Migration and Upgrade of Cisco ASR 900 RSP1 or ASR 900 RSP2 Module to ASR 900 RSP3 Module

This document details the migration requirements while migrating the ASR 900 RSP1 or ASR 900 RSP2 module to ASR 900 RSP3 module and the supported interface modules (IM).

Ethernet Interface Modules

The ASR900 RSP3 module supports three new interface modules (IM)s with higher port density. It also supports the IMs supported on the ASR 900 RSP1 and ASR 900 RSP2 modules.

IM Part Numbers	Description
IMs Supported on ASR 900 RSP3	
A900-IMA8Z (8X10GE)	8-port 10 Gigabit Ethernet Interface Module
A900-IMA1C (1X100GE)	1-port 100 Gigabit Ethernet Interface Module
A900-IMA2F (2X40GE)	2-port 40 Gigabit Ethernet QSFP Interface Module

Backup of Licenses and Running Configuration

The Cisco ASR 900 Series Router platform licenses are configured on the RSP on the router. It is recommended to backup the license before performing a migration. Licenses should be re-installed after a migration. For information on the licenses, see Cisco IOS XE Software for Cisco ASR 900 Series Aggregation Services Routers Data Sheet.

For information on licensing the Cisco ASR 900 Series Routers, see Licensing Information.

Procedure

Step 1   Procure the license UDI details using the **show license udi** command.

Example:

```
Router# show license udi

SlotID   PID                 SN                  UDI
----------------------------------------------------------------------------
*6       ASR-903             FOX1637P0UB         ASR-903:FOX1637P0UB
```

The command lists the serial number of the RSP inserted in the router.

Step 2   Save the license file to an external drive (USB) using the **license save bootflash:lic.txt** command.

Step 3   Backup the license file in an external drive (USB) or a TFTP server.

Step 4   Backup the running configuration in an external drive (USB) or a TFTP server. You will need to access this server to replace the configuration after the migration.

Migration of RSPs and IMs

General Restrictions

- IP SLA UDP Jitter versions 2 and 3 are supported only on RSP2 and *not* supported on RSP3.

- Installing a mixture of RSPs such as ASR 900 RSP2 with ASR 900 RSP3 is *not* supported.

- TDM IM (A900-IMA16D) and 1-Port OC12/STM-4 (OC-12) (A900-IMA4OS) IM are *not* supported in Cisco IOS XE Release 3.16S.

- Supported feature scale values should be used during migration. For information on supported scale values, see Data Sheets.

- When replacing one RSP with another RSP (either during RMA or migration of one RSP to another), ensure that RSP image version of the replaced RSP is same as that of Active RSP.

  Follow these steps:

  1. Have a USB with the active configuration, the IOS-XE .bin and the ROMMON image.

  2. Insert the USB into the new RSP.

  3. Remove the old RSP and insert the new RSP.

  4. Boot the new RSP and check the ROMMON version.

      If required, upgrade the ROMMON from the USB, and reboot.

  5. Press Break on the terminal keyboard within 60 seconds of power up to put the router into ROMMON mode.

6. Boot from ROMMON usb0: active image .bin.

7. Copy the .bin file to bootflash:

8. Perform File System cleanup using the **delete standby bootflash** command.

9. Load the router configuration from the USB. However, if you have a redundant RSP in the router, the active configuration is automatically copied to the standby RSP.

10. Reboot into package mode by expanding the .bin to the package and setting auto boot.

11. Wait for SSO mode and check the status of both RSPs using the **show platform** and **show redundancy** commands.

Carrier Ethernet Restrictions

Table 1: EFP/TEFP Scale Support

Feature	Scale
MAC scale per BD	64K
MAC scale on system with BDI (software MAC learning)	16K
Hardware MAC learning in system	200K
Total Static MAC in system	1K
EFP scale in system	5K 16K - Starting with Cisco IOS XE Fuji 16.7.1 release and later.
Number of TEFPs	Equal to number of ports with 1 TEFP per port
VLAN scale per TEFP	1K

- **EFP**

  - Priority tag is not supported under the same EFP.

  - L2VPN VPLS VC statistics are not supported.

  - Dynamically changing Trunk EFP number on an interface is not supported.

  - EFP shut is supported starting with Cisco IOS XE Release 3.18SP.

  - BDI statistics is not supported.

