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

Customer Release Notes

VSP Operating System Software

Software Release 8.2.7.0
February, 2021

INTRODUCTION:

This document provides specific information for version 8.2.7.0 of agent software for the VSP Operating System Software.

The purpose of this version is to address customer and internally found software issues. This release also includes a couple of minor feature enhancements as indicated in the New in this Release section of this document.

Newly Purchased Switches Require Software Upgrade. You should promptly upgrade the VOSS software to the latest version available by visiting the Extreme Portal.

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 **XA1400** platforms, in order to improve the throughput of a FE tunnel over WAN circuit, the following enhancements were added: **IPSec compression**, **TCP adjust-mss, configurable ISIS Hello Padding and IPSec fragment-before-encrypt.**

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 8.2.7.0 FROM PREVIOUS RELEASE:

For DVR deployments refer also to Outstanding Issues Section before upgrading.

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 8.2.7.0, 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 VSP 4900-12MXU-12XE
- Virtual Services Platform VSP 4900-24S
- Virtual Services Platform VSP 4900-24XE

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 Platform 1440
- ExtremeAccess Platform 1480

Extreme Switching 5520 Series
- 5520-24T
- 5520-24W
- 5520-48T
- 5520-48W
- 5520-12MW-36W
- 5520-24X
- 5520-48SE

SPECIAL INSTRUCTIONS FOR UPGRADING FROM PREVIOUS RELEASES:

