



CHAPTER 6

Configuring the MWAM

This chapter discusses how to configure the MWAM. It includes the following sections:

- [Before You Begin, page 6-2](#)
- [VLAN Configuration Tasks, page 6-4](#)
- [MWAM Session Configuration Tasks, page 6-8](#)
- [Verifying the MWAM Configuration, page 6-14](#)
- [Converting to Supervisor Mode, page 6-15](#)
- [Configuring Remote Console and Logging, page 6-16](#)
- [Clearing MWAM Session from Supervisor Console, page 6-18](#)
- [Recovering from MWAM Processor Lockout, page 6-19](#)
- [Recover from Session/Telnet Command after Reload, page 6-20](#)
- [Recovering from Session Loss, page 6-21](#)

For a complete description about the commands used in configuring the MWAM, see Appendix A, “[Command Reference](#)”. To locate documentation about other commands that appear in this chapter, refer to the following books:

- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*—Chapter 2
- *Cisco 7600 Series Internet Router IOS Software Configuration Guide*—Chapter 2

Before You Begin

Before you configure the MWAM, read the following required sections:

- Release Notes
- Using the CLI
- Unsupported Commands
- Booting the Application Image

Release Notes

Refer to the latest release notes for your configuration. The release notes contain additional information that became available after the initial release of the product. These release notes describe the features, modifications, and caveats for the MWAM and its associated software and hardware platforms.

**Note**

The most current version of these release notes can be found on Cisco.com (for MWAM), click:

Documentation>Routers>Cisco 7600 Series Routers>General Information>Release Notes>Release Notes for Cisco Multiprocessor WAN Application Module with Cisco IOS Release

On Cisco.com (for IOS), click:

Documentation>Cisco IOS Software>Cisco Software Releases 12.3 Mainline>General Information>Release Notes>Cisco IOS Release 12.3 Cross-Platform Release Notes and Caveats

**Caution**

We strongly recommend that you read these release notes before using your MWAM or upgrading your MWAM software.

Each release note contains the following sections:

- System Requirements
- New and Changed Information
- Performance
- External Interfaces
- IP Address Management
- Reliability/Availability
- MWAM Installation and Configuration
- Limitations and Restrictions
- Caveats
- MIBs

Using the CLI

In configuring the MWAM, you use two command line interfaces:

- Main CLI on the Supervisor console to:
 - boot the device and load the application image
 - assign VLANs to the MWAM
 - configure MWAM VLANs on the Supervisor module
- Session CLI to each MWAM processor to:
 - configure subinterfaces on the VLANs
 - assign IP addresses to the subinterfaces
 - configure the application

On the Supervisor console, the main commands are:

- **mwam module** command—Configures connectivity between the switch fabric and the individual processors on the MWAM
- **show mwam module** command—Shows information about the individual MWAM processors. You must also configure any real external interfaces required by the application and VLANs to forward traffic to the switch fabric.

On the session CLI to the MWAM processor, you can access Cisco IOS commands to configure the application as required. This includes configuring the VLAN subinterfaces to connect to the switch fabric.

**Note**

To get a basic understanding of the Cisco IOS CLI and Cisco IOS command modes (see Chapter 4, “[Command-Line Interface \(CLI\) Basics](#)” and refer to Chapter 2, “Command Line Interfaces”, in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* and the *Cisco 7600 Series Router IOS Software Configuration Guide*).

Unsupported Commands

**Note**

Support for NTP/Clock configuration on the MWAM was introduced in release 12.3(3)B1.

If NTP is configured on the MWAM, the processors synchronize with the NTP server clock. The Gi0/0 interface must be up and the NTP server must be reachable for synchronization to occur. If the MWAM is configured in Supervisor mode, the configuration must be downloaded before the Gi0/0 can come up.

If NTP is disabled (the default), the processors synchronize (once every minute) with the processor control complex.

The following NTP/Clock commands are not supported on the MWAM:

- `clock calendar-valid`
- `ntp master`
- `ntp update-calendar`

Booting the Application Image

As described in the “[Booting the Application Image](#)” section on page 5-12, the MWAM boots to the application image when initially powered on. Before “[Assigning VLANs to the MWAM](#)”, ensure that the AP image has been downloaded to the MWAM. If it has not, follow the procedures described in Chapter 4, “[Loading the MWAM](#)”.

VLAN Configuration Tasks

A virtual LAN (VLAN) configures switches and routers according to logical rather than physical topologies. Using VLANs, you can combine any collection of LAN segments within an internetwork into an autonomous user group, which appears as a single LAN. VLANs locally segment the network into different broadcast domains so that packets are switched only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

This section describes how to configure the VLANs for the MWAM.

The tasks discussed are:

- [Assigning VLANs to the MWAM](#)
- [Assigning MWAM Traffic to VLAN QoS Policies](#), page 6-5
- [Configuring MWAM VLANs on the Supervisor Module](#), page 6-6
- [Configuring Layer 3 Interfaces on the VLANs](#), page 6-7

Assigning VLANs to the MWAM



Note

By default, the MWAM is in trunking mode and assigned to VLAN 1.