  - Up to 50% of line rate traffic can be achieved during L2 flood because of hardware limitation.

  - With scaled EFP configurations, pending-issue/acknowledgement clears in the system and the traffic resumes approximately after 25 to 30 minutes during a reload.

- **BFD**

- BFD on MLPS TP is not supported on the RSP3 module.

- BFD over port-channel works only on hardware in RSP1 and RSP2, as it supports only software in RSP3.

- BFD Dampening is not supported.

- **MAC Limiting**

  - MAC-learning limit is not supported in RSP3 at hardware level, in releases prior to Cisco IOS XE Fuji 16.7.1 release.

  - Maximum of two aging profiles is supported on the router, in addition to the default aging profile.

  - MAC aging timer modification is not supported.

- **CFM**

  - The Maintenance Association (MA) service short name is configured in string format (for hardware timers):

    - Domain name is only 5 bytes (5 characters).

    - MA varies from 1 to 6 bytes (service name can be of any value between 1 to 6 characters).

  - Port-MEP is not supported on an interfae with untagged EFP .

  - For offloaded MA, CCM threshold cannot be modifed. The default value is 3.5.

  - If UP MEP CFM session is configured on an interface that is physically down, RMEP (removed MEP) is not learned until the interface is up.

  - MIP filtering is not supported.

  - Adding BDI for a TEFP BD causes traffic disruption and the CFM session flaps.

  - Toggling of CC interval from HW (3.3ms, 100ms, 10ms) to SW (1s, 10s) causes the local MEP programming to fail. We recommed you remove and reconfigure the MEP.

  - CFM packets keep flowing on removal of TEFP, that is configured with CFM. We recommended that you remove CFM session, and then remove the TEFP.

- **SPAN**

  - Do not add any data port as a destination port for SPAN session.

  - Jumbo sized packets and bad CRC packets are not spanned.

  - If span session is configured with default MTU and when frame comes with higher MTU than the configured value of span session; Tx interface has some extra packets.

- **G.8032 Ethernet Ring Protection**

  - A maximum limit of 1000 rings per TEFP is supported.

  - Starting with Cisco IOS XE Release 3.18SP, 16 rings are supported. A total of 8 rings with 2 instances each is the maximum scale supported.

- **VPLS**

  - VPLS over TE is not supported.

  - VPLS over 802.1ad is not supported.

- **Storm Control**

  - Storm control on a port channel is not supported.

  - Storm control statistics (current incoming traffic rate) is not supported.

  - Invalid traffic (traffic on non-existing EFP, or on an STP blocked port) is also considered for ethernet policing. Hence, invalid incoming traffic may cause a storm control trigger.

  - Storm control detection could be with +/- 5% deviation of configured rate.

  - Minimum high or low watermark that can be configured is 146 kbps (as per the BCM limitation).

  - Twelve static L2 ACL entries are used for a storm control. The overall L2 ACL limits are reduced.

  - Minimum PPS is 292.

  - Storm control on Layer3 multicast traffic is not supported.

  - Storm control is not supported on point-to-point connection, but local connect broadcast storm control is supported.

- **EVC Local Connect**

  - Egress filtering based on encapsulation, VLAN translation, terminal, and facility loopback is not supprted.

  - CFM and ethernet loopback is not supported.

  - Layer2 protocol tunnelling is not suppoted. Only Layer2 protoocol peering and forwarding is supported.

  - Local connect with Trunk EFP is not supported.

  - Local connect members with service instances is not supported.

  - In case of single encap dot1q with rewite pop1 at ingress and encap dot1q without rewrite at egress, egress filtering is not spplied at the RSP3 as the egress traffic is untagged. The random dot1q tag is present due to a ASIC limitation.

- **Ethertype**

  - Dynamic updating of custom ethertype from dot1q to tunnelling or viceversa is not supprted.

  - Dot1q packets are permitted on an interface with custom ethertype. The outer 0x8100 packets are supprted

  - Dot1q tunnelling etherytpe CFI preservation is not supported.

  - Custom ethertype on routing interfaces is not supported.

  - Push is not supported.

  - 802.1ad is not supported.

- DHCP is not supported.

- Rewrite push is not supported on ingress.

- CFM with custom ethertype is not supported.

- **802.1ad**

  - 802.1ad is not supported on port-channel interfaces.

