

Service Diagnostics 2.0 CFM Scripts

Last Updated: October, 2009

The Service Diagnostics 2.0 CFM Scripts feature provides a bundled set of Tool Command Language (Tcl) scripts, Embedded Menu Manager (EMM)-based Menu Definition Files (MDFs) and Embedded Event Manager (EEM) policies. These policies facilitate diagnosing common networking issues in Connectivity Fault Management (CFM) for Cisco Carrier Ethernet Operations, Administration, and Maintenance (OAM). The EMM feature is available in Cisco IOS Release 12.4(20)T and later Cisco IOS images, and may be used to guide you in installing and deploying these scripts and policies.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for the Service Diagnostics 2.0 CFM Scripts.”](#)

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

Prerequisites for Service Diagnostics 2.0 CFM Scripts	2
Restrictions for Service Diagnostics 2.0 CFM Scripts	2
Information About Service Diagnostics 2.0 CFM Scripts.....	2
How to Use the Service Diagnostics 2.0 CFM Scripts.....	3
Configuration Examples for Service Diagnostics 2.0 CFM Scripts.....	18
Additional References	18
Feature Information for the Service Diagnostics 2.0 CFM Scripts.....	19
Glossary	20

Prerequisites for Service Diagnostics 2.0 CFM Scripts

- You understand what EEM and EMM are used for.
- You understand what eXtensible Markup Language (XML) for MDF files is used for.
- You understand what Tcl scripting means.
- You have access to the CCO website in order to download the scripts: <http://www.cisco.com/go/iossd>

Restrictions for Service Diagnostics 2.0 CFM Scripts

- This feature is only available in CFM for Cisco Carrier Ethernet OAM.

Information About Service Diagnostics 2.0 CFM Scripts

To use the Service Diagnostics 2.0 CFM Scripts feature, you should understand the following concepts:

- [Service Diagnostics 2.0 CFM Scripts Overview](#)
- [Benefits of Service Diagnostics 2.0 CFM Scripts](#)

Service Diagnostics 2.0 CFM Scripts Overview

If your image has the EMM feature, it is much easier to use the MDF versus the Zip file. If not, you must use the Tcl shell (tclsh) helper scripts.

Deploying the script via tclsh requires you to enter parameters. There are two types of parameters (parameters refer to keywords and arguments): mandatory common and policy specific. The mandatory common parameters are as follows:

- Notification method: The script uses selective notification methods to send diagnostic messages after executing the policy scripts.

The values for the notification methods can be:

- all
- email
- email,syslog
- snmp
- snmp,email
- snmp,syslog
- syslog

Note: Because of the size limitation of syslog and Simple Network Management Protocol (SNMP), the script sends only summary messages for the syslog and SNMP methods. Both summary and detailed messages are delivered if “email” is chosen. You can also choose multiple notification methods.

- Configuration history: Cisco IOS configuration history to be included in the notification message.
Value: TRUE to enable, FALSE to disable.
- Event history: Event history to be included in the notification message.
Value: TRUE to enable, FALSE to disable.
- Command history: Cisco IOS commands issued by the policy script to be included in the notification message.
Value: TRUE to enable, FALSE to disable.
- Prepend: Prefixes the trigger message to the notification message.

Value: TRUE to enable, FALSE to disable.

- User policy directory: The full path where EEM user policy scripts and other service diagnostic scripts are stored.
- User library directory: The full path where EEM library files are stored.

The policy-specific parameters are as follows:

- *ma-list*: Full path filename containing one Maintenance Association (MA) per line. The asterisk (*) wild card can be used for all MAs configured in Cisco IOS software.
- *p2p*: Point-to-point services.

Value: TRUE if specified MAs associated with P2P services have Up Maintenance Association End Points (MEPs) on the local interface without service multiplexing (that is, there is only one service/MEP per interface). FALSE if TRUE criteria is not met.
- *timer*: Timer is in minutes. The default is 360 (6 hours). The minimum value is 60 (1 hour).
- *domain-name*: A valid domain name.
- *ma-name*: A valid MA name under the above specified domain, for which details needs to be collected.
- *optional-mep-id*: Remote MEPs MEP-ID for the above specified MA. This input is optional.
- *policy-name*: Where policy-name can be cfm_shut.tcl, cfm_unshut.tcl, cfm_autotrace.tcl, cfm_cctimeout.tcl or cfm_ondemand.tcl.

Benefits of Service Diagnostics 2.0 CFM Scripts

- There are vast troubleshooting capabilities that can be automated using the existing scripting capabilities and embedded management tools in Cisco IOS software.
- This feature combines one or more tools (EEM and EMM) to automate common diagnostic scenarios.
- Using the Service Diagnostics 2.0 CFM Scripting feature, you are isolated from the rigors of Tcl script and/or EEM policy writing.
- The Service Diagnostics 2.0 CFM Scripting feature provides a simple interface for deploying and receiving feedback from scenario-specific troubleshooting scripts.
- The Service Diagnostics 2.0 CFM Scripting feature provides both the CLI Tcl shell user interface as well as EMM Menu Definition Files (MDFs) for deploying troubleshooting diagnostic scripts.

