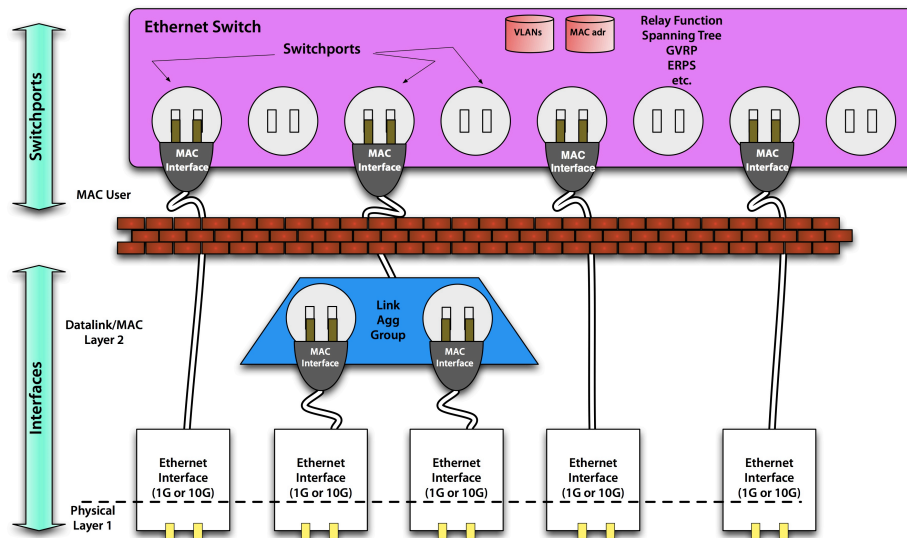
<sup>10</sup> Provider bridging is described in 802.1ad. It is an addendum to 802.1Q and will eventually be integrated into that standard.

## 5.1 Interfaces and switchports

Consider an Ethernet switch as a black box with a number of ports. The switch provides an intelligent relay service between the ports. Each port connects to an actual Ethernet interface or some other entity that provides an Ethernet MAC interface (which is why this is called MAC-layer bridging) such as a Link Aggregation Group. In theory, the ports on the switch, or *switchports*, don't really know what is below them. They will deal with anything that provides an Ethernet MAC interface.

In the following figure, three of the Ethernet interfaces are connected directly to switchports and two of them are aggregated into a link aggregation group, or LAG. The LAG provides an Ethernet MAC interface upwards, so the switchport just sees it as another interface.

Figure 5-1 Interfaces and switchports



Provisioning an interface<sup>11</sup> on the packetVX module is done in *Interface Configuration mode*. For example:

```
> INTERFACE gig 1/1/3
> DESCRIPTION "Gig Ethernet to Customer 1"
> EXIT
```

Associating (connecting) a *switchport* with an *interface* is done by provisioning a switchport with the same name. For example:

```
> SWITCHPORT gig 1/1/3
> PVID 100
> EXIT
```

<sup>11</sup> If the system is configured using the Ethernet Services (Eservice) model described in 6.2, "Ethernet services", configuring the UNIs and NNIs will automatically configure the interfaces and switchports.

## 5.2 Port mirroring

Port mirroring provides a means for network operators to troubleshoot and monitor ingress and/or egress traffic on physical Ethernet ports. To accomplish this, the operator configures a port to simulate—mirror—the activity of another port. For example, an operator wants to see the traffic that is landing on port X. The entire ingress traffic on port X is mirrored to be exported to port Y. In this example, port Y is called a **Mirror-To-Port (MTP)** and port X is called a **Mirror-From-Port (MFP)**.

<b>Note</b>	The packetVX linecards do not support mirroring CPU generated packets from the packetVX modules.
-------------	--

### Considerations

You should be familiar with the following before using port mirroring:

- A single port on a virtual switch is used as an MTP port. If the cumulative traffic that needs to be mirrored across all MFPs is greater than the maximum bandwidth supported on the MTP, you may not see all the mirrored packets.
- Performance monitoring (PM) counters are only available to active switching interfaces. PM counters are not available on the MTP port, since it is not part of any active switch interface.
- Port mirroring only mirrors the traffic seen on the port. It does not classify or filter the traffic.
- MTP and MFP ports can be on different sides of stacking ports or on separate modules.
- **MTP:** The following ports cannot be an MTP port: stacking, switch, NNI, UNI, or a member of a Link Aggregation Group.
  - If you try to configure any of the above settings on an MTP, the system rejects the configuration.

The following example tries to configure an NNI on an MTP:

```
BTI7000:sw1# configure terminal
BTI7000:sw1(config)# interface gigabitEthernet 1/1/11
BTI7000:sw1(config-if GigE 1/1/11)# mirror mirror-to-port
BTI7000:sw1(config-if GigE 1/1/11)# exit
BTI7000:sw1(config)# nni gigabitEthernet 1/1/11
% Cannot do this operation on an mirror to port(MTP).
BTI7000:sw1(config)#
```

- If you try to configure a stacking, switch, NNI, UNI or LAG member port as an MTP, the system rejects the configuration.

The following example tries to configure an NNI port as an MTP:

```
BTI7000:sw1(config)# nni gigabitEthernet 1/1/4
NNI GigE 1/1/4 created.
BTI7000:sw1(config-nni GigE 1/1/4)# exit
BTI7000:sw1(config)# interface gigabitEthernet 1/1/4
BTI7000:sw1(config-if GigE 1/1/4)# mirror mirror-to-port
```

```
% Invalid Configuration. Check UNI/NNI/Stacking/LAG Configuration.  
BTI7000:sw1(config-if GigE 1/1/4)#
```

- **MFP:** Any physical port can be used as the MFP.

<b>Note</b>	Egress frames mirrored from a UNI on a Private EService retain the S-VLAN tag of the EService.
-------------	--

### Configuring port mirroring

Port mirroring is configured using the Command Line Interface (CLI), within Ethernet interface configuration mode. This section provides examples on configuring ports to serve as an MTP and MFP. For detailed information about the port mirroring commands refer to the *BTI 7000 Series Command Line Reference Guide*.

The following example configures port 1/3/1 as an MTP:

```
BTI7000:sw1# configure terminal  
BTI7000:sw1(config)# interface gigabitEthernet 1/3/1  
BTI7000:sw1(config-if GigE 1/3/1)# mirror mirror-to-port
```

The following example configures port mirroring to monitor the incoming traffic on port 1/5/1:

```
BTI7000:sw1# configure terminal  
BTI7000:sw1(config)# interface gigabitEthernet 1/5/1  
BTI7000:sw1(config-if GigE 1/5/1)# mirror mirror-from-port ingress
```

The following example configures port mirroring to monitor outgoing traffic from port 1/6/1:

```
BTI7000:sw1# configure terminal  
BTI7000:sw1(config)# interface gigabitEthernet 1/6/1  
BTI7000:sw1(config-if GigE 1/6/1)# mirror mirror-from-port egress
```

The following example configures port mirroring to monitor both incoming and outgoing traffic on port 1/7/1:

```
BTI7000:sw1# configure terminal  
BTI7000:sw1(config)# interface gigabitEthernet 1/7/1  
BTI7000:sw1(config-if GigE 1/7/1)# mirror mirror-from-port both
```

<b>Note</b>	An MTP port configuration overrides an MFP port configuration.
-------------	--

The following example removes the MFP configuration on port 1/7/1. The same command removes an MTP configuration on a port:

```
BTI7000:sw1# configure terminal  
BTI7000:sw1(config)# interface gigabitEthernet 1/7/1  
BTI7000:sw1(config-if GigE 1/7/1)# no mirror
```

The following example is a **show interface** output for port 1/1/11, which is configured as an MFP:

```
BTI7000# show interface gigabitEthernet 1/1/11  
GigE 1/1/11  
  State is IS-NR  
  fiber type is none, wavelength is 0  
  MTU 9600 bytes
```



```
MAC Address is 00-14-d0-30-a4-62
Flow control configured as auto, Flow control status is off
Full-duplex, 1000Mb/s
loopback is off
phyPmMon is disabled
Mirroring Configuration: mirror ingress traffic
Signal Degrade BERT is 10e-6
OPR threshold (Min: 0.0, Max: 0.0)
.
.
.
.
    transmit utilization (current bin = 228 seconds) 0.0%
BTI7000
```

The following example displays how the port mirroring configuration displays in a **show running configuration** output:

```
interface gigabitEthernet 1/1/11
    admin-state enable
    circuit-id
    loopback facility off
    pm 15-min threshold cv 382
    pm 15-min threshold es 25
    pm 15-min threshold ses 4
    pm 15-min threshold uas 10
    pm 24-hour threshold cv 3820
    pm 24-hour threshold es 250
    pm 24-hour threshold ses 40
    pm 24-hour threshold uas 10

    signal-degrade none
    wavelength 0
    mirror mirror-to-port
    exit
!
```

## 5.3 Link Aggregation

---

Link aggregation, specified in IEEE 802.1AX, allows subscriber links (UNIs) and the network's backbone capacity to grow incrementally as demand on the network increases. Link aggregation allows you to bundle multiple Ethernet interfaces, of the same speed, to create a pipe with more capacity. This bundle is called a Link Aggregation Group (LAG).

The current link aggregation implementation supports:

- up to 27 LAGs
- Eight members per LAG

In general, Ethernet bridges may not re-order packets; packets must be delivered in the same order in which they originate. Link Aggregation modifies this requirement and requires that packets within a single *flow* or *conversation* may not be re-ordered. Link Aggregation puts the onus of meeting this requirement on the transmitter—the receiver can simply receive packets from the various links and forward them to their destinations. In most systems, this is accomplished by having the transmitting node split the traffic, based on various header fields that would define a conversation. In the packetVX, the following choices are available:

- Source MAC address
- Destination MAC address
- Combination of Source and Destination MAC addresses
- Source IP address
- Destination IP address
- Combination of Source and Destination IP addresses

The system selects each specified field from each packet to be transmitted and creates a hash<sup>12</sup> from 1 to *n* (where *n* is the number of available links<sup>13</sup>). This ensures that all packets in the same conversation are sent over the same link and therefore are not re-ordered.

As a result, a LAG with *n* links does not usually have *n* times the carrying capacity of a single link. For example, if all traffic that is received during some time interval belongs to a single conversation, it will all be sent over one link. The bandwidth association with a conversation can never exceed the capacity of a single link in the LAG.

Link aggregation also provides resilience to link failure since links that are not operational are automatically removed from the bundle (and reinserted when they recover), and the traffic is then split over the remaining links.

A LAG is provisioned by creating a LAG interface, assigning members to the group, and then using the group in all the same places that a real physical interface is used.

**Note** LAG member interfaces must all be the same type.

---

<sup>12</sup> For all of these, the source port number and the VLAN ID are part of the hash; therefore, the discrimination is finer than just the indicated header field(s).

<sup>13</sup> As links fail and recover, the value of *n* is changed accordingly.

The following example creates a LAG on virtual switch 1 for a UNI interface. For more information about provisioning LAGs refer to [5.4, “Link aggregation group provisioning”](#):

```
BTI7000:sw1(config)# uni lag 1
BTI7000:sw1(config-if lag 1)# distribution src-mac
BTI7000:sw1(config-if lag 1)# exit
BTI7000:sw1(config)# interface gigabitEthernet 1/1/1
BTI7000:sw1(config-if GigE 1/1/1)# lag 1
BTI7000:sw1(config-if GigE 1/1/1)# lacp mode active
BTI7000:sw1(config-if lag 1)# exit
BTI7000:sw1(config)# interface gigabitEthernet 1/1/2
BTI7000:sw1(config-if GigE 1/1/2)# lag 1
BTI7000:sw1(config-if GigE 1/1/2)# lacp mode active
BTI7000:sw1(config-if lag 1)# exit
```

### Maxlinks

Normally, all available interfaces in a LAG are used to carry traffic. If there are two interfaces in the LAG, traffic is split (as appropriate) across them. There are situations where it is desirable for one or more interfaces to be part of the group but not carry traffic—to act as warm standby links. The link aggregation standard achieves this behavior by allowing a maximum number of active links to be specified. If the number of available links in the group exceeds this maximum, the additional links are held as standby links.

The packetVX accomplishes this by specifying the maximum number of links in the LAG. For example, in the LAG configured above:

```
BTI7000:sw1(config)# uni lag 1
BTI7000:sw1(config-uni lag 1)# shutdown
BTI7000:sw1(config-uni lag 1)# exit
BTI7000:sw1(config)# interface lag 1
BTI7000:sw1(config-if lag 1)# shutdown
BTI7000:sw1(config-if lag 1)# max-links 1
BTI7000:sw1(config-if lag 1)# no shutdown
BTI7000:sw1(config-if lag 1)# exit
BTI7000:sw1(config)# uni lag 1
BTI7000:sw1(config-uni lag 1)# no shutdown
BTI7000:sw1(config-uni lag 1)# exit
```

Even though two links are added to the LAG, only one of them is active. The other link is kept as a standby link:

- Active/Standby LAG switchover times are generally in the 60 msec to 150 msec range when there is a link fault (such as a cable cut). The switchover times apply to both switchover upon failure and switchover upon recovery.
- Cross-Card Active/Standby LAG switchover times are approximately 2 seconds when the switchover is triggered by a module failure or module reboot. Switchover times upon recovery are generally in the 60msec to 150msec range.

### Minlinks

Minlinks is a link aggregation feature that allows you to specify the minimum number of LAG member ports that must be in a link-up state, before the LAG can transition into a link-up state.

Minlinks should be used when the LAG is part of a protected network, for example ERPS, and it is preferable for the network to undergo a protection switch rather than have a link fall below a particular bandwidth.

For example, consider an ERPS ring in which each switch-to-switch connection is a LAG containing four 10G Ethernet. If the network manager knows that each connection must be able to transport at least 30G of traffic to provide the necessary service, he can set minlinks to three. If one of the links in a LAG fails, there are still three available and the path stays up. If a second one fails, there are fewer than three and the LAG goes down, forcing a protection switch.

Configuring the minimum number of ports in a link-up state is accomplished within LAG interface mode, using the command **min-links**. The following example sets the minimum number of ports to three on LAG ID 8:

```
BTI7000:sw1: configure terminal
BTI7000:sw1(config)# uni lag 8
BTI7000:sw1(config-uni lag 8)# shutdown
BTI7000:sw1(config-uni lag 8)# exit
BTI7000:sw1(config)# interface lag 8
BTI7000:sw1(config-if lag 8)# shutdown
BTI7000:sw1(config-if lag 8)# min-links 3
BTI7000:sw1(config-if lag 8)# no shutdown
BTI7000:sw1(config-if lag 8)# exit
BTI7000:sw1(config)# uni lag 8
BTI7000:sw1(config-uni lag 8)# no shutdown
BTI7000:sw1(config-uni lag 8)# exit
```

### 5.3.1 Link Aggregation Group distribution

Link Aggregation Groups (LAGs) distribute traffic across the member links based on a hash of various fields in the Ethernet frame. The goal of this approach is to ensure that all Ethernet packets that constitute a "conversation" follow the same path so they are not accidentally reordered.

The algorithm is different for Ethernet frames that are "directed" (unicast to a known address) and those that are "flooded" (broadcast, multicast, or sent to an unknown destination <sup>14</sup>).

#### LAG Distribution for directed traffic

For directed packets there is a choice of the following mode parameters:

- 1 Source MAC Address + Ingress Port + VLAN ID + Ethertype
- 2 Destination MAC Address + Ingress Port + VLAN ID + Ethertype
- 3 Combination of 1 and 2
- 4 IP Source Address (IPv4 or IPv6) + IP Source Port Number
- 5 IP Destination Address (IPv4 or IPv6) + IP Destination Port

<sup>14</sup> If an Ethernet Service has learning disabled, then all frames received on that service are flooded. This is acceptable if the service is an E-LINE service, since there is usually only two ports on any switch that forward that service. Note that all frames in that service are treated as "flooded" if they are forwarded over a LAG.

## 6 Combination of 4 and 5

Mode 3, above, is the most general hash for Ethernet traffic. Using IP addresses (mode 6) makes sense when the majority of the traffic is between IP routers. In this case, the MAC addresses are always the router addresses so there is little variation, but, the IP addresses are the actual IP end points.

The result of the hash is a 3-bit value that is indexed into a list of Ethernet interfaces, so there can be up to eight members of a LAG. If there are fewer than eight members (usually the case) then the list has repeated values. For example, if there are only two members, the list contains 1, 2, 1, 2, 1, 2, 1, 2. If there are three members the list contains 1, 2, 3, 1, 2, 3, 1, 2, etc.

It is important to note that in the example of three members, members 1 and 2 (which show up three times in the table) have a higher probability of having a conversation mapped to them than member 3 (which only shows up twice). The probabilities are uneven unless the number of members is a power of 2 (for example, 2, 4, 8). This does not mean that four members have traffic split evenly, it is still a matter probability base on the number of conversations and their addresses. However, with enough variety in conversations, the probability is higher that the load is more evenly spread with four members than with three or five.

### LAG Distribution for flooded traffic

For flooded packets, the distribution algorithm is fixed (not configurable). If an Ethernet frame is not an IP multicast packet, the LAG member is chosen based on the low-order 4-bits of a hash generated from the combination of each of the following: MAC source address, MAC destination address, and incoming Ethernet interface number. If the packet is an IP multicast packet, the hash uses the low-order 4-bits of the IP source address, IP destination address, and the incoming Ethernet interface number.

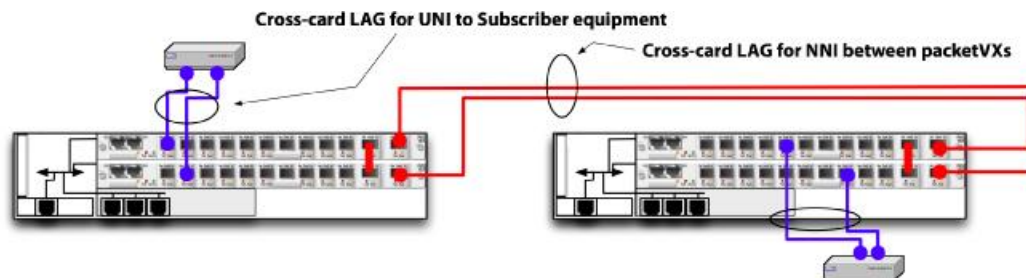
In this case the 4-bit result is used to select a trunk from a 16 entry table. (Note that on the PVX80 the hash is a 6-bit value that can select from up to 64 entries.)

## 5.3.2 Link Aggregation and stacking

When used in a stacking configuration (see 4.3, “Stacking”), Link Aggregation can provide additional resiliency.

A stack contains two packetVX modules that are connected with a stacking port and behave as a single bridge. Since they operate as a single bridge, they also support a unified implementation of link aggregation. A LAG can contain interfaces from both packetVX modules in a stack. As a result, not only will Link Aggregation provide resilience against a link failure, but if the interfaces are from both modules (often called *cross-card LAG*), there is also resilience against a module failure.

The following figure shows that if any of the four packetVX modules fail, full connectivity is maintained between the two subscriber systems.

**Figure 5-2 Cross-card LAG for UNI and NNI**

### 5.3.3 LACP active and standby links within a LAG

A LAG can be configured in one of two ways, LAG N and LAG N+M. The LAG N implementation automatically distributes and load balances the traffic across the working links within a LAG. This maximizes the use of the LAG if Ethernet links go down or come back up. The LAG N+M implementation uses LACP to support active and standby links within the LAG. If an active Ethernet links go down, it fails over to a standby link.

While any two ports on a given system may be capable of aggregation, it is not necessarily the case that an arbitrary selection of such ports can be aggregated. A system may reasonably limit the number of ports attached to a single LAG, or the particular way more than two ports can be combined.

In cases where both communicating systems (via LACP) have constraints on aggregation, it is necessary for them both to agree on the links to be selected for aggregation.

Every link between systems operating LACP is assigned a unique priority. This priority comprises (in priority order) the LACP System Priority, LACP System ID, LACP Port Priority, and Port Number of the higher-priority system. In priority comparisons, numerically lower values have higher priority.

Ports are considered for active use in an aggregation in link priority order, starting with the port attached to the highest priority link. Each port is selected for active use if preceding higher priority selections can also be maintained; otherwise the port is selected as standby.

A port that is selected as standby as a result of limitations on aggregation capability can be viewed as providing a “hot standby” facility, as it is able to take part in the aggregation upon failure of one of the active links in the LAG. The ability to hold links in a standby mode in this way provides the possibility of using LACP even where the system is incapable of supporting distribution and collection with more than one port. Parallel links could be automatically configured as standby links, and deployed to mask link failures without any disruption to higher layer protocols.

LACP link protection reverts to a higher-priority (lower-numbered) link when that higher-priority link becomes operational or a link is added to the LAG that is determined to be higher in priority.

Generally, when using active and standby links within a LAG, you should set your LACP wait-time to zero from the default of 2 seconds. There are several reasons for this:

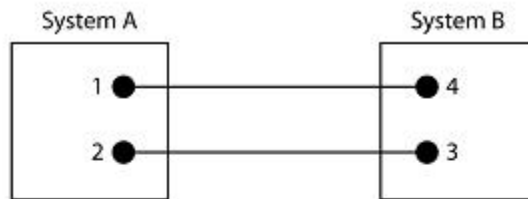
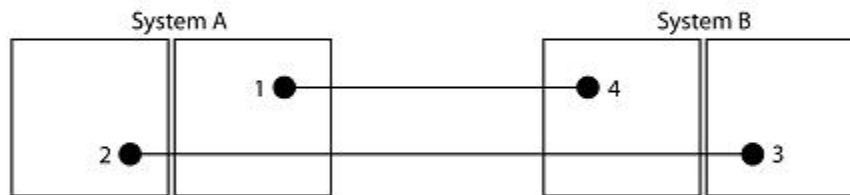
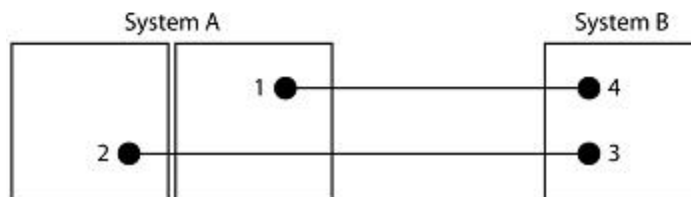
- If there is a protection switch on the equipment (or a failure of the fiber), then there is a 2 second outage while LACP wait-time expires. With this set to zero, the protection switch happens as fast as possible.
- In some complex configurations, especially interconnected ERPS and MSTP networks, this can cause unintended network topology changes and result in loops.

### 5.3.4 Sample 1+1 LAG configuration

In this example, two systems, A and B, are connected by two parallel links. Each system can support a maximum of one link in the aggregation. When LACP is configured on ports, it tries to configure the maximum number of compatible ports in a port channel, up to the maximum allowed by the hardware (in this example one port). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails.

<b>Note</b>	For all of the following scenarios, if an active link fails, it is replaced by the highest priority standby link, which maintains the intended bandwidth for the LAG.
-------------	---

<b>Note</b>	For stacked configurations, if the same port number is used on the primary and secondary packetVX™ module, the one which is the first member in the virtual switch has the higher priority port.
-------------	--

**Figure 5-3 1+1 LACP configuration example****Non-Stacked System****Stacked System****Stacked/Non-Stacked System****Table 5-1 1+1 LACP configuration scenario A**

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default)	Port 3 – 128 (default) Port 4 – 128 (default)
Resulting Configuration	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 2 (link state = standby)</li> </ul>	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 4 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 3 (link state = standby)</li> </ul>



**Table 5-2 1+1 LACP configuration scenario B**

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 400 Port 2 – 300	Port 3 – 200 Port 4 – 100
Resulting Configuration	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 1 (link state = standby)</li> </ul>	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 4 (link state = standby)</li> </ul>

**Table 5-3 1+1 LACP configuration scenario C**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default)	Port 3 – 128 (default) Port 4 – 128 (default)
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 1 (link state = standby)</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 4 (link state = standby)</li> </ul>

**Table 5-4 1+1 LACP configuration scenario D**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 100 Port 2 – 200	Port 3 – 200 Port 4 – 100
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul>

**Table 5-4 1+1 LACP configuration scenario D (Continued)**

Parameter	System A	System B
	Active Links (in priority order):	Active Links (in priority order):
	<ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 1 (link state = in – bundle)</li> </ul>	<ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – bundle)</li> </ul>
	Standby Links (in priority order):	Standby Links (in priority order):
	<ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 2 (link state = standby)</li> </ul>	<ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 3 (link state = standby)</li> </ul>

### 5.3.5 Sample N+N LAG configuration

In this example, two systems, A and B, are connected by four parallel links. Each system can support a maximum of two links in an aggregation. When LACP is configured on ports, it tries to configure the maximum number of compatible ports in a port channel, up to the maximum allowed by the hardware (in this example two ports). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails.

**Note** For all of the following scenarios, if an active link fails, it is replaced by the highest priority standby link, which maintains the intended bandwidth for the LAG.

**Note** For stacked configurations, if the same port number is used on the primary and secondary packetVX™ module, the one which is the first member in the virtual switch has the higher priority port.

Figure 5-4 N+N LACP configuration example

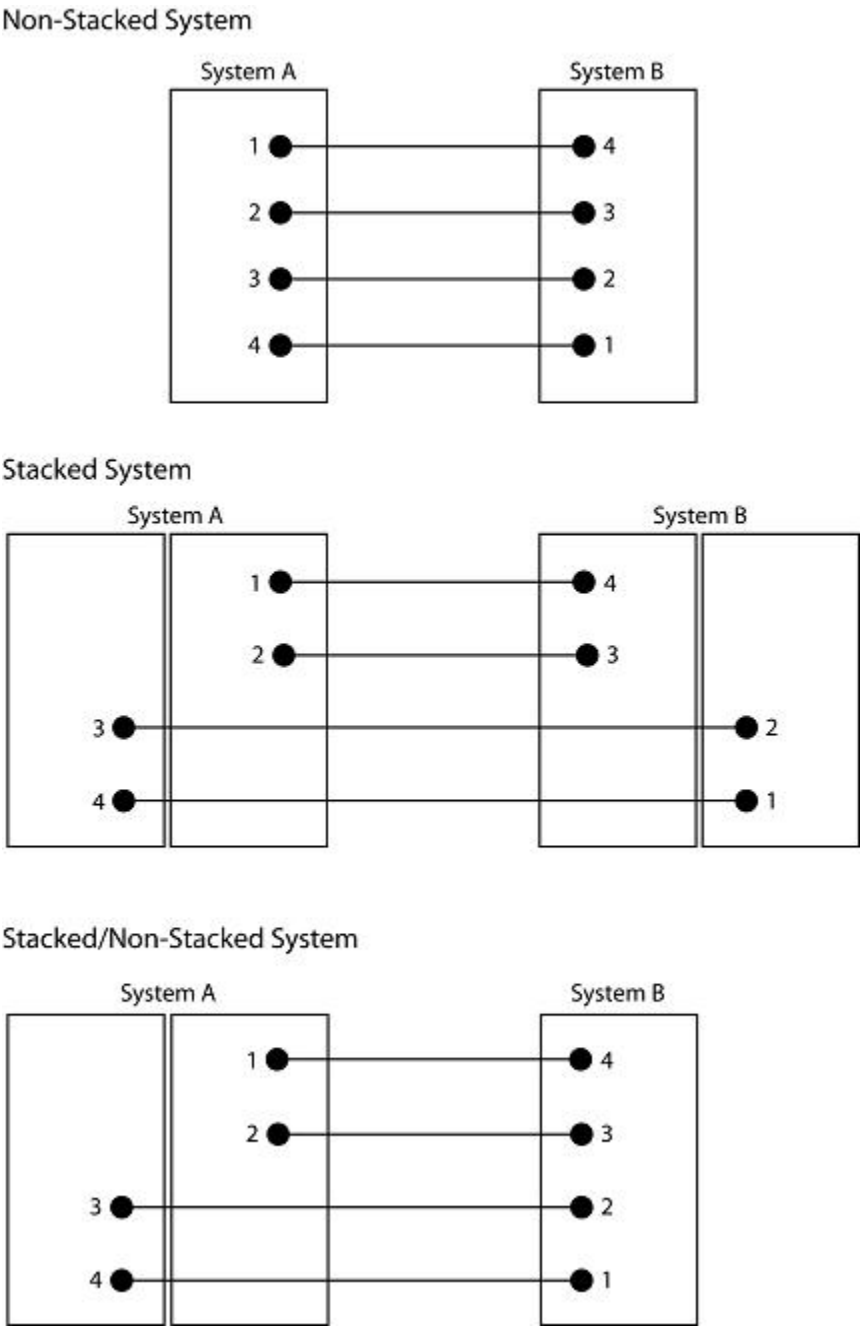


Table 5-5 N+N LACP configuration scenario A

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default)	Port 1 – 128 (default) Port 2 – 128 (default)

**Table 5-5 N+N LACP configuration scenario A (Continued)**

Parameter	System A	System B
	Port 3 – 128 (default)	Port 3 – 128 (default)
	Port 4 – 128 (default)	Port 4 – 128 (default)
Resulting Configuration	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 3 (link state = standby)</li> <li>Port 4 (link state = standby)</li> </ul>	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 2 (link state = standby)</li> <li>Port 1 (link state = standby)</li> </ul>

**Table 5-6 N+N LACP configuration scenario B**

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100	Port 1 – 100 Port 2 – 200 Port 3 – 300 Port 4 – 400
Resulting Configuration	High Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 2 (link state = standby)</li> <li>Port 1 (link state = standby)</li> </ul>	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 3 (link state = standby)</li> <li>Port 4 (link state = standby)</li> </ul>

**Table 5-7 N+N LACP configuration scenario C**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default)	Port 1 – 128 (default) Port 2 – 128 (default)

**Table 5-7 N+N LACP configuration scenario C (Continued)**

Parameter	System A	System B
	Port 3 – 128 (default)	Port 3 – 128 (default)
	Port 4 – 128 (default)	Port 4 – 128 (default)
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 2 (link state = standby)</li> <li>Port 1 (link state = standby)</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 3 (link state = standby)</li> <li>Port 4 (link state = standby)</li> </ul>

**Table 5-8 N+N LACP configuration scenario D**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 3 (link state = standby)</li> <li>Port 4 (link state = standby)</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 2 (link state = standby)</li> <li>Port 1 (link state = standby)</li> </ul>

### 5.3.6 Sample N+M LAG configuration

In this example, two systems, A and B, are connected by four parallel links. Each system can support a maximum of three links in an aggregation. When LACP is configured on ports, it tries to configure the maximum number of compatible ports in a port channel, up to the maximum

allowed by the hardware (in this example three ports). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails.

<b>Note</b>	For all of the following scenarios, if an active link fails, it is replaced by the highest priority standby link, which maintains the intended bandwidth for the LAG.
-------------	---

<b>Note</b>	For stacked configurations, if the same port number is used on the primary and secondary packetVX™ module, the one which is the first member in the virtual switch has the higher priority port.
-------------	--

Figure 5-5 N+M LACP configuration example

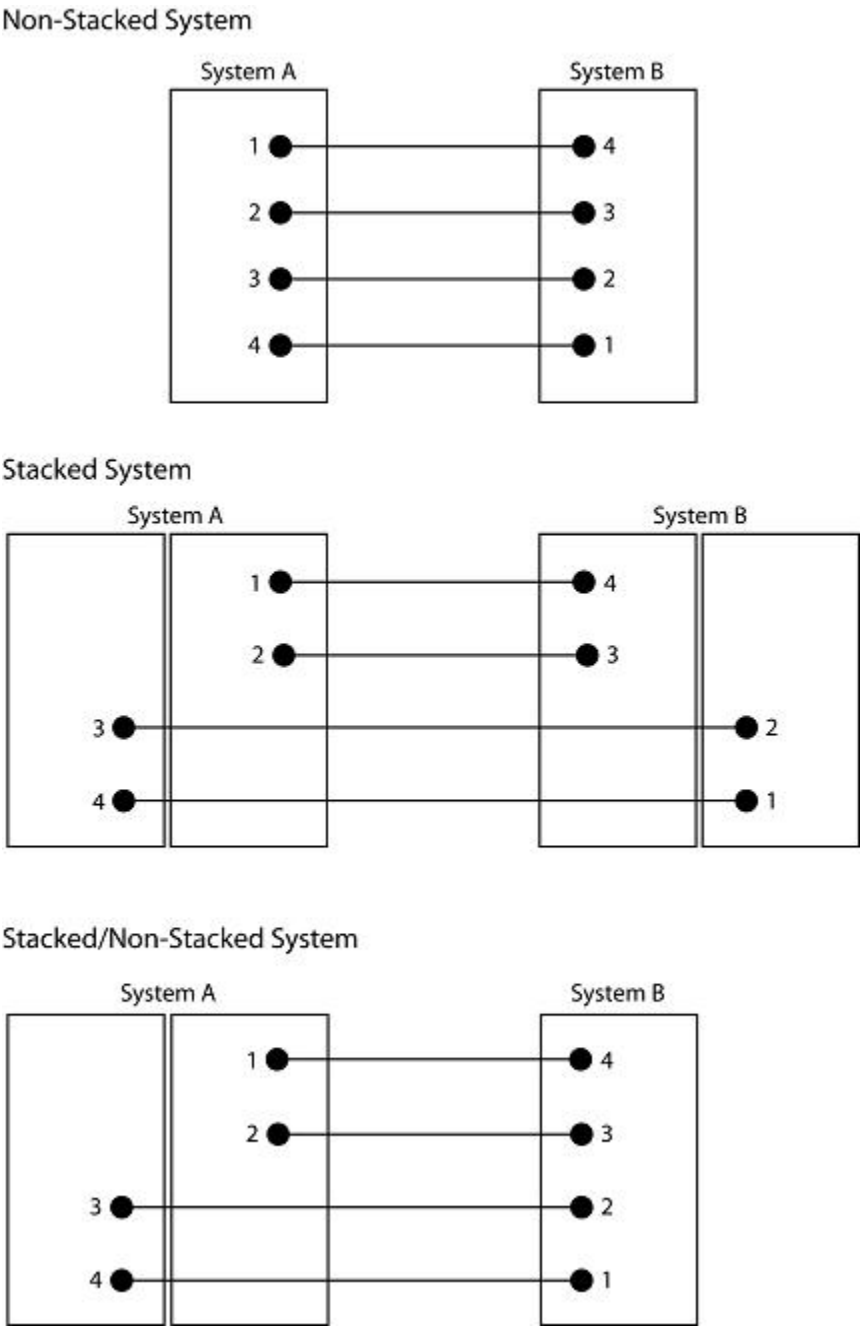


Table 5-9 N+M LACP configuration scenario A

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default)	Port 1 – 128 (default) Port 2 – 128 (default)

**Table 5-9 N+M LACP configuration scenario A (Continued)**

Parameter	System A	System B
	Port 3 – 128 (default)	Port 3 – 128 (default)
	Port 4 – 128 (default)	Port 4 – 128 (default)
Resulting Configuration	High Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 4 (link state = standby)</li> </ul>	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 1 (link state = standby)</li> </ul>

**Table 5-10 N+M LACP configuration scenario B**

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100	Port 1 – 100 Port 2 – 200 Port 3 – 300 Port 4 – 400
Resulting Configuration	High Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 1 (link state = standby)</li> </ul>	High Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – standby)</li> <li>Port 3 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = bundle)</li> </ul>

**Table 5-11 N+M LACP configuration scenario C**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default)	Port 1 – 128 (default) Port 2 – 128 (default)



**Table 5-11 N+M LACP configuration scenario C (Continued)**

Parameter	System A	System B
	Port 3 – 128 (default)	Port 3 – 128 (default)
	Port 4 – 128 (default)	Port 4 – 128 (default)
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 1 (link state = standby)</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 4 (link state = standby)</li> </ul>

**Table 5-12 N+M LACP configuration scenario D**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100	Port 1 – 100 Port 2 – 200 Port 3 – 300 Port 4 – 400
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 4 (link state = standby)</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 1 (link state = standby)</li> </ul>

### 5.3.7 Sample LACP misconfiguration

In this example, two systems, A and B, are connected by four parallel links. System A can support a maximum of two links in an aggregation and System B can support a maximum of three links in an aggregation. When LACP is configured on ports, it tries to configure the

maximum number of compatible ports in a port channel, up to the maximum allowed by the hardware (in this example two ports for System A and three ports for System B). If LACP cannot aggregate all the ports that are compatible (for example, the remote system might have more restrictive hardware limitations), then all the ports that cannot be actively included in the channel are put in hot standby state and are used only if one of the channeled ports fails.

<b>Note</b>	For all of the following scenarios, if an active link fails, it is replaced by the highest priority standby link, which maintains the intended bandwidth for the LAG.
-------------	---

<b>Note</b>	For stacked configurations, if the same port number is used on the primary and secondary packetVX™ module, the one which is the first member in the virtual switch has the higher priority port.
-------------	--

Figure 5-6 LACP misconfiguration example

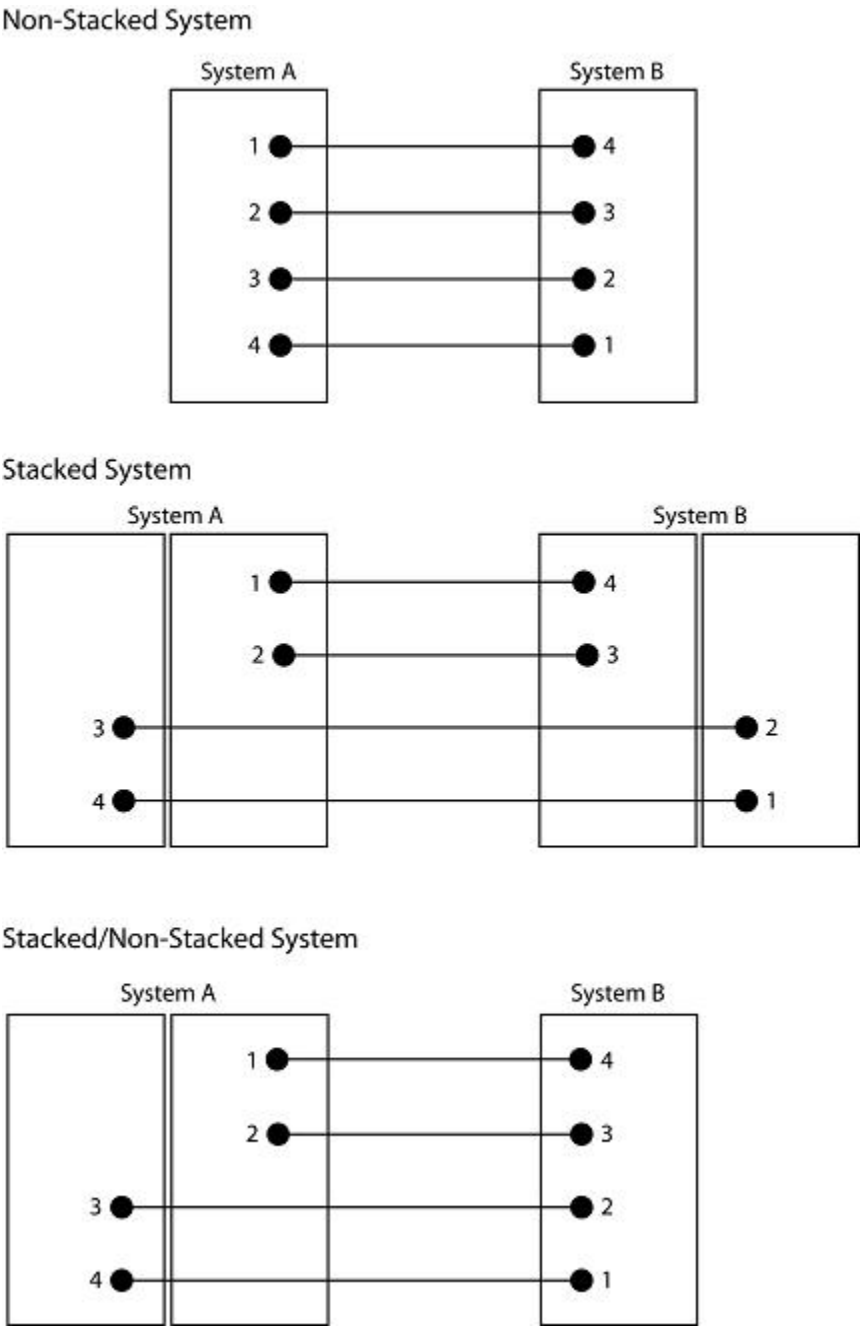


Table 5-13 LACP misconfiguration scenario A

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default)	Port 1 – 128 (default) Port 2 – 128 (default)

**Table 5-13 LACP misconfiguration scenario A (Continued)**

Parameter	System A	System B
	Port 3 – 128 (default)	Port 3 – 128 (default)
	Port 4 – 128 (default)	Port 4 – 128 (default)
Resulting Configuration	High Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 3 (link state = standby)</li> <li>Port 4 (link state = standby)</li> </ul>	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> <li>Port 2 (link state = down, in this case this is really a standby link)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 1 (link state = standby)</li> </ul>

**Table 5-14 LACP misconfiguration scenario B**

Parameter	System A	System B
LACP System Priority	32767 (default)	32767 (default)
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100
Resulting Configuration	High Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 2 (link state = standby)</li> <li>Port 1 (link state = standby)</li> </ul>	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System ID</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> <li>Port 3 (link state = down, in this case this is really a standby link)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System A</li> <li>Port 4 (link state = standby)</li> </ul>

**Table 5-15 LACP misconfiguration scenario C**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05

**Table 5-15 LACP misconfiguration scenario C (Continued)**

Parameter	System A	System B
LACP Port Priority	Port 1 – 128 (default) Port 2 – 128 (default) Port 3 – 128 (default) Port 4 – 128 (default)	Port 1 – 128 (default) Port 2 – 128 (default) Port 3 – 128 (default) Port 4 – 128 (default)
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 2 (link state = standby)</li> <li>Port 1 (link state = standby)</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> <li>Port 3 (link state = down, in this case this is really a standby link)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port number</li> <li>Port 4 (link state = standby)</li> </ul>

**Table 5-16 LACP misconfiguration scenario D**

Parameter	System A	System B
LACP System Priority	2000	1000
LACP System ID	00:14:d0:00:3e:7e	00:14:d0:00:4b:05
LACP Port Priority	Port 1 – 100 Port 2 – 200 Port 3 – 300 Port 4 – 400	Port 1 – 400 Port 2 – 300 Port 3 – 200 Port 4 – 100
Resulting Configuration	Lower Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 1 (link state = in – bundle)</li> <li>Port 2 (link state = in – bundle)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by System B</li> <li>Port 3 (link state = standby)</li> <li>Port 4 (link state = standby)</li> </ul>	Higher Priority System <ul style="list-style-type: none"> <li>determined by LACP System Priority</li> </ul> Active Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 4 (link state = in – bundle)</li> <li>Port 3 (link state = in – bundle)</li> <li>Port 2 (link state = down, in this case this is really a standby link)</li> </ul> Standby Links (in priority order): <ul style="list-style-type: none"> <li>determined by port priority</li> <li>Port 1 (link state = standby)</li> </ul>

## 5.4 Link aggregation group provisioning

---

Link aggregation groups (LAGs) allow multiple Ethernet interfaces that are running at the same speed to be grouped together providing increased transport performance and/or increased robustness.

### LAGs on the packetVX

The packetVX supports the following LAG capacity:

- up to 27 LAGs
- Each group supports up to 8 members

When 10 GbE is encapsulated in OTU2 wrappers, the link aggregation software relies on the OTU2 for the detection of Loss of Signal (LOS), Loss of Frame (LOF), and Signal Degrade (SD) failures. The OTU2 framer triggers the software to remove the LOS port from the LAG. When the defect clears, the software adds the port back to the LAG.

If a fiber cut occurs between two nodes, the link aggregation software relies on OTU2 for the detection of backward defect indications (BDI) and backward error indications (BEI). The OTU2 framer triggers the software to cause the port to be unavailable; the traffic continues along the available links. When the defect clears, the port is automatically transitioned to an available state and resumes carrying traffic.

### Link aggregation control protocol

The Link Aggregation Control Protocol (LACP) operates between packetVX modules to control the addition or removal of ports from the LAG.

#### 5.4.1 Displaying LACP system priority and LACP system ID

Use this procedure to display the LACP system priority and LACP system ID for the packetVX™.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- Equipment must be provisioned.
- The member must be created and associated with a Virtual Switch.
- The Virtual Switch must be created.

#### Step 1 Enter the privileged EXEC mode

To enter the privileged EXEC mode, enter the following command:

```
BTI7000> enable
```

The system responds with the following prompt:

```
BTI7000#
```

## Step 2 Enter the configuration mode

To enter the configuration mode, enter the following:

```
BTI7000# configure terminal
```

The system responds with the following prompt:

```
BTI7000(config)#
```

## Step 3 Display virtual switch Information

To display a virtual switch, enter the following command:

```
show virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
show virtual-switch 1
```

## CLI Command Example

```
BTI7000(config)# show virtual-switch 1
```

```
SwitchId: 1
  Bridge Mode is provider
  Bridge ID is 00:14:d0:00:4b:05
  Aging Time is 300 sec
  MSTP is administratively enabled
  GVRP is administratively enabled
  LACP is administratively enabled
  802.1x is administratively disabled
  802.lag is administratively disabled
  Y.1731 is administratively enabled
  CCM_OFFLOAD is administratively disabled
  ERPS is administratively enabled
  LACP System Priority is 100
  LACP system-id is 00:14:d0:00:4b:05

Tunnel MAC Address Profile: DEFAULT_TMA_PROFILE

EVC MEG Name:
EVC MEG Level:      4
Switch Name:        SWITCH_1
MIP Auto create:    enabled
MIP Auto create MEL: 4
Primary Member:     1/3
Time As Primary:    87127 seconds
Last Forced Switch: 0 seconds

Members:
      Admin      Stacking  Stacking Port  Backplane
```

Location	State	State	Comm State	Comm State
-----	-----	-----	-----	-----
1/3	enable	primary	no connection	no connection

You have successfully completed this procedure.

## 5.4.2 Setting LACP system priority

Use this procedure to set the LACP system priority for the packetVX™.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- Equipment must be provisioned.
- The member must be created and associated with a Virtual Switch.
- The Virtual Switch must be created.

#### Step 1 Enter the privileged EXEC mode

To enter the privileged EXEC mode, enter the following command:

```
BTI7000> enable
```

The system responds with the following prompt:

```
BTI7000#
```

#### Step 2 Enter the configuration mode

To enter the configuration mode, enter the following:

```
BTI7000# configure terminal
```

The system responds with the following prompt:

```
BTI7000(config)#
```

#### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 4 Set the LACP system priority

To set the LACP System Priority, enter the following command:



```
lACP system-priority <priority>
```

where *<system-priority>* > is 0 – 65535 and the default value is 32767.

For example, the command string might be

```
lACP system-priority 200
```

**Note** The switch with the lowest LACP system priority value decides the standby and active links in the aggregation.

**Note** This is a global command and affects all interfaces that are using LACP. This command causes a traffic interruption.

You have successfully completed this procedure.

### 5.4.3 Setting LACP port priority

Use this procedure to set the LACP port priority for the packetVX™.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- Equipment must be provisioned.
- The member must be created and associated with a Virtual Switch.
- The Virtual Switch must be created.

#### Step 1 Enter the privileged EXEC mode

To enter the privileged EXEC mode, enter the following command:

```
BTI7000> enable
```

The system responds with the following prompt:

```
BTI7000#
```

#### Step 2 Enter the configuration mode

To enter the configuration mode, enter the following:

```
BTI7000# configure terminal
```

The system responds with the following prompt:

```
BTI7000(config)#
```

#### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where *<switch\_id>* is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### **Step 4 Navigate to the desired port.**

To navigate to the desired port, enter the following command:

```
interface <gigabitEthernet | tenGigabitEthernet> <shelf/slot/port>
```

For example, the command string might be

```
interface gigabitEthernet 1/3/2
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-if GigE 1/3/2)#
```

#### **Step 5 Set the LACP port priority**

To set the LACP port priority, enter the following command:

```
lacp port-priority <priority>
```

where <priority> is 0 – 65535 and the default value is 128.

For example, the command string might be

```
lacp port-priority 200
```

You have successfully completed this procedure.

### **5.4.4 Creating a link aggregation group**

This procedure describes how to create a link aggregation group for a switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### **Prerequisites**

- An Ethernet interface must be created before you can add it to the LAG.

#### **Step 1 Enter the privileged EXEC mode**

```
BTI7000> enable
```

The system responds with the following prompt:

```
BTI7000#
```

#### **Step 2 Enter the configuration mode**

```
BTI7000# configure terminal
```

The system responds with the following prompt:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch**

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Create a link aggregation group and specify an interface link aggregation group**

```
BTI7000:sw1(config)# <uni | nni> lag <lag#> <interface-id>
```

where <lag#> is the LAG identifier (1 to 27)

For example, the command string might be

```
uni lag 1
```

**Step 5 Exit from the link aggregation group interface mode**

```
exit
```

**Step 6 Create a "raw" interface on the port(s) to be added to the LAG**

```
BTI7000:sw1(config)# interface  
    < gigabitEthernet | tenGigabitEthernet> 1/1/1
```

**Step 7 Add an Ethernet interface to the LAG**

```
BTI7000:sw1(config-if GigE 1/1/1)# lag <lag#>
```

where <lag#> is the LAG identifier (1 to 27)

For example, the command string might be

```
lag 1
```

**Step 8 Set the LACP mode.**

```
BTI7000:sw1(config-uni GigE 1/1/1)# lacp mode active
```

**Step 9 Repeat step 7 for all interfaces to be added to the LAG.**

```
uni lag 1
```

```
exit
```

```
interface gigabitEthernet 1/1/8
```

```
lag 1
```

```
exit
```

```
interface gigabitEthernet 1/1/9
```

```
lag 1
```

```
exit
```

**Step 10 Set the distribution mode.**

```
BTI7000:sw1(config)# interface lag 1
BTI7000:sw1(config-if lag 1)# distribution src-mac
```

You have successfully completed this procedure.

## 5.4.5 Setting the maximum number of links for a LAG

Use this procedure to set the maximum number of links in a LAG.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- Equipment must be provisioned.
- The Virtual Switch must be created.
- The member must be created and associated with a Virtual Switch.
- The LAG must be created.

#### Step 1 Enter the privileged EXEC mode

```
BTI7000> enable
```

The system responds with the following prompt:

```
BTI7000#
```

#### Step 2 Enter the configuration mode

```
BTI7000# configure terminal
```

The system responds with the following prompt:

```
BTI7000(config)#
```

#### Step 3 Select a virtual switch

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier.

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 4 Specify the interface type.

```
BTI7000:sw1(config)# uni|nni lag <lag#>
```

where <lag#> is the LAG identifier

For example, if specifying a UNI interface

```
uni lag 1
```

The CLI prompt should now appear as follows:

```
BTI7000sw1(config-uni LAG 1)#
```

**Step 5 Navigate to the desired LAG interface.**

```
BTI7000:sw1(config)# interface lag <lag#>
```

where <lag#> is the LAG identifier (1 to 27)

For example, the command string might be

```
interface lag 1
```

The CLI prompt should now appear as follows:

```
BTI7000sw1(config-if LAG 1)#
```

**Step 6 Take the LAG interface out of service.**

```
BTI7000sw1(config-if LAG 1)# shutdown
```

**Step 7 Set the maximum number of members in the LAG.**

**Note** The LAG must be out of service.

```
max-links <size>
```

where <size> is 1 to 8. The default value is 8.

For example, the command string might be

```
max-links 4
```

**Step 8 Put the LAG interface back into service.**

```
no shutdown
```

**Step 9 Exit out of the LAG interface configuration mode.**

```
exit
```

**Step 10 Navigate to the LAG**

```
BTI7000:sw1(config)# <uni | nni> lag <interface-id>
```

For example, the command string might be

```
uni lag 1
```

You have successfully completed this procedure.

## 5.4.6 Setting the minimum number of LAG member ports

Use this procedure to set the minimum number of member ports in a LAG (link aggregation group).

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Prerequisites**

- Equipment must be provisioned.
- The Virtual Switch must be created.
- The member must be created and associated with a Virtual Switch.
- The LAG must be created.

**Step 1 Enter the privileged EXEC mode**

```
BTI7000> enable
```

The system responds with the following prompt:

```
BTI7000#
```

**Step 2 Enter the configuration mode**

```
BTI7000# configure terminal
```

The system responds with the following prompt:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch**

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier.

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Specify the interface type.**

```
BTI7000:sw1(config)# uni|nni lag <lag#>
```

where <lag#> is the LAG identifier

For example, the command string might be

```
uni lag 1
```

The CLI prompt should now appear as follows:

```
BTI7000sw1(config-uni LAG 1)#
```

**Step 5 Navigate to the desired LAG interface.**

```
BTI7000:sw1(config)# interface lag <lag#>
```

where <lag#> is the LAG identifier (1 to 27)

For example, the command string might be

```
interface lag 1
```

The CLI prompt should now appear as follows:

```
BTI7000sw1(config-if LAG 1)#
```

**Step 6 Take the LAG interface out of service.**

```
BTI7000sw1(config-if LAG 1)# shutdown
```

**Step 7 Set the minimum number of LAG member ports.**

**Note** The LAG must be out of service.

```
min-links <size>
```

where<size> is 1 to 8. The default value is 1.

For example, the command string might be

```
min-links 4
```

**Step 8 Put the LAG interface back into service.**

```
no shutdown
```

**Step 9 Exit out of the LAG interface configuration mode.**

```
exit
```

**Step 10 Navigate to the LAG interface.**

```
BTI7000:sw1(config)# <uni | nni> lag <interface-id>
```

For example, the command string might be

```
uni lag 1
```

You have successfully completed this procedure.

## 5.5 Ethernet bridging

---

The primary role of the packetVX is to operate as an Ethernet bridge. An Ethernet bridge is an internetworking device that operates at Layer 2 in the OSI network model.

Ethernet bridges do not use a routing protocol to determine how to forward packets. Ethernet bridges use methods called learning and flooding.

### Learning

Ethernet bridges inspect the source address of each ingress packet to learn where that address is located (that is, which port relative to the bridge itself). All subsequent received packets addressed *to* that address are forwarded to the learned port.

### Flooding

Received packets that are addressed to destinations that have not yet been learned or to a broadcast or multicast address are flooded—that is, sent to every port (other than the one on which each was received) in the hope that the appropriate destination(s) will get the packet.

Learning works because in a conversation between two stations the initial packet(s) from the station initiating the conversation are flooded, thereby ensuring that all bridges learn its address. The destination station likely responds to the initial packets and the response is forwarded along the path learned by the bridges back to the source, thereby ensuring that the bridges along that path learn the responding station's address. After the first exchange, all of the bridges along the path have learned both addresses, and forwarding is efficient.

### Ethernet bridging problem

The problem with the basic learning bridge is loops and flooded packets. If a loop is configured in the network, a flooded packet eventually finds its way around the loop and is flooded again.

### Spanning Tree Protocol solution

The solution to the problem of loops and flooded packets is to create a spanning tree in the network (a loop free network that includes all nodes) which can be done by logically removing links in the network. The Spanning Tree Protocol is an automatic and distributed protocol that logically disables ports within each loop in the network—that is, received packets are discarded and packets received on other ports are not forwarded to the port.

For further information on spanning tree protocols, see section [5.7, “Spanning Tree Protocol \(STP, RSTP, and MSTP\)”](#).



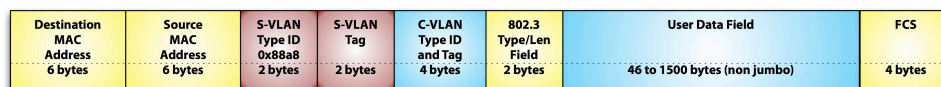
## 5.6 Introduction to Provider Bridging

802.1Q added VLAN tags to the Ethernet frame, providing multiple broadcast domains in bridged Ethernet networks<sup>15</sup>. After a few years, it became evident that 802.1Q VLANs had two limitations that reduced their utility for service providers. First, different subscribers could be using the same VLAN ID, so the subscriber VLAN could not be carried across the network uniquely—for example, two customers could both be using VLAN 112. This could, in theory, be addressed by translating VLANs at the ingress point. But this exposed the second problem—if each customer VLAN results in a VLAN in the provider domain, the 4000 VLANs defined in 802.1Q simply aren't enough. An addendum to 802.1Q, 802.1ad – Provider Bridges, addressed these limitations.

802.1ad adds an additional VLAN tag outside of the 802.1Q VLAN tag (hence the name Q-in-Q). The inner (original) VLAN tag is called the customer VLAN, or C-VLAN, and the new outer VLAN tag is called the service provider VLAN, or S-VLAN. The S-VLAN has roughly the same 32-bit structure as the original VLAN tag (C-VLAN) except that the tag identifier is different.

The following figure shows the resulting frame format.

**Figure 5-7 S-VLAN tagged frame format**



Using S-VLANs, the network can support over 4000 customers (or customer virtual connections), each of which can encompass over 4000 C-VLANs, and the C-VLANs can be carried transparently with no potential for conflict since they are hidden behind the S-VLAN.

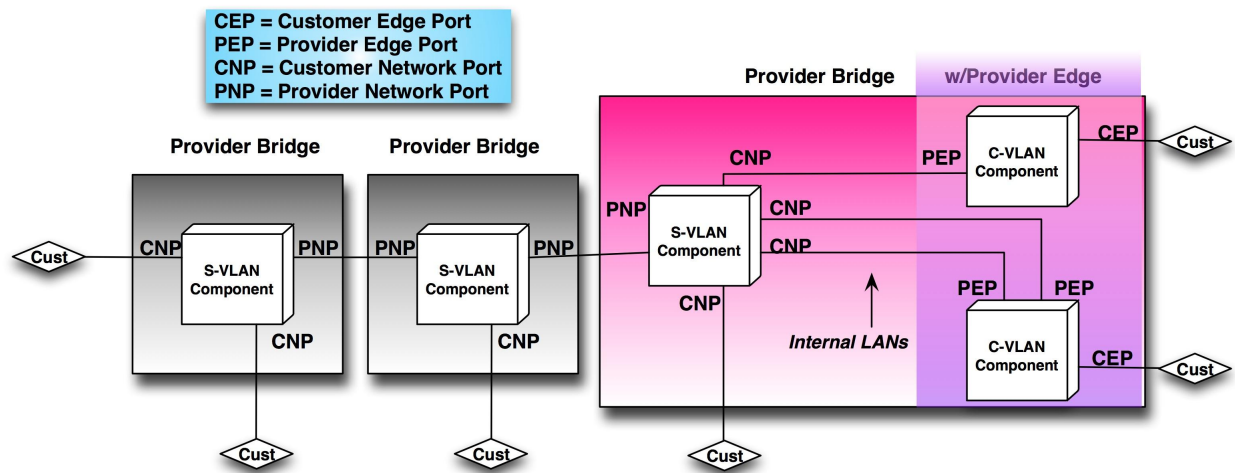
Architecturally, there are two different types of forwarding entities associated with Provider Bridges:

- A C-VLAN component, which is a function of the bridge, in which each port is capable of recognizing, inserting, and removing Customer VLAN tags. A C-VLAN component has one Customer Edge port (CEP) and one or more (internal) Provider Edge ports (PEP)<sup>16</sup>.
- An S-VLAN component, which is a function of the bridge in which each port is capable of recognizing, inserting, and removing Service VLAN tags. An S-VLAN component has zero or more Customer Network ports (CNP) and zero or more Provider Network ports (PNPs).

A Provider Bridge (PB) contains one S-VLAN component and zero or more C-VLAN components. If there is a C-VLAN component, the switch is also referred to as a Provider-Edge Bridge (PEB).

<sup>15</sup> VLAN tags were added in 802.1Q not 802.3. This means that they aren't part of the basic Ethernet MAC definition, but rather a function of Ethernet bridges. VLAN tags have very little significance in single, unbridged, Ethernet LAN.

<sup>16</sup> Each PEP represents one service or S-VLAN. Each CNP (to which a PEP connects) provides a port-based service (i.e., all frames on the CNP are assumed to be part of the same service).

**Figure 5-8 Architecture of a Provider (and Provider Edge) Bridge**

The packetVX module provides both PB and PEB capability; therefore, it is necessary to configure each switchport to indicate its role in the bridge<sup>17</sup>.

```
> SWITCHPORT gig 1/1/5
> PVID 100
> PORT-TYPE [customerEdgePort | customerNetworkPort
| providerNetworkPort]
> EXIT
```

### 5.6.1 S-VLAN encapsulation

#### S-VLAN encapsulation

Provider bridges create tunnels across the provider network to carry Subscriber Services. Each tunnel carries one service. For Provider Bridges implemented according to IEEE standard 802.1ad, the tunnels are implemented as Service Provider VLANs, which are identified by a Service Provider VLAN (S-VLAN) tag. The S-VLAN tag is contained in a 4-byte field (although the actual tag value is only 12 bits) that is added to each packet to identify which tunnel the packet is in. Proper allocation and use of S-VLAN tags ensures segregation of subscriber traffic within the provider network.

**Note** Since the S-VLAN field is twelve bits long, S-VLAN values can range from 0 to 4095. The supported range is 2 to 4089, since zero is an invalid value, and 1 and 4090 to 4095 are reserved.

Each Service is associated with an S-VLAN tag. The tag is added to the packet before it is transmitted on an NNI, and it is removed before it is transmitted on a UNI. All other aspects of the packet are unchanged — the source and destination addresses, the customer VLAN tags and protocol types, and the user data.

<sup>17</sup> As noted above, most of this configuration is avoided when using the Ethernet Service (ESERVICE) model.

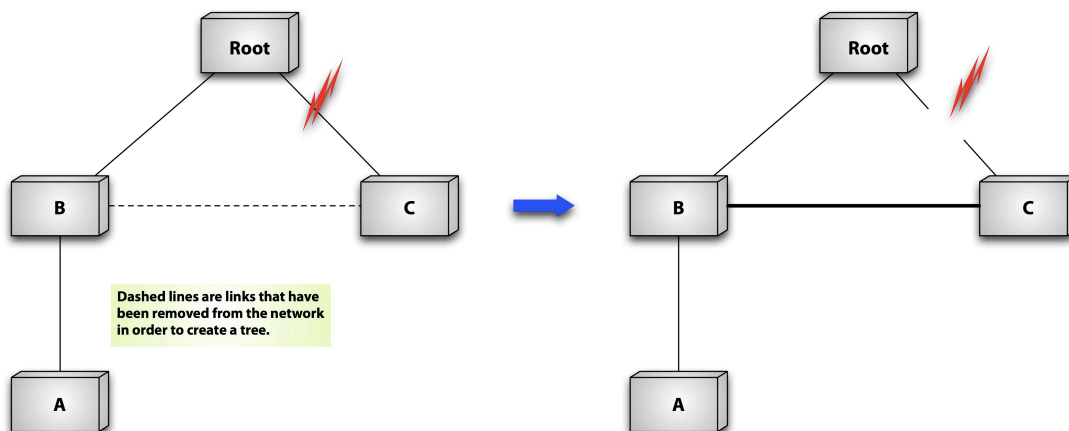
## 5.7 Spanning Tree Protocol (STP, RSTP, and MSTP)

The Spanning Tree Protocol (STP) is a distributed protocol used to dynamically configure a loop-free bridging topology. STP operates through the exchange of protocol messages called Bridge Protocol Data Units (BPDUs) between participating bridges.

The protocol operates by selecting a single bridge to be the root of the spanning tree. The root is chosen to be the bridge with the lowest bridge ID. (The bridge ID is an 8-byte value consisting of a 2-byte settable bridge priority followed by the 6-byte MAC address of the bridge.) The bridge with the lowest bridge ID on each LAN segment is the designated bridge for that segment (the root bridge is, by definition, the designated bridge on each of its attached segments) and on that bridge the port is a designated port. Only the designated bridge transmits BPDUs on a LAN segment. On each bridge, the LAN segment that is closest to the root bridge is called the root port. If a port is not a root port or a designated port (and clearly any given port cannot be both), then it must be part of a loop and is put into a blocking state, logically breaking the loop.

The Spanning Tree Algorithm continually ensures that the tree is spanning the network (i.e., connecting every node). If there is a link failure, the spanning tree algorithm will reconfigure the network to make it whole again (if there are sufficient redundant links to achieve this).

**Figure 5-9 Spanning Tree failure recovery**



The spanning tree starts out with the **B – C** link being blocked. When the failure hits the **Root – C** link, the spanning tree reconfigures to the state on the right, where the **B – C** link is put into service and there is, again, a path between all bridges. If the **Root – C** link recovers, the spanning tree will go back to its initial state (the spanning tree algorithm is always revertive).

### Rapid Spanning Tree Protocol

There are two problems with the Spanning Tree Algorithm originally defined in 802.1D: convergence time and efficient packet routing. One important premise of the STP is that a partition in the network (i.e., lack of connectivity) is better than a loop. Therefore, the algorithm defined a very conservative process that all ports perform before actually forwarding packets. Each time there is a state transition in the network, the affected ports on the affected bridges go through this process. This could take a minute or more, depending on the size of the network.

The solution to the convergence-time problem is the Rapid Spanning Tree Protocol, which is an upward-compatible modification to the original STP.

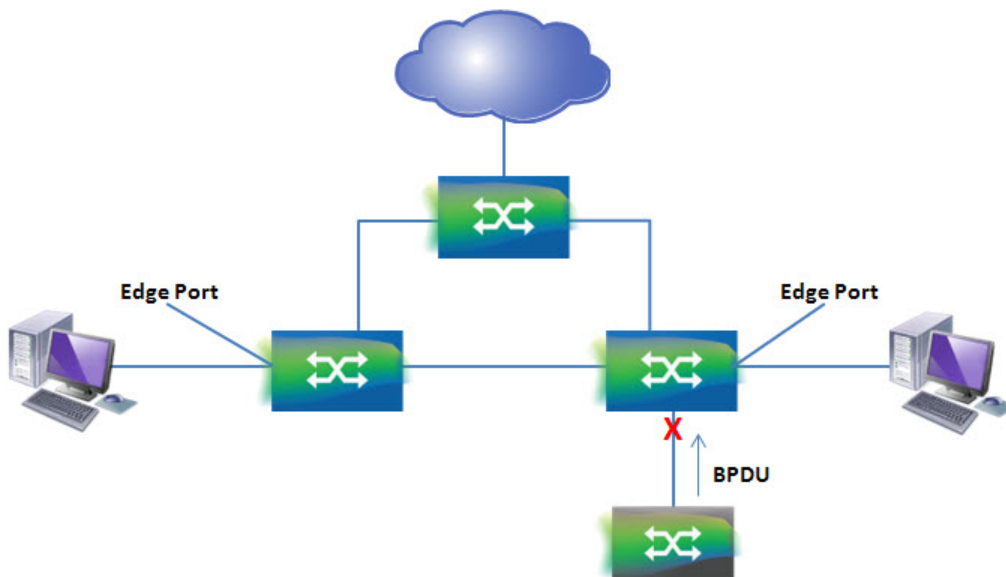
RSTP nodes can interoperate with STP nodes by talking down to them, i.e., reverting to the original STP. RSTP convergence is substantially faster (can be well under a second in some cases) in many configurations. It does this in several ways, but primarily it exploits the fact that ports are not all created equal. For example, ports on the root bridge can transition to forwarding state quickly in most cases. Similarly, ports that are configured to be edge ports (i.e., have no spanning tree peer bridges on them) can transition to forwarding state quickly. Also, the decision process on point-to-point links is much simpler than on shared Ethernet LANs (and most LANs have transitioned to point-to-point links over the past 15 years).

One of the things that makes spanning tree recovery take a long time is the actual detection of a failed link. Ethernet does not inherently provide an indication of a failed link. Other transport systems such as SONET and OTN support line conditioning as part of their basic design. The packetVX modules provide hardware-based link-failure detection to detect failed links faster and initiate recovery sooner.

### BPDU protection

Generally, the port on the access device will be connected to a PC or file server. In this case, the access port can be configured as an edge port to implement rapid transfer on these ports. Normally, there are no spanning tree BPDUs to be transmitted to the edge port; however, malicious attacks might send corrupted packets to the edge port. When enabled, BPDU protection provides a defense against such attacks by shutting down the edge port while the BPDU is being received, as seen in the following figure.

**Figure 5-10 BPDU protection**



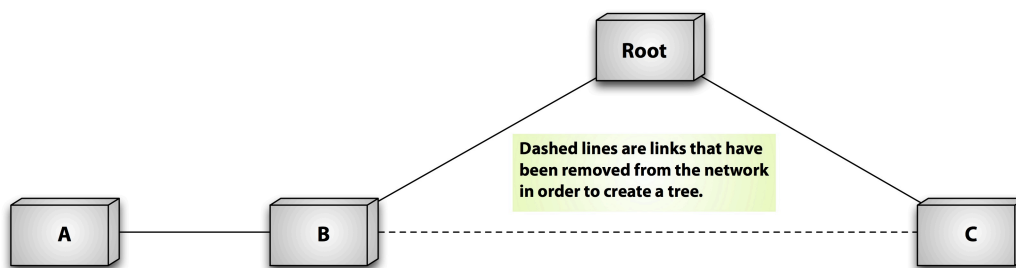
## Multiple Spanning Tree Protocol

The solution to the sub-optimal forwarding issue is the Multiple Spanning Tree Protocol (MSTP).

Forwarding in most contemporary routing systems is along a tree. With IP routing, for example, each router builds a tree to each destination rooted at itself. Therefore, forwarding to each destination is optimal. With the original spanning tree, there is only one tree, rooted at the root bridge, so forwarding from the root is optimal but forwarding between any two bridges may or may not be optimal, depending on where they are relative to the root and what connections exist.

Consider the following figure:

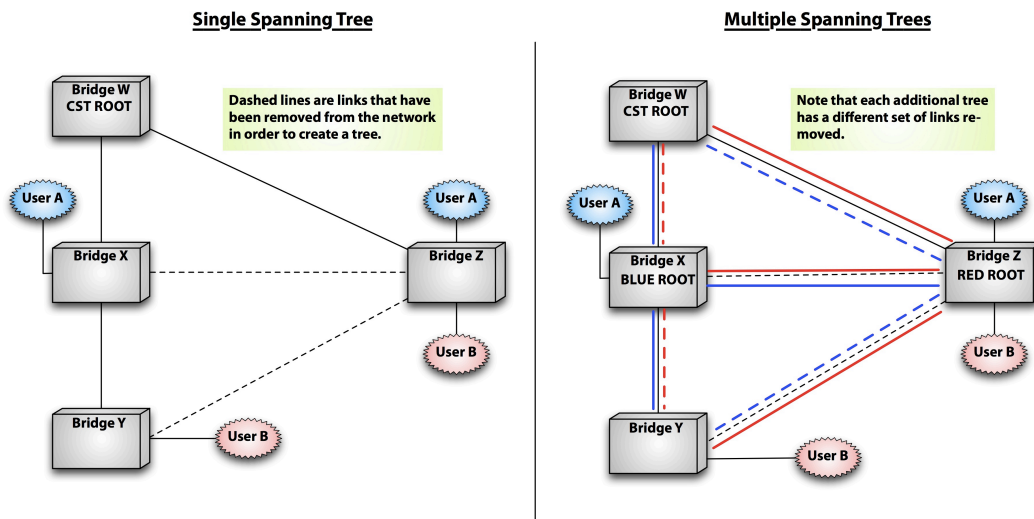
**Figure 5-11 Spanning Tree forwarding**



Forwarding from **A** to **B** is optimal as is forwarding from **A** or **B** or **C** to the root. But forwarding from **A** or **B** to **C** is not optimal since rather than using the direct path from **B** to **C** all of the packets have to go up to the root and back down again. In many networks, especially enterprise networks, this is not a problem. Packet flow tends to be client-server based, so as long as the servers are connected through the root, the vast majority of traffic routing is optimal. In service provider networks where customers are connected in different places, even if the flows are client-server based, it is not possible to ensure that all of the servers are connected to the same root bridge.

MSTP is a VLAN-focused extension of RSTP<sup>18</sup>, providing the ability to create multiple spanning trees and assign VLANs to spanning trees that most closely reflect their optimal forwarding paths. MSTP provides a single Common Spanning Tree Instance (CSTI), which is automatically created, and reflects the RSTP without multiple spanning tree support, and Multiple Spanning Tree Instances (MSTIs) that are configured to meet varied forwarding requirements.

<sup>18</sup> RSTP was added as an update to 802.1D in 2004 whereas MSTP is standardized in 802.1Q.

**Figure 5-12 Multiple Spanning Trees**

```

> SPANNING-TREE MST CONFIGURATION
> INSTANCE 3 VLAN 1-50 ! e.g. BLUE INSTANCE
> INSTANCE 4 VLAN 100 ! e.g. RED INSTANCE
> NO INSTANCE 2 ! delete previous spanning tree
> EXIT

```

Once the spanning tree has been defined, parameters can be applied to achieve the correct operation. For example, for the red spanning tree, Bridge **Z** must become the root. The best way to achieve this is to reduce its priority value (remember lower priority value means higher priority).

```

> SPANNING-TREE 4
> PRIORITY 4K ! range is 0 to 60K in 4K increments
> EXIT ! default is 32K

```

In the packetVX module, MSTP operates only on NNIs (switchports configured as Provider Network ports). On UNIs, if the Layer 2 Control Protocol profile is set to peer for spanning tree, the Ethernet Service peers with a private instance of RSTP. In other words, the packetVX module creates a private rapid spanning tree (common instance) for each Eservice that is peering a spanning tree.

### 5.7.1 MSTP provisioning

This procedure explains how to provision Multiple Spanning Tree Protocol (MSTP) for the switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### PrerequisitesPrerequisites

A virtual switch must be created and a packetVX must be added as a member. See [4.2.1, “Create a virtual switch”](#) and [4.2.2, “Add a member to a virtual switch”](#)

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

## **Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

## **Step 3 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

## **Step 4 Navigate to the desired port.**

```
BTI7000:sw1(config)# nni <gigabitEthernet |  
                        tenGigabitEthernet <shelf/slot/port> | <lag> <lag number>
```

```
BTI7000:sw1(config-nni TenGigE 1/1~)# spanning-tree 0
```

## **Step 5 Modify port attributes as required.**

```
BTI7000:sw1(config-nni TenGigE 1/1~)# cost <cost>
```

```
BTI7000:sw1(config-nni TenGigE 1/1~)# port-priority <priority> (0 to  
240 in increments of 4)
```

```
BTI7000:sw1(config-nni TenGigE 1/1~)# port-state <disable | enable>
```

### **CLI Command Example**

```
nni tenGigabitEthernet 1/1/1
```

```
spanning-tree 0
```

```
cost 1000
```

```
exit
```

```
exit
```

## **Step 6 Navigate to port CIST level.**

You have successfully completed this procedure.

## 5.7.2 Loop Guard

As part of MSTP, Loop Guard provides extra protection against potential STP forwarding loops on NNI ports or LAGs. These loops may be created when an STP blocking port transitions, erroneously, to the forwarding state when scheduled BPDUs are not received.

By performing extra checks, the Loop Guard feature ensures that the relevant STP port remains in a discard state under relevant conditions, to avoid a potential forwarding loop.

The port remains in a discard state if:

- BPDUs reception is not resumed, and there are no STP status changes on other STP ports on the same bridge; Or,
- STP status changes, on other STP ports, do not trigger the blocking port to transition to a forwarding state.

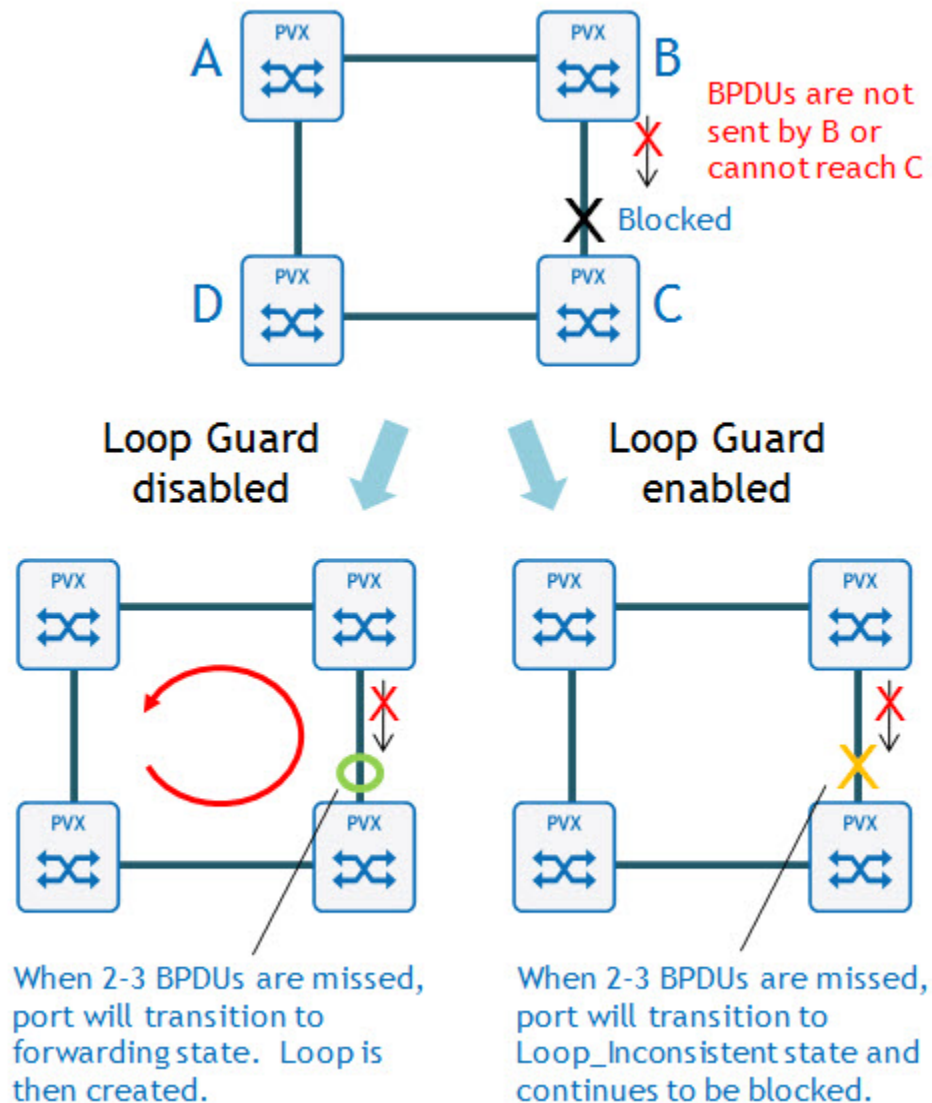
The port transitions to a forwarding state if:

- BPDUs reception is resumed and newly received BPDUs transition blocking ports to a forwarding state; Or,
- STP status changes on other STP ports force the local STP to transition to a forwarding state.

<b>Note</b>	An STP port may be shared by multiple MSTP instances. Loop Guard control, on a port, affects all MSTP instances configured on this port.
-------------	--

BTI Loop Guard functionality is illustrated in the following figure:



**Figure 5-13 Loop Guard Functionality**

When Loop Guard is enabled on an NNI port (non-designated), the port transitions to a loop-inconsistent state instead of moving to the listening/learning/forwarding states when two or three BPDUs are missed.

Loop Guard is enabled or disabled on a per-NNI port or LAG basis, using the CLI or the proNX 900 Node Controller. Refer to 5.7.4, “Configuring packetVX loop guard” or A.12.4, “Provision or modify CIST port settings”. By default, Loop Guard is disabled.

### 5.7.3 Loop Guard configuration considerations

On which ports to configure Loop Guard is dependent on the particular network environment. Consider configuring Loop Guard on ports on which failovers are likely to occur. To determine

if loop guard should be enabled or disabled, consider the following port behavior based on the configuration:

- **Enable:** The network performs extra checks to ensure that the STP port does not transition to a forwarding state, when BPDU reception is resumed, and prevents newly received BPDUs from transition blocking ports to a forwarding state.
- **Disable:** The Loop Guard feature ensures that the relevant STP port remains in a discard state under relevant conditions, to avoid a potential forwarding loop.

The port remains in a discard state if:

- BPDU reception is not resumed, and there are no STP status changes on other STP ports on the same bridge; Or,
- STP status changes, on other STP ports, do not trigger the blocking port to transition to a forwarding state.

The port transitions to a forwarding state if:

- BPDU reception is resumed and newly received BPDUs transition blocking ports to a forwarding state; Or,
- STP status changes on other STP ports force the local STP to transition to a forwarding state.

## 5.7.4 Configuring packetVX loop guard

This procedure explains how to enable or disable Loop Guard on an NNI port, on the packetVX. By default, Loop Guard is disabled.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- To enable/disable Loop Guard follow these steps:

**Step 1** Select the virtual switch that contains the NNI interface that you are configuring. The virtual switch can be selected from **EXEC** or global configuration mode. The following example selects virtual switch 1 from **EXEC** mode:

```
BTI7000> enable
BTI7000# virtual-switch 1
BTI7000:sw1#
```

**Step 2** Enter configuration mode for the NNI interface that is being configured. This example configures the NNI 10 gigabit Ethernet interface on shelf 1/slot 1/port 2:

```
BTI7000:sw1# configure terminal
BTI7000:sw1(config)# nni tenGigabitEthernet 1/1/2
BTI7000:sw1(config-nni TenGigE 1/1~)# spanning-tree 0
BTI7000:sw1(config-nni TenGigE 1/1~)#
```

**Step 3** Enable Loop Guard on the port:

```
BTI7000:sw1(config-nni TenGigE 1/1~)# loop-guard enable
BTI7000:sw1(config-nni TenGigE 1/1~)#
```

**Step 4** Disable Loop Guard on the port:

```
BTI7000:sw1(config-nni TenGigE 1/1~)#loop-guard disable  
BTI7000:sw1(config-nni TenGigE 1/1~)#
```

**Step 5** Display the configuration. This example shows loop guard enabled :

```
BTI7000:sw1(config-nni TenGigE 1/1~)# show  
Switch: 1, Shelf: 1, Slot: 1, Port Type: GigEX, Port: 2  
  Designated Root is 00:14:d0:30:2e:80  
  Designated Bridge is 00:14:d0:30:2e:80  
  Designated Port is 17  
  Path Cost is 2000  
  Port Priority is 128  
  Port State is Discarding  
  Port Role is Disabled  
  Regional Root is 00:14:d0:30:2e:80  
  Regional Root Cost 0  
  Restricted Role is Disabled  
  Restricted TCN is Disabled  
  Forced Port State is Enabled  
  Loop Guard State is Enabled  
  
BTI7000:sw1(config-nni TenGigE 1/1~)#
```

You have successfully completed this procedure.

