Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router for Cisco IOS Release 15.1(1)MR2

September 22, 2011

OL-24058-01

These release notes are for the Cisco MWR Mobile Wireless Edge Router for Cisco IOS Release 15.1(1)MR2. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode.

For a list of the software caveats that apply to Cisco IOS Release 15.1(1)MR2, see the "Caveats in Cisco IOS Release 15.1(1)MR2" section on page 35.

To review all Cisco MWR 2941 release notes, including *Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router for Cisco IOS Release 15.1(1)MR2,* 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 15.1S, go to:

http://www.cisco.com/en/US/products/ps11280/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 Mobile Wireless Router is a cell-site access platform specifically designed to aggregate and transport mixed-generation radio access network (RAN) traffic. The router is used at the cell site edge as a part of a 2G, 3G, or 4G radio access network (RAN). The Cisco MWR 2941 includes the following models:

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

The Cisco MWR 2941 router helps enable a variety of RAN solutions by extending IP connectivity to devices using Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), Node Bs using HSPA or LTE, base transceiver stations (BTSs) using Enhanced Data Rates for GSM Evolution (EDGE), Code Division Multiple Access (CDMA), CDMA-2000, EVDO, or WiMAX, and other cell-site equipment. It transparently and efficiently transports cell-site voice, data, and signaling traffic over IP using traditional T1 and E1 circuits, as well as alternative backhaul networks such as Carrier Ethernet and DSL, Ethernet in the First Mile (EFM), and WiMAX. It also supports standards-based Internet Engineering Task Force (IETF) Internet protocols over the RAN transport network, including those standardized at the Third-Generation Partnership Project (3GPP) for IP RAN transport. Custom designed for the cell site, the Cisco MWR 2941 features a small form factor, extended operating temperature, and cell-site DC input voltages.

System Requirements

Table 1 lists the supported system configurations for the Cisco MWR 2941:

Memory Requirements

Table 1 lists the required memory for using this software.

Table 1 Cisco IOS Release 15.1(1)MR1 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-adviprank9-mz.151-1.MR2.bin	128 MB	512 MB	RAM
Cisco MWR 2941 Mobile Wireless Edge Router	RAN Optimization	mwr2941-advipran-mz.151-1.MR2.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 IOS Software, 2900 Software (MWR2900-ADVIPRANK9-M), Version 15.1(1)MR2, RELEASE
SOFTWARE (fc2)
```

Upgrading to a New Software Release

Release 15.1(1)MR2 does not support the following features that were supported in Release 12.4(20)MR1:

- GSM Abis optimization
- IP Header Compression (IPHC)
- Reduced HWIC support—Release 15.1(1)MR2 does not support the HWIC-1GE-SFP, HWIC-4SHDSL, HWIC-1ADSL, and HWIC-1 ADSL-I HWICs.
- GRE offload

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

http://www.cisco.com/en/US/products/hw/routers/ps259/products_tech_note09186a00801fc986.shtml

New and Changed Information

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

Support for Existing Cisco MWR 2941 Software Features

Release 15.1(1)MR2 supports the software features supported in Release 15.0(2)MR. For more information about Release 15.0(2)MR and previous releases, see http://www.cisco.com/en/US/products/ps9395/prod_release_notes_list.html.

New Hardware Features in Release 15.1(1)MR2

There are no new hardware features in Release 15.1(1)MR2.

New Software Features in Release 15.1(1)MR2

Release 15.1(1)MR2 introduces the following new software feature:

- Support monitoring internal port (to NPU) tail drop—Release 15.1(1)MR2 allows you to monitor internal port tail drop by using the following new CLI:

  switch tail-drop accounting winpath.

New Hardware Features in Release 15.1(1)MR1

There are no new hardware features in Release 15.1(1)MR1.

New Software Features in Release 15.1(1)MR1

Release 15.1(1)MR1 introduces the following new software features:

- System-level switch buffer limit increased—Release 15.1(1)MR1 has increased the system-level switch buffer limit from 350 to 420.
- Global buffer limit for queueing—Release 15.1(1)MR1 allows you to configure global buffer limit for queueing with a new CLI. The buffer-limit range is 350 to 450, and default value is 420. The feature introduces the following new command:

  switch buffer-limit—Configure global queue buffer limit.

New Hardware Features in Release 15.1(1)MR

This release introduces support for the GLC-EX-SMD SFP. For instructions on how to install this SFP, see

http://www.cisco.com/en/US/docs/interfaces_modules/transceiver_modules/installation/note/78_15160.html.

New Software Features in Release 15.1(1)MR

Release 15.1(1)MR introduces the following new software features:

- Support for IPv6
- Support for New MIBs
- T1 and E1 Local Switching
- Ethernet Loopback
- Two-Way Active Measurement Protocol

Support for IPv6

Release 15.1(1)MR introduces support for IPv6. The following sections summarize the supported IPv6 features in Release 15.1(1)MR:

- IPv6 Limitations
- Supported IPv6 Features
- Supported IPv6 Commands

IPv6 Limitations

The Release 15.1(1)MR implementation of IPv6 has the following limitations:

- IPv6 is only supported on loopback and Vlan interfaces; IPv6 is not supported on other interface types.

- Release 15.1(1)MR supports IPv6 prefixes of up to 64 bits. For example, 2001::DB8/64 is supported, while 2001::DB8/65 is not supported. Full 128-bit addresses are supported.
- IPv6 equal cost multiple path is not supported.
- BGPv6 with BFD is not supported.

Supported IPv6 Features

The following table summarizes the supported IPv6 features in Release 15.1(1)MR. For information about how to configure these features, see the hyperlinked section or refer to the *IPv6 Configuration Guide, Cisco IOS Release 15.1S.*

Supported IPv6 Features
Implementing IPv6 Addressing and Basic Connectivity
Implementing Bidirectional Forwarding Detection for IPv6
Implementing Multiprotocol BGP for IPv6
Implementing DHCP for IPv6
Implementing IS-IS for IPv6
Implementing IPv6 for Network Management
Implementing IPv6 over MPLS
Implementing IPv6 VPN over MPLS
Implementing OSPF for IPv6
Implementing QoS for IPv6
Implementing QoS for IPv6
Implementing Static Routes for IPv6

Supported IPv6 Commands

Table 2 summarizes the supported commands in Release 15.1(1)MR. For more information about these commands, refer to the *Cisco IOS IPv6 Command Reference*.

Table 2 Supported IPv6 Commands

aaa new-model	**ipv6 ospf hello-interval**	**show clock**
clear cef table	**ipv6 ospf mtu-ignore**	**show ipv6 cef**
clear ipv6 dhcp binding	**ipv6 ospf name-lookup**	**show ipv6 cef adjacency**
clear ipv6 dhcp client	**ipv6 ospf neighbor**	**show ipv6 cef non-recursive**
clear ipv6 dhcp conflict	**ipv6 ospf network**	**show ipv6 cef platform**
clear ipv6 dhcp relay binding	**ipv6 ospf priority**	**show ipv6 cef summary**
clear ipv6 mtu	**ipv6 ospf retransmit-interval**	**show ipv6 cef switching statistics**
clear ipv6 neighbors	**ipv6 ospf transmit-delay**	**show ipv6 cef traffic prefix-length**
clear ipv6 route	**ipv6 prefix-list**	**show ipv6 cef tree**
clear ipv6 traffic	**ipv6 prefix-list sequence-number**	**show ipv6 cef vrf**
crypto key generate rsa	**ipv6 route**	**show ipv6 dhcp**

Table 2 Supported IPv6 Commands

debug ipv6 cef drop	ipv6 route static bfd	show ipv6 dhcp binding
debug ipv6 cef events	ipv6 router ospf	show ipv6 dhcp conflict
debug ipv6 cef receive	ipv6 source-route	show ipv6 dhcp database
debug ipv6 cef table	ipv6 unicast-routing	show ipv6 dhcp interface
debug ipv6 dhcp	match dscp	show ipv6 dhcp pool
debug ipv6 dhcp database	match protocol	show ipv6 interface
debug ipv6 icmp	match protocol (zone)	show ipv6 mtu
debug ipv6 nd	maximum-paths (IPv6)	show ipv6 neighbors
debug ipv6 packet	mpls ldp router-id	show ipv6 ospf
hostname	neighbor activate	show ipv6 ospf border-routers
ip address	neighbor ebgp-multihop	show ipv6 ospf database
ip unnumbered	neighbor remote-as	show ipv6 ospf event
ipv6 address	neighbor send-community	show ipv6 ospf flood-list
ipv6 address anycast	neighbor send-label	show ipv6 ospf graceful-restart
ipv6 address autoconfig	neighbor translate-update	show ipv6 ospf interface
ipv6 address eui-64	neighbor update-source	show ipv6 ospf neighbor
ipv6 address link-local	network (BGP and multiprotocol BGP)	show ipv6 ospf request-list
ipv6 cef	network (IPv6)	show ipv6 ospf retransmission-list
ipv6 cef accounting	passive-interface (IPv6)	show ipv6 ospf statistics
ipv6 dhcp database	ping	show ipv6 ospf summary-prefix
ipv6 dhcp pool	ping ipv6	show ipv6 ospf timers rate-limit
ipv6 dhcp server	ping vrf	show ipv6 ospf traffic
ipv6 enable	prefix-delegation	show ipv6 ospf virtual-links
ipv6 hop-limit	prefix-delegation pool	show ipv6 protocols
ipv6 host	set dscp	show ipv6 route
ipv6 icmp error-interval	show adjacency	show ipv6 route summary
ipv6 mtu	show bfd neighbors	show ipv6 route vrf
ipv6 nd advertisement-interval	show bfd summary	show ipv6 routers
ipv6 nd cache interface-limit (global)	show bgp ipv6 unicast	show ipv6 static
ipv6 nd cache interface-limit (interface)	show bgp ipv6 community	show ipv6 traffic
ipv6 nd dad attempts	show bgp ipv6 community-list	show isis database
ipv6 nd dad time	show bgp ipv6 unicast dampening dampened-paths	show isis ipv6 rib
ipv6 nd managed-config-flag	show bgp ipv6 filter-list	show isis spf-log
ipv6 nd ns-interval	show bgp ipv6 flap-statistics	show isis topology
ipv6 nd other-config-flag	show bgp ipv6 inconsistent-as	show key chain

Table 2 Supported IPv6 Commands

ipv6 nd prefix	**show bgp ipv6 labels**	**show mpls forwarding-table**
ipv6 nd ra interval	**show bgp ipv6 neighbors**	**ssh**
ipv6 nd ra lifetime	**show bgp ipv6 paths**	**summary-prefix (IPv6 OSPF)**
ipv6 nd ra suppress	**show bgp ipv6 peer-group**	**synchronization (IPv6)**
ipv6 nd reachable-time	**show bgp ipv6 prefix-list**	**telnet**
ipv6 nd router-preference	**show bgp ipv6 quote-regexp**	**telnet**
ipv6 neighbor	**show bgp ipv6 regexp**	**timers lsa arrival**
ipv6 ospf area	**show bgp ipv6 route-map**	**timers pacing flood (IPv6)**
ipv6 ospf authentication	**show bgp ipv6 summary**	**timers pacing lsa-group (IPv6)**
ipv6 ospf bfd	**show bgp vpnv6 unicast**	**timers pacing retransmission (IPv6)**
ipv6 ospf cost	**show cdp entry**	**timers spf (IPv6)**
ipv6 ospf database-filter all out	**show cdp neighbors**	**timers throttle lsa**
ipv6 ospf dead-interval	**show cef**	**timers throttle spf**
ipv6 ospf demand-circuit	**show cef interface**	**traceroute**
ipv6 ospf encryption	**show cef table**	**vrf definition**
ipv6 ospf flood-reduction	**show clns neighbors**	**vrf forwarding**

Sample IPv6 Configurations

The following sections provide sample configurations for IPv6.

- Basic Connectivity
- Static Route
- BFD
- Multiprotocol BGP
- DHCP
- IS-IS
- Network Management
- IPv6 over MPLS
- IPv6 VPN over MPLS
- OSPFv3
- QoS

This section displays partial configurations intended to demonstrate specific features.

Basic Connectivity

The following example shows how to enable IPv6 on the router.