I. 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
```

II. 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.

III. 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.

IV. 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.

V. 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.

VI. 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.

VII. 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 8.2.5 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)
VOSS4400.8.2.7.0.sha512	SHA512 Checksums	1395
VOSS4400.8.2.7.0.md5	MD5 Checksums	476
VOSS4400.8.2.7.0.tgz	Release 8.2.7.0 archived software distribution	112257549
VOSS4400.8.2.7.0_mib.zip	Archive of all MIB files	1173409
VOSS4400.8.2.7.0_mib.txt	MIB file	7797260
VOSS4400.8.2.7.0_mib_sup.txt	MIB file	1413418
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 4900 Series

File Name	Module or File Type	File Size (bytes)
VOSS4900.8.2.7.0.sha512	SHA512 Checksums	532
VOSS4900.8.2.7.0.md5	MD5 Checksums	1547
VOSS4900.8.2.7.0.tgz	Release 8.2.7.0 archived software distribution	244709557
VOSS4900.8.2.7.0_mib.zip	Archive of all MIB files	1173409
VOSS4900.8.2.7.0_mib.txt	MIB file	7797260
VOSS4900.8.2.7.0_mib_sup.txt	MIB file	1436064
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827

File Name	Module or File Type	File Size (bytes)
restconf_yang.tgz	YANG model	506020
TPVM_7400_8.2.7.0.img	Third Party Virtual Machine (TPVM)	1677066240

Virtual Services Platform 7200 Series

File Name	Module or File Type	File Size (bytes)
VOSS7200.8.2.7.0.sha512	SHA512 Checksums	1395
VOSS7200.8.2.7.0.md5	MD5 Checksums	476
VOSS7200.8.2.7.0.tgz	Release 8.2.7.0 archived software distribution	126645329
VOSS7200.8.2.7.0_mib.zip	Archive of all MIB files	1173409
VOSS7200.8.2.7.0_mib.txt	MIB file	7797260
VOSS7200.8.2.7.0_mib_sup.txt	MIB file	1379657
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 7400 Series

File Name	Module or File Type	File Size (bytes)
VOSS7400.8.2.7.0.sha512	SHA512 Checksums	1703
VOSS7400.8.2.7.0.md5	MD5 Checksums	592
VOSS7400.8.2.7.0.tgz	Release 8.2.7.0 archived software distribution	244359326
VOSS7400.8.2.7.0_mib.zip	Archive of all MIB files	1173409
VOSS7400.8.2.7.0_mib.txt	MIB file	7797260
VOSS7400.8.2.7.0_mib_sup.txt	MIB file	1430261
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827
restconf_yang.tgz	YANG model	506020
TPVM_7400_8.2.7.0.img	Third Party Virtual Machine (TPVM)	1677066240
FIGWVM_7400_8.2.7.0.qcow2	Fabric Ipsec Gateway Virtual Machine	1970339840

Virtual Services Platform 8200 Series

File Name	Module or File Type	File Size (bytes)
VOSS8200.8.2.7.0.sha512	SHA512 Checksums	1395
VOSS8200.8.2.7.0.md5	MD5 Checksums	476
VOSS8200.8.2.7.0.tgz	Release 8.2.7.0 archived software distribution	126644966
VOSS8200.8.2.7.0_mib.zip	Archive of all MIB files	1173409
VOSS8200.8.2.7.0_mib.txt	MIB file	7797260
VOSS8200.8.2.7.0_mib_sup.txt	MIB file	1379657
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827
restconf_yang.tgz	YANG model	506020

Virtual Services Platform 8400 Series

File Name	Module or File Type	File Size (bytes)
VOSS8400.8.2.7.0.sha512	SHA512 Checksums	1395
VOSS8400.8.2.7.0.md5	MD5 Checksums	476
VOSS8400.8.2.7.0.tgz	Release 8.2.7.0 archived software distribution	188151657
VOSS8400.8.2.7.0_mib.zip	Archive of all MIB files	1173409
VOSS8400.8.2.7.0_mib.txt	MIB file	7797260
VOSS8400.8.2.7.0_mib_sup.txt	MIB file	1379657
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827
restconf_yang.tgz	YANG model	506020

ExtremeAccess 1400 Series

File Name	Module or File Type	File Size (bytes)
VOSS1400.8.2.7.0.sha512	SHA512 Checksums	1247
VOSS1400.8.2.7.0.md5	MD5 Checksums	424
VOSS1400.8.2.7.0.tgz	Release 8.2.7.0 archived software distribution	322405938
VOSS1400.8.2.7.0_mib.zip	Archive of all MIB files	1173409
VOSS1400.8.2.7.0_mib.txt	MIB file	7797260
VOSS1400.8.2.7.0_mib_sup.txt	MIB file	1087469
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827

Extreme Switching 5520 Series

File Name	Module or File Type	File Size (bytes)
5520.8.2.7.0.sha512	SHA512 Checksums	1974
5520.8.2.7.0.md5	MD5 Checksums	671
5520.8.2.7.0.voss	Release 8.2.7.0 archived software distribution	99133886
5520.8.2.7.0_mib.zip	Archive of all MIB files	1173409
5520.8.2.7.0_mib.txt	MIB file	7797260
5520.8.2.7.0_mib_sup.txt	MIB file	1435650
VOSSv820_HELP_EDM_gzip.zip	EDM Help file	4414827
restconf_yang.tgz	YANG model	506020

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 VOSS4400.8.2.7.0.tgz
software activate 8.2.7.0.GA
```

or

```
software add VOSS4900.8.2.7.0.tgz
software activate 8.2.7.0.GA
```

or

```
software add VOSS7200.8.2.7.0.tgz
software activate 8.2.7.0.GA
```

or

```
software add VOSS7400.8.2.7.0.tgz
software activate 8.2.7.0.GA
```

or

```
software add VOSS8200.8.2.7.0.tgz
software activate 8.2.7.0.GA
```

or

```
software add VOSS8400.8.2.7.0.tgz
software activate 8.2.7.0.GA
```

or

```
software add VOSS1400.8.2.7.0.tgz
software activate 8.2.7.0.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
Added support for the Optic 10063 on VSP520-48SE (VOSS-19530)

For **XA1400** platforms, in order to improve the throughput of a FE tunnel over WAN circuit, the following enhancements were added: **IPSec compression**, **TCP adjust-mss, configurable ISIS Hello Padding and IPSec fragment-before-encrypt**

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 IPSec compression **must** be used only for tunnels where latency is greater than 70ms; for tunnels with smaller latency values it can have a negative impact on the throughput.

Note: Before using a release without support for this enhancement, follow the next sequence:

- Default the IPSec compression on all logical interfaces:
  - `XA1480:1(config)#logical-intf isis 1`
  - `XA1480:1(config-isis-1-1.1.1.1)#no ipsec`
  - `XA1480:1(config-isis-1-1.1.1.1)#no ipsec compression`
  - `XA1480:1(config-isis-1-1.1.1.1)#ipsec`
  - `XA1480:1(config-isis-1-1.1.1.1)#exit`
  - `XA1480:1(config)#`
- Save config
- Load new image

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

XA1480-1:1(config-isis-2-15.15.15.151)#
```