## 5.8 Storm Control

The BTI™ packetVX provides Layer-2 storm protection to maintain network performance during periods of excessive traffic. Storm Control is supported on configured, ingress NNI ports on a per-port basis, and on NNI LAGs, for the following L2 packet types:

- Broadcast
- Multicast
- Unicast DLF (destination lookup fail)

Operators have the ability to set BTI pre-defined, traffic line rate limits on NNI ports and LAGs. For LAGs, a limit allocated for a LAG instance is distributed across its member interfaces.

The operator uses a percentage value to configure the rate limits, for each packet type. Automatically, the percentages are converted to packets-per-seconds (pps) on the BTI 7000 Series modules. Refer to the following table for the pre-defined rate limits and pps conversion information, which is based on an average frame size of 1,000 bytes:

**Table 5-17 Storm Control Rate Limiting Levels**

Line Rate	Limit in Percentage of Line Rate	Limit in Packets Per Second
1 Gbps	60	75,000
	40	50,000
	20	25,000
10 Gbps	60	750,000
	40	500,000
	20	250,000

When the limit is reached on a packet type, additional incoming packets are dropped, which avoids an adverse impact on network performance. For example, if the broadcast limit is set to 40% (50,000 packets-per-second) and the receiving rate is 62,000 pps, only 50,000 pps of the broadcast traffic is forwarded and 12,000 pps is discarded.

By default, Storm Control is disabled, with the rate limit set to 100%. Storm Control allocation can be enabled and modified using the CLI command, **storm-control**, or using the proNX 900:

- To modify Storm Control limits using the CLI, refer to [5.8.3, “Configuring packetVX storm control”](#)
- To modify Storm Control limits using the GUI, refer to [A.2.2.1, “Using the E-services model to provision a UNI, NNI or E-NNI on an Ethernet switch”](#)

Storm Control is not supported on UNI ports. Traffic flow on UNI ports is supported by traffic settings configured in the bandwidth profile applied to the UNI port. Refer to [8.3, “Bandwidth profiles and traffic policing”](#) for additional information on configuring and applying bandwidth profiles on a UNI port.

### 5.8.1 Storm Control on NNI ports

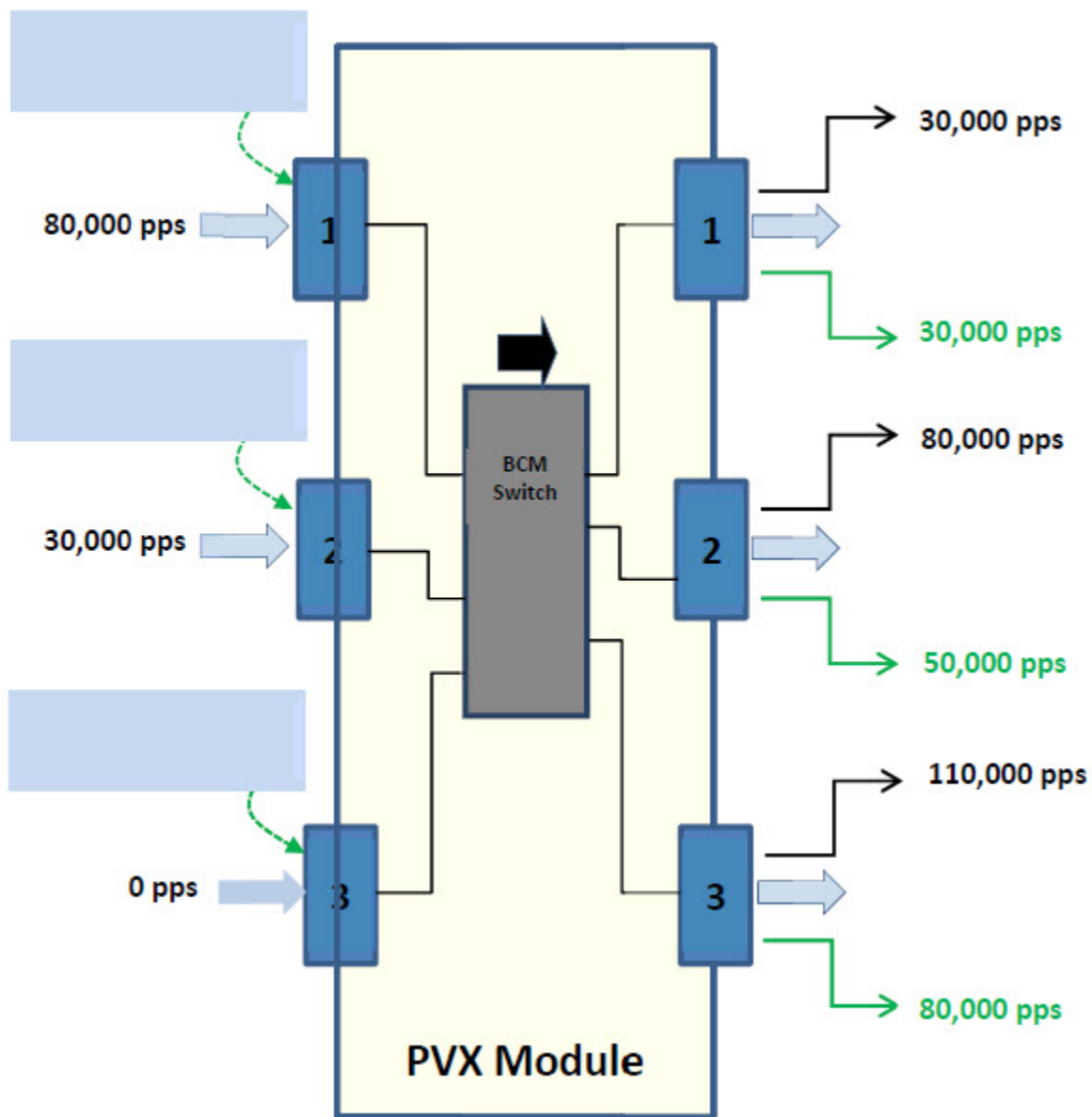
Storm Control functionality on NNI port is illustrated in the following figure. This example shows three NNI ports on one packetVX. Two Broadcast traffic flows are injected on Port-1 and Port-2 ,respectively, while no inbound traffic is on Port-3.

- Port-1: 80,000 pps
- Port-2: 30,000 pps

Egress traffic on all three ports is monitored. Assume Storm Control limits are configured as:

- Port-1: 40%
- Port-2: 60%
- Port-3: 20%

**Figure 5-14 Storm Control Functionality on NNI Ports**



The following table compares NNI ports traffic flow rates with and without Storm Control.

**Table 5-18 NNI Ports rate limiting levels**

NNI Port	Traffic Flow Rate		Comments
	Without Storm Control	With Storm Control	
Port-1	30,000 pps	30,000 pps	Egress traffic comes from port-2.
Port-2	80,000 pps	50,000 pps	Egress traffic comes from port-1.

**Table 5-18 NNI Ports rate limiting levels (Continued)**

NNI Port	Traffic Flow Rate		Comments
Port-3	110,000 pps	80,000 pps	Egress traffic comes from both ports-1 and -2.

## 5.8.2 Storm Control on NNI LAGs

Storm Control functionality on a typical NNI LAG is illustrated in the figure below. This example is based on the following assumptions and configurations:

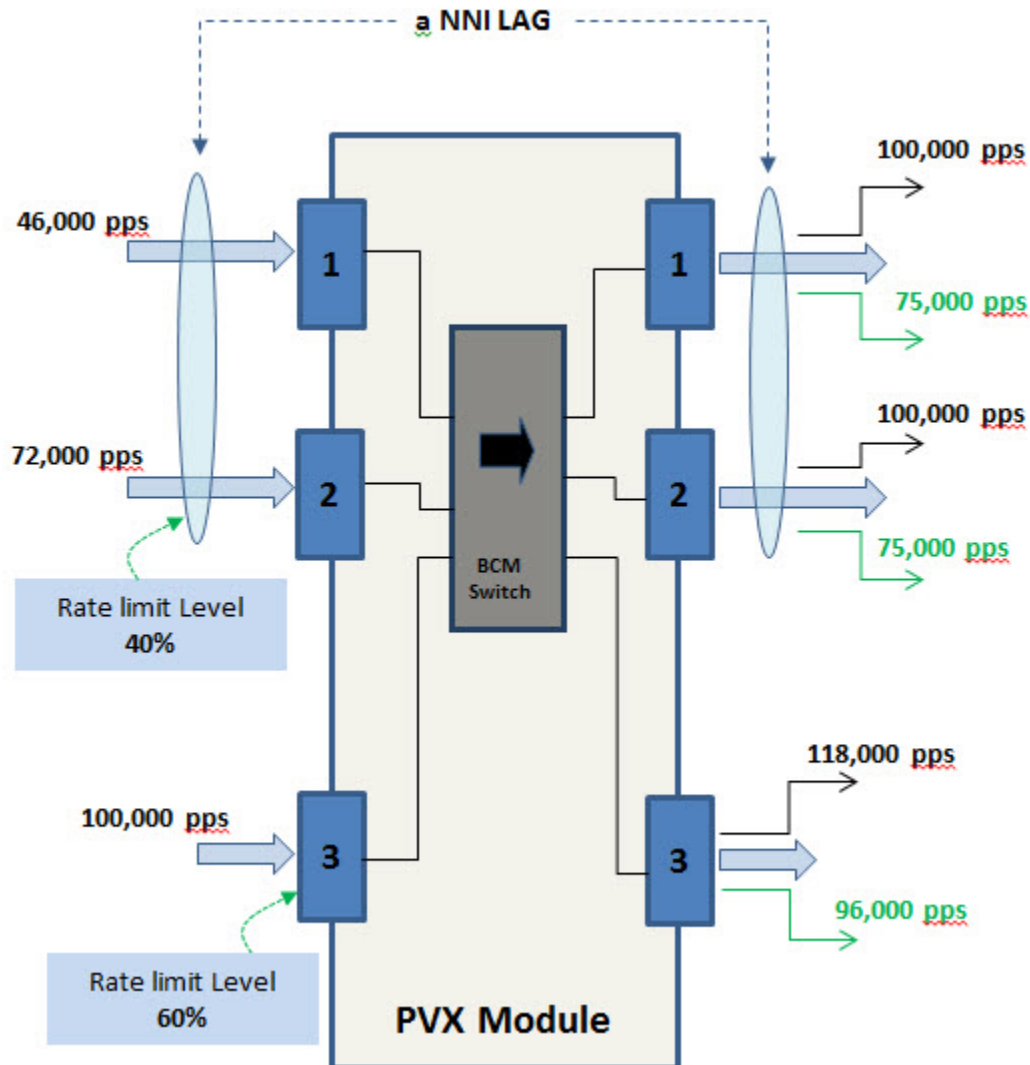
- All ports are GbE ports.
- One NNI LAG is configured with the max number of allowable interfaces as “2”.
- Ports-1 and -2 are configured as two interfaces and attached to the LAG.
- Port-3 is an independent NNI port.

Broadcast packets are injected on all three ports with the following rates:

- Port-1: 46,000 pps with a frame size of 1,100 bytes
- Port-2: 72,000 pps with a frame size of 1,100 bytes
- Port-3: 100,000 pps with a frame size of 1,100 bytes

Egress traffic on all three ports is monitored. Assume Storm Control limits are configured as:

- LAG: 40%
- Port-3: 60%

**Figure 5-15 Storm Control Functionality on NNI LAGs**

The following table compares NNI LAGs traffic flow rates with and without Storm Control.

**Table 5-19 NNI LAGs rate limiting levels**

NNI	Traffic Flow Rate		Comments
	Without Storm Control	With Storm Control	
Port-1	100,000 pps	75,000 pps	Egress traffic comes from port-3
Port-2	100,000 pps	75,000 pps	Egress traffic comes from port-3
Port-3	118,000 pps	96,000 pps	Egress traffic comes from both port-1 and port-2

A traffic rate limit allocated for a LAG instance is distributed and applied to all its member interfaces.



### 5.8.3 Configuring packetVX storm control

This procedure explains how to configure Storm Control, to allocate traffic rate line limits on NNI ports and LAGs, on the packetVX. By default, Storm Control is disabled on configured NNI ports and LAGs .

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- To configure Storm Control follow these steps:

**Note** This procedure assumes an NNI port and LAG interface exist. If an NNI interface needs to be created, refer to [6.1.2.2, “Sample NNI configuration”](#) for information about defining an NNI.

- Step 1** Select the virtual switch that contains the NNI interface that you are configuring. The virtual switch can be selected from **EXEC** or global configuration mode. This example selects virtual switch 1 from **EXEC** mode:

```
BTI7000> enable
BTI7000# virtual-switch 1
BTI7000:sw1#
```

- Step 2** Enter configuration mode for the NNI interface that is being configured. This example configures the NNI 10 gigabit Ethernet interface on shelf 1/slot 1/port 2:

```
BTI7000:sw1# configure terminal
BTI7000:sw1(config)#nni tenGigabitEthernet 1/1/2
BTI7000:sw1(config-nni TenGigE 1/1~)#
```

- Step 3** Set the Storm Control rate limit. This examples configures Storm Control on the broadcast, multicast, and unicast packets:

```
BTI7000:sw1(config-nni TenGigE 1/1~)#storm-control broadcast 60
BTI7000:sw1(config-nni TenGigE 1/1~)#storm-control multicast 20
BTI7000:sw1(config-nni TenGigE 1/1~)# no storm-control unicast
BTI7000:sw1(config-nni TenGigE 1/1~)#
```

**Note** When MAC learning is disabled, we recommend that a low threshold, or preferably, no threshold is set in this type of network environment.

- Step 4** Display the configuration. This example shows only the portion of the output that includes the Storm Control configuration:

```
BTI7000:sw1(config-nni TenGigE 1/1~)# show
Storm-control:
  broadcast: 60%
  multicast: 20%
  unicast-dlf: disabled
```

You have successfully completed this procedure.

## 5.9 GVRP

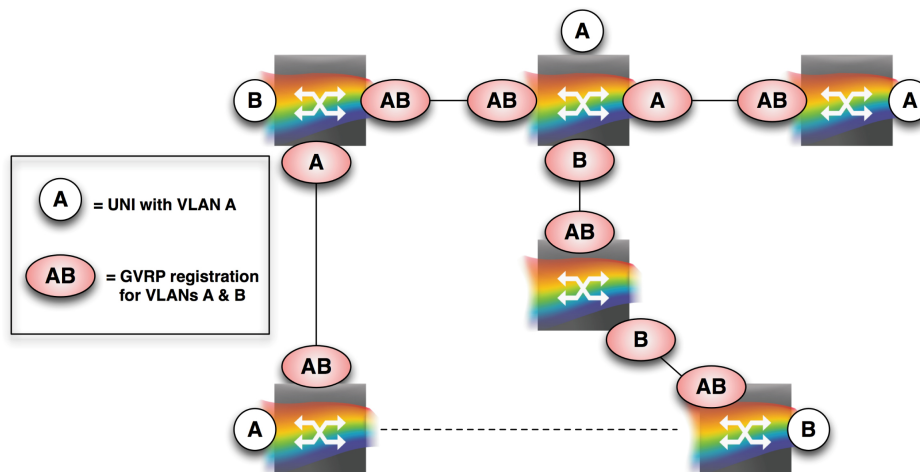
The Generic Attributes Registration Protocol (GARP) is defined in 802.1D as a means for bridges to distribute information amongst themselves about membership in various *groups*. 802.1D defines GMRP (GARP Multicast Registration Protocol) to distribute multicast group membership. 802.1Q defines GVRP (GARP VLAN Registration Protocol) to distribute information about VLAN membership.

GVRP addresses the problem of determining which inter-bridge links (NNIs) must be members of which VLANs. In a VLAN-bridge, packets in VLAN *x* can only be transmitted on links that are members of VLAN *x*. VLAN *x* subscriber interfaces (UNIs) are manually configured, but it can be cumbersome to define a VLAN member for all VLANs across all NNIs<sup>19</sup>. One fall-back would be to simply define all VLANs on NNIs, but this means that all flooded packets will be flooded everywhere, which is a large waste of bandwidth.

GVRP, in effect, advertises VLAN membership backwards through the network. If a node must receive packets in VLAN *x*, it sends a registration for VLAN *x* to all of its neighbors. Each of those neighbors adds the receiving link to VLAN *x* and then forwards a registration to all of its neighbors.

Consider the following figure:

**Figure 5-16 GVRP-based VLAN registration**



The end points (circles) for VLANs A and B are defined by the network manager. As the bridges with these end points begin advertising their end points, VLAN membership is automatically added to the inter-bridge links (ovals).

VLAN membership is added to a port based on received GVRP registrations not transmitted registrations. For example, the lower left bridge in the figure has registered A on its NNI link not because it has a subscriber interface for A but because it has received a registration for A on the

<sup>19</sup> Imagine a network with a few thousand subscriber services (S-VLANs) and 20 or 30 NNIs and a half dozen alternative paths (spanning tree). Getting the VLAN membership right would be both cumbersome and error prone.

link – that is, we need to send packets for VLAN A (and in this case, B also) on the link because there are VLAN A subscribers that are accessible through the link.

The result is the minimum number of VLAN memberships. This is important to limit packet flooding. Packet flooding within a VLAN is done to only the links that are in the VLAN. So ensuring that VLAN membership is minimized also ensures that flooding is minimized.

VLAN registration is refreshed regularly and especially after a spanning tree topology change.

There are two configuration options associated with GVRP. GVRP can be enabled and disabled on a switchport basis. If GVRP is disabled, no registrations will be sent on the link and received registrations will be dropped.

```
> SWITCHPORT gig 1/1/17
> GVRP DISABLE ! default is ENABLE
> EXIT
```

It is also possible to avoid having a specific NNI become a member of a particular VLAN even if a GVRP registration is received.

```
> VLAN 122
> FORBID NNI tenG 1/1/3
> EXIT
```

Any registration request received on tenG 1/1/3 for VLAN 122 will be ignored. It will never be a member of VLAN 122.

## 5.10 Link Layer Discovery Protocol

---

This section describes how the Link Layer Discovery Protocol (LLDP) is implemented on the BTI packetVX.

LLDP is a protocol that provides transmission and receipt of physical topology information between the packetVX and other BTI packet devices, such as the 700-series and SA-810, and other network devices that are attached to the same IEEE 802 local area network (LAN):<sup>20</sup>

### packetVX implementation of LLDP

LLDP is managed on a per port basis using SNMP or the CLI, or the BTI proNX Service Manager. Each network element can determine its immediate Ethernet neighbors from the chassis and port IDs discovered through LLDP. An Ethernet topology can then be built with this information.

### LLDP implementation guidelines

- LLDP assumes that a physical port is connected to a switch as a point-to-point link.
- The TLV (type-length-value) format is used to support the following configurable properties: Chassis ID, Port ID, and Time-to-Live.
- By default, LLDP is enabled on all NNI interfaces and disabled on UNI interfaces. The default LLDP role for a mirror-to-port is disabled:
  - When enabled, the port transmits and receives LLDP packets.
  - When disabled, the port does not process any LLDP packets.
- LLDP packets are tunneled across an EPLINE when ingressing the Service UNIs.
- If a UNI is carrying any eService other than EPLINE, LLDP packets arriving on the port are discarded.
- Tunneled LLDP packets are carried over the multicast MAC address: 01-00-0c-cd-cd-d5. To change the MAC address profile use the command **lldp** <String>, from Profile Tunnel-MAC-Address mode.
- Provisioning LLDP is accomplished using the packetVX CLI, proNX 900 Node Controller, and SNMP interfaces.
- A virtual switch is identified as a Bridge ID, within the Chassis ID; however, the Bridge ID is not supported as a configurable LLDP property.
- LLDP is not intended to be a network configuration or signaling tool.
- When a change is made in a remote database, the packetVX advertises this change event within ten seconds.
- SNMP support: The **packetVX-bridge.my** MIB provides the LLDP management information.

<sup>20</sup> IEEE Std 802.1AB™-2005.

## 5.10.1 LLDP Configuration

This section describes the packetVX CLI commands that support LLDP. For more information about these commands refer to the *BTI 7000 Series packetVX Command Line Reference Guide*.

### Enabling/Disabling LLDP

To change the port role for LLDP participation, use the command **lldp** <enabled | disabled>, from Ethernet interface configuration mode. The following example enables port 1/1/1 to transmit and receive LLDP frames:

```
BTI7000:sw1(config-if TenGigE 1/1/1)# lldp enabled
BTI7000:sw1(config-if TenGigE 1/1/1)#
```

### Examples of the show commands

The following output of the **show interface** command shows the physical interface information:

```
BTI7000# show interfaces tenGigabitEthernet 1/3/2

TenGigE 1/3/2
  State is IS-NR
  fiber type is none, wavelength is 1310
  Line Mapping is 10ge-lanphy
  Error Correction is none
  MTU 9600 bytes
  MAC Address is 00-14-d0-32-08-0d
  Flow control configured as auto, Flow control status is off
  Full-duplex, 10000Mb/s
  loopback is off
  phyPmMon is disabled
  Mirroring Configuration: none
  LLDP is enabled
    Neighbor Port:
      System Name: BTI_160_2
      Chassis Id 00:14:d0:32:db:40
      Port Id Xgig1/13/2
  Signal Degrade BERT is none
  OPR threshold (Min: -12.2, Max: 2.5)
  OPT threshold (Min: -7.9, Max: 0.9)
  SES Level is 0
.
.
.
  transmit utilization (current bin = 228 seconds) 0.0%
BTI7000#
```

The following portion of the **show running-configuration** command shows that interface 1/1/1 is participating in LLDP:

```
!
interface tenGigabitEthernet 1/1/1
  admin-state enable
  circuit-id
```

```

lldp enabled
loopback facility off
mtu 9600
.
.

```

The following output of the **show lldp neighbors** command provides current LLDP configuration and information learned by the system:

VS Type	Port	Admin		Remote Port Information		
		State	System	ChassisId	PortId	
1 GigE	1/1/1	enabled	ClayFace	00:14:d0:31:c8:c5	Gig21/1/1	
1 GigE	1/1/2	enabled	ClayFace	00:14:d0:31:c8:c5	Gig21/1/2	

The following output of the **show profile l2control** command shows the LLDP profiles on the Eservices:

Profile Name	Dot1x	GMRP	GVRP	LACP	STP	LLDP
DEFAULT_CEP_PROFILE	peer	discard	discard	peer	discard	discard
DEFAULT_CNP_PROFILE	peer	tunnel	tunnel	peer	tunnel	tunnel
DEFAULT_UNI_PROFILE	peer	discard	discard	peer	discard	discard
DEFAULT_EPLAN_PROFILE	discard	tunnel	tunnel	discard	tunnel	discard
DEFAULT_EPLINE_PROFILE	tunnel	tunnel	tunnel	tunnel	tunnel	tunnel
DEFAULT_EVP_ALL_PROFILE	discard	discard	discard	discard	discard	discard
DEFAULT_EVP_UNI_LAG_PROFILE	peer	discard	discard	peer	discard	discard

The following output of the **show profile tunnel-mac-address** command shows the MAC address profile of the LLDP packets:

```
BTI7000# show profile tunnel-mac-address
```

```

Tunnel MAC Address Profile: DEFAULT_TMA_PROFILE
Dot1x Tunnel MAC Address: 01-00-0c-cd-cd-d3
GMRP Tunnel MAC Address: 01-00-0c-cd-cd-d2
GVRP Tunnel MAC Address: 01-00-0c-cd-cd-d1
LACP Tunnel MAC Address: 01-00-0c-cd-cd-d4
STP Tunnel MAC Address: 01-00-0c-cd-cd-d0
LLDP Tunnel MAC Address: 01-00-0c-cd-cd-d5

```

## 5.11 Forwarding database provisioning

The packetVX employs a forwarding database (FDB). The FDB can contain both address entries and VLAN entries, either or both of which can be used to limit the forwarding of a packet to fewer than "all ports"—usually none or one for a unicast packet.

### MAC address learning

All received packets are forwarded everywhere, or flooded, unless forwarding is restricted by entries in the forwarding database. Media Access Control (MAC) addresses are learned by the FDB.

### MAC address aging

When the MAC address learning feature is enabled, the FDB entries "age out" according to the value set for the aging timer. The aging timer for a particular FDB entry (that is, a source MAC address) is reset when it is learned or relearned.

To set the MAC address aging timer, see [5.11.1, “Setting the MAC address aging timer”](#).

### Static MAC addresses

Static filtering controls allow the network administrator to impose a level of control over the permitted connectivity in the network, by setting static MAC Address filters in the FDB.

To add or remove a static unicast or multicast entry in the MAC Address table for the currently selected switch, see [5.11.2, “Adding and removing static MAC addresses”](#).

### 5.11.1 Setting the MAC address aging timer

Use this procedure to set the Media Access Control (MAC) address aging timer for the switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- Create a virtual switch.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Global Configuration mode

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Enter the mac-address-table aging-timer command syntax

To set the MAC address aging timer, enter the following command:

```
[no|default] mac-address-table aging-time [<time>]
```

where <time> is the aging timer value from 1 to 604800 seconds. (300 seconds is the default value.)

If `mac-address-table aging-time 600` is entered, the MAC aging timer is set for 10 minutes duration.

If `default mac-address-table-aging time` is entered, the MAC aging timer is set for 5 minutes duration.

If no `mac-address-table aging-time` is entered, the MAC address aging timer is disabled.

You have successfully completed this procedure.

## 5.11.2 Adding and removing static MAC addresses

Use this procedure to add or remove a static unicast or multicast entry in the Media Access Control (MAC) Address table for the currently selected switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- The switchport and vlan need to be created.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```



The CLI prompt should now appear as follows:

```
BTI7000#
```

## Step 2 Access the Global Configuration mode

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

## Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

## Step 4 Enter the mac-address-table static command syntax

To add or remove static MAC addresses, enter the following command:

```
[no] mac-address-table static {unicast|multicast} <mac-addr> vlan  
<vlan-id> switchport <interface-type> <interface-id>
```

**Note** For variable parameter ranges and default values, see the *BTI 7000 Series \$Command Line Interface Reference Guide*.

If `mac-address-table static unicast 12-34-56-78-9a-bc vlan 1 switchport tenGigabitEthernet 1/2` is entered, a static unicast MAC address of 12-34-56-78-9a-bc associated with VLAN 1, a 10 GbE interface, located in shelf one, slot two is added to the MAC Address table.

You have successfully completed this procedure.

## 5.12 Viewing the configuration of a switch

---

This procedure describes how to display the configuration of a switch as a list of CLI commands. In general, only commands that change the configuration from the default value are displayed, unless the include-defaults option is specified.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- None

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Display the system configuration for the switch

To display the system configuration, enter the following command:

```
show running-config [include-defaults]
```

For example, the command string might be

```
BTI7000# show running-config
equipment 1 pec BT7A50AA
  admin-state enable
  exit
equipment 1/1 pec BT7A81AA
  admin-state enable
  custom-1 one
  custom-2 two
  custom-3 three
  exit
equipment 1/5 pec BT7A20CA
  admin-state enable
  exit
equipment 11 pec BT7A50AA
  admin-state enable
  shelf-config 3
  exit
equipment 11/1 pec BT7A81AA
  admin-state disable
  exit
```

You have successfully completed this procedure.

## 5.13 Station loopback

Station loopback provides the ability for the operator to verify the integrity of links across a network.

When a station loopback is started on a switch, the switch loops back certain specified traffic based on configured match criteria. The match criteria are specified in a class map associated with the station loopback instance.

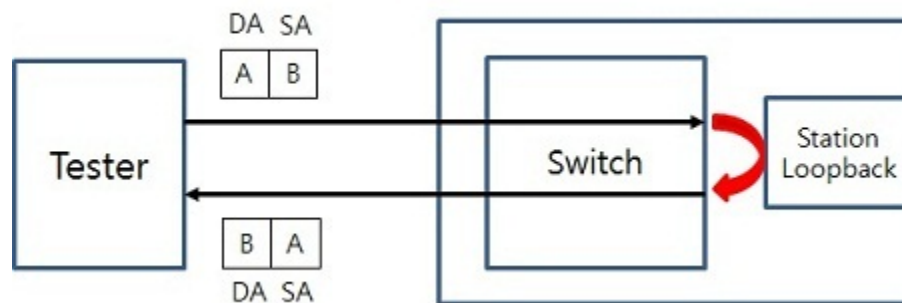
All incoming frames that match the criteria in the class maps for all active station loopback instances are looped back.

Station loopback applies at the switch level. When a station loopback is started, all ports on the switch participate and examine incoming frames for matches. Frames that match are looped back on the port on which they are received. The switch swaps the MAC DA and SA, and recalculates the CRC before sending the frame back.

As a configurable option, packetVX records the MAC address pairs (DA and SA) of frames that are looped back, as follows:

- The last 10 MAC address pairs of the frames looped back.
- The last 10 unique MAC address pairs of the frames looped back.

The BTI 7000 Series station loopback feature is supported in hardware (FPGA), and interoperates with any vendor setup.



The following are the characteristics of this feature:

- Station loopback is supported on all packetVX modules.
- Up to 128 station loopback instances can be active at the same time, up to a 1 Gbps capacity.
- Only unicast frames are looped back. Multicast and broadcast frames are not looped back.
- Ethernet service OAM messages are not looped back at the UNI nodes.
- Ethernet service OAM messages may be looped back at intermediate nodes depending on MD level configuration.
- Station loopback can co-exist with loss and delay measurement tests, but cannot co-exist with SLA throughput tests. Before starting station loopback, you must first disable all SLA throughput tests.

- On the packetVX 24/2 and 24/4 modules, when station loopback is enabled, you cannot use port 24. The resources associated with port 24 are used for station loopback on these modules. Conversely, if you are using port 24, you must not enable station loopback on the switch.

### 5.13.1 Configuring a station loopback

**Step 1** Enable station loopback on the switch. For example:

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# station-loopback enable
```

**Step 2** Create the class map for matching the incoming frames. For example:

```
BTI7000:sw1(config)# class-map cvlan200 type ingress-cos
Profile "cvlan200" created.
BTI7000:sw1(config-c-map)# match c-vlan 200
BTI7000:sw1(config-c-map)# exit
```

**Step 3** Create a station loopback instance. For example:

```
BTI7000:sw1(config)# station-loopback instance-name s100c200 s-vlan
100 class-map cvlan200
```

**Step 4** Start the station loopback. For example:

```
BTI7000:sw1(config)# station-loopback instance-name s100c200 start
```

**Step 5** Display the station loopback status. For example:

```
BTI7000:sw1(config)# show station-loopback
virtual switch id : 1
station loopback is enabled

-----
Instance name          SVLAN Class-map          Status
-----
s100c200               100   cvlan200             active
-----
```

**Step 6** Display the results of the loopback.

```
BTI7000:sw1(config)# show station-loopback statistics
Virtual Switch: 1

-----
MAC Record      :                               Enable
-----
MAC SWAP CNT   : RX              0 : TX              0
-----
:              DA              :              SA
: 00:00:00:00:00:00 : 00:00:00:00:00:00 :
: 00:00:00:00:00:00 : 00:00:00:00:00:00 :
: 00:00:00:00:00:00 : 00:00:00:00:00:00 :
Last 10         : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
MAC-swapped     : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
```

```
Frames      : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
-----
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
10 Unique    : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
MAC-swapped  : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
Frames       : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
              : 00:00:00:00:00:00 : 00:00:00:00:00:00 :
-----
```



## 6.0 Configuring Ethernet services

---

Provider Bridging is about providing well defined services to a multitude of individual subscribers. Rather than being somewhat ill-defined, as in an enterprise network, traffic flows are defined and are expected to flow between specific switching ports. Performance metrics are defined and measured. Segregation of traffic for security is critical.

The BTI<sup>TM</sup> packetVX<sup>®TM</sup> is designed for provisioning well-defined Ethernet services (Eservice) to subscribers. Switches and ports are configured in terms of the services that they provide. The supported service types are defined based on the Metro Ethernet Forum (MEF) definitions<sup>21</sup>. There are three basic types of services:

- **Ethernet Line or E-LINE Services:** These are services that define a point-to-point traffic flow, i.e., a traffic flow between exactly two user ports in the network.
- **Ethernet LAN or E-LAN Services:** These are services that define multipoint-to-multipoint traffic flow, i.e., traffic flow between multiple user ports (two or more) in the network.
- **Ethernet Tree or E-TREE Services:** These are services that define point-to-multipoint traffic flow, i.e., traffic flow between a set of user leaf ports and one or more root ports. Traffic does not flow directly between leaf ports.

Each service is further divided into *Private* and *Virtual Private* services, based on whether a port (UNI) is shared with other services or not. In addition, two internal capabilities are modeled as Eservices, the management VLAN service (mgmtVLAN), and the Ethernet Ring Protection Service, G.8032 (ERPS). Configuration of these services is very much like configuration of the subscriber services but there are several additional parameters and rules associated with them, which are also discussed in this guide.

This section covers the following topics:

- [6.1, “UNIs, NNIs and E-NNIs”](#)
- [6.1.1, “External Network to Network Interface \[E-NNI\]”](#)

<sup>21</sup> Metro Ethernet Forum Technical Specification MEF6-1 Ethernet Services Definition - Phase II

- 6.1.2, “Sample UNI, NNI and E-NNI configurations”
- 6.2, “Ethernet services”
- 6.3, “Ethernet services provisioning”
- 6.4, “Provisioning profiles”



## 6.1 UNIs, NNIs and E-NNIs

---

There are three types of *switchports* associated with Eservices—User Network Interfaces ( UNIs), Network-to-Network Interfaces (NNIs) and External Network-to-Network Interfaces (E-NNIS). UNIs, NNIs and E-NNIs can be connected to any type of physical interface, 1 GbE, 10 GbE (in 10G LAN or OTN mode), or multiple 1 GbE or 10 GbE organized into a link aggregation group. For more information about switchports, see [Chapter 5, “Configuring Ethernet Bridging and STP”](#).

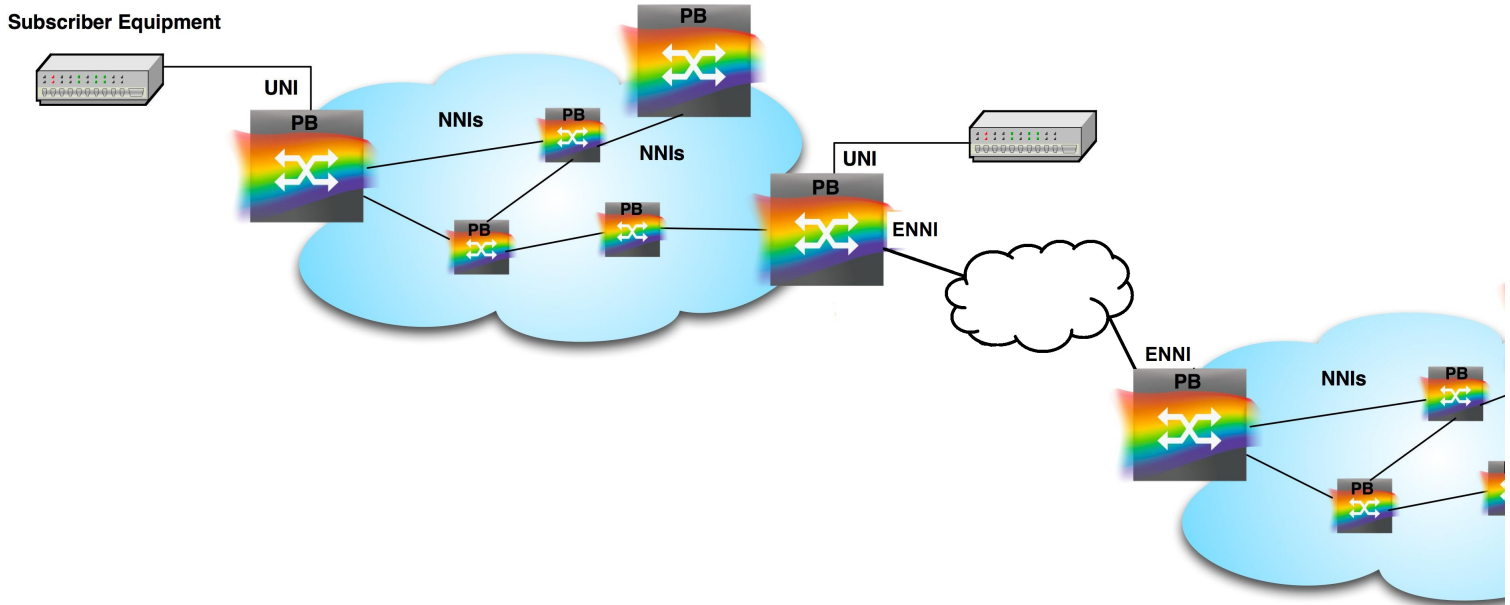
UNIs are the end points of Eservices, the places that connect to the subscriber. Eservices are primarily described in terms of their end points, the UNIs.

NNIs are the links that connect Provider Bridges together. It is not common to explicitly associate an NNI with an Eservice since this is done automatically by GVRP. The primary use of this capability is for the ERPS Service type (see [Chapter 11, “Configuring Ethernet Ring Protection Switching \(ERPS\)”](#)). This capability is also useful when connecting to Ethernet switches that do not support GVRP. Those devices will not be sending GVRP messages to automatically register VLANs on the NNI, therefore explicitly associating the NNI with services is necessary to ensure proper forwarding.

E-NNI's allow for the creation of Ethernet Services that span multiple network provider domains. E-NNIS must be explicitly associated to an access service as GVRP is not supported on E-NNI ports. (see [6.1.1, “External Network to Network Interface \[E-NNI\]”](#))

It is also often necessary to explicitly add NNIs to the Management VLAN service (see [Chapter 10, “Configuring Management VLAN services”](#)). If the Management VLAN service is being used only to manage BTI 7000 Series systems, then it might only have a single UNI (the one with the management station). That UNI will cause GVRP to advertise the MVLAN outward but there will not be any UNIs to cause it to advertise in the reverse direction.

The following figure shows a simple network showing an Eservice with UNIs, NNIs and E-NNIs.

**Figure 6-1 A simple network with UNIs, NNIs and E-NNIs**

The packetVX module splits configuration of the UNI into two parts. First, the UNI itself has a set of configuration parameters. These parameters apply to all of the services that are configured on the UNI. There are also configuration parameters for the Service UNI. The Service UNI parameters apply only to a specific service on the UNI.

UNI parameters are set in UNI configuration mode:

```
> UNI gig 1/1/19
> ! this is UNI configuration mode
> EXIT
```

Service UNI parameters are set in Service UNI configuration mode. This can be entered in two ways. The first is from UNI configuration mode:

```
> UNI gig 1/1/19
> ! this is UNI configuration mode
> ESERVICE customer1
> ! this is SERVICE UNI configuration mode
> EXIT
> EXIT
```

The second way to configure the Service UNI is from Eservice configuration mode:

```
> ESERVICE customer2
> ! this is ESERVICE configuration mode
> UNI gig 1/1/4
> ! this is SERVICE UNI configuration mode
> EXIT
```

### 6.1.1 External Network to Network Interface [E-NNI]

A network with an E-NNI configuration allows a service provider to offer Ethernet services that have UNIs residing in other service providers' network domains.

E-NNI's allow for the creation of Ethernet Services that span multiple network provider domains.

An individual segment within a provider's domain is called an OVC (Operator Virtual Circuit). An OVC can be a UNI or an E-NNI.

There are three types of OVCs:

- **Point-to-point OVCs :** [1 UNI + 1 E-NNI or 1 E-NNI + 1 E-NNI] - transport a class of services called Access Ethernet Line [E-LINE] services and associate two EVC. An OVC must associate at most one OVC at a given UNI. An OVC may associate more than one OVC at a given E-NNI. At least one of the OVC s associated by an OVC must be at an E-NNI.
- **Multipoint to Multipoint OVCs :** transport a class of services called Access Ethernet LAN [E-LAN] services and can associate more than two OVC s.
- **Rooted Multipoint OVCs:** ETree and EVTree are partially supported. By default a UNI is provisioned as a leaf and a E-NNI as root.

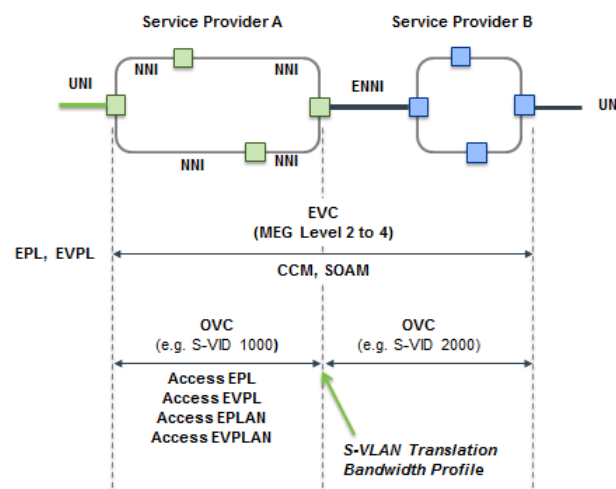
Ethernet Access services are OVC based Ethernet services.

S-VLAN translation is used to switch from one providers S-VLAN to the other providers S-VLAN. At the ingress and egress of the OVC, the S-VLAN ID in the outer tag will be translated to and from the external VLAN.

Bandwidth profiles are also specified to ensure that bandwidth restrictions are enforced across the leasing provider boundaries.

Customer equipment should be provisioned to the Ingress Bandwidth Profile of the service.

Service level CCMs remain supported from one providers SVLAN to another, using Service MEG.



### 6.1.1.1 Ethernet Access (E-Access) services

The following OVC based Ethernet services are supported -:

- E-Line
- E-LAN
- E-Tree

**Note** E-Tree is supported with limitations.

E-Access specifies two types of ethernet services :

- Access Ethernet Private Line Service (Access EPL) : is a port based and associates one OVC end point at a UNI and one OVC end point at an E-NNI.
- Access Ethernet Virtual Private Line (Access EVPL) : is VLAN based and associates one OVC end point at a UNI and one OVC end point at an E-NNI, and supports multiple service instances including a mix of access EPL, EVPL and EVC services.

An Access EPL and EVPL service MUST use a Point-to-Point OVC that associates a UNI OVC End Point and an E-NNI OVC End Point. E-NNI traffic is controlled by S-VLAN which maps traffic independently of service type. Therefore Access EPL and EVPL service instances can be assigned to the same E-NNI port.

The table below shows the typical pairing service between service provider services and the access provider services

Service Provider		Access Provider	
		Access -EPL (Port Based)	Access-EVPL (VLAN-Based)
Port Based	EPL	Pairing Service	
	EP-LAN	Pairing Service	
VLAN based	EVPL		Pairing Service
	EVP-LAN		Pairing Service

#### UNI service attribute and parameters for the Access EPL and EVPL services

An access EPL and EVPL service instance should assign UNI service attributes and values listed in the following table.

UNI Service Attributes and Parameters for the Access EPL and EVPL service		
Service Attribute	Service Attributes and Values Access EPL Service	Service Attributes and Values Access EVPL Service
UNI Identifier	Arbitrary text string to identify the UNI	Arbitrary text string to identify the UNI
Physical Medium	UNI Type 2 Physical Interface [5] except for PON interfaces2	UNI Type 2 Physical Interface [5] except for PON interfaces2
Speed	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000	10 Mbps, 100 Mbps, 10/100 Mbps Auto-negotiation, 10/100/1000 Mbps Auto-negotiation, 1 Gbps, or 10 Gbps.

UNI Service Attributes and Parameters for the Access EPL and EVPL service		
Service Attribute	Service Attributes and Values Access EPL Service	Service Attributes and Values Access EVPL Service
	Mbps Auto-negotiation, 1 Gbps, or 10 Gbps.	
Mode	Full Duplex	Full Duplex
MAC Layer	IEEE 802.3-2005 [5]	IEEE 802.3-2005 [5]
UNI MTU Size	MUST be $\geq 1522$	MUST be $\geq 1522$
CE-VLAN ID for untagged and priority frames	CE VLAN ID value is between 1 -4094 All untagged and any CE-VLAN tagged frames are mapped	CE VLAN ID value is between 1 -4094 MUST be specified if untagged / priority tagged frames are to be supported CE-VLAN IDs are included in the OVC Endpoint Map
Maximum number of OVCs per UNI	1 There is one OVC per UNI	1 or greater
Service Instance	1	Multiple service instances, including a mix of Access and EVC services
Ingress Bandwidth Profile per UNI	Is not specified.	Is not specified.
Egress Bandwidth Profile per UNI	Is not specified	Is not specified

### OVC end point per UNI service attributes and parameter values for Access EPL and EVPL Services

An Access EPL and EVPL service instance should assign OVC per UNI service attributes and values according to the following table.

OVC per UNI Service Attributes for Access EPL and EVPL Services		
Attributes for OVC per UNI Service Attributes	Service Attributes and Values for Access EPL Services	Service Attributes and Values for Access EVPL Services
UNI Identifier	A string formed by the concatenation of the UNI Identifier and the OVC Identifier	A string formed by the concatenation of the UNI Identifier and the OVC Identifier
OVC end point map	A list of CE-VLAN ID(s) that map to the OVC End Point at the UNI. 1-4095	MUST specify mapping table of CE-VLAN ID to OVC End Point. MUST NOT contain all CE-VLAN ID values mapped to a single OVC End Point. (This configuration is reserved for the Access EPL service)
Class of Service Identifier for Service Frames	The CoS Identifier for Service Frames MUST be the OVC End Point.	The CoS Identifier for Service Frames MUST be the OVC End Point to which the Service Frame is mapped; that OVC MUST have a single CoS Name.

<b>OVC per UNI Service Attributes for Access EPL and EVPL Services</b>		
<b>Attributes for OVC per UNI Service Attributes</b>	<b>Service Attributes and Values for Access EPL Services</b>	<b>Service Attributes and Values for Access EVPL Services</b>
Ingress Bandwidth Profile Per OVC End Point at a UNI	Specify <CIR, CBS, EIR, EBS, CM, CF>; CIR values <sup>2</sup> up to 70% of the UNI speed are supported	Specify <CIR, CBS, EIR, EBS, CM, CF>; supports CIR values up to 70% of the UNI speed
Ingress Bandwidth Profile Per Class of Service Identifier at a UNI	Not used.	Not used.
Egress Bandwidth Profile Per OVC End Point at a UNI	Is not specified	Is not specified
Egress Bandwidth Profile Per Class of Service Identifier at a UNI	Is not specified	Is not specified

### OVC service attributes for Access EPL and EVPL services per UNI

<b>OVC Service Attribute</b>	<b>EPL Values</b>	<b>EVPL Values</b>
OVC Identifier	A string of at most 45 bytes that uniquely identifies the OVC within a given CEN	A string of at most 45 bytes that uniquely identifies the OVC within a given CEN
OVC Type	MUST be Point-to-Point	MUST be Point-to-Point
OVC End Point List	A list of OVC End Point Identifiers, exactly 2, one OVC End Point at the UNI, one at the E-NNI.	A list of OVC End Point Identifiers, exactly 2, one OVC End Point at the UNI, one at the E-NNI.
Max number of UNI OVC End Points	MUST be 1	MUST be 1
Maximum Number E-NNI OVC End Points	MUST be 1	MUST be 1
OVC Maximum Transmission Unit Size	An integer number of bytes > or = to 1526 It is recommended to be at least 2000 bytes. It must be less than or equal to the E-NNI MTU size. When an E-NNI frame is larger than the OVC MTU that is mapped to an OVC, then the frame must be discarded. If an OVC is part of the EVC its MTU should be set to at least the MTU size of the EVC	An integer number of bytes > or = to 1526
CE-VLAN ID Preservation	Yes	Yes
CE-VLAN CoS ID Value Preservation	Yes	MUST be Yes
S-VLAN ID Preservation	N/A as only one E-NNI in the service instance	N/A as only one E-NNI in the service instance
S-VLAN CoS ID Value Preservation	N/A as only one E-NNI in the service instance	N/A as only one E-NNI in the service instance

OVC Service Attribute	EPL Values	EVPL Values
Color Forwarding	SHOULD be yes. When Ingress BWP at UNI has EIR = 0 frames egressing at E-NNI MUST be marked green.	SHOULD be yes. When Ingress BWP at UNI has EIR = 0 frames egressing at E-NNI MUST be marked green.
Service Level Specification	Supports values for the following attributes: { One-way Frame Delay, One-way Frame Delay Range, One-way Mean Frame Delay, Inter Frame Delay Variation, One-way Frame Loss Ratio, One-way Availability, One-way High Loss Intervals, One-way Consecutive High Loss Intervals} and Not Specified (N/S)	Supports values for each of the following attributes: { One-way Frame Delay, One-way Frame Delay Range, One-way Mean Frame Delay, Inter Frame Delay Variation, One-way Frame Loss Ratio, One-way Availability, One-way High Loss Intervals, One-way Consecutive High Loss Intervals} and Not Specified (N/S).
Unicast Frame Delivery	MUST Deliver Unconditionally	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Multicast Frame Delivery	MUST Deliver Unconditionally	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.
Broadcast Frame Delivery	MUST Deliver Unconditionally	Deliver Unconditionally or Deliver Conditionally. If Delivered Conditionally, MUST specify the delivery criteria.

### OVC End Point per E-NNI Service Attributes

The OVC End Point per E-NNI attribute values associated with the Access EPL and EVPL services are shown in table below.

OVC End Point per E-NNI Service Attribute Name	Possible EPL Values	Possible EVPL Values
OVC End Point Identifier	No additional constraints	No additional constraints
Class of Service Identifier for E-NNI Frames	The CoS Identifier for E-NNI Frames is the OVC End Point to which the E-NNI Frame is mapped  The OVC has a single CoS Name which is associated with the entire set of S-Tag PCP values {0 – 7}.	The CoS Identifier for E-NNI Frames is the OVC End Point to which the E-NNI Frame is mapped  The OVC has a single CoS Name which is associated with the entire set of S-Tag PCP values {0 – 7}.
Ingress Bandwidth Profile Per OVC End Point	Specify <CIR, CBS, EIR, EBS, CM, CF>;configuration supports CIR2 values up to 70% of the E-NNI  Color Mode = “color aware”  CBS >= 12176 bytes  MUST NOT be combined with any other type of ingress bandwidth	Specify <CIR, CBS, EIR, EBS, CM, CF>;configuration supports CIR2 values up to 70% of the E-NNI  Color Mode = “color aware”  CBS >= 12176 bytes  MUST NOT be combined with any other type of ingress bandwidth
Ingress Bandwidth Profile Per E-NNI	Not used.	Not used.

OVC End Point per E-NNI Service Attribute Name	Possible EPL Values	Possible EVPL Values
Class of Service Identifier		
Egress Bandwidth Profile Per End Point	MUST NOT specify.	MUST NOT specify.
Egress Bandwidth Profile Per E-NNI Class of Service Identifier	MUST NOT specify.	MUST NOT specify.

### E-NNI Service Attributes

The following table specifies the E-NNI Service Attributes for the Access EVPL service. The Maximum Number of OVC End Points per OVC is required to be exactly 1 for Access EVPL as this service does not support “hairpin switching” of traffic.

An Access EPL and EVPL Service instance **MUST** assign E-NNI Service Attributes and values according to the following table.

E-NNI Service Attribute Name	Possible EPL Values	Possible EVPL Values
Operator E-NNI Identifier	A string that is unique across the Operator MEN	A string that is unique across the Operator MEN
Physical Layer	Each link in an E-NNI <b>MUST</b> be one of the following physical layers in full duplex: <ul style="list-style-type: none"> <li>1000Base-SX, 1000Base-LX</li> <li>1000Base T, 10GBASE-SR, 10GBASE-LX4, 10GBASE-LR, 10GBASE-ER</li> <li>10GBASE-SW, 10GBASE-LW, 10GBASE-EW</li> </ul>	Each link in an E-NNI <b>MUST</b> be one of the following physical layers in full duplex: <ul style="list-style-type: none"> <li>1000Base-SX, 1000Base-LX</li> <li>1000Base T, 10GBASE-SR, 10GBASE-LX4, 10GBASE-LR, 10GBASE-ER</li> <li>10GBASE-SW, 10GBASE-LW, 10GBASE-EW</li> </ul>
Frame Format	The E-NNI Frame is an Ethernet frame and is defined to consist of the first bit of the Destination MAC Address through the last bit of the Frame Check Sequence. E-NNI Frames use Service VLAN tags (S-tags), as defined in IEEE Std 802.1ad-2005[4], to map frames to End Points	The E-NNI Frame is an Ethernet frame and is defined to consist of the first bit of the Destination MAC Address through the last bit of the Frame Check Sequence. E-NNI Frames use Service VLAN tags (S-tags), as defined in IEEE Std 802.1ad-2005[4], to map frames to End Points
Number of Links	An integer with the value of 1 or 2 If the Number of Links is one, then the Protection Mechanism attribute <b>MUST</b> be set to “none.” If the Number of Links is 2 and LAG is implemented, then the Protection Mechanism attribute <b>MUST</b> be set to “Link Aggregation.”	An integer with the value of 1 or 2 If the Number of Links is one, then the Protection Mechanism attribute <b>MUST</b> be set to “none.” If the Number of Links is 2 and LAG is implemented, then the Protection Mechanism attribute <b>MUST</b> be set to “Link Aggregation.” If the conditions specified are not met, then the Protection Mechanism attribute <b>MUST</b> be set to “other.”



E-NNI Service Attribute Name	Possible EPL Values	Possible EVPL Values
	If the conditions specified are not met, then the Protection Mechanism attribute MUST be set to "other."	
Protection Mechanism	Link aggregation, none or other	Link aggregation, none or other
E-NNI Maximum Transmission Unit Size	<p>The E-NNI Maximum Transmission Unit Size MUST be at least 1526 bytes.</p> <p>The E-NNI Maximum Transmission Unit Size SHOULD be at least 2000 bytes.</p> <p>When an E-NNI Frame is larger than the MTU Size, the receiving Operator MEN for this frame will discard it.</p>	<p>The E-NNI Maximum Transmission Unit Size MUST be at least 1526 bytes.</p> <p>The E-NNI Maximum Transmission Unit Size SHOULD be at least 2000 bytes.</p> <p>When an E-NNI Frame is larger than the MTU Size, the receiving Operator MEN for this frame will discard it.</p>
End Point Map	<p>Each S-VLAN ID value associated with an instance of Access EPL Service MUST map to a distinct End Point, of Type = "OVC"</p> <p>Note : The E-NNI will be connected to a Single Subscriber End UNI</p>	<p>Each S-VLAN ID value associated with an instance of Access EVPL Service MUST map to a distinct End Point, of Type = "OVC"</p> <p>Note : The E-NNI will be connected to a multiple Subscriber End UNI</p>
Maximum Number of OVCs	An integer greater or equal to 1	An integer greater or equal to 1
Maximum Number of OVC End Points per OVC	An integer greater or equal to 1	An integer greater or equal to 1

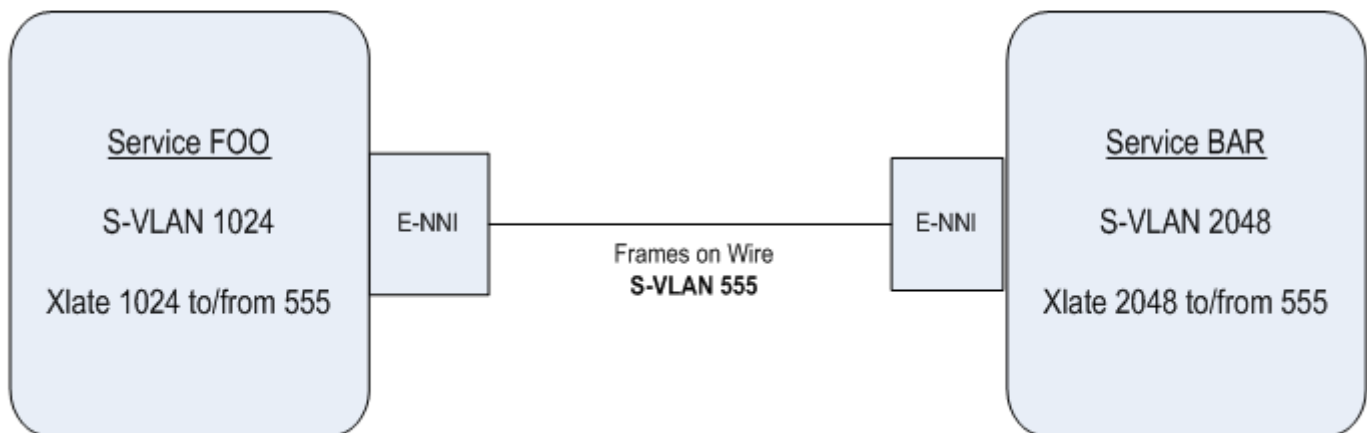
### 6.1.1.2 E-NNI S-VLAN translation

The E-NNI performs S-VLAN translation at both ingress and egress. The two services providers must agree on the external S-VLAN ID used across the E-NNI link and provision the E-NNI's in accordance with xref.

An example of an E-NNI translation is shown below.

## Service Provider Domain A

## Service Provider Domain B



Service provider A terminates an OVC carrying S-VLAN 1024 at an E-NNI connected to service provider B. The OVC carries the traffic on S-VLAN 2048. The two service providers agree that across the E-NNI, the EVC traffic will be translated to and from S-VLAN 555. Both E-NNIs are STATIC member of the S-VLAN 1024. The E-NNI's perform S-VLAN translation in both the ingress and egress directions.

The internal S-VLAN ID's [1024 & 2048] are only required at the E-NNI link interface. Therefore service provider A and service provider B will be unaware of each others local S-VLAN ID.

When reprovisioning the OVC each provider can change the internal S-VLAN however the external S-VLAN must always remain the same.

Provider A and B can change the internal S-VLAN ID without having to inform each other.

### **6.1.1.3 E-NNI bandwidth profile**

The following bandwidth profiles can be provisioned :

- Ingress and egress bandwidth profile on ENNI
- Ingress and egress bandwidth profile per OVC
- Ingress and egress bandwidth profile per Cos

The bandwidth profile describes the bandwidth limitation in terms of four parameters:

- Committed Information Rate (CIR)
- Committed Burst Size (CBS)

- Excess Information Rate (EIR)
- Excess Burst Size (EBS)

CIR is the basic rate committed by the service provider, for example, 125 Mb/s. The SLA documents that frames presented to the E-NNI at an average rate of CIR or lower are delivered with a probability defined in the QoS definition, for example, greater than 99.8%. EIR is the excess information rate. The excess rate allows the subscriber to use excess bandwidth that might be available in the network. This excess traffic is subject to the same class of service, except that the traffic in excess of CIR has a lower probability of successful frame delivery—it is more likely to be discarded if the network is congested.

Only one ingress or one egress Bandwidth Profile can be applied to a specific E-NNI.

The meter mode must be set to two rated TCM mode in the ingress bandwidth profile and single rated TCM mode in the egress bandwidth . The meter mode cannot be modified after the bandwidth profile has been added.

Colour aware mode should be enabled.

The ingress CIR for an OVC at the ENNI should be greater than the corresponding ingress CIR at the UNI due to the presence of the added SVLAN tag (4 bytes) at the ENNI. As an example, if the average frame size was 200 bytes, the CIR should be increased by 2%. MEF Bandwidth Profile traffic parameters such as CIR count only Service Frame bits, not interframe gap or preamble bits.

#### 6.1.1.4 E-NNI provisioning specifications

The following table lists the supported provisioning specifications :

Provisioning features	Details
Service multiplexing	E-NNI supports multiple services over a single E-NNI.
S-VLAN translation	<p>S-VLAN translation is supported at both egress and ingress of E-NNI</p> <p>S-VLAN translations MUST be one-to-one [each service S-VLAN can be mapped to only one S-VLAN across an E-NNI].</p> <p>SVLAN translation entries + CVLAN translation entries &lt;0-256&gt; per switch.</p> <p>SVLAN translation entries + CVLAN mapping entries &lt;0-1024&gt; per switch.</p> <p>SVLAN bundling is not supported</p>
MSTP	MSTP is disabled throughout the E-NNI network
GVRP	GVRP is disabled throughout th E-NNI network
LLDP	LLDP is supported on the E-NNI network
LAGs	E-NNI's support LAGs provisioning
LACP	LACP is supported in E-NNI provisioning
ERPS Services	E-NNI ports MUST NOT be allowed in ERPS Services.
EPLINE, EPLAN, EVPLAN, EVPLINE, EPTREE, EVPTREE services	EPLINE, EPLAN, EVPLAN, EVPLINE, EPTREE, EVPTREE services are supported in E-NNI

Provisioning features	Details
CCM's at MEG level 2, 3 and 4	CCM's at MEG level 2, 3 and 4 are permitted to cross the E-NNI port
Operator MEG	Operator MEG is not supported on E-NNI
Bandwidth profile	Bandwidth profile creation is supported at E-NNI
Hairpin switching	Is not supported on E-NNI ports
OVC End Point map bundling	Is not supported on E-NNI ports

## 6.1.2 Sample UNI, NNI and E-NNI configurations

This section details sample UNI, NNI and E-NNI configurations.

### 6.1.2.1 Sample UNI configuration

First, select the virtual switch that the packetVX is a member of.

```
BTI7000> enable !access privileged EXEC mode
BTI7000#
BTI7000# configure terminal !enter global configuration mode
BTI7000(config)#
BTI7000(config)# virtual-switch 1 !select a virtual switch (#1 here)
BTI7000:sw1(config)#
```

Now create the UNI. This is done using the UNI command and specifying either an interface identification or a link aggregation group number. For example:

```
BTI7000:sw1(config)# uni gigabitEthernet 1/2/3 !shelf 1, slot 2, interface 3
or
BTI7000:sw1(config)# uni lag 2
```

The default maximum frame size on a UNI is 1522 bytes. This allows a maximum-sized (non-jumbo) Ethernet frame of 1518 bytes plus a four byte customer VLAN tag. The maximum frame size can be configured higher:

```
BTI7000:sw1(config)# uni gig 1/2/3
BTI7000:sw1(config-uni GigE 1/2/3)# frame-size 2048
BTI7000:sw1(config-uni GigE 1/2/3)# exit
```

The maximum-sized frame that can be transferred by the packetVX is 9600 bytes. When a packet is transmitted on an NNI an additional four byte tag (the provider VLAN tag) is added, so the maximum size that should be configured on a UNI is 9596 bytes.

**Note** For step-by-step UNI provisioning information, see [6.3.1, “Define a UNI”](#).

### 6.1.2.2 Sample NNI configuration

First, select the virtual switch that the packetVX is a member of.

```
BTI7000> enable !access privileged EXEC mode
BTI7000#
BTI7000# configure terminal !enter global configuration mode
BTI7000(config)#
```

```
BTI7000(config)# virtual-switch 1 !select a virtual switch (#1 here)
BTI7000:sw1(config)#
```

Now create the NNI. This is done using the NNI command and specifying either an interface identification or a link aggregation group number. For example:

```
BTI7000:sw1(config)# nni gigabitEthernet 1/2/3 !shelf 1, slot 2, interface 3
or
BTI7000:sw1(config)# nni lag 2
```

The default maximum frame size on an NNI is 9600 bytes. This allows the NNI to carry any payload configured on the UNIs (as long as the maximum frame size on the UNI does not exceed 9596 bytes). The maximum frame size can be reduced. For example,

```
BTI7000:sw1(config)# nni gig 1/2/3
BTI7000:sw1(config-enni GigE 1/2/3)# frame-size 2048
BTI7000:sw1(config-enni GigE 1/2/3)# exit
```

**Note** For step-by-step NNI provisioning information, see [6.3.2, “Define an NNI”](#).

### 6.1.2.3 Sample E-NNI configuration

First, select the virtual switch that the packetVX is a member of.

```
BTI7000> enable
BTI7000# configure terminal
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)#
```

Now create the NNI. This is done using the NNI command and specifying either an interface identification or a link aggregation group number. For example:

```
BTI7000:sw1(config)# enni gigabitEthernet 1/2/3
or
BTI7000:sw1(config)# enni lag 2
```

The default maximum frame size on an E-NNI is 9600 bytes. This allows the E-NNI to carry any payload configured on the UNIs (as long as the maximum frame size on the UNI does not exceed 9596 bytes). The maximum frame size can be reduced. For example,

```
BTI7000:sw1(config)# enni gig1/2/3
BTI7000:sw1(config-enni GigE 1/2/3)# frame-size 2048
BTI7000:sw1(config-enni GigE 1/2/3)# exit
```

**Note** For step-by-step E-NNI provisioning information, see [6.3.3, “Define an E-NNI and OVC”](#).

## 6.1.3 Private and Virtual Private services

### Private and Virtual Private services

UNIs can be dedicated to a single service or they can be shared by multiple services (technically called *service multiplexing*). When all UNIs in a service are dedicated to a single service, that is, they do not allow service multiplexing, the service is called a *private* service. If one or more

UNIs in a service are configured to allow service multiplexing, the service is called a *virtual private* service (regardless of whether another service is actually defined on the UNIs).

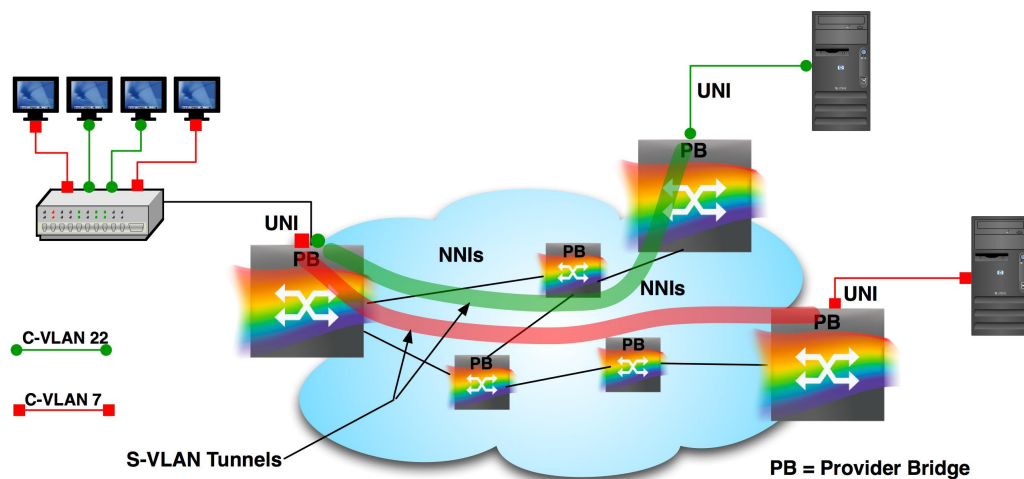
Private services (EPLINE and EPLAN<sup>22</sup>) are port-based services. With these services, since the port is “owned” by a single subscriber, the bridge does not worry about customer VLANs at all. All traffic is encapsulated into the S-VLAN and forwarded.

Virtual private services (EVPLINE, EVPLAN, and EVPPTREE) are VLAN-mapped services. For each service on each UNI, a list of customer VLANs (C-VLANs) is specified. For example, C-VLANs 7, 9, and 11 can be mapped to one service, and C-VLANs 20 and 22 can be mapped to another service on the same UNI. Untagged packets can also be mapped to one of the services on the UNI.

The following figure shows how a pair of Ethernet Virtual Private Networks could be used. The subscriber equipment at the top left of the diagram is an Ethernet switch. It is assigning different user ports to different C-VLANs. The two ports with red squares are assigned to C-VLAN 7 and the two ports with green circles are assigned to C-VLAN 22. Two Ethernet services (EVPLINES) are defined on the packetVX UNI. This is service multiplexing. One service maps C-VLAN 7 from the UNI and the other maps C-VLAN 22 from the UNI. In both cases, other C-VLANs could also be mapped to the same services.

In this example, the two services terminate on different packetVX modules on the other end.

**Figure 6-2 Ethernet Virtual Private Line services**



<sup>22</sup> Although EPTREE services are considered as “private” services, they are not port-mapped services. See 6.2.5, “Ethernet Tree Service (E-TREE)” for more information on E-TREE services.

## 6.2 Ethernet services

---

Before configuring an Eservice, all of the UNIs must be provisioned. For example:

```
> UNI <name> (for example, UNI gig 1/1/1)
> EXIT
```

There are several parameters that can also be set for UNIs. For information, see the *BTI 7000 Series Command Line Interface Reference Guide*.

If services traverse multiple switches, then, before traffic can flow, all switches that are part of the route must be commissioned, and NNIs must be provisioned between the switches (regardless of whether the NNIs are explicitly associated with the service or automatically chosen by the system) so that the service layer protocols for the E-service know where the flow terminates. For example:

```
> NNI tengig 1/1/3
> EXIT
```

Eservices are defined using the **ESERVICE** command mode. The **ESERVICE** command includes the service name and the service type. The mode brackets the other items that are configured for the service.

```
> ESERVICE servicename TYPE [epline | evpline | eplan | evplan | eptree |
evptree]
> ! specification of the ESERVICE parameters and UNIs
> EXIT
```

Basic configuration of an Eservice requires the following:

using the **mac-learning** command

- Eservice name
- Eservice type
- The S-VLAN number
- The local UNIs that are part of the service
- If it is a Virtual Private Service, the C-VLANs that are mapped
- The spanning tree instance that the service is assigned to (if it is not the Internal Spanning Tree (IST)).

An E-LINE service (EPLINE or EVPLINE) can only have two end points. They can be on the same switch or on two different switches. The system will ensure that you don't define more than two UNIs on a single node in this case.

Other parameters that can be set for the service are maximum frame size and whether C-VLAN translation is enabled. See the *BTI 7000 Series Command Line Interface Reference Guide* for information about setting these parameters.

## MAC learning

By default, MAC learning is enabled for E-LAN, E-LINE and E-TREE services. Since an E-LINE service is point-to-point, you may want to turn off MAC learning in some situations and have the bridge forward all traffic to the other end. This can be done for the end nodes, as well as, for the intermediate nodes. On an intermediate node carrying an E-LINE service, you may need to explicitly define the VLAN before you can disable MAC learning.

To turn off MAC learning:

```
> vlan 1000
> mac-learning disable
> exit
```

If you disable MAC learning, storm control settings should be set with a low threshold, or preferably, no threshold.

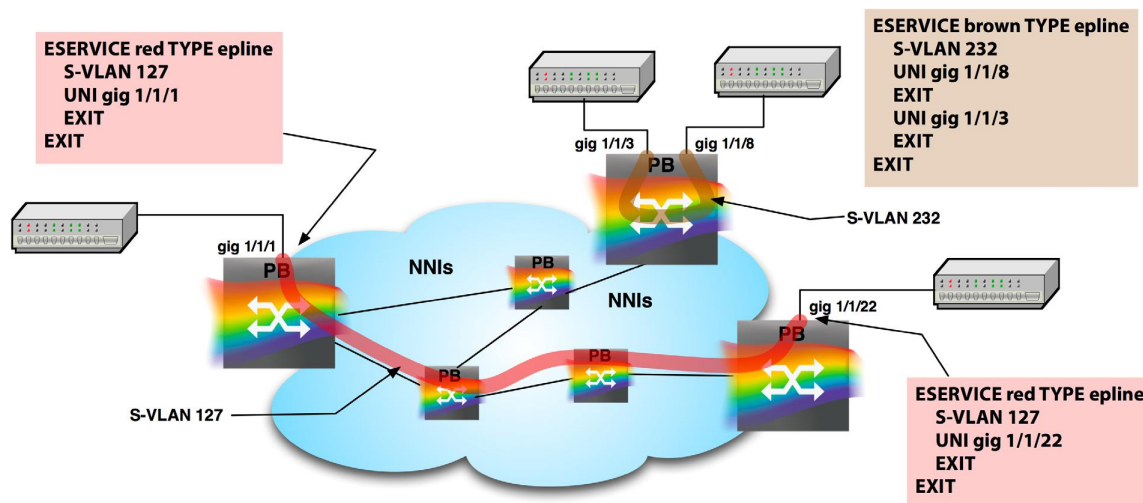
To turn MAC learning back on:

```
> vlan 1000
> mac-learning enable
> exit
```

### 6.2.1 Ethernet Private Line (EPLINE)

An Ethernet Private Line service is a point-to-point service between two UNIs on the provider network. The end points can be on the same switch or on different switches. Private services are port-mapped, (as opposed to C-VLAN mapped), and the ports cannot be shared by other services. The following figure shows the basic configuration for two EPLINE services, one that has both end points terminating on the same packetVX module and one that has the end points on different packetVX modules.

Figure 6-3 EPLINE services: basic configuration





## 6.2.2 Ethernet Virtual Private Line (EVPLINE)

An Ethernet Virtual Private Line service is a point-to-point service between two UNIs on the provider network. The end points can be on the same switch or on different switches. This is a virtual private service, so one or both of the UNIs can be shared with other services (service multiplexing) and the traffic is assigned to the service based on the C-VLAN.

Figure 6-2 on page 6-16 shows a pair of EVPLINE services that co-terminate on the same UNI on one end and terminate on different UNIs (on different packetVX modules) on the other end.

Configuration of the “red square” service shown in this figure would be as follows:

```
> ESERVICE red-square TYPE evpline
> S-VLAN 101
> UNI gig 1/1/1
> C-VLAN 7-8
> EXIT
```

Only one UNI is specified, gig 1/1/1, and C-VLANs 7 and 8 are mapped from that UNI to the service. This configuration would be the same on both sides of the service — although the actual UNI name (e.g., gig 1/1/1) might be different on each.

Configuration of the “green circle” service shown in this figure would follow the same pattern:

```
> ESERVICE green-circle TYPE evpline
> S-VLAN 200
> UNI gig 1/1/1
> C-VLAN 20
> C-VLAN 22
> EXIT
```

The only differences are the name of the service, the S-VLAN number, and the C-VLANs that are mapped from the UNI.

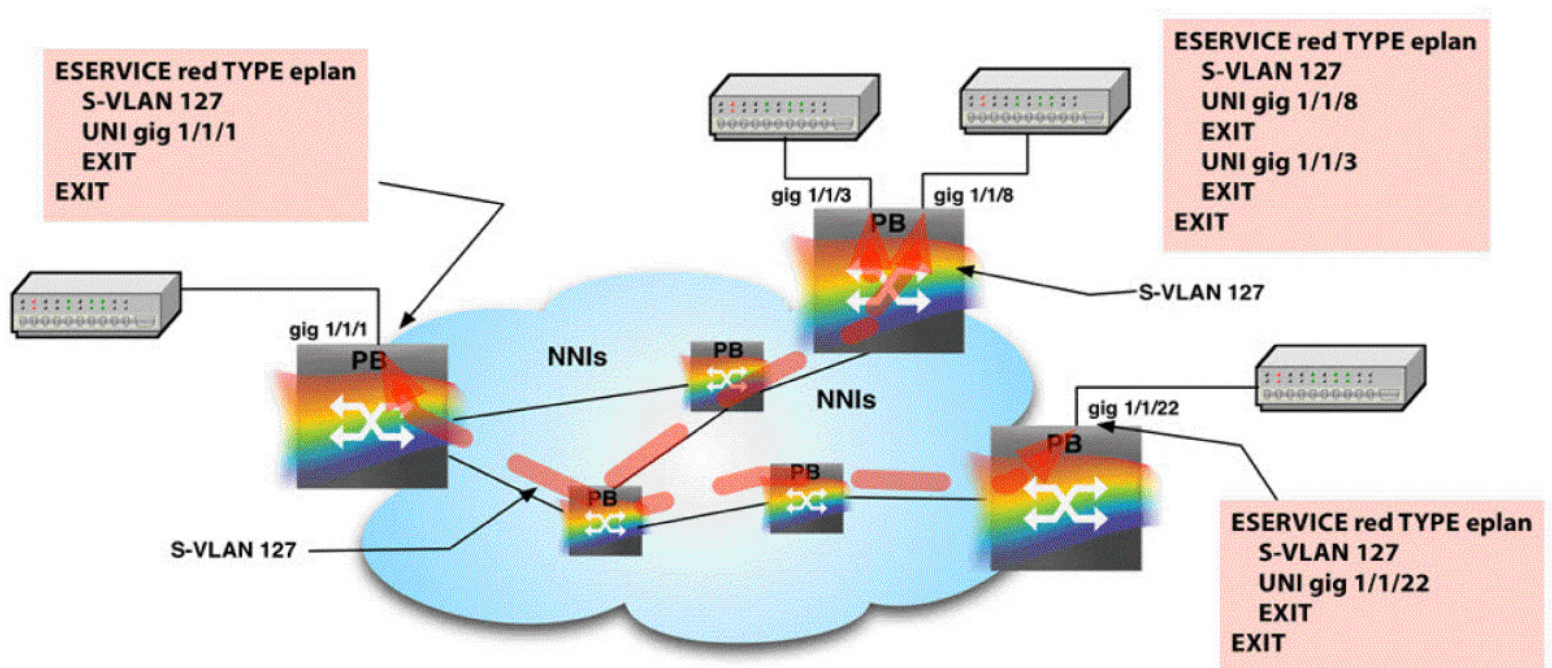
<b>Note</b>	When adding an EVP service to a UNI port, there is a period of about 20 seconds before traffic starts flowing, and during which existing traffic on that UNI is interrupted.
-------------	--

## 6.2.3 Ethernet Private LAN (EPLAN)

An Ethernet Private LAN service is a multipoint service between two or more UNIs on the provider network. The end points can be on the same switch or on different switches. Since this is a private service, it is port-mapped, not C-VLAN mapped, and the ports cannot be shared by other services. As with any bridged LAN, packets are directed in the EPLAN using MAC addresses.

The following figure shows an EPLAN service with 4 UNIs.

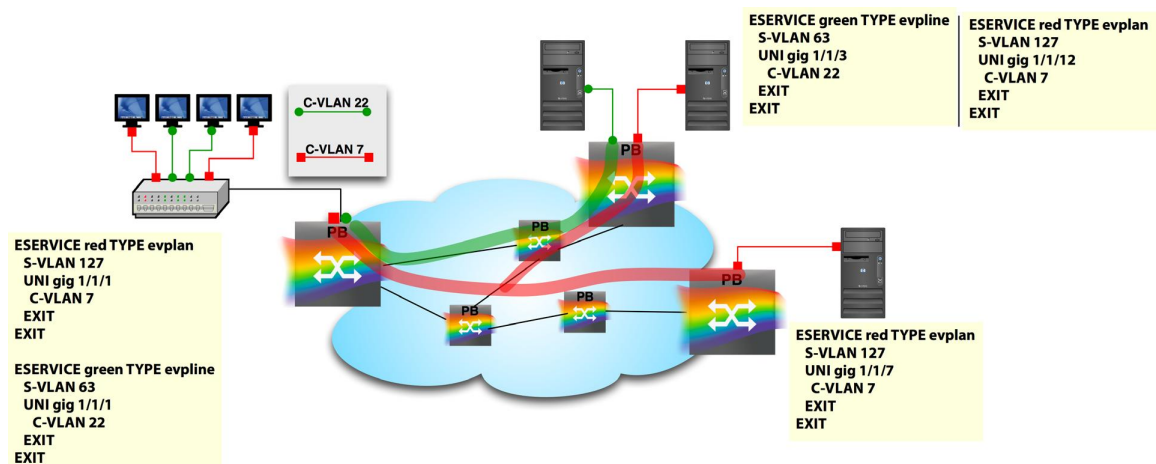
Figure 6-4 EPLAN services: basic configuration



## 6.2.4 Ethernet Virtual Private LAN (EVPLAN)

An Ethernet Virtual Private LAN service is a multipoint service between two or more UNIs on the provider network. The end points can be on the same switch or on different switches. Since this is a *virtual private* service, one or more of the UNIs can be shared with other services (service multiplexing) and the traffic is assigned to the service based on C-VLAN. Within the EVPLAN service, packets are forwarded based on MAC address. The following figure shows an EVPLAN.

Figure 6-5 EVPLAN services: basic configuration



The red VLAN (127) is the EVPLAN and has three UNIs, one of which is service-multiplexed UNIs. The UNI gig 1/1/1 on the left bridge is multiplexed with the green EVPLINE<sup>23</sup> (which terminates on gig 1/1/3 of the top bridge). The red VLAN has two other end points, gig 1/1/12 on the top bridge and gig 1/1/7 on the right bridge.

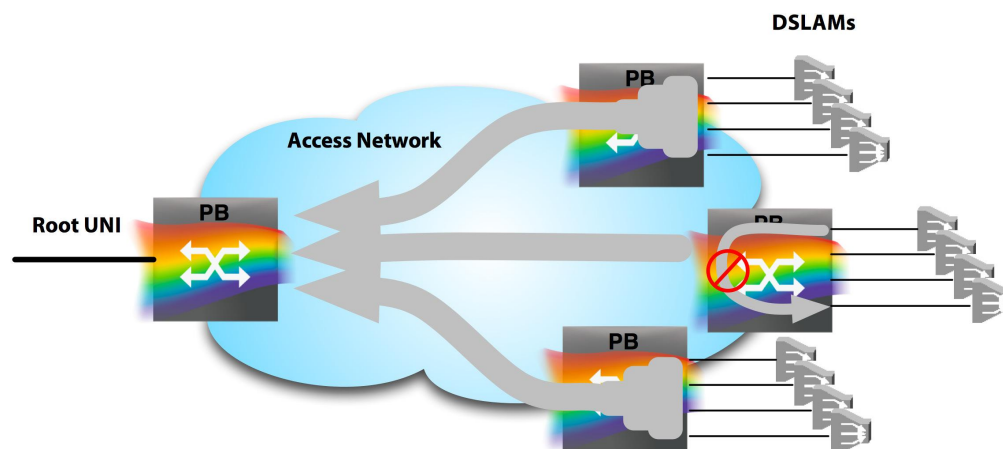
## 6.2.5 Ethernet Tree Service (E-TREE)

An E-TREE service is used for a multipoint service in which one set of subscribers (UNIs), the leaves, can only send and receive packets from a well-defined set of one or more root UNIs, but not with each other. From the point-of-view of the root UNIs, the service is an E-LAN service, but from the point-of-view of the leaf UNIs, there are restrictions on packet forwarding.

E-TREE service is useful in broadband access networks where the provider wants to ensure that all traffic is forwarded through a specific node for routing and/or metering and not allowing subscribers to communicate directly between each other.

The following figure provides the basic layout of an E-TREE network.

**Figure 6-6 Basic E-TREE network**



As shown in the figure, traffic from a leaf UNI can only flow to the root, not to another leaf UNI even though they are in the same service/VLAN. Traffic from a root UNI can be forwarded anywhere. There are a number of important configuration rules associated with E-TREE:

- Leaf UNIs cannot be service multiplexed—an E-TREE service on a UNI cannot be multiplexed with any other service.
- Root UNIs can be service multiplexed. (From the root point of view the E-TREE looks like an EVPLAN service).
- Important: Leaf-to-leaf communication can only be restricted between UNIs on the same packetVX node, not between packetVX nodes. As a result, the network shown in the preceding figure should be implemented as a separate service (and hence separate S-VLAN) on each of the three packetVX NEs that have leaf UNIs. These three services can then be service-multiplexed on the Root UNI.

<sup>23</sup> Actually this could be an EVPLINE or an EVPLAN. An EVPLINE can have only two UNIs, but an EVPLAN can have two or more. An EVPLAN with two nodes looks very much like an EVPLINE except that you can add more UNIs to the EVPLAN.

- All UNIs in an E-TREE are C-VLAN mapped regardless of whether the service is EPTREE or EVPTREE.
- The difference between EPTREE and EVPTREE is relevant only on the root UNI.

To distinguish between root UNIs and leaf UNIs the FORWARDING parameter is used. For services other than E-TREE, the default value (and the only value) for FORWARDING is NORMAL. For E-TREE, the default value is ETREE-LEAF. Configuration of the E-TREE service on one of the leaf nodes on the right side of the preceding figure is summarized as follows:

```
> ! The following is a summary of the leaf configuration on the node
> ESERVICE dslam1 TYPE EVPTREE
> S-VLAN 1002
> UNI gig 1/1/1
> C-VLAN 1-1000
> FORWARDING ETREE-LEAF ! This is default, shown here for clarity
> EXIT
> UNI gig 1/1/2
> C-VLAN 1-1000
> FORWARDING ETREE-LEAF
> EXIT
> ...
> EXIT
>
> ! The following is a summary of the configuration on the node containing the
root.
> ESERVICE dslam1 TYPE EVPTREE
> S-VLAN 1002
> UNI gig 1/1/7
> C-VLAN 1-1000
> FORWARDING NORMAL ! This makes it the root port
> EXIT
> EXIT
```

For an E-TREE service, the only difference between an EPTREE and EVPTREE is whether the root UNI is service multiplexed.

## 6.2.6 Mapping untagged packets to a service

With Virtual Private services (EVPLINE and EVPLAN), a common requirement is to map untagged packets on the UNI (i.e., packets without a C-VLAN tag) to one of the services. This is done by selecting a default C-VLAN for the UNI<sup>24</sup> (the C-PVID) and mapping it to the appropriate Eservice for that UNI. For example, choosing VLAN 17 for this purpose, the configuration would be:

```
ESERVICE orange TYPE evpline
> S-VLAN 112
> UNI gig 1/1/13
> C-VLAN 1-5
> C-VLAN 17 ! mapping the C-PVID here
```

<sup>24</sup> This C-VLAN is not actually added to the packet. The packet is transported with an S-VLAN tag only.

