Cisco Media Encapsulator 2.1

Installation and Configuration Guide

78-21051-02

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks.

Third party trademarks mentioned 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. (1110R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

Contents

About This Guide v

Install Encapsulator Software 7

Software Prerequisites 8
Cisco Media Encapsulator Application Installation 11

Feature Reference 15

SDT Feature 16
HLS Ad Insertion Support 19
SNMP 23

Appendix A Recommended Platform Configuration 26

Server Hardware 27
Hard Drive Configuration 28
Network Interface Configuration 29

Appendix B Maintenance Procedures 31

Transferring the Encapsulator File 32
Log File Procedure 33
Restart Procedures 34
Customer Support 35

Appendix B Common Linux Configurations 37

Ethernet and Static Route Configuration 38
DNS Configuration 42

About This Guide

Introduction

This guide provides installation and local configuration information for the Cisco Media Encapsulator. This document also refers to the product as the Encapsulator.

Purpose

This guide provides setup information and instructions for installing the Encapsulator software application. The Encapsulator is managed remotely by the Linear Stream Manager, and LSM is required for any Encapsulator deployment. Refer to the Cisco Linear Stream Manager Quick Start Guide for installation instructions, and see the Cisco Linear Stream Manager User Guide for channel configuration instructions. To view these documents, go to the following URL: http://www.cisco.com/en/US/customer/products/ps11787/tsd_products_support_series_home.html

Audience

This guide is written for field operations personnel who are responsible for installing and using Encapsulator software.

Required Skills and Expertise

System operators or engineers who install the Encapsulator software need the following skills:

- Knowledge of Linux
- An understanding of Network IP addresses

1

Install Encapsulator Software

Introduction

This chapter describes how to install the Encapsulator software on the system for the first time. This chapter also lists software prerequisites and instructions for how to install them.

Please review Appendix A, “Recommended Platform Configuration” prior to software installation.

In This Chapter

- Software Prerequisites..... 8
- Cisco Media Encapsulator Application Installation..... 11

Software Prerequisites

Certain software prerequisites must be installed to prepare the system for the installation of Cisco Media Encapsulator. All instructions assume you are running as root.

It is mandatory to use Red Hat Linux Version 5.8 for all new installations.

Please see vendor specific information for Red Hat operating system installation.

Note: A minimum of 250MB of available space is required for application installation.

Complete the following steps to modify operating system configuration before installing software prerequisites:

Step 1 Check all relevant Ethernet ports to make sure they are set to be operational on boot and parameters correctly set for the network configuration. Location: /etc/sysconfig/network-scripts/ifcfg-eth0, 1, etc. Ensure that onboot=yes for each port.

See “Ethernet and Static Route Configuration” on page 38 in Appendix C for additional details.

Step 2 Enter **iptables -F** to flush the IP table.

Step 3 Enter **chkconfig iptables off** to turn off IP Filters. Additional filtering rules can be added after installation, depending on deployment-specific security policies.

Step 4 Make sure ports 9200-9900 are not part of the local port range. To check the current range, enter **cat /proc/sys/net/ipv4/ip_local_port_range**. If the local port range overlaps 9200-9900 and must be changed, modify /etc/sysctl.conf using vi or another editor to add **net.ipv4.ip_local_port_range = 32000 65000**. Next, for changes to take effect, run the following command: **sysctl –p**.

Step 5 Disable the swap space to enable better system performance. To check the current configuration, enter **cat /etc/fstab**. Modify /etc/fstab using vi or another editor to comment out the swap entry. Insert a # at the beginning of the swap entry.

Step 6 Check to make sure that, if enabled, SELinux is set to “permissive” mode. Location: /etc/selinux/config. Ensure that SELINUX=permissive. A reboot of the

system will be required after this change. Note: If you have custom SELinux policies, you may want to use the semanage utility to manage your existing policy, rather than configuring permissive mode.