How to Use the Service Diagnostics 2.0 CFM Scripts

This section contains the following tasks. You can choose to use either tclsh or EMM.

- [Installing Scripts Using tclsh CLI Parser Mode](#) (required if not using EMM)
- [Installing Scripts Using EMM](#) (required if not using tclsh)
- [Deploying the CFM Shut Script Using tclsh CLI Parser Mode](#) (required if not using EMM)
- [Deploying the CFM Unshut Script Using tclsh CLI Parser Mode](#) (required if not using EMM)
- [Deploying the CFM Autotrace Script Using tclsh CLI Parser Mode](#) (required if not using EMM)
- [Deploying the CFM CC Timeout Using tclsh CLI Parser Mode](#) (required if not using EMM)
- [Deploying the CFM OnDemand Script Using tclsh CLI Parser Mode](#) (required if not using EMM)
- [Deploying Scenarios Using EMM](#) (required if not using tclsh)
- [Displaying Status Using tclsh Scripts](#) (required if not using EMM)
- [Displaying Status Using EMM](#) (required if not using tclsh)
- [Removing Scenarios Using tclsh CLI Parser Mode](#) (required if not using EMM)

- [Removing Scenarios Using EMM](#) (required if not using tclsh)

Installing Scripts Using tclsh CLI Parser Mode

Perform this task to install scripts using tclsh CLI parser mode.

Summary Steps

1. Download the diagnostic scripts.
2. Unzip the scenario archive.
3. **enable**
4. **mkdir** directory
5. **copy** [/erase] source-url destination-url
6. **mkdir** directory
7. **copy** [/erase] source-url destination-url

Table 1. Detailed Steps

	Command or Action	Purpose
Step 1	Download the diagnostic scripts to your UNIX or Windows-based workstation from CCO at: http://www.cisco.com/go/iossd The scripts will be posted after running on the official CFM 8.1 image.	You need these scripts to facilitate diagnosing common networking issues in the CFM for Cisco Carrier Ethernet OAM. Scripts will be organized into diagnostic scenarios. For example, sdiag_cfm_2.02.zip.
Step 2	Unzip the scenario archive.	Retrieves each diagnostic scenario.
Step 3	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 4	mkdir <i>directory</i> Example: device# mkdir svc-diag	Creates a directory (chosen by you) on the device to store the diagnostic scripts that you will be using as a part of this feature.
Step 5	copy <i>source-url destination-url</i> Example: device# copy tftp disk0:/svc-diag	Copies the policy scripts to the device's directory that you created in Step 4. The device will prompt for the following information: <ul style="list-style-type: none"> • Address or name of remote host. • Source filename. Give the full path where the script has to be copied from. • Destination filename. Give the full path where the script should be copied to (for example, disk0:/svc-diag/filename.tcl). Note: The storage location, in this case disk0, depends on the storage in the device. The storage can be disk, bootflash, or flash. The following files should be copied to the svc-diag directory: <ul style="list-style-type: none"> • cfm_autotrace.tcl • cfm_cctimeout.tcl • cfm_ondemand.tcl • cfm_shut.tcl • cfm_unshut.tcl • cfmod.tcl • collectEmailParameters.tcl • sdiag_cfm_display.tcl • sdiag_cfm_undeploy.tcl • sdiag_cfm.tcl
Step 6	mkdir <i>directory</i> Example: device# mkdir user-library	Creates a place on the device to store the user libraries and email template. You choose the name of the library.
Step 7	copy <i>source-url destination-url</i> Example: device# copy tftp disk0:/user-library	Copies the library scripts to the device's directory that you created in Step 6. The device will prompt for the following information: <ul style="list-style-type: none"> • Address or name of remote host.

	Command or Action	Purpose
		<ul style="list-style-type: none"> Source filename. Give the full path where the script has to be copied from. Destination filename. Give the full path where the script should be copied to (for example, disk0:/user-library/filename.tcl). <p>Note: The storage location, in this case disk0, depends on the storage in the device. The storage can be disk, bootflash, or flash. The following files should be copied to the user-library directory:</p> <ul style="list-style-type: none"> cfm_lib.tcl diag_lib.tcl email_template_cmd lib.tcl lib_2.tcl tclIndex userlib.tcl userlib_2.tcl <p>Note: The Diagnostic Tcl scripts posted on CCO will be digitally signed. If your Cisco IOS device image supports Tcl script signing, you may use this feature to verify the integrity of the downloaded scripts. For more information, see the Signed Tcl Scripts topic here: http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/m_signed_tcl.html</p>

Installing Scripts Using EMM

If your image has the EMM feature, it is much easier to use the MDF rather than the ZIP file. Perform this task to install scripts using EMM.

Summary Steps

1. Download the MDF.
2. **enable**
3. **mkdir** *directory*
4. **mkdir** *directory*
5. **emm mdf** *mdf-url*
6. Select menu option 1 to install the scripts.

