Cisco Connected Grid Switch Software Configuration Guide for IOS Release 15.0(2)ED

First Published: May 2013
Last Updated: January 2015

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

No combinations are authorized or intended under this document.

CONTENTS

Overview

This document describes how to configure the software features in IOS release 15.0(2)ED for the Cisco 2520 Connected Grid Switch and and Ethernet Switch Module (ESM). Use this document in conjunction with additional software configuration documentation listed in the supported hardware table for each feature.

This chapter provides an overview of the following features in IOS release 15.0(2)ED:

- Switch Boot Optimization, page 1-1
- Dying Gasp, page 1-1
- Asymmetric VLAN Mapping, page 1-2
- VLAN Trunking Protocol, page 1-2
- Voice VLAN, page 1-2
- Smart Call Home, page 1-2

Switch Boot Optimization

Switch Boot Optimization disables memory test, file system check (FSCK), and power-on self-test (POST) to minimize switch boot time. This feature is disabled by default. When this feature is enabled and there is a system crash for some reason, the switch automatically disables the boot optimization feature and saves all the crash information in the first reload. Then the boot loader performs all necessary checks. The boot optimization is reenabled after the system comes up successfully.

Related Topics

Chapter 2, “Configuring Switch Boot Optimization”

Dying Gasp

The Dying Gasp feature enables the Cisco CGS 2520 to send dying gasp messages through SNMP, syslog, or Ethernet-OAM (Operations Administration and Maintenance) to report the abrupt loss of power to the host platform.

Related Topics

Chapter 3, “Configuring Dying Gasp”

Asymmetric VLAN Mapping

The asymmetric VLAN mapping feature for the Cisco CGS 2520 provides a method for restricting traffic on VLAN trunk ports. The feature lets you specify lists of VLANs that are allowed to forward traffic on the trunk port in the ingress direction, egress direction, or in both directions.

Related Topics

Chapter 4, "Configuring Asymmetric VLAN Mapping"

VLAN Trunking Protocol

VLAN Trunking Protocol (VTP) is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP on the Cisco CGS 2520 Switch and Cisco Connected Grid 10-port Ethernet Switch Module Interface Card (ESM) minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Related Topics

Chapter 5, "Configuring VLAN Trunking Protocol"

Voice VLAN

The Voice VLAN feature enables access ports on the switch to carry IP voice traffic from a Cisco IP phone. Voice VLAN supports users connecting to both a Cisco IP phone and another data device, such as a PC, through the IP phone to a switch port. The voice traffic and data traffic can be treated differently with voice traffic having higher priority.

Related Topics

Chapter 6, "Configuring Voice VLAN"

Smart Call Home

Smart Call Home provides a notification and alert system for critical system events. A range of message formats are available for compatibility with pager services, standard e-mail, or XML-based automated parsing applications.

Common uses can include direct paging of a network support engineer, e-mail notification to a network operations center, and XML delivery to a support website.

Related Topics

Chapter 7, "Configuring Smart Call Home"

CHAPTER 2

Configuring Switch Boot Optimization

This chapter describes how to configure the Switch Boot Optimization feature for Cisco Connected Grid switches.

This chapter includes the following sections:

- Supported Hardware, page 2-1
- Information About Switch Boot Optimization, page 2-1
- Configuring Switch Boot Optimization, page 2-2

Supported Hardware

Feature	Hardware	Minimum Software Release	Related Documentation
Switch Boot Optimization	Cisco CGS 2520 Switch	Cisco IOS Release 15.0(2)ED	Release Notes for Cisco IOS Release 15.0(2)ED
	Cisco Connected Grid Ethernet Switch Module (ESM)	Cisco IOS Release 15.0(2)ED	Cisco Connected Grid Ethernet Switch Module Interface Card Software Configuration Guide

Information About Switch Boot Optimization

The normal switch boot process involves a memory test, file system check (FSCK), and power-on self-test (POST).

The **boot fast** command in global configuration mode minimizes switch boot time by disabling these tests. By default, **boot fast** is disabled.

If the system crashes when **boot fast** is enabled, reload sequences occur immediately if your switch is set up to automatically bring up the system by using information in the BOOT environment variable. Otherwise, these reload sequences occur after you enter the manual boot command in bootloader configuration mode.

First Reload

The switch disables the boot fast feature and displays the following warning message:

```
“Saving the crash information to flash.
Reloading with boot fast feature disabled...”
```

After the system message appears, the system saves the crash information and automatically resets itself for the next reload cycle.

Second Reload

The boot loader performs its normal full memory test and FSCK check with LED status progress. If the memory and FSCK tests are successful, the system performs additional POST tests and the results are displayed on the console.

After the system comes up successfully, the fast boot feature is reenabled.

Configuring Switch Boot Optimization

Caution The memory test, filesystem check and POST are required for proper functioning of the system. Enabling switch boot optimization may lead to uncertain system behavior.

To enable the switch boot optimization feature, enter the following global configuration command:

boot fast

To disable the switch boot optimization feature, enter the following command:

no boot fast

Verifying Switch Boot Optimization Configuration

Command	Purpose
show boot	Display information about the switch boot optimization configuration

Boot Fast Output Example

The following is example output for boot fast on a CGS 2520.

```
Switch#conf t
Switch(config)#boot fast
Switch(config)#end
Switch#sh boot
Boot optimization   : enabled


Switch#conf t
Switch(config)#no boot fast
Switch(config)#end
Switch#sh boot
Boot optimization   : disabled
```

CHAPTER 3

Configuring Dying Gasp

This chapter describes the Dying-Gasp feature for the Supported Hardware, which enables the systems to send *dying gasp* messages through SNMP, syslog, or Ethernet-OAM (Operations Administration and Maintenance) to report the abrupt loss of power to the host platform.

This chapter includes the following sections:

Supported Hardware

Feature	Hardware	Minimum Software Release	Related Documentation
Dying Gasp	Cisco CGR 2010	Cisco IOS Release 15.2(3)T	Cisco Connected Grid Router Software Configuration Guide
	Cisco CGS 2520	Cisco IOS Release 15.0(2)ED	Release Notes for Cisco IOS Release 15.0(2)ED

Information About Dying Gasp

Dying Gasp resides on a hardware component on the High-performance WAN Interface Card (HWIC) and supports the Fast Ethernet and Gigabit Ethernet interfaces. The networking devices rely on a temporary back-up power supply on a capacitor, that allows for a graceful shutdown and the generation of the dying-gasp message. This temporary power supply is designed to last from 10 to 20 milliseconds to perform these tasks.

Dying-Gasp packets are created when you configure the host by using the **dying-gasp** configuration command. The **show dying-gasp packets** command displays the detailed information about the created packets.

The SNMP server for the SNMP Dying Gasp message is specified through the **snmp-server host** configuration command. The syslog server sending the syslog Dying Gasp message is specified through the **logging host hostname-or-ipaddress transport udp** command. The Ethernet-OAM Dying Gasp packets are created for interfaces where Ethernet-OAM is enabled.

Dying Gasp packets can be sent to a maximum number of 5 servers for each notification type.

Configuring Dying Gasp

To enable dying-gasp notification through syslog, SNMP trap, or Ethernet OAM, use the **dying-gasp** command:

Command Syntax	Description
dying-gasp primary {**syslog** | **snmp-trap** | **ethernet-oam**} **secondary** {**syslog** | **snmp-trap** | **ethernet-oam**}	• **dying-gasp**—Dying Gasp configuration command • **primary**—Dying Gasp primary notification • **secondary**—Dying Gasp secondary notification • **ethernet-oam**—Enable Ethernet OAM notification • **snmp-trap**—Enable trap notification sent to SNMP server • **syslog**—Enable system logger

Verifying Dying Gasp Configuration

The following are descriptions of the **show dying-gasp** command keywords:

Command Syntax	Description
show dying-gasp {**status** | **packets** [**snmp-trap** | **syslog** | **ethernet-oam**]}	• **dying-gasp**—Dying Gasp information • **status**—Dying Gasp configuration status • **packets**—Detailed information about the created packets • **snmp-trap**—Dying Gasp SNMP trap information • **syslog**—Dying Gasp Syslog message information • **ethernet-oam**—Dying Gasp Ethernet OAM message information

show dying-gasp Output Examples

The following is sample output for the **show dying-gasp status** command on a CGR 2010:

```
Router# show dying-gasp status
Dying Gasp Configuration
SNMP Trap Enabled
Syslog Enabled
Ethernet OAM Disabled
```

The following is sample output for the **show dying-gasp status** command on a CGS 2520:

```
Switch# show dying-gasp status
Dying Gasp Configuration
SNMP Trap Enabled (secondary)
Syslog Enabled (primary)
Ethernet OAM Disabled
Switch#
```

The following is sample output for the **show dying-gasp packets snmp-trap** command:

```
Router# show dying-gasp packets snmp-trap
SNMP Trap packet for server 3.1.1.2, link type IP
Interface, via GigabitEthernet0/0, local IP address 10.2.2.9
Encap type is ARPA, local hardware address 0022.bdd4.2f48
Next hop IP address 10.2.2.8, next hop hardware address 0000.0c07.ac09

SNMP Trap packet for server 3.1.1.4, link type IP
Interface, via GigabitEthernet0/1, local IP address 20.2.2.7
Encap type is ARPA, local hardware address 0012.001a.2f08
Next hop IP address 20.2.2.8, next hop hardware address 0cd0.0c02.ac10
```

debug dying-gasp

To turn on debugging for dying gasp, issue the **debug dying-gasp** command:

Command Syntax	Description
debug dying-gasp	**dying-gasp**—Dying Gasp debug information

Configuring Asymmetric VLAN Mapping

This chapter describes how to configure the asymmetric VLAN mapping feature for Cisco Connected Grid switches. This chapter includes the following sections:

Supported Hardware

Supported Hardware	Hardware Minimum Software Release	Related Documentation
Cisco CGS 2520 Switch	Cisco IOS Release 15.0(2)ED	Cisco 2500 Series Connected Grid Switches Configuration Guides

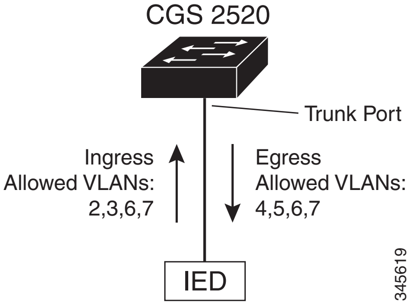
Information About Asymmetric VLAN Mapping

The asymmetric VLAN mapping feature for the Cisco CGS 2520 provides a method for restricting traffic on VLAN trunk ports. The feature lets you specify lists of VLANs that are allowed to forward traffic on the trunk port in the ingress direction, egress direction, or in both directions.

This feature is useful in a utility substation environment where a VLAN trunk is connected between a Cisco CGS 2520 switch and an intelligent electronic device (IED). The trunk port on the Cisco CGS 2520 can be configured to allow ingress traffic for a given VLAN, such as generic object oriented substation events (GOOSE) messages from the IED, and the trunk port can be configured to allow traffic for specific VLAN IDs in the egress direction, allowing the IED to subscribe to GOOSE messages with those VLAN IDs. All other VLAN traffic on the trunk port can be blocked.

In the example shown in Figure 4-1, there are six VLANs (2, 3, 4, 5, 6, 7) configured on a Cisco CGS 2520 switch. Using the asymmetric VLAN mapping feature on a trunk port, packets tagged with VLANs 2 and 3 can only enter the system through that interface, packets tagged with VLANs 4 and 5 can only go out of the system (but cannot enter the system), and packets tagged with VLANs 6 and 7 can both enter and exit the system. Any other tagged packets are dropped at the interface level where this feature is configured.

Figure 4-1 Asymmetric VLAN Mapping Between a Cisco CGS 2520 and an IED



Configuration Guidelines

These are the guidelines for configuring asymmetric VLAN mapping:

- The asymmetric VLAN mapping feature is applicable only to Layer 2 trunk ports that are in NNI mode.
- The asymmetric VLAN mapping feature should only be configured on interfaces facing IEDs.
- The feature operates at the VLAN level, so it is applicable to all of the tagged frames received on the interface where the feature is configured. For non-tagged frames, native VLAN functionality is applied.
- VLANs must already exist on the switch prior to being included in the allowed ingress, egress, or bidirectional VLAN lists.
- The maximum number of VLANs that can be included in the allowed ingress, egress, or bidirectional VLAN lists for all interfaces on the switch is 945.
- If the ternary content addressable memory (TCAM) table on the switch is full, then it is not possible to configure asymmetric VLAN mapping.

Interaction with Other Features

The asymmetric VLAN mapping feature is configured on interfaces facing IEDs, so all other Layer 2 control protocols, such as Spanning Tree BPDUs, CDP, and VTP packets should not be exchanged between the interface and an attached IED.

When the asymmetric VLAN mapping feature is enabled on an interface, CDP, STP, and VTP are disabled and cannot be configured on the interface until any configuration statements for asymmetric VLAN mapping are removed. In addition, the **no switchport** and **switchport mode access** configuration statements are not allowed when configuration statements for asymmetric VLAN mapping are present on the interface.

When the asymmetric VLAN mapping feature is configured for an interface, the VLAN mapping feature (VLAN ID translation) and the allowed VLAN feature cannot be configured for that interface.