```
> EXIT
> EXIT
```

Then, this C-PVID, i.e., the default C-VLAN, is configured on the UNI.

```
> UNI gig 1/1/13
> C-PVID 17
> EXIT
```

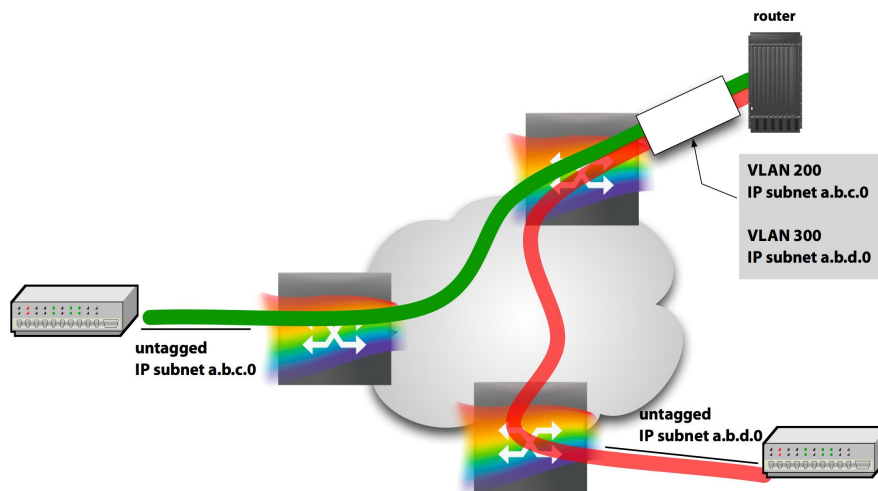
Alternatively, if the Eservice has already been defined, the mapping can be added directly in the UNI configuration:

```
> UNI gig 1/1/13
> C-PVID 17 ! define the C-PVID
> ESERVICE orange ! enter ESERVICE UNI mode
> C-VLAN 17 ! map VLAN 17 to the service
> EXIT
> EXIT
```

## 6.2.7 Services with untagged-to-tagged translation

Most subscriber networks operate untagged. IP routers, however, frequently support multiple logical IP subnets on a single LAN by configuring VLANs. This results in a common situation in which one side of a service is untagged (we are talking about C-tags) and the other side is tagged.

**Figure 6-7 Network with untagged-to-tagged translation**



To support this configuration, a translation from untagged to tagged must occur at the untagged UNIs. The C-tagged interface (the router interface in the preceding figure) is configured normally with two EVPLINE services, one mapping C-VLAN 200 to the service and the other mapping C-VLAN 300 to the service.

At the untagged UNIs, the UNIs are configured as *virtual-untagged*. For example:

```
> UNI gig 1/1/7
> SERVICE-TYPE virtual-untagged
```

```
> C-PVID 200
> EXIT
```

This UNI is then assigned to an EVPLINE service:

```
> ESERVICE green TYPE evpline
> S-VLAN 17
> UNI gig 1/1/7
> EXIT
> EXIT
```

Although it is an EVPLINE service, the untagged UNI cannot be service-multiplexed. Also the C-VLAN map is automatically created when the UNI is configured this way so it is not necessary to specify a C-VLAN map in the Service-UNI configuration.

## 6.2.8 L2 Control Packets

The networks that connect to UNIs on the Provider Bridge are usually subscriber networks that also contain Ethernet switches. Ethernet switches use a variety of protocols to communicate with each other. These *layer 2 control protocols* include the Spanning Tree Protocol, GVRP, and LACP. It is likely that these protocol messages will appear at the UNI of a Provider Bridge.

The Provider Bridge has three options in reacting to these protocols:

- DISCARD – drop them and forget about them
- TUNNEL – encapsulate them and send them to the subscriber equipment at the other side of the service
- PEER – actually process the protocol messages, i.e., treat the subscriber bridge as a peer. The Provider Bridge creates a private context (e.g., a spanning tree context) for each Eservice in which the UNIs are peering the protocols.

The Metro Ethernet Forum provides the rules (in MEF 6.1) for how each protocol can be handled. The following table includes a subset of that information:

Protocol	EPLINE	EVPLINE/EVPLAN	EPLAN
Spanning Tree (all types)	MUST TUNNEL	MUST PEER or DISCARD	SHOULD TUNNEL
LACP	SHOULD TUNNEL	MUST PEER or DISCARD	MUST PEER or DISCARD
GVRP	MUST TUNNEL	PEER, TUNNEL, DISCARD	PEER, TUNNEL, DISCARD

To configure the handling for these protocols, each service has an *L2 Control Protocol* profile and a *Tunnel MAC Address profile*. There are default profiles that are automatically assigned to a service, based on the type of service, but the defaults can be changed by creating new profiles and assigning them to the service. For example<sup>25</sup>:

```
> PROFILE L2CONTROL new-eplan
> STP TUNNEL
> GVRP DISCARD
> EXIT
```

<sup>25</sup> When a new profile is created, the default for all protocols is TUNNEL. Any protocol not specified in the profile will be tunneled (if allowable for the service).



This profile can then be applied to the UNI:

This profile can then be applied to the UNI:

```
> UNI gig 1/1/8
> SET PROFILE L2CONTROL new-eplan
> EXIT
```

## 6.2.9 Sample Eservices configuration

First, select the virtual switch that the packetVX is a member of.

```
BTI7000> enable
BTI7000#
BTI7000# configure terminal !enter global configuration mode
BTI7000(config)#
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)#
```

Create the NNI, and then create the UNI or UNIs as described in [6.1.2.1, “Sample UNI configuration”](#).

**Note** If the Ethernet service spans multiple packetVX nodes, it will have to traverse NNIs between those nodes. It is not necessary to explicitly associate the NNIs with each Ethernet service, since this is done automatically using the GVRP protocol; however, the NNIs must be created.

Next, create the Eservice using the ESERVICE command.

```
BTI7000:sw1(config)# eservice <name> type [EPLINE | EVPLINE | EPLAN | EVPLAN
| EPTREE | EVPTREE]
```

**Table 6-1 Ethernet service options**

Service	Description
EPLINE (Ethernet Private Line)	Port-based VLAN mapping, MAC learning enabled for VLAN.
EPLAN (Ethernet Private LAN)	Port-based VLAN mapping, MAC learning enabled for VLAN.
EPTREE (Ethernet Private TREE)	C-VLAN to S-VLAN mapping, MAC learning enabled, restricted forwarding for leaf UNIs.
EVPLINE (Ethernet Virtual Private LINE)	C-VLAN to S-VLAN mapping, MAC learning enabled for VLAN.
EVPLAN (Ethernet Virtual Private LAN)	C-VLAN to S-VLAN mapping, MAC learning enabled for VLAN.
EVPTREE (Ethernet Virtual Private TREE)	C-VLAN to S-VLAN mapping, MAC learning enabled, restricted forwarding for leaf UNIs, service multiplexing allowed on root UNI(s).

The critical parameters for definition of an ethernet service include the following:

- Service name (on the ESERVICE command)
- Service type (on the ESERVICE command)

- S-VLAN ID
- Listing of UNIs
- Spanning tree instance (when needed)

For example:

```
BTI7000:sw1(config)# eservice test type EPLINE
BTI7000:sw1(config-eservice)# s-vlan 113
BTI7000:sw1(config-eservice)# uni gig 1/1/7
BTI7000:sw1(config-uni-eservice)# exit
BTI7000:sw1(config-eservice)# spanning-tree 2
BTI7000:sw1(config-eservice)# exit
```

**Important** The default VLAN map for multiple spanning tree (MSTP) has all VLANs in instance 0 (the common spanning tree). If a service is put into an instance other than 0, that vlan-to-instance mapping must be configured on every bridge in the MSTP region (other than the bridges containing the UNIs since they already have the mapping) otherwise other bridges will end up in different regions and forwarding will not follow the expected paths. This can be done by configuring all bridges as follows:

```
> SPANNING-TREE MST CONFIGURATION
> INSTANCE <n> VLAN <a-b> (e.g. INSTANCE 2 VLAN 101-200)
> EXIT
```

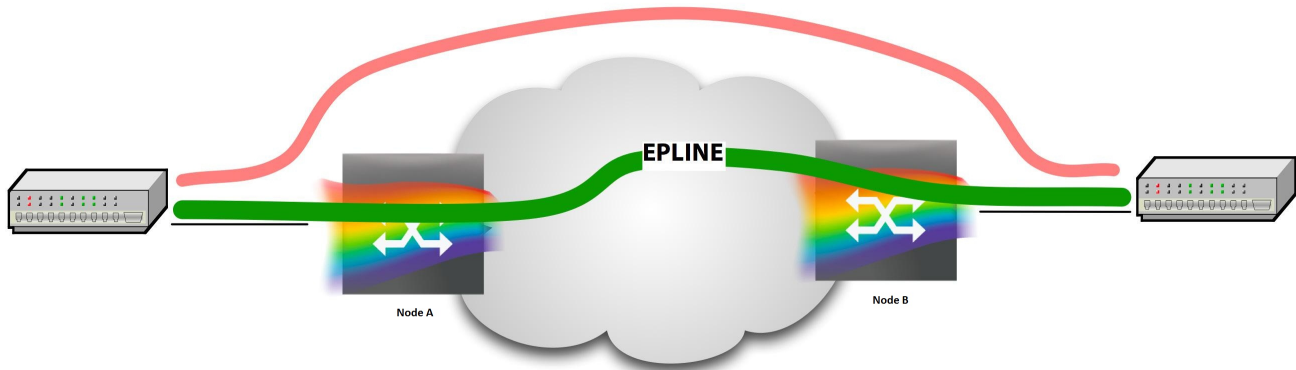
**Note** For step-by-step Eservice provisioning information, see [6.3.4, “Provisioning Eservices”](#).

## 6.2.10 Ethernet Fault Propagation Shut Down

Frequently, subscriber devices are designed to be connected by a pair of connections—one providing the working connection and one providing the protecting path, to use in case the working path fails. This is a common mechanism between SONET/SDH devices. The two devices monitor the working link, and, when a loss of signal or loss of framing or other failure is detected, they switch over to the protecting link.

There is a problem when the working link is carried over an Ethernet service--refer to the following figure. A failure on one UNI is not seen at the other UNI because they are not connected. A failure in the middle of the Ethernet network is not detected at either UNI. In both of these cases the switchover to the protection link does not occur.



**Figure 6-8 Ethernet Fault Propagation Shutdown Usage****Protect path - may go through Ethernet cloud or not**

Ethernet Fault Propagation Shutdown (E-FPSD) addresses this issue. When enabled on a service-UNI, that UNI (in cooperation with the other UNI) monitors both the remote UNI and the network path between them. If a fault is detected, the UNI turns off its transmit laser--within about three seconds--which forces the local device to detect the failure and switch to the protecting path. When the fault is repaired, the laser is turned on (after a short settling period to avoid bouncing) and the subscriber device can switch back to the working path. Note that the actual switching decisions are made by the subscriber devices, and not the Ethernet switches.

E-FPSD can only be used on optical UNIs (not copper) and only for EPLINE services. E-FPSD can be enabled on both UNIs of the service.

E-FPSD is configured on a service-UNI as follows:

```
> ESERVICE xxx
> UNI gig 1/2/3
> EFPSD ENABLE
> EXIT
> EXIT
```

## 6.3 Ethernet services provisioning

---

This section describes the procedures required to provision Eservices using the Eservices model.

### 6.3.1 Define a UNI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- Add the packetVX equipment to a virtual switch.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Global Configuration mode

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier. For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 4 Create a UNI

To create the UNI, enter the following command:

```
BTI7000(config)#uni <gigabitEthernet|tenGigabitEthernet>  
<shelf/slot/port> | <lag> <lag number>
```

#### Step 5 Define the UNI's maximum frame size

To define the UNI's maximum frame size, enter the following command:

```
BTI7000:sw1(config-uni GigE 1/1~)#frame-size<frame size>
```

### CLI command example:

```
uni GigabitEthernet 1/1/1
frame-size 2048
exit
```

When a UNI is switched through a NNI, the bridging protocol adds bytes to the UNI frame. If the specified UNI frame size plus the bridging protocol bytes exceeds 9600 bytes, the frames cannot pass. The following table specifies the maximum allowable UNI frame size for the bridge mode.

Bridge mode	Maximum frames at NNI	Maximum frames at UNI
802.lad Provider bridge	9600 bytes	9596 bytes

You have successfully completed this procedure.

## 6.3.2 Define an NNI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

This procedure describes how to define an NNI.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Global Configuration mode

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Create a NNI

To create a NNI, enter the following command:

```
BTI7000(config)# nni <gigabitEthernet |
tenGigabitEthernet> <shelf/slot/port> |
<lag> <lag number>
```

### Step 4 Define the NNI's maximum frame size

To define the NNI's maximum frame size, enter the following command.

```
BTI7000:sw1(config-nni TenGigE 1/1~)#frame-size <frame size>
```

**CLI command example:**

```
nni tenGigabitEthernet 1/1/2
frame-size 9600
exit
```

You have successfully completed this procedure.

### 6.3.3 Define an E-NNI and OVC

The following rules apply :

- The E-NNI SVLAN ID must be agreed on with the service provider
- GVRP is disabled on the E-NNI port but is supported on the OVC
- MSTP is disabled on the E-NNI port
- It is recommended to set the OVC Maximum Transmission Unit Size to at least 2000 bytes. It must be less than or equal to the E-NNI MTU size. When an E-NNI frame is larger than the OVC MTU that is mapped to an OVC, then the frame must be discarded. If an OVC is part of the EVC its MTU should be set to at least the MTU size of the EVC .

**Note** E-NNI traffic is controlled by S-VLAN which maps traffic independently of service type. Therefore Access EPL and EVPL service instances can be assigned to the same E-NNI port. An Access EPL service is port based at the End UNI. Therefore the UNI bandwidth profile must be set in compliance with Access service Bandwidth profile to prevent excessive traffic loads and the possibility of packets being dropped.

Once an E-NNI is created, the system will automatically configure the E-NNI port as a **provider network port external** switchport.

**Step 1 Creat the E-NNI :** Use the command **E-NNI** <interface-type> <interface-id> to create an E-NNI.

**Note** Once the E-NNI is created it will follow the provisioning features listed in xref.

```
BTI7000:sw1# configure terminal
BTI7000:sw1(config)# E-NNI tenGig 1/3/1
BTI7000:sw1(config e-nni)# show

E-NNI GigE 1/3/1:
Virtual Switch is 1
Admin Status is enabled, Operational Status is down
full duplex, 1000Mb/s
Max frame size is 9600
Port type is (E-NNI)
PVID is 1
Provider tag ethertype (TPID) is 88A8
```

```
useDEI is enabled
Trust Incoming PCP is enabled
Trust Incoming DSCP is enabled
Storm-control:
  broadcast: disabled
  multicast: disabled
  unicast-dlf: disabled
Profiles:
  Scheduler: "DEFAULT_SCHEDULER_PROFILE"
  Priority Traffic Class Map: "DEFAULT_PRIORITY_TC_MAP_PROFILE"
  PCP Encoding/Decoding: "DEFAULT_8P0D_PROFILE"
```

**Note** Use the following commands to configure the E-NNI requirements :

#### Commands

<code>default {frame-size   s-tag-ethertype }</code>	This command resets the maximum frame size back to its default value and resets the Tag Protocol ID (TPID) for the service provider tag.
<code>[no] frame-size &lt;bytes&gt;</code>	This command sets the maximum frame size of the E-NNI.
<code>[no default] s-tag-ethertype &lt;tag-id&gt;</code>	This command sets the tag protocol id (TPID) for the service
<code>set profile dscp-phb &lt;name&gt;</code>	This command sets the E-NNI to use the DSCP PHB profile specified by name
<code>[un]set profile pcg-encoding-decoding &lt;name&gt;</code>	This command sets the E-NNI to use the specified PCP Encoding/Decoding profile.
<code>[un]set profile priority-tc-map &lt;name&gt;</code>	This command sets the port to use the specified Priority Traffic Class Map profile.
<code>set profile scheduler &lt;name&gt;</code>	This command sets the E-NNI to use the specified scheduler profile.
<code>[no] storm-control {broadcast multicast unicast}&lt;rate&gt;</code>	This command configures line rate limits to manage egress traffic on E-NNI ports, caused by excessive ingress Broadcast, Multicast and Unicast DLF traffic.
<code>trust-incoming-dscp {enable disable}</code>	This command sets the E-NNI switchport to trust or not trust the incoming packet's DSCP field
<code>trust-incoming-pcp {enable disable}</code>	This command sets the E-NNI switchport to trust or not trust the incoming packet's PCP field.
<code>usedei {enable disable}</code>	This command sets the E-NNI switchport to use DEI bit on the S-TAG to lookup the PCP decoding table.

#### Related commands :

`admin-state {enable|disable}`  
`[no] shutdown`

## Step 2 Create the OVC

The Access eservice and eservice type must be created. To create an OVC you must change the existing service from an EVC to an OVC, using the **access enable** command

and assign an SVLAN to the access service. E-NNI's must be explicitly added to OVC's. They cannot be dynamically discovered as GVRP is disabled on the E-NNI.

```
BTI7000:sw1# configure terminal
BTI7000:sw1(config)# eservice Cust2014 type EPLINE
BTI7000:sw1(config-eservice)# access enable
BTI7000:sw1(config-eservice)# s-vlan 1024 [Note : The access EPLINE
eservice is now created and the OVC has been created with an S-VLAN of
1024]
BTI7000:sw1(config-eservice)# E-NNI 1/3/1
BTI7000:sw1(config-E-NNI-eservice)#
```

### Step 3 Set ingress and egress bandwidth profile per OVC

Ingress and egress bandwidth profile is applied to all ingress / egress service frames that are mapped to the OVC.

**Note** The ingress CIR for an OVC at the E-NNI should be greater than the corresponding ingress CIR at the UNI due to the presence of the added SVLAN tag (4 bytes) at the E-NNI. As an example, if the average frame size was 200 bytes, the CIR should be increased by 2%. MEF Bandwidth Profile traffic parameters such as CIR count only Service Frame bits, not interframe gap or preamble bits.

The bandwidth profile must be created before issuing this command. For example this command shows how to create a bandwidth profile named OVCGOLD and displays its provisionable attributes.

```
BTI7000:sw1(config)# profile bandwidth OVCGOLD
Profile "platinum" created.
BTI7000:sw1(config-profile-bw)# ?
conform-action      - Configure action for the bandwidth profile
exceed-action       - Configure action for packets exceeding CIR limits
internal-priority   - Configure the internal priority value
meter 1             - Configure the Meter engine
police              - Configure the Committed Information Rate
                    - cbs
                    - cir
                    - ebs
                    - eir
```

<sup>1</sup>The meter mode must be set to two rated TCM mode in the ingress bandwidth profile and single rated TCM mode in the egress bandwidth . The meter mode cannot be modified after the bandwidth profile has been added.

After the bandwidth profile has been created it will be displayed as an option when setting the ingress and egress as shown in the following example.

```
BTI7000:sw1(config-E-NNI Gige 1/3/1)# set ingress profile bandwidth ?

- 100MEG
- OVCGOLD
- BRONZE
- SILVER
```

```
BTI7000:sw1(config)# eservice Cust2014
BTI7000:sw1(config-eservice)# E-NNI gigabitEthernet 1/3/1
BTI7000:sw1(config-E-NNI-eservice)# set egress profile bandwidth
OVCGOLD
BTI7000:sw1(config-E-NNI-eservice)# set ingress profile bandwidth
OVCGOLD
```

#### **Step 4 Set ingress and egress service-policy per OVC**

Ingress and egress bandwidth profile is applied to all ingress / egress service frames that are mapped to the OVC.

The service policy must be created before issuing this command. For example this command shows how to create a class-map named ALL and its provisionable attributes. The service policy is created and assigned a class map.

```
BTI7000:sw1(config)# class-map ALL
BTI7000:sw1(config-c-map)#
BTI7000:sw1(config-c-map)# match
c-vlan          - Configure C-VLAN filter
c-vlan-priority - Set priority for the C-Vlan filter
ethertype       - Set EtherType filter
ip              - Set the IP filter
mac             - Set the MAC address filter
s-vlan-priority - Set priority for the S-Vlan filter
tcp-control     - Set the TCP control filter
tcp-udp-port    - Set the TCP/UDP port filter
```

```
BTI7000:sw1(config)# service-policy Cust1 [Note : Create a service
policy]
BTI7000:sw1(config-p-map)# ALL [Note : Assign a class-map to the
service policy]
```

After the service policy has been created it will be displayed as an option when setting the ingress and egress as shown in the following example.

```
BTI7000:sw1(config-E-NNI-eservice)# service policy?
  <string>          - Profile name (the following are provisioned):
                    - test
                    - Cust1
BTI7000:sw1(config-E-NNI-eservice)#

BTI7000:sw1(config)# eservice Cust2014
BTI7000:sw1(config-eservice)# E-NNI gigabitEthernet 1/3/1
BTI7000:sw1(config-E-NNI-eservice)# set egress service policy CUST1
BTI7000:sw1(config-E-NNI-eservice)# set ingress service policy test
```

#### **Step 5 Perform internal to external VLAN translation**



```
BTI7000:sw1(config-E-NNI-eservice)# external-vlan 777
BTI7000:sw1(config-E-NNI-eservice)#
```

Performing the above command will enable the S-VLAN translation to switch between one provider's SVLAN to another. The OVC is running over S-VLAN 1024. At the ingress and egress of the ten 10G E-NNI [1/3/1], the S-VLAN ID in the outer tag will be translated to and from 777. At the other end of the E-NNI boundary, the partner service provider must also define an S-VLAN translation between its local S-VLAN and external S-VLAN 777. The translation S-VLAN must be the same on both E-NNI interfaces for the service to work.

## Step 6 Set ingress and egress bandwidth profile on E-NNI

Ingress / egress bandwidth profile, is applied to all ingress/ egress frames of all OVCs at the E-NNI.

The bandwidth profile must be created before issuing this command. For example this command shows how to create a bandwidth profile named Platinum and displays its provisionable attributes.

```
BTI7000:sw1(config)# profile bandwidth platinum
Profile "platinum" created.
BTI7000:sw1(config-profile-bw)# ?
conform-action      - Configure action for the bandwidth profile
exceed-action       - Configure action for packets exceeding CIR limits
internal-priority   - Configure the internal priority value
meter              - Configure the Meter engine
police              - Configure the Committed Information Rate
```

The meter mode must be set to two rated TCM mode in the ingress bandwidth profile and single rated TCM mode in the egress bandwidth. After the bandwidth profile has been created it will be displayed as an option when setting the ingress and egress as shown in the following example.

```
BTI7000:sw1(config-E-NNI Gige 1/3/1)# set ingress profile
bandwidth ?
```

- 100MEG
- OVCGOLD
- BRONZE
- SILVER
- PLATINUM

```
BTI7000:sw1(config)# E-NNI gigabitEthernet 1/3/1
BTI7000:sw1(config-E-NNI Gige 1/3/1)# set egress profile bandwidth
PLATINUM
BTI7000:sw1(config-E-NNI Gige 1/3/1)# set ingress profile bandwidth
PLATINUM
```

Related commands : BTI7000:sw1(config)# show profile bandwidth <name>

## Step 7 Set ingress and egress service policy per CoS

Ingress / egress bandwidth profile is applied to the ingress / egress frames with a specific CoS identifier for an OVC at the E-NNI.

```
BTI7000:sw1(config)# eservice Cust2014
BTI7000:sw1(config-eservice)# E-NNI gigabitEthernet 1/3/1
BTI7000:sw1(config-E-NNI-eservice)# set ingress service-policy insp
BTI7000:sw1(config-E-NNI-eservice)#
```

```
BTI7000:sw1(config)# eservice Cust2014
BTI7000:sw1(config-eservice)# E-NNI gigabitEthernet 1/3/1
BTI7000:sw1(config-E-NNI-eservice)# set egress service-policy egsp
BTI7000:sw1(config-E-NNI-eservice)#
```

### **Step 8 View E-NNI configuration**

Perform the following command to view E-NNI Service configuration, E-NNI membership and E-NNI S-VLAN translation information.

```
BTI7000:sw1# Show running configuration
```

```
interface gigabitEthernet 1/3/1
  admin-state enable
  circuit-id
  loopback facility off
  mtu 9600

switchport gigabitEthernet 1/3/1
  admin-state disable
  acceptable-frame-type tagged
  port-type providernetworkport external
  set egress profile bandwidth platinum
  set profile pcg-encoding-decoding DEFAULT_8P0D_PROFILE
  set profile priority-tc-map DEFAULT_PRIORITY_TC_MAP_PROFILE
  set profile scheduler DEFAULT_SCHEDULER_PROFILE
  trust-incoming-dscp enable
  trust-incoming-pcp enable
  usedei enable
  exit

E-NNI gigabitEthernet 1/1/14

  eservice "Cust04"
    set egress profile bandwidth " "
    set egress service-policy " "
    set ingress profile bandwidth " "
    set ingress service-policy " "
  exit
exit
```

```

profile bandwidth "GOLD"
  exceed-action set-dei enable
  meter mode tr-tcm color blind
  police cbs 256
  police cir
  police ebs
  police eir
  exit

eservice "Cust2014" type EPLINE
  s-vlan 1024
  admin-state enable
  access enable
  c-vlan-translate disable
  cfm crosscheck enable
  cfm interval 1min
  cfm me v1024
  lock-nni disable
  exit
external-vlan 777

switchport gigabitEthernet 1/1/14

  spanning-tree 0
    cost 20000
    exit
  exit

```

### 6.3.4 Provisioning Eservices

This procedure describes how to provision Eservices and associate member UNI ports to them. This procedure is used for MEF-based Eservice provisioning.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Pre-requisites:

- Create a Virtual Switch.
- Add a packetVX as a member.
- To provision an Ethernet service, the switch must be configured as a provider bridge.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Global Configuration mode**

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Create a NNI**

See [6.3.2, “Define an NNI”](#).

**Step 4 Create a UNI**

See [6.3.1, “Define a UNI”](#).

**Step 5 Create the Eservice**

To create the Ethernet service, enter the following command:

```
BTI7000:sw1(config)#eservice <string> type <EPLINE | EPLAN | EVLINE |  
EVPLAN | ERPS | EPTREE | EVPTREE | MGMVLAN>
```

For example:

```
eservice CustomerA type EPLAN
```

The following table describes each Ethernet service option.

**Table 6-2 Ethernet service options**

Service	Description
EPLINE (Ethernet Private Line)	Port-based VLAN mapping, MAC learning enabled for VLAN.
EPLAN (Ethernet Private LAN)	Port-based VLAN mapping, MAC learning enabled for VLAN.
EPTREE (Ethernet Private TREE)	C-VLAN to S-VLAN mapping, MAC learning enabled, restricted forwarding for leaf UNIs.
EVPLINE (Ethernet Virtual Private LINE)	C-VLAN to S-VLAN mapping, MAC learning enabled for VLAN.
EVPLAN (Ethernet Virtual Private LAN)	C-VLAN to S-VLAN mapping, MAC learning enabled for VLAN.
EVPTREE (Ethernet Virtual Private TREE)	C-VLAN to S-VLAN mapping, MAC learning enabled, restricted forwarding for leaf UNIs, service multiplexing allowed on root UNI(s).

**Step 6 Define the maximum frame size for the Ethernet service**

The frame size affects the interface and Eservice frame size. For example, if you set the interface frame size to 1500, then the UNI or Eservice frame size must be 1500 or less.

To define the maximum frame size, enter the following command:

```
BTI7000:sw1(config-eservice)#frame-size <frame size>
```

For example:

```
frame-size 9600
```

#### Step 7 Define the S-VLAN for the Ethernet service

To define the S-VLAN, enter the following command:

```
BTI7000:sw1(config-eservice)#s-vlan <vlan-id>
```

For example:

```
s-vlan 100
```

#### Step 8 Associate UNI(s) to the Ethernet service

To associate UNIs, enter the following command:

```
BTI7000:sw1(config-eservice)#uni<gigabitEthernet|tenGigabitEthernet|lag><shelf/slot/port>
```

For example:

```
uni gig 1/1/1
```

#### Step 9 Enable FPSD on the UNI (optional)

Enter the following command:

```
BTI7000:sw1(config-eservice)#efpsd enable
```

#### Step 10 Define the forwarding mode of the UNI (optional)

Enter the following command:

```
forwarding {normal|etree-leaf}
```

For example:

```
BTI7000:sw1(config-eservice)#forwarding etree-leaf
```

#### Step 11 Define TPID {aware | blind} (optional)

Enter the following command

```
BTI7000:sw1(config-uni-eservice)# tpid blind
```

**Note** This command either discards incoming frames with TPID 0X88A8 and other Tag Protocol Identifiers (TPIDs) will be transmitted {aware} or configures all customer frames as un-tagged and transmits frames to peer UNIs {blind}. This command is configured on EPLAN and EPLINE services and is provisioned using the CLI only. The default setting is aware.

You have successfully completed this procedure.

**Note** The NNI port is automatically added to the Eservice by the GVRP protocol.

## 6.4 Provisioning profiles

---

This section provides information about provisioning profiles.

### 6.4.1 Layer 2 Control Frame Profile provisioning

This procedure explains how to provision layer 2 control frame profiles for the switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- A Virtual Switch must be created and selected.

#### Step 1 Open or create a layer 2 control frame profile

To either open or create a layer 2 control frame profile, enter the following command:

```
enable
```

```
BTI7000# configure terminal
```

```
BTI7000 (config)#
```

```
BTI7000:(config)# profile l2control <profile-name>
```

For example, the command string might be

```
BTI7000:(config)# profile l2control NoDotX
```

The CLI prompt should appear as follows:

```
BTI7000:(config-profile-l2c NoDotX)#
```

#### Step 2 Display the current profile

To display the current profile, enter the following command:

```
show
```

For example, the display might be

```
L2 Control Profile: NoDotX
```

```
Dot1x: tunnel
```

```
GMRP: tunnel
```

```
GVRP: tunnel
```

```
LACP: tunnel
```

```
STP : tunnel
```

#### Step 3 Configure the switch to peer at 802.1x frames

To configure the switch to peer at 802.1x frames, enter the following command:

```
dot1x peer
```

#### Step 4 Configure spanning tree frames to tunnel

To configure spanning tree frames to tunnel, enter the following command:

```
stp tunnel
```

**Step 5 Configure the switch to peer at LAG frames**

To configure the switch to peer at LAG frames, enter the following command:

```
lacp peer
```

**Step 6 Display the current profile**

To display the current profile, enter the following command:

```
show
```

For example, the display should be

```
L2 Control Profile: NoDotX
Dot1x: peer
GMRP: tunnel
GVRP: tunnel
LACP: peer
STP: tunnel
```

**Step 7 Exit from the current command configuration mode**

To exit from the current command configuration mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows

```
BTI7000:sw1(config)#
```

**Step 8 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 9 Create a switchport for a GE interface**

To create a switchport for a GE interface, enter the following command:

```
switchport <interface-type> <interface-id>
```

For example, the command string might be

```
switchport gigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-sp 1/1/1)#
```

**Step 10 Apply the control frame profile to the port**

To apply the control frame profile to the port, enter the following command:

```
set profile l2control <profile-name>
```

For example, the command string might be

```
set profile l2control NoDotX
```

**Step 11 Display the current switchport**

To display the current switchport, enter the following command:

```
show
```

For example, the display could be

```
Switchport GigE 1/1/1:
  Virtual Switch is 1
  Admin Status is up, Operational Status is notPresent
  Port type is Customer Edge Port (UNI)
  Default Priority is 0
  useDEI is disabled
  Trust Incoming PCP is enabled
  Trust Incoming DSCP is enabled
  Profiles:
    Control Frame:           "DEFAULT_CEP_PROFILE"
    Scheduler:               "DEFAULT_SCHEDULER_PROFILE"
    Priority Traffic Class Map: "DEFAULT_PRIORITY_TC_MAP_PROFILE"
    PCP Encoding/Decoding:   "DEFAULT_8P0D_PROFILE"
```

**Step 12 Exit from the current command configuration mode**

To exit from the current command configuration mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 13 Apply the L2 Control Protocol Profile to a UNI.**

All services on UNI must share the same profile, so the profile is assigned to the UNI itself (rather than the ESERVICE or the ESERVICE-UNI).

Enter the following commands:

```
uni gigabitethernet <shelf/slot/port>
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-UNI gig 1/1/7)#
set profile l2control nodotx
exit
```

You have successfully completed this procedure.



## 6.4.2 Tunnel MAC Address Profile provisioning

This procedure describes how to provision Tunnel MAC address profiles for the switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- A Virtual Switch must be created and selected.

### Step 1 Provision a Tunnel MAC address profile .

To provision a tunnel MAC address profile, enter the following command:

```
BTI7000:sw1(config)# profile tunnel-mac-address CustA
BTI7000:sw1(config-profile-tma)# dot1x 01.00.de.ad.be.ef
```

### Step 2 Display the current profile

To display the current profile, enter the following command:

```
BTI7000:sw1(config-profile-tma)# show
```

For example, the display might be

```
Tunnel MAC Address Profile: CustA
Dot1x Tunnel MAC Address:    01-00-de-ad-be-ef
GMRP Tunnel MAC Address:    01-00-0c-cd-cd-d2
GVRP Tunnel MAC Address:    01-00-0c-cd-cd-d1
LACP Tunnel MAC Address:    01-00-0c-cd-cd-d4
STP Tunnel MAC Address:     01-00-0c-cd-cd-d0
```

You have successfully completed this procedure.



## 7.0 Configuring Ethernet Services OAM

---

BTI™ packetVX® modules are designed to facilitate the delivery of Ethernet services (Eservices) to subscribers. The provisioning model for packetVX is centered on the concept of Eservices. This includes MEF service types such as EPLINE, EVPLINE, EPLAN, and EVPLAN. Further, to simplify the configuration of Eservices, packetVX utilizes dynamic signaling to configure intermediate nodes.

Once Eservices are established end-to-end, monitoring is provided utilizing the OAM mechanisms defined in ITU-T Recommendation Y.1731 and IEEE 802.1ag. These protocols use continuity check messages (CCMs) to monitor the connectivity of Eservices.

**Note** For Ethernet OAM on an ERPS service, see [Chapter 11, “Configuring Ethernet Ring Protection Switching \(ERPS\)”](#).

This section covers the following topics:

- [7.1, “Ethernet Service OAM”](#)
- [7.2, “Loopbacks and linktrace”](#)
- [7.3, “Ethernet Service OAM configuration”](#)
- [7.4, “Interoperability considerations with third-party devices”](#)
- [7.5, “Advanced procedures — Global settings”](#)
- [7.6, “Advanced procedures — Eservice settings”](#)
- [7.7, “Troubleshooting”](#)

## 7.1 Ethernet Service OAM

Ethernet Service OAM (operations, administration, and maintenance) is a new concept for Ethernet networks not supported by older generation technology. While older generations of technology are capable of transporting Ethernet frames, they are not capable of providing useful information when a problem occurs. In particular, if a link goes down in the network, there is no indication which services on the network are affected.

Two protocols are defined to provide Ethernet Service OAM functions: ITU-T and IEEE 802.1ag:

- **ITU-T:** Defines standard Y.1731 to address the functions of Connectivity/Fault Management (CFM) and Performance Management (PM). CFM deals with path integrity between end-points in a service. PM deals with performance attributes of the path such as delay, delay variation, and frame loss rate.
- **IEEE 802.1ag:** Defines a protocol that covers only CFM.

The two standards are extremely similar. They differ in some terminology and have a few small and subtle differences in the way the protocol messages are encoded. The following table provides a translation between 802.1ag and the Y.1731 terms used in this document.

**Table 7-1 CFM terminology**

IEEE 802.1ag term	ITU Y.1731 term	Description
MA (Maintenance association)	ME (Maintenance entity)	ME represents an entity that requires management and is a relationship between to MEPs.
MD (Maintenance domain)	MEG (Maintenance entity group)	Consists of MEs that belong to the same service inside a common OAM domain
MEP (Maintenance association end point)	MEP (Maintenance entity group end point)	Resides at the edge of an ME and confine CFM messages within the domain via the MEG level. Periodically transmit and receive continuity check messages (CCMs) from other MEPs within the ME. Each MEP has a unique MEP ID (1-8191) in the ME.
MIP (Maintenance domain intermediate point)	MIP (Maintenance entity group intermediate point)	Passive point within a MEG that catalogs and forwards information received from MEPs. Responds only to CFM linktrace and loopback messages. Has only one level associated with it.
MEL (MEG Level)	MEL (MEG Level)	In the OAM frame, distinguishes between the OAM flows of nested MEGs

The switch supports the following CFM protocol messages: continuity check (CCMs), loopback messages (LBMs) and replies (LBRs), and linktrace messages (LTMs) and replies (LTRs). For information about loopback and linktrace, see [7.2, “Loopbacks and linktrace”](#).

### CCMs

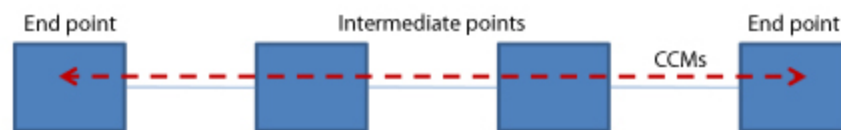
CCMs are multicast or unicast messages exchanged among MEPs that let MEPs discover other MEPs within an ME.

CCMs have the following characteristics:

- Transmitted at periodic intervals by MEPs
- Terminated by remote MEPs at the same level
- Unidirectional
- Indicate the status of the bridge port on which the MEP is configured

packetVX modules use continuity check messages (CCMs) to monitor the status of Eservices across the network. The CCMs non-intrusively monitor end-to-end connectivity. If connectivity is lost (determined by the loss of three consecutive CCM messages), the system reports an Eservice as down. If an Eservice goes down, the system reports the total unavailable seconds (UAS). This is useful information for service providers as they need to report on their conformance to SLA agreements with their customers.

The following figure illustrates the use of CCMs to test the continuity of an Eservice.



### CFM and Eservices

An Eservice is identified by an S-VLAN and a globally unique service ID. An Eservice can be point-to-point (E-LINE) or multipoint-to-multipoint (E-LAN).

The packetVX supports CFM on Eservice MEs only.

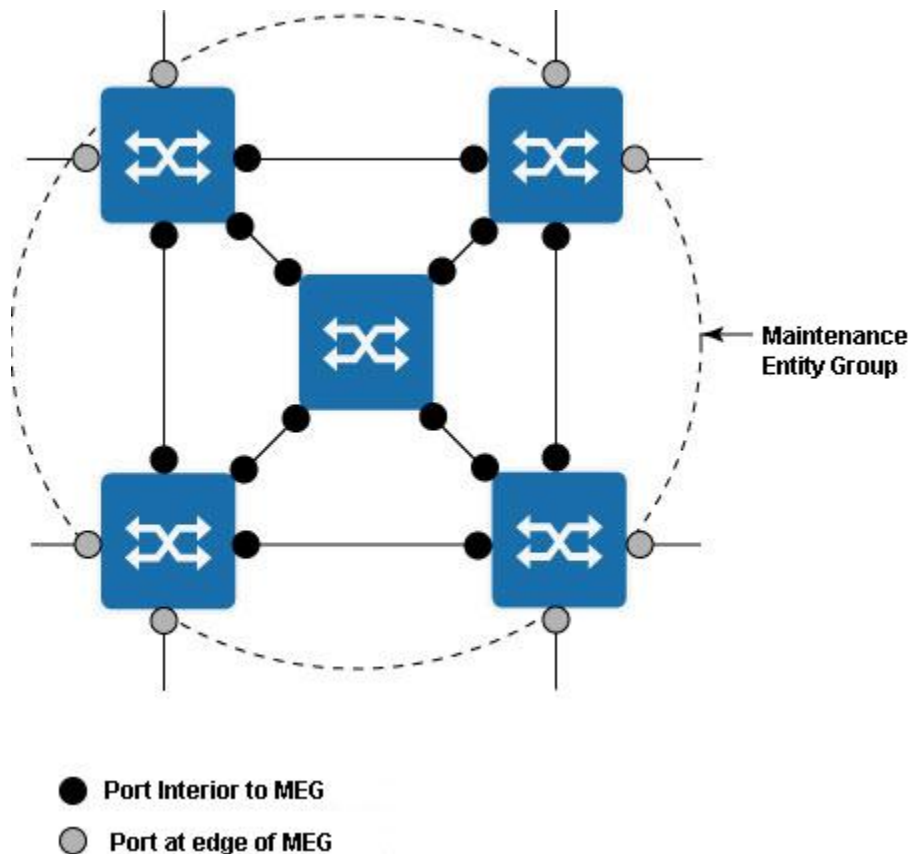
When CFM is enabled, the following OAM functions are automatically provided for Eservice MEs:

- The operational status of each Eservice: up, down, or partially connected
- The number of UNIs associated with the same Eservice. If the number of end points changes, a trap is generated.
- The UAS (unavailable seconds) for the same Eservice
- The following alarms for each Eservice:
  - Loss of continuity
  - Mismatch and unexpected MEG level
  - Unexpected MEP
- The following diagnostic tools:
  - loopback
  - linktrace

## Maintenance Entity Group (MEGs)

A MEG is a group of MEP associations that is owned and operated by a single entity<sup>26</sup>. As shown in the following figure, a MEG is defined by the set of ports internal to it and at its boundary.

**Figure 7-1 Typical MEG**



Each MEG has a unique MEG ID (that uniquely identifies the Ethernet service in the network). The MEG ID consists of the Unique MEG Code (UMC) and the ITU Carrier Code (ICC). In BTI 7000 Series equipment, the UMC is configured as the MEG name, and the ICC is configured as the ME name. The MEG name must be configured on a switch and the ME name must be configured on an Ethernet service before MEPs can be configured. By default, the MEG name is "BTI", and the ME name is "v" appended by the S-VLAN ID for the service.

You should be familiar with these guidelines before configuring MEG and ME names:

- The MEG name is configured on a virtual switch. All virtual switches in the network must have the same MEG name.
- The configured MEG name is used as the Unique MEG Code (UMC) in service level CCMs in the UP direction.

<sup>26</sup> MEPs are created on the network side of the UNI, the UNI-N, and the CCMs reflect connectivity from UNI-N to UNI-N and do not reflect the actual state of the UNI. In the packetVX module, they do, however, carry information about the state of the UNI.

- The ME name is configured per Ethernet service on a virtual switch. The ME name uniquely identifies the service within the network. Therefore, the same ME name must be configured for the same Ethernet service on all switches in the network.
- The configured ME name is used as the ITU Carrier Code (ICC) in service level CCMs in the UP direction.

### **MEG level configuration considerations**

The MEG level provides a hierarchical relationship that parallels the structure of customer, service provider, and operator. For example, a customer MEG might have a maintenance level of 6, a service provider a MEG maintenance level of 4, and an operator MEG a maintenance level of 0. All levels of the hierarchy must operate together.

You should be familiar with these guidelines before configuring MEG levels:

- The MEG level is configured on a virtual switch, and it applies to both the MEPs and the MIPs.
- The configured MEG level is used in service level Y.1731 messages, and has a range from 2 to 4.
- The configured MEG level for all switches in the network must be the same.

### **MEG Intermediate Points (MIPs)**

A MEG Intermediate Point (MIP) is a provisioned OAM reference point capable of reacting to diagnostic OAM frames initiated by MEPs. The most notable capability is the ability to respond to an LTM to provide path information. MIPs do not initiate proactive or diagnostic OAM frames. The MEG level used in the response message is taken from the MEG level in the request message.

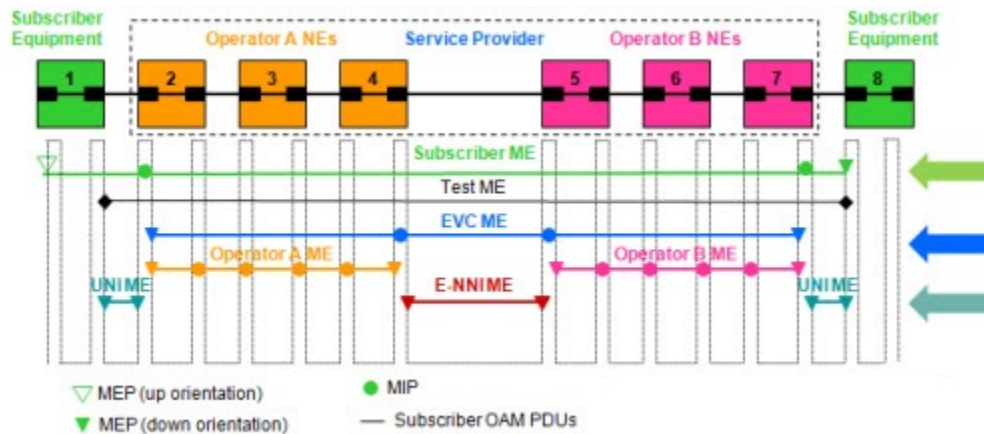
MIPs can be created automatically or manually. If MIPs are configured for auto-creation, they will be created by the switch on the NNI for each Eservice. Manually creating MIPs must be done by associating the NNI with an Eservice and creating the MIP in the NNI-Eservice configuration.

### **CFM and MEG levels**

When CFM is enabled, CFM messages are transmitted within a MEP, depending on the MEG level and MEP status (up or down).

CFM exchanges messages and performs operations on a per-MEG basis. For example, CFM can be run at the operator level; however, higher provider and customers levels will not allow network discovery.

The following figure and table show a typical hierarchy of operator, service provider, and customer MEGs.

**Figure 7-2 MEs in OAM domains**

Maintenance Entity	MEG Level
Customer	5 or 6
Provider	2, 3, or 4
Operator	0 or 1

**Note** The switch supports CFM on MEs only.

### CFM message processing

The following table describes how a MEP processes a CFM message, depending on the MEG level.

Level relative to MEP	Rules for processing
Same level	Process all CFM frames
Lower level	Drop all CFM frames
Higher level	Forward all CFM frames without further processing

### Implementation of CFM auto-discovery

When CFM monitoring is enabled on the switch, the CFM protocols automatically discover the ME, MEG, MIP, and MEPs that comprise an Eservice, their maintenance levels and names, and the remote end points of the Eservice. Automatic discovery enables the UNI to transmit the CFM CCMs periodically that announce the identity of the MEP. It also enables the UNIs to track the CCMs received from other remote MEPs. CFM adds the newly discovered remote MEP ID to the MEP list. Thus, CFM can discover the number of end points in an Eservice. When a UNI is removed from the Eservice, CFM notifies the other remote end points, the remote MEP list is flushed, and a discovery process is triggered.



## 7.2 Loopbacks and linktrace

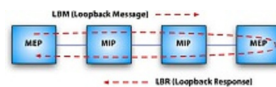
Ethernet Service OAM also includes two mechanisms for troubleshooting faults in Ethernet networks: loopback and linktrace.

### Loopback

Loopback is similar to an ICMP echo request (PING) in IP networks. A loopback request sends an Y.1731-formatted LBM (loopback message) from the local MEP (end point) to a remote MEP. The remote MEP responds with an Y.1731 LBR (loopback reply) to indicate that it has received the LBM. In this way, a service provider can test for end-to-end continuity of an Eservice.

The following figure illustrates the use of loopback messages.

**Figure 7-3 Loopback messages**

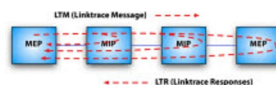


### Linktrace

Linktrace is similar to a traceroute request in IP networks. A linktrace request sends an Y.1731-formatted LTM (linktrace message) from the local MEP to a remote MEP. All intermediate points (MIPs) between the local MEP and the remote MEP respond to the LTM with an Y.1731-formatted LTR (linktrace reply), to indicate that it has received the LTM. In this way, a service provider can determine the exact path of an Eservice across their network. In addition, linktrace can be used to determine where a break in end-to-end continuity may have occurred.

The following figure illustrates the use of linktrace messages.

**Figure 7-4 Linktrace messages**



## 7.3 Ethernet Service OAM configuration

---

The design approach on packetVX modules is to make the configuration and operation of Ethernet Service OAM simple and intuitive. As a result, the majority of provisioning steps are performed automatically when an Eservice is created. Typically, the user needs to set only one parameter when the packetVX module is first configured.

packetVX modules have been designed so that the average user does not need to understand the terminology (MEPs, MIPs, MEGs, etc.).

### 7.3.1 Basic configuration using proNX 900



The majority of CFM provisioning steps are performed automatically when a new Ethernet service is created. Typically, only the Switch Name must be modified.

- Step 1** In the Navigation pane, expand the tree for the slot that corresponds to the location of the packetVX module.
- Step 2** Select the Packet Ethernet view, right click on **Switch: x**, and click **Provision Switch**.
- Step 3** In the **Switch** dialog, click on the **Advanced** tab and modify the following parameters as required:
- **Switch Name:** Used to provide a unique CFM name to the node/switch
  - **MEG Name:** Defines the MEG Name. This is used as the Unique MEG Code (UMC) in service level CCMs. Typically modified only for non-packetVX module interoperability.
  - **MIP Auto Creation:** When enabled (default), the packetVX module will automatically create MIPs on all the NNIs for all transiting Eservices.
  - **MEG ID Pad:** When enabled (default), the packetVX module will pad the ITU Carrier Code (ICC) with nulls to 6 bytes before concatenating the UMC.
  - **MEG Level:** Defines the CFM MEG Level for service level CCMs.

The screenshot shows the 'Advanced' tab of a configuration window. It contains several sections: 'Connectivity Fault Management' with fields for Switch Name (BTI\_1), MEG Name (BTI), MEG ID Pad (checked), MEG Level (4), and MIP Auto Creation (Enabled); 'Link Aggregation Control Protocol' with LACP System Priority (32767); 'Profiles' with Tunnel MAC Address (DEFAULT\_TMA\_PROFILE); 'Protocol Administrative State' with checkboxes for MSTP, LACP, GVRP, Y.1731, 802.1ag, ERPS, and SLA Measurement; and 'ERPS' with VLAN Propagate (Fast). At the bottom are 'Apply', 'Close', and 'Help' buttons.

**Step 4** Click **Apply**.

You have successfully completed this procedure.

## 7.3.2 Provisioning CFM and the CCM interval using the CLI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Pre-requisites:

- Create a virtual switch.
- Add a packetVX as a member.

At this point, CFM MIP auto-creation is enabled. If required, the switch name or MEG name can be changed. See [7.5.2, “Changing a MEG name and MEG level”](#)

- Provision an Ethernet service.

CFM is automatically enabled and packetVX starts sending CCMs after the Eservice is created and the UNI is associated with it.

The following example describes how to provision CFM and how to change the CCM interval from the 1-minute default to a 10-second interval.

### Step 1 Associate an S-VLAN with the Ethernet Service

```
BTI7000:sw1(config)# eservice MyEpline type epline
BTI7000:sw1(config-eservice)# s-vlan 10
```

### Step 2 Add a UNI to the Ethernet Service.

```
BTI7000:sw1(config-eservice)# uni gigabitethernet 1/1/1
```

At this point, CFM is automatically enabled, and CCMs are sent at 1 minute intervals by default.

**Step 3 Exit from the uni-eservice mode.**

```
BTI7000:sw1(config-uni-eservice)# exit
```

**Step 4 Change the CCM interval.**

```
BTI7000:sw1(config-eservice)# cfm interval 10sec
```

This changes the CCM interval from the 1-minute default setting to 10 seconds.

### 7.3.3 Basic configuration using the CLI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000 (config)#
```

**Step 3 Create a virtual switch**

To create a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

```
name <switch_name>
```

where

<switch\_id> is the virtual switch identifier

<switch\_name> is the name of the virtual switch

For example, the command string might be as follows:

```
virtual-switch 1 ABC_1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### 7.3.4 Viewing the operational state and unavailable seconds (UAS) of an Ethernet service using proNX 900

Authorization Required

Superuser

Provisioning

Maintenance

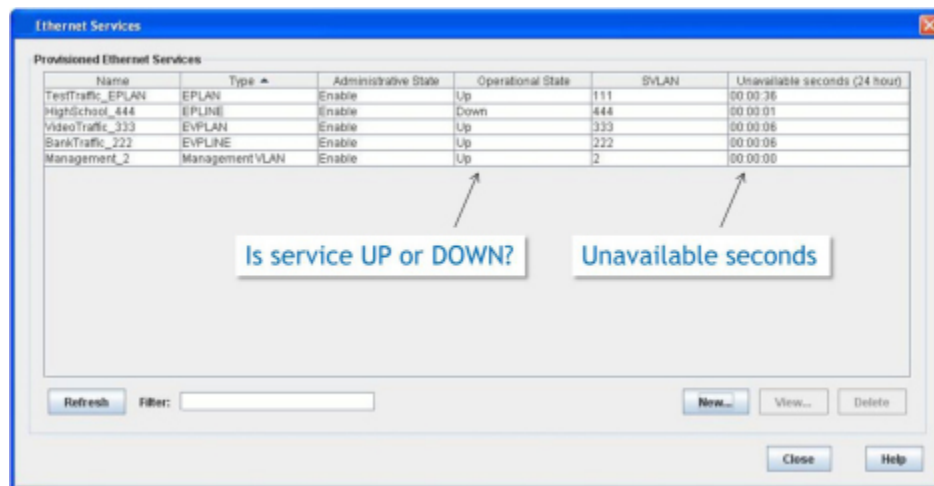
Surveillance

**Step 1** In the Navigation pane, expand the tree by clicking the + sign beside a switch.

**Step 2** Right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **View**.

Columns 4 and 6 display the operational state and unavailable seconds for the Eservice, respectively.



You have successfully completed this procedure.

### 7.3.5 Viewing the operational state and unavailable seconds (UAS) of an Ethernet service using the CLI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1** Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BT17000#
```

**Step 2** View the operational state of an Ethernet service

To view the operation state of an Ethernet service, enter the following command:

```
show eservice [<service-name>] [name <service-name> [brief]
```

where

<service-name> is the name of the Ethernet service

For example, the command string might be as follows:

```
BTI7000# show eservice TestTraffic_EPLAN
```

The Ethernet service settings are returned, including its operational state. For example:

```
Ethernet Service "TestTraffic_EPLAN"
  Virtual Switch is 1
  Service type is EPLAN
  Admin State is enable, Operational State is up
  S-VLAN is 111
  MSTP instance is 0
  Number of UNIs is 2
  Number of NNIs is 0
  Lock NNIs is disable
  Topology is multi-point
  Maximum frame size is 9600
  C-VID Translation is disable
  CFM Maintenance Entity Name is "v111"
  CFM Crosscheck is enabled
  CFM Continuity Check Message Interval is 1min
  EthService UAS : 0 hours 55 minutes 30 seconds

Associated UNIs:
  GigE 1/1/7
```

MEP Id	Type	Remote State	Remote Switch Name	Remote Port
5 (4584)	remote	ok	Node_108ES	Gig21/5/7
3 (4664)	remote	ok	Node_110	Gig1/1/7
1 (5454)	local	---	---	---
2 (5931)	remote	ok	Node_106	Gig1/1/7
4 (6006)	remote	ok	Node_107	Gig1/1/7
6 (6051)	remote	ok	Node_108MS	Gig1/1/7

```

Forwarding type is normal
EFPSD is disabled
TPID aware

Node-105:sw1(config)#
```

### Step 3 View the unavailable seconds for an Ethernet service

To view the unavailable seconds for an Ethernet service, enter the following command:

```
show eservice [<service-name>] pm {history {15-min|24-hour}} interval
{15-min [bin <bin>]|total}
```

where

`<service-name>` is the name of the Ethernet service

`<bin>` is the specific interval to show; 0 is the current interval

For example, the command string might be as follows:

```
BTI7000# show eservice test pm history 15-min
```

The unavailable seconds for the Ethernet service are returned. For example:

```
BTI7000> show eservice test pm history 15-min

BTI7000> show eservice test pm history 15-min
SW:1, E-Service: test
  Interval:15-min, Bin: Current
    EthService UAS : 0 hours 0 minutes 0 seconds

  Interval:15-min, Bin: 1
    EthService UAS : 0 hours 0 minutes 0 seconds

  Interval:15-min, Bin: 2
    EthService UAS : 0 hours 0 minutes 0 seconds

  Interval:15-min, Bin: 3
    EthService UAS : 0 hours 0 minutes 0 seconds

  Interval:15-min, Bin: 4
    EthService UAS : 0 hours 0 minutes 0 seconds

  Interval:15-min, Bin: 5
    EthService UAS : 0 hours 0 minutes 0 seconds

  Interval:15-min, Bin: 6
    EthService UAS : 0 hours 0 minutes 0 seconds

  Interval:15-min, Bin: 7
    EthService UAS : 0 hours 0 minutes 0 seconds
```

You have successfully completed this procedure.

### 7.3.6 Viewing the end points of an Eservice using proNX 900 Node Controller

- Step 1** In the Navigation pane, expand the tree by clicking the + sign beside a switch.
- Step 2** Right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **View**.
- Step 4** In the **View Ethernet Service** dialog, click the **CFM** tab.

- All available remote MEPs and the values for the following parameters are displayed in the **Remote MEPs** field:
  - **Remote Switch:** The name of the remote switch selected in Step 1
  - **Remote Port:** The physical port on which the remote UNI has been provisioned
  - **MEP ID:** The auto-generated MEP ID
  - **MAC Address:** The MAC Address of the physical port on the remote UNI
  - **State:** The connectivity status to the remote UNI. (Does not indicate the port status of the remote UNI)

Remote MEPs					
Remote Switch	Remote Port	MEP ID	MAC Address	State	
Node_126	Gig1/1/8	9995	08:14:60:00:3fa7	Ok	
Node_127	Gig1/1/8	9995	08:14:60:00:3fc5	Ok	
Node_128	Gig1/1/8	4815	08:00:00:00:01:08	Failed	
Node_130	Gig1/1/8	4535	08:14:60:00:46b7	Ok	

- All current defects and the values for the following parameters are listed in the **Defects** field:
  - **Loss of Continuity:** Raised after 3x missed CC messages
  - **Miss-merge:** Mismatched ME Name across the same Eservice
  - **Unexpected Period:** Crosscheck Interval mismatch between the two MEPs

Defects		
Defect	Remote MEP ID(s)	
Loss of Continuity	4815	
Remote MEP Defect	6095, 4535	

You have successfully completed this procedure.

### 7.3.7 Viewing the endpoints of an Eservice using the CLI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 View the endpoints of an Eservice

To view the endpoints of an Eservice, enter the following command:

```
show eservice [<service-name>] [brief]
```

where



<service-name> is the name of the Ethernet service

For example, the command string might be as follows:

```
BTI7000# show eservice TestTraffic_EPLAN
```

The Eservice settings are returned, including end point information. For example:

```
Ethernet Service "TestTraffic_EPLAN"
  Virtual Switch is 1
  Service type is EPLAN
  Admin State is enable, Operational State is up
  S-VLAN is 111
  MSTP instance is 0
  Number of UNIs is 2
  Number of NNIs is 0
  Lock NNIs is disable
  Topology is multi-point
  Maximum frame size is 9600
  C-VID Translation is disable
  CFM Maintenance Entity Name is "v111"
  CFM Crosscheck is enabled
  CFM Continuity Check Message Interval is 1min
  EthService UAS : 0 hours 55 minutes 30 seconds

Associated UNIs:
  GigE 1/1/7
```

MEP Id	Type	Remote State	Remote Switch Name	Remote Port
5 (4584)	remote	ok	Node_108ES	Gig21/5/7
3 (4664)	remote	ok	Node_110	Gig1/1/7
1 (5454)	local	---	---	---
2 (5931)	remote	ok	Node_106	Gig1/1/7
4 (6006)	remote	ok	Node_107	Gig1/1/7
6 (6051)	remote	ok	Node_108MS	Gig1/1/7

```

Forwarding type is normal
EFPSD is disabled
TPID aware

Node-105:sw1(config)#
```

You have successfully completed this procedure.

### 7.3.8 Performing a loopback test using proNX 900

Authorization Required

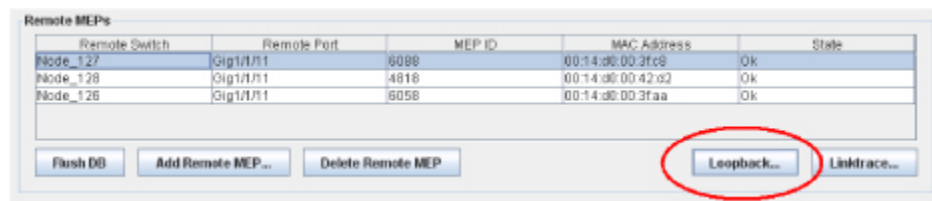
Superuser

Provisioning

Maintenance

Surveillance

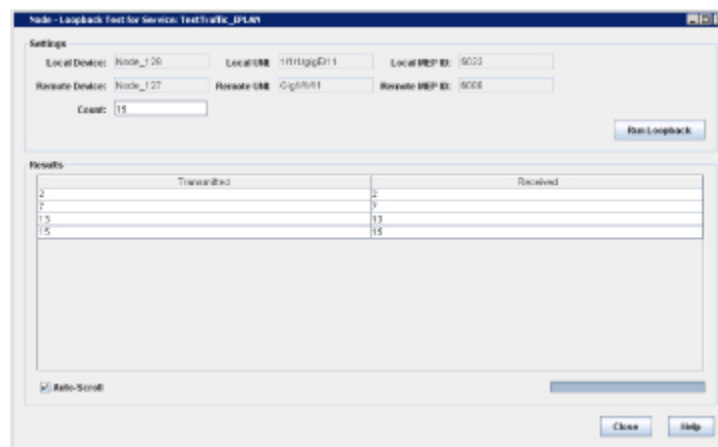
- Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 2** In the **Ethernet Services** dialog, select a service from the **Provisioned Ethernet Services** list, and then click **View**.
- Step 3** In the **View Ethernet Service** dialog, click the **CFM** tab.
- Step 4** On the **CFM** tab, select an MEP from the **Remote MEPs** list, and then click **Loopback**.



- Step 5** In the **Loopback Test** dialog, enter a value (0 to 2147483647) in the **Count** field, and then click **Run Loopback**.

**Note** The value 0 causes the loopback test to run indefinitely.

The loopback test runs the number of times specified in the **Count** field, and the results are displayed.



- Step 6** Click **Close**.

You have successfully completed this procedure.

### 7.3.9 Performing a loopback test using the CLI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the Administration Configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Create a virtual switch

To create a virtual switch, enter the following command:

```
virtual-switch <switch_id> name <switch_name>
```

#### Step 4 Exit configuration mode

```
BTI7000:sw1(config)# exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1#
```

#### Step 5 Determine if the remote endpoint is available

To determine if the remote endpoint is available, enter the following command:

```
BTI7000:sw1# loopback eservice MyEpline rmep <mep_id> count <#>
```

You have successfully completed this procedure.

### 7.3.10 Performing a linktrace test using proNX 900

Authorization Required

Superuser

Provisioning

Maintenance

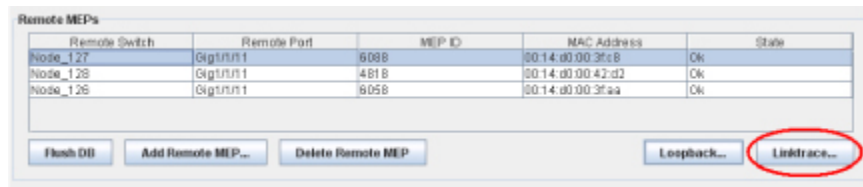
Surveillance

**Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 2** In the **Ethernet Services** dialog, select a service from the **Provisioned Ethernet Services** list, and then click **View**.

**Step 3** In the **View Ethernet Service** dialog, click the **CFM** tab.

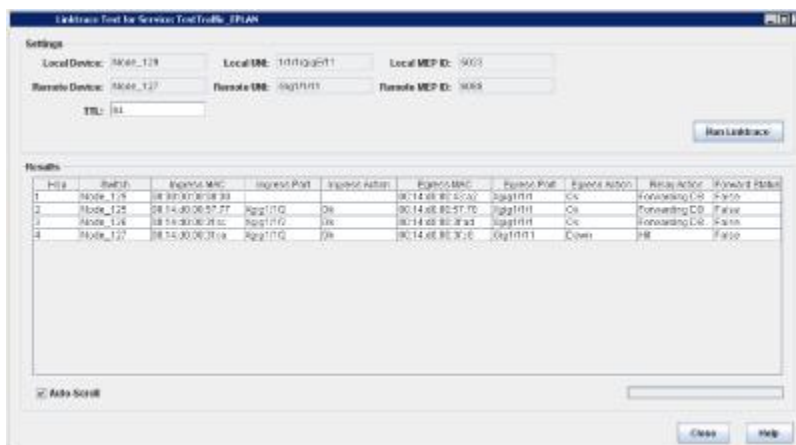
**Step 4** On the **CFM** tab, select a remote switch from the **Remote MEPs** list, and then click **Linktrace**.



**Step 5** In the **Linktrace** dialog for the Eservice, enter a value in the **TTL** field, and then click **Run Linktrace**.

The results (parameter values) of the test are displayed in the **Results** section of the dialog:

- **Hop:** Indicates the hop number
- **Switch:** Indicates the CFM "Switch Name" of the packetVX module
- **Ingress MAC:** Equivalent to the physical MAC address of the Ingress ports
- **Ingress Port:** Indicates the actual port through which traffic has entered on the switch
- **Egress MAC:** Equivalent to the physical MAC address of the Egress port
- **Egress Port:** Indicates the actual port through which traffic has exited from the switch
- **Egress Action:** Indicates the status of a specified egress port:
  - **OK:** Port is up and operational
  - **Down:** Port is down
- **Relay Action:** Indicates whether the port is a MIP (Forwarding DB) or a MEP (Hit)



**Step 6** Click **Close**.

You have successfully completed this procedure.

## 7.3.11 Performing a linktrace test using the CLI

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Create a virtual switch

To create a virtual switch, enter the following command:

```
virtual-switch <switch_id> name <switch_name>
```

### Step 4 Exit configuration mode

```
BTI7000:sw1(config)# exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1#
```

### Step 5 Determine the path that the traffic is taking in the network

To determine the path, enter the following command:

```
BTI7000:sw1# linktrace eservice MyEpline rmep <mep_id>
```

You have successfully completed this procedure.

## 7.4 Interoperability considerations with third-party devices

---

The packetVX module has been designed to make the configuration and usage of Ethernet Service OAM as simple and intuitive as possible. This is achieved by automatically configuring and discovering service end points. When interworking with third-party devices, it may be necessary to modify the default values selected by the packetVX software.

### MEG ID

The MEG ID is a 48-octet field contained in CCM messages that uniquely identifies the Eservice. packetVX constructs the MEG ID by concatenating the ITU Carrier Code (ICC) and the Unique MEG Code (UMC), which corresponds to a concatenation of the ME name and MEG name respectively. The default value for the MEG name is "BTI". The default value for the ME name is "v" followed by the S-VLAN ID of the Eservice. For example, if the S-VLAN ID for an Eservice is "1234", the default ME name is "v1234" and the MEG ID is "v1234BTI".

If padding for the MEG ID is enabled, and if the ICC is shorter than 6 bytes, the ICC is padded with nulls to 6 bytes before concatenating the UMC.

If padding for the MEG ID is disabled, the ICC is concatenated with the UMC with no padding in between. In this situation, there is a possibility that the concatenation of the UMC and ICC exceeds 13 bytes. If this occurs, the ICC is truncated such that the resulting MEG ID is 13 bytes in length.

It may be necessary to manually configure the MEG name, the ME name, and the padding attribute to match the MEG ID configured on third-party devices.

### MEG Level (MEL)

The MEL is a 3-bit field contained in Y.1731 messages that identifies nested OAM flows. The MEL for service level messages is configurable, and has a default value of 4. It may be necessary to manually configure the MEL.

### Remote MEP ID

The MEP ID is a value between 1 and 8191 that uniquely identifies the local end point within a MEG. The packetVX module automatically generates the local MEP ID every time a UNI is added to an Eservice. It may be necessary to manually configure the remote MEP ID.

### CCM interval

The default CCM interval on packetVX is 1 minute. packetVX supports these values for the CCM interval: 10 seconds, 1 minute (and 1 second for EPLINE services). It may be necessary to modify the CCM interval to ensure that all devices within an Eservice are using the same value.

### IEEE 802.1ag mode of operation

The packetVX module uses ITU-T Recommendation Y.1731 for Ethernet Service OAM. This may be changed to IEEE 802.1ag; however, because this is a global setting, the protocol to be used must be determined when the packetVX module is first installed.

<b>Note</b>	If G.8032 is to be utilized for ring protection, Y.1731 must be used.
-------------	---

<b>Note</b>	The packetVX cannot generate loopback and linktrace messages in 802.1ag mode.
-------------	---

## 7.5 Advanced procedures — Global settings

The following parameters are set at the global level on packetVX modules:

- MEG name
- MEG level
- MIP auto-creation
- MEG ID pad
- Y.1731 or 802.1ag

Parameters that are set at the global level apply to all Eservices.

### 7.5.1 Viewing global settings

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1** To view global settings, enter the following command:

```
show virtual-switch [<switch_id>|all][brief]
```

where

switch\_id is the switch identifier

For example, the syntax might be as follows:

```
show virtual-switch 4
```

The resulting output should appear as follows:

```
SwitchId: 4
  Bridge Mode is provider
  Bridge ID is 00:14:d0:33:47:0d
  Aging Time is 300 sec
  Link hold down interval is 3 sec
  MSTP is administratively enabled
  GVRP is administratively enabled
  LACP is administratively enabled
  802.1x is administratively disabled
  802.1ag is administratively disabled
  Y.1731 is administratively enabled
  CCM_OFFLOAD is administratively disabled
  ERPS is administratively enabled
  SLA Measurement is administratively disabled
  LACP System Priority is 32767
  LACP system-id is 00:14:d0:33:47:0d
  Vlan Propagation mode across ERPS Rings is fast

  Tunnel MAC Address Profile: DEFAULT_TMA_PROFILE
```



```

EVC MEG Name:          BC1
EVC MEG Level:         4
MEG-ID Pad:            enabled
Switch Name:           BC1_4
MIP Auto create:       enabled
MIP Auto create MEL:   4
CPU Mirror:            Disable
LLDP trap time interval: 60 seconds
Primary Member:        11/3
Time As Primary:       1495 seconds

```

Members:

Location	Stacking State	Stacking Port Comm State	Backplane Comm State
11/3	primary	no connection	connection ok
11/5	secondary	no connection	connection ok

You have successfully completed this procedure.

## 7.5.2 Changing a MEG name and MEG level

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Enter the virtual switch configuration mode

```
virtual-switch <switch_id>
```

### Step 4 Enter a name for the MEG and a level

To enter a name for the MEG enter the following command:

```
BTI7000:sw1(config)# cfm meg <name> level <level>
```

You have successfully completed this procedure.

### 7.5.3 Viewing all MIPs

Use this procedure to view all MIPs auto-created on the packetVX module.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1** To view all MIPs, enter the following command:

```
show cfm mip
```

The auto-created MIPs are returned. For example,

VS	Ethernet Service Name	Port Name	Active
1	test	TenGigE 1/1/2	yes

You have successfully completed this procedure.

### 7.5.4 Disabling MIP auto-creation

Use this procedure to disable auto-creation of MIPs. Once auto-creation is disabled, the user must configure MIPs manually at the Eservice level.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Enter the virtual switch configuration mode**

```
virtual-switch <switch_id>
```

The CLI prompt should now appear as follows (for virtual switch 1):

```
BTI7000:sw1(config)#
```

**Step 4 Disable auto-creation of MIPs**

```
BTI7000:sw1(config)# cfm mip autocreate disable
```

```
BTI7000:sw1(config)# show virtual 1
```

An example of the system response is:

```
SwitchId: 1
  Bridge Mode is provider
  Bridge ID is 00:14:d0:00:31:a6
  Aging Time is 300 sec
  Link hold down interval is 3 sec
  MSTP is administratively enabled
  GVRP is administratively enabled
  LACP is administratively enabled
  802.1x is administratively disabled
  802.lag is administratively disabled
  Y.1731 is administratively enabled
  CCM_OFFLOAD is administratively disabled
  ERPS is administratively enabled
  SLA Measurement is administratively disabled
  LACP System Priority is 32767
  LACP system-id is 00:14:d0:00:31:a6
  Vlan Propagation mode across ERPS Rings is fast

Tunnel MAC Address Profile: DEFAULT_TMA_PROFILE

EVC MEG Name:          BC1
EVC MEG Level:         4
MEG-ID Pad:            enabled
Switch Name:           BC1_1
MIP Auto create:       disabled
MIP Auto create MEL:   4
CPU Mirror:            Disable
LLDP trap time interval: 60 seconds
Primary Member:        1/1
Time As Primary:       79097 seconds
```

Members:

	Stacking	Stacking Port	Backplane
Location	State	Comm State	Comm State
1/1	unstacked	no connection	no connection

You have successfully completed this procedure.

## 7.5.5 Auto-creating MIPs

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Note** After Auto-creation is enabled, MIPs are created for Eservices. Eservices that are created before MIP auto-creation is enabled will not have MIPs associated with the S-VLAN until the switch is restarted.

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Enter the virtual switch configuration mode.**

```
virtual-switch <switch_id>
```

The CLI prompt should now appear as follows (for virtual-switch 1):

```
BTI7000:sw1(config)#
```

**Step 4 Enable auto-creation of MIPs and set the MIP level**

```
BTI7000:sw1(config)# cfm mip autocreate enable
```

```
BTI7000:sw1(config)# show virtual 1
```

The system response is:

```
SwitchId: 1
  Bridge Mode is provider
  Bridge ID is 00:14:d0:00:31:a6
  Aging Time is 300 sec
  Link hold down interval is 3 sec
  MSTP is administratively enabled
  GVRP is administratively enabled
  LACP is administratively enabled
  802.1x is administratively disabled
  802.1ag is administratively disabled
  Y.1731 is administratively enabled
  CCM_OFFLOAD is administratively disabled
  ERPS is administratively enabled
  SLA Measurement is administratively disabled
  LACP System Priority is 32767
  LACP system-id is 00:14:d0:00:31:a6
  Vlan Propagation mode across ERPS Rings is fast

Tunnel MAC Address Profile: DEFAULT_TMA_PROFILE

EVC MEG Name:          BTI
EVC MEG Level:         4
MEG-ID Pad:            enabled
Switch Name:           BTI_1
```

```

MIP Auto create:          enabled
MIP Auto create MEL:      4
CPU Mirror:               Disable
LLDP trap time interval:  60 seconds
Primary Member:           1/1
Time As Primary:          79097 seconds

```

Members:

Location	Stacking State	Stacking Port Comm State	Backplane Comm State
1/1	unstacked	no connection	no connection

You have successfully completed this procedure.

## 7.5.6 Changing the MEG ID pad

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Enter the virtual switch configuration mode

```
virtual-switch <switch_id>
```

### Step 4 Set the MEG ID pad parameter

To enable or disable padding:

```
BTI7000:sw1(config)# cfm pad [ enable | disable ]
```

You have successfully completed this procedure.

## 7.5.7 Disabling the protocol Y.1731

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1** To disable the protocol Y.1731, enter the following command:

```
protocol y.1731 disable
```

There is no system response if the command is successful.

You have successfully completed this procedure.

## 7.5.8 Enabling the protocol 802.1ag

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1** To enable the protocol 802.1ag, enter the following command:

```
protocol 802.1ag enable
```

There is no system response if the command is successful.

You have successfully completed this procedure.

## 7.6 Advanced procedures — Eservice settings

The following parameters are set at the Eservice level on packetVX modules:

- CCM enabled/disabled
- CCM interval
- ME name
- MEP ID
- Remote MEP list and MIPs

Changes to these parameters affect only the given Eservice.

### 7.6.1 Viewing Eservice settings

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 View the Eservice settings

To view the Eservice settings, enter the following command:

```
show eservice [<service-name>] [brief]
```

where

*service-name* is the name of the service

For example, the command string might be as follows:

```
BTI7000# show eservice brief
```

The Eservice settings are returned. For example:

VS	Name	Type	Oper	Admin	S-VLAN	MSTI	Max-Frame
1	testepan1	EPLAN	unknown	enable	31	0	1522
1	testepan2	EPLAN	unknown	enable	32	0	1522
1	testepan3	EPLAN	unknown	enable	33	0	1522
1	testepan4	EPLAN	unknown	enable	34	0	1522

You have successfully completed this procedure.

## 7.6.2 Disabling or enabling CFMs

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Note** After disabling CFM crosscheck on an Eservice, the remote MEP list is not deleted, so the Eservice goes into an Operational Down state. The workaround is to use the **cfm flush-rmep-db** command on a UNI assigned to the Eservice.

### Step 1 Access the Eservice Configuration mode

To access the Eservice Configuration, enter the following command:

```
eservice <service-name> [type <service-type>]
```

where

*service-name* is the name of the Ethernet service

*service-type* is the type of Ethernet service

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Enable or disable CFMs

```
BTI7000# cfm crosscheck {enable|disable}
```

where

*enable* enables CCM transmission and cross-checking

*disable* disables CCM transmission and cross-checking

There is no system response if the command is successful.

You have successfully completed this procedure.

## 7.6.3 Changing the CCM interval

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Step 1 Access the Eservice Configuration mode

To access the Eservice Configuration, enter the following command:

```
eservice <service-name> [type <service-type>]
```

where

*service-name* is the name of the Ethernet service

*service-type* is the type of Ethernet service

The CLI prompt should now appear as follows:

```
BTI7000#
```



**Step 2 Change the CCM interval**

To change the CCM interval, enter the following command:

```
cfm interval <interval>
```

where

*interval* is the interval for the crosscheck

For example, the command string might be

```
cfm interval 1min
```

The CCM interval is changed.

**Note** There are only two valid intervals: 10 seconds and 1 minute.

You have successfully completed this procedure.

**7.6.4 Changing a ME name**

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Note** You cannot change the ME name if there is a UNI/NNI assigned to the Eservice.

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Create a virtual switch**

If the switch does not exist, it is created by this command:

```
virtual-switch <switch_id> name <switch_name>
```

**Step 4 Change the ME name**

To change the ME name, enter the following command:

```
BTI7000:sw1(config)# eservice MyEservice type epline
```

```
BTI7000:sw1(config-eservice)# s-vlan 100
```

```
BTI7000:sw1(config-eservice)# cfm me <name>
```

You have successfully completed this procedure.

## 7.6.5 Adding a remote MEP ID

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

This procedure adds a remote MEP ID to a service.

**Note** In an interoperability scenario, the switch may not auto-discover all remote MEPs. The user may need to add the MEP IDs of the remote MEPs manually.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Enter the virtual switch configuration mode

```
virtual-switch <switch_id>
```

### Step 4 Add the remote MEP ID

To add the remote MEP ID, enter the following command:

```
cfm mep-list mep-id <id>
```

where *id* is the value of the MEP ID

For example, the command string might be as follows:

```
BTI7000:sw4(config-eservice)# cfm mep-list mep-id  
1001
```

You have successfully completed this procedure.

