IBM Networking OS 7.5

Release Notes

for the EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch,
Second Edition (replaces 88Y7945)

Note: Before using this information and the product it supports, read the general information in the *Safety information and Environmental Notices* and *User Guide* documents on the IBM *Documentation* CD and the *Warranty Information* document that comes with the product.

Second Edition (November 2012)

P/N: 00D2335

Release Notes

This release supplement provides the latest information regarding IBM Networking OS 7.5 for EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch (collectively referred to as EN4093 throughout this document). Where required, differences between the EN4093 and EN4093R are detailed.

This supplement modifies and extends the following Networking/ OS documentation for use with N/OS 7.5:

- *IBM Networking OS Application Guide for the EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch*
- *IBM Networking OS Command Reference for the EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch*
- *IBM Networking OS ISCLI Reference for the EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch*
- *IBM Networking OS BBI Quick Guide for the EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch*
- *EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch User's Guide*

The publications listed above are available at the following address:

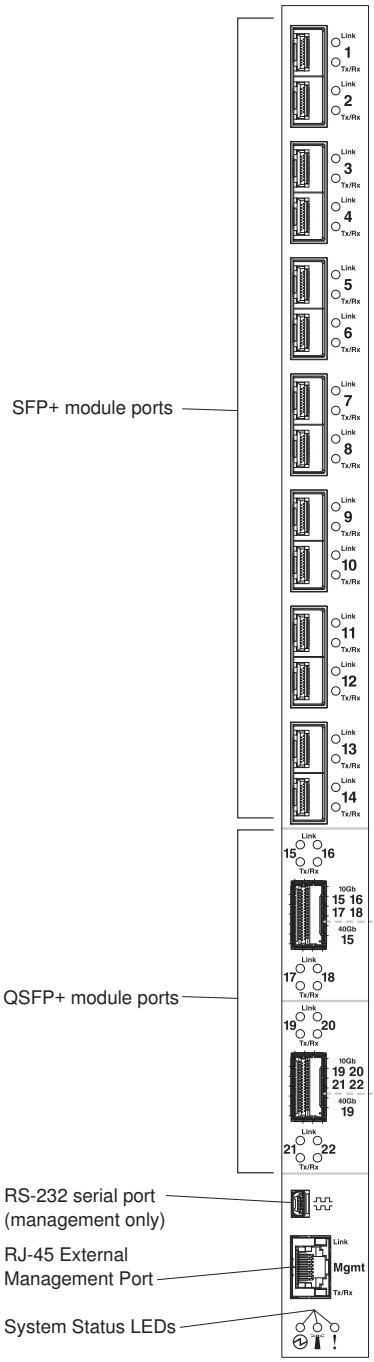
http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp

Please keep these release notes with your product manuals.

Hardware Support

N/OS 7.5 software is supported on the EN4093, shown in Figure 1, is a high performance Layer 2-3 embedded network switch that features tight integration with IBM Flex System chassis management module.

Figure 1. EN4093 10Gb Scalable Switch Faceplate



The EN4093 has the following port capacities:

- Fourteen 10Gb SFP+ ports
- Two 40Gb QSFP+ ports
- Fourty-Two 10Gb internal ports (maximum)
- One 1Gb RJ-45 external management port
- One 1Gb internal management port
- One mini-USB serial port

Transceivers

The following transceivers and DACs are available:

Table 1. EN4093 Transceivers and DACs

Description	Part number
Transceivers	
1000Base-SX SFP (MMFiber) transceiver	81Y1622
1000Base-T SFP transceiver 4	81Y1618
1000Base-LX SFP LX transceiver	90Y9424
10GBase-SR SFP+ (MMFiber) transceiver	44W4408
10GBase-SR SFP+ (MMFiber) transceiver	46C3447
IBM BNT SFP+ LR transceiver	90Y9412
IBM BNT QSFP+ 40Gbase-SR transceiver	49Y7884
Direct Attach Cables (DACs)	
1m IBM Passive DAC SFP+	90Y9427
3m IBM Passive DAC SFP+	90Y9430
5m IBM Passive DAC SFP+	90Y9433
1m 40Gb QSFP+ to 4 x 10Gb SFP+ Breakout Cable	49Y7886
3m 40Gb QSFP+ to 4 x 10Gb SFP+ Breakout Cable	49Y7887
5m 40Gb QSFP+ to 4 x 10Gb SFP+ Breakout Cable	49Y7888
10m IBM MTP Fiber Optical Cable (Requires transceiver 49Y7884)	90Y3519
30m IBM MTP Fiber Optical Cable (Requires transceiver 49Y7884)	90Y3521
1m QSFP+ to QSFP+ DAC	49Y7890
3m QSFP+ to QSFP+ DAC	49Y7891

The switch also supports MSA-compliant copper direct-attach cables (DAC), up to 7 m (23 ft.) in length.

Updating the Switch Software Image

The switch software image is the executable code running on the EN4093. A version of the image comes pre-installed on the device. As new versions of the image are released, you can upgrade the software running on your switch. To get the latest version of software supported for your EN4093, go to the following website:

http://www.ibm.com/systems/support

To determine the software version currently used on the switch, use the following switch command:

```
>> # /info/sys/gen
```

The typical upgrade process for the software image consists of the following steps:

- Load a new software image and boot image onto an FTP or TFTP server on your network.

  Note: Software loading options also include SFTP. Some screen prompts may appear slightly different than depicted in this document.
- Transfer the new images to your switch.
- Specify the new software image as the one which will be loaded into switch memory the next time a switch reset occurs.
- Reset the switch.

For instructions on the typical upgrade process using the menu-based CLI, the ISCLI, or the BBI, see “Loading New Software to Your Switch” on page 6.

ATTENTION: Although the typical upgrade process is all that is necessary in most cases, upgrading from (or reverting to) some versions of N/OS requires special steps prior to or after the software installation process. Please be sure to follow all applicable instructions in the following sections to ensure that your switch continues to operate as expected after installing new software.

Loading New Software to Your Switch

The EN4093 can store up to two different switch software images (called `image1` and `image2`) as well as special boot software (called `boot`). When you load new software, you must specify where it should be placed: either into `image1`, `image2`, or `boot`.

For example, if your active image is currently loaded into `image1`, you would probably load the new image software into `image2`. This lets you test the new software and reload the original active image (stored in `image1`), if needed.

ATTENTION: When you upgrade the switch software image, always load the new boot image and the new software image before you reset the switch. If you do not load a new boot image, your switch might not boot properly (To recover, see “Recovering from a Failed Software Upgrade” on page 39).

To load a new software image to your switch, you will need the following:

- The image and boot software loaded on an FTP or TFTP server on your network.

  Note: Be sure to download both the new boot file and the new image file.
- The hostname or IP address of the FTP or TFTP server

  Note: The DNS parameters must be configured if specifying hostnames.
- The name of the new software image or boot file

When the software requirements are met, use one of the following procedures to download the new software to your switch. You can use the N/OS CLI, the ISCLI, or the BBI to download and activate new software.

Loading Software via the N/OS CLI

1. Enter the following Boot Options command:

   ```
   >> # /boot/gtimg
   ```

2. Enter the name of the switch software to be replaced:

   ```
   Enter name of switch software image to be replaced
    ["image1"/"image2"/"boot"]: <image>
   ```

3. Enter the hostname or IP address of the FTP or TFTP server.

   ```
   Enter hostname or IP address of FTP/TFTP server: <hostname or IP address>
   ```

4. Enter the name of the new software file on the server.

   ```
   Enter name of file on FTP/TFTP server: <filename>
   ```

   The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (usually `/tftpboot`).

5. Enter your username for the server, if applicable.

   ```
   Enter username for FTP server or hit return for
   TFTP server: {<username> /<Enter>}
   ```

   If entering an FTP server username, you will also be prompted for the password. The system then prompts you to confirm your request. Once confirmed, the software will load into the switch.

6. If software is loaded into a different image than the one most recently booted, the system will prompt you whether you wish to run the new image at next boot. Otherwise, you can enter the following command at the `Boot Options#` prompt:

   ```
   Boot Options# image
   ```

   The system then informs you of which software image (`image1` or `image2`) is currently set to be loaded at the next reset, and prompts you to enter a new choice:

   ```
   Currently set to use switch software "image1" on next reset.
   Specify new image to use on next reset ["image1"/"image2"]:
   ```

   Specify the image that contains the newly loaded software.

7. Reboot the switch to run the new software:

```
Boot Options# reset
```

   The system prompts you to confirm your request. Once confirmed, the switch will reboot to use the new software.

Loading Software via the ISCLI

1. In Privileged EXEC mode, enter the following command:

```
Router# copy {tftp|ftp} {image1|image2|boot-image}
```

2. Enter the hostname or IP address of the FTP or TFTP server.

```
Address or name of remote host: <name or IP address>
```

3. Enter the name of the new software file on the server.

```
Source file name: <filename>
```

   The exact form of the name will vary by server. However, the file location is normally relative to the FTP or TFTP directory (for example, `tftpboot`).

4. If required by the FTP or TFTP server, enter the appropriate username and password.
5. The switch will prompt you to confirm your request.

   Once confirmed, the software will begin loading into the switch.

6. When loading is complete, use the following commands to enter Global Configuration mode to select which software image (`image1` or `image2`) you want to run in switch memory for the next reboot:

```
Router# configure terminal
Router(config)# boot image {image1|image2}
```

   The system will then verify which image is set to be loaded at the next reset:

```
Next boot will use switch software image1 instead of image2.
```

7. Reboot the switch to run the new software:

```
Router(config)# reload
```

   The system prompts you to confirm your request. Once confirmed, the switch will reboot to use the new software.

