6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

Customer Release Notes

VSP Operating System Software

Software Release 8.1.8.0
December 2020

INTRODUCTION:

This document provides specific information for version 8.1.8.0 of agent software for the VSP Operating System Software.

The purpose of this version is to address customer and internally found software issues.

Extreme Networks recommends that you thoroughly review this document prior to installing or upgrading this product.

For the latest firmware versions, visit the download site at:
www.extremenetworks.com/support/

NEW IN THIS RELEASE:

For **XA1440** platforms, in order to improve throughput of a FE tunnel over WAN circuit (VOSS-18731) the **IPSEC compression** and **TCP adjust-mss** enhancements were added.
Please see “New Features in this release” section below for more information.

IMPORTANT NOTES BEFORE UPGRADING TO THIS RELEASE:

If upgrading systems from either release 4.2.1.0 or release 4.2.1.1 that have ISIS enabled link(s) configured with HMAC-MD5 authentication, then you need to perform the procedure described in the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** in order to avoid potential network connectivity loss.

If upgrading systems running 4.1.X releases which also have TACACS+ enabled, refer to the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** for upgrade instructions.

If upgrading systems running 6.0.x releases or older, refer to the section ***SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES*** for instructions about the need to step-through a 6.1.x release prior to going to 7.1.x release.

UPGRADE CONSIDERATION WHEN UPGRADING TO 8.1.8.0 FROM PREVIOUS RELEASE:

If you have a VLAN with VRRP instance of 37 provisioned and functional on a node running with several other VLANs with DvR enabled, upon upgrade to 8.1.8.0, VRRP configuration for instance 37 is removed from that VLAN. This would result in traffic loss for members of that VLAN. Recommend renumbering the VRRP instance IDs to values other than 37 and 38 on that VLAN before upgrading.
DvR uses the same multicast addresses as VRRP ID 37 and 38 for its DvR controller and leaf implementation.

PLATFORMS SUPPORTED:

Virtual Services Platform 4400 Series
Virtual Services Platform VSP 4450GSX-PWR+
Virtual Services Platform VSP 4450GSX-DC
Virtual Services Platform VSP 4450GTS-DC
Virtual Services Platform VSP 4450GTX-HT-PWR+

Virtual Services Platform 4900 Series
Virtual Services Platform VSP 4900-48P
Virtual Services Platform VSP4900-12MXU-12XE
Virtual Services Platform VSP4900-24S
Virtual Services Platform VSP4900-24XE

Virtual Services Platform 7200 Series
Virtual Services Platform VSP 7254XSQ
Virtual Services Platform VSP 7254XTQ

Virtual Services Platform 7400 Series
Virtual Services Platform VSP 7432CQ
Virtual Services Platform VSP 7400-48Y-8C

Virtual Services Platform 8200 Series
Virtual Services Platform 8284XSQ

Virtual Services Platform 8400 Series
Virtual Services Platform 8404
Virtual Services Platform 8404C

ExtremeAccess Platform XA1400 Series
ExtremeAccess Platfrom 1440
ExtremeAccess Platform 1480

SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES:

1. The following procedure should be followed when upgrading systems running one of the following two releases, 4.2.1.0 or 4.2.1.1 which also have ISIS enabled links with HMAC-MD5 authentication on:

   Disable ISIS authentication throughout the network a system at a time, a link at a time by disabling it on either side of each link, ensuring the link is stable before moving to the next. When a system has been reconfigured free of ISIS HMAC-MD5 authentication in all of its links, save the configuration file and perform the upgrade to release 4.2.3.0 or greater. After all these systems have been upgraded to release 4.2.3.0 or greater, you may re-enable authentication a system at a time, a link at a time and save the configuration file in each of the involved systems.

   Example:

```
VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)#no isis hello-auth
VSP:1(config-if)#save config
VSP:1(config-if)# PERFORM THE UPGRADE
VSP:1(config)#interface gigabitethernet x/y
VSP:1(config-if)# isis hello-auth type hmac-md5 key <keyname> [key-id
<keyed>]
VSP:1(config-if)#save config
```

2. The following procedure should be followed when upgrading systems running 4.1.X releases which also have TACACS+ enabled on:

   When you upgrade from VOSS 4.1.X to VOSS 4.2 or a higher release, the TACACS+ host configurations will be lost. After the upgrade, the TACACS+ host configurations will not take effect so you must reconfigure them. After you make the configurations, you must save the changes on the device. You should also save the configuration to a file to retain the configuration settings.

3. Upgrading DVR configurations from releases 6.0.1.1 and earlier to 6.0.1.2 and beyond.
   a. All DVR nodes must be upgraded to the same release.
   b. All DVR leaves should be upgraded first.