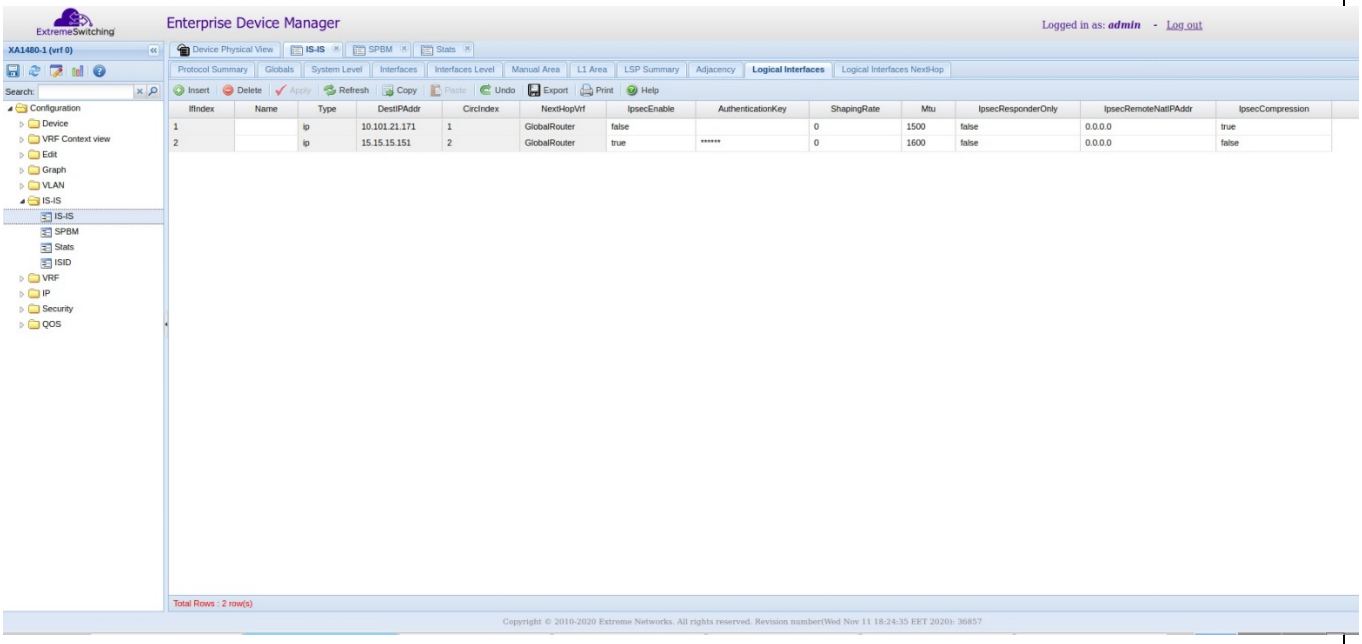
```
XA1480-1:1(config-if)#show isis logical-interface ipsec
********************************************************************************
               Command Execution Time: Fri Dec 04 14:00:45 2020 UTC
********************************************************************************

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

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:



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 will be auto derived based of the tunnel MTUs or can be manual configured by the user.
    - The MSS auto-derived value 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 user configures 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-derived 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 one 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 is a tunnel with MTU <= 1500 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.

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.
- Before using a release without support for this enhancement, follow the next sequence:
    - Default the TCP mss:
        - `XA1480-1:1(config)#router isis`
        - `XA1480-1:1(config-isis)#ip tcp adjust-mss`
        - `XA1480-1:1(config-isis)#`
        - `XA1480-1:1(config-isis)#no ip tcp adjust-mss mss`
        - `XA1480-1:1(config-isis)#`
    - Save config
    - Load new image

CLI commands

Mode: router isis configuration
ip tcp adjust-mss [mss <500-1250>]

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

no ip tcp adjust-mss [mss]
```
      XA1480-1:1(config)#router isis
```
Disable tcp adjust-mss:
```
      XA1480-1:1(config-isis)#no ip tcp adjust-mss
```
Set the mss value to default (auto derived based on te logical interfaces MTU)
```
      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
----------------------------------------------------------------------------------------------------------------
```

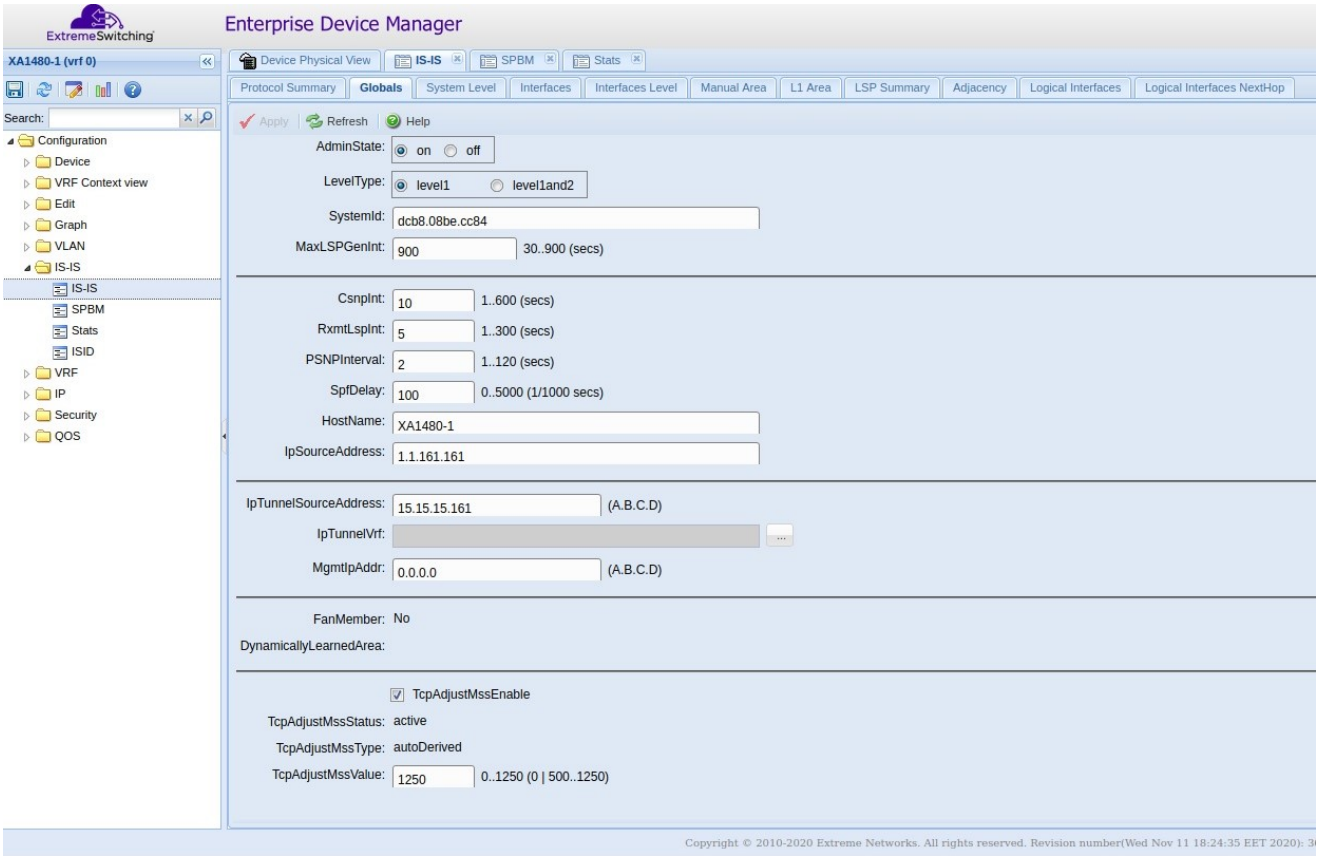
```
XA1480-1:1(config)#show isis tcp adjust-mss
********************************************************************************
               Command Execution Time: Fri Dec 04 15:29:54 2020 UTC
********************************************************************************