```
ipv6 unicast-routing
ipv6 cef
ipv6 address
```

For more information about configuring basic IPv6 connectivity, refer to Implementing IPv6 Addressing and Basic Connectivity.

Static Route

The following example shows how to configure an IPv6 static route on the Cisco MWR 2941.

```
Router# configure terminal
Router(config)# ipv6 route 2001:DB8::/64 102::2
Router(config)# exit
Router#
```

For more information about how to configure static routes for IPv6, see Implementing Static Routes for IPv6.

BFD

The following examples show how to configure BFD for IPv6.

- Example: Specifying an IPv6 Static BFDv6 Neighbor
- Example: Associating an IPv6 Static Route with a BFDv6 Neighbor
- Example: Displaying OSPF Interface Information about BFD
- Example: IPv6 VPN Configuration Using IPv4 Next Hop

Example: Specifying an IPv6 Static BFDv6 Neighbor

The following example specifies a fully configured IPv6 static BFDv6 neighbor. The interface is Ethernet 0/0 and the neighbor address is 2001::1.

```
Router(config)# ipv6 route static bfd ethernet 0/0 2001:DB8:1::1
```

Example: Associating an IPv6 Static Route with a BFDv6 Neighbor

In this example, the IPv6 static route 2001:0DB8::/32 is associated with the BFDv6 neighbor 2001:DB8:1::1 over the Ethernet 0/0 interface:

```
Router(config)# ipv6 route static bfd ethernet 0/0 2001:DB8:1::1
Router(config)# ipv6 route 2001:0DB8::/32 ethernet 0/0 2001:DB8:1::1
```

Example: Displaying OSPF Interface Information about BFD

The following display shows that the OSPF interface is enabled for BFD:

```
Router# show ipv6 ospf interface

Serial10/0 is up, line protocol is up
  Link Local Address 2001:DB8:1::1, Interface ID 42
  Area 1, Process ID 1, Instance ID 0, Router ID 10.0.0.1
  Network Type POINT_TO_POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT, BFD enabled
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:07
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 10.1.0.1
  Suppress hello for 0 neighbor(s)
```

For more information about how to configure BFD, refer to Implementing Bidirectional Forwarding Detection for IPv6.

Multiprotocol BGP

Example: IPv6 VPN Configuration Using IPv4 Next Hop

The following example illustrates a 6VPE next hop:

```
interface Loopback0
 ip address 192.168.2.11 255.255.255.255
!
router bgp 100
 neighbor 192.168.2.10 remote-as 100
 neighbor 192.168.2.10 update-source Loopback0
!

 address-family vpnv6
 neighbor 192.168.2.10 activate
 neighbor 192.168.2.10 send-community extended
 exit-address-family
```

By default, the next hop advertised will be the IPv6 VPN address:

```
[0:0]::FFFF:192.168.2.10
```

Note that it is a 192-bit address in the format of [RD]::FFFF:IPv4-address.

When the BGP IPv6 VPN peers share a common subnet, the MP_REACH_NLRI attribute contains a link-local address next hop in addition to the global address next hop. This situation typically occurs in an interautonomous-system topology when ASBRs are facing each other. In that case, the link-local next hop is used locally, and the global next hop is readvertised by BGP.

The BGP next hop is the keystone for building the label stack. The inner label is obtained from the BGP NLRI, and the outer label is the label distribution protocol (LDP) label to reach the IPv4 address embedded into the BGP next hop.

For more information about how to configure multiprotocol BGP, refer to Implementing Multiprotocol BGP for IPv6.

DHCP

The following examples show how to configure DHCP for IPv6:

- Stateful DHCP—Server
- Stateful DHCP—Client
- Stateless DHCP—Server
- Stateless DHCP—Client

Stateful DHCP—Server

```
ipv6 dhcp pool dhcp-pool
prefix-delegation pool client-prefix-pool1 lifetime 1800 600
dns-server 2001:0DB8:3000:3000::42
domain-name example.com

interface vlan 102
ipv6 address 102::2/64
ipv6 dhcp server dhcp-pool
ipv6 local pool client-prefix-pool1 2001:0DB8:1200::/48 48
```

Stateful DHCP—Client

```
interface vlan 102
ipv6 dhcp client pd prefix-from-provider
interface vlan 101
ipv6 address prefix-from-provider 2001:0DB8::5:0:0:0:100/64
```

Stateless DHCP—Server

```
ipv6 dhcp pool dhcp-pool
dns-server 2001:0DB8:3000:3000::42
domain-name example.com

interface vlan 102
ipv6 address 2001:0DB8:1234:42::1/64
ipv6 dhcp server dhcp-pool
```

Stateless DHCP—Client

```
interface vlan 102
ipv6 address autoconfig
```

For more information about how to configure DHCP, refer to Implementing DHCP for IPv6.

IS-IS

The following example shows how to configure IS-IS routing for IPv6 traffic.

```
interface Vlan306
 mtu 4470
 ip address 10.36.1.1 255.255.255.0
 no ptp enable
 ipv6 address 2001:DB8:1::1/64
 ipv6 enable
 ipv6 router isis isis-600-1
 mpls ip
 bfd interval 150 min_rx 50 multiplier 3
!
router isis isis-600-1
 net net 2001:DB8.0000.0000.0003.00
 bfd all-interfaces
 !
 address-family ipv6
  maximum-paths 3
 exit-address-family
!
```

For more information about how to configure IS-IS for IPv6, refer to Implementing IS-IS for IPv6.

Network Management

```
aaa new-model
ip domain name example.com
username myusername password 0 mypassword
crypto key generate rsa
  int vlan 102
ipv6 address 2001:DB8::2/64
```

For more information about how to configure network management for IPv6, refer to Implementing IPv6 for Network Management.

IPv6 over MPLS

The following example shows how to configure IPv6 over MPLS.

```
router bgp 100
bgp router-id 192.168.1.1
bgp log-neighbor-changes
no bgp default route-target filter
no bgp default ipv4-unicast
neighbor 10.0.4.4 remote-as 100
neighbor 10.0.4.4 update-source Loopback0
!
address-family ipv4
  neighbor 10.0.4.4 activate
  no auto-summary
exit-address-family
!
address-family ipv6
  redistribute ospf 6
  network 2001:DB8:0::/64
  network 2001:DB8:1::/64

  neighbor 10.0.4.4 activate
  neighbor 10.0.4.4 send-label
exit-address-family
!
```

For more information about how to configure IPv6 over MPLS, refer to Implementing IPv6 over MPLS.

IPv6 VPN over MPLS

The following example shows how to configure an IPv6 VPN over MPLS (6VPE).

