Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router for Cisco IOS Release 12.4(20)MRA1

September 23, 2010

OL-20878-01

These release notes are for the Cisco MWR Mobile Wireless Edge Router for Cisco IOS Release 12.4(20)MRA1. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode.

The Cisco MWR 2941 includes the following models:

- Cisco MWR 2941-DC
- Cisco MWR 2941-DC-A

For a list of the software caveats that apply to Cisco IOS Release 12.4(20)MRA1, see the "Caveats in Cisco IOS Release 12.4(20)MR2" section on page 28.

To review all Cisco MWR 2941 release notes, go to:

http://www.cisco.com/en/US/products/ps9395/prod_release_notes_list.html

To review release notes for the Cisco IOS Software Release 12.4T, go to:

http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

Contents

This document contains the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Introduction

The Cisco MWR 2941-DC Mobile Wireless Router is a cell-site gateway specifically designed to optimize, aggregate, and backhaul mixed-generation RAN traffic. The Cisco MWR 2941-DC optimizes cell-site voice, data, and signaling traffic as part of the Cisco Unified RAN Backhaul solution for reliable transport across any available backhaul networks including E1/T1, ATM, DSL, Carrier Ethernet, cable, microwave, WiMAX, and satellite. Custom designed for the cell site, the Cisco MWR 2941-DC features a small form factor, extended operating temperature, and cell-site DC input voltages. It comprises a high-performance host processor joined with a powerful network processing engine, precise clocking and synchronization, and feature-rich Cisco IOS® Software tailored for RAN backhaul applications.

Cisco IOS Release 12.4(20)MRA1 for the Cisco MWR 2941 is a specific technology early deployment release, and is an upgrade path for Release 12.4(19)MR3, which introduced a variety of RAN solution features including PWE3 Circuit Emulation Service over Packet Switched Networks (CESoPSN), GSM Abis Optimization over IP, IEEE 1588–2008 Timing over Packet (ToP), Adaptive Clock Recovery (ACR), and Synchronous Ethernet.

System Requirements

The Cisco MWR 2941 router requires the following system configuration for the Cisco IOS Release 12.4(20)MRA1 software.

Memory Requirements

Table 1 lists the required memory for using this software.

Table 1 Cisco IOS Release 12.4(20)MRA1 Memory Requirements

Platform	Feature Set	Software Image	Recommended Flash Memory	Recommended DRAM Memory	Runs From
Cisco MWR 2941 Mobile Wireless Edge Router	RAN Optimization	mwr2941-iprank9-mz .124-20.MRA1.bin	128 MB	512 MB	RAM
Cisco MWR 2941 Mobile Wireless Edge Router	RAN Optimization	mwr2941-ipran-mz .124-20.MRA1.bin	128 MB	512 MB	RAM

Determining the Software Version

To determine the image and version of Cisco IOS software running on your Cisco MWR 2941 router, log in to the router and enter the **show version** EXEC command:

```
Router> show version
     Cisco Internetwork Operating System Software
    IOS (tm) 2900 Software (MWR2941-IPRANK9-MZ), Version 12.4(20)MRA, EARLY DEPLOYMENT
    RELEASE SOFTWARE (fcl)
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to the *Software Installation and Upgrade Procedures* at:

http://www.cisco.com/web/psa/products/index.html

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco MWR 2941 router.

New Hardware Features in Release 12.4(20)MRA1

There are no new hardware features in Cisco IOS Release 12.4(20)MRA1.

New Software Features in Release 12.4(20)MRA1

There are no new software features in Cisco IOS Release 12.4(20)MRA1.

New Hardware Features in Release 12.4(20)MRA

There are no new hardware features in Cisco IOS Release 12.4(20)MRA.

New Software Features in Release 12.4(20)MRA

Cisco IOS Release 12.4(20)MRA introduces support for Network Timing Reference (NTR). NTR is a highly accurate method of distributing frequency and clocking over DSL networks; it allows the Cisco MWR 2941 to exchange frequency and clocking information over a DSL connection. This release introduces the following command-line interface (CLI) changes in order to support NTR.

- **shdsl ntr enable** —Enables Network Timing Reference (NTR) on a specified DSL wire.
- **network-clock-select**—Release 12.4(20)MRA1 modifies this command to allow an SHDSL controller as a network clock source.

- **show network-clocks**—Release 12.4(20)MRA1 modifies this command to include NTR clocking information.
- **show controller**—Release 12.4(20)MRA1 modifies this command to include NTR clocking information.

Sample Configurations

The following section contains a sample configuration for the Release 12.4(20)MRA1 software features.

Network Timing Reference

The following partial sample configuration uses Network Timing Reference (NTR).

```
!
controller E1 0/0
 clock source line
!
controller SHDSL 1/0
 termination cpe
  dsl-group 0 pairs  0, 1
  shdsl annex B
  shdsl ntr enable 0, 1
  shdsl rate 4608
 !
 dsl-group 1 pairs  2, 3
  shdsl annex B
  shdsl rate 4608
 !
network-clock-select hold-timeout 600
network-clock-select mode nonrevert
network-clock-select 1 SHDSL 1/0.0
network-clock-select 2 SHDSL 1/0.1
network-clock-select 3 E1 0/0
!
```

For more information about how to configure NTR, see the Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide, Release 12.4(20)MR

New Hardware Features in Release 12.4(20)MR2

Release 12.4(20)MR2 introduces support for the Cisco MWR 2941-DC-A router.

Note The Cisco MWR 2941-DC and 2941-DC-A support the same features with the exception of commands related to the 1PPS, 10Mhz, 2.048Mhz, and 1.544Mhz timing ports included on the MWR 2941-DC-A. For more information about these features, see New Software Features in Release 12.4(20)MR2.

New Software Features in Release 12.4(20)MR2

Release 12.4(20)MR2 introduces the following new software features:

- PPP over DSL—Release 12.4(20)MR2 introduces support for point-to-point protocol (PPP) over ADSL and SHDSL connections.

- MLPPP over ADSL—Release 12.4(20)MR2 introduces support for MLPPP load sharing across multiple ADSL links. Release 12.4(20)MR2 does not support MLPPP load sharing across SHDSL links.
- Limited DSL QoS support—Release 12.4(20)MR2 supports the following QoS features:
  - Matching based on DSCP value on egress SHDSL interfaces
  - Priority percent queuing on egress SHDSL interfaces
  - ATM Class of Service (CoS) traffic classes on SHDSL interfaces except for UBR
- Timing port commands—Release 12.4(20)MR2 supports the following commands for the 1PPS, 10Mhz, 2.048Mhz, and 1.544Mhz timing ports that are included on the MWR 2941-DC-A.

Note The following commands are only supported on the Cisco MWR 2941-DC-A as the Cisco MWR 2941-DC does not have these timing ports.

  - **ptp input**—Enables PTP input clocking using the 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or time of day messages using the 1PPS interface.
  - **ptp output**—Enables PTP output clocking using the 1.544Mhz, 2.048Mhz, or 10Mhz timing interface or time of day messages using the 1PPS interface.
  - **network-clock-select**—This command is modified to include timing sources using the 10Mhz, 2.048Mhz, or 1.544Mhz.
  - **ptp tod**—Configures the time of day message format used by the 1PPS interface.
  - **ptp update-calendar**—Configures the router to periodically update the system calendar to match the PTP clock.

Sample Configurations

The following sections provide partial sample configurations for the features introduced in release 12.4(20)MR2.

- PPP over ADSL
- PPP over SHDSL
- MLPPP over ADSL

PPP over ADSL

```
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl bitswap both
 hold-queue 224 in
 pvc 1/150
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface ATM2/0
 no ip address
 load-interval 30
```

```
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl bitswap both
 hold-queue 224 in
 pvc 1/151
  encapsulation aal5mux ppp dialer
  dialer pool-member 2
 !
!
interface Dialer0
 ip address 30.0.0.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname ppp-client
 ppp chap password 0 mypassword
!
interface Dialer1
 ip address 40.0.0.2 255.255.255.0
 encapsulation ppp
 dialer pool 2
 dialer-group 2
 ppp authentication chap callin
 ppp chap hostname ppp-client
 ppp chap password 0 mypassword
!
dialer-list 1 protocol ip permit
dialer-list 2 protocol ip permit
!
```

PPP over SHDSL

```
!
controller SHDSL 1/0
 termination cpe
 dsl-group 0 pairs  0, 1 m-pair
  shdsl annex B
  shdsl rate 4608
 !
 dsl-group 1 pairs  2, 3 m-pair
  shdsl annex B
  shdsl rate 4608
 !
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
!
interface ATM1/0.1 point-to-point
 ip address 10.1.1.1 255.255.255.0
 pvc 0/11
  protocol ip 10.1.1.2 broadcast
 !
!
interface ATM1/1
 no ip address
 load-interval 30
 no atm ilmi-keepalive
!
```

```
interface ATM1/1.1 point-to-point
 pvc 1/150
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface Dialer0
 ip address 30.0.0.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer persistent
 dialer-group 1
 no keepalive
 ppp authentication chap callin
 ppp chap hostname ppp-client
 ppp chap password 0 mypassword
!