Assigning VLANs to the MWAM requires you to understand the mapping between the processors on the MWAM and the Ethernet port/VLAN that connects the processor to the switch fabric (see [Table 1-2 on page 1-5](#) and [Figure 1-2 on page 1-5](#) for this information).

To assign VLANs to the MWAM, enter this command for each of the three switch fabric interface ports (ports 1, 2, and 3) that connect the Supervisor module to the MWAM:

	Command	Purpose
Step 1	Sup-7606> enable	Enters privileged EXEC mode.
Step 2	Sup-7606# configure terminal	Enters the configuration mode.
Step 3	Sup-7606(config)# mwam module slot_number port port_number allowed-vlan vlan_ID	Configures the Ethernet connectivity from the backplane (that is, switch fabric) to the individual processors on the MWAM.
		Note One of the allowed VLANs must be the administrative VLAN.

This example assigns VLANs 1-1005 to ports 1-3 that connect to the MWAM in slot 5:

```
Sup-7606>
Sup-7606> enable

Sup-7606# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sup-7606(config)# mwam module 5 port 1 allowed-vlan 1-1005
Sup-7606(config)# mwam module 5 port 2 allowed-vlan 1-1005
Sup-7606(config)# mwam module 5 port 3 allowed-vlan 1-1005
```

**Note**

You may need to wait up to 30 seconds for spanning tree to converge for connectivity.

Assigning MWAM Traffic to VLAN QoS Policies

**Note**

This feature was introduced with Cisco IOS Release 12.2(14)ZA7.

Quality of Service (QoS) policies can be applied to differentiate levels of service to GGSN-based subscribers. A QoS policy is assigned to the same VLAN to which MWAM ports are assigned (see [Assigning VLANs to the MWAM, page 6-4](#)).

To assign MWAM traffic to the QoS policy, enter the following command for each of the three switch fabric interface ports (ports 1, 2, and 3) that connect the Supervisor module to the MWAM:

	Command	Purpose
Step 1	Sup-7606> enable	Enters privileged EXEC mode.
Step 2	Sup-7606# configure terminal	Enters the configuration mode.
Step 3	Sup-7606(config)# mwam module slot_number port port_number vlan-based	Assigns MWAM traffic on the specified port to VLAN-based QoS policies.

The following example assigns traffic to QoS policies for the switch fabric interface ports of the MWAM in slot 5:

```
Sup-7606>
Sup-7606> enable

Sup-7606# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Sup-7606(config)# mwam module 5 port 1 vlan-based
Sup-7606(config)# mwam module 5 port 2 vlan-based
Sup-7606(config)# mwam module 5 port 3 vlan-based
```

Configuring MWAM VLANs on the Supervisor Module

You must configure the VLANs on the Supervisor 2 module to forward traffic to the switch fabric. On the session CLI to the MWAM processor, you access the Cisco IOS commands to configure the VLANs. Two configuration modes are available for configuring Supervisor module VLANs:

- VLAN database mode
- Global configuration mode



Caution

RPR+ redundancy does not support configurations entered in VLAN database mode. If you have a high-availability configuration with redundant Supervisor modules using RPR(+), configure the VLANs in global configuration mode and not in the VLAN database mode; otherwise, the VLAN information would not be synchronized to the redundant Supervisor module.

VLAN Database Mode



Note

You cannot configure extended-range VLANs in VLAN database mode. You can configure extended-range VLANs only in global configuration mode.

To configure VLANs on the Supervisor 2 module in the VLAN database mode, perform this task:

	Command	Purpose
Step 1	Sup-7606> enable	Enters privileged EXEC mode.
Step 2	Sup-7606# vlan database	Enters VLAN database mode.
Step 3	Sup-7606(vlan)# vlan <i>vlan_ID</i>	Specifies a VLAN (1-1005) to configure.
Step 4	Sup-7606(vlan)# exit	Updates the VLAN database and returns to privileged EXEC mode.

This example shows how to configure VLANs on the Supervisor 2 module in the VLAN database mode:

```
Sup-7606> enable
Sup-7606# vlan database
Sup-7606(vlan)# vlan 100
VLAN 100 added:
    Name: VLAN100
Sup-7606(vlan)# exit
APPLY completed.
Exiting...
```

Global Configuration Mode



Note

Release 12.1(11b)E or later supports VLAN configuration in global configuration mode.

To configure VLANs on the Supervisor 2 module in the global configuration mode, perform this task:

	Command	Purpose
Step 1	Sup-7606# configure terminal	Enters global configuration mode.
Step 2	Sup-7606(config)# vlan <i>vlan_ID</i> {[- <i>vlan_ID</i>] [, <i>vlan_ID</i>] }	Enters VLAN configuration mode and creates an Ethernet VLAN, a range of Ethernet VLANs, or several Ethernet VLANs in a comma-separated list (do not enter space characters).
Step 3	Sup-7606(config-vlan)# end	Updates the VLAN database and returns to privileged EXEC mode.

This example shows how to configure VLANs on the Supervisor 2 module in global configuration mode:

```
Sup-7606# configure terminal
Sup-7606(config)# vlan 100-200
Sup-7606(config-vlan)# end
```

Configuring Layer 3 Interfaces on the VLANs

You can configure layer 3 interfaces on the MWAM VLANs if required by the application.



