



BTI 7000 Series

Release 13.5.0

NE Build 13-5-0 C002, proNX™ 900 Build 13-5-0 C001

Release Notes

Part No.: BT7A76AA Rev. 01

May 2017

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.

Obtaining technical support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

End User License Agreement

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (EULA) posted at <http://www.juniper.net/cm/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Document Identification

Juniper Networks BTI7000 Release 13.5.0 Release Notes Rev. 01

Abstract

This document provides information related to the current release.

Publication History

Revision	Date	Changes
01	May 2017	Baseline

Contents

1. Introduction.....	1
1.1 Purpose.....	1
1.2 New Features.....	1
1.3 Dual 10G Multiprotocol Transponder Ethernet Mapping.....	2
1.4 Scaling in packetVX.....	3
2 Resolved Issues	4
3 Known Issues.....	5
4 Known Limitations	6
4.1 Software Limitations	6
4.2 Hardware Limitations	18
4.3 proNX 900 Node Controller Limitations	18
5 Related Documentation	20
6 Upgrade Considerations.....	21
Storm Control values out of range after upgrade.....	21
Stacked packetVX environment.....	21
ERPS in a Stacked or Non-stacked packetVX environment	22
LAG MEP IDs Change after the Upgrade	22

1. Introduction

1.1 Purpose

This document describes BTI Systems 7000 Series Release 13.5 Network Element and proNX 900 software features, supported hardware, and resolved and known issues.

1.2 New Features

BTI 7000 Series Release 13.5 provides support for the following:

- Support for the BT8A78MD03 multiplexer/demultiplexer for the 96-channel ROB4 module
- SNMP log file size limit
 - Limiting the size of the SNMP log file to 1000 entries
 - 300 characters per entry
 - Wraps when full
- Disk and CPU usage PM and alarms:
 - Disk Usage High alarm
 - Disk usage PM
 - CPU usage PM (instantaneous/minimum/maximum/average)
 - Supported on the following modules:
 - SCP (all)
 - PVX modules (all)
 - ROADM-on-a-Blade (ROB) modules (all)
 - Dual 10G Multiprotocol Transponder (BT7A49AA, BT7A49AA-I02)
 - 10-Port Multiprotocol Muxponder (BT7A48AA/BA, BT7A48AA-I02/BA-I02)
- Increased number of Ethernet services that can have a PVX bandwidth profile:
 - PVX: 768
 - PVX80: 256

1.3 Dual 10G Multiprotocol Transponder Ethernet Mapping

The Dual 10G Multiprotocol Transponders (BT7A49AA, BT7A49AA-I02) support multiple methods for mapping a 10GbE LAN PHY signal into an OTN frame.

The protocol mapping that you choose determines how the Ethernet signal is mapped and how Ethernet maintenance signals are handled. This is shown in the following table:

Client Protocol	Line Protocol	Description
10GELAN	10GELAN	Regenerates a 10GbE LAN PHY signal. Ethernet LF and RF signals are generated in cases of failure. LF and RF signals are also propagated through if received.
10GELAN	10GELANFEC 10GELANEFEC	Maps a 10GbE LAN PHY signal into an OTU2 signal using GFP-F. Both FEC and EFEC options are supported. Ethernet maintenance signals are carried over Client Management Frames (CMF). NOTE: Where possible, it is recommended that you use 10GELANFECEPV3 (or 10GELANEFECEPV3) instead of this mapping.
10GELAN	10GELANFECEPCMF 10GELANEFECEPCMF	Maps a 10GE LAN PHY signal into an Extended Payload OTU2 signal using GFP-F. Both FEC and EFEC options are supported. Ethernet maintenance signals are carried over Client Management Frames (CMF). NOTE: Where possible, it is recommended that you use 10GELANFECEPV3 (or 10GELANEFECEPV3) instead of this mapping.
10GELAN	10GELANFECEPV3 10GELANEFECEPV3	Maps a 10GE LAN PHY signal into an Extended Payload OTU2 signal using GFP-F. Both FEC and EFEC options are supported. Ethernet maintenance signals are carried using ordered set transparency. NOTE: This mapping is only supported on the BT7A49AA-I02 transponder.
10GELAN	OTU2eFEC OTU2eEFEC	Maps a 10GE LAN PHY signal into an OTU2e signal using GFP-F. Both FEC and EFEC options are supported.

1.4 Scaling in packetVX

- The number of services that can terminate on a single packetVX is 500. This limit assumes that CCM sessions (1 minute intervals) are operated on all services and that customer spanning tree is not peered on any UNIs. This value is also limited by other things like PSM (proNX Service Manager) accumulating service information from the node. This number is reduced if customer spanning tree is being peered on any UNIs.
- The number of services that can be supported per SCP is 1000. This limit assumes that CCM sessions (1 minute intervals) are operated on all services.
- The number of services that can be supported network wide is 2000. This limit assumes that CCM sessions (1 minute intervals) are operated on all services. Services that are not running CCM sessions do not count against this network-wide limit.
- The total number of MEPs that are supported network-wide is 4000.

2 Resolved Issues

The following issues have been resolved in release 13.5:

Issue	Description
44922	When FPSD takes effect on a client port on a BT7A49AA-I02 transponder module, the client port laser turns off and on intermittently instead of turning off and staying off. This problem only occurs on a BT7A49AA-I02 module with the line port configured for 10GELANEFEC, 10GELANEFEC-EPCMF, 10GELANEFEC-EPV3, OTU2EFEC, or OTU2eEFEC.
43740	Protection group provisioning on the BT7A49AA and BT7A49AA-I02 modules is allowed for invalid protocols.
42683	The maximum number of Ethernet services that can have a bandwidth profile is too low.
42392	A database backup operation fails with a "Database backup failed. Resource unavailable, try again" message.
41607 41587	ROB2 cards can change unexpectedly to a "Circuit pack degraded" state after running for a long time.
40341	An ACL cannot be created on a non-stacking chassis.
39614	A ROB4 module cannot be used to spare for a ROB2 module without deleting and reprovisioning the module. This problem also occurs when using a ROB2 module to spare for a ROB4 module.