  - 802.1ad is not supported on bridge-domian interfaces.

  - Encap dot1ad, do1q on NNI ports with rewrite configured as **rewrite ingress tag pop2 symm** at egress incorrectly pushes two dot1q tags. Pop2 is not supprted.

Multicast, MPLS and Segment Routing Restrictions

Table 2: Multicast Scale Differences

	RSP1B	**RSP2**			**RSP3**
Templates	Default Template	Default Template	Video Template	IP Template	Default Template
IPv4 Mroutes	3990	1000	2000	1000	4000
IPv6 Mroutes	1000	1000	1000	1000	1000

The following table shows the multicast feature support in the various RSP platforms. For more information on profile-related support, see IP Multicast: Multicast Configuration Guide, Cisco IOS XE Everest 16.6.1 (Cisco ASR 900 Series).

Table 3: Multicast Feature Support on RSPx Platforms

Feature	RSP1	RSP2	RSP3
PIMv4	Yes	Yes	Yes
PIMv6	Yes	Yes	Yes
IGMPSN over EFP	Yes	Yes	Yes
IGMPSN over TEFP	Yes	Yes	Yes
IGMPSN over PC	Yes	Yes	Yes
PIM BFD	Yes	Yes	Yes
MLDPv4 with routed core*[1]	No	Yes	Yes
MLDPv4 with BDI in core*	No	Yes	Yes
MLDPv6 with Routed core*	No	Yes	Yes
MLDPv6 with BDI in core*	No	Yes	Yes

Feature	RSP1	RSP2	RSP3
MVPN-GRE with routed core (IPv4)*	No	Yes	Yes
MVPN-GRE with BDI in core (IPv4)*	No	Yes	Yes
Extranet SSC (IPv4)	No	Yes	No
Extranet RSC (IPv4)	No	Yes	No
P2MP-TE	No	Yes	No

[1] *Feature support may vary based on the different release version.

Following are the limitations for RSP3:

- RSP3 does not support Extranet and P2MP-TE.

- MPLS counters are not supported.

- BDI statistics are not supported.

- IP MTU and MPLS MTU are supported. But MPLS MTU support is restricted only to CPU originated traffic. For the forwarded traffic, it is the IP MTU that decides the behavior.

- LFA/RLFA is only supported on single member link port-channel.

- MPLS TE FRR over single member link PO is supported.

- Routed PW does not support the following:

    - IPv6 traffic

    - LFA/RLFA feature

    - BFD

    - PTP

    - QoS

    - Multicast

    - VRRP and HSRP

    - ACL

    - IP fragmentation on disposition

- **VPLS**

    - By default VC counters are not supported.

    - MTU configured under VFI is used only for session negotiation and not for data fragmentation.

    - EoMPLS VC stats are not supported.

- **VPLS backup PW**

- MAC address learnt on the virtual circuit does not clear when psuedowire state gets change from UP to STBY or vice versa.

- Member BDI must not be in the same group as psuedowire interfaces.

- Physical interface must not be configured as a member in L2VPN context.

- Only 2 psuedowires must be configured in L2VPN context.

- BDI must not be configured with any IP configuration like "mpls ip", "dhcp ip" or "static ip".

- Only 1000 VPLS active and 1000 standby VPLS sessions are supported as the maximum number of BDI on RSP3 is 1000.

- VPLS backup PW with BGP Auto-discovery is not supported.

- L3VPN PIC Edge is supported in software if BGP next-hop is over BGP-LU. Due to this, sub-second is not guaranteed for all the prefixes.

- **Segment Routing**

  - Supports only 4 label stack.

  - SR TE tunnel can have only 1 transport label.

  - ODN is not supported.

- **Flex LSP**

  - L2VPN/L3VPN over EXP-NULL over Flex-LSP is not supported.

  - Flex LSP tunnel statistics are not supported.

- **BGP Multipath**

  - BGP maximum paths are not supported over MPLS TE and MPLS TE FRR.

  - Hierarchical BGP PIC edge or BGP Maximum Path is not supported.

  - The combination of IPv4 address family BGP PIC edge with VPNv4 PIC edge is not supported (Hierarchical BGP PIC edge).

  - The combination of IPv4 address family maximum paths with VPNv4 PIC edge is not supported (Hierarchical BGP maximum-paths).

- **ECMP**

  - L4 header lookup is not supported for hardware loopback.