```
vrf definition B
rd 52:62

address-family ipv4
  route-target export 52:62
  route-target import 52:62
exit-address-family
!
address-family ipv6
  route-target export 52:62
  route-target import 52:62
exit-address-family
!


vrf definition C
rd 53:63
!
address-family ipv4
  route-target export 53:63
  route-target import 53:63
exit-address-family
!
address-family ipv6
  route-target export 53:63
  route-target import 53:63
exit-address-family

interface Vlan52
vrf forwarding B
ipv6 address 2001:DB8:0:1/64
ipv6 enable
!
interface Vlan53
vrf forwarding C
```

```
ipv6 address 2001:DB8:1:1/64
ipv6 enable
!

router bgp 100
bgp router-id 1.1.1.1
bgp log-neighbor-changes
no bgp default route-target filter
no bgp default ipv4-unicast
neighbor 10.10.4.4 remote-as 100
neighbor 10.10.4.4 update-source Loopback0
!
address-family ipv4
  neighbor 10.10.4.4 activate
  no auto-summary
exit-address-family
!
address-family vpnv6
  neighbor 10.10.4.4 activate
  neighbor 10.10.4.4 send-community both
exit-address-family
!

address-family ipv6 vrf B
  redistribute connected
  redistribute static
exit-address-family
!
address-family ipv6 vrf C
  neighbor 2001:DB8:100:1:: remote-as 104
  neighbor 2001:DB8:100:1:: activate

exit-address-family
```

For more information about how to configure IPv6 VPN over MPLS, see Implementing IPv6 VPN over MPLS.

OSPFv3

The following example shows to to configure OSPF version 3 in order to route IPv6 traffic.

```
!
interface Vlan405
 ip address 192.168.1.2 255.255.255.0
 no ptp enable
 ipv6 address 2001:DB8:1::2/64
 ipv6 ospf 600 area 200
 mpls ip
 bfd interval 250 min_rx 100 multiplier 3

ipv6 router ospf 600
 router-id 10.0.5.6
 bfd all-interfaces
 event-log size 5 one-shot
 timers throttle spf 200 500 5000
 timers throttle lsa 0 20 5000
 timers lsa arrival 15
 timers pacing flood 15
!
```

For more information about how to configure OSPF v3, see Implementing OSPF for IPv6.

QoS

The following partial configuration examples show how to use QoS features on a network with IPv4 and IPv6 traffic:

- Applying Ingress QoS to IPv6 Traffic
- Applying Ingress QoS to IPv4 Traffic
- Applying Ingress QoS to IPv4 and IPv6 Traffic
- Applying Egress QoS to IPv4 and IPv6 Traffic

Applying Ingress QoS to IPv6 Traffic

The following example classifies IPv6 traffic based on DSCP value and marks the traffic with a CoS and QoS group value.

```
class-map match-all ipv6_llq
  match protocol ipv6
  match dscp af43 af41 cs6 cs7
class-map match-all ipv6_premium
  match protocol ipv6
  match dscp af33, af13
class-map match-all ipv6_hsps
  match protocol ipv6
  match dscp af12

policy-map input-policy
 class ipv6_llq
  set cos 5
  set qos-group 5
 class ipv6_prem
  set qos-group 4
  set cos 4
 class ipv6_hsps
  set cos 3
  set qos-group 3

interface GigabitEthernet0/4
 switchport access vlan 1000
 switchport mode access
 service-policy input input-policy
```

Applying Ingress QoS to IPv4 Traffic

The following example classifies IPv4 traffic based on DSCP value and marks the traffic with a CoS and QoS group value.

```
class-map match-all ipv4_proto
   match protocol ip
   match dscp af11  af23  af33  af43

policy-map input-policy
 class ipv4_proto
  set cos 5
  set qos-group 5

interface GigabitEthernet0/4
 switchport access vlan 1000
 switchport mode access
 service-policy input input-policy
```

Applying Ingress QoS to IPv4 and IPv6 Traffic

The following example classifies both IPv4 and IPv6 traffic based on the DSCP value and marks the traffic with a CoS and QoS group value.

```
class-map match-any llq
  match dscp ef
  match dscp af43
  match dscp af41
  match dscp cs7
  match dscp cs6

policy-map input-policy
 class llq
  set cos 5
  set qos-group 5

interface GigabitEthernet0/4
 switchport access vlan 1000
 switchport mode access
 service-policy input input-policy
```

Applying Egress QoS to IPv4 and IPv6 Traffic

The following example performs the following QoS functions:

- Matches all IPv4 and IPv6 traffic based on QoS group
- Applies egress queuing based on QoS group
- Applies egress shaping to all traffic

```
class-map match-all q0
 match qos-group 0
class-map match-all q1
 match qos-group 1
class-map match-all q2
 match qos-group 2
class-map match-all q3
 match qos-group 3

policy-map child_policy_egress
 class q3
  priority percent 60
 class q2
  bandwidth remaining percent 50
 class q1
  bandwidth remaining percent 45
class q0
  bandwidth remaining percent 4
policy-map parent_policy_egress
 class class-default
  shape average 380000000
  service-policy child_policy_egress

interface GigabitEthernet0/5
 switchport trunk allowed vlan 331
 switchport mode trunk
 service-policy output parent_policy_egress
```

For more information about how to configure QoS for IPv6, see Implementing QoS for IPv6.

Support for New MIBs

Release15.1(1)MR introduces support for the following MIBs:

- IP-MIB
- IP-FORWARD-MIB
- CISCO-IETF-BFD-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FLASH-MIB

For more information about these MIBs and limitations, see IPv6 MIBs, page 33

T1 and E1 Local Switching

Release15.1(1)MR introduces support for T1 and E1 local switching. You can use the following commands to configure T1 and E1 local switching:

- **tdm-group**—Configures a list of time slots for creating clear channel groups (pass-through) for time-division multiplexing (TDM) cross-connect.
- **connect**—Defines connections among T1 or E1 controller ports for drop-and-insert (also called TDM cross-connect).

Note Local switching is only supported between onboard T1 and E1 ports; local switching between HWIC T1 and E1 ports is not supported.

Note You cannot add a TDM-GROUP to a controller where the CEM-GROUP is defined. Channel-group also conflicts with CEM-GROUP, which cannot coexist.

For more information about these commands, see the *Cisco MWR 2941 Router Command Reference, Release 15.1(1)MR*.

Configuring T1 and E1 Local Switching

Follow these steps to configure T1 and E1 local switching

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**controller** {**t1** | **e1**} *slot/port*	Enter T1 or E1 controller configuration mode.
Step 3	**tdm-group** *tdm-group-no* **timeslot** *timeslot-list*	Specify the TDM group and timeslots for which you want to enable local switching.
Step 4	**controller** {**t1** | **e1**} *slot/port*	Enter T1 or E1 controller configuration mode for the second controller.
Step 5	**tdm-group** *tdm-group-no* **timeslot** *timeslot-list*	Specify the second set TDM group and timeslots for which you want to enable local switching.
Step 6	**exit**	Exit controller configuration mode.
Step 7	**connect** *connection-id* {**t1** | **e1**} *slot/port-1 tdm-group-no-1* {**t1** | **e1**} *slot/port-2 tdm-group-no-2*	Use the connect command to enable local switching.
Step 8	**show connection**	(Optional) Use the **show connection** command to verify your configuration.

Configuration Examples

The following examples show how to use T1 and E1 local switching:

TDM Local Switching—E1

```
controller E1 0/0
 tdm-group 0 timeslots 1-31
controller E1 0/1
 tdm-group 0 timeslots 1-31
connect st E1 0/0 0 E1 0/1 0
```

TDM Local Switching—T1

```
controller T1 0/0
 tdm-group 0 timeslots 1-24
controller T1 0/1
 tdm-group 0 timeslots 1-24
connect stanley T1 0/0 0 T1 0/1 0
```

Non-Channelized Local Switching

```
controller E1 0/0
 tdm-group 0 timeslots 1-31

controller E1 0/1
 tdm-group 0 timeslots 1-31

connect st1 E1 0/0 0 E1 0/1 0
```

Channelized Local Switching

```
controller E1 0/0
 tdm-group 0 timeslots 1-10
 tdm-group 1 timeslots 11-20

controller E1 0/1
tdm-group 0 timeslots 1-10
 tdm-group 1 timeslots 11-20

connect st1 E1 0/0 0 E1 0/1 0
connect st2 E1 0/0 1 E1 0/1 1
```

Channelized Local Switching on Multiple Channels

```
controller E1 0/0
 tdm-group 0 timeslots 1-10
 tdm-group 1 timeslots 11-20
tdm-group 2 timeslots 21-25
tdm-group 3 timeslots 26-31
```

```
controller E1 0/1
tdm-group 0 timeslots 1-10
 tdm-group 1 timeslots 11-20
tdm-group 2 timeslots 21-25
tdm-group 3 timeslots 26-31

connect st1 E1 0/0 0 E1 0/1 0
connect st2 E1 0/0 1 E1 0/1 1
connect st3 E1 0/0 2 E1 0/1 2
connect st4 E1 0/0 3 E1 0/1 3
```

Channelized Local Switching with Segmented Timeslots