3 Known Issues

The following are known issues in this release:

Issue	Description
42122	Description: Auto-provisioning is not supported for the following ROB modules in releases 11.3.0 and earlier: BT7A07AA-I02, BT7A07BA-I02, BT7A07CA-I02
26641	Description: For the 96-channel ROB4 cards, the PM validity flag on L1,C1,C2,C3,C4 ports for 15min & 1day historical PM bins are not updated consistently and show PRTL. This limitation is not applicable to DOL ROB2/ROB4/DLA2-44chs cards.
24638	Description: After rebooting a packetVX module, the STP cost may become very large (for example, 200000000).

4 Known Limitations

Known limitations are issues that are not planned to be resolved and that might not be described in the documentation set for this release. These limitations might be described in a future release of the documentation set where applicable and necessary. Once a limitation is described in the documentation set, the limitation might be removed from this list (without notice).

4.1 Software Limitations

Issue	Description
36199	<p>Description: Egress Bandwidth Profile is supported on PVX80 ENNI with EPL and EPLAN services where ingress and egress ports must be in the same set (port 7, 8) or (port 1 to 6) for Egress Bandwidth Profile to be effective. Egress Bandwidth Profile is not supported on PVX80 ENNI with EVPL and EVPLAN services. Ingress Bandwidth Profile is supported on PVX80.</p> <p>Workaround: None.</p>
34830	<p>Description: Circuit pack and port auto-provisioning on the 10 Port Multiprotocol Muxponders (BT7A48AA-I02/BA-I02), are supported in the following releases only: 11.1.3, 12.1.0, 12.1.1, 12.1.2, 12.2.0, 12.2.1, 12.2.2.</p> <p>In the releases where autoprovisioning is supported, the module will auto provision as a BT7A48AA/BA pack.</p> <p>In the releases where it is not supported, the AUTOPROVFAIL event will be generated against the circuit pack. The functionality of the card is not affected.</p> <p>Workaround: When autoprovisioning is not supported the user may provision the pack as BT7A48AA/BA manually.</p>
33879	<p>Description: In release 10.3, 10.4, 11.1, 11.2 and 12.2 when a 10 Port Multiprotocol Muxponder module [BT7A48AA-I02 & BT7A48AB-I02] is installed into a shelf a CONTCOM alarm will be raised after 2 minutes.</p> <p>Workaround: Wait 30 seconds. The alarm should clear and the module will provision and function as normal.</p>
33754	<p>Description: Under certain situations when both port mirroring and stacking are configured at the SLA responder, incorrect Ethernet SLA loss measurements may be reported.</p> <p>Workaround: Before performing SLA frame loss measurements, disable port mirroring on the packetVX/packetVX80 where the SLA responder resides.</p>
33145	<p>Description: If GVRP is set to tunnel in an I2control profile, applying the profile to a UNI LAG port will return an error.</p> <p>Workaround: First, apply the I2control profile to the UNI LAG port with GVRP set to discard. Next, change the profile to set GVRP to tunnel.</p>

Issue	Description
33100	<p>Description: If you configure the Ethernet service-type on a UNI LAG to virtual-untagged before adding interfaces to the LAG, the service may not tag and untag frames correctly for incoming and outgoing frames on the newly added LAG members. This problem occurs on the packetVX80 only.</p> <p>Workaround: On a packetVX80, add interfaces to the UNI LAG before you configure the Ethernet service-type.</p>
32999	<p>Description: After you enable or disable EPRS CCMs on a node in an ERPS ring, traffic on the ring ports on that node may be dropped for 5 to 10 ms.</p> <p>Workaround: None</p>
32087	<p>Description: When upgrading a stacked PVX node, there is a small window in which the "Stacking link not present" alarm will be raised due to the current PVX stacking design. The stacking link is UP, and traffic is not affected.</p> <p>Workaround: Reload the secondary PVX again after upgrading. This will clear the false "Stacking link not present" alarm.</p>
31936	<p>Description: If the SCP is restarted immediately after a provisioning change, the new provisioning may be lost.</p> <p>Workaround: Wait at least 30 seconds after the last provisioning change before restarting the SCP.</p>
31003	<p>Description: Manually clearing an ERPS protection switch while the wait-to-restore timer is running may result in a traffic loss for a number of seconds.</p> <p>Workaround: Wait for a minimum of 20 seconds to elapse after the failed link has recovered before clearing the protection switch.</p>
30868	<p>Description: When using PSM to retrieve packetVX historical PMs, PSM may display PM points in the wrong bin. This occurs when the duration of the PM retrieval crosses a 15-minute bin boundary.</p> <p>Workaround: Start the PSM on-demand historical PM collection at least one minute before the start of a new 15-minute bin interval.</p>
30614	<p>Description: After stopping and restarting station loopback instances on a virtual switch, the unique MAC-swapped Frames table may contain duplicate entries.</p> <p>Workaround: Before restarting station-loopback, clear the recorded MAC addresses with the clear station-loopback statistics command.</p>
30249	<p>Description: Adding a UNI to an Ethernet service may cause the forbidden NNIs on the S-VLAN associated with that service to be removed.</p> <p>Workaround: If this occurs, recreate the list of forbidden NNIs on the S-VLAN.</p>
30217	<p>Description: When a Dual 10G Multiprotocol Transponder module (BT7A49AA-I02) (with ports provisioned with 0C192 - 0C192/EFEC) is deleted and a database restore is performed, the database restore function fails.</p> <p>Workaround: This may happen if the restoring database is significantly different from the current database. To restore traffic, power cycles the system.</p>