Step 7 Create a core file directory if it does not already exist. Application core files are written to the /var/core directory. Enter **mkdir /var/core.**

Step 8 Enter chmod 755 /var/core. Next, proceed to the Supplemental Software Installation section below.

Supplemental Software Installation

The following RPM packages are required prior to CME installation:

"tzdata-java" "2010o-1.el5.x86_64"\

"java-1.6.0-openjdk" "1.6.0.0-1.16.b17.el5.x86_64"\

"lm_sensors" "2.10.7-9.el5.x86_64"\

"net-snmp-libs" "5.3.2.2-9.el5_5.1.x86_64"\

"net-snmp" "5.3.2.2-9.el5_5.1.x86_64"\

"rsyslog" "4.6.5-0.x86_64"\

"mongo-10gen" "2.0.5-mongodb_1.x86_64"\

"mongo-10gen-server" "2.0.5-mongodb_1.x86_64"\

As a convenience, supplemental RPM files have been included with the installer.

Step 1 Locate the bin installer that you transferred to the server.

Step 2 Enter chmod 755 cisco-media-encapsulator-2.0.0-bXXX.bin

Step 3 Enter ./cisco-media-encapsulator-2.0.0-bXXX.bin

WARNINGS will be generated for any changes that have not been completed in previous steps. Ensure warnings are addressed prior to moving on with the installation. The installer will generate ERRORs indicating that there are requisite RPMs required before the Cisco Media Encapsulator application can be installed. Choose **No** to exit the installer, and follow the instruction below to install any missing requisite RPMs.

The RPMs and a sample install script will be extracted to the following directory:

/tmp/cme_installer_rpm

To install all prerequisite RPMs, run the following two commands:

1. cd /tmp/cme_installer_rpm
2. ./sample_rpm_install

Once the RPM install script has finished, proceed to the Cisco Media Encapsulator Installation and Upgrades section below to finish the application installation.

If any errors occur during the RPM install, you must manually correct any RPM dependencies before proceeding to the next section.

Cisco Media Encapsulator Application Installation

These instructions assume that you have already completed all steps to install software prerequisites from the Software Prerequisites section. It is also assumed that you have transferred the software image to the Encapsulator. See “Transferring the Encapsulator File” on page 32 for instructions.

Before You Begin

For HSS configurations, it is recommended to include the following entry in the *.isml file during publishing point provisioning:

<meta name="restartOnEncoderReconnect" content="True" />

If this entry is not added, you will be required to manually shut down and start the publishing points after the Encapsulator upgrade for Microsoft IIS origins.

Transfer the Encapsulator File

See Transferring the Encapsulator File on page 32 for information on transferring the software image to the Encapsulator.

Installing the Cisco Media Encapsulator Application

Locate the bin installation and change the file permissions if this step was not already completed during the software prerequisite steps.

Step 1 Enter chmod 755 cisco-media-encapsulator-2.0.0-bXXX.bin

Step 2 Enter ./cisco-media-encapsulator-2.0.0-bXXX.bin

If there are any WARNINGS or ERRORs during prerequisite checks, the installer will advise to you to correct them prior to continuing with installation.

Step 3 If all prerequisites are met, the installer will continue installing the Encapsulator application. You will see the following message after upgrade:

CME Upgrade Completed Successfully! Installer log is available at /var/log/cme/install.log.

After installation completes, proceed to the Verifying Successful Application Installation procedure.

Verifying Successful Application Installation

If no WARNINGS are ERRORs were generated during the installation, the Cisco Media Encapsulator application will start automatically.

To verify that the application has been installed and is running, enter the following command:

service cmed status

Example output:

ChannelManager (pid 30961) is running...

For new installations, return to the Cisco Linear Stream Manager Quick Start Guide to set up the Cisco Media Encapsulator as a managed resource. The Quick Start Guide and additional documentation can be found at: http://www.cisco.com/en/US/customer/products/ps11787/tsd_products_support_series_home.html.

2

Feature Reference

Introduction

This chapter provides reference information for Encapsulator features. These features are configured locally on the Encapsulator server and not managed by the Linear Stream Manager.