QoS on DSL connection
!
controller SHDSL 1/0
 termination cpe
 dsl-group 0 pairs  0, 1, 2, 3 m-pair
  shdsl annex F-G coding 32-TCPAM
  shdsl rate 16384
 !
!
class-map match-all d2
 match dscp 2
class-map match-all d3
 match dscp 3
!
policy-map llq
 class d2
    priority percent 5
 class d3
    priority percent 94
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 service-policy output llq
!
interface ATM1/0.1 point-to-point
 pvc 1/150
  cbr 16384
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface Dialer0
 ip address 30.0.0.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer idle-timeout 0
 dialer persistent
 dialer-group 1
 no keepalive
 ppp authentication chap callin
 ppp chap hostname ppp-client
 ppp chap password 0 mypassword
!
```

```
dialer-list 1 protocol ip permit
```

MLPPP over ADSL

```
!
interface ATM1/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl bitswap both
 hold-queue 224 in
 pvc 1/150
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface ATM2/0
 no ip address
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
 dsl bitswap both
 hold-queue 224 in
 pvc 1/151
  encapsulation aal5mux ppp dialer
  dialer pool-member 1
 !
!
interface Dialer0
 ip address 30.0.0.2 255.255.255.0
 encapsulation ppp
 dialer pool 1
 dialer-group 1
 ppp authentication chap callin
 ppp chap hostname ppp-client
 ppp chap password 0 mypassword
 ppp multilink
!
dialer-list 2 protocol ip permit
!
```

For more information about how to configure PPP over DSL and MLPPP over ADSL, see the Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide, Release 12.4(20)MR or the Cisco IOS Dial Technologies Command Reference.

New Hardware Features in Release 12.4(20)MR1

Release 12.4(20)MR1 of the Cisco IOS Software has the following new hardware features:

- Release 12.4(20)MR1 introduces support for these HWICs:
  - HWIC-1ADSL
  - HWIC-1ADSL-I
- Release 12.4(20)MR1 introduces support for the SFP-GE-T module.

New Software Features in Release 12.4(20)MR1

There are no new software features in Release 12.4(20)MR1.

New Hardware Features in Release 12.4(20)MR

Release 12.4(20)MR of the Cisco IOS Software has the following new hardware features:

- Release 12.4(20)MR introduces support for the following interface cards:
  - HWIC-4SHDSL
  - HWIC-1GE-SFP
  - HWIC-D-9ESW
- Release 12.4(20)MR introduces support for the following SFP modules:
  - CWDM-SFP-1470
  - CWDM-SFP-1490
  - CWDM-SFP-1510
  - CWDM-SFP-1530
  - CWDM-SFP-1550
  - CWDM-SFP-1570
  - CWDM-SFP-1590
  - CWDM-SFP-1610
  - DWDM-SFP-4612
  - DWDM-SFP-4692
  - DWDM-SFP-4772
  - DWDM-SFP-4851
  - DWDM-SFP-5012
  - DWDM-SFP-5092
  - DWDM-SFP-5172
  - DWDM-SFP-5252
  - DWDM-SFP-5413
  - DWDM-SFP-5494
  - DWDM-SFP-5575
  - DWDM-SFP-5655
  - DWDM-SFP-5817
  - DWDM-SFP-5898
  - DWDM-SFP-5979
  - DWDM-SFP-6061
  - GLC-ZX-SM-RGD
  - GLC-LX-SM-RGD

- GLC-SX-MM-RGD
- SFP-GE-L
- SFP-GE-S
- SFP-GE-Z

New Software Features in Release 12.4(20)MR

The following software features are supported in Release 12.4(20)MR of the Cisco IOS software:

- Ethernet over MPLS (EoMPLS) pseudowires in VLAN mode—This release introduces support for EoMPLS pseudowires for VLANs.
- PTP redundancy—This release introduces support for PTP redundancy using multicast as defined in the IEEE 1588-2008 standard. This feature allows the Cisco MWR 2941 to use multicast routing to establish redundant paths between an external PTP client and one or more PTP multicast master clocks.

Note The Cisco MWR 2941 does not offer general support for multicast.

- Slave mode unicast delay-request while in PTP multicast mode—Enables the router to send PTP Delay_Req messages in unicast fashion while in PTP multicast slave mode. This setting eliminates unnecessary traffic generated by multicast messages that are dropped by all recipients except one.
- BGP routing
- IS–IS routing
- BFD for BGP and IS-IS routing protocols
- Layer 3 VPNs— Layer 3 VPNs provide an alternative to traditional VPNs that is easier to manage and expand than conventional VPNs through use of layer 3 communication protocols and a peer architecture.
- Generic Routing Encapsulation (GRE)—GRE is a tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. GRE tunneling allows you to transport a pseudowire over an IP backhaul network when MPLS routing is not available between a cell site (BTS or Node-B) and an aggregation point (BSC or RNC).
- GRE Offload—The Cisco MWR 2941 offloads GRE handling to the network processor for improved performance.
- Quality of Service (QoS) support—This release introduces support for QoS features on some interfaces. For more information, see the *Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide, Release 12.4(20)MR.*
- Cisco Networking Services (CNS)—CNS is a collection of services that can provide remote configuration of Cisco IOS networking devices and remote execution of some command-line interface (CLI) commands. CNS allows a Cisco MWR 2941 deployed and powered on in the field to automatically download its configuration. The Cisco MWR 2941 supports CNS on all Gigabit Ethernet interfaces except HWIC interface module interfaces.

- Non-contiguous GSM timeslots—Release 12.4(20)MR provides support for non-contiguous timeslots in a GSM channel group. You can configure timeslots in a GSM channel group with gaps of up to 15 timeslots. You can use the remaining timeslots to configure a tdm-group, which is a typical configuration for an Ater and SS7 environment. The Cisco MWR 2941 does not support other options such as channel-groups in a gap between GSM time slots.
- ATM Class of Service (CoS) commands—Release 12.4(20)MR supports the following ATM CoS commands:
  - **ubr+**—Allows you to configure an unspecified bit rate (UBR) quality of service (QoS) and specify the output peak cell rate and output minimum guaranteed cell rate for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), virtual circuit (VC) class, or VC bundle member.
  - **vbr-nrt**—Allows you to configure the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specify output peak cell rate (PCR), output sustainable cell rate (SCR), and output maximum burst cell size for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), VC class, or VC bundle member.
  - **vbr-rt**—Allows you to configure the real-time variable bit rate (VBR) for VoATM voice connections.
- Larger MTU size—This release introduces support for MTU sizes of up to 4470 bytes on switched virtual interfaces (SVIs). The default MTU size is 1500 bytes, and the maximum MTU size supported over MLPPP links is 1536 bytes.
- Distributed Multilink Point-to-Point Protocol (dMLPPP)—dMLPPP allows you to combine T1 or E1 connections into a bundle that has the combined bandwidth of all of the connections in the bundle, providing improved capacity and CPU utilization over MLPPP.The dMLPPP offload feature improves the performance for traffic in dMLPPP applications such as PWE3 over MLPPP, IP over MLPPP, and GSMmux over MLPPP by shifting processing of this traffic from the main CPU to the network processor. dMLPPP also uses interleaving to improve processing of delay-sensitive packets.The MWR 2941 supports dMLPPP for up to 16 T1/E1 links per MLPPP bundle and up to 12 bundles per router.
- Multiclass MLPPP—The MWR 2941 implementation of dMLPPP also supports Multiclass MLPPP. Multiclass MLPPP is an extension to MLPPP functionality that allows you to divide traffic passing over a multilink bundle into several independently sequenced streams or classes. Each multiclass MLPPP class has a unique sequence number, and the receiving network peer processes each stream independently. The multiclass MLPPP standard is defined in RFC 2686.
- Distributed IP Header Compression (dIPHC)—dIPHC allows the MWR 2941 to compress IP packet headers for more efficient use of bandwidth. Release 12.4(20)MR improves dIPHC performance by shifting processing from the main CPU to the network processor. The MWR 2941 supports dIPHC for GSM-Abis traffic and decompression for TCP and non-TCP packet streams as defined by RFC 2507. The MWR 2941 supports dIPHC offload for up to 24 E1 or T1 connections.

Note The Cisco MWR 2941 does not support some PPP and MLPPP options when the bundle is offloaded to the network processor. For more information, see Limitations and Restrictions or the *Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide, Release 12.4(20)MR*.

- Channel-Associated Signaling (CAS)—This release introduces support for CAS signaling, a form of in-band digital signaling for T1 and E1 connections. CAS transmits signaling information inside each DS0 channel rather than in a separate channel and can also be described as robbed bit signaling. The Cisco MWR 2941 supports CAS for SAToP and CESoPSN pseudowires and is compliant with the ITU G.704 standard for CRC-4 and non-CRC-4 formats and the ANSI T1.403 standard for SF and ESF frame formats.

New Hardware Features in Release 12.4(19)MR3

There are no new hardware features in Release 12.4(19)MR3 of the Cisco IOS software.

New Software Features in Release 12.4(19)MR3

The following software features are supported in Release 12.4(19)MR3 of the Cisco IOS software:

- Release 12.4(19)MR3 introduces support for IS-IS routing. For instructions on how to configure IS-IS, see the Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4T.

New Hardware Features in Release 12.4(19)MR2

There are no new hardware features in Release 12.4(19)MR2 of the Cisco IOS software.

New Software Features in Release 12.4(19)MR2

The following features are supported in release 12.4(19)MR2 of the Cisco IOS software:

- PWE3 Circuit Emulation over PSN (Packet Switched Network)—Allows you to create pseudowires (PWs) that emulate unstructured and structured T1s and E1s over an MPLS infrastructure, down to NxDS0 circuits. The Cisco MWR 2941 supports the following PWE3 standards:
  - Structure-agnostic TDM over Packet (SAToP)—Encapsulates TDM bit-streams (T1, E1, T3, E3) as PWs over PSNs; the feature is compliant with RFC 4553.
  - Structure-aware TDM Circuit Emulation Service over Packet-Switched Network (CESoPSN)—Encapsulates structured (NxDS0) TDM signals as PWs over PSNs; the feature is compliant with RFC 5086.
  - Transportation of Service Using ATM over MPLS—Uses an Asynchronous Transfer Mode (ATM) PW to carry cells over an MPLS network; the feature is compliant with RFCs 4717 and 4816.
- GSM Abis Optimization over IP Implementation—Allows the Cisco MWR 2941 to optimize GSM voice and data traffic and maximize effective utilization of E1/T1 backhaul connections.
- Clocking features—Cisco IOS Release 12.4(19)MR2 introduces several new clocking features that are supported on the ASM-M2900-TOP daughter card, also known as the RTM Module. The RTM module supports the following new clocking features:
  - Precision Time Protocol (PTP)—Clocking and clock recovery based on the IEEE 1588-2008 standard; allows the Cisco MWR 2941 router to receive clocking from another PTP-enabled device or provide clocking to a PTP-enabled device.