Note VLANs must exist before you can configure the layer 3 interfaces on them.

To configure the Layer 3 VLAN interface, perform this task:

	Command	Purpose
Step 1	Sup-7606# configure terminal	Enters global configuration mode.
Step 2	Sup-7606(config)# interface <i>vlan</i> <i>vlan_ID</i>	Selects an interface to configure.
Step 3	Sup-7606(config-if)# ip address <i>ip_address subnet_mask</i>	Configures the IP address and IP subnet.
Step 4	Sup-7606(config-if)# no shutdown	Enables the interface.
Step 5	Sup-7606(config-if)# exit	Exits configuration mode.

This example shows how to configure the Layer 3 VLAN interface:

```
Sup-7606# configure terminal
Sup-7606(config)# interface vlan 100

Sup-7606(config-if)# ip address 10.10.1.10 255.255.255.0

Sup-7606(config-if)# no shutdown
Sup-7606(config-if)# exit
```


MWAM Session Configuration Tasks

This section details the MWAM session configuration tasks that should be performed.

- [Configuring a LAN Port for Layer 2 Switching, page 6-12](#)
- [Configuring Subinterfaces on MWAM Processor, page 6-13](#)
- [Configuring the MWAM Memory Allocation, page 6-17](#)

Configuring the Application to the MWAM

To configure the application on an MWAM processor, complete the following steps (see [Cisco IOS Restrictions and Limitations on the MWAM, page 6-9](#) for information about Cisco IOS restrictions and limitations on the MWAM architecture):

	Command	Purpose
Step 1	Sup-7600> enable	Enters privileged EXEC mode.
Step 2	Sup-7600# session slot <i>slot_number</i> processor <i>processor_number (2-6)</i>	Establishes a session to the MWAM processor to allow Cisco IOS configuration. Note You can only configure interface Gi0/0.
Step 3	mwam-6-4> enable	Enters privileged EXEC mode.
Step 4	mwam-6-4# dir bootflash:	Displays the bootflash directory. Note If response is 0 bytes free, format the bootflash file system.
Step 5	mwam-6-4# format bootflash:	Formats the bootflash file system to enable it to store files (see caution).  Caution Use format command <i>only</i> if the response to dir bootflash: is 0 bytes free.
Step 6	Configure the application.	Refer to the configuration guide for the application.
Step 7	mwam-6-4# copy running-config startup-config	Copies the running configuration to NVRAM on the MWAM (if in local mode) or Supervisor bootflash (if in Supervisor mode).

This example shows how to establish a session to an MWAM processor:

```
Sup-7606> enable
Sup-7606# session slot 6 processor 4
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.64 ... Open <<<<< last part of address indicates slot 6, processor 4

mwam-6-4#

Press RETURN to get started!

mwam-6-4# dir bootflash:
Directory of bootflash:/
```



```
No files in directory
524288 bytes total (0 bytes free) <<<response indicates that bootflash requires formatting
```

```
mwam-6-4# format bootflash:
```

```
Format operation may take a while. Continue? [confirm]
Format operation will destroy all data in "bootflash:". Continue? [confirm]
Format of bootflash complete
```

After configuring the application, make a backup of the configuration as follows:

```
mwam-6-4# copy running-config startup-config
Destination filename [startup-config]?
.
.
.
```

Cisco IOS Restrictions and Limitations on the MWAM

When you establish a session to an MWAM processor, you can access Cisco IOS commands to configure the application as required. This section describes Cisco IOS restrictions and limitations required by the MWAM architecture. The following topics are covered:

- [Reload Command](#)
- [Hot Standby Router Protocol Configuration, page 6-10](#)
- [Multicast MAC Addressing, page 6-10](#)
- [Copy Running Configuration Command, page 6-10](#)
- [Copy TFTP Command, page 6-11](#)
- [Erase Startup Configuration Command, page 6-11](#)
- [Show Startup Configuration Command, page 6-11](#)
- [Squeeze Bootflash Command, page 6-12](#)

Reload Command

The Cisco IOS **reload** command reloads a Cisco router. However, at the MWAM processor level, use the Cisco IOS **reload** command with caution. Two MWAM processors reside on one processor complex. When the **reload** command is issued for one processor, *both* processors on the complex are reloaded. In the following example, reloading processor 4 also reloads processor 5 because they share a complex.

```
MWAM-7-4# reload
!!!! WARNING !!!!!
CPU 5 in this complex will also be reloaded. All the changed configs
there will be lost unless saved before confirming the reload.
Proceed with reload? [confirm]
Mar 23 05:55:41.915: This processor is being reloaded, session connection from sup will be
reset
Mar 23 05:55:43.819:%SYS-5-RELOAD:Reload requested by console. Reload Reason:Reload
command.
```

Also, if you issue the reload command at the Supervisor level, the reload occurs for the entire chassis, which includes all modules in the chassis. If the chassis contains five MWAMs, and each MWAM contains five active processors, then 25 routers are reloaded by this operation.