  - If P node receives flow with 4 labels, RSP3 considers only first 3 labels for load balancing hashing in hardware.

  - At P node, hardware load balancing happens only if FRR is disabled and all paths point to same next-hop.

  - At P node, hardware load balancing is not supported on different next-hops.

RSP3 - QoS Restrictions

Ingress Queuing:

- The router does not support queuing on ingress interfaces.

Egress Queuing - The router supports tail drop queuing on egress interfaces using the **queue-limit** command.

- Queue allocation is per EFP/TEFP per TC(qos-group) for L2 interfaces with egress policy map applied.

- Queue allocation is per Port per TC(qos-group) for L3 interfaces.

- If class is matching multiple TC(qos-group) then multiple queues are generated for this class. For L2 interface, queues belonging to all EFP with the same TC comes under same class.

- Configuring shaping using committed burst (bc) is supported and excess burst (be) is not supported on the router.

- Granularity at lower rates is 384Kbps and at higher rates is 1.5 percent.

- Priority Level command and Priority command are not supported in the same policy.

- Strict Priority and bandwidth command cannot be configured in the same policy-map.

- Mixed bandwidth types are not supported in the same policy. For example, if you use bandwidth remaining percent command in one class, you cannot use bandwidth percent or bandwidth remaining ratio command in the same policy.

- The bandwidth and bandwidth-remaining commands are not supported on class containing the Priority command.

- Priority propagation is not supported.

Ingress Marking (QoS marking):

- The router does not support hierarchical marking.

- COS to PREC/DSCP marking does not work for L2 flows.

- PREC/DSCP to COS marking does not work on L3 flows.

- set mpls experimental imposition command is not supported for L2VPN. Mark to qos-group, which internally marks to EXP value as qos-group marked.

- set cos inner command is not supported on the router.

- Ingress COS marking is supported only with no rewrite type EFPs and rewrite PUSH cases.

- Ingress COS marking is not supported for all remaining POP rewrite types.

- Ingress marking to qos-group, mark the egress COS based on qos-group marked value.

- With L3VPN, Ingress marking to mpls experimental imposition, mark the egress PREC based on mpls exp imposition value.

- With L3VPN, BDI based configuration; classification based on COS is supported only for marking.

- set cos command has no effect unless there is a egress push action to add an additional header at egress. The COS value set by this action will be used in the newly added header as a result of the push rewrite. If there are no push rewrite on the packet, the new COS value will have no effect.

Egress Marking Limitations:

- Egress COS marking is supported. Match on qos-group and set cos command is supported.

- For Egress L3 BDI, match on qos-group and mark to COS is supported.

- Egress MPLS EXP and PREC/DSCP marking are not supported.

Ingress Congestion Avoidance:

- WRED is not supported on ingress interfaces.

Egress Congestion Avoidance:

- WRED is only supported on egress interfaces.

- WRED based on discard-class only supported.

- Class-map match condition must be qos-group and WRED based on discard-class.

- Queuing feature to support WRED in a class such as shape or bandwidth are supported.

- You must apply WRED within a policy-map.

- WRED is not supported in priority queues.

- You can configure a maximum of 2 WRED curves per class.

- You can configure WRED with either the shape or the fair-queue (CBWFQ) commands.

- WRED is supported in the class-default class if there are no other user-defined classes in the policy-map.

- The default value for exponential-weighting-constant is 9.

- The default value for mark-probability is 10.

- You can specify the minimum-threshold and maximum-threshold in terms of bytes or microseconds. Setting threshold values in terms of packets is not supported.

- Aggregate-WRED is not supported.

Legacy Ether Channel QoS:

- Egress QoS policy-map is supported only on a member-link interface and not on a port-channel, port-channel EVC and port-channel TEFP.

- Egress Match EFP policy is not supported on PC member-links.

- Egress Match VLAN policy is not supported on PC member-links.

- A maximum of 8 member-links will be bundled into a port-channel.

- All the other restrictions that are applicable to a regular port interface on the Cisco RSP3 Module are applicable to a port-channel interface and port-channel EVC.

Migration of ASR 900 RSP1 or ASR 900 RSP2 to ASR 900 RSP3-400

The upgrade depends on the boot time, installation of licenses, and copying the configuration. The complete upgrade procedure including replacing interface modules is estimated at approximately 1 hour.