## 7.6.6 Viewing the remote MEPs of an Eservice

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

## Step 2 View the Eservice settings

To view the eservice settings, enter the following command:

```
show eservice [<service-name>][brief]
```

where

*service-name* is the name of the service

For example, the command string might be as follows:

```
BTI7000# show eservice PVX_TEST
```

The Eservice settings are returned, including the remote MEPs. For example:

```
Ethernet Service "PVX_TEST"
  Virtual Switch is 1
  Service type is EVPLAN
  Admin State is enable, Operational State is up
  S-VLAN is 239
  MSTP instance is 0
  Number of UNIs is 1
  Number of NNIs is 2
  Lock NNIs is disable
  Topology is multi-point
  Maximum frame size is 1522
  C-VID Translation is disable
  CFM Maintenance Entity Name is "vvv239" (autogenerated ICC : "vvv239")
  CFM Crosscheck is enabled
  CFM Continuity Check Message Interval is 1min
  EthService UAS : 0 hours 2 minutes 0 seconds

Associated UNIs:
  GigE 1/1/6
    Filter-sequence is 50
      
```

MEP Id	Type	Remote State	Remote Switch Name	Remote Port
1 (4523)	local	---	---	---
2 (5424)	remote	ok	BC1_1	Gig1/1/5

```

      Forwarding type is normal
      EFPSD is disable

Associated NNIs:
  TenGigE 1/1/1
  TenGigE 1/1/2
```

You have successfully completed this procedure.

## 7.6.7 Flushing the MEP list

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Note** This procedure clears the MEP table and forces a re-discovery of all remote MEPs.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Configure the virtual switch

If the switch does not exist, it is created by this command:

```
virtual-switch <switch_id> name <switch_name>
```

### Step 4 Flush the MEP list

To flush the MEP list, enter the following commands:

```
BTI7000:sw1(config)# eservice MyEservice type epline
```

```
BTI7000:sw1(config-eservice)# s-vlan 100
```

```
BTI7000:sw1(config-eservice)# uni gig 1/1/1
```

```
BTI7000:sw1(config-uni-eservice)# cfm flush-rmep-db
```

You have successfully completed this procedure.

## 7.6.8 Creating MIPs manually

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- MIP Auto-creation must be disabled.
- Create an NNI.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Enter the virtual switch configuration mode**

```
virtual-switch <switch_id>
```

The CLI prompt should now appear as follows (for virtual-switch 1):

```
BTI7000:sw1(config)#
```

**Step 4 Add an NNI to an Ethernet service manually**

To add an NNI to an Eservice, enter the following commands:

```
BTI7000:sw1(config)# eservice MyEpline type epline
```

```
BTI7000:sw1(config-eservice)# s-vlan 10
```

```
BTI7000:sw1(config-eservice)# nni gig 1/1/1
```

```
BTI7000:sw1(config-nni-eservice)# cfm mip
```

```
BTI7000:sw1(config-nni-eservice)# show
```

```
NNI GigE 1/1/11, Ethernet Service "Test"  
  Virtual Switch is 1  
  CFM MIP is enabled
```

You have successfully completed this procedure.

## 7.7 Troubleshooting

### 7.7.1 Number of CCMs sent

packetVX modules record statistics on the number of CCMs sent for each Eservice. The number of CCMs can be queried.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1** To query the number of CCMs, enter the following command:

```
show uni-eservice [uni <interface-type> [<interface-id>]] [eservice
<service-name>]
```

where

*interface-type* is the interface type

*interface-id* is the interface identifier

*service-name* is the name of the Ethernet service

For example, the command string might be

```
BTI7000# show uni-eservice uni gig 1/1/1
```

The displayed result should be similar to the following:

```
C-VLANs:
  100
MEP-ID is 5341
State is invalid(0)
Direction is invalid(0)
Mac Address is 00-14-d0-00-44-dd
Auto-generate is yes
Number of CCM Messages sent is 1175
Number of CCM Sequence Errors is 0
Forwarding type is normal
```

### 7.7.2 Defects

packetVX modules diagnose connectivity problems and provide a list of defects for a given Eservice. The list of defects can be queried.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Step 1** To query the list of defects, enter the following command:

```
show uni-eservice [uni <interface-type> [<interface-id>]] [eservice
<service-name>]
```

where

*interface-type* is the interface type

*interface-id* is the interface identifier

*service-name* is the name of the Ethernet service

For example, the command string might be

```
BTI7000# show uni-eservice brief
```

The displayed result should be similar to the following:

VS	UNI name	Ethernet Service Name	C-VLANs
1	LAG 1	testevplan1	2000 2003
1	LAG 1	testevplan2	2001 2004
1	GigE 1/1/7	testevplan1	2000 2003
1	GigE 1/1/7	testevplan2	2001 2004
1	TenGigE 1/1/1	testevplan1	2000 2003
1	TenGigE 1/1/1	testevplan2	2001 2004

The following table summarizes the defect conditions.

Defect	Description
Loss of continuity	A MEP detects LOC with a peer MEP when it stops receiving CCM frames.
Mismerge	A MEP detects Mismerge when it receives a CCM frame with a correct MEG level but incorrect MEG ID.
Unexpected MEP	A MEP detects Unexpected MEP when it receives a CCM frame with a correct MEG level, a correct MEG ID but an unexpected MEP ID.
Unexpected MEG Level	A MEP detects Unexpected MEG Level when it receives a CCM frame with the incorrect MEG level.
Unexpected Period	A MEP detects Unexpected Period when it receives a CCM frame with a correct MEG level, a correct MEG ID, a correct MEP ID, but with a Period field value different than the MEP's own CCM transmission period.
Signal fail (ERPS)	A MEP declares a Signal Fail condition upon detection of defect conditions, including LOC, Mismerge, UnexpectedMEP, etc.
RDI	A MEP detects RDI when it receives a CCM frame with the RDI field set.





## 8.0 Configuring Quality of Service and Class of Service

---

*"Quality of Service (QoS) is one of the most elusive, confounding, and confusing topics in data networking today. Why has such an apparently simple concept reached such dizzying heights of confusion? After all, it seems that the entire communications industry appears to be using the term with some apparent ease, and with such common usage, it is reasonable to expect a common level of understanding of the term."*<sup>27</sup>

Adding insult to injury, the term Class of Service is added into the fray. Although these terms are often confused and used interchangeably, Class of Service (CoS) is a much more clearly defined concept. Class of Service *implies that services can be categorized into separate classes, which can, in turn, be treated individually.*<sup>28</sup> The treatment that is applied to these different classes of service is called Quality of Service.

This section covers the following topics:

- 8.1, "Service Level Agreements"
- 8.2, "Packet flow"
- 8.3, "Bandwidth profiles and traffic policing"
- 8.4, "Packet classification"
- 8.5, "Transmission queuing and scheduling"
- 8.6, "CoS on intermediate switches"
- 8.7, "Quality of Service configuration"
- 8.8, "SLA monitoring"

<sup>27</sup> Ferguson, Paul and Huston, Geoff. Quality of Service, Delivering QoS on the Internet and in Corporate Networks. John Wiley & Sons, Inc. 1998.

<sup>28</sup> *ibid.*

## 8.1 Service Level Agreements

---

In the context of a provider-based networking device, it is easy and useful to tie the meanings down to a business agreement. We can hypothesize a *service level agreement* (SLA) between the subscriber and the service provider. The SLA indicates that the service provider will accept a list of Ethernet traffic types distinguished in particular ways and assign each traffic type to one of a list of standard classes of service. Each class of service (CoS) will have a set of service-quality characteristics (the quality of the service, or QoS). We'll use the following two SLAs to describe the capabilities.

### SLA 1

*“The provider will transport traffic bidirectionally from an Ethernet connection in New York to an Ethernet connection in Chicago. The two ports will be dedicated to this connection and all frames presented at a port will be transferred unmodified to the other port subject to bandwidth limitations described herein.*

*Both ports will be bandwidth limited according to the following bandwidth profile (...) and all traffic will be transported with a quality of service defined in provider's 'Best Efforts Delivery' offering.”*

### SLA 2

*“The provider will transport traffic bidirectionally from an Ethernet connection in New York to an Ethernet connection in Chicago. The two ports will be dedicated to this connection and all frames presented at a port will be transferred unmodified to the other port subject to bandwidth limitations described herein.*

*Traffic received on the ports will be classified as follows:*

*All RTP traffic (as defined elsewhere) will be limited according to the following bandwidth profile (...) and will be transported with a quality of service defined in provider's 'Voice Grade Delivery' offering.”*

*All other traffic will be bandwidth limited according to the following bandwidth profile (...) and all traffic will be transported with a quality of service defined in provider's 'Best Efforts Delivery' offering.”*

These SLAs include several components of the agreement:

- 1 The number of ports and where they are and whether they are dedicated or shared
- 2 The relevant classes of service: Best Efforts Delivery and Voice Grade Delivery
- 3 How the traffic will be assigned to a class of service (all traffic in SLA 1 and RTP traffic vs. non-RTP traffic in SLA 2)
- 4 The bandwidth associated with each class of service
- 5 What the QoS characteristics are for each class of service (i.e., “as described in the relevant offering document”)

The QoS can include metrics such as:

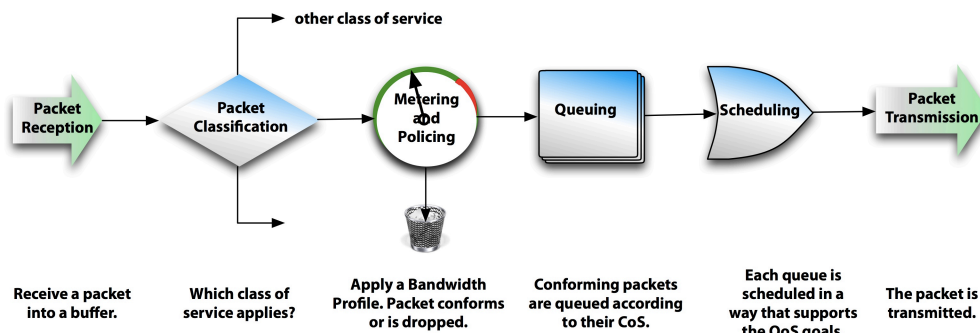
- Frame Loss Rate
- Maximum and/or average packet delay
- Maximum packet delay variation
- Average throughput

These QoS characteristics cannot be enforced by a single switch in a provider network, but rather, every switch needs to segregate each CoS and ensure that the packet queuing and transmission scheduling for that CoS on that switch is implemented to support the desired characteristics. This section provides information about configuring a switch to provide the appropriate quality of service.

## 8.2 Packet flow

The various tasks associated with classification, rate enforcement (bandwidth policing), and supporting the QoS objectives happen as a packet flows through the bridge, as shown in the following figure.

**Figure 8-1 Packet flow in the switch**



## 8.3 Bandwidth profiles and traffic policing

Bandwidth limitations are applied to a classified flow of traffic using a bandwidth profile. The bandwidth profile describes the bandwidth limitation in terms of four parameters:

- Committed Information Rate (CIR)
- Committed Burst Size (CBS)
- Excess Information Rate (EIR)
- Excess Burst Size (EBS)

CIR is the basic rate committed by the service provider, for example, 125 Mb/s. The SLA documents that frames presented to the UNI at an average rate of CIR or lower are delivered with a probability defined in the QoS definition, for example, greater than 99.8%. EIR is the excess information rate. The excess rate allows the subscriber to use excess bandwidth that might be available in the network. This excess traffic is subject to the same class of service, except that the traffic in excess of CIR has a lower probability of successful frame delivery—it is more likely to be discarded if the network is congested.

Since all traffic is actually arriving at the switch at the line rate (1 Gb/s) regardless of the CIR, the switch absorbs a burst of traffic at the line rate and then averages it out over time to determine the actual rate. CBS and EBS define the sizes of the bursts that are absorbed.

### Considerations for networks running releases earlier than 10.3

There is a third rate that is often referred to as the Peak Information Rate (PIR). PIR is the sum of CIR and EIR (i.e.  $PIR = CIR + EIR$ ).

In packetVX releases earlier than 10.3, the switch treats the configured EIR as PIR. For example, if the configuration is CIR=10Mbps and EIR=15Mbps, the switch interprets the configured 15Mbps setting as PIR. Internally, it sets the actual EIR to 5Mbps.

This is changed in release 10.3. From release 10.3 onwards, the configured EIR is interpreted as the EIR. The equivalent configuration to the above example in release 10.3 is CIR=10Mbps and EIR=5Mbps.

Note the following:

- If you are running a release earlier than 10.3 you should verify the configured bandwidth profiles to ensure that they are defined properly for your network environment.
- If you upgrade to release 10.3, you should review previously defined bandwidth profiles. If necessary, modify the profiles based on the release 10.3 implementation of traffic policing.

### 8.3.1 Bandwidth profile rate enforcement

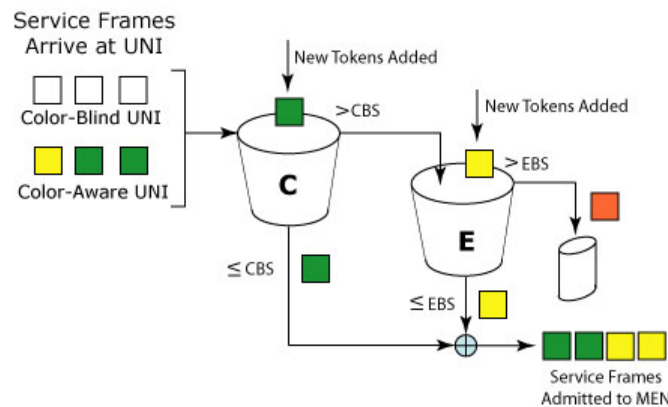
From an implementation perspective, the bandwidth profile rates are enforced through an algorithm that is implemented through a token bucket algorithm (TBA). The MEF has defined a two-rate, three-color marker (trTCM) algorithm that can be implemented through two token buckets.

One bucket, the Committed (C) bucket, determines CIR-conforming, in-profile service frames. The other bucket, the Excess (E) bucket, determines EIR-conforming excess service frames.

Each token bucket consists of a bucket of bytes referred to as tokens. Initially, each token bucket is full of tokens. As service frames enter the provider's network, the trTCM algorithm decrements the number of tokens in the C bucket (green tokens) by the number of bytes received from the service frame. If there are enough green tokens, the service frame is CIR-conforming, colored green, and allowed into the service provider's network.

If there are not enough green tokens for the frame, the E bucket is checked to determine if any E bucket tokens (yellow tokens) remain. If yellow tokens are available, the service frame is colored yellow and allowed into the provider's network. If there are not enough yellow tokens available, the service frame is declared red and discarded.

**Figure 8-2 trTCM algorithm**



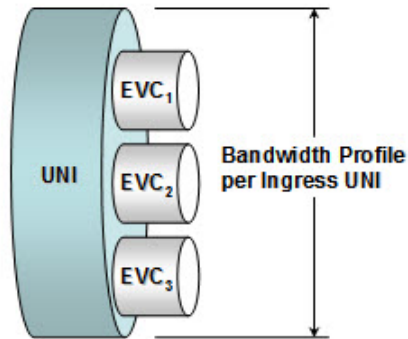
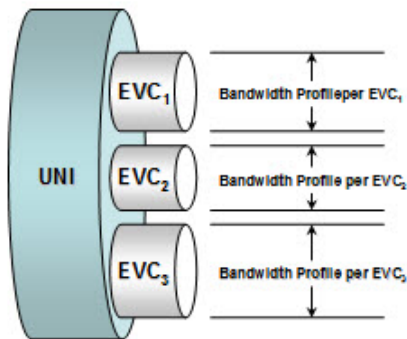
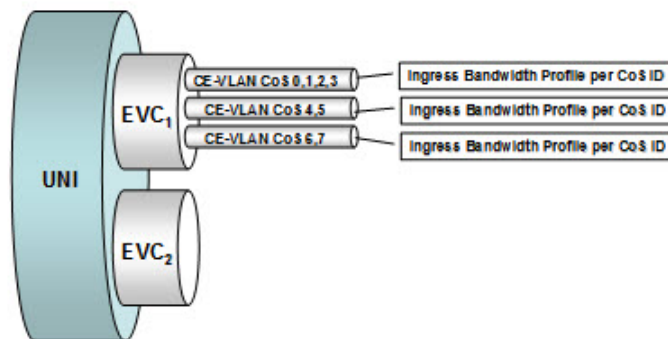
## 8.3.2 Ingress and egress bandwidth profiles

Ingress and egress bandwidth profiles are provisioned using policing and packet queuing or scheduling parameters.

### 8.3.2.1 Ingress bandwidth profiles

There are three types of ingress bandwidth profiles:

- Ingress Bandwidth Profile per Ingress UNI, which is applied to all ingress service frames for all EVCs at the UNI
- Ingress Bandwidth Profile per EVC Service Attribute, which is applied to all ingress service frames for an EVC at the UNI
- Ingress Bandwidth Profile per Class of Service Identifier Service Attribute, which is applied to all ingress service frames with a specific CoS identifier

**Figure 8-3 Ingress Bandwidth Profile per Ingress UNI****Figure 8-4 Ingress Bandwidth Profile per EVC Service Attribute****Figure 8-5 Ingress Bandwidth Profile per Class of Service Identifier Service Attribute**

### 8.3.2.2 Egress bandwidth profiles

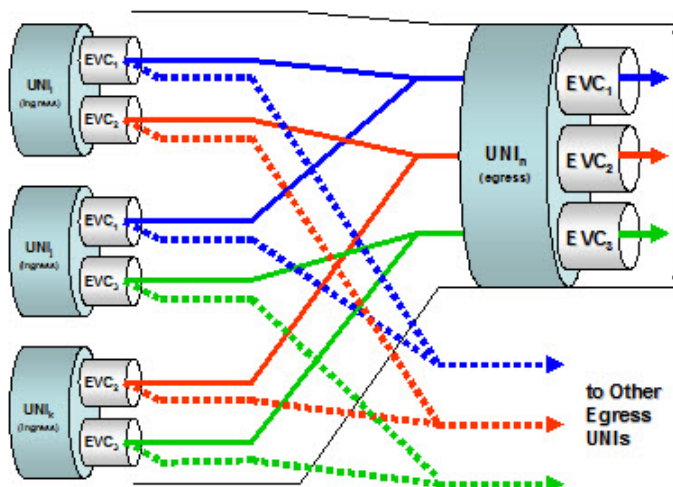
There are three types of egress bandwidth profiles:

- Egress Bandwidth Profile per Egress UNI Service Attribute, which is applied to the sequence consisting of all egress service frames at the UNI
- Egress Bandwidth Profile per EVC Service Attribute, which is applied to the egress service frames that are mapped to the EVC

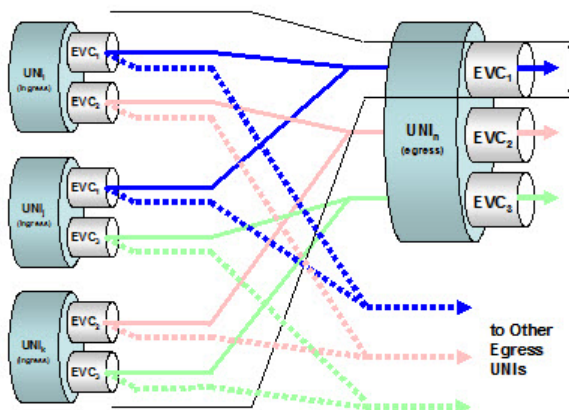
- Egress Bandwidth Profile per Class of Service Identifier Service Attribute, which is applied to the egress service frames with the CoS identifier

**Note** An egress profile on a packetVX 80 is not supported on a UNI.

**Figure 8-6 Egress Bandwidth Profile per Egress UNI Service Attribute**



**Figure 8-7 Egress Bandwidth Profile per EVC Service Attribute**



Traffic below the CIR is guaranteed to be forwarded. Traffic above the CIR but below the EIR is forwarded on a best-effort basis. Traffic above the EIR is dropped.

For example, if you set policing on an ingress queue to be 1 Mbps, and traffic exceeds that 1 Mb/s rate, all traffic that exceeds the 1 Mb/s is dropped.

### 8.3.3 Configuring bandwidth profiles

A bandwidth profile is defined on a packetVX module as follows:

```
> PROFILE BANDWIDTH bigcustomer ! bigcustomer is the profile name
> POLICE CIR <rate> ! e.g. 512Kbps, 100Mbps, 1Gbps
```



```
> POLICE CBS <KiBytes>
> POLICE EIR <rate>
> POLICE EBS <KiBytes>
> EXIT
```

<b>Note</b>	1 kibibyte (KiB) = 1024 bytes 1 kilobyte (kB) = 1000 bytes
-------------	---

The rates are rounded to 64 Kb/s increments up to 1 Mb/s and they are rounded to 1 Mb/s increments above 1 Mb/s. The burst sizes are rounded up to the next increment of 4 KiBytes.

If all the traffic on a UNI is subject to this bandwidth profile, as in SLA 1 in 8.1, “[Service Level Agreements](#)”, the bandwidth profile can be applied to the UNI. Packet-level classification is not required.

```
> UNI gig 1/1/7
> SET INGRESS PROFILE BANDWIDTH bigcustomer
> EXIT
```

If the bandwidth profile applies to a subset of the traffic, the classification process has to occur first, and then the bandwidth profile is applied to this subset.

<b>Note</b>	The proNX 900 Node Controller uses the following parameter terms, in place of the command <b>police</b> , to configure a bandwidth profile as described in section A.5.4, “ <a href="#">Bandwidth profile parameters</a> ”: <ul style="list-style-type: none"> <li>• Meter CIR</li> <li>• Meter CBS</li> <li>• Meter EIR</li> <li>• Meter EBS</li> </ul>
-------------	--

The bandwidth profile allows a number of additional specifications in addition to the four POLICE commands described above. First, there is a set of commands that define what happens to green and yellow packets—red packets are discarded.

For green packets, the IP DSCP (differentiated services code point) field and the IP type of service field can be set:

```
> CONFORM-ACTION [set-dscp-transmit <value> | set-tos-priority <value>]
```

For yellow packets, the DEI bit or the DSCP field can be set:

```
> EXCEED-ACTION [set-dei <value> | set-dscp-transmit <value>]
```

Yellow packets are marked, by default, with the “Discard Eligibility” bit in the VLAN tag if they are forwarded over an NNI. This allows the next switch to know that they are non-conforming.

One additional command—**meter mode**—is available to describe some finer details about how the bandwidth meter works. The **meter mode** command allows the user to specify whether the meter is a single rate (srTCM) or a two rate (trTCM) meter and also allows specification of whether the policing is done in a color blind or color aware manner. The single rate (srTCM) profile can be applied to only egress traffic.

```
> METER MODE [TR-TCM | sr-tcm] [color aware | COLOR BLIND]
```

**Note** TR-TCM and COLOR BLIND are the defaults.

When configuring a bandwidth profile in srTCM meter mode, the following additional steps are necessary:

```
> no exceed-action set-dei
> no police eir
> no police ebs
```

### Guidelines for setting committed burst size

The need for burst tolerance goes up as the CIR goes down as a percentage of the line rate. If the CIR is equal to the line rate, almost no burst tolerance is needed—all received traffic conforms to the bandwidth profile. If the CIR is very low compared to the line rate, a lot more burst tolerance is needed.

There is a tendency to configure a lot more than is needed. Making CBS larger does not necessarily increase service performance and can decrease performance in some cases. Burst sizes should be thought of in terms of multiples of maximum frame size (MFS). Considering a standard MFS of 1522, 2 MiB is about 1300 MFS. Allowing a subscriber to burst 1300 MFS (or 32,000 64-byte packets) into the system at line rate regardless of the CIR makes poor use of system resources and can allow one subscriber to crowd out other subscribers.

**Note** 1 mebibyte (MiB) = 1024 \* 1024 bytes  
1 megabyte (MB) = 1000 \* 1000 bytes

The following guidelines are sufficient in many service configurations; however, there may be some configurations that require additional tuning:

- If the CIR is above 70% of line rate, we recommend CBS = 4 to 6 times the MFS.
- If the CIR is between 40% and 70% of line rate, we recommend CBS = 6 to 12 times the MFS.
- If the CIR is less than 40% of the line rate, we recommend 10 to 20 times the MFS.
- If the CIR is towards the lower end of the range, CBS should move towards the higher end.

For example, if CIR=100 Mbps on a 1Gbps line (10%), 16 times the standard 1522 MFS is 24352, CBS=24 is appropriate.

### Additional considerations for setting burst size

- The default value for CIR is 1Mbps.
- The default value for EIR is 10Mbps.
- The default value for CBS and EBS is 8 KiBytes.
- In a Two-Rate meter, CIR may be zero, which means that all traffic is yellow, or red. In this case EIR and EBS must be greater than zero.
- In a Two-Rate meter, EIR may be zero, if no excess rate is desired.

## 8.4 Packet classification

Incoming packets can be assigned to a CoS at two levels:

- UNI
- SERVICE UNI<sup>29</sup> based on matching certain packet criteria

The packet classification has two primary effects. First, it defines a bandwidth profile that is used to control the rate of packets incoming in that class. Second, it sets the internal priority of the packets. The internal priority, a value from 0 to 7 (inclusive) is used to select the appropriate transmit queue for the packet. This is the primary determinant of the QoS for the flow.

Internal Priority is set using the bandwidth profile.

```
> PROFILE BANDWIDTH bigcustomer
> POLICE commands, etc.
> INTERNAL PRIORITY <0 to 7>
> EXIT
```

Internal priority on a UNI can be set in three ways. First, there is the default internal priority, which is 0. In the absence of any other specification, this will be applied. Second, the priority default can be changed on the UNI:

```
> UNI gig 1/1/5
> PRIORITY DEFAULT 3
> EXIT
```

An internal priority can be associated with a bandwidth profile. If the bandwidth profile is assigned to a UNI (as described in 8.3.3, “[Configuring bandwidth profiles](#)”), all frames received on the UNI will be assigned the indicated *internal priority*.

Finally, the priority can be taken directly from the incoming packet. This is uncommon on a UNI since it could give stations the ability to spoof the intended priority, but there are circumstances where it makes sense. This is accomplished by using the TRUST-INCOMING-PCP ENABLE command in the UNI configuration.

Classifying packets on a Service UNI is a bit more involved and a lot more powerful. The first step is to describe the packets to classify. This is done by defining a *class map* that specifies the fields of the packet to be matched:

```
> CLASS MAP name TYPE INGRESS-COS
> <list of MATCH commands>
> EXIT
```

The MATCH commands include:

- MATCH C-VLAN {<vlan-id> | <vlan-id start> <vlan-id end>}
- MATCH C-VLAN-PRIORITY <priority>
- MATCH MAC SRC <mac address>
- MATCH MAC DEST <mac address>

<sup>29</sup> For an understanding of the distinction between UNI and SERVICE UNI, see [Chapter 6, “Configuring Ethernet services”](#).

- MATCH ETHERTYPE <value>
- MATCH IP SRC <ip-address>
- MATCH IP DEST <ip-address>
- MATCH IP PROTOCOL <value>
- MATCH IP TCP-UDP-PORT DEST <port #>
- MATCH IP TCP-UDP-PORT SRC <port #>
- MATCH IP DSCP <value>

**Note** For matching a range of VLANs, the range values must be a power of 2, and the start VLAN ID must be a multiple of the range. This implies that the start VLAN ID must also be a power of 2. For example:

```
match c-vlan 64-71
```

This command matches VLAN IDs 64 through 71 inclusively. The range value in this example is  $71-64+1=8$ , which is a power of 2. The start VLAN ID is 64, which is a multiple of the range value of 8.

A class map can have multiple MATCH commands—all of them must match in order for the classification to be a match. For example:

```
> CLASS MAP rtp-voice
> MATCH IP DEST 10.1.4.3 ! address of voice switch
> MATCH IP TCP-UDP-PORT DEST 5004
> EXIT
```

Once the class map is defined, it is paired with a bandwidth profile into a *policy map*.

```
> POLICY MAP silver-voice
> CLASS-MAP rtp-voice PROFILE BANDWIDTH bigcustomer
> EXIT
```

**Note** An egress profile on a packetVX 80 is not supported on a UNI.

Finally, the policy map can be applied to a SERVICE UNI.

```
> ESERVICE customer1
> UNI gig 1/1/4
> SET INGRESS SERVICE-POLICY silver-voice
> EXIT
> EXIT
```

Once the internal priority is determined, it is marked into the PCP field of the S-VLAN tag when the packet is sent on an NNI. This allows the next switch to know how to enqueue the packet.

## 8.5 Transmission queuing and scheduling

All the techniques described in 8.4, “[Packet classification](#)” focus on the goal of applying an internal priority to each received packet. Next, the internal priority has to be turned into a quality of service.

Quality of service involves attributes such as delay and frame loss. To think about how the switch can affect these attributes, consider how impairments such as excessive delay and frame loss happen.

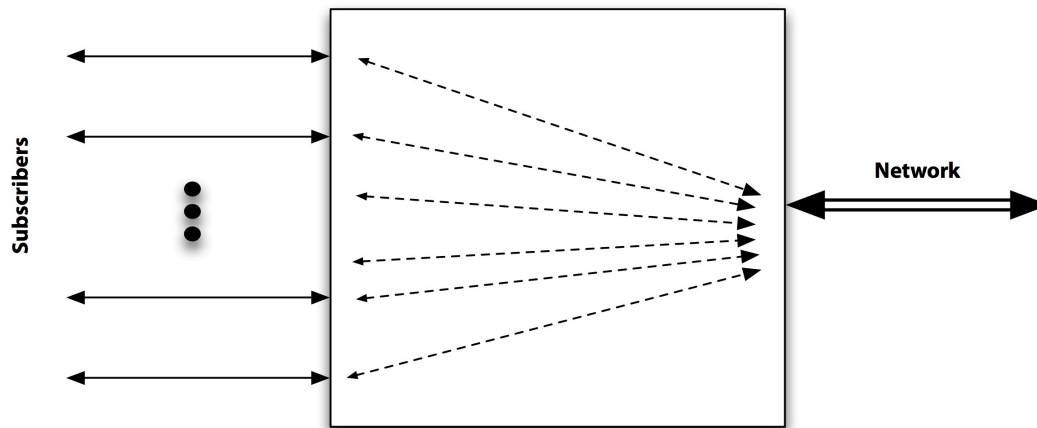
Delay in a network has four sources:

- 1 The inherent delay through each switch or router. These store and forward devices perform processing on each packet; therefore, packets presented at an input do not instantaneously appear on an output. In contemporary devices, this delay is small, a few microseconds.
- 2 Propagation time. We live in a world limited by the speed of light. Whether a network connection is electrical or optical, signal propagation takes some time. Signals usually travel between 50% and 80% of the speed of the light, depending on the medium. So, a link from, say New York to Chicago (about 1500 kilometers), has a propagation time of 7 to 10ms. If the distance is above a few kilometers, this is a much larger factor than the switch/router latency.
- 3 Transmission time. We transmit packets on a link at a fixed rate, usually 1 Gb/s or 10 Gb/s today. A 1500-byte Ethernet packet is about 12,000 bits. Therefore, it takes 12 $\mu$ s or 1.2 $\mu$ s, respectively, to transmit.
- 4 Queuing delay. A packet arriving at the input to a switch (or router) will be forwarded to an output link. If there are packets already in the queue for the output link, the packet will have to wait.

<b>Note</b>	Clearly the first three items are fixed delay. We can't strap a jet engine onto a packet and get it there faster than these fixed limits allow. The only variable that can be controlled is item 4.
-------------	---

If the queue is empty when a packet is placed into it, there is no additional delay, items 1, 2, and 3 completely describe how long it will take to get to the next node. Most switches, especially in a provider network, perform aggregation—they take a large number of subscriber interfaces (UNIs) and transport them over a small number of network trunks (NNIs).

Consider the following figure:

**Figure 8-8 Aggregation in a provider switch**

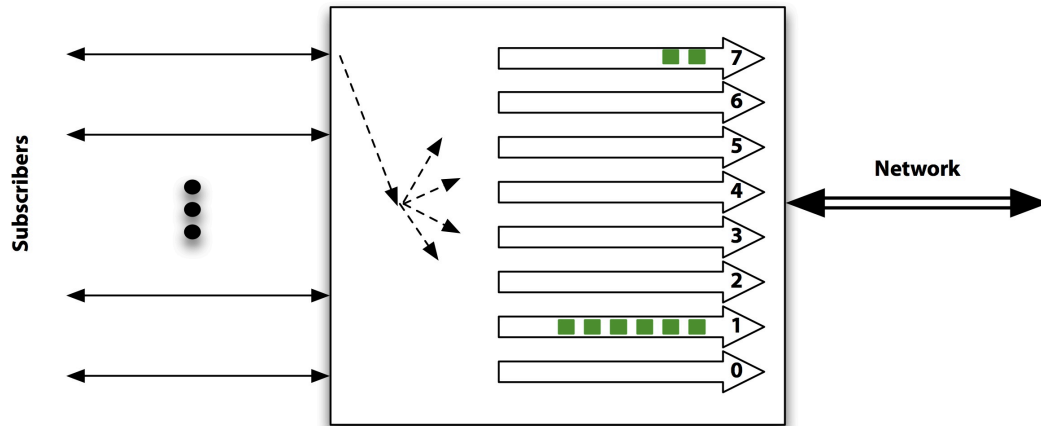
During the busy part of the day, the odds of an incoming subscriber packet finding the Network interface transmit queue empty are low. If there are four 1500-byte packets queued up already, the next packet will have to wait an additional 5 $\mu$ s (assuming a 10 Gb/s link), which could be greater than or equal to the inherent delay. 5 $\mu$ s may not seem like a long time, but with 20 or 30 subscribers, the queue could be longer than four packets, and, in terms of queuing delay, we have to consider that it can happen at each switch in the path. So, queuing delay has several important properties:

- It is the only one that can be controlled.
- It is variable (all other delay sources are fixed), and it can vary widely.
- It can be very large (compared to the sources other than propagation over a long haul).
- When it is bad, it is likely to be bad at multiple nodes in the path, which makes it worse.

The other, somewhat insidious, effect of having a long queue is that it can result in packet drops. Packet drops can happen because a switch is congested—its buffer pool is full from many packets being queued to many interfaces, or because it has artificially limited the depth of a queue and drops packets when that queue depth is reached.

Keeping the transmit queue short will reduce delay, reduce the variation in delay, and can reduce the frame loss—all attributes of a better quality of service. We can't really reduce the number of packets queued to an interface (other than by dropping packets), but we can have multiple queues and select packets for transmission based on the priority of the queue.

The following figure shows a scenario in which there are eight queues feeding the network interface. These queues are numbered 0 through 7, and the number represents the priority of the queue (zero being the lowest). When a packet comes in, an *internal priority* is assigned (see 8.2, “[Packet flow](#)”), and then the internal priority is mapped to a class of service queue.

**Figure 8-9 Multiple transmission queues**

The default mapping is *internal priority x* is mapped to *class of service x* with one exception — *internal priority 0* is mapped to *class of service 1* and vice versa<sup>30</sup>. The mapping can be changed with a *transmit class map*.

```
> PROFILE PRIORITY-TC-MAP standard-customer
> PRIORITY 5 COS-QUEUE 7
> PRIORITY 6 COS-QUEUE 7
> PRIORITY 0 COS-QUEUE 1 ! just restating the default
> PRIORITY 1 COS-QUEUE 1
> EXIT
>
> NNI tenG 1/1/3 ! this can be done both UNIs and NNIs
> SET PROFILE PRIORITY-TC-MAP standard-customer
> EXIT
```

If the switch has a rule that each time a packet is selected to be transmitted, it is selected from the highest priority queue that has a packet in it, clearly the high-priority packets will have shorter queues and shorter waits than other priorities<sup>31</sup>. In [Figure 8-9](#) there are packets queued to class 7 and to class 1.

The next packet to be selected will be taken from class 7, as will the one after that. Then, if class 7 is empty (and it may not be if another packet has arrived) a packet will be selected from class 1. Clearly the trade-off for reducing delay for class 7 is increasing it for the lower classes.

And clearly the choice can't be quite this simplistic, otherwise it would be possible for higher priority traffic to completely starve out lower priority traffic. The network manager has two ways to control how packets are selected from the various CoS queues. A minimum and maximum bandwidth can be specified for each queue, and the actual scheduling algorithm can be selected.

<sup>30</sup> This is done because “0” is usually the default priority applied to packets and it usually means “best effort”. By mapping the default to class 1, it allows one class of service that is below best effort, often called “background”. Packets with an internal priority of 1, therefore, are mapped to the background queue.

<sup>31</sup> Of course we can't ignore the old adage that “if everything is high priority, then there is no priority”. Prioritization depends on the premise that as the priority goes up the number of packets (actually bytes) that need to be transmitted go down — i.e., the club gets more and more exclusive.

The switch keeps track of the rate of transmission from each CoS queue. If a queue falls below its minimum, its priority increases. If a queue exceeds its maximum, its priority decreases. Consider the example above. We can build a scheduler profile and apply it to the NNI:

```
> PROFILE SCHEDULER standard ALGORITHM sp
> COS-QUEUE 1 MAX-BW 10000000 ! in Kbps this 10G
> COS-QUEUE 7 MAX-BW 10000000
> COS-QUEUE 1 MIN-BW 500000 ! this is 500Mbps
> COS-QUEUE 7 MIN-BW 100000 ! 100Mbps
> EXIT
> NNI tenG 1/1/1
> SET PROFILE SCHEDULER standard
> EXIT
```

The algorithm indicates strict priority, which is the default, and represents the behavior described in the previous example. The profile sets a maximum bandwidth on each queue to the link speed (10 Gb/s). It also sets a minimum bandwidth for queue 1 to 500 Mb/s. If the servicing rate on that queue falls below 500 Mb/s then the scheduler will give that queue more opportunity to transmit as long as the service rate on queue 7 (which innately has higher priority) is transmitting at least 100 Mb/s, that is, above its minimum. This is how the high priority traffic is kept from starving lower priority traffic.

packetVX modules support several other algorithms:

- **Round Robin (rr):** The scheduler cycles through each queue in order and schedules one packet from each. The minimum and maximum values influence the scheduler, but in general this mode does not provide a lot of distinction between classes of service.
- **Weighted Round Robin (wrr):** Each CoS queue requires a weight to be specified in the scheduler profile (COS-QUEUE x WEIGHT y). In wrr mode, the scheduler provides access to each CoS queue in round robin order. The scheduler services each queue one packet at a time, until the desired weighting has been fulfilled. For example, if CoS 7 has a weight of 4, and CoS 6 has a weight of 2, and all other queues have a weight of 1, the queues are serviced in the following order. 76543210 76 77 76543210 76 77 ...
- **Deficit Round Robin (drr):** The problem with rr and wrr is that they are packet-based. If the packet sizes across the various CoS queues are similar, they work well. If there are widely varying packet sizes, the results can be skewed. Deficit Round Robin addresses this by applying the weight against bytes transmitted rather than packets transmitted.
- **Strict Priority + WRR/DRR (sp+wrr, sp+drr):** These modes provide the best of both worlds. Any queue whose weight is set to 0 is treated as a strict priority queue (which is serviced first), and the other queues are treated as wrr or drr queues.

<b>Note</b>	To achieve the desired priority for traffic that passes through a packetVX 80 module, we recommend that you use a weight value that is divisible by two, when configuring the class of service (CoS) queue on any packetVX. If you use a weight of one or use consecutive weight values, you notice that the packetVX 80 is not forwarding traffic as expected.
-------------	---



## 8.6 CoS on intermediate switches

---

When traffic comes in from a UNI (subscriber) for subsequent forwarding into the provider network, most of the heavy lifting is done when the packet first arrives from the subscriber. Once traffic is in the network, the goal is to maintain the CoS characteristics

When the edge switch (the one connected to the subscriber) receives a packet, it determines its color (based on conformance to the bandwidth profile) and its class of service. These are both marked into the packet—the color is marked in the DEI bit of the S-VLAN tag (set for yellow packets), and the priority is marked in the Priority Code Point (PCP) field. The incoming NNI can use these two fields rather than having to be configured to re-create them:

```
> NNI tenG 1/1/2
> USEDEI ENABLE
> TRUST-INCOMING-PCP ENABLE
> EXIT
```

## 8.7 Quality of Service configuration

---

This section provides the provisioning procedures required to provision Quality of Service.

### 8.7.1 Define a Bandwidth Profile

Use this procedure to define a Bandwidth Profile.

**Pre-requisites:**

- None

<b>Note</b>	1	Bandwidth profiles applied to an egress NNI and UNI must be single-rate.
	2	When meter mode is set to single-rate, values for EIR and EBS cannot be set.

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch (optional)**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Create a bandwidth profile**

To create a bandwidth profile, enter the following command:

```
BTI7000:sw1(config)# profile bandwidth <string>
```

**Step 5 Define the Committed Information Rate**

To define the Committed Information Rate in Kb/s, Mb/s, or Gb/s, enter the following command:

```
BTI7000:sw1(config-profile-bw)# police cir <cir>
```

**Step 6 Define the Committed Burst Size**

To define the Committed Burst Size in Kbytes, enter the following command:

```
BTI7000:sw1(config-profile-bw)# police cbs <cbs>
```

**Step 7 Define Excess Information Rate (for two-rate only)**

To define the Excess Information Rate in Kb/s, Mb/s, or Gb/s, enter the following command:

```
BTI7000:sw1(config-profile-bw)# police eir <eir>
```

**Step 8 Define the Committed Burst Size (for two-rate only)**

To define the Committed Burst Size in Kbytes, enter the following command:

```
BTI7000:sw1(config-profile-bw)# police ebs <ebs>
```

**Step 9 Define Meter Mode and Color Mode**

To define Meter Mode and Color Mode, enter the following command:

```
BTI7000:sw1(config-profile-bw)# meter mode <sr-tcm | tr-tcm> color  
<aware | blind>
```

where *sr-tcm* is single rate and *tr-tcm* is two rate.

**Step 10 Define the Internal Priority as required (for ingress only)**

To define the Internal Priority, enter the following command:

```
BTI7000:sw1(config-profile-bw)# internal-priority <0-7>
```

**Step 11 Define the DSCP re-transmit action for conform and exceed**

To define the DSCP re-transmit action for conform and exceed enter the following commands:

```
BTI7000:sw1(config-profile-bw)# conform-action set-dscp-transmit  
<value 0-63>
```

```
BTI7000:sw1(config-profile-bw)# exceed-action set-dscp-transmit <value  
0-63>
```

You have successfully completed this procedure.

## 8.7.2 Define a Class Map

This procedure describes how to define a Class Map.

**Pre-requisites**

- None

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch (optional).**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Define a Class Map profile**

To define a Class Map profile, enter the following command:

```
BTI7000:sw1(config)# class-map <string> type {ingress-cos | egress-  
cos | service-map}
```

**Step 5 Define a set of traffic classes to match**

To define a set of traffic classes, enter one or more of the following command:

```
BTI7000:sw1(config-c-map)# match c-vlan <vlan-id>
```

```
BTI7000:sw1(config-c-map)# match c-vlan-priority <priority>
```

```
BTI7000:sw1(config-c-map)# match ethertype <value 0-65535>
```

```
BTI7000:sw1(config-c-map)# match ip <dest | src> <ip-addr>
```

```
BTI7000:sw1(config-c-map)# match ip protocol <protocol 0-255>
```

```
BTI7000:sw1(config-c-map)# match ip dscp <dscp value>
```

```
BTI7000:sw1(config-c-map)# match mac <dest | src> <mac-addr>
```

```
BTI7000:sw1(config-c-map)# match s-vlan-priority <priority>
BTI7000:sw1(config-c-map)# match tcp-control <value 0-63>
BTI7000:sw1(config-c-map)# match tcp-udp-port <dest | src> <port
0-65535>
```

### CLI command example

```
class-map ClassMap_CustomerA type ingress-cos
match c-vlan 10
exit
class-map ClassMap_CustomerB type ingress-cos
match c-vlan 20
exit
```

**Note** The switch supports layer 2 match criteria for per-CoS bandwidth on egress. Layer 3 and 4 match criteria is not supported.

You have successfully completed this procedure.

## 8.7.3 Create a service policy

This procedure describes how to create a service policy that makes a correlation between a Class of Service map and a bandwidth profile.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI70000(config)#
```

### Step 3 Select a virtual switch (optional)

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where *<switch\_id>* is the virtual switch identifier

For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Create a service policy profile.**

To create a service policy profile, enter the following command syntax:

```
BTI7000:sw1(config)# service-policy <string>
```

**Step 5 Identify the Class Map and Bandwidth Profile to be used**

To identify the Class Map and bandwidth profile to be used, enter the following command syntax:

```
BTI7000:sw1(config-p-map)# class-map <ClassMap> profile bandwidth <BW  
Profile>
```

**CLI command example**

```
service-policy ServicePolicy_CustomerA  
class-map Class_CustomerA profile bandwidth BW_CustomerA  
exit
```

You have successfully completed this procedure.

## 8.7.4 Applying a bandwidth profile to a UNI or NNI

This procedure explains how to apply a bandwidth profile to an ingress or egress UNI or NNI.

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 4 Navigate to the desired UNI or NNI

To navigate to the desired UNI or NNI, enter the following command syntax:

```
BTI7000:sw1(config)# <uni | nni> <gigabitEthernet  
| tenGigabitEthernet <shelf/slot/port> | <lag> <lag number>
```

#### Step 5 Apply a Bandwidth Profile to the UNI or NNI (ingress or egress)

```
BTI7000:sw1(config-nni TenGigE 1/1~)# set <egress | ingress> profile  
bandwidth <BW_Profile>
```

##### CLI command example

```
nni ten 1/1/1  
set egress profile bandwidth BandwidthProfile_NetworkPort  
exit
```

You have successfully completed this procedure.

## 8.7.5 Applying a bandwidth profile based on an Ethernet Service

This procedure describes how to apply a bandwidth profile based on an Ethernet service.

### Prerequisites

<b>Note</b>	A maximum of 768 ingress bandwidth profiles can be applied per UNI, per EVC or per CoS. On the PVX80, the maximum is 256.  A maximum of 64 egress bandwidth profiles can be applied per EVC or per CoS.
-------------	---

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows

```
BTI7000(config)#
```

#### Step 3 Select a virtual switch

To select a virtual switch, enter the following command syntax:

```
virtual-switch <switch_id>
```

where `<switch_id>` is the virtual switch identifier

For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Navigate to the desired Ethernet service

```
BTI7000:sw1(config)# eservice <E-Service>
```

### Step 5 Navigate to the desired UNI within the Ethernet service

```
BTI7000:swl(config-eservice)# uni <gigabitEthernet |
tenGigabitEthernet
        <shelf/slot/port> | <lag> <lag number>
```

### Step 6 Apply the Bandwidth Profile to the UNI (egress and/or ingress)

```
BTI7000:swl(config-uni-eservice)# set <egress| ingress> profile
bandwidth <BW_Profile>
```

## CLI command example

```

eservice EVPLAN_CustomerA
uni gig 1/1/1
set ingress profile bandwidth BandwidthProfile_EVC_CustomerA
exit
exit

```

You have successfully completed this procedure.

### 8.7.6 Applying a bandwidth profile based on a Class of Service

This procedure describes how to apply a bandwidth profile based on a Class of Service.

### Prerequisites

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

enable

The CLI prompt should now appear as follows:

BTI7000#

## Step 2 Access the Administration Configuration mode



To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### **Step 3 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### **Step 4 Navigate to the desired Ethernet service**

```
BTI7000:sw1(config)# eservice <E-Service>
```

### **Step 5 Navigate to the desired UNI within the Eservice**

```
BTI7000:sw1(config-eservice)# uni <gigabitEthernet |  
                                tenGigabitEthernet <shelf/slot/port> | <lag> <lag number>
```

### **Step 6 Apply the Service Policy Profile to the UNI (egress and/or ingress)**

```
BTI7000:sw1(config-eservice)# set {egress | ingress} service-policy  
<name>
```

```
<PolicyMap>
```

#### **CLI command example**

```
eservice EVPLAN_CustomerA  
uni gig 1/1/1  
set ingress service-policy PolicyMap_CustomerA  
exit  
exit
```

You have successfully completed this procedure.

## **8.7.7 Creating a Scheduler Profile**

This procedure describes how to create a Scheduler Profile. The scheduling options are SP, RR, WRR, DRR, SP+WRR, SP+DRR.

#### **Pre-requisites:**

- None

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Optionally, select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Create a Scheduler Profile**

```
BTI7000:sw1(config)# profile scheduler <string> algorithm  
                        <sp | rr | drr | sp+wrr | sp+drr>
```

**Step 5 Modify Queue weights as required**

This step applies to WRR, SP+WRR, DRR, SP+DRR only.

```
BTI7000:sw1(config-profile-sched)# cos-queue <Cos-queue> weight <Cos-  
weight>
```

<b>Note</b>	The scheduler on the packetVX 80 module requires that the weight values of the queues be a multiple of 2 (i.e. an even number). In a mixed network of packetVX 80 and other PVX modules, we recommend that you follow this rule on all PVX modules in order to ensure consistent handling of traffic in the network.
-------------	--

**Step 6 Modify Queue bandwidth as required**

```
BTI7000:sw1(config-profile-sched)# cos-queue <Cos-queue> <max-bw | min-  
bw> <bw in Kb/s>
```

**Step 7 Modify the maximum frame size as required**

This step applies to DRR and SP+DRR only.

```
BTI7000:sw1(config-profile-sched)# mtu-quanta <2 | 16>
```

### CLI command example

```
profile scheduler NetworkPortSchedule_WRR algorithm WRR
exit
profile scheduler NetworkPortSchedule_WRR algorithm WRR
cos-queue 0 weight 1
cos-queue 1 weight 10
cos-queue 2 weight 20
cos-queue 0 max-bw 100000
cos-queue 0 min-bw 10000
exit
```

You have successfully completed this procedure.

## 8.7.8 Applying a Scheduler Profile to a UNI or NNI

This procedure describes how to apply a Scheduler Profile.

### Pre-requisites:

- Create a virtual switch.
- Add a packetVX to the virtual switch.
- Create a Scheduler Profile.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where `<switch_id>` is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### **Step 4 Navigate to the desired UNI or NNI**

```
BTI7000:sw1(config)# <uni | nni>
                    <gigabitEthernet | tenGigabitEthernet>
                    <shelf/slot/port> | <lag> <lag number>
```

#### **Step 5 Apply a Scheduler Profile to the UNI or NNI**

```
BTI7000:sw1(config-uni Gige 1/1/1)# set profile scheduler
                                   <Sched_Profile>
```

##### **CLI command example**

```
nni ten 1/1/1
set profile scheduler CustomerA_WRR
exit
```

You have successfully completed this procedure.

## **8.7.9 Mapping customer traffic priorities (DSCP/PCP)**

This procedure describes how to map customer traffic priorities.

#### **Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### **Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### **Step 3 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 4 Navigate to the desired UNI or NNI

```
BTI7000:sw1(config)# <uni | nni>
                  <gigabitEthernet | tenGigabitEthernet>
                  <shelf/slot/port> | <lag> <lag number>
```

#### Step 5 Apply the DSCP/PCP profile to the UNI or NNI

**Note** DSCP/PCP profiles are mutually exclusive. You can specify a DSCP profile or you can specify a PCP profile but you cannot specify both on a single interface.

```
BTI7000:sw1(config-uni GigE 1/1/1)# set profile dscp-phb <name>
BTI7000:sw1(config-uni GigE 1/1/1)# set profile pcp-encoding-decoding
<name>
```

#### Step 6 Disable or enable DSCP/PCP trust on the UNI or NNI

```
BTI7000:sw1(config-uni GigE 1/1/1)# trust-incoming-dscp {enable |
disable }
BTI7000:sw1(config-uni GigE 1/1/1)# trust-incoming-pcp {enable |
disable }
```

##### CLI command example

```
nni ten 1/1/1
trust-incoming-pcp enable
exit
```

You have successfully completed this procedure.

## 8.7.10 Creating a Traffic Class Map Profile

This procedure describes how to create a Traffic Map Class Profile.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Optionally, select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Create a new traffic class map profile**

```
BTI7000:sw1(config)# profile priority-tc-map <string>
```

**Step 5 Modify the priority to queue mapping as required**

```
BTI7000:sw1(config-profile-tcmap)# priority <priority> cos-queue  
<class>
```

**CLI command example**

```
profile priority-tc-map CustomerA_TC_MAP  
priority 7 cos-queue 4  
priority 6 cos-queue 3  
priority 5 cos-queue 3  
priority 4 cos-queue 2  
priority 3 cos-queue 2  
priority 2 cos-queue 1  
priority 1 cos-queue 1  
priority 0 cos-queue 0  
exit
```

You have successfully completed this procedure.

## 8.7.11 Applying a Traffic Class Map Profile to a UNI/NNI

This procedure describes how to apply a Traffic Map Class Profile to a UNI/NNI.

**Pre-requisites:**

- Create the Traffic Class Map Profile.

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Navigate to the desired UNI or NNI**

```
BTI7000:sw1(config)# 0 <uni | nni> <gigabitEthernet |  
tenGigabitEthernet | lag> <shelf/slot/port>
```

**Step 5 Apply a traffic class map profile to the UNI or NNI**

```
BTI7000:sw1(config-uni GigE 1/1/1)# set profile priority-tc-map  
<TC_Map_Profile>
```

**CLI command example**

```
uni gigabitEthernet 1/1/12  
set profile priority-tc-map CustomerA_TC_MAP  
exit
```

You have successfully completed this procedure.

## 8.8 SLA monitoring

---

An important aspect to providing Service Level Agreements (SLAs) to subscribers is monitoring the services to ensure that SLA requirements are being met. On the packetVX this is done in two ways:

- In-service monitoring
- On-demand testing

**Important** If SLA Monitoring is enabled on a packetVX 24/4 or 24/2 module, copper ports 23 and 24 are not available as network interfaces. SLA monitoring is disabled by default, but can be enabled as part of the Virtual Switch configuration as follows:

```
sla-measurement {enable | disable}
```

**Note** SLA monitoring is not supported on ETREE services.

### 8.8.1 In-service monitoring

Ethernet services can be configured to monitor SLA metrics on an ongoing basis and record an event if any of the monitored characteristics are out of specification. Three metrics are monitored, with measurements taken between pairs of end points:

- Frame loss (one way)
- Round-trip delay
- Round-trip delay variation

Configuration of in-service SLA monitoring has two parts. One part involves configuring the UNIs in the Ethernet Service to exchange messages to actually measure the characteristics of the service. The results of these measurements are stored in the standard PM bins: 15-minute, 24-hour, and Untimed. The other part involves defining an SLA Profile that can be assigned to the service to define when to generate an event.

#### 8.8.1.1 Defining an SLA profile

Defining an SLA profile is similar to defining other profiles on the packetVX. The definition is opened with a profile name, and several parameters are then specified. Once defined, the named profile can be applied to a service.

Up to 768 measurements can be made at the same time in a single virtual switch.

A MEP sends DMM frames with ETH-DM request information to its peer MEP and receives DMR frames with ETH-DM reply information from its peer MEP. Based on the reply information, two-way frame delay and delay variation measurements are carried out.

For an SLA, the profile definition is opened and closed as follows:

```
> PROFILE SLA-MEASUREMENT <profile name>
> ... list of thresholds ...
> EXIT
```

The following are the thresholds that can be set in the profile:



```

> THRESHOLD PACKET-LOSS-RATIO [near-end | far-end] <decimal fraction>
> THRESHOLD DELAY-AVG <microseconds>
> THRESHOLD DELAY-MAX <microseconds>
> THRESHOLD DELAY-VAR-AVG <microseconds>
> THRESHOLD DELAY-VAR-MAX <microseconds>

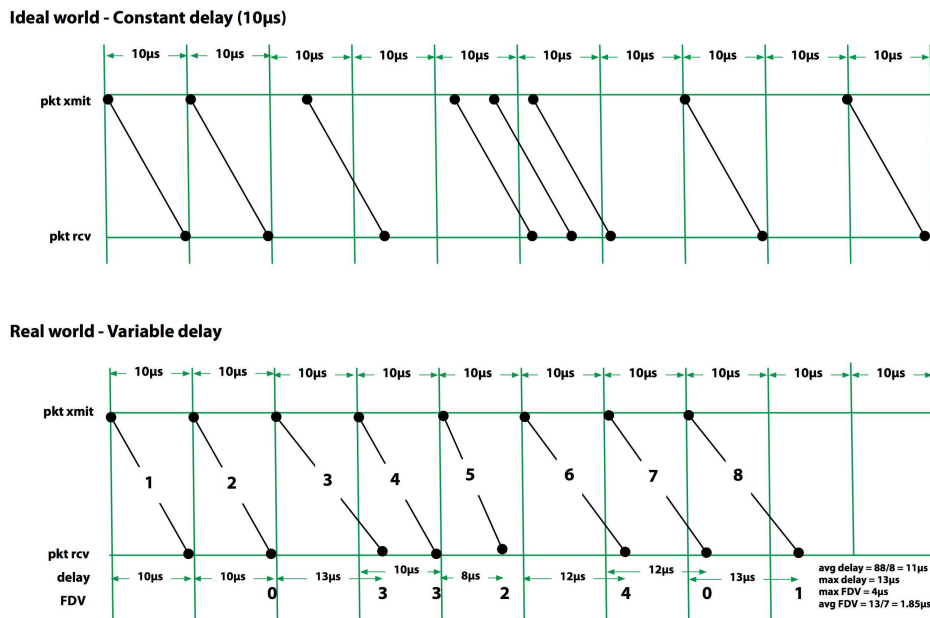
```

where

Parameter	Description
near-end	Represents the loss for the other system to send to this system
far-end	Represents the loss for this system to sent to the other system
DELAY	The time that it takes for a packet to be sent from one side of the service to the other and back again. It is the round trip time. When monitoring delay, the average is computed over the current bin (specified in the MONITOR-PERIOD). A threshold crossing alert will be generated if the average of the delay measurements in the current bin exceeds the specified amount or if a single sample exceeds the specified MAX value.
DELAY-VAR	The difference between one sample and the next. If the delay for Sample One is 10 milliseconds, and the delay for Sample Two is 11 milliseconds, the delay variation is 1 millisecond (1000 microseconds) as is the average to this point. If the delay for Sample Three is 9 milliseconds, its variation is 2 milliseconds and the average delay variation is 1500 microseconds. If the delay for Sample 4 is 10, then the average delay is 1333 $\mu$ s — $(+1+2+1)/3$ .

The following figure shows how these values relate to each other. The top graph depicts an ideal situation, where delay is constant. Whenever a packet is transmitted, it is received<sup>32</sup> 10 microseconds later (the slope of the lines is the same from packet to packet). Except in a completely empty network, this never really happens. The bottom graph depicts a more realistic case, where there is variability in the delay.

<sup>32</sup> The packetVX computes round trip delay, so in this figure, the delay represents the time for a packet to make a round trip.

**Figure 8-10 Delay and Delay Variation of packets**

After the SLA profile is defined, it is applied to the Eservice-UNI. For example:

```
> UNI gig 1/1/1
> SET PROFILE SLA-MEASUREMENT <profilename>
> EXIT
> EXIT
```

### 8.8.1.2 Initiating in-service monitoring

SLA monitoring must be explicitly activated between service end points. Each monitoring session has an initiator end point and a responder end point. These end points are identified by their MEP (Maintenance End Point) IDs. From each Eservice-UNI, you can monitor up to four end points. (In an E-LINE service, there is only one other end point, but in an E-LAN service there can be many.)

To configure an end point as a responder, use the following command:

```
> sla-measure rmeqid <id 1-8191> loss-delay responder
```

To configure an end point as an initiator, use the following command:

```
> sla-measure rmeqid <id 1-8191> loss-delay initiator
```

The SLA profile is applied to the initiator. The following example sets up both the responder and the initiator for an existing Eservice named “customer”:

On the responder:

```
> ESERVICE customer
> UNI gig 1/1/1
> SLA-MEASURE RMEPID 1 LOSS-DELAY RESPONDER
> EXIT
> EXIT
> EXIT
```

On the initiator:

```
> ESERVICE customer
> UNI gig 1/1/17
> SLA-MEASURE RMEPID 2 LOSS-DELAY INITIATOR
> EXIT
> SET-PROFILE SLA-MEASUREMENT goldservice
> EXIT
> EXIT
```

In-service SLA measurement is active for the specified pair of end points. Events will be generated whenever the connection between the end points violates the SLA profile specified.

The current status of in-service monitoring can be viewed. For example:

```
BTI7000:sw2(config)# show uni-eservice uni gig 1/3/11 eservice evplan rmepid
4712 pm interval 15-min bin 0
```

VS	E-Service	UNI	r-MepId
2	evplan	GigE 1/3/11	4712

Interval: 15-min, Bin: Current  
Near End Frame Loss Ratio : 0.000 %  
Far End Frame Loss Ratio : 0.000 %  
Two way Delay Minimum : 26 microseconds  
Two way Delay Maximum : 29 microseconds  
Two way Delay Average : 27 microseconds  
Two way Delay Variation Minimum : 0 microseconds  
Two way Delay Variation Maximum : 3 microseconds  
Two way Delay Variation Average : 0 microseconds

## 8.8.2 On-demand testing

On-demand testing provides the ability to measure the throughput between a pair of end points against a bandwidth profile. The maximum rate that can be tested is 1 Gb/s.

On-demand testing involves the following steps:

- Set the on-demand responder Eservice administration state to test and then configure the UNI.
- Set the on-demand initiator Eservice administration state to test then configure the UNI.
- Start the throughput test. Before starting the test, the state of the responder and initiator must be "ready;" otherwise, the test fails.
- Stop the throughput test. Before stopping the test, the state of the initiator must be "running."

The following example shows how the responder Eservice is configured:

```
> ESERVICE customer
> ADMIN-STATE TESTING
> UNI gig 1/1/1
> SLA-MEASUREMENT RMEPID 1 THROUGHPUT RESPONDER
> INGRESS SERVICE-POLICY <name> CLASS-MAP [<name>]
> EXIT
```

```
> EXIT
> EXIT
```

**Note** After creating the throughput responder endpoint, it is in an initialization state until the initiator end point is configured.

The following example shows how the initiator Eservice is configured:

```
> ESERVICE customer
> ADMIN-STATE TESTING
> UNI gig 1/1/17
> SLA-MEASUREMENT RMEPID 2 THROUGHPUT INITIATOR
> INGRESS SERVICE-POLICY <name> CLASS-MAP [<name>]
> S-VLAN-PRIORITY n ! optional
> <frame-size specification> ! see below
> THROUGHPUT START
> EXIT
> EXIT
> EXIT
```

**Note** After creating the throughput initiator endpoint, it is in an initialization state until the responder end point is configured.

Up to six frame sizes can be tested on a throughput test; for example: 68, 256, 512, 1024, 1522, and 2048. The frame sizes are set on the initiator with the `frame-size-n` command in the location indicated in the preceding example.

```
> FRAME-SIZE-1 68
> FRAME-SIZE-2 256
> ...
> FRAME-SIZE 6 2000
```

**Note** If a frame size entry is not specified (e.g., if `FRAME-SIZE-4` is not set), it is skipped.

The results of the throughput test can be viewed from the following modes in the CLI:

- In Global configuration mode, using the command `show throughput`
- In Service-UNI configuration mode, using the command `show throughput {rmepid <id>}`
- In Throughput configuration mode, using the command `show`

These commands display the results of the throughput test. For example:

```
BTI7000:sw2(config-throughput-init)# show
VS    E-Service    UNI          r-MepId  test    initiator  responder
--  -----  -
2    evplan    GigE 1/3/11  4712    initiator ready      -----
                                     role    state    oper state

bandwidthProfileName: bw2
servicePolicyName:
classMapName:
initiatorSVlanPriority: 0
```

CIRrate test result: pass

N	frameSize	Far End Throughput (Mbps)	Near End Throughput (Mbps)
1	68	700	700
2	256	700	700
3	512	700	700
4	9600	700	700
5	0	0	0
6	0	0	0

### 8.8.3 SLA monitoring provisioning

This section describes the procedures required to provision SLA monitoring.

#### 8.8.3.1 Configuring an SLA profile

This procedure explains how to define an SLA profile.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- A virtual switch must be provisioned.

##### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

##### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

##### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

##### Step 4 Enable SLA measurement

To enable SLA measurement enter the following command:

```
protocol sla-measurement enable
```

#### **Step 5 Define the SLA profile**

To define an SLA profile enter the following command:

```
profile sla-measurement <profile_name>
```

For example, the command string might be

```
profile sla-measurement Profile1
```

#### **Step 6 Specify the thresholds in the SLA profile**

To specify the thresholds in the SLA profile enter one or more of the following commands:

```
> THRESHOLD PACKET-LOSS-RATIO [near-end | far-end] <decimal fraction>
> THRESHOLD DELAY-AVG <microseconds>
> THRESHOLD DELAY-MAX <microseconds>
> THRESHOLD DELAY-VAR-AVG <microseconds>
> THRESHOLD DELAY-VAR-MAX <microseconds>
```

For example, the command string might be

```
threshold delay-avg 10
```

#### **Step 7 Specify the monitoring period**

To specify the monitoring period enter the following command:

```
monitor period <15-minutes | 24-hours>
```

For example, the command string might be

```
monitor period 15-minutes
```

#### **Step 8 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### **Step 9 Apply the SLA profile to an Eservice UNI**

To apply the SLA profile to an Eservice UNI, enter the following commands:

```
eservice <servicename>
uni gigabitethernet <shelf/slot/port>
set profile sla-measurement <profile_name>
```

For example, the command strings might be

```
eservice Service1
uni gigabitethernet 1/1/1
```

```
set profile sla-measurement Profile1
```

You have successfully completed this procedure.

### 8.8.3.2 Configuring in-service monitoring

This procedure explains how to configure in-service monitoring.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- A virtual switch must be provisioned.
- The Eservice must already exist

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Access the Eservice configuration mode for the Eservice

To access the Eservice configuration mode, enter the following command:

```
eservice <service_name>
```

The CLI prompt should now appear as follows:

```
BTI7000(config-eservice)#
```

#### Step 4 Associate the UNI of the responder to the Ethernet service

To associate the UNI, enter the following command:

```
BTI7000:sw1(config-eservice)#uni<gigabitEthernet|tenGigabitEthernet|lag><shelf/slot/port>
```

For example, the command string might be

```
uni gigabitEthernet 1/1/1
```

#### Step 5 Specify the responder's SLA measurement type

To specify a responder enter the following command:

```
sla-measurement rmepid <rmepid> loss-delay responder
```

For example, the command string might be

```
sla-measurement rmepid 1 loss-delay responder
```

#### **Step 6 Exit to the top level command mode**

To exit to the top level command mode, enter the following commands:

```
exit
exit
exit
exit
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### **Step 7 Access the Eservice configuration mode for the Eservice**

To access the Eservice configuration mode, enter the following command:

```
eservice <service_name>
```

The CLI prompt should now appear as follows:

```
BTI7000(config-eservice)#
```

#### **Step 8 Associate the UNI of the initiator to the Ethernet service**

To associate the UNI, enter the following command:

```
BTI7000:sw1(config-eservice)#uni<gigabitEthernet|tenGigabitEthernet|
lag><shelf/slot/port>
```

For example, the command string might be

```
uni gigabitEthernet 1/1/17
```

#### **Step 9 Specify the initiator's SLA measurement type**

To specify an initiator enter the following command:

```
sla-measurement rmepid <rempid> <loss-delay> initiator
```

For example, the command string might be

```
sla-measurement rmepid 2 loss-delay initiator
```

#### **Step 10 Exit to the previous command configuration mode**

To exit from the current command configuration mode, enter the following command:

```
exit
```

#### **Step 11 Apply the SLA profile to the Eservice UNI**

To apply the SLA profile to the Eservice UNI, enter the following commands:

```
set profile sla-measurement <profile_name>
```

For example, the command strings might be



```
set profile sla-measurement Profile1
```

You have successfully completed this procedure.

### 8.8.3.3 Configuring on-demand testing

This procedure explains how to configure on-demand testing.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- A virtual switch must be provisioned.
- The Eservice must already exist

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Access the Eservice configuration mode for the Eservice

To access the Eservice configuration mode, enter the following command:

```
eservice <service_name>
```

The CLI prompt should now appear as follows:

```
BTI7000(config-eservice)#
```

#### Step 4 Associate the UNI of the responder to the Ethernet service

To associate the UNI, enter the following command:

```
BTI7000:sw1(config-eservice)#uni<gigabitEthernet|tenGigabitEthernet|lag><shelf/slot/port>
```

For example, the command string might be

```
uni gigabitEthernet 1/1/1
```

#### Step 5 Specify the responder's SLA measurement type

To specify a responder enter the following commands:

```
sla-measurement rmepid <rempid> throughput responder
ingress service-policy <name> class-map <name>
```

For example, the command strings might be:

```
sla-measurement rmepid 1 throughput responder
ingress bandwidth Bandwidth-Profile1
or
ingress service-policy Service-Policy1 class-map Class-Map1
```

#### **Step 6 Exit to the top level command mode**

To exit to the top level command mode, enter the following commands:

```
exit
exit
exit
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### **Step 7 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### **Step 8 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### **Step 9 Access the Eservice configuration mode for the Eservice**

To access the Eservice configuration mode, enter the following command:

```
eservice <service_name>
```

The CLI prompt should now appear as follows:

```
BTI7000(config-eservice)#
```

#### **Step 10 Associate the UNI of the initiator to the Ethernet service**

To associate the UNI, enter the following command:

```
BTI7000:sw1(config-eservice)#uni<gigabitEthernet|tenGigabitEthernet|
lag><shelf/slot/port>
```

For example, the command string might be

```
uni gigabitEthernet 1/1/17
```

#### **Step 11 Specify the initiator's SLA measurement type**

To specify an initiator enter the following commands:

```
sla-measurement rmepid <rmepid> throughput initiator
ingress service-policy <name> class-map <name>
s-vlan-priority <n>
<frame-size specification>
throughput start
```

For example, the command strings might be:

```
sla-measurement rmepid 1 throughput initiator
ingress service-policy Service-Policy1 class-map Class-Map1
s-vlan-priority 1
frame-size-1 68
throughput start
```

You have successfully completed this procedure.



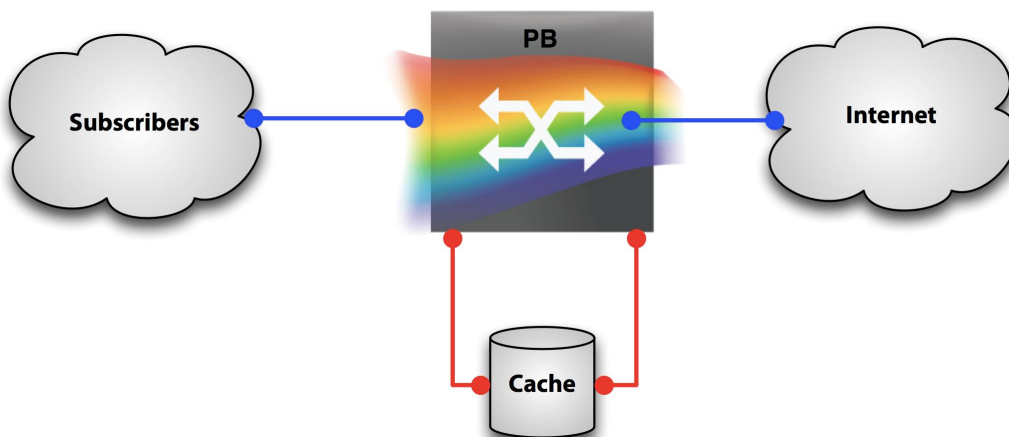
## 9.0 Configuring flow redirection

The BTI™ packetVX® operates as a Provider Bridge, with Ethernet services configured on the UNIs for transport across the network. If the UNI is configured for a *private* service, all packets on the UNI are considered to be part of the service. If the UNI is configured for *virtual private services*, there can be multiple services terminating on the UNI (service multiplexing), and packets are mapped to specific services based on their C-VLAN ID (C-VLAN-mapping).

There are situations where it is desirable to be able to split the packets within a C-VLAN into multiple services based on other criteria. One example of this is with the WideCast Transparent Cache caching service. To conserve processing resources on the WideCast server, it is desirable to forward only traffic that it might be able to cache, e.g., web traffic, and to bypass the server for other traffic, such as mail, file transfers, etc.

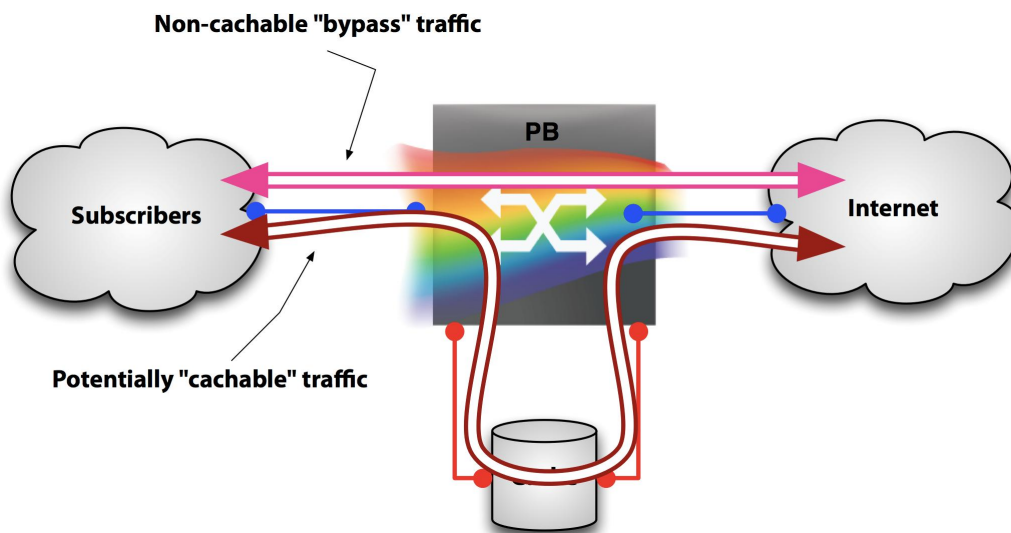
Consider the following figure.

**Figure 9-1 Caching service connected to packetVX network**



All traffic between the subscribers and the Internet could be routed through the cache; in most networks, 80% of the traffic is subject to caching. In this scenario, it would be useful to map some traffic to a service that goes through the cache and other traffic to a service that bypasses the cache, as shown in the following figure.

**Figure 9-2 Cacheable and bypass traffic**



Traffic arriving from subscribers or from the Internet is split into two services, one that goes directly from UNI to UNI and bypasses the cache, and another that goes through the cache. This split could be based on TCP or UDP port or other criteria.

## 9.1 Service maps and service policies

The packetVX implements a capability called *flow redirection* to address the requirement described in [Chapter 9, “Configuring flow redirection”](#). The class map feature of the packetVX is used to define criteria for flow redirection.

Class maps are defined as follows:

```
> CLASS-MAP name TYPE map-type
> <list of MATCH commands>
> EXIT
```

For flow redirection, the map-type is SERVICE-MAP. The class map contains a list of match commands, all of which must be met (and condition) for the service mapping to be effective, but multiple class maps can be used to effect an "or" condition.

The MATCH commands that are available in the class map are as follows:

```
> MATCH C-VLAN <vlan-id>
> MATCH C-VLAN-PRIORITY <priority>
> MATCH IP SRC <ip-address>
> MATCH IP DEST <ip-address>
> MATCH TCP-UDP-PORT DEST <port #> or <port # range>
> MATCH TCP-UDP-PORT SRC <port #> or <port # range>33
> MATCH IP DSCP <value>
> MATCH IP-PROTOCOL [TCP | UDP | ICMP | IGMP | VALUE <n>]
```

For example, the following class map matches all TCP port 80 (web) traffic on C-VLAN 700:

```
> CLASS-MAP V700-DP80 TYPE SERVICE-MAP
> MATCH C-VLAN 700
> MATCH IP-PROTOCOL TCP
> MATCH TCP-UDP-PORT DEST 80
> EXIT
```

Similarly, the following class map matches all TCP ports greater than 1023 on C-VLAN 700:

```
> CLASS-MAP V700-DPBIG TYPE SERVICE-MAP
> MATCH C-VLAN 700
> MATCH IP-PROTOCOL TCP
> MATCH TCP-UDP-PORT DEST 1024 65535
> EXIT
```

The class maps, once defined, are combined into a SERVICE POLICY before they are applied to the Service UNI.

```
> SERVICE-POLICY redirect-dest
> CLASS-MAP V700-DP80
> CLASS-MAP V700-DPBIG
> EXIT
```

Specifying two class maps (or more) indicates that if one map doesn't match, the next one should be tried. This provides the ability to specify map1 or map2 or map3, etc.

<sup>33</sup> If a range is specified, it must adhere to the requirement that it begin on a value that is  $2^n$  and end at  $2^{m-1}$  (with  $m > n$ ). For example, 64 to 127.

A service policy must be defined even if there is only a single class map.



## 9.2 Applying service policies to service UNIs

A service policy can be applied to a service UNI in the same way that a C-VLAN map is typically applied. For example:

```
> ESERVICE cache1 TYPE evpline
> S-VLAN 200
> UNI gig 1/1/6
> SET SERVICE-MAP SERVICE-POLICY redirect-dest
> EXIT
> EXIT
```

This service defines the redirection to the cache on the subscriber side as seen in [Figure 9-2 on page 9-2](#). It can be paired with a bypass service that is simply defined by a VLAN map. For example:

```
> ESERVICE bypass TYPE evpline
> S-VLAN 201
> UNI gig 1/1/6
> C-VLAN 700
> EXIT
> EXIT
```

The problem with this scenario is that these two service definitions are not disjoint. When services are defined only by C-VLAN map, there is no ambiguity. If C-VLAN 700 is mapped to service A, then it is not also in service B (on a given UNI). But in this case, some packets from C-VLAN 700 are mapped to bypass and some are mapped to *cache1*, and the results are different depending on what order the services are evaluated. This issue is addressed in two ways.

First, C-VLAN-map-based definitions, such as the bypass service described above, always evaluated last. So, if there are only two services defined, one using a service policy and one using a C-VLAN map, there is no ambiguity. If, however, there are two or more services defined with a service policy, an additional command is provided: FILTER-SEQUENCE. The FILTER-SEQUENCE command takes a value that provides a relative ordering. For example:

```
> ESERVICE bypass TYPE evpline
> S-VLAN 201
> UNI gig 1/1/6
> FILTER-SEQUENCE 20
> SET SERVICE-MAP SERVICE-POLICY redirect2
> EXIT
> EXIT
> ESERVICE cache1 TYPE evpline
> S-VLAN 200
> UNI gig 1/1/6
> FILTER-SEQUENCE 10
> SET SERVICE-MAP SERVICE-POLICY redirect1
> EXIT
> EXIT
```

Specifying that UNI gig 1/1/6 has a lower sequence number<sup>34</sup> in the redirect1 service means that it will be evaluated before UNI gig 1/1/6 in the redirect2 service.

For traffic coming from the Internet side, similar service definitions are needed, but for the cache1 service we want to look at the source ports rather than the destination ports (the differences are **inbold** text).