Hot Standby Router Protocol Configuration

The MWAM architecture imposes some limitations on the configuration of the Hot Standby Router Protocol (HSRP). You must not configure HSRP groups for processors that are in the same processor complex. Because of the MWAM architecture, when one processor fails (crashes), both processors in the complex reload. For this reason, HSRP groups are not supported for processors in the same complex.

You can configure HSRP groups for processors on the same MWAM as long as they are not in the same complex. A preferable strategy is to configure HSRP groups to span processors on different MWAMs.

Multicast MAC Addressing

The Cisco IOS supports multicast Media Access Control (MAC) addressing in multiple ways. The MWAM supports some of these ways better than others. For applications, such as HSRP, where a single multicast MAC address is used, the MWAM can support the address in the same way as any other MAC address.

Each processor complex supports up to eight explicit MAC address entries. However, when exceeding this limit, the MWAM must use the multicast promiscuous mode. In this mode, all multicast addresses are received by the processor and must be validated in software rather than hardware. This restriction places additional load on the processor. Other types of multicast MAC addressing in the Cisco IOS (for example, IP multicast routing) require the multicast promiscuous mode at all times.

When the multicast promiscuous mode is enabled on both processors in a complex, each one processes *all* of the multicast packets. This condition leads to additional processing at the MAC layer. For this reason, Cisco recommends that IP multicast routing be configured on only one processor per complex.

You can determine the mode with the **show controller** command.

Copy Running Configuration Command



Note

The following restrictions were introduced with release 12.2(14)ZA5.

Local Mode Operation

For MWAMs operating in local mode, the **copy running-config** command copies the running configuration to NVRAM on the MWAM. See the example that follows:

```
mwam-6-4# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

```
mwam-6-4# show startup
Using 505 out of 524280 bytes
!
!NVRAM config last updated at <time stamp>
```

```
<configuration>
```

```
end
```

Supervisor Mode Operation

For MWAMs operating in Supervisor mode, the **copy running-config** command copies the running configuration to the Supervisor module(s). See the example that follows:

```
mwam-6-4# copy running-config startup-config
Destination filename [startup-config]?
```

```
Writing bootflash:SL0T6PC4.cfg
Config uploaded to supervisor in slot 1
```

```
Writing bootflash:SL0T6PC4.cfg
Config uploaded to supervisor in slot 2
```

```
Config uploaded to 2 supervisor(s)
```

**Note**

If redundant Supervisor modules are equipped and the **copy running-config startup-config** command succeeds for one Supervisor but fails for the other, you must manually correct the failure. If differences exist in an MWAM configuration file between the master and slave Supervisor modules, the file at the master Supervisor module is written over the file at the slave Supervisor module.

Copy TFTP Command**Note**

The following restriction was introduced with release 12.2(14)ZA5.

**Caution**

The command **copy tftp://.../filename startup-config** (issued at the MWAM processor level) copies the *filename* configuration to NVRAM on the MWAM. This action causes an MWAM that is configured in Supervisor mode to revert to local mode when the next reload operation occurs. Because a file exists in NVRAM, the MWAM processor gets its configuration locally and not from the Supervisor bootflash. To return to the Supervisor mode, perform the procedure provided in the [“Converting to Supervisor Mode” section on page 6-15](#).

Erase Startup Configuration Command**Note**

The following restrictions were introduced with release 12.2(14)ZA5.

Local Mode

When operating in local mode, use the command **erase startup-config** (issued at the MWAM processor level) to erase the local NVRAM configuration file.

Supervisor Mode

When operating in Supervisor mode, erase the configuration file in the Supervisor bootflash with the following commands from the Supervisor console:

- **delete bootflash:SL0T \times PCy.cfg** for the master Supervisor
- **delete slavebootflash:SL0T \times PCy.cfg** for the slave Supervisor

Show Startup Configuration Command**Note**

The following restrictions were introduced with release 12.2(14)ZA5.

Local Mode

When operating in local mode, the command **show startup-config** (issued at the MWAM processor level) shows the contents of the NVRAM configuration file.

Supervisor Mode

When operating in Supervisor mode, show the startup configuration using the following commands from the Supervisor console:

- **more bootflash: SLOTxPCy.cfg** for the master Supervisor
- **more slavebootflash: SLOTxPCy.cfg** for the slave Supervisor



Note

If you enter **show startup-config** from the MWAM console while in Supervisor mode, the system response is `startup-config is not present` because this command is reading the NVRAM on the MWAM.

Squeeze Bootflash Command

When operating in Supervisor mode, the operator must maintain adequate file space on the Supervisor bootflash. This includes periodically using the **squeeze bootflash** command to consolidate available space.

Configuring a LAN Port for Layer 2 Switching

To configure physical interfaces that connect to the servers or the clients in the corresponding VLAN, perform this task at the MWAM processor level:

	Command	Purpose
Step 1	<code>pro-6-2# configure terminal</code>	Enters configuration mode.
Step 2	<code>pro-6-2(config)# interface type¹ slot/port</code>	Selects the LAN port to configure.
Step 3	<code>pro-6-2(config-if)# switchport</code>	Configures the LAN port for Layer 2 switching. Note You must enter the switchport command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional switchport commands with keywords.
Step 4	<code>pro-6-2(config-if)# switchport mode access</code>	Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.
Step 5	<code>pro-6-2(config-if)# switchport access vlan vlan_ID</code>	Configures the default VLAN, which is used if the interface stops trunking.
Step 6	<code>pro-6-2(config-if)# no shutdown</code>	Activates the interface.

1. *type* = ethernet, fastethernet, gigabitethernet, or tengigabitethernet

This example shows how to configure a physical interface as a Layer 2 interface and assign it to a VLAN:

```
pro-6-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

pro-6-2(config)# interface gigabitethernet 1/1
```

```

pro-6-2(config-if)# switchport

pro-6-2(config-if)# switchport mode access

pro-6-2(config-if)# switchport access vlan 100

pro-6-2(config-if)# no shutdown

pro-6-2(config-if)# exit

```

Configuring Subinterfaces on MWAM Processor

The IEEE 802.1Q protocol is used to provide trunks between switches. The switches use the trunks to share VLANs and transfer data between VLANs on different switches. Create as many subinterfaces as needed to connect to different networks. You will configure 802.1Q encapsulation on each subinterface to the VLANs created on the Supervisor module.

To enable 802.1Q encapsulation on each of the processors on the MWAM, use the following commands in the interface configuration mode:

	Command	Purpose
Step 1	pro-6-2# configure terminal	Enters configuration mode.
Step 2	pro-6-2(config)# interface gigabitethernet slot/port	Specifies the subinterface on which IEEE 802.1Q will be used.
Step 3	pro-6-2(config-if)# encapsulation dot1Q vlan_id	Defines the encapsulation format as IEEE 802.1Q (dot1q), and specifies the VLAN identifier.
Step 4	pro-6-2(config-if)# ip address ip-address mask	Sets a primary IP address for an interface.

This example shows how to enable IEEE 802.1Q on VLANs 310 and 401.

```

pro-6-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
pro-6-2(config)# interface GigabitEthernet0/0
pro-6-2(config-if)# no ip address
!
pro-6-2(config-if)# interface GigabitEthernet0/0.310
pro-6-2(config-if)# encapsulation dot1Q 310
pro-6-2(config-if)# ip address 10.1.1.44 255.255.255.0
!
pro-6-2(config-if)# interface GigabitEthernet0/0.401
pro-6-2(config-if)# encapsulation dot1Q 401
pro-6-2(config-if)# ip address 10.121.68.44 255.255.255.0

```

Verifying the MWAM Configuration

To verify the configuration, enter these commands:

	Command	Purpose
Step 1	Sup-7600# show spanning-tree vlan <i>vlan_ID</i>	Displays the spanning tree state for the specified VLAN.
Step 2	Sup-7600# show mwam mod <i>slot_number</i> <i>port_number</i> [state traffic]	Displays the trunk configuration.



Note

In the following examples, the MWAM is installed in slot 3 (Gi3/1).

This example shows how to verify that the module is in the forwarding (FWD) state:

```
Sup-7606# show spanning-tree vlan 100
VLAN0100
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0009.e9b2.b864
             This bridge is the root
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32768
             Address     0009.e9b2.b864
             Hello Time 2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 15

Interface          Role Sts Cost          Prio.Nbr Type
-----
Gi3/1              Desg FWD 4             128.129 P2p
Gi4/1              Desg FWD 4             128.193 P2p
Po261              Desg FWD 3             128.833 P2p
Router
```

This example shows how to verify that the VLAN information displayed matches the VLAN configuration:

```
Sup-7606#show mwam module 3 port 1 state
Mwam module 3 data-port 1:
  Switchport: Enabled
  Administrative Mode: trunk
  Operational Mode: trunk
  Administrative Trunking Encapsulation: dot1q
  Operational Trunking Encapsulation: dot1q
  Negotiation of Trunking: Off
  Access Mode VLAN: 1 (default)
  Trunking Native Mode VLAN: 1 (default)
  Trunking VLANs Enabled: 1-1000
  Pruning VLANs Enabled: 2-1001
  Vlans allowed on trunk:1-1000
  Vlans allowed and active in management domain:1-2,95,100
  Vlans in spanning tree forwarding state and not pruned:
    1-2,95,100
  Allowed-vlan : 1-1000

Sup-7606#show mwam module 3 port 1 traffic
Specified interface is up line protocol is up
  Hardware is C6k 1000Mb 802.3, address is 00e0.b0ff.3a18 (bia 00e0.b0ff.3a18)
```