Default Settings

Parameters	Default
Asymmetric VLAN mapping feature on VLAN trunk ports	Disabled

Configuring Asymmetric VLAN Mapping

Beginning in privileged EXEC mode, follow these steps to configure asymmetric VLAN mapping:

	Command	Purpose
Step 1	**show vlan**	Verify that the VLANs for which you are configuring mapping rules exist on the switch. If not, create the VLANs on the switch.
Step 2	**interface** *type slot/port*	Specify the interface to be configured as the trunk interface, and enter interface configuration mode. The *type* can be **fastethernet**, **gigabitethernet**, or **tengigabitethernet**.
Step 3	**port-type nni**	Configure the interface as an NNI. Asymmetric VLAN mapping is supported only on NNI ports.
Step 4	**switchport mode trunk**	Configure the port as a trunk port.
Step 5	**switchport trunk allowed asymmetric-vlan bidirectional** {**add** | **except** | **none** | **remove**} *vlan-list*	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in both the ingress and egress directions. The **add** keyword adds VLANs to the current list. The **except** keyword indicates all VLANs except those specified by *vlan-list*. The **none** keyword specifies none of the VLANs. The **remove** keyword removes VLANs from the current list. The *vlan-list* parameter is either a single VLAN number from 1 to 4094; a range of VLANs described by two VLAN numbers, the lower one first, separated by a hyphen; or a comma-separated list of VLANs. Do not enter any spaces between comma-separated VLANs or in hyphen-specified ranges.
Step 6	**switchport trunk allowed asymmetric-vlan ingress** {**add** | **except** | **none** | **remove**} *vlan-list*	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in the ingress direction; that is, from the IED to the switch. Traffic coming into the trunk port from all other VLANs is blocked. See step 5 for the description of the **add**, **except**, **none**, **remove**, and *vlan-list* parameters.

	Command	Purpose
Step 7	**switchport trunk allowed asymmetric-vlan egress** {**add** | **except** | **none** | **remove**} *vlan-list*	Specifies which of the VLANs configured on the switch are allowed to send traffic through the trunk port in the egress direction; that is, from the switch to the IED. Traffic from all other VLANs is blocked from exiting the trunk port. See step 5 for the description of the **add**, **except**, **none**, **remove**, and *vlan-list* parameters.
Step 8	**no vtp**	Disable VTP. VTP cannot be configured on the same interface where asymmetric VLAN mapping is configured.
Step 9	**no cdp enable**	Disable CDP. CDP cannot be configured on the same interface where asymmetric VLAN mapping is configured.
Step 10	**exit**	Return to global configuration mode.

The following example shows how to configure asymmetric VLAN mapping for a Fast Ethernet port connected to an IED. The switch has six VLANs configured on it. A trunk port is configured on the Fast Ethernet port. Traffic for VLANs 6 and 7 is allowed in both the ingress and egress direction on the trunk port; traffic for VLANs 2 and 3 is allowed from the IED to the switch; traffic for VLANs 4 and 5 is allowed from the switch to the IED. Traffic from any other VLANs is blocked at the port.