```
controller E1 0/0
 tdm-group 0 timeslots 1,3,20-22
 tdm-group 1 timeslots 24,26,29-30
controller E1 0/1
tdm-group 0 timeslots 1,3,20-22
 tdm-group 1 timeslots 24,26,29-30

connect st1 E1 0/0 0 E1 0/1 0
connect st2 E1 0/0 1 E1 0/1 1
```

Ethernet Loopback

You can use per-port and per-VLAN Ethernet loopback to test connectivity at initial startup, to test throughput, and to test quality of service (QoS) in both directions.

This feature introduces the following new commands for Ethernet loopback:

- **ethernet loopback facility**—Configures per-port loopbacks for testing connectivity across multiple devices.
- **ethernet loopback**—Starts or stop an Ethernet loopback function on an interface.
- **show ethernet loopback**—Displays the Ethernet loopbacks configured on the switch or the specified interface.

Note Ethernet loopback is only supported on onboard Gigabit Ethernet interfaces; it is not supported on HWIC Ethernet interfaces.

For more information about these commands, see the *Cisco MWR 2941 Router Command Reference, Release 15.1(1)MR*.

Configuring Ethernet Loopback

Follow these steps to use Ethernet loopback on the Cisco MWR 2941:

Caution The Cisco MWR 2941 does not support Ethernet loopback while keepalive messages are enabled on the remote Ethernet interface. Before beginning Ethernet loopback on the Cisco MWR 2941, ensure that you disable keepalive messages on the remote Ethernet interface. If the remote Ethernet interface is a Cisco MWR 2941, use the **no keepalive** command to disable keepalive messages. When you have completed testing and disabled Ethernet loopback, use the **keepalive [***period* **[***retries***]]** command to enable keepalive messages.

Caution Loopback is supported only in a single direction over an Ethernet link; the Cisco MWR 2941 does not support bidirectional loopback.

	Command	Purpose
Step 1	**clear mac-address-table [dynamic | secure] [address** *mac-address*] **[interface** *type slot/port* **| vlan** *vlan-id*]	Clear the MAC address table on the router.
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**no mac-address-table learning {vlan** *vlan-id* **| interface** *interface slot/port***}**	Disable MAC address learning on the router.
Step 3	**interface** *interface-id*	Specify the Ethernet interface on which you want to enable Ethernet loopback.
Step 4	**ethernet loopback facility** [**vlan** *vlan-id*] **swap** [**timeout** {*seconds* | **none**}]	Configure the loopback parameters for the interface.
Step 5	**ethernet loopback** {**start** *interface-id* | **stop** {*interface-id* | **all**}}	Enable Ethernet loopback on the interface.
Step 6	**ethernet loopback** {**start** *interface-id* | **stop** {*interface-id* | **all**}}	Disable Ethernet loopback on the interface. You can specify a single interface or use the **all** keyword to disable loopback on all Ethernet interfaces.
Step 7	**exit**	Exit interface configuration mode.
Step 8	**mac-address-table learning {vlan** *vlan-id* **| interface** *interface slot/port***}**	Enable MAC address learning on the router.
Step 9	**show ethernet loopback** [*interface-id*] [| {**begin | exclude | include**} *expression*]	Displays the Ethernet loopbacks configured on the router or the specified interface.

Two-Way Active Measurement Protocol

Two-Way Active Measurement Protocol (TWAMP) is an IETF standard that defines a flexible method for measuring round-trip IP performance between any two devices that support the standard. With TWAMP, IP performance of the underlying transport can be measured between network elements that incorporate the TWAMP standards. TWAMP functionality encompasses a Control-Client and Session Sender, and Server and Session-Reflector. Specific parts of this functionality can be co-located or distributed among various network elements. The MWR-2941 implements TWAMP function as Session-reflector and Sever which will be tested based on RFC 5357.

This feature introduces the following new commands:

- **ip sla responder twamp**—Configures the router as a TWAMP responder and enters TWAMP configuration mode.
- **ip sla server twamp**—Configures the router as a TWAMP server and enters TWAMP configuration mode.
- **show ip sla twamp connection**—Display information about TWAMP connections.
- **show ip sla twamp session**—Display information about TWAMP test results for the specified client.

- **show ip sla twamp standards**—Displays the IP SLA standards for TWAMP that are supported on the device.

Configuring TWAMP

The following sections describe how to configure TWAMP:

- Configuring the TWAMP Server
- Configuring the TWAMP Reflector

Configuring the TWAMP Server

The TWAMP server and reflector functionality are configured on the same device.

Note The Cisco MWR 2941 does not support the TWAMP sender and client roles.

Follow these steps to configure the TWAMP server:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip sla server twamp**	Configure the router as a TWAMP server, and enter TWAMP configuration mode.
Step 3	**port** *port-number*	(Optional) Specify the port to be used by the TWAMP server to listen for connection and control requests. The same port negotiates for the port to which performance probes are sent. The configured port should not be an IANA well-known port or any port used by other applications. The default is port 862.
Step 4	**timer inactivity** *seconds*	(Optional) Set the maximum time, in seconds, the session can be inactive before the session ends. The range is 1–6000 seconds. The default is 900 seconds.
Step 5	**end**	Return to privileged EXEC mode.
Step 6s	**show ip sla twamp standards**	(Optional) Display the IP SLA standards for TWAMP that are supported on the device.
Step 7	**show ip sla twamp connection requests**	(Optional) Display the number and the source of TWAMP connections.
Step 8	**show ip sla twamp connection detail**	(Optional) Display the connection ID, client IP address and port number, mode and status of TWAMP connections, and the number of test requests.
Step 9	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Note When configuring the TWAMP client, ensure that the session-sender timeout value is greater than 0. If you configure the timeout value as 0, the Cisco MWR 2941 will wait 3 hours before clearing the TWAMP session from memory.

To disable the IP SLA TWAMP server, enter the **no ip sla server twamp** global configuration command. This example shows how to configure a switch as an IP SLA TWAMP server:

```
Router(config)# ip sla server twamp
Router(config-twamp-srvr)# port 9000
```

```
Router(config-twamp-srvr)# timer inactivity 300
```

Configuring the TWAMP Reflector

The TWAMP server and reflector functionality are both configured on the same device.

Beginning in privileged EXEC mode, follow these steps to configure the TWAMP reflector:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip sla responder twamp**	Configure the router as a TWAMP responder, and enter TWAMP configuration mode.
Step 3	**timeout** *seconds*	(Optional) Set the maximum time, in seconds, the session can be inactive before the session ends. The range is 1–604800 seconds. The default is 900 seconds.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show ip sla twamp session** [**source-ip** *ip-address* **source-port** *port-number*]	(Optional) Display information about TWAMP test results for the specified client.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

To disable the IP SLA TWAMP reflector, enter the **no ip sla responder twamp** global configuration command. This example shows how to configure a device as an IP SLA TWAMP reflector:

```
Router(config)# ip sla responder twamp
Router(config-twamp-srvr)# timeout 300
```

New Hardware Features in Release 15.0(2)MR

There are no new hardware features in Release 15.0(2)MR.

New Software Features in Release 15.0(2)MR

Release 15.1(1)MRA introduces the following new software features:

- PTP Boundary Clock—Release 15.0(2)MR introduces support for PTP boundary clock based on the 1588 version 2 standard. You can configure the router as a PTP boundary clock using the **ptp mode** global command and the **ptp boundary** interface command, as shown in the following example.