    This feature introduces a variety of new global commands: **ptp domain**, **ptp mode**, **ptp priority1**, and **ptp priority2**; the following interface commands: **ptp announce**, **ptp clock-destination**, **ptp clock-source**, **ptp delay-req**, **ptp enable**, **ptp master**, **ptp slave**, and **ptp sync**; and the following show commands: **show ptp clock**, **show ptp foreign-master-record**, **show ptp parent**, **show ptp port**, and **show ptp time-property**.
  - Adaptive Clock Recovery (ACR)—Pseudowire-based Timing over Packet (TOP) that allows the MWR 2941 to use in-band or out-of-band clocking on a virtual or regular TDM pseudowire interface. ACR allows the Cisco MWR 2941 to recover clocking from the headers of a packet

stream and is compliant with the G.823 and G.824 standards. You can use the **recovered-clock slave** command to configure out-of-band clock recovery and the **recovered-clock recovered adaptive** command to configure adaptive clock recovery.

- Synchronous Ethernet—Allows the network to transport frequency and time information over Ethernet. You can use the **network-clock-select** command to configure synchronous Ethernet.

Note The RTM module is not required to use Synchronous Ethernet.

- ATM—This release includes ATM support with AAL0 and AAL5 encapsulation, F4 and F5 OAM (Operation, Administration, and Maintenance) monitoring, and Virtual Path (VP) shaping.
- IMA—This feature allows you to connect one or more interfaces to an ATM network using Inverse Multiplexing ATM (IMA). You can define IMA groups that can contain up to 8 bundles, with up to 24 links per bundle.
- IP Header Compression over PPP—This feature introduces support for IP header compression over PPP that is compliant with RFCs 2507, 2508, and 3544.
- Distributed Multilink PPP—Release 12.4(19)MR2 supports multilink PPP that is compliant with the RFC 1990 specification.
- Flexlink—Backup switchport interfaces using the **switchport backup interface** command.
- IEEE 802.1d Ethernet Switching
- IEEE 802.1q VLANS
- VLAN Trunking Protocol (VTP)
- Per-VLAN Spanning Tree (PVST)+
- BITS Clocking
- Open Shortest Path First (OSPF)
- Bi-Directional Forwarding Detection (BFD) for OSPF
- VPN Routing and Forwarding (VRF) Lite for OSPF
- ATM cell switching
- Label Distribution Protocol (LDP)

Limitations and Restrictions

Caution The Cisco MWR 2941 router does not support online insertion and removal (OIR) of WAN interface cards. Any attempt to perform OIR on a card in a powered-on router might cause damage to the card.

Cisco IOS Release 12.4(20)MRA1 for the Cisco MWR 2941 router has the following limitations and restrictions:

- UMTS Iub Optimization not supported—Release 12.4(20)MRA1 does not support UMTS Iub optimization.
- L2TP not supported—The MWR 2941 currently does not support L2TP.
- PTP Boundary mode not supported—This release does not support PTP Boundary mode.
- PTP Transparent mode not supported—This release does not support PTP Transparent mode.

- Multicast used for PTP redundancy only—This release provides support for multicast in order to establish PTP redundancy; the Cisco MWR 2941 does not support multicast for other uses.
- Channel group limitations on GSM-Abis interfaces—Only one channel group per E1/T1 is supported on GSM-Abis interfaces. You can configure 1 GSM group with TDM groups in order to use drop and insert on the same controller.

  You can use gaps between non-contiguous GSM timeslots to configure a tdm-group, which is a typical configuration for an Ater and SS7 environment. However, the Cisco MWR 2941 does not support other options such as channel-groups in a gap between GSM time slots.
- Out-of-band master mode not supported—This release does not support out-of-band master mode for Timing over Packet/adaptive clock recovery. If your network design requires out-of-band master clocking, you can use the CEoPs SPA on the 7600 router for this purpose.
- ACR out-of-band payload limitation—The MWR 2941 only supports the payload-size values 486 (625 packets per second) or 243 (1250 packets per second) for out-of-band clock recovery.
- T1 SAToP is not supported on the HWIC-4T1/E1.
- Limited OAM support—ATM OAM (Operation, Administration, and Maintenance) is not supported on the short haul side of the Cisco MWR 2941.
- The Cisco MWR 2941 does not support the **mpls traffic-eng tunnels** command at the global or interface level.
- QoS Limitations—The Cisco MWR 2941 provides limited QoS support. For more information, see the *Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide, Release 12.4(20)MR*.
- IPHC compression and decompression limitations—The MWR 2941 only supports dIPHC compression for GSM-Abis traffic and decompression for TCP and non-TCP packet streams as defined by RFC 2507. If you require IPHC for traffic flows other than GSM-Abis traffic, contact Cisco support for assistance.
- The Cisco MWR 2941 does not support the following options on offloaded dMLPPP bundles:
  - **ppp multilink idle-link**
  - **ppp multilink queue depth**
  - **ppp multilink fragment maximum**
  - **ppp multilink slippage**
  - **ppp timeout multilink lost-fragment**

Note If you have a bundle that requires the use of these options, contact Cisco support for assistance.

  For more information about configuring dMLPPP, see the *Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide*.
- MPLS pseudowire ping not supported—This release does not support the **ping mpls pseudowire** command. We recommend that you use the **ping mpls ipv4** command for operation and maintenance of MPLS connections.
- IPSec over GRE not supported—The Cisco MWR 2941 does not support IPSec over GRE.
- CAS limitations—The Cisco MWR 2941 implementation of CAS has the following limitations:
  - CAS is not supported on T1 and E1 HWICs.
  - When configuring a CESoPSN pseudowire to use CAS, you must configure the controller to use CAS signalling prior to creating a cem group, tdm group, or channel group. Otherwise the Cisco MWR 2941 rejects the **mode cas** command.

  - CAS is only supported on pseudowire connections between two Cisco MWR 2941 routers; the 7600 router does not currently support CAS.
- PTP only supported on Gigabit Ethernet interfaces—The Cisco MWR 2941 only supports PTP traffic on onboard Gigabit Ethernet interfaces.
- PTP Master clocking not supported—Release 12.4(20)MRA1 contains commands to configure the Cisco MWR 2941 as a Master clock. These commands are intended for trial use only and are not designed for use in a production network.
- PTP clocking over Virtual Routing and Forwarding (VRF) is not supported.
- The HWIC-D-9ESW card has the following limitations:
  - The maximum throughput for all interfaces on the card is 100 Mbps due to the upper limit of the stacking port.
  - Ethernet over MPLS (EoMPLS) is not supported.
  - Inter-chassis stacking is not supported.
  - If you install the HWIC-D-9ESW card, the operating temperature range is 32 to 104°F (0C to 40C).
  - PTP, pseudowire-based clocking, or synchronous Ethernet are not supported.
- The HWIC-1GE-SFP has the following limitations:
  - PTP, pseudowire-based clocking, and synchronous Ethernet are not supported.
  - The HWIC-1GE-SFP functions as a layer 3 routed port only; it does not function as a layer 2 switch. Interface performance is subject to the limitations of the host processor.
  - The performance of the HWIC-1GE-SFP is significantly below that of the onboard GigabitEthernet interfaces.

Supported Hardware

Release 12.4(20)MRA1 supports the following interface cards:

- HWIC-4T1/E1
- HWIC-4SHDSL
- HWIC-1GE-SFP
- HWIC-D-9ESW
- HWIC-1ADSL
- HWIC-1ADSL-I

Release 12.4(20)MRA1 supports the following SFP modules:

- CWDM-SFP-1470
- CWDM-SFP-1490
- CWDM-SFP-1510
- CWDM-SFP-1530
- CWDM-SFP-1550
- CWDM-SFP-1570
- CWDM-SFP-1590

- CWDM-SFP-1610
- DWDM-SFP-4612
- DWDM-SFP-4692
- DWDM-SFP-4772
- DWDM-SFP-4851
- DWDM-SFP-5012
- DWDM-SFP-5092
- DWDM-SFP-5172
- DWDM-SFP-5252
- DWDM-SFP-5413
- DWDM-SFP-5494
- DWDM-SFP-5575
- DWDM-SFP-5655
- DWDM-SFP-5817
- DWDM-SFP-5898
- DWDM-SFP-5979
- DWDM-SFP-6061
- GLC-BX-D
- GLC-BX-U
- GLC-ZX-SM-RGD
- GLC-LX-SM-RGD
- GLC-SX-MM-RGD
- SFP-GE-L
- SFP-GE-S
- SFP-GE-T
- SFP-GE-Z

Other hardware interfaces are not supported.

Caution The Cisco MWR 2941 router does not support online insertion and removal (OIR) of WAN interface cards. Any attempt to perform OIR on a card in a powered-on router might cause damage to the card.

For instructions on how to install HWICs and SFPs, see the documentation included with the product. For information about how to configure HWICs and SFPs, see the *Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide, Release 12.4(20)MR.*

Supported MIBs

The Cisco MWR 2941 router supports the following MIBs:

- CISCO-ACCESS-ENVMON-MIB
- CISCO-CDP-MIB
- CISCO-CONFIG-COPY-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-EXT-MIB
- CISCO-ENTITY-FRU-CONTROL-MIB
- CISCO-ENTITY-SENSOR-MIB
- CISCO-ENTITY-VENDORTYPE-OID-MIB
- CISCO-ENVMON-MIB
- CISCO-FLASH-MIB
- CISCO-IETF-PW-MIB
- CISCO-IETF-PW-TC-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IMAGE-MIB
- CISCO-IP-RAN-BACKHAUL-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-RTTMON-MIB
- CISCO-SMI
- CISCO-SYSLOG-MIB
- CISCO-TC
- CISCO-VTP-MIB
- ENTITY-MIB
- HCNUM-TC
- IANAifType-MIB
- IF-MIB
- IMA-MIB
- INET-ADDRESS-MIB
- MPLS-VPN-MIB
- OLD-CISCO-CHASSIS-MIB
- OLD-CISCO-INTERFACES-MIB
- OLD-CISCO-SYS-MIB
- OLD-CISCO-TS-MIB
- PerfHist-TC-MIB
- RFC1213-MIB
- RMON2-MIB
- RMON-MIB
- SNMP-FRAMEWORK-MIB
- SNMP-TARGET-MIB
- SNMPv2-CONF
- SNMPv2-MIB
- SNMPv2-SMI
- SNMPv2-TC

Caveats

This section documents the open and resolved caveats for the Cisco MWR 2941 router running Cisco IOS Release 12.4(19)MR2 and later.

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels. Only select severity 3 caveats are listed.

For information on caveats in Cisco IOS Software Releases 12.4T, see

http://www.cisco.com/en/US/products/ps6441/prod_release_notes_list.html

Note If you have an account with Cisco.com, you can use the Bug Toolkit to find caveats of any severity for any release. To reach the Bug Toolkit, log in to Cisco.com and click the **Support** tab and select **Support** from the drop-down menu. Under Frequently Used Resources, click **Bug Toolkit**. You must then log in. Another option is to go directly to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

The following sections document the opened and resolved caveats by Cisco IOS release:

Caveats in Cisco IOS Release 12.4(20)MRA1

The following sections describe the caveats in Cisco IOS Release 12.4(20)MRA1.

Open Caveats

This section lists the open caveats in Cisco IOS Release 12.4(20)MRA1.

- CSCtd58271

  Description: The router does not receive MPLS pseudowire packets when you configure the **mpls ldp explicit-null** command. The **show mpls l2 vc 1000 detail** command output will shows zero packets received.

