Cisco MWR 2941 Router Overview

The Cisco MWR 2941 Mobile Wireless Router is cell-site access platforms 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/E1 circuits, including leased line, microwave, and satellite, as well as alternative backhaul networks, including Carrier Ethernet, 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.

Note

The Cisco MWR 2941-DC and 2941-DC-A support the same features except for commands related to the 1PPS, 10Mhz, 2.048Mhz, and 1.544Mhz timing ports that are included on the 2941-DC-A. For more information, see the Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.2(33)MRA.

This chapter includes the following sections:

- Introduction, page 1-2
- Features, page 1-3
- Network Management Features, page 1-22
- Limitations and Restrictions, page 1-23
Introduction

A typical RAN is composed of thousands of base transceiver stations (BTSs)/Node Bs, hundreds of base station controllers/radio network controllers (BSCs/RNCs), and several mobile switching centers (MSCs). The BTS/Node Bs and BSC/RNC are often separated by large geographic distances, with the BTSs/Node Bs located in cell sites uniformly distributed throughout a region, and the BSCs, RNCs, and MSCs located at suitably chosen Central Offices (CO) or mobile telephone switching offices (MTSO).

The traffic generated by a BTS/Node B is transported to the corresponding BSC/RNC across a network, referred to as the backhaul network, which is often a hub-and-spoke topology with hundreds of BTS/Node Bs connected to a BSC/RNC by point-to-point time division multiplexing (TDM) trunks. These TDM trunks may be leased-line T1/E1s or their logical equivalents, such as microwave links or satellite channels.

RAN Transport Solutions

The Cisco MWR 2941 Mobile Wireless Router supports a variety of RAN transport solutions, including the following:

- IP/Multiprotocol Label Switching (MPLS) RAN backhaul: Allows you to create a high-speed backhaul for a variety of traffic types, including GSM, CDMA, HSPA/LTE, CDMA, EVDO, and WiMAX networks.
- Cell-site operations support networks: Facilitates telemetry to cell sites for remote operations and network element management.
- Cell-site IP points of presence (POPs): Allows you to offer IP services and applications at cell sites.
- Carrier Ethernet features including Resilient Ethernet Protocol (REP), Ethernet Connectivity Fault Management (CFM), Ethernet Local Management Interface (E-LMI), and Ethernet Operations, Administration, and Maintenance (OAM)
- Network clocking features including PTP, pseudowire-based clocking, and synchronous Ethernet.
- Flexible backhaul transport including MLPPP over T1, E1, xDSL, and Ethernet
Features

The following sections describe the features available in the Cisco MWR 2941 router.

Cisco Pseudowire Emulation Edge-to-Edge

Cisco Pseudowire Emulation Edge-to-Edge (PWE3) allows you to transport traffic using traditional services such as E1/T1 over a packet-based backhaul technology such as MPLS or IP. A pseudowire (PW) consists of a connection between two provider edge (PE) devices that connects two attachment circuits (ACs), such as ATM VPIs/VCIs or E1/T1 links.

Figure 1-1  Cisco MWR 2941 Router in a PWE3—Example

PWs manage encapsulation, timing, order, and other operations in order to make it transparent to users; the PW tunnel appears as an unshared link or circuit of the emulated service.

There are limitations that impede some applications from utilizing a PW connection. For more information, see the section describing the PW service.

Cisco supports the following standards-based PWE types:

- Structure-agnostic TDM over Packet, page 1-3
- Structure-aware TDM Circuit Emulation Service over Packet-Switched Network, page 1-4
- Transportation of Service Using ATM over MPLS, page 1-4
- Transportation of Service Using Ethernet over MPLS, page 1-4

Structure-agnostic TDM over Packet

SAToP encapsulates TDM bit-streams (T1, E1, T3, E3) as PWs over PSNs. It disregards any structure that may be imposed on streams, in particular the structure imposed by the standard TDM framing.

The protocol used for emulation of these services does not depend on the method in which attachment circuits are delivered to the PEs. For example, a T1 attachment circuit is treated the same way for all delivery methods, including: PE on copper, multiplex in a T3 circuit, mapped into a virtual tributary of
a SONET/SDH circuit, or carried over a network using unstructured Circuit Emulation Service (CES). Termination of specific carrier layers used between the PE and circuit emulation (CE) is performed by an appropriate network service provider (NSP).

For instructions on how to configure SAToP, see Configuring Structure-Agnostic TDM over Packet (SAToP), page 4-76. For a sample SAToP configuration, see TDM over MPLS Configuration, page A-14.

**Structure-aware TDM Circuit Emulation Service over Packet-Switched Network**

CESoPSN encapsulates structured (NxDS0) TDM signals as PWs over PSNs. It complements similar work for structure-agnostic emulation of TDM bit-streams, such as PWE3-SAToP.

Emulation of NxDS0 circuits saves PSN bandwidth and supports DS0-level grooming and distributed cross-connect applications. It also enhances resilience of CE devices due to the effects of loss of packets in the PSN.

CESoPSN supports channel-associated signaling (CAS) for E1 and T1 interfaces. CAS provides signaling information within each DS0 channel as opposed to using a separate signaling channel. CAS also referred to as in-band signaling or robbed bit signaling.

For instructions on how to configure SAToP, see Configuring Circuit Emulation Service over Packet-Switched Network (CESoPSN), page 4-76. For a sample SAToP configuration, see TDM over MPLS Configuration, page A-14.