```
Router# configure terminal
Router(config)# ptp mode boundary
Router(config)# ptp priority1 128
Router(config)# ptp priority2 128
Router(config)# ptp domain 1
Router(config)# interface Vlan1
Router(config-if)# ip address 192.168.1.2 255.255.255.0
Router(config-if)# ptp announce interval 3
Router(config-if)# ptp announce timeout 2
Router(config-if)# ptp sync interval -4
Router(config-if)# ptp delay-req interval -4
Router(config-if)# ptp boundary unicast-negotiation
Router(config-if)# ptp clock-source 192.168.1.1
Router(config-if)# ptp enable
```

For more information about how to configure PTP boundary clock, see the *Cisco MWR 2941 Mobile Wireless Edge Router Software Configuration Guide, Release 15.0(1)MR* and the *Cisco MWR 2941 Router Command Reference, Release 15.0(1)MR*.

New Hardware Features in Release 15.0(1)MR

There are no new hardware features in Release 15.0(1)MR.

New Software Features in Release 15.0(1)MR

Release 15.0(1)MR introduces the following new software features:

- REP Age Timer—You can configure how long a REP interface remains up without receiving a hello from a neighbor. You can use the **rep lsl-age-timer** value interface configuration command to set the time from 120 ms to 10000 ms. The LSL hello timer is then set to the age-timer value divided by three. In normal operation, three LSL hellos are sent before the age timer on the peer switch expires and searches for hello messages.
- SSM/ESMC—Provides clock frequency synchronization on SONET/SDH and synchronous Ethernet links. The SSM/ESMC feature introduces the following new commands:
  - **esmc mode ql-disabled**—Disables quality level mode on a synchronous Ethernet interface.
  - **esmc mode**—Enables ESMC messages on an interface.
  - **esmc process**—Enables the router to send and receive ESMC messages on synchronous Ethernet interfaces.
  - **network-clock clear wait-to-restore**—Stops the wait-to-restore timer for a clock source.
  - **network-clock eec**—Specifies the Ethernet Equipment Clock (EEC) type.
  - **network-clock external hold-off**—Overrides the hold-off timer value for an external interface.
  - **network-clock hold-off**—Configures a hold-off value on an interface.
  - **network-clock hold-off global**—Configures a general hold-off timer.
  - **network-clock input-source**—Selects an interface or external timing input as a clock source and sets a priority for the clock.
  - **network-clock output-source**—Configures the router to transmit clocking to an external timing source using a timing output interface.
  - **network-clock output-source line**—Transmits clocking received from an external source to another external device using timing output interfaces.
  - **network-clock quality-level**—Specifies a quality level for a line or external timing device.
  - **network-clock revertive**—Specifies whether the router reverts to a higher priority clock when it becomes available.
  - **network-clock source quality-level**—Specifies a quality level for a clock source.
  - **network-clock synchronization automatic**—Enables automatic selection of a clock synchronization source.
  - **network-clock synchronization mode ql-enabled**—Enables automatic selection of a clock source based on quality level (QL).

  - **network-clock synchronization participate**—Configures the router to exchange timing messages using the G.781 synchronization option 1 or 2.
  - **network-clock synchronization ssm option**—Configures the router to exchange timing messages using the G.781 synchronization option 1 or 2.
  - **network-clock wait-to-restore**—Configures the amount of time that an interface waits before reverting to a restored clock source.
  - **network-clock wait-to-restore global**—Configures the amount of time that the router waits before reverting to a restored clock source.
  - **sabit**—Specifies the S_{an} status bit used to indicate clock quality level for the Synchronization Status Message (SSM) in synchronous Ethernet.
  - **ssm**—Enables sync status message

- PTP on multiple VLANs— You can enable PTP on up to three VLANs at a time using the **ptp enable** command. The following restrictions apply:
  - All PTP-enabled VLANs must use PTP master or PTP slave; you cannot configure PTP master and PTP slave VLANs at the same time.
  - All PTP-enabled VLANs must use multicast or unicast, but not both.
- CFM Extension for Microwave 1+1 Hot Standby (HSBY)—The Nokia Siemens Networks (NSN) Microwave 1+1 Hot Standby Protocol (HSBY) feature extends CFM Continuity Check messages to enable detection and handling of hardware failures with microwave outdoor units (ODUs). The feature also adds support for non-Cisco TLVs within Continuity Check messages. In this protection protocol, the MWR 2941 acts as the indoor unit (IDU).

  The HSBY feature introduces the following commands:
  - **link-protection enable**—Globally enables HSBY protocol on the router.
  - **link-protection group**—Specifies the HSBY link-protection group of which the MEP interface is a member.
  - **link-protection management vlan**—Specifies the management VLAN used for all configured link protection groups for HSBY protocol.
  - **link-protection group pccm vlan**—Specifies the VLAN used for ODU-to-ODU Continuity Check Messages (P–CCMs) for HSBY protocol.
  - **show link-protection**—Displays the status of configured link protection groups.
  - **show link-protection statistics**—Displays the counters for each link protection port.
  - **clear link-protection statistics**—Clears the counters for a link protection port.
- CFM 802.1ag—Release 15.0(1)MR introduces support for the IEEE 802.1ag–2007 version of Ethernet OAM Connectivity Fault Management (CFM), which is the standard for Layer 2 ping, Layer 2 traceroute, and end-to-end connectivity check of the Ethernet network.

Note Release 15.0(1)MR does not support the 802.1ag Draft 1 version of CFM.

  Release 15.0(1)MR also supports Ethernet Link Management Interface (E-LMI), which enables Customer Edge (CE) devices to receive notifications and status information for remote User Network Interfaces (UNIs) and Ethernet Virtual Connections (EVC).

  This feature introduces the following new commands:
  - **ais**—Enables the Alarm Indication Signal (AIS) function for a specific maintenance association.

- **alarm** —Configures an alarm when fault alarms are enabled.
- **clear ethernet cfm ais domain**—Clears a maintenance endpoint (MEP) or server maintenance endpoint (SMEP) out of the Alarm Indication Signal (AIS) defect condition.
- **clear ethernet cfm maintenance-points remote**—Purges the contents of the continuity check database.
- **clear ethernet cfm statistics**—Clears a maintenance endpoint (MEP) or server maintenance endpoint (SMEP) out of the Alarm Indication Signal (AIS) defect condition.
- **clear ethernet cfm traceroute-cache**—Removes the contents of the Ethernet CFM traceroute cache.
- **continuity-check**—Enables the transmission of continuity check messages (CCMs) for a maintenance association.
- **cos**—Sets the class of service (CoS) for a maintenance endpoint (MEP) that will be sent in Ethernet connectivity fault management (CFM) messages.
- **disable**—Disable the generation of Alarm Indication Signal (AIS) frames resulting from a link-status change on a server maintenance endpoint (SMEP).
- **ethernet cfm ais link-status**—Enables Alarm Indication Signal (AIS) generation from a server maintenance endpoint (SMEP).
- **ethernet cfm alarm**—Configures Ethernet connectivity fault management (CFM) alarm settings.
- **ethernet cfm global**—Enables Ethernet connectivity fault management (CFM) globally on a device.
- **ethernet cfm ieee**—Enables the Ethernet Connectivity Fault Management 802.1ag Standard (CFM IEEE) version of CFM.
- **ethernet cfm interface**—Enables Ethernet connectivity fault management (CFM) processing on a port.
- **ethernet cfm mep crosscheck**—Enables cross-checking between the list of configured remote maintenance endpoints (MEPs) of a domain and MEPs learned through continuity check messages (CCMs).
- **ethernet cfm mip**—Globally provisions maintenance intermediate points (MIPs) at a specified maintenance level for VLAN IDs that are not associated with specific maintenance associations (MAs). You can also use this command to enable level filtering.
- **id**—Configures a maintenance domain identifier (MDID).
- **level**—Configures a maintenance level to receive Alarm Indication Signal (AIS) frames transmitted by a link-status change on a server maintenance endpoint (SMEP).
- **maximum meps**—Specifies the number of maintenance endpoints (MEPs) across the network in a maintenance association.
- **mep archive hold-time**—Specifies the amount of time that data from a missing maintenance end point (MEP) is kept in the continuity check database or that entries are held in the error database before they are purged.
- **mip auto-create**—Enables the automatic creation of a maintenance intermediate point (MIP) at a maintenance domain level.
- **mep crosscheck mpid**—Statically defines a remote maintenance endpoint (MEP) within a maintenance domain.

  - **mep mpid**—Statically defines the maintenance endpoints (MEPs) within a maintenance association.
  - **period**—Configures a specific Alarm Indication Signal (AIS) transmission interval on a server maintenance endpoint (SMEP).
  - **ping ethernet**—Sends Ethernet connectivity fault management (CFM) loopback messages to a destination maintenance endpoint (MEP).
  - **ping ethernet vlan**—Sends Ethernet connectivity fault management (CFM) loopback messages to a maintenance endpoint (MEP) or maintenance intermediate point (MIP) destination.
  - **sender-id**—Indicate the contents of the Sender ID TLV field transmitted in Ethernet connectivity fault management (CFM) messages for the maintenance association.
  - **service**—Configures a maintenance association within a maintenance domain and enters CFM service configuration mode.
  - **show ethernet cfm errors**—Displays connectivity fault management (CFM) continuity check error conditions logged on a device since it was last reset or since the log was last cleared.
  - **show ethernet cfm maintenance-points local**—Displays information about maintenance points configured on a device.
  - **show ethernet cfm maintenance-points remote detail**—Displays information about a remote maintenance point in the continuity check database**.**
  - **show ethernet cfm maintenance-points remote domain**—Displays detailed information about remote maintenance endpoints (MEPs) configured statically in the MEP list and their status in the continuity check database (CCDB).
  - **show ethernet cfm mpdb**—Display the contents of a maintenance intermediate point (MIP) continuity check database (CCDB).
  - **show ethernet cfm smep**—Displays connectivity fault management (CFM) system maintenance end point (SMEP) settings on a device.
  - **show ethernet cfm traceroute-cache**—Displays the contents of the traceroute cache.
  - **traceroute ethernet**—Send Ethernet connectivity fault management (CFM) traceroute messages to a destination maintenance endpoint (MEP).

  This feature modifies the following commands:

  - **ethernet cfm domain level**—Release 15.0(1)MR does not support the **direction outward** keywords.
  - **show ethernet cfm maintenance-points remote**—Release 15.0(1)MR does not support the **level** keyword.
  - **show ethernet cfm maintenance-points remote detail**—This command is updated to include the suspend state in the command output. Additionally, the **level** keyword is not supported in this release.

- Spanning Tree Features

  Release 15.0(1)MR supports the following spanning tree features:

  - Multiple Spanning Tree Protocol (MSTP)—MSTP is defined in the IEEE 802.1s standard and enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs. MSTP provides for multiple forwarding paths for data traffic and enables load balancing. MSTP improves the fault tolerance of a network because it ensures that a failure on one forwarding path (MSTP instance)

does not impact traffic on other forwarding paths. MSTP is commonly deployed on the backbone and distribution layers of a Layer 2 switched network, providing the high availability required in a service-provider environment.

- Rapid Spanning Tree Protocol (RSTP)—RSTP is defined by the IEEE 802.1W standard and improves Spanning Tree Protocol (STP) convergence. RSTP provides rapid convergence by using an explicit handshake, eliminating forwarding delay and improving the speed at which designated and root bridge ports move to a forwarding state. The rapid reconvergence provided by RSTP supports delay-sensitive traffic such as voice and video.
- Disabling MAC Learning—Allows you to manage the available MAC address table space by limiting which VLANs can learn MAC addresses.

This feature introduces the following new commands:

- **abort/exit**—Exits the MST configuration submode.
- **clear spanning-tree counters**—Clears the spanning-tree protocol counters.
- **clear spanning-tree detected protocol**—Forces an MST port to renegotiate with the neighbors, restarting the protocol migration process.
- **instance**—Maps a VLAN or a group of VLANs to a multiple spanning tree (MST) instance.
- **mac address-table learning**—Enables MAC-address learning.
- **name**—Sets the name of a Multiple Spanning Tree (MST) region.
- **private-vlan synchronize**—Maps the secondary VLANs to the same instance as the primary VLAN.
- **revision**—Sets the revision number for the MST configuration.
- **show**—Displays the Multiple Spanning Tree (MST) configuration.
- **show mac address-table learning**—Displays the MAC-address learning state.
- **show spanning-tree mst**—Displays information about the Multiple Spanning Tree (MST) protocol.
- **spanning-tree bpdufilter**— Enables bridge protocol data unit (BPDU) filtering on an interface.
- **spanning-tree bpduguard**—Enables bridge protocol data unit (BPDU) guard on an interface.
- **spanning-tree guard**—Enables or disables STP guard mode.
- **spanning-tree link-type**—Configures the link type for a port.
- **spanning-tree loopguard default**—Enables loop guard as a default on all ports of a given bridge.
- **spanning-tree mode**—Switches between Per-VLAN Spanning Tree+ (PVST+) and Multiple Spanning Tree (MST) modes.
- **spanning-tree mst**—Sets the path cost and port-priority parameters for a Multiple Spanning Tree (MST) instance.
- **spanning-tree mst configuration**—Enters MST-configuration submode.
- **spanning-tree mst forward-time**—Sets the forward-delay timer for all the instances on the router.
- **spanning-tree mst hello-time**—Sets the hello-time delay timer for all the instances on the router.
- **spanning-tree mst max-age**—Sets the max-age timer for all the instances on the router.
- **spanning-tree mst max-hops**—Specifies the number of possible hops in the region before a bridge protocol data unit (BPDU) is discarded.
- **spanning-tree mst priority**—Specifies a bridge priority for the spanning tree.

  - **spanning-tree mst root**—Designates the primary and secondary root, sets the bridge priority, and sets the timer value for an MST instance.
  - **spanning-tree portfast**—Enables PortFast mode, where the interface is immediately put into the forwarding state upon linkup without waiting for the timer to expire.
  - **spanning-tree portfast bpdufilter**—Enables bridge protocol data unit (BPDU) filtering on an interface.
  - **spanning-tree portfast bpduguard**—Enables bridge protocol data unit (BPDU) guard on the interface.
  - **spanning-tree portfast bpdufilter default**—Enables BPDU filtering on all ports that are already configured for PortFast.
  - **spanning-tree portfast bpduguard default**—Enables BPDU guard on all ports that are already configured for PortFast.
  - **spanning-tree portfast default**—Enables PortFast by default on all access ports.

- CEF Load Sharing of Equal Cost Paths— The CEF Equal Cost Paths feature allows you to define one or more paths to a destination and shares traffic across the available paths of the same cost. CEF defines two types of load sharing: per-packet load sharing, which splits all traffic evenly across the available paths and per-destination load sharing, which balances traffic while ensuring the traffic bound for the same destination uses the same path.

  Release 15.0(1)MR introduces support for per-destination load balancing. You can configure per-destination load sharing on Ethernet ports, VLANs, MLPPP bundles, or pseudowires.

  This feature introduces support for the following commands:

  - **ip cef load-sharing algorithm universal**—Sets the load sharing algorithm to the universal algorithm that uses a source and destination, and ID hash.
  - **ip cef load-sharing algorithm include**-ports source destination—Sets the load sharing algorithm to the include-ports algorithm that uses source IP, source port, destination IP, destination port and ID hash.
  - **ip load-sharing per-destination**—Per-destination load balancing is enabled by default when you enable Cisco Express Forwarding
  - **show ip cef exact-route**—To display the exact route for a source-destination IP address pair, use the show ip cef exact-route command in user EXEC or privileged EXEC mode
  - **show ip cef exact-route platform**—To display the exact route in platform for a source-destination IP address pair, use the show ip cef exact-route platform command in user EXEC or privileged EXEC mode

- 802.1Q Tunneling—802.1Q tunneling enables service providers to use a single VLAN to support customers who have multiple VLANs, while preserving customer VLAN IDs and keeping traffic in different customer VLANs segregated. Release 15.0(1)MR provides support for the following 802.1Q tunneling features:
  - Cisco QinQ—A Cisco implementation of 802.1Q that a dds an extra layer of 802.1Q tags to 802.1Q-tagged packets that enter the network. The extra tagging layer provided by QinQ allows you to expand the available VLAN space in the network by mapping multiple customer VLANs to a single service provider VLAN.
  - Layer 2 Protocol Tunneling (L2PT)—Layer 2 protocol tunneling allows Layer 2 protocol data units (PDUs) (CDP, STP, and VTP) to be tunneled through a network. L2PT allows tunnel ports to process STP, VTP, and CDP packets by creating separate spanning tree domains (different spanning tree roots) for customer switches.

This feature introduces support for the following commands:

- **clear l2protocol-tunnel counters**—Clears the layer 2 tunnel protocol counters on the router.
- **dot1q tunneling ethertype**—Defines the Ethertype field type used by peer devices when implementing QinQ VLAN tagging.
- **l2protocol-tunnel**—Enables the protocol tunneling on an interface and specifies the type of protocol to be tunneled.
- **l2protocol-tunnel drop-threshold**—Specifies the maximum number of packets that can be processed for the specified protocol on that interface before being dropped.
- **l2protocol-tunnel shutdown-threshold**—Specifies the maximum number of packets that can be processed for the specified protocol on that interface in one second.
- **show dot1q-tunnel**—Displays a list of 802.1Q tunnel-enabled ports.
- **show l2protocol-tunnel**—Displays the protocols that are tunneled on an individual interface or on all interfaces.
- **switchport access vlan**—Configures a VLAN when an interface is in access mode.
- **switchport mode**—Specifies the interface type for a port. You can use this command to put a switch port in access or dot1q mode.
- **switchport vlan mapping**—Maps incoming traffic from an original vlan to a translated VLAN. Traffic exiting the network is mapped from the translated VLAN to the original VLAN.
- **switchport vlan mapping enable**—Enables VLAN mapping on a switch port.

- CESoPSN over UDP—Release 15.0(1)MR allows you to configure a CESoPSN pseudowire with UDP as a transport protocol. The feature introduces the following new commands:
  - **encapsulation udp**—Configures a CESoPSN pseudowire to use UDP.
  - **udp port local** *local-port* **remote** *remote-port*—Specifies the local and remove UDP ports used for the CESoPSN pseudowire connection.
- Embedded Event Manager 3.0—Release 15.0(1)MR supports version 3.0 of Embedded Event Manager. For more information, see the Network Management Configuration Guide, Cisco IOS Release 15.0S.

  For more information about how to configure the router, see the *Cisco MWR 2941 Mobile Wireless Edge Router Software Configuration Guide, Release 15.0(1)MR*

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 15.1(1)MR2 for the Cisco MWR 2941 router has the following limitations and restrictions:

- Synchronous Ethernet is not supported on the SFP-GE-T module.
- Port channels are not supported.
- Release 15.1(1)MR2 does not support ATM over MPLS N-to-1 Cell Mode or 1-to-1 Cell Mode.
- SPAN and RSPAN are not supported.

- VLAN Query Protocol (VQP) and VLAN Management Policy Server (VMPS) are not supported
- CFM Extension for Microwave 1+1 Hot Standby (HSBY) is only supported on Gigabit Ethernet interfaces 0/0–0/5.
- CEF Limitations—Cisco Express Forwarding (CEF) has the following limitations.
  - Load balancing on GRE interfaces is not supported
  - Load balancing on IOS switch interfaces is not supported
  - Packets may choose different egress interfaces when interface is up/down
  - Up to 16 interfaces are supported for load balancing
  - SNMP traps for CEF load balancing is not supported
- Ingress vlan classification and marking is not supported on dot1q tunnel interfaces.
- Release 15.1(1)MR2 does not support the 802.1ad standard for VLAN scalability. However, the release supports supports QinQ, a Cisco-proprietary system for double-tagging.to provide VLAN scalability in the provider networks.
- Release 15.1(1)MR2 does not support the **switchport vlan mapping default drop** command.
- Release 15.1(1)MR2 does not support translation between CFM draft 1 and IEEE standardized 802.1ag CFM.
- Ethernet LCK is not supported.
- OAM Manager.is not supported.
- CFM Draft 1.0 is not supported.
- CFM for Customer VLANs (C-VLANs) is not supported.
- Ethernet Locked Signal is not supported.
- Rapid PVST+ is not supported.
- VLAN translation is not supported on HWIC interfaces.
- Rate limiting and policing are not supported on HWIC or onboard Gigabit Ethernet interfaces.
- GSM Abis optimization not supported—Release 15.1(1)MR2 does not support GSM Abis optimization feature that was supported in Release 12.4(20)MR1.
- Reduced HWIC support—Release 15.1(1)MR2 does not support the HWIC-1GE-SFP, HWIC-4SHDSL, HWIC-1ADSL, and HWIC-1ADSL-I HWICs that were supported in Release 12.4(20)MR1.
- GRE offload not supported—Release 15.1(1)MR2 does not support the GRE offload feature that was supported in Release 12.4(20)MR1.
- UMTS Iub Optimization not supported—Release 15.1(1)MR2 does not support UMTS Iub optimization.
- L2TP not supported—The MWR 2941 currently does not support L2TP.
- 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.
- 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 12.2(33)MRB*.
- 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, Release 15.1(1)MR*.

- 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.
- 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.
- PPPoA not supported—This release does not provide support for PPPoA.
- ADSL not supported—This release does not support ADSL.
- PTP Master clocking not supported—Release 15.1(1)MR2 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.
- IP Header Compression not supported—Release 15.1(1)MR2 does not support IP Header Compression or distributed IP Header Compression.
- BFD interface support limitations—Release 15.1(1)MR2 only supports BFD on switched virtual interfaces (SVIs).
- Multicast interface limitations—Multicast is only supported on VLANs and Ethernet interfaces. Multicast routing is not supported on other interface types.

- Release 15.1(1)MR2 supports up to 64 VLANs if the HWIC-D-9ESW card is in use; otherwise it supports a maximum of 255 VLANs as in previous releases.
- The Cisco MWR 2941 does not support access control lists (ACLs) for layer 3 forwarding through the network processor.
- The **show interfaces** command displays inaccurate information when used with the **counters** keyword. The counters for multicast packets display as 0 even if multicast traffic is passing on the router. To display correct multicast counters, use the **show interfaces** command without the **counters** keyword.
- The multicast packet counters in the **show interfaces** *type number* **counters** command output are set to 0 even if multicast traffic is enabled. To see accurate counters for multicast traffic, use the **show interfaces** command without the **counters** keyword.
- Virtual path-to-virtual path local switching is not supported.
- Local switching is only supported between onboard T1 and E1 ports; local switching between HWIC T1 and E1 ports is not supported.
- Ethernet loopback is only supported on onboard Gigabit Ethernet interfaces; it is not supported on HWIC Ethernet interfaces.

Supported Hardware—Cisco MWR 2941-DC Router

The Cisco MWR 2941 supports the following interface cards:

- HWIC-4T1/E1
- HWIC-D-9ESW

Note Release 15.1(1)MR2 does not support the HWIC-1GE-SFP, HWIC-4SHDSL, HWIC-1ADSL, and HWIC-1ADSL-I HWICs that were supported in Release 12.4(20)MR1.

The Cisco MWR 2941 router 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-EX-SMD
- GLC-LX-SM-RGD
- GLC-SX-MM-RGD
- GLC-ZX-SM-RGD
- SFP-GE-L
- SFP-GE-S
- 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 Mobile Wireless Edge Router Software Configuration Guide, Release 15.1(1)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-BFD-MIB
- CISCO-IETF-PW-MIB
- CISCO-IETF-PW-TC-MIB
- CISCO-IF-EXTENSION-MIB
- CISCO-IMAGE-MIB
- CISCO-MEMORY-POOL-MIB
- CISCO-PROCESS-MIB
- CISCO-PRODUCTS-MIB
- CISCO-RESILIENT-ETHERNET-PROTOCOL-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
- IP-FORWARD-MIB
- IP-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

Note Release 15.1(1)MR2 provides limited support for the CISCO-CLASS-BASED-QOS-MIB MIB for tail drop monitoring; the router supports the cbQosQueueingDiscardPkt64 object within the cbQosQueueingStatsTable table for tail drop accounting. Other objects in this table and other tables within the CISCO-CLASS-BASED-QOS-MIB are not supported.

IPv6 MIBs

Release 15.1(1)MR2 provides support for the IPv6 with the IP-MIB, IP-FORWARD-MIB, CISCO-IETF-BFD-MIB, CISCO-CONFIG-MAN-MIB, and CISCO-FLASH-MIB. The following limitations apply to these MIBs:

- IP-MIB
  - ipSystemStatsTable—Partially supported
  - ipIfStatsTable—Partially supported
  - ipAddrTable—Supported only for IPv4
  - ipNetToMediaTable—Supported only for IPv4

Note For more information about partially supported tables, see Support for the ipSystemStatsTable and ipIfStatsTable Tables.

- IP-FORWARD-MIB
  - ipCidrRouteTable—Deprecated
  - ipForwardTable—Deprecated

Support for the ipSystemStatsTable and ipIfStatsTable Tables

Table 3 summarizes the limitations for the ipSystemStatsTable and ipIfStatsTable tables; it indicates which objects within the table are supported and whether the counters for the object include forwarded packets, host-terminated packets, or both.

Table 3 ipSystemStatsTable and ipIfStatsTable Table Limitations Summary

Table	Object	Supported	Forwarded Packets Counted	Host-Terminated Packets Counted
ipSystemStatsTable	ipSystemStatsInAddrErrors			
	ipSystemStatsInTruncatedPkts			
	ipSystemStatsInForwDatagrams	X	X	X
	ipSystemStatsHCInForwDatagrams	X	X	X
	ipSystemStatsInReceives	X		X
	ipSystemStatsHCInReceives	X		X
	ipSystemStatsInOctets	X		X
	ipSystemStatsHCInOctets	X		X
ipIfStatsTable	ipIfStatsInNoRoutes			
	ipIfStatsInTruncatedPkts			
	ipIfStatsInForwDatagrams	X	X	X
	ipIfStatsHCInForwDatagrams	X	X	X
	ipIfStatsInAddrErrors			
	ipIfStatsInReceives	X		X

Table 3 ipSystemStatsTable and ipIfStatsTable Table Limitations Summary (continued)

Table	Object	Supported	Forwarded Packets Counted	Host-Terminated Packets Counted
	ipIfStatsHCInReceives	X		X
	ipIfStatsInOctets	X		X
	ipIfStatsHCInOctets	X		X

Caveats

This section documents the open and resolved caveats for the Cisco MWR 2941 router running Cisco IOS Release 15.0(1)MR 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 15.0S, go to:

http://www.cisco.com/en/US/products/ps10890/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 15.1(1)MR2

The following sections describe the caveats in Release 15.1(1)MR2.

Open Caveats

There are no open caveats in Release 15.1(1)MR2.

Closed Caveats

- CSCti98219

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCts23221

  Symptom: Add CLI to monitor internal port (to NPU) tail drop.

  Conditions: L3 traffic goes through the NPU. For bursty L3 traffic, some packets might get dropped on the internal switchport that is connected to the NPU.

  The new CLI is added: **switch tail-drop accounting winpath**.

  Workaround: None.

- CSCts33585

  Symptom: 2941 router is not responding to IPv6 ND Network Solicitation packets that are destined for its directly connected unique global IPv6 address. But it does respond to NS packets destined for the solicited multicast address.

  Conditions: Occurs when MWR-2941 router is running 15.1(1)MR IOS, configured with IPv6 unique global addressing, and connected to another router, with transit traffic flowing and static routing.

  Workaround: Use an IGP to mask the issue, or configure the static route to point to the link local address of next hop.

- CSCts45807

  Symptom: Traceback on 2941 while reloading the other connected 2941.

  Conditions: None.

  Workaround: None.

Caveats in Cisco IOS Release 15.1(1)MR1

The following sections describe the caveats in Release 15.1(1)MR1.

Open Caveats

There are no open caveats in Release 15.1(1)MR1.

Closed Caveats

- CSCti48483

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CCSCti48504

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  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-20110928-sip.shtml.

- CSCtj04672

  The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

  - NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
  - Session Initiation Protocol (Multiple vulnerabilities)
  - H.323 protocol

  All the vulnerabilities described in this document are caused by packets in transit on the affected devices when those packets require application layer translation.

  Cisco has released free software updates that address these vulnerabilities.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  - Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload
  - ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

- CSCto90222

  Symptom: Router crashed when shutting down an MLPPP member link.

  Conditions: Occurs when running 16Mbps 1500 bytes traffic over MLPPP bundle with 8 E1 members, and fragmentation is disabled on MLPPP link. If you then shut down a E1link, MWR2941 will crash.

  Workaround: Enable fragmentation on the MLPPP link.

- CSCtr24839

  Description: Increase Ethernet egress Qos buffer limits for both queue level and port level to 512.

  Conditions: For the GE interface, the queue level buffer limit was 60 and port level buffer limit was 200, which may cause TCP low throughput. Occurs when the buffer limit is reached and tail drop happens.

  Workaround: None.

- CSCtr60898

  Symptom: MWR2941-DC in IOS 15.0(1)MR or 15.0(2)MR reports incorrect ATM PVC counter values and ATM0/IMA0 input after **clear counters** command is executed.

  Conditions: Occurs when **clear counters** command is executed.

  Workaround: None.

- CSCtr63658

  Description: This is an enhancement which increases the default value of system-level switch buffer limit from 350 to 420.

  Conditions: None.

  Workaround: None.

- CSCtr74892

  Description: Average rate on VBR-RT PVCs on ATM IMA is reset to 0 cps after E1 flap.

  Conditions: Flap of E1 links that belong to ATM IMA that is configured with VBR-RT service class.

  Workaround: Reapply the configuration of VBR-RT service class under PVC config mode.

- CSCtr82589

  Description: Add a new CLI to configure global buffer limit for queueing. The buffer-limit range is 350 to 450, and default value is 420. The following example shows the new CLI:

```
2941-7(config)# switch buffer-limit ?
  <350-450>  total queue buffer limit
```

  Conditions: None.

  Workaround: None.

- CSCtr91901

  Description: MWR 2941 does not save the **network-clock-select mode revert** command in the startup configuration.

  Conditions: Occurs when the router is reloaded, after the **network-clock-select mode revert** command is accepted in the running configuration, and successfully copied to the startup configuration. When the router is reloaded, the command has been changed to **network-clock-select mode nonrevert**.

  Workaround: None.

Caveats in Cisco IOS Release 15.1(1)MR

The following sections describe the caveats in Release 15.1(1)MR.

Open Caveats

- CSCtj52205

  Symptom: An ATM/IMA interface can remain down for 30 seconds while the peer IMA interface is active; the ATM/IMA interface status is inconsistent on both sides. This can result in packet loss during the interface status transition.

Conditions: Occurs when the ATM/IMA interface status changes, due to performing a shutdown/no shutdown on the interface or removing a T1/E1 cable.

Workaround: No Workaround

- CSCto90222

  Symptom: The MWR 2941 crashes when you disable an E1 link within an MLPPP bundle.

  Conditions: Occurs under the following conditions:

  - The router is configured with an MLPPP bundle
  - The MLPPP bundle has 8 or more E1 members
  - Fragmentation is disabled on the MLPPP link
  - There is approximately 16 Mbps of traffic passing over the MLPPP bundle

  Workaround: None.

- CSCtq10011

  Symptom: The MWR 2941 displays inaccurate traffic rate counters on the serial interface.

  Conditions: Occurs when you display counters for the serial interface.

  Workaround: None.

Closed Caveats

- CSCtg89367

  Symptom: The MWR 2941 internal Ethernet tsec interface stops sending host traffic.

  Conditions: Occurs when you configure an MTU size of 4470 on a VLAN interface while OSPF routing is enabled. To verify the condition, issue the **show platform hardware ethernet tsec 1** command to see if the number of interface resets increases.

  Workaround: Use the default MTU size for the VLAN interface or apply the **ip ospf mtu-ignore** command to the VLAN interface.

- CSCth03022

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  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-20110928-sip.shtml.

- CSCti36876

  Symptom: The MWR 2941 displays traceback messages and the MLPPP link can flap when the MLPPP backhaul link is overloaded.

  Conditions: Occurs when the MLPPP bundle is overloaded.

  Workaround: None; try to keep traffic throughput below the line rate of 32 Mbps in order to avoid traceback messages.

- CSCtj63773

Symptom: The MWR 2941 **show version** output displays an incorrect configuration register value of 0x0 after a software upgrade.

Conditions: Occurs when you upgrade the router from a 12.2MR release to 15.0MR release.

Workaround: The output is incorrect; issue the **test platform hardware configreg_read** command and then issue the **show version** command again to display the correct configuration register value.

- CSCto88686

  Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS Software and Cisco IOS XE Software that could allow an unauthenticated, remote attacker to cause a reload of an affected device or trigger memory leaks that may result in system instabilities. Affected devices would need to be configured to process SIP messages for these vulnerabilities to be exploitable.

  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-20110928-sip.shtml.

Caveats in Cisco IOS Release 15.0(2)MR

The following sections describe the caveats in Release 15.0(2)MR.

Open Caveats

- CSCtg89367

  Symptom: The MWR 2941 internal Ethernet tsec interface stops sending host traffic.

  Conditions: Occurs when you configure an MTU size of 4470 on a VLAN interface while OSPF routing is enabled. To verify the condition, issue the **show platform hardware ethernet tsec 1** command to see if the number of interface resets increases.

  Workaround: Use the default MTU size for the VLAN interface or apply the **ip ospf mtu-ignore** command to the VLAN interface.

- CSCti36876

  Symptom: The MWR 2941 displays traceback messages and the MLPPP link can go in and out of service.

  Conditions: Occurs when the MLPPP bundles is overloaded.

  Workaround: Maintain a traffic load of less than 32 Mbps on the MLPPP bundle.

Closed Caveats

- CSCto13107

  Symptom: PTP connections on the MWR 2941 operating across multiple hops are unstable.

  Conditions: Occurs when the MWR 2941 is configured as a boundary clock and exchanging PTP traffic that travels more than one network hop to reach a destination device.

  Workaround: None.

Caveats in Cisco IOS Release 15.0(1)MR

The following sections describe the caveats in Release 15.0(1)MR.

Open Caveats

- CSCtg30671

  Symptom: The Cisco MWR 2941 does not permit changes to a PVC configured with cell packing. The router displays the following message:

  ```
  ATMCMDFAIL:Unable to Configure PVC(1) 1/40 on ATM0/IMA0.1.Possibly multiple users
  configuring IOS simultaneously
   Further info about other user:
   Process id: 256, Process: AToM manager, TTY: 0, Location: Console
  ```

  Conditions: Occurs in the following topology:

  mwr1---MPLS---mwr2---MPLS---mwr3----MPLS---7600

  The error occurs under the following conditions:

  - The mwr2 and mwr3 routers have IMA PVCs configured.
  - The mwr2 router has a PVC with cell packing configured and is passing traffic.
  - The mwr3 router has a PVC with cell packing configured and is passing traffic.
  - The 7600 has cell packing configured for both PVCs.

  Workaround: None.

- CSCtg89367

  Symptom: The internal tsec Ethernet interface remains in a reset state and does not send host traffic. A reload is required to restore service.

  Conditions: Occurs when you configure a VLAN interface with an MTU of 4470 and OSPF routing is enabled. To verify the condition, use the **show platform hardware ethernet tsec 1** command to see if the number of interface resets increases.

  Workaround: You can use one of the following workarounds:

  - Use the default MTU size for the VLAN interface.
  - Issue the **ip ospf mtu-ignore** command on the OSPF-enabled VLAN interface.

- CSCth37415

  Symptom: The 1.544 GPS interface is not available when configuring an input network clocking source.

  Conditions: Occurs when you configure the network synchronization automatic command. This command assigns a clock source based on clock priority and quality. This clock selection mechanism does not support 1.544 GPS interface as an input clock source.

  Workaround: Remove the network synchronization automatic command and use the **network-clock-select** command to configure this interface as a clock source.

  Note The **network-clock-select** command only supports priority-based clock source selection; it does not support automatic clock selection.

- CSCti44873

Symptom: The multilink interface fails to restore proper bandwidth after a reload.

Conditions: Occurs when you apply and remove a **bandwidth** statement on a multilink bundle interface.

Workaround: Remove the **bandwidth** statement from the interface.

- CSCtj39710

  Symptom: The show mpls forwarding command displays incorrect output; the **bytes label switched** statistic only displays statistics for one path.

  Conditions: Occurs when you use equal cost multipath with MPLS forwarding.

  Workaround: Use **show platform hardware winpath cef label** command to display statistics for each packet flow that is routed or the **show interface summary** command to display the packets routed though each interface.

- CSCtj52205

  Symptom: The Cisco MWR 2941 ATM/IMA interface drops for approximately 30 seconds while the peer IMA interface recovers; this condition can result in packet loss during an interface status transition.

  Conditions: Occurs when the ATM/IMA interface changes status, such as when you perform **shutdown/no shutdown** or connect a T1/E1 cable.

  Workaround: None.

- CSCtj59001

  Symptom: Interface statistics for the Gigabit Ethernet interface such as packets/bytes are inaccurate after processing traffic for a long period of time.

  Conditions: Occurs when the Gigabit Ethernet interface processes traffic for an extended period of time.

  Workaround: Issue the **clear counters** command to reset the Gigabit Ethernet interface statistics accounting.

- CSCtj63773

  Symptom: When you upgrade from a 12.2(33) release to Release 15.0(1)MR and reload the MWR 2941, the router displays an incorrect notification that the configuration register is set to 0x0.

  Conditions: Occurs when you upgrade to Release 15.0(1)MR from a 12.2(33) release.

  Workaround: Use the **test platform hardware configreg_read** command to perform a configuration register read value reset. After you execute this command, the **show version** command displays the correct configuration register value.

Closed Caveats

- CSCtb22933

  Symptom: The MWR can display a traceback `error_index=195 [WP_ERR_CH_ALREADY_CREATED]` after an ATM pseudowire VC flaps repeatedly.

  Conditions: Occurs when an ATM pseudowire flaps repeatedly due to a timing or IP routing issue.

  Workaround: Ensure that the ATM pseudowire is configured properly.

- CSCte14963

  Symptom: The MWR 2941 displays traceback messages when you change the IMA group ID on the E1 controller. The traceback messages block configuration of the IMA group on the controller.

Conditions: Occurs when you enable and disable **scrambling-payload** multiple times before changing the ima-group ID.

Workaround: None.

- CSCtf79922

  Symptom: The MWR 2941 displays the following traceback and error messages when you delete and reconfigure a VLAN.