Issue	Description
29555	<p>Description: When running an SLA throughput test while there is background traffic, some packets from the test may be dropped at the NNI even when there should be enough bandwidth.</p> <p>Workaround: Ensure the SLA throughput test is running at a higher S-VLAN priority than the other traffic.</p>
29146	<p>Description: When using the proNX900 GUI to clear historical PMs (OSC, PORT, WCH) bins 1 to 96, the PMs are not cleared properly.</p> <p>Workaround: Use TL1 to clear these historical PMs.</p>
29023	<p>Description: When restoring a database, circuit pack power feed failure conditions against the BT7A49AA-I02 transponder (on a node with more than one chassis) are converted to alarms.</p> <p>Workaround: Perform a warm reboot of the SCP after restoring the database.</p>
28119	<p>Description: When sending in a high priority flow of 9600-byte packets, as in an SLA throughput test, some packets may be dropped in favor of traffic from a lower priority flow.</p> <p>Workaround: Run the SLA throughput test using a smaller frame size.</p>
28103	<p>Description: If the database that you are restoring does not match the provisioning currently running on the card, you must perform a cold reboot on the card after restoring.</p>
28030	<p>Description: When running a throughput test with large packet sizes and a small CIR value, the resulting throughput may be lower than expected.</p> <p>Workaround: Use CIR values greater than 10 Mbps when running a throughput test.</p>
28029	<p>Description: When running a best-effort throughput test where one or both endpoints are on a PVX80 module, yellow packets may not be handled correctly and the resulting best-effort throughput may be lower than expected. If you are running a CIR throughput test instead, ensure packets are not marked yellow by setting the exceed action correctly at both ends:</p> <pre>exceed-action set-dei disable</pre>
27695	<p>Description: A FEC-EFEC provisioning mismatch between transponder module line ports may cause an unexpected LCK-XCVR condition to be raised.</p> <p>Workaround: Fix the provisioning error by setting both ends to FEC or both ends to EFEC.</p>
27508	<p>Description: When deleting both a UNI and statically-configured NNIs from an EVPLAN service, the remaining endpoints may show the deleted UNI as down rather than removed from the service.</p> <p>Workaround: Delete the UNI first before deleting the NNIs. This allows the CCM flush messages from the deleted UNI to reach the other endpoints.</p>
26106	<p>Description: For Layer 1 PMs (performance monitoring) on packetVX modules, the 10G ports do not report invalid blocks. The GigE ports do not report Code Violations. There is no known workaround.</p> <p>The 10G ports on the packetVX 80 properly report invalid blocks.</p>

Issue	Description
26018	Description: When responding to historical PM queries for STM-N counts, the BTI 7000 returns temperature values with a different precision for a TL1 query versus an SNMP query.
26011	Description: When upgrading a network running G.8032-V1, multiple ports may be blocked on the ring isolating a node. Workaround: For workaround procedures refer to the Appendix—Upgrade Considerations.
25965	Description: The packetVX does not support GVRP/GMRP tunneling on a UNI LAG on any EVP Eservice.
25871	Description: In a network configuration where a Transponder 49AA card is connected to a Transponder 49AA-I02 card, the 49AA-I02 card will always interpret a Local Fault (LF) as a Remote Fault (RF). Workaround: None.
25727 25625 25624	Description: For ERPSv2, RAPS packets may not be forwarded to across node, if a subring with a neighbor is configured in the subring. Workaround: To avoid this issue do not configure neighbors in a subring.
25651	Description: When egress mirroring a UNI port that is tunneling Customer Bridge Spanning tree BPDUs (01:80:c2:00:00:00), the BPDUs are not forwarded to the Mirror-To-Port.
25436	Description: After an upgrade, the SLA Loss-Delay Measurement may return invalid values (all zeros). Workaround: If this happens, remove the Initiator/Responder pair and recreate them.
25358	Description: Adding a member to a virtual switch causes a traffic hit.
25191	Description: When adding a UNI to a service, the PCP and DSCP profile and trust settings are reset to their defaults, leading to unexpected PCP and DSCP profile enforcement behavior. Workaround: Add the UNI to the service prior to changing the PCP and DSCP profile and trust settings. In situations where the problem occurs, remove the UNI from the service, delete and recreate the UNI, and re-add it to the service. Then change the PCP and DSCP profile and trust settings to the desired values.
25165	Description: When an SF exists on an ERPS ring port, the other ring port on that node will incorrectly show a Remote SF status. This takes place automatically, even though the second port did not receive an R-APS SF message directly. This problem does not affect ERPS operation.
25058	Description: In a stacked environment, MAC Address entries for frames ingressing then egressing the Secondary packetVX are not displayed. Traffic running to/from the Primary to Secondary is shown correctly.
24954	Description: On UNI and NNI ports, frames with sizes larger than 9216 bytes are not accounted for in the 1519+ received byte counter. They are accounted in global statistics only. However, the frames are passing through the system successfully.

