CHAPTER 29

Monitoring and Managing the Cisco MWR 2941 Router

The Cisco MWR 2941 supports a variety of network management features, including Mobile Wireless Transport Manager (MTWM), Cisco Active Network Abstraction (ANA), SNMP, and Cisco Networking Services (CNS). The following sections describe the network management features on the Cisco MWR 2941.

Understanding Network Management Features for the Cisco MWR 2941

The following sections describe the network management features available on the Cisco MWR 2941.

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 instructions on how to configure MIBs on the Cisco MWR 2941, see Configuring SNMP Support and Enabling Remote Network Management.

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).

Configuring Network Management Features

The following sections describe how to configure network management features on the Cisco MWR 2941.

Using Cisco Mobile Wireless Transport Manager (MWTM)

You can use Cisco network management applications, such as Cisco Mobile Wireless Transport Manager (MWTM), to monitor and manage the Cisco MWR 2941. This Network Management tool provides monitoring and management capabilities to the RAN-O solution. The Cisco MWTM addresses the element-management requirements of mobile operators and provides fault, configuration, and troubleshooting capability. The Cisco MWTM provides the following key features:

- Event Monitoring
- Web-Based Reporting
- Autodiscovery and Topology

- Inventory
- OSS Integration
- Security
- Client/Server Architecture
- Multiple OS Support

The Cisco MWTM integrates with any SNMP-based monitoring system, such as Cisco Info Center products. In addition, the Cisco MWTM collects a large amount of performance data that can be exported or directly accessed from the database. This data can then be used by performance reporting applications. For more information about MWTM, see http://www.cisco.com/en/US/products/ps6472/tsd_products_support_series_home.html.

Configuring SNMP Support

Use the following instructions to configure SNMP support: setting up the community access, establishing a message queue for each trap host, enabling the router to send SNMP traps, enabling SNMP traps for alarms, and enabling SNMP traps for a specific environment. You might also need to enter other configuration commands, depending on the requirements for your system configuration and the protocols you plan to route on the interface.

Note To view the current MIBs that the Cisco MWR 2941 supports, see the *Release Notes for Cisco MWR 2941 Mobile Wireless Edge Router.*

Note In the following procedure, press the **Return** key after each step unless otherwise noted. At any time, you can exit the privileged level and return to the user level by entering **disable** at the `Router#` prompt.

To configure a Cisco MWR 2941 for SNMP, follow these steps while in the global configuration mode:

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command	Purpose

Step 3	`Router(config)# snmp-server community string [view view-name] [ro | rw] [number]`
	
	Example:
	`Router(config)# snmp-server community xxxxx RO`
		Sets up the community access string to permit access to SNMP. The **no** form of this command removes the specified community string.
		
		The syntax is as follows:
		• *string*—Community string that acts like a password and permits access to the SNMP protocol.
		• **view** *view-name*—(Optional) Previously defined view. The view defines the objects available to the community.
		• **ro**—(Optional) Specifies read-only access. Authorized management stations are able only to retrieve MIB objects.
		• **rw**—(Optional) Specifies read-write access. Authorized management stations are able to both retrieve and modify MIB objects.
		• *number*—(Optional) Integer from 1 to 99 that specifies an access list of IP addresses that are allowed to use the community string to gain access to the SNMP agent.
		
		The example shows how to configure the community access string as xxxxx with read-only access.

Step 4	`Router(config)# snmp-server queue-length length`
	
	Example:
	`Router(config)# snmp-server queue-length 100`
		Establishes the message queue length for each trap host, use the **snmp-server queue-length** command. The syntax is as follows:
		• *length*—Integer that specifies the number of trap events that can be held before the queue must be emptied.
		
		The examples shows how to configure the number of trap events as 100.