```
mwr2941-1# sh mpls l2 vc 1000 det
Local interface: CE0/0 up, line protocol up, CESoPSN Basic up
  Destination address: 10.0.40.1, VC ID: 1000, VC status: up
    Output interface: Vl555, imposed label stack {45 56}
    Preferred path: not configured
    Default path: active
    Next hop: 10.55.55.1
  Create time: 19:39:24, last status change time: 19:38:00
  Signaling protocol: LDP, peer 10.0.40.1:0 up
    MPLS VC labels: local 16, remote 56
    Group ID: local 0, remote 0
```

```
    MTU: local 0, remote 0
    Remote interface description: Provider-0
  Sequencing: receive enabled, send enabled
  Sequencing resync disabled
  VC statistics:
    packet totals: receive 0, send 70823102
    byte totals:   receive 0, send 3121119161
    packet drops:  receive 0, seq error 0, send 0
```

Conditions: Occurs when the **mpls ldp explicit-null** command is configured.

Workaround: Use the **no mpls ldp explicit-null** command.

- CSCte23440

  Description: The MWR 2941 displays OSPF/BFD failures when it receives a burst of host-destined traffic.

  Conditions: Occurs under the following conditions:

  – The MWR2941 is configured with BFD and OSPF on each uplink.

  – MPLS is enabled on the uplinks.

  – The MWR2941 acts as MPLS LER/LSR.

  Workaround: None.

- CSCtf12109

  Description: The MWR 2941 displays one of the following symptoms:

  – The router periodically shows the console message `%NET_CLK_SEL-6-NETCLK_REF_MON_FAIL: Reference Packet Timing fails stratum level 3 parameters.`

  – The packet timing clock has locked but the show network-clock command output shows the clock state as holdover.

  In both cases the **show platform hardware stratum all** command output contains the following:

  – A frequency of 38.88 MHz instead of 16.384 MHz.

```
Rounders reference Frequencies Detected:
  PHYB_P0_P2 (custom)
  PHYB_P1_P3 Not detected
  10MHz/2.048MHz/1.544MHz GPS (custom)
  8KHz PRI 8 KHz detected
  64KHz Mon 64 KHz detected
  BITS 2.048 MHz detected
  16.384MHz RTM 38.88 MHz detected
```

  – The byte at offset 0x08 in the register contents shows the value 0xEF.

```
ZL30130 Register Dump:
  0x00: B8 02 C7 74 00 FF 01 F0 EF DF 7F 00 FF FF 0F FF
```

  Conditions: Occurs when the MWR 2941 is configured for packet timing. Symptoms can occur after you apply the **ptp enable** command or after a router reload.

  Workaround: Reload the MWR 2941.

- CSCtf17127

  Description: An ATM and TDM pseudowire path switch initiated by BFD takes more than one second to re-route on MWR 2941.

  Conditions: Occurs under the following conditions:

  - The Cisco MWR 2941 uses an interior gateway routing protocol such as OSPF or IS-IS for pseudowire IP route selection.
  - The routing protocol uses Bidirectional Forwarding Detection (BFD) to detect pseudowire path failures.
  - The pseudowire destination IP address is multiple IP hops away from the MWR 2941.
  - The path failure results in a route that goes out a different interface than the previous path used.
  - There are more than 200 routes in the IP routing table that are affected by the path failure that changes the pseudowire path.

  Workaround: Reduce the total number of routes impacted by the path change to under 200 by using a routing design where the MWR2941 is not in the core or backbone routing area and use route filtering, summarization, or a stub area to limit the routing table size.

  For TDM pseudowires, structure-aware TDM emulation (CESoPSN) suffers less end-to-end data loss for a delayed pseudowire route switch than structure-agnostic emulation (SATOP).

- CSCtf20171

  Description: A router in an L3 MPLS or daisy-chain network can incorrectly forward traffic destined for another router in the chain. The issue occurs when there is a router between the MWR 2941 and the destination router.

  Conditions: Occurs in an MPLS-enabled or daisy-chain network topology after the network recovers from a failure of a router in the chain.

  Workaround: None; the issue requires that you perform a shutdown/no shutdown on the appropriate interface destination router.

- CSCtg59285

  Description: MWR 2941 does not preserve the DSCP value of a packet that passes from an ingress interface to an egress interface.

  Conditions: Occurs on L3VPN traffic when the MWR 2941 is receiving MPLS packets and forwarding them using IP.

  Workaround: No workaround

- CSCtg68386

  Description: The SFP-GE-Z interface reports an incorrect product identifier in the **show inventory** command output and in the corresponding rows of the ENTITY-MIB.

  Conditions: Occurs on the MWR 2941-DC and MWR 2941-DC-A with the 12.2(33)MRB, 12.4(20)MR02, and earlier images. The error only occurs on SFPs with vendor part number SCP6894-C8-BME. This error does not impact the SFP operation.

  Workaround: None.

- CSCtg94447

  Description: When you apply the **ip address negotiated** command to a dialer interface, the interface output rate drops to 20 pps.

  Conditions: Occurs with a PPP over ADSL or PPP over SHDSL configuration.

  Workaround: Use a statically configured IP address.

Resolved Caveats

This section lists the resolved caveats for Cisco IOS Release 12.4(20)MRA1.

- CSCsz43987

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

  Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

  http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-cucm.shtml

- CSCtc73759

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd33567

  The H.323 implementation in Cisco IOS Software contains two vulnerabilities that may be exploited remotely to cause a denial of service (DoS) condition on a device that is running a vulnerable version of Cisco IOS Software.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds to mitigate these vulnerabilities other than disabling H.323 on the vulnerable device.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-h323.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtd86472

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCte14603

  A vulnerability in the Internet Group Management Protocol (IGMP) version 3 implementation of Cisco IOS Software and Cisco IOS XE Software allows a remote unauthenticated attacker to cause a reload of an affected device. Repeated attempts to exploit this vulnerability could result in a sustained denial of service (DoS) condition. Cisco has released free software updates that address this vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-igmp.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each

advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf17624

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

- CSCtf72678

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device when SIP operation is enabled.

  Cisco has released free software updates that address these vulnerabilities. There are no workarounds for devices that must run SIP; however, mitigations are available to limit exposure to the vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

  Cisco Unified Communications Manager (CUCM) is affected by the vulnerabilities described in this advisory. Two separate Cisco Security Advisories have been published to disclose the vulnerabilities that affect the Cisco Unified Communications Manager at the following locations:

http://www.cisco.com/warp/public/707/cisco-sa-20090826-cucm.shtml

http://www.cisco.com/warp/public/707/cisco-sa-20100922-cucm.shtml

- CSCtf91428

  The Cisco IOS Software Network Address Translation functionality contains three denial of service (DoS) vulnerabilities. The first vulnerability is in the translation of Session Initiation Protocol (SIP) packets, the second vulnerability in the translation of H.323 packets and the third vulnerability is in the translation of H.225.0 call signaling for H.323 packets.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20100922-nat.shtml.

  Note: The September 22, 2010, Cisco IOS Software Security Advisory bundled publication includes six Cisco Security Advisories. Five of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses vulnerabilities in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory. The table at the following URL lists releases that correct all Cisco IOS Software vulnerabilities that have been published on September 22, 2010, or earlier:

  http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml

  Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Security Advisory Bundled Publication" at the following link:

  http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep10.html

Caveats in Cisco IOS Release 12.4(20)MRA

The following sections describe the caveats in Cisco IOS Release 12.4(20)MRA.

Open Caveats

This section lists the open caveats in Cisco IOS Release 12.4(20)MRA..

- CSCtd58271

  Description: The router does not receive MPLS pseudowire packets when you configure the **mpls ldp explicit-null** command. The **show mpls l2 vc 1000 detail** command output will shows zero packets received.