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type nni
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed asymmetric-vlan bidirectional 6,7
Switch(config-if)# switchport trunk allowed asymmetric-vlan ingress 2,3
Switch(config-if)# switchport trunk allowed asymmetric-vlan egress 4,5
Switch(config-if)# no vtp
Switch(config-if)# no cdp enable
Switch(config-if)# exit
```

Verifying Asymmetric VLAN Mapping Configuration

Command	Purpose
show vlan asymmetric	Display the asymmetric VLAN mapping configuration in summary

CHAPTER 5

Configuring VLAN Trunking Protocol

This chapter describes how to use the VLAN Trunking Protocol (VTP) and the VLAN database for managing VLANs with the Cisco CGS 2520 Switch and Cisco Connected Grid 10-port Ethernet Switch Module Interface Card (ESM).

For complete syntax and usage information for the commands used in this chapter, see the command reference listed in Supported Hardware.

The chapter consists of these sections:

Supported Hardware

Supported Hardware	Hardware Minimum Software Release	Related Documentation
Cisco CGS 2520 Switch	Cisco IOS Release 15.0(2)ED	Cisco 2500 Series Connected Grid Switches Configuration Guides
		CGS 2520 Switch Software Configuration Guide, 12.2(53)EX (Configuring VLANS)
		Catalyst 3750 Switch Command Reference, Cisco IOS Release 15.0(2)SE and Later
Cisco Connected Grid 10-port Ethernet Switch Module Interface Card (ESM)	Cisco IOS Release 15.0(2)ED	Connected Grid Ethernet Switch Module Interface Card Getting Started Guide

Information About VTP

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes misconfigurations and configuration inconsistencies that can cause several problems, such as duplicate VLAN names, incorrect VLAN-type specifications, and security violations.

Before you create VLANs, you must decide whether to use VTP in your network. Using VTP, you can make configuration changes centrally on one or more switches (CGS 2520 or ESM) and have those changes automatically communicated to all the other switches in the network. Without VTP, you cannot send information about VLANs to other switches.

VTP is designed to work in an environment where updates are made on a single switch and are sent through VTP to other switches in the domain. It does not work well in a situation where multiple updates to the VLAN database occur simultaneously on switches in the same domain, which would result in an inconsistency in the VLAN database.

The switch supports VLANs, but the number of configured features affects the usage of the switch hardware. If the switch is notified by VTP of a new VLAN and the switch is already using the maximum available hardware resources, it sends a message that there are not enough hardware resources available and shuts down the VLAN. The output of the **show vlan** user EXEC command shows the VLAN in a suspended state.

VTP version 1 and version 2 support only normal-range VLANs (VLAN IDs 1 to 1005). Cisco IOS Release 12.2(52)SE and later support VTP version 3. VTP version 3 supports the entire VLAN range (VLANs 1 to 4094). Extended range VLANs (VLANs 1006 to 4094) are supported only in VTP version 3. You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured in the domain.

These sections contain this conceptual information:

- VTP Domain, page 5-2
- VTP Modes, page 5-3
- VTP Advertisements, page 5-4
- VTP Version 2, page 5-5
- VTP Version 3, page 5-5
- VTP Pruning, page 5-6

VTP Domain

A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.

By default, the switch is in the VTP no-management-domain state until it receives an advertisement for a domain over a trunk link (a link that carries the traffic of multiple VLANs) or until you configure a domain name. Until the management domain name is specified or learned, you cannot create or modify VLANs on a VTP server, and VLAN information is not propagated over the network.

If the switch receives a VTP advertisement over a trunk link, it inherits the management domain name and the VTP configuration revision number. The switch then ignores advertisements with a different domain name or an earlier configuration revision number.

Caution Before adding a VTP client switch to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. If you add a switch that has a revision number higher than the revision number in the VTP domain, it can erase all VLAN information from the VTP server and VTP domain. Refer to Adding a VTP Client Switch to a VTP Domain, page 5-17 for the procedure for verifying and resetting the VTP configuration revision number.

When you make a change to the VLAN configuration on a VTP server, the change is propagated to all switches in the VTP domain. VTP advertisements are sent over all IEEE trunk connections, including IEEE 802.1Q. VTP dynamically maps VLANs with unique names and internal index associates across multiple LAN types. Mapping eliminates excessive device administration required from network administrators.

If you configure a switch for VTP transparent mode, you can create and modify VLANs, but the changes are not sent to other switches in the domain, and they affect only the individual switch. However, configuration changes made when the switch is in this mode are saved in the switch running configuration and can be saved to the switch startup configuration file.

For domain name and password configuration guidelines, see VTP Configuration Guidelines, page 5-8.

VTP Modes

You can configure a supported switch to be in one of the VTP modes listed in Table 5-1.

Table 5-1 VTP Modes

VTP Mode	Description
VTP server	In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links. VTP server is the default mode. **Note** In VTP server mode, VLAN configurations are saved in NVRAM. If the switch detects a failure while writing a configuration to NVRAM, VTP mode automatically changes from server mode to client mode. If this happens, the switch cannot be returned to VTP server mode until the NVRAM is functioning.
VTP client	A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode. In VTP versions 1 and 2, in VTP client mode, VLAN configurations are not saved in NVRAM. In VTP version 3, VLAN configurations are saved in NVRAM in client mode.

Table 5-1 VTP Modes (continued)

VTP Mode	Description
VTP transparent	VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode. In VTP versions 1 and 2, the switch must be in VTP transparent mode when you create extended-range VLANs. VTP version 3 also supports creating extended-range VLANs in client or server mode. Refer to the Extended-Range VLANs section within the "Configuring VLANs" chapter of the *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX.* When the switch is in VTP transparent mode, the VTP and VLAN configurations are saved in NVRAM, but they are not advertised to other switches. In this mode, VTP mode and domain name are saved in the switch running configuration, and you can save this information in the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command.
VTP off	A switch in VTP off mode functions in the same manner as a VTP transparent switch, except that it does not forward VTP advertisements on trunks.

VTP Advertisements

Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.

Because trunk ports send and receive VTP advertisements, you must ensure that at least one trunk port is configured on the switch and that this trunk port is connected to the trunk port of another switch. Otherwise, the switch cannot receive any VTP advertisements. For more information on trunk ports, see the Configuring VLAN Trunks section of the "Configuring VLANs" chapter of the *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX.*

VTP advertisements distribute this global domain information:

- VTP domain name
- VTP configuration revision number
- Update identity and update timestamp
- MD5 digest VLAN configuration, including maximum transmission unit (MTU) size for each VLAN.
- Frame format

VTP advertisements distribute this VLAN information for each configured VLAN:

- VLAN IDs (IEEE 802.1Q)
- VLAN name
- VLAN type
- VLAN state
- Additional VLAN configuration information specific to the VLAN type

In VTP version 3, VTP advertisements also include the primary server ID, an instance number, and a start index.

VTP Version 2

If you use VTP in your network, you must decide which version of VTP to use. By default, VTP operates in version 1.

VTP version 2 supports these features that are not supported in version 1:

- Token Ring support—VTP version 2 supports Token Ring Bridge Relay Function (TrBRF) and Token Ring Concentrator Relay Function (TrCRF) VLANs. For more information about Token Ring VLANs, see the Normal-Range VLANs section within the “Configuring VLANs” chapter of the *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX*.
- Unrecognized Type-Length-Value (TLV) support—A VTP server or client propagates configuration changes to its other trunks, even for TLVs it is not able to parse. The unrecognized TLV is saved in NVRAM when the switch is operating in VTP server mode.
- Version-Dependent Transparent Mode—In VTP version 1, a VTP transparent switch inspects VTP messages for the domain name and version and forwards a message only if the version and domain name match. Because VTP version 2 supports only one domain, it forwards VTP messages in transparent mode without inspecting the version and domain name.
- Consistency Checks—In VTP version 2, VLAN consistency checks (such as VLAN names and values) are performed only when you enter new information through the CLI or SNMP. Consistency checks are not performed when new information is obtained from a VTP message or when information is read from NVRAM. If the MD5 digest on a received VTP message is correct, its information is accepted.

VTP Version 3

VTP version 3 supports these features that are not supported in version 1 or version 2:

- Enhanced authentication—You can configure the authentication as **hidden** or **secret**. When **hidden**, the secret key from the password string is saved in the VLAN database file, but it does not appear in plain text in the configuration. Instead, the key associated with the password is saved in hexadecimal format in the running configuration. You must reenter the password if you enter a takeover command in the domain. When you enter the **secret** keyword, you can directly configure the password secret key.
- Support for extended range VLAN (VLANs 1006 to 4094) database propagation. VTP versions 1 and 2 propagate only VLANs 1 to 1005. If extended VLANs are configured, you cannot convert from VTP version 3 to version 1 or 2.

  Note VTP pruning still applies only to VLANs 1 to 1005, and VLANs 1002 to 1005 are still reserved and cannot be modified.

- Private VLAN support.
- Support for any database in a domain. In addition to propagating VTP information, version 3 can propagate Multiple Spanning Tree (MST) protocol database information. A separate instance of the VTP protocol runs for each application that uses VTP.
- VTP primary server and VTP secondary servers. A VTP primary server updates the database information and sends updates that are honored by all devices in the system. A VTP secondary server can only back up the updated VTP configurations received from the primary server to its NVRAM.

By default, all devices come up as secondary servers. You can enter the **vtp primary** privileged EXEC command to specify a primary server. Primary server status is only needed for database updates when the administrator issues a takeover message in the domain. You can have a working VTP domain without any primary servers. Primary server status is lost if the device reloads or domain parameters change, even when a password is configured on the switch.

- The option to turn VTP on or off on a per-trunk (per-port) basis. You can enable or disable VTP per port by entering the [**no**] **vtp** interface configuration command. When you disable VTP on trunking ports, all VTP instances for that port are disabled. You cannot set VTP to *off* for the MST database and *on* for the VLAN database on the same port.

  When you globally set VTP mode to off, it applies to all the trunking ports in the system. However, you can specify on or off on a per-VTP instance basis. For example, you can configure the switch as a VTP server for the VLAN database but with VTP *off* for the MST database.

VTP Pruning

VTP pruning increases network available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to reach the destination devices. Without VTP pruning, a switch floods broadcast, multicast, and unknown unicast traffic across all trunk links within a VTP domain even though receiving switches might discard them. VTP pruning is disabled by default.

VTP pruning blocks unneeded flooded traffic to VLANs on trunk ports that are included in the pruning-eligible list. Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning eligible switch trunk ports. If the VLANs are configured as pruning-ineligible, the flooding continues. VTP pruning is supported in all VTP versions.

Figure 5-1 shows a switched network without VTP pruning enabled. Port 1 on Switch A and Port 2 on Switch D are assigned to the Red VLAN. If a broadcast is sent from the host connected to Switch A, Switch A floods the broadcast and every switch in the network receives it, even though Switches C, E, and F have no ports in the Red VLAN.

Figure 5-1 Flooding Traffic without VTP Pruning

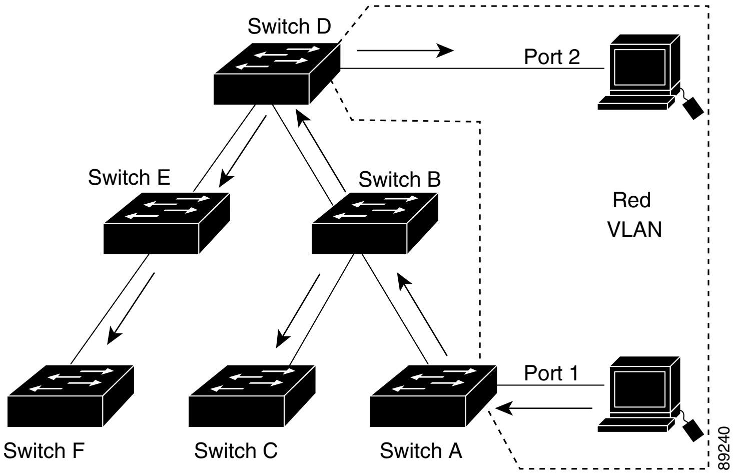
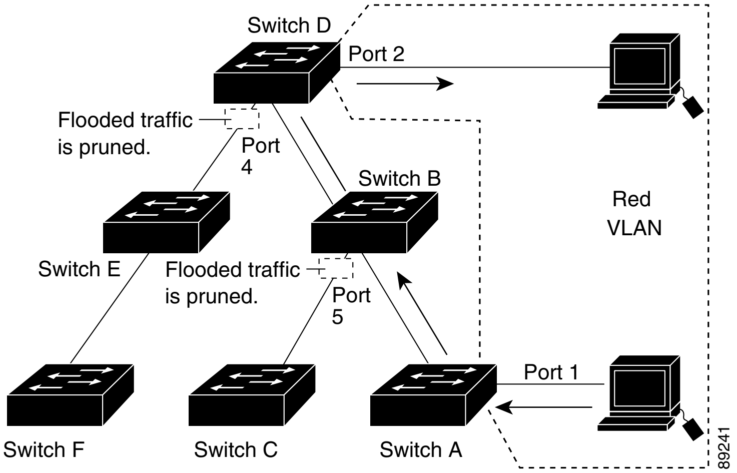


Figure 5-2 shows a switched network with VTP pruning enabled. The broadcast traffic from Switch A is not forwarded to Switches C, E, and F because traffic for the Red VLAN has been pruned on the links shown (Port 5 on Switch B and Port 4 on Switch D).

Figure 5-2 Optimized Flooded Traffic with VTP Pruning



Enabling VTP pruning on a VTP server enables pruning for the entire management domain. Making VLANs pruning-eligible or pruning-ineligible affects pruning eligibility for those VLANs on that trunk only (not on all switches in the VTP domain). (See Enabling VTP Pruning, page 5-15.)

VTP pruning takes effect several seconds after you enable it. VTP pruning does not prune traffic from VLANs that are pruning-ineligible. VLAN 1 and VLANs 1002 to 1005 are always pruning-ineligible; traffic from these VLANs cannot be pruned. Extended-range VLANs (VLAN IDs higher than 1005) are also pruning-ineligible.

VTP pruning is not designed to function in VTP transparent mode. If one or more switches in the network are in VTP transparent mode, you should do one of these:

- Turn off VTP pruning in the entire network.
- Turn off VTP pruning by making all VLANs on the trunk of the switch upstream to the VTP transparent switch pruning ineligible.

To configure VTP pruning on an interface, use the **switchport trunk pruning vlan** interface configuration command, refer to Changing the Pruning-Eligible List, page 5-15. VTP pruning operates when an interface is trunking. You can set VLAN pruning-eligibility, whether or not VTP pruning is enabled for the VTP domain, whether or not any given VLAN exists, and whether or not the interface is currently trunking.

Configuring VTP

This section contains the following configuration information:

Default Settings

Feature	Default Setting
VTP domain name	Null.
VTP mode (VTP version 1 and version 2)	Server.
VTP mode (VTP version 3)	The mode is the same as the mode in VTP version 1 or 2 before conversion to version 3.
VTP version	Version 1.
MST database mode	Transparent.
VTP version 3 server type	Secondary.
VTP password	None.
VTP pruning	Disabled.

VTP Configuration Guidelines

You use the **vtp** global configuration command to set the VTP password, the version, the VTP file name, the interface providing updated VTP information, the domain name, and the mode, and to disable or enable pruning. For more information about available keywords, see the command descriptions in the command reference for this release listed in Supported Hardware. The VTP information is saved in the VTP VLAN database. When VTP mode is transparent, the VTP domain name and mode are also saved in the switch running configuration file, and you can save it in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command. You must use this command if you want to save VTP mode as transparent if the switch resets.

When you save VTP information in the switch startup configuration file and restart the switch, the configuration is selected as follows:

- If the VTP mode is transparent in both the startup configuration and the VLAN database and the VTP domain name from the VLAN database matches that in the startup configuration file, the VLAN database is ignored (cleared). The VTP and VLAN configurations in the startup configuration file are used. The VLAN database revision number remains unchanged in the VLAN database.

- If the VTP mode or the domain name in the startup configuration does not match the VLAN database, the domain name and the VTP mode and configuration for the first 255 VLANs use the VLAN database information.

Domain Names

When configuring VTP for the first time, you must always assign a domain name. You must configure all switches in the VTP domain with the same domain name. Switches in VTP transparent mode do not exchange VTP messages with other switches, and you do not need to configure a VTP domain name for them.

Note If NVRAM and DRAM storage is sufficient, all switches in a VTP domain should be in VTP server mode.

Caution Do not configure a VTP domain if all switches are operating in VTP client mode. If you configure the domain, it is impossible to make changes to the VLAN configuration of that domain. Make sure that you configure at least one switch in the VTP domain for VTP server mode.

Passwords

You can configure a password for the VTP domain, but it is not required. If you do configure a domain password, all domain switches must share the same password and you must configure the password on each switch in the management domain. Switches without a password or with the wrong password reject VTP advertisements.

If you configure a VTP password for a domain, a switch that is booted without a VTP configuration does not accept VTP advertisements until you configure it with the correct password. After the configuration, the switch accepts the next VTP advertisement that uses the same password and domain name in the advertisement.

If you are adding a new switch to an existing network with VTP capability, the new switch learns the domain name only after the applicable password has been configured on it.

Caution When you configure a VTP domain password, the management domain does not function properly if you do not assign a management domain password to each switch in the domain.

VTP Version

Follow these guidelines when deciding which VTP version to implement:

- All switches in a VTP domain must have the same domain name, but they do not need to run the same VTP version.
- A VTP version 2-capable switch can operate in the same VTP domain as a switch running VTP version 1 if version 2 is disabled on the version 2-capable switch (version 2 is disabled by default).
- If a switch running VTP version 1 but capable of running VTP version 2 receives VTP version 3 advertisements, it automatically moves to VTP version 2.

- If a switch running VTP version 3 is connected to a switch running VTP version 1, the VTP version 1 switch moves to VTP version 2, and the VTP version 3 switch sends scaled-down versions of the VTP packets so that the VTP version 2 switch can update its database.
- A switch running VTP version 3 cannot move to version 1 or 2 if it has extended VLANs.
- Do not enable VTP version 2 on a switch unless all of the switches in the same VTP domain are version-2-capable. When you enable version 2 on a switch, all of the version-2-capable switches in the domain enable version 2. If there is a version 1-only switch, it does not exchange VTP information with switches that have version 2 enabled.
- We recommend placing VTP version 1 and 2 switches at the edge of the network because they do not forward VTP version 3 advertisements.
- If there are TrBRF and TrCRF Token Ring networks in your environment, you must enable VTP version 2 or version 3 for Token Ring VLAN switching to function properly. To run Token Ring and Token Ring-Net, disable VTP version 2.
- VTP version 1 and version 2 do not propagate configuration information for extended-range VLANs (VLANs 1006 to 4094). You must configure these VLANs manually on each device. VTP version 3 supports extended-range VLANs. You cannot convert from VTP version 3 to VTP version 2 if extended VLANs are configured.
- When a VTP version 3 device trunk port receives messages from a VTP version 2 device, it sends a scaled-down version of the VLAN database on that particular trunk in VTP version 2 format. A VTP version 3 device does not send VTP version 2-formatted packets on a trunk unless it first receives VTP version 2 packets on that trunk port.
- When a VTP version 3 device detects a VTP version 2 device on a trunk port, it continues to send VTP version 3 packets, in addition to VTP version 2 packets, to allow both kinds of neighbors to coexist on the same trunk.
- A VTP version 3 device does not accept configuration information from a VTP version 2 or version 1 device.
- Two VTP version 3 regions can only communicate in transparent mode over a VTP version 1 or version 2 region.
- Devices that are only VTP version 1 capable cannot interoperate with VTP version 3 devices.

Configuration Requirements

When you configure VTP, you must configure a trunk port so that the switch can send and receive VTP advertisements to and from other switches in the domain.

For more information, see the Configuring VLAN Trunks section in the “Configuring VLANS” chapter of the *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX.*

If you are configuring VTP on a cluster member switch to a VLAN, use the **rcommand** privileged EXEC command to log in to the member switch. For more information about the command, see the command reference for this release listed in Supported Hardware.

In VTP versions 1 and 2, when you configure extended-range VLANs on the switch, the switch must be in VTP transparent mode. VTP version 3 also supports creating extended-range VLANs in client or server mode.

Configuring VTP Mode

You can configure VTP mode as one of these:

- When a switch is in VTP server mode, you can change the VLAN configuration and have it propagated throughout the network.
- When a switch is in VTP client mode, you cannot change its VLAN configuration. The client switch receives VTP updates from a VTP server in the VTP domain and then modifies its configuration accordingly.
- When you configure the switch for VTP transparent mode, VTP is disabled on the switch. The switch does not send VTP updates and does not act on VTP updates received from other switches. However, a VTP transparent switch running VTP version 2 does forward received VTP advertisements on its trunk links.
- VTP off mode is the same as VTP transparent mode except that VTP advertisements are not forwarded.

Follow these guidelines:

- For VTP version 1 and version 2, if extended-range VLANs are configured on the switch, you cannot change VTP mode to client or server. You receive an error message, and the configuration is not allowed. VTP version 1 and version 2 do not propagate configuration information for extended range VLANs (VLANs 1006 to 4094). You must manually configure these VLANs on each device.

Note For VTP version 1 and 2, before you create extended-range VLANs (VLAN IDs 1006 to 4094), you must set VTP mode to transparent by using the **vtp mode transparent** global configuration command. Save this configuration to the startup configuration so that the switch starts in VTP transparent mode. Otherwise, you lose the extended-range VLAN configuration if the switch resets and boots up in VTP server mode (the default).

- VTP version 3 supports extended-range VLANs. If extended VLANs are configured, you cannot convert from VTP version 3 to VTP version 2.
- If you configure the switch for VTP client mode, the switch does not create the VLAN database file (vlan.dat). If the switch is then powered off, it resets the VTP configuration to the default. To keep the VTP configuration with VTP client mode after the switch restarts, you must first configure the VTP domain name before the VTP mode.

Caution If all switches are operating in VTP client mode, do not configure a VTP domain name. If you do, it is impossible to make changes to the VLAN configuration of that domain. Therefore, make sure you configure at least one switch as a VTP server.

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

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp domain** *domain-name*	Configure the VTP administrative-domain name. The name can be 1 to 32 characters. All switches operating in VTP server or client mode under the same administrative responsibility must be configured with the same domain name. This command is optional for modes other than server mode. VTP server mode requires a domain name. If the switch has a trunk connection to a VTP domain, the switch learns the domain name from the VTP server in the domain. You should configure the VTP domain before configuring other VTP parameters.
Step 3	**vtp mode** {**client** | **server** | **transparent** | **off**} {**vlan** | **mst** | **unknown**}	Configure the switch for VTP mode (client, server, transparent or off). (Optional) Configure the database: • **vlan**—the VLAN database is the default if none are configured. • **mst**—the multiple spanning tree (MST) database. • **unknown**—an unknown database type.
Step 4	**vtp password** *password*	(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters. If you configure a VTP password, the VTP domain does not function properly if you do not assign the same password to each switch in the domain. See Configuring a VTP Version 3 Password, page 5-13 for options available with VTP version 3.
Step 5	**end**	Return to privileged EXEC mode.
Step 6	**show vtp status**	Verify your entries in the *VTP Operating Mode* and the *VTP Domain Name* fields of the display.
Step 7	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file. **Note** Only VTP mode and domain name are saved in the switch running configuration and can be copied to the startup configuration file.

When you configure a domain name, it cannot be removed; you can only reassign a switch to a different domain.

To return a switch in another mode to VTP server mode, use the **no vtp mode** global configuration command. To return the switch to a no-password state, use the **no vtp password** global configuration command.

This example shows how to configure the switch as a VTP server with the domain name *eng_group* and the password *mypassword*:

```
Switch(config)# vtp domain eng_group
Setting VTP domain name to eng_group.
Switch(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
Switch(config)# vtp password mypassword
Setting device VLAN database password to mypassword.
Switch(config)# end
```

Configuring a VTP Version 3 Password

Beginning in privileged EXEC mode, follow these steps to configure the password when using VTP version 3:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp password** *password* [**hidden** | **secret**]	(Optional) Set the password for the VTP domain. The password can be 8 to 64 characters. • (Optional) **hidden**—Enter **hidden** to ensure that the secret key generated from the password string is saved in the nvam:vlan.dat file. If you configure a takeover by configuring a VTP primary server, you are prompted to reenter the password. • (Optional) **secret**—Enter **secret** to directly configure the password. The secret password must contain 32 hexadecimal characters.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp password**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file.

To clear the password, enter the **no vtp password** global configuration command.

This example shows how to configure a hidden password and how it appears.