Command	Purpose
Step 5 `Router(config)# snmp-server enable traps [notification-type] [notification-option]` **Example:** `Router(config)# snmp-server enable traps snmp linkdown linkup coldstart warmstart`	Enables the router to send SNMP traps or notifications. Use the **no** form of this command to disable SNMP notifications. The syntax is as follows: • ***notification-type***—**snmp [authentication]**—Enables RFC 1157 SNMP notifications. Note that use of the **authentication** keyword produces the same effect as not using the **authentication** keyword. Both the **snmp-server enable traps snmp** and **snmp-server enable traps snmp authentication** forms of this command globally enable (or, if using the **no** form, disable) the following SNMP traps: – authentication failure – linkup – linkdown – coldstart – warmstart • ***notification-option***—(Optional) **atm pvc** [**interval** *seconds*] [**fail-interval** *seconds*]—The optional interval seconds keyword/argument combination specifies the minimum period between successive traps, in the range from 1 to 3600. Generation of PVC traps is dampened by the notification interval to prevent trap storms. No traps are sent until the interval lapses. The default interval is 30. The optional fail-interval seconds keyword/argument combination specifies the minimum period for storing the failed time stamp, in the range from 0 to 3600. The default fail-interval is 0. • **envmon** [**voltage** | **shutdown** | **supply** | **fan** | **temperature**]—When the **envmon** keyword is used, you can enable a specific environmental notification type, or accept all notification types from the environmental monitor system. If no option is specified, all environmental notifications are enabled. The option can be one or more of the following keywords: **voltage**, **shutdown**, **supply**, **fan**, and **temperature**. • **isdn** [**call-information** | **isdn u-interface**]—When the **isdn** keyword is used, you can specify the **call-information** keyword to enable an SNMP ISDN call information notification for the ISDN MIB subsystem, or you can specify the **isdnu-interface** keyword to enable an SNMP ISDN U interface notification for the ISDN U interface MIB subsystem. • **repeater** [**health** | **reset**]—When the **repeater** keyword is used, you can specify a repeater option. If no option is specified, all repeater notifications are enabled. The option can be one or more of the following keywords: – **health**—Enables IETF Repeater Hub MIB (RFC 1516) health notification. – **reset**—Enables IETF Repeater Hub MIB (RFC 1516) reset notification.

	Command	Purpose
Step 6	`Router(config)# snmp-server enable traps ipran`	Enables SNMP traps for all IP-RAN notifications. **Note** Besides enabling SNMP traps for all IP-RAN notifications, you can also enable traps for IP-RAN GSM alarms, UMTS alarms, and general information about the backhaul utilization. For descriptions on how to use these SNMP commands, see the *Cisco MWR 2941 Mobile Wireless Edge Router IOS Command Reference, Release 15.0(1)MR*.
Step 7	`Router(config)# snmp-server enable traps envmon`	Enables SNMP traps for a specific environment, use the **snmp-server enable traps envmon** command.

Step 8	`Router(config)# snmp-server host` *host-addr* `[traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]` *community-string* `[udp-port port] [notification-type]`
	Example:
	`Router(config)# snmp-server host 10.20.30.40 version 2c`
		Specifies the recipient of an SNMP notification operation. To remove the specified host, use the **no** form of this command.
		The syntax is as follows:
		• *host-addr*—Name or Internet address of the host (the targeted recipient).
		• **traps**—(Optional) Sends SNMP traps to this host. This is the default.
		• **informs**—(Optional) Sends SNMP informs to this host.
		• **version**—(Optional) Version of the SNMP used to send the traps. Version 3 is the most secure model because allows packet encryption with the **priv** keyword. If you use the version keyword, one of the following must be specified:
		– **1**—SNMPv1. This option is not available with informs.
		– **2c**—SNMPv2C.
		– **3**—SNMPv3. The following three optional keywords can follow the version 3 keyword:
		–**auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication
		–**noauth** (Default). The noAuthNoPriv security level. This is the default if the [auth | noauth | priv] keyword choice is not specified.
		–**priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called “privacy”).
		• *community-string*—Password-like community string sent with the notification operation. Though you can set this string using the **snmp-server host** command by itself, we recommend you define this string using the **snmp-server community** command before using the **snmp-server host** command.
		• **udp-port** *port*—UDP port of the host to use. The default is 162.

Command	Purpose
	• *notification-type*—(Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the following keywords: – **aaa_server**—Enable SNMP AAA Server traps. – **atm**—Enable SNMP atm Server traps. – **ccme**—Enable SNMP ccme traps. – **cnpd**—Enable NBAR Protocol Discovery traps. – **config**—Enable SNMP config traps. – **config-copy**—Enable SNMP config-copy traps. – **cpu**—Allow cpu related traps. – **dial**—Enable SNMP dial control traps. – **dnis**—Enable SNMP DNIS traps. – **ds0-busyout**—Enable ds0-busyout traps. – **ds1**—Enable SNMP DS1 traps. – **ds1-loopback**—Enable ds1-loopback traps. – **ds3**—Enable SNMP DS3 traps. – **dsp**—Enable SNMP dsp traps. – **eigrp**—Enable SNMP EIGRP traps. – **entity**—Enable SNMP entity traps. – **envmon**—Enable SNMP environmental monitor traps. – **flash**—Enable SNMP FLASH notifications. – **frame-relay**—Enable SNMP frame-relay traps. – **hsrp**—Enable SNMP HSRP traps. – **icsudsu**—Enable SNMP ICSUDSU traps. – **ipmulticast**—Enable SNMP ipmulticast traps. – **ipran**—Enable IP-RAN Backhaul traps. – **ipsla**—Enable SNMP IP SLA traps. – **isdn**—Enable SNMP isdn traps. – **l2tun**—Enable SNMP L2 tunnel protocol traps. – **mpls**—Enable SNMP MPLS traps. – **msdp**—Enable SNMP MSDP traps. – **mvpn**—Enable Multicast Virtual Private Networks traps. – **ospf**—Enable OSPF traps. – **pim**—Enable SNMP PIM traps.