```

MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 1000Mb/s
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 77
Queueing strategy: fifo
Output queue :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 1000 bits/sec, 1 packets/sec
 24598 packets input, 2138920 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
 928697 packets output, 68993318 bytes, 0 underruns
  0 output errors, 0 collisions, 34 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out

```

Converting to Supervisor Mode



Note

This feature requires Cisco IOS 12.2(14)ZA5 (or higher) on the Supervisor module and an MWAM image that supports Supervisor bootflash storage of MWAM configuration files. It also requires the ROMMON to be upgraded as described in the [“Upgrading the ROMMON Image”](#) section on page 5-11.

The default mode for the MWAM configuration file storage is Supervisor mode.

New Behavior

Cisco IOS 12.3(13)T introduces new behavior when converting to the Supervisor mode.

When an MWAM image boots on an MWAM processor, it queries a persistent flag to determine if the operating mode has ever been set. If the persistent flag is set to a mode (Supervisor or local), the MWAM boots up in that mode. If the flag has *never* been set, the MWAM determines the operating mode on the basis of the NVRAM contents. If the NVRAM startup-config file is 0 bytes long, the mode is set to Supervisor; if the NVRAM startup-config file is longer than 0 bytes, the mode is set to local.

Old Behavior

For MWAMs with earlier Cisco releases, the operating mode is determined solely by the contents of the NVRAM. If the NVRAM startup-config file is 0 bytes long, the mode is set to Supervisor; if the NVRAM startup-config file is longer than 0 bytes, the mode is set to local.

Currently deployed MWAMs that have pre-existing configuration files stored in NVRAM will continue to operate in local mode. If you choose to operate the MWAMs in local mode, you can use the **no mwam bootflash access** command in global configuration mode from the Supervisor console to ensure that MWAM access to TFTP/RCP services on the Supervisor is denied with appropriate error messages.

Steps to Convert to Supervisor Mode

To convert an MWAM processor from local mode to Supervisor mode, complete the following steps.

	Command	Purpose
Step 1	Sup-7606> enable	Enters privileged EXEC mode on the Supervisor.
Step 2	Sup-7600# session slot slot_number processor processor_number (2-6)	Establishes a session to the MWAM processor.
Step 3	mwam-6-4> enable	Enters privileged EXEC mode on the MWAM processor.
Step 4	mwam-6-4# show mwam config-mode	Shows the current configuration mode (local or Supervisor) of the MWAM processor.
Step 5	mwam-6-4# mwam config-mode supervisor	Changes the configuration mode to the Supervisor mode.

This example shows how to convert processor 4 on the MWAM in slot 6 to the Supervisor mode:

```
Sup-7606> enable
Sup-7606# session slot 6 processor 4

mwam-6-4> enable
mwam-6-4# show mwam config-mode
mwam config-mode local

mwam-6-4# mwam config-mode supervisor
Writing bootflash:SLOT6PC4.cfg
Config uploaded to supervisor in slot 1

Writing bootflash:SLOT6PC4.cfg
Config uploaded to supervisor in slot 2

Successfully changed mode: mwam config-mode supervisor
```



Caution

If you are operating in the Supervisor mode in a chassis that does not have redundant Supervisor modules, back up both the *startup-config* file of the Supervisor module and all *SLOT*PC*.cfg* files on the bootflash device. Failure to take this precaution could result in the loss of all MWAM configurations, along with the Supervisor configuration.

Configuring Remote Console and Logging



Note

The Remote Console and Logging feature requires Cisco IOS 12.2(14)ZA4 (or higher) on the Supervisor module. It also requires the ROMMON to be upgraded as described in the [“Upgrading the ROMMON Image”](#) section on page 5-11.

To configure the remote console and logging feature, complete the following steps:

	Command	Purpose
Step 1	Sup-7606# configure terminal	Enters configuration mode on the Supervisor console.
Step 2	Sup-7606(config)# logging listen mwam udp_port	Configures UDP port for MWAM logging input to the Supervisor module. Note If you are configuring “ Remote Console Support for the Processor Control Complex ” section on page 1-15, you must use UDP port 4000.
Step 3	Sup-7606(config)# mwam module {slot_number all } cpu {processor_number all } logging log_level	(Optional) Configures the severity level of MWAM logging information to send to the Supervisor module.
Step 4	Sup-7606(config)# exit	Exits configuration mode.
Step 5	Sup-7606# session slot slot_number processor processor_number	Establishes a Telnet session to the MWAM processor.
Step 6	mwam-6-4# configure terminal	Enters configuration mode on the MWAM processor console.
Step 7	mwam-6-4(config)# logging main-cpu udp_port [log_level] [ip_address]	Configures MWAM log redirection to the Supervisor module. Note You must specify the same UDP port number that you designated for the Supervisor module in Step 2 .

When the Remote Console and Logging feature is configured, you can use the **execute-on** command to initiate a remote command request to an MWAM processor (see Appendix A, “[Command Reference](#)” for details).

Configuring the MWAM Memory Allocation

To reallocate the IO memory from the total available DRAM space on Cisco MWAM routers, use the **memory-size iomem** command in global configuration mode. To revert to the default memory allocation, use the **no** form of this command. By default, 32 MB is allocated for IO memory on each processor of a Cisco MWAM router.

The **iomem** configuration command is available on processors 2, 4, or 6, and it will be applied to the respective partner processors 3, 5, or 7 as well when configured. When 1 or 2 GB of total DRAM is available per MWAM processor complex, the permitted values for the IO memory are 32 MB, 64 MB, and 128 MB. When 512 MB of total DRAM is available per MWAM processor complex, only the default 32 MB IO memory option is available. After the IO memory is specified in the command line, the remaining DRAM memory will be used for the processor memory. After configuration, it must be saved and reloaded for the reallocation to occur.

The **memory-size iomem** command is applied in the global configuration mode as follows:

	Command	Purpose
Step 1	Sup-7606> enable	Enters privileged EXEC mode.
Step 2	Sup-7606# session slot <i>slot_number</i> processor <i>processor_number (2-6)</i>	Establishes a session to the MWAM processor. For example, Sup-7606 session slot 7 processor 2 Note The default escape character is Ctrl-^ , then x. You can also type 'exit' at the remote prompt to end the session. Trying 127.0.0.72 ... Open
Step 3	mwam-6-4>	Press RETURN to get started.
Step 4	mwam-6-4> enable	
Step 5	mwam-6-4# configure terminal	Enters configuration mode. Enter configuration commands one per line. End with Ctrl/Z .
Step 6	Router (config)# memory-size iomem 64	This example allocates 64 MB of the DRAM memory to I/O memory and the remaining to processor memory.
Step 7	Router# copy system:running-config nvram:startup-config	The memory configuration will be saved to non volatile memory.
Step 8	Router# reload	

Clearing MWAM Session from Supervisor Console

To clear an MWAM session from the Supervisor console, complete the following steps:

	Command	Purpose
Step 1	Sup-7606# show tcp brief	Displays a concise description of TCP connection endpoints, including endpoints on the MWAM. Tip The command output displays the foreign address of the TCP connection between the processor control complex of the MWAM and the switch fabric interface. The address of this connection appears in the format 127.0.0.xy, where x is the MWAM slot number and y is the MWAM processor number. Correlate the foreign address to the TCB to perform the next step.
Step 2	Sup-7606# clear tcp tcb <i>tcb_addr</i>	Clears the Transmission Control Block (TCB) address of the TCP connection to the MWAM. The TCB address is an internal identifier for the endpoint.

This example shows how to clear an MWAM session on processor 2 of the MWAM in slot 7.