Loading Software via BBI

You can use the Browser-Based Interface to load software onto the EN4093. The software image to load can reside in one of the following locations:

- FTP server
- TFTP server
- Local computer

After you log onto the BBI, perform the following steps to load a software image:

1. Click the Configure context tab in the toolbar.
2. In the Navigation Window, select System > Config/Image Control.

   The Switch Image and Configuration Management page appears.
3. If you are loading software from your computer (HTTP client), skip this step and go to the next. Otherwise, if you are loading software from a FTP/TFTP server, enter the server's information in the FTP/TFTP Settings section.
4. In the Image Settings section, select the image version you want to replace (Image for Transfer).
   - If you are loading software from a FTP/TFTP server, enter the file name and click **Get Image**.
   - If you are loading software from your computer, click **Browse**.

     In the File Upload Dialog, select the file and click **OK**. Then click **Download via Browser**.

   Once the image has loaded, the page refreshes to show the new software.

New and Updated Features

N/OS 7.5 for EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch (EN4093) has been updated to include several new features, summarized in the following sections. For more detailed information about configuring EN4093 features and capabilities, refer to the complete N/OS 7.5 documentation as listed on page 3.

CEE/FCoE/VNICs

Note: CEE/FCoE/VNIC stacking mode is applicable only to EN4093R.

CEE and FCoE are supported in stand-alone and stacking mode. FCoE and VNIC can be configured in stacking mode.

CEE/FCoE/Stacking

Note: CEE/FCoE/Stacking mode is applicable only to EN4093R.

CEE and FCoE are supported in stand-alone and stacking mode.

CPU Packet Logging

Note: This feature is new only to the EN4093R. This feature was introduced on EN4093 in a previous release.

Additional information can be viewed in the CPU packet logs. This includes:

- Information that helps to distinguish IPv4 packet types.
- Information about packets sent from CPU.
- Packet logs that can be viewed based on parameters such as ingress ports, VLANs, and others.
- Information that helps to trace packets being received by CPU.
- Rate at which packets are received by CPU.

CPU Usage Statistics

Note: This feature is new only to the EN4093R. This feature was introduced on EN4093 in a previous release.

You can view CPU utilization statistics for each module running on the system using the >>Main# stats/mp/ncpu command. The output includes system-wide CPU utilization information, and a per-thread CPU utilization information for the last 1, 5, 60, and 300 seconds. Following is a sample output of the command:

```
>> Main# stats/mp/ncpu
------------------------------------------------------------------------
Total CPU Utilization: For 1 second: 5.64%
                       For 5 second: 6.12%
                       For 1 minute: 6.00%
                       For 5 minute: 3.20%
------------------------------------------------------------------------
Thread  Thread                    Utilization                   Status
  ID     Name        1sec       5sec       1Min       5Min
------------------------------------------------------------------------
1     STEM       0.00%      0.00%      0.00%      0.00%       idle
2     STP        0.15%      0.11%      0.13%      0.12%       idle
3     MFDB       0.00%      0.00%      0.00%      0.00%       idle
4     TND        0.00%      0.00%      0.00%      0.00%       idle
5     CONS       0.01%      0.09%      0.01%      0.00%    running
```

Following is a sample output of the command to view thread statistics:

```
>> Main# stats/mp/nthr
STEM thread stats:
-------------------------------------------------------------------------------
----------
Thread Thread      Stack       Total   Invoked    Max    Messages Queue   Status
  ID   Name   Used  /  Max Runtime(us) Count Runtime(us)in Queue  Hwat
-------------------------------------------------------------------------------
   1   STEM                        0      0         0      0              idle
   2   STP    3884   32748      136979    378      6135      0       5      idle
   3   MFDB    524    8172      111700    439      2324      0      13      idle
   4   TND                        940     32       182      0              idle
   5   CONS  11692   40940       15245   1222      6284      0       1   running
```

Diagnostics Enhancement

The following commands have been added to improve the ability to diagnose system issues:

- EN 4093(config)# **show logging** [**messages**] [**severity** *<0-7>*] [**reverse**] | [**head**|**last**] *<line number>*
- EN 4093(config)# **show environment power**
- EN 4093(config)# **show environment fan**
- EN 4093# **show version** [**brief**]
- EN 4093# **show tech-support** [**l2|l3|link|port**]
- EN 4093# **system idle** *<0-60>*
- EN 4093(config)# **logging synchronous** [**level** *<severity-level>***|all**]
- EN 4093# **show who**
- EN 4093(config)# **access user clear** *<session ID>*
- EN 4093# **show line**
- EN 4093# **clear line** *<session ID>*

- `EN 4093# [no]` **`debug lacp packet`**
- `EN 4093# [no]` **`debug spanning-tree bpdu`** [**`receive`**|**`transmit`**]

For detailed description of these commands, see the *IBM Networking OS 7.5 Command Reference* and *IBM Networking OS 7.5 ISCLI Reference Guides*.

Note: Use the debug commands with caution as they can disrupt the operation of the switch under high load conditions.

Edge Virtual Bridging (EVB)

- EVB can be configured using ISCLI, IBM N/OS CLI, and Browser-based Interface (BBI).
- EVB can be configured in stand-alone and stacking mode.

EVB and FCoE

Note: This section is applicable only to EN4093R.

In stand-alone mode, EVB and FCoE can be configured on the same switch port.

Link Aggregation Group (LAG) Enhancement

Link Aggregation is used for grouping several physical ports into one logical port with any device that supports the standard.

You can now add up to 32 ports to a static trunk or dynamic trunk.

For dynamic trunks that require a guaranteed amount of bandwidth in order to be considered useful, you can specify the minimum number of links for the trunk. You can now configure the minimum link requirement to be 16 ports.

LLDP

LLDP transmissions can be configured to enable or disable inclusion of the following optional information:

Table 2. LLDP Optional Information Types

Type	Description	Default
portdesc	Port Description	Enabled
sysname	System Name	Enabled
sysdescr	System Description	Enabled
syscap	System Capabilities	Enabled
mgmtaddr	Management Address	Enabled
portvid	IEEE 802.1 Port VLAN ID	Disabled
portprot	IEEE 802.1 Port and Protocol VLAN ID	Disabled
vlanname	IEEE 802.1 VLAN Name	Disabled
protid	IEEE 802.1 Protocol Identity	Disabled
macphy	IEEE 802.3 MAC/PHY Configuration/Status, including the auto-negotiation, duplex, and speed status of the port.	Disabled
powermdi	IEEE 802.3 Power via MDI, indicating the capabilities and status of devices that require or provide power over twisted-pair copper links.	Disabled
linkaggr	IEEE 802.3 Link Aggregation status for the port.	Disabled
framesz	IEEE 802.3 Maximum Frame Size for the port.	Disabled
dcbx	Data Center Bridging Capability Exchange Protocol (DCBX) for the port.	Enabled

MSTP

Multiple Spanning Tree Protocol (MSTP) is supported in stacking and stand-alone mode.

OSPFv3 Over IPsec

BBI and SNMP support for OSPFv3 over IPsec has been added.

Persistent Terminal Length

The screen length for the current session can be set using the command: `>>Main# lines` *<0-300>*.

However, when the switch is reloaded, the screen length is set to default.

To set the screen length to be persistent across multiple sessions, use the following commands:

Telnet and SSH:

```
>>Main# /cfg/sys/linevty <0-300>
```

Console:

```
>>Main# /cfg/sys/linecons <0-300>
```

The commands to set a persistent screen length are saved in the startup configuration and will be applied even when the switch is reloaded. If you need to change the screen length for a particular session, you can do so using the command for setting the current session's screen length.

Precision Time Protocol

As defined in the IEEE 1588-2008 standard, Precision Time Protocol (PTP) is a precision clock synchronization protocol for networked measurement and control systems. PTP provides system-wide synchronization accuracy and precision in the sub-microsecond range with minimal network and local clock computing resources. The synchronization is achieved through the exchange of messages: General messages that carry data but need not be time stamped; Event messages that are time stamped and are critical for clock synchronization accuracy.

A PTP network consists of PTP-enabled devices such as switches or routers. These devices consist of the following types of clocks:

- Master clock: In a PTP domain, the clock with the most precise time is considered the master clock. A best master clock algorithm determines the highest quality clock in a network.
- Ordinary clock: An ordinary clock synchronizes its time with the Master clock. The ordinary clock has a bidirectional communication with the master clock. By receiving synchronization/delay response and sending delay request packets, the ordinary clock adjusts its time with the master clock.
- Boundary clock: A boundary clock connects to multiple networks. It synchronizes with the attached master clock and in turn acts as a master clock to all attached ordinary clocks. Boundary clocks help to reduce the effect of jitter in Ethernet-based networks.
- Transparent clock: A transparent clock listens for PTP packets and adjusts the correction field in the PTP event packets as they pass the PTP device.

EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch supports the configuration of ordinary clock and transparent clock. It cannot be a master clock as the switch does not participate in the master clock selection process.

Note: IBM Networking OS does not support IPv6 for PTP.

By default, PTP version 2 is installed on the switch but is globally disabled. Use the following command to globally enable PTP:

```
EN 4093(config)# ptp {ordinary|transparent} enable
```

PTP is configured on switch ports. In case of trunk ports, the PTP configuration must be the same on all ports participating in the same trunk. The switch uses only one port from a trunk (typically the one used by a multicast protocol) to forward PTP packets.

By default, PTP is enabled on all the switch ports. To disable PTP on a port, use the following commands:

```
EN 4093(config)# interface port <port number>
EN 4093(config-if)# no ptp
```

Note: PTP cannot be enabled on management ports.

PTP packets have a Control Plane Protection (CoPP) queue of 36. You cannot change this CoPP priority. However, you can modify the PTP queue rate using the following command:

```
EN 4093(config)# qos protocol-packet-control rate-limit-packet-queue <0-47> <1-10000>
```

Ordinary Clock Mode

When the EN4093 10Gb Scalable Switch is configured as an ordinary clock, it synchronizes its clock with the master clock. If the EN4093 does not detect a master clock, it will not synchronize its clock with any other device. In this mode, the EN4093's clock cannot be modified manually or using another time protocol such as Network Time Protocol (NTP).