	Command	Purpose
		– **pppoe**—Enable SNMP pppoe traps. – **pw**—Enable SNMP PW traps. – **rsvp**—Enable RSVP flow change traps. – **snmp**—Enable SNMP traps. – **srst**—Enable SNMP srst traps. – **syslog**—Enable SNMP syslog traps. – **tty**—Enable TCP connection traps. – **voice**—Enable SNMP voice traps. – **vrrp**—Enable SNMP vrrp traps. – **vtp**—Enable SNMP VTP traps. – **xgcp**—Enable XGCP protocol traps. The example specifies a recipient of the SNMP operation with a host-address of 10.20.30.40 with a version SNMP of SNMPv2C.

Step 9	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode.

Enabling Remote Network Management

To enable remote network management of the Cisco MWR 2941, do the following:

	Command	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	`Router(config)# ip host` *hostname ip_address*	Assigns a host name to each of the network management workstations, where *hostname* is the name assigned to the Operations and Maintenance (O&M) workstation and *ip_address* is the address of the network management workstation.
Step 4	`Router(config)# interface loopback` *number* `Router(config-if)# ip address` *ip_address subnet_mask*	Creates a loopback interface for O&M. **Note** For more information about creating loopback interfaces, see Chapter 19, "Configuring Multiprotocol Label Switching."
Step 5	`Router(config-if)# exit` `Router(config)#`	Exits interface configuration mode.

	Command	Purpose
Step 6	`Router(config)# snmp-server host` *hostname* `[traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]}]` *community-string* `[udp-port` *port*`] [`*notification-type*`]`	Specifies the recipient of a Simple Network Management Protocol (SNMP) notification operation. The *hostname* is the name assigned to the Cisco Info Center workstation with the **ip host** command in Step 3.
Step 7	`Router(config)# snmp-server community` *public* `RO` `Router(config)# snmp-server community` *private* `RW`	Specifies the public and private SNMP community names.
Step 8	`Router(config)# snmp-server enable traps`	Enables the transmission of SNMP traps.
Step 9	`Router(config)# snmp-server trap-source loopback` *number*	Specifies the loopback interface from which SNMP traps should originate, where *number* is the number of the loopback interface you configured for the O&M in Step 4.

Step 10	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits configuration mode.

Show Commands for Monitoring the Cisco MWR 2941 Router

To monitor and maintain the Cisco MWR 2941 router, use the following commands:

Command	Purpose
show atm cell-packing	Information about Layer 2 transport ATM cell-packing.
show cem circuit	Summary about the CEM circuit state, including controller, interface, and AC. Also displays specific CEM circuit state, circuit parameters, and statistics/counters.
show cem platform	CEM errors and information.
show connection	Displays the status of interworking connections.
show controllers	All network modules and their interfaces. Also displays the status of the VWIC relays when a VWIC is installed.
show controllers gigabitethernet *slot/port*	Information about initialization block, transmit ring, receive ring, and errors for the Fast Ethernet controller chip.
show controllers e1	Information about controller status specific to the controller hardware. Also displays statistics about the E1 link. If you specify a slot and a port number, statistics for each 15-minute period appears.

Command	Purpose
show controllers t1	Information about cable length, framing, firmware, and errors associated with the T1. With the Cisco MWR 2941 router, this command also shows the status of the relays on the VWIC.
show dsl interface atm	Displays information specific to the asymmetric digital subscriber line (ADSL) for a specified ATM interface.
show gsm traffic	Traffic rates in bits per second at 1 second, 5 seconds, 1 minute, 5 minutes, and 1 hour intervals for GSM data transmitted and received over the backhaul.
show gsm-abis efficiency [history]	The history of the GSM efficiency averages for compression/decompression at 1-second, 5-second, 1-minute, 5-minute, and 1-hour intervals.
show gsm-abis errors	Error statistics counters of the GSM for compression/decompression.
show gsm-abis packets	Packet statistics counters of the GSM for compression/decompression.
show gsm-abis peering [details]	Peering status, statistics, and history of the GSM compression/decompression.
show interface *type slot/port*	Configuration and status of the specified interface.
show interface switchport backup	Status information about the backup switchport.
show interface virtual-cem *slot/port*	Status of the CEM interface.
show interface gigabitethernet *slot/port*	Status of the FE interface.
show ip mroute	Contents of the multicast routing (mroute) table. **Note** Multicast routing applies only to PTP redundancy.
show ip rtp header-compression	RTP header compression statistics.
show ip tcp header-compression	Transmission Control Protocol (TCP)/IP header compression statistics **Note** The Cisco MWR 2941 supports UDP header-compression in IEFT format only.
show mpls l2transport vc	Information about Any Transport over MPLS (AToM) virtual circuits (VCs) that are enabled to route Layer 2 packets on a router.
show network-clocks	Network clocking configuration.
show platform hardware	Status of hardware devices on the Cisco MWR 2941 router.
show policy-map	Configuration of all classes for a specified service policy map or of all classes for all existing policy maps.