```
mwr2941-1# sh mpls l2 vc 1000 det
Local interface: CE0/0 up, line protocol up, CESoPSN Basic up
  Destination address: 10.0.40.1, VC ID: 1000, VC status: up
    Output interface: Vl555, imposed label stack {45 56}
    Preferred path: not configured
    Default path: active
    Next hop: 10.55.55.1
  Create time: 19:39:24, last status change time: 19:38:00
  Signaling protocol: LDP, peer 10.0.40.1:0 up
    MPLS VC labels: local 16, remote 56
    Group ID: local 0, remote 0
    MTU: local 0, remote 0
    Remote interface description: Provider-0
  Sequencing: receive enabled, send enabled
  Sequencing resync disabled
  VC statistics:
    packet totals: receive 0, send 70823102
    byte totals:   receive 0, send 3121119161
```

```
    packet drops:  receive 0, seq error 0, send 0
```

Conditions: Occurs when the **mpls ldp explicit-null** command is configured.

Workaround: Use the **no mpls ldp explicit-null** command.

- CSCte23440

  Description: The MWR 2941 displays OSPF/BFD failures when it receives a burst of host-destined traffic.

  Conditions: Occurs under the following conditions:

  – The MWR2941 is configured with BFD and OSPF on each uplink.

  – MPLS is enabled on the uplinks.

  – The MWR2941 acts as MPLS LER/LSR.

  Workaround: None.

- CSCtf12109

  Description: The MWR 2941 displays one of the following symptoms:

  – The router periodically shows the console message `%NET_CLK_SEL-6-NETCLK_REF_MON_FAIL: Reference Packet Timing fails stratum level 3 parameters.`

  – The packet timing clock has locked but the show network-clock command output shows the clock state as holdover.

  In both cases the **show platform hardware stratum all** command output contains the following:

  – A frequency of 38.88 MHz instead of 16.384 MHz.

```
Rounders reference Frequencies Detected:
  PHYB_P0_P2 (custom)
  PHYB_P1_P3 Not detected
  10MHz/2.048MHz/1.544MHz GPS (custom)
  8KHz PRI 8 KHz detected
  64KHz Mon 64 KHz detected
  BITS 2.048 MHz detected
  16.384MHz RTM 38.88 MHz detected
```

  – The byte at offset 0x08 in the register contents shows the value 0xEF.

```
ZL30130 Register Dump:
  0x00: B8 02 C7 74 00 FF 01 F0 EF DF 7F 00 FF FF 0F FF
```

  Conditions: Occurs when the MWR 2941 is configured for packet timing. Symptoms can occur after you apply the **ptp enable** command or after a router reload.

  Workaround: Reload the MWR 2941.

- CSCtf17127

  Description: An ATM and TDM pseudowire path switch initiated by BFD takes more than one second to re-route on MWR 2941.

  Conditions: Occurs under the following conditions:

  – The Cisco MWR 2941 uses an interior gateway routing protocol such as OSPF or IS-IS for pseudowire IP route selection.

  – The routing protocol uses Bidirectional Forwarding Detection (BFD) to detect pseudowire path failures.

  – The pseudowire destination IP address is multiple IP hops away from the MWR 2941.

  - The path failure results in a route that goes out a different interface than the previous path used.
  - There are more than 200 routes in the IP routing table that are affected by the path failure that changes the pseudowire path.

  Workaround: Reduce the total number of routes impacted by the path change to under 200 by using a routing design where the MWR2941 is not in the core or backbone routing area and use route filtering, summarization, or a stub area to limit the routing table size.

  For TDM pseudowires, structure-aware TDM emulation (CESoPSN) suffers less end-to-end data loss for a delayed pseudowire route switch than structure-agnostic emulation (SATOP).

- CSCtf20171

  Description: A router in an L3 MPLS or daisy-chain network can incorrectly forward traffic destined for another router in the chain. The issue occurs when there is a router between the MWR 2941 and the destination router.

  Conditions: Occurs in an MPLS-enabled or daisy-chain network topology after the network recovers from a failure of a router in the chain.

  Workaround: None; the issue requires that you perform a shutdown/no shutdown on the appropriate interface destination router.

- CSCtg59285

  Description: MWR 2941 does not preserve the DSCP value of a packet that passes from an ingress interface to an egress interface.

  Conditions: Occurs on L3VPN traffic when the MWR 2941 is receiving MPLS packets and forwarding them using IP.

  Workaround: No workaround

- CSCtg68386

  Description: The SFP-GE-Z interface reports an incorrect product identifier in the **show inventory** command output and in the corresponding rows of the ENTITY-MIB.

  Conditions: Occurs on the MWR 2941-DC and MWR 2941-DC-A with the 12.2(33)MRB, 12.4(20)MR02, and earlier images. The error only occurs on SFPs with vendor part number SCP6894-C8-BME. This error does not impact the SFP operation.

  Workaround: None.

- CSCtg94447

  Description: When you apply the **ip address negotiated** command to a dialer interface, the interface output rate drops to 20 pps.

  Conditions: Occurs with a PPP over ADSL or PPP over SHDSL configuration.

  Workaround: Use a statically configured IP address.

Resolved Caveats

This section lists the resolved caveats for Cisco IOS Release 12.4(20)MRA..

- CSCte49396

  Description: The MWR 2941 can reload due to chunk corruption when you enable CPU utilization statistics collection using the **process cpu statistics limit entry-percentage** command.

  Conditions: Occurs with the 12.4(20)MRA image.

Workaround: Use the **no process cpu statistics limit** command to disable collection of CPU utilization statistics.

- CSCte67461

  Description: When an external device uses the MWR 2941-DC-A 10MHz output clock as a clock source and the external device's TDM clock is not synchronized to the MWR 2941-DC-A's TDM clock, both devices can experience timing slips.

  Conditions: MWR2941-DC-A is configured as PTP slave, and PTP is the only valid clock source, and PTP slave is in FREERUN mode.

  Occurs under the following conditions.

  - The MWR2941-DC-A is configured as a PTP slave device
  - PTP is the only valid clock source
  - PTP slave is in FREERUN mode.

  Workaround: Use the T1/E1 interface for clock output instead of 10MHz.

- CSCte86001

  Description: The MWR 2941 can drop packets when you apply a policy-map with more than 2 user classes to an egress MLPPP interface.

  Conditions: Occurs with a PWE/GRE/MLPPP configuration.

  Workaround: None

- CSCtg35849

  Description: The Console becomes unresponsive after a routing change under a heavy traffic load. Most traffic is dropped and the console can be unresponsive until the traffic load is reduced or the router is power cycled.

  Conditions: Occurs when the router is processing more than 6 Megabits of traffic with small (64 byte) IP packets and the destination route is removed or changes. The error has been observed when an MLPPP backhaul with multiple links switches to a redundant MLPPP bundle path while carrying 20 Mbps of 64-byte IP packets.

  Workaround: None.

- CSCtg59285

  Description: The DSCP value of ingress packets are not preserved at the egress side of the router.

  Conditions: Occurs on L3VPN connections when the MWR 2941 receives an MPLS packet and forwards it using IP.

  Workaround: None.

- CSCtg71359

  Description: Pings sent from the CE or host computer to a network node address fail because the ping packets fail to create an adjacency to the CE or host computer on the VRF subnet.

  Conditions: Occurs on the MWR 2941 with a L3VPN configuration and static routing on the VRF using only static routing or a single interface for the VRF.

  Workaround: Configure a static ARP entry for the CE router or host computer on the PE device.

- CSCtg71826

  Description: The MWR 2941 sets the L-bit to 1 (M bits=00) in CESoPSN data packets upon detecting an RxRAI alarm.

Conditions: Occurs after the MWR 2941 receives an AIS indication from the network. This issue occurs only with T1 controllers.

Workaround: None.

- CSCtg72036

  Description: The MWR 2941 T1 controller displays an RxRAI alarm for an extended period.

  Conditions: Occurs after the MWR 2941 receives an AIS indication from the network. This issue occurs only with T1 controllers.

  Workaround: None

- CSCtg93932

  Description: Network traffic and ping packets sent to the outbound ADSL interface of the MWR 2941 over an extended period begin to fail at a 50% rate.

  Conditions: Occurs in a back-to-back MWR 2941 configuration with ADSL backhaul and Ethernet shorthaul and a single ATM-routed PVC.

  Workaround: Power cycle the MWR 2941.

Caveats in Cisco IOS Release 12.4(20)MR2

The following sections describe the caveats in Cisco IOS Release 12.4(20)MR2.

Open Caveats

The following caveats apply to Cisco IOS Release 12.4(20)MR2.

- CSCtc31618

  Description: LDP session over MLPPP stays down even if the congestion over MLPPP clears.

  Conditions: When the user configures static routes to enable LDP for MPLS over MLPPP and the MLPPP path is congested, the LDP session goes down. If congestion clears or there is no congestion, LDP remains down.

  Workaround: Clear the MLPPP interface using the **clear interface multilink** command.

- CSCtd58271

  Description: When you configure the **mpls ldp explicit-null** command, the MWR 2941 drops MPLS packets within the pseudowire circuit. The **show mpls l2 vc 1000 detail** command output shows that the MWR 2941 does not receive pseudowire packets.

  Conditions: Occurs when you enable **mpls ldp explicit-null** is enabled.

  Workaround: Use the **no mpls ldp explicit-null** command to resolve the issue.

- CSCte23440

  Description: When the MWR 2941 is configured as an MPLS Label Edge Router (LER)/Label Switch Router (LSR), a burst of host-bound traffic causes an OSPF/BFD failure.

  Conditions: Occurs when the MWR 2941 is configured as an MPLS LER/LSR with BFD, OSPF, and MPLS enabled on each uplink.

  Workaround: None.

- CSCte49396

Description: When you enable CPU utilization statistics collection, the MWR 2941 can reload due to chunk corruption.

Conditions: Occurs when you use the **process cpu statistics limit entry-percentage number** command to enable CPU utilization statistics collection.

Workaround: Use the **no process cpu statistics limit** command to disable CPU utilization statistics collection.

- CSCte86001

  Description: When you configure an MPLS pseudowire over GRE/IP/MLPPP and enable a QoS configuration containing more than two classes on an egress MLPPP interface, the MWR 2941 drops packets unexpectedly.

  Conditions: Occurs with a pseudowire/GRE/MLPPP configuration with two or more user classes configured within a QoS policy-map.

  Workaround: None.

- CSCtf12109

  Description: The MWR 2941 displays one of the following symptoms:

  – The router periodically shows the console message `%NET_CLK_SEL-6-NETCLK_REF_MON_FAIL: Reference Packet Timing fails stratum level 3 parameters.`

  – The packet timing clock has locked but the show network-clock command output shows the clock state as holdover.

  In both cases the **show platform hardware stratum all** command output contains the following:

  – A frequency of 38.88 MHz instead of 16.384 MHz.