As an ordinary clock, the EN4093 synchronizes with a single PTP domain. The switch uses a delay-request mechanism to synchronize with the master clock. The switch uses a source IP address for the packets it generates. You can create a loopback interface for this purpose. By default, the switch uses the lowest interface in the VLAN from which the sync messages are received. To assign a loopback interface, use the following command:

```
EN 4093(config)# ip ptp source-interface loopback <interface number>
```

Note: If there are no interfaces on the switch that belong to the VLAN from which the sync messages are received, then the ordinary clock will not function. An error message will be generated. You can view this message using the `EN 4093# show ptp` command.

Transparent Clock Mode

When the EN4093 is configured as a transparent clock, its time can be set manually or using any time protocol. You must configure PTPv2 for the transparent clock to function. The switch does not modify PTPv1 packets as they pass through the switch.

As a transparent clock, the EN4093 supports syntonization (synchronization of clock frequency but not time) and synchronization with multiple domains.

Event packets received on all ports on the switch that have PTP enabled will be adjusted with the residence time. The switch sends all PTP packets to the multicast group address: 224.0.1.129. You can use Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), or any other multicast protocol to route the PTP packets.

Tracing PTP Packets

PTP packets can be traced on the PTP ports. These packets can be identified by their destination IP address and UDP ports. The following table includes the IEEE standard specification:

Table 3. IEEE Standard PTP Messages

Message	IP Address/UDP Port
PTP-primary: All PTP messages except peer delay mechanism messages	224.0.1.129
PTP-pdelay: Peer delay mechanism messages	224.0.0.107
Event Messages: Sync, delay request, peer delay request, peer delay response	319
General Messages: Announce, follow-up, delay response, peer delay response follow-up, management	320

Viewing PTP Information

The following table includes commands for viewing PTP information:

Table 4. PTP Information Commands

Command	Description
`EN 4093(config)# show ptp`	Displays global PTP information
`EN 4093(config)# show interface port <port number>`	Displays port information including port-specific PTP information
`EN 4093(config)# show ptp counters`	Displays ingress and egress PTP counters

Running Configuration

The following ISCLI command has been added to compare the running configuration with the startup configuration stored in FLASH.

```
EN 4093# show running-config diff
```

SNMP MIBs

- Added MIBs required for accessing LLDP data, as specified in RFC2737 and IEEE 802.AB.
- Added MIBs required for accessing MLDv2 information.
- Added entity MIBs, as specified in RFC2737 and RFC4133.
- Added MIBs required for managing host resources, as specified in RFC1514 and RFC2790.
- (New only to EN4093R) Added CPU MIB that helps to provide more information on module-wise CPU utilization.
- (New only to EN4093R) Added MIBs required for the management of port-based VLANs in bridge entities, as specified in IETF RFC4363.

Stacking

The EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch can be configured in stand-alone or stacking mode.

Static Multicast ARP

The Microsoft Windows operating system includes the Network Load Balancing (NLB) technology that helps to balance incoming IP traffic among multi-node clusters. In multicast mode, NLB uses a shared multicast MAC address with a unicast IP address. Since the address resolution protocol (ARP) can map an IP address to only one MAC address, port, and VLAN, the packet reaches only one of the servers (the one attached to the port on which the ARP was learnt).

To avoid the ARP resolution, you must create a static ARP entry with multicast MAC address. You must also specify the list of ports through which the multicast packet must be sent out from the gateway or Layer 2/Layer 3 node.

With these configurations, a packet with a unicast IPv4 destination address and multicast MAC address can be sent out as per the multicast MAC address configuration. NLB maps the unicast IP address and multicast MAC address as follows:

Cluster multicast MAC address: 03-BF-W-X-Y-Z; where W.X.Y.Z is the cluster unicast IP address.

You must configure the static multicast ARP entry only at the Layer 2/Layer 3 or Router node, and not at the Layer 2-only node.

IBM Networking OS supports a maximum of 20 static multicast ARP entries.

Note: If you use the ACL profile or IPMC-OPT profile, an ACL entry is consumed for each Static Multicast ARP entry that you configure. Hence, you can configure a maximum of 640 ACL and multicast MAC entries together.The ACL entries have a higher priority. In the default profile, the number of static multicast ARP entries that you configure does not affect the total number of ACL entries.

Configuring Static Multicast ARP

To configure multicast MAC ARP, you must perform the following steps:

- Configure the static multicast forwarding database (FDB) entry: Since there is no port list specified for static multicast ARP, and the associated MAC address is multicast, you must specify a static multicast FDB entry for the cluster MAC address to limit the multicast domain. If there is no static multicast FDB entry defined for the cluster MAC address, traffic will not be forwarded. Use the following command:

```
>> Main# /cfg/l2/fdb/mcast add <cluster MAC address> <port(s)>
```

- Configure the static multicast ARP entry: Multicast ARP static entries should be configured without specifying the list of ports to be used. Use the following command:

```
>> Main# /cfg/l3/arp/static add <destination unicast IP address> <destination
multicast MAC address> <cluster VLAN number>
```

Configuration Example

Consider the following example:

- Cluster unicast IP address: 10.10.10.42
- Cluster multicast MAC address: 03:bf:0A:0A:0A:2A
- Cluster VLAN: 42
- List of individual or port trunks to which traffic should be forwarded: 54 and 56

Following are the steps to configure the static multicast ARP based on the given example:

1. Configure the static multicast FDB entry.

```
>> Main# /cfg/l2/fdb/mcast add 03:bf:0A:0A:0A:2A 42 54 56
```

2. Configure the static multicast ARP entry:

```
>> Main# /cfg/l3/arp/static add 10.10.10.42 03:bf:0A:0A:0A:2A 42
```

You can verify the configuration using the following commands:

- Verify static multicast FDB entry:

```
>> Main# /info/l2/fdb/mcast/find 03:bf:0A:0A:0A:2A

 Multicast Address  VLAN  Port(s)
 -----------------  ----  ---------
 03:bf:0A:0A:0A:2A    42  54 56
```

- Verify static multicast ARP entry:

```
>> Main# /info/l3/arp/dump

 Current ARP configuration:
  rearp 5
 Current static ARP:
   ip              mac               port  vlan
   --------------- ----------------- ----- ----
   10.10.10.42     03:bf:0A:0A:0A:2A         42
 ------------------------------------------------
 Total number of arp entries : 2
     IP address    Flags    MAC address    VLAN  Age Port
   --------------- ----- ----------------- ----  --- ----
   10.10.10.1       P    fc:cf:62:9d:74:00   42
   10.10.10.42      P    03:bf:0A:0A:0A:2A   42      0
```

Limitations

- You must configure the ARP only in the Layer 2/Layer 3 node or the router node but not in the Layer 2-only node. Networking/ OS cannot validate if the node is Layer 2-only.
- The packet is always forwarded to all the ports as specified in the Multicast MAC address configuration. If VLAN membership changes for the ports, you must update this static multicast MAC entry. If not, the ports, whose membership has changed, will report discards.
- ACLs take precedence over static multicast ARP. If an ACL is configured to match and permit ingress of unicast traffic, the traffic will be forwarded based on the ACL rule, and the static multicast ARP will be ignored.

Switch Partition

Switch Partition (SPAR) facilitates the creation of multiple partitions within a switch to form a virtual switching context with respect to data plane partition of a switch. Each SPAR defined in a switch represents a switch partition in the data plane hardware. Data plane traffic is not shared between SPARs on the same switch. SPAR provides a simple Ethernet interface connectivity option for connecting Blade server chassis to network infrastructure.

SPAR is implemented as a dedicated VLAN with a set of internal server ports and a single uplink port or link aggregation (LAG). Since multiple uplink ports or LAGs are not allowed in SPAR, the possibility of misconfiguration or loop creation is eliminated. A port can only be a member of one SPAR.

A SPAR operates as a Layer 2 broadcast network. Hosts on the same VLAN attached to a SPAR can communicate with each other and with the upstream switch. Hosts on the same VLAN but attached to different SPARs communicate via the upstream switch.

The default SPAR is SPAR-0.

SPAR operates in two processing modes. The default mode is pass-through domain mode.

- Local Domain: In local domain processing mode, VLAN classification and assignment is based on the user-defined VLAN.
- Pass-through Domain: In pass-through domain processing mode, VLAN classification and assignment is based on the outer tag, which contains the unique domain VLAN ID of the SPAR. The inner tag with the user-defined VLAN remains unchanged.

Note: UFP and SPAR cannot be configured together.

Local Domain Processing

Each SPAR on a switch has a unique VLAN ID. This implicitly provides data separation between SPARs. If multiple networks share the uplink, then the upstream switch port must be configured as a 802.1Q trunk port so it can process multiple VLAN traffic from a SPAR. The SPAR domain uses a single uplink port or LAG shared among all the VLANs. For link redundancy or greater bandwidth, the uplinks can be grouped as static or LACP LAG.

If a VLAN is defined on multiple SPARs, then egress port mask is used to prevent communication between the SPARs in the same local domain VLAN. Since port membership of each SPAR is unique, the egress port mask ensures that different SPAR ports in the same local domain VLAN do not communicate with each other.

In local domain processing, all SPAR ports must have the following settings:

- Tagging must be enabled. (`>>Main# /cfg/port/tag ena`)
- TAGIPVID is disabled on all SPAR ports.
  (`>>Main# /cfg/port/tagipvid dis`)
- PVID is based on any VLAN defined in SPAR.
  (`>>Main# /cfg/port/pvid <VLAN number>`)

Layer 2 Switching

The EN4093 10Gb Scalable Switch learns MAC+VLAN on a per-port basis and not on a per-SPAR basis. If the switch detects the same MAC+VLAN combination on multiple SPAR ports, it considers it as station move. Hence SPAR deployment in local domain topology is restricted within distinct physical networks. Multiple SPAR domains within a physical network must not share the same set of VLANs to avoid the same MAC+VLAN combination appearing on more than one SPAR.

Pass-Through Domain Processing

In this processing mode, each SPAR is identified by its unique VLAN domain ID. Packets are classified based on the SPAR domain ID (outer tag) and not the user-defined VLAN (inner tag). SPAR ports must be configured in tunnel mode.