**Transportation of Service Using ATM over MPLS**

An Asynchronous Transfer Mode (ATM) over MPLS PW is used to carry ATM cells over an MPLS network. It is an evolutionary technology that allows you to migrate packet networks from legacy networks, yet provides transport for legacy applications. ATM over MPLS is particularly useful for transporting 3G voice traffic over MPLS networks.

You can configure ATM over MPLS in the following modes:

- **N-to-1 Cell Mode**—Maps one or more ATM virtual channel connections (VCCs) or virtual permanent connection (VPCs) to a single pseudowire.
- **1-to-1 Cell Mode**—Maps a single ATM VCC or VPC to a single pseudowire.
- **Port Mode**—Maps one physical port to a single pseudowire connection.

The Cisco MWR 2941 also supports cell packing and PVC mapping for ATM over MPLS pseudowires. For more information about how to configure ATM over MPLS, see “Configuring Transportation of Service Using ATM over MPLS” section on page 4-77. For sample ATM over MPLS configurations, see “ATM over MPLS Configuration” section on page A-17.

**Transportation of Service Using Ethernet over MPLS**

Ethernet over MPLS (EoMPLS) PWs provide a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core network. EoMPLS PWs encapsulate Ethernet protocol data units (PDUs) inside MPLS packets and use label switching to forward them across an MPLS network. EoMPLS PWs are an evolutionary technology that allows you to migrate packet networks from legacy networks while providing transport for legacy applications. EoMPLS PWs also simplify provisioning, since the provider edge equipment only requires Layer 2 connectivity to the connected customer edge (CE) equipment. The Cisco MWR 2941 implementation of EoMPLS PWs is compliant with the RFC 4447 and 4448 standards.

For instructions on how to create an EoMPLS PW, see Configuring Transportation of Service Using Ethernet over MPLS, page 4-83.
Limitations

When configuring an EoMPLS pseudowire on the Cisco MWR 2941, you cannot configure an IP address on the same interface as the pseudowire.

Generic Routing Encapsulation (GRE) Tunneling

Generic routing encapsulation (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). The Cisco MWR 2941 supports GRE encapsulation for the following PW connection types:

- ATM over MPLS
- SAToP
- CESoPSN
- Ethernet over MPLS

The Cisco MWR 2941 implementation of GRE can interoperate with the Cisco 7600 router and provides compliance with RFCs 2784 and 4023. The Cisco MWR 2941 supports up to 128 GRE tunnels. For more information about how to configure GRE tunneling, see Configuring GRE Tunneling, page 4-74.

Resilient Ethernet Protocol (REP)

A REP segment is a chain of ports connected to each other and configured with a segment ID. Each segment consists of standard (nonedge) segment ports and two user-configured edge ports. A switch can have only two ports belonging to the same segment, and each segment port can have only one external neighbor. A segment can go through a shared medium, but on any link, only two ports can belong to the same segment. REP is supported only on Layer 2 trunk interfaces.

Figure 1-2 shows an example of a segment consisting of six ports spread across four switches. Ports E1 and E2 are configured as edge ports. When all ports are operational (as in the segment on the left), a single port is blocked, shown by the diagonal line. When there is a network failure, as shown in the diagram on the right, the blocked port returns to the forwarding state to minimize network disruption.
The segment shown in Figure 1-2 is an open segment; there is no connectivity between the two edge ports. The REP segment cannot cause a bridging loop, and you can safely connect the segment edges to any network. All hosts connected to switches inside the segment have two possible connections to the rest of the network through the edge ports, but only one connection is accessible at any time. If a host cannot access its usual gateway because of a failure, REP unblocks all ports to ensure that connectivity is available through the other gateway.

The segment shown in Figure 1-3, with both edge ports located on the same switch, is a ring segment. In this configuration, there is connectivity between the edge ports through the segment. With this configuration, you can create a redundant connection between any two switches in the segment.

REP segments have these characteristics:

- If all ports in the segment are operational, one port (referred to as the alternate port) is in the blocked state for each VLAN.
- If VLAN load balancing is configured, two ports in the segment control the blocked state of VLANs.
- If one or more ports in a segment is not operational, causing a link failure, all ports forward traffic on all VLANs to ensure connectivity.
- In case of a link failure, the alternate ports are unblocked as quickly as possible. When the failed link comes back up, a logically blocked port per VLAN is selected with minimal disruption to the network.
You can construct almost any type of network based on REP segments. REP also supports VLAN load-balancing, controlled by the primary edge port but occurring at any port in the segment.

REP has these limitations:

- You must configure each segment port; an incorrect configuration can cause forwarding loops in the networks.
- REP can manage only a single failed port within the segment; multiple port failures within the REP segment cause loss of network connectivity.
- You should configure REP only in networks with redundancy. Configuring REP in a network without redundancy causes loss of connectivity.

### Link Integrity

REP does not use an end-to-end polling mechanism between edge ports to verify link integrity. It implements local link failure detection. The REP Link Status Layer (LSL) detects its REP-aware neighbor and establishes connectivity within the segment. All VLANs are blocked on an interface until it detects the neighbor. After the neighbor is identified, REP determines which neighbor port should become the alternate port and which ports should forward traffic.

Each port in a segment has a unique port ID. The port ID format is similar to that used by the spanning tree algorithm: a port number (unique on the bridge), associated to a MAC address (unique in the network). When a segment port is coming up, its LSL starts sending packets that include the segment ID and the port ID. The port is declared operational after it performs a three-way handshake with a neighbor in the same segment.

A segment port does not become operational if:

- No neighbor has the same segment ID.
- More than one neighbor has the same segment ID.
- The neighbor does not acknowledge the local port as a peer.