Command	Purpose
show policy-map interface	Statistics and the configurations of the input and output policies that are attached to an interface.
show ppp multilink	MLP and multilink bundle information.
show ppp multilink interface *number*	Multilink information for the specified interface.
show protocols	Protocols configured for the router and the individual interfaces.
show ptp clock	PTP clock information.
show ptp foreign-master-record	PTP foreign master records.
show ptp parent	PTP parent properties.
show ptp port	PTP port properties.
show ptp time-property	PTP clock time properties.
show xconnect all	xconnect information.

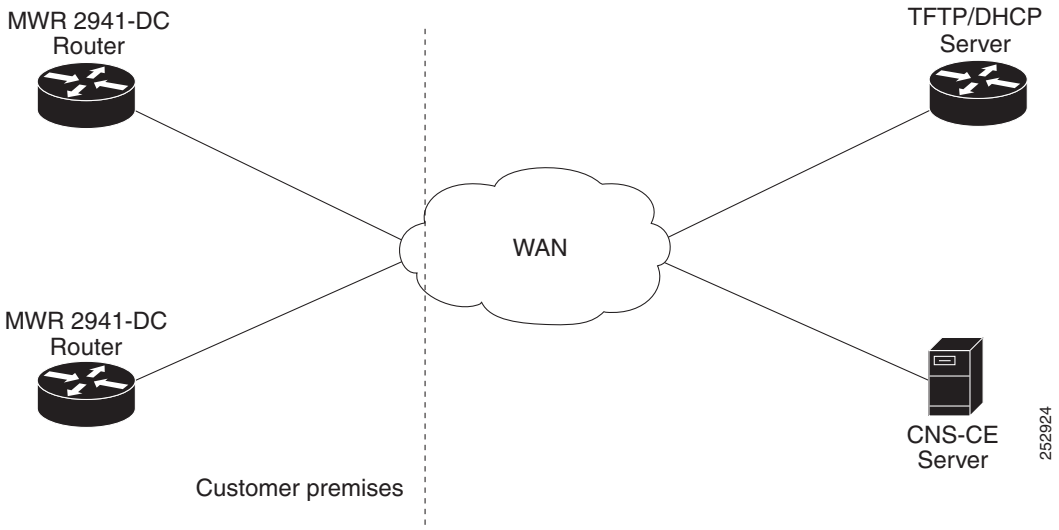
Configuring Cisco Networking Services (CNS)

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.

To enable CNS, you need the following items:

- A DHCP server (standalone or enabled on the carrier edge router)
- A TFTP server (standalone or enabled on the carrier edge router)
- A server running the Cisco Configuration Engine (formerly known as the CNS-CE server)



Note These devices must be connected through onboard Ethernet interfaces. CNS connections over Ethernet HWICs and non-Ethernet interfaces are not supported.

The following sections describe how to configure CNS on the Cisco MWR 2941.

- Process Overview
- Configuring a DHCP Server
- Configuring a TFTP Server
- Configuring the Cisco Configuration Engine
- Verifying the Configuration
- Zero Touch Deployment Sample Configuration

Process Overview

The following sections provide an overview of the steps that take place during a Cisco MWR 2941 zero-touch deployment and image download.

Zero-Touch Deployment

The following sequence of events takes place when a CNS-enabled Cisco MWR 2941 boots and receives a configuration.

1. The Cisco MWR 2941 boots and sends a DHCP Discover message
2. The DHCP Server replies with DHCP Offer
3. The Cisco MWR 2941 sends DHCP Request
4. The DHCP Server replies with option 150 for TFTP
5. The Cisco MWR 2941 requests network-confg file via TFTP
6. The TFTP server sends the Cisco MWR 2941 a network-config file
7. The Cisco MWR 2941 sends an HTTP request to the CNS-CE server

8. The CNS-CE server sends a configuration template to the Cisco MWR 2941
9. Successful event
10. Publish success event

Image Download

The following events take place when a CNS-enabled Cisco MWR 2941 downloads a new image.