Table 2. Detailed Steps

	Command or Action	Purpose
Step 1	Download the MDF containing the diagnostic scripts from CCO: http://www.cisco.com/go/iossd For example: cfm.mdf.	The MDF contains all the scripts and policy files needed for a scenario. It is like a ZIP file in that respect, but also contains menu definitions to guide the user. You download cfm.mdf to a location of your choosing.
Step 2	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 3	mkdir <i>directory</i> Example: device# mkdir svc-diag	Creates a directory (chosen by you) on the device to store the diagnostic scripts that EMM will be using as a part of this feature.
Step 4	mkdir <i>directory</i> Example: device# mkdir user-library	Creates a place on the device where EMM will store the user libraries and email template. You choose the name of the library.
Step 5	emm mdf <i>mdf-url</i> Example: device# emm mdf tftp://172.16.0.0/gmokashi/cfm.mdf	Launches EMM. The MDF will query the device's available file systems and present a default directory that has sufficient free space to contain the diagnostic scripts and policies. The <i>mdf-url</i> is the location that you chose in Step 1 to store cfm.mdf when you downloaded it from CCO.
Step 6	Select menu option 1 to install the scripts.	Prompts you for the directory where you want to store the CFM diagnostic policies. You would choose the directory that you created

		in Step 3. Also, prompts you for the directory where you want to store the user library files. You would choose the <i>directory</i> that you created in Step 4.
--	--	--

Examples

```
device# emm mdf tftp://172.16.0.0 /gmokashi/cfm.mdf
=====
Connectivity Fault Management Diagnostics

Enter ? for help or ?# for item help
-----
-----
1. Install Diagnostic Scripts
2. Set Global Variables (email parameters)
3. Deploy CFM Scenarios
4. Display Registered Policies
5. Display Environment Variables
6. Remove Diagnostic Policies
7. Exit

Enter selection [7]:

Press the number 1 key. (No Enter key is needed.) You will be prompted for
directories for the EEM user library and user policies as follows:

Enter ? for help

Enter a directory to store the CFM diagnostic policies in the form of a URL
(excluding filename, e.g. disk0:/svc-diag

Enter value [disk0:/svc-diag]:

Enter ? for help

Enter a directory for the user library files in the form of a URL (excluding
filename, e.g. disk0:/user-library

Enter value [disk0:/user-library]:
```

Deploying the CFM Shut Script Using tclsh CLI Parser Mode

The CFM shut script (cfm_shut.tcl) detects and reacts to network failures that break connectivity of a point-to-point Layer 2 Ethernet service. It is targeted for point-to-point environments with non-Ethernet Load Management Interface (ELMI) Carrier Ethernets (CEs) in order to reduce CE blackholing of traffic when remote User to Network Interface (UNI) failures occur. The CFM shut script works by performing a shutdown of the UNI interface associated with an Up MEP.

Perform this task to deploy the CFM shut script using tclsh CLI parser mode.

Restrictions

The CFM shut script should be executed only when the following criteria are met:

- Point-to-point services (no multipoint services) exist.
- Target interface has an Up MEP (no Down MEP).

- No service multiplexing on the target interface exists. (Multiple services on the target interface are not recommended).

Note: `cfm_shut.tcl` should be used only when the above conditions are met.

Summary Steps

1. **enable**
2. **tclsh** *storage-type#:/directory/sdiag_cfm.tcl cfm_shut.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library ma-list p2p*

Table 3. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: <code>device> enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	tclsh <i>storage-type#:/directory/sdiag_cfm.tcl cfm_shut.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library ma-list p2p</i> Example: <code>device# tclsh disk0:/svc-diag/sdiag_cfm.tcl cfm_shut.tcl email TRUE TRUE TRUE TRUE disk0:/svc-diag disk0:/user-library disk0:/svc-diag/ma_list.txt TRUE</code>	Runs the CFM shut script where: <ul style="list-style-type: none"> • You have the option of choosing either disk, flash or bootflash for the <i>storage-type#</i>. In the example, disk0 has been chosen. • <i>directory</i> is the directory you created for the diagnostic scripts. • <i>sdiag_cfm.tcl</i> is the registration script. • <i>cfm_shut.tcl</i> is the EEM policy script. • Notification is email. • Configuration history is set to TRUE. • Event history is set to TRUE. • Command history is set to TRUE. • Prepend is set to TRUE. • User policy directory is <code>disk0:/svc-diag</code>. • User library directory is <code>disk0:/user-library</code>. • MA list file is <code>disk0:/svc-diag/ma_list.txt</code>. • P2P flag is TRUE.

Examples

After the script is triggered, the local interface corresponding to the vlan xxx MA name xxx domain xxx will be shut down.

The sample notification message that is sent as a result of CFM shut script execution is:

```
SERV-DIAG_CFM_shut: Service failure detected on vlan 104, CFM MD D5. Reason: Remote MEP timeout. Action: Interface Fa0/10 with local MEP 1071 has been shutdown.
```

Troubleshooting Tips

You might get a syslog message on the device indicating that the remote CFM port state is going from Up to Down state. The reasons could be:

- The remote UNI interface is down.
- The network is down.

Examples of detailed syslog messages are as follows:

- `%E_CFM-6-REMOTE_MEP_UP`: Continuity Check message is received from a remote MEP with mpid * vlan * MA name * domain * interface status Down event code PortState
- `%E_CFM-3-REMOTE_MEP_DOWN`: Remote MEP mpid * vlan * MA name * in domain * changed state to down with event code TimeOut

Note: The * in the above examples indicates corresponding values for each variable.