Each port creates an adjacency with its immediate neighbor. After the neighbor adjacencies are created, the ports negotiate to determine one blocked port for the segment, the alternate port. All other ports become unblocked. By default, REP packets are sent to a BPDU class MAC address. The packets can also be sent to the Cisco multicast address, which is used only to send blocked port advertisement (BPA) messages when there is a failure in the segment. The packets are dropped by devices not running REP.

### Fast Convergence

Because REP runs on a physical link basis and not a per-VLAN basis, only one hello message is required for all VLANs, reducing the load on the protocol. We recommend that you create VLANs consistently on all switches in a given segment and configure the same allowed VLANs on the REP trunk ports. To avoid the delay introduced by relaying messages in software, REP also allows some packets to be flooded to a regular multicast address. These messages operate at the hardware flood layer (HFL) and are flooded to the whole network, not just the REP segment. Switches that do not belong to the segment treat them as data traffic. You can control flooding of these messages by configuring a dedicated administrative VLAN for the whole domain.

The estimated convergence recovery time on fiber interfaces is less than 200 ms for the local segment with 200 VLANs configured. Convergence for VLAN load balancing is 300 ms or less.
VLAN Load Balancing

One edge port in the REP segment acts as the primary edge port; the other as the secondary edge port. The primary edge port always participates in VLAN load balancing in the segment. REP VLAN balancing is achieved by blocking some VLANs at a configured alternate port and all other VLANs at the primary edge port. When you configure VLAN load balancing, you can specify the alternate port in one of three ways:

- Enter the port ID of the interface. To identify the port ID of a port in the segment, enter the `show interface rep detail` interface configuration command for the port.
- Enter the neighbor offset number of a port in the segment, which identifies the downstream neighbor port of an edge port. The neighbor offset number range is –256 to +256; a value of 0 is invalid. The primary edge port has an offset number of 1; positive numbers above 1 identify downstream neighbors of the primary edge port. Negative numbers identify the secondary edge port (offset number -1) and its downstream neighbors.

**Note** You configure offset numbers on the primary edge port by identifying the downstream position from the primary (or secondary) edge port. You would never enter an offset value of 1 because that is the offset number of the primary edge port itself.
Figure 1-4 shows neighbor offset numbers for a segment where E1 is the primary edge port and E2 is the secondary edge port. The red numbers inside the ring are numbers offset from the primary edge port; the black numbers outside the ring show the offset numbers from the secondary edge port. Note that you can identify all ports (except the primary edge port) by either a positive offset number (downstream position from the primary edge port) or a negative offset number (downstream position from the secondary edge port). If E2 became the primary edge port, its offset number would then be 1, and E1 would be -1.

- By entering the preferred keyword to select the port that you previously configured as the preferred alternate port with the `rep segment segment-id preferred` interface configuration command.

When the REP segment is complete, all VLANs are blocked. When you configure VLAN load balancing, you must also configure triggers in one of two ways

- Manually trigger VLAN load balancing at any time by entering the `rep preempt segment segment-id` privileged EXEC command on the switch that has the primary edge port.
- Configure a preempt delay time by entering the `rep preempt delay seconds` interface configuration command. After a link failure and recovery, VLAN load balancing begins after the configured preemption time period elapses. Note that the delay timer restarts if another port fails before the time has elapsed.

When VLAN load balancing is configured, it does not start working until triggered by either manual intervention or a link failure and recovery.

When VLAN load balancing is triggered, the primary edge port sends a message to alert all interfaces in the segment about the preemption. When the secondary port receives the message, it is reflected into the network to notify the alternate port to block the set of VLANs specified in the message and to notify the primary edge port to block the remaining VLANs.

You can also configure a particular port in the segment to block all VLANs. Only the primary edge port initiates VLAN load balancing, which is not possible if the segment is not terminated by an edge port on each end. The primary edge port determines the local VLAN load balancing configuration.

Reconfigure the primary edge port to reconfigure load balancing. When you change the load balancing configuration, the primary edge port again waits for the `rep preempt segment` command or for the configured preempt delay period after a port failure and recovery before executing the new configuration. If you change an edge port to a regular segment port, the existing VLAN load balancing status does not change. Configuring a new edge port might cause a new topology configuration.
Spanning Tree Interaction

REP does not interact with STP or with the Flex Link feature, but can coexist with both. A port that belongs to a segment is removed from spanning tree control and STP BPDUs are not accepted or sent from segment ports.

To migrate from an STP ring configuration to REP segment configuration, begin by configuring a single port in the ring as part of the segment, and continue by configuring contiguous ports to minimize the number of segments. Each segment always contains a blocked port, so multiple segments means multiple blocked ports and a potential loss of connectivity. When the segment has been configured in both directions to the edge ports, you then configure the edge ports.

REP Ports

Ports in REP segments are Failed, Open, or Alternate.
- A port configured as a regular segment port starts as a failed port.
- After the neighbor adjacencies are determined, the port changes to alternate port state, blocking all VLANs on the interface. Blocked port negotiations occur and when the segment settles, one blocked port remains in the alternate role, and all other ports become open ports.
- When a failure occurs in a link, all ports move to the open state. When the alternate port receives the failure notification, it changes to the open state, forwarding all VLANs.

A regular segment port converted to an edge port, or an edge port converted to a regular segment port, does not always result in a topology change. If you convert an edge port into a regular segment port, VLAN load balancing is not implemented unless it has been configured. For VLAN load balancing, you must configure two edge ports in the segment.

A segment port that is reconfigured as a spanning tree port restarts according the spanning tree configuration. By default, this is a designated blocking port. If PortFast is configured or if STP is disabled, the port goes into the forwarding state.