1. The CNS-CE server requests inventory (disk/flash info) from the Cisco MWR 2941-DC
2. The Cisco MWR 2941-DC sends an inventory
3. The CNS-CE server sends an image location
4. The Cisco MWR 2941-DC sends an TFTP image request
5. The Cisco MWR 2941-DC downloads an image from the TFTP server
6. The Cisco MWR 2941-DC indicates that the image download is complete
7. The CNS-CE server reboots the Cisco MWR 2941-DC router

Configuring a DHCP Server

The Cisco MWR 2941 requires a DHCP server for zero-touch deployment. The DHCP server is typically implemented on the carrier edge router. You can use the following sample configuration to enable a DHCP server on the edge router.

```
ip dhcp excluded-address 30.30.1.6
ip dhcp excluded-address 30.30.1.20 30.30.1.255
!
ip dhcp pool mwrdhcp
network 30.30.1.0 255.255.255.0
option 150 ip 30.30.1.6
! Specifies the TFTP server address
!
default-router 30.30.1.6
```

Configuring a TFTP Server

You need to set up a TFTP server in order to provide a bootstrap image to 2941s when they boot.

Creating a Bootstrap Configuration

The TFTP server should store a configuration that the Cisco MWR 2941 uses to boot. The following sample configuration specifies 30.30.1.20 as the CNS server IP address and port 80 for the configuration service.

```
hostname test-2941
!
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
cns id hostname image
cns exec 80
logging buffered 20000
```

```
!
end
```

For more information about the commands used in this configuration, see the *Cisco MWR 2941 Mobile Wireless Edge Router IOS Command Reference, Release 15.0(1)MR*. *Cisco Configuration Engine Installation & Configuration Guide* at http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html.

Enabling a TFTP Server on the Edge Router

The Cisco MWR 2941 requires a TFTP server for zero-touch deployment. The TFTP server is typically implemented on the carrier edge router. You can use the following global configuration commands enable a TFTP server on the edge router that can send a configuration to the Cisco MWR 2941 router.

```
tftp-server sup-bootflash:network-confg
tftp-server sup-bootflash:test-2941-confg
```

Once the Cisco MWR 2941 boots with this configuration, it can connect to the CNS-CE server.

Configuring the Cisco Configuration Engine

The Cisco Configuration Engine (formerly known as the Cisco CNS Configuration Engine) allows you to remotely manage configurations and IOS software images on Cisco devices including the Cisco MWR 2941.

Once the Cisco MWR 2941 downloads the bootstrap configuration and connects to the Cisco Configuration Engine server, you can use the server to download a full configuration to the router. You can also use the CNS-CE server to complete any of the following tasks:

- Manage configuration templates—The CNS-CE server can store and manage configuration templates.
- Download a new image—You can use the CNS-CE server to load a new IOS image on a Cisco MWR 2941 router.
- Loading a new config—You can use the CNS-CE server to load a new configuration file on a Cisco MWR 2941 router.
- Enable identification—You can use a unique CNS agent ID to verify the identity of a host device prior to communication with the CNS-CE server.
- Enable Authentication—You can configure the CNS-CE server to require a unique password from the 2941 router as part of any communication handshake.
- Enable encryption—You can enable Secure Socket Layer (SSL) encryption for the HTTP sessions between the CNS agent devices (Cisco MWR 2941 routers) and the CNS-CE server.

For instructions about how to use the CNS-CE server, see the *Cisco Configuration Engine Installation & Configuration Guide* at http://www.cisco.com/en/US/products/sw/netmgtsw/ps4617/tsd_products_support_series_home.html.

Verifying the Configuration

You can use the following IOS commands to verify the CNS configuration on the Cisco MWR 2941.

- **show cns event connection**
- **show cns image connection**
- **show cns image inventory**

- **debug cns all**

Zero Touch Deployment Sample Configuration

The following configuration example sets the Cisco MWR 2941 to boot using configurations stored on a CNS–CE server with the IP address 30.30.1.20.

Note This section provides partial configurations intended to demonstrate a specific feature.

```
hostname 2941
!
cns trusted-server all-agents 30.30.1.20
cns event 30.30.1.20 11011 keepalive 60 3
cns config initial 30.30.1.20 80
cns config partial 30.30.1.20 80
cns id hostname
cns id hostname event
cns id hostname image
cns exec 80
logging buffered 20000
!
end
```