```
Rounders reference Frequencies Detected:
  PHYB_P0_P2 (custom)
  PHYB_P1_P3 Not detected
  10MHz/2.048MHz/1.544MHz GPS (custom)
  8KHz PRI 8 KHz detected
  64KHz Mon 64 KHz detected
  BITS 2.048 MHz detected
  16.384MHz RTM 38.88 MHz detected
```

  – The byte at offset 0x08 in the register contents shows the value 0xEF.

```
ZL30130 Register Dump:
  0x00: B8 02 C7 74 00 FF 01 F0 EF DF 7F 00 FF FF 0F FF
```

  Conditions: Occurs when the MWR 2941 is configured for packet timing. Symptoms can occur after you apply the **ptp enable** command or after a router reload.

  Workaround: Reload the MWR 2941.

- CSCtf17127

  Description: An ATM and TDM pseudowire path switch initiated by BFD takes more than one second to re-route on MWR 2941.

  Conditions: Occurs under the following conditions:

  – The Cisco MWR 2941 uses an interior gateway routing protocol such as OSPF or IS-IS for pseudowire IP route selection.

  – The routing protocol uses Bidirectional Forwarding Detection (BFD) to detect pseudowire path failures.

  – The pseudowire destination IP address is multiple IP hops away from the MWR 2941.

  - The path failure results in a route that goes out a different interface than the previous path used.
  - There are more than 200 routes in the IP routing table that are affected by the path failure that changes the pseudowire path.

  Workaround: Reduce the total number of routes impacted by the path change to under 200 by using a routing design where the MWR2941 is not in the core or backbone routing area and use route filtering, summarization, or a stub area to limit the routing table size.

  For TDM pseudowires, structure-aware TDM emulation (CESoPSN) suffers less end-to-end data loss for a delayed pseudowire route switch than structure-agnostic emulation (SATOP).

- CSCtf20171

  Description: One of the routers in an MPLS-enabled L3 or daisy-chain network can incorrectly forward traffic destined for another router in the chain. The issue occurs when there is a router between the router that experienced a failure and the destination router.

  Conditions: Occurs in an MPLS-enabled or daisy-chain network topology after the network recovers from a failure of a router in the chain.

  Workaround: None; the issue requires that you perform a shutdown/no shutdown on the appropriate interface destination router.

Resolved Caveats

The following caveats are resolved in Cisco IOS Release 12.4(20)MR2.

- CSCtb89206

  Description: The Cisco MWR 2941 triggers a software-forced reload indicating WINPATH_2941-2-SYSTEMERR in the console log.

  Conditions: The conditions for this reload are extremely rare, and the condition is not reproducible. The reload may be more susceptible to occur during periods of low traffic volume with at least one ATM pseudowire configured.

  Workaround: None. If the problem occurs, obtain the crashinfo file(s) from the MWR 2941 flash: directory and contact Cisco support.

- CSCtd89944

  Description: When the MWR 2941 drops a compressed IPHC packet, the remaining packets in the flow are dropped until the bundle drops and recovers.

  Conditions: Occurs when IPHC is enabled and packet loss occurs on the MLP backhaul interface.

  Workaround: None.

- CSCte43602

  Description: The router displays WP_ERR_HOST_CMD_FAILED and P_ERR_WMM_HOST_CMD_FAILED traceback messages similar to the following.

```
Jan 14 13:12:58.259: Error Traceback:
        File = ../sources/core/wpi_host_cmd.c
        Function=WPI_HostCommand
        Line = 583
        error_index=290 [WP_ERR_HOST_CMD_FAILED]
 -Traceback= 0x4958E88 0x49FDEF0 0x4A25744 0x4BF1048 0x49EE20C 0x49FA488 0x4922D64
0x4923CA0 0x4345D8C 0x4345E20 0x50DCD30 0x50DCDCC 0x434651C 0x4341924 0x4344DF0
0x2478F28
Jan 14 13:12:58.267: Error Traceback:
        File = ../../sources/hardware/core/wpi_hw_wmm.c
        Function=WPI_WmmHostCmdLocal
```

```
        Line = 867
        error_index=287 [WP_ERR_WMM_HOST_CMD_FAILED]
 -Traceback= 0x4958E88 0x49FDEF0 0x4C2B754 0x4C16D78 0x4C2B56C 0x4C2DCD4 0x4C2B448
0x49EF028 0x49F9DC8 0x4922694 0x492310C 0x4923CA0 0x4345D8C 0x4345E20 0x50DCD30
0x50DCDCC
```

Telnet sessions to the router fail leaving only console access.

Conditions: The error occurs under the following conditions:

- The router is running Release 12.4(20)MR1 or 12.2(33)MRA software
- The router is processing high rates of Ethernet-routed traffic (IP or MPLS)
- The router is running a routing protocol such as OSPF or BFD
- The router is sending traffic with small packet sizes (mostly less than 100 bytes) at a high traffic rate (200 Mbps or more)

The WP_ERR_HOST_CMD_FAILED and WP_ERR_WMM_HOST_CMD_FAILED traceback messages can display after several days.

Workaround: None.

- CSCte64426

  Description: The MWR2941 displays a memory allocation failure message and eventually runs out of memory.

  Conditions: Occurs in a back-to-back MWR 2941 setup configured with an SHDSL backhaul, Ethernet shorthaul, and a single ATM routed PVC. At a traffic rate of 3 Mbps, the MWR2941 displays a memory allocation failure after approximately 5 minutes and eventually runs out of memory.

  Workaround: Power cycle the MWR 2941.

- CSCte93437

  Description: When passing traffic, the MWR 2941 experiences a DSLSAR-1-ALLOCFAIL_BUF_FBQ memory allocation failure and displays a traceback message.

  Conditions: Traffic is initially sent at a rate below the oversubscription rate and then raised to an oversubscribed rate for the given packet size. The error can also occur when traffic is started at high rate after the router boots and all interfaces come up.

  Workaround: Perform a shut/no shut on the ATM interface whose virtual access is down.

Caveats in Cisco IOS Release 12.4(20)MR1

The following caveats apply to Cisco IOS Release 12.4(20)MR1.

Open Caveats

This section lists the open caveats in Cisco IOS Release 12.4(20)MR1.

- CSCta38195

  Description: BFD adjacencies remain in the DOWN state.

  Conditions: Occurs when BFD is configured for BGP, and a user either issues the **clear ip bgp *** command or disables and re-enables an SVI interface on which BFD is configured.

  Workaround: None

- CSCta98701

  Description: Ingress QoS packet counters can display an invalid value.

  Conditions: Occurs when dynamically adding or removing class-maps in an ingress QoS policy applied on a Gigabit Ethernet interface.

  Workaround: Issue the **clear counters** command.

- CSCtc09497

  Description: The Cisco MWR 2941 returns WP_ERR_WMM_FIFO_GET and WP_ERR_ATMSW_TX_CHANNEL_NEEDS_RX_HANDLE traceback messages when ATM CoS commands are applied to existing Cell Switching ATM PVCs. In addition, the **show controller atm** command displays the following message for some PVCs that were active before ATM CoS commands were applied: "Channel is not created on SAR yet."

  Conditions: Occurs when the user updates the configuration of a PVC with an ATM CoS configuration, such as by enabling, disabling, or removing an ATM connection.

  Workaround: Remove and restore the PVC configuration.

- CSCtb89206

  Description: The Cisco MWR 2941 triggers a software-forced reload indicating WINPATH_2941-2-SYSTEMERR in the console log.

  Conditions: The conditions for this reload are extremely rare, and the condition is not reproducible. The reload may be more likely to occur during periods of low traffic volume with at least one ATM pseudowire configured.

  Workaround: None

- CSCtc31618

  Description: LDP session over MLPPP stays down even if the congestion over MLPPP clears.

  Conditions: When the user configures static routes to enable LDP for MPLS over MLPPP and the MLPPP path is congested, the LDP session goes down. If congestion clears or there is no congestion, LDP remains down.

  Workaround: Clear the MLPPP interface using the **clear interface multilink** command.

- CSCtc42045

  Description: Invalid class_index: error on applying service policy on MLPPP.

  Conditions: When **no priority** is applied on a priority class in a policy, and there is no service policy, the service policy is applied to MLPPP, and an invalid class_index error is seen.

  Workaround: Remove the class-map statement from the policy-map and add it to the policy-map again, then configure priority and apply this policy-map to the multilink interface.

- CSCtc76787

  Description: The message **bandwidth of** *xx* **is not available** (*yy*) may be observed when a service policy is attached to an interface and the interface is activated or inactivated. As a result, the service policy is programatically removed from the interface.

  Conditions: This condition may occur due to a rounding error when the total amount of allocated bandwidth specified by service policies on an interface is equal to exactly 100%, as shown in the following configuration example.

```
policy-map policy1
class high
priority percent 99
class class-default
```

```
bandwidth percent 1

interface multilink 1
service-policy output policy1
```

Workaround: Configure the total amount of allocated bandwidth to be slightly less than 100% by using the **remaining** keyword on the bandwidth command. The following examples demonstrate service policies that allocate 99.99% of available bandwidth.