Deploying the CFM Unshut Script Using tclsh CLI Parser Mode

Perform this task to deploy the CFM unshut script using tclsh CLI parser mode. This script performs network recovery when the remote MEP port state is changed to Up. Only the ports shut down by the Shut scripts will be unshut.

Summary Steps

1. **enable**
2. **tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_unshut.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library**

Table 4. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_unshut.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library Example: device# tclsh disk0:/svc-diag/sdiag_cfm.tcl cfm_unshut.tcl email TRUE TRUE TRUE TRUE disk0:/svc-diag disk0:/user-library	Runs the CFM shut script where: <ul style="list-style-type: none"> • You have the option of choosing either disk, flash or bootflash for the <i>storage-type#</i>. In the example, disk0 has been chosen. • <i>directory</i> is the directory you created for the diagnostic scripts. • <i>sdiag_cfm.tcl</i> is the registration script. • <i>cfm_shut.tcl</i> is the EEM policy script. • Notification is email. • Configuration history is set to TRUE. • Event history is set to TRUE. • Command history is set to TRUE. • Prepend is set to TRUE. • User policy directory is disk0:/svc-diag. • User library directory is disk0:/user-library.

Examples

After the script is triggered, the local interface corresponding to the vlan xxx MA name xxx domain xxx will be unshut.

A sample notification message that is sent as a result of CFM unshut script execution:

```
SERV-DIAG_CFM_unshut: Service recovery detected on vlan 103, CFM MD D6. Reason:
Remote MEP reachable. Action: Interface Fa0/7 with local MEP mpid 1052 has been
unshut.
```

Troubleshooting Tips

You may receive a syslog message on the device indicating that the remote CFM port state has changed to the Up state. The reasons could be:

- The network is up.
- The remote UNI port state goes from Down to Up (New).
- The remote UNI port state goes from Down to Up (Returning).
- The remote UNI port state goes from AdmDn to Up (New).
- The remote UNI port state goes from AdmDn to Up (Returning).

Examples of the trigger syslog messages for the CFM shut script are as follows:

- %E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from a remote MEP with mpid vlan MA name domain interface status Up event code PortState
- %E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from a remote MEP with mpid vlan MA name domain interface status Up event code New

- %E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from a remote MEP with mpid vlan MA name domain interface status Up event code Returning
- %E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from a remote MEP with mpid vlan MA name domain interface status AdmDn event code Returning
- %E_CFM-6-REMOTE_MEP_UP: Continuity Check message is received from a remote MEP with mpid vlan MA name domain interface status AdmDn event code New

Note: The above examples are not the real syslog messages. They are missing the MA name, domain name, and so on.

Deploying the CFM Autotrace Script Using tclsh CLI Parser Mode

The script automatically starts and records the result of a traceroute operation upon timer expiration based on a user-specified MA list. The relevancy of the script is to try to keep the CFM traceroute cache as up-to-date as possible.

Perform this task to deploy the CFM autotrace script using tclsh CLI parser mode.

Restrictions

This script will be triggered by the autotrace timer (in minutes) specified by you.

Specifications for the autotrace timer:

- Default value is 360 minutes.
- Minimum value is 60 minutes.
- Traceroute cache hold-timer $\geq n * \text{auto-trace timer}$ where $n \geq 1$, $n = 1.5$ recommended.

Summary Steps

1. **enable**
2. **tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_autotrace.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library ma-list timer**

Table 5. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_autotrace.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library ma-list timer Example: device# tclsh disk0:/svc-diag/sdiag_cfm.tcl cfm_autotrace.tcl email TRUE TRUE disk0:/svc-diag disk0:/user-library disk0:/svc-diag/ma_list.txt 120	Runs the CFM shut script where: <ul style="list-style-type: none"> • You have the option of choosing either disk, flash or bootflash for the <i>storage-type#</i>. In the example, disk0 has been chosen. • <i>directory</i> is the directory you created for the diagnostic scripts. • <i>sdiag_cfm.tcl</i> is the registration script. • <i>cfm_autotrace.tcl</i> is the EEM policy script. Notification is email. • Configuration history is set to TRUE. • Event history is set to TRUE. • Command history option is set to TRUE. • Prepend is set to TRUE. • User policy directory is disk0:/svc-diag. • User library directory is disk0:/user-library. • MA list file is disk0:/svc-diag/ma_list.txt. • Timer value is 120 minutes.

Examples

When triggered by the autotrace timer specified by you, the script performs the following actions:

- Retrieves a list of MAs from the MA list file.
- Retrieves a list of domains based on the MA list.
- Retrieves all MEP IDs based on domains and the MA list.
- Performs traceroute on all MEP IDs in each domain and MA list.
- Generates summary and detailed autotrace report.