```
Switch(config)# vtp password mypassword hidden
Generating the secret associated to the password.
Switch(config)# end
Switch# show vtp password
VTP password: 89914640C8D90868B6A0D8103847A733
```

Configuring a VTP Version 3 Primary Server

Beginning in privileged EXEC mode, follow these steps on a VTP server to configure it as a VTP primary server (version 3 only), which starts a takeover operation:

	Command	Purpose
Step 1	**vtp primary-server** [**vlan** | **mst**] [**force**]	Change the operational state of a switch from a secondary server (the default) to a primary server and advertise the configuration to the domain. If the switch password is configured as **hidden**, you are prompted to reenter the password. • (Optional) **vlan**—Select the VLAN database as the takeover feature. This is the default. • (Optional) **mst**—Select the multiple spanning tree (MST) database as the takeover feature. • (Optional) **force**—Entering **force** overwrites the configuration of any conflicting servers. If you do not enter **force**, you are prompted for confirmation before the takeover.

This example shows how to configure a switch as the primary server for the VLAN database (the default) when a hidden or secret password was configured:

```
Switch# vtp primary vlan
Enter VTP password: mypassword
This switch is becoming Primary server for vlan feature in the VTP  domain

VTP Database Conf Switch ID      Primary Server Revision System Name
------------ ---- -------------- -------------- -------- --------------------
VLANDB       Yes  00d0.00b8.1400=00d0.00b8.1400 1        stp7

Do you want to continue (y/n) [n]? y
```

Enabling the VTP Version

VTP version 2 and version 3 are disabled by default.

- When you enable VTP version 2 on a switch, every VTP version 2-capable switch in the VTP domain enables version 2. To enable VTP version 3, you must manually configure it on each switch.
- With VTP versions 1 and 2, you can configure the version only on switches in VTP server or transparent mode. If a switch is running VTP version 3, you can change to version 2 when the switch is in client mode if no extended VLANs exist, no private VLANs exist, and no hidden password was configured.

Caution VTP version 1 and VTP version 2 are not interoperable on switches in the same VTP domain. Do not enable VTP version 2 unless every switch in the VTP domain supports version 2.

- In TrCRF and TrBRF Token ring environments, you must enable VTP version 2 or VTP version 3 for Token Ring VLAN switching to function properly. For Token Ring and Token Ring-Net media, disable VTP version 2 must be disabled.
- VTP version 3 is supported on switches running Cisco IOS Release 12.2(52) SE or later.

Caution In VTP version 3, both the primary and secondary servers can exist on an instance in the domain.

For more information on VTP version configuration guidelines, see VTP Version, page 5-9.

Beginning in privileged EXEC mode, follow these steps to configure the VTP version:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp version** {**1** | **2** | **3**}	Enable the VTP version on the switch. The default is VTP version 1.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp status**	Verify that the configured VTP version is enabled.
Step 5	**copy running-config startup-config**	(Optional) Save the configuration in the startup configuration file.

To return to the default VTP version 1, use the **no vtp version** global configuration command**.**

Enabling VTP Pruning

Pruning increases available bandwidth by restricting flooded traffic to those trunk links that the traffic must use to access the destination devices. You can only enable VTP pruning on a switch in VTP server mode.

Beginning in privileged EXEC mode, follow these steps to enable VTP pruning in the VTP domain:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**vtp pruning**	Enable pruning in the VTP administrative domain. By default, pruning is disabled. You need to enable pruning on only one switch in VTP server mode.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show vtp status**	Verify your entries in the *VTP Pruning Mode* field of the display.

To disable VTP pruning, use the **no vtp pruning** global configuration command.

With VTP versions 1 and 2, when you enable pruning on the VTP server, it is enabled for the entire VTP domain. In VTP version 3, you must manually enable pruning on each switch in the domain.

Only VLANs included in the pruning-eligible list can be pruned. By default, VLANs 2 through 1001 are pruning-eligible on trunk ports. Reserved VLANs and extended-range VLANs cannot be pruned. To change the pruning-eligible VLANs, see Changing the Pruning-Eligible List.

Changing the Pruning-Eligible List

The pruning-eligible list applies only to trunk ports. Each trunk port has its own eligibility list. VTP pruning must be enabled for this procedure to take effect.

Beginning in privileged EXEC mode, follow these steps to remove VLANs from the pruning-eligible list on a trunk port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Identify an interface, and enter interface configuration mode.

	Command	Purpose
Step 3	**switchport trunk pruning vlan** {**add** | **except** | **none** | **remove**} *vlan-list* [,*vlan*[,*vlan*[,,,]]	Configure the list of VLANs allowed to be pruned from the trunk. (See Enabling VTP Pruning.) **add**—Adds the defined list of VLANs to those currently set, instead of replacing the list. **except**—Lists the VLANs that should be calculated by inverting the defined list of VLANs. **none**—Indicates an empty list. **remove**—Removes the defined list of VLANs from those currently set instead of replacing the list. *vlan-list*—Is either a single VLAN number from 1 to 1005 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen that represents the VLAN IDs of the allowed VLANs when this port is in trunking mode. For explanations about using the add, except, none, and remove keywords, refer to the command reference for this release listed in Supported Hardware. Separate nonconsecutive VLAN IDs with a comma and no spaces; use a hyphen to designate a range of IDs. Valid IDs are from 2 to 1001. VLANs that are pruning-ineligible receive flooded traffic. The default list of VLANs allowed to be pruned contains VLANs 2 to 1001. **Note** To return to the default pruning-eligible list of all VLANs, use the **no switchport trunk pruning vlan** interface configuration command.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries in the *Pruning VLANs Enabled* field of the command display.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring VTP on a Per-Port Basis

With VTP version 3, you can enable or disable VTP on a per-port basis. You can enable VTP only on ports that are in trunk mode. Incoming and outgoing VTP traffic are blocked, not forwarded.

Beginning in privileged EXEC mode, follow these steps to enable VTP on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Identify an interface, and enter interface configuration mode.
Step 3	**vtp**	Enable VTP on the specified port.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show running-config interface** *interface-id*	Verify the change to the port.
Step 6	**show vtp status**	Verify the configuration.

To disable VTP on the interface, use the **no vtp** interface configuration command.

```
Switch(config-if)# vtp
Switch(config-if)# end
```

Adding a VTP Client Switch to a VTP Domain

Before adding a VTP client to a VTP domain, always verify that its VTP configuration revision number is *lower* than the configuration revision number of the other switches in the VTP domain. Switches in a VTP domain always use the VLAN configuration of the switch with the highest VTP configuration revision number. With VTP versions 1 and 2, adding a switch that has a revision number higher than the revision number in the VTP domain can erase all VLAN information from the VTP server and VTP domain. With VTP version 3, the VLAN information is not erased.

Beginning in privileged EXEC mode, follow these steps to verify and reset the VTP configuration revision number on a switch *before* adding it to a VTP domain:

	Command	Purpose
Step 1	**show vtp status**	Check the VTP configuration revision number. If the number is 0, add the switch to the VTP domain. If the number is greater than 0, follow these steps: **a.** Write down the domain name. **b.** Write down the configuration revision number. **c.** Continue with the next steps to reset the switch configuration revision number.
Step 2	**configure terminal**	Enter global configuration mode.
Step 3	**vtp domain** *domain-name*	Change the domain name from the original one displayed in Step 1 to a new name.
Step 4	**end**	The VLAN information on the switch is updated and the configuration revision number is reset to 0. You return to privileged EXEC mode.
Step 5	**show vtp status**	Verify that the configuration revision number has been reset to 0.
Step 6	**configure terminal**	Enter global configuration mode.
Step 7	**vtp domain** *domain-name*	Enter the original domain name on the switch.
Step 8	**end**	The VLAN information on the switch is updated, and you return to privileged EXEC mode.
Step 9	**show vtp status**	(Optional) Verify that the domain name is the same as in Step 1 and that the configuration revision number is 0.

After resetting the configuration revision number, add the switch to the VTP domain.

Note You can use the **vtp mode transparent** global configuration command to disable VTP on the switch and then to change its VLAN information without affecting the other switches in the VTP domain.

Verifying VTP Configuration

To view VTP configuration information, enter any or all of the following commands.

Command	Purpose
show vtp counters	Display counters about VTP messages that have been sent and received.
show vtp devices [**conflict**]	Display information about all VTP version 3 devices in the domain. Conflicts are VTP version 3 devices with conflicting primary servers. The **show vtp devices** command does not display information when the switch is in transparent or off mode.
show vtp interface [*interface-id*]	Display VTP status and configuration for all interfaces or the specified interface.
show vtp password	Display the VTP password. The form of the password displayed depends on whether or not the **hidden** keyword was entered and if encryption is enabled on the switch.
show vtp status	Display the VTP switch configuration information.

CHAPTER 6

Configuring Voice VLAN

This chapter describes how to configure Voice VLAN on the Cisco 2520 Connected Grid Switch (CGS 2520) and the Cisco Connected Grid 10-port Ethernet Switch Module Interface (ESM).

Voice VLAN is referred to as an *auxiliary VLAN* in some Catalyst 6500 family switch documentation.

Note For complete syntax and usage information for the commands used in this chapter, see the command reference for 15.0(2)SE listed in Supported Hardware.

This chapter consists of these sections:

Supported Hardware

Supported Hardware	Hardware Minimum Software Release	Related Documentation
Cisco CGS 2520 Switch	Cisco IOS Release 15.0(2)ED	Cisco 2500 Series Connected Grid Switches Configuration Guides
		CGS 2520 Switch Software Configuration Guide, 12.2(53)EX (Configuring VLANS)
		Catalyst 3750 Switch Command Reference, Cisco IOS Release 15.0(2)SE and Later
Cisco Connected Grid Ethernet Switch Module (ESM)	Cisco IOS Release 15.0(2)ED	Connected Grid Ethernet Switch Module Interface Card Getting Started Guide

Information About Voice VLAN

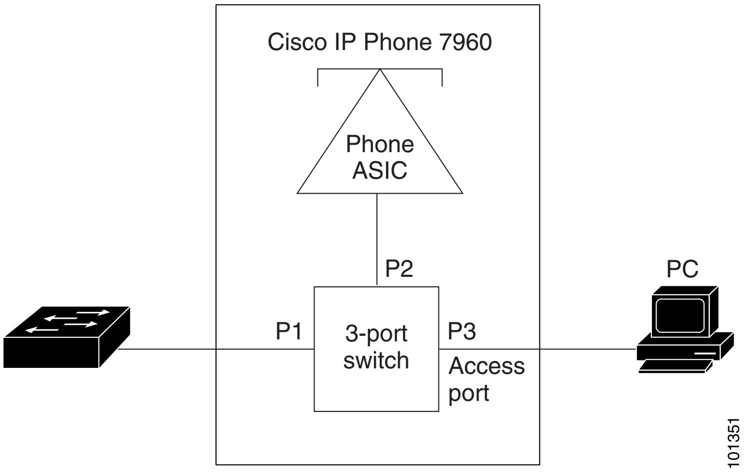
The Voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.

When using a configurable IP phone, you can configure it to forward traffic with an IEEE 802.1p priority. You can also configure the switch to trust or override the traffic priority assigned by an IP phone. For example, a Cisco IP phone (such as 7960 series) contains an integrated three-port 10/100 switch as shown in Figure 6-1. The ports provide dedicated connections to these devices:

- Port 1 connects to the switch or other voice-over-IP (VoIP) device.
- Port 2 is an internal 10/100 interface that carries the IP Phone traffic.
- Port 3 (access port) connects to a PC or other device.

Figure 6-1 shows one way to connect a Cisco IP Phone.

Figure 6-1 Cisco 7960 IP Phone Connected to a Switch



Cisco IP Phone Voice Traffic

You can configure an access port with an attached Cisco IP Phone to use one VLAN for voice traffic and another VLAN for data traffic from a device attached to the phone. You can configure access ports on the switch to send Cisco Discovery Protocol (CDP) packets.

Cisco IP Phone Data Traffic

The switch can also process tagged data traffic (traffic in IEEE 802.1Q or IEEE 802.1p frame types) from the device attached to the access port on the Cisco IP Phone (see Figure 6-1). You can configure Layer 2 access ports on the switch to send CDP packets that instruct the attached phone to configure the phone access in trusted mode. In this case, all traffic received through the access port on the Cisco IP Phone passes through the phone unchanged.

Note Untagged traffic from the device attached to the Cisco IP Phone passes through the phone unchanged, regardless of the trust state of the access port on the phone.

Configuring Voice VLAN

These sections contain this configuration information:

- Default Voice VLAN Configuration, page 6-3
- Voice VLAN Configuration Guidelines, page 6-3
- Configuring a Port Connected to a Cisco IP Phone, page 6-4

Default Voice VLAN Configuration

The Voice VLAN feature is disabled by default.

When the Voice VLAN feature is enabled, all untagged traffic is sent according to the default CoS priority of the port.

Voice VLAN Configuration Guidelines

These are the Voice VLAN configuration guidelines:

- Voice VLAN configuration is only supported on switch access ports; Voice VLAN configuration is not supported on trunk ports.

Note Trunk ports can carry any number of Voice VLANs, similar to regular VLANs. The configuration of Voice VLANs is not required on trunk ports.

  Voice VLAN should be present and active on the switch for the IP phone to correctly communicate on the Voice VLAN. Use the **show vlan** privileged EXEC command to display the configured VLANs.

- You must enable CDP on the switch port connected to the Cisco IP Phone to send the configuration to the phone. (CDP is globally enabled by default on all switch interfaces.)
- The Port Fast feature is automatically enabled When you configure Voice VLAN, the Port Fast feature is disabled by default.
- If the Cisco IP Phone and a device attached to the phone are in the same VLAN, they must be in the same IP subnet. These conditions indicate that they are in the same VLAN:
  - They both use IEEE 802.1p or untagged frames.
  - The Cisco IP Phone uses IEEE 802.1p frames, and the device uses untagged frames.
  - The Cisco IP Phone uses untagged frames, and the device uses IEEE 802.1p frames.
  - The Cisco IP Phone uses IEEE 802.1Q frames, and the Voice VLAN is the same as the access VLAN.
- The Cisco IP Phone and a device attached to the phone cannot communicate if they are in the same VLAN and subnet but use different frame types because traffic in the same subnet is not routed (routing would eliminate the frame type difference).
- You cannot configure static secure MAC addresses in the Voice VLAN.

- Voice VLAN ports can also be these port types:
  - Dynamic access port. (See the Configuring Dynamic-Access Ports on VMPS Clients section within the Configuring VLANs chapter of *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX*.)
  - IEEE 802.1x authenticated port. (See the Configuring 802.1x Readiness Check section within the Configuring IEEE 802.1x Port-Based Authentication chapter of the *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX*.)

    Note If you enable IEEE 802.1x on an access port on which a Voice VLAN is configured and to which a Cisco IP Phone is connected, the phone loses connectivity to the switch for up to 30 seconds.

  - Protected port. (See the Configuring Protected Ports section within the Configuring Port-Based Traffic Control chapter of the *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX*.)
  - A source or destination port for a SPAN or RSPAN session.
  - Secure port. (See the Configuring Port Security section within the Configuring Port-Based Traffic Control chapter of the *CGS 2520 Switch Software Configuration Guide, 12.2(53)EX*.)

    Note When you enable port security on an interface that is also configured with a Voice VLAN, you must set the maximum allowed secure addresses on the port to two plus the maximum number of secure addresses allowed on the access VLAN. When the port is connected to a Cisco IP Phone, the phone requires up to two MAC addresses. The phone address is learned on the Voice VLAN and might also be learned on the access VLAN. Connecting a PC to the phone requires additional MAC addresses.

Configuring a Port Connected to a Cisco IP Phone

Because a Cisco IP Phone also supports a connection to a PC or other device, a port connecting the switch to a Cisco IP Phone can carry mixed traffic. You can configure a port to decide how the Cisco IP Phone carries voice traffic and data traffic.

These sections contain this configuration information:

- Configuring Cisco IP Phone Voice Traffic, page 6-4
- Configuring the Priority of Incoming Data Frames, page 6-5

Configuring Cisco IP Phone Voice Traffic

You can configure a port connected to the Cisco IP Phone to send CDP packets to the phone to configure the way in which the phone sends voice traffic. The phone can carry voice traffic in IEEE 802.1Q frames for a specified Voice VLAN with a Layer 2 CoS value. It can use IEEE 802.1p priority tagging to give voice traffic a higher priority and forward all voice traffic through the native (access) VLAN. The Cisco IP Phone can also send untagged voice traffic or use its own configuration to send voice traffic in the access VLAN. In all configurations, the voice traffic carries a Layer 3 IP precedence value (the default is 5).

Beginning in privileged EXEC mode, follow these steps to configure voice traffic on a port:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface connected to the phone, and enter interface configuration mode.
Step 3	**switchport voice vlan** {*vlan-id* | **dot1p** | **none** | **untagged**}}	Configure how the Cisco IP Phone carries voice traffic: • *vlan-id*—Configure the phone to forward all voice traffic through the specified VLAN. By default, the Cisco IP Phone forwards the voice traffic with an IEEE 802.1Q priority of 5. Valid VLAN IDs are 1 to 4094. • **dot1p**—Configure the phone to use IEEE 802.1p priority tagging for voice traffic and to use the default native VLAN (VLAN 0) to carry all traffic. By default, the Cisco IP Phone forwards the voice traffic with an IEEE 802.1p priority of 5. • **none**—Allow the phone to use its own configuration to send untagged voice traffic. • **untagged**—Configure the phone to send untagged voice traffic.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport** or	Verify your Voice VLAN entries.
	show running-config interface *interface-id*	Verify your QoS and Voice VLAN entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure a port connected to a Cisco IP Phone and how to use IEEE 802.1p priority tagging for voice traffic, and to use the default native VLAN (VLAN 0) to carry all traffic:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport voice vlan dot1p
Switch(config-if)# end
```