```
policy-map policy1
class high
priority percent 99
class class-default
bandwidth remaining percent 99

policy-map policy2
class one
priority percent 99
class two
bandwidth remaining percent 66
class class-default
bandwidth remaining percent 33
```

- CSCtc79736

  Description: When VLAN interface MTU size is set to greater than 1600, the router can drop large egress packets.

  Conditions: Occurs when the VLAN interface MTU size is set to greater than 1600.

  Workaround: Set the VLAN interface MTU size smaller or use the default MTU setting of 1500.

- CSCtd02352

  Description: The mwr2941 router may crash during CEM interface configuration when the number of dejitter buffers requested exceeds the available number of buffers in the shared pool.

  Conditions: The mwr2941 router has a shared pool of buffers that are used for CEM dejitter buffers. You can use the **show platform hardware winpath iw qnodes** command to display the number of available buffers in the shared pool:

  ```
  Router# show platform hardware winpath iw qnodes | include Local Free Buffer Count
  Local Free Buffer Count: 4096
  ```

  Each CEM interface creates dejitter buffers from this shared pool. For example, the following configuration takes 65 buffers from the shared pool:

  ```
  interface CEM 0/0
   cem 0
    dejitter 64
  ```

  Each CEM interface will deplete the shared pool of buffers. When the number of requested dejitter buffers for a CEM interface configuration exceeds the number of buffers available in the shared pool, the router can crash.

  Workaround: Use the **show platform hardware winpath iw qnodes | include Local Free Buffer Count** command to ensure that the CEM configuration does not exceed the number of buffers available in the shared pool.

- CSCtd14234

  Description: The ATM pseudowire VC remains UP on the router when the Shorthaul IMA interface is down due to alarm condition.

  Conditions: Occurs when the shorthaul IMA interface has an AIS or LOS alarm condition.

Workaround: Apply a **shutdown/no shutdown** to the IMA interface.

- CSCtd44830

  Description: The console may display an WP_ERR_CH_NOT_DISABLED error when shutting down a multilink bundle.

  Conditions: This problem can occur when the output hold queue is explicitly configured to be greater than 256 and there is congestion on the bundle causing packets to be queued by the outbound channel.

  Workaround: Use the default output hold queue value or configure the output hold queue to be less than or equal to 256. The interface command to configure the output hold queue is **hold-queue 256 output**.

- CSCtd44864

  Description: Under certain conditions, IS-IS adjacencies are not be formed on an SVI interface.

  Conditions: The issue occurs on Cisco IOS Release 12.4(20)MR when IS-IS is configured on an SVI interface with MTU set to 4470 bytes.

  Workaround: Set the interface MTU size to the default 1500 bytes.

- CSCtd47439

  Description: Under certain conditions, the MWR 2941 may experience a software reload upon enabling link noise monitor on a controller.

  Conditions: This issue only occurs upon enabling link noise monitor on an HWIC controller.

  Workaround: Do not configure link noise monitor on an HWIC controller.

- CSCtd58232

  Description: The PTP protocol times out, and ptp slave cannot lock to ptp master.

  Conditions: Can occur when unicast PTP master or mixed mode ptp slave performs multiple ARP requests back-to-back, usually after the 2941 reboots when multiple PTP peers begin PTP negotiation with the 2941.

  Workaround: Restart the failing PTP peer(s) one at a time, in order to avoid simultaneous ARP requests by 2941.

Resolved Caveats

This section lists resolved caveats for Cisco IOS Release 12.4(20)MR1.

- CSCtc84729

  Description: Traceback are seen in console output when the IMA interface is shut/no shut.

  Conditions: When port mode pseudowire is configured on IMA interface and shutdown/no shutdown commands are applied on the IMA interface, tracebacks can display on the console. These tracebacks do not affect pseudowire service.

  Workaround: None. The traceback do not affect service.

- CSCtc97903

  Description: After upgrading the MWR2941 to 12.4(20)MR IP connectivity through the VLANs configured on the GigabitEthernet uplink interface fails if an ingress QoS service-policy is configured.

Conditions: An ingress QoS service-policy is configured on the GigabitEthernet uplink interface. Upon reloading the MWR2941 with the 12.4(20)MR release IP connectivity is lost via the GigabitEthernet interface.

Workaround: The ingress QoS service-policy must be removed to restore IP network connectivity.

- CSCtd11955

  Description: PTP redundancy does not function properly.

  Conditions: Occurs in all PTP redundancy configurations.

  Workaround: None.

- CSCtd27623

  Description: The router crashes when you apply a service policy with two class-maps containing multiple **match ip dscp** values within a single **match** statement, as in the following configuration.

```
class-map match-any class1
match ip dscp af31 af32 af33 ef

class-map match-any class2
match ip dscp af23 af33 af41

policy-map mlppp
class class1
priority percent <value>
class class2
bandwidth remaining percent 67
class class-default
bandwidth remaining percent 32

interface multilink 1
service policy output mlppp
```

  Conditions: Occurs when a service policy contains two class-maps with multiple **match ip dscp** values within a single **match** statement.

  Workaround: Configure the class-map definition as in the following example.

```
class match-any class1
match ip dscp af31
match ip dscp af32
match ip dscp af33
match ip dscp ef

class match-any class2
match ip dscp af23
match ip dscp af33
match ip dscp af41

policy-map mlppp
class class1
priority percent <value>
class class2
bandwidth remaining percent 67
class class-default
bandwidth remaining percent 32

interface multilink 1
service policy output mlppp
```

- CSCtd44144

  Description: IS-IS point-to-point routing does not function properly.

Conditions: Occurs on all IS-IS point-to-point configurations.

Workaround: None.

Caveats in Cisco IOS Release 12.4(20)MR

The following caveats apply to Cisco IOS Release 12.4(20)MR.

Open Caveats

This section lists the open caveats in Cisco IOS Release 12.4(20)MR.

- CSCsx38538

  Description: ATM subinterface on HWIC-4SHDSL can remain in down state when ATM OAM is configured.

  Conditions: Occurs when F5 ATM OAM is enabled using the **oam-pvc manage cc segment** command.

  Workaround: Disable ATM OAM and re-enable it.

- CSCta38195

  Description: BFD adjacencies remain in the DOWN state.

  Conditions: Occurs when BFD is configured for BGP, and a user either issues the **clear ip bgp *** command or disables and re-enables an SVI interface on which BFD is configured.

  Workaround: None

- CSCta98701

  Description: Ingress QoS packet counters could display invalid value.

  Conditions: When dynamically adding or removing class-maps in an ingress QoS policy applied on a Gigabit Ethernet interface, the QoS packet counters could show invalid value.

  Workaround: Issue the **clear counters** command.

- CSCtc09497

  Description: The MWR 2941 returns WP_ERR_WMM_FIFO_GET and WP_ERR_ATMSW_TX_CHANNEL_NEEDS_RX_HANDLE traceback messages when ATM CoS commands are applied to existing Cell Switching ATM PVCs. In addition, the **show controller atm** command displays the following message for some PVCs that were active before ATM CoS commands were applied: “Channel is not created on SAR yet.”

  Conditions: Occurs when the user updates the configuration of a PVC with an ATM CoS configuration, such as by enabling, disabling, or removing an ATM connection.

  Workaround: Remove and restore the PVC configuration.

- CSCtb89206

  Description: The Cisco MWR 2941 triggers a software-forced reload indicating WINPATH_2941-2-SYSTEMERR in the console log.

  Conditions: The conditions for this reload are extremely rare, and the condition is not reproducible. The reload may be more likely to occur during periods of low traffic volume with at least one ATM pseudowire configured.

  Workaround: None

- CSCtc31618

  Description: LDP session over MLPPP stays down even if the congestion over MLPPP clears.

  Conditions: When the user configures static routes to enable LDP for MPLS over MLPPP and the MLPPP path is congested, the LDP session goes down. If congestion clears or there is no congestion, LDP remains down.

  Workaround: Clear the MLPPP interface using the **clear interface multilink** command.

- CSCtc42045

  Description: Invalid class_index: error on applying service policy on MLPPP.

  Conditions: When **no priority** is applied on a priority class in a policy, and there is no service policy, the service policy is applied to MLPPP, and an invalid class_index error is seen.

  Workaround: Remove the class-map statement from the policy-map and add it to the policy-map again, then configure priority and apply this policy-map to the multilink interface.

- CSCtc76787

  Description: The message **bandwidth of** *xx* **is not available** (*yy*) may be observed when a service policy is attached to an interface and the interface is activated or inactivated. As a result, the service policy is programatically removed from the interface.

  Conditions: This condition may occur due to a rounding error when the total amount of allocated bandwidth specified by service policies on an interface is equal to exactly 100%, as shown in the following configuration example.

```
policy-map policy1
class high
priority percent 99
class class-default
bandwidth percent 1

interface multilink 1
service-policy output policy1
```

  Workaround: Configure the total amount of allocated bandwidth to be slightly less than 100% by using the **remaining** keyword on the bandwidth command. The following examples demonstrate service policies that allocate 99.99% of available bandwidth.

```
policy-map policy1
class high
priority percent 99
class class-default
bandwidth remaining percent 99

policy-map policy2
class one
priority percent 99
class two
bandwidth remaining percent 66
class class-default
bandwidth remaining percent 33
```

- CSCtc76787

  Description: Traceback are seen in console output when the IMA interface is shut/no shut.

  Conditions: When port mode pseudowire is configured on IMA interface and shutdown/no shutdown commands are applied on the IMA interface, tracebacks can display on the console. These tracebacks do not affect pseudowire service.

  Workaround: None. The traceback do not affect service.

- CSCtc97903

  Description: After upgrading the MWR 2941-DC to 12.4(20)MR, IP connectivity through the VLANs configured on the GigabitEthernet uplink interface fails if an ingress QoS service-policy is configured.

  Conditions: An ingress QoS service-policy is configured on the GigabitEthernet uplink interface. Upon reloading the MWR 2941 with the 12.4(20)MR release, IP connectivity is lost via the GigabitEthernet interface.

  Workaround: Remove and restore the ingress QoS service-policy to restore IP network connectivity.

- CSCtd11955

  Description: PTP redundancy does not function properly.

  Conditions: Occurs in all PTP redundancy configurations.

  Workaround: None.

Resolved Caveats

This section lists resolved caveats for Cisco IOS Release 12.4(20)MR.

- CSCta05846

  Description: IMA interface stays down after a router reload.

  Conditions: Occurs with IMA between the 2941 and 7600 when the MWR 2941 is reloaded.

  Workaround: Perform a shut/no shut of the IMA interface.

- CSCta33248

  Description: Tracebacks reported to the console.

  Conditions: This problem can occur when configuration or system changes are made that result in host-based routing/switching of packets for serial interfaces. In certain traffic cases this overloads the receive queues for the serial interfaces in the attached network processor.

  Workaround: Disconnect or disable router from traffic sources or reload the router.

Caveats in Cisco IOS Release 12.4(19)MR3

The following caveats apply to Cisco IOS Release 12.4(19)MR3.

Open Caveats

This section lists the open caveats in Cisco IOS Release 12.4(19)MR3.

- CSCsy18615

  Description: If you indiscriminately remove and add a multilink PPP interface, this may cause the router to reload unexpectedly. This may occur when packets are unexpectedly received by a multilink interface during a transitional state.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the underlying multilink components in the sequence as indicated by the following configuration example. In the example, the multilink interface consists of two underlying links.