```
Sup-7606#show tcp brief
TCB      Local Address      Foreign Address      (state)
4345AC80  9.3.67.21.23       10.76.82.75.33713   ESTAB
509F0CD0  9.3.67.21.23       10.76.82.75.33777   ESTAB
43456D80  9.3.67.21.23       10.76.82.75.33712   ESTAB
43455A10  127.0.0.12.30211   127.0.0.72.23       ESTAB <<<< Connection to clear
4343BD18  9.3.67.21.23       9.3.66.4.11000      ESTAB
43449A0C  127.0.0.12.24068   127.0.0.71.23       ESTAB

Sup-7606#clear tcp tcb 43455A10

Sup-7606#
```

Recovering from MWAM Processor Lockout

Occasionally, you may discover that you are unable to log into an MWAM processor, either because of a configuration mistake or you have forgotten the password. On other Cisco routers the password recovery procedure involves setting the configuration register in ROMMON to ignore the startup-config. On MWAM processors you do not have access to the ROMMON. Instead, you issue the **recover-ios** command on the processor control complex. This forces the processor to ignore its configuration when it is reloaded.

To recover from the MWAM processor lockout condition, complete the following steps:

	Command	Purpose
Step 1	Sup-7606# session slot <i>slot_number processor 1</i>	Establishes a Telnet session to MWAM processor 1. Note User name is <i>root</i> and password is <i>cisco</i> .
Step 2	root@mwam-5# recover-ios <i>complex_number</i>	Sets the configuration register to boot with a clean configuration. Note The <i>complex_number</i> can be 0, 1, 2, or all .
Step 3	root@mwam-5# reload complex <i>complex_number</i>	Reloads the processor complex. Note If the reload complex command is not recognized, contact the Cisco TAC Escalation Center to complete the recovery procedure.
Step 4	root@mwam-5# normal-ios	Sets the configuration register to boot with a normal configuration to ensure that processors do not ignore their startup configurations.

The following example shows how to recover from the lockout condition on processor complex 0 of the MWAM in slot 5:

```
Sup-7600# session slot 5 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.51 ... Open

SVCWAM Image version 1.2(2.1-Eng)
Fri Oct 3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
```

```

Kernel 2.4.10.komodo on an i686
login: root
Password:

SVCMWAM Image version 1.2(2.1-Eng)
Fri Oct 3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.

root@mwam-5# recover-ios 0
processing -p
processing -c
Setting DHCP options for processor complex 0
Setting config-reg value to: 0x40
Base external MAC: "0005.9A3B.A180"
Internet Software Consortium DHCP Server V3.0.1rc6
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.
Listening on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Sending on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Listening on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on Socket/fallback/fallback-net