- Boot time for the interface modules :15 minute

- license installation time: 15 minutes.

- Configuration replace and copying configuration: 30 minutes

Before you begin

Ensure supported scale values are set before migration.

Procedure

Step 1	Remove the standby RSP1 or RSP2 module (in high availability HA mode) from the router chassis followed by the active RSP1 or RSP2 module. Skip Step2 if interface module upgrade is *not* required.
Step 2	Replace the IMs with the high-density IMs of the same media type in the same slot. For more information on supported IMs, see Ethernet Interface Modules, on page 1.
Step 3	Insert the RSP3 in slot0 in the router chassis and the second RSP3 in slot1 (HA mode).
Step 4	Wait for the RSP3 in both slots to boot the image and reach the Hot standby state (HA mode).
Step 5	Ensure that the IMs reach the OK state after the reload.

Difference Between RSP1B and RSP3C

The following table shows the differences between RSP1B and RSP3C for Quality of Service.

Table 4: RSP1B versus RSP3C

Feature	RSP1B	RSP3C
Egress Classification	Supported based on the following: • CoS • Inner CoS • Prec • DSCP • EXP • VLAN • Inner VLAN • QoS-Group • Discard-Class	Supported based on the following: • QoS-group

Feature	RSP1B	RSP3C
Ingress Marking	Supported based on the following: • CoS • Prec • DSCP • EXP (Imposition) • EXP (Topmost) • QoS-Group • Discard-Class	Supported based on the following: • CoS (for L2 flows) • Prec (for L3 flows) • DSCP (for L3 flows) • EXP (Imposition for L3 VPN) • EXP (Topmost on LSR) • QoS-Group • Discard-Class (for WRED)
Egress Marking	Supported based on the following: • CoS • Prec • DSCP • EXP (Topmost)	Only egress COS marking for L2 flow is supported with no other egress marking support. TC & DP based EXP marking is supported on L2VPN flows.
Egress Policing	Supported (SRTCM)	Not supported
Bandwidth on Parent Policy	Supported	Not supported
Egress LLQ	Two-level priority + Policing + Shaping	Two-level priority + Shaping
Egress WRED	Supported based on the following: • Cos-based • Discard-class-based • DSCP-based • Precedence-based	Supported based on the following: • Discard-class-based
H-QoS-Egress	• Topmost policy: class-default • Middle policy: match EFP/VLAN/class-default • Lowest policy: match qos-group/cos/prec/dscp	• 1st Level: Class-default • 2nd Level: Multi-efp match • 3rd Level: Match EFP/class-default • 4th Level: Match QoS-Group
MPLS QoS mode: Uniform mode/PIPE mode for L3 VPN	PREC maps to EXP by default on imposition and EXP does not map back to PREC on disposition	PREC maps to EXP by default on imposition and EXP maps back to PREC on disposition

Feature	RSP1B	RSP3C
EXP marking at Imposition	EXP marking at imposition does not alter DSCP value for L3VPN scenario	EXP marking at imposition does overwrite DSCP value for L3VPN scenario
IPv6 QoS on Port Channel	Supported	Not supported
Maximum Ingress Policers	2K per system	32K per system
Egress queues	32K queues per system	48K VOQs per system
TCAM Resources	4K per system	2K per ASIC and 4K per system

Installing the Licenses and Running Configuration

Install the licenses after the image is loaded and the router is in hot standby state. For information on the supported images and licenses, see Cisco IOS XE Software for Cisco ASR 900 Series Aggregation Services Routers Data Sheet.

For information on configuring licensing on the Cisco ASR 900 Series Routers, see Licensing Information.

Procedure

Step 1 Insert the external drive (USB) in the provided RSP slot or access the TFTP server to copy the license information. Copy the license file to the bootflash.

Step 2 Execute the license boot command for the license type. For information on booting licenses using software activation commands, see Configuring the Cisco IOS Software Activation Feature.

Step 3 Install the license using the **license install usb0:** *license-file* command or use the **license install** *tftp://tftp-server-address / location-license-file / license-file*

After installation, "Installing...Feature:*feature -name*...Supported: Supported" message is displayed.

Step 4 Save router configuration and reload the router for activation of licenses.

Step 5 Wait for the router to reach hot standby state (HA mode).