Sample notification message that is sent as a result of CFM unshut script execution:

```
SERV-DIAG_CFM_autotrace: A total of 4 MEPS for valid MAs specified in
flash:/cfm/ma_list.txt have been automatically tracerouted. Results stored in the
CFM traceroute cache.
```

```
CFM Domain D6
  MA MA3-L6-103 - vlan 103
    mpid 1052, mac address 0024.50e1.8e00
    mpid 1054, mac address 0024.50e1.8e00
CFM Domain D5
  MA MA4-L5-105 - vlan 105
    mpid 1071, mac address 0024.50e1.8e00
```

Deploying the CFM CC Timeout Using tclsh CLI Parser Mode

The CFM CC timeout script provides the capability to diagnose and attempts to isolate the location of network failures that break connectivity of Layer 2 Ethernet service as detected by the CFM Continuity Check (CC) protocol.

Perform this task to deploy the CFM CC timeout script using tclsh CLI parser mode.

Summary Steps

1. **enable**
2. **tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_cctimeout.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library ma-list**

Table 6. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_cctimeout.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library ma-list Example: device# tclsh disk0:/svc-diag/sdiag_cfm.tcl cfm_cctimeout.tcl email FALSE FALSE FALSE FALSE disk0:/svc-diag disk0:/user-library disk0:/svc-diag/ma_list.txt	Runs the CFM shut script where: <ul style="list-style-type: none"> • You have the option of choosing either disk, flash or bootflash for the <i>storage-type#</i>. In the example, disk0 has been chosen. • <i>directory</i> is the directory you created for the diagnostic scripts. • <i>sdiag_cfm.tcl</i> is the registration script. • <i>cfm_cctimeout.tcl</i> is the EEM policy script. • Notification is syslog and email. • Configuration history is set to FALSE. • Event history is set to FALSE. • Command history option is set to FALSE. • Prepend is set to FALSE. • User policy directory is disk0:/svc-diag. • User library directory is disk0:/user-library. • MA list file is disk0:/svc-diag/ma_list.txt.

Examples

When triggered, the script performs the following actions:

- Inspects the CFM Continuity Check Database (CCDB) to verify if the failure is persistent or transient. If persistent, the remote MEP should NOT be present in the CCDB. If transient, an entry will be present and the script collects the information available from the remote MEPs in the entry.
- Inspects and captures the associated entry or entries found in the CFM errorDB. Executes **show ethernet cfm errors domain-id domain-name service ma-name**. Parses the output to look for entries with the Remote MEP MPID parsed from the syslog. If an entry with matching remote MEP-ID is found, the script saves the remote MEP's MAC address and corresponding error reason code for each matching entry. Here we are looking for a "Lifetime Timer Expired" as the reason for a persistent failure.
- Performs fault and connectivity verification by executing **ping ethernet mac-addr domain domain-name vlan svlan-id**.
- Performs path discovery/fault isolation by using the CFM linktrace protocol. Executes the **traceroute ethernet mac-addr domain domain-name vlan svlan-id** command.
- Generates summary and detailed CC timeout report.

Sample notification message that is sent as a result of CFM CC timeout execution:

```
SERV-DIAG_CFM_timeout: Diagnostics for rmep 0024.50e1.8e00 on vlan 103, CFM MD
D6.CCDB: 0 found; ErrorDB: 3 found; Reasons: RxAIS, RxRDI, Timeout; Ping: fail;
Trace: fail
```

DETAILED MESSAGE:

```
Diagnostics for rmep 0024.50e1.8e00 on vlan 103, CFM MD D6, level = 6 ;
```

```
Details of remote MEP was not found in CCDB.
```

```
Details of remote MEP collected from Error DB.
```

```
MEP ID - 1052
```

```
MAC Address - 0023.aca1.3700
```

```
Reason - "Receive AIS"
```

```
MEP ID - 1052
```

```
MAC Address - 0024.50e1.8e00
```

```
Reason - "Lifetime Timer Expired"
```

```
MEP ID - 1052
```

```
MAC Address - 0024.50e1.8e00
```

```
Reason - "Receive RDI"
```

```
Output of loopback operation performed to remote MEP:      Ping to "0024.50e1.8e00"
failed.
```

```
Output from Traceroute operation to remote MEP: Traceroute failed.
```

TRACEROUTE OUTPUT:

```
Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds Tracing the
route to 0024.50e1.8e00 on Domain D6, Level 6, vlan 103 Path to 0024.50e1.8e00 via
FastEthernet0/3 is down. Traceroute terminated.
```

Troubleshooting Tips

The trigger for action is a CFM syslog message raised when a remote MEP has expired from CCM DB.

The trigger syslog message is:

```
%E_CFM-3-REMOTE_MEP_DOWN: Remote MEP mpid vlan MA name in domain changed state to down with event code TimeOut
```

Note: The above example is missing the actual values for MA name, domain name, and so on.

Deploying the CFM OnDemand Script Using tclsh CLI Parser Mode

The script is used to perform troubleshooting and collect information regarding the service associated with a given CFM Maintenance Association (MA) name or Maintenance Association End Point <MEP, MA> combination. The trigger will be done manually with you providing the desired domain name, MA name and optionally a remote MEPID.

Perform this task to deploy the CFM OnDemand script using tclsh CLI parser mode.