For instructions on how to configure REP, see Configuring Resilient Ethernet Protocol (REP), page 4-14.

Ethernet Operations, Administration, and Maintenance (OAM)

Ethernet Operations, Administration, and Maintenance (OAM) is a protocol for installing, monitoring, and troubleshooting Ethernet metropolitan-area networks (MANs) and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the Open Systems Interconnection (OSI) model. The OAM features covered by this protocol are Discovery, Link Monitoring, Remote Fault Detection, Remote Loopback, and Cisco Proprietary Extensions.

The following sections describe the Ethernet OAM features supported on the Cisco MWR 2941.
- Overview
- Link OAM
- Ethernet Connectivity Fault Management (CFM)
- Ethernet Local Management Interface (E-LMI)
Overview

Ethernet OAM is a protocol for installing, monitoring, and troubleshooting metro Ethernet networks and Ethernet WANs. It relies on a new, optional sublayer in the data link layer of the OSI model. Ethernet OAM can be implemented on any full-duplex point-to-point or emulated point-to-point Ethernet link. A system-wide implementation is not required; OAM can be deployed for part of a system; that is, on particular interfaces.

Normal link operation does not require Ethernet OAM. OAM frames, called OAM protocol data units (PDUs), use the slow protocol destination MAC address 0180.c200.0002. They are intercepted by the MAC sublayer and cannot propagate beyond a single hop within an Ethernet network.

Ethernet OAM is a relatively slow protocol with modest bandwidth requirements. The frame transmission rate is limited to a maximum of 10 frames per second; therefore, the impact of OAM on normal operations is negligible. However, when link monitoring is enabled, the CPU must poll error counters frequently. In this case, the required CPU cycles will be proportional to the number of interfaces that have to be polled.

Two major components, the OAM client and the OAM sublayer, make up Ethernet OAM. The following sections describe these components.

OAM Client

The OAM client is responsible for establishing and managing Ethernet OAM on a link. The OAM client also enables and configures the OAM sublayer. During the OAM discovery phase, the OAM client monitors OAM PDUs received from the remote peer and enables OAM functionality on the link based on local and remote state as well as configuration settings. Beyond the discovery phase (at steady state), the OAM client is responsible for managing the rules of response to OAM PDUs and managing the OAM remote loopback mode.

OAM Sublayer

The OAM sublayer presents two standard IEEE 802.3 MAC service interfaces: one facing toward the superior sublayers, which include the MAC client (or link aggregation), and the other interface facing toward the subordinate MAC control sublayer. The OAM sublayer provides a dedicated interface for passing OAM control information and OAM PDUs to and from a client.

The OAM sublayer is made up of three components: control block, multiplexer, and packet parser (p-parser). Each component is described in the following sections.

Control Block

The control block provides the interface between the OAM client and other blocks internal to the OAM sublayer. The control block incorporates the discovery process, which detects the existence and capabilities of remote OAM peers. It also includes the transmit process that governs the transmission of OAM PDUs to the multiplexer and a set of rules that govern the receipt of OAM PDUs from the p-parser.

Multiplexer

The multiplexer manages frames generated (or relayed) from the MAC client, control block, and p-parser. The multiplexer passes through frames generated by the MAC client untouched. It passes OAM PDUs generated by the control block to the subordinate sublayer; for example, the MAC sublayer. Similarly, the multiplexer passes loopback frames from the p-parser to the same subordinate sublayer when the interface is in OAM remote loopback mode.
P-Parser

The p-parser classifies frames as OAM PDUs, MAC client frames, or loopback frames and then dispatches each class to the appropriate entity. OAM PDUs are sent to the control block. MAC client frames are passed to the superior sublayer. Loopback frames are dispatched to the multiplexer.

Link OAM

Link OAM is defined in the IEEE 802.3ah and IEEE 802.3 Clause 57 standards and provides for discovery, Link Monitoring, Remote Fault Indication, Remote Loopback, and Cisco proprietary extensions. The following sections describe Link OAM:

- Discovery
- Link Monitoring
- Remote Failure Indication
- Remote Loopback
- Cisco Vendor-Specific Extensions
- OAM Messages

Discovery

Discovery is the first phase of Ethernet OAM and it identifies the devices in the network and their OAM capabilities. Discovery uses information OAM PDUs. During the discovery phase, the following information is advertised within periodic information OAM PDUs:

- OAM mode—Conveyed to the remote OAM entity. The mode can be either active or passive and can be used to determine device functionality.
- OAM configuration (capabilities)—Advertises the capabilities of the local OAM entity. With this information a peer can determine what functions are supported and accessible; for example, loopback capability.
- OAM PDU configuration—Includes the maximum OAM PDU size for receipt and delivery. This information along with the rate limiting of 10 frames per second can be used to limit the bandwidth allocated to OAM traffic.
- Platform identity—A combination of an organization unique identifier (OUI) and 32-bits of vendor-specific information. OUI allocation, controlled by the IEEE, is typically the first three bytes of a MAC address.

Discovery includes an optional phase in which the local station can accept or reject the configuration of the peer OAM entity. For example, a node may require that its partner support loopback capability to be accepted into the management network. These policy decisions may be implemented as vendor-specific extensions.

Link Monitoring

Link monitoring in Ethernet OAM detects and indicates link faults under a variety of conditions. Link monitoring uses the event notification OAM PDU and sends events to the remote OAM entity when there are problems detected on the link. The error events include the following:

- Error Symbol Period (error symbols per second)—The number of symbol errors that occurred during a specified period exceeded a threshold. These errors are coding symbol errors.
- Error Frame (error frames per second)—The number of frame errors detected during a specified period exceeded a threshold.
Chapter 1  Cisco MWR 2941 Router Overview

Features

- Error Frame Period (error frames per n frames)—The number of frame errors within the last n frames has exceeded a threshold.