Step 6 Load the saved configuration from the external drive (USB) or the TFTP server. Use the **configure replace usb0:** *modified-config* command or the **configure replace** *tftp://tftp-server-address / location-config / modified-config* command.

Upgrading IMs to High Density IM

Upgrading to High Density Interface Modules

This procedure is for upgrading the existing IMs to the high-density port IM in the same slot. This procedure is applicable to the following

- 8-port 1 Gigabit Ethernet SFP Interface Module to 8-port 1 Gigabit Ethernet SFP Interface Module + 1-port 10 Gigabit Ethernet SFP+ Interface Module

- 8-port 1 Gigabit Ethernet Cu Interface Module to 8-port 1 Gigabit Ethernet RJ45 (Copper) Interface Module + 1-port 10 Gigabit Ethernet SFP Interface Module

- 1-port 10 Gigabit Ethernet Interface Module to 2-port 10 Gigabit Ethernet Interface Module

- 8-port 10 Gigabit Ethernet Interface Module (8X10 GE)

- 1-port 100 Gigabit Ethernet Interface Module (1X100 GE)

- 2-port 40 Gigabit Ethernet QSFP Interface Module (2X40 GE)

Before you begin

Defaulting of interfaces is required before upgrading of inteface modules (IM)s. If defaulting is not performed, the interfaces may get corrupted and reload of router is required.

Procedure

Step 1   Save the running configuration to the router bootflash or external drive (USB) or TFTP server.

Step 2   Perform a default of all the interfaces on the IM using the **hw-module subslot** *bay* **default** command. For more information, see Cisco IOS Interface and Hardware Component Command Reference.

Example:

```
Router# hw-module subslot 0/1 default

Proceed with setting all interfaces as default for the module? [confirm]
%Setting all interfaces in 0/1 to default state
Interface GigabitEthernet0/1/0 set to default configuration
Interface GigabitEthernet0/1/1 set to default configuration
Interface GigabitEthernet0/1/2 set to default configuration
Interface GigabitEthernet0/1/3 set to default configuration
Interface GigabitEthernet0/1/4 set to default configuration
Interface GigabitEthernet0/1/5 set to default configuration
Interface GigabitEthernet0/1/6 set to default configuration
Interface GigabitEthernet0/1/7 set to default configuration
Interface TenGigabitEthernet0/1/8 set to default configuration
Router#
*Jun  3 19:27:52.302: %TRANSCEIVER-6-REMOVED: SIP0: iomd:  Transceiver module removed from
 TenGigabitEthernet0/1/8
*Jun  3 19:27:52.589: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Jun  3 19:27:52.616: %SPA_OIR-6-OFFLINECARD: SPA (A900-IMA8S1Z) offline in subslot 0/1
*Jun  3 19:27:53.985: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/4/8, changed state to
down
*Jun  3 19:27:54.686: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/4/8,
 changed state to down
*Jun  3 19:28:16.696: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*Jun  3 19:28:22.000: %ASR900IM-3-DIFF_IM_INSERTED:  Different IM type inserted  -
A900-IMA1X[0/1] in bay 1
*Jun  3 19:28:41.205: %SPA_OIR-6-ONLINECARD: SPA (A900-IMA1X) online in subslot 0/1
*Jun  3 19:28:41.207: %TRANSCEIVER-6-INSERTED: SIP0: iomd:  transceiver module inserted in
 TenGigabitEthernet0/1/0
```

Press **enter** for confirmation.

Console messages are displayed for the interfaces. Ensure that the **interface *interface-name* set to default configuration** message is displayed before performing Step 3.

Step 3 Remove the IM from the bay and insert the new IM. See IM slot compatibility matrix for supported slots before inserting the new IM.

The default configuration is displayed.

Note If the default configuration is *not* displayed, the IM may enter the Out of Service state. To recover the IM, insert the old IM, enter the default interface configuration and then reinsert the new IM. For more information, see Cisco ASR 903 Series Aggregation Services Router Hardware Installation Guide .

Step 4 Copy the saved running configuration from the bootflash or the external drive (USB) or TFTP server. Rename the interface names in the configuration file.

Step 5 Configure the additional or new 10 Gigabit Ethernet port.