SPAR provides single or multiple VLAN connectivity through a single uplink port or LAG (static or LACP) without requiring VLAN definition within the SPAR domain.

Pass-through domain operates in Q-In-Q mode. Inside SPAR, different user-defined VLAN traffic is classified into single S-VLAN associated with the SPAR.

Although the uplink can be shared by multiple networks using the pass-through domain, SPAR will not be server-VLAN aware. Hence, multiple VLAN traffic will be mixed together in a single broadcast domain(i.e. broadcast traffic on different VLANs from the upstream network will reach all servers attached to the SPAR pass-through domain). The servers drop the packets if they do not belong to the desired VLAN. The pass-through implementation uses ingress VLAN tagging i.e. TAGIPVID is enabled on all SPAR ports.

In pass-through domain processing mode, all SPAR ports must have the following settings:

- TAGPVID is disabled. (`>>Main# /cfg/port/tagpvid dis`)
- TAGIPVID is enabled on all SPAR ports.
  (`>>Main# /cfg/port/tagipvid ena`)
- PVID is based on the SPAR DVLAN.
  (`>>Main# /cfg/port/pvid <DVLAN number>`)

SPAR VLAN Management

SPAR VLANs use the same 4000 VLAN space available for other applications/features on the switch. The VLAN ID can be in the range of 2 - 4094. VLAN 1 and the management VLAN 4095 are reserved for the default switch context.

A VLAN assigned to a SPAR cannot be used for any other switch application. Similarly, VLAN used by any other switch application cannot be assigned to a SPAR.

SPAR member ports cannot be members of any other VLAN.

Example Configuration

This example includes configuration of SPAR 1 in pass-through mode and SPAR 2 in local domain mode.

1. Create SPAR 1.

```
>>Main# /cfg/spar 1
```

2. Add uplink port to SPAR 1.

```
>>SPAR 1 Configuration# uplink
>>SPAR 1 Uplink Configuration# port Ext 1
>>SPAR 1 Uplink Configuration# ..
```

3. Configure domain mode.

```
>>SPAR 1 Configuration# domain
>>SPAR 1 Domain Configuration# mode passthrough
```

4. Configure SPAR VLAN.

```
>>SPAR 1 Domain Configuration# dvlan
>>SPAR 1 Default VLAN Domain Configuration# sparvid 4081
```

5. Add member ports.

```
>>SPAR 1 Default VLAN Domain Configuration# addsport INTA5-INTA10
>>SPAR 1 Default VLAN Domain Configuration# ..
>>>SPAR 1 Domain Configuration# ..
```

6. Enable SPAR 1.

```
>>SPAR 1 Configuration# ena
>>SPAR 1 Configuration# ..
```

7. Create SPAR 2.

```
>>Configuration# spar 2
```

8. Add uplink port to SPAR 2.

```
>>SPAR 2 Configuration# uplink port Ext 2
```

9. Configure domain mode.

```
>>SPAR 2 Configuration# domain
>>SPAR 2 Domain Configuration# mode local
```

10. Configure SPAR VLAN.

```
>>SPAR 2 Domain Configuration# dvlan
>>SPAR 2 Default VLAN Domain Configuration# sparvid 4082
```

11. Add member ports.

```
>>SPAR 1 Default VLAN Domain Configuration# addsport INTA11-INTA14
>>SPAR 1 Default VLAN Domain Configuration# ..
```

12. Configure local domain 1.

```
>>SPAR 2 Domain Configuration# lvlan 1
>>SPAR 2 Local VLAN Domain 1 Configuration# vid10
>>SPAR 2 Local VLAN Domain 1 Configuration# addsport INTA11-INTA14
>>SPAR 2 Local VLAN Domain 1 Configuration# ena
>>SPAR 2 Local VLAN Domain 1 Configuration# ..
```

13. Configure local domain 2.

```
>>SPAR 2 Domain Configuration# lvlan 2
>>SPAR 2 Local VLAN Domain 2 Configuration# vid20
>>SPAR 2 Local VLAN Domain 2 Configuration# addsport INTA11-INTA14
>>SPAR 2 Local VLAN Domain 2 Configuration# ena
>>SPAR 2 Local VLAN Domain 2 Configuration# ..
```

14. Configure local domain 3.

```
>>SPAR 2 Domain Configuration# lvlan 3
>>SPAR 2 Local VLAN Domain 3 Configuration# vid30
>>SPAR 2 Local VLAN Domain 3 Configuration# addsport INTA11-INTA14
>>SPAR 2 Local VLAN Domain 3 Configuration# ena
>>SPAR 2 Local VLAN Domain 3 Configuration# ..
>>SPAR 2 Domain Configuration# ..
```

15. Enable SPAR 2.

```
>>SPAR 2 Configuration# ena
```

Unsupported Features

The following features are not supported when SPAR is configured:

- 802.1x
- FCoE
- Hotlinks
- IGMP
- Layer 3 Configuration
- Management VLAN
- Private VLAN
- Protocol VLAN
- Edge Virtual Bridging
- sFlow
- Stacking
- STP, RSTP, MRSTP, PVST
- UFP
- vLAG

- VMAP
- VMready
- VNIC

Limitations

The following restrictions apply:

- SPAR VLANs are automatically added to Spanning Tree Group (STG) 1 regardless of the STP mode selected. STP is turned off on all SPAR ports.
- Trunks (static or LACP) created on the default switch cannot reference any SPAR ports. Trunks must first be defined in the SPAR context before they can be used by SPAR. Use the commands in the following menus to define trunks in the SPAR context:
  `>>Main# /cfg/spar <number>/uplink` menu;
  `>>Main# /cfg/layer 2` menu.
- ACLs defined on the default switch can be used for SPAR ports. However, the following restrictions apply:
  - An ACL cannot be shared across SPAR ports if:
    - An exit port (`>>Main# /cfg/acl/acl <number>/egrport`) is used as a filtering criteria and the exit port does not belong to the same SPAR as the port on which the ACL is applied.
    - A monitor port is used as a filtering criteria, and the monitor port does not belong to the same SPAR as the mirrored port and is not defined on the default switch.
  - The above ACL restrictions apply to all ACLs defined in an ACL group.
- Port mirroring can be configured on SPAR ports with the following restrictions:
  - The monitor port must belong to the same SPAR as the mirrored port, or must be defined on the default switch.
- Layer 2 failover features can be configured on SPAR ports. However, the Layer 2 failover AMON option is not supported. Only the Layer 2 failover MMON option can be used when all ports defined within the trigger belong to the same SPAR.

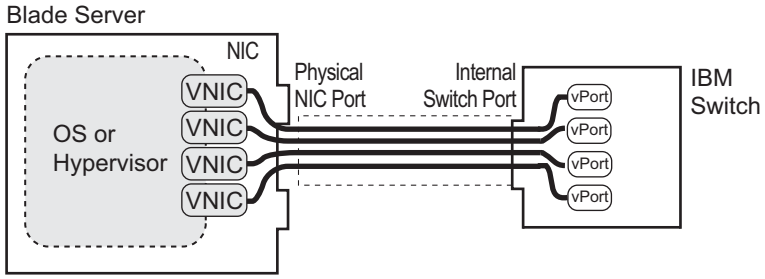
Unified Fabric Port

Virtualization is widely deployed in data centers today for isolating traffic and allocating bandwidth. However, virtualization introduces the overhead of managing two network entities: server and network. Unified Fabric Port (UFP) helps reduce this overhead by providing the ability to manage server side network functionality of the Network Interface Card (NIC) by applying network policies defined on the switch.

UFP is an architecture that logically subdivides a high-speed physical link connecting to a server NIC or to a Converged Network Adapter (CNA). UFP provides a switch fabric component to control the NIC. To the server operating system (OS) or to the hypervisor, each subdivision, called channel, appears as an independent physical NIC. Each channel has a unique identity and profile that defines its properties and functionality. The server communicates with the switch over the channel as defined in the channel profile. The channels share the high-speed physical link bandwidth.

For each channel, vNIC on the server side communicates with virtual port on the switch side. Any 10 Gbps internal (server) port can be configured as an UFP port.

Figure 2. UFP vPorts



Note: The EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch does not support UFP and VNIC configuration simultaneously.

UFP Protocol

The UFP protocol is a link-level protocol that runs as a separate instance for each physical communication link established between a server NIC and a switch port. The UFP protocol has three categories of operation:

- Channel Initialization: The server NIC and the switch port negotiate the number of channels and establish channel identifiers. Each UFP channel has a data component and a control component. The two components have the same UFP channel ID.
- Channel Control: For an established channel. the switch can modify channel properties by sending a control message on the UFP channel. While the channel ID is the same for the control and data components, the destination MAC address of the control message frame is a well-known address.
- Channel Data Path: The UFP protocol supports two types of data paths: local domain and pass-through domain. Local domain includes a server with multiple NICs connecting to a single physical switch domain with a single VLAN domain. Pass-though domain includes a server with multiple NICs connecting to multiple physical switching domains, where each domain has its own VLAN.

Channel Initialization

The channel initialization process sequence is as follows:

1. The server NIC sends a UFP channel request to the switch.
2. The switch sends back a UFPCHAN Type-Length-Value (TLV) with the number of UFP channels available. If the switch can satisfy the number channels requested by the server NIC, it sends an acknowledgement and provides channel identifiers for each requested channel.
3. Data and control traffic flowing between the server NIC and the switch port is tagged with the UFP channel identifier to which it belongs.

UFP channel initialization uses the Channel Discovery and Configuration Protocol (CDCP) TLV, as defined in the IEEE 802.1Qbg standard. The fields of the CDCP TLV and exchange sequence of TLVs, as defined in the IEEE 802.1Qbg specification, apply unmodified to UFP channel initialization. At any time after a UFP channel is assigned a channel ID, the switch can change the channel ID. In addition, after the establishment of a UFP channel, the switch and server NIC exchange channel properties in Edge Virtual Bridging (EVB) TLVs (also described in the IEEE 802.1Qbq specification). For UFP channels, the bits for the STD and ECP (Edge Control Protocol) capabilities are set in the EVB TLV. The exchanged EVB TLVs provide an indication of ECP readiness at the switch and at the server NIC. Communication between UFP channels on the same physical switch port is not allowed.