To return the port to its default setting, use the **no switchport voice vlan** interface configuration command.

Configuring the Priority of Incoming Data Frames

Note To set priority of incoming data frames, the switch must be running the LAN Base image.

You can connect a PC or other data device to a Cisco IP Phone port. To process tagged data traffic (in IEEE 802.1Q or IEEE 802.1p frames), you can configure the switch to send CDP packets to instruct the phone how to send data packets from the device attached to the access port on the Cisco IP Phone. You can configure the phone to not change (trust) or to override (not trust) the priority of frames arriving on the phone port from connected devices.

Beginning in privileged EXEC mode, follow these steps to set the priority of data traffic received from the non-voice port on the Cisco IP Phone:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the interface connected to the Cisco IP Phone, and enter interface configuration mode.
Step 3	**switchport priority extend** {**cos** *value* | **trust**}	Sets the priority of data traffic received from the Cisco IP phone access port: • **cos** *value*—Configures the phone to override the priority received from the PC or the attached device with the specified CoS value. The value is a number from 0 to 7, with 7 as the highest priority. The default priority is cos 0. • **trust**—Configures the phone access port to trust the priority received from the PC or the attached device.
Step 4	**end**	Return to privileged EXEC mode.
Step 5	**show interfaces** *interface-id* **switchport**	Verify your entries.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

This example shows how to configure a port connected to a Cisco IP Phone to not change the priority of frames received from the PC or the attached device:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport priority extend trust
Switch(config-if)# end
```

To return the port to its default setting, use the **no switchport priority extend** interface configuration command.

Verifying Voice VLAN Configuration

Command	Purpose
show interfaces *interface-id* **switchport**	Display Voice VLAN configuration for an interface

CHAPTER 7

Configuring Smart Call Home

This chapter describes how to configure the Smart Call Home feature for Cisco Connected Grid switches. This chapter includes the following sections:

Supported Hardware

Supported Hardware	Hardware Minimum Software Release	Related Documentation
Cisco Connected Grid 10-port Ethernet Switch Module Interface Card (ESM) **Note** ESM is installed within the Cisco CGR 2010 router	Cisco IOS Release 15.0(2)ED	Cisco Connected Grid Ethernet Switch Module Interface Card Software Configuration Guide
Cisco CGS 2520 Switch	Cisco IOS Release 15.0(2)ED	Cisco 2500 Series Connected Grid Switches Configuration Guides

Information About Smart Call Home

Smart Call Home provides a notification and alert system for critical system events. A range of message formats are available for compatibility with pager services, standard e-mail, or XML-based automated parsing applications.

Common uses can include direct paging of a network support engineer, e-mail notification to a network operations center, and XML delivery to a support website.

The Smart Call Home feature provides these functions:

- Multiple message-format options:
  - Short text—Suitable for pagers or printed reports.
  - Plain text—Full formatted message information suitable for human reading.
  - XML—Machine readable format using Extensible Markup Language (XML) and Adaptive Markup Language (AML) document type definitions (DTDs).
- Multiple concurrent message destinations.
- Multiple message categories including configuration, diagnostics, environmental conditions, inventory, and syslog events.
- Message filtering by severity and pattern matching.
- Message transmission scheduling.
- Continuous device health monitoring and real-time diagnostics alerts.
- Secure message transport directly from your device or through a downloadable transport gateway aggregation point. Use a transport gateway aggregation point to support multiple devices or devices not connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices, including associated field notices, security advisories and end-of-life information.

Default Settings

Parameters	Default
Smart Call Home feature status	Disabled
User-defined profile status	Active
Transport method	e-mail
Message format type	XML
Destination message size for a message sent in long text, short text, or XML format	3,145,728
Alert group status	Enabled
Smart Call Home message severity threshold	0 (debugging)
Messages per minute rate limit	20

Configuring Smart Call Home

Configuration Overview

Before you configure Smart Call Home:

- Get the customer e-mail, phone, and street address for the Smart Call Home contact for configuration in the destination profile. This information identifies the source of messages sent to the Cisco server.
- If using e-mail message delivery, identify the name or IPv4 address of a primary Simple Mail Transfer Protocol (SMTP) server and any backup servers.
- Verify IP connectivity from the switch to the e-mail server or the destination HTTP server.
- If servers are specified by name, the switch must have IP connectivity to a domain name server.

Configuring Customer Contact Information

- E-mail address (required)
- Phone number (optional)
- Street address (optional)
- Contract ID (optional)
- Customer ID (optional)
- Site ID (optional)

Beginning in privileged EXEC mode, follow these steps to configure the customer contact information:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**contact-email-addr** *email-address*	Configure the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 4	**phone-number** +*phone-number*	(Optional) Configure the customer's phone number. **Note** The number must begin with a plus (**+**) prefix, and may contain only dashes (-) and numbers. Enter up to 16 characters. If you include spaces, you must enclose your entry in quotes (" ").

	Command	Purpose
Step 5	**street-address** *street-address*	(Optional) Configure the customer's street address to which RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (" ").
Step 6	**customer-id** *text*	(Optional) Assign a customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (" ").
Step 7	**site-id** *text*	(Optional) Assign a customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry in quotes (" ").
Step 8	**contract-id** *text*	(Optional) Configure the customer's contract ID for the switch. Enter up to 64 characters. If you include spaces, you must enclose your entry in quotes (" ").
Step 9	**exit**	Return to global configuration mode.

This example shows how to configure contact information:

```
Switch# configure terminal
Switch(config)# call-home
Switch(cfg-call-home)# contact-email-addr username@example.com
Switch(cfg-call-home)# phone-number +1-800-555-4567
Switch(cfg-call-home)# street-address "1234 Picaboo Street, Any city, Any state, 12345"
Switch(cfg-call-home)# customer-id Customer1234
Switch(cfg-call-home)# site-id Site1ManhattanNY
Switch(cfg-call-home)# contract-id Company1234
Switch(cfg-call-home)# exit
```

Configuring VRF for Use With Smart Call Home

If an interface configured on the specified VRF can connect to the mail server, the Smart Call Home feature uses it to send e-mail messages. If no appropriate interface is configured on the specified VRF, or if the corresponding VRF table does not exist on the switch, no messages are sent.

Beginning in privileged EXEC mode, follow these steps to use a VRF interface for Smart Call Home e-mail or for HTTP messages:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter configuration mode.
Step 1	**interface** *type*	Select an interface to configure.
Step 2	**ip address** *ip_address mask*	Assign an IP address and subnet mask to the interface.
Step 3	**vrf forwarding** *call_home_vrf_name*	Associate the *call_home_vrf_name* VRF with the interface.
Step 4	**exit**	Return to global configuration mode.

This example shows how to configure Smart Call Home to use a VRF interface:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# ip address 10.10.10.10 0.0.0.0
Switch(config-if)# vrf forwarding call_home_vrf
Switch(config-if)# exit
```

Configuring Destination Profiles

- Destination Profile Overview, page 7-5
- Configuring a Destination Profile to Send E-mail Messages, page 7-5
- Configuring Smart Call Home to Use VRF for E-mail Messages, page 7-6
- Configuring a Destination Profile to Send HTTP Messages, page 7-9
- Configuring Smart Call Home Traffic Rate Limiting, page 7-10
- Destination Profile Management, page 7-10

Destination Profile Overview

A destination profile contains the required delivery information for an alert notification. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

To use the Smart Call Home feature, you need to both enable Smart Call Home and configure a profile. You must configure required fields in the profiles. If a required field is not configured, that profile cannot initiate notification messages.

You can use the predefined destination profile or define a custom profile. If you define a new destination profile, you must assign a profile name.

You can configure these attributes for a destination profile:

- Profile name—A string that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case sensitive. You cannot use *all* as a profile name.
- Transport method—The transport mechanism, either e-mail or HTTP to deliver alerts.
  - For user-defined destination profiles, e-mail is the default, and you can enable either or both transport mechanisms. If you disable both methods, e-mail is enabled.
- Destination address—The e-mail or HTTP address to which the alert should be sent.
- Message formatting—The message format used for the alert.
  - For user-defined destination profiles, the options are long-text, short-text, or XML. The default is XML.
- Message size—The maximum message size. The valid range is 50 to 3,145,728 bytes, and the default is 3,145,728 bytes.

Configuring a Destination Profile to Send E-mail Messages

- Configuring Smart Call Home to Use VRF for E-mail Messages, page 7-6 (optional)
- Configuring the Mail Server, page 7-6 (required)
- Configuring a Destination Profile for E-mail, page 7-7 (required)
- Configuring Other E-mail Options, page 7-7 (optional)

Configuring Smart Call Home to Use VRF for E-mail Messages

Beginning in privileged EXEC mode, follow these steps to configure Smart Call Home to use a VRF instance for Smart Call Home e-mail messages:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration submode.
Step 3	**vrf** *call_home_vrf_name*	Specify the VRF instance to use for Smart Call Home e-mail messages. If a VRF is not specified, the default routing table is used.
Step 4	**exit**	Return to global configuration mode.

This example shows how to configure Smart Call Home to use a VRF interface:

```
Switch# configure terminal
Switch(config)# call-home
Switch(cfg-call-home)# vrf call_home_vrf
Switch(cfg-call-home)# exit
```

Configuring the Mail Server

Beginning in privileged EXEC mode, follow these steps to use the e-mail message transport:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**mail-server** {*ipv4-address* | *name*} **priority** *number*	Specify an e-mail server and its relative priority among configured e-mail servers, where: • *ipv4-address*—Specify the IPv4 address of the mail server. • *name*—Specify the mail-server fully qualified domain name (FQDN) of 64 characters or less. • *number*—Assign a number between 1 (highest priority) and 100 (lowest priority). Higher priority servers (lower priority numbers) are tried first. You can repeat this step to configure a total of five e-mail servers.