```
> CLASS-MAP V700-SP80 TYPE SERVICE-MAP
> MATCH C-VLAN 700
> MATCH IP-PROTOCOL TCP
> MATCH TCP-UDP-PORT SRC 80
> EXIT
> CLASS-MAP V700-SPBIG TYPE SERVICE-MAP
> MATCH C-VLAN 700
> MATCH IP-PROTOCOL TCP
> MATCH TCP-UDP-PORT SRC 1024 65535
> EXIT
> SERVICE-POLICY redirect-source
> CLASS-MAP V700-SP80
> CLASS-MAP V700-SPBIG
> EXIT
> ESERVICE bypass TYPE evpline
> S-VLAN 201
> UNI gig 1/1/6
> FILTER-SEQUENCE 20 ! This is not necessary. Always last anyway.
> C-VLAN 700
> EXIT
> EXIT
> ESERVICE cache1 TYPE evpline
> S-VLAN 200
> UNI gig 1/1/6
> FILTER-SEQUENCE 10
> SET SERVICE-MAP SERVICE-POLICY redirect-source
> EXIT
```

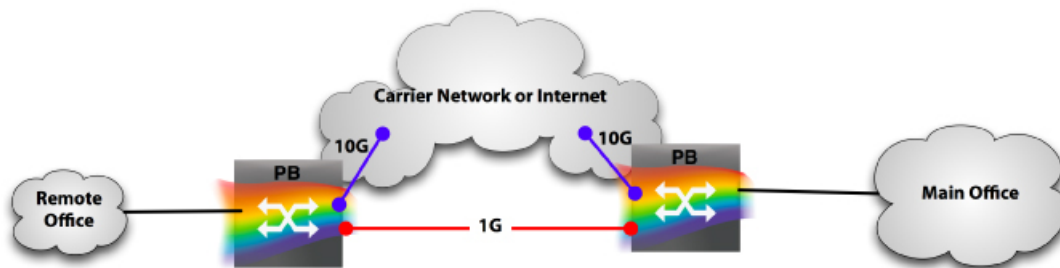
---

<sup>34</sup> If a range is specified, it must adhere to the requirement that it begin on a value that is  $2^n$  and end at  $2^{m-1}$  (with  $m > n$ ). For example, 64 to 127.

## 9.3 Another application for flow redirection

Flow redirection can be used to differentiate traffic within a VLAN that requires a different quality of service. Consider the following figure.

**Figure 9-3 Flow-redirection application example**



The provider is providing an Eservice from the Remote Office to the Main Office. The edge bridges have 10G links into the network cloud. One of the applications that runs over the service is VoIP. The latency across the cloud could be too large for good voice quality. The carrier has a 1G link between the edge bridges. This is not enough for all the traffic that has to be carried (there are other subscribers on the edges, after all), but it is enough for the VoIP.

To split off the VoIP traffic, we need to redirect SIP, RTP, and RTCP. For example:

```
> CLASS-MAP SIP TYPE SERVICE-MAP
> ! This MAP will match all packets destined to port 5060 on all VLANs
> MATCH TCP-UDP-PORT DEST 5060
> EXIT
> CLASS-MAP RTP TYPE SERVICE-MAP
> ! This MAP will match all packets destined to port 5004 on all VLANs
> MATCH TCP-UDP-PORT DEST 5004
> EXIT
> CLASS-MAP RTCP TYPE SERVICE-MAP
> ! This MAP will match all packets destined to port 5005 on all VLANs
> MATCH TCP-UDP-PORT DEST 5005
> EXIT
> SERVICE-POLICY redirect-voice
> CLASS-MAP SIP
> CLASS-MAP RTP
> CLASS-MAP RTCP
> EXIT
> ESERVICE voice TYPE evpline
> S-VLAN 100
> UNI gig 1/1/17
> SET SERVICE-MAP SERVICE-POLICY redirect-voice
> EXIT
> SPANNING-TREE 1
> EXIT
>
> ESERVICE notvoice TYPE evpline
```

```
> S-VLAN 101
> UNI gig 1/1/17
> C-VLAN 2-4090
> EXIT
> EXIT
```

The following should be noted about this example:

- **FILTER-SEQUENCE** is not used. Since there is only one service that uses a service policy on the UNI, there is no ambiguity.
- The *voice* service is assigned to a different spanning tree. Assuming that the default spanning tree instance will forward packets through the cloud to get between the end points, a second instance must be defined that will cause the voice packets to travel over the GbE.

<b>Note</b>	The service is really a private line service (EPLINE) in that all the traffic (on all C-VLANs) from one port is being transferred to the other. However, since we are splitting the traffic into two different services, we have to use EVPLINE. This is why the <code>notvoice</code> service maps all VLANs to the service, and the <code>voice</code> service does care about VLANs at all.
-------------	--

---

## 9.4 Define a class map for flow redirect

---

This procedure describes how to define a class map for flow redirect.

### Pre-requisites

- None

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Select a virtual switch (optional).

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 4 Define a Class Map profile

To define a Class Map profile, enter the following command:

```
BTI7000:sw1(config)# class-map <string> type service-map
```

For example, the command string might be:

```
class-map V700-DP80 type service-map
```

#### Step 5 Define a set of traffic classes to match

To define a set of traffic classes, enter one or more of the following commands:

```
BTI7000:sw1(config-c-map)# match c-vlan <vlan-id>
```

```
BTI7000:sw1(config-c-map)# match c-vlan-priority <priority>
```

```
BTI7000:sw1(config-c-map)# match ethertype <value 0-65535>
BTI7000:sw1(config-c-map)# match ip <dest | src> <ip-addr>
BTI7000:sw1(config-c-map)# match ip protocol <protocol 0-255>
BTI7000:sw1(config-c-map)# match ip dscp <dscp value>
BTI7000:sw1(config-c-map)# match mac <dest | src> <mac-addr>
BTI7000:sw1(config-c-map)# match s-vlan-priority <priority>
BTI7000:sw1(config-c-map)# match tcp-control <value 0-63>
BTI7000:sw1(config-c-map)# match tcp-udp-port <dest | src> <port
0-65535>
```

### CLI command examples

The following class map example matches all TCP port 80 (web) traffic on C-VLAN 700:

```
> CLASS-MAP V700-DP80 TYPE SERVICE-MAP
> MATCH C-VLAN 700
> MATCH IP-PROTOCOL TCP
> MATCH TCP-UDP-PORT DEST 80
> EXIT
```

The following class map example matches all TCP port 80 (web) traffic on C-VLAN 700:

```
> CLASS-MAP V700-DPBIG TYPE SERVICE-MAP
> MATCH C-VLAN 700
> MATCH IP-PROTOCOL TCP
> MATCH TCP-UDP-PORT DEST 1024 65535
> EXIT
```

<b>Note</b>	The switch supports layer 2 match criteria for per-CoS bandwidth on egress. Layer 3 and 4 match criteria is not supported.
-------------	--

You have successfully completed this procedure.

---

## 9.5 Create a service policy for flow redirect

---

This procedure describes how to create a service policy for flow redirect.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI70000(config)#
```

### Step 3 Select a virtual switch (optional)

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Create a service policy profile.

To create a service policy profile, enter the following command syntax:

```
BTI7000:sw1(config)# service-policy <string>
```

For example, the command string might be:

```
> SERVICE-POLICY redirect-dest
```

### Step 5 Identify the Class Map(s) to be used

To identify the Class Map and bandwidth profile to be used, enter the following command syntax:

```
BTI7000:sw1(config-p-map)# class-map <ClassMap>
```

#### CLI command example

```
> SERVICE-POLICY redirect-dest  
> CLASS-MAP V700-DP80  
> CLASS-MAP V700-DPBIG  
> EXIT
```

You have successfully completed this procedure.



## 10.0 Configuring Management VLAN services

---

System administrators can connect to the BTI 7000 Series™ in several different ways:

- SCP: Front panel craft interfaces
- NMS and OSC ports
- General Communications Channel (GCC): Remote IP management through OTU2 ports on the Transponder, Muxponder, and BTI™ packetVX® 10G interfaces.

**Note** The packetVX 80 does not support GCC.

- Management VLAN (M-VLAN): IP over a packetVX Ethernet service.

Management VLAN is provisioned much like other Ethernet services, as follows:

- 1 The user defines an Ethernet service of type **MGMTVLAN**.
- 2 Assigns a provider S-VLAN, a customer C-VLAN, and associates UNI and NNI ports to this Eservice
- 3 After an IP address is assigned to the service, the system can be managed through that IP address over the UNI and NNI ports associated with the service, allowing the user to telnet to the CLI or connect using proNX 900 Node Controller.

This section describes M-VLAN provisioning and includes the following topics:

- [10.1, “Managing the BTI 7000 Series: GCC, NMS, Craft, and Management VLAN”](#)
- [10.2, “Configuring the Management VLAN service”](#)
- [10.3, “Configuration flowchart”](#)
- [10.4, “Provisioning Management VLANs”](#)

## 10.1 Managing the BTI 7000 Series: GCC, NMS, Craft, and Management VLAN

---

BTI has various mechanisms for allowing an administrator to connect to or remotely manage the system using IP:

- **Craft ports:** The SCP front panel has two craft ports, one Ethernet and one serial. The administrator can assign an IP address to the craft port, which traditionally has been used for direct, non-routed access for an administrator who is physically present in front of the node.
- **NMS port:** Located on the Main Shelf Interface (MSI) module, the NMS port is a 100 Mb/s Ethernet port to which the administrator assigns an IP address and gateway for management of the node over a routed IP network.

The GCC (General Communications Channel) allows a user to create point-to-point (PPP) links between nodes using 10G ports configured for OTU2 on Transponder, Muxponder, and packetVX modules. GCC links are unnumbered and share the IP address assigned to the NMS port.

With Management VLAN (M-VLAN), the user can now configure an Eservice dedicated to carrying management traffic, and run IP directly over an Ethernet VLAN on ports associated with that service. Unlike GCC, M-VLAN is a numbered IP interface; a separate IP address must be assigned to the service. The M-VLAN service is effectively an IP-addressable Ethernet interface attached to one of the VLANs carried by the packetVX module. Note that while multiple UNI and NNI ports may be associated with the service, the IP address is assigned to the service as a whole, not individual ports.

As with the NMS and GCC interfaces, the OSPF routing protocol can be configured to run over M-VLAN to distribute IP route information through the network topology.

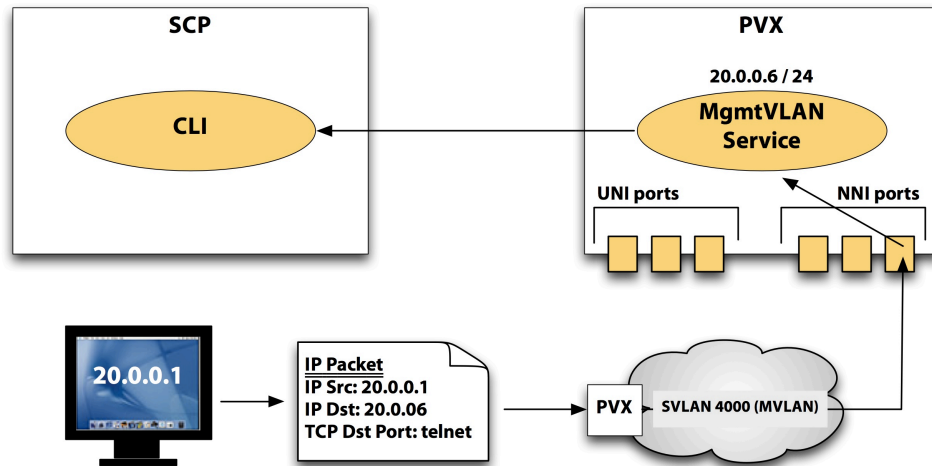
The system functions as an IP router. Packets arriving on the M-VLAN destined for other IP subnets are routed through the system. IP packets can be routed between the NMS port, GCC links, and the M-VLAN. For example, if a remote node on a GCC link wishes to ping another node reachable through the M-VLAN, the software properly routes between the two networks.

**Note** Only one MgmtVLAN service can be configured per virtual switch.

Since a M-VLAN is an Eservice, features that work for other Eservices also work for M-VLAN; for example, MSTP, class-of-service profiles, ACLs, L2 ping, and trace.

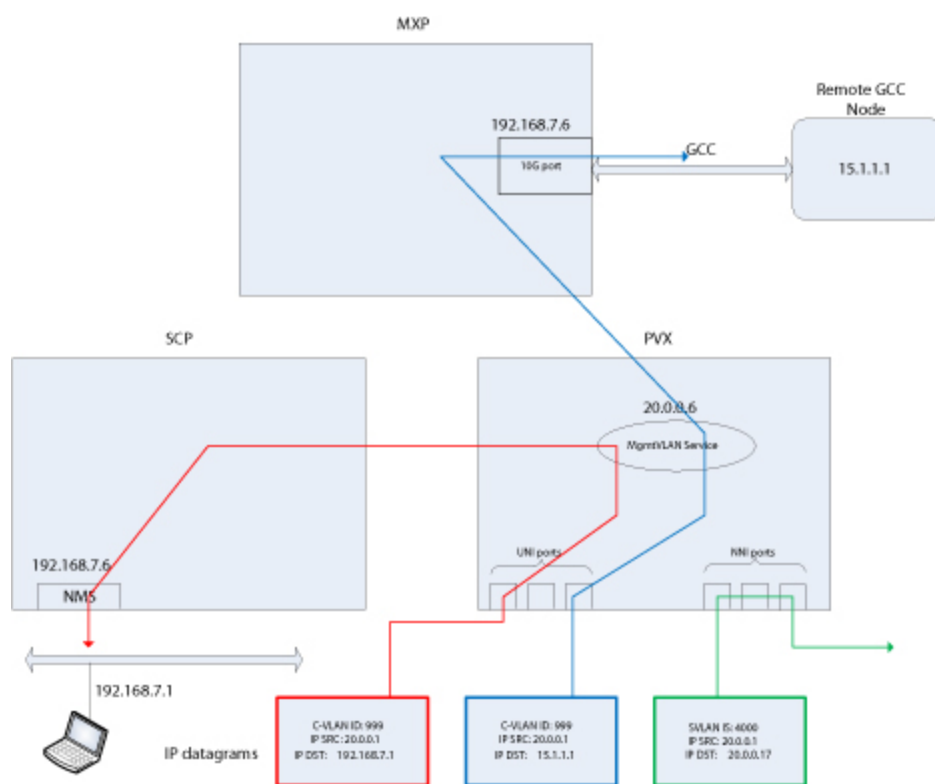
Internally, the MgmtVLAN service is similar to an **EVPLAN** service; it is a multipoint LAN service connecting multiple provider bridges through NNI ports over an S-VLAN. The administrator can associate UNI ports with the service, allowing systems on the M-VLAN to be reached through a customer VLAN. The main difference between a MgmtVLAN service and an EVPLAN is that with MgmtVLAN, when IP and ARP frames are either multicast or unicast to the virtual switch's bridge ID MAC address, those frames are received by the packetVX module and processed by the system's IP stack. Once received, the IP stack either routes the packets out through another interface (for example, the NMS port or a GCC link) or hands the packet to a local application (for example, the CLI, SNMP). Otherwise, however, the MgmtVLAN behaves like an EVPLAN. UNI ports mapped to the service can be mapped to other services, with the C-VLAN mapping table determining which customer VLAN maps to which service.

The following figure shows the IP packet flow through the system when an administrator telnets to the system from across the packetVX network. In this case, the administrator telnets into the system—IP 20.0.0.6. The packets are carried across the provider-bridged network in the MgmtVLAN—S-tag=4000. Packets arrive on an NNI port with a destination MAC address of the virtual switch's bridge MAC address and the M-VLAN's IP address as the destination IP. The packets are routed internally to the CLI running on the SCP.



The following figure shows how the system acts as an IP router. Packets arriving on the MgmtVLAN service can be routed out any other IP interface on the system. Three different packets are routed. The first packet (on the left in red) arrives on a UNI and is destined for another node on the NMS port's Ethernet segment. The packet is routed from the packetVX module to the SCP, where it is sent out the NMS port to the destination PC. The second packet (in the middle in blue) also arrives on a UNI and is routed to a remote node connected over a GCC link through an OTU2 port on a Muxponder (MXP). Finally, the third packet (on the right in green) arrives on an NNI port and is destined for another node on the M-VLAN's IP subnet. The packet is simply bridged out to another NNI rather than routed.

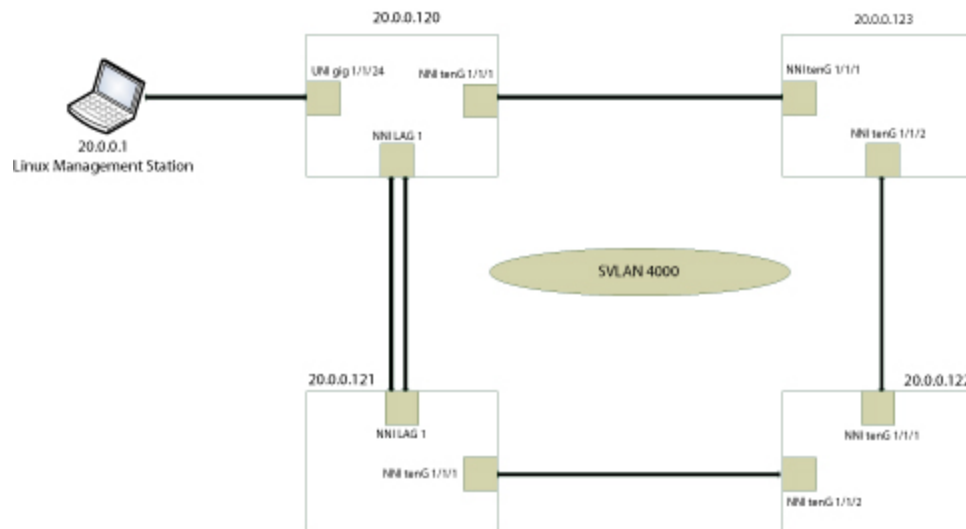
This figure also shows that although the M-VLAN is a provider service that operates on an S-VLAN, the user traffic can also be C-tagged. See [10.2, “Configuring the Management VLAN service”](#) for information about configuring M-VLAN over UNI ports.



## 10.2 Configuring the Management VLAN service

Provisioning the Management VLAN (MgmtVLAN) service is much like provisioning an EVPLAN service, but with additional steps. In general, the administrator first creates the service, assigns an S-VLAN to it, associates UNI and/or NNI ports with it, and optionally maps a customer VLAN to it. A few extra steps are needed for M-VLAN to assign an IP address to the service and to configure a C-VLAN ID for the service if the administrator wishes to manage the system from a customer VLAN.

Consider the topology in the following figure:



In this topology, there are four systems in a ring configuration running on S-VLAN 4000 connected through either 10G or LAG NNI ports. Each node has an IP address on the 20.0.0.0/24 IP subnet. A Linux system running network management software is connected to node 20.0.0.120 through a copper UNI port. The administrator wishes to manage each of the systems in the ring using that network management system.

Let's examine how we would provision a node in this topology for MgmtVLAN service. Using node 20.0.0.120 as an example, we first start with the basic configuration that allows it to communicate with the other nodes on the S-VLAN in the ring. Then we cover how to allow the node to reach the Linux system via a UNI port.

### 10.2.1 Basic configuration

The following are the basic first steps to configure the service. Once the virtual switch is created, the user creates the MgmtVLAN service and assigns an S-VLAN to it:

```
BTI7000:sw1(config)# eservice mgmt type MGMTVLAN
SW 1: E-service: mgmt created.
BTI7000:sw1(config-eservice)# s-vlan 4000
```

The next step is to assign an IP address to the service. Note that unlike GCC links, which are unnumbered IP interfaces, the MgmtVLAN service is numbered, and thus a separate IP address and subnet mask must be assigned.

```
BTI7000:sw1(config-eservice)# ip 20.0.0.120/24
```

<b>Note</b>	This address/mask must be on a separate IP subnet from any other IP interfaces on the system.
-------------	---

Next, associate one or more NNI ports with the service. Assuming that the NNI ports have been created already, we first assign the NNI port for the link between 20.0.0.120 and 20.0.0.123:

```
BTI7000:sw1(config-eservice)# nni tenGigabit 1/1/1
```

Then, assign a LAG NNI that runs between 20.0.0.120 and 20.0.0.121:

```
BTI7000:sw1(config-eservice)# nni LAG 1
```

At this point, the system is accessible via the IP address 20.0.0.120 on S-VLAN 4000. The configuration on the other nodes in the system is similar. Once they are configured, you can then reach them using the ping command:

```
BTI7000:sw1# ping 20.0.0.122
Ping #1 from SCP-1-5 to 20.0.0.122: succeeded.
Ping #2 from SCP-1-5 to 20.0.0.122: succeeded.
Ping #3 from SCP-1-5 to 20.0.0.122: succeeded.
```

## 10.2.2 MgmtVLAN via UNI ports and C-VLANs

Further to the provisioning of the topology described in [10.2.1, “Basic configuration”](#), the node 20.0.0.120 must also be provisioned such that a Linux system attached on a UNI port can run network management software to manage the nodes in the ring. Configuring the service for C-VLAN and UNI access requires extra configuration on not just the node with the UNI port, but on the other nodes in the ring as well, depending on whether or not the C-VLAN is tagged or untagged.

### MgmtVLAN and tagged C-VLANs

To provision access via a C-tagged customer VLAN requires a few extra steps on the nodes to be managed. First, on node 20.0.0.120, we must first add the UNI to the MgmtVLAN service:

```
BTI7000:sw1(config-eservice)# uni gig 1/1/1
SW: 1, E-Service: mgmtvlan, UNI gig 1/1/1 created.
```

Then, as you would with an EVPLAN service, we configure a C-VLAN on the UNI we just attached to the service. Assuming the Linux system in the above topology is using C-VLAN 999:

```
BTI7000:sw1(config-eservice-uni)# c-vlan 999
```

This command creates a mapping from C-VLAN 999 to S-VLAN 4000 on that UNI, allowing c-tagged traffic arriving on that UNI to flow to S-VLAN 4000.

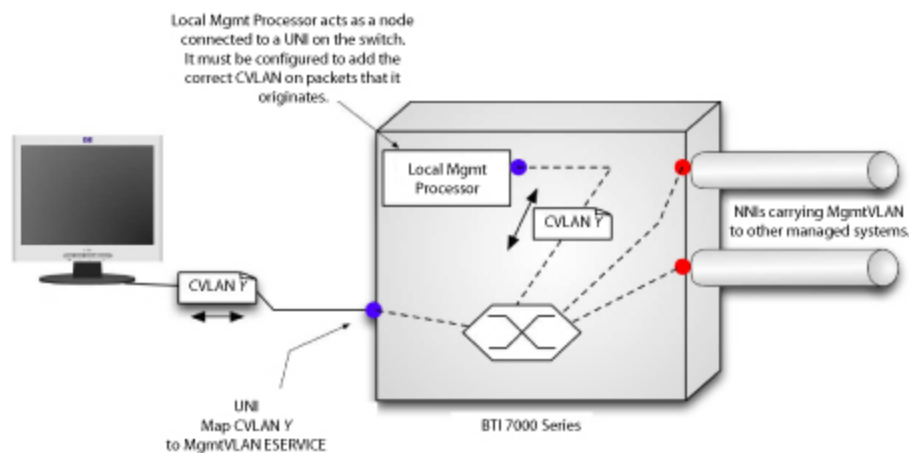
Next, we need to configure the C-VLAN ID for the service itself. This is done in the Eservice mode of the CLI:

```
BTI7000:sw1(config-eservice)# c-vlan 999
```

Configuring a C-VLAN at both the Eservice and eservice-uni mode is slightly perplexing, but makes sense with a bit of explanation. We need to instruct the service to C-tag packets that the node itself generates. With other Ethernet services, the packetVX does not C-tag packets. When Ethernet frames flow between a UNI port and a service, the system examines the C-tag on the incoming packets and using the configured C-VLAN mappings to bridge the frame onto the appropriate S-VLAN. No C-tags are added or removed from the frames themselves.

But consider the case above where we ping another node from the CLI. In that case, the packetVX itself is generating the packets, rather than bridging or routing them. If the destination of the ping packets is a node on a C-VLAN, those packets must be C-tagged, and since the packetVX is generating the packets, it is responsible for applying the C-tag itself before transmitting. The C-VLAN command in the CLI's Eservice mode instructs the MgmtVLAN service to apply a C-tag to outgoing IP packets using the specified C-VLAN ID in the tag.

The following figure shows a system with a UNI connection (blue dot on left) to a management station running on C-VLAN Y, and NNI ports (red dots) carrying the MgmtVLAN traffic to other managed systems in the topology. When the administrator on this system issues a ping request to the management station on the UNI, the local processor on the system has to apply a C-tag to the ping packet before transmitting so that the switch knows how to bridge the packet. Conceptually, the local processor on the MgmtVLAN has a UNI connection (blue dot) to the switch. Like any station on a UNI, it needs to C-tag the packet for the switch to be able to forward the packet. The C-VLAN command tells the local processor what C-VLAN ID to use (if any) when transmitting packets.



In summary, configuring the MgmtVLAN service for communicating with other nodes on a C-VLAN requires two steps:

- 1 Configure the C-VLAN (in this example, C-VLAN 999) for packets originating from the system node (the local processor blue dot in above diagram):

```
BTI7000:sw1(config-eservice)# c-vlan 999
```

**Note** This command should be run on all packetVX nodes that communicate with nodes on a C-tagged C-VLAN, even those with no UNI ports configured.

- 2 Configure the C-VLAN for UNI ports attached to the MgmtVLAN service (blue dot on left):

```
BTI7000:sw1(config-eservice)# uni gig 1/1/1
BTI7000:sw1(config-eservice-uni)# c-vlan 999
```

### **MgmtVLAN and untagged C-VLANs**

If the packetVX needs to communicate with a node on an untagged C-VLAN, the configuration procedure is again similar to that of an EVPLAN. In this situation, we set the MgmtVLAN service's C-VLAN parameter to 0, indicating that no C-tagging should be done for IP packets originating from this node.

- 1** Configure the MgmtVLAN service's c-vlan to 0:

```
BTI7000:sw1(config-eservice)# c-vlan 0
```

If any UNI ports are associated with the service, we still need to provision them for un-C-tagged traffic. This is done in the same way as with EVPLAN services: Select an unused C-VLAN number, associate it with the UNI port, then set the UNI port's C-PVID to that C-VLAN ID.

- 2** Configure any UNI ports associated with the service with an unused C-VLAN ID:

```
BTI7000:sw1(config-eservice)# uni gig 1/1/1
BTI7000:sw1(config-eservice-uni)# c-vlan 10
```

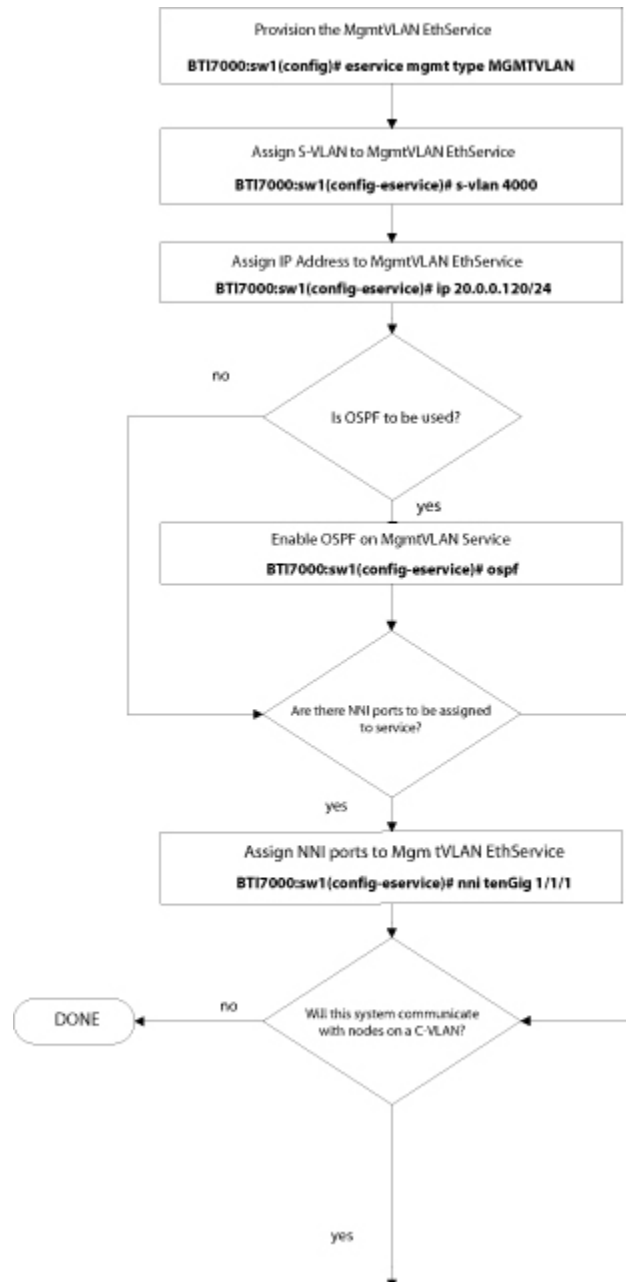
- 3** Configure the C-PVID on the UNI to the unused C-VLAN ID from Step 2.

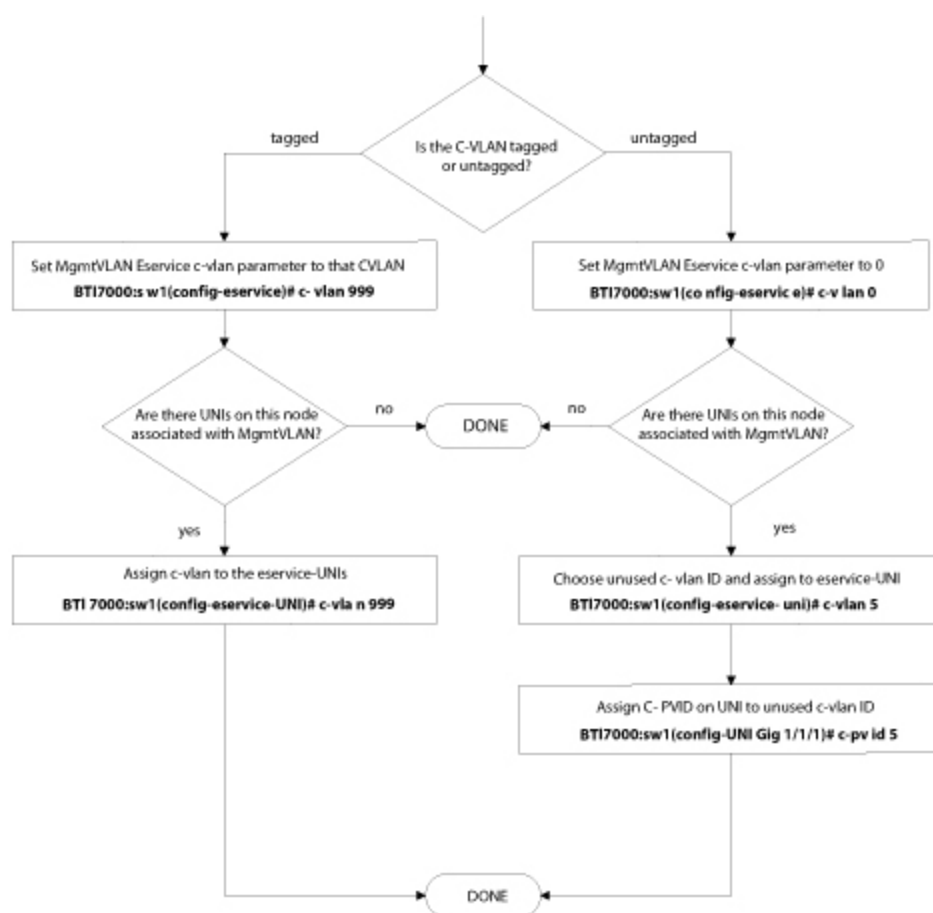
```
BTI7000:sw1(config)# uni gig 1/1/1
BTI7000:sw1(config-uni GigE 1/1/1)# c-pvid 10
```



## 10.3 Configuration flowchart

The following flowcharts show the step-by-step sequence of configuration steps for provisioning the MgmtVLAN service.

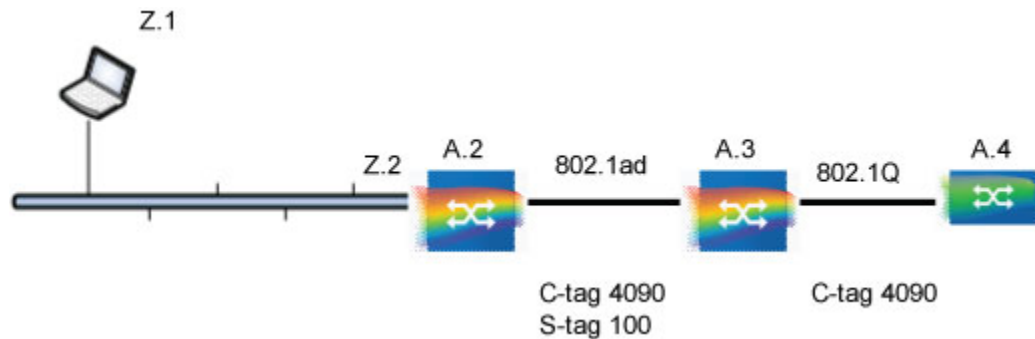




## 10.4 Provisioning Management VLANs

### 10.4.1 Configuring NMS Ethernet to Management VLAN

This procedure describes how to configure NMS Ethernet to Management VLAN, as shown in the following figure.



In this scenario, traffic received on the NMS port is routed across the Management VLAN. Two separate IP addresses are required in this example: one for the NMS port and one for the Management VLAN. These addresses must be on separate IP subnetworks. The IP address 10.128.3.9/8 is assigned to the NMS port while the address 192.168.1.9/24 is assigned to the Management VLAN service.

#### Step 1 Provision the management interface port

To provision the management interface port, enter the following command:

```
BTI7000(config)# interface mgmteth
```

#### Step 2 Configure the interface IP address and netmask

To configure the interface IP address and netmask, enter the following command:

```
BTI7000(config-if MgmtEth)# ip 10.128.3.9/8
```

#### Step 3 Exit configuration mode

To exit, enter the following command syntax:

```
BTI7000(config-if MgmtEth)# exit
```

#### Step 4 Set system level parameters

To set system level parameters, enter the following command:

```
BTI7000(config)# system
BTI7000(config-sys)# gate 10.128.1.1
```

#### Step 5 Exit system mode

To exit enter the following command:

```
BTI7000(config-sys)# exit
```

**Step 6 Specify the virtual switch.**

```
BTI7000(config)# virtual-switch 1
```

**Step 7 Create NNI TenGigE 1/1/2.**

To create NNI TenGigE 1/1/2, enter the following command:

```
BTI7000:sw1(config)# nni ten 1/1/2
```

**Step 8 Exit configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-nni TenGigE 1/1/~)# exit
```

**Step 9 Create the management VLAN Eservice**

To create the management VLAN, enter the following command:

```
BTI7000:sw1(config)# eservice mgmtvlan type MGMTVLAN
```

**Step 10 Assign the VLAN ID and IP address to the management VLAN service and associate an NNI with it.**

Enter the following commands:

```
BTI7000:sw1(config-eservice)# s-vlan 100
```

```
BTI7000:sw1(config-eservice)# ip 192.168.1.9/24
```

```
BTI7000:sw1(config-eservice)# nni ten 1/1/2
```

**Step 11 Exit configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-nni-eservice)# exit
```

**Step 12 Associate a CVLAN with the service if required**

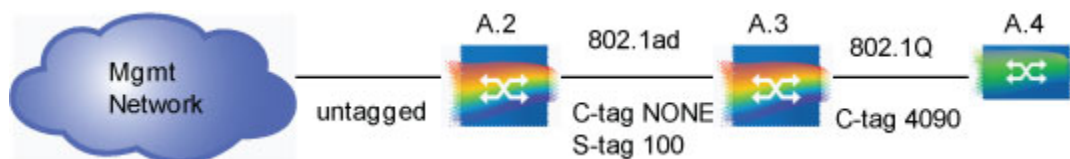
If a C-tag is required for the management VLAN (for example to reach the A.4 device in the diagram), specify the desired C-VLAN ID by entering the following command for the eservice on the A.2 and A.3 NEs:

```
BTI7000:sw1(config-eservice)# c-vlan 4090
```

You have successfully completed this procedure.

## 10.4.2 Configuring Untagged to Tagged Management VLAN

This procedure describes how to configure an untagged to a tagged Management VLAN, as shown in the following figure.



In this scenario, a user on a UNI port is managing nodes in the provider network. Traffic arrives at the UNI UNTAGGED and is carried over the S-VLAN assigned to the Management VLAN service. On node A.2, the provisioning is the same as in the UNI to NNI Management VLAN scenario, except that no C-VLAN is associated with the service.

**Step 1 Create NNI TenGigE 1/1/2**

To create NNI TenGigE 1/1/2, enter the following command syntax:

```
BTI7000:sw1(config)# nni ten 1/1/2
```

**Step 2 Exit configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-nni TenGigE 1/1/~)# exit
```

**Step 3 Create UNI GigE 1/1/3**

To create the UNI GigE 1/1/3, enter the following command:

```
BTI7000:sw1(config)# uni gig 1/1/3
```

```
BTI7000:sw1(config)# c-pvid 100
```

**Note** The value of c-vlan-id parameter must match the value of the vlan-id parameter specified for the C-VLAN specified in step 6.

**Step 4 Exit configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-uni GigE 1/1/3)# exit
```

**Step 5 Create the management VLAN Eservice**

To create the management VLAN, enter the following command:

```
BTI7000:sw1(config)# eservice mgmtvlan type MGMTVLAN
```

**Step 6 Assign the VLAN ID and IP address to the management VLAN and associate an NNI with it**

Enter the following command:

```
BTI7000:sw1(config-eservice)# s-vlan 100
```

```
BTI7000:sw1(config-eservice)# c-vlan 100
```

```
BTI7000:sw1(config-eservice)# ip 192.168.1.9/24
```

```
BTI7000:sw1(config-eservice)# nni ten 1/1/2
```

**Step 7 Exit configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-nni-eservice)# exit
```

**Step 8 Add the UNI**

Enter the following command:

```
BTI7000:sw1(config-eservice)# uni GigE 1/1/3
```

### Step 9 Exit configuration mode

To exit, enter the following command:

```
BTI7000:sw1(config-uni-eservice)# exit
```

### Step 10 Associate a UNI with the management VLAN Eservice

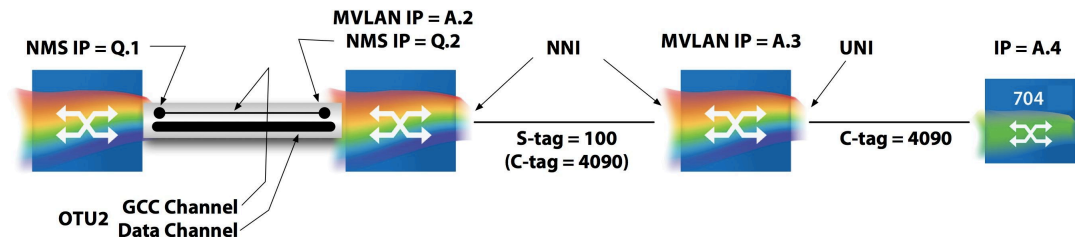
Enter the following command:

```
BTI7000:sw1(config-eservice)# uni gig 1/1/3
```

You have successfully completed this procedure.

## 10.4.3 Configuring GCC to Management VLAN Routing

This procedure describes how to configure GCC to Management VLAN routing, as shown in the following figure.



In this scenario, traffic from a GCC link is routed across the Management VLAN with an ultimate destination of a node on a customer VLAN on node A.2. The GCC link is provisioned on interface tenGig 1/1/1 and routed over an NNI on port tenGig 1/1/2 which is part of the Management VLAN service.

### Step 1 Create interface GCC TenGigE 1/1/1

To create the interface, enter the following command:

```
BTI7000:sw1(config)# interface ten 1/1/1
BTI7000:sw1(config-if TenGigE 1/1/1)# shut
BTI7000:sw1(config-if TenGigE 1/1/1)# line-mapping otu2-gfp1
BTI7000:sw1(config-if TenGigE 1/1/1)# no shut
BTI7000:sw1(config-if TenGigE 1/1/1)# exit
BTI7000:sw1(config)# int gcc ten 1/1/1
```

### Step 2 Exit configuration mode

To exit, enter the following command:

```
BTI7000:sw1(config-gcc TenGigE 1/1/1)# exit
```

### Step 3 Create NNI TenGigE 1/1/2

To create the NNI Ten GigE 1/1/2, enter the following command:

```
BTI7000:sw1(config)# nni ten 1/1/2
```

**Step 4 Exit configuration mode**

To exit, enter the following command:

```
BTI7000:sw1(config-nyi ten 1/1~)# exit
```

**Step 5 Create the management VLAN Eservice**

To create the management VLAN, enter the following command:

```
BTI7000:sw1(config)# eservice mgmtvlan type MGMTVLAN
```

**Step 6 Assign the VLAN ID and IP address to the management VLAN service and associate an NNI with it**

To create the NNI TenGigE 1/1/2, enter the following command:

```
BTI7000:sw1(config-eservice)# s-vlan 100
```

```
BTI7000:sw1(config-eservice)# ip 192.168.1.9/24
```

```
BTI7000:sw1(config-eservice)# nni ten 1/1/2
```

You have successfully completed this procedure.





## 11.0 Configuring Ethernet Ring Protection Switching (ERPS)

---

Chapter 5, “[Configuring Ethernet Bridging and STP](#)” described the operation of the Spanning Tree Protocol (STP) and its variants. Spanning Tree is a general topology maintenance protocol that works in any network topology and is (initially) completely plug and play — you can connect a number of Ethernet bridges together and power them on and spanning tree will automatically ensure a loop-free topology without any configuration or intervention.

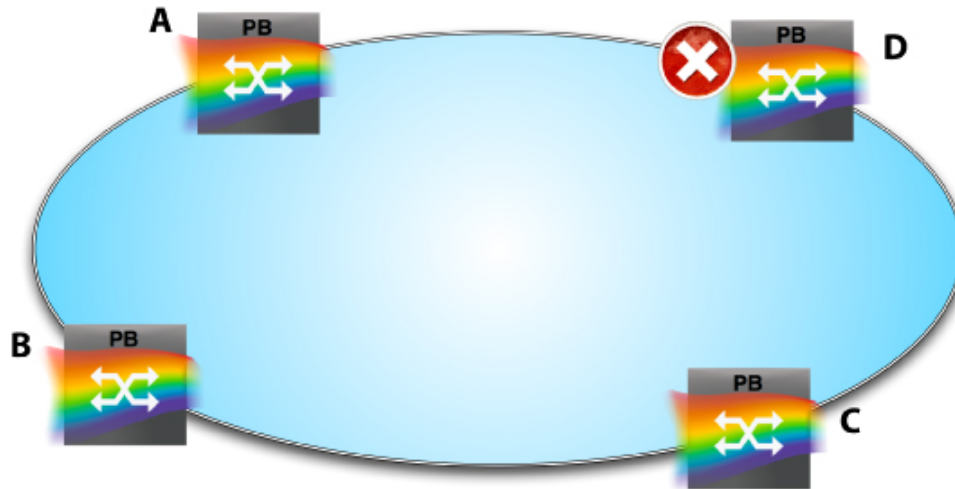
As noted in that chapter, the cost of this generality is convergence time. Although with rapid spanning tree (RSTP) it is possible to achieve sub-second re-convergence after a network failure, getting very low convergence time (e.g., in the 50ms range) is rare and highly dependent on the situation; for example, where the failure is with respect to the root of the tree.

Ethernet Ring Protection as documented in ITU standard G.8032 provides an alternative to spanning tree that can provide very fast (sub 50ms) convergence<sup>35</sup>. To achieve this, however, G. 8032 pared back on the generality of STP in two ways: (1) it does not work in an arbitrary topology, just in a ring and (2) it is not plug and play, it requires configuration. In return for these restrictions, ERPS provides sub-50ms protection switching. In addition, ERPS allows configuration of non-revertive protection switching, which STP does not.

Several concepts in G.8032 are the same as spanning tree. Consider the following diagram of a simple four-node ring.

---

<sup>35</sup> G.8032 sets these conditions for convergence time: “In an Ethernet Ring, without congestion, with all Ethernet Ring Nodes in the idle state (i.e., no detected failure, no active automatic or external command, and receiving only 'NR, RB' R-APS messages), with less than 1200 km of ring fibre circumference, and fewer than 16 Ethernet Ring Nodes, the switch completion time (transfer time as defined in [ITU-T G.808.1]) for a failure on a ring link shall be less than 50 ms.”

**Figure 11-1 Simple four-node ring**

To break the loop, spanning tree would put one of the links (in this case the left link on node **D**) into a blocking state. If a link failure is detected on any other link, the blocking port will resume a forwarding role to heal the ring (this is what we mean by re-convergence and re-convergence time, above).

In a topology like this, there really are no other ways to achieve a loop-free forwarding topology, so ERPS will result in exactly the same situation—one port on the ring in blocking state but ready to come back into forwarding if a failure occurs. The mechanism for achieving this result is different, however.

This section covers the following topics:

- 11.1, “G.8032 operation”
- 11.2, “Failure detection”
- 11.3, “ERPS Model in the packetVX”
- 11.4, “Basic ERPS configuration”
- 11.5, “Revertive vs. Non-Revertive operation”
- 11.6, “packetVX, BTI 700 Series, and BTI Service Access 800 Series on ERPS rings”
- 11.7, “ERPS and Spanning Tree”
- 11.8, “Multiple rings”
- 11.9, “Administrative control of protection switching”
- 11.10, “ERPS provisioning”
- 11.11, “Replacing a packetVX in an ERPS network: non-interconnected nodes”
- 11.12, “Removing a packetVX in an ERPS network: non-interconnected nodes”
- 11.13, “Adding a packetVX in an ERPS network: non-interconnected nodes”

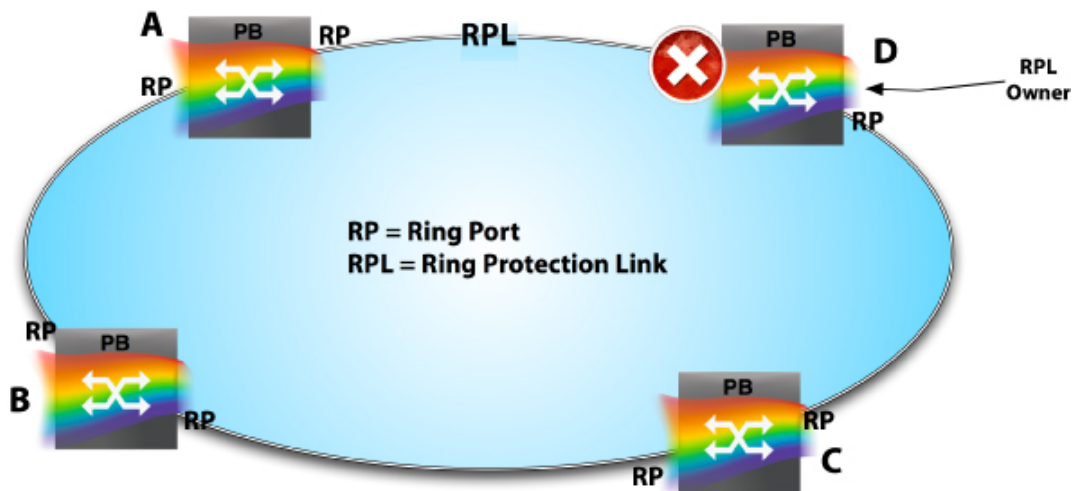
For more information about implementing ERPS, contact BTI for a copy of *packetVX™ Ethernet Ring Protection Switching (G.8032) Implementation and Migration MOP (Method of Procedure)*.

## 11.1 G.8032 operation

In spanning tree, the root is the important node from a configuration point of view. With ERPS, one of the links in the ring is called the Ring Protection Link (RPL) and one of the two switches that connect to the RPL is called the *RPL Owner*.

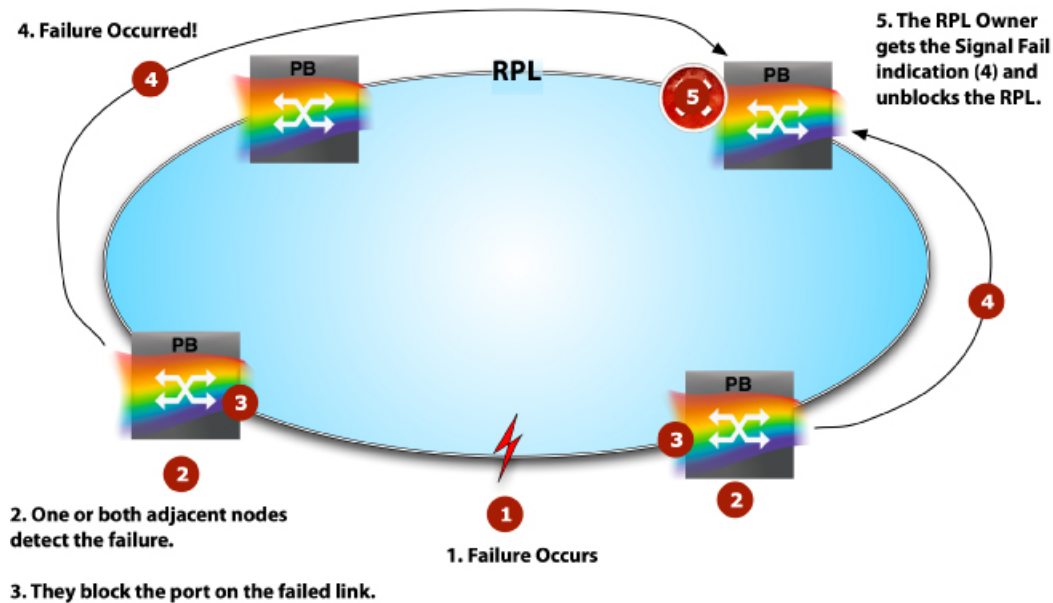
In normal ring operation, the RPL Owner blocks its port on the ring<sup>36</sup> and sends R-APS (ring automatic protection switch) messages around the ring, with an indication that the RPL is blocked (RB). These are forwarded around the ring.

Figure 11-2 ERPS Normal Ring



If any node detects a link failure, it blocks the failed port (to avoid a transient loop if it comes back quickly) and sends a SF (signal failure) message around the ring. When the RPL Owner sees the failure indication, it immediately unblocks the RPL and the ring is restored.

<sup>36</sup> This is a difference between the concepts of spanning tree root and ERPS RPL Owner. With STP the blocking port ends up as far from the root as possible and in ERPS the blocking port is on the RPL Owner.

**Figure 11-3 ERPS Failure Sequence**

When the failure is repaired, the nodes adjacent to the failure stop sending the SF messages around the ring. Instead, they start sending No Request (NR) messages around the ring. When the RPL Owner sees this, it starts a Wait to Restore timer (if the ring is configured for Revertive operation). Upon expiry of that timer, it blocks its RPL port and sends the RB indication around the ring. Upon receipt of a R-APS message with an RB, any node that has a blocked port unblocks it and normal operation is once again achieved.

## 11.2 Failure detection

---

Fast protection switching relies on fast failure detection. Regardless of the protection mechanism, a protection switch/re-convergence cannot begin until the fault is detected. For a 50ms recovery, it is generally accepted that failure detection has to occur within 10ms of failure.

The packetVX uses two methods for detecting failure:

- PVX checks the state of each link every few milliseconds. This is called linkscan. Linkscan is performed automatically and is not configurable, and produces the quickest detection of link failure.
- If Y.1731 link-level Connectivity Check Messages (CCMs ) are enabled, PVX can also declare a failure when 3 consecutive link-level CCMs are lost. In general, this does not occur because a link failure will already have been declared before even the first CCM is lost.

## 11.3 ERPS Model in the packetVX

On the packetVX, ERPS is configured as an Eservice. Following are the characteristics of the ERPS service:

- 1 The ERPS service has an S-VLAN like all other Eservices. The S-VLAN is used to carry the R-APS messages for the ring.
- 2 Unlike other Eservices, the ERPS service is not automatically enabled. You must enable ERPS services by setting the administrative state to enable.
- 3 At least one NNI port must be defined for the ERPS service. One NNI port is required for an interconnect node of a ladder ring, and two are required for a non-interconnect node. (Refer to 11.8.2, “Ladder rings” for information about ladder ring configurations.)
- 4 One NNI on each ring must be configured as the RPL Owner.<sup>37</sup>
- 5 If CCM is enabled on the NNI, then the NNI must have a unique ME-NAME defined:
  - ME-NAMEs cannot be the same on a main ring and a sub-ring on the same node.
  - ME-NAMEs can be duplicated on links in a ring, if they are on different nodes.

**Note** It is not necessary to enable CCM for an ERPS service. However, the CCM setting must be consistent between interconnected NNIs. You cannot have CCM enabled on the NNI at one side of the link and disabled on the NNI at the other side of the link.

- 6 To avoid a loop when provisioning an ERPS ring, disable the NNI selected as the RPL on each ring, until ERPS is configured completely and each service has been enabled.
- 7 Up to 16 ERPS services can be configured on a packetVX.
- 8 The Wait-to-Restore timer can be set to short, which is 20 seconds. This causes the ring to return to idle faster after recovery from failure.
- 9 The Wait-to-Block timer is used when a force or manual switch is configured on the ring. This timer configures the duration of time to wait before clearing the manual or forced switch.

**Note** Before creating an ERPS Eservice, all Eservices on the Virtual-Switch that are on an MSTI (Instances 1-16) must be returned to the CIST (Instance 0).

### BTI ERPS feature matrix

The following table outlines the ERPS support in BTI software releases:

**Table 11-1 ERPS supported feature matrix**

ERPS Feature	System Software Introduced	
	Pre-release 10.2	Release 10.2
R-APS Message	ERPS V1	ERPS V1 or V2 (default)

<sup>37</sup> A strict reading of the standard would have a node as the RPL Owner rather than a port, and the RPL Owner's port on the RPL is blocked. Making this an attribute of the port simplifies configuration when multiple ERPS services are provisioned on a node.

**Table 11-1 ERPS supported feature matrix (Continued)**

ERPS Feature	System Software Introduced	
	Pre-release 10.2	Release 10.2
Ladder Rings	Not supported	ERPS V2 mode supported for non-virtual channels
Ring Recovery	Revertive	Revertive
Switch Commands	Forced, Manual, Normal	Manual, Forced, Clear
MEG Level	Supported (MEG level 6, not configurable)	Supported (configurable) <sup>1</sup>
Wait-to-block Timer	Not supported	Supported

<sup>1</sup>In release 10.2, MEG levels 1 through 6 are supported. In release 11.2, MEG levels 1 through 3, and 5 through 6 are supported. MEG level 4 is reserved for service level CCMs. In release 12.2, MEG levels 0, 1, 5, and 6 are supported. The other levels are reserved for service level CCMs.

### 11.3.1 Migrating from ERPS Version 1 to Version 2

This section outlines what you need to do to migrate ERPS services to ERPS Version 2 for a multiple ring environment:

- The node must be upgraded to BTI software release 10.x.
- The ERPS services need to be re-provisioned:
  - 1 To prevent loops, manually block all RPLs using the command **admin-state disable** or **shutdown**.
  - 2 On each ring, one at a time:
    - 1 Delete the ERPS service across all the nodes of the particular ring.
- a) Delete one ring at a time.
- b)
  - 2 Re-provision ERPS across all the nodes of the particular ring. By default, the new ERPS service uses ERPS V2.
  - 3 Enable the blocked RPLs.
- 3 Go to the next ring, and repeat the procedure.

**Note** A single NE can have co-existing ERPS versions, since each ring is independent.

## 11.4 Basic ERPS configuration

---

This section explains the configuration of the basic four-node ring shown in [Figure 11-2 on page 11-3](#). If we assume that the ring ports are the same on each node, say tenG 1/1 and tenG 1/1/2, each node would be configured as follows:

```
> ESERVICE ring1 TYPE erps
> S-VLAN 77
> NNI tenG 1/1/1
> ME-NAME LINKAB39
> CCM ENABLE40
> EXIT
> NNI tenG 1/1/2
> ME-NAME LINKAD
> CCM ENABLE
> EXIT
> ADMIN-STATE ENABLE
>EXIT
```

To create the RPL owner:

```
> ESERVICE ring1
> NNI tenG 1/1/1
> RING-PROTECT-LINK ENABLE
> EXIT
> EXIT
```

The ERPS state machine initially puts the NNI port with the highest MAC address in blocking state. This port remains in this state temporarily until the RPL owner blocks the RPL port, at which time the initially-blocked port becomes unblocked.

<sup>39</sup> Each ring segment must have a different ME-NAME, and both sides of the segment should agree on the name. In this network, we can have ME-NAMEs LINKAB, LINKBC, LINKCD, and the RPL is LINKAD. ME-NAME is between 1 and 6 characters long, and is only required if CCMs are enabled.

<sup>40</sup> This is optional. By default, CCM is disabled.



## 11.5 Revertive vs. Non-Revertive operation

**Note** Only Revertive mode is supported in the current release.

When provisioning ERPS, the default recovery mode is Revertive. In many networks, it may be desirable to choose the RPL Owner in order to optimize the path for traffic around the ring. This provides the best use of the available bandwidth while the ring is in an idle state. The revertive recovery mode is used to restore the optimal path for traffic after a failure has been rectified. To note, there will be a traffic disruption for some services (<50ms) on both the failure and the recovery. The revertive recovery mode uses the Wait-to-Restore Timer to determine when to block the RPL after the failure has been corrected. The Wait-to-Restore Timer defaults to 5 minutes but can be set as high as 15 minutes.

```
> ESERVICE ring1 type erps
> S-VLAN 77
> RECOVERY revertive
> WAIT-TO-RESTORE 7
> ...
```

**Note** The wait-to-restore is set on the RPL owner while the recovery mode is set on all nodes in the ring.

The blocked port can be reset back to the Ring Protection Link by operating a protection-switch clear on the RPL owner.

```
> ESERVICE ring 1
> protection-switch-mode clear
> ...
```

## 11.6 packetVX, BTI 700 Series, and BTI Service Access 800 Series on ERPS rings

---

The ERPS implementation on the packetVX can interwork with the following network elements:

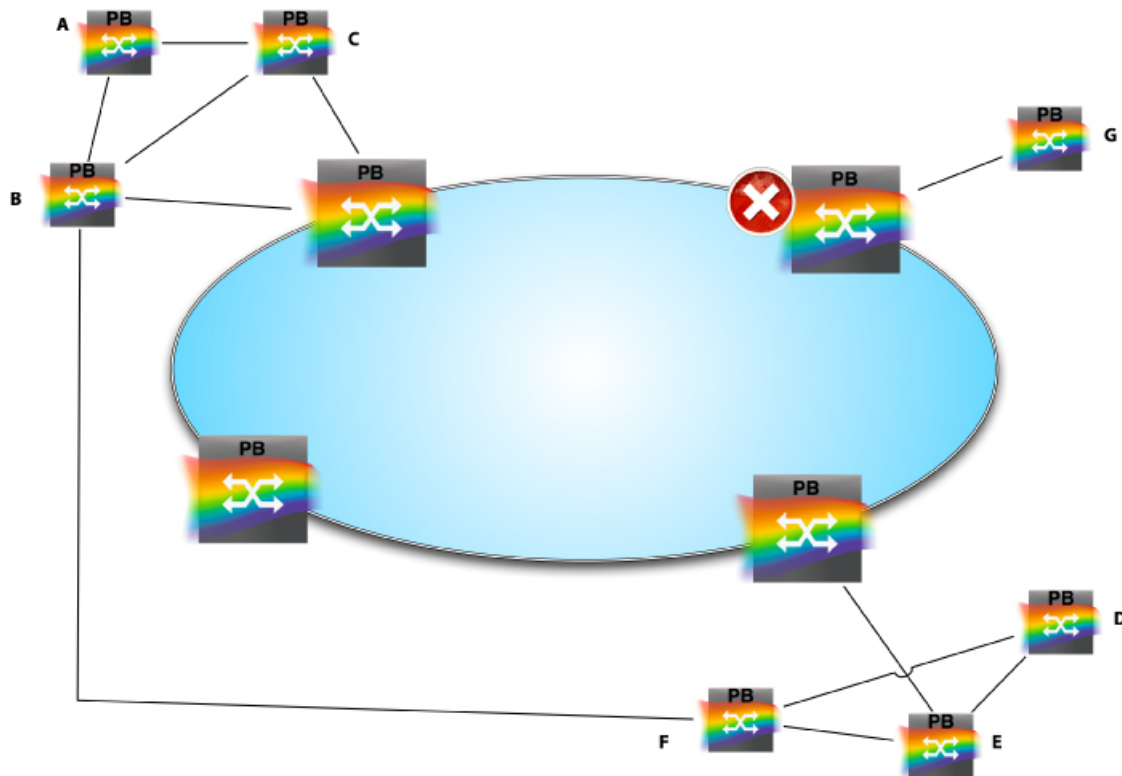
- BTI 700 Series (BTI 704, BTI 712, BTI 718) - release 1.4 and later (ERPSv1)
- BTI 700 Series (BTI 718E) - release 2.0 and later (ERPSv2)
- BTI Service Access 800 Series - release 1.1 and later (ERPSv2)

The packetVX, BTI 700 Series, and BTI Service Access 800 Series network elements can coexist on the same ring. Any device can be the RPL owner, and any device can act as the interconnection node on interconnected rings.

## 11.7 ERPS and Spanning Tree

Many networks have a core ring with many smaller networks attached to the core. It may be desirable to convert the core ring to use ERPS, but the attached networks may not be amenable to using ERPS (for example, they may be mesh networks). In addition, it is important to protect against loops that can be caused due to interconnection of two or more of these external networks. Consider the network in the following figure:

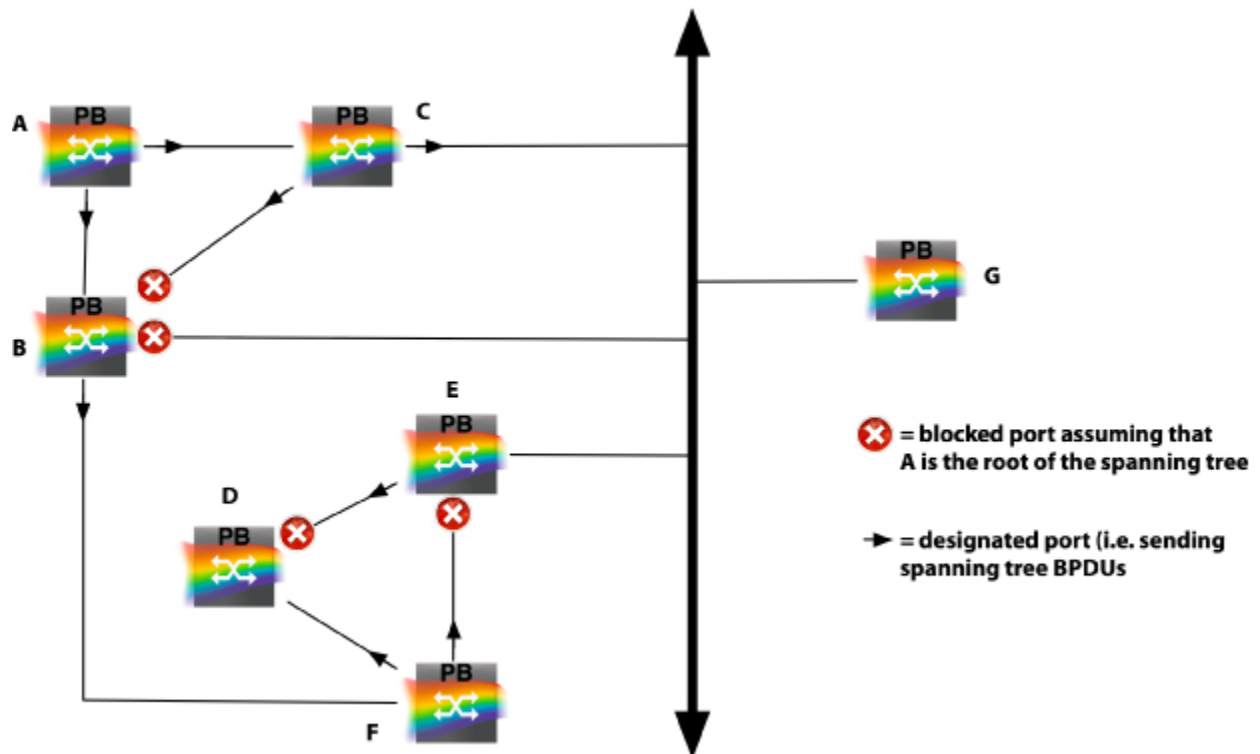
**Figure 11-4 ERPS ring with external Spanning Tree attachments**



This network shows both these scenarios. There are two attached networks that have relatively complex topologies (upper left and lower right), and these two networks are also connected together externally.

The packetVX supports these network configurations by disabling spanning tree processing on all ERPS NEs and acting as a multiport repeater for spanning tree messages. In other words, a Spanning Tree Bridge Protocol Data Unit (BPDU)<sup>41</sup> that enters any NNI on an ERPS NE will be forwarded unmodified to all other NNIs on the NE. This makes the ERPS ring look like a single shared LAN in the spanning-tree topology. The resulting spanning-tree topology is shown in the following figure:

<sup>41</sup> Only Provider Bridge Spanning Tree BPDUs are recognized in this context.

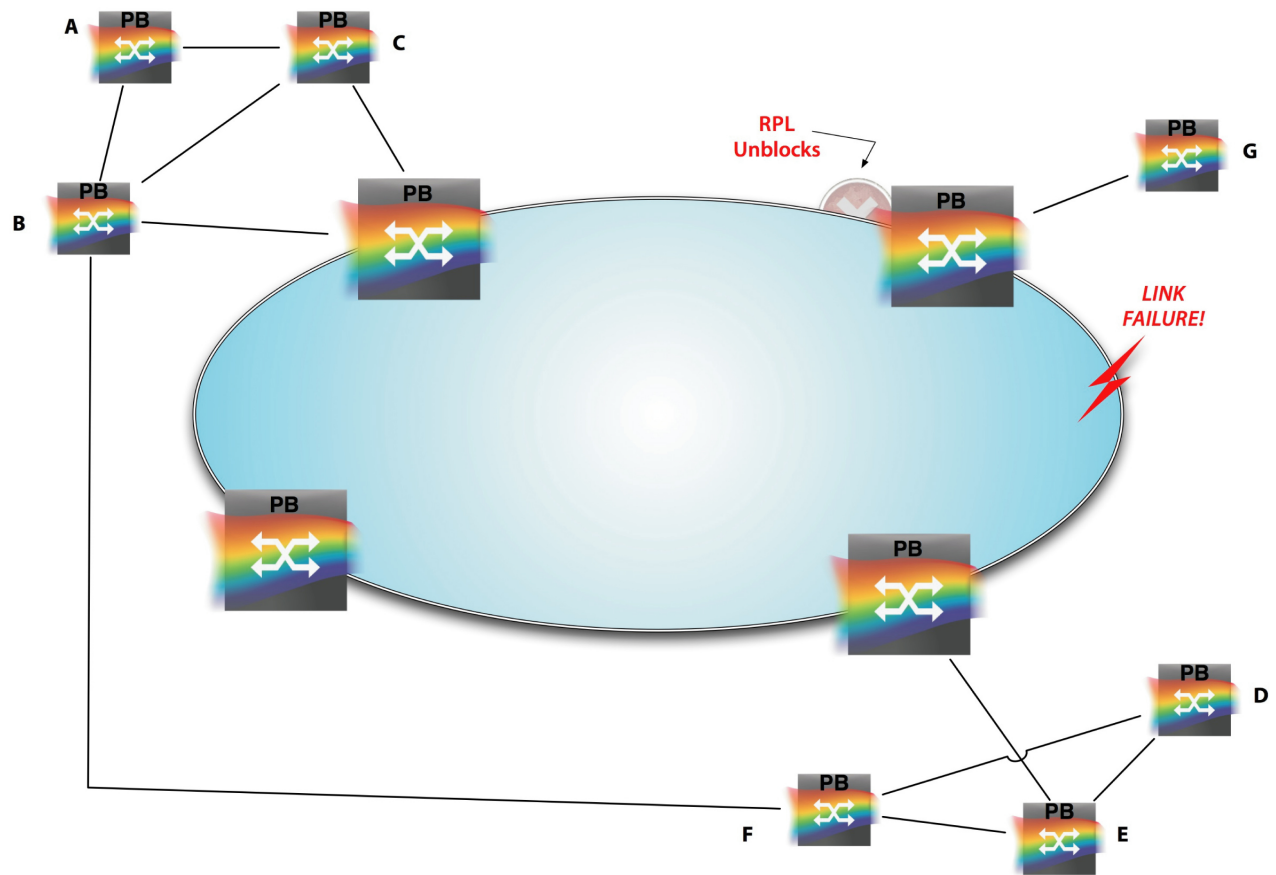
**Figure 11-5 Equivalent spanning-tree topology**

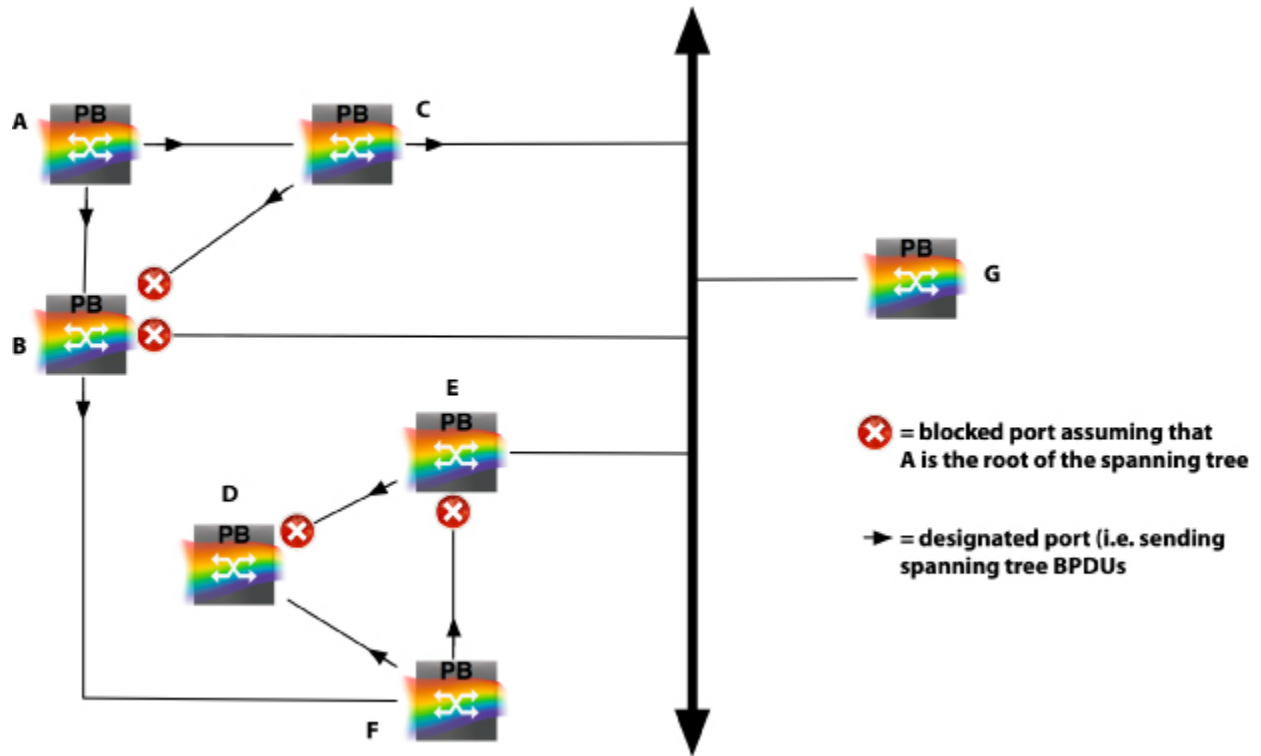
Note that the ERPS NEs do not appear in the topology at all. They are represented by the shared Ethernet LAN. NEs C, B, G, and E are all adjacent on this LAN (they look like they are connected together). With spanning tree, each LAN, whether point-to-point or shared, has exactly one bridge sending BPDUs, that is, the designated bridge. This is shown by the arrows in the figure.

One important side effect of this topology involves rapid reconfiguration (that is, Rapid Spanning Tree Protocol (RSTP)). Several rapid reconfiguration optimizations that were introduced in RSTP (and carried into Multiple Spanning Tree Protocol (MSTP)) were based on point-to-point LANs. If a bridge knows that there is only one other device on the LAN, it can make decisions much more quickly. For example, once it gets a response from its peer, it doesn't have to wait to see if there are any laggards on the connection. Since the ERPS ring appears as a shared LAN, these optimizations are not used and many reconfigurations in this network will not converge in the sub-second time expected with RSTP in pure point-to-point networks.

There is a failure scenario in which full forwarding is not restored quickly when tunneling MSTP. The problem occurs only where there is a double fault on the ring, and is a result of the different recovery procedures designed into the two protocols. Consider the network described above with a failure on the ERPS ring.

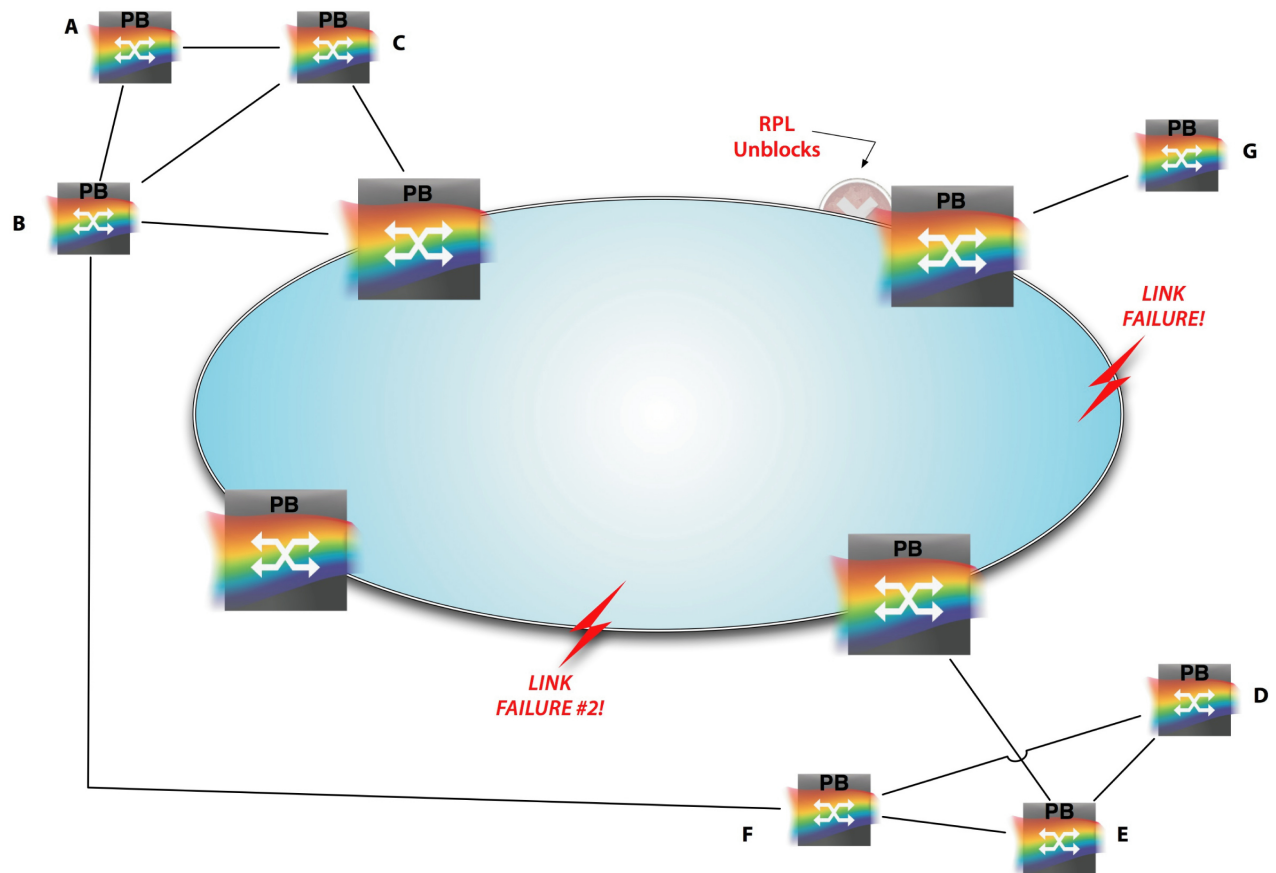
Figure 11-6 Single failure on ERPS ring

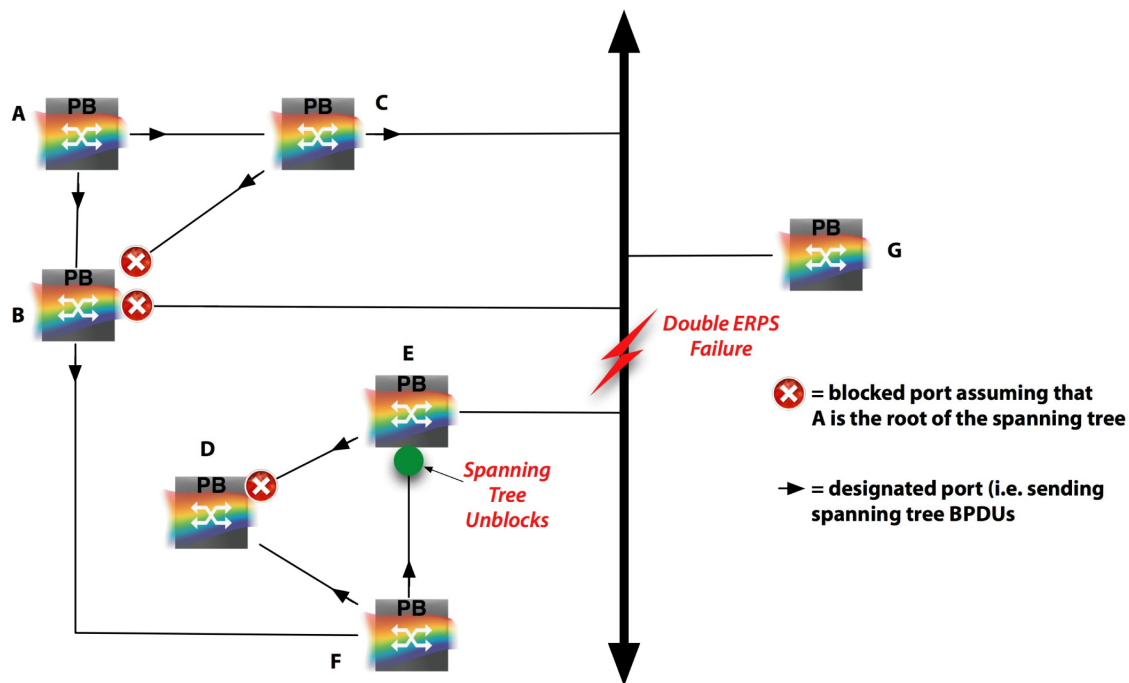


**Figure 11-7 Single failure on ERPS ring equivalent spanning-tree topology**

With a single failure on the ERPS ring the ring will recover quickly (by unblocking the Ring Protection Link (RPL)). The spanning tree topology will not even detect the failure. However, with two failures on the ring, the spanning tree will reconfigure.

### Figure 11-8 Double failure on ERPS ring



**Figure 11-9 Double failure on ERPS ring equivalent spanning-tree topology**

In this case, the ERPS NE that is providing connectivity for the **D-E-F** subnet (specifically to **E**) is isolated on the ring and can no longer provide transit between the two external subnets. The link between **E** and **F** unblocks and connectivity is restored.

The problem occurs when the faults recover on the ERPS ring. For example, when fault number **2** is repaired, the network reverts back to the configuration shown in [Figure 11-6](#) and [Figure 11-7](#). The RPL stays unblocked since there is still a ring failure, and BPDUs starting at the root (**A**) are again carried over the ring to **E** which causes the **E-F** link to block again. The problem is that addresses are not learned in the right place on the ERPS ring. ERPS NEs do not flush their address databases until the ring is fully restored. So when **E** sends a packet to **C** (or other NEs in the other subnet) it sends it through the ERPS ring. But the ERPS NE connected to **E** might very well have last seen packets from **C** coming from **E** (during the double failure) and does not forward it around the ring.

**Note** In this scenario, there is a partial lack of connectivity which continues until addresses age out of the database on the ERPS NE (5 minutes from the last time each address was seen).



## 11.8 Multiple rings

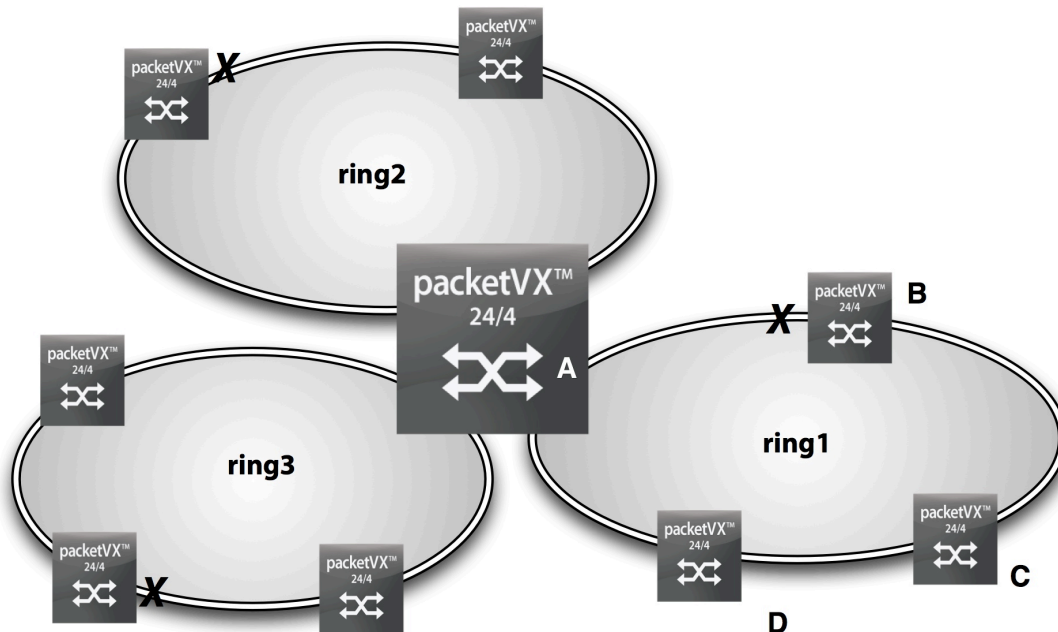
There are two types of multiring configurations to consider: independent rings and ladder rings.

### 11.8.1 Independent rings

#### Independent rings

Multiple independent rings flow through a single packetVX module, but, do not have any links in common. Independent rings are configured as separate ERPS services with the basic configuration; no additional configuration is required. A multiple independent ring configuration is displayed in the following figure:

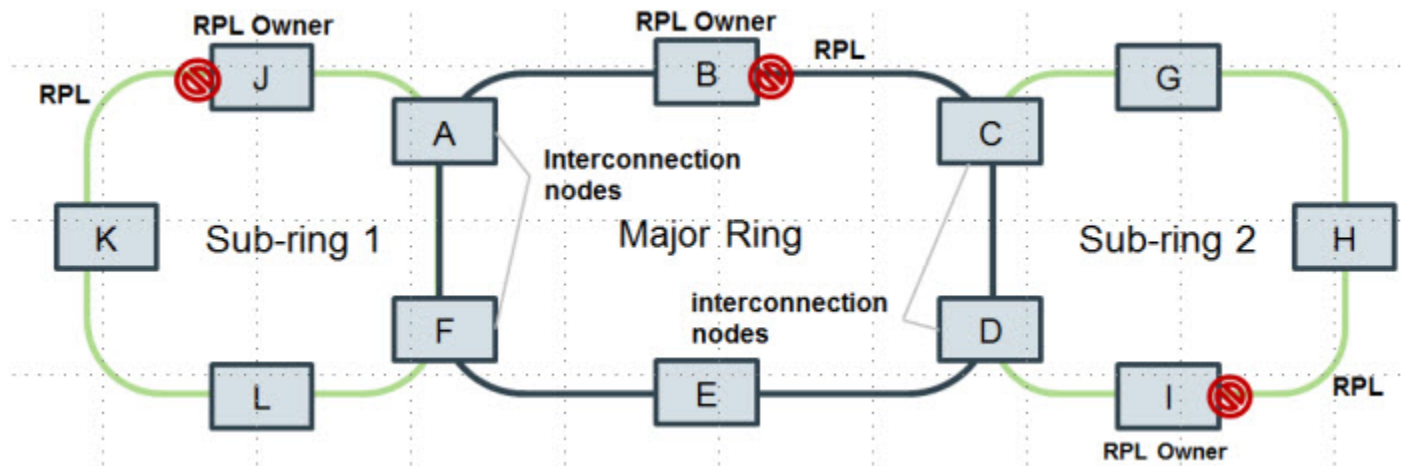
**Figure 11-10 Multiple Independent Rings**



This figure shows three rings traversing the node in the center. Since the rings are non-overlapping, they are configured as three separate and independent ERPS services. Each service has a different name, a different S-VLAN, its own RPL and RPL owner, and different NNIs.

### 11.8.2 Ladder rings

Ladder rings are interconnected rings joined by two interconnection nodes, as shown in the following example:

**Figure 11-11 Ladder Ring Network**

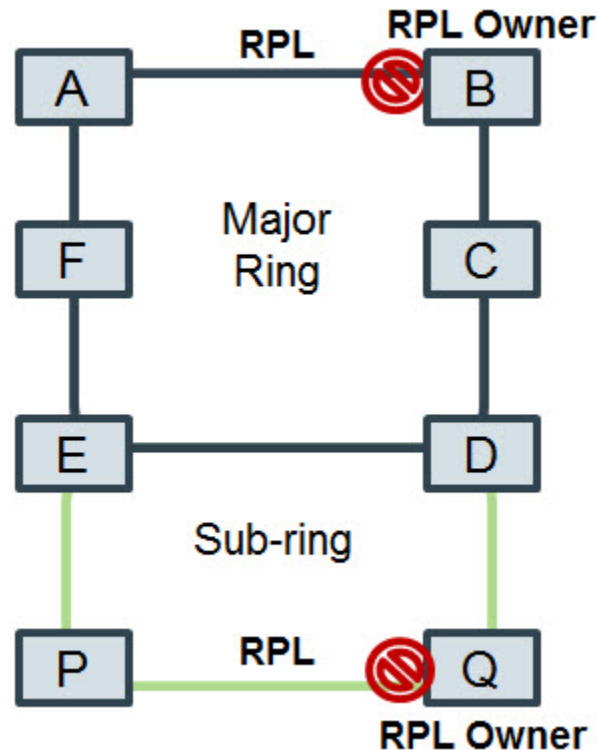
- The major ring is connected to an interconnection node through two ports.
- A sub-ring is an Ethernet ring that uses another ring to close one of its paths. For example, there are two nodes on the sub-ring that are logically adjacent, however, they use another ring to connect with each other.

### 11.8.2.1 Ladder rings without R-APS virtual channel

Interconnected rings without a virtual channel do not rely on the major ring to provide services for the interconnected rings:

- The sub-ring R-APS channel is terminated at the interconnected nodes, and its R-APS messages are not tunnelled between the interconnected nodes. R-APS messages are transmitted only to the sub-ring port.
- The sub-ring RPL only blocks the data channel not the R-APS channel. The R-APS channel is never blocked on any of its sub-ring nodes.
- If there is a link failure of any ring link of the sub-ring, the R-APS channel of the sub-ring may be segmented, preventing R-APS message exchange between some of the sub-ring's nodes.

Following is an example of a sub-ring without an R-APS virtual channel:

**Figure 11-12 Sub-ring without R-APS virtual channel****Key functionalities**

The key functionalities of no virtual channels are:

- No VC increases scalability for complex topologies:
  - Each ring is a completely independent
  - Adding additional sub-rings, or sub-ring to sub-ring, does not have an impact to the overall complexity of the network.
- No VC reduces provisioning and planning complexities.

**11.8.2.2 Ladder ring interoperability with the BTI 700 Series**

To interoperate ladder ring configurations with the BTI 700 Series Releases 1.4., 1.4.1, and 1.5, and 2.0, follow these guidelines:

- You must set the Ring IDs on the BTI 700 Series NEs to 1.
- If you are running in ERPS V1 mode, then you must set the MEG level on the BTI 700 Series NEs to 6 and the MEG Name to `DERPS`.
- If you are running in ERPS V2 mode, then you must set the MEG level on the BTI 700 Series NEs to 0 and the MEG NAME to `BTI-L0`.
- Up to eight ERPS services are supported.

- ME-NAMES must be unique on all links on a node:
  - ME-NAMES cannot be the same on a main ring and a sub-ring on the same node.
  - ME-NAMES can be duplicated on links in a ring, if they are on different nodes.

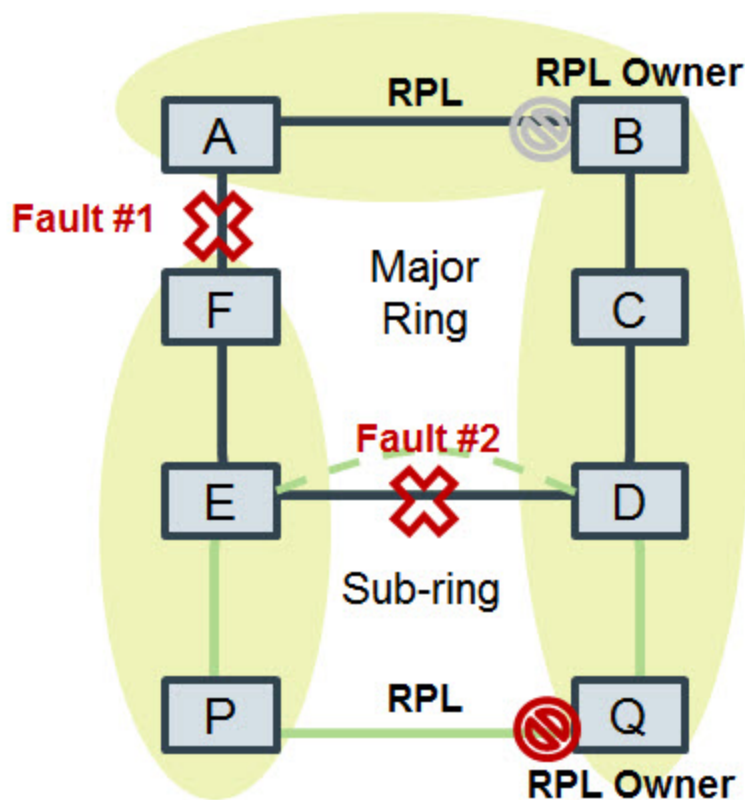
### 11.8.3 Managing segmentation between interconnected nodes

In a multiple ring network, protection switching occurs within only the local ring. A network with interconnected nodes experiences segmentation when double faults occur on interconnected nodes.

The following is an example of a double fault on interconnected nodes. In this scenario the faults occur only in the major ring:

- The major and sub rings are segmented.
- Nodes F, E and P are blocked at node Q and isolated from nodes A, B, C, D, and Q.
- Traffic can continue to pass through nodes A, B, C, and D.

**Figure 11-13 Multiple Failure**



## 11.9 Administrative control of protection switching

There are four types of administrative control of ERPS protection switching: *manual*, *forced*, *normal*, and *clear*.

The Protection Switch operation is used to place a port into a blocking state (unblocking the RPL). A Manual Switch cannot be operated on a ring in a protection state and will clear if a failure occurs on the ERPS ring while the protection switch is in place. A Force Switch can be operated on a ring in any state and will not clear if there is a failure on the ring (and may cause the ring to segment).

**Warning** Using force protection switching can create a loss of connectivity on the ring.

Executing the protection-switch clear command removes the protection switch operated on the ERPS Service. This command can also be used to return a ring in the Pending state to the Idle state if operated on the RPL Owner, whether the Pending state is due to the WTR running or a non-revertive mode ring protection switch.

Normal protection switching clears the protection switch mode for ERPS V1 configurations.

To enable manual or force protection switching on a ring port, navigate to the ESERVICE-NNI and then enable the protection switching mode:

```
> ESERVICE ring1 ! existing ring
> NNI gig 1/1/1
> protection-switch enable
> exit
> protection-switch-mode [manual | force | normal | clear]
> exit
> exit
```

### State Priority

The following table outlines the priority request, from highest to lowest, for each time a local request changes or an R-APS message is received:

**Table 11-2 Priority requests hierachy**

Request/State and Status	Type	Priority
Clear	local	highest
FS	local	
R-APS (FS)	remote	
local SF (Note)	remote	
local clear SF	local	
R-APS (SF)	remote	
R-APS (MS)	remote	
MS	local	
WTR Expires	local	

**Table 11-2 Priority requests hierachy (Continued)**

<b>Request/State and Status</b>	<b>Type</b>	<b>Priority</b>
WTR Running	local	
WTB Expires	local	
WTB Running	local	
R-APS (NR, RB)	remote	
R-APS (NR)	remote	lowest

**Note**

If an Ethernet ring node is in the Forced Switch state, local SF is ignored.

## 11.10 ERPS provisioning

This section provides the following ERPS configuration examples:

- Single ring
- Ladder ring with a shared node
- Ladder ring with a shared link

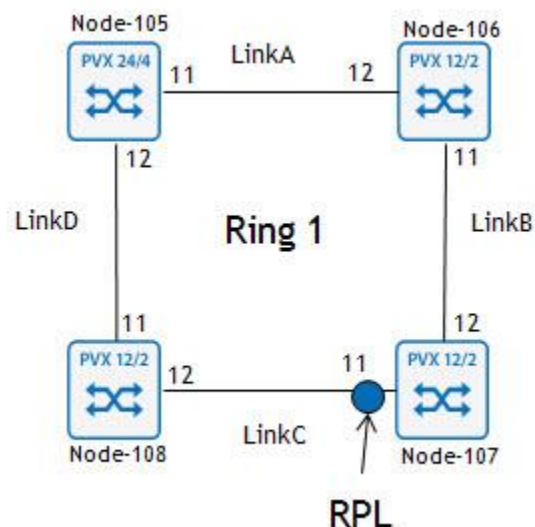
**Note** To avoid a loop when provisioning an ERPS Ring, disable the NNI selected as the RPL on each Ring, until ERPS is configured completely and each service has been enabled.

### 11.10.1 Provision ERPS on a single ring

Use this procedure to provision Ethernet Ring Protection Switching (ERPS) on a single ring, as shown in the following figure.

**Note** Before creating an ERPS Eservice, all Eservices on the Virtual-Switch that are on an MSTI (Instances 1-16) must be returned to the CIST (Instance 0).

**Figure 11-14 Single ring**



**Note** This procedure shows how to provision ERPS with CCM enabled. CCM is optional, and does not need to be enabled for ERPS to work properly.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
BTI7000# enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows

```
BTI7000(config)#
```

**Step 3 Disable the RPL on Node-107**

```
nmi gigabitethernet 1/1/11
shutdown
exit
```

**Step 4 Provision Node-105**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nmi gigabitethernet 1/1/11
me-name LinkA
ccm enable
exit
nmi gigabitethernet 1/1/12
me-name LinkD
ccm enable
exit
admin-state enable
exit
```

**Step 5 Provision Node-106**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nmi gigabitethernet 1/1/11
me-name LinkB
ccm enable
exit
nmi gigabitethernet 1/1/12
me-name LinkA
ccm enable
exit
```



```
admin-state enable
exit
```

**Step 6 Provision Node-107 and the RPL**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
me-name LinkC
ccm enable
ring-protect-link enable
exit
nni gigabitethernet 1/1/12
me-name LinkB
ccm enable
exit
admin-state enable
exit
```

**Step 7 Provision Node-108**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
me-name LinkD
ccm enable
exit
nni gigabitethernet 1/1/12
me-name LinkC
ccm enable
exit
admin-state enable
exit
```

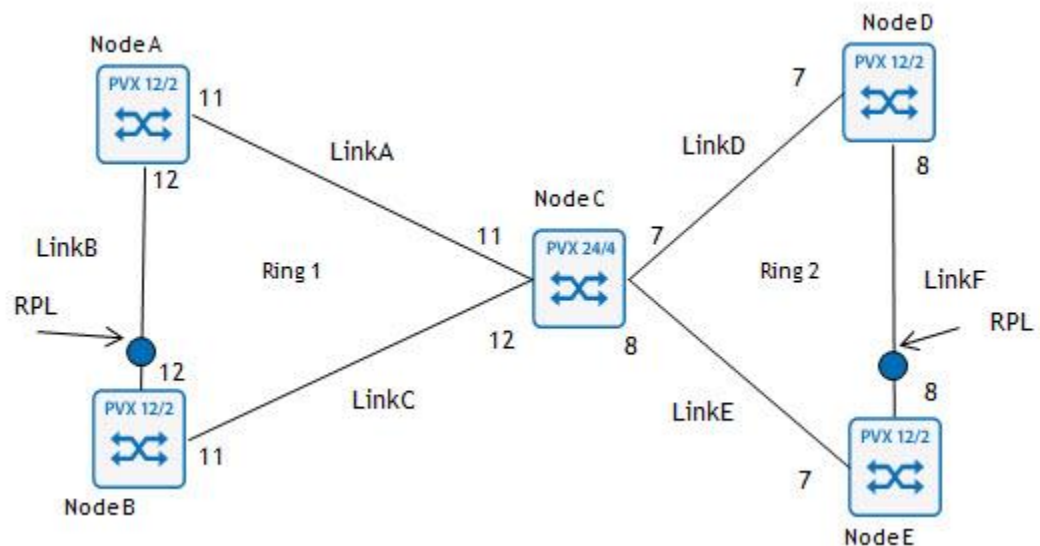
You have successfully completed this procedure.

## 11.10.2 Provision ERPS on multiple independent rings with a shared node

Use this procedure to provision Ethernet Ring Protection Switching (ERPS) on an independent ring with one shared node, as shown in the following figure.

**Note** Before creating an ERPS Eservice, all Eservices on the Virtual-Switch that are on an MSTI (Instances 1-16) must be returned to the CIST (Instance 0).

**Figure 11-15 Independent rings - shared node**



### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Provision Node A

```
virtual-switch 1
eservice Ring1 type ERPS
```

```
s-vlan 100
nni gigabitethernet 1/1/11
exit
nni gigabitethernet 1/1/12
exit
admin-state enable
exit
```

**Step 4 Disable the RPL on Node B**

```
nni gigabitethernet 1/1/12
shutdown
exit
```

**Step 5 Provision Node B**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
exit
nni gigabitethernet 1/1/12
exit
admin-state enable
exit
```

**Step 6 Provision Node C (shared node)**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
exit
nni gigabitethernet 1/1/12
exit
admin-state enable
exit
```

**Provision Ring2:**

```
virtual-switch 1
eservice Ring2 type ERPS
s-vlan 200
nni gigabitethernet 1/1/7
```

```
exit
nni gigabitethernet 1/1/8
exit
admin-state enable
exit
```

**Step 7 Provision Node D**

```
virtual-switch 1
eservice Ring2 type ERPS
s-vlan 200
nni gigabitethernet 1/1/7
exit
nni gigabitethernet 1/1/8
exit
admin-state enable
exit
```

**Step 8 Disable the RPL on Node E**

```
nni gigabitethernet 1/1/8
shutdown
exit
```

**Step 9 Provision Node E**

```
virtual-switch 1
eservice Ring2 type ERPS
s-vlan 200
nni gigabitethernet 1/1/7
exit
nni gigabitethernet 1/1/8
exit
admin-state enable
exit
```

**Step 10 Provision RPL for Ring1 on Node B and enable the RPL link**

```
virtual-switch 1
eservice Ring1
nni gigabitethernet 1/1/12
ring-protect-link enable
exit
exit
```

```
nmi gigabitethernet 1/1/12
no shutdown
exit
```

### Step 11 Provision RPL for Ring2 on Node E and enable the RPL link

```
virtual-switch 1
eservice Ring2
nni gigabitethernet 1/1/8
ring-protect-link enable
exit
exit
nni gigabitethernet 1/1/8
no shutdown
exit
```

You have successfully completed this procedure.

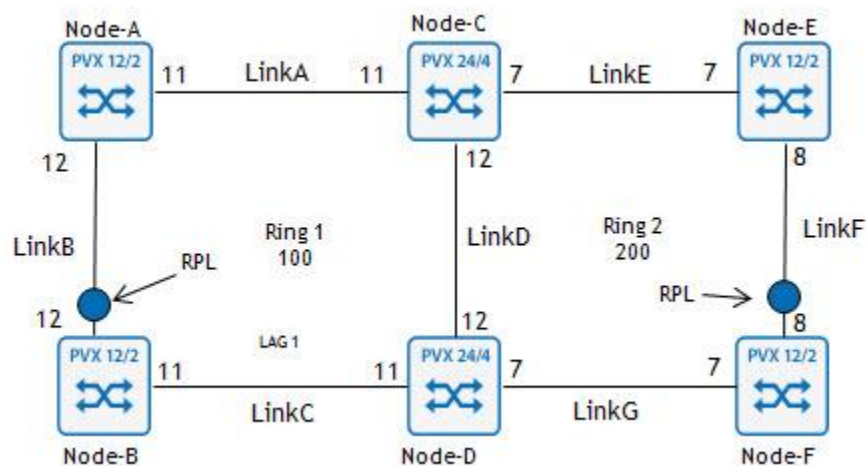
### 11.10.3 Provision ERPS on ladder rings

Use this procedure to provision Ethernet Ring Protection Switching (ERPS) on a ladder ring.

**Note** Before creating an ERPS Eservice, all Eservices on the Virtual-Switch that are on an MSTI (Instances 1-16) must be returned to the CIST (Instance 0).

In the following figure, Ring 1 is the main ring and Ring 2 is the ladder ring.

**Figure 11-16 Ladder ring**



## Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows;

```
BTI7000#
```

## **Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows;

```
BTI7000(config)#
```

## **Step 3 Provision Main Ring (Node-A)**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
exit
nni gigabitethernet 1/1/12
exit
admin-state enable
exit
```

## **Step 4 Provision Main Ring (Node-B) and Set as the RPL for Ring 1**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
exit
nni gigabitethernet 1/1/12
ring-protect-link enable
exit
admin-state enable
exit
```

## **Step 5 Provision Main Ring (Node-C)**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
exit
nni gigabitethernet 1/1/12
```

```
exit
admin-state enable
exit
```

**Step 6 Provision Main Ring (Node-D)**

```
virtual-switch 1
eservice Ring1 type ERPS
s-vlan 100
nni gigabitethernet 1/1/11
exit
nni gigabitethernet 1/1/12
exit
admin-state enable
exit
```

**Step 7 Disable the RPL on Node-B**

```
nni gigabitethernet 1/1/12
shutdown
exit
```

**Step 8 Provision Sub-ring (Node-C)**

```
virtual-switch 1
eservice Ring2 type ERPS
s-vlan 200
property interconnect
no virtual-channel
nni gigabitethernet 1/1/7
exit
admin-state enable
exit
```

**Step 9 Provision Sub-ring (Node-D)**

```
virtual-switch 1
eservice Ring2 type ERPS
s-vlan 200
property interconnect
no virtual-channel
nni gigabitethernet 1/1/7
exit
admin-state enable
```

```
exit
```

**Step 10 Provision Sub-ring (Node-E)**

```
virtual-switch 1
eservice Ring2 type ERPS
s-vlan 200
no virtual-channel
nni gigabitethernet 1/1/7
exit
nni gigabitethernet 1/1/8
exit
admin-state enable
exit
```

**Step 11 Disable the RPL on Node-F**

```
nni gigabitethernet 1/1/8
shutdown
exit
```

**Step 12 Provision Sub-ring (Node-F)**

```
virtual-switch 1
eservice Ring2 type ERPS
s-vlan 200
no virtual-channel
nni gigabitethernet 1/1/7
exit
nni gigabitethernet 1/1/8
exit
admin-state enable
exit
```

**Step 13 Provision RPL for Ring 2 on Node-F**

```
virtual-switch 1
eservice Ring2
nni gigabitethernet 1/1/8
ring-protect-link enable
exit
exit
```

**Step 14 Enable the RPL link on Node-B**

```
nni gigabitethernet 1/1/12
```



```
no shutdown
exit
```

**Step 15 Enable the RPL link on Node-F**

```
nmi gigabitethernet 1/1/8
no shutdown
exit
```

You have successfully completed this procedure.

### 11.10.4 Enable manual protection switching

A manual protection switch places the operating port into a blocking state. In the event of a Signal Fail (SF) condition raised elsewhere on the ring, the port automatically becomes unblocked. A manual protection switch is possible only when the ring is in an 'Idle' state.

Use this procedure to enable a manual protection switch.

**Step 1 Navigate to the ERPS Service**

To navigate to the ERPS Service, the following command:

```
BTI7000:sw1(config)# eservice ERPS_Test
```

**Step 2 Navigate to the NNI to be placed in Manual-Switch mode**

To navigate to the NNI to be placed in Manual-Switch mode, enter the following command:

```
BTI7000:sw1(config-eservice)# nni ten 1/1/3
```

**Step 3 Enable 'Protection-Switch' on the NNI (no action will be taken at this point).**

```
BTI7000:sw1(config-nni-eservice)# protection-switch enable
```

**Step 4 From the ERPS Eservice level, set the 'Protection Switch Mode' to 'Manual'.**

```
BTI7000:sw1(config-eservice)# protection-switch-mode manual
```

You have successfully completed this procedure.

### 11.10.5 Disable manual protection switching

Use this procedure to disable manual protection switching. This clears manual protection switching on the RPL owner.

**Step 1 Navigate to the ERPS Service**

```
BTI7000:sw1(config)# eservice ERPS_Test
```

**Step 2 From the ERPS Eservice level, set the 'Protection Switch Mode' to 'clear'**

```
BTI7000:sw1(config-eservice)# protection-switch-mode clear
```

**Note** This command is for an ERPS V2 system. On an ERPS V1 system, the command is:

```
protection-switch-mode normal
```

For more information about the feature differences between ERPS V1 and ERPS V2 refer to the ERPS feature matrix in [11.3, “ERPS Model in the packetVX”](#).

**Step 3 Navigate to the NNI to be removed from Manual-Switch mode.**

```
BTI7000:sw1(config-eservice)# nni ten 1/1/3
```

**Step 4 Disable ‘Protection-Switch’ on the NNI (no action will be taken at this point).**

To disable ‘Protection-Switch’ on the NNI, enter the following command:

```
BTI7000:sw1(config-nni-eservice)# protection-switch disable
```

You have successfully completed this procedure.

## 11.10.6 Enable forced protection switching

Use this procedure to enable a forced protection switch.

Forced protection switching forces the operating port into a blocking state. In the event of a Signal Fail (SF) condition raised elsewhere on the ring, the ports will NOT automatically become unblocked. Forced protection switch is possible when the ring is in an ‘Idle’ or ‘Protect’ state.

**Step 1 Navigate to the ERPS Service**

To navigate to the ERPS Service, the following command:

```
BTI7000:sw1(config)# eservice ERPS_Test type ERPS
```

**Step 2 Navigate to the NNI to be placed in Force-Switch mode**

To navigate to the NNI to be placed in Force-Switch mode, enter the following command:

```
BTI7000:sw1(config-eservice)# nni ten 1/1/3
```

**Step 3 Enable ‘Protection-Switch’ on the NNI (no action will be taken at this point).**

```
BTI7000:sw1(config-nni-eservice)# protection-switch enable
```

**Step 4 From the ERPS Eservice level, set the ‘Protection Switch Mode’ to ‘Force’**

```
BTI7000:sw1(config-eservice)# protection-switch-mode force
```

You have successfully completed this procedure.

## 11.10.7 Disable forced protection switching

Use this procedure to disable forced protection switching. This clears forced protection switching on the RPL owner.

**Step 1 Navigate to the ERPS Service .**

To navigate to the ERPS Service, the following command:

```
BTI7000:sw1(config)# eservice ERPS_Test type ERPS
```

**Step 2 From the ERPS Eservice level, set the ‘Protection Switch Mode’ to ‘Clear’**

```
BTI7000:sw1(config-eservice)# protection-switch-mode clear
```

For ERPS V1 you use the **normal** command option instead of **clear**.

**Step 3 Navigate to the NNI to be removed from Force-Switch mode.**

To navigate to the NNI to be removed from Force-Switch mode, enter the following command:

```
BTI7000:sw1(config-eservice)# nni ten 1/1/3
```

**Step 4 Disable ‘Protection-Switch’ on the NNI (no action will be taken at this point).**

To disable ‘Protection-Switch’ on the NNI, enter the following command:

```
BTI7000:sw1(config-nni-eservice)# protection-switch disable
```

You have successfully completed this procedure.

## 11.10.8 Modifying ERPS service parameters

Some ERPS service settings cannot be directly modified after the ERPS service is administratively enabled. For these settings, there are two methods for modifying an enabled ERPS service—deleting or disabling the service. The method you choose is dependent on the parameter that you are changing.

Following is a list of the ERPS service parameters that require the Eservice to be deleted and re-provisioned to change parameter values:

- MEG levels
- Property interconnection
- S-VLAN

Modifications to ERPS service parameters, not listed above, require that the Eservice is disabled before and enabled after changes are made. The exceptions to this are the following commands, which can be issued at any time:

- **ccm {enable|disable}**
- **wait-to-block-timer <time>**
- **wait-to-restore-timer {<time> | short}**

The following procedure shows how to delete an Eservice, and re-provision the service with new values:

**Step 1 Administratively disable one of the NNI ports on the ring (effectively preventing an Ethernet loop from occurring)**

To administratively disable one of the NNI ports on the ring, the following command:

```
BTI7000:sw1(config-nni TenGigE 1/1/1)# admin-state disable
```

**Step 2 From the ERPS Eservice, administratively disable the service**

```
BTI7000:sw1(config)# eservice ERPS_Test type ERPS
```

```
BTI7000:sw1(config-eservice)# admin-state disable
```

<b>Note</b>	You can only disable the ERPS service when the ring is in protection or force switch mode.
-------------	--

**Step 3 Remove the two NNI's from the ERPS Service**

To remove the two NNI's from the ERPS Service, enter the following command:

```
BTI7000:sw1(config-eservice)# no nni tenGigabitEthernet 1/1/1
```

```
BTI7000:sw1(config-eservice)# no nni tenGigabitEthernet 1/1/2
```

**Step 4 Delete the ERPS Service.**

To delete the ERPS Service, enter the following command:

```
BTI7000:sw1(config)# no eservice ERPS_Test
```

**Step 5 Re-provision the ERPS service with the updated parameters**

For example:

```
BTI7000:sw1(config)# eservice ERPS_Test type ERPS
```

```
BTI7000:sw1(config-eservice)# s-vlan 4089
```

```
BTI7000:sw1(config-eservice)# recovery revertive
```

```
BTI7000:sw1(config-eservice)# wait-to-restore-timer short
```

```
BTI7000:sw1(config-eservice)# nni ten 1/1/3
```

```
BTI7000:sw1(config-nni-eservice)# me-name Lnk12
```

```
BTI7000:sw1(config-nni-eservice)# ccm enable
```

```
BTI7000:sw1(config-nni-eservice)# ring-protect-link enable
```

```
BTI7000:sw1(config-nni-eservice)# exit
```

```
BTI7000:sw1(config-eservice)# nni ten 1/1/4
```

```
BTI7000:sw1(config-nni-eservice)# me-name Lnk11
```

```
BTI7000:sw1(config-nni-eservice)# ccm enable
```

```
BTI7000:sw1(config-nni-eservice)# exit
```

**Note** You can only change the RPL and the wait-to-restore timer when the ring is in protection or force switch mode.

**Step 6 Administratively enable the ERPS service**

To administratively enable the ERPS service, enter the following command:

```
BTI7000:sw1(config-eservice)# admin-state enable
```

**Step 7 Re-enable the manually disabled NNI port**

To re-enable the manually disabled NNI port, enter the following command:

```
BTI7000:sw1(config-nni TenGigE 1/1/1)# admin-state enable
```

You have successfully completed this procedure.

## 11.11 Replacing a packetVX in an ERPS network: non-interconnected nodes

---

This section describes how to replace a BTI packetVX that is associated with virtual switches that are part of an ERPS (Ethernet Ring Protection Switching) network configuration, with non-interconnected nodes.

Up to two PVX modules may be a member of a single virtual switch. When a PVX is replaced in a ladder ring network, its MEP associations for the virtual switches are not automatically learned. You need to re-associate the MEPs to the virtual switches of the replaced PVX.

The PVX replacement process involves:

- Disabling the NNI interfaces that face the node associated with the PVX.
- Physically removing and replacing the PVX.
- Forcing the MEPs (Maintenance End Point) to relearn the remote information.
- Restoring the NNI interfaces.

### Before you begin

You should be familiar with the procedures for replacing a PVX. Refer to the *BTI 7000 Series Alarm and Troubleshooting Guide*, section "Replacing packetVX modules."

### 11.11.1 Replace a packetVX in an ERPS network: non-interconnected nodes

Use this procedure to replace a packetVX (PVX) module that is associated to a virtual switch in an ERPS network configuration, with non-interconnected nodes.

<b>Note</b>	Before you proceed, you should be familiar with physically replacing PVX modules; refer to the <i>BTI 7000 Series Alarm and Troubleshooting Guide</i> .
-------------	---

<b>Note</b>	This procedure impacts traffic.
-------------	---------------------------------

These steps are an example of replacing a PVX that is associated to virtual switch 1.

#### Step 1 From Configuration mode, shutdown all NNIs facing the failed PVX:

```
BTI7000(config)# virtual-switch 8
BTI7000:sw8(config)# nni tenGigabitEthernet 11/5/2
BTI7000:sw8(config-nni TenGigE 11/5/2)# shutdown

BTI7000(config)# virtual-switch 2
BTI7000:sw2(config)# nni tenGigabitEthernet 1/7/1
BTI7000:sw2(config-nni TenGigE 1/7/1)# shutdown

BTI7000(config)# virtual-switch 9
```

```
BTI7000:sw9(config)# nni gigabitEthernet 11/7/1
BTI7000:sw9(config-nni GigE 11/7/1)# shutdown
```

**Step 2 Shutdown all ERPS NNIs on the failed PVX:**

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/2
BTI7000:sw1(config-nni TenGigE 1/3/2)# shutdown

BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni TenGigE 1/3/1)# shutdown

BTI7000:sw1(config)# nni gigabitEthernet 1/3/1
BTI7000:sw1(config-nni GigE 1/3/1)# shutdown
```

**Step 3 Physically replace the failed PVX:**

Refer to the *BTI 7000 Series Alarm and Troubleshooting Guide*, "Replacing a PVX module.

When the PVX is installed, it automatically learns its MEP.

**Step 4 For each ERPS Service-NNI facing the new PVX, re-associate the MEPS:**

```
BTI7000:config)# virtual-switch 8
BTI7000:sw8(config)# eservice ERPS_MainRing
BTI7000:sw8(config-eservice)# nni tenGigabitEthernet 11/5/2
BTI7000:sw8(config-nni-eservice)# flush-remote-mep

BTI7000:config)# virtual-switch 2
BTI7000:sw2(config)# eservice ERPS_MainRing
BTI7000:sw2(config-eservice)# nni tenGigabitEthernet 1/7/1
BTI7000:sw2(config-nni-eservice)# flush-remote-mep

BTI7000:config)# virtual-switch 9
BTI7000:sw9(config)# eservice ERPS_MainRing
BTI7000:sw9(config-eservice)# nni gigabitEthernet 11/7/1
BTI7000:sw9(config-nni-eservice)# flush-remote-mep
```

**Step 5 Enable all ERPS NNIs on the new PVX:**

```
BTI7000:config)# virtual-switch 1
BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/2
BTI7000:sw1(config-nni TenGigE 1/3/2)# no shutdown

BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni TenGigE 1/3/1)# no shutdown

BTI7000:sw1(config)# nni gigabitEthernet 1/3/1
```

```
BTI7000:sw1(config-nni GigE 1/3/1)# no shutdown
```

**Step 6 Enable all NNIs facing the failed PVX:**

```
BTI7000:config)# virtual-switch 8
```

```
BTI7000:sw8(config)# nni tenGigabitEthernet 11/5/2
```

```
BTI7000:sw8(config-nni TenGigE 11/5/2)# no shutdown
```

```
BTI7000:config)# virtual-switch 2
```

```
BTI7000:sw2(config)# nni tenGigabitEthernet 1/7/1
```

```
BTI7000:sw2(config-nni TenGigE 1/7/1)# no shutdown
```

```
BTI7000:config)# virtual-switch 9
```

```
BTI7000:sw9(config)# nni gigabitEthernet 11/7/1
```

```
BTI7000:sw9(config-nni GigE 11/7/1)# no shutdown
```

You have successfully completed this procedure.



## 11.12 Removing a packetVX in an ERPS network: non-interconnected nodes

This section describes how to remove a BTI packetVX (PVX) that is associated to a virtual switch in an ERPS (Ethernet Ring Protection Switching) network configuration, with non-interconnected nodes.

Removing a PVX involves:

- Disabling the NNIs that face the node associated with the PVX.
- Connecting the cables to another PVX in the ring.
- Changing the ME-Name that was used on the removed PVX to match the ME-Name on the virtual switch that is now being used. This is only required if ccm is enabled.
- Associating the remote MEPs to the virtual switch that is now being used.
- Enabling the NNIs that face the node associated with the PVX that is now being used.

<b>Note</b>	Up to eight ERPS services can be configured on a PVX. You need to keep this in mind when determining to which PVX you are using, to replace the PVX that is removed.
-------------	--

### Before you begin

You should be familiar with the physical module and cabling tasks for removing a PVX. Refer to the *BTI 7000 Series Alarm and Troubleshooting Guide*, section "Replacing packetVX modules."

### 11.12.1 Remove a packetVX in an ERPS network: non-interconnected nodes

Use this procedure to remove a packetVX (PVX) module whose nodes are a member of a ring network, and redirect the cabling and interfaces to another PVX in the ring.

<b>Note</b>	Before you proceed, you should be familiar with the physical tasks for removing a PVX module; refer to the <i>BTI 7000 Series Alarm and Troubleshooting Guide</i> .
-------------	---

<b>Note</b>	This procedure impacts traffic.
-------------	---------------------------------

These steps are an example of removing a PVX of virtual switch 2, that resides in the middle of virtual switches 1 and 3. These steps also assume that the cables are already disconnected from this PVX.

#### Step 1 Shutdown all NNIs facing the virtual switch 2:

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni TenGigE 1/3/1)# shutdown
```

```
BTI7000(config)# virtual-switch 3
BTI7000:sw3(config)# nni tenGigabitEthernet 1/9/2
BTI7000:sw3(config-nni TenGigE 1/9/2)# shutdown
```

**Step 2 Physically connect the cables from virtual switch 1 to virtual switch 3:**

**Step 3 Change the ME-Name of virtual switch 1 to match that of virtual switch 3:**

You need to change the name since the ME-Name on virtual switch 1 was associated to the ME-Name of the PVX you removed.

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# eservice ERPS_MainRing
BTI7000:sw1(config-eservice)# shutdown
BTI7000:sw1(config-eservice)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni-eservice)# me-name Lk2
BTI7000:sw1(config-nni-eservice)# exit
BTI7000:sw1(config-nni-eservice)# no shutdown
```

**Step 4 Associate the MEPs to virtual switch 3:**

```
BTI7000(config)# virtual-switch 3
BTI7000:sw3(config)# eservice ERPS_MainRing
BTI7000:sw3(config-eservice)# nni tenGigabitEthernet 1/9/2
BTI7000:sw3(config-nni-eservice)# flush-remote-mep
```

**Step 5 Enable all ERPS NNIs on virtual switches 1 and 3:**

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni TenGigE 1/3/1)# no shutdown

BTI7000(config)# virtual-switch 3
BTI7000:sw3(config)# nni tenGigabitEthernet 1/9/2
BTI7000:sw3(config-nni TenGigE 1/9/2)# no shutdown
```

You have successfully completed this procedure.

## 11.13 Adding a packetVX in an ERPS network: non-interconnected nodes

This section describes how to add a BTI packetVX (PVX) to an ERPS (Ethernet Ring Protection Switching) network configuration, with non-interconnected nodes.

Adding a PVX to an ERPS ring involves:

- Disabling the NNIs on each end of the ring, from which the PVX is going to be added.
- Physically installing the PVX.
- Provisioning the NNIs and ERPS Eservice on the PVX.
- Changing the ME-Name to match that of the new PVX. This is only required if ccm is enabled.
- Forcing the MEPs (Maintenance End Point) to relearn the remote information.

### Before you begin

You should be familiar with the procedures for physically installing a PVX. Refer to the *BTI 7000 Series Common Equipment and Installation Guide*.

### 11.13.1 Add a packetVX in an ERPS network: non-interconnected nodes

Use this procedure to add a packetVX (PVX) module to a ring network, with non-interconnected nodes.

**Note** Before you proceed, you should be familiar with the physical tasks for installing a PVX module; refer to the *BTI 7000 Series Common Equipment and Installation Guide*.

**Note** This procedure impacts traffic.

These steps are an example of adding a PVX of virtual switch 2, between virtual switches 1 and 3.

#### Step 1 Shutdown the NNIs that will be facing virtual switch 2:

On virtual switch 1:

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni TenGigE 1/3/1)# shutdown
```

On virtual switch 3:

```
BTI7000(config)# virtual-switch 3
BTI7000:sw3(config)# nni tenGigabitEthernet 1/9/2
BTI7000:sw3(config-nni TenGigE 1/9/2)# shutdown
```

#### Step 2 Physically install the PVX, including connecting the cables to the new ports.

**Step 3 Provision NNIs and the ERPS Service on the new NE:**

On virtual switch 2:

```
BTI7000(config)# virtual-switch 2
BTI7000:sw2(config)# nni tenGigabitEthernet 1/7/1
BTI7000:sw3(config-nni TenGigE 1/7/1)# exit
BTI7000:sw2(config)# nni tenGigabitEthernet 1/7/2
BTI7000:sw2(config-nni TenGigE 1/7/2)# exit

BTI7000:sw2(config)# eservice ERPS_MainRing
BTI7000:sw2(config-eservice)# s-vlan 2
BTI7000:sw2(config-nni-eservice)# nni tenGigabitEthernet 1/7/1
BTI7000:sw2(config-nni-eservice)# me-name Lk1
BTI7000:sw2(config-nni-eservice)# ccm enable
BTI7000:sw2(config-nni-eservice)# exit
BTI7000:sw2(config-nni-eservice)# nni tenGigabitEthernet 1/7/2
BTI7000:sw2(config-nni-eservice)# me-name Lk2
BTI7000:sw2(config-nni-eservice)# ccm enable
BTI7000:sw2(config-nni-eservice)# exit
BTI7000:sw2(config-eservice)# admin-state enable
```

**Step 4 Change the ME-Name of virtual switch 1 to match that of virtual switch 2:**

You need to change the name since the ME-Name on virtual switch 1 was associated to the ME-Name of virtual switch 3.

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# eservice ERPS_MainRing
BTI7000:sw1(config-eservice)# shutdown
BTI7000:sw1(config-eservice)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni-eservice)# me-name Lk1
BTI7000:sw1(config-nni-eservice)# exit
BTI7000:sw1(config-eservice)# no shutdown
```

**Step 5 Force the remote MEPs on virtual switches 1 and 3 to learn the MEP of virtual switch 2:**

On virtual switch 1:

```
BTI7000(config)# virtual-switch 1
BTI7000:sw1(config)# eservice ERPS_MainRing
BTI7000:sw1(config-eservice)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni-eservice)# flush-remote-mep
```

On virtual switch 3:

```
BTI7000(config)# virtual-switch 3
```

```
BTI7000:sw3(config)# eservice ERPS_MainRing
BTI7000:sw3(config-eservice)# nni tenGigabitEthernet 1/9/2
BTI7000:sw3(config-nni-eservice)# flush-remote-mep
```

**Step 6 Enable the NNIs on virtual switches 1 and 3, which are facing virtual switch 2:**

On virtual switch 1:

```
BTI7000:config)# virtual-switch 1
BTI7000:sw1(config)# nni tenGigabitEthernet 1/3/1
BTI7000:sw1(config-nni TenGigE 1/3/1)# no shutdown
```

On virtual switch 3:

```
BTI7000:config)# virtual-switch 3
BTI7000:sw3(config)# nni tenGigabitEthernet 1/9/2
BTI7000:sw3(config-nni TenGigE 1/9/2)# no shutdown
```

You have successfully completed this procedure.



## 12.0 BTI™packetVX® Security

---

### Access control lists

BTI packetVX modules support the configuration of access control lists (ACLs) to provide security on the network. ACLs are similar to firewalls in that they can be configured to identify traffic flows and drop the associated packets.

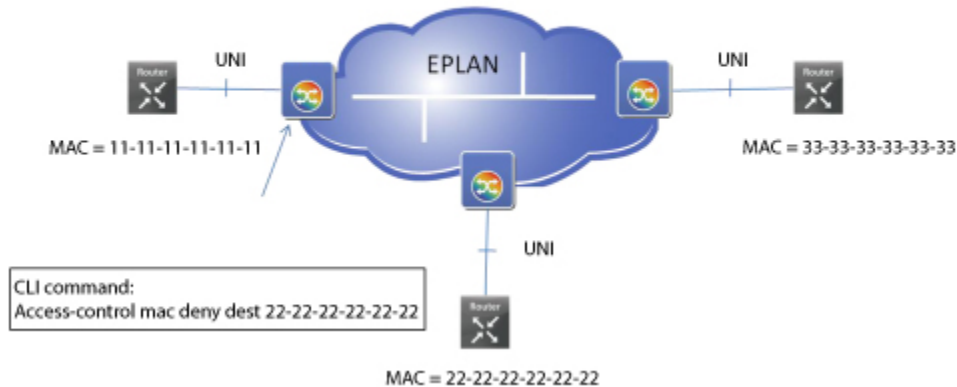
ACLs are configured at the switch level and apply to all ports on a packetVX module. ACLs can be configured to match based on the following combinations:

- Source MAC address
- Destination MAC address
- Source and destination MAC addresses
- Source IP address
- Destination IP address
- Source and destination IP address

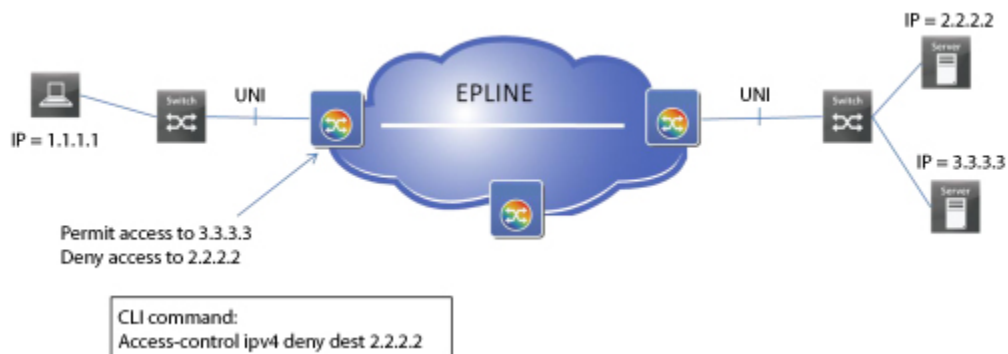
<b>Note</b>	As of R7.3, packetVX modules support only ACLs for IP addresses specified in v4 format.
-------------	---

### Example 1

In this example, the network is providing an EPLAN service to link three sites together. The customer has requested that the network be configured so that Site 1 can send traffic to Site 3 but not to Site 2. Since all sites have routers identified by unique MAC addresses, an ACL based on destination MAC address can be configured on the packetVX module connected to Site 1 to deny all traffic destined to the MAC address of the router at Site 2.

**Figure 12-1 ACL example based on destination MAC address****Example 2**

In this example, the network is providing an EPLINE service to link two sites together. The customer has requested that the network be configured so that a client at Site 1 can send traffic to one server at Site 2 but not the other. Since the servers are identified by unique IP addresses, an ACL based on destination IP address can be configured on the packetVX module connected to Site 1 to deny all traffic destined to the IP address of the disallowed server at Site 2.

**Figure 12-2 ACL example based on destination IP address**

This section covers the following topics:

- 12.1, “Adding an access control”
- 12.2, “Removing an access control”



## 12.1 Adding an access control

Use this procedure to add an access control for the selected switch.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- A Virtual Switch must already be created and selected.
- The mode must be set to Switch Configuration mode.

### Step 1 Enter the access-control command syntax

To define an IPv4 or MAC based access control for the currently selected switch, enter the following command syntax at the command line interface:

```
access-control {mac|ipv4} deny [source <address>] [dest <address>]
```

where <address> is a valid MAC or IPv4 source or destination address of the access control being defined. The following is a valid MAC address format:

```
xx-xx-xx-xx-xx-xx
```

The following is a valid IPv4 address format:

```
xxx.xxx.xxx.xxx[/prefix]
```

If access-control mac deny source 11-22-33-44-55-66 dest aa-bb-cc-dd-ee-ff is entered, then packets from MAC address 11-22-33-44-55-66 are denied permission to be received by MAC address aa-bb-cc-dd-ee-ff.

You have successfully completed this procedure.

## 12.2 Removing an access control

---

This procedure explains how to remove an access control for the currently selected switch.



### Prerequisites

- If necessary, acquire the access control indexes you need by using the **show access-control** command.
- A Virtual Switch must be selected.

### Step 1 Enter the no access-control command syntax

To remove an IPv4 or MAC based access control for the currently selected switch, enter the following command syntax at the command line interface:

```
no access-control {mac|ipv4} <access-control-index>
```

where *<access-control-index>* is the index of the access control being removed.

If no access-control mac 2 is entered, the access control with an access control index of 2 is removed.

You have successfully completed this procedure.

## 13.0 Performance management

---

This section provides information about monitoring BTI™ packetVX® module performance.

- [13.1, “Supported performance metrics”](#)
- [13.2, “Ethernet service performance monitoring statistics”](#)
- [13.3, “Displaying and clearing performance monitor counts on packetVX modules”](#)
- [13.4, “Displaying and setting Threshold Crossing Alerts on packetVX modules”](#)

## 13.1 Supported performance metrics

### 13.1.1 Physical PMs supported on packetVX modules

Table 13-1 Physical PMs (gauges)

PM	Supported transceivers
<b>Optical Power Received</b> Optical Power Received measures the minimum, maximum, and average optical power (dBm) received. Measurements are accurate to $\pm 3.0$ dBm for SFPs; to $\pm 2.0$ dBm for XFPs.	Noncopper SFPs All XFPs
<b>Optical Power Transmitted</b> Optical Power Transmitted measures the minimum, maximum, and average optical power (dBm) transmitted. Measurements are accurate to $\pm 3.0$ dBm for SFPs; to $\pm 2.0$ dBm for XFPs.	Noncopper SFPs All XFPs
<b>Supply Voltage</b> Supply Voltage measures the supply voltage on the 3.3V supply for SFPs; on the 5.0V supply for XFPs.	Noncopper SFPs All XFPs
<b>Supply Voltage 2</b> Second Supply Voltage measures the supply voltage on the 3.3V supply.	All XFPs
<b>Temperature</b> Temperature measures the temperature ( $^{\circ}\text{C}$ ) of the transceiver.	All SFPs All XFPs
<b>Tx Bias Current</b> Laser Bias Current measures the laser bias current (mA).	Noncopper SFPs All XFPs

### 13.1.2 GE port Ethernet (Layer 1) PMs supported on packetVX modules

Table 13-2 Layer 1 Gigabit Ethernet PMs (counters)

PM
<b>Coding Violations</b> Coding Violations measure the number of 8B/10B coding violations and disparity errors.
<b>Errored Seconds</b> Errored Seconds measures the number of seconds during which one or more coding violations are detected, or a Loss of Synchronization (LOSYNC) or Loss of Signal (LOS) defect is present.
<b>Severely Errored Seconds</b> Severely Errored Seconds measures the number of seconds during which the number of detected coding violations exceeds the severely errored seconds level (SESLVL), or a Loss of Synchronization (LOSYNC) defect or Loss of Signal (LOS) defect is present. The SESLVL value for Layer 1 Gigabit Ethernet is 1250.
<b>Unavailable Seconds</b> Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES. In seconds that are counted as unavailable, the counting of CV, ES, and SES is inhibited.

### 13.1.3 10 GE (Layer 1) PMs supported on packetVX modules

Table 13-3 10 GE (Layer 1) PMs (counters)

PM
<b>Invalid Blocks</b> Invalid Blocks measures the number of invalid 64/66B coding blocks.
<b>Errored Seconds</b> Errored Seconds measures the number of seconds during which one or more errored blocks/code violations are detected, or LOSYNC (Loss of Synchronization) or LOS (Loss of Signal) is detected.
<b>Severely Errored Seconds</b> Severely Errored Seconds measures the number of detected invalid blocks exceeds the severely errored seconds level (SESLVL), or in which a Loss of Synchronization (LOSYNC) defect or Loss of Frame (LOF) defect is present. The SESLVL value for 10GELAN is 8554.
<b>Unavailable Seconds</b> Unavailable Seconds measures the number of seconds during which the link was considered unavailable. A link becomes unavailable at the onset of 10 consecutive seconds that qualify as SES, and continues to be unavailable until the onset of 10 consecutive seconds that do not qualify as SES. In seconds that are counted as unavailable, the counting of In seconds that are counted as unavailable, the counting of INVBLK, ES, and SES is inhibited.

### 13.1.4 10GE WAN PHY PMs

Table 13-4 10GE WAN PHY PMs (counters)

PM
<b>CV-S</b> Section Coding Violations
<b>ES-S</b> Section Errored Seconds
<b>SES-S</b> Section Severely Errored Seconds
<b>UAS-S</b> Section Unavailable Seconds
<b>SEFS-S</b> Section Severely Errored Framing Seconds
<b>CV-L</b> Line Coding Violations
<b>ES-L</b> Line Errored Seconds
<b>SES-L</b> Line Severely Errored Seconds
<b>UAS-L</b> Line Unavailable Seconds

**Table 13-4 10GE WAN PHY PMs (counters) (Continued)**

<b>PM</b>
<b>CV-P</b> Path Coding Violations
<b>ES-P</b> Path Errored Seconds
<b>SES-P</b> Path Severely Errored Seconds
<b>UAS-P</b> Path Unavailable Seconds

## 13.1.5 10 GE Port OTN (Layer 1) PMs

Table 13-5 OTN ( Layer 1) PMs(counters)

PM
<b>NUMBITSCR</b> Number of Bits Corrected measures the total number of bits corrected by the Forward Error Correction (FEC) decoder according to the Reed-Solomon RS(255,239) forward error correction scheme.
<b>NUMBYTESCR</b> Number of Bytes Corrected measures the total number of bytes corrected by the forward error correction scheme.
<b>UNCRCDWRD</b> Uncorrectable Code Words measures the total number of errored code words received that could not be corrected by the Forward Error Correction scheme.
<b>BER</b> Bit Error Rate (Instantaneous) provides an estimate of the instantaneous Bit Error Ratio of the line by evaluating the ratio of the number of bits corrected to the total bits received over a 10-second time window.
<b>BER-AVG</b> Bit Error Rate (Average) provides an estimate of the average Bit Error Ratio of the line by evaluating the ratio of the number of bits corrected to the total bits received over the duration of the entire collection interval.
<b>OTU-EB</b> OTU Errored Blocks measures the number of frames containing one or more Bit Interleaved Parity (BIP) errors, using the OTU-2 SM BIP-8 byte in the incoming OTN signal. Up to eight BIP-8 errors can be detected per OTU-2 frame. However, regardless of the number of BIP-8 errors detected, a single frame can count for no more than one errored block.
<b>OTU-BBE</b> OTU Background Block Errors measures the number of errored blocks not occurring during seconds counted as OTU-SES seconds.
<b>OTU-ES</b> OTU Errored Seconds measures the number of seconds during which one or more errored blocks was detected or a Loss of Frame (LOF) or a Loss of Signal (LOS) defect was present.
<b>OTU-SES</b> OTU Severely Errored Seconds measures the number of seconds during which the number of detected errored blocks exceeds the severely errored seconds level (SESLVL), or a Loss of Frame (LOF) or Loss of Signal (LOS) defect was present. The SESLVL value for OTN is 30% of the nominal block rate.
<b>OTU-OFS</b> OTU Out-of-Frame Seconds measures the number of seconds during which a Out of Frame (OOF) defect was present.
<b>OTU-UAS</b> OTU-2 Unavailable Seconds measures the number of seconds during which the OTN line is unavailable. A second is considered OTU-UAS at the onset of 10 consecutive OTU-SES seconds, and is no longer considered OTU-UAS after 10 consecutive seconds that are not OTU-SES seconds.

## 13.1.6 Ethernet (Layer 2) PMs

Table 13-6 Ethernet (Layer 2) PMs (counters)

PM
<b>Broadcast Packets</b> Broadcast Packets measures the total number of good frames received that were directed to the broadcast address. (This number does not include frames that were directed to the multicast address.)
<b>Frame Checksum Errors</b> Frame Checksum Errors measures the number of received frames that had a valid length but had either a bad Frame Check Sequence (FCS Error) or a bad FCS with a non-integral number of OCTETS (alignment errors).
<b>Discarded Packets</b> Discarded Packets measures the total number of frames dropped due to a lack of resources or other reasons. This number is not necessarily the number of frames dropped, but rather the number of time that dropped frames could be detected.
<b>Received Packet Fragments</b> Received Packet Fragments measures the total number of received frames that were less than 64 octets long (excluding framing bits, but including Frame Check Sequence (FCS) octets) and had either a bad FCS with a integral number of octets (FCS error) or a bad FCS with a non-integral number of octets (alignment error).
<b>Multicast Packets</b> Multicast Packets measures the total number of good frames received that were directed to a multicast address. (This number does not include frames that were directed to the broadcast address.)
<b>Oversized Packets</b> Oversized Packets measures the total number of received Ethernet frames with a length greater than the maximum frame size (MFS), and with a valid or invalid Frame Check Sequence (FCS).
<b>Received Packets (Over 1518 Bytes)</b> Received Packets (Over 1518 Bytes) measures the total number of frames received that were greater than or equal to 1519 bytes in length (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Packets (64 Bytes)</b> Received Packets (64 Bytes) measures the total number of 64 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Packets (65 to 127 Bytes)</b> Received Packets (65 to 127 Bytes) measures the total number of 65-127 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Packets (128 to 255 Bytes)</b> Received Packets (128 to 255 Bytes) measures the total number of 128-255 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Packets (256 to 511 Bytes)</b> Received Packets (256 to 511 Bytes) measures the total number of 256-511 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Packets (512 to 1023 Bytes)</b> Received Packets (512 to 1023 Bytes) measures the total number of 512-1023 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Packets (1024 to 1518 Bytes)</b>



**Table 13-6 Ethernet (Layer 2) PMs (counters) (Continued)**

<b>PM</b>
Received Packets (1024 to 1518 Bytes) measures the total number of 1024-1518 byte frames received (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Byte Count (Total)</b>
Received Byte Count (Total) measures the total number of bytes of data (including those in bad frames) received (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Transmitted Byte Count (Total)</b>
Transmitted Byte Count (Total) measures the total number of bytes of data (including those in bad frames) transmitted (excluding framing bits, but including Frame Check Sequence (FCS) octets).
<b>Received Packets (Total)</b>
Received Packets (Total) measures the total number of frames (bad frames, broadcast frames, and multicast frames) received.
<b>Transmitted Packets (Total)</b>
Transmitted Packets (Total) measures the total number of frames (bad frames, broadcast frames, and multicast frames) transmitted.
<b>Received Pause Packets</b>
Total Pause Frame Count in Receive Direction measures the total number of pause frames received.
<b>Transmitted Pause Packets</b>
Transmitted Pause Packets measures the total number of pause frames transmitted.
<b>Undersized Packets (&lt;64 Bytes)</b>
Undersized Packets (<64 Bytes) measures the total number of frames received that were less than 64 octets long (excluding framing bits, but including Frame Check Sequence (FCS) octets) and were otherwise well formed.

## 13.1.7 Link Aggregation Group PMs supported on packetVX modules

Table 13-7 Link Aggregation Group PMs (counters)

PM
<b>Link Access Control PDUs Received</b> Link Access Control PDUs Received measures the number of valid Link Aggregation Control Protocol Data Units received for the interval.
<b>Marker PDUs Received</b> Marker PDUs Received measures the number of valid marker Protocol Data Units received for the interval.
<b>Marker Response PDUs Received</b> Marker Response PDUs Received measures the number of valid markers response Protocol Data Units received for the interval.
<b>Invalid Link Access Control Packets Received</b> Invalid Link Access Control Packets Received measures the number of illegal Protocol Data Units received for the interval.
<b>Link Access Control PDUs Transmitted</b> Link Access Control PDUs Transmitted measures the number of Link Aggregation Control Protocol Data Units transmitted for the interval.
<b>Marker PDUs Transmitted</b> Marker PDUs Transmitted measures the number of marker Protocol Data Units transmitted for the interval.
<b>Marker Response PDUs Transmitted</b> Marker Response PDUs Transmitted measures the number of marker responses transmitted for the interval.

## 13.1.8 MSTP PMs supported on packetVX modules modules

Table 13-8 MST Instance PMs (counters)

PM
<b>RCCR</b> CIST Region Configuration Changes measures the number of configuration changes detected by CIST in the tree
<b>TCCC</b> CIST/MSTI Region Configuration Changes measures the number of configuration changes detected by MSTI in the tree
<b>NRBC</b> CIST/MSTI New Root Bridges measures the number of times this module detected a new root bridge change

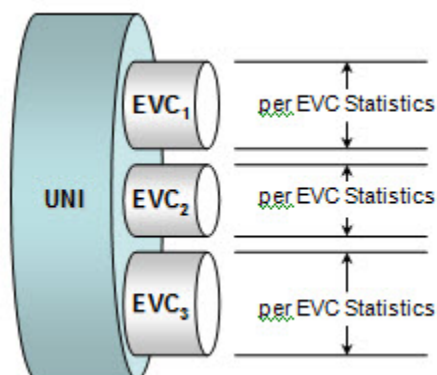
Table 13-9 MST Instance Port PMs (counters)

PM
<b>CIST/MSTI Forward Transitions</b> The number of times this port transition into forward state in CIST and/or MSTI
<b>CIST Protocol Migrations</b> The number of times this port transitions to support other version of spanning-tree
<b>Received BPDUs</b> The number of BPDUs received on this port for a particular MSTI instance
<b>Transmitted BPDUs</b> The number of BPDUs transmitted from this port for a particular MSTI instance
<b>Received BPDUs (Global Ports)</b> The number of BPDUs received on this port for the CIST
<b>Transmitted BPDUs (Global Ports)</b> The number of BPDUs transmitted from this port for the CIST
<b>Received Topology Change Notification BPDUs (Global Ports)</b> The number of Topology Change Notifications received on this port for the CIST
<b>Transmitted Topology Change Notification BPDUs (Global Ports)</b> The number of Topology Change Notifications transmitted from this port for the CIST
<b>Invalid BPDUs Received</b> The number of Invalid BPDUs received on this port and are dropped
<b>Invalid Configuration BPDUs Received (Global Ports)</b> The number of Invalid Configuration BPDUs received on this port and dropped
<b>Invalid Topology Change Notification BPDUs Received (Global Ports)</b> The number of Invalid Topology Change Notification received on this port and dropped

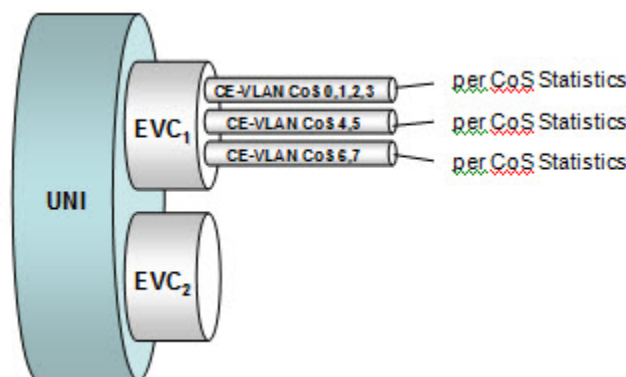
### 13.1.9 Ethernet Services PMs supported on packetVX modules

Ethernet service statistics are collected on all Ethernet services associated with a bandwidth profile, and include GbE and 10 GbE interfaces. Statistics are collected on a per Ethernet Virtual Circuit (EVC) and per Class of Service (CoS) basis.

The following figure shows performance monitoring (PM) statistics collection per EVC.



The following figure shows PM statistics collection per Class of Service.



Ethernet Service PM statistics support 32-bit and 64-bit counter type PMs for 15-minute, 24-hour and untimed intervals. Binning of historical PMs maintains 32 15-minute and one 24-hour bin.

Threshold Crossing Alerts (TCAs) are supported for the 15-minute and 24-hour bin for Rx/Tx bandwidth utilization PM only, and are associated with CIR and EIR. Since there are two threshold levels associated with the PM, there are two trigger points for TCAs. One TCA is generated when the CIR threshold is crossed and another when the EIR level is crossed.

**Table 13-10 Ethernet Service PMs (counters)**

PM
<b>Unavailable Seconds</b>
Unavailable Seconds measures the number of seconds during which the link was considered unavailable.

**Table 13-11 Ethernet Service Bandwidth Profile PMs (counters)**

<b>PM</b>
<b>octetstotal</b> Received or Transmitted Bytes (64-bit counter) measures the number of bytes received or transmitted.
<b>octetsvlt</b> Violate Frames (64-bit counter) measures the number of violate bytes received.
<b>octetscnfexc</b> Conform and Exceeded Bytes (64-bit counter) measures the number of conform and exceed bytes received.
<b>btwutlz</b> Bandwidth Utilization (32-bit counter) measures the bandwidth utilization for the interval.

### 13.1.10 ERPS PMs supported on packetVX modules

Table 13-12 ERPS Port PMs (counters)

PM
<b>Transmitted PDUs</b> Number of ERPS R-APS messages transmitted from this port
<b>Received PDUs</b> Number of ERPS R-APS messages received at this port
<b>Discarded PDUs</b> Number of EPRS R-APS messages discarded at this port
<b>Blocked State Transitions</b> Number of transitions of this port from unblocked state to blocked state
<b>Unblocked State Transitions</b> Number of transitions of this port from blocked state to unblocked state
<b>Failed State Transitions</b> Number of times this port transitioned to failed state
<b>Recoveries from Failed State</b> Number times this port recovered from failed state

### 13.1.11 Protocol threshold crossing alerts (TCAs) and ranges supported on packetVX modules

The following table lists the 15-minute and 1-day default threshold values for TCA-supported PMs for packetVX modules. The default 15-minute and 1-day ranges are as follows:

- Second-based montypes (e.g., ES, SES), 15-minute range = 0 to 899; 1-day range = 0 to 86400.
- All other montypes, 15-minute range = 0 to 38700; 1-day range = 0 to 215913600.

Protocol	PM	15-Minute default value	1-Day default value
<b>Layer 1 GE</b>	Coding Violations	382	3820
	Errored Seconds	25	250
	Severely Errored Seconds	4	40
<b>Layer 1 10GELAN</b>	Errored Seconds	25	250
	Severely Errored Seconds	4	40
	Invalid Blocks	382	3820
<b>Layer 1 10GE WAN PHY</b>	Invalid Blocks	382	3820
	Errored Seconds	25	250
	Severely Errored Seconds	4	40
	Unavailable Seconds	10	10
	Coding Violations - Section	382	3820
	Errored Seconds - Section	25	250
	Severely Errored Seconds - Section	4	40
	Unavailable Seconds - Section	10	10
	Severely Errored Framing Seconds - Section	2	8
	Coding Violations - Line	18336	183360
	Errored Seconds - Line	25	250
	Severely Errored Seconds - Line	4	40
	Unavailable Seconds - Line	10	10
	Coding Violations - Path	15	125
	Errored Seconds - Path	12	100
	Severely Errored Seconds - Path	3	7
	Unavailable Seconds - Path	10	10
<b>Layer 2 GE and 10GELAN</b>	Discarded Packets	0	0
	Frame Checksum Errors	0	0
	Received Packet Fragments	0	0

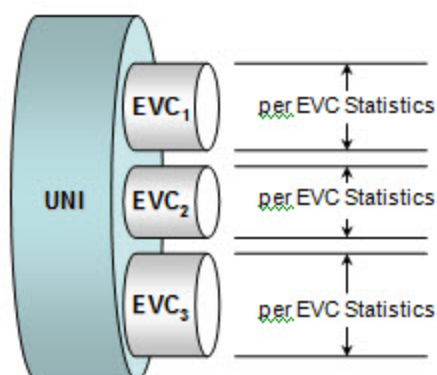
Protocol	PM	15-Minute default value	1-Day default value
	Oversized Packets (>9600 Bytes)	0	0
	Undersized Packets (<64 Bytes)	0	0
<b>Layer 1 OTN</b>	Uncorrectable Codewords	10	100
	OTU Errored Blocks	0	0
	OTU Background Block Errors	382	3820
	OTU Errored Seconds	25	250
	OTU Severely Errored Seconds	4	40
	OTU Out-of-Frame Seconds	2	8
<b>Ethernet Service Bandwidth Profile</b>	Bandwidth Utilization	0	0



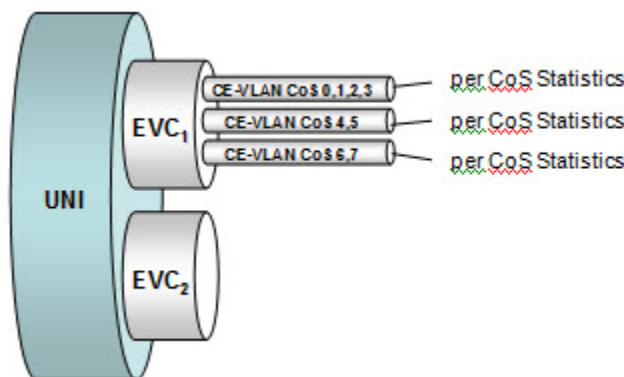
## 13.2 Ethernet service performance monitoring statistics

Ethernet service statistics are collected on all Ethernet services associated with a bandwidth profile, and include GbE and 10 GbE interfaces. Statistics are collected on a per Ethernet Virtual Circuit (EVC) and per Class of Service (CoS) basis.

The following figure shows performance monitoring (PM) statistics collection per EVC.



The following figure shows PM statistics collection per Class of Service.



Ethernet Service PM statistics support 32-bit and 64-bit counter type PMs for 15-minute, 24-hour and untimed intervals. Binning of historical PMs maintains 32 15-minute and one 24-hour bin.

Threshold Crossing Alerts (TCAs) are supported for the 15-minute and 24-hour bin for Rx/Tx bandwidth utilization PM only, and are associated with CIR and EIR. Since there are two threshold levels associated with the PM, there are two trigger points for TCAs. One TCA is generated when the CIR threshold is crossed and another when the EIR level is crossed.

## 13.2.1 Display Ethernet Service PM statistics per EVC

Use this procedure to retrieve Ethernet service PM statistics.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Note** Ethernet service PM statistics are supported on the ingress direction and on UNI Eservices only.

PM statistics can be viewed from within the Eservice as well as by using the CLI commands.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows;

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows;

```
BTI7000(config)#
```

### Step 3 Select a virtual switch (optional).

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Enter the following command:

```
show uni-eservice uni <interface-type> <interface-id> eservice
<service-name> { ingress } pm
{ history { 15-min | 24-hour } |
interval { 15-min [bin <bin>] | 24-hour [bin <bin>] |
total } |}
```

where:

- <interface-type> is the interface type
- <interface-id> is the interface identifier

## Output example

```
BTI7000:sw1(config)# show uni-eservice uni gigabitEthernet 1/1/6 eservice ServiceA
ingress pm interval total
```

```
SW: 1, E-Service: ServiceA, UNI GigE 1/1/6
Interval: Untimed, Bin: Current
  ingress conform bytes           : 400817152
  ingress violate bytes (red)     : 111182848
  ingress total bytes             : 512000000
  ingress BW Util (%)             : 40.96
```

```
BTI7000:sw1(config)#
```

You have successfully completed this procedure.

## 13.2.2 Display Ethernet Service PM statistics per CoS

Use this procedure to retrieve Class of Service Ethernet Service PM statistics on Ethernet services associated with a bandwidth profile.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

- Set up the Class of Service.

<b>Note</b>	Ethernet service PM statistics are supported on the ingress direction only and on UNI Eservices only.
-------------	---

Ethernet service PM statistics are displayed when you enter the CLI command syntax specified in this procedure. PM statistics can be viewed from within the Eservice as well as by using the CLI commands.

Eservice per CoS PMs will not count until the class-map match is met.

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Select a virtual switch (optional)

To select a virtual switch, enter the following command syntax:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4** Enter the following command:

```
show uni-eservice uni <interface-type> <interface-id> eservice
<service-name> service-policy {ingress} <policy-name> class-map <class-
name> pm
{history {15-min|24-hour}|interval {15-min [bin <bin>]|24-hour [bin
<bin>]|total}|thresholds {15-min|24-hour}}
```

where:

- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <service-name> is the name of the Eservice
- <policy-name> is the name of the service-policy
- <class-name> is the name of the class-map
- <bin> is the specific interval to show

**Output Example 1 - Bandwidth profile used in the service policy**

```
BTI7000:sw1(config)# show profile bandwidth
bwprofile55
```

```
Profile Name: bwprofile55
```

```
Meter
```

```
Mode   : Two-rate TCM, Color Blind
CIR     : 1000448 Kbps
CBS     : 16 Kbytes
EIR     : 1000448 Kbps
EBS     : 16 Kbytes
```

```
BTI7000:sw1(config)#
```

**Output example 2 - 24 hour interval**

```
BTI7000:sw1(config)# show uni-eservice uni gigabitEthernet 1/1/3
eservice evplan service-policy ingress three class-map 10_3 pm
interval 24-hour
```

```
SW: 1, E-Service: evplan, UNI GigE 1/1/3, service-policy: three, Class-
map: 10_3
```

```
Interval: 24-hour, Bin: Current
```

```

ingress conform bytes           : 2017035356203
ingress violate bytes (red)     : 0
ingress total bytes             : 2017035356203
ingress BW Util (%)             : 48.1

```

### Output example 3 - 15 minute interval

```

BTI7000:sw1(config)# show uni-eservice uni gigabitEthernet 1/1/3
eservice evplan service-policy ingress three class-map 10_3 pm
interval 15-min

```

```

SW: 1, E-Service: evplan, UNI GigE 1/1/3, service-policy: three, Class-
map: 10_3

```

```

Interval: 15-min, Bin: Current
ingress conform bytes           : 25083610618
ingress violate bytes (red)     : 0
ingress total bytes             : 25083610618
ingress BW Util (%)             : 48.12

```

### Output example 4 - History 24 hour interval

```

BTI7000:sw1(config)# show uni-eservice uni gigabitEthernet 1/1/3
eservice evplan service-policy ingress three class-map 10_3 pm history
24-hour

```

```

SW: 1, E-Service: evplan, UNI GigE 1/1/3, service-policy: three, Class-
map: 10_3

```

```

Interval: 24-hour, Bin: Current
ingress conform bytes           : 2030690175016
ingress violate bytes (red)     : 0
ingress total bytes             : 2030690175016
ingress BW Util (%)             : 48.1

```

```

Interval: 24-hour, Bin: 1
ingress conform bytes           : 973956122909
ingress violate bytes (red)     : 0
ingress total bytes             : 973956122909
ingress BW Util (%)             : 41.44

```

You have successfully completed this procedure.

## 13.2.3 Display Ethernet Service PM Thresholds

Use this procedure to retireve Ethernet Service PM thresholds. These threshold values are used to trigger Threshold Crossing Alerts (TCA) when the Ethernet Service PM statistics reaches or exceeds the sets value.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Note** Ethernet service PM statistics are supported on ingress direction and UNI Eservices only.

**Step 1 Access the Privileged EXEC mode**

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

**Step 2 Access the Administration Configuration mode**

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

**Step 3 Select a virtual switch (optional).**

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Enter the following command:**

```
show uni-eservice uni <interface-type> <interface-id> eservice  
<service-name> service-policy {ingress} <policy-name> class-map <class-  
name> pm  
{history {15-min|24-hour}|interval {15-min [bin <bin>]|24-hour [bin  
<bin>]|total}|thresholds {15-min|24-hour}}
```

where:

- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <service-name> is the name of the Eservice
- <policy-name> is the name of the service-policy
- <class-name> is the name of the class-map
- <bin> is the specific interval to show

**Output example**

Default values are derived from the CIR and EIR of the bandwidth profile.

```
BTI7000:sw1(config)# show uni-eservice uni gig 1/1/19 eservice  
evplan31 service-policy ingress servicepolicy55 class-map classmap55
```

```
pm thresholds 15-min
```

```
SW: 1, E-Service: evplan31, UNI GigE 1/1/19, service-policy:
servicepolicy55, Class-map: classmap55
```

```
Interval: 15-min, Bin: 1
  ingress CIR BW Threshold (%) : 14.14
  ingress EIR BW Threshold (%) : 14.14
```

```
BTI7000:sw1(config)#
```

### Per EVC example

```
show uni-eservice uni <if-type> <if-id> eservice <name> {ingress} pm {
history <interval> { 15-min | 24-hour } | interval <interval> { 15-min
[bin <bin>] | 24-hour [bin <bin>] | total } | thresholds { 15-min | 24-
hour }
```

### Per CoS example

```
show uni-eservice uni <if-type> <if-id> eservice <name> service-policy
{ingress} <name> class-map <name> pm { history <interval> { 15-min |
24-hour } | interval <interval> { 15-min [bin <bin>] | 24-hour [bin
<bin>] | total } | thresholds { 15-min | 24-hour }
```

You have successfully completed this procedure.

## 13.2.4 Set the Ethernet service PM Threshold per Eservice

Use this procedure to set the Ethernet service PM Threshold per EVC.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- The port on the Ethernet interface must be created and a transceiver present in the port.
- The mode must be set to Ethernet Interface Configuration mode.

**Step 1** Enter the following command at the Eservice UNI level:

```
pm {15-min|24-hour} threshold <Rx bandwidth utilization> <value>
where
```

- <Rx bandwidth utilization> is cir-bw-util, eir-bw-util
  - cir-bw-util - sets the committed information rate threshold (% line rate)
  - eir-bw-util - sets the exceeded information rate threshold (% line rate)
- <value> is the threshold value

For example, the command string might be

```
pm 15-min threshold ingress cir-bw-util 80
```

You have successfully completed this procedure.

### 13.2.5 Set the Ethernet service PM Threshold per Class of Service

Use this procedure to set the Ethernet service PM Threshold per CoS.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The port on the Ethernet interface must be created and a transceiver present in the port.
- The mode must be set to Ethernet Interface Configuration mode.

**Step 1** Enter the following command at the Eservice UNI level:

```
pm {15-min|24-hour} threshold service-policy ingress <policy-name>  
class-map <class name> <Rx bandwidth utilization> <value>
```

where

- <Rx bandwidth utilization> is cir-bw-util, eir-bw-util
  - cir-bw-util - sets the committed information rate threshold (% line rate)
  - eir-bw-util - sets the exceeded information rate threshold (% line rate)
- <value> is the threshold value

For example, the command string might be

```
pm 15-min threshold service-policy ingress policy1 class-map class1  
cir-bw-util 80
```

You have successfully completed this procedure.