Channel Control

After UFP channels are established, the server NIC and switch port exchange UFP messages for control and configuration of each UFP channel. The UFP messages are in a standard TLV format and are of three types:

- Configuration TLV: Used by the switch to send configuration information to the server NIC. One configuration TLV is supported: NIC-Props TLV.
- Operational TLV: Used by the switch and the server NIC to perform runtime operations. Two operational TLVs are supported: Link-Down TLV and Link-Up TLV.
- Information/Statistics TLV: Used for analysis of information and statistics. One TLV is supported: End-of-TLV.

UFP messages are exchanged using ECP frames. The UFP TLV includes the type, length, flags, status, and payload fields, where the type field values are described in the following table:

Table 5. UFP TLV Type Values

TLV	Type	Description	Mandatory
END-OF-TLV	0	Indicates end of TLV sequence	Y
NIC-PROPS	1	Used by the switch to send NIC/Channel properties	Y
LINK-DOWN	2	Simulate link down event on vNIC	Y
LINK-UP	3	Simulate link up event on vNIC	Y

The flag values in the UFP TLV are as follows:

Table 6. UFP TLV Flag Values

Bit	Name	Interpretation
0x0	Request/Acknowledgement	Indicates a request (0) or acknowledgement (1)
0x1	Fragment	Indicates a TLV is fragmented. The receiver needs to wait for the next UFP frame before responding

The status field values in the UFP TLV are described in the following table:

Table 7. UFP TLV Status Values

Status	Name	Interpretation
0x0	Success	Request completed successfully
0x1	Not Supported	UFP TLV not recognized
0x2	Invalid Request	Invalid UFP request
0x3	Invalid State	Cannot handle the request in the current state
0x4	Insufficient Resource	NIC does not have sufficient resources to handle the request
0x5	Unspecified Error	Operation unsuccessful due to an unknown error
0x6	CNA Pre-boot Config Mismatch	Configuration mismatch between CNA and switch

Channel Data Path

The UFP protocol supports two types of data paths (or channels):

- Type 1 or local domain: Untagged frames are associated with the channel VLAN ID. If tagging is enabled on the switch port, the frames belong to the VLAN specified in the tag.
- Type 2 or pass-through domain: All tagged and untagged frames are associated with the channel VLAN ID. The tags inserted by the OS are passed through without any modification.

The channel type is set via the EVB TLV sent by the switch to the server NIC. A *type* value of 001b indicates local domain, and a value of 010b indicates pass-through domain.

At any point in time, the switch can change the channel type by sending an updated UFP TLV.

Local Domain

In local domain data path type, a server NIC connects with a switch port that belongs to a single VLAN domain. Switching is based on the inner VLAN tag controlled by the server (or Hypervisor), or on the port PVID. All Layer 2 and Layer 3 features are supported in local domain type.

Pass-through Domain

In pass-through domain data path type, a server NIC may connect with a switch port that belongs to multiple VLAN domains. Each UFP channel is a separate VLAN domain. Switching is based on the outer VLAN tag inserted by the switch at ingress. The outer VLAN tag is based on the UFP channel VLAN ID. The switch strips the outer tag on egress. The inner VLAN tag, controlled by the server (or Hypervisor), is not modified.

To implement pass-through domain, you must configure the virtual port in tunnel mode using the following command:

```
>>Main# /cfg/virt/ufp/port <num>/vport <num>/network mode tunnel
```

Virtual Ports

A single physical switch port is configured with virtual ports (vPorts). Each UFP channel connects the server NIC with a switch vPort. Properties, such as native VLAN and bandwidth, defined for a vPort are applied to the traffic that belongs to the vPort.

Note: A maximum of four vPorts can be configured per physical switch port.

vPort-VLAN Mapping

In local domain data path type, the switch and server identify the vPort/vNIC based on the port and VLAN tag in the incoming and outgoing packets. Since no two vPorts carry traffic for the same VLAN, the port+VLAN combination can be uniquely mapped to a vPort. When a vPort is initialized, the switch communicates a list of allowed VLANs, including the native VLAN to which the vPort belongs, to the server NIC. The server NIC uses this information to filter incoming and outgoing traffic based on the VLAN. All packets are single tagged with the vPort's native VLAN.

vPort-S-Tag Mapping

A vPort can also be identified with an S-tag (service tag or outer tag). When a vPort is initialized, the switch communicates the UFP channel ID of the vPort to the server NIC. When the server NIC or switch transmit frames, they add this S-tag to indicate the vPort or vNIC to which the packet is being transmitted. No VLAN mapping is required. Such packets can be single tagged (with native VLAN) or double tagged (with S-tag).

UFP vPort Mode

The UFP mode is configured based on the type of switching domain (single VLAN or multiple VLANs) a vPort is being connected to. For local domain data path types, trunk or access mode is configured. For pass-through domain data path type, tunnel mode is configured.

UFP vPort mode can be configured using the following command:

```
>>Main# /cfg/virt/ufp/port <num>/vport <num>/network mode {access|trunk|tunnel|fcoe}

Dafult mode is 'tunnel'
```

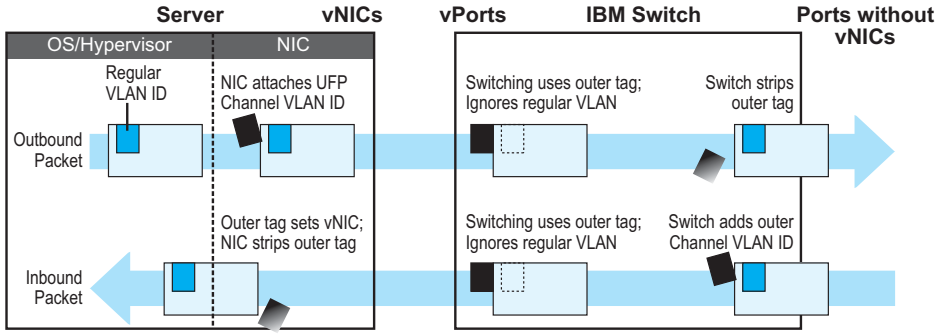
Tunnel Mode

In tunnel mode, a vPort can belong to only one VLAN. An outer tag with the vPort's VLAN ID is inserted in packets that egress the vPort. The inner VLAN tag remains unchanged. The switch processes packets based on the outer tag. When all the ports or vPorts that belong to a particular VLAN are placed in tunnel mode, they belong to one pass-through domain.

Tunnel mode of operation is useful in virtualized environments where it is desired to place all virtual machine (VM) data traffic, which needs to be sent to an upstream switch for Layer 2 or Layer 3 processing, in one domain. In such cases, the UFP port or vPort must be in tunnel mode and the upstream switch port must be in 802.1Q trunk mode.

Note: Two vPorts on a physical port cannot be members of the same VLAN.

Figure 3. Packet pass-through in Tunnel Mode

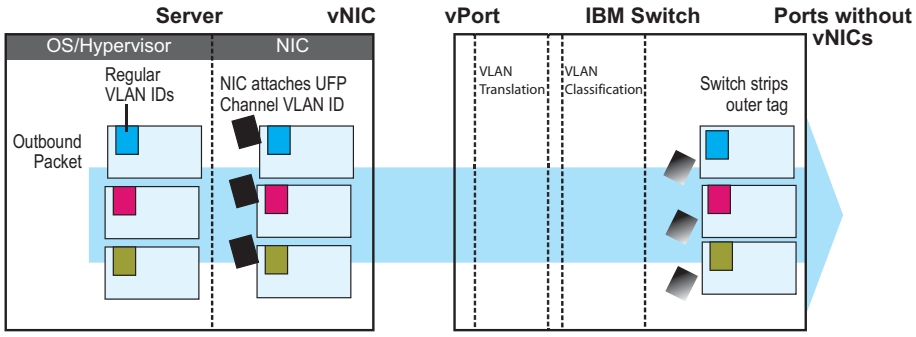


802.1Q Trunk Mode

In trunk mode, a vPort can carry packets that have inner tag belonging to up to 32 VLANs. This is restricted to a maximum of 4000 VLANs for all UFP vPorts configured on the switch. For each VLAN in the inner tag, a VLAN translation entry is required.

Note: Two vPorts operating in trunk mode on the same physical port cannot carry the same set of VLANs in the inner tag.

Figure 4. Packet passing through in Trunk Mode



Access Mode

In access mode, a vPort carries packets with inner tags that belong to one VLAN. The vPort is associated with the VLAN defined by using the command:

```
>>Main# /cfg/virt/ufp/port <port number>/vport <port number>/network/defvlan <VLAN Nmber>
```

FCoE Mode

A vPort configured in FCoE mode can only be attached to a Fibre Channel (FC) VLAN. Only one vPort on a physical port can be configured in FCoE mode. A vPort in FCoE mode operates as a local domain data path type with packets being single tagged.

UFP Bandwidth Provisioning

UFP provides one mode of bandwidth provisioning for vPort: Strict Bandwidth Provisioning Mode.

Strict Bandwidth Provisioning Mode

In this mode, the switch and NIC apply bidirectional bandwidth control on the vPort as per the defined configuration. By default, a bandwidth of 2.5 Gbps per vPort is guaranteed. If other vPorts are idle, the bandwidth of a vPort can be up to 10 Gbps. A minimum bandwidth of 1 Gbps is provisioned which can be raised by 100 Mbps increments. The sum of the minimum bandwidth guaranteed for all vPorts together cannot exceed the capacity of the physical link.

A vPort can also be configured with a maximum bandwidth.

This mode works with the port scheduler to avoid unintended packet drop due to policing through EFP metering block. If flow control is enabled, the switch provides a no drop packet forwarding behavior, thereby improving end-to-end Transmission Control Protocol (TCP) throughput performance.

Note: If a vPort is configured with low upper limit, it might lead to head-of-line (HOL) congestion on egress port.