Summary Steps

1. **enable**
2. **tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_ondemand.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library domain-name ma-name optional-mep-id**

Table 7. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	tclsh storage-type#:/directory/sdiag_cfm.tcl cfm_ondemand.tcl notification configuration-history event-history command-history prepend-trigger-message directory-name my-library domain-name ma-name optional-mep-id Example: device# tclsh disk0:/svc-diag/sdiag_cfm.tcl cfm_ondemand.tcl email,snmp FALSE FALSE FALSE TRUE disk0:/svc-diag disk0:/user-library Domain1 MA-L6-104 [1024]	Runs the CC timeout script where: <ul style="list-style-type: none"> • You have the option of choosing either disk, flash or bootflash for the <i>storage-type#</i>. In the example, disk0 has been chosen. • <i>directory</i> is the directory you created for the diagnostic scripts. • <i>sdiag_cfm.tcl</i> is the registration script. • <i>cfm_ondemand.tcl</i> is the EEM policy script. • Notification is email and SNMP. • Configuration history option is set to FALSE. • Event history is set to FALSE. • Command history is set to FALSE. • Prepend is set to TRUE. • User policy directory is disk0:/svc-diag. • User library directory is disk0:/user-library. • Domain is Domain1. • MA is MA-L6-104. • MEP ID is 1024.

Examples

The script does the following:

- Inspects the CFM CCDB and collects the information available from the remote MEPs.
- Inspects and captures the entries found in the CFM errorDB.
- Performs fault and connectivity verification by executing **ping ethernet mac-addr domain domain-name vlan svlan-id**.
- Performs path discovery/fault isolation by using the CFM linktrace protocol. Executes the **traceroute ethernet mac-addr domain domain-name vlan svlan-id** command and inspects the CFM traceroute cache

(**show ethernet traceroute-cache**) in order to compare the last successful and recorded traceroute operation against the failed one.

Generates summary and detailed on demand reports.

Sample notification message that is sent as a result of CFM OnDemand script execution:

```
SERV-DIAG_CFM_ondemand: Diagnostics for rmep 0024.50e1.8e00 on vlan 103, CFM MD
D6.CCDB: 1 found, 1 with UP IF state; ErrorDB: 1 found; Reasons: RxRDI; Ping: pass;
Trace: pass
```

DETAILED MESSAGE:

```
Diagnostics for rmep 0024.50e1.8e00 on vlan 103, CFM MD D6, level = 6;
```

Details of remote MEP collected from CCDB:

MEP ID - 1052

MAC Address - 0024.50e1.8e00

Interface status - Up

Port status - Up

RDI state - TRUE

CC packet statistics - 7659/0(Received/Error)

Details of remote MEP collected from Error DB

MEP ID - 1052

MAC Address - 0024.50e1.8e00

Reason - "Receive RDI"

Output of loopback operation performed to remote MEP: Ping to "0024.50e1.8e00" was successful.

Output from Traceroute operation to remote MEP: Traceroute successful.

TRACEROUTE OUTPUT:

Type escape sequence to abort. TTL 64. Linktrace Timeout is 5 seconds Tracing the route to 0024.50e1.8e00 on Domain D6, Level 6, vlan 103 Traceroute sent via FastEthernet0/3, path found via MPDB.

B = Intermediary Bridge

! = Target Destination

* = Per hop Timeout

```
-----
              MAC      Ingress      Ingr Action  Relay Action
Hops  Host      Forwarded   Egress       Egr Action   Previous Hop
-----
! 1    3400-13    0024.50e1.8e00 Fa0/3      IngOk        RlyHit:MEP
              Not Forwarded                0023.aca1.3700
-----
```

Troubleshooting Tips

This script will be triggered on user demand by issuing the following command after `cfm_ondemand.tcl` is registered.

```
device# tclsh cfmmod.tcl ma-name domain-name -m mep-id -n notification
```

where

the **-m** and **-n** keywords are optional. The **-m** keyword is for the MEP ID. The **-n** keyword is for the notification method, whether it is snmp, email, and so on. This wrapper script is specifically designed and coded for the "on-demand" script, for your ease of use.

Deploying Scenarios Using EMM

Perform this task to deploy scenarios using EMM. You must first install the diagnostics scripts following the steps in [Installing Scripts Using EMM](#).

Summary Steps

1. **enable**
2. **emm mdf** *mdf-url*
3. Select menu item 2.
4. Answer questions regarding EEM variables.

Table 8. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	emm mdf <i>mdf-url</i> Example: device# emm mdf ftp://172.16.0.0/gmokashi/cfm.mdf	Launches EMM.
Step 3	Select menu item 2.	When using EMM for the first time, you need to select menu item 2. From there on, you can select any menu item. After you exit from a menu and relaunch EMM, you do not need to select item 1 and item 2 again. EMM will give an error whenever you select an incorrect item.
Step 4	Answer the questions regarding EEM environment variables, that is <code>_email_to</code> , <code>_email_server</code> , and so on.	You will be prompted for inputs one at a time.