In This Chapter

- SDT Feature 16
- HLS Ad Insertion Support 1916
- SNMP 23

SDT Feature

The DVB standard for Service Description Table as part of the Service Information tables provides a way for a MPEG video transport stream to identify its content using values in a string format. This can be used by service operators to provide a "bread crumbing" functionality, so that each packet of a stream can be inspected to identify through which nodes on the network that particular packet has passed. It also provides a mechanism for fault isolation of problematic streams.

SDT Functionality

This feature of the Cisco Media Encapsulator assumes that the service operator will use the SDT standard for bread crumbing in the following way:

1. Video streams which have SDT enabled include SDT information on MPEG PID 0x11. There is no minimum or maximum amount of time between the arrival of TS packets containing SDT information.
2. The SDT access unit will include the Service Descriptor descriptor, as specified by the DVB SDT standard. This will contain a string in the service_name field, which needs to be parsed and cached, to later be passed on to the network node adjacent and downstream from the Encapsulator which understands this relayed information.
3. Each SDT-supporting node that each packet passes through on the network will append its own unique identifier to the existing SDT service_name information. The delimiter between different unique identifiers within the SDT information of one SDT access unit will be the pipe ("|") character.
4. In this release, each SDT access unit is restricted to data contained within a single MPEG TS cell on the transport stream, even though the DVB standard says the SDT section may be up to 1024 bytes. If the incoming SDT data exceeds a single TS cell, it will be silently truncated to the data contained within the first TS cell (188 bytes).
5. The service operator will have tools that can read the SDT information from a stream

and aid in troubleshooting.

6 The end-user video clients may receive the Fragmenter Information box (containing the SDT data). Therefore, no sensitive information regarding the internal setup of the service operator's network should be included in the SDT data or unique identifier.

7 This feature is only currently supported for HSS (Microsoft Smooth) outputs.

SDT Unique Identifier Configuration

In order to manually specify the value of the Encapsulator's unique identifier (to be included in the SDT ISO BMFF box), the XML parameter with key **UniqueId** can be included in the cme_config.xml configuration file.

Example configuration entry:

```
<parameter key="UniqueId">fragmenter-id</parameter>
```

This parameter has a maximum length of 255 characters, and may contain any UTF-8 character that is valid in an XML string. If the parameter exceeds the maximum length of 255 characters, an error message will be printed in the CME log, and only the first 255 characters will be used. If this parameter is not specified or contains invalid characters, then by default the hostname of the Encapsulator system will be used as the value of the unique identifier. It should be noted that, in a multiple Encapsulator environment, it is up to the user to configure each Encapsulator with a unique identifier that is not used by any other Encapsulator in the environment.

SDT Modes

There are three modes of operation for the SDT feature: "off", "auto", and "on", as described below:

- **OFF mode**: the Encapsulator's publisher will never send the FragmenterId box

(the box that normally contains the information received from SDT, as well as the local Encapsulator's uniqueId).

- **ON mode**: the Encapsulator's publisher will always send the FragmenterId box, and this box will always contain the uniqueId, but only contain the information received from SDT if SDT has been received on the incoming stream; otherwise this SDT information field in the box will simply be an empty string.
- **AUTO mode**: the Encapsulator's publisher will only send the FragmenterId box in the event that the CME has found SDT information which contains valid and non-empty service_name information on the incoming stream. In the case that the incoming stream has no SDT information that contains a valid and non-empty service_name field, then the Encapsulator publisher will not send the FragmenterId box.

The XML parameter with key **SDTMode** must also be included in the cme_config.xml configuration file.

Example configuration entry:

```
<parameter key="SDTMode">on</parameter>
```

This parameter may have values of "on", "auto", or "off", and is not case-sensitive. If this parameter is not specified, it will default to "off" and the SDT feature will be disabled.