By default, uplink ports have a separate traffic class for storage traffic with guaranteed bandwidth. Rest of the bandwidth is shared equally among other traffic.

Use the following command to configure strict bandwidth provisioning:

```
>>Main# /cfg/virt/ufp/port <num>/vport <num>/qos bw {minbw|maxbw}

minbw - Set minimum guaranteed bandwidth
maxbw - Set maximum allowed bandwidth
```

UFP Configuration Examples

Example 1: Access Mode

1. Turn on UFP.

```
>>Main# /cfg/virt/ufp on
```

2. Configure internal port as UFP.

```
>>UFP Global Configuration# port INTA1
>>Port INTA1 UFP Configuration# ena
```

3. Configure virtual port.

```
>>Port INTA1 UFP Configuration# vport 1
>>Virtual Port INTA1.1 Configuration# ena
```

4. Configure vPort access mode.

```
>>Virtual Port INTA1.1 Configuration# network
>>Virtual Port INTA1.1 Network Configuration# mode access
```

5. Configure vPort default VLAN.

```
>>Virtual Port INTA1.1 Network Configuration# defvlan 100
```

6. Ensure tagging is disabled on vPort.

```
>>Virtual Port INTA1.1 Network Configuration# deftag d
>>Virtual Port INTA1.1 Network Configuration# ..
```

7. Specify QoS parameters for the vPort.

```
>>Virtual Port INTA1.1 Configuration# qos
>>Virtual Port INTA1.1 QOS Configuration# bw
>>Virtual Port INTA1.1 Bandwidth Configuration# minbw 25                (in percentage)
>>Virtual Port INTA1.1 Bandwidth Configuration# maxbw 100               (in percentage)
>>Virtual Port INTA1.1 Bandwidth Configuration# /
```

8. Configure PVID of external port 1.

```
>>Main# /cfg/port EXT1
>>Port EXT1# pvid 100
>>Port EXT1# /
```

9. Apply the configuration.

```
>>Main# apply
```

Example 2: Trunk Mode

1. Turn on UFP.

```
>>Main# /cfg/virt/ufp on
```

2. Configure internal port 1 as UFP.

```
>>UFP Global Configuration# port INTA1
>>Port INTA1 UFP Configuration# ena
```

3. Configure virtual port.

```
>>Port INTA1 UFP Configuration# vport 3
>>Virtual Port INTA1.1 Configuration# ena
```

4. Configure vPort trunk mode.

```
>>Virtual Port INTA1.3 Configuration# network
>>Virtual Port INTA1.3 Network Configuration# mode trunk
```

5. Configure vPort default VLAN.

```
>>Virtual Port INTA1.3 Network Configuration# defvlan 100
```

6. Ensure tagging is disabled on vPort.

```
>>Virtual Port INTA1.3 Network Configuration# deftag d
>>Virtual Port INTA1.3 Network Configuration# ..
```

7. Specify QoS parameters for the vPort.

```
>>Virtual Port INTA1.3 Configuration# qos
>>Virtual Port INTA1.3 QOS Configuration# bw
>>Virtual Port INTA1.3 Bandwidth Configuration# minbw 25                (in percentage)
>>Virtual Port INTA1.3 Bandwidth Configuration# maxbw 100               (in percentage)
>>Virtual Port INTA1.3 Bandwidth Configuration# ..
>>Virtual Port INTA1.3 Network Configuration# ..
>>Virtual Port INTA1.3 Configuration# ..
>>Port INTA1 UFP Configuration# ..
>>UFP Global Configuration# ..
```

8. Configure internal port 2 as UFP.

```
>>UFP Global Configuration# port INTA2
>>Port INTA2 UFP Configuration# ena
```

9. Configure virtual port.

```
>>Port INTA2 UFP Configuration# vport 3
>>Virtual Port INTA2.3 Configuration# ena
```

10. Configure vPort trunk mode.

```
>>Virtual Port INTA2.3 Configuration# network
>>Virtual Port INTA2.3 Network Configuration# mode trunk
```

11. Configure vPort default VLAN.

```
>>Virtual Port INTA2.3 Network Configuration# defvlan 100
```

12. Ensure tagging is disabled on vPort.

```
>>Virtual Port INTA2.3 Network Configuration# deftag d
>>Virtual Port INTA2.3 Network Configuration# ..
```

13. Specify QoS parameters for the vPort.

```
>>Virtual Port INTA2.3 Configuration# qos
>>Virtual Port INTA2.3 QOS Configuration# bw
>>Virtual Port INTA2.3 Bandwidth Configuration# minbw 25                (in percentage)
>>Virtual Port INTA2.3 Bandwidth Configuration# maxbw 100               (in percentage)
>>Virtual Port INTA2.3 Bandwidth Configuration# /
```

14. Enable tagging on external port 1.

```
>>Main# /cfg/port EXT1
>>Port EXT1# tag ena
>>Port EXT1# pvid 100
>>Port EXT1# /
```

15. Configure VLAN 200 parameters.

```
>>Main# /cfg/l2/vlan 200
>>VLAN 200# ena
>>VLAN 200# def EXT1
>>VLAN 200# addvport INTA1.3
>>VLAN 200# addvport INTA2.3
>>VLAN 200# /
```

16. Configure VLAN 300 parameters.

```
>>Main# /cfg/l2/vlan 300
>>VLAN 300# ena
>>VLAN 300# def EXT1
>>VLAN 300# addvport INTA1.3
>>VLAN 300# addvport INTA2.3
>>VLAN 300# /
```

17. Apply the configuration.

```
>>Main# apply
```

Example 3: Tunnel Mode

1. Turn on UFP.

```
>>Main# /cfg/virt/ufp on
```

2. Configure internal port as UFP.

```
>>UFP Global Configuration# port INTA1
>>Port INTA1 UFP Configuration# ena
```

3. Configure virtual port.

```
>>Port INTA1 UFP Configuration# vport 1
>>Virtual Port INTA1.1 Configuration# ena
```

4. Configure vPort access mode.

```
>>Virtual Port INTA1.1 Configuration# network
>>Virtual Port INTA1.1 Network Configuration# mode tunnel
```

5. Configure vPort default VLAN.

```
>>Virtual Port INTA1.1 Network Configuration# defvlan 4000
```

6. Ensure tagging is disabled on vPort.

```
>>Virtual Port INTA1.1 Network Configuration# deftag d
>>Virtual Port INTA1.1 Network Configuration# ..
```

7. Specify QoS parameters for the vPort.

```
>>Virtual Port INTA1.1 Configuration# qos
>>Virtual Port INTA1.1 QOS Configuration# bw
>>Virtual Port INTA1.1 Bandwidth Configuration# minbw 25                (in percentage)
>>Virtual Port INTA1.1 Bandwidth Configuration# maxbw 100               (in percentage)
>>Virtual Port INTA1.1 Bandwidth Configuration# ..
>>Virtual Port INTA1.1 Network Configuration# ..
```

8. Configure tagging on external port 1.

```
>>Main# /cfg/port EXT1
>>Port EXT1# tagipvid enable
>>Port EXT1# tagpvid disable
>>Port EXT1# pvid 4000
>>Port EXT1# /
```

9. Apply the configuration.

```
>>Main# apply
```

Example 4: FCoE Mode

1. Enable CEE.

```
>>Main# /cfg/cee/on
```

2. Enable FIPs.

```
>>Main# /cfg/fcoe/fips/on
```

3. Turn on UFP.

```
>>Main# /cfg/virt/ufp on
```

4. Configure internal port as UFP.

```
>>UFP Global Configuration# port INTA1
>>Port INTA1 UFP Configuration# ena
```

5. Configure virtual port.

```
>>Port INTA1 UFP Configuration# vport 2
>>Virtual Port INTA2.1 Configuration# ena
```

6. Configure vPort access mode.

```
>>Virtual Port INTA2.1 Configuration# network
>>Virtual Port INTA2.1 Network Configuration# mode fcoe
```

7. Configure vPort default VLAN.

```
>>Virtual Port INTA2.1 Network Configuration# defvlan 1102
```

8. Ensure tagging is disabled on vPort.

```
>>Virtual Port INTA2.1 Network Configuration# deftag d
>>Virtual Port INTA2.1 Network Configuration# ..
```

9. Specify QoS parameters for the vPort.

```
>>Virtual Port INTA2.1 Configuration# qos
>>Virtual Port INTA2.1 QOS Configuration# bw
>>Virtual Port INTA2.1 Bandwidth Configuration# minbw 25                (in percentage)
>>Virtual Port INTA2.1 Bandwidth Configuration# maxbw 100               (in percentage)
>>Virtual Port INTA2.1 Bandwidth Configuration# ..
>>Virtual Port INTA2.1 Network Configuration# ..
```

10. Enable tagging on external port.

```
>>Main# /cfg/port EXT1
>>Port EXT1# tag enable
>>Port EXT1# pvid 1102
>>Port EXT1# /
```

11. Apply the configuration.

```
>>Main# apply
```

Limitations

The following restrictions apply when configuring UFP:

- FCoE must be configured only on vPort 2.
- If using Emulex NIC, FCoE can be configured on vPort 1 of an ITE server NIC.
- UFP port in FCoE mode cannot operate with FIP Auto VLAN feature.
- UFP does not support VMready Local Group configuration.
- UFP cannot be configured in stacking mode.
- VLANs having member vPorts configured in trunk or access modes cannot have member vPorts configured in tunnel mode.
- vPorts on a physical port, if configured in trunk or access mode, must be members of separate VLANs.
- A tunnel mode uplink port can be member of only one VLAN.
- A vPort in trunk mode can be a member of up to 32 VLANs.
- VLANs 4002-4005 are reserved for outer tagging.
- VLAN translation is not applied on packets that egress an UFP port.
- UFP bandwidth is guaranteed lossless only for unicast traffic.
- When CEE is on, FCoE vPort must be used for lossless priority traffic. For lossy priority traffic, a non-FCOE UFP vPort must be used. If lossless and lossy traffic is mixed, the lossless property of FCoE vPort is not guaranteed.