- Error Frame Seconds Summary (error seconds per m seconds)—The number of error seconds (1-second intervals with at least one frame error) within the last m seconds has exceeded a threshold.

Since IEEE 802.3ah OAM does not provide a guaranteed delivery of any OAM PDU, the event notification OAM PDU may be sent multiple times to reduce the probability of a lost notification. A sequence number is used to recognize duplicate events.

Remote Failure Indication

Faults in Ethernet connectivity that are caused by slowly deteriorating quality are difficult to detect. Ethernet OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer via specific flags in the OAM PDU. The following failure conditions can be communicated:

- Link Fault—Loss of signal is detected by the receiver; for instance, the peer's laser is malfunctioning. A link fault is sent once per second in the information OAM PDU. Link fault applies only when the physical sublayer is capable of independently transmitting and receiving signals.

- Dying Gasp—An unrecoverable condition has occurred; for example, a power failure. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.

- Critical Event—An unspecified critical event has occurred. This type of event is vendor specific. A critical event may be sent immediately and continuously.

Remote Loopback

An OAM entity can put its remote peer into loopback mode using the loopback control OAM PDU. Loopback mode helps an administrator ensure the quality of links during installation or when troubleshooting. In loopback mode, every frame received is transmitted back on the same port except for OAM PDUs and pause frames. The periodic exchange of OAM PDUs must continue during the loopback state to maintain the OAM session.

The loopback command is acknowledged by responding with an information OAM PDU with the loopback state indicated in the state field. This acknowledgement allows an administrator, for example, to estimate if a network segment can satisfy a service-level agreement. Acknowledgement makes it possible to test delay, jitter, and throughput.

When an interface is set to the remote loopback mode the interface no longer participates in any other Layer 2 or Layer 3 protocols; for example Spanning Tree Protocol (STP) or Open Shortest Path First (OSPF). The reason is that when two connected ports are in a loopback session, no frames other than the OAM PDUs are sent to the CPU for software processing. The non-OAM PDU frames are either looped back at the MAC level or discarded at the MAC level.

From a user's perspective, an interface in loopback mode is in a link-up state.

Cisco Vendor-Specific Extensions

Ethernet OAM allows vendors to extend the protocol by allowing them to create their own type-length-value (TLV) fields.

OAM Messages

Ethernet OAM messages or OAM PDUs are standard length, untagged Ethernet frames within the normal frame length bounds of 64 to 1518 bytes. The maximum OAM PDU frame size exchanged between two peers is negotiated during the discovery phase.
OAM PDUs always have the destination address of slow protocols (0180.c200.0002) and an Ethertype of 8809. OAM PDUs do not go beyond a single hop and have a hard-set maximum transmission rate of 10 OAM PDUs per second. Some OAM PDU types may be transmitted multiple times to increase the likelihood that they will be successfully received on a deteriorating link.

Four types of OAM messages are supported:

- Information OAM PDU—A variable-length OAM PDU that is used for discovery. This OAM PDU includes local, remote, and organization-specific information.
- Event notification OAM PDU—A variable-length OAM PDU that is used for link monitoring. This type of OAM PDU may be transmitted multiple times to increase the chance of a successful receipt; for example, in the case of high-bit errors. Event notification OAM PDUs also may include a time stamp when generated.
- Loopback control OAM PDU—An OAM PDU fixed at 64 bytes in length that is used to enable or disable the remote loopback command.
- Vendor-specific OAM PDU—A variable-length OAM PDU that allows the addition of vendor-specific extensions to OAM.

For instructions on how to configure Ethernet Link OAM, see Configuring Ethernet Link Operations, Administration, and Maintenance (OAM), page 4-32.

**Ethernet Connectivity Fault Management (CFM)**

The Cisco MWR 2941 supports Ethernet Connectivity Fault Management (CFM) as defined in 802.1ag Draft 1.0. Ethernet Connectivity Fault Management (CFM) is an end-to-end per-service-instance Ethernet layer operations, administration, and maintenance (OAM) protocol. It includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

Ethernet CFM provides the following benefits:

- End-to-end service-level OAM technology
- Reduced operating expense for service provider Ethernet networks
- Competitive advantage for service providers

**Note**

Release 12.2(33)MRA supports the Draft 1.0 version of Ethernet CFM; it does not support the IEEE 802.1ag-2007 version.

For instructions on how to configure CFM, see Configuring Ethernet CFM, page 4-29.

**Ethernet Local Management Interface (E-LMI)**

Ethernet Local Management Interface (LMI) is an Ethernet layer operation, administration, and management (OAM) protocol. It provides information that enables autoconfiguration of customer edge (CE) devices and provides the status of Ethernet virtual connections (EVCs) for large Ethernet metropolitan-area networks (MANs) and WANs. Specifically, Ethernet LMI notifies a CE device of the operating state of an EVC and the time when an EVC is added or deleted. Ethernet LMI also communicates the attributes of an EVC and a user-network interface (UNI) to a CE device.

For instructions on how to configure E-LMI, see Configuring Ethernet Local Management Interface (E-LMI), page 4-37.
Clocking and Timing

The following sections describe the clocking and timing features available on the Cisco MWR 2941.