HLS Ad Insertion Support

Ad Marker Templates

In its current form, the Event Signaling and Management API specifies how an ABR packager may call out to an external Placement Opportunity Insertion Server (POIS) for each SCTE-35 marker the packager receives. In response, the POIS returns format-specific (i.e. HSS, HLS, HDS) data to be incorporated by the packager into the desired output format. For example, for HLS the POIS would respond with additional tags to add to an HLS playlist.

In most cases, the mapping from SCTE-35 to format-specific data is deterministic and does not require information beyond what is already carried by the SCTE-35 marker. In this case, the packager may be able to make the translation itself, given a set of well-defined per-format templates. For this set of deterministic responses, the call to the ESAM API is therefore optional.

This document describes the mapping from SCTE-35 to per-format data. For HLS, both a template and a description of how to transform an SCTE-35 into that template are provided.

If desired, the encapsulator may choose to perform the transformation as described in lieu of making a callout to the ESAM API.

ESAM Template Configuration

To enable ESAM, the /usr/local/cisco/conf/cme_config.xml file must be updated, setting the name of the ESAMTemplate parameter to the path of the ESAM Template File. The ESAM Template file contains a parameterized version of a simulated response from an ESAM server. The parameters in the template will be substituted with the corresponding values from the SCTE-35 marker, producing the ESAM response used to condition the

content. A sample template file is provided below.

The Cisco Media Encapsulator supports dynamic ad replacement by third party APIs. CableLabs Event Signaling and Management (ESAM) is one such API, and mDialog is also supported with a different API. To enable mDialog support, the "Include Cue Points" option must be enabled in the LSM HLS Output configuration page.

If both mDialog and ESAM are enabled, the ESAM support will take priority.

Apple HLS

For HLS, tags will be added to the HLS stream playlist for each segment within the duration of an ad break. The tags will include a subset of information found in the template XML file. The #EXT-X-ADSTART tag will be placed just before the first segment within the ad break while the #EXT-X-ADEND will be placed just before the first segment after the end of the ad break. All segments in between will be labeled with #EXT-X-ADSPAN tags. All tags include the UPID from the SCTE-35 marker. Additionally, the #EXT-X-ADSPAN tag includes the TimeFromSignal, indicating the elapsed time from the beginning of the avail (as indicated by the StreamTime element). The TimeFromSignal is expressed in decimal units of seconds.

Splice Insert Tags

First Segment:

```
#EXT-X-ADSTART:UPID="$startSignal$"

#EXT-X-DISCONTINUITY
```

Span Segment:

```
#EXT-X-ADSPAN:UPID="$startSignal$"TimeFromSignal=...
```

End Segment:

```
#EXT-X-ADEND:UPID="$endSignal$"

#EXT-X-DISCONTINUITY
```

Template Format

The packager will accept an ESAM template file which defines the template ad marker for each output format. The format of this template will be equivalent to that of the ESAM ManifestConfirmConditionNotification. Within the template, a few variables are defined, delimited by the '$' character. These include:

1. *acquisitionPointIdentity* – configured on the packager/JITP
2. *acquisitionSignalID* – randomly generated per signal
3. *signalPointID* –extracted from segmentation_upid in SCTE-35 Segmentation Descriptor
4. *startSignal* – signalPointID of OUT SCTE-35 marker
5. *endSignal* – signalPointID of IN SCTE-35 marker
6. *duration* – extracted from segmentation_duration in SCTE-35 Segmentation Descriptor

Note: the ${*timeFromSignal*} macro is not actually a template variable. Instead, this string is passed as-is to the HLS publisher, which then substitutes the elapsed ad break time so far, as specified above.