4. Upgrading from releases 6.0.x and earlier
   a. Direct upgrade from 6.0.x or earlier releases to 7.x releases is not supported.
   b. Please upgrade to a 6.1.x release first (Release 6.1.6.0 or higher is recommended). Then upgrade to the desired 7.x release (Release 7.1.1.0 or higher recommended).

Review items 5, 6, and 7 if the ISIS L1 area is **`00.1515.fee1.900d.1515.fee1.900d`**, 00.0000.0000 or all zero's.

5. Legacy ZTF Procedures for Releases 7.0.0.0 - 7.1.2.0, 8.0.0.0, 8.0.1.0, and 8.0.5.0
   a. Boot with factory-defaults fabric.
   b. ISIS manual-area set to 00.0000.0000, Dynamically Learned Area (DLA) displayed as 00.0000.0000 and ISIS enabled with other parameters.
   c. HELLO PDUs not sent.
   d. Listen on active ISIS interfaces for ISIS HELLO with non-zero Area ID. Zeros of any length up to 13 bytes are considered a zero value.
   e. When an ISIS HELLO with a non-zero Area ID is received, use that area ID as the DLA and start sending HELLO with DLA on all ISIS interfaces.
   f. DLA set and displayed as learned in the previous step.
   g. Saving the configuration will save into the configuration file `manual-area 00.0000.0000`.
   h. Boot with the saved configuration. The ZTF procedures are triggered. ISIS interfaces in passive mode not sending ISIS HELLOs. Only process incoming ISIS HELLO with non-zero Area ID.

   Note: You can reach the fourth step by manually configuring the ISIS/SPBM with a manual-area equal to 0 (all values of 0, regardless of the length of zeros, are considered the same) and enabling ISIS.

6. Modified ZTF Procedures for Releases 7.1.3.0+ and 8.0.6.0+
   a. Boot with factory-defaults fabric
   b. ISIS manual-area set to 00.1515.fee1.900d.1515.fee1.900d, Dynamically Learned Area (DLA) is blank and ISIS enabled with other parameters.
   c. HELLO PDUs not sent
   d. Listen on active ISIS interfaces for ISIS HELLO with and Area ID not equal to **`00.1515.fee1.900d.1515.fee1.900d`**.
   e. When an ISIS HELLO with an Area ID not equal to **`00.1515.fee1.900d.1515.fee1.900d`** is received, use that Area ID as the DLA and start sending HELLO with DLA on all ISIS interfaces.
   f. DLA set and displayed as learned in the previous step.

g. Saving the configuration file will save into the configuration file `manual-area 00.1515.fee1.900d.1515.fee1.900d`.

h. Boot with the saved configuration. ZTF procedures are triggered. ISIS interfaces in passive mode not sending ISIS HELLO's, only processing incoming ISIS HELLO with an Area ID note equal to **`00.1515.fee1.900d.1515.fee1.900d`**.

Note: You can reach the fourth step by manually configuring the ISIS/SPBM with a manual-area equal to 00.1515.fee1.900d.1515.fee1.900d and enabling ISIS.

7. Migration to a Release supporting Modified ZTF such as 7.1.3.0+ or 8.0.6.0+

   a. From Pre-ZTF feature Release such as 6.1.6.0

   The following considerations should be taken into account when upgrading to this release from a pre-ZTF release:

   i. Check the ISIS manual area (show isis manual-area).
   ii. Determine if the manual area equals 00.1515.fee1.900d.1515.fee1.900d.
   iii. This is a normal Area ID before the upgrade. After the upgrade, ZTF procedures, as previously described, will be triggered.
   - If the existing behavior is desired, the ISIS manual area used in the network needs to be changed to a different value. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The changes to the manual area within the topology should be made before any upgrades are performed.

   b. From a Release Running Legacy ZTF such as 7.1.2.0

   The following considerations should be taken into account when upgrading to a release supporting Modified ZTF from a Legacy ZTF release.

   - Check the ISIS manual area (show isis manual-area).
   - Determine if the manual area equals 00.0000.0000 or is a 00 of any length.
   - This Area ID triggered the ZTF procedures before the upgrade. After the upgrade, ZTF procedures, as previously described, will NOT be triggered.
   - If the existing behavior is desired, replace the value of ISIS manual area with 00.1515.fee1.900d.1515.fee1.900d. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The change should be made before the upgrade.
   - Determine if the manual area equals 00.1515.fee1.900d.1515.fee1.900d.
     - This is a normal Area ID before the upgrade. After the upgrade to a release implementing
   - Modified ZTF, the ZTF procedures, as previously described, will be triggered.
   - If this is not desired, replace the value of ISIS manual area with a different value. Note, if ISIS is the management network used to get to the node, it will not form an ISIS adjacency after the upgrade and not join the network. This will isolate the node. The change should be made before the upgrade.