```
Mar 24 03:18:32.203 HKT: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan441,
changed state to up
Mar 24 03:18:32.203 HKT: Error Traceback:
        File = ../sources/iw/classifier/wpi_iw_dfc.c
        Function=WPI_IwSystemCreateEmc
        Line = 1485
        error_index=575 [WP_INVALID_IW_EMC_FLOW_EXISTS_IN_HASH]
Mar 24 03:18:32.203 HKT: -Traceback= 261314C 26B0BC8 273B3B8 26FEA78 27649B4 2633520
26336B8 2633B98 2633F38 25FE1B8 25FE678 25FF538 30C36B4 3095110 3095780 30DE8A0
Mar 24 03:18:32.203 HKT: Error Traceback:
        File = ../sources/iw/core/wpi_iw_flow_aggregation.c
        Function=WP_IwFlowAggregationDelete
        Line = 2790
        error_index=483 [WP_ERR_IW_FLOW_AGG_NOT_EMPTY]
Mar 24 03:18:32.203 HKT: -Traceback= 261314C 26B0BC8 2726D70 26336F4 2633B98 2633F38
25FE1B8 25FE678 25FF538 30C36B4 3095110 3095780 30DE8A0 30DEAB8 3C69C30 2067A08
```

  Conditions: Occurs when you delete and reconfigure VLANs quickly.

  Workaround: Wait a few seconds when removing and reconfiguring a VLAN.

- CSCtg35849

  Symptom: The console becomes unresponsive after a routing change while the MWR 2941 is processing a heavy traffic load. The majority of traffic is dropped and the console can remain unresponsive until the traffic load diminishes or the router is reloaded.

  Conditions: Occurs when the router is processing at least 6 Megabits of traffic with small (64 byte) IP packets and the destination route drops or changes. This condition has only been observed on MLPPP backhaul interfaces when multiple links in a bundle switch to a redundant MLPPP bundle path while the router is processing up to 20 Mbps of 64-byte IP packets.

  Workaround: None.

- CSCti18895

  Symptom: The router does not process the remaining bandwidth percent command on a policy map applied to a Gigabit Ethernet interface.

  Conditions: Occurs when the class has the highest **remaining bandwidth percent** configuration of all classes in the policy map and the rate of traffic for the class is significantly lower than the overall bandwidth allocated to the interface.

  Workaround: Configure lower priority classes in the policy map with lower percentages until the desired bandwidth allocation is reached.

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-DC mobile wireless edge router include the following guides:

- Cisco MWR 2941 Mobile Wireless Edge Router documents
  - *Cisco MWR 2941 Mobile Wireless Edge Router Hardware Installation Guide*
  - *Cisco MWR 2941 Mobile Wireless Edge Router Software Configuration Guide, Release 15.1(1)MR*
  - *Cisco MWR 2941 Router Command Reference, Release 15.1(1)MR*
  - *Regulatory Compliance and Safety Information for the Cisco MWR 2941 Mobile Wireless Edge Routers*
- Release Notes—*Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router for Cisco IOS Release 15.1(1)MR2*
- 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 Router for Cisco IOS Release 15.1(1)MR2