Upgrading the 1 Gigabit Ethernet Interface Modules to High Density 2-port 40 Gigabit Ethernet QSFP Interface Module

This procedure is for upgrading the existing IMs to the high-density port IM in the same slot. This procedure is applicable to the following

- 8X1 Gigabit Ethernet SFP IM to 2-port 40 Gigabit Ethernet QSFP IM

- 8x1 Gigabit Ethernet Cu IM to 2-port 40 Gigabit Ethernet QSFP IM

Before you begin

Defaulting of interfaces is required before upgrading of interface modules (IM). If defaulting is not performed, the interfaces may get corrupted and reload of router is required.

Procedure

Step 1 Save the running configuration to the router bootflash or external drive (USB) or TFTP server. See IM slot compatibility matrix for supported slots before inserting the new IM.

Step 2 Perform a default of all the interfaces on the IM using the **hw-module subslot** *bay* **default** command. For more information, see Cisco IOS Interface and Hardware Component Command Reference.

Example:

```
Router# hw-module subslot 0/1 default

Proceed with setting all interfaces as default for the module? [confirm]
%Setting all interfaces in 0/1 to default state
Interface GigabitEthernet0/1/0 set to default configuration
Interface GigabitEthernet0/1/1 set to default configuration
Interface GigabitEthernet0/1/2 set to default configuration
Interface GigabitEthernet0/1/3 set to default configuration
Interface GigabitEthernet0/1/4 set to default configuration
Interface GigabitEthernet0/1/5 set to default configuration
Interface GigabitEthernet0/1/6 set to default configuration
```

```
Interface GigabitEthernet0/1/7 set to default configuration
Interface TenGigabitEthernet0/1/8 set to default configuration
Router#
*Jun  3 19:27:52.302: %TRANSCEIVER-6-REMOVED: SIP0: iomd:  Transceiver module removed from
 TenGigabitEthernet0/1/8
*Jun  3 19:27:52.589: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Jun  3 19:27:52.616: %SPA_OIR-6-OFFLINECARD: SPA (A900-IMA8S1Z) offline in subslot 0/1
*Jun  3 19:27:53.985: %LINK-3-UPDOWN: Interface TenGigabitEthernet0/4/8, changed state to
down
*Jun  3 19:27:54.686: %LINEPROTO-5-UPDOWN: Line protocol on Interface TenGigabitEthernet0/4/8,
 changed state to down
*Jun  3 19:28:16.696: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*Jun  3 19:28:22.000: %ASR900IM-3-DIFF_IM_INSERTED:  Different IM type inserted  -
A900-IMA1X[0/1] in bay 1
*Jun  3 19:28:41.205: %SPA_OIR-6-ONLINECARD: SPA (A900-IMA1X) online in subslot 0/1
*Jun  3 19:28:41.207: %TRANSCEIVER-6-INSERTED: SIP0: iomd:  transceiver module inserted in
 TenGigabitEthernet0/1/0
```

Press **enter** for confirmation.

Console messages are displayed for the interfaces. Ensure that the **interface** *interface-name* **set to default configuration** message is displayed before performing Step 3.

Step 3 Remove the IM from the bay and insert the 2-port 40 Gigabit Ethernet QSFP IM.

The default configuration is displayed

Note If the default configuration is *not* displayed, the IM may enter the Out of Service state. To recover the IM, insert the old IM, enter the default interface configuration and then reinsert the new SFP IM. For more information, see Cisco ASR 903 Series Aggregation Services Router Hardware Installation Guide .

Step 4 Copy the saved running configuration from the bootflash or the external drive (USB) or TFTP server. Rename the interface names in the configuration file.

Step 5 Configure the ports on the IM.

Additional References

Related Documents

Related Topic	Document Title
Cisco ASR 903 Series Aggregation Services Router Hardware Installation Guide	http://www.cisco.com/c/en/us/td/docs/wireless/asr_900/hardware/installation/ASR903-HW-install.html
Licensing Information	http://www.cisco.com/c/en/us/support/routers/asr-903-series-aggregation-services-routers/products-licensing-information-listing.html
Data Sheets	http://www.cisco.com/c/en/us/products/routers/asr-903-series-aggregation-services-routers/datasheet-listing.html

Related Topic	Document Title
Configuration Guides	http://www.cisco.com/c/en/us/support/routers/ asr-903-series-aggregation-services-routers/ products-installation-and-configuration-guides-list.html
Cisco IOS master command list	Cisco IOS Master Command List , All Releases

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html