NOTES FOR UPGRADE:

Please see "Release Notes for VSP Operating System Software (VOSS)" for software release 8.1.5 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

FILE NAMES FOR THIS RELEASE:

Virtual Services Platform 4400 Series

File Name	Module or File Type	File Size (bytes)
VOSS4400.8.1.8.0.sha512	SHA512 Checksums	1395
VOSS4400.8.1.8.0.md5	MD5 Checksums	476
VOSS4400.8.1.8.0.tgz	Release 8.1.8.0 archived software distribution	110247162
VOSS4400.8.1.8.0_mib.zip	Archive of all MIB files	1160789
VOSS4400.8.1.8.0_mib.txt	MIB file	7702128
VOSS4400.8.1.8.0_mib_sup.txt	MIB file	1364272
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 4900 Series

File Name	Module or File Type	File Size (bytes)
VOSS4900.8.1.8.0.sha512	SHA512 Checksums	1547
VOSS4900.8.1.8.0.md5	MD5 Checksums	532
VOSS4900.8.1.8.0.tgz	Release 8.1.8.0 archived software distribution	239079120
VOSS4900.8.1.8.0_mib.zip	Archive of all MIB files	1160789
VOSS4900.8.1.8.0_mib.txt	MIB file	7702128
VOSS4900.8.1.8.0_mib_sup.txt	MIB file	1385881
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7200.8.1.8.0.sha512	SHA512 Checksums	1395
VOSS7200.8.1.8.0.md5	MD5 Checksums	476
VOSS7200.8.1.8.0.tgz	Release 8.1.8.0 archived software distribution	124591831
VOSS7200.8.1.8.0_mib.zip	Archive of all MIB files	1160789
VOSS7200.8.1.8.0_mib.txt	MIB file	7702128
VOSS7200.8.1.8.0_mib_sup.txt	MIB file	1369354
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7400 Series

File Name	Module or File Type	File Size (bytes)
VOSS7400.8.1.8.0.sha512	SHA512 Checksums	1547
VOSS7400.8.1.8.0.md5	MD5 Checksums	532
VOSS7400.8.1.8.0.tgz	Release 8.1.8.0 archived software distribution	238732165
VOSS7400.8.1.8.0_mib.zip	Archive of all MIB files	1160789
VOSS7400.8.1.8.0_mib.txt	MIB file	7702128
VOSS7400.8.1.8.0_mib_sup.txt	MIB file	1380078
VOSS7400v815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020
TPVM_7400_8.1.8.0.img	Third Party Virtual Machine (TPVM)	1677066240

Virtual Services Platform 8200 Series

File Name	Module or File Type	File Size (bytes)
VOSS8200.8.1.8.0.sha512	SHA512 Checksums	1395
VOSS8200.8.1.8.0.md5	MD5 Checksums	476
VOSS8200.8.1.8.0.tgz	Release 8.1.8.0 archived software distribution	124597074
VOSS8200.8.1.8.0_mib.zip	Archive of all MIB files	1160789
VOSS8200.8.1.8.0_mib.txt	MIB file	7702128
VOSS8200.8.1.8.0_mib_sup.txt	MIB file	1369354
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 8400 Series

File Name	Module or File Type	File Size (bytes)
VOSS8400.8.1.8.0.sha512	SHA512 Checksums	1395
VOSS8400.8.1.8.0.md5	MD5 Checksums	476
VOSS8400.8.1.8.0.tgz	Release 8.1.8.0 archived software distribution	185806759
VOSS8400.8.1.8.0_mib.zip	Archive of all MIB files	1160789
VOSS8400.8.1.8.0_mib.txt	MIB file	7702128
VOSS8400.8.1.8.0_mib_sup.txt	MIB file	1369354
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669
restconf_yang.tgz	YANG model	506020

ExtremeAccess 1400 Series

File Name	Module or File Type	File Size (bytes)
VOSS1400.8.1.8.0.sha512	SHA512 Checksums	1395
VOSS1400.8.1.8.0.md5	MD5 Checksums	476
VOSS1400.8.1.8.0.tgz	Release 8.1.8.0 archived software distribution	320548759
VOSS1400.8.1.8.0_mib.zip	Archive of all MIB files	1160789
VOSS1400.8.1.8.0_mib.txt	MIB file	7702128
VOSS1400.8.1.8.0_mib_sup.txt	MIB file	1045725
VOSSv815_HELP_EDM_gzip.zip	EDM Help file	4328669

Note about image download:

Ensure images are downloaded using the binary file transfer. Perform MD5 checksum check on downloaded files to ensure file integrity.

Check that the file type suffix is ".tgz" and the image names after download to device match those shown in the above table. Some download utilities have been observed to append ".tar" to the file name or change the filename extension from ".tgz" to ".tar". If file type suffix is ".tar" or file name does not exactly match the names shown in above table, rename the downloaded file to the name shown in the table above so that the activation procedures will operate properly.