Issue	Description
24858	<p>Description: After resetting both the primary and secondary packetVXs or after a failover, the MEP ID of a LAG UNI may be recalculated and deviate from the original value.</p> <p>This causes the eServices, of which the LAG is a member, to go Operationally down due to the failed remote MEP ID.</p> <p>Workaround: To clear this, go to the S-UNI of the eService and execute the command: <code>cfm flush-rmep-db</code>. This forces the eService to relearn the new MEP IDs.</p>
24758	<p>Description: If you change the UNI's default priority from zero (default=0) to other value, and add that UNI to the Eservice, the default priority goes back to zero.</p> <p>Workaround: To set the preferred default priority on the UNI follow this procedure:</p> <ol style="list-style-type: none"> 1. After adding the UNI to an Eservice, change the default-priority to another value. 2. Modify this value back to the preferred default priority value.
24616 24111	<p>Description: An egress profile on a packetVX 80 is not supported on a UNI.</p>
24573	<p>Description: The maximum number of allowed Service-Map Service-Policies (on S-UNI) is 256. Attempting to create a 257th Service-Map Service-Policy fails but does not return an error.</p>
24297	<p>Description: PCP and DSCP Trust do not work for Private Services.</p>
24114	<p>Description: In a stacked environment, if LAGs exist on the system and the LACP protocol is disabled globally, the Secondary may still transmit LACP PDUs.</p> <p>Workaround: Restarting the Primary packetVX stops this behavior; however, it is generally recommended that you do not disable the LACP protocol globally.</p>
24113	<p>Description: After disabling CFM crosscheck on an Eservice, the remote MEP list is not deleted, so the Eservice goes into an Operational Down state.</p> <p>Workaround: Use the <code>cfm flush-rmep-db</code> command on a UNI assigned to the Eservice.</p>
24074	<p>Description: CVLAN translation does not work on packetVX modules if the ingress NNI on that switch is set to 8100.</p>
24023	<p>Description: The CLI command, show vlan all, does not display dynamically learned VLANs.</p> <p>Workaround: To display dynamically learned VLANs, use the command, show vlan dynamic, which displays all the VLANs learned dynamically on a virtual switch, in addition to any statically configured VLANs.</p>
23991	<p>Description: When there are two UNI ports at EPLINE/EVPLINE Eservice, the existing NNI port cannot be deleted because it belongs to the forbidden port list.</p> <p>Workaround: To delete an NNI port, remove the NNI port from the VLAN's forbidden port list.</p>

Issue	Description
23771	Description: Egress frames mirrored from a UNI on a PRIVATE eService retain the S-VLAN tag of the eService.
23709	Description: Attempting to set the DSCP value of a frame with an Egress bandwidth profile on a packetVX 80 does not function correctly. No workaround known.
23620	Description: When performing a database restore, where the difference between the current configuration and the database being restored is significant, some alarms may not clear, automatically. Workaround: Reboot the SCP following the database restore.
23617	Description: Non-provider bridge BPDUs (01:80:C2:00:00:00) tunnel correctly and egress the UNI, without the C-Tag that was matching the C-PVID of the UNI. However, all the other L2 control frames continue to egress the UNI with the CTAG. For example: GVRP 01:80:C2:00:00:21 LACP 01:80:C2:00:00:02
23603	Description: When there are "Unexpected MEP" and "Unexpected Period" defects reported on the local MEP, an incorrect RMepID is displayed. Workaround: To clear the "Unexpected Period" defect, perform a "ccm flush" on both the far end and the near end. There is no workaround for the RMepID display issue.
23388	Description: Reverting an upgrade back to 8.1.x may result in spurious circuit pack upgrade failure alarms. Workaround: Restart the SCP to clear the alarms.
22629	Description: Disabling or deleting an ERPS service is not detected as a ring failure and can lead to a network storm. Workaround: Refer to the following sections in the <i>BTI 7000 Series packetVX Solutions Guide</i> for the procedures for changing the ME-Name: <ul style="list-style-type: none"> • Adding a packetVX in an ERPS network • Removing a packetVX in an ERPS network • Replacing a packetVX in an ERPS network
22251	Description: When a "Link down" event occurs on a 10G interface with line-mapping set to otu2-gpf1, the event is not raised as an alarm, but it is raised as a condition. Workaround: When line-mapping is set to otu2, look at both the alarm and condition tables for "Link down" events. Note that when line-mapping is set to 10ge-lanphy, both the alarm and condition are raised properly.
22225	Description: PVX LEDs are not set correctly for "Link down" events but events are posted to the alarm and condition tables. Workaround: In order to detect "Link down" events, examine both the alarm and condition tables.
22078	Description: Disabling GVRP does not remove VLANs from an NNI. A loop occurs, if the MSTP is also disabled. Workaround: MSTP or ERPS must be enabled to block one link to prevent the loop.