An example template file is shown below:

```
<ManifestConfirmConditionNotification>
<ManifestResponse acquisitionPointIdentity="$acquisitionPointIdentity$"
    acquisitionSignalID="$acquisitionSignalID$"
    signalPointID="$signalPointID$" duration="$duration$" dataPassThrough="false">
    <SegmentModify>
        <FirstSegment>
            <Tag locality="before" value="#EXT-X-DISCONTINUITY"/>
            <Tag locality="before"
                value="#EXT-X-ADSTART:UPID=$startSignal$"/>
        </FirstSegment>
        <SpanSegment>
            <Tag adapt="true"
                value="#EXT-X-ADSPAN:UPID=$startSignal$,TimeFromSignalStart=
               ${timeFromSignal}"
            />
        </SpanSegment>
        <LastSegment>
            <Tag locality="before"
                value="#EXT-X-ADEND:UPID=$endSignal$"/>
            <Tag locality="before" value="#EXT-X-DISCONTINUITY"/>
        </LastSegment>
```

```
    </SegmentModify>
</ManifestResponse>
</ManifestConfirmConditionNotification>
```

SNMP

On a Cisco Media Encapsulator, the SNMP MIB file can be found at:

/usr/share/snmp/mibs/INLET-VIDEO-ENCODER-MIB.my

Target trap destinations are stored at:

/etc/rsyslog.conf

TrapName	OID	Encapsulator Alarm
inletTrapCPUHigh	1.3.6.1.4.1.27265.71.21.1.9	CPU High
inletTrapMemoryLow	1.3.6.1.4.1.27265.71.21.1.10	Memory High
inletTrapDiskLow	1.3.6.1.4.1.27265.71.21.1.11	Disk Usage High
inletTrapEthernetOutputStateChange	1.3.6.1.4.1.27265.71.21.1.2	Ethernet Down
inletTrapInputUnderflow	1.3.6.1.4.1.27265.71.21.1.20	InputUnderflowAlarm
inletTrapInputOverflow	1.3.6.1.4.1.27265.71.21.1.21	InputOverflowAlarm
inletTrapOutputOverflow	1.3.6.1.4.1.27265.71.21.1.22	OutputOverflowAlarm
inletTrapPrimaryOutputFail	1.3.6.1.4.1.27265.71.21.1.23	PrimaryOutputNotConnected
inletTrapSecondaryOutputFail	1.3.6.1.4.1.27265.71.21.1.24	SecondaryOutputNotConnected
inletTrapSegmentationDuration	1.3.6.1.4.1.27265.71.21.1.25	Segment Duration
inletTrapChannelExited	1.3.6.1.4.1.27265.71.21.1.26	ChannelExitedAlarm
inletTrapContinuityCount	1.3.6.1.4.1.27265.71.21.1.27	TR101-290 Continuity Count Error
inletTrapPID	1.3.6.1.4.1.27265.71.21.1.28	TR101-290 PID Error
inletTrapPCR	1.3.6.1.4.1.27265.71.21.1.29	TR101-290 PCR Error

TrapName	OID	Encapsulator Alarm
inletTrapPTS	1.3.6.1.4.1.27265.71.21.1.30	TR101-290 PTS Error
inletTrapSyncByte	1.3.6.1.4.1.27265.71.21.1.31	TR101-290 Sync Byte Error
inletTrapTransportError	1.3.6.1.4.1.27265.71.21.1.32	TR101-290 Transport Error
inletTrapCRC	1.3.6.1.4.1.27265.71.21.1.33	TR101-290 CRC Error
inletTrapPAT	1.3.6.1.4.1.27265.71.21.1.34	TR101-290 PAT Error
inletTrapPMT	1.3.6.1.4.1.27265.71.21.1.35	TR101-290 PMT Error
inletTrapCAT	1.3.6.1.4.1.27265.71.21.1.36	TR101-290 CAT Error

A

Recommended Platform Configuration

In This Appendix

- Server Hardware 27
- Hard Drive Configuration 28
- Network Interface Configuration 29

This appendix provides the recommended platform configuration for Cisco Media Encapsulator.

Server Hardware

Please see the below for recommended blade and rack mount server configurations.