================================================================================
                              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


ExtremeSwitching
Enterprise Device Manager
XA1480-1 (vrf 0)
Device Physical View
IS-IS
SPBM
Stats
Protocol Summary
Globals
System Level
Interfaces
Interfaces Level
Manual Area
L1 Area
LSP Summary
Adjacency
Logical Interfaces
Logical Interfaces NextHop
Search:
Configuration
Device
VRF Context view
Edit
Graph
VLAN
IS-IS
IS-IS
SPBM
Stats
ISID
VRF
IP
Security
QOS
Apply
Refresh
Help
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):

ISIS Hello Padding

ISIS pads the Hello packets to the full interface Maximum Transmission Unit (MTU), in order to detect MTU mismatches. For FE NNI links, all hello packets are padded and on non-FE pt-to-pt NNI links the hello packets are padded, till a hello packet is received from the other side.

This release includes a mechanism (CLI Only) to disable the hello padding, to avoid hello packets fragmentation.

- The default state is hello padding enabled (therefore, no change after upgrade).
- After disabling padding, the config can be saved to a file. ***Note***, the new config file cannot be used in prior release. In order to downgrade, disable or use default keyword to enable padding and save config file.
- The config command to enable/disable padding is a global flag that will take affect on all ISIS NNI links. This flag can be used dynamically, that is, does not require disabling ISIS or any NNI link.

CLI Commands

show mode:

```
6001:1#show isis
********************************************************************************
            Command Execution Time: Thu Jan 28 22:11:29 2021 UTC
********************************************************************************

================================================================================================================
                                ISIS General Info
================================================================================================================
                           AdminState : enabled
                           RouterType : Level 1
                            System ID : 0001.0001.6001
                Max LSP Gen Interval : 900
                              Metric : wide
                 Overload-on-startup : 20
                            Overload : false
                       Csnp Interval : 10
                       PSNP Interval : 2
                  Rxmt LSP Interval : 5
                           spf-delay : 100
                         Router Name : 6001
                  ip source-address :
                ipv6 source-address :
            ip tunnel source-address :
                           Tunnel vrf :
                       ip tunnel mtu :
                  Num of Interfaces : 2
               Num of Area Addresses : 1
                 Inband Mgmt Clip Ip :
                            backbone : disabled
            Dynamically Learned Area :
                           FAN Member : No
                       Hello Padding : enabled
```

Config mode:

```
6001:1#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
6001:1(config)#router isis
6001:1(config-isis)#no hello-padding
6001:1(config-isis)#show isis
********************************************************************************
            Command Execution Time: Thu Jan 28 22:02:10 2021 UTC
********************************************************************************

================================================================================================================
```

```
                              ISIS General Info
================================================================================================================
                         AdminState : enabled
                         RouterType : Level 1
                          System ID : 0001.0001.6001
                Max LSP Gen Interval : 900
                             Metric : wide
                 Overload-on-startup : 20
                            Overload : false
                       Csnp Interval : 10
                       PSNP Interval : 2
                  Rxmt LSP Interval : 5
                          spf-delay : 100
                        Router Name : 6001
                  ip source-address :
                ipv6 source-address :
             ip tunnel source-address :
                         Tunnel vrf :
                      ip tunnel mtu :
                 Num of Interfaces : 2
              Num of Area Addresses : 1
                Inband Mgmt Clip Ip :
                           backbone : disabled
             Dynamically Learned Area :
                         FAN Member : No
                     Hello Padding : disabled
```