Issue	Description
21658	<p>Description: If two interfaces have MAC Address with the same values in the lowest 11 bits of the address, automatically generated MEP IDs can produce identical values.</p> <p>If identical MEP IDs are detected in the network, one of the MEP IDs must be manually changed.</p> <p>Workaround: Change one of the MEP IDs using the config-eservice-uni mode command: <code>cfm mep-id <value></code>.</p>
21591	<p>Description: Multiple GCC0 and/or ODCC channels between two nodes can lead to nodes becoming unreachable. When using GCC/ODCC management, it is recommended to have a single GCC and/or ODCC channels between two nodes.</p> <p>Workaround: Ensure there is only a single GCC0 and/or ODCC channel between two nodes by de-provisioning all GCC0/ODCC channels between the two nodes except one. If a site becomes unreachable, reset the SCP on either end of the span.</p>
21454 25059	<p>Description: packetVX static multicast entries do not take effect. Traffic continues to be cast on all ports associated with the VLAN IDs.</p> <p>Workaround: Use multiple unicast entries instead.</p>
21369	<p>Description: Modification or reconfiguration on a link, with a LAG as part of a UNI, may fail.</p> <p>Workaround: To modify or reconfigure the link, follow this procedure in the order specified:</p> <ol style="list-style-type: none"> 1. Remove a link from the LAG. 2. Shutdown. 3. Perform a modification or reconfiguration operation. <p>Once modification or reconfiguration operation is successfully completed, you can enable and put back the link to a LAG.</p>
21368	<p>Description: Cu SFPs and Cu ports on the packetVX do not properly detect loss of fiber connection and incorrectly reports IS-NR (In Service - Normal) status instead of reporting OOS (Out of Service) status.</p> <p>Workaround: You can determine the Out-of-Service condition by observing port statistics using the show interfaces command, to check if receive (or transmit) packet counters are not incremented, and to check the fiber disconnect condition (either fiber cut or fiber loose connection).</p>
21274	<p>Description: Trace Identifier Mismatch Alarm does not immediately clear when the expected trace identifier field is cleared for a port.</p> <p>Workaround: A workaround is not required. The alarm clears after 10 seconds.</p>
21215	<p>Description: The upgrade of a DOL network to Release 10.1 should not subsequently be cancelled to the previous release. Doing so may impact traffic.</p>
21017	<p>Description: packetVX software does not support connecting a link between two PVXs UNI ports as shown below:</p> <pre>Uni --- PVX ---x-- UNI ---x-- PVX --- UNI</pre>

Issue	Description
20960	<p>Description: PacketVX modules in a stacking configuration reinitialize five minutes apart during software upgrades, to minimize a traffic hit.</p> <p>Since Release 9.1, a mechanism is in place for both modules to reinitialize at the same time, to complete the software upgrade in the rare event that a fault is detected during resynchronization.</p> <p>Workaround: A workaround is not required. Software upgrades should be scheduled during a maintenance window to minimize customer impacts.</p>
20727	<p>Description: Restarting both the active and standby packetVX modules in the stack may result in disrupting the availability of the standby.</p> <p>Workaround: Adding a 10 second delay between restarts eliminates this problem.</p>
20610	<p>Description: If the stacking link in a stacked packet configuration is not active when configuring ports for auto-negotiation on the Standby packetVX, the ports may not properly auto-negotiate when the stacking link is established.</p> <p>Workaround: Restart the standby packetVX or remove and re-provision the port after the stacking link is established.</p>
20608	<p>Description: During an SCP restart, the Storm Control traffic pattern changes to a rate which does not correspond to the latest settings, but, corresponds to a previous setting.</p> <p>Workaround: Performing an SCP reboot should only be done at least 45 seconds after the last provisioning change.</p>
20402	<p>Description: When executing a cold restart on an ESI module, transient CONTCOM alarms will appear in TL1. These can be ignored and will clear once the circuit pack has restarted.</p> <p>Workaround: None.</p>
20261	<p>Description: It is not possible to remove GCC from service on a packet port.</p> <p>Workaround: GCC must be deleted from the port to remove it from service.</p>
20248	<p>Description: If inheriting an IP gateway from OSPF when any node in the OSPF had route redistribution "default originate," do not assign a system gateway. Doing so may result in the node becoming "unreachable."</p> <p>Workaround: Correct the provisioning and restart the SCP.</p> <p>This issue was found in Release 9.2.</p>
19999	<p>Description: The CLI does not allow the IP-NMS port to be unassigned.</p> <p>Workaround: Use the TL1 interface to change the IP-NMS port to unassigned.</p>
19888	<p>Description: The service state of the IP-NMS interface cannot be changed if OSPF Interfaces are configured.</p> <p>Workaround: Determine if the IP-NMS Interface is in the desired service state before configuring OSPF Interfaces.</p>

Issue	Description
19887	<p>Description: If an OSPF Interface is deprovisioned, it may still appear to have an OSPF neighbor when using the RTRV-OSPF-NGHBR command. This information is incorrect and can be ignored since an OSPF neighbor on that interface does not exist.</p> <p>Workaround: None.</p>
19826	<p>Description: Virtual, untagged members of management VLAN are not supported.</p> <p>This issue was found in Release 9.1.</p>
19787	<p>Description: When restoring a database through ODCC/GCC/OSPF to a remote node, the remote node's SCP may need resetting to continue to be accessible remotely.</p> <p>Workaround: Remove OSPF from service and restore it to service</p>
19700	<p>Description: When replacing an SCP with one that is running a different release, the IP NMS gateway information is not restored.</p> <p>Workaround: Perform the SCP replacement upgrade by directly connecting to the SCP.</p>
19687	<p>Description: Loss of Synchronization alarms may not clear during an upgrade of the 10 G Muxponder.</p> <p>Workaround: Restart the SCP to clear the alarm.</p>
19673	<p>Description: A cold restart of the Common Communication Module may cause transient circuit pack failure alarms on active modules.</p> <p>Workaround: The alarms will clear automatically.</p>
19654	<p>Description: A recently powered on Common Communication Module that is not connected to an SCP will periodically flash the green LED on and off.</p>
19548	<p>Description: A change to the ntpClientPollingRate via SNMP may not be reflected immediately.</p> <p>Workaround: The polling rate will respond within a few minutes.</p>
19524	<p>Description: A cold restart of an ESI may result in a transient "connected device unsupported" alarm.</p> <p>Workaround: Wait for the alarm to clear.</p>
19482	<p>Description: It may take several seconds after an OSPF interface is created using the CLI for it to be displayed.</p> <p>Workaround: Wait until the command completes.</p>
19264	<p>Description: During a database restore operation, the TID will not be restored correctly if the database is updated with a different TID value.</p> <p>Workaround: Restart the SCP after the database restore.</p>
19155	<p>Description: During cold reboot of a Common Communication Module (CCM), a circuit pack missing alarm is raised.</p> <p>Workaround: Wait for the CCM to complete the restart and the alarm will clear.</p>