- Network Clocking Overview
- Precision Timing Protocol (PTP)
- Pseudowire-based Clocking
- Synchronous Ethernet

Network Clocking Overview

Clock synchronization is important for a variety of applications, including synchronization of radio cell towers. While legacy TDM protocols incorporate timing features, packet-switched networks such as Ethernet do not natively include these features. The Cisco MWR 2941 supports legacy TDM technologies while supporting a variety of technologies that distribute clocking information over packet-switched networks.

Clocking is typically distributed from the core network outward to the BTS or Node B at the network edge. The Cisco MWR 2941 receives and transmits clocking information using any of the following ports:

- T1/E1
- Ethernet (GigabitEthernet and FastEthernet)
- DSL
- BITS/SYNC port
- 1PPS
- 1.544Mhz
- 2.048Mhz
- 10Mhz

Precision Timing Protocol (PTP)

The Cisco MWR 2941 supports the Precision Time Protocol (PTP) as defined by the IEEE 1588-2008 standard. PTP provides for accurate time synchronization on over packet-switched networks. Nodes within a PTP network can act in one of the following roles:

- Grandmaster—A device on the network physically attached to the primary time source. All other clocks are ultimately synchronized to the grandmaster clock.
- Ordinary clock—An ordinary clock is a 1588 clock with a single PTP port that can serve in one of the following roles:
  - Master mode—Distributes timing information over the network to one or more slave clocks, thus allowing the slave to synchronize its clock to the master.
  - Slave mode—Synchronizes its clock to a master clock.
- Boundary clock—The device participates in selecting the best master clock and can act as the master clock if no better clocks are detected.
- Transparent clock—A device such as a switch that calculates the time it requires to forward traffic and updates the PTP time correction field to account for the delay, making the device transparent in terms of timing calculations.
Note
The Cisco MWR 2941 does not currently act as a boundary clock or a transparent clock.

Note
The 1588-2008 standard defines other clocking devices that are not described here.

PTP Domains
PTP devices use a best master clock algorithm to determine the most accurate clock on a network and construct a clocking hierarchy based on the grandmaster clock. A given clocking hierarchy is called a PTP domain.

Clock synchronization
PTP master devices periodically launch an exchange of messages with slave devices to help each slave clock recompute the offset between its clock and the master clock. Periodic clock synchronization mitigates any drift between the master and slave clocks.

PTP Redundancy
The Cisco MWR 2941 supports the multicast- and unicast-based timing as specified in the 1588-2008 standard. The Cisco MWR 2941 can use multicast routing to establish redundant paths between an external PTP client and one or more PTP multicast master clocks. The Cisco MWR 2941 functions as a multicast router only for PTP traffic and only allows multicast traffic to pass from the PTP master clocks to the PTP client (the PTP client can send unicast traffic).

When configured as a multicast PTP router, the Cisco MWR 2941 selects the best path toward a Rendezvous Point (RP) using the active routing protocol, sends a Cisco Protocol Independent Multicast (PIM) join message to the RP, and forwards PTP multicast messages to the PTP client. The Cisco MWR 2941 also supports PIM forwarding. For instructions on how to configure PTP redundancy using multicast, see Configuring PTP Redundancy, page 4-44.

Hot Standby Master Clock
The Cisco MWR 2941 supports a hot standby master clock for PTP clocking; the Cisco MWR 2941 selects the best clock source between two PTP master clocks and switches dynamically between them if the clock quality of the standby clock is greater than that of the current master clock. For instructions on how to configure a hot standby master clock, see Configuring PTP Clocking, page 4-39.

Hybrid Clocking
The Cisco MWR 2941 supports a hybrid clocking mode that uses clock frequency obtained from the synchronous Ethernet port while using phase (ToD or 1PPS) obtained using PTP. For instructions on how to configure hybrid clocking, see Configuring PTP Clocking, page 4-39.

Pseudowire-based Clocking
Pseudowire-based clocking allows the Cisco MWR 2941 router to
- Transmit and receive clocking information over a pseudowire interface
- Receive clocking over a virtual pseudowire interface.
The Cisco MWR 2941 can transmit clocking information within packet headers (in-band) or as a separate packet stream (out-of-band).

Pseudowire-based clocking also supports adaptive clock recovery (ACR), which allows the Cisco MWR 2941 to recover clocking from the headers of a packet stream. For instructions on how to configure pseudowire-based clocking, see Configuring Clocking and Timing, page 4-39. For more information about using pseudowires, see Cisco Pseudowire Emulation Edge-to-Edge, page 1-3.

### Synchronous Ethernet

Synchronous ethernet is a timing technology that allows the Cisco MWR 2941 to transport frequency and time information over Ethernet. Because frequency and time are embedded in Ethernet packets, synchronous Ethernet must be supported by each network element in the synchronization path. Synchronous Ethernet is defined in the ITU-T G.781, G.8261, G.8262, and G.8264, Telcordia GR-253-CORE, and Telcordia GR-1244-CORE standards.

You can use synchronous Ethernet in conjunction with an external timing technology such as GPS to synchronize timing across the network. For instructions on how to configure synchronous Ethernet, see Configuring Clocking and Timing, page 4-39.

### Network Clock Quality Selection using REP

Ethernet Synchronization Message Channel (ESMC) is a method for indicating the quality of a clock source on a synchronous Ethernet network segment. ESMC is described in the G.8264 (2008) standard and is similar to the Synchronization Status Message (SSM) message used in SONET and SDH. ESMC is based on the Organization Specific Slow Protocol defined in the IEEE 802.3 standard.

Release 12.2(33)MRA provides support for ESMC for synchronous Ethernet segments using REP. Release 12.2(33)MRA does not provide support the G.8264 standard.