To restore default behavior, use

```
6001:1(config-isis)#default hello-padding
```

or

```
6001:1(config-isis)#no hello-padding
```

Config File: When padding is disabled or in the verbose mode, “show running-config” will show the padding option

```
#
# ISIS CONFIGURATION
#

router isis
sys-name "6001"
no backbone enable
no hello-padding
is-type l1
system-id 0001.0001.6001

manual-area 49.0000
exit
router isis enable
```

IPSec fragment-before-encrypt

When IPSec over FE adjacency is used, this enhancement allows to fragment the packets, based on the tunnel MTU, before they are encrypted and IPSec encapsulated.

The IPSec fragment-before-encrypt is an option per logical interface and its default state is **disabled.** In the default (disabled) state, the packets are first encrypted & IPSec encapsulated and after that fragmented. The fragmentation is applied only if final packet (including IPSec header) is bigger than the tunnel's MTU. So, when there is a tunnel with fragment before encryption disabled, the packets egressing the specific NNI port will be ESP and fragmented IP packets (both packets are encrypted but they will have different headers).

When the IPSec fragment-before-encrypt is enabled on logical interface, the fragmentation of the packets will happen before encryption and IPSec encapsulation. In this case the packets will be fragmented base on the tunnel MTU minus the IPSec header, so that the final packet to not exceed the tunnel's MTU. For this tunnel the packets egressing the specific NNI port will be only ESP packets.

The IPSec fragment-before-encrypt can be enabled only if IPSec over FE is into IPSec decoupled mode (IPSec source and destination IPs are different than the FE ones). So, prior to enable IPSec fragment-before-encrypt on logical interface the next configurations need to be made:

- IPSec tunnel source address needs to be configured globally (under *router isis*)
- Per logical interface: (under *logical-interface isis*)
    - IPSec need to be disabled
    - IPSec tunnel-destination-IP or IPSec remote-nat-ip or IPSec responder-only need to be configured

CLI commands:

Enable/Disable IPSec Fragment-before-encrypt:

```
Mode: isis logical interface configuration

      [no] ipsec fragment-before-encrypt
```

To display IPSec fragment-before-encrypt:

```
Mode: global

      show isis logical-interface ipsec
```

```
XA1480:1(config-isis-2-192.168.20.1)#ipsec ?
 compression               Enable IPSec compression on this logical interface
 encryption-key-length     Set IPSec encryption key length
 fragment-before-encrypt   Enable IPSec fragment before encrypt on this
                           logical interface

 remote-nat-ip             IPSec remote NAT IP address. This needs to be
                           configured in IPSec initiator logical interface
                           when there is NAT on both side the of the IPSec
                           tunnel.
```

```
 responder-only              Indicates if IPSec session of this logical
                             interface should be in responder only mode.
                             Whenever it is configured this logical interface
                             will not initiate the IPSec connection but only
                             respond to the incoming connection. By default both
                             the sides of IPSec connection will be initiators.
                             When there is NAT in between the IPSec connection,
                             configure this on the IPSec responder logical
                             interface.
 tunnel-dest-ip              Specify IPSec Tunnel Dest IP address
 <cr>


XA1480:1(config-isis-2-192.168.20.1)#ipsec fragment-before-encrypt
XA1480:1(config-isis-2-192.168.20.1)#ipsec

XA1480:1(config-isis-2-192.168.20.1)#sho isis logical-interface ipsec
********************************************************************************
               Command Execution Time: Fri Jun 04 21:02:20 2021 UTC
********************************************************************************

================================================================================================================
                                    ISIS Logical Interface IPSec
================================================================================================================
ID       Auth-Key   Responder-Only   Remote NAT IP        Auth-Key-Len Compression Frag-before-encrypt
----------------------------------------------------------------------------------------------------------------
2        ******     False            -                    128          False       True

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

================================================================================================================
                            IPSec Tunnel General Info
================================================================================================================
       IPSec tunnel source-ip-address : 10.3.1.55

================================================================================================================
                                ISIS IPSec Tunnels
================================================================================================================

ID     IPSec Dst Ip        TUNNEL_NEXT_HOP
                           PORT/MLT   VLAN      VRF
----------------------------------------------------------------------------------------------------------------
2      10.101.21.141       Port1/8    450       GlobalRouter
----------------------------------------------------------------------------------------------------------------

 1 out of 1 Total Num of Logical ISIS interfaces
```

```
XA1480:1(config-isis-2-192.168.20.1)#no ipsec
XA1480:1(config-isis-2-192.168.20.1)#no ipsec fragment-before-encrypt
XA1480:1(config-isis-2-192.168.20.1)#ipsec

XA1480:1(config-isis-2-192.168.20.1)#show isis logical-interface ipsec
********************************************************************************
               Command Execution Time: Fri Jun 04 22:25:50 2021 UTC
********************************************************************************

================================================================================================================
                                    ISIS Logical Interface IPSec
================================================================================================================
ID       Auth-Key   Responder-Only   Remote NAT IP        Auth-Key-Len Compression Frag-before-encrypt
```

```
-------------------------------------------------------------------------------------------------------------
2        ******     False           -                   128          False       False

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

=============================================================================================================
                          IPSec Tunnel General Info
=============================================================================================================
       IPSec tunnel source-ip-address : 10.3.1.55

=============================================================================================================
                             ISIS IPSec Tunnels
=============================================================================================================

ID     IPSec Dst Ip        TUNNEL_NEXT_HOP
                           PORT/MLT   VLAN      VRF
-------------------------------------------------------------------------------------------------------------
2      10.101.21.141       Port1/8    450       GlobalRouter
-------------------------------------------------------------------------------------------------------------
 1 out of 1 Total Num of Logical ISIS interfaces
-------------------------------------------------------------------------------------------------------------
```