This example shows how to configure a primary mail server (*smtp.example.com*) and a secondary mail server that is at IP address 192.168.0.1:

```
Switch# configure terminal
Switch(config)# call-home
Switch(cfg-call-home)# mail-server smtp.example.com priority 1
Switch(cfg-call-home)# mail-server 192.168.0.1 priority 2
Switch(cfg-call-home)# exit
```

Configuring a Destination Profile for E-mail

Beginning in privileged EXEC mode, follow these steps to configure a destination profile for e-mail transport:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**profile** *name*	Configure the specified destination profile. If the specified destination profile does not exist, it is created.
Step 4	**destination transport-method email**	Configure the message transport method. The default is e-mail.
Step 5	**destination address email** *email_address*	Configure the destination e-mail address for Smart Call Home messages.
Step 6	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**}	(Optional) Configure a message format. The default is XML.
Step 7	**destination message-size** *bytes*	(Optional) Configure a maximum destination message size (from 50 to 3145728 bytes) for the destination profile. The default is 3145728 bytes.
Step 8	**active**	(Optional) Enable the destination profile. By default, a user-defined profile is enabled when it is created.
Step 9	**exit**	Exit Smart Call Home destination profile configuration mode, and return to Smart Call Home configuration mode.
Step 10	**end**	Return to privileged EXEC mode.

Configuring Other E-mail Options

Beginning in privileged EXEC mode, follow these steps to configure other e-mail options:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**sender from** *email-address*	(Optional) Assign the e-mail address that appears in the *from* field in Smart Call Home e-mail messages. If you do not specify an address, the contact e-mail address is used.
Step 4	**sender reply-to** *email-address*	(Optional) Assign the e-mail address that appears in the reply-to field in Smart Call Home e-mail messages.
Step 5	**source-ip-address** *ip_address*	(Optional) Assign the source IP address to use for Smart Call Home e-mail messages. **Note** You must specify a valid IP address that is already configured on an interface.

	Command or Action	Purpose
Step 6	**source-interface** {**async** | **auto-template** | **BVI** | **CTunnel** | **dialer** | **fastEthernet** | **filter** | **filtergroup** | **gigabitEthernet** | **group-async** | **groupVI** | **lex** | **loopback** | **port-channel** | **portgroup** | **pos-channel** | **tunnel** | **vif** | **virtual-template** | **virtual-TokenRing** | **vlan** | **fcpa**}	(Optional) Configure the name of the source interface to use for Smart Call Home email messages. Valid names are: • **async**—async interface • **auto-template**—auto-template interface • **BVI**— bridge-group virtual interface • **CTunnel**—CTunnel interface • **dialer**—dialer interface • **fastEthernet**—FastEthernet IEEE 802.3 • **filter**—filter interface • **filtergroup**—filter Group interface • **gigabitEthernet**—GigabitEthernet IEEE 802.3z • **group-async**—async group interface • **groupVI**—group virtual interface • **lex**—LAN Extender (lex) interface • **loopback**—Loopback interface • **port-channel**—Ethernet Channel of interfaces • **portgroup**—Portgroup interface • **pos-channel**—packet-over-SONET/SDH (POS) Channel of interfaces • **tunnel** —Tunnel interface • **vif**—pragmatic general multicast (PGM) Multicast Host interface • **virtual-template**—virtual template interface • **virtual-TokenRing**—virtual TokenRing • **vlan**—VLANs • **fcpa**—Fiber Channel **Note** The specified source interface must be configured with a valid IP address and be able to ping the mail server.

Note You can configure either a source IP address or a source interface, but not both.

This example shows how to configure the e-mail options with a source IP address:

```
Switch(cfg-call-home)# sender from username@example.com
Switch(cfg-call-home)# sender reply-to username@example.com
Switch(cfg-call-home)# source-ip-address 10.10.10.10
```

This example shows how to configure the e-mail options with a source interface:

```
Switch(cfg-call-home)# sender from username@example.com
Switch(cfg-call-home)# sender reply-to username@example.com
Switch(cfg-call-home)# source-interface fastEthernet 0/1
```

Configuring a Destination Profile to Send HTTP Messages

- Configuring the HTTP Source Interface, page 7-9
- Configuring a Destination Profile for HTTP, page 7-9

Configuring the HTTP Source Interface

Beginning in privileged EXEC mode, follow these steps to configure an HTTP client source interface:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http client source-interface** *type number*	Configure the source interface for the HTTP client. If the interface is associated with a VRF instance, the HTTP messages use the VRF instance.

Configuring a Destination Profile for HTTP

Beginning in privileged EXEC mode, follow these steps to configure a destination profile for HTTP transport:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**profile** *name*	Configure the specified destination profile. If the specified destination profile does not exist, it is created.
Step 4	**destination transport-method http**	Enable the HTTP message transport method.
Step 5	**destination address http** *url*	Configure the destination URL for Smart Call Home messages. **Note** When entering a destination URL, include either **http://** or **https://**, depending on whether the server is a secure server. HTTPS support is available only in cryptographic Cisco IOS images. If the destination is a secure server, you must also configure a trustpoint certificate authority.
Step 6	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**}	(Optional) Configure a preferred message format. The default is XML.
Step 7	**destination message-size** *bytes*	(Optional) Configure a maximum message size for the destination profile.
Step 8	**active**	Enable the destination profile. By default, a profile is enabled when it is created.

	Command or Action	Purpose
Step 9	**exit**	Exit Smart Call Home destination profile configuration mode, and return to Smart Call Home configuration mode.
Step 10	**end**	Return to privileged EXEC mode.

This example shows how to configure a destination profile for HTTP transport:

```
Switch# configure terminal
Switch(config)# call-home
Switch(config-call-home)# profile test
Switch(cfg-call-home-profile)# destination transport-method http
Switch(cfg-call-home-profile)# destination address http https://example.url.com
Switch(cfg-call-home-profile)# destination preferred-msg-format xml
Switch(cfg-call-home-profile)# destination message-size 3,145,728
Switch(cfg-call-home-profile)# active
Switch(cfg-call-home-profile)# exit
Switch(cfg-call-home)# end
```

Configuring Smart Call Home Traffic Rate Limiting

Beginning in privileged EXEC mode, follow these steps to configure Smart Call Home traffic rate limiting:

	Command	Purpose
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration submode.
Step 3	**rate-limit** *number*	(Optional) Specify the number of messages sent per minute. The range is from 1 to 60. The default is 20.

This example shows how to configure Smart Call Home traffic rate limiting:

```
Switch# configure terminal
Switch(config)# call-home
Switch(config-call-home)# profile test
Switch(cfg-call-home-profile)# rate-limit 20
```

Destination Profile Management

- Activating and Deactivating a Destination Profile, page 7-11
- Copying a Destination Profile, page 7-11
- Renaming a Destination Profile, page 7-12
- Verifying the Smart Call Home Profile Configuration, page 7-12

Activating and Deactivating a Destination Profile

Except for the predefined CiscoTAC-1 profile, all Smart Call Home destination profiles are automatically activated when you create them. If you do not want to use a profile right way, you can deactivate the profile. The CiscoTAC-1 profile is inactive by default and must be activated for use.

Beginning in privileged EXEC mode, follow these steps to activate or deactivate a destination profile:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**profile** *name*	Configure the specified destination profile. If the specified destination profile does not exist, it is created.
Step 4	**active**	Enable the destination profile. By default, a new profile is enabled when it is created.
Step 5	**no active**	Disable the destination profile.
Step 6	**end**	Exit Smart Call Home destination profile configuration mode, and return to privileged EXEC mode.

This example shows how to activate a destination profile:

```
Switch# configure terminal
Switch(config)# call-home
Switch(config-call-home)# profile test
Switch(cfg-call-home-profile)# active
Switch(cfg-call-home)# end
```

This example shows how to deactivate a destination profile:

```
Switch# configure terminal
Switch(config)# call-home
Switch(config-call-home)# profile test
Switch(cfg-call-home-profile)# no active
Switch(cfg-call-home)# end
```

Copying a Destination Profile

Beginning in privileged EXEC mode, follow these steps to create a new destination profile by copying an existing profile:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**copy profile** *source_profile target_profile*	Create a new destination profile with the same configuration settings as the existing destination profile: • *source_profile*—Specify the existing name of the profile. • *target_profile*—Specify a name for the new copy of the profile.

This example shows how to activate a destination profile:

```
Switch# configure terminal
Switch(config)# call-home
Switch(config-call-home)# profile test
Switch(cfg-call-home-profile)# copy profile profile1 profile2
```

Renaming a Destination Profile

Beginning in privileged EXEC mode, follow these steps to change the name of an existing profile:

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration mode.
Step 3	**rename profile** *source_profile target_profile*	Rename an existing source file: • *source_profile*—Specify the existing name of the profile. • *target_profile*—Specify a new name for the existing profile.

This example shows how to rename a destination profile:

```
Switch# configure terminal
Switch(config)# call-home
Switch(config-call-home)# profile test
Switch(cfg-call-home-profile)# rename profile profile1 profile2
```

Verifying the Smart Call Home Profile Configuration

To verify the profile configuration, use the **show call-home profile** command. See Verifying Smart Call Home Configuration, page 7-18 for more information and examples.

Subscribing to Alert Groups

- Overview of Alert Group Subscription, page 7-13
- Configuring Alert Group Subscription, page 7-13
- Configuring Periodic Notification, page 7-14
- Configuring Message Severity Threshold, page 7-14
- Configuring Syslog Pattern Matching, page 7-15

Overview of Alert Group Subscription

An alert group is a predefined subset of Smart Call Home alerts supported on all switches. The alerts are grouped based on their type:

- Configuration
- Diagnostic
- Environment
- Inventory
- Syslog

The trigger events for each alert group are listed in Alert Group Trigger Events and Commands, page 7-22, and the contents of the alert group messages are listed in Message Contents, page 7-25.

You can specify one or more alert groups to be received by a destination profile.

Note A Smart Call Home alert is sent only to destination profiles that have subscribed to the alert group containing that Smart Call Home alert. The alert group must also be enabled.

Configuring Alert Group Subscription

Beginning in privileged EXEC mode, follow these steps to subscribe a destination profile to an alert group:

	Command	Purpose
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**call-home**	Enter Smart Call Home configuration submode.
Step 3	**alert-group** {**all** | **configuration** | **diagnostic** | **environment** | **inventory** | **syslog**}	Enable the specified alert group. Use the keyword **all** to enable all alert groups. By default, all alert groups are enabled.
Step 4	**profile** *name*	Enter the Smart Call Home destination profile configuration submode for the specified destination profile.
Step 5	**subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]	Subscribe this destination profile to the Configuration alert group. To configure the Configuration alert group for periodic notification, see Configuring Periodic Notification, page 7-14.
Step 6	**subscribe-to-alert-group all**	Subscribe to all available alert groups.
Step 7	**subscribe-to-alert-group diagnostic** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}]	Subscribe this destination profile to the Diagnostic alert group. To configure the Diagnostic alert group to filter messages based on severity, see Configuring Message Severity Threshold, page 7-14.
Step 8	**subscribe-to-alert-group environment** [**severity** {**catastrophic** | **critical** | **debugging** | **disaster** | **fatal** | **major** | **minor** | **normal** | **notification** | **warning**}]	Subscribe this destination profile to the Environment alert group. To configure the Environment alert group to filter messages based on severity, see Configuring Message Severity Threshold, page 7-14.

	Command	Purpose
Step 9	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]	Subscribe this destination profile to the Inventory alert group. To configure the Inventory alert group for periodic notification, see Configuring Periodic Notification, page 7-14.
Step 10	**subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**} [**pattern** *string*]]	Subscribe this destination profile to the Syslog alert group. To configure the Syslog alert group to filter messages based on severity, see Configuring Message Severity Threshold, page 7-14. To specify a pattern to be matched in the syslog message, see Configuring Syslog Pattern Matching, page 7-15. If the pattern contains spaces, you must enclose it in quotes (" ").
Step 11	**exit**	Exit the Smart Call Home destination profile configuration submode.

Configuring Periodic Notification

When you subscribe a destination profile to either the Configuration or the Inventory alert group (see Configuring Alert Group Subscription, page 7-13), you can receive the alert group messages asynchronously or periodically at a specified time:

- Daily—Specify the time of day to send, using an hour:minute format *hh:mm*, with a 24-hour clock (for example, 14:30).
- Weekly—Specify the day of the week and time of day in the format *day hh:mm*, where the day of the week is spelled out (for example, monday).
- Monthly—Specify the date from 1 to 31, and the time of day in the format *date hh:mm*.

Configuring Message Severity Threshold

When you subscribe a destination profile to the Diagnostic, Environment, or Syslog alert group (see Configuring Alert Group Subscription, page 7-13), you can set a threshold for sending alert group messages based on levels of severity of a message. Any message with a value lower than the threshold specified in the destination profile is not sent to the destination.

The severity threshold is configured using the keywords in Table 7-1 and ranges from catastrophic (level 9, highest level of urgency) to debugging (level 0, lowest level of urgency). If no severity threshold is configured, the default is debugging (level 0).

Note Smart Call Home severity levels are not the same as system message logging severity levels.

Table 7-1 Severity and Syslog Level Mapping

Level	Keyword	Syslog Level	Description
9	**catastrophic**	–	Catastrophic network failure.
8	**disaster**	–	Significant network impact.
7	**fatal**	Emergency (0)	System is unusable.
6	**critical**	Alert (1)	Critical conditions, immediate attention needed.

Table 7-1 Severity and Syslog Level Mapping (continued)

Level	Keyword	Syslog Level	Description
5	**major**	Critical (2)	Major conditions.
4	**minor**	Error (3)	Minor conditions.
3	**warning**	Warning (4)	Warning conditions.
2	**notification**	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	**normal**	Information (6)	Normal event signifying return to normal state.
0	**debugging**	Debug (7)	Debugging messages.

Configuring Syslog Pattern Matching

When you subscribe a destination profile to the Syslog alert group (see Configuring Alert Group Subscription, page 7-13), you can specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message is sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes (“ ”) when configuring it. You can specify up to five patterns for each destination profile.