Examples

1. After installation, select menu item 2 and answer the questions regarding EEM environment variables, for example: `_email_to`, `_email_server`, and so on.

```

=====
                          Connectivity Fault Management Diagnostics

                                     Enter ? for help or ?# for item help
-----
1. Install Diagnostic Scripts
2. Set Global Variables (email parameters)
3. Deploy CFM Scenarios
4. Display Registered Policies
5. Display Environment Variables
6. Remove Diagnostic Policies
7. Exit

Enter selection [7]:

```

2. After setting up the EEM environment, select menu item 3 to be presented with the following CFM deployment sub-menu:

```
=====
                          Connectivity Fault Management Scenario Deployment

                                          Enter ?# for item help
-----
1. Deploy CFM CC-Timeout Script
2. Deploy CFM On-Demand Script
3. Deploy Action Shut Script
4. Deploy CFM Action Unshut Script
5. Deploy CFM Action Auto Trace Script
6. Return to main CFM menu
```

Enter selection [6]:

3. Select the menu item corresponding to the desired diagnostics. You will be prompted for inputs one at a time. An example question is the type of notification desired:

Select the type of notification to be sent when a problem is diagnosed

- ```

1. Email Only
2. SNMP Only
3. Syslog Only
4. Email and Syslog
5. Email and SNMP
6. Syslog and SNMP
7. Email, Syslog, and SNMP
```

Enter choice:

If you select email reporting, you may add more information to the report, such as configuration change history:

Do you want to log configuration history?

- ```

1. Yes
2. No
```

Enter choice:

Displaying Status Using tclsh Scripts

Perform this task to display status using tclsh CLI parser mode.

Summary Steps

1. **enable**
2. **tclsh storage-type#:/directory/sdiag_cfm_display.tcl policy-name**

Table 9. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	tclsh <i>storage-type#:/directory/sdiag_cfm_display.tcl policy-name</i> Example: device# tclsh disk0:/svc-diag/sdiag_cfm_display.tcl cfm_shut.tcl	Displays the status where: <ul style="list-style-type: none"> You have the option of choosing either disk, flash or bootflash for the storage-type#. In the example, disk0 has been chosen. <i>directory</i> is the directory you created for the diagnostic scripts. Displays status where policy-name can be: <ul style="list-style-type: none"> cfm_autotrace.tcl cfm_cctimeout.tcl cfm_ondemand.tcl cfm_shut.tcl cfm_unshut.tcl

Examples

```
device# tclsh disk0:/svc_diag/sdiag_cfm_display.tcl cfm_shut.tcl
THE INPUTS GIVEN FOR CFM SHUT SCENARIO ARE:
Notification : SYSLOG,EMAIL
Configuration history option : FALSE
Event history option : FALSE
Command history option : TRUE
Prepend option : TRUE
MA File name is : disk0:/cfm/ma_list.txt
P2P service option : TRUE
```

Displaying Status Using EMM

Perform this task to display status using EMM.

Summary Steps

- enable**
- emm mdf mdf-url**
- Select the desired "Display" menu option (4 or 5)

Table 10. Detailed Steps

	Command or Action	Purpose
Step 1	enable Example: device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	emm mdf mdf-url Example: device# emm mdf ftp://172.16.0.0/gmokashi/cfm.mdf	Launches EMM. You need to launch EMM in order to display the parameter settings for the script.
Step 3	Select the desired "Display" menu option (4 or 5)	Displays parameter settings.

Examples

In the sample CFM MDF below, type the number 4 to display registered policies, and type the number 5 to display the inputs given by the user for a specific policy.

```
=====
```


Connectivity Fault Management Diagnostics

Enter ? for help or ?# for item help

- ```

```
1. Install Diagnostic Scripts
  2. Set Global Variables (email parameters)
  3. Deploy CFM Scenarios
  4. Display Registered Policies
  5. Display Environment Variables
  6. Remove Diagnostic Policies
  7. Exit

Enter selection [7]:

**Removing Scenarios Using tclsh CLI Parser Mode**

Perform this task to uninstall a policy script and all the inputs related to the policy using tclsh CLI parser mode.

## Summary Steps

1. **enable**
2. **tclsh storage-type#:/directory/sdiag\_cfm\_undeploy.tcl policy-name**

**Table 11.** Detailed Steps

|               | Command or Action                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>device> enable                                                                                                                            | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 2</b> | <b>tclsh</b><br><i>storage-type#:/directory/sdiag_cfm_undeploy.tcl policy-name</i><br><br><b>Example:</b><br>device# tclsh<br>disk0:/svc-diag/sdiag_cfm_undeploy.tcl cfm_shut.tcl | Uninstalls the policy script where: <ul style="list-style-type: none"> <li>• You have the option of choosing either disk, flash or bootflash for the <i>storage-type#</i>. In the example, disk0 has been chosen.</li> <li>• <i>directory</i> is the directory you created for the diagnostic scripts.</li> </ul> Uninstalls the policy script where policy-name can be: <ul style="list-style-type: none"> <li>• cfm_autotrace.tcl</li> <li>• cfm_cctimeout.tcl</li> <li>• cfm_ondemand.tcl</li> <li>• cfm_shut.tcl</li> <li>• cfm_unshut.tcl</li> </ul> |

## Examples

```
device# tclsh disk0:/svc-diag/sdiag_cfm_undeploy.tcl cfm_shut.tcl
```

```
cfm_shut.tcl is unregistered successfully
```

**Removing Scenarios Using EMM**

Perform this task to uninstall a policy script and all the inputs related to the policy using EMM.

## Summary Steps

1. **enable**
2. **emm mdf mdf-url**
3. Select the menu item entitled "Remove Diagnostic Policies."