UCS B Series (blade)

Product Part Number	Description	Quantity
UCSB-B200-M3-U	UCS B200 M3 Blade Server	1
UCS-CPU-E5-2665	2.40 GHz E5-2665 processor	2
UCS-MR-1X082RY-A	8GB DDR3-1600-MHz	16
A03-D300GA2	300GB 6Gb SAS 10K	2
UCSB-MLOM-40G-01	VIC 1240 modular LOM for M3 blade servers	1

UCS C Series (1RU rack mount)

Product Part Number	Description	Quantity
UCSC-C220-M3S	UCS C220 M3 1RU Server	1
UCS-CPU-E5-2665	2.40 GHz E5-2665 processor	2
UCS-MR-1X082RY-A	8GB DDR3-1600-MHz	16
A03-D300GA2	300GB 6Gb SAS 10K	2
UCSC-RAID-11-C220	RAID SAS Card for C220 (0/1/10/5/50)	1
UCSC-PSU-650W	650W power supply	2

Also, for C Series only, choose one of the following network adapters, depending on deploy requirements.

UCSC-PCIE-IRJ45 Quad Port 1Gb NIC Adapter

OR

UCSC-PCIE-ITG Intel X540 Dual Port 10GBase-T Adapter

Contact your Cisco representative for hardware inquiries that fall outside the above recommended hardware configurations.

Hard Drive Configuration

Encapsulator logs and core files will be written to the following two directories. It is recommended to configure each in a separate partition.

Files	Directory	Recommended Partition size
Application log files	/var/log	20 Gb or greater
Application core files	/var/core	5 Gb or greater

Network Interface Configuration

It is recommended to configure a separate network interface for Input, Output, and Management.

Interface Number	Description	Usage
Interface 1	Management	Control of Encapsulator from LSM server
Interface 2	Input	Ingest of ATS multicast streams from transcoder
Interface 3	Output	Post encapsulated output to origin server(s)

Note: For UCS C series rack mount deployments, if 10G interfaces are used, they should be mapped to Input and Output interfaces.

B

Maintenance Procedures

In This Appendix

- Transferring the Encapsulator File 32
- Log File Procedure 33
- Restart Procedures 34
- Customer Support 35

This appendix contains information about procedures you can use with Cisco Media Encapsulator.

Note: In general, you should make sure you are running as root user before executing the commands in these procedures.

Transferring the Encapsulator File

You may find the Cisco Media Encapsulator software on your software DVD or at the following URL:

http://www.cisco.com/en/US/products/ps11787/tsd_products_support_series_home.html

Transfer the following bin file to the Cisco Media Encapsulator root directory via sftp or scp:

cisco-media-encapsulator-2.0.1-bXXX.bin

In this file name, XXX represents the software build version.

According to your operating system, choose one of the following transfer methods:

Windows

Recommended programs: FileZilla, WinSCP, or other client that supports sftp.

If using FileZilla, complete the following steps to transfer the bin file:

Step 1 From the File menu, choose **Site Manager**.

Step 2 Click New Site.

Step 3 Enter the Host name.

Step 4 For Protocol, choose **SFTP**.

Step 5 For Logon Type, choose **Normal**.

Step 6 Enter the user name and password.

Step 7 Click **Connect**.

Step 8 Navigate to the directory on the Encapsulator where you want to transfer the image, and drag the rpm file into this location.

Linux/Unix

For SFTP, enter **sftp@<encap_ip> put <cisco-media-encapsulator-2.0.1-bXXX.bin>**.

For SCP, enter **cisco-media-encapsulator-2.0.1-bXXX.bin <user>@<ip>:<directory>**.

Log File Procedure

How to get log files for support

Step 1 Run the following command **/usr/local/cisco/bin/grablogs** to create the logfile package named “fraglogs…tar.gz”. The output log file will be located in the /tmp directory.

Step 2 Transfer the log file off of the Encapsulator server via SFTP or other file transfer method.

Step 3 Send the file to Cisco for further analysis.

Restart Procedures

How to restart the Encapsulator service

Enter **service cmed restart** to restart the Encapsulator service.

How to restart the operating system

Enter **shutdown –r 1** to restart the system.

Note: this will give a 1 minute delay before the kernel reboots.

Customer Support

If You Have Questions

If you have questions about this product, contact the representative who handles your account for information.