Enabling Smart Call Home

Beginning in privileged EXEC mode, follow these steps to enable or disable the Smart Call Home feature:

	Command	Purpose
Step 1	**configure terminal**	Enter configuration mode.
Step 2	**service call-home**	Enable the Smart Call Home feature.

Testing Smart Call Home Communications

You can test Smart Call Home communications by manually sending messages. To send a user-defined Smart Call Home test message, use the **call-home test** command. To send a specific alert group message, use the **call-home send** command.

- Manually Sending a Smart Call Home Test Message, page 7-16
- Manually Sending a Smart Call Home Alert Group Message, page 7-16
- Sending a Request for an Analysis and Report, page 7-17
- Sending the Output of a Command, page 7-17

Manually Sending a Smart Call Home Test Message

Beginning in privileged EXEC mode, follow these steps to manually send a Smart Call Home test message:

Command	Purpose
call-home test [*"test-message"*] **profile** *name*	Send a test message to the specified destination profile. Your test message text is optional but must be enclosed in quotes (" ") if it contains spaces. If you do not configure message text, a default message is sent.

Manually Sending a Smart Call Home Alert Group Message

Beginning in privileged EXEC mode, follow these steps to manually trigger a Smart Call Home alert group message:

	Command	Purpose
Step 1	**call-home send alert-group configuration** [**profile** *name*]	Send a configuration alert group message to a specific destination profile or to all subscribed destination profiles.
Step 2	**call-home send alert-group diagnostic** {**module** *number* | *slot/subslot* | *slot/bay_number* | **switch** *x* **module** *number*} [**profile** *name*]	Send a diagnostic alert group message to the specified destination profile or to all subscribed destination profiles. You must specify the module or port whose diagnostic information should be sent. If a virtual switching system (VSS) is used, you must specify the switch and module.
Step 3	**call-home send alert-group inventory** [**profile** *name*]	Send an inventory alert group message to the specified destination profile or to all subscribed destination profiles.

When manually sending Smart Call Home alert group messages, note these guidelines:

- Only configuration, diagnostic, and inventory alert group messages can be sent.
- When you send a configuration, diagnostic, or inventory alert group message to a specific destination profile, the message is sent, regardless of the active status, subscription status, or severity setting of the profile.
- When you send a configuration or inventory alert group message and do not specify a destination profile, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.
- When you send a diagnostic alert group message and do not specify a destination profile, the command produces these results:
  - An active profile that subscribes to diagnostic events with a severity level of less than 4 receives the message whether or not the module or interface had a diagnostic event.
  - An active profile that subscribes to diagnostic events with a severity level of 4 or higher receives the message only if the specified module or interface had a diagnostic event of level 4 or higher. Otherwise, the destination profile receives no diagnostic message.

Sending a Request for an Analysis and Report

You can use the **call-home request** command to submit information about your system to Cisco to receive helpful information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references.

Beginning in privileged EXEC mode, follow these steps to submit a request for report and analysis information from the Cisco Output Interpreter tool:

	Command	Purpose
Step 1	**call-home request output-analysis** *"show-command"* [**profile** *name*] [**ccoid** *user-id*]	Send the output of the specified **show** command for analysis. The **show** command must be in quotes (“ ”).
Step 2	**call-home request** {**config-sanity** | **bugs-list** | **command-reference** | **product-advisory**} [**profile** *name*] [**ccoid** *user-id*]	Send the output of a predetermined set of commands for analysis. Specify the type of report requested.

When manually sending a Smart Call Home report and analysis request, note these guidelines:

- If you specify a **profile** *name*, the request is sent to the profile. The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message is sent to the Cisco TAC.
- The **ccoid** *user-id* is the registered identifier of the Smart Call Home user. If you specify a *user-id*, the response is sent to the e-mail address of the registered user. If you do not specify a *user-id*, the response is sent to the contact e-mail address of the device.
- Based on the keyword that specifies the type of report, this information is returned:
  - **config-sanity**—Information on best practices for the current running configuration.
  - **bugs-list**—Known bugs in the running version and in the current features.
  - **command-reference**—Reference links to all commands in the running configuration.
  - **product-advisory**—Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that can affect devices in your network.

This example shows a request for analysis of a user-specified **show** command:

```
Switch# call-home request output-analysis "show diagnostic result module all" profile TG
```

Sending the Output of a Command

You can use the **call-home send** command to enter a command and to e-mail the command output to Cisco or to a specified e-mail address.

Beginning in privileged EXEC mode, follow these steps to enter a command and e-mail the command output:

Command	Purpose
call-home send *"command"* [**email** *email-addr*] [**tac-service-request** *SR*]	Enter the specified command and e-mail the output.

When sending the command output, note these guidelines:

- You can specify any **run** command, including commands for all modules. You must enclose the command in quotes (“ ”).
- If you specify an e-mail address, the command output is sent to that address. If you do not specify an e-mail address, the output is sent to the Cisco TAC (attach@cisco.com). The e-mail is sent in long text format with any specified service number in the subject line.
- The service number is required only if you do not specify an e-mail address, or if you specify a Cisco TAC e-mail address.

This example shows how to send the output of a command to an e-mail address that you specify:

```
Switch# call-home send "show diagnostic result module all" email support@example.com
```

Verifying Smart Call Home Configuration

Beginning in privileged EXEC mode, enter these commands to display the configured Smart Call Home information:

Command	Purpose
show call-home	Display the Smart Call Home configuration in summary.
show call-home detail	Display the Smart Call Home configuration in detail.
show call-home alert-group	Display the available alert groups and their status.
show call-home mail-server status	Check and display the availability of the configured e-mail server.
show call-home profile {**all** | *name*}	Display the configuration of the specified destination profile. Use the keyword **all** to display the configuration of all destination profiles.
show call-home statistics	Display the statistics of Smart Call Home events.

Examples 7-1 to 7-7 show the results when using different options of the **show call-home** command.

Example 7-1 Configured Smart Call Home Information

```
Switch# show call-home
Current Smart Call Home settings:
    Smart Call Home feature : enable
    Smart Call Home message's from address: crdc_3560_test_bed@cisco.com
    Smart Call Home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: crdc_3560_testbed@cisco.com

    contact person's phone number: +8602124057927
    street address: 966. Yishan Rd. Shanghai, China
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: 123456
    source ip address: Not yet set up
    source interface: Not yet set up
    Mail-server[1]: Address: 64.102.124.15 Priority: 10
    Mail-server[2]: Address: 171.71.177.236 Priority: 20
    Rate-limit: 20 message(s) per minute

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: CiscoTAC-1
    Profile Name: prof-1

Switch#
```

Example 7-2 Configured Smart Call Home Information in Detail

```
Switch# show call-home detail
Current Smart Call Home settings:
    Smart Call Home feature : enable
    Smart Call Home message's from address: crdc_3560_test_bed@cisco.com
    Smart Call Home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: crdc_3560_testbed@cisco.com

    contact person's phone number: +8602124057927
    street address: 966. Yishan Rd. Shanghai, China
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: 123456
    source ip address: Not yet set up
    source interface: Not yet set up
    Mail-server[1]: Address: 64.102.124.15 Priority: 10
    Mail-server[2]: Address: 171.71.177.236 Priority: 20
    Rate-limit: 20 message(s) per minute

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Enable  configuration info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    syslog                   Enable  syslog info

Profiles:

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 16 day of the month at 13:10

    Periodic inventory info message is scheduled every 16 day of the month at 12:55
    Alert-group               Severity
    ------------------------  ------------
    diagnostic                minor
    environment               warning
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Profile Name: prof-1
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): diazhang@cisco.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        warning
    COUNTERS                  warning

Switch#
```

Example 7-3 Available Smart Call Home Alert Groups

```
Switch# show call-home alert-group
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- -------------------------------
    configuration            Disable configuration info
    diagnostic               Disable diagnostic info
    environment              Disable environmental info
    inventory                Enable  inventory info
    syslog                   Disable syslog info

Switch#
```

Example 7-4 E-mail Server Status Information

```
Switch# show call-home mail-server status
Please wait. Checking for mail server status ...

Translating "smtp.example.com"
    Mail-server[1]: Address: smtp.example.com Priority: 1 [Not Available]
    Mail-server[2]: Address: 192.168.0.1 Priority: 2 [Not Available]

Switch#
```

Example 7-5 Information for All Destination Profiles (Predefined and User-Defined)

```
Switch# show call-home profile all

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 1 day of the month at 09:27

    Periodic inventory info message is scheduled every 1 day of the month at 09:12

    Alert-group               Severity
    ------------------------  ------------
    diagnostic                minor
    environment               minor

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major

Switch#
```

Example 7-6 Information for a User-Defined Destination Profile

```
Switch# show call-home profile campus-noc

Profile Name: campus-noc
    Profile status: ACTIVE
    Preferred Message Format: long-text
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): noc@example.com
    HTTP  address(es): Not yet set up

    Alert-group               Severity
    ------------------------  ------------
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    N/A                       N/A

Switch#
```

Example 7-7 Smart Call Home Statistics

```
Switch# show call-home statistics
Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   6                    6                    0
    Config      4                    4                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   2                    2                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total Failed    10                   10                   0
    Config      9                    9                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      1                    1                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Total Ratelimit
      -dropped  0                    0                    0
    Config      0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0

Last call-home message sent time: 2012-10-29 01:03:17 GMT+00:00

Switch#
```

Alert Group Trigger Events and Commands

Smart Call Home trigger events are grouped into alert groups, with each alert group assigned to execute Cisco IOS commands when an event occurs. The command output is included in the message. These tables list the trigger events included in each alert group, including the severity level of each event and the executed commands for the alert group:

- Smart Call Home Syslog Alert Group Events and Actions, Table 7-2 on page 7-23
- Smart Call Home Environmental Alert Group Events and Actions, Table 7-3 on page 7-23
- Smart Call Home Inventory Alert Group Events and Actions, Table 7-4 on page 7-24
- Smart Call Home Diagnostic Failure Alert Group Events and Actions, Table 7-5 on page 7-24
- Smart Call Home Test Alert Group Events and Actions, Table 7-6 on page 7-25
- Smart Call Home Configuration Alert Group Events and Actions, Table 7-7 on page 7-25

Table 7-2 Smart Call Home Syslog Alert Group Events and Actions

Alert Group Description:	Event logged to syslog		
Executed Commands:	**show inventory**, **show logging**		
Smart Call Home Trigger Event	**Syslog Event**	**Sev**	**Description**
SYSLOG	LOG_EMERG	0	System is unusable.
	LOG_ALERT	1	Action must be taken immediately.
	LOG_CRIT	2	Critical conditions.
	LOG_ERR	3	Error conditions.
	LOG_WARNING	4	Warning conditions.
	LOG_NOTICE	5	Normal but significant condition, such as recovery from failure.
	LOG_INFO	6	Informational.
	LOG_DEBUG	7	Debug-level messages.

Table 7-3 Smart Call Home Environmental Alert Group Events and Actions

Alert Group Description:	Events related to power and environment sensing elements such as temperature alarms		
Executed Commands:	**show environment**, **show env power**, **show inventory**, **show logging**, **show version**		
Smart Call Home Trigger Event	**Syslog Event**	**Sev**	**Description**
TEMP_FAILURE	TempHigh	2	The chassis temperature exceeds the normal threshold.
TEMP_FAILURE	CriticalTemp	2	The chassis temperature exceeds the critical threshold.
TEMP_FAILURE	ShutdownTemp	2	The high chassis temperature is causing a system shutdown.
TEMP_RECOVER	TempOk	2	The chassis temperature is normal.
POWER_FAILURE	PowerSupplyBad	2	A power supply has failed or been turned off.
POWER_RECOVERY	PowerSupplyGood	2	A failed power supply is fixed.
POWER_FAULTY	PowerSupplyFaulty	4	A power supply is in a faulty state.
POWER_CRITICAL	PowerSupplyCritical	2	A power supply is in a critical state.
POWER_FAILURE	InlinePowerSupplyBad	4	An inline power source has failed or been turned off.
POWER_RECOVERY	InlinePowerSupplyGood	4	A failed inline power source is fixed.
POWER_FAILURE	RedundantPowerSupplyFailure	2	The redundant power supply has failed.
POWER_RECOVERY	RedundantPowerSupplyOk	2	The redundant power supply is fixed.

Table 7-4 Smart Call Home Inventory Alert Group Events and Actions

Alert Group Description:	Inventory status is provided whenever a unit is rebooted by removing and replacing the power cable or when modules are inserted or removed. This is not a critical event, and the information is used for status and entitlement.	
Executed Commands:	**show env power**, **show inventory oid**, **show version**	
Smart Call Home Trigger Event	**Syslog Event**	**Description**
INSERTION	Switch	A switch was inserted in a stack.
	PowerSupply	A power supply was inserted.
	Module	A replaceable module was inserted. (There is no alert for insertion of an SFP module.)
REMOVAL	Switch	A switch was removed from a stack.
	PowerSupply	A power supply was removed.
	Module	A replaceable module was removed. (There is no alert for removal of an SFP module.)

Table 7-5 Smart Call Home Diagnostic Failure Alert Group Events and Actions

Alert Group Description:	Events related to standard or intelligent switches	
Executed Commands:	**show buffers**, **show diagnostic result**, **show diagnostic result detail** (for nonstackable switches), **show diagnostic result switch all**, **show diagnostic result switch all detail** (for stackable switches), **show inventory**, **show logging**, **show version**	
Smart Call Home Trigger Event:	ONDEMAND	
Syslog Event	**Sev**	**Description**
DIAG		The switch stack failed the heart beat status test.
		One or more ASICs or ports on the switch failed the send and receive path test.
		The switch failed the test for the content-addressable memory (CAM) mask and value entries and the lookup.
		The stack ring, port ASICs or both failed the communication test.
		The stack port failed the internal loopback test.
		The port ASICs (or their send and receive buffers) failed the internal memory test.