ESMC provides the following benefits:

- Quality level (QL) enabled implementation – This will ensure that the highest quality level clock that is available is used.
- Helps a node derive timing from most reliable source
- Prevents timing loops

For instructions on how to configure network clock quality selection using REP, see Configuring Network Clock Quality Selection Using REP, page 4-49.

For more information about REP, see Resilient Ethernet Protocol (REP), page 1-5.

### Routing Protocols

In addition to static routing, the Cisco MWR 2941 supports the following dynamic routing protocols:

- **OSPF**—An Interior Gateway Protocol (IGP) designed expressly for IP networks that supports IP subnetting and tagging of externally derived routing information. OSPF also allows packet authentication and uses IP multicast when sending and receiving packets.
- **IS-IS**—An Open System Interconnection (OSI) protocol that specifies how routers communicate with routers in different domains.
- **BGP**—An interdomain routing protocol designed to provide loop-free routing between separate routing domains that contain independent routing policies (autonomous systems).
Features

For instructions on how to configure routing on the Cisco MWR 2941, see Configuring Routing Protocols, page 4-66.

Bidirectional Forwarding Detection

Bidirectional Forwarding Detection (BFD) provides a low-overhead, short-duration method of detecting failures in the forwarding path between two adjacent routers, including the interfaces, data links, and forwarding planes. BFD is a detection protocol that you enable at the interface and routing protocol levels. For instructions on how to configure BFD, see the “Configuring BFD” section on page 4-67.

MLPPP Optimization Features

The Cisco MWR 2941 supports several features that improve the performance of Multilink Point-to-Point Protocol (MLPPP) connections and related applications such as PWE3 over MLPPP and IP over MLPPP.

Distributed Multilink Point-to-Point Protocol (dMLPPP) Offload

Distributed Multilink Point-to-Point Protocol (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 and IP over MLPPP by shifting processing of this traffic from the main CPU to the network processor.

The Cisco MWR 2941 supports up to four serial links per T1/E1 connection and up to 24 MLPPP bundles. You can use the fixed T1/E1 ports to create up to 64 MLPPP links; if you install two four-port T1/E1 HWICs, you can create up to 96 MLPPP links.

The MWR 2941 implementation of multilink (dMLPPP) uses interleaving to allow short, delay-sensitive packets to be transmitted within a predictable amount of time. Interleaving allows the MWR 2941 to interrupt the transmission of delay-insensitive packets in order to transmit delay-sensitive packets. You can also adjust the responsiveness of the MWR 2941 to delay-sensitive traffic by adjusting the maximum fragment size; this value determines the maximum delay that a delay-sensitive packet can encounter while the MWR 2941 transmits queued fragments of delay-insensitive traffic.

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.

The MWR 2941 supports the following multiclass MLPPP classes:

- Class 0- Data traffic that is subject to normal MLPPP fragmentation. Appropriate for non-delay-sensitive traffic.
- Class 1- Data traffic that can be interleaved but not fragmented. Appropriate for delay-sensitive traffic such as voice.

For instructions on how to configure MLPPP backhaul, see Configuring MLPPP Backhaul, page 4-57.
Chapter 1      Cisco MWR 2941 Router Overview

Features

Note

The Cisco MWR 2941 does not support some PPP and MLPPP options when the bundle is offloaded to
the network processor; you can retain these options by disabling MLPPP and IPHC offloading for a given
bundle. For more information, see MLPPP Offload, page 4-65.

Note

The output for the show ppp multilink command for an offloaded MLPPP bundle differs from the output
for a non-offloaded bundle. For more information, see Appendix B, “Cisco MWR 2941 Router
Command Reference.”

Layer 3 Virtual Private Networks (VPNs)

A Virtual Private Network (VPN) is an IP-based network that delivers private network services over a
public infrastructure. VPNs allow you to create a set of sites that can communicate privately over the
Internet or other public or private networks.

A conventional VPN consists of a full mesh of tunnels or permanent virtual circuits (PVCs) connecting
all of the sites within the VPN. This type of VPN requires changes to each edge device in the VPN in
order to add a new site. Layer 3 VPNs are easier to manage and expand than conventional VPNs because
they use layer 3 communication protocols and are based on a peer model. The peer model enables the
service provider and customer to exchange Layer 3 routing information, enabling service providers to
relay data between customer sites without customer involvement. The peer model also provides
improved security of data transmission between VPN sites because data is isolated between improves
security between VPN sites.

The Cisco MWR 2941 supports the following MPLS VPN types:

- Basic Layer 3 VPN—Provides a VPN private tunnel connection between customer edge (CE)
devices in the service provider network. The provider edge (PE) router uses Multiprotocol Border
Gateway Protocol (MP-BGP) to distribute VPN routes and MPLS Label Distribution Protocol (LDP)
to distribute Interior Gateway Protocol (IGP) labels to the next-hop PE router.

- MPLS Carrier Supporting Carrier (CSC) VPN—Enables an MPLS VPN-based service provider to
allow other service providers to use a segment of its backbone network. MPLS CSC VPNS use
MPLS LDP to distribute MPLS labels and IGP to distribute routes.

- Inter-Autonomous System (AS) VPN—An inter-AS VPN allows service providers running separate
networks to jointly offer MPLS VPN services to the same end customer; an inter-AS VPN can begin
at one customer site and traverse multiple service provider backbones before arriving at another
customer site.

For instructions on how to configure an layer 3 VPN, see Layer 3 Virtual Private Networks (VPNs),
page 1-19.