Issue	Description
19140	<p>Description: In software releases 8.1.1 and 8.1.2, the 7200 shelf (PEC BT8A51AR) displays in the inventory as BT8A51AA, when the 7200 is auto-provisioned or when provisioned manually.</p> <p>After an upgrade a shelf mismatch alarm is raised, but, there is no impact on the system.</p> <p>Workaround: Manually edit the shelf PEC through proNX 900 or TL1.</p>
19125	<p>Description: Following an upgrade from a release prior to 7.3, Threshold Crossing Alerts (TCAs) for physical PMs on a port may become disabled.</p> <p>The PhyPMMon port parameter defaults to "OFF". This parameter is not supported.</p> <p>This was found in Release 8.2.1.</p> <p>Workaround: Set the PhyPMMon port parameter to "ON".</p>
19122	<p>Description: CoS Weight for the WRR Scheduler does not take affect for traffic traversing across the Hi-Gig stacking links. This is because Hi-Gig stacking link follows strict queue scheduling across all COS queue with the following priority mapping. This strict priority applies to all traffic traversing the stacking links:</p> <p>Schedule mode: strict</p> <p>Priority to queue mappings:</p> <p>PRI0 0 ==> COSQ 1</p> <p>PRI0 1 ==> COSQ 0</p> <p>PRI0 2 ==> COSQ 2</p> <p>PRI0 3 ==> COSQ 3</p> <p>PRI0 4 ==> COSQ 4</p> <p>PRI0 5 ==> COSQ 5</p> <p>PRI0 6 ==> COSQ 6</p> <p>COSQ 7 is reserved for internal control plane traffic and is excluded from carrying user data traffic.</p> <p>Workaround: None.</p>
18973	<p>Description: When using the CLI, users cannot query PMs by specific MONTYPE.</p> <p>Workaround: Use the "all" option to view all MONTYPE PMs.</p>
18885, 19286	<p>Description: OSPF is not supported on M-VLAN or GCC interfaces in a stacked PVX.</p> <p>Workaround: None.</p>
18366	<p>Description: The UNI interface may allow Y1731 - SLA Measurement packets to egress.</p> <p>Workaround: Enable MAC learning on line-based services.</p>
18359	<p>Description: It is possible to enable both Drop Conform and TOS Conform in Bandwidth Profiles on the packetVX.</p>
18266	<p>Description: The Coding Violation PM for 1 GE ports and the Invalid Blocks PM for 10 GE port montype entities are not counted.</p>

Issue	Description
18125	<p>Description: A newly connected expansion shelf with pack installed may not auto provision.</p> <p>Workaround: Manually provision the packs in the expansion shelf.</p> <p>Status: No fix planned.</p>
18045	<p>Description: When upgrading from Release 7.2.x to 8.2.x, you may encounter a temporary stoppage in traffic.</p> <p>Workaround: None. However, you should perform this upgrade during a maintenance window.</p>
17865	<p>Description: If the values for MEG and MIP are different, MEP creation may fail when provisioning a UNI.</p> <p>Workaround: Ensure that MEG and MIP values are the same and re-provision the UNI and the EService.</p>
17819	<p>Description: OSPF IS State will only ever show IS-NR.</p> <p>Workaround: For the true state of the link, check the state of the port through which this link passes.</p>
17748	<p>Description: The ERPS NNI failures count is one instance higher than the recoveries count.</p> <p>Workaround: None.</p>
17651	<p>Description: On an upgrade from release 8.1.2 to 8.1.3, the CCM in the main shelf may experience a CONTCOM failure, which will result in CONTCOM failures to service modules present in the main shelf. Traffic is not affected by CONTCOM failures.</p> <p>Workaround: Restart the CCM to resolve the CONTCOM alarms.</p>
17516	<p>Description: If both ends of an EFPD-enabled EPLINE service have different CCM intervals configured on their MEPs, in the absence of data being transmitted on the MEPs, EFPD will engage on both ends.</p> <p>Workaround: Configure the CCM intervals to match each other.</p>
17457	<p>Description: When LACP state is globally disabled on a virtual switch and globally re-enabled, the LAG interfaces on that switch remain in a DOWN state, instead of the appropriate In-bundle or Standby state. Traffic through the LAG recovers correctly.</p> <p>This issue was found in Release 8.2.</p> <p>Workaround: Cold-restart the packetVX.</p>
17304	<p>Description: Priority-tc-map queue does not work in a stacked pVX configuration.</p> <p>Workaround: None.</p>
17128	<p>Description: Alarms present on the system may be raised a second time with a different time stamp after an SCP restart.</p> <p>Workaround: None.</p>
17098	<p>Description: When an active module is removed from the 7200 shelf immediately following a CCM reset, it may take up to 30 seconds before the REPLUNITMISS (Circuit Pack Missing) alarm is reported by the system.</p> <p>Workaround: None.</p>