Load activation procedures:

```
software add VOSS4400.8.1.8.0.tgz
software activate 8.1.8.0.GA
```

or

```
software add VOSS4900.8.1.8.0.tgz
software activate 8.1.8.0.GA
```

or

```
software add VOSS7200.8.1.8.0.tgz
software activate 8.1.8.0.GA
```

or

```
software add VOSS7400.8.1.8.0.tgz
software activate 8.1.8.0.GA
```

or

```
software add VOSS8200.8.1.8.0.tgz
software activate 8.1.8.0.GA
```

or

```
software add VOSS8400.8.1.8.0.tgz
software activate 8.1.8.0.GA
```

or

```
software add VOSS1400.8.1.8.0.tgz
software activate 8.1.8.0.GA
```

COMPATIBILITY:

This software release is managed with Enterprise Device Manager (EDM), which is integrated into the agent software.

CHANGES IN THIS RELEASE:

New Features in This Release

For **XA1440** platforms, in order to improve throughput of a FE tunnel over WAN circuit (VOSS-18731) the **IPSEC compression** and **TCP adjust-mss** enhancements were added.

IPSEC compression

The **IPSEC compression** is part of the IPSEC over FE feature and it is added to reduce the size of the IP datagram in order to improve the communication performance between hosts connected behind XA BEBs.

- The IPSEC compression is a per logical-interface setting. User can have multiple IPSEC FE adjacencies with or without compression at the same time.
- The default state of IPSEC compression is *disabled*.
- To have the IPSEC compression for a FE adjacency with IPSEC, IPSEC compression needs to be enabled on both sides of the link (both of the BEBs).
- In order to enable/disable IPSEC compression for a logical interface, the IPSEC need to be disabled. If the user tries to change the IPSEC compression setting for a logical-interface with IPSEC enable the error message "*Error: IPSec is enabled on logical interface, please disable IPSec before modifying ipsec compression*" will be generated.
- The recommendation is to use IPSEC compression only for tunnels where latency is greater than 70ms.

CLI commands

show mode:

```
XA1480-1:1(config-isis-2-15.15.15.151)#show isis logical-interface ipsec
************************************************************************************
                Command Execution Time: Fri Dec 04 14:34:40 2020 UTC
************************************************************************************

====================================================================================================
                          ISIS Logical Interface IPSec
====================================================================================================
ID       Authentication-Key                Responder-Only   Remote NAT IP    Compression
----------------------------------------------------------------------------------------------------
2        ******                            False            -                False

----------------------------------------------------------------------------------------------------
 1 out of 2 Total Num of Logical ISIS interfaces
----------------------------------------------------------------------------------------------------
XA1480-1:1(config-isis-2-15.15.15.151)#
```

config mode:

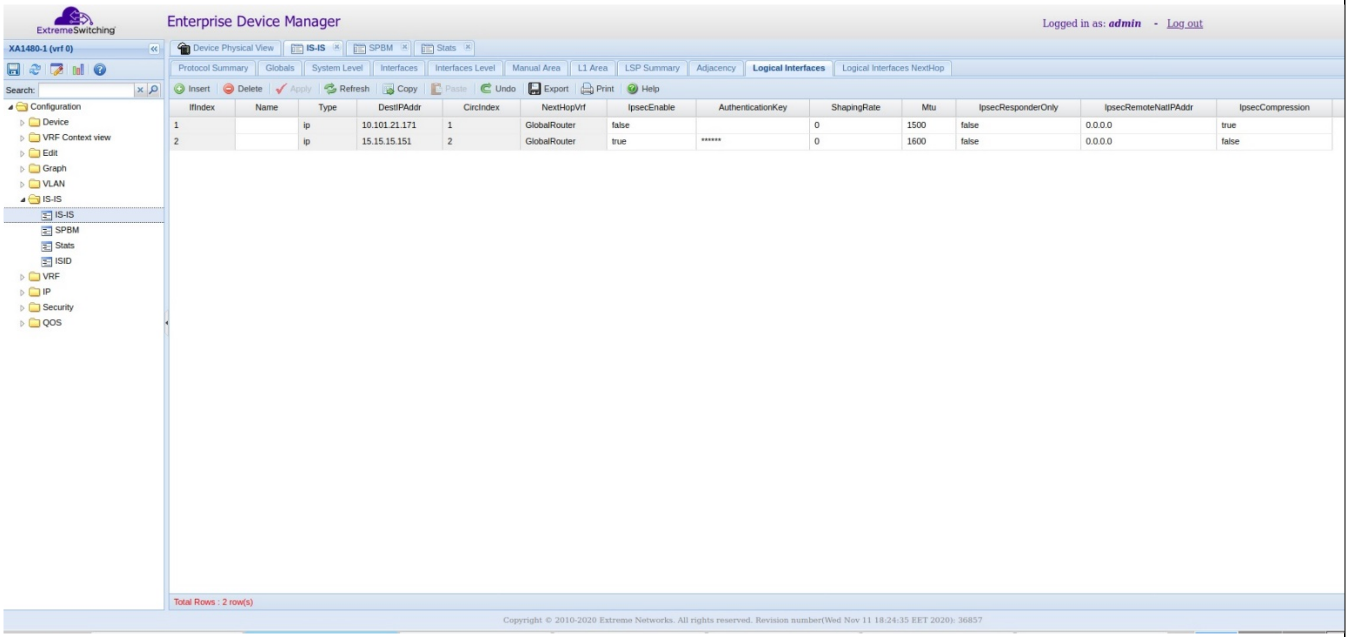
```
XA1480-1:1(config-isis-2-15.15.15.151)#ipsec compression
XA1480-1:1(config-isis-2-15.15.15.151)#
XA1480-1:1(config-if)#show isis logical-interface ipsec
************************************************************************************
                Command Execution Time: Fri Dec 04 14:00:45 2020 UTC
************************************************************************************
```

```
=========================================================================================
                          ISIS Logical Interface IPSec
=========================================================================================
ID        Authentication-Key              Responder-Only   Remote NAT IP     Compression
-----------------------------------------------------------------------------------------
2         ******                          False            -                 True

-----------------------------------------------------------------------------------------
 1 out of 2 Total Num of Logical ISIS interfaces
-----------------------------------------------------------------------------------------


XA1480-1:1(config-isis-2-15.15.15.151)#no ipsec compression
XA1480-1:1(config-isis-2-15.15.15.151)#
```