CLI consistency check and corresponding error messages

In the following scenarios error messages will be displayed:

- Try to enable IPSec fragment-before-encrypt when IPSec is enabled on logical interface

  ```
  Error: IPSec is enabled on logical interface, please disable IPSec before configuring ipsec fragment-before-encrypt
  ```

- Try to enable IPSec fragment-before-encrypt when IPSec tunnel source address is not configured globally

  ```
  Error: You need to configure ipsec tunnel-source-address before modifying fragment-before-encrypt
  ```

- Try to enable IPSec fragment-before-encrypt when no IPSec tunnel destination IP or IPSec remote nat IP or IPSec responder only is configured on the logical interface

  ```
  Error: You need to have ipsec tunnel-dst-ip or for NAT case ipsecRemoteNatIp or ipsec responder-only configured before modifying fragment-before-encrypt
  ```

- Try to enable IPSec on a logical interface when IPSec fragment before encrypt is enable but no IPSec tunnel destination IP or IPSec remote nat IP or IPSec responder only is configured

  ```
  Error: IPSec fragment-before-encrypt is enabled on logical interface. You need to have ipsec tunnel-dst-ip or ipsecRemoteNatIp or ipsec responder-only configured before enable ipsec
  ```

- Try to remove IPSec tunnel source address from the router isis global configuration when IPSec fragment-before-encrypt is enabled on at least one logical interface

```
    Error: You need to disable fragment-before-encrypt from logical
    interface before removing IPSec tunnel source address
```

Configuration example with a logical interface having fragment-before-encrypt enabled

```
XA1480:1(config)#show running-config module isis
config terminal
#
# ISIS CONFIGURATION
#
router isis
sys-name "XA1440-bfit"
ip-source-address 1.11.3.55
ip-tunnel-source-address 192.168.10.1
ipsec tunnel-source-address 10.3.1.55
is-type l1
manual-area c0.2000.0000.00
exit
#
# LOGICAL ISIS CONFIGURATION
#
logical-intf isis 2 dest-ip 192.168.20.1 mtu 1500
isis
isis spbm 1
isis enable
auth-key ******
ipsec tunnel-dest-ip 10.101.21.141
ipsec fragment-before-encrypt
ipsec
exit
```

Note:

It is recommended to enable IPSec fragment-before-encrypt for the FE + IPSec tunnels over a WAN circuit.