Issue	Description
17025	<p>Description: During an upgrade, the secondary state of the amplifier object may not be reported. This is not service affecting.</p> <p>Workaround: None. The secondary state will appear correctly once the upgrade is completed.</p>
16989	<p>Description: There may be a short delay in the reporting of CONTCOM alarms for modules installed in the 7200 Main Shelf after removing a 7200 Main Shelf Common Communications Module (CCM).</p> <p>Workaround: None.</p>
16866	<p>Description: The Signal Degrade threshold alarm is not activated for SONET/ SDH protocols on the 10G Dual Transponder.</p> <p>Workaround: None.</p>
16695 16988 17132	<p>Description: Conditions that should be masked by alarms may appear as transient alarms following a Common Communications Module (CCM) restart or reconnection of an expansion shelf. This issue is not traffic affecting.</p> <p>Workaround: None.</p>
16647	<p>Description: Cold restarts on 8-Port Multiprotocol Muxponder may cause you to lose GCC IP connectivity.</p> <p>Workaround: None.</p>
16284	<p>Description: Canceling a software upgrade from a pre-8.1 release to an 8.1 release will not properly complete.</p> <p>Workaround: Refer to the Upgrade Guide for the procedure to cancel a software upgrade, or to perform a software downgrade.</p>
16280	<p>Description: Downgrading from 8.1.1 to a pre-8.1 release fails.</p> <p>Workaround: Refer to the Upgrade Guide for the procedure to cancel a software upgrade, or to perform a software downgrade.</p> <p>Status: No fix planned.</p>
16251	<p>Description: When the STP role of a packetVX port is set to Disabled, the port continues forwarding traffic.</p> <p>Workaround: Leave the link in the spanning tree but disable forwarding of packets in the relevant VLANs by adding those VLANs to the Forbidden list on both sides of the link. As a result, the links can never become members of the VLANs in question and therefore traffic in those VLANs will never be forwarded over the link.</p>
16005	<p>Description: All alarms for an expansion shelf are not masked when the expansion shelf is placed out of service.</p>
15969	<p>Description: A warm reset of the CCM causes transient CONTCOM alarms on service modules in the same shelf as the CCM. This is not traffic affecting.</p>
15963	<p>Description: Removing the CCM from the main shelf results in CONTCOMM alarms for all the modules in the shelf.</p> <p>Workaround: insert the CCM back into the shelf.</p>

Issue	Description
15896, 16333	<p>Description: During an upgrade/downgrade, a DSP Communications failure alarm may occur on the OLAM module.</p> <p>Workaround: After upgrading/downgrading, restart the OLAM module to clear the alarm.</p>
15438	<p>Description: If the Management VLAN IP address is changed on a system that is already configured for Management VLAN, the Management VLAN may no longer function properly.</p> <p>Workaround: Restart the SCP after the change is made.</p>

4.2 Hardware Limitations

Issue	Description	Affects
10514	<p>Description: 4G SFPs operate with reduced extinction ratio on packetVX modules.</p> <p>Workaround: The optical performance of the 4G SFPs (BP3AD2SS and BP3AD2MS) is not IEEE 802.3 compliant, but has proven to work in most applications. The packetVX modules should use BP3AD1SS (850nm) and BP3AM1MS (1310nm) SFPs.</p>	BT7A81AA BT7A81BA BT7A81CA

4.3 proNX 900 Node Controller Limitations

Issue	Description
23013	<p>Description: After a remote ODCC node loses and recovers communications, a ProNX 900 session may not recover when using the File > Re-establish Login menu to re-establish the session.</p> <p>Symptom: Within the Optical Groups navigation, the drop-down menus for all the modules are not functional.</p> <p>Workaround: Close and re-open the ProNX 900 session to recover all menu functionality.</p>
17800	<p>Description: The Commit button is greyed-out in the Upgrade window.</p> <p>Workaround: Exit the proNX 900 and restart it to commit the upgrade, or type the command into the Telnet window.</p>
17692	<p>Description: The proNX 900 does not respond to database delete events, manual refreshes are required.</p> <p>Workaround: To view updates after a database delete, refresh the proNX 900 to view the updates. In addition, if the TID has changed a new session is required.</p>

Issue	Description
16487	<p>Description: Pre-8.2 releases of proNX 900 do not discover Eservices.</p> <p>Workaround: You must first upgrade proNX900 to the latest version before upgrading packetVX nodes from pre-8.2 releases to a higher release.</p>
15321	<p>Description: After a cold restart of 10G Transponder, the system raises the following error in proNX: "Error retrieving inventory for SLOT-X-X: Internal Application Error."</p> <p>Workaround: None.</p>
13411	<p>Description: In this release, it is not possible to filter layer 3 fields in policy maps.</p> <p>Workaround: None.</p>
3459	<p>Description: A user with 'maintenance' user privileges is not permitted, after disabling a loopback, to set the port to AINS on a Wavelength Translator, Wavelength Manager or Wavelength Regenerator module.</p> <p>Workaround: Use an account with the user privilege level of 'provisioning' or above to successfully disable a loopback and set the port to AINS.</p>

5 Related Documentation

For more information on the BTI 7000 Series, refer to these publications:

- *BTI 7000 Series Common Equipment Installation Guide*
- *BTI 7000 Series Test and Turn-up Guide*
- *BTI 7000 Series Upgrade Guide*
- *BTI 7000 Series Operations Solutions Guide*
- *BTI 7000 Series Transponder Solutions Guide*
- *BTI 7000 Series Muxponder Solutions Guide*
- *BTI 7000 Series packetVX® Solutions Guide*
- *BTI 7000 Series Optical Amplifier and DCM Solutions Guide*
- *BTI 7000 Series Multiplexing Solutions Guide*
- *BTI 7000 Series Alarm and Troubleshooting Guide*
- *BTI 7000 Series SNMP Overview Guide*
- *BTI 7000 Series TL1 Reference Guide*
- *BTI 7000 Series Command Line Reference Guide*
- *BTI 7000 Series Dynamic Optical Layer Engineering Guideline*
- *BTI 7000 Series Management Communications Channel Solutions Guide*
- *BTI 7000 Series Transceiver Information Guide*
- *BTI 7000 Series Product Guide*

6 Upgrade Considerations

This section explains how to work around various issues that may arise after upgrading from BTI software Releases 8.x or 9.x to Releases 10.3.x and later.