SNMP object:
For IPSec Compression new object was added into rcIsisLogicalInterfaceTable from rcIsis.mib:

```
rcIsisLogicalInterfaceIpsecCompression OBJECT-TYPE
       SYNTAX       TruthValue
       MAX-ACCESS   read-create
       STATUS       current
       DESCRIPTION  "Indicate if IPSec compression is enabled on logical interface.
                     This object is applicable only for ExtremeAccess platforms XA1440 and
                     XA1480."
                     DEFVAL { false }
::= { rcIsisLogicalInterfaceEntry 24 }
```

EDM:



IfIndex	Name	Type	DestIPAddr	CircIndex	NextHopVrf	IpsecEnable	AuthenticationKey	ShapingRate	Mtu	IpsecResponderOnly	IpsecRemoteNatIPAddr	IpsecCompression
1		ip	10.101.21.171	1	GlobalRouter	false		0	1500	false	0.0.0.0	true
2		ip	15.15.15.151	2	GlobalRouter	true	******	0	1600	false	0.0.0.0	false

Total Rows : 2 row(s)

Copyright © 2010-2020 Extreme Networks. All rights reserved. Revision number(Wed Nov 11 18:24:35 EET 2020): 36857

TCP adjust-mss

In order to improve the throughput for the TCP session over the FE adjacency the IP TCP adjust-MSS enhancement was added.

- The default state of the feature is enabled and auto-derived

- When enbled, the MSS adjustment functionality will only become active when at least one FE tunnel with MTU <= 1500 is configured. The feature is inactive if no FE tunnels with MTU <= 1500 are configured
- Deleting the last tunnel with MTU <= 1500 will result in the feature becoming inactive
- The MSS value can be auto derived based of the tunnel MTUs or can be manual configured by the user.
  - The MSS auto-derived value is equals will be min(Tunnels MTUs) - 250B (size for VXLAN + MIM + IPSEC + IP+TCP headers) . So. if there are multiple FE tunnels configured on the XA (with MTU <=1500) then the lowest of all tunnel MTUs will be used to auto derive the TCP MSS adjust value and the same value is applied to all TCP syn packets that are going via NNI to UNI and vice-versa.
  - User can override the auto derived TCP adjust MSS value by explicitly configuring a value. If the uses config a value when tcp adjust-mss is inactive, the configured value will be applied when a logical intf with mtu <=1500 is configured. If user wants to go back to the auto-derive MSS value the "no ip tcp adjust-mss mss" command can be used.

- User can explicitly disable the TCP adjust mss enhancement by issuing "*no ip tcp adjust-mss*" command.
- To have TCP adjust-MSS active for a tunnel, it is enough to have the enhancement enabled/active at only side of the tunnel. The MSS is adjusted for NNI to UNI and UNI to NNI TCP packets.
- Recommendation is to turn off this enhancement on the head-end side XA explicitly and keep this enabled only at branch side XAs as it enough to be enabled on only one side.
- The user can disable tcp adjust-mss at one end because the adjust-mss will happen on the other end (branch XA) when there, a tunnel with MTU < 1500 is coming into the picture. For the XA where the feature was disabled, even if a tunnel with MTU <= 1500 will be configured, no mss-adjust will happen. (In this way, for the head-end XA the tcp-mss adjust will happen only thought the tunnel with the branch XA.)