Intelligent Cell Site IP Services

The Cisco RAN-O and IP-RAN solutions allow you to deliver profit-enhancing services. This is
achieved through the set of IP networking features supported in Cisco IOS software that extends to the
cell site (see Figure 1-5 on page 1-20).
Cell Site Points-of-Presence

The cell site becomes a physical Point-of-Presence (POP) from which to offer hotspot services, or voice and wired ISP services, to nearby enterprises and residences. Because many cell sites are located in and around downtown areas, hotels, airports, and convention centers, they make attractive sites for co-locating public wireless LAN (PWLAN) access points and other wireless data overlays. Many of these wireless data radios are IP-based. IP networking features, like Mobile IP, VoIP, IP Multicast, VPN, and content caching, enable delivery of new revenue-generating services over these radios. The corresponding traffic “rides for free” on the spare backhaul bandwidth made available by Cisco Abis solutions (Figure 1-5).

Quality of Service (QoS)

This section describes the Quality of Service (QoS) features on the Cisco MWR 2941. The Cisco MWR 2941 supports the following QoS features:

- **Traffic Classification**
- **Traffic Marking**
- **Traffic Queuing**
- **Traffic Shaping**
Chapter 1      Cisco MWR 2941 Router Overview

Features

Note

The Cisco MWR 2941 support for QoS varies based on the interface and traffic type. For more information about the QoS limitations, see Configuring Quality of Service (QoS), page 4-84.

For instructions on how to configure QoS on the Cisco MWR 2941, see Configuring Quality of Service (QoS), page 4-84.

Traffic Classification

Classifying network traffic allows you to organize packets into traffic classes based on whether the traffic matches specific criteria. Classifying network traffic is the foundation for enabling many QoS features on your network. For instructions on how to configure traffic classification, see Configuring Classification, page 4-91.

Traffic Marking

Marking network traffic allows you to set or modify the attributes for packets in a defined traffic class. You can use marking with traffic classification to configure variety of QoS features for your network. For instructions on how to configure traffic marking, see Configuring Marking, page 4-93.

Traffic Queuing

The Cisco MWR 2941 supports class-based WFQ (CBWFQ) for congestion management. CBWFQ extends the standard WFQ functionality to provide support for user-defined traffic classes. For CBWFQ, you define traffic classes based on match criteria such as input interface. Packets satisfying the match criteria for a class constitute the traffic for that class. For more instructions on how to configure traffic queuing, see Configuring Congestion Management, page 4-96.

Traffic Shaping

Regulating the packet flow on the network is also known as traffic shaping. Traffic shaping allows you to control the speed of traffic leaving an interface. This way, you can match the flow of the traffic to the speed of the interface receiving the packet.

The Cisco MWR 2941 supports Class-Based Traffic Shaping. Class-Based Traffic Shaping allows you to regulate the flow of packets leaving an interface on a per-traffic-class basis, matching the packet flow to the speed of the interface. For more instructions on how to configure traffic shaping, see Configuring Shaping, page 4-98.

ATM Classes of Service (CoS)

The Cisco MWR 2941 supports the following ATM classes of service (CoS):

- Unspecified Bit Rate (UBR)—A QoS class that allows devices to send any amount of data up to a specified maximum across the network but provides no guarantees for cell loss rate or delay. You can apply this QoS type to an ATM PVC, SVC, VC class, or VC bundle member.

- Non-Real Time Variable Bit Rate (VBR-NRT)—A QoS class used for connections in which there is no fixed timing relationship between samples but that still need a guaranteed QoS.

- Real-Time Variable Bit Rate (VBR-RT)—A QoS class used for connections in which there is a fixed timing relationship between samples.
Network Management Features

This section provides an overview of the network management features for the Cisco MWR 2941. For more information about management features on the Cisco MWR 2941, see “Monitoring and Managing the Cisco MWR 2941 Router” section on page 4-103.

Cisco Mobile Wireless Transport Manager (MWTM)

You can use Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco MWR 2941. Cisco MWTM addresses the element-management requirements of mobile operators and provides fault, configuration, and troubleshooting capability. For more information about MWTM, see http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html.

Cisco Active Network Abstraction (ANA)

You can also use Cisco Active Network Abstraction (ANA) to manage the Cisco MWR 2941. Cisco ANA is a powerful, next-generation network resource management solution designed with a fully distributed OSS mediation platform which abstracts the network, its topology and its capabilities from the physical elements. Its virtual nature provides customers with a strong and reliable platform for service activation, service assurance and network management. For more information about ANA, see http://www.cisco.com/en/US/products/ps6776/tsd_products_support_series_home.html.

SNMP MIB Support

To view the current MIBs that the Cisco MWR 2941 supports, see the Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.4(20)MR.

For instructions on how to configure MIBs on the Cisco MWR 2941, see Configuring SNMP Support, page 4-104 and Enabling Remote Network Management, page 4-107.

Cisco Networking Services (CNS)

Cisco Networking Services (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.

Note

The Cisco MWR 2941 only supports CNS over motherboard Ethernet interfaces. Other interface types do not support CNS.

For instructions on how to configure CNS, see Configuring Cisco Networking Services (CNS), page 4-110.
Limitations and Restrictions

The following sections describe the limitations and restrictions that apply to the Cisco MWR 2941 router.

Hardware Limitations and Restrictions

To view a list of supported hardware and restrictions for the Cisco MWR 2941, see the Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.4(20)MR.

Caution

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

Software Limitations and Restrictions

For information about software limitations and restrictions for the Cisco MWR 2941, see the Release Notes for Cisco MWR 2941-DC Mobile Wireless Edge Router for Cisco IOS Release 12.4(20)MR.