Limitations:

The SNMP & EDM support is not available into this release. In order to configure IPSec fragment-before-encrypt **only the CLI commands** can be used.

Note: Before using a release without support for this enhancement, follow the next sequence:

- Default the IPSec fragment-before-encrypt on all logical interfaces:

```
XA1480:1(config)#logical-intf isis 1
XA1480:1(config-isis-1-1.1.1.1)#no ipsec
XA1480:1(config-isis-1-1.1.1.1)#no ipsec fragment-before-encrypt
XA1480:1(config-isis-1-1.1.1.1)#ipsec
XA1480:1(config-isis-1-1.1.1.1)#exit
XA1480:1(config)#
```

- Save config
- Load new image

Old Features Removed From This Release
None.

Problems Resolved in This Release	
VOSS-19396	VOSS 8.2: EDM connection with IE 11 fails and only show revision number
VOSS-19437	XA1480 DHCP relay fails once Management VLAN is enabled
VOSS-19470	Network traffic large impact after upgrade of few dvr leaf nodes
VOSS-19533	VSP 7432CQ (VOSS 8.2.5) - Channelized port LED not working
VOSS-19714	All interface LEDs don't work after upgrade to 8.2.6.0
VOSS-19791	Node may crash in "smltSlave"
VOSS-19792	IPMC error: The maximum number of Egress Records (pepstreams) 7645 has been reached!
VOSS-19793	Switch rebooted when restarting BGP
VOSS-19794	OSPF logs writing ipa, nbr-rtid backward Right -> left for VSP7400 and XA platforms
VOSS-19759	Slow throughput seen on XA
VOSS-19795	CLI command "ip ospf apply redistribute" without DVR on the end breaks redistribution of DVR host-entries into OSPF
VOSS-19833	Source IP address accepted even the IP address is not presented in config
VOSS-19834	BFD configuration accepted but not shown in config
VOSS-19836	Multicast IP address programmed in the datapath but missing on CP
VOSS-19838	Low throughput between XA1400s from remote location going over NAT to the head end location.
VOSS-19839	Can’t create a static route with next hop leaked from ISIS in GRT
VOSS-19840	SSH connectivity loss when a logical interface is configured
VOSS-19854	A management CLIP IP address that fell in the range of a configured VLAN IP address range had been allowed. This has been corrected.
VOSS-19856	“show mgmt ip arp” command should not have “clip” as a parameter
VOSS-19857	tMainTask running within process SSIO is causing constant 60% CPU churn polling I/O card data
VOSS-20197	LLDP floods on flex-uni untagged port

Fixes from Previous Releases
VOSS 8.2.7.0 incorporates all fixes from prior releases, up to and including VOSS 7.1.7.0, VOSS 8.0.9.0 and VOSS 8.1.8.0.

OUTSTANDING ISSUES:

Please see “Release Notes for VSP Operating System Software (VOSS)” for software release 8.2.5 available at https://www.extremenetworks.com/support/release-notes for details regarding Known Issues.

VOSS-20030	An interaction between DVR host learning and wireless solutions configured with proxy-ARP and bridging at the AP may create instability within the DVR domain due to specific combinations of roaming events and topology factors. This interaction is exposed when a client roams between AP's connected to different BEB's and both AP's momentarily respond for the client IP on both BEB's (host duplication). These interactions can be avoided by using VRRP instead of DVR for wireless segments.
VOSS-20291	XA 1400: FE interface in decoupled mode is failing to come up if IP compression is added along with Frag-before-encrypt flag. Workaround: The IPSec compression cannot be used in the same time with IPsec frag-before-encryption. If you have both enable on the logical interface, disable one of them in order to avoid the issue
VOSS-20258	XA1440: EDM: IP Compression is not editable from EDM Workaround: use CLI to configure

KNOWN LIMITATIONS:

Please see "Release Notes for VSP Operating System Software (VOSS)" for software release 8.2.5 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.

Trademarks