**Table 12.** Detailed Steps

|               | Command or Action                                                                                         | Purpose                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>device> enable                                                    | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| <b>Step 2</b> | <b>emm mdf <i>mdf-url</i></b><br><br><b>Example:</b><br>device# emm mdf ftp://172.16.0.0/gmokashi/cfm.mdf | Launches EMM.                                                       |
| <b>Step 3</b> | Select the menu item entitled "Remove Diagnostic Policies."                                               | Do this to remove the scenarios.                                    |

### Examples

In the sample CFM MDF below, type the number 6.

```

=====
 Connectivity Fault Management Diagnostics

 Enter ? for help or ?# for item help

1. Install Diagnostic Scripts
2. Set Global Variables (email parameters)
3. Deploy CFM Scenarios
4. Display Registered Policies
5. Display Environment Variables
6. Remove Diagnostic Policies
7. Exit

Enter selection [7]:

```

### Configuration Examples for Service Diagnostics 2.0 CFM Scripts

There are no configuration examples for Service Diagnostics 2.0 CFM Scripts.

### Additional References

The following sections provide references related to the Service Diagnostics CFM Scripts feature.

**Table 13.** Related Documents

| Related Topic               | Document Title                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Embedded Menu Manager       | Cisco IOS and NX-OS Software Embedded Menu Manager<br><a href="http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_emm.html">http://www.cisco.com/en/US/docs/ios/netmgmt/configuration/guide/nm_emm.html</a>                                                                                                                                                                    |
| Service Diagnostics Phase 1 | Cisco IOS Service Diagnostics: Border Gateway Protocol, Open Shortest Path First and Quality of Service Scripts<br><a href="http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps9424/white_paper_cisco_ios_service_design_bgp_osp_qos.html">http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6555/ps9424/white_paper_cisco_ios_service_design_bgp_osp_qos.html</a> |

**Table 14.** Standards

| Standard                                                    | Title |
|-------------------------------------------------------------|-------|
| No new or modified standards are supported by this feature. | —     |

**Table 15.** MIBs

| MIB                                                                                                                    | MIBs Link                                                                                                                                                                                                              |
|------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| No new or modified MIBs are supported by this feature, and support for existing MIBs are not modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB locator found at the following URL:<br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**Table 16.** RFCs

| RFC                                                                                                                         | Title |
|-----------------------------------------------------------------------------------------------------------------------------|-------|
| No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature. | —     |

**Table 17.** Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Link                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.<br>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.<br>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. | <a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a> |

## Feature Information for the Service Diagnostics 2.0 CFM Scripts

Table 18 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note:** Table 18 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 18.** Feature Information for the Service Diagnostics 2.0 CFM Scripts

| Feature Name                        | Releases                     | Feature Information                                                                                                                                                      |
|-------------------------------------|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service Diagnostics 2.0 CFM Scripts | Cisco IOS Release 12.2(52)SE | Facilitates diagnosing common networking issues in Connectivity Fault Management (CFM) for the Cisco Carrier Ethernet Operations, Administration, and Maintenance (OAM). |

## Glossary

**CE**—Carrier Ethernet

**CFM**—Connectivity Fault Management

**CLI**—Command Line Interface

**EEM**—Embedded Event Manager

**ELMI**—Ethernet Local Management Interface

**EMM**—Embedded Menu Manager

**IOS**—Internetwork Operating System

**MA**—Maintenance Association

**MDF**—Menu Definition File

**MEP**—Maintenance Association End Point

**non-ELMI**—non-Ethernet Local Management Interface

**OAM**—Operations, Administration, and Maintenance

**syslog**—System log allows you to log significant system information to a remote server.

**Tcl**—Tool Command Language

**UNI**—User to Network Interface

**XML**—eXtensible Markup Language



Americas Headquarters  
Cisco Systems, Inc.  
San Jose, CA

Asia Pacific Headquarters  
Cisco Systems (USA) Pte. Ltd.  
Singapore

Europe Headquarters  
Cisco Systems International BV  
Amsterdam, The Netherlands

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](http://www.cisco.com/go/offices).

CCDE, CD (X), CDS, Cisco IaaS, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nexus Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, GGR, Flip Channels, Hio for Good, Hio Mind, HioShare (Design), Flip Ultra, Flip Video, Flip Video (Design), Indent Broadband, and We Come to the Human Network are trademarks. Changing the Way We Work, Live, Play and Learn, Cisco Capital, Cisco Capital (Design), Cisco Financial (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks, and Access Register, Altonet, All about AsyncOS, Bringing the Meeting to You, Catalyst, CCDA, CCDE, CCIE, CCIP, CCNA, CCNP, CDS, DCV, Giga, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumina, Cisco Nexus, Cisco Prime, Cisco Systems, Cisco Systems Global, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMore, I/YNX, IOS, iPhone, IronPort, the IronPort logo, LaserLink, LightStream, Linksys, MeetingPlace, MeetingPlace Online Sound, MGX, Networkers, Networking Academy, PCNow, PX, PowerKEY, PowerPanel, PowerTV, PowerTV (Design), PowerVu, Prism, ProConnect, ROSA, Boulder Edge, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. ©2009