For more information about the CLI commands used in these procedures, refer to the *BTI 7000 Series Command Line Reference Guide*.

Storm Control values out of range after upgrade

Issue

Releases prior to 9.2 do not support Storm Control. After upgrading from a release prior to 9.2, the Storm Control values may be corrupt, and the system prevents you from shutting down NNI interfaces, for example:

```
BTI7000:sw1(config-nni TenGigE 11/~)# shutdown

% Storm Control rate limit specified is out of range,
allowed 0 through 100
```

Workaround

To clear this condition, you must use SNMP to build an SNMP set request that sets all three storm control values as a single PDU. Valid storm control values are: 100%, 60%, 40%, and 20%. Note that 100% means that Storm Control protection is not configured.

Note: All three storm control attributes must be set automatically, otherwise, the set fails.

The following example shows an SNMP set request using the value 20%:

```
snmpset -v 2c -c private <IP address>
pvxL2IntfBcastLimit.1.1.3.xGigE.1 i 20
pvxL2IntfMcastLimit.1.1.3.xGigE.1 i 20
pvxL2IntfDlfLimit.1.1.3.xGigE.1 i 20

BTI-7000-MIB::pvxL2IntfBcastLimit.1.1.3.xGigE.1 = INTEGER: 20
BTI-7000-MIB::pvxL2IntfMcastLimit.1.1.3.xGigE.1 = INTEGER: 20
BTI-7000-MIB::pvxL2IntfDlfLimit.1.1.3.xGigE.1 = INTEGER: 20

<user id>-lx2:~/erpsv2/OLS-ERPSV2-N2$
```

Stacked packetVX environment

Issue

Upgrading causes corruption in the data structure. Although traffic is not affected, you may observe undesired system behavior.

Workaround

Perform a cold reboot on each stacked packetVX module simultaneously, to allow the system to re-initialize its state and return to normal behavior. Follow this procedure:

1. Enter Privileged EXEC mode.
2. For each packetVX, type the command: **reload <shelf/slot> cold**, for example:

```
BTI7000:sw1(config)# reload <shelf/slot> cold
```

```
BTI7000:sw1(config)# reload <shelf/slot> cold
```

This procedure is a one-time event for upgrades from releases prior to 9.2.

After the system is upgraded to Release 10.3.x or later, the data structure remains clear of further corruption during subsequent upgrades. Simultaneous cold reboot is not expected.

ERPS in a Stacked or Non-stacked packetVX environment

Issue

When upgrading a network running G.8032-V1, multiple ports may be blocked on the ring isolating a node (Known issue: 26011).

Workaround

Before you upgrade, remove ERPS V1. After the upgrade, migrate to ERPS V2, which involves re-provisioning the ERPS services. Follow this procedure:

1. To prevent loops, manually block all RPLs using the command **admin-state disable**, or **shutdown**.
2. On each ring, one at a time: Delete the ERPS service across all the nodes of the particular ring.
3. Delete one ring at a time.
4. Re-provision ERPS across all the nodes of the particular ring. By default, the new ERPS service uses ERPS V2.
5. Enable the blocked RPLs.
6. Go to the next ring and repeat this procedure.

Issue

In ERPS v1, when upgrading from Releases 8.x or 9.x to 10.3.x or later, MSTP NNIs adjacent to the ERPS rings may lose their VLAN membership on some eServices.

If this happens you must toggle the administrative state down and up on the MSTP node.

Workaround

To avoid this from occurring, you must first upgrade each ERPS node, before upgrading all other nodes.

LAG MEP IDs Change after the Upgrade

Issue

In Releases prior to 10.x, the MEP ID for a UNI LAG is based on the MAC address of the first member of the LAG. Beginning with Release 10.x, the MEP ID is based on the MAC address of the LAG.

This is a service affecting issue. After the upgrade the operational state of the system is down, since there is no translation to accommodate the different MEP ID rules.

Workaround

To resolve this issue follow this procedure. You must repeat these steps for every service that has a LAG UNI as a remote MEP ID and is part of the upgrade:

1. Go to the eService configuration for the DOWN eService—the end with the LAG as a Remote MEP, not Local MEP:

```
BTI7000:sw1(config)# eservice <service-name> [type  
<service-type>]
```

2. Display the existing eService configuration, and take note of the old and new LAG MEP IDs, and the SLA Initiator (if there is one) :

```
BTI7000:sw1(config)# show eservice [<service-name>] [name  
<service-name>]
```

3. Go to the service UNI on the eService:

```
BTI7000:sw1(config-eservice)# uni<interface-type>  
<interface-id>
```

4. If an SLA Initiator/Responder exists, you must delete it before you continue with the next step:

```
BTI7000:sw1(config-uni-eservice)# no sla rmep <mep id>  
loss initiator
```

5. Relearn all the remote MEP IDs on the service UNI:

```
BTI7000:sw1 (config-uni-eservice)# cfm flush-rmep-db
```

6. Add the new SLA Initiator/Responder

```
BTI7000:sw1(config-uni-eservice)# sla rmep <mep id> loss  
init
```

Repeat these steps for every service with a LAG UNI as a remote MEP ID.