root@mwam-5# reload complex 0

root@mwam-5# normal-ios
Base external MAC: "0005.9A3B.A180"
Internet Software Consortium DHCP Server V3.0.1rc6
Copyright 1995-2001 Internet Software Consortium.
All rights reserved.
For info, please visit http://www.isc.org/products/DHCP
Wrote 0 deleted host decls to leases file.
Wrote 0 new dynamic host decls to leases file.
Wrote 0 leases to leases file.
Listening on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Sending on LPF/eth0/02:00:00:00:0f:00/128.0.1.0/24
Listening on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on LPF/eth1/02:00:00:00:0f:10/128.0.2.0/24
Sending on Socket/fallback/fallback-net

```

Recover from Session/Telnet Command after Reload

If the session between a Supervisor module and an MWAM processor fails to recover from a reload after 10 minutes, Cisco recommends that you perform the following steps to recover.

Configure **ip rcmd rcp-enable** on the Supervisor module. For Supervisor release SXF4 and later, also configure **ip rcmd remote-host <localuser> <MWAM EOBC address> <remoteuser> enable** on the Supervisor module for each MWAM processor. For the supervisor **config-mode** to work, this remote IP address has to be, not just any IP, but the EOBC address(127.0.0.xy, where x = slot, y = processor). For example, for MWAM slot 10 processor 2, configure **ip rcmd remote-host 127.0.0.102 enable**.

Recovering from Session Loss

If the session between a Supervisor module and an MWAM processor fails, Cisco recommends that you perform the following steps to attempt a recovery and collect information. The collected information can be useful in determining the cause of the session loss.

An example of an error message indicating loss of session is shown below:

```
MWAM: No response from IOS complex 1, resetting complex
MWAM: No response from IOS complex 0, resetting complex
```

To attempt recovery and collect troubleshooting information, complete the following steps:

	Command	Purpose
Step 1	After stopping traffic, do the following: Sup-7606> enable Sup-7606# session slot <i>slot_number</i> processor 1	Enters privileged EXEC mode and establishes a Telnet session to MWAM processor 1. Note User name is <i>root</i> and password is <i>cisco</i> .
Step 2	root@mwam-4# show processor <i>processor_number</i>	Displays information about the suspect MWAM processor.
Step 3	root@mwam-4# show tech-support	Displays information about the MWAM processors for technical support personnel.
Step 4	root@mwam-4# reload processor <i>processor_number</i>	Reloads the suspect MWAM processor.
Step 5	Sup-7606# session slot <i>slot_number</i> processor <i>processor_number (2-6)</i>	Establishes a session to the suspect MWAM processor.
Step 6	mwam-4-2> enable	Enters privileged EXEC mode of the MWAM processor.
Step 7	mwam-4-2# show version	Displays version information about the MWAM processor.
Step 8	mwam-4-2# show tech-support	Displays information about the MWAM processor for technical support personnel.
Step 9	mwam-4-2# dir bootflash:	Displays the bootflash directory of the MWAM processor.

The following example illustrates these steps:

```
Sup-7606# session slot 4 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.51 ... Open
```

```
SVCMWAM Image version 1.2(2.1-Eng)
Fri Oct 3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
Kernel 2.4.10.komodo on an i686
login: root
Password:
```

```
SVCMWAM Image version 1.2(2.1-Eng)
Fri Oct 3 05:32:39 EDT 2003
Copyright (c) 2002-2003 by cisco Systems, Inc.
All rights reserved.
```

```

root@mwam-4# show processor 2
Processor 2, Complex 1, Core 0
  Complex Status is Online
  Information
  Health Monitoring
    0 User Resets, 0 IOS Reloads, 0 Unknown Resets
    0 Timeouts
    0 Consecutive heartbeats missed
    108878/108878 Heartbeats acked since last reset
    0% CPU Utilization
  Messages
    1831/1831 VRTC Update(s) acked by PC
    108878/108878 Heartbeats(s) acked from IOS
    0/0 ROMMON Config Msg(s) acked from ROMMON
    0/0 Supervisor Switchover Msg(s) acked from IOS
    0/0 Prepare Reload Msg(s) acked from IOS

root@mwam-4# show tech-support
----- show version -----

SVCMWAM Image version 2.1(1.0)
Mon Feb 23 01:29:45 EST 2004
Copyright (c) 2002-2003, 2004 by cisco Systems, Inc.
All rights reserved.

~snipped~

root@mwam-4# reload processor 2
root@mwam-4#
Jun 16 01:55:22.575: %SVCLC-SP-5-STRRECVD: mod 4: <MWAM: Resetting complex 1 at
user request.>
~snipped~

Sup-7606# session slot 4 processor 2
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.64 ... Open

mwam-4-2#

Press RETURN to get started!

mwam-4-2> enable
mwam-4-2# show version
Cisco IOS Software, MWAM Software (MWAM-G4JS-M), Version 12.3(7)T1, RELEASE SOFT
WARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Thu 22-Apr-04 06:59 by eaarmas

ROM: System Bootstrap, Version 12.2(11)YS RELEASE SOFTWARE

Router uptime is 1 day, 6 hours, 47 minutes
System returned to ROM by power-on
System restarted at 16:06:07 IST Mon Jun 14 2004
Running default software

Cisco MWAM (MWAM) processor with 473088K/32768K bytes of memory.
SB-1 CPU at 700MHz, Implementation 1, Rev 0.2

Last reset from power-on
1 Gigabit Ethernet interface
511K bytes of non-volatile configuration memory.

```

```
Configuration register is 0x0
```

```
mwam-4-2# show tech-support
```

```
----- show version -----
```

```
~snipped~
```

```
mwam-4-2# dir bootflash:
```

```
Directory of bootflash:/
```

```
  0  -rw-          3107  Feb 25 2004 09:48:28 +05:30  running-config
```

```
524288 bytes total (520797 bytes free)
```