### 13.2.6 Clear Eservice PMs per EVC

Use this procedure to clear Eservice performance monitor counter bins for an Ethernet interface per EVC.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:



```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Select a virtual switch (optional)

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Enter the following command:

```
clear uni-eservice uni <interface-type> <interface-id> eservice <service-name>
{ ingress } pm [ interval { all [bin current [<mon-type>]] | total [<mon-type>] | 15-
min [bin { all [<mon-type>] | current [<mon-type>] |
<bin> [<mon-type>] } ] | 24-hour [bin { all [<mon-type>] | current [<mon-type>] |<bin>
[<mon-type>] } ] ]
```

where

- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <bin #> is the historical bin identifier
- <montype> is each montype (or all) to clear

#### Per EVC example

```
clear uni-eservice uni gig 1/1/6 eservice evpline ingress pm interval
total
```

You have successfully completed this procedure.

## 13.2.7 Clear Eservice PMs per CoS

Use this procedure to clear Eservice performance monitor counter bins for an Ethernet interface per Class of Service.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode enter, the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

### Step 3 Select a virtual switch (optional).

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Enter the following command:

```
clear uni-eservice uni <interface-type> <interface-id> eservice <service-name> service-  
policy ingress <policy name> class-map <class name> pm [ interval { all [bin current  
[<mon-type>]] | total [<mon-type>] | 15-min [bin { all [<mon-type>] | current [<mon-  
type>] | <bin> [<mon-type>] } ] | 24-hour [bin { all [<mon-type>] | current [<mon-type>] |  
<bin> [<mon-type>] } ] } ]
```

where

- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <bin #> is the historical bin identifier
- <montype> is each montype (or all) to clear

**Per CoS example 1**

```
clear uni-eservice uni gig 1/1/3 eservice evplan service-policy ingress three class-map  
10_3 pm interval all
```

**Per CoS example 2**

```
clear uni-eservice uni gig 1/1/1 eservice evplan1 service-policy ingress servicepolicy1  
class-map classmap1 pm interval all
```

You have successfully completed this procedure.

## 13.3 Displaying and clearing performance monitor counts on packetVX modules

This section provides information about displaying and clearing performance monitor counts for Ethernet interfaces, and LACP and MSTP BPDU counts on packetVX modules.

### 13.3.1 Display performance monitor counts for an Ethernet interface

Use this procedure to display performance monitor counts for an Ethernet interface.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Pre-requisites:

- The Ethernet interface must be created and a transceiver present in the port.

**Note** For information about supported PMs, see [13.1, “Supported performance metrics”](#).

#### Step 1 Enter the following command:

```
show interfaces [<interface-type> <interface_id>]
```

where

- <interface-type> is the interface type
- <interface-id> is the interface identifier

For example, to display the total PM counts, the command string might be

```
show interfaces gigabitEthernet 1/1/1
```

You have successfully completed this procedure.

### 13.3.2 Display the performance monitor history for an Ethernet interface

Use this procedure explains display the performance monitor history for an Ethernet interface.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The port on the Ethernet switch must be provisioned and a transceiver present in the port.

#### Step 1 Enter the following command:

```
show interfaces <interface-type> <interface_id> pm history { 15-min | 24-hour } }
```

where

- <interface-type> is the interface type

- <interface-id> is the interface identifier

For example, to display all bins in a specific performance monitor counts interval, the command string might be

```
show interfaces gigabitEthernet 1/1/1 pm history 15-min
```

You have successfully completed this procedure.

### 13.3.3 Display the performance monitor interval for an Ethernet interface

Use this procedure to display the performance monitor interval for an Ethernet interface.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The port on the Ethernet interface must be created and a transceiver present in the port.

**Step 1** Enter the following command:

```
show interfaces <interface-type> <interface_id> pm interval { 15-min  
bin <bin> | 24-hour bin <bin> | total }
```

where

- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <bin #> is the bin interval to retrieve

For example, to display the current PM counts for an interval, the command string might be

```
show interfaces gigabitEthernet 1/1/1 pm interval 15-min
```

To display a specific bin in a PM counts interval, the command string might be

```
show interfaces gigabitEthernet 1/1/1 pm interval 15-min bin 1
```

You have successfully completed this procedure.

### 13.3.4 Display LACP BPDUs counts for a LAG

Use this procedure to display LACP BPDUs counts for a LAG.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The LAG must be provisioned.

**Note** For information about supported PMs, see [13.1, “Supported performance metrics”](#).

**Step 1** Enter the following command:

```
show lacp {<lag-id> | all} pm [ interval {15-min | 24-hour | total |  
all } [ bin {<bin #> | current | all } [ montype <montype> ] ] ]
```

where

- <lag-id> is the LAG identifier
- <bin #> is the bin interval to retrieve
- <montype> is the montype to retrieve

For example, to display the total LACP BPDU counts for a LAG, the command string might be

```
show lacp 2 pm interval total
```

To display a specific bin in a BPDU counts interval for a LAG, the command string might be

```
show lacp 2 pm interval 15-min bin 0
```

To display all bins in a specific BPDU counts interval for a LAG, the command string might be

```
show lacp 2 pm interval 15-min
```

To display a montype in a bin in a specific BPDU counts interval for a LAG, the command string might be

```
show lacp 2 pm interval 15-min bin 4 montype rx-lacpdu
```

You have successfully completed this procedure.

### 13.3.5 Display MSTP BPDU counts for the CIST

Use this procedure to display MSTP BPDU counts for the CIST.

The MSTP must be provisioned.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

The packetVX spanning-tree PM combines CIST and MSTP BPDU statistics on the interface as described in IEEE standard 802.1Q-2005, section 14.6 "Encoding and decoding of STP Configuration, RST and MST BPDUs."

**Note** For information about supported PMs, see [13.1, "Supported performance metrics"](#).

**Step 1** Enter the following command:

```
show spanning-tree pm {mst <instance-id> | cist } [ interface  
<interface-type> <interface-id> ] [ interval { 15-min | 24-hour | total  
| all } [ bin { <bin> | current | all } [montype <montype>] ] ]
```

where

- <instance-id> is the Spanning Tree Instance identification number
- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <bin #> is the bin interval to retrieve
- <montype> is the montype to retrieve

For example, to display the total BPDU counts, the command string might be

```
show spanning-tree pm cist interface gigabitEthernet 1/1/11 interval
total
```

To display a specific bin in a BPDU counts interval, the command string might be

```
show spanning-tree pm cist interface gigabitEthernet 1/1/11 interval
15-min bin 4
```

To display all bins in a specific BPDU counts interval, the command string might be

```
show spanning-tree pm cist interface gigabitEthernet 1/1/11 interval
15-min
```

To display a montype in a bin in a specific BPDU counts interval, the command string might be

```
show spanning-tree pm cist interface gigabitEthernet 1/1/11 interval
15-min bin 4 montype ftc
```

You have successfully completed this procedure.

### 13.3.6 Display MSTP BPDU counts for an MST instance

Use this procedure to display MSTP BPDU counts for an MST instance.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The MSTP must be provisioned. See [5.7.1, “MSTP provisioning”](#).

**Note** For information about supported PMs, see [13.1, “Supported performance metrics”](#).

**Step 1** Enter the following command:

```
show spanning-tree pm {mst <instance-id> | cist } [ interface
<interface-type> <interface-id> ] [ interval { 15-min | 24-hour | total
| all } ] [ bin { <bin> | current | all } ] [montype <montype>] ] ]
```

where

- <instance-id> is the Spanning Tree Instance identification number
- <interface-type> is the interface type
- <interface-id> is the interface identifier

- <bin #> is the bin interval to retrieve
- <montype> is the montype to retrieve

For example, to display the total BPDU counts for the MST instance, the command string might be

```
show spanning-tree pm mst 1 interface gigabitEthernet 1/1/11 interval total
```

To display a specific bin in a BPDU counts interval for the MST instance, the command string might be

```
show spanning-tree pm mst 1 interface gigabitEthernet 1/1/11 interval 15-min bin 4
```

To display all bins in a specific BPDU counts interval for the MST instance, the command string might be

```
show spanning-tree pm mst 1 interface gigabitEthernet 1/1/11 interval 15-min
```

To display a montype in a bin in a specific BPDU counts interval for the MST instance, the command string might be

```
show spanning-tree pm mst 1 interface gigabitEthernet 1/1/11 interval 15-min bin 4 montype ftc
```

You have successfully completed this procedure.

### 13.3.7 Display MSTP Topology Change counts for an MST instance

Use this procedure to display MSTP Topology Change counts for an MST instance.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The MSTP must be provisioned.

**Note** For information about supported PMs, see [13.1, “Supported performance metrics”](#).

**Step 1** Enter the following command:

```
show spanning-tree pm {mst <instance-id> | cist } [ interface <interface-type> <interface-id> ] [ interval { 15-min | 24-hour | total | all } ] [ bin { <bin> | current | all } ] [ montype <montype> ] ]
```

where

- <instance-id> is the Spanning Tree Instance identification number
- <interface-type> is the interface type
- <interface-id> is the interface identifier



- <bin #> is the bin interval to retrieve
- <montype> is the montype to retrieve

For example, to display the total Topology Change counts for an MST instance, the command string might be

```
show spanning-tree pm mst 1 interval total
```

To display a specific bin in a Topology Change counts intervals for an MST instance, the command string might be

```
show spanning-tree pm mst 1 interval 15-min bin 4
```

To display all bins in a specific Topology Change counts intervals for an MST instance, the command string might be

```
show spanning-tree pm mst 1 interval 15-min
```

To display a montype in a bin in a specific Topology Change counts intervals for an MST instance, the command string might be

```
show spanning-tree pm mst 1 interval 15-min bin 4 montype tcc
```

You have successfully completed this procedure.

### 13.3.8 Clear LACP BPDU counts

Use this procedure to clear LACP BPDU counts for a LAG.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The LAG must be provisioned.

**Step 1** Enter the following command:

```
clear lacp {<lag-id> | all} pm [ interval {15-min | 24-hour | total |  
all } [ bin {<bin #> | current | all } [ montype <mon-type> ] ] ]
```

where

- <lag-id> is the LAG identifier
- <bin #> is the bin interval to retrieve
- <montype> is the montype to retrieve

For example, to clear all BPDU counts for a LAG, the command string might be

```
clear lacp 1 pm
```

or

```
clear interfaces lag 1 pm
```

To clear all BPDU counts for an interval, the command string might be

```
clear lacp 1 pm interval 15-min
```

or

```
clear interfaces lag 1 pm interval 15-min
```

To clear all BPDU counts for a bin, the command string might be

```
clear lacp 1 pm interval 15-min bin 3
```

or

```
clear interfaces lag 1 pm interval 15-min bin 3
```

To clear all BPDU counts for a performance metric, the command string might be

```
clear lacp 1 pm interval 15-min bin 3 montype rx-lacpdu
```

or

```
clear interfaces lag 1 pm interval 15-min bin 3 montype rx-lacpdu
```

You have successfully completed this procedure.

### 13.3.9 Clear MSTP BPDU counts for the CIST

Use this procedure to clear MSTP BPDU counts for the CIST.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The MSTP must be provisioned.

**Step 1** Enter the following command:

```
clear spanning-tree pm {mst <instance-id> | cist } [ interface  
<interface-type> <interface-id> ] [ interval { 15-min | 24-hour |  
total | all } [ bin { <bin> | current | all } [ montype <mon-type>] ] ]
```

where

- <instance-id> is the Spanning Tree Instance identification number
- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <bin #> is the bin interval to clear
- <montype> is the montype to clear

For example, to clear all BPDU counts for the CIST, the command string might be

```
clear spanning-tree pm cist
```

To clear all BPDU counts for an interval, the command string might be

```
clear spanning-tree pm cist interval 15-min
```

To clear all BPDU counts for a specific interface and interval, the command string might be

```
clear spanning-tree pm cist interface gigabitEthernet 1/1/1 interval
15-min
```

To clear all BPDU counts for an interface, the command string might be

```
clear spanning-tree pm cist interface gigabitEthernet 1/1/1
```

To clear all BPDU counts for a bin, the command string might be

```
clear spanning-tree pm cist interface gigabitEthernet 1/1/1 interval
15-min bin 4
```

or

```
clear spanning-tree pm cist interval 15-min bin 4
```

To clear all BPDU counts for a performance metric, the command string might be

```
clear spanning-tree pm cist interface gigabitEthernet 1/1/1 interval
15-min bin 3 montype ftc
```

or

```
clear spanning-tree pm cist interval 15-min bin 3 montype ftc
```

You have successfully completed this procedure.

### 13.3.10 Clear MSTP BPDU counts for an MST instance

Use this procedure to clear MSTP BPDU counts for an MST instance.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The MSTP must be provisioned.

**Step 1** Enter the following command:

```
clear spanning-tree pm {mst <instance-id> | cist } [ interface
<interface-type> <interface-id> ] [ interval { 15-min | 24-hour |
total
| all } [ bin { <bin> | current | all } [ montype <mon-type>] ] ]
```

where

- <instance-id> is the Spanning Tree Instance identification number
- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <bin #> is the bin interval to clear
- <montype> is the montype to clear

For example, to clear all BPDU counts for an interface, the command string might be

```
clear spanning-tree pm mst 1 interface gigabitEthernet 1/1/1
```

To clear all BPDU counts for an interval, the command string might be

```
clear spanning-tree pm mst 1 interface gigabitEthernet 1/1/1 interval 15-min
```

To clear all BPDU counts for a bin, the command string might be

```
clear spanning-tree pm mst 1 interface gigabitEthernet 1/1/1 interval 15-min bin 4
```

To clear all BPDU counts for a performance metric, the command string might be

```
clear spanning-tree pm mst 1 interface gigabitEthernet 1/1/1 interval 15-min bin 3 montype ftc
```

You have successfully completed this procedure.

### 13.3.11 Clear MSTP Topology Change counts for an MST instance

Use this procedure to clear MSTP Topology Change counts for an MST instance.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The MSTP must be provisioned.

**Step 1** Enter the following command:

```
clear spanning-tree pm {mst <instance-id> | cist } [ interface <interface-type> <interface-id> ] [ interval { 15-min | 24-hour | total | all } [ bin { <bin> | current | all } [ montype <mon-type>] ] ]
```

where

- <instance-id> is the Spanning Tree Instance identification number
- <interface-type> is the interface type
- <interface-id> is the interface identifier
- <bin #> is the bin interval to clear
- <montype> is the montype to clear

For example, to clear all Topology Change counts for an MST instance, the command string might be

```
clear spanning-tree pm mst 1
```

To clear all Topology Change counts for an interval, the command string might be

```
clear spanning-tree pm mst 1 interval 15-min
```

To clear all Topology Change counts for a bin, the command string might be

```
clear spanning-tree pm mst 1 interval 15-min bin 4
```

To clear all Topology Change counts for a performance metric, the command string might be

```
clear spanning-tree pm mst 1 interval 15-min bin 3 montype tcc
```

You have successfully completed this procedure.

## 13.4 Displaying and setting Threshold Crossing Alerts on packetVX modules

Threshold Crossing Alerts (TCAs) are autonomously reported events that signal to the management system that the value of a counter-type performance-metric (PM) parameter has reached or exceeded a preset threshold. TCAs are supported for each monitored parameter for the protocol configured, for both the current 15-minute and 24-hour bins.

You can display the TCAs for each interface created on a packetVX module. When an interface is created, default TCAs are provided. However, you can set the level of any TCA to a value that falls within its allowed range.

### 13.4.1 Display the performance monitor TCAs for an Ethernet interface

Use this procedure to display the performance monitor TCAs for Ethernet interfaces.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The port on the Ethernet interface must be created and a transceiver present in the port.

**Step 1** Enter the following command:

```
show interfaces <interface-type> <interface-id> pm threshold {15- min | 24-hour}
```

where

- <interface-type> is the interface type
- <interface-id> is the interface identifier

For example, the command string might be

```
show interfaces gigabitEthernet 1/1/1 pm threshold 15-min
```

You have successfully completed this procedure.

### 13.4.2 Set the performance monitor threshold for TCAs

Use this procedure to set the performance monitor threshold for Threshold Crossing Alerts (TCAs).

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

#### Prerequisites

- The port on the Ethernet interface must be created and a transceiver present in the port.
- The mode must be set to Ethernet Interface Configuration mode.

**Step 1** Enter the following command:

```
pm {15-min|24-hour} threshold <monitor-type> <value>
```

where

- <monitor-type> is the interval to retrieve
- <value> is the threshold value

For example, the command string might be

```
pm 15-min threshold discards 1000
```

You have successfully completed this procedure.





## 14.0 Replacing BTI™ packetVX® modules and transceivers

---

This section provides instructions for replacing BTI packetVX modules and transceivers.

- [14.1, “Replacing packetVX modules”](#)
- [14.2, “Replacing optical transceivers”](#)
- [14.3, “Replacing copper transceivers”](#)

## 14.1 Replacing packetVX modules

---

Use this procedure to replace a packetVX module.

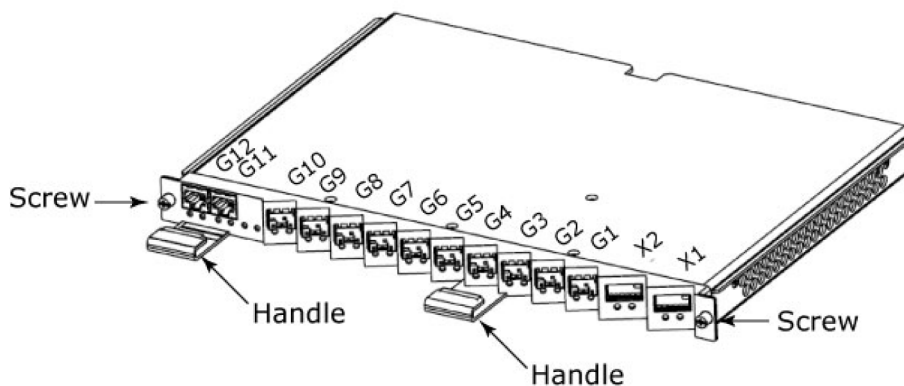
### What you need

- Slot-head or Phillips screwdriver
- Electrostatic discharge (ESD) wrist strap
- packetVX module
- Isopropyl alcohol and lint-free pads

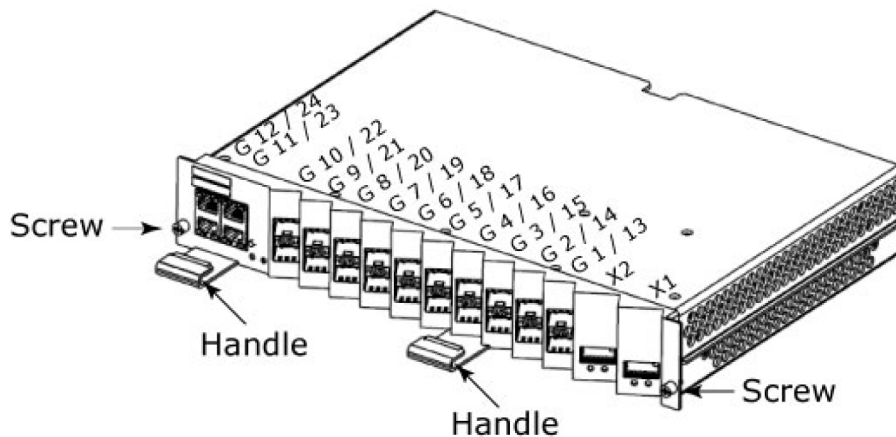
### Key module replacement features

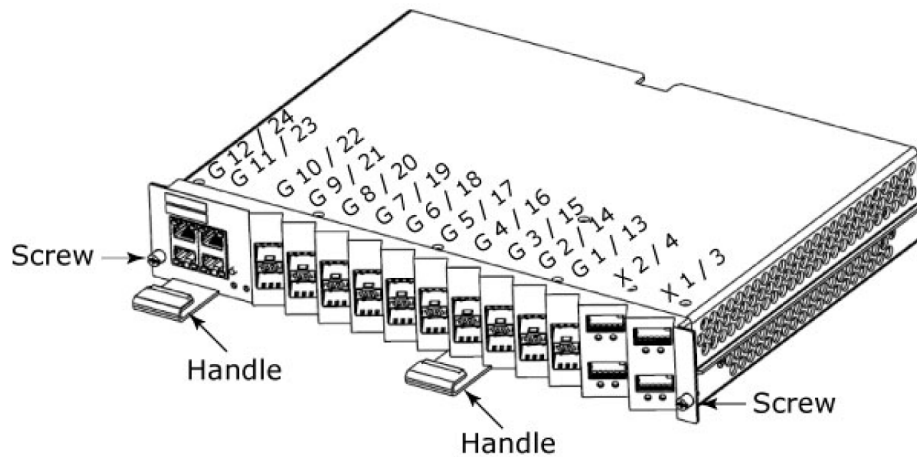
The following figures show the key features of the packetVX modules and indicate the key features for replacing them.

**Figure 14-1 packetVX module BT7A81AA 12/2**



**Figure 14-2 packetVX BT7A81BA 24/2 module**



**Figure 14-3 packetVX module BT7A81CA 24/4****Replacement procedure**

Follow these steps to replace a packetVX module:

**Step 1 Reroute Traffic**

**Caution** Failure to reroute traffic can result in lost data. Select an alternate route for the traffic that passes through the module. Transfer traffic to this alternate route before proceeding with this procedure.

**Step 2 Move the Cables**

Shelf cables may need to be moved aside to get clear access to the module. The cables rest on the handles that are at the front of the module.

**Step 3 Disconnect the Cables**

Disconnect the optical cables from the ports on the faceplate of the module.

**Note** Ensure that the optical ports on the module and the optical cables are protected with protective caps while disconnected.

**Step 4 Loosen the Faceplate Screws**

- a) Facing the front of the shelf, locate the faceplate screws.
- b) Using a slot-head or Phillips screwdriver, loosen the screws.

**Step 5 Remove the Module**

- a) Grasp the handles on the front of the module and firmly pull the module straight out.

**Note** An equipment missing alarm appears once you remove the module.

- b) Place the module on a flat work surface.

**Step 6 Replace the Module**

- a) Align the replacement module to the slot in which the module is being inserted.
- b) Carefully push the module straight into the slot.

#### **Step 7 Replace the Faceplate Screws**

- a) Facing the front of the shelf, align the module with its mounting holes.
- b) Using a slot-head or Phillips screwdriver, carefully tighten the faceplate screws:
  - Partially tighten the first screw.
  - Partially tighten the other screw.
  - Fully tighten the first screw.
  - Fully tighten the other screw.

**Caution** Tighten with no more than 4.7 in-lbs of torque.

#### **Step 8 Replace the SFP or XFP Transceivers**

See [14.2, “Replacing optical transceivers”](#) and [14.3, “Replacing copper transceivers”](#) to insert the SFPs or XFPs into the module, and then return to this procedure.

#### **Step 9 Reconnect Optical Cables**

Clean the optical cables and then reconnect them to their original positions.

**Note** If you loop excess fiber around the fiber management spool, allow sufficient slack for the fiber management spool to move freely.

#### **Step 10 Replace Cables**

If any cables were moved to access the module, replace the cables to their original locations.

You have successfully completed this procedure.

## 14.2 Replacing optical transceivers

Use this procedure to replace optical small form factor (SFP) or 10 Gb/s (XFP) transceivers.

### What you need

- Electrostatic discharge (ESD) wrist strap
- Replacement transceiver
- Isopropyl alcohol and lint-free pads

### Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.



Invisible laser radiation can be emitted from the aperture ports of various modules when no fiber cable is connected. Avoid exposure and do not stare into open apertures to avoid permanent eye damage.

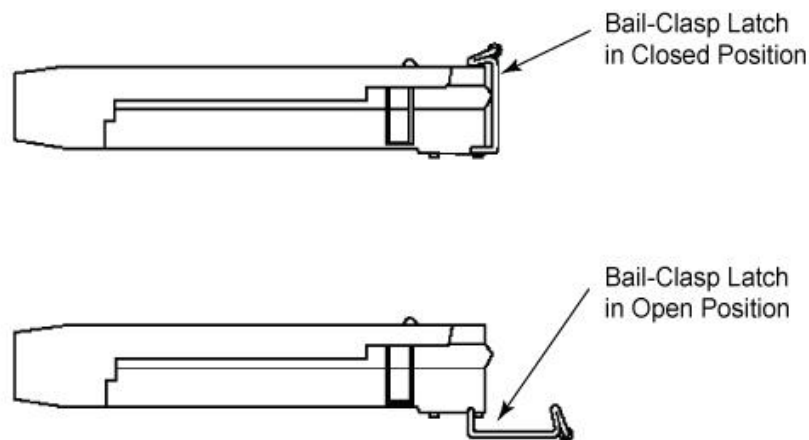


Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

### Transceiver key features

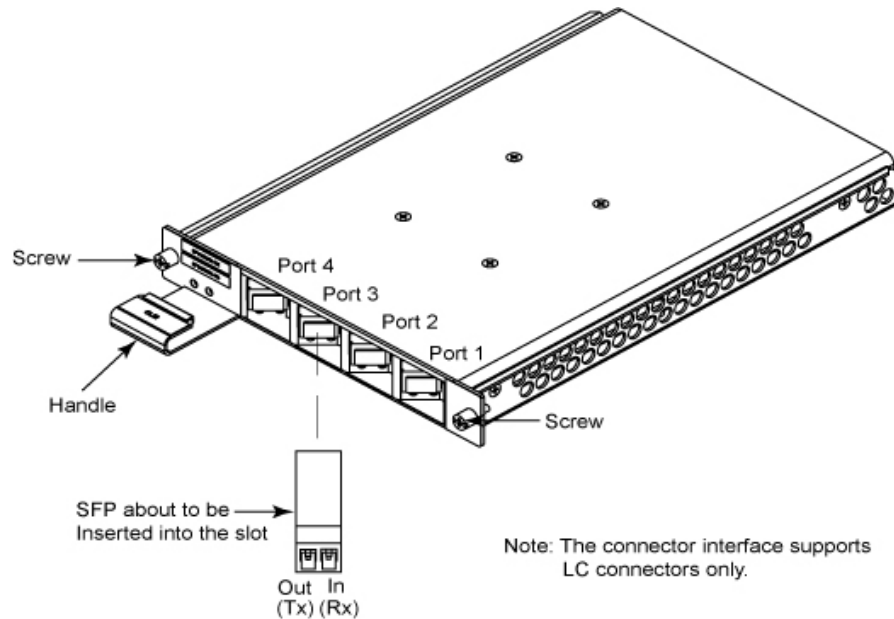
The following figure shows a typical SFP transceiver with a bale-clasp latch.

#### SFP transceiver with a bale-clasp latch



The following figure shows an SFP transceiver about to be inserted into its slot in a generic module.

### Transceiver insertion



### Replacement procedure

Follow these steps to replace a transceiver:

#### Step 1 Reroute Traffic

**Caution** Failure to reroute traffic can result in lost data. Select an alternate route for the traffic that passes through the module. Transfer traffic to this alternate route before proceeding with this procedure.

#### Step 2 Remove the Transceiver Port from Service

Remove the port from service.

#### Step 3 Move the Cables

Shelf cables may need to be moved aside to get clear access to the transceiver. The cables rest on the handles that are at the front of the circuit pack.

#### Step 4 Disconnect the Optical Cables

Disconnect the optical cables from the optical ports of the transceiver. Label the cables transmit and receive so that you can reconnect them to the correct ports later in this procedure.

**Note** Ensure that the optical ports on the transceiver and the optical cables are protected with protective caps while disconnected.

**Step 5 Disengage the Latch Handle**

Facing the front of the shelf, locate the latch handle on the transceiver. For a bale-clasp latch, pull the latch handle down until it is at a 90-degree angle to the transceiver.

**Step 6 Remove the Transceiver**

- a) Grasp the latch handle on the transceiver and firmly pull the transceiver straight out.

**Note** If the transceiver port is provisioned, an alarm (REPLUNITMISS) appears and the red LED turns on once you remove the transceiver.

- b) Place the transceiver into anti-static packaging and then lay it on a flat work surface.

**Step 7 Insert the Replacement Transceiver**

- a) Hold the transceiver so that the optical connectors face you. On an SFP, the product label will be visible. On an XFP, the product label is not visible.
- b) Ensure that the latch handle is in the closed position. For a bale-clasp latch, this is in the upright position.
- c) Align the transceiver to the port in which it is being inserted.
- d) Carefully slide the transceiver straight into the port until it clicks.

**Note** If the port is provisioned and the replacement transceiver has the same the wavelength, the REPLUNITMISS alarm clears.

**Note** If the port is provisioned, but the replacement transceiver has a different wavelength, the mismatch alarm (REPLUNITMEA) appears and the red LED turns on.

- e) Remove the plastic protective cover, if fitted.

**Step 8 Clean the Ends of the Fiber Optic Cables**

Use lint-free pads with isopropyl alcohol to clean the ends of the fiber optic cables.

**Step 9 Connect the Optical Cables**

**Note** Before connecting the optical cables to the transceiver, ensure that both the optical cable connectors and the optical surfaces are clean and that there is no residue on the optical surfaces.

Connect the input and output optical cables to the transceiver as follows:

- a) Ensure that the latch handle (or bale) of the transceiver is in the closed (up) position.
- b) Carefully slide the bottom of the male optical connector along the bottom of the transceiver opening.
- c) Gently push the male optical connector into the opening until a distinctive click is heard. Then continue exerting pressure on the connector to ensure a good connection is achieved.

**Step 10 Restore the Transceiver Port to Service**

**Important** XFPs and DWDM SFPs take about 90 seconds to reach a stable operating temperature. As a result, the REPLUNITFAIL (SFP or XFP Failure) alarm is disabled for 95 seconds after a transceiver is seated. If there is a transceiver hardware fault, the REPLUNITFAIL alarm is raised subsequent to the 95-second time delay.

### **Step 11 Replace the Cables**

If any cables were moved to access the transceiver, replace the cables to their original locations.

You have successfully completed this procedure.



## 14.3 Replacing copper transceivers

Use this procedure to replace copper (electrical) small form factor pluggable (SFP) transceivers.

### What you need

- Electrostatic discharge (ESD) wrist strap
- Replacement SFP transceiver

### Prerequisites

To prevent potential damage from electrostatic discharge, observe the following when handling transceivers:

- Do not remove a transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of a transceiver.
- Always store or transport a transceiver in anti-static packaging.

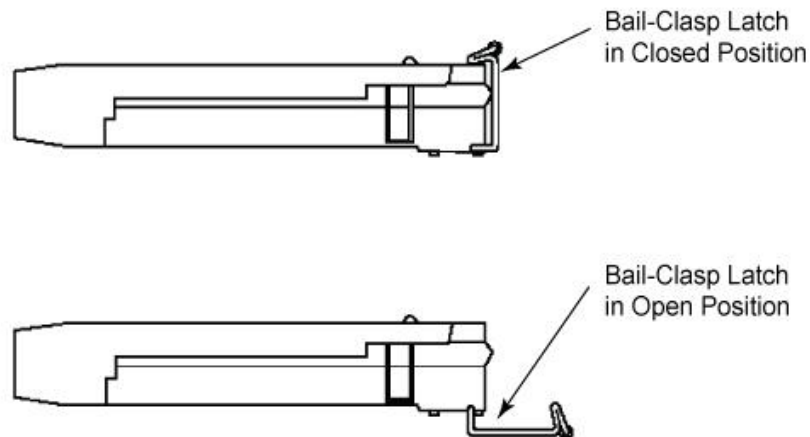


**Caution**

Use an ESD wrist strap whenever you open the equipment, particularly when you are handling modules as well as SFP and XFP transceivers. To work properly, the wrist strap must make good contact at both ends (that is, with your skin at one end and with the chassis at the other).

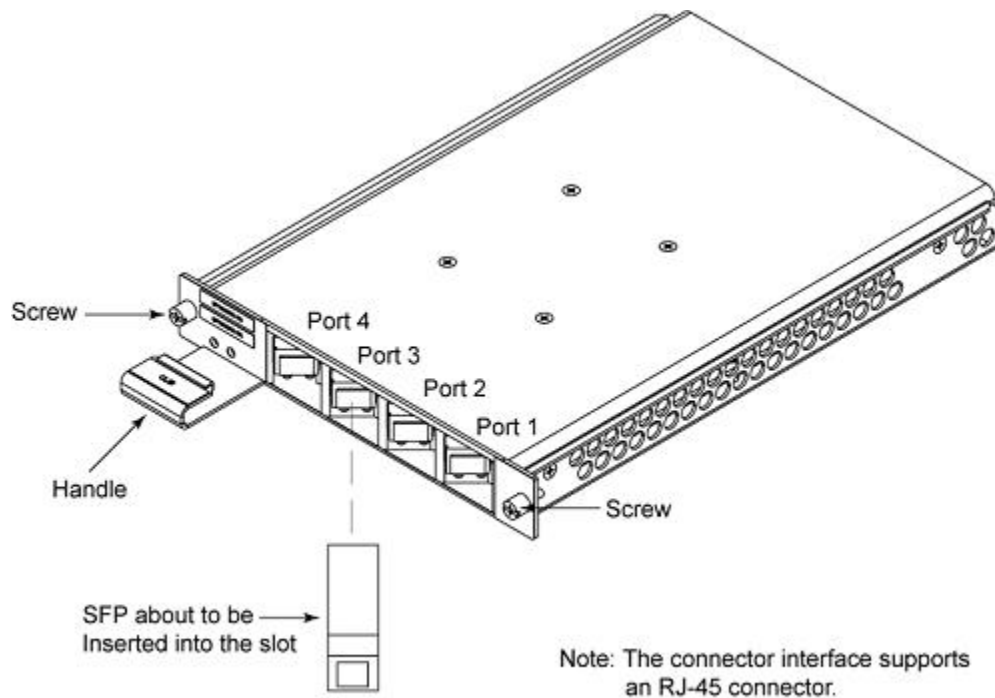
The following figure shows a typical SFP transceiver with a bale-clasp latch.

**Figure 14-6 SFP Transceiver key features**



The following figure shows a copper SFP transceiver about to be inserted into its slot in a generic module.

**Figure 14-7 Copper SFP insertion into a generic module**



To prevent potential damage from electrostatic discharge, observe the following when handling SFP transceivers:

- Do not remove an SFP transceiver from its packaging until you are ready to install it into a module.
- Do not touch any of the pins, connections, or components of an SFP transceiver.
- Always store or transport an SFP transceiver in anti-static packaging.

## Procedure

### Step 1 Reroute Traffic

**Important** Failure to reroute traffic can result in lost data. Select an alternate route for the traffic that passes through the SFP transceiver and then transfer traffic to the alternate route before proceeding with this procedure.

### Step 2 Remove SFP port from service

### Step 3 Move Cables

Shelf cables may need to be moved aside to get clear access to the SFP transceiver. The cables rest on the handles that are at the front of the module.

### Step 4 Disconnect Cable

Disconnect the electrical cable from the electrical (RJ45) port of the SFP transceiver.

**Step 5 Disengage Latch Handle**

Facing the front of the module, locate the latch handle on the SFP transceiver. For a bale-clasp latch, pull the latch handle down until it is at a 90-degree angle to the transceiver.

**Step 6 Remove Transceiver**

- a) Grasp the latch handle on the SFP transceiver and firmly pull the transceiver straight out.

**Note** If the SFP transceiver port is provisioned, an SFP missing alarm (REPLUNITMISS) appears and the red LED turns on once you remove the transceiver.

- b) Place the SFP transceiver into anti-static packaging and then lay it on a flat work surface.

**Step 7 Insert the SFP Replacement Transceiver**

- a) Hold the SFP transceiver so that the RJ45 connector faces you and the product label is visible.
- b) Ensure that the latch handle is in the closed position. For a bale-clasp latch, this is in the upright position.
- c) Carefully slide the SFP transceiver straight into the port until it clicks.

**Note** If you are going from an optical to an electrical SFP, provision a wavelength with a value of 0.

- d) Remove the plastic protective cover, if fitted.

**Step 8 Connect an RJ45 Cable to the Transceiver**

Connect an RJ45 cable to each electrical SFP transceiver as follows:

- a) Ensure that the latch of the SFP transceiver is in the closed position
- b) Push the RJ45 connector into the SFP transceiver until a distinctive click is heard.

**Note** A Link Down alarm can occur when no signal is connected to the transceiver. To clear a Link Down alarm, refer to the *Alarm and Troubleshooting Guide*.

**Step 9 Restore SFP Port to Service****Step 10 Replace Cables**

If any cables were moved to access the SFP transceiver, replace the cables to their original locations.

You have successfully completed this procedure.



## 15.0 Alarms and events on BTI™ packetVX®modules

---

The BTI proNX 900 Node Controller allows you to view alarms and events reported on a packetVX module at any time.

Any fault condition pertaining to the module is reported as an autonomous alarm. For information about clearing alarms pertaining to packetVX modules, see the *Alarm and Troubleshooting Guide*.

An event reported on a packetVX module can indicate the module's status, a periodic report of information, or asynchronous command completion information.

The following are the alarms supported on either packetVX modules or ports:

- AIS-L (Line Alarm Indication Signal)
- LOS (Loss of Signal for FC or GE client-side port)
- LOSYNC (Loss of Synchronization for FC or GE client-side port)
- REPLUNITFAIL (Circuit Pack, SFP/XFP Failure)
- REPLUNITMEA (SFP or XFP Mismatch)
- REPLUNITMISS (SFP or XFP Missing)
- REPLUNITUNK (Circuit Pack, SFP/XFP Unknown)
- T-OPR-HT (OPR High Threshold)
- T-OPR-LT (OPR Low Threshold)
- T-OPT-HT (OPT High Threshold for SFP or XFP)
- T-OPT-LT (OPT Low Threshold for SFP)
- WNA (Wavelength Not Achievable)



## **Appendix A: Using BTI™ proNX 900 to provision and monitor packetVX® modules**

---

This section provides the proNX 900 provisioning procedures that are required to initialize and maintain a packetVX module and its software.

## A.1 Provisioning packetVX modules

---

packetVX modules can be provisioned before they are physically present in the shelf.

### Provisioning settings and custom settings

When you provision a packetVX module, you specify settings such as its name and its Product Equipment Code (PEC), and provide brief identification information about the module. You can also provision custom information to record information specific to your environment. For example, you may want to record information about equipment usage, upgrades, and maintenance.

A packetVX module must be provisioned before a port on the module can be provisioned. When a module is physically present in the shelf, the system checks whether the module type matches the provisioned packetVX module type. If the inserted module type does not match the provisioned module type, an equipment mismatch alarm is raised. The alarm clears when the proper module type is inserted or when the provisioning data is updated to resolve the mismatch.

### Displaying module information

Once a packetVX module is provisioned, you can view the specified settings and inventory information, such as, the module's hardware release number and date of manufacture.

### Navigating the packetVX module

From the Packet Ethernet view, which is accessed from the View menu or the Packet Ethernet button on the toolbar, you can view and provision the switch components.

In the Navigation tree on the left side, expand the tree and view sub-items by clicking the plus sign (+) beside an object. To collapse the tree and hide sub-items, click the minus sign (-) beside an object.

### Removing and restoring service

A packetVX module should be removed from service before it is deleted, so that alarms are not raised. A module that has been removed from service can be restored to service.

### Restarting a module

packetVX modules support only cold restarts. A cold restart recycles the power on the module and is service affecting.

### Deleting a module

If you want to change the type of packetVX module that is either preprovisioned or physically present in a shelf, you must first delete it.



## A.1.1 Provision packetVX module settings

### Prerequisites

- The shelf is provisioned.
- The shelf is configured for either a double-width slot or a double-width-double-height slot, depending on the module to be provisioned.

### Provisioning module settings

Follow these steps to provision settings for a packetVX module:

- Step 1** In the toolbar, click the System Configuration icon. The System Configuration view of the shelf displays in the Navigation pane.
- Step 2** In the Navigation pane, right-click a double-width slot or a double-width, double-height slot, and then click **Provision Module**.
- Step 3** On the **Settings** tab of the **Provision Module** dialog, click **PVX** in the **Name** list.  
The first available Product Equipment Code (PEC) and, if available, the Common Language Equipment Identification (CLEI) code for the selected module type automatically appear in the **PEC/CLEI** list.
- Step 4** Select the PEC for the module type from the **PEC/CLEI** list.
- Step 5** Optionally, enter information (up to 20 alphanumeric characters) about the module in the **ID** field.
- Step 6** Choose one of the following from the **State Management** list:
- **IS** — to set the state of the module to In Service
  - **OOS** — to set the state of the module to Out of Service
- Step 7** Optionally, click the **Custom Settings** tab, and then enter information in any of the **Custom** fields.
- Step 8** Click **Apply**, and then click **Close**.  
The discovery process for packetVX functionality initiates. When the process is completed, the Slot PVX folder can be expanded.

You have successfully completed this procedure.

## A.1.2 Display module information

- The packetVX module is installed in the shelf.

### Displaying module settings

Follow these steps to view parameters for a packetVX module:

**Step 1** In the toolbar, click the System Configuration icon. The System Configuration view of the shelf displays in the Navigation pane.

**Step 2** In the Navigation pane, right-click a packetVX module, and then click **Display Module Inventory**.

The **Display Inventory Information** dialog displays **General**, **Hardware**, **Manufacturing**, and **Testing** parameters for the module. See [Table A-1](#).

**Step 3** Click **Close**.

You have successfully completed this procedure.

**Table A- 1 Module inventory information**

Type	Parameter	Description
<b>General</b>	Full Name	Official name of the module
	Name	Short name of the module
	Shelf Number	The shelf in which the module is installed
	Slot Number	The slot in which the module is installed
<b>Hardware</b>	PEC Code	The product equipment code assigned by the manufacturer
	Serial Number	The serial number of the module
	CLEI Code	The Common Language Equipment Identifier number assigned by Telcordia. The CLEI identifies the physical hardware.
	Release Number	The hardware release number
	Firmware	The firmware number
	USI	The unique serial identifier
<b>Manufacturing</b>	Manufacturing Date	The date that the module was manufactured
	Manufacturing Location	The location where the module was manufactured
<b>Testing</b>	Testing Date	The date that the manufacturer tested the module
	Testing Location	The location where the manufacturer tested the module

### A.1.3 Remove a module from service

#### Prerequisites

- The packetVX module is provisioned and in service.

#### Removing a module from service

Follow these steps to remove a packetVX module from service:

- Step 1** In the toolbar, click the System Configuration icon. The System Configuration view of the shelf displays in the Navigation pane.
- Step 2** In the Navigation pane, right-click a module, and then click **Provision Module**.
- Step 3** On the **Settings** tab of the **Provision Module** dialog, click the Remove button beside the **State** field.
- Step 4** In the **Remove Entity** dialog, click **Yes**.
- Step 5** Click **Close**.

You have successfully completed this procedure.

### A.1.4 Restore a module to service

#### Prerequisites

- The packetVX module is provisioned and out of service.

#### Restoring a module to service

Follow these steps to restore a packetVX module to service:

- Step 1** In the toolbar, click the System Configuration icon. The System Configuration view of the shelf displays in the Navigation pane.
- Step 2** In the Navigation pane, right-click a module, and then click **Provision Module**.
- Step 3** On the **Settings** tab of the **Provision Module** dialog, click the **Restore** button beside the **State** field.
- Step 4** Click **Close**.

You have successfully completed this procedure.

## A.1.5 Restart a module

### Prerequisites

- The packetVX module is provisioned.

### Restarting a module

Follow these steps to restart a packetVX module:

- Step 1** In the toolbar, click the System Configuration icon. The System Configuration view of the shelf displays in the Navigation pane.
- Step 2** In the Navigation pane, right-click a module, select **Restart Module->Cold Restart**.
- Step 3** In the **Restart** confirmation dialog, click **Yes**.  
A CONTCOM (Control Communications Failure with Circuit Pack) alarm is raised during a cold or warm restart.

You have successfully completed this procedure.

## A.1.6 Delete a packetVX module

### Prerequisites

- The packetVX module is provisioned and removed from service.

### Deleting a module

Follow these steps to delete a packetVX module:

- Step 1** In the toolbar, click the System Configuration icon. The System Configuration view of the shelf displays in the Navigation pane.
- Step 2** In the Navigation pane, right-click a module, and then click **Delete Module**.
- Step 3** In the **Delete Module** confirmation dialog, click **Yes**.

You have successfully completed this procedure.

## A.2 Setting up an Ethernet switch

---

This section includes the step-by-step procedures for provisioning and deleting an Ethernet switch.

### A.2.1 Provisioning an Ethernet switch

This section provides the procedures for provisioning an Ethernet switch.

#### A.2.1.1 Provision an Ethernet switch

##### Prerequisites

- The packetVX module is provisioned and in service.

##### Provisioning an Ethernet switch

Follow these steps to provision an Ethernet switch on a packetVX module:

**Step 1** In the toolbar, click the Packet Ethernet icon. The Packet Ethernet view of the shelf displays in the Navigation pane.

**Step 2** Right-click on **Virtual Switches** and choose **Create Switch**. The **Create Switch** dialogue appears.

**Step 3** From the drop-down menus, select a switch number and mode type. In the **Switch Name** field, specify a unique name for the switch. Click **Apply**.

**Step 4** Add a switch member.

Click **Provision Switch**. The **Switch** dialog appears. Select the **Members** tab and click **Add**. The dialog that lists the available packetVX switches appears. Highlight the switch that you want to add as a member and click **Add**. The switch appears in the table.

- If you are not adding this member to a stacking port configuration, click **Apply** and go to Step 6.
- If you are adding this member as a stacking port, stay within the **Members** tab dialog and go to next step.

**Step 5** Configure the stacking ports.

Go to the **Stacking Ports** section, and continue as follows:

- In the **Member Instance 1** panel click **Add**. The **Add Stacking Port** dialog appears, which includes the list of available ports. Highlight the first port that is going to serve as the initial primary stacking port and click **Apply**. The port is added to the instance 1 table. To assign a port to serve as the initial secondary port, go to the **Member Instance 2** panel, click **Add**, highlight the second port, and click **Apply** to add the port to the instance 2 table.
- Click **Apply** to complete adding the stacking ports.

**Step 6** To continue provisioning the switch, select the **Advanced** tab. Accept the default settings or specify the parameter settings.

Click **Apply** and **Close** to complete provisioning the switch.

You have successfully completed this procedure.

**Table A- 2 Ethernet switch provisioning parameters**

Tab/Heading	Parameter	Description	Range of Values	Default Value
<b>General</b>				
<b>General</b>	Switch	The number assigned to the switch	1 to 11	not applicable
	Mode	The type of Ethernet bridge	Provider Bridge Q Bridge	Provider Bridge
<b>Packet Forwarding</b>	MAC Learning	The state of unicast MAC address learning	enabled	enabled
	Aging Timer	The maximum age of a dynamically learned entry in the MAC Address table	1 to 604800	300
<b>Members</b>				
	Card	The packetVX module	AID for packetVX module	
	Instance	The instance number of the packetVX module	Up to 4 ports per stacking member instance.	
	State	Read-only. The stacking state of the switch.	Disabled: The administrative state of the switch is disabled.  Unstacked: There is only one module enabled on the switch.  For a multiple module configuration: <ul style="list-style-type: none"> <li>Primary: The module that is currently in control.</li> <li>Secondary: The standby module.</li> </ul> Not Present: There are no modules in the switch.	The current state.

**Table A- 2 Ethernet switch provisioning parameters (Continued)**

Tab/Heading	Parameter	Description	Range of Values	Default Value
	Port State	The communication state of the stacking interface.	Connection OK: If there is communication across the stacking port.  No Connection: If there is no communication across the stacking port.	The current state.
	Backplane State	The state between the primary and secondary modules.	Connection OK: The primary module can communicate with the secondary module.  No Connection: The primary module cannot connect with the secondary module.	The current state.
<b>Stacking Ports</b>	Member Instance 1: • Port • State	<ul style="list-style-type: none"> <li>Port: The member port that is assigned, initially, as the primary port.</li> <li>State: The administrative status of the port.</li> </ul>	An available member port.	Not applicable
	Member Instance 2: • Port • State	<ul style="list-style-type: none"> <li>Port: The member port that is assigned, initially, as the secondary port.</li> <li>State: The administrative status of the port.</li> </ul>	An available member port.	Not applicable
<b>Advanced</b>				
<b>Connectivity Fault Management</b>	Switch Name	The name assigned to the switch	alphanumeric characters	BTI_<switchNumber>
	MEG Name	The CFM Maintenance Entity Group (MEG) name	1 to 5 alphanumeric characters	BTI
	MIP auto Creation	The state of the MIP Auto Creation for a CFM level	Enabled Disabled	Enabled
	MEG Level	The CFM level	4 to 7	4
	MIP Level	The CFM MIP level	4 to 7	4

**Table A- 2 Ethernet switch provisioning parameters (Continued)**

<b>Tab/Heading</b>	<b>Parameter</b>	<b>Description</b>	<b>Range of Values</b>	<b>Default Value</b>
<b>Link Aggregation Control Protocol</b>	LACP System Priority	The LACP system priority	1 to 65535	32767
<b>Profiles</b>	Tunnel Mac Address Profiles	The Profile Tunnel MAC address Configuration mode to configure the MAC addresses for tunneling protocols	1 to 32 alphanumeric characters	Default TMA profile
<b>Protocol Administrative State</b>	MSTP LACP GVRP Y.1731 802.1ag ERPS SLA Measurement	Enables or disables the protocol administrative state.	Not applicable	Enabled: MSTP, LACP, GVRP, Y.1731 and ERPS  Disabled: 802.1ag, and SLA Measurement
<b>ERPS</b>	VLAN Propagate	Controls how the user traffic is converged when there is an ERPS ring failure.	Fast: Traffic is converged in the order of the ERPS timers. This causes redundant traffic throughout the rings.  Slow: Traffic is converged based on the shortest path. Redundant traffic does not occur; however, convergence is not in the order of the ERPS timers.	Fast

### A.2.1.2 Delete an Ethernet switch

#### Prerequisites

- The Ethernet switch is provisioned.
- All child entities of the Ethernet switch, e.g., UNIs, NNIs, switchports, and VLANs, are deleted.
- Ports are removed from the MSTP configuration.

#### Deleting an Ethernet switch

Follow these steps to delete an Ethernet switch on a packetVX module:



- Step 1** In the toolbar, click the Packet Ethernet icon. The Packet Ethernet view of the shelf displays in the Navigation pane.
- Step 2** In the Navigation pane, under Virtual Switches, right-click **Switch** and then click **Delete Switch**.
- Step 3** In the confirmation dialog, click **Yes**.

You have successfully completed this procedure.

## A.2.2 Provisioning ports on an Ethernet switch

This section provides the procedures for provisioning a port on an Ethernet switch.

### A.2.2.1 Using the E-services model to provision a UNI, NNI or E-NNI on an Ethernet switch

#### Prerequisites

- The Ethernet switch is provisioned.

#### Provisioning a UNI, NNI or E-NNI on an Ethernet switch

Follow these steps to provision a UNI, NNI or E-NNI on an Ethernet switch:

- Step 1** In the toolbar, click the System Configuration or Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click an unprovisioned port on an Ethernet switch, select **Provision**, and then click **UNI**, **NNI** or **E-NNI**.
- Step 3** In the **Port** dialog, specify the provisionable parameters for the port, or accept the defaults. See [Table A-3](#).
- Step 4** Click **Apply**.
- Step 5** Click the **Provision Port** button to specify the provisionable port-setting parameters. See [A.2.2.7, “UNI, NNI, E-NNI and switchport port-setting parameters”](#).
- Step 6** Click **Apply**, then click **Close**.

You have successfully completed this procedure.

**Table A- 3 UNI , NNI and E-NNI parameters**

Parameter	Range of values	Description
Service Type (UNI only)	Virtual Single Private	The service type of the UNI

**Table A- 3 UNI , NNI and E-NNI parameters (Continued)**

Parameter	Range of values	Description
	Unspecified Virtual Untagged Virtual Multiple	
Max Frame Size	1518 to 9600	The maximum frame size
Max Service Frame Size (UNI only)	1518 to 9600	The maximum service frame size
Customer PVID (UNI only)	2 to 4090	The customer PVID number
Mode	Half Duplex Full Duplex Auto	Full Duplex
Broadcast Storm Control	100% or 60% or 40% or 20% By default, the rate is set to 100%: storm control is disabled.	The rate limit used to manage broadcast traffic on NNI / E-NNI ports and LAGs. Select <b>Broadcast Storm Control</b> to enable storm control for broadcast traffic.
Multicast Storm Control	100% or 60% or 40% or 20% By default, the rate is set to 100%: storm control is disabled.	The rate limit used to manage multicast traffic on NNI / E-NNI ports and LAGs. Select <b>Multicast Storm Control</b> to enable storm control for multicast traffic.
Unicast DLF Storm Control	100% or 60% or 40% or 20% By default, the rate is set to 100%: storm control is disabled.	The rate limit used to manage unicast DLF traffic on NNI / E-NNI ports and LAGs. Select <b>Unicast DLF Storm Control</b> to enable storm control for multicast traffic.

### A.2.2.2 Using the Provider Bridge model to provision a switchport on an Ethernet switch

#### Prerequisites

- The Ethernet switch is provisioned.

#### Provisioning a switchport on an Ethernet switch

Follow these steps to provision a switchport on an Ethernet switch:

- Step 1** In the toolbar, click the System Configuration or Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click an unprovisioned port on an Ethernet switch of a packetVX module, select **Provision** , and then click **Switchport**.
- Step 3** In the **Port** dialog, specify the provisioning parameters for the port on the **General**, **Layer 2**, **Layer 1**, **Services**, **GVRP**, and **GCC0** tabs, clicking **Apply** before displaying the next tab, or accept the defaults. See [A.2.2.7, “UNI, NNI, E-NNI and switchport port-setting parameters”](#).

**Step 4** Click **Close**.

You have successfully completed this procedure.

### A.2.2.3 Configure Port Mirroring

**Prerequisites**

- The packetVX module is provisioned and in service.

Configuring port mirroring involves two procedures:

- Selecting the port from which you want traffic mirrored—Mirror-from-Port (MFP).
- Selecting the port that receives the mirrored traffic—Mirror-to-Port (MTP).

**Considerations**

You should be familiar with the following considerations before using port mirroring:

- A single port on a virtual switch is used as an MTP.
- The following ports cannot be an MTP port: stacking, switch, NNI, UNI, or a member of a Link Aggregation Group.
- Any physical port can be used as the MFP.
- If the cumulative traffic that needs to be mirrored across all MFP is greater than the maximum bandwidth supported on the MTP, you may not see all the mirrored packets.
- Performance monitoring (PM) counters are only available to active switching interfaces. PM counters are not available on the MTP port, since it is not part of any active switch interface.
- Port mirroring only mirrors the traffic seen on the port. It does not classify or filter the traffic.
- MTP and MFP ports can be on different sides of stacking ports or on separate modules.

**Configuring port mirroring**

Follow these steps to configure port mirroring on a physical port:

**Step 1** In the toolbar, click the **Packet Ethernet** icon. Navigate to **Virtual Switches > Switch: <x> >Ports**.

**Step 2** Select a port. Right-click and click **Provision Port**; the **Port - x** dialog appears. (The port can be any of the type: Switchport, UNI, NNI, LAG.)

**Step 3** Click the **Layer 1** tab. Go to the **Mirroring** field. From the drop-down menu choose what traffic you want to mirror, or choose None if you don't want traffic mirrored for this port.

**Step 4** Click **Apply** and **Close**.

**Step 5** Navigate to **Virtual Switches > Switch:x > Port Mirroring**. Right-click; click **Provision Port Mirroring**. The **Port Mirroring (Switchx)** dialog appears.

From the **Mirror To Port** drop down menu, choose the port that receives the mirrored traffic. Click **Apply**.

**Step 6** Click the **Mirror From Ports** tab to see a listing of all the ports that are mirroring traffic to the selected MTP.

**Step 7** Click **Close**.

You have successfully completed this procedure.

#### A.2.2.4 View or modify port settings on an Ethernet switch

##### Prerequisites

- The port on the Ethernet switch is provisioned.

##### Viewing or modifying port settings on an Ethernet switch

Follow these steps to view or modify port settings on an Ethernet switch:

**Step 1** In the toolbar, click the System Configuration or Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click a port on packetVX, then click **Provision Port**.

**Step 3** In the **Port** dialog, click a tab in the dialog to view the corresponding parameters, or modify the provisionable parameters on the tab and then click **Apply**. See [A.2.2.7, “UNI, NNI, E-NNI and switchport port-setting parameters”](#) for more information.

**Step 4** Click **Close**.

You have successfully completed this procedure.

#### A.2.2.5 View transceiver inventory information

##### Prerequisites

- The transceiver is installed in the port.

##### Viewing transceiver inventory information

Follow these steps to view parameters for an SFP or XFP transceiver on a packetVX module:

**Step 1** In the toolbar, click the System Configuration or Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click a module, click **Display SFP/XFP Inventory**, and then click the port number.

<b>Note</b>	Ports labeled $Gn$ support only SFP transceivers; ports labeled $Xn$ support only XFP transceivers.
-------------	---

The **Display Inventory Information** dialog displays **General**, **Characteristic**, and **Vendor** parameters for the transceiver. See [Table A-4](#).

**Step 3** Click **Close**.

You have successfully completed this procedure.

**Table A- 4 SFP or XFP transceiver inventory information**

Parameter	Range of Values	Description
Full Name	Alphanumeric characters	Full name of the transceiver
Name	Alphanumeric characters	Short name of the transceiver (SFP or XFP)
Shelf Number	Integer	The shelf in which the module is installed
Slot Number	Integer	The slot in which the module is installed
Port Number	Integer	The module port in which the transceiver is inserted
Wavelength	Numeric	<p>The wavelength of the transceiver in nm.</p> <p><b>Note</b></p> <p>Some transceivers have a wavelength value that is specified only to the nearest nm, whereas others specify wavelength to the nearest 0.01 nm.</p> <p><b>Note</b></p> <p>If a transceiver that does not have a wavelength value specified in its memory is inserted into a module, a REPLUNITUNK alarm is raised against the transceiver.</p>
Minimum Wavelength <b>Note</b> This parameter is supported by a tunable XFP only.	Numeric	The minimum wavelength supported, represented in nm with 0.01 nm resolution.
Maximum Wavelength <b>Note</b> This parameter is supported by a tunable XFP only.	Numeric	The maximum wavelength supported, represented in nm with 0.01 nm resolution.
Wavelength Spacing <b>Note</b> This parameter is supported by a tunable XFP only.	Numeric	The grid spacing in GHz (100GHz, 50GHz)

**Table A- 4 SFP or XFP transceiver inventory information (Continued)**

Parameter	Range of Values	Description
Reach	Numeric	<p>The maximum transmit distance of the transceiver in kilometers using 9 micron SM fiber.</p> <p><b>Note</b></p> <p>If a transceiver that does not have a reach value specified in its memory is inserted into a module, a REPLUNITUNK alarm is raised again</p>
Connector Type	LC	The listed transceiver connector type
Digital Diagnostics Implemented	Yes No	<p>The digital diagnostic implementation parameter. When set to Yes, this parameter enables the recording of performance data in historical bins.</p> <p><b>Note</b></p> <p>If this parameter is set to No or is not specified in the transceiver's memory, all historical bins are filled with dummy values and marked as invalid.</p>
Tx Fault Implemented	Yes No	<p>The transceiver fault implemented parameter on the transceiver</p> <p><b>Note</b></p> <p>The system allows transceivers that do not use this flag to indicate through the inventory table that the installed transceiver will never indicate a transmitter fault.</p>
Signal Encoding	8B10B 4B5B NRZ MANCHESTER SONET_SCRAMBLED	<p>The encoding scheme for the transceiver</p> <p><b>Note</b></p> <p>The system does not use the encoding parameter. It is the operating company's responsibility to ensure that both end points of a span use the same encoding.</p>
Minimum bit rate	Integer	<p>The minimum bit rate supported by the transceiver</p> <p><b>Note</b></p> <p>If a transceiver inserted in a module port does not have a minimum baud rate value specified in its memory, the system raises a REPLUNITUNK alarm against the transceiver.</p>
Maximum bit rate	Integer	<p>The maximum bit rate supported by the transceiver</p> <p><b>Note</b></p> <p>If a transceiver inserted in a module port does not have a maximum baud rate value</p>

**Table A- 4 SFP or XFP transceiver inventory information (Continued)**

Parameter	Range of Values	Description
		specified in its memory, the system raises a REPLUNITUNK alarm against the transceiver.
Nominal bit rate	Integer	The nominal bit rate supported by the transceiver
		<b>Note</b> If a transceiver inserted in a module port does not have a nominal baud rate value specified in its memory, the system raises a REPLUNITUNK alarm against the transceiver.
LOS implemented	Yes No	The loss of signal implementation parameter. When set to Yes, this parameter raises the LOS alarm against the transceiver.
Tx Disable Implemented	Yes No	The transceiver disable implemented parameter. When set to Yes, this parameter disables the transmitter of the transceiver when the module is placed in the Out of Service state.
Media	Electrical Optical Unknown	The type of connector used by the transceiver
PEC Code	String	The product equipment code assigned by the manufacturer
Name	Alphanumeric characters	The name of the transceiver's vendor
Part Number	Alphanumeric characters	The part number assigned to the transceiver by the vendor
OUI	Alphanumeric characters	The vendor's organization unique identifier
CLEI Code	String	The Common Language Equipment Identifier number assigned by Telcordia. The CLEI identifies the physical hardware.
Serial Number	Integer	The serial number of the transceiver
Release Number	Alphanumeric characters	The hardware release number
Manufacturing Date	YYYY-MM-DD	The date that the transceiver was manufactured

### A.2.2.6 Delete a port on an Ethernet switch

#### Prerequisites

- Port must be provisioned.

### Deleting a port on an Ethernet switch

Follow these steps to delete a port on a packetVX module:

**Step 1** In the Navigation pane, right-click a port on a packetVX module, and then click **Delete Port**.

**Step 2** In the **Delete Port** confirmation dialog, click **Yes**.

You have successfully completed this procedure.

### A.2.2.7 UNI, NNI, E-NNI and switchport port-setting parameters

**Table A- 5 General port parameters**

Type	Parameter	Range of Values	Description
Ethernet	Port Number	1 to 24	The number of the port
	Port Type	10 GigE (10GbE) GigE (Gigabit Ethernet)	The port type
	MAC address	Integer expressed as 00-00-00-00-00-00	The MAC address
	Interface type	PNP (provider network port) PNP external (provider network port external) CEP (customer edge port) CNP Port-Based (customer network port)	The port type <b>Note</b> Provisionable on switchports only.
State Management	Layer 2 Status: Admin	Enabled (default) Disabled	The Layer 2 state of the port
	Layer 1 Status: Admin	Enabled (default) Disabled	The Layer 1 state of the port

**Table A- 6 Layer 2 port parameters**

Type	Parameter	Range of Values	Description
General	PVID	2 to 4090	The Port VLAN Identifier assigned to either untagged or priority tagged frames.
	Default Priority	0 to 7 Default = 0	The default priority for untagged traffic entering a tag-enabled port
	Control Frame	Profile name	The Control Frame profile to be used
	Allowed Frame Type	All Tagged Untagged Priority Tagged	The frame types allowed by the port



Table A- 6 Layer 2 port parameters (Continued)

Type	Parameter	Range of Values	Description
	Use DEI	True False	Indicates whether the port can use DEI bit on the S-TAG to lookup the PCP decoding table
	TPID	0x8100 0x88a8 0x9100	The default priority for untagged traffic entering a tag-enabled port
	Ingress Filtering	True (default) False	Enables or disables ingress filtering
			<b>Note</b> This control does not affect VLAN-independent BPDU frames, such as GVRP and STP.
	Egress Bandwidth	Profile name Not specified	The Egress Bandwidth profile to be used
	Ingress Bandwidth	Profile name Not specified	The Ingress Bandwidth profile to be used
	Scheduler	DEFAULT_SCHEDULER_PROFILE	The Scheduler profile to be used
	Priority TC Map	Profile name	The Priority TC Map profile to be used
QoS	DSCP PHB	Default DSCP PHB Profile Not specified	The DSCP PHB profile to be used
	Trust Incoming DSCP	True False	Indicates whether the DSCP field of the incoming packet can be trusted or is ignored
	PCP Enc/Dec	Default 8POD Profile Default 7P1D Profile Default 6P2D Profile Default 5P3D Profile Not specified	The PCP Encoding/Decoding profile to be used
	Trust Incoming PCP	True False	Indicates whether the PCP field of the incoming packet can be trusted or is ignored
UNI	Service Type	Virtual Single Private Unspecified Virtual Untagged Virtual Multiple	The service type of the UNI
	Max Frame Size	1518 to 9600	The maximum frame size
	Customer PVID	0 to 4094	The customer PVID number
NNI / E-NNI	Max Frame Size	1518 to 9600	The maximum service frame size

**Note**  
Applies to UNI ports only.

**Table A- 6 Layer 2 port parameters**

Type	Parameter	Range of Values	Description
<b>Note</b>			
Applies to NNI / E-NNI ports only.			

**Table A- 7 Layer 1 port parameters**

Type	Parameter	Range of Values	Description
General	PEC	PEC string	The Product Equipment Code of the transceiver
	MTU Size	1518 to 9600 bytes	Maximum transmission unit size of the IP port
	Wavelength	800 nm to 1650 nm	The wavelength of the port
	Fiber Type	NDSF DSF NONE MULTIMODE NZDSF	The type of fiber connected to the port
	Media Rate	Auto	The Ethernet speed and duplex rate in Mbps
	Physical PM Thld Mon	Enabled Disabled	Enables or disables reporting of Physical PMs for the port
	SD Bit Error Ratio	10e-(3-12)	The value of the signal degrade Bit Error Rate Test (BERT)
	Mirroring	None Mirror Ingress From: Configures port mirroring to monitor the incoming traffic on this port. Mirror Egress From: Configures port mirroring to monitor outgoing traffic from this port. Mirror Both From: Configures port mirroring to monitor the incoming and outgoing traffic from this port.	Configures port mirroring.
	Vendor PN 1, 2, 3	1 to 20 alphanumeric characters	The Vendor part numbers .
	ID 1	A text string up to 32 characters.	User-defined description of the physical location of the equipment.
	Link Change Counter	Not applicable	The number of times the operational state changes for this equipment.
	Custom 1	0 to 255 alphanumeric characters	The custom fields for specific operating company information.

**Table A- 7 Layer 1 port parameters (Continued)**

Type	Parameter	Range of Values	Description
<b>Thresholds</b>	Remote ID	A text string	The remote node and port to which the packetVX is connected.
	Optical Power Received MIN	Measurements are accurate to $\pm 3.0$ dBm for SFPs; to $\pm 2.0$ dBm for XFPs.	Minimum optical power (dBm) received, measured for noncopper SFPs and all XFPs.
	Optical Power Transmitted MIN	Measurements are accurate to $\pm 3.0$ dBm for SFPs; to $\pm 2.0$ dBm for XFPs.	Minimum optical power (dBm) transmitted, measured for noncopper SFPs and all XFPs.
	Optical Power Received MAX	Measurements are accurate to $\pm 3.0$ dBm for SFPs; to $\pm 2.0$ dBm for XFPs.	Maximum optical power (dBm) received, measured for noncopper SFPs and all XFPs.
	Optical Power Transmitted MAX	Measurements are accurate to $\pm 3.0$ dBm for SFPs; to $\pm 2.0$ dBm for XFPs.	Maximum optical power (dBm) transmitted, measured for noncopper SFPs and all XFPs.
<b>OTN</b>	Line Mapping <sup>1</sup>	Not applicable OTU2 GFP-1 10GE LAN PHY 10GE WAN PHY	The line-mapping mode for the port
	Error Correction <sup>1</sup>	FEC (Forward Error Correction) EFEC (Enhanced Forward Error Correction)	The error correction for OTU2 line-mapping
	Loopback <sup>1</sup>	Operate Release	Operates or releases a facility loopback on the port
<b>LLDP</b>	Admin Status	Enabled: The default on an NNI port Disabled: The default on a UNI port	Sets the LLDP participation on the port.
	Remote Chassis Type	Not applicable	The type of identification used for the chassis learned by LLDP.
	Remote Port Type	Not applicable	The type of identification used for the port learned by LLDP.
	Show Raw Id Values	Not applicable	When enabled shows the chassis and port IDs in an ASCII string format.
	Remote Chassis Id	A string value	The chassis ID learned by LLDP.
	Remote Port Id	InterfaceShelf/slot/port For example, Xgig1/3/1	The port ID learned by LLDP.

<sup>1</sup> Applies to XFP ports only.**Table A- 8 Services parameters**

Parameter	Range of Values	Description
Name	Up to 256 alphanumeric values	User-specified name of the profile

**Table A- 8 Services parameters (Continued)**

Parameter	Range of Values	Description
Type	EPLINE EPLAN EPTREE EVPLINE EVPLAN EVPTREE	The type of service
Access	Select Access option	Provisions an Access Eservice
Admin State	Enable Disable	The GVRP status
Operational State	Up Down Partially connected	The operational state of the service
SVLAN	2 to 4090	The VLAN identifier
Unavailable seconds (UAS) (24 hour)	A service becomes unavailable at the onset of 10 consecutive seconds that quality as UAS, and continues to be unavailable until the onset of 10 consecutive seconds that do not quality as UAS	Measures the number of seconds during which the service was considered unavailable

**Table A- 9 GVRP parameters**

Type	Parameter	Range of Values	Description
Settings	Admin State	Enable Disable	The GVRP status
	Restricted VLAN Registration	Enable Disable	The VLAN-registration status

**Table A- 10 GCC0 parameters**

Type	Parameter	Range of Values	Description
Settings	GCC0 Mode	Disabled Full Rate (uses the full available bandwidth) Low Rate (limits channel traffic to 192/Kbs)	The rate of the GCC0
	State	See the <i>Operations Solutions Guide</i> .	The primary and secondary states of the GCC0

### A.2.2.8 Forwarding database provisioning

The packetVX employs a forwarding database (FDB). The FDB can contain both address entries and VLAN entries, either or both of which can be used to limit the forwarding of a packet to fewer than "all ports" — usually none or one for a unicast packet.

#### MAC address learning

All received packets are forwarded everywhere, or flooded, unless forwarding is restricted by entries in the forwarding database. Media Access Control (MAC) addresses are learned by the FDB.

#### MAC address aging

When the MAC address learning feature is enabled, the FDB entries "age out" according to the value set for the aging timer. The aging timer for a particular FDB entry (that is, a source MAC address) is reset when it is learned or relearned.

#### Static MAC addresses

Static filtering controls allow the network administrator to impose a level of control over the permitted connectivity in the network, by setting static MAC Address filters in the FDB.

#### Add an entry to the forwarding database:

##### Prerequisites

- The Ethernet switch is provisioned.

##### Adding an entry to the forwarding database

Follow these steps to add a static unicast or static multicast entry in the forwarding database for an Ethernet switch:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Forwarding DB** under an Ethernet switch, and then click **View Forwarding Database**.

**Step 3** In the **Forwarding Database** dialog, click the **Dynamic Unicast**, **Static Unicast** or **Static Multicast** tab, and then click the **New** button on the tab.

**Step 4** In the dialog for the new entry, specify the following:

- **Switch** — the switch to which you want to apply the entry
- **VLAN** — the VLAN ID
- **MAC Address** — the MAC address of the entry

**Step 5** Click **Apply**, and then click **Close**.

The entry appears in the list on the **Forwarding Database** dialog.

**Step 6** In the **Forwarding Database** dialog, click **Close**.

You have successfully completed this procedure.

### View forwarding database information:

#### Prerequisites

- The Ethernet switch is provisioned.
- The MAC Address table contains addresses.

#### Viewing forwarding database information

Follow these steps to view information about a dynamic unicast, static unicast, and static multicast entry in the forwarding database for an Ethernet switch:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Forwarding DB** under an Ethernet switch, and then click **View Forwarding Database**.

**Step 3** From the **Viewing Switch** drop-down list in the **Forwarding Database** dialog, select **All** or a particular switch

**Step 4** Click the tab that corresponds to the type of entry that you want to view.

**Step 5** Select an entry from the table, and then click **View**. See [Table A-11](#).

**Step 6** Click **Close**.

You have successfully completed this procedure.

**Table A- 11 Forwarding Database parameters**

Parameter	Range of Values	Description
MAC address	A valid MAC address	The MAC address of the entry
Switch	All Provisioned switch IDs	The switch identifier
VLAN	2 - 4090	The VLAN identifier
Port	Port number (X1 to X4, G1 to G24)	The port number from which the address was learned

### Remove an entry from the forwarding database:

#### Prerequisites

- The forwarding database contains entries.

### Removing an entry from the forwarding database

Follow these steps to remove a static unicast or static multicast entry in the forwarding database for an Ethernet switch:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Forwarding DB** under an Ethernet switch, and then click **View Forwarding Database**.
- Step 3** In the **Forwarding Database** dialog, click the **Static Unicast** or **Static Multicast** tab, and then the entry that you want to remove
- Step 4** Click **Delete**.
- Step 5** In the confirmation dialog, click **Yes**.
- Step 6** Click **Close**.

You have successfully completed this procedure.

## A.3 Provision an Ethernet switch

---

### Prerequisites

- The packetVX module is provisioned and in service.

### Provisioning an Ethernet switch

Follow these steps to provision an Ethernet switch on a packetVX module:

- Step 1** In the toolbar, click the Packet Ethernet icon. The Packet Ethernet view of the shelf displays in the Navigation pane.
- Step 2** Right-click on **Virtual Switches** and choose **Create Switch**. The **Create Switch** dialogue appears.
- Step 3** From the drop-down menus, select a switch number and mode type. In the **Switch Name** field, specify a unique name for the switch. Click **Apply**.
- Step 4** Add a switch member.
- Click **Provision Switch**. The **Switch** dialog appears. Select the **Members** tab and click **Add**. The dialog that lists the available packetVX switches appears. Highlight the switch that you want to add as a member and click **Add**. The switch appears in the table.
- If you are not adding this member to a stacking port configuration, click **Apply** and go to Step 6.
  - If you are adding this member as a stacking port, stay within the **Members** tab dialog and go to next step.
- Step 5** Configure the stacking ports.
- Go to the **Stacking Ports** section, and continue as follows:
- In the **Member Instance 1** panel click **Add**. The **Add Stacking Port** dialog appears, which includes the list of available ports. Highlight the first port that is going to serve as the initial primary stacking port and click **Apply**. The port is added to the instance 1 table. To assign a port to serve as the initial secondary port, go to the **Member Instance 2** panel, click **Add**, highlight the second port, and click **Apply** to add the port to the instance 2 table.
  - Click **Apply** to complete adding the stacking ports.
- Step 6** To continue provisioning the switch, select the **Advanced** tab. Accept the default settings or specify the parameter settings.
- Click **Apply** and **Close** to complete provisioning the switch.

You have successfully completed this procedure.



Table A- 12 Ethernet switch provisioning parameters

Tab/Heading	Parameter	Description	Range of Values	Default Value
<b>General</b>				
<b>General</b>	Switch	The number assigned to the switch	1 to 11	not applicable
	Mode	The type of Ethernet bridge	Provider Bridge Q Bridge	Provider Bridge
<b>Packet Forwarding</b>	MAC Learning	The state of unicast MAC address learning	enabled	enabled
	Aging Timer	The maximum age of a dynamically learned entry in the MAC Address table	1 to 604800	300
<b>Members</b>				
	Card	The packetVX module	AID for packetVX module	
	Instance	The instance number of the packetVX module	Up to 4 ports per stacking member instance.	
	State	Read-only. The stacking state of the switch.	Disabled: The administrative state of the switch is disabled.  Unstacked: There is only one module enabled on the switch.  For a multiple module configuration: <ul style="list-style-type: none"> <li>• Primary: The module that is currently in control.</li> <li>• Secondary: The standby module.</li> </ul> Not Present: There are no modules in the switch.	The current state.
	Port State	The communication state of the stacking interface.	Connection OK: If there is communication across the stacking port.  No Connection: If there is no communication	The current state.

**Table A- 12 Ethernet switch provisioning parameters (Continued)**

Tab/Heading	Parameter	Description	Range of Values	Default Value
			across the stacking port.	
	Backplane State	The state between the primary and secondary modules.	Connection OK: The primary module can communicate with the secondary module.  No Connection: The primary module cannot connect with the secondary module.	The current state.
<b>Stacking Ports</b>	Member Instance 1: <ul style="list-style-type: none"> <li>Port</li> <li>State</li> </ul>	<ul style="list-style-type: none"> <li>Port: The member port that is assigned, initially, as the primary port.</li> <li>State: The administrative status of the port.</li> </ul>	An available member port.	Not applicable
	Member Instance 2: <ul style="list-style-type: none"> <li>Port</li> <li>State</li> </ul>	<ul style="list-style-type: none"> <li>Port: The member port that is assigned, initially, as the secondary port.</li> <li>State: The administrative status of the port.</li> </ul>	An available member port.	Not applicable
<b>Advanced</b>				
<b>Connectivity Fault Management</b>	Switch Name	The name assigned to the switch	alphanumeric characters	BTI_<switchNumber>
	MEG Name	The CFM Maintenance Entity Group (MEG) name	1 to 5 alphanumeric characters	BTI
	MIP auto Creation	The state of the MIP Auto Creation for a CFM level	Enabled Disabled	Enabled
	MEG Level	The CFM level	4 to 7	4
	MIP Level	The CFM MIP level	4 to 7	4
<b>Link Aggregation Control Protocol</b>	LACP System Priority	The LACP system priority	1 to 65535	32767
<b>Profiles</b>	Tunnel Mac Address Profiles	The Profile Tunnel MAC address Configuration mode to configure the MAC	1 to 32 alphanumeric characters	Default TMA profile

Table A- 12 Ethernet switch provisioning parameters (Continued)

Tab/Heading	Parameter	Description	Range of Values	Default Value
		addresses for tunneling protocols		
<b>Protocol Administrative State</b>	MSTP	Enables or disables the protocol administrative state.	Not applicable	Enabled: MSTP, LACP, GVRP, Y.1731 and ERPS
	LACP			
	GVRP			
	Y.1731			Disabled: 802.1ag, and SLA Measurement
	802.1ag			
	ERPS			
	SLA Measurement			
<b>ERPS</b>	VLAN Propagate	Controls how the user traffic is converged when there is an ERPS ring failure.	Fast: Traffic is converged in the order of the ERPS timers. This causes redundant traffic throughout the rings.  Slow: Traffic is converged based on the shortest path. Redundant traffic does not occur; however, convergence is not in the order of the ERPS timers.	Fast

## A.4 Link aggregation group provisioning

---

Link aggregation groups (LAG) allow multiple Ethernet interfaces that are running at the same speed, to be grouped together providing increased transport performance and or increased robustness.

### LAGs on packetVX modules

packetVX modules supports up to 27 link aggregation groups. Each group supports up to 8 members.

When 10GbE is encapsulated in OTU2 wrappers, the link aggregation software relies on the OTU2 for the detection of Loss of Signal (LOS), Loss of Frame (LOF), and Signal Degrade (SD) failures. The OTU2 framer triggers the software to remove the LOS port from the LAG. When the defect clears, the software adds the port back to the LAG.

If a fiber cut occurs between two nodes, the link aggregation software relies on OTU2 for the detection of backward defect indications (BDI) and backward error indications (BEI). The OTU2 framer triggers the software to cause the port to be unavailable. Traffic continues along the available links. When the defect clears, the port is automatically transitioned to an available state and continues to manage traffic .

### Link aggregation control protocol

The link aggregation control protocol (LACP) operates between packetVX modules to control the addition or removal of ports from the LAG.

While any two ports on a given system may be capable of aggregation, it is not necessarily the case that an arbitrary selection of such ports can be aggregated. A system may reasonably limit the number of ports attached to a single LAG, or the particular way more than two ports can be combined.

In cases where both communicating systems (via LACP) have constraints on aggregation, it is necessary for them both to agree on the links to be selected for aggregation.

Every link between systems operating LACP is assigned a unique priority. This priority comprises (in priority order) the LACP System Priority, LACP System ID, LACP Port Priority, and Port Number of the higher-priority system. In priority comparisons, numerically lower values have higher priority.

Ports are considered for active use in an aggregation in link priority order, starting with the port attached to the highest priority link. Each port is selected for active use if preceding higher priority selections can also be maintained; otherwise the port is selected as standby.

A port that is selected as standby as a result of limitations on aggregation capability can be viewed as providing a “hot standby” facility, as it is able to take part in the aggregation upon failure of one of the active links in the LAG. The ability to hold links in a standby mode in this way provides the possibility of using LACP even where the system is incapable of supporting distribution and collection with more than one port. Parallel links could be automatically configured as standby links, and deployed to mask link failures without any disruption to higher layer protocols.

LACP link protection reverts to a higher-priority (lower-numbered) link when that higher priority link becomes operational or a link is added to the LAG that is determined to be higher in priority.

### A.4.1 Provision a UNI, NNI or E-NNI link aggregation group

#### Prerequisites

- The ports are provisioned on the Ethernet switch.

#### Provisioning a UNI, NNI or E-NNI link aggregation group

Follow these steps to provision a UNI, NNI or E-NNI link aggregation group (LAG) on an Ethernet switch:

- Step 1** In the toolbar, click the **Packet Ethernet** icon, to list the Ethernet switches. Expand **Virtual Switches**.
- Step 2** Navigate to **Virtual Switches > Switch <x> > LAG**. Right-click **LAG**, and click one of the following ports:
  - Provision UNI LAG**
  - Provision NNI LAG**
  - Provision E-NNI LAG**
  - Provision Switchport LAG**
- Step 3** In the **Port** dialog, specify values for the provisionable parameters of the LAG, or accept the default settings. See [Table A-13](#).
- Step 4** Click **Apply**, which enables the **Provision LAG** option.
- Step 5** Click **Provision LAG** to specify the provisionable LAG settings for the port. See [A.4.7](#), “UNI, NNI E-NNI and switchport LAG parameters”.
- Step 6** Click **Apply**, then click **Close**.

You have successfully completed this procedure.

**Table A- 13 UNI LAG , NNI and E-NNI LAG provisioning parameters**

Parameter	Range of values	Description
Service Type (UNI LAG only)	Virtual Single	The service type of the UNI
	Private	
	Unspecified	
	Virtual Untagged	
	Virtual Multiple	

**Table A- 13 UNI LAG , NNI and E-NNI LAG provisioning parameters (Continued)**

Parameter	Range of values	Description
Max Frame Size	1518 to 9600	The maximum frame size
Max Service Frame Size (UNI LAG only)	1518 to 9600	The maximum service frame size
Customer PVID (UNI LAG only)	2 to 4090	The customer PVID number
Mode	Half Duplex Full Duplex Auto	The duplex mode

## A.4.2 Provision a switchport link aggregation group

### Prerequisites

- The ports are provisioned on the Ethernet switch.

### Provisioning a switchport link aggregation group

Follow these steps to provision a switchport link aggregation group (LAG) on an Ethernet switch:

- Step 1** In the Navigation pane, right-click **LAG** under an Ethernet switch, and then click **Provision Switchport LAG**.
- Step 2** In the **Port** dialog, specify values for the provisionable parameters of the LAG, or accept the default settings. See [A.4.7, “UNI, NNI E-NNI and switchport LAG parameters”](#).
- Step 3** Click **Apply**, then click **Close**.

You have successfully completed this procedure.

## A.4.3 Map customer VLANs to a link aggregation group

### Prerequisites

- The LAG has been created.
- Static VLANs have been provisioned. See [A.6.1, “Provision a Static VLAN”](#).
- Only applies to 802.1ad provisioned LAGs (Switchports)

### Mapping customer VLANs to a link aggregation group

Follow these steps to map a customer VLAN to a link aggregation group on an Ethernet switch:

- Step 1** In the toolbar, click the **Packet Ethernet** icon, to list the Ethernet switches.  
Expand **Virtual Switches**.

**Step 2** Navigate to **Virtual Switches > Switch <x> > LAG**.

Expand **LAG**, and right-click on the LAG you are configuring.

**Step 3** Select **Map Customer VLANs**; the Customer VLAN mapping dialog appears.

**Step 4** Click **New** to enable the **Map Details** configuration options. Enter values in the following fields:

- **Customer VLAN Range Start** — the first VLAN in the range. Enter a value from 2 to 4090.
- **Customer VLAN Range End** — the last VLAN in the range. Enter a value that is greater than the value specified as the start value of the range.
- **Service VLAN** — the SVLAN to which the customer VLAN will be mapped

**Step 5** Click **Apply**.

**Step 6** Click **Close**.

You have successfully completed this procedure.

## A.4.4 Delete a customer VLAN mapping from a link aggregation group

### Prerequisites

- The customer VLAN mapping has been created.
- Only applies to 802.1ad provisioned LAGs (Switchports).

### Deleting a customer VLAN mapping from a link aggregation group

Follow these steps to delete a customer VLAN mapping from a link aggregation group on an Ethernet switch:

**Step 1** In the toolbar, click the **Packet Ethernet** icon, to list the Ethernet switches.

Expand **Virtual Switches**.

**Step 2** Navigate to **Virtual Switches > Switch <x> > LAG**.

Expand **LAG**, and right-click on the LAG you are configuring.

**Step 3** Select **Map Customer VLANs**; the Customer VLAN mapping dialog appears.

**Step 4** From the **Customer VLANs** panel, select the mapping you want to delete and click **Delete**.

The mapping entry is removed from the **Customer VLANs** list.

**Step 5** Click **Close**.

You have successfully completed this procedure.

## A.4.5 View or modify link aggregation group settings

### Prerequisites

- The LAG has been created.

### Viewing or modifying link aggregation group settings

Follow these steps to view or modify a link aggregation group on an Ethernet switch:

**Step 1** In the Navigation pane, right-click the LAG whose settings you want to view or modify, then click **Provision LAG**.

**Step 2** In the **LAG** dialog, click a tab to view the corresponding parameters, or modify the provisionable parameters on the tab, then click **Apply**. See [A.4.7, “UNI, NNI E-NNI and switchport LAG parameters”](#).

Depending on the parameters that were modified, a confirmation dialog may display.

**Step 3** Click **Apply**, then click **Close**.

You have successfully completed this procedure.

## A.4.6 Delete a link aggregation group

### Prerequisites

- The link aggregation group has been created.

### Deleting a link aggregation group

Follow these steps to delete a link aggregation group on an Ethernet switch:

**Step 1** In the Navigation pane, right-click the LAG you want to delete, and then click **Delete LAG**.

**Step 2** In the confirmation dialog, click **Yes**.

You have successfully completed this procedure.

## A.4.7 UNI, NNI E-NNI and switchport LAG parameters

Table A- 14 General LAG parameters

Type	Parameter	Range of Values	Description
Ethernet	Port Number	1 to 48	The number of the port
	Port Type	1: Gigabit 2: TenGigabit	The port type
	MAC address	Integer expressed as 00-00-00-00-00-00	The MAC address



**Table A- 14 General LAG parameters (Continued)**

Type	Parameter	Range of Values	Description
	Interface type	PNP (provider network port) CEP (customer edge port) CNP Port-Based (customer network port port-based)	The port type <b>Note</b> Provisionable on switchports only.
State Management	Layer 2 Status: Admin	Enabled (default) Disabled	The Layer 2 state of the port
	Layer 1 Status: Admin	Enabled (default) Disabled	The Layer 1 state of the port
	Status Qualifier	See the <i>Operations Solutions Guide</i> .	The primary and secondary states of the port
Settings	Minimum Links	1 to 8	The minimum number of LAG member ports that must be in a link-up state, before the LAG can transition into a link-up state.
	Maximum Links	1 to 8	The maximum number of LAG member ports. If the number of member ports exceeds the maximum value set, the ports with the lower LACP priority become active.
LAG Port List	Available Ports	Available provisioned ports	
	Ports in LAG	Provisioned ports added (i.e., user-specified) from the Available Ports list	

**Table A- 15 Layer 2 LAG parameters (UNI ,NNI and E-NNI only)**

Type	Parameter	Range of Values	Description
General	PVID	2 to 4090	The Port VLAN Identifier assigned to either untagged or priority tagged frames.
	Default Priority	0 to 7 Default = 0	The default priority for untagged traffic entering a tag-enabled port
	Control Frame	Profile name	The Control Frame profile to be used
	Allowed Frame Type	All Tagged Untagged Priority Tagged	The frame types allowed by the port
	Use DEI	True False	Indicates whether the port can use DEI bit on the S-TAG to lookup the PCP decoding table
	TPID	0x8100 0x88a8	The default priority for untagged traffic entering a tag-enabled port

**Table A- 15 Layer 2 LAG parameters (UNI ,NNI and E-NNI only) (Continued)**

Type	Parameter	Range of Values	Description
		0x9100	
	Ingress Filtering	True (default) False	Enables or disables ingress filtering
			<b>Note</b> This control does not affect VLAN-independent BPDU frames, such as GVRP and STP.
QoS	Egress Bandwidth	Profile name Not specified	The Egress Bandwidth profile to be used
	Ingress Bandwidth	Profile name Not specified	The Bandwidth profile to be used
	Scheduler	DEFAULT_SCHEDULER_PROFILE	The Scheduler profile to be used
	Priority TC Map	Profile name	The Priority TC Map profile to be used
	DSCP PHB	Default DSCP PHB Profile Not specified	The DSCP PHB profile to be used
	Trust Incoming DSCP	True False	Indicates whether the DSCP field of the incoming packet can be trusted or is ignored
	PCP Enc/Dec	Default 8POD Profile Default 7P1D Profile Default 6P2D Profile Default 5P3D Profile Not specified	The PCP Encoding/Decoding profile to be used
	Trust Incoming PCP	True False	Indicates whether the PCP field of the incoming packet can be trusted or is ignored
UNI	Service Type	Virtual Single	The service type of the UNI
		Private	
		Unspecified	
		Virtual Untagged	
		Virtual Multiple	
	Max Frame Size	1518 to 9600	The maximum frame size
	Customer PVID	0 to 4094	The customer PVID number
NNI / E-NNI	Max Frame Size	1518 to 9600	The maximum frame size
			<b>Note</b> Applies to NNI / E-NNI ports only.

**Table A- 16 Layer 1 LAG parameters**

Type	Parameter	Range of Values	Description
General	Distribution	Source MAC	The distribution for the LAG
		Source and Destination MAC	
		Destination MAC	
		Source and Destination IP	
		Source IP	
		Destination IP	
	MAC Selection	Dynamic Disable	The MAC selection mode
	MTU Size	1518 to 9600 bytes	Maximum transmission unit (MTU) of the IP port
LACP Mode	Mode	not specified active passive on	Set the LACP mode

**Table A- 17 Service parameters**

Type	Description
Name	Name of the service
Type	Service type
Administrative state	Administrative state of the service
Operational state	Operational state of the service
SVLAN	SVLAN of the service
Unavailable seconds	Unavailable seconds

**Table A- 18 GVRP parameters**

Type	Parameter	Range of Values	Description
Settings	Admin State	Enable	The GVRP status
		Disable	
	Restricted VLAN Registration	Enable Disable	The VLAN-registration status

## A.5 Managing profiles

---

packetVX modules are pre-configured with a set of default profiles, described in the following table.

Profile Name	Profile Type
Default _5P3D_Profile	PCP Encoding Decoding
Default _6P2D_Profile	PCP Encoding Decoding
Default _7P1D_Profile	PCP Encoding Decoding
Default _8P0D_Profile	PCP Encoding Decoding
Default_CEP_Profile	Control Frame
Default_CNP_Profile	Control Frame
Default_DSCP_PHB_Profile	DSCP PHB
Default _EPLAN_Profile	Control Frame
Default _EPLINE_Profile	Control Frame
Default_EVP_All_Profile	Control Frame
Default_Priority_TC_Map_Profile	Priority Traffic Class Map
Default_Scheduler_Profile	Scheduler
Default_TMA_Profile	Tunnel MAC Address
Default_UNI_Profile	Control Frame

Also, you can create any of the following types of profile:

- Bandwidth
- Class Map
- Control Frame
- Priority Traffic Class Map
- Scheduler
- Service Policy
- SLA Measurement
- Tunnel MAC Address

New profiles can be either created from scratch or based on certain default profiles, and then modified or deleted as required.

**Note** Default profiles cannot be modified or deleted.

### A.5.1 Create a profile

#### Prerequisites

- The packetVX module is provisioned.

## Creating a profile

Follow these steps to create a profile for a packetVX module:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Profile Manager**, and then click **Display Profile Manager**.
- Step 3** In the **Profile Manager** dialog, do one of the following on the **Provisioning** tab:
- In the **Profiles** list, choose a default profile that can be copied, and then click **Copy**.
  - Click **New**, choose a profile type in the **Select New Profile to Create** dialog, and then click **Select**.
- Step 4** Specify values for the provisionable parameters of the profile. See the following:
- [A.5.4, “Bandwidth profile parameters”](#)
  - [A.5.5, “Class Map profile parameters”](#)
  - [A.5.6, “Control Frame profile parameters”](#)
  - [A.5.7, “Priority Traffic Class Map profile parameters”](#)
  - [A.5.8, “Scheduler profile parameters”](#)
  - [A.5.9, “Service Policy profile parameters”](#)
  - [A.5.10, “Tunnel MAC Address profile parameters”](#)

<b>Note</b>	If a new profile was created in the previous step, the profile must be named. If the profile was copied, it must be given a new name.
-------------	---

- Step 5** Click **Apply**, then click **Close**.
- The name of the profile appears in the **Profiles** list.

You have successfully completed this procedure.

## A.5.2 View or modify profile settings

### Prerequisites

- The profile has been created.

### Viewing or modifying profile settings

Follow these steps to view or modify a profile's settings:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Profile Manager**, and then click **Display Profile Manager**.

**Step 3** In the **Profile Manager** dialog, select any profile other than a default profile in the **Profiles Name** list on the **Provisioning** tab.

Read-only information for the profile appears below the **Profiles** list.

**Step 4** Click **Edit**.

**Step 5** Revise the modifiable parameters of the profile as required. See the following for information:

- [A.5.4, “Bandwidth profile parameters”](#)
- [A.5.5, “Class Map profile parameters”](#)
- [A.5.6, “Control Frame profile parameters”](#)
- [A.5.7, “Priority Traffic Class Map profile parameters”](#)
- [A.5.8, “Scheduler profile parameters”](#)
- [A.5.9, “Service Policy profile parameters”](#)
- [A.5.10, “Tunnel MAC Address profile parameters”](#)

**Step 6** Click **Apply** and then click **Close**.

You have successfully completed this procedure.

## A.5.3 Delete a profile

### Prerequisites

- The profile has been created.

### Deleting a profile

Follow these steps to delete a profile for a packetVX module:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Profile Manager**, and then click **Display Profile Manager**.

**Step 3** In the **Profile Manager** dialog, select a profile in the **Profiles** list on the **Provisioning** tab.

**Step 4** Click **Delete**.

**Step 5** In the confirmation dialog, click **Yes** and then click **Close**.

You have successfully completed this procedure.

## A.5.4 Bandwidth profile parameters

Table A- 19 Bandwidth profile parameters

Parameter	Description	Range of Values	Default Value
Name	The name of the profile	32-character string (A-Z, a-z, 0-9, _ (underscore) only)	Not applicable
DSCP Conform Action	The DSCP (Differentiated Services Code Point) filter applied to traffic that conforms to the profile	0 to 63 af11 af12 af13 af21 af22 af23 af31 af32 af33 af41 af42 af43 cs1 cs2 cs3 cs4 cs5 cs6 cs7 ef	Not applicable
TOS Conform Action	The TOS (Type of Service) priority for traffic that conforms to the profile	Not used Do not change Change	Not applicable
DEI Exceed Action	The dei bit is set on traffic that exceeds the Committed Information Rate (CIR) bandwidth limit.	Enable Disable	Enable
DSCP Exceed Action	The DSCP value set on transmitted frames	Integer (0-63)	Not applicable
PM Monitor Counter Mode	The performance monitoring mode	Conform and Exceed Conform Violate Not Used Violate and Exceed	Not applicable
Meter Color Aware	The mode that the Meter engine will operate	Color Blind	Not applicable

**Table A- 19 Bandwidth profile parameters (Continued)**

Parameter	Description	Range of Values	Default Value
		Color Aware	
Meter Mode	The metering engine scheme used	Not used TR TCM SR TCM	Not applicable
Meter CIR (kbps)	The Committed Information Rate	64 kbps to 10 Gbps	1000 kbps
Meter CBS (kbytes)	The Committed Burst Size	4 to 2048 KiBytes (KiB)	8 KiB
Meter EIR (kbps)	The Excess Information Rate.	64 kbps to 10 Gbps	1000 kbps
Meter EBS (kbytes)	The Excess Burst Size	0 to 2048 KiB	8 Kib
Internal Priority	The internal priority for the profile	0 to 7	Not applicable

**Note** The CLI uses the following commands, in place of the term **Meter** to configure a bandwidth profile, as described in section 8.3.3, “[Configuring bandwidth profiles](#)”:

- police cir
- police cbs
- police eir
- police ebs

## A.5.5 Class Map profile parameters

**Table A- 20 Class Map profile parameters**

Parameter	Description	Range of Values	Default Value
Name	User-specified name of the profile	32-character string (A-Z, a-z, 0-9, _ (underscore) only)	Not applicable
Type	The type of class map profile	Egress per CoS Ingress per CoS	Not applicable
Match Type	Defines the filter action	match all	match all
CVLAN	The VLAN ID to be mapped.  When matching a range of VLANs, this field is used for the range start value.	1 to 4094  <b>Note</b> For matching a range of VLANs, the value must be a power of 2, and the start VLAN ID must be a multiple of the range.	Not applicable
CVLAN End	The VLAN ID end value when matching a range of VLANs.	1 to 4094  <b>Note</b> For matching a range of VLANs, the value must be a power of 2,	Not applicable



Table A- 20 Class Map profile parameters (Continued)

Parameter	Description	Range of Values	Default Value
		and the start VLAN ID must be a multiple of the range.	
CVLAN Priority	The CVLAN priority filter	0 to 7	Not applicable
SVLAN Priority	The SVLAN priority filter	0 to 7	Not applicable
Source IP Address	The source IP address	Valid IPv4 address	Not applicable
Source Netmask	A valid IP mask	An IP address in dotted notation; i.e., 0.0.0.0 – 255.255.255.255	Not applicable
Destination IP Address	The destination IP address	Valid IPv4 address	Not applicable
Destination Netmask	A valid IP mask	An IP address in dotted notation; i.e., 0.0.0.0 – 255.255.255.255	Not applicable
IP Protocol	The IP filter	0 to 255	Not applicable
DSCP	The DSCP filter value	0 to 63	Not applicable
	<b>Note</b> Applies only when Type = Ingress per CoS.		
L4 Source Port	The source TCP/IP port number	0 to 65535	Not applicable
L4 Source Port End	The source TCP/IP port end number	0 to 65535	Not applicable
L4 Destination Port	The destination TCP/IP port number	0 to 65535	Not applicable
L4 Destination Port End	The destination TCP/IP port end number	0 to 65535	Not applicable
TCP Control	The TCP Control filter	0 to 63	Not applicable
Source MAC Address	The source MAC address	Valid MAC address	Not applicable
Destination MAC Address	The destination MAC address	Valid MAC address	Not applicable
Ethernet Type	The Ethernet type filter	0 to 65535	Not applicable
Source MAC Mask	The source MAC mask address	Valid MAC address	Not applicable
Destination MAC Mask	The destination MAC mask address	Valid MAC address	Not applicable

## A.5.6 Control Frame profile parameters

Table A- 21 Control Frame profile parameters

Parameter	Description	Range of Values
Name	The name of the profile	32-character string (A-Z, a-z, 0-9, _ (underscore) only)

**Table A- 21 Control Frame profile parameters (Continued)**

Parameter	Description	Range of Values
LACP	The behavior of the control packet for the LACP protocol	Discard Peer Tunnel  <b>Note</b> When applied to a LAG interface, the value of "LACP" must be set to "peer".
STP	The behavior of the control packet for the STP protocol	Discard Peer Tunnel
Dot1x	The behavior of the control packet for the Dot1x protocol	Discard Peer Tunnel  <b>Note</b> When applied to a LAG interface, the value of "Dot1x" must be set to "peer".
GVRP	The behavior of the control packet for the GVRP protocol	Discard Peer Tunnel
GMRP	The behavior of the control packet for the GMRP protocol	Discard Peer Tunnel
LLDP	The behavior of the control packet for the LLDP (Link Layer Discovery) protocol	Discard Peer Tunnel

## A.5.7 Priority Traffic Class Map profile parameters

**Table A- 22 Priority Traffic Class Map profile parameters**

Parameter	Description	Range of Values	Default Value
Name	User-specified name of the profile	32-character string (A-Z, a-z, 0-9, _ (underscore) only)	Not applicable
Priority 7	The egress (CoS) queue mapped to the priority	0 to 7	7
Priority 6	The egress (CoS) queue mapped to the priority	0 to 7	6
Priority 5	The egress (CoS) queue mapped to the priority	0 to 7	5
Priority 4	The egress (CoS) queue mapped to the priority	0 to 7	4

**Table A- 22 Priority Traffic Class Map profile parameters (Continued)**

Parameter	Description	Range of Values	Default Value
Priority 3	The egress (CoS) queue mapped to the priority	0 to 7	3
Priority 2	The egress (CoS) queue mapped to the priority	0 to 7	2
Priority 1	The egress (CoS) queue mapped to the priority	0 to 7	0
Priority 0	The egress (CoS) queue mapped to the priority	0 to 7	1

## A.5.8 Scheduler profile parameters

Note: To achieve the desired priority for traffic that passes through a packetVX 80 module, we recommend that you use a weight value that is divisible by two, when configuring the class of service (CoS) queue on any packetVX. If you use a weight of one or use consecutive weight values, the packetVX 80 does not forward traffic as expected.

**Table A- 23 Scheduler profile parameters**

Parameter	Description	Range of Values	Default Value
Name	User-specified name of the profile	32-character string (A-Z, a-z, 0-9, _ (underscore) only)	Not applicable
Algorithm	The schedule algorithm	Weighted Round Robin Round Robin Strict Priority Strict Priority + Deficit Round Robin Strict Priority + Weighted Round Robin Deficit Round Robin	Not applicable
Queue 0 Weight	The weight of the Cos Queue	0 to 255	1
Queue 1 Weight	The weight of the Cos Queue	0 to 255	1
Queue 2 Weight	The weight of the Cos Queue	0 to 255	1
Queue 3 Weight	The weight of the Cos Queue	0 to 255	1
Queue 4 Weight	The weight of the Cos Queue	0 to 255	1
Queue 5 Weight	The weight of the Cos Queue	0 to 255	1
Queue 6 Weight	The weight of the Cos Queue	0 to 255	1

**Table A- 23 Scheduler profile parameters (Continued)**

Parameter	Description	Range of Values	Default Value
Queue 7 Weight	The weight of the Cos Queue	0 to 255	1
Queue 1 Min Bandwidth (kbps)	The minimum bandwidth for the CoS queue	0 to 10000000	0
Queue 1 Max Bandwidth (kbps)	The maximum bandwidth for the CoS queue	0 to 10000000	0
Queue 2 Min Bandwidth (kbps)	The minimum bandwidth for the CoS queue	0 to 10000000	0
Queue 2 Max Bandwidth (kbps)	The maximum bandwidth for the CoS queue	0 to 10000000	0
Queue 3 Min Bandwidth (kbps)	The minimum bandwidth for the CoS queue	0 to 10000000	0
Queue 3 Max Bandwidth (kbps)	The maximum bandwidth for the CoS queue	0 to 10000000	0
Queue 4 Min Bandwidth (kbps)	The minimum bandwidth for the CoS queue	0 to 10000000	0
Queue 4 Max Bandwidth (kbps)	The maximum bandwidth for the CoS queue	0 to 10000000	0
Queue 5 Min Bandwidth (kbps)	The minimum bandwidth for the CoS queue	0 to 10000000	0
Queue 5 Max Bandwidth (kbps)	The maximum bandwidth for the CoS queue	0 to 10000000	0
Queue 6 Min Bandwidth (kbps)	The minimum bandwidth for the CoS queue	0 to 10000000	0
Queue 6 Max Bandwidth (kbps)	The maximum bandwidth for the CoS queue	0 to 10000000	0
Queue 7 Min Bandwidth (kbps)	The minimum bandwidth for the CoS queue	0 to 10000000	0
Queue 7 Max Bandwidth (kbps)	The maximum bandwidth for the CoS queue	0 to 10000000	0
MTU Quanta	The maximum frame size for the profile	byte16k byte2k	Not applicable
<b>Note</b> Applies only when Algorithm = Deficit Round Robin (DDR) or Strict Priority + Weighted Round Robin (SP + WRR).			

## A.5.9 Service Policy profile parameters

Table A- 24 Service Policy profile parameters

Parameter	Description	Range of Values	Default Value
Name	User-specified name of the profile	32-character string (A-Z, a-z, 0-9, _ (underscore) only)	Not applicable
Class Map	The Class Map assigned to the profile	A valid Class Map	Not applicable
Bandwidth Profile	The Bandwidth profile assigned to the profile	A valid Bandwidth profile	Not applicable

## A.5.10 Tunnel MAC Address profile parameters

Table A- 25 Tunnel MAC Address profile parameters

Parameter	Description	Range of Values	Default Value
Name	User-specified name of the profile	32-character string (A-Z, a-z, 0-9, _ (underscore) only)	Not applicable
LACP	The destination MAC address for the LACP tunneling protocol	Valid MAC address	Not applicable
STP	The destination MAC address for the STP tunneling protocol	Valid MAC address	Not applicable
Dot1x	The destination MAC address for the Dot1x tunneling protocol	Valid MAC address	Not applicable
GVRP	The destination MAC address for the GVRP tunneling protocol	Valid MAC address	Not applicable
GMRP	The destination MAC address for the GMRP tunneling protocol	Valid MAC address	Not applicable
LLDP	The destination MAC address for the LLDP tunneling protocol	Valid MAC address	Not applicable

## A.6 Provisioning VLANs

---

This section provides information about provisioning static VLANs and adding member switchports.

**Note** VLAN provisioning is typically performed using MEF E-Service provisioning. However, when GVRP is not required, static VLANs can be used and provisioned.

### A.6.1 Provision a Static VLAN

#### Prerequisites

- The Ethernet switch is provisioned.

#### Provisioning a Static VLAN

Follow these steps to provision a Static VLAN on an Ethernet switch:

- Step 1** In the toolbar, click on the **Packet Ethernet** icon.
- Step 2** In the Navigation pane, navigate to the Switch that you are configuring. Expand the Switch view and navigate to **VLANs**. Expand **VLANs** and right-click **Static VLANs**. Click **Provision Static VLANs**. The **Static VLANs (Switch)** dialog appears.
- Step 3** In the **VLANs** section, click **New**.
- Step 4** In the **Settings** section, specify the following VLAN parameters:
- **ID** — the VLAN identifier (1 to 4090)
  - **MAC Learning** — the state of unicast MAC address learning (**Enable** or **Disable**)
  - **Admin State** — the administrative state of the VLAN (**Enable** or **Disable**)
- Step 5** On the **Members** tab, select ports from the **Available Ports** list that you want to move to the **Member Ports** list, and then click >>.
- Step 6** Select ports from the **Member Ports** list that you want to add to the **Untagged Ports** list, and then click >>.
- Step 7** On the **Forbidden** tab, select ports from the **Available Ports** list that you want to move to the **Forbidden Ports** list, and then click >>.
- Step 8** Click **Apply**, then click **Close**.

You have successfully completed this procedure.

## A.6.2 View or modify a Static VLAN

### Prerequisites

- The VLAN is provisioned.

### Viewing or modifying a Static VLAN

Follow these steps to view and, if necessary, modify a Static VLAN on an Ethernet switch:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Static VLANs** under **VLANS** for a packetVX module, and then click **Provision Static VLANs**.

**Step 3** In the **Static VLANs** dialog, select a VLAN in the **VLANS** list.  
The VLAN settings appear in the **Settings** section.

**Step 4** Modify the VLAN settings as required.

**Note** The VLAN ID cannot be changed.

**Step 5** Click **Apply**, then click **Close**.

You have successfully completed this procedure.

## A.6.3 Delete a Static VLAN

### Prerequisites

- The VLAN is provisioned.

### Deleting a Static VLAN

Follow these steps to delete a static VLAN on an Ethernet switch:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Static VLANs** under the **VLAN** folder for a switch on a packetVX module, and then click **Provision Static VLANs**.

**Step 3** In the **Static VLANs** dialog, select a VLAN in the **VLANS** list.

**Step 4** Click **Delete**.

**Note** If members or forbidden members exist, you will receive an error message. These errors must be addressed before you can delete the VLAN.

**Step 5** In the confirmation dialog, click **Yes**.

**Step 6** Click **Close**.

You have successfully completed this procedure.



## A.7 Provisioning Ethernet services

This section provides information about provisioning EPLINE, EPLAN, EVPLINE, EVPLAN, EPTREE, and EVPTREE services on an Ethernet switch.

### A.7.1 Provision an Ethernet service

#### Prerequisites

- The packetVX module is provisioned.
- UNIs, NNIs and E-NNIs must be provisioned.

#### Provisioning an Ethernet service

Follow these steps to provision an Ethernet service:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Ethernet Services**, then click **Provision Ethernet Services**.

**Step 3** In the **Ethernet Services** dialog, click **New**, choose one of the following Ethernet service types in the **Select Ethernet Service Type** dialog, then click **Select**:

- EPLINE
- EPLAN
- EPTREE
- EVPLINE
- EVPLAN
- EVPTREE

**Step 4** In the **Create Ethernet Service** dialog, specify the provisionable settings on the **Service** tab, then click **Apply**. See [A.7.7, “Ethernet service parameters”](#).

<b>Note</b>	The <b>UNIs/NNIs</b> and <b>CFM</b> tabs are not available until the settings specified on the <b>Service</b> tab are applied.
-------------	--

The name of the service appears in the **Provisioned Ethernet Services** list in the **Ethernet Services** dialog.

**Step 5** Click the **UNIs/NNIs** tab, then click **Add** to add a UNI, NNI to the service.

**Step 6** In the **Add UNIs / NNIs / E-NNIs to Service** dialog, select an applicable port from the **Ports** list, specify the port settings as required, click **Apply** then click **Close**. See [A.7.8, “UNI, NNI and E-NNI parameters for Ethernet services”](#).

The port appears in the **Associated Ports** list on the **UNIs/NNIs** tab.

**Step 7** On the **CFM** tab, specify the provisionable parameters, then click **Apply**. See [A.9.8, “CFM parameters for Ethernet services”](#).

**Step 8** Click **Close** on each open dialog box.

You have successfully completed this procedure.

## A.7.2 Add a UNI, NNI or E-NNI to an Ethernet service

- The Ethernet service is provisioned.

### Adding a UNI, NNI or E-NNI to an Ethernet service

Follow these steps to add a UNI , NNI or E-NNI port to an Ethernet service :

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Ethernet Services**, then click **Provision Ethernet Services**.

**Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, then click **View**.

**Step 4** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab, then click **Add**.

**Step 5** In the **Add UNIs / NNIs to Service** dialog, choose a UNI, NNI port in the **Ports** list.

**Step 6** Specify the provisionable parameters for the port, click **Apply**, then click **Close**. See [A.7.8, “UNI, NNI and E-NNI parameters for Ethernet services”](#) for information.

The port appears in the **Associated Ports** list on the **UNIs/NNIs** tab.

**Step 7** For an EPTREE or EVPTREE service, configure the UNI ports as root or leaf UNIs, as follows:

- a) Add UNIs to the EPTREE or EVPTREE service as instructed above.
- b) In the **Associated Ports** list, select the UNI port to configure, then click **Edit**.
- c) From the drop-down menu in the **E-Tree Forwarding** field, select **normal** to configure a root UNI, or **etree-leaf** (default) to configure a leaf UNI.

<b>Note</b>	To configure an E-TREE service, at least one UNI must be configured as a leaf, otherwise the service is E-LAN.
-------------	--

**Step 8** Click **Close** to close the **View Ethernet Service** dialog.

**Step 9** Click **Close** to close the **Ethernet Service** dialog.

You have successfully completed this procedure.

### A.7.3 Modify UNI, NNI or E-NNI settings for an Ethernet service

#### Prerequisites

- The UNI, NNI or E-NNI has been added to the Ethernet service.

#### Modifying UNI , NNI or E-NNI settings for an Ethernet service

Follow these steps to modify UNI , NNI or E-NNI settings for an Ethernet service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Ethernet Services**, then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **View**.
- Step 4** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab.
- Step 5** Select a port from the **Associated Ports** list, then click **Edit**.
- Step 6** In the **Edit Service** dialog for the UNI , NNI or E-NNI Association, modify the provisionable parameters for the port, click **Apply**, then click **Close**. See [A.7.8, “UNI, NNI and E-NNI parameters for Ethernet services”](#) for information.
- Step 7** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

### A.7.4 Delete a UNI, NNI or E-NNI from an Ethernet service

#### Prerequisites

- The UNI, NNI or E-NNI has been added to the Ethernet service.

#### Deleting a UNI, NNI or E-NNI from an Ethernet service

Follow these steps to delete a UNI, NNI or E-NNI from an Ethernet service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Ethernet Services**, then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, then click **View**.
- Step 4** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab.

**Step 5** Select a port from the **Associated Ports** list, then click **Delete**.

**Step 6** In the confirmation dialog, click **Yes**.

The port is removed from the **Associated Ports** list.

**Step 7** Click **Close** to close the **View Ethernet Service** dialog.

**Step 8** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.7.5 View or modify an Ethernet service

### Prerequisites

- The Ethernet service is provisioned.

### Viewing or modifying an Ethernet service

Follow these steps to view and, if necessary, modify an Ethernet service:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Ethernet Services**, then click **Provision Ethernet Services**.

**Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, then click **View**.

**Step 4** In the **View Ethernet Service** dialog, click a tab to view the corresponding parameters, or modify the provisionable parameters on the tab and click **Apply**. See the following topics for information:

- [A.7.7, “Ethernet service parameters”](#)
- [A.7.8, “UNI, NNI and E-NNI parameters for Ethernet services”](#)
- [A.9.8, “CFM parameters for Ethernet services”](#)

**Step 5** Click **Close** to close the **View Ethernet Service** dialog.

**Step 6** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.7.6 Delete an Ethernet service

### Prerequisites

- The Ethernet service is provisioned.

## Deleting an Ethernet service

Follow these steps to delete an Ethernet service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Ethernet Services**, then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, then click **Delete**.
- Step 4** In the **Delete Service** dialog, click **Yes**.
- Step 5** Click **Close** on each open dialog box.

You have successfully completed this procedure.

## A.7.7 Ethernet service parameters

The table below lists the parameters that can be configured for the following Ethernet services:

- EPLAN
- EPLINE
- EPTREE
- EVPLAN
- EVPLINE
- EVPTREE

**Table A- 26 Ethernet service parameters**

Type	Parameter	Description	Range of Values	Default Value
Settings	Name	User-specified name of the service	Up to 256 alphanumeric characters	Not applicable
	SVLAN	The VLAN identifier	2 to 4090	Not applicable
	Frame Size	The maximum frame size	1522 to 9600 bytes	1522
	Type	The type of service	The selected Ethernet service type	
	Translate CVLAN	The CVLAN ID translation	True False	False
	Spanning Tree Instance	The Spanning Tree identification number	0 to 16	0
	Lock NNIs	Enables (checked) or disables (unchecked) locking NNIs. If enabled, the switch will not allow any dynamic VLAN protocols, such as GVRP, to add NNIs to the service.	Checked (enabled) Unchecked (disabled)	Unchecked

**Table A- 26 Ethernet service parameters (Continued)**

Type	Parameter	Description	Range of Values	Default Value
	Access Service	Enables (checked) or disables (unchecked) the flag for the service acting as an access service.	Checked (enabled) Unchecked (disabled)	Unchecked
State Management	Administrative State	The administrative state of the service	Enable Disable	Enable
	Operational State	The operational state of the service	Up Down Partial Connected	Not applicable

### A.7.8 UNI, NNI and E-NNI parameters for Ethernet services

The table below lists the UNI, NNI and E-NNI parameters that can be configured for the following Ethernet services:

- EPLAN
- EPLINE
- EPTREE
- EVPLAN
- EVPLINE
- EVPTREE

**Table A- 27 UNI NNI and E-NNI Ethernet service parameters**

Type	Parameter	Description	Range of Values	Default Value
Ports	Port	The UNI, NNI or E-NNI to be associated to the Ethernet service	Applicable ports	Not applicable
	EFPSD Enabled	For an EPLINE service, enables (checked) or disables (unchecked) Ethernet fault propagation shutdown (EFPSD)	Checked (enabled) Unchecked (disabled)	Unchecked (disabled)
Profiles	Ingress Bandwidth	The Bandwidth profile to be used on ingress frames	Bandwidth profile Not specified	Not specified
	Ingress Service Policy	The Service Policy profile to be used on ingress frames	Service Policy profile Not specified	Not specified
	Egress Bandwidth	The Bandwidth profile to be used on egress frames	Bandwidth profile Not specified	Not specified
	Egress Service Policy	The Service Policy profile to be used on egress frames	Service Policy profile Not specified	Not specified

**Table A- 27 UNI NNI and E-NNI Ethernet service parameters (Continued)**

Type	Parameter	Description	Range of Values	Default Value
CVLAN ID Mapping	Range Start	The first ID in the range of CVLAN identifiers	1 to 4094	Not applicable
	Range End	The last ID in the range of CVLAN identifiers	1 to 4094	Not applicable
SVLAN ID Mapping	SVLAN identifiers	The SVLAN identifiers	1 to 4094	Not applicable
Service Map Filter	Service Map Service Policy	The Service Map Service Policy profile to be used on	Service Map Service Policy Not specified	Not applicable
	Filter Sequence Number	The File Sequence Number to be used		Not applicable
Packet Forwarding	TPID action	Sets the TPID action on EPLINE and EPLAN services.	None Blind Aware	None
Access	S-VLAN translation	Provisions the S-VLAN translation	1 to 4094	0 (Not Used)
E-Tree	Forwarding	Configures a UNI port to be a leaf (Etree-leaf) or a root (Normal) port.	Etree-leaf Normal	Etree-leaf

## A.8 Provisioning Management VLAN Ethernet services

---

This section provides information about provisioning Management VLAN services on an Ethernet switch.

### A.8.1 Provision a Management VLAN Ethernet service

#### Prerequisites

- The packetVX module is provisioned.
- UNIs and NNIs must be provisioned.

#### Provisioning a Management VLAN Ethernet service

Follow these steps to provision a Management VLAN Ethernet service:

<b>Note</b>	You can provision only one Management VLAN Ethernet service per Ethernet switch.
-------------	--

- Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 2** In the **Ethernet Services** dialog, click **New**.
- Step 3** In the **Select Ethernet Service Type** dialog, choose **Management VLAN**, and then click **Select**.
- Step 4** In the **Create Ethernet Service** dialog, specify the provisionable settings on the Service table, and then click **Apply**. See [A.8.7, “Service parameters for Management VLAN services”](#).

<b>Note</b>	The <b>Management VLAN</b> and <b>UNI/NNIs</b> tabs are not available until the settings specified on the <b>Service</b> tab are applied.
-------------	---

The name of the service appears in the **Provisioned Ethernet Services** list in the **Ethernet Services** dialog.

- Step 5** Click the **Management VLAN** tab, specify the settings as required, and then click **Apply**. See [A.8.9, “Management VLAN parameters”](#).
- Step 6** Click the **UNIs/NNIs** tab, and then click **Add** to add a UNI or NNI to the service.
- Step 7** In the **Add UNIs / NNIs to Service** dialog, select an applicable port from the **Ports** list, specify the port settings as required, and then click **Apply**. See [A.8.8, “UNI/NNI parameters for Management VLAN services”](#).

The port appears in the **Associated Ports** list on the **UNIs/NNIs** tab.

- Step 8** Click **Close** on each open dialog box.



You have successfully completed this procedure.

## A.8.2 Add a UNI or NNI to a Management VLAN Ethernet service

### Prerequisites

- The Ethernet service is provisioned.

### Adding a UNI or NNI to a Management VLAN Ethernet service

Follow these steps to add UNI or NNI to a Management VLAN Ethernet service:

- Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 2** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **View**.
- Step 3** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab, and then click **Add**.
- Step 4** In the **Add UNIs / NNIs to Service** dialog, choose a UNI or NNI port in the **Ports** list.
- Step 5** Specify the provisionable parameters for the port, click **Apply**, and then click **Close**. See [A.8.8, “UNI/NNI parameters for Management VLAN services”](#) for information. The port appears in the **Associated Ports** list on the **UNIs/NNIs** tab.
- Step 6** Click **Close** to close the **View Ethernet Service** dialog.
- Step 7** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.8.3 Modify UNI or NNI settings for a Management VLAN service

### Prerequisites

- The UNI or NNI has been added to the Ethernet service.

### Modifying UNI or NNI settings for a Management VLAN service

Follow these steps to modify UNI or NNI settings for a Management VLAN service:

- Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 2** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **View**.
- Step 3** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab.

**Step 4** Select a port from the **Associated Ports** list, and then click **Edit**.

**Step 5** In the **Edit Service** dialog for the UNI or NNI association, modify the provisionable parameters for the port, click **Apply**, and then click **Close** on each open dialog box. See [A.8.8, “UNI/NNI parameters for Management VLAN services”](#) for information.

You have successfully completed this procedure.

## A.8.4 Delete a UNI or NNI from a Management VLAN service

### Prerequisites

- The UNI or NNI has been added to the Ethernet service.

### Deleting a UNI or NNI from a Management VLAN service

Follow these steps to delete a UNI or NNI from a Management VLAN service:

**Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 2** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **View**.

**Step 3** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab.

**Step 4** Select a port from the **Associated Ports** list, and then click **Delete**.

**Step 5** In the confirmation dialog, click **Yes**.

The port is removed from the **Associated Ports** list.

**Step 6** Repeat steps 4 and 5 for all ports listed in the **Associated Ports** list. All associated ports must be deleted before the UNI or NNI can be deleted.

**Step 7** Click **Close** on each open dialog box.

You have successfully completed this procedure.

## A.8.5 View or modify a Management VLAN service

### Prerequisites

- The Ethernet service is provisioned.

### Viewing or modifying a Management VLAN service

Follow these steps to view and, if necessary, modify a Management VLAN service:

**Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 2** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **View**.

**Step 3** In the **View Ethernet Service** dialog, click a tab in the dialog to view the corresponding parameters, or modify the provisionable parameters on the tab and then click **Apply**. See the following topics for information:

- [A.8.7, “Service parameters for Management VLAN services”](#)
- [A.8.8, “UNI/NNI parameters for Management VLAN services”](#)
- [A.8.9, “Management VLAN parameters”](#)

**Step 4** Click **Close**.

**Step 5** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.8.6 Delete a Management VLAN Ethernet service

### Prerequisites

- The Ethernet service is provisioned.

### Deleting a Management VLAN service

Follow these steps to delete a Management VLAN service:

**Step 1** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 2** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **Delete**.

**Step 3** In the **Delete Service** dialog, click **Yes**.

**Step 4** Click **Close** on each open dialog box.

You have successfully completed this procedure.

## A.8.7 Service parameters for Management VLAN services

Table A- 28 Service parameters for Management VLAN

Type	Parameter	Description	Range of Values	Default Value
Settings	Name	User-specified name of the profile	Up to 256 alphanumeric characters	Not applicable
	SVLAN	The VLAN identifier	2 to 4090	Not applicable
	Frame Size	The maximum frame size	1518 to 9600 bytes	1522
	Type	The type of service	The selected Ethernet service type	

**Table A- 28 Service parameters for Management VLAN (Continued)**

Type	Parameter	Description	Range of Values	Default Value
State Management	Translate CVLAN	The CVLAN ID translation	True False	False
	Spanning Tree Instance	The Spanning Tree identification number	0, 1, 64	0
	Administrative State	The administrative state of the service	Enable Disable	Enable
	Operational State	The operational state of the service	Up Down Partial Connected	Not applicable

## A.8.8 UNI/NNI parameters for Management VLAN services

**Table A- 29 UNIs/NNIs parameters for Management VLAN**

Type	Parameter	Description	Range of Values	Default Value
Ports	Port	The UNI or NNI to be associated to the Ethernet service	Applicable ports	Not applicable
Profiles	Ingress Bandwidth	The Bandwidth profile to be used on ingress frames	Bandwidth profile Not specified	Not specified
	Ingress Service Policy	The Service Policy profile to be used on ingress frames	Service Policy profile Not specified	Not specified
	Egress Bandwidth	The Bandwidth profile to be used on egress frames	Bandwidth profile Not specified	Not specified
	Egress Service Policy	The Service Policy profile to be used on egress frames	Service Policy profile Not specified	Not specified
CVLAN ID Mapping	Range Start	The first ID in the range of CVLAN identifiers	1 to 4094	Not applicable
	Range End	The last ID in the range of CVLAN identifiers	1 to 4094	Not applicable

## A.8.9 Management VLAN parameters

**Table A- 30 Management VLAN parameters**

Type	Parameter	Description	Range of Values	Default Value
Settings	IP Address	The IP address for the Management VLAN	Valid IP address	Not applicable
	Subnet Mask	The IP subnet mask for the Management	Integer	Not applicable
	Gateway	The gateway for the Management VLAN	An IP address in dotted notation	Not applicable

**Table A- 30 Management VLAN parameters (Continued)**

Type	Parameter	Description	Range of Values	Default Value
CVLAN (Optional)	CVLAN	The CVLAN identifier	2 - 4090	Not applicable

## A.9 Provisioning CFM for Ethernet services

---

This section provides information about provisioning CFM for the following Ethernet service types:

- EPLAN
- EPLINE
- EPTREE
- EVPLAN
- EVPLINE
- EVPTREE

### A.9.1 Add a MIP to an NNI Ethernet Service

#### Prerequisites

- The Ethernet Service is provisioned and associated with an NNI port.

#### Adding a MIP to an NNI Ethernet Service

Follow these steps to add a MIP to an NNI Ethernet service:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 3** In the **Ethernet Services** dialog, select the Ethernet service from the **Provisioned Ethernet Services** list, and then click **View**.

**Step 4** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab.

**Step 5** On the **UNIs/NNIs** tab, select a port from the **Associated Ports** list, and then click **Add MIP**.

**Step 6** Click **Close**.

**Step 7** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

### A.9.2 Remove a MIP from an NNI Ethernet Service

#### Prerequisites

- A MIP exists on the NNI Ethernet service.

### Removing a MIP from an NNI Ethernet Service

Follow these steps to add an Ethernet service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select the Ethernet service from the **Provisioned Ethernet Services** list, and then click **View**.
- Step 4** In the **View Ethernet Service** dialog, click the **UNIs/NNIs** tab.
- Step 5** On the **UNIs/NNIs** tab, select a port from the **Associated Ports** list, and then click **Remove MIP**.
- Step 6** Click **Close**.
- Step 7** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

### A.9.3 Add a remote MEP to a UNI Ethernet service

#### Prerequisites

- The Ethernet service is provisioned and associated with a UNI port.

#### Adding a remote MEP to a UNI Ethernet service

Follow these steps to add a remote MEP to a UNI Ethernet service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service from the **Provisioned Ethernet Services** list, and then click **View**.
- Step 4** In the **View Ethernet Service** dialog, click the **CFM** tab.
- Step 5** On the **CFM** tab, click **Add Remote MEP**.
- Step 6** In the **Add Remote MEP** dialog, enter a remote MEP ID (1 to 8191), and then click **OK**.  
The remote MEP appears in the **Remote MEPs** list in the **View Ethernet Service** dialog .
- Step 7** Click **Close** to close the **Add Remote MEP** dialog.

**Step 8** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.9.4 Delete a remote MEP from a UNI Ethernet Service

### Prerequisites

- A remote MEP exists on the UNI Ethernet service.

### Deleting a remote MEP from a UNI Ethernet Service

Follow these steps to delete a remote MEP from a CFM:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 3** In the **Ethernet Services** dialog, select a service from the **Provisioned Ethernet Services** list, and then click **View**.

**Step 4** In the **View Ethernet Service** dialog, click the **CFM** tab.

**Step 5** On the **CFM** tab, select an MEP from the **Remote MEPs** list, and then click **Delete Remote MEP**.

The remote MEP is removed from the **Remote MEPs** list.

**Step 6** Click **Close** to close the **View Ethernet Service** dialog.

**Step 7** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.9.5 Flush the remote MEP database of an Ethernet service

### Prerequisites

- A remote MEP exists on the UNI Ethernet service.

### Flushing the remote MEP database of an Ethernet service

Follow these steps to flush the remote MEP database of an Ethernet service:

**Step 1** In the toolbar, click the Packet Ethernet icon.



- Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service from the **Provisioned Ethernet Services** list, and then click **View**.
- Step 4** In the **View Ethernet Service** dialog, click the **CFM** tab, and then click **Flush DB**.
- Step 5** Click **Close** to close the **View Ethernet Service** dialog.
- Step 6** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.9.6 Run a loopback test on a UNI Ethernet Service

### Prerequisites

- A remote MEP exists on the UNI Ethernet service.

### Running a loopback test on a UNI Ethernet Service

Follow these steps to run a loopback test on an Ethernet service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service from the **Provisioned Ethernet Services** list, and then click **View**.
- Step 4** In the **View Ethernet Service** dialog, click the **CFM** tab.
- Step 5** On the **CFM** tab, select an MEP from the **Remote MEPs** list, and then click **Loopback**.

**Note** CFM does not apply to EVPTrees or EPTrees.

- Step 6** In the **Loopback Test** dialog, enter a value (0 to 2147483647) in the **Count** field, and then click **Run Loopback**.

**Note** The value 0 causes the loopback test to run indefinitely.

The loopback test runs the number of times specified in the **Count** field, and the results are displayed.

- Step 7** Click **Close** on each open dialog box.

You have successfully completed this procedure.

## A.9.7 Run a linktrace test on a UNI Ethernet service

### Prerequisites

- A remote MEP exists on the UNI Ethernet service.

### Running a linktrace test on a UNI Ethernet service

Follow these steps to run a linktrace test on an Ethernet service:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provision Ethernet Services**.

**Step 3** In the **Ethernet Services** dialog, select a service from the **Provisioned Ethernet Services** list, and then click **View**.

**Step 4** In the **View Ethernet Service** dialog, click the **CFM** tab.

**Step 5** On the **CFM** tab, select an MEP from the **Remote MEPs** list, and then click **Linktrace**.

**Step 6** In the **Linktrace** dialog for the Ethernet service, enter a value in the **TTL** field, and then click **Run Linktrace**.

The results of the test are displayed in the Results section of the dialog.

**Step 7** Click **Close** on each open dialog.

You have successfully completed this procedure.

## A.9.8 CFM parameters for Ethernet services

The table below lists the CFM parameters for the following Ethernet service types:

- EPLAN
- EPLINE
- EPTREE
- EVPLAN
- EVPLINE
- EVPTREE

**Table A- 31 CFM Ethernet service parameters**

Type	Parameter	Description	Range of Values	Default Value
Settings	Crosscheck	The state of CCM transmission and cross-checking	Enabled Disabled	Disabled

**Table A- 31 CFM Ethernet service parameters (Continued)**

Type	Parameter	Description	Range of Values	Default Value
MEP	ME Name	The name of the CFM Maintenance Entity	1 to 32 alphanumeric characters	Not applicable
	Crosscheck Interval	The interval between CCM transmission and cross-checking	10 seconds 1 minute	1 minute
	MEP ID	The identifier of the remote maintenance endpoint	1 to 8191	Not applicable
	Active State		True False	Not applicable
	Sent CCMs	The number of CCMs transmitted	Integer	0
	MEP ID Type	The method by which the MEP ID type is defined	Autogenerated User Defined	Not specified
	MAC Address	The MAC address	A valid MAC address	Not applicable
Defects	Auto Generated	The status of autogeneration for the MEP	True False	True
	Defects	Defect detected at the remote MEP		Not applicable
	Remote MEP IDs	The Remote MEP on which the defect is detected	MEP ID	Not applicable
Remote MEPs	Remote Switch			Not applicable
	Remote Port			Not applicable
	MEP ID	The remote MEP ID	1 to 8191	Not applicable
	MAC Address		A valid MAC address	Not applicable
	State			Not applicable

## A.10 Provision Ethernet Ring Protection Switching (ERPS)

---

The section provides information about provisioning Ethernet Ring Protection Switching (ERPS) on an Ethernet switch, using the proNX 900 Node Controller .

<b>Note</b>	The proNX 900 does not discover Eservices on BTI software releases earlier than 8.2.
-------------	--

### A.10.1 Provision Ethernet Ring Protection Switching (ERPS)

#### Prerequisites

- The packetVX module is provisioned.

#### Provisioning ERPS

Follow these steps to provision ERPS:

- Step 1** In the toolbar, click the **Packet Ethernet** icon.
- Step 2** In the Navigation pane, navigate to the Switch that is being configured, if necessary, expand to see the options for that Switch.
- Step 3** Right-click **Ethernet Services**, and click **Provision Ethernet Services**.  
The **Ehternet Services** dialog appears.
- Step 4** In the **Ethernet Services** dialog, click **New**.  
The **Select Ethernet Service Type** dialog appears.
- Step 5** In the **Select Ethernet Service Type** dialog, highlight **ERPS** and click **Select**.
- Step 6** In the **Create Ethernet Service** dialog, specify the provisionable settings on the **Service**, **ERPS**, and **NNIs** tabs, clicking **Apply** after working on each tab. See the following topics:
- [A.10.8, “Service and ERPS parameters for ERPS services”](#)
  - [A.10.9, “NNI parameters for ERPS services”](#)

<b>Note</b>	The <b>ERPS</b> and <b>NNIs</b> tabs are not available until the settings specified on the <b>Service</b> tab are applied.
-------------	--

- Step 7** Click **Close**.  
The name of the service appears in the **Provisioned Ethernet Services** list in the **Ethernet Services** dialog.
- Step 8** Click **Close** to close the dialog.

You have successfully completed this procedure.

## A.10.2 Add an NNI to an ERPS service

### Prerequisites

- The ERPS Ethernet service is provisioned.

### Adding an NNI to an ERPS service

Follow these steps to add an NNI to an ERPS service:

- Step 1** In the toolbar, click the **Packet Ethernet** icon.
- Step 2** In the Navigation pane, navigate to the Switch that is being configured; if necessary, expand to see the options for that Switch.
- Step 3** Right-click **Ethernet Services**, and click **Provision Ethernet Services**.  
The **Ehternet Services** dialog appears.
- Step 4** In the **Ethernet Services** dialog, select an ERPS Ethernet service from the list, and click **View**.
- Step 5** In the **View Ethernet Service** dialog, click the **NNIs** tab, and then click **Add** .
- Step 6** In the **Add New NNI Mapping** dialog, select an NNI from the **NNIs** list, and then click **Apply**.  
The NNI is added to the **NNI** list on the **NNIs** tab of the **View Ethernet Service** dialog.
- Step 7** In the **NNI Details** section of the **Add New NNI Mapping** dialog, specify values for the provisionable parameters of the NNI; see [A.10.9, “NNI parameters for ERPS services”](#). Click **Apply**.
- Step 8** Click **Close**.
- Step 9** Click **Close**.

You have successfully completed this procedure.

## A.10.3 Modify NNI settings for an ERPS service

### Prerequisites

- The NNI has been added to the ERPS Ethernet service.

### Modifying NNI settings for an ERPS service

Follow these steps to modify NNI settings for an ERPS service:

- Step 1** In the toolbar, click the Packet Ethernet icon.

- Step 2** In the Navigation pane, navigate to the Switch that is being configured; if necessary, expand to see the options for that Switch.
- Step 3** Right-click **Ethernet Services**, and click **Provision Ethernet Services**.  
The **Ehternet Services** dialog appears.
- Step 4** In the Ethernet Services dialog, select an ERPS Ethernet service from the list, and click **View**.
- Step 5** In the **View Ethernet Service** dialog click the **NNIs** tab.
- Step 6** Select an NNI from the **NNIs** list, and then click **Edit**.
- Step 7** In the **Edit NNI Mapping** dialog, modify the provisionable parameters of the NNI; See [A.10.9, “NNI parameters for ERPS services”](#). Click **Apply**.
- Step 8** Click **Close** on each open dialog.

You have successfully completed this procedure.

## A.10.4 Delete an NNI from an ERPS service

### Prerequisites

- The NNI has been added to the ERPS Ethernet service.

### Deleting an NNI from an ERPS service

Follow these steps to delete an NNI from an ERPS service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, navigate to the Switch that is being configured; if necessary, expand to see the options for that Switch.
- Step 3** Right-click **Ethernet Services**, and click **Provision Ethernet Services**.  
The **Ehternet Services** dialog appears.
- Step 4** In the Ethernet Services dialog, select an ERPS Ethernet service from the list, and click **View**.
- Step 5** In the **View Ethernet Service** dialog, click the **NNIs** tab.
- Step 6** Select an NNI from the **NNIs** list, and click **Delete**.
- Step 7** In the confirmation dialog, click **Yes**.  
The NNI is removed from the **NNIs**list.
- Step 8** Click **Close** to close the **View Ethernet Service** dialog.

**Step 9** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.10.5 Operate a manual or forced protection switch

### Prerequisites

- The Ethernet Service is provisioned and associated with an NNI port.

### Operating a manual or forced protection switch

Follow these steps to operate a manual or forced protection switch:

**Step 1** In the toolbar, click the Packet Ethernet icon.

**Step 2** In the Navigation pane, navigate to the Switch that is being configured; if necessary, expand to see the options for that Switch.

**Step 3** Right-click **Ethernet Services**, and click **Provision Ethernet Services**.  
The **Ehternet Services** dialog appears.

**Step 4** In the **Ethernet Services** dialog, choose an ERPS service from the **Provisioned Ethernet Services** list, and then click **View**.

**Step 5** On the **ERPS** tab, click **Edit** in the **Operations** section.

**Step 6** In the **Operate Switch** dialog, enable **Manual Switch**, **Force Switch**, or **Normal Switch** button, and then select a port from the **On Port** list.

**Step 7** Click **Apply**.

**Step 8** On the **ERPS** tab, click **Close**.

**Step 9** Click **Close**.

**Step 10** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.10.6 View or modify an ERPS service

### Prerequisites

- The Ethernet service is provisioned.

### Viewing or modifying an ERPS service

Follow these steps to view and, if necessary, modify an ERPS service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, navigate to the Switch that is being configured; if necessary, expand to see the options for that Switch.
- Step 3** Right-click **Ethernet Services**, and click **Provision Ethernet Services**.  
The **Ehternet Services** dialog appears.
- Step 4** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** and click **View**.
- Step 5** In the **View Ethernet Service** dialog, click a tab in the dialog to view the corresponding parameters, or modify the provisionable parameters on the tab and then click **Apply**.  
See [A.10.8, “Service and ERPS parameters for ERPS services”](#) and [A.10.9, “NNI parameters for ERPS services”](#).
- Step 6** Click **Close** to close the **View Ethernet Service** dialog.
- Step 7** Click **Close** to close the **Ethernet Services** dialog.

You have successfully completed this procedure.

## A.10.7 Delete an ERPS service

### Prerequisites

- The Ethernet service is provisioned.
- All associations with the ERPS service must be deleted before the ERPS service can be deleted.

### Deleting an ERPS service

Follow these steps to delete an ERPS service:

- Step 1** In the toolbar, click the Packet Ethernet icon.
- Step 2** In the Navigation pane, right-click **Ethernet Services**, and then click **Provisioned Ethernet Services**.
- Step 3** In the **Ethernet Services** dialog, select a service in the **Provisioned Ethernet Services** list, and then click **Delete**.
- Step 4** In the **Delete Service** dialog, click **Yes**.  
The service is removed from the **Provisioned Ethernet Services** list. However, if all associations have not been received, an error message is returned.
- Step 5** Click **Close** to close the dialog.

You have successfully completed this procedure.



## A.10.8 Service and ERPS parameters for ERPS services

Table A- 32 Service parameters for ERPS services

Type	Parameter	Description	Range of Values	Default Value
Settings	Name	User-specified name of the profile	Up to 256 alphanumeric characters	Not applicable
	SVLAN	The VLAN identifier	2 to 4090	Not applicable
	Type	The type of service	The selected Ethernet service type	Not applicable
	Lock NNIs	Indicates the ports are NNIs.	Locked Not Locked	Not applicable
State Management	Administrative State	The administrative state of the service	Enable Disable	Enable
	Operational State	The operational state of the service	Up Down Partial Connected	Not applicable

Table A- 33 ERPS parameters

Type	Parameter	Description	Range of Values	Default Value
Settings	Compatible Version	The version of ERPS that is running on your system.	Version 1 Version 2	Not applicable
	Ring Property	The ring property of the service	Normal Inter-connect	Not applicable
	RPL Node Type	The type of RPL assigned to the node.	RPL Owner Non-RPL Owner	Not applicable
	Down MEG Level	Optional. The MEG level used on CCM messages sent for DOWN MEPs for the Eservice. The Eservice must be disabled to configure MEG levels.	0 to 7 <b>Note</b> If upgrading to ERPS Version 2, the Down MEG level must be set to six, to allow ERPS V1 and V2 nodes in the same ring.	Zero
	Revert Mode	The fault recovery mode	Revertive Non-Revertive	Revertive
	Monitoring	The type of fault management	CFM	Not applicable
	Up MEG Level	Optional. The MEG level used on CCM messages sent for UP MEPs for the Eservice. The Eservice must be disabled to configure MEG levels.	0 to 7	1
Operations	Protection Switch Mode	The protection switch mode	Manual Forced	Clear

**Table A- 33 ERPS parameters (Continued)**

Type	Parameter	Description	Range of Values	Default Value
			Clear	
	on port	The port on which the switch mode is set.	A UNI or NNI port.	Not applicable
Timers	Guard (ms)	The amount of time, in milliseconds, during which earlier R-APS messages in the network are flushed out, and R-APS messages received are ignored	10 to 2000 ms	500 ms
	Periodic (s)	The interval, in seconds, at which periodic R-APS PDUs are transmitted	5 to 10 s	5
	Wait to Block (ms)	The amount of time, in milliseconds, to wait before clearing a manual or forced switch mode.	5500 to 7000 ms	5500 milliseconds
	Hold (ms)	The amount of time during which reporting of the fault is delayed	0 to 10000 ms	0
	Wait to Restore (min)	The amount of time, in minutes, before which the recovered link is returned to operation and RPL is again blocked	5 to 15 mins Short (20s)	5 minutes
		<b>Note</b> This timer applies only when Revert Mode is set to Revertive.		
Status	Ring State	The ring protection status	Enable Disable	Not applicable
Virtual Links	Virtual Channel	Configures the sub-ring to run with or without an R-APS Virtual channel: <ul style="list-style-type: none"> <li>Only configurable in V2 mode.</li> <li>Only effective on nodes in a sub-ring.</li> <li>Can only be configured if ERPS is disabled.</li> </ul>	False: Run with an R-APS Virtual Channel. Both the traffic and R-APS channels are blocked when the ring port is set to blocked state.  True: Run without an R-APS Virtual Channel. The traffic channel is blocked, but the R-APS channel is not blocked, when the ring port is set to blocked state.	False
	VLAN ID	The VLAN identifier	2 - 4090	Not applicable

## A.10.9 NNI parameters for ERPS services

Type	Parameter	Description	Range of Values	Default Value
NNI settings	Ring Protection Link	The state of ring protection	Disable Enable	Disable
	Neighbor	The RPL (ring-protection-link) neighbor node on the ERPS ring.	Disable Enable	Disable
	Next Neighbor	The neighbor node next to the RPL neighbor node, and the neighbor node on the other side of the RPL owner on the ERPS ring.	Disable Enable	Disable
Connectivity Fault Management	ME Name	The unique name of the CFM Maintenance Entity: <ul style="list-style-type: none"> <li>ME-NAMES cannot be the same on a main ring and a sub-ring on the same node.</li> <li>ME-NAMES can be duplicated on links in a ring, if they are on different nodes.</li> </ul>	1 to 32 alphanumeric characters	Not applicable
	Remote MEP ID	The identifier of the remote maintenance endpoint	1 to 8191	Not applicable
	Local MEP ID	The identifier of the local maintenance endpoint	1 to 8191	Not applicable
	ECFM Info	The provisioned information about the ECFM entities in the ring.	System generated	Not applicable

## A.11 Access control list provisioning

---

In an access control list (ACL)-based security model, when a subject requests to perform an operation on an object, the system first checks the list for an applicable entry to decide whether to proceed with the operation.

In networking, ACL refers to a list of rules detailing service ports that are available on a device. Access control lists can generally be configured to control both inbound and outbound traffic, and in this context they are similar to firewalls.

### A.11.1 Add an entry to the Access Control List

#### Prerequisites

- The Ethernet switch is provisioned.

#### Adding an entry to the Access Control List

Follow these steps to add an entry to the Access Control List on an Ethernet switch:

- Step 1** In the Navigation pane, right-click **Access Control** under an Ethernet Switch of a packetVX module, and then click **Display Access Control**.
- Step 2** In the **Access Control** dialog, click **New**.
- Step 3** In the **Access Control Entry** section, enable the **IP Address** or **MAC Address** button.
- Step 4** Specify the source and destination addresses.
- Step 5** Click **Apply**.  
The entry appears in the **Access Control List**.
- Step 6** Click **Close**.

You have successfully completed this procedure.

### A.11.2 Delete an entry from the Access Control List

#### Prerequisites

- The entry appears on the Access Control List.

#### Deleting an entry from the Access Control List

Follow these steps to delete an entry from the Access Control List on an Ethernet switch:

- Step 1** In the Navigation pane, right-click **Access Control** under an Ethernet Switch of a packetVX module, and then click **Display Access Control**.

**Step 2** In the **Access Control** dialog, choose an entry from the **Access Control List**, and then click **Delete**.

**Step 3** In the confirmation dialog, click **Yes** .

The entry is removed from the **Access Control List** in the **Access Control** dialog.

**Step 4** Click **Close**.

You have successfully completed this procedure.

## A.12 Managing Multiple Spanning Tree Protocol (MSTP)

Multiple Spanning Tree Protocol (MSTP) provides the ability to create multiple spanning trees and assign VLANs to a spanning tree that closely reflects its optimal forwarding path. MSTP provides a single Common Spanning Tree Instance (CSTI) that is automatically created and Multiple Spanning Tree Instances (MSTI) that are configured to meet varied forwarding requirements. The packetVX module currently supports up to 16 MSTP instances per switch.

This section provides information about provisioning MSTP.

### A.12.1 Provision Multiple Spanning Tree Protocol (MSTP)

#### Prerequisites

- Ports are provisioned on the Ethernet switch.

#### Provisioning MSTP

Follow these steps to provision MSTP on an Ethernet switch:

**Step 1** In the Navigation pane, right-click **MSTP** under an Ethernet Switch of a packetVX module, then click **Manage MSTP**.

**Step 2** In the **MSTP** dialog, specify the provisionable MSTP parameters, including the *Name* parameter, as described in the following table.

Table A- 34 MSTP parameters

Type	Parameter	Description	Range of Values	Default Value
General	Name (optional)	User-configured name of the MST region	Alphanumeric characters	Not applicable
	Max Hops	The maximum number of possible hops in the region before a Bridge Protocol Data Unit (BPDU) is discarded	6 to 40	20
	Revision Level	The MST configuration revision number	0 to 65535	0
CIST	Priority	The priority of the member in the virtual switch	Integer	32768

**Step 3** Click **Apply**.

**Step 4** Click **Close**.

You have successfully completed this procedure.

## A.12.2 Add MST instances

### Prerequisites

- MSTP is provisioned.
- S-VLANs are provisioned. See [A.6.1, “Provision a Static VLAN”](#)

### Adding an MST instance

Follow these steps to add an MST instance:

- Step 1** In the Navigation pane, right-click **MSTP** under the **MSTP** folder on an Ethernet Switch, and then click **Manage MST Instances**.
- Step 2** In the **Provision MST Instances** dialog, click **New**.
- Step 3** In the **Instance ID** field, enter the integer that identifies the MST instance. The default is 1.
- Step 4** In the **Bridge Priority** field, enter a value. The default is 32768.
- Step 5** In the **VLANs** field, enter a VLAN identifier.
- Step 6** Click **Apply**.  
The MST instance appears on the **MST Instance VLAN Map** list.
- Step 7** Click **Close**.

You have successfully completed this procedure.

## A.12.3 Delete MST instances

### Prerequisites

- The MST instance has been added to the MSTP configuration.

### Deleting an MST instance

Follow these steps to delete an MST instance:

- Step 1** In the Navigation pane, right-click **MSTP** under an Ethernet Switch, and then click **Manage MST Instances**.
- Step 2** In the **Provision MST Instances** dialog, select an MST instance from the **MST Instance VLAN Map** list.
- Step 3** Click **Delete**.
- Step 4** In the confirmation dialog, click **Yes**.  
The MST instance is removed from the **MST Instance VLAN Map**.

**Step 5** Click **Close**.

You have successfully completed this procedure.

## A.12.4 Provision or modify CIST port settings

### Prerequisites

- MSTP must be provisioned.

### Provisioning or modifying CIST port settings

Follow these steps to provision or modify CIST port settings:

**Step 1** In the Navigation pane, right-click **CIST Ports** under the **MSTP** folder on an Ethernet Switch, and then click **Provision CIST Ports**.

**Step 2** In the **CIST Ports** dialog, select a port from the **CIST Ports** list.

**Step 3** Specify the port's provisionable parameters in the **Port Details** section, as described in the following table.

**Table A- 35 CIST port parameters**

Parameter	Description	Range of Values	Default Value
Priority	The priority of the member in the virtual switch	0 to 240 steps of 16	128
Path Cost	The path cost for the instance	6 to 200000000	xGigE - 2000 xGigE LAG - 1900 GigE - 20000 GigE LAG - 19900
Restricted Role	Enables or disables the restricted role feature	True False	False
Restricted TCN	Enables or disables the restricted Topology Change Notification (TCN) feature	True False	False
Forced Port State	Enables or disables the port	Enable Disable	Enable
Link-Type	Specifies the port link type.	Point to Point Shared	Not applicable
Loop Guard	Enables or disables loop guard on the CIST, NNI port.	Enable Disable	Disable
<b>Note</b> This parameter is available on the CIST Port page only when an NNI port is			



**Table A- 35 CIST port parameters (Continued)**

Parameter	Description	Range of Values	Default Value
	selected as the current interface type.		
UNI or NNI	An information only field that indicates the current interface type.	NNI UNI	The current interface type.

**Step 4** Click **Apply**.

**Step 5** Click **Close**.

You have successfully completed this procedure.

## A.12.5 Provision or modify MSTI port settings

### Prerequisites

- The CIST port has been provisioned.
- The MST instance has been added to the MSTP.

### Provisioning or modifying MSTI port settings

Follow these steps to provision or modify MSTI port settings:

**Step 1** In the Navigation pane, right-click **MSTI Ports** under the MSTP folder on an Ethernet Switch, and then click **Provision MSTI Ports**.

**Step 2** In the **MSTI Ports** dialog, select an MST instance from the **MST Instance** list.  
The ports assigned to the MST instance appear in the **Ports in MST Instance** list.

**Step 3** Select a port in the **Ports in MST Instance** list, and then specify the provisionable settings in the **Port Details** section.

**Table A- 36 MSTI port parameters**

Parameter	Description	Range of Values	Default Value
Priority	The priority of the member in the virtual switch	0 to 240 steps of 16	128
Path Cost	The path cost for the instance	6 to 200000000	xGigE - 2000 xGigE LAG - 1900 GigE - 20000 GigE LAG - 19900

**Step 4** Click **Apply**.

**Step 5** Click **Close**.

You have successfully completed this procedure.

## A.13 Viewing PM statistics on packetVX modules

This section provides information about performance metrics for packetVX modules.

The packetVX spanning-tree PM combines CIST and MSTP BPDU statistics on the interface, as described in the IEEE standard 802.1Q 2005, section 14.6 "Encoding and decoding of STP Configuration, RST and MST BPDUs."

### A.13.1 View PM statistics on packetVX modules

#### Prerequisites

- The ports on the Ethernet switch must be provisioned and a transceiver present in the port.

#### Viewing PM statistics

Follow these steps to view the PM statistics for a packetVX module:

**Step 1** In the Navigation pane, do any of the following:

- Right-click **Switch**, select **View PMs**, and then click a PM type.
- Right-click a LAG, and then click **View LAG Port PMs**.
- Right-click a port, select **View PMs**, and then click **Layer 1 PMs** or **Layer 2 PMs**.
- Right-click **Ethernet Services**, select **View PMs**, and then click **Ethernet Service PMs** or **Ethernet Service Bandwidth Profile PMs**.
- Right-click **MSTP**, select **View PMs**, and then click **MSTI PMs** or **MSTI Port PMs**.
- Right-click **PM Statistics** and choose **Display PM Statistics**.

**Step 2** In the **PM Statistics** dialog, specify the parameters for the PMs you want to retrieve.

**Table A- 37 Performance monitoring parameters**

Parameter	Range of values	Description
Select PM	Ethernet Service Ethernet Service Bandwidth Profile ERPS Port LAG Port Layer 1 Interface Layer 2 Interface MST Instance MST Instance Port SLA Measurement	Depends on the location on the Navigation pane from which the <b>PM Statistics</b> dialog was accessed
Type	Protocol All (Layer 1 and Layer 2 Interfaces only)	Protocol

**Table A- 37 Performance monitoring parameters (Continued)**

Parameter	Range of values	Description
	Physical (Layer 1 and Layer 2 Interfaces only)	
Time Group	Current	Current
	Historical	
Bin Type	15 Minute Bin	15 Minute Bin
	1-Day Bin	
	Untimed	

**Step 3** Optionally, clear the **Show All** check box, and then do the following:

- a) Click **Select**.
- b) In the **Select** dialog, move an entity to or from the **Selected** list.
- c) Click **Apply**.

**Step 4** Choose a value in the **Refresh (sec)** list to specify the monitoring interval.

**Step 5** Click **Start**.

The PM data appears in table format, with all entities listed in separate rows and the applicable metrics listed in separate columns. See the following:

- [13.1.1, “Physical PMs supported on packetVX modules”](#)
- [13.1.2, “GE port Ethernet \(Layer 1\) PMs supported on packetVX modules”](#)
- [13.1.3, “10 GE \(Layer 1\) PMs supported on packetVX modules”](#)
- [13.1.4, “10GE WAN PHY PMs”](#)
- [13.1.5, “10 GE Port OTN \(Layer 1\) PMs”](#)
- [13.1.6, “Ethernet \(Layer 2\) PMs”](#)
- [13.1.7, “Link Aggregation Group PMs supported on packetVX modules”](#)
- [13.1.9, “Ethernet Services PMs supported on packetVX modules”](#)
- [13.1.10, “ERPS PMs supported on packetVX modules”](#)
- [13.1.8, “MSTP PMs supported on packetVX modules modules”](#)

**Step 6** To change the table format, do any of the following:

- Clear the **Transpose Table** check box to change the column-to-row presentation of data.
- Click **Customize Table** to add or remove metrics from the PM data.
- Click **Export** to save the data retrieved to CSV (.csv) format.
- Select a metric in the table, and then click **Clear Counter** to clear the data for that metric.

- Click **Clear Table** to clear the data for all metrics.

**Step 7** Click **Close**.

You have successfully completed this procedure.

## A.13.2 Set threshold crossing alerts on packetVX modules

### Prerequisites

- The ports on the Ethernet switch must be provisioned and a transceiver present in the port.

### Setting threshold crossing alerts

Follow these steps to set threshold crossing alerts for a packetVX module:

**Step 1** In the Navigation pane, do any of the following:

- Right-click **Switch**, select **View PMs**, and then click **Layer 1 PMs**, **Layer 2 PMs**, or **Ethernet Service Bandwidth Profile PMs**.
- Right-click a port, select **View PMs**, and then click **Layer 1 PMs** or **Layer 2 PMs**.
- Right-click **Ethernet Services**, select **View PMs**, and then click **Ethernet Service Bandwidth Profile PMs**.
- Right-click **PM Statistics** and then click **Display PM Statistics**.

**Step 2** In the **PM Statistics** dialog, click **Set Thresholds**.

**Step 3** In the **Thresholds** dialog, select a switch, and then specify TCA values as required. See [13.1.11, “Protocol threshold crossing alerts \(TCAs\) and ranges supported on packetVX modules”](#).

**Step 4** Click **Apply**.

**Step 5** Click **Close** to close the **Thresholds** dialog.

**Step 6** Click **Close** to close the **PM Statistics** dialog.

You have successfully completed this procedure.

## A.14 Alarms and events on packetVX modules

---

The proNX 900 Node Controller allows you to view alarms and events reported on a packetVX module at any time.

If a packetVX module is in the In-Service state or Out-of-Service state, any fault condition pertaining to the module is reported as an autonomous alarm. For information about clearing alarms pertaining to packetVX modules, see the *Alarm and Troubleshooting Guide*.

An event reported on a packetVX module can indicate the module's status, a periodic report of information, or asynchronous command completion information.

For a description of the information provided by the proNX 900 Node Controller about an alarm or event, see the *proNX 900 Node Controller Online Help*.

### A.14.1 View alarms for a packetVX module

#### Prerequisites

- A packetVX module must be provisioned and physically present in the shelf.

#### Viewing alarms

Perform the following steps to view alarms and events on a packetVX module:

**Step 1** In the Navigation pane, click on one of the following tabs:

- **Alarms** — click this tab to display a list of the active alarms on the module
- **Conditions** — click this tab to display a list of the conditions on the module
- **Events** — click this tab to display a list of the active events on the module

**Step 2** Double-click on an alarm, condition or event in the list to display detailed information for the selected alarm or event.

**Step 3** Click **Close**.

You have successfully completed this procedure.

## Appendix B: Ethernet services provisioning using the 802.1ad model

---

This section is optional and describes the procedures required to provision Ethernet services using the 802.1ad model.

## B.1 Create an Ethernet interface (optional)

---

This is an optional procedure that describes how to create an Ethernet interface for the packetVX module. This procedure is used in a traditional IEEE 802.1ad Provider Bridge type role.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- The packetVX must be a member of the virtual switch.

#### Step 1 Access the global configuration mode

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows

```
BTI7000(config)#
```

#### Step 2 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 3 Create an Ethernet interface

The following types of Ethernet interfaces can be created

- gigabitEthernet (see step 3a)
- tenGigabitEthernet (see step 3b)
- Link Aggregation Group (see step 3c)

**a)** To create a gigabitEthernet interface, enter the following command:

```
interface gigabitEthernet <interface-id>
```

For example, the command string might be

```
interface gigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-if 1/1/1)#
```

**b)** To create a tenGigabitEthernet interface, enter the following command:



```
interface gigabitEthernet <interface-id>
```

For example, the command string might be

```
interface tenGigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-if 1/1/1)#
```

c) Create a LAG.

#### **Step 4 Exit the previous command mode**

To exit the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

You have successfully completed this procedure.

## B.2 Create an Ethernet switchport (optional)

---

This procedure is optional and explains how to create an Ethernet switchport for a packetVX module. This procedure is used in a traditional IEEE 802.1ad Provider Bridge type role.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- The packetVX must be added to the virtual switch.

#### Step 1 Access the global configuration mode

To access the global configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 2 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### Step 3 Create an Ethernet switchport

The following types of Ethernet switchports can be created:

- gigabitEthernet (see step 3a)
- tenGigabitEthernet (see step 3b)
- Link Aggregation Group (see step 3c)

**a)** To create a gigabitEthernet switchport, enter the following command syntax:

```
switchport gigabitEthernet <interface_id>
```

For example, the command string might be

```
switchport gigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-sp 1/1/1)#
```

b) To create a tenGigabitEthernet switchport, enter the following command syntax:

```
switchport tenGigabitEthernet <interface_id>
```

For example, the command string might be

```
switchport tenGigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-sp 1/1/1)#
```

c) Create a LAG.

#### Step 4 Set the switchport type

To set the switchport type, enter the following command:

```
switchport port-type <type>
```

where <type> is one of the following port types that is based on the selected bridge mode

**Table B- 1 Port Types**

Bridge Mode	Port Type	Description
Provider	customerEdgePort - CEP	C-VLAN to S-VLAN mapping
	customerNetworkPort port-based - CNP	Direct S-VLAN port based mapping
	providerNetworkPort (default) - PNP	802.1ad tagged frames

**Note** When changing the port type of a switchport among PNP, CEP, and CNP, the system will reset parameter values back to their defaults.

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-sp 1/1/1)#
```

#### Step 5 Exit to the previous command mode

To exit the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

You have successfully completed this procedure.

## B.3 Provider bridge with 802.1ad Q-in-Q tagging provisioning (optional)

---

This procedure is optional and describes how to manually provision a provider bridge with 802.1ad Q-in-Q tagging for the switch. This procedure is used in a traditional IEEE 802.1ad Provider Bridge type role.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

### Prerequisites

- Create a Virtual Switch.
- Add a packetVX as a member.
- To provision 802.1ad Q-in-Q tagging the switch must be configured as a provider bridge.

### Provider bridge with 802.1ad Q-in-Q tagging procedure

In Provider bridge mode, all VLAN references are S-VLAN (outer tag) references. For CEP ports, use the C-VLAN map to associate C-VLANs with S-VLANs. Add the CEP ports as untagged members of the S-VLAN. Add a CNP as an untagged member of the S-VLAN through setting the PVID from within switchport settings.

#### Step 1 Access the Privileged EXEC mode

To access the Privileged EXEC mode, enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

#### Step 2 Access the Administration Configuration mode

To access the administration configuration mode, enter the following command:

```
configure terminal
```

The CLI prompt should now appear as follows:

```
BTI7000(config)#
```

#### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 4 Provision a GbE port**

To provision a GbE port, enter the following command:

```
interface <interface-type> <interface-id>
```

For example, the command string might be

```
interface gigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-if 1/1/1)#
```

**Step 5 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 6 Provision a 10 GbE port**

To provision a 10 GbE port, enter the following command:

```
interface <interface-type> <interface-id>
```

For example, the command string might be

```
interface tenGigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-if 1/1/1)#
```

**Step 7 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

**Step 8 Provision a Layer 2 GbE interface**

To provision a layer 2 GbE interface, enter the following command:

```
switchport <interface-type> <interface-id>
```

For example, the command string might be

```
switchport gigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-sp 1/1/1)#
```

**Step 9 Set the port type**

Provider Bridges can be set as one of three port types:

- customerEdgePort - CEP
- customerNetworkPort - CNP
- providerNetworkPort port-based (default) - PNP

To set the port type, enter the following command:

```
switchport port-type <type>
```

where <type> is one of the three port types listed above.

**Note** When changing the port type of a switchport among PNP, CEP, and CNP, the system will reset parameter values back to their defaults.

For example, the command string might be

```
switchport port-type customerEdgePort
```

The CLI prompt should appear as follows

```
BTI7000:sw1(config-sp 1/1/1)#
```

#### **Step 10 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

#### **Step 11 Provision a Layer 2 10 GbE interface**

To provision a layer 2 10GE interface, enter the following command:

```
switchport <interface-type> <interface-id>
```

For example, the command string might be

```
switchport tenGigabitEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-sp 1/1/1)#
```

#### **Step 12 Display the current switchport**

To display the current switchport, enter the following command:

```
show
```

For example, the display could be

```
Switchport TenGigE 1/1/1:
  Admin Status is up, Operational Status is notPresent
  Port type is Provider Network Port (NNI)
  PVID is 1
  Provider tag ethertype (TPID) is 88A8
  Default Priority is 0
```

```

usedEI is disabled
Acceptable Frame Type is invalid(137740880)
Ingress Filtering is enabled
GVRP is enabled
Number of failed GVRP registrations is 130674780
Last PDU Origin is 75-32-11-08-01-00
Restricted VLAN Registration is disabled

Trust Incoming PCP is enabled
Trust Incoming DSCP is enabled
Profiles:
  Scheduler:                "DEFAULT_SCHEDULER_PROFILE"
  Priority Traffic Class Map: "DEFAULT_PRIORITY_TC_MAP_PROFILE"
  PCP Encoding/Decoding:    "DEFAULT_8P0D_PROFILE"

```

**Note** This release does not support customized profiles.

### Step 13 Exit to the previous command mode

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 14 Create a VLAN

To create a VLAN, enter the following command:

```
vlan <vlan-id>
```

For example, the command string might be

```
vlan 100
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-vlan 100)#
```

### Step 15 Add a switchport to the VLAN as an untagged port

To add a switchport to the VLAN as an untagged port, enter the following command:

```
member switchport <interface-type> <interface-id> untagged
```

For example, the command string might be

```
member switchport gigabitEthernet 1/1/1 untagged
```

### Step 16 Add a switchport to the VLAN as a tagged port

To add a switchport to the VLAN as a tagged port, enter the following command syntax:

```
member switchport <interface-type> <interface-id> tagged
```

For example, the command string might be

```
member switchport tenGigabitEthernet 1/1/1 tagged
```

### **Step 17 Exit to the previous command mode**

To exit to the previous command mode, enter the following command:

```
exit
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### **Step 18 Provision a customer VLAN map for a GbE switchport**

To provision a customer VLAN map for a GbE switchport, enter the following command syntax:

```
c-vlan-map switchport <interface-type> <interface-id>
```

For example, the command string might be

```
c-vlan-map switchport gigaEthernet 1/1/1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config-cvlan-sp 1/1/1)#
```

### **Step 19 Map a customer VLAN to a service provider VLAN**

To map a customer VLAN to a service provider VLAN, enter the following command:

```
map c-vlan <vlan-range> s-vlan <service-vlan-id>
```

For example, the command string might be

```
map c-vlan 2 s-vlan 100
```

### **Step 20 Create a link aggregation group**

You have successfully completed this procedure.



## Appendix C: Converting from the 802.1ad model to the Eservices model

---

This section describes how to convert from the 802.1ad model to the Eservices model.

## C.1 Converting a PNP interface into an NNI interface

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

In Release 7.1.2 and earlier, packetVX used the 802.1ad provisioning model. In Release 7.2 and later, packetVX uses the Ethernet Services provisioning model. After you have upgraded from Release 7.1.2 to Release 7.2, the provider port types will be 802.1ad provider network ports (PNP). To use these ports as part of an Eservice, the PNP must be migrated to Network to Network Interfaces (NNI).

This procedure describes the initial and mandatory steps required to migrate from an IEEE 802.1ad Provider Bridge Provisioning model to a MEF Eservices provisioning model.

**Caution** This procedure is traffic-affecting.

### Step 1 Access the Privileged EXEC mode

Enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

```
configure terminal
```

The CLI prompt appears as follows:

```
BTI7000(config)#
```

### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switchswitch_id>
```

where<switch\_id> is the virtual switch identifier. For example, the command string might be:

```
virtual-switch 1
```

The CLI prompt should now display as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Modify the Maximum Frame Size on the new NNI as required

```
BTI7000:sw1(config-nni TenGigE 1/1~)# frame-size<frame size>
```

**Caution** A traffic hit will occur on Jumbo Frame traffic until the frame size is modified appropriately.

### Step 5 Repeat steps 1 to 7 for all required NNI ports

**Step 6 Repeat steps 1 to 8 for all required nodes**

You have successfully completed this procedure.

## C.2 Converting a CNP or CEP interface into a UNI interface

---

This procedure provides the optional process of migrating existing traffic from an IEEE 802.1ad Provider Bridge provisioning model to a MEF Eservices model. This process migrates existing IEEE Customer Edge Ports (CEP) and Customer Network Ports (CNP) to MEF User Network Interface (UNI) ports. This process is optional and is required only if existing traffic is to be migrated and managed as a MEF Eservice.

Authorization Required

Superuser

Provisioning

Maintenance

Surveillance

**Warning** This procedure is traffic-affecting.

### Step 1 Access the Privileged EXEC mode

Enter the following command:

```
enable
```

The CLI prompt should now appear as follows:

```
BTI7000#
```

### Step 2 Access the Administration Configuration mode

```
configure terminal
```

The CLI prompt appears as follows:

```
BTI7000(config)#
```

### Step 3 Select a virtual switch

To select a virtual switch, enter the following command:

```
virtual-switch <switch_id>
```

where <switch\_id> is the virtual switch identifier

For example, the command string might be

```
virtual-switch 1
```

The CLI prompt should now appear as follows:

```
BTI7000:sw1(config)#
```

### Step 4 Create a new temporary UNI that will be used to mimic the port to be migrated on any available GE or 10GE interface

```
BTI7000:sw1(config)# uni <gigabitEthernet | tenGigabitEthernet | lag<  
<shelf/slot/port>
```

### Step 5 Optionally, define the frame size of the port

```
BTI7000:sw1(config-uni GigE 1/1/~)# frame-size <frame size>
```

### Step 6 Exit from UNI configuration mode

```
BTI7000:sw1(config-uni GigE 1/1/~)# exit
```

**Step 7 Create a new temporary Eservice that will be used to carry traffic during migration**

To create the Eservice, enter the following command:

```
BTI7000:sw1(config)# eservice <string> type <EPLINE | EPLAN | EPVLINE  
| EVPLAN
```

**Step 8 Define the frame size of the Eservice**

```
BTI7000:sw1(config-eservice)# frame-size <frame size>
```

**Step 9 Define the SVLAN for the Eservice**

```
BTI7000:sw1(config-eservice)# s-vlan <vlan-id>
```

**Step 10 Add the new UNI to the new Eservice**

```
BTI7000:sw1(config-eservice)# uni <gigabitEthernet |  
tenGigabitEthernet | lag> <shelf/slot/port>
```

**Step 11 Repeat steps 1 to 10 on all applicable nodes****Step 12 Perform a traffic connectivity and integrity test over the new temporary Eservice****Step 13 Migrate live traffic onto the temporary Eservice**

When you are satisfied with the integrity of the new Eservice, migrate traffic over to the new UNI. Perform this step simultaneously on all UNIs on the Eservice

**Step 14 Remove all member Switchport(s) from the VLAN to be migrated to an Eservice (Customer and Network ports)**

Enter the following command:

```
BTI7000:sw1(config-vlan)# no member switchport <gigabitEthernet |  
tenGigabitEthernet | lag> <shelf/slot/port>
```

**Step 15 Delete the "Switchport" and "Interface" of the physical port to be migrated to a UNI**

```
BTI7000:sw1(config)# no switchport <gigabitEthernet |  
tenGigabitEthernet | lag> <shelf/slot/port>
```

**Step 16 Delete the original VLAN entry for the Eservice to be migrated**

```
BTI7000:sw1(config)# no VLAN (vlan_id>
```

**Step 17 Create a new UNI to replace the port to be migrated**

To create the UNI, enter the following command:

```
BTI7000:sw1(config)# uni <gigabitEthernet | tenGigabitEthernet | lag>  
<shelf/slot/port>
```

**Step 18 Define the frame size of the port**

```
BTI7000:sw1(config-uni GigE 1/1/~)# frame-size <frame size>
```

**Step 19 Create a new EService to replace the original VLAN that is to be migrated.**

**Step 20 Add the new UNI to the new Eservice**

Enter the following command:

```
BTI7000:sw1(config)# eservice <string> type <EPLINE | EPLAN | EVLINE |  
EVPLAN>
```

**Step 21 Define the frame size of the Eservice**

Enter the following command:

```
BTI7000:sw1(config-eservice)# frame-size <frame size>
```

**Step 22 Define the S-VLAN of the Eservice**

Enter the following command:

```
BTI7000:sw1(config-eservice)# s-vlan <vlan-id>
```

**Step 23 Add the UNI to a LAG**

**Step 24 Add the new UNI to the new Eservice**

**Step 25 Repeat the above steps on all applicable nodes**

**Step 26 Perform a traffic connectivity and integrity test over the new Eservice**

**Step 27 Migrate live traffic onto the new EService**

When you are satisfied with the integrity of the Eservice, migrate traffic back over to the original UNI. Perform this step simultaneously on all UNIs on the Eservice. Ensure migrated traffic flows error-free and alarm-free for several minutes.

**Step 28 Repeat step 4 to 26 for all ports to be migrated**

**Note** The same temporary UNI and Eservice can be used for all ports to be migrated.

**Step 29 Remove all temporary Eservices and UNIs**

You have successfully completed this procedure.





*Part Number:*  
*Document Version:*  
*Published:*  
*Type:*

*BT7A73DA*  
*01*  
*March 2017*  
*STANDARD*

*product release 13.5*