Limitations:

- We cannot support different TCP adjust MSS values if user has configured different FE tunnel MTUs on different tunnels.
- If user has some FE tunnels and some regular NNIs on same XA (FC adjacency) then TCP adjust mss value will be applied to all TCP packets traversing across regular NNIs and FE tunnels.

CLI commands

Mode: `router isis configuration`

ip tcp adjust-mss [mss <500-1250>]

```
      XA1480-1:1(config)#router isis
      XA1480-1:1(config-isis)# ip tcp adjust-mss 1100
      XA1480-1:1(config-isis)#
```

no ip tcp adjust-mss [mss]

```
      XA1480-1:1(config)#router isis
      XA1480-1:1(config-isis)#no ip tcp adjust-mss ?
        mss  Set TCP MSS value to default
        <cr>
      XA1480-1:1(config-isis)#no ip tcp adjust-mss mss
```

Show IP TCP adjust MSS info:

Mode: privExec
show isis tcp adjust-mss

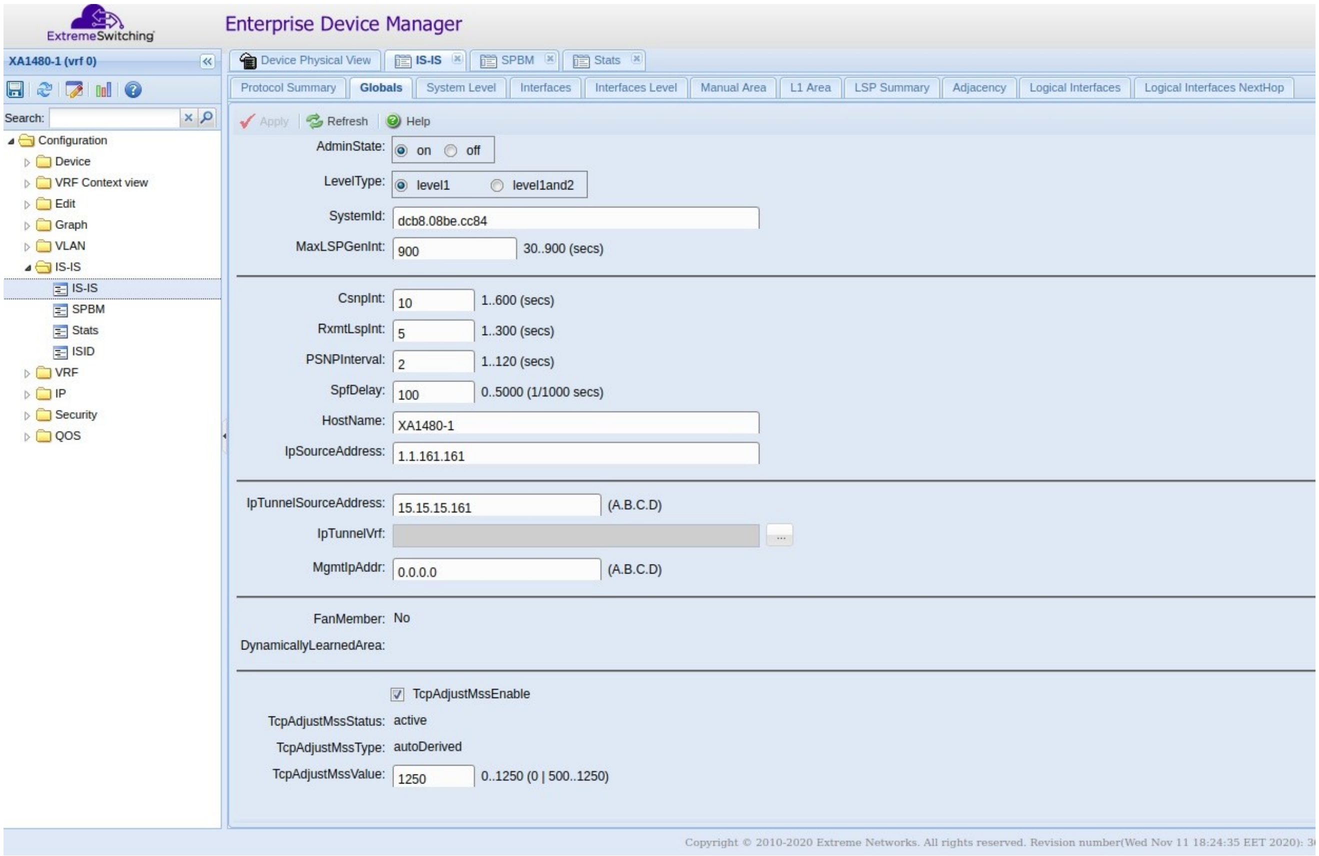
```
XA1480-1:1#show isis tcp adjust-mss
************************************************************************************
                Command Execution Time: Fri Dec 04 15:28:59 2020 UTC
************************************************************************************

================================================================================
                              ISIS TCP Adjust MSS
================================================================================
ENABLE            STATUS            TCP MSS                   TCP MSS
                                    TYPE                      VALUE
--------------------------------------------------------------------------------
TRUE              INACTIVE          AUTO-DERIVED              0
XA1480-1:1#

XA1480-1:1(config)#show isis logical-interface mtu
************************************************************************************
                Command Execution Time: Fri Dec 04 15:29:47 2020 UTC
************************************************************************************

====================================================================================================
                           ISIS Logical Interface Mtu
====================================================================================================
ID       NAME                                                              MTU
----------------------------------------------------------------------------------------------------
1        --                                                                1500
2        --                                                                1600

----------------------------------------------------------------------------------------------------
 2 out of 2 Total Num of Logical ISIS interfaces
----------------------------------------------------------------------------------------------------

XA1480-1:1(config)#show isis tcp adjust-mss
************************************************************************************
                Command Execution Time: Fri Dec 04 15:29:54 2020 UTC
************************************************************************************

================================================================================
                              ISIS TCP Adjust MSS
================================================================================
ENABLE            STATUS            TCP MSS                   TCP MSS
                                    TYPE                      VALUE
--------------------------------------------------------------------------------
TRUE              ACTIVE            AUTO-DERIVED              1250

XA1480-1:1(config)#
XA1480-1:1(config)#router isis
XA1480-1:1(config-isis)#ip tcp adjust-mss mss 1100
XA1480-1:1(config-isis)#show isis tcp adjust-mss
************************************************************************************
                Command Execution Time: Fri Dec 04 15:30:11 2020 UTC
************************************************************************************

================================================================================
                              ISIS TCP Adjust MSS
================================================================================
ENABLE            STATUS            TCP MSS                   TCP MSS
                                    TYPE                      VALUE
--------------------------------------------------------------------------------
TRUE              ACTIVE            MANUAL-CONFIG             1100

XA1480-1:1(config-isis)#no ip tcp adjust-mss mss
XA1480-1:1(config-isis)#show isis tcp adjust-mss
************************************************************************************
                Command Execution Time: Fri Dec 04 15:30:29 2020 UTC
************************************************************************************
```

```
================================================================================
                              ISIS TCP Adjust MSS
================================================================================
ENABLE            STATUS            TCP MSS                   TCP MSS
                                    TYPE                      VALUE
--------------------------------------------------------------------------------
TRUE              ACTIVE            AUTO-DERIVED              1250
XA1480-1:1(config-isis)#
```