Table 7-6 Smart Call Home Test Alert Group Events and Actions

Alert Group Description:	—	
Executed Commands:	**show inventory**, **show version** (Output from these commands is attached only to XML-formatted messages.)	
Smart Call Home Trigger Event:	—	
Syslog Event	**Sev**	**Description**
TEST	1	User-generated test message.

Table 7-7 Smart Call Home Configuration Alert Group Events and Actions

Alert Group Description:	User generated request for configuration.	
Executed Commands:	**show inventory**, **show running-config all**, **show startup-config**, **show version**	
Smart Call Home Trigger Event:	—	
Syslog Event	**Sev**	**Description**
—	—	—

Message Contents

These tables display the content formats of alert group messages:

- Table 7-8 describes the content fields of a short text message. These messages are for reactive and proactive events, inventory changes, and test messages. Short text messages are not used for configuration or inventory-at-startup messages.
- Table 7-9 describes the content fields that are common to all long text and XML messages. The fields specific to a particular alert group message are after the common fields.
- Table 7-10 describes the content fields for reactive messages (system failures that require a TAC case) and proactive messages (issues that might result in degraded system performance).
- Table 7-11 describes the content fields for an inventory message.

Table 7-8 Format for a Short Text Message

Data Item	Description
Device identification	Configured device name
Date/time stamp	Time stamp of the triggering event
Error isolation message	Text description of the triggering event
Alarm urgency level	Number that indicates the severity of the alarm. The range is from 0 (most severe) to 7 (least severe).

Table 7-9 Common Fields for All Long Text and XML Messages

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD*T*HH:MM:SS* **Note** The time shown reflects the timezone offset from UTC.	CallHome/EventTime
Message name	Name of message. Specific event names are listed in Alert Group Trigger Events and Commands, page 7-22.	(for short text message only)
Message type	Specifically Smart Call Home.	CallHome/Event/Type
Message subtype	Specific type of message: full, delta, or test.	CallHome/Event/SubType
Message group	Specifically reactive or proactive. (The default is reactive.)	(for long text message only)
Severity level	Severity level of message. (See Table 7-1 on page 7-14.)	Body/Block/Severity
Source ID	Product type for routing, typically the product family name.	(for long text message only)
Device ID	Unique device identifier (UDI) for the end device that generated the message. This field is empty if the message is nonspecific to a fabric switch. The format is *type@Sid@serial.* • *type* is the product model number from the backplane SEEPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number· • *serial* is the number identified by the Sid field. Example: DS-C9509@C@12345678	CallHome/CustomerData/ContractData/DeviceId
Customer ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ContractData/CustomerId
Contract ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ContractData/ContractId
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	CallHome/CustomerData/ContractData/SiteId

Table 7-9 Common Fields for All Long Text and XML Messages (continued)

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Server ID	If the message is generated from the fabric switch, this is the unique device identifier (UDI) of the switch. If the message is proxied or originated by a source other than the switch, this field shows the UDI of the source. The format is *type@Sid@serial*. • *type* is the product model number from the backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number· • *serial* is the number identified by the Sid field. Example: SSE1120@C@12345678	(For long text message only)
Message description	Short text describing the error.	CallHome/MessageDescription
Device name	Node that experienced the event. This is the hostname of the device.	CallHome/CustomerData/SystemInfo/Name
Contact name	Name of person to contact for issues associated with the node experiencing the event.	CallHome/CustomerData/SystemInfo/Contact
Contact e-mail	E-mail address of person identified as the contact.	CallHome/CustomerData/SystemInfo/ContactEmail
Contact phone number	Phone number of the person identified as the contact.	CallHome/CustomerData/SystemInfo/ContactPhoneNumber
Street address	Optional field containing street address for replacement part shipments.	CallHome/CustomerData/SystemInfo/StreetAddress
Model name	Model name of the switch. This is the specific model as part of a product family name.	CallHome/Device/Cisco_Chassis/Model
Serial number	Chassis serial number.	CallHome/Device/Cisco_Chassis/SerialNumber
Chassis part number	Top assembly number of the chassis.	CallHome/Device/Cisco_Chassis/AdditionalInformation/ AD@name="PartNumber"/
System Object ID (used for stackable switches only)	The System ObjectID that uniquely identifies the system.	CallHome/Device/Cisco_Chassis/AdditionalInformation/ AD@name="sysObjectID"
SysDesc (used for stackable switches only)	System description for the managed element.	CallHome/Device/Cisco_Chassis/AdditionalInformation/ AD@name="sysDescr"

Table 7-9 Common Fields for All Long Text and XML Messages (continued)

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
These fields can be repeated if multiple commands are executed for this alert group.		
Command output name	The exact syntax of the issued CLI command.	/aml/Attachments/Attachment/Name
Attachment type	The type is “command output”.	/aml/Attachments/Attachment@type
MIME type	Text or encoding type.	/aml/attachments/attachment/Data@encoding
Command output text	Output of command automatically executed. (See Alert Group Trigger Events and Commands, page 7-22.)	/aml/attachments/attachment/atdata

Table 7-10 Fields for a Reactive or Proactive Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/HardwareVersion
Affected FRU name	Name of the affected component generating the message	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
Affected FRU serial number	Serial number of the affected component	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
Affected FRU part number	Part number of the affected component	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	Slot number of the component generating the event message	CallHome/Device/Cisco_Chassis/Cisco_Card/ LocationWithinContainer
FRU hardware version	Hardware version of the affected component	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	Software version running on the affected component	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString
Process name	Name of process	/aml/body/process/name
Process ID	Unique process ID	/aml/body/process/id
Process state	State of process (for example, running or stopped)	/aml/body/process/processState
Process exception	Exception or reason code	/aml/body/process/exception

Table 7-11 Fields for an Inventory Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Chassis hardware version	Hardware version of chassis	CallHome/Device/Cisco_Chassis/HardwareVersion
Affected FRU name	Name of the component generating the message	CallHome/Device/Cisco_Chassis/Cisco_Card/Model
Affected FRU s/n	Serial number of the component	CallHome/Device/Cisco_Chassis/Cisco_Card/SerialNumber
Affected FRU part number	Part number of the component.	CallHome/Device/Cisco_Chassis/Cisco_Card/PartNumber
FRU slot	Slot number of the component that generated the message	CallHome/Device/Cisco_Chassis/Cisco_Card/LocationWithinContainer
FRU hardware version	Hardware version of the component	CallHome/Device/Cisco_Chassis/Cisco_Card/HardwareVersion
FRU software version	Software version running on the component	CallHome/Device/Cisco_Chassis/Cisco_Card/SoftwareIdentity/VersionString

Sample Syslog Alert Notification in Long-Text Format

```
From: crdc_3560_testbed@cisco.com
Sent: Monday, October 29, 2012 9:35 AM
To: Diankun Zhang (diazhang)
Subject: System Notification From Switch - syslog - 2012-10-29 01:34:44 GMT+00:00


TimeStamp : 2012-10-29 01:34 GMT+00:00
Message Name : syslog
Message Type : Smart Call Home
Message Group : reactive
Severity Level : 2
Source ID : CGS2520
Device ID : WS-C3560V2-48PS-CR@C@FDO1335Z1BY
Customer ID :
Contract ID :
Site ID : 123456
Server ID : WS-C3560V2-48PS-CR@C@FDO1335Z1BY
Event Description : *Oct  29 01:34:44.481: %CLEAR-5-COUNTERS: Clear
counter on all interfaces by lab on console
System Name : Switch
Contact Email : crdc_3560_testbed@cisco.com
Contact Phone : +8602124057927
Street Address : 966. Yishan Rd. Shanghai, China
Affected Chassis : WS-C3560V2-48PS-CR
Affected Chassis Serial Number : FDO1335Z1BY
Affected Chassis Part No : 800-33161-01
Supervisor Software Version : 12.2(20110301:143745)103
```

```
Command Output Name : show logging
Attachment Type : command output
MIME Type : text/plain
Command Output Text :
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0
flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 38 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 38 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    File logging: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 40 message lines logged

Log Buffer (1000000 bytes):

*Oct  29 00:00:51.573: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan1, changed state to downAuth Manager registration failed

*Oct  29 00:00:53.242: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled
for type vlan
*Oct  29 00:00:56.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Oct  29 00:00:57.017: %SYS-5-CONFIG_I: Configured from memory by console
*Oct  29 00:00:58.359: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C3560 Software (C3560-IPSERVICESK9-M), Experimental
Version 12.2(20110301:143745) [diazhang-CSCtj33100_V122_58_0_57_SE 103]
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 01-Mar-11 21:57 by diazhang
*Oct  29 00:00:58.502: %SSH-5-ENABLED: SSH 1.99 has been enabled

*Oct  29 01:29:37.198: %CLEAR-5-COUNTERS: Clear counter on all interfaces
by lab on console
*Oct  29 01:31:40.301: %SYS-5-CONFIG_I: Configured from console by lab on
console
Switch#
Command Output Name : show inventory
Attachment Type : command output
MIME Type : text/plain
Command Output Text : NAME: "1", DESCR: "WS-C3560V2-48PS"
PID: WS-C3560V2-48PS-CR, VID:      , SN: FDO1335Z1BY

Switch#
```

Sample Syslog Alert Notification in XML Format

```
From: crdc_3560_testbed@cisco.com
```

```
Sent: Monday, October 29, 2012 9:30 AM
To: Diankun Zhang (diazhang)
Subject: System Notification From Switch - syslog - 2012-10-29 01:29:37 GMT+00:00


<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope xmlns:soap-env="http://www.w3.org/2003/05/soap-
envelope">
<soap-env:Header>
<aml-session:Session xmlns:aml-
session="http://www.cisco.com/2004/01/aml-session" soap-
env:mustUnderstand="true" soap-env:role="http://www.w3.org/2003/05/soap-
envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml-
session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>M22:FDO1335Z1BY:AF3BE582</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block xmlns:aml-block="http://www.cisco.com/2004/01/aml-
block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-
block:Type>
<aml-block:CreationDate>2012-10-29 01:29:38 GMT+00:00</aml-
block:CreationDate>
<aml-block:Builder>
<aml-block:Name>ESM</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>G23:FDO1335Z1BY:AF3BE582</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>2</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome"
version="1.0">
<ch:EventTime>2012-10-29 01:29:37 GMT+00:00</ch:EventTime>
<ch:MessageDescription>*Oct  29 01:29:37.198: %CLEAR-5-COUNTERS: Clear
counter on all interfaces by lab on console</ch:MessageDescription>
<ch:Event>
<ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType>
<ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>Cisco Connected Grid Ethernet Switch Module</ch:Series>
</ch:Event>
<ch:CustomerData>
<ch:UserData>
<ch:Email>crdc_3560_testbed@cisco.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId>123456</ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>WS-C3560V2-48PS-CR@C@FDO1335Z1BY</ch:DeviceId>
```

```
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>Switch</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>crdc_3560_testbed@cisco.com</ch:ContactEmail>
<ch:ContactPhoneNumber>+8602124057927</ch:ContactPhoneNumber>
<ch:StreetAddress>966. Yishan Rd. Shanghai, China</ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>WS-C3560V2-48PS-CR</rme:Model>
<rme:HardwareVersion></rme:HardwareVersion>
<rme:SerialNumber>FDO1335Z1BY</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="800-33161-01" />
<rme:AD name="SoftwareVersion" value="12.2(20110301:143745)103" />
<rme:AD name="SystemObjectId" value="1.3.6.1.4.1.9.1.102" />
<rme:AD name="SystemDescription" value="Cisco IOS Software, C3560
Software (C3560-IPSERVICESK9-M), Experimental Version
12.2(20110301:143745) [diazhang-CSCtj33100_V122_58_0_57_SE 103]
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 01-Mar-11 21:57 by diazhang" />
</rme:AdditionalInformation>
</rme:Chassis>
</ch:Device>
</ch:CallHome>
</aml-block:Content>
<aml-block:Attachments>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited, 0
flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 36 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 36 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    File logging: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 38 message lines logged

Log Buffer (1000000 bytes):

*Oct  29 00:00:51.573: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Vlan1, changed state to downAuth Manager registration failed
*Oct  29 00:00:53.242: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled
for type vlan
*Oct  29 00:00:56.723: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to down
*Oct  29 00:00:57.017: %SYS-5-CONFIG_I: Configured from memory by console
*Oct  29 00:00:58.359: %SYS-5-RESTART: System restarted --
Cisco IOS Software, C3560 Software (C3560-IPSERVICESK9-M), Experimental
Version 12.2(20110301:143745) [diazhang-CSCtj33100_V122_58_0_57_SE 103]
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Tue 01-Mar-11 21:57 by diazhang
*Oct  29 00:00:58.502: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Oct  29 00:01:00.817: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/1, changed state to up
*Oct  29 00:01:02.377: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed
state to up
*Oct  29 00:14:03.407: %SYS-5-CONFIG_I: Configured from console by lab on
console
*Oct  29 00:14:11.871: %CALL_HOME-3-SMTP_SEND_FAILED: Unable to send
notification using all SMTP servers (ERR 7, error in connecting to SMTP
server)
*Oct  29 01:02:50.930: %CLEAR-5-COUNTERS: Clear counter on all interfaces
by lab on console
*Oct  29 01:16:27.175: %SYS-5-CONFIG_I: Configured from console by lab on
console
Switch#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain">
<![CDATA[NAME: "1", DESCR: "WS-C3560V2-48PS"
PID: WS-C3560V2-48PS-CR, VID:      , SN: FDO1335Z1BY


Switch#]]></aml-block:Data>
</aml-block:Attachment>
</aml-block:Attachments>
</aml-block:Block>
</soap-env:Body>
</soap-env:Envelope>
```