VLAG Capacity Enhancement

The maximum number of configurable VLAG instances is as follows:

- **With STP off:** Maximum of 31 VLAG instances
- **With STP on:**
  - **PVRST/MSTP with one VLAG instance per VLAN/STG:** Maximum of 31 VLAG instances
  - **PVRST/MSTP with one VLAG instance belonging to multiple VLANs/STGs:** Maximum of 20 VLAG instances

VLAN

Up to 4000 VLANs can be simultaneously configured on the EN4093.

VMready VMcheck

The EN4093 primarily identifies virtual machines by their MAC addresses. An untrusted server or a VM could identify itself by a trusted MAC address leading to MAC spoofing attacks. Sometimes, MAC addresses get transferred to another VM, or they get duplicated.

The VMcheck solution addresses these security concerns by validating the MAC addresses assigned to VMs. The switch periodically sends hello messages on server ports. These messages include the switch identifier and port number. The hypervisor listens to these messages on physical NICs and stores the information, which can be retrieved using the VMware Infrastructure Application Programming Interface (VI API). This information is used to validate VM MAC addresses. Two modes of validation are available: Basic and Advanced.

Use the following command to select the validation mode or to disable validation:

```
>>Main# /cfg/virt/vmgroup <VM group number>/validate {basic|advanced|disable}
```

Basic Validation

This mode provides port-based validation by identifying the port used by a hypervisor. It is suitable for environments in which MAC reassignment or duplication cannot occur.

The switch, using the hello message information, identifies a hypervisor port. If the hypervisor port is found in the hello message information, it is deemed to be a trusted port. Basic validation should be enabled when:

- A VM is added to a VM group, and the MAC address of the VM interface is in the Layer 2 table of the switch.
- A pre-provisioned VM interface that belongs to a VM group connects to the switch.
- A trusted port goes down. Port validation must be performed to ensure that the port does not get connected to an untrusted source when it comes back up.

Use the following command to set the action to be performed if the switch is unable to validate the VM MAC address:

```
>>Main# /cfg/virt/vmcheck/action/basic {log|link}

log - generates a log
link - disables the port
```

Advanced Validation

This mode provides VM-based validation by mapping a switch port to a VM MAC address. It is suitable for environments in which spoofing, MAC reassignment, or MAC duplication is possible.

When the switch receives frames from a VM, it first validates the VM interface based on the VM MAC address, VM Universally Unique Identifier (UUID), Switch port, and Switch ID available in the hello message information. Only if all the four parameters are matched, the VM MAC address is considered valid.

In advanced validation mode, if the VM MAC address validation fails, an ACL can be created to drop the traffic received from the VM MAC address on the switch port. Use the following command to specify the number of ACLs to be used for dropping traffic:

```
>>Main# /cfg/virt/vmcheck/acls <1-640>
```

Use the following command to set the action to be performed if the switch is unable to validate the VM MAC address:

```
>>Main# /cfg/virt/vmcheck/action/advanced {log|link|acl}
```

Following are the other VMcheck commands:

Table 8. VMcheck Commands

Command	Description
>>Main# /cfg/virt/vmware/hello {ena|dis|addport <*port number*>| rmport <*port number*>|haddr|htimer|cur}	Hello messages setting: enable/disable/add port/remove port/advertise this IP address in the hello messages instead of the default management IP address/set the timer to send the hello messages/view current hello message settings
>>Main# /cfg/virt/vmcheck/{trust|notrust} <*port number*>	Mark a port as trusted/untrusted
>>Main# /cfg/virt/vmcheck/cur	View current VMcheck settings
>>Main# /oper/virt/vmcheck/acl/{remall|remmac [<*port number*>]|remport <*port number*>}	Delete ACL(s): all ACLs/an ACL by MAC address ((optional) and port number) /all ACLs installed on a port

Supplemental Information

This section provides additional information about configuring and operating the EN4093 and N/OS.

The Boot Management Menu

The Boot Management menu allows you to switch the software image, reset the switch to factory defaults, or to recover from a failed software download.

You can interrupt the boot process and enter the Boot Management menu from the serial console port. When the system displays Memory Test, press **<Shift B>**. The Boot Management menu appears.

```
Resetting the System ...
Memory Test ..............................

1 - Change booting image
2 - Change configuration block
3 - Boot in recovery mode (tftp and xmodem download of images to
    recover switch)
4 - Xmodem download (for boot image only - use recovery mode for
    application images)
5 - Reboot
6 - Exit

Please choose your menu option: 3
```

The Boot Management menu allows you to perform the following actions:

- To change the booting image, press 1 and follow the screen prompts.
- To change the configuration block, press 2, and follow the screen prompts.
- To perform a software image recovery, press 3 and follow the screen prompts.
- To perform an Xmodem download (boot image only), press 4 and follow the screen prompts.
- To exit the Boot Management menu, press 6. The booting process continues.

Recovering from a Failed Software Upgrade

Use the following procedure to recover from a failed software upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
   - Speed: 9600 bps
   - Data Bits: 8
   - Stop Bits: 1
   - Parity: None
   - Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing <**Shift B**> while the Memory Test is in progress and the dots are being displayed.

4. Select **3** for **Boot in recovery mode**. You will see the following display:

```
Entering Rescue Mode.
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

   – If you choose option **x** (Xmodem serial download), go to step 5.
   – If you choose option **t** (TFTP download), go to step 6.

5. **Xmodem download**: When you see the following message, change the Serial Port characteristics to 115200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before
initiating the download.
```

   a. Press <**Enter**> to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start XModem on your terminal emulator.
   b. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
Change the baud rate back to 9600 bps, hit the <ESC> key.
```

   c. When you see the following prompt, enter the image number where you want to install the new software and press <**Enter**>.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

   d. The following message is displayed when the image download is complete. Continue to step 7.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

6. **TFTP download**: The switch prompts you to enter the following information:

```
Performing TFTP rescue. Please answer the following questions (enter
'q' to quit):
IP addr    :
Server addr:
Netmask    :
Gateway    :
Image Filename:
```

a. Enter the required information and press <**Enter**>.

b. You will see a display similar to the following:

```
        Host IP    : 10.10.98.110
        Server IP  : 10.10.98.100
        Netmask    : 255.255.255.0
        Broadcast  : 10.10.98.255
        Gateway    : 10.10.98.254
Installing image 6.8.3_OS.img from TFTP server 10.10.98.100
```

c. When you see the following prompt, enter the image number where you want to install the new software and press <**Enter**>.

```
Install image as image 1 or 2 (hit return to just boot image): 1
```

d. The following message is displayed when the image download is complete. Continue to step 7.

```
Installing image as image1...
Image1 updated successfully
Please select one of the following options:
        T) Configure networking and tftp download an image
        X) Use xmodem 1K to serial download an image
        R) Reboot
        E) Exit
```

7. Image recovery is complete. Perform one of the following steps:
   – Press **r** to reboot the switch.
   – Press **e** to exit the Boot Management menu
   – Press the Escape key (<**Esc>**) to re-display the Boot Management menu.

Recovering a Failed Boot Image

Use the following procedure to recover from a failed boot image upgrade.

1. Connect a PC to the serial port of the switch.
2. Open a terminal emulator program that supports Xmodem download (for example, HyperTerminal, CRT, PuTTY) and select the following serial port characteristics:
   – Speed: 9600 bps
   – Data Bits: 8
   – Stop Bits: 1
   – Parity: None
   – Flow Control: None
3. Boot the switch and access the Boot Management menu by pressing <**Shift B**> while the Memory Test is in progress and the dots are being displayed.
4. Select **4** for **Xmodem download**. You will see the following display:

```
Perform xmodem download

To download an image use 1K Xmodem at 115200 bps.
```

5. When you see the following message, change the Serial Port characteristics to 115200 bps:

```
Change the baud rate to 115200 bps and hit the <ENTER> key before
initiating the download.
```

   a. Press <**Enter**> to set the system into download accept mode. When the readiness meter displays (a series of “C” characters), start Xmodem on your terminal emulator.You will see a display similar to the following:

```
Extracting images ... Do *NOT* power cycle the switch.
**** RAMDISK ****
Un-Protected 38 sectors
Erasing Flash...
.................................. done
Erased 38 sectors
Writing to
Flash...9....8....7....6....5....4....3....2....1....done
Protected 38 sectors
**** KERNEL ****
Un-Protected 24 sectors
Erasing Flash...
...................... done
Erased 24 sectors
Writing to Flash...9....8....7....6....5....4....3....2....1....
```

   b. When you see the following message, change the Serial Port characteristics to 9600 bps:

```
Change the baud rate back to 9600 bps, hit the <ESC> key.
```

Boot image recovery is complete.

Chassis Management Module

The switch management port IP address can only be configured via the CMM web interface. The switch-based configuration interfaces (such as the menu-based CLI, ISCLI, BBI, etc.) cannot be used for this purpose.

When configuring the IP interface, which is dedicated to the internal management port (IF128, MGT1), you cannot use a subnet that is already configured on any other enabled interface (IF1-127). This results in IF128 being disabled and an IP configuration of all zeros displayed on the CMM user interface. The CMM event log will indicate that a "`Duplicate route`" was detected.

For example, consider that the interface dedicated to the external management port (EXTM, IF127) is configured or enabled to the following IP address and mask:

```
Interface information:
127: IP4 192.168.71.120  255.255.255.0
```

The switch will reject an attempt made from the CMM CLI to configure the internal management port (MGT1, IF128) to the following IP address and mask:

```
system:switch[1]> ifconfig -i 192.168.71.130 -s 255.255.255.0
```

In this scenario, the switch rejects the attempt by disabling any current configuration on IF128, and responds to the CMM with an IP address, mask, and gateway that contains all zeros.

On the CMM CLI, the resulting condition appears as follows:

```
system:switch[1]> ifconfig
Ethernet ScSE
Enabled
-c  static
-i   0.0.0.0
-s   0.0.0.0
-g   0.0.0.0
system:mm[1]> displaylog
1  I  IOMod_01  04/03/12  08:02:49  (iomodule01) Duplicate route
detected to I/O module iomodule01.
2  I  IOMod_01  04/03/12  08:02:49  (iomodule01) I/O module 1 IP
address was changed to 0.0.0.0.
```

VLAGs

For optimal VLAG operation, adhere to the following configuration recommendations:

- The ISL should include enough ports to accommodate the peer-to-peer traffic.
- Any port-related configuration, such as applied ACLs, should be the same for all ports included in the same VLAG, across both peer switches.
- Configure VLAG health checking as shown in the *Application Guide*.

External Port Link Negotiation

Autonegotiation settings for each external switch port should be the same as those of the devices being connected. In a valid configuration, both ends of a port link are set with autonegotiation on, or both ends are set to specific speed and link properties with autonegotiation disabled.

Port Mirroring Tags BPDU Packets

When you perform port mirroring, Spanning Tree BPDU packets are VLAN tagged at the monitoring port. This is standard behavior of port mirroring on the EN4093. All mirrored egress traffic is tagged.

Secure Management Network

The following EN4093 attributes are reserved to provide secure management access to and from the chassis management module:

- MGT port (MGT1)
- VLAN 4095
- IP interface 127, 128
- Gateway 4
- STG 128

For more information about remotely managing the EN4093 through the external ports, see “Accessing the Switch” in the *IBM Networking OS 7.5 Application Guide*.

Note: The external uplink ports (EXT*x*) cannot be members of management VLANs.

Secure Shell (SSH)

Because SSH key generation is CPU intensive, the EN4093 attempts to avoid unnecessary key generation. The process generates three server keys:

1. One key is generated to replace the current server key, if used.
2. A second key is generated as a spare, in case the current server key is used and the specified interval expires.
3. A third key is generated for use at the next reboot.

Therefore, if you never login via SSH, you will only see two key generation events. You may see all three events directly following a reboot. If you want to witness the key generation after the specified interval has expired, then you must login via SSH at least once during each expiration interval.

Spanning Tree Configuration Tips

To ensure proper operation with switches that use Cisco Per VLAN Spanning Tree (PVST+), you must do one of the following:

- Create a separate Spanning Tree Group for each VLAN.
- Manually add all associated VLANs into a single Spanning Tree Group.

When using Layer 2 Trunk Failover, disable Spanning Tree Protocol on external ports.

Syslog Configuration Tip

The *facility* parameter traditionally is used to correlate services (such as IP, CLI, etc.) to messages. This is done to distinguish between the different services that are running in the network/device. However, for the EN4093, there is a single configured facility value (0-7) used on all messages. By configuring a unique facility value for each switch, a single SYSLOG server can distinguish between the various EN4093s in the network. Refer to “System Host Log Configuration” in the *Command Reference.*

Trunk Group Configuration Tips

Please be aware of the following information when you configure trunk groups:

- Always configure trunk groups first, on both ends, before you physically connect the links.
- Configure all ports in a trunk group to the same speed (you cannot aggregate 1Gb ports with 10GBASE-SFP+ ports).
- Configure all ports in a trunk group with the same duplex.
- Configure all ports in a trunk group with the same flowcontrol.

vCenter Synchronization

When applying distributed VM group configuration changes, the switch will attempt to synchronize settings with the VMware vCenter for virtualization management. If the vCenter is unavailable, an error message will be displayed on the switch. Be sure to evaluate all error message and take the appropriate actions to ensure the expected changes are properly applied. If corrective actions are not taken, synchronization may remain incomplete when connection with the vCenter is restored.

Solution: When the switch connection with the vCenter is restored, use the following operational command to force synchronization:

```
>> # /oper/virt/vmware/scan
```

VRRP Configuration

Although the Virtual Router Redundancy Protocol (VRRP) standard permits up to 255 virtual router instances, the N/OS 7.5 implementation only allows up to 128 virtual router instances (corresponding to the number of supported IP interfaces). Each virtual router instance can be assigned a unique Virtual Router ID (VRID) between 1 and 255.

Known Issues

This section describes known issues for N/OS 7.5 on the EN4093 and EN4093R 10Gb Virtual Fabric Scalable Switch.

Boot Configuration Block

- In the CLI, the boot configuration command (`/boot/conf` <*block*>) examines only the initial character of the *block* option. Invalid *block* strings (those other than `active`, `backup`, or `factory`) that use a valid first character (a, b, or f) will be interpreted as the matching valid string. (ID: 42422)

Chassis Management Module (CMM)

- False switch errors might be reported in the CMM event log after the Flex Chassis power is cycled off/on. These events imply that the switch has experienced an electrical or thermal issue, as shown below:

```
Info 08:42 AM           I/O module iomodule02 is within the
recommended
                        temperature range.
Info 08:42 AM Recovery: I/O module iomodule02 current fault.
Err  08:42 AM           I/O module iomodule02 current fault.
Err  08:42 AM           I/O module iomodule02 temperature fault.
Warn 08:42 AM           I/O module iomodule02 is over recommended
                        temperature.
```

  These false switch errors occur and recover within the same minute and only intermittently occur as a result of a chassis power cycle. Ignore these false error messages. (ID: 60687)

- NTP configuration can only be saved via the CMM web interface. NTP configuration using the switch-based configuration interfaces (such as the menu-based CLI, ISCLI, BBI, etc.) will be overridden by the CMM whenever the switch or CMM are restarted. (ID: 60460)

FCoE

- In N/OS 7.5, the EN4093 supports up to 175 simultaneous FCoE sessions. When this capacity is reached, traffic for additional sessions is dropped, though some host servers and uplink devices may consider all sessions fully established. (ID: 60337, 64842)

Hotlinks

- Prior to enabling hotlinks, Spanning-Tree should be globally disabled using the following command (ID: 47917):

```
EN 4093(config)# spanning-tree mode dis
```

IPsec

- IPsec does not support virtual links. (ID: 48914)

ISCLI Configuration Scripts

When using the ISCLI, configuration commands are applied to the active switch configuration immediately upon execution. As a result, when using the ISCLI to load a configuration script containing a long list of processor-intensive commands (such as static route definitions), switch response to other management functions (such as Telnet access for additional management sessions) may be slow or even time-out while the switch individually applies each scripted command. (ID 31787)

Solution: The CLI may be used as an alternative to the ISCLI. Because CLI commands are not fully processed until the CLI `apply` command is given, the equivalent configuration script can be loaded in its entirety and then applied as a whole without undue impact on other management sessions.

LACP

- If a static trunk on a EN4093 is connected to another EN4093 with LACP configured (but no active LACP trunk), the `/info/l2/trunk` command might erroneously report the static trunk as forwarding.
- If you configure LACP (active/passive) on one port, also configure LACP on the partner switch, at the end of the link. If you connect LACP with a static trunk, there will be no connectivity on that link.
- Since LACP trunks use LACPDU packet to maintain trunking with the partner, there is a possibility for those packets to be dropped from an extremely busy trunk. If this happens, some links in the LACP trunk might be removed, then aggregated back to the trunk if an LACPDU is received. To avoid this unstable LACP trunk link, you can add more links to the trunk to increase the bandwidth, or use regular static trunk if there are no more links available.
- Under some conditions, setting the LACP timeout value on partner switches to “short” may cause LACP links to flap in and out of service. If this situation occurs, set the LACP timeout value to “long.” (ID: 63405, 64518)

Menu-Based CLI

- When dynamic VLAN configuration is enabled for features such as QBG, VMready, or FCoE, whenever automatic changes are made to the switch VLAN configuration, any other unapplied changes pending from menu-based CLI configuration session will be automatically applied. (ID: 65392)

OSPF

- Some changes to OSPF configuration (such as creating a new area or changing an area’s type) may result in OSPF state reconvergence. (ID: 46445, 48483)
- OSPFv3 over IPsec
  - This combination can only be configured only on a per-interface basis. Configuration based on virtual links is not currently supported.
  - The current implementation for OSPFv3 allows the use of only one protocol (AH or ESP) at any given time. AH and ESP cannot be applied together.

Ports and Transceivers

- Under repeated and rapid removal and reinsertion a port transceiver, it is possible that the resulting port state may not be represented accurately within the switch. (ID 32412)

  Solution: Once you have removed a transceiver from a switch port, wait five seconds before reinserting any transceiver into the same port. This allows the port to stabilize, and promotes accurate port state information within the switch.
- When the link speed for an external connection is forced (i.e. no Auto-Negotiation) to 100 Mbps and then changed to 10 Mbps, if the external device is changed first, the external device may erroneously report the link as DOWN even after the switch is changed to 10 Mbps.

  Solution: At the external device, disconnect and reconnect the cable.
- Interoperability with Older Hubs

  The command-line interface might display link up and link down messages continuously for an external port that is connected to certain older hub models configured for 100 Mbps half-duplex. The display might show link up erroneously. This behavior has been observed when connecting the GbESM with the following devices:

  – NETGEAR FE104 100 hub

  – SBS 1000Base-T NIC

  – 3Com Linkbuilder FMS100 Hub 3C250 TX/I

  – 3Com SuperStack II 100TX 3C250C-TX-24/12

  – Nortel Baystack 204 Hub
- If the EN4093 is connected to an application switch which requires a link speed of 100 Mbps half-duplex, then enable auto negotiation on the EN4093 port with port speed=any, mode=any, fctl=both, and auto=on.

QSFP+

- The QSFP+ ports do not auto-negotiate. The desired speed must be configured to match on both ends of the connection, and the switch reset for changes to take effect. (ID: 46340)
- After you upgrade switch software and reset the switch, you must configure the QSFP+ port mode. Use the following command (ID: 46858):

  `boot qsfp-40gports` *<15,19>*

SLP

When using multi-value attributes that contain a list of comma-separated values, the service reply will match if it contains one or more of the values. It is not required that all values match. (ID: 60086)

Stacking

- LLDP status changes are not reflected in the master switch system logs. (ID: 65325)

UFP

- In N/OS 7.5, the EN4093 does not support UFP QoS statistics. (ID: 64021, 64371)