SNMP

```
rcIsisGlobalTcpAdjustMssEnable  OBJECT-TYPE
          SYNTAX        TruthValue
          MAX-ACCESS    read-write
          STATUS        current
          DESCRIPTION   "Enable or disable adjusting the maximum segment size (MSS) value of
TCP packets. This object is applicable only for ExtremeAccess platforms XA1440 and XA1480."
          DEFVAL         { true }
::= { rcIsisGlobalGroup 27 }

rcIsisGlobalTcpAdjustMssStatus  OBJECT-TYPE
           SYNTAX        INTEGER{active(1),inactive(2)}
           MAX-ACCESS    read-only
           STATUS        current
           DESCRIPTION   "Status of TCP adjust MSS.
                          This object is applicable only for ExtremeAccess platforms XA1440
and XA1480."
           DEFVAL             { inactive }
::= { rcIsisGlobalGroup 28 }

rcIsisGlobalTcpAdjustMssType  OBJECT-TYPE
           SYNTAX             INTEGER{autoDerived(1),manualConfig(2)}
           MAX-ACCESS         read-write
           STATUS             current
           DESCRIPTION        "Type of TCP adjust MSS.
                              This object is applicable only for ExtremeAccess platforms
XA1440 and XA1480."
           DEFVAL              { autoDerived }
::= { rcIsisGlobalGroup 29 }

rcIsisGlobalTcpAdjustMssValue  OBJECT-TYPE
          SYNTAX              Integer32 (0 | 500..1350)
          MAX-ACCESS          read-write
          STATUS              current
          DESCRIPTION         "TCP adjust MSS value.
                              If rcIsisGlobalTcpAdjustMssEnable is true,
rcIsisGlobalTcpAdjustMssValue is 0 or different than 0,no matter what
rcIsisGlobalTcpAdjustMssType is.
                              If rcIsisGlobalTcpAdjustMssEnable is false,
rcIsisGlobalTcpAdjustMssValue is different than 0 only if rcIsisGlobalTcpAdjustMssType is
manualConfig. This object is applicable only for ExtremeAccess platforms XA1440 and XA1480."
          DEFVAL              { 0 }
::= { rcIsisGlobalGroup 30 }
```