  ```
  int multilinkl 1
  ```

```
shutdown
no int multilink 1

int serial0/1:0
shutdown
int serial0/2:0
shutdown

controller t1 0/1
shutdown
controller t1 0/2
shutdown

controller t1 0/1
no channel-group 0
controller t1 0/2
no channel-group 0

controller t1 0/1
channel-group 0 timeslot 1-24
controller t1 0/2
channel-group 0 timeslot 1-24

int serial0/1:0
no ip address
encapsulation ppp
ppp multilink group 1

int serial0/2:0
no ip address
encapsulation ppp
ppp multilink group 1

interface multilink 1
ip address 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
ppp timeout multilink lost-fragment 1

controller t1 0/1
no shutdown
controller t1 0/2
no shutdown

int serial0/1:0
no shutdown
int serial0/2:0
no shutdown
```

- CSCsy30207

  Description: If you indiscriminately remove and add a multilink PPP interface, this may cause the router to reload unexpectedly. This may occur when packets are unexpectedly received by a multilink interface during a transitional state.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the underlying multilink components in the sequence as indicated by the following configuration example. In the example, the multilink interface consists of two underlying links.

```
int multilinkl 1
shutdown
```

```
no int multilink 1

int serial0/1:0
shutdown
int serial0/2:0
shutdown

controller t1 0/1
shutdown
controller t1 0/2
shutdown

controller t1 0/1
no channel-group 0
controller t1 0/2
no channel-group 0

controller t1 0/1
channel-group 0 timeslot 1-24
controller t1 0/2
channel-group 0 timeslot 1-24

int serial0/1:0
no ip address
encapsulation ppp
ppp multilink group 1

int serial0/2:0
no ip address
encapsulation ppp
ppp multilink group 1

interface multilink 1
ip address 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
ppp timeout multilink lost-fragment 1

controller t1 0/1
no shutdown
controller t1 0/2
no shutdown

int serial0/1:0
no shutdown
int serial0/2:0
no shutdown
```

Resolved Caveats

This section lists the closed caveats in Cisco IOS Release 12.4(19)MR3.

- CSCso25507

  Description: Authentication & authorization with TACACS fails. When making modem calls with TACACS AAA servers, authorization failed with the following error message:

  ```
  TPLUS(00000002): Fail to set vrf socket option - FAIL
  ```

Conditions: Occurs when configuring the following AAA and TACACS configuration:

```
aaa new-model
aaa authentication login logintest local
aaa authorization exec default tacacs
aaa accounting exec wait-start tacacs+

tacacs-server host X.X.X.X
tacacs-server key X
```

Issue was observed on the Cisco AS5400 running 12.4(19.9)T1 image.

Workaround: None.

- CSCsy62813

  Symptom: A multilink bundle which is under heavy packet load may cause the router to reload.

  Conditions: This symptom has been observed when an interface which has just joined a multilink bundle receives packets at a rate faster than the router can process them.

  Workaround: There is no workaround.

- CSCsy88148

  Symptom: The MWR 2941 does not support the IS-IS routing protocol. IS-IS Hello packets are dropped by MWR 2941 ethernet switch.

  Workaround: There is no workaround.

- CSCsq24002

  Cisco IOS Software contains a vulnerability that could allow an attacker to cause a Cisco IOS device to reload by remotely sending a crafted encryption packet. Cisco has released free software updates that address this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-tls.shtml.

- CSCsx25880

  A vulnerability exists in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software that could allow an unauthenticated attacker to cause a denial of service (DoS) condition on an affected device when the Cisco Unified Border Element feature is enabled. Cisco has released free software updates that address this vulnerability. For devices that must run SIP there are no workarounds; however, mitigations are available to limit exposure of the vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090923-sip.shtml.

- CSCsz22425

  Symptom: When 7600 is reloaded (or switchover occurs), TDM/PWE3 circuit is re-established but packets may not transmitted by the MWR 2941 across the network.

  Workaround: Transmission on circuit may be recovered by shut/no-shut of CEM controller on MWR 2941.

- CSCsz49123

  Symptom: When the MWR 2941 is setup as an IP SLA responder, the jitter and round trip times measured are much higher than when compared to other Cisco platforms such as the ISR.

  Conditions: This defect occurs when the MWR 2941 is setup as an IP SLA responder and is connected to another Cisco device setup as the collector. With another device such as an ISR setup in an identical topology to compare the round trip and jitter times with.

  Workaround: No workarounds for this defect.

- CSCsz88220

  Symptom: When Flexlink is configured on the MWR 2941 and both links are on, in certain setup, a layer 2 loop occurs during or after the MWR 2941 boots.

  Conditions: Occurs when the MWR 2941 is configured with flexlink and you create a new VLAN that involves both of the configured flexlink ports, and both ports are up during boot or a configuration change. The error can occur during the MWR 2941 boot due to configuration process timing or when you configure new VLANs.

  The problem involves a specific IOS configuration; you can detect a layer 2 loop from a switch connected to the MWR 2941 as a MAC address flapping between two ports, or where one of the ports is directly connected.

  Workaround: No workarounds for this defect.

Caveats in Cisco IOS Release 12.4(19)MR2

The following caveats apply to Cisco IOS Release 12.4(19)MR2.

Open Caveats

This section lists the open caveats in Cisco IOS Release 12.4(19)MR2.

- CSCsy18615

  Description: If you indiscriminately remove and add a multilink PPP interface, this may cause the router to reload unexpectedly. This may occur when packets are unexpectedly received by a multilink interface during a transitional state.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the underlying multilink components in the sequence as indicated by the following configuration example. In the example, the multilink interface consists of two underlying links.

```
int multilinkl 1
shutdown
no int multilink 1

int serial0/1:0
shutdown
int serial0/2:0
shutdown

controller t1 0/1
shutdown
controller t1 0/2
shutdown

controller t1 0/1
no channel-group 0
controller t1 0/2
no channel-group 0

controller t1 0/1
channel-group 0 timeslot 1-24
controller t1 0/2
channel-group 0 timeslot 1-24

int serial0/1:0
no ip address
```

```
encapsulation ppp
ppp multilink group 1

int serial0/2:0
no ip address
encapsulation ppp
ppp multilink group 1

interface multilink 1
ip address 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
ppp timeout multilink lost-fragment 1

controller t1 0/1
no shutdown
controller t1 0/2
no shutdown

int serial0/1:0
no shutdown
int serial0/2:0
no shutdown
```

- CSCsy30207

  Description: If you indiscriminately remove and add a multilink PPP interface, this may cause the router to reload unexpectedly. This may occur when packets are unexpectedly received by a multilink interface during a transitional state.

  Workaround: Perform the **shutdown** and **no shutdown** commands on the underlying multilink components in the sequence as indicated by the following configuration example. In the example, the multilink interface consists of two underlying links.

```
int multilinkl 1
shutdown
no int multilink 1

int serial0/1:0
shutdown
int serial0/2:0
shutdown

controller t1 0/1
shutdown
controller t1 0/2
shutdown

controller t1 0/1
no channel-group 0
controller t1 0/2
no channel-group 0

controller t1 0/1
channel-group 0 timeslot 1-24
controller t1 0/2
channel-group 0 timeslot 1-24

int serial0/1:0
no ip address
encapsulation ppp
```

```
ppp multilink group 1

int serial0/2:0
no ip address
encapsulation ppp
ppp multilink group 1

interface multilink 1
ip address 192.168.1.1 255.255.255.0
ppp multilink
ppp multilink interleave
ppp multilink group 1
ppp multilink fragment delay 0 1
ppp multilink multiclass
ppp timeout multilink lost-fragment 1

controller t1 0/1
no shutdown
controller t1 0/2
no shutdown

int serial0/1:0
no shutdown
int serial0/2:0
no shutdown
```

Resolved Caveats

There are no resolved caveats for Cisco IOS Release 12.4(19)MR2.

Troubleshooting

The following sections describe troubleshooting commands you can use with the Cisco MWR 2941.

Collecting Data for Router Issues

To collect data for reporting router issues, issue the following command:

- **show tech-support**—Displays general information about the router if it reports a problem.

Collecting Data for ROMmon Issues

To collect data for ROMmon issues, issue the following command while in EXEC mode:

- **show rom-monitor**—Displays currently selected ROM monitor.

Note If you contact Cisco support for assistance, we recommend that you provide any crashinfo files stored in flash memory. For more information about crashinfo files, see http://www.cisco.com/en/US/products/hw/routers/ps167/products_tech_note09186a00800a6743.shtml.

Related Documentation

Related documents for implementing the Cisco MWR 2941 mobile wireless edge router are available on Cisco.com

To access the related documentation on Cisco.com, go to:

http://www.cisco.com/en/US/products/ps9395/tsd_products_support_series_home.html

Documents related to the Cisco MWR 2941 mobile wireless edge router include the following guides:

- Cisco MWR 2941 Mobile Wireless Edge Router documents
  - *Cisco MWR 2941 Mobile Wireless Edge Routers Hardware Installation Guide*
  - *Cisco MWR 2941-DC Mobile Wireless Edge Router Software Configuration Guide, Release 12.4(20)MR*
  - *Cisco Regulatory Compliance and Safety Information for the Cisco MWR 2941 Routers*
- Release Notes—*Release Notes for Cisco MWR 2941-DC-A Mobile Wireless Edge Router for Cisco IOS Release 12.4(20)MRA1*
- Cisco Interface Cards Installation Guides
  - *Quick Start Guide: Interface Cards*
  - Cisco Interface Cards Installation Guide

Services and Support

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New* in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Release Notes for Cisco MWR 2941 Mobile Wireless Edge Routers for Cisco IOS Release 12.4(20)MRA