EDM



AdminState: ● on ○ off

LevelType: ● level1 ○ level1and2

SystemId: dcb8.08be.cc84

MaxLSPGenInt: 900 30..900 (secs)

CsnpInt: 10 1..600 (secs)

RxmtLspInt: 5 1..300 (secs)

PSNPInterval: 2 1..120 (secs)

SpfDelay: 100 0..5000 (1/1000 secs)

HostName: XA1480-1

IpSourceAddress: 1.1.161.161

IpTunnelSourceAddress: 15.15.15.161 (A.B.C.D)

IpTunnelVrf:

MgmtIpAddr: 0.0.0.0 (A.B.C.D)

FanMember: No

DynamicallyLearnedArea:

☑ TcpAdjustMssEnable

TcpAdjustMssStatus: active

TcpAdjustMssType: autoDerived

TcpAdjustMssValue: 1250 0..1250 (0 | 500..1250)

Copyright © 2010-2020 Extreme Networks. All rights reserved. Revision number(Wed Nov 11 18:24:35 EET 2020): 3

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-16741	VSP 4450GSX-PWR+ rebooting multiple times/day with core file and no backtrace
VOSS-16746	VSP 4450GSX-PWR+ rebooting with core file
VOSS-17947	Host connectivity issues when ECMP limit exceeded
VOSS-17973	Switch rebooted with the following ERROR: Assertion failed sync.c:655
VOSS-18673	Node may crash in "smltSlave"
VOSS-18696	XA - Default route not in action even though default route learned from adjacent switch via FE Tunnel
VOSS-18724	Switch crashed with SmtpTask backtrace when a DNS response came in corrupted, with a different name than the one interogated
VOSS-18731	Low throughput between XA1400s from remote location going over NAT to the head end location.

Problems Resolved in This Release	
VOSS-18760	SSH connectivity loss when a logical interface is configured
VOSS-18811	CLIP IP of DVR leaf no longer reachable after reboot
VOSS-18816	OSPF logs writing ipa, nbr-rtid backward Right -> left for VSP7400 and XA platforms
VOSS-18862	DHCPv6 relay setting “ipv6 nd other-config-flag” is not passing config to DHCP client
VOSS-18870	User account not retained after save/reboot
VOSS-18871	Disabling of ro and rw accounts not retained across reboots
VOSS-18872	"SW WARNING Total ECMP group limit reached: 1024" message appearing in the logs
VOSS-18921	EDM SPBM>Interfaces SPBM Displays All ISIS Interfaces Above Line 50 With First Logical Interface Index
VOSS-18946	IPMC error: The maximum number of Egress Records (pepstreams) 7645 has been reached!
VOSS-18948	Switch crashes when EDM is used to create MLT
VOSS-18949	Multicast IP address programmed in the datapath but missing on CP
VOSS-18962	V3 user/group configuration does not create vrf512 entry.
VOSS-19002	Communication to IP addresses lost when both SMLT links are UP
VOSS-19032	cli command "ip ospf apply redistribute" without DVR on the end breaks redistribution of DVR host-entries into OSPF
VOSS-19035	Crashed with core dump when connected console and before providing the credentials
VOSS-19055	Source IP address accepted even the IP address is not presented in config
VOSS-19077	Switch rebooted when restarting BGP
VOSS-19120	BGP routes are not installed into routing table when same routes are not advertised by IGP anymore
VOSS-19140	BFD configuration accepted but not shown in config
VOSS-19152	Reachability issues for clients on the DVR leaves when the DVR host moves rapidly on the same Leaf node
VOSS-19200	EDM edit port shows nothing when 8418XSQ modules installed in slots 2 and 3 (slots 1 and 4 are empty)
VOSS-19248	Can’t create a static route with next hop leaked from ISIS in GRT.
VOSS-18819, VOSS-19300	XA 1400: ICMP unreachable causing issue in default route, tunnels down
VOSS-19350	Not able to add new NSSA under new VRFs after having 24 areas

Fixes from Previous Releases
VOSS 8.1.8.0 incorporates all fixes from prior releases, up to and including VOSS 7.1.7.0 and VOSS 8.0.9.0.

OUTSTANDING ISSUES:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.1.5 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Issues.

KNOWN LIMITATIONS:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.1.5 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Limitations.

Regular cleanup of unneeded files on USB drives is recommended to minimize possibility of USB corruption when a system is reset, shut down, or power is lost.

DOCUMENTATION CORRECTIONS:

For other known issues, please refer to the product release notes and technical documentation available at: https://www.extremenetworks.com/support/documentation.

GLOBAL SUPPORT

By Phone: +1 800-998-2408 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
www.extremenetworks.com/support/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
6480 Via Del Oro
San Jose, CA 95119

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Extreme Networks Support website.

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries. All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see:

www.extremenetworks.com/company/legal/trademarks