If you have technical questions, contact Cisco support. Use the following link for the TAC Service Request Tool:

http://tools.cisco.com/ServiceRequestTool/create/launch.do

C

Common Linux Configurations

In This Appendix

- Ethernet and Static Route Configuration 38
- DNS Configuration 42

This appendix contains information about common Linux procedures.

Ethernet and Static Route Configuration

Ethernet and static route configurations are kept within the following directory:

/etc/sysconfig/network-scripts/

Each interface will have a corresponding file in this directory where X indicates the interface number.

Example:

/etc/sysconfig/network-scripts/ifcfg-ethX

Use vi or other suitable command line editor to configure each required interface.

Example:

DEVICE=eth0
BOOTPROTO=none
ONBOOT=yes
NETWORK=10.10.10.0
NETMASK=255.255.255.0
IPADDR=10.10.10.100
GATEWAY=10.10.10.1

Note: *You will only add GATEWAY to the interface which will be used for the default route.*

To add a static route to an existing interface, edit the following file, where X equals the interface number.

Edit the file /etc/sysconfig/network-scripts/route-ethX

Example: Adding a static route on interface Ethernet interface 0(ifcfg-eth0)

Edit the file /etc/sysconfig/network-scripts/route-eth0

Add the line:

239.0.0.0/24 nexthop via 10.10.10.1

You can apply changes to the network interfaces after configuration by restarting the network services. **Note:** if you are not logged into the server through a console connection or KVM, this command will terminate your session and require a re-login.

service network restart

To check the routing table, enter the following command.

netstat –rn

Example output:

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
172.18.36.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
0.0.0.0	172.18.36.1	0.0.0.0	UG	0	0	0	eth0

Use ping or traceroute commands to determine proper interface and route configuration, or contact your system administrator or further technical support.

Note: For installations exceeding 25 linear channels, it is recommended to increase the network interface rx buffer size.

This can be done from the UCS Management console or within the operating system as follows:

Connect to the UCS Manager by navigating to the IP of the FIA in a browser, and then clicking **Launch UCS Manager** and opening the .jnlp file it downloads.

Step 1 Log in (default username is admin, password)

Step 2 On the left hand side top bar (Equipment, Servers, LAN, etc.) click **Servers**

Step 3 Scroll down to Policies, expand it, right-click **Adapter Policies**

Step 4 Click Create Ethernet Adapter Policy

Step 5 Create a policy with the following values:

Transmit Queues: 1

Ring Size: 4096

Receive Queues: 32

Ring Size: 4096

Completion Queues: 33

Interrupts: 35

Step 6 Click **OK** to save the policy

Step 7 Go back to the Servers list, expand "Service Profiles" and then expand the configured group

Step 8 Locate the service profile on your blade, expand it, and then expand the list item "vNICs"

Step 9 For each vNIC, set the Adapter Policy to the one you just created, and click **Save Changes**. Note your blade will then reboot immediately to allow changes to take effect.

Optionally, you can use the ethtool command to change the rx buffer as follows, where X indicates the interface number:

Enter **ethtool -G ethX rx 4096**

The following command can be used to verify the changes:

Enter **ethtool -g ethX**

Example:

[root@localhost ~]# ethtool -g eth0

Ring parameters for eth0:

Pre-set maximums:

RX: 4096

RX Mini: 0

RX Jumbo: 0

TX: 4096

DNS Configuration

DNS or static hosts entries will be required if the user configures CME output publishers using a name instead of IP address.

Use vi or other suitable command line editor to configure DNS name server.

```
/etc/resolv.conf
```

Add an entry to for the DNS server in the following format:

```
nameserver <ip address>
```

Example：

```
nameserver 10.10.10.10
```

Optionally static host entries can be configured if the user does not require DNS.

```
/etc/hosts
```

Add an entry to the hosts file in the following format:

```
<ip> <hostname>
Example:
10.10.10.10 xyzcdn.com
```

Cisco Systems, Inc.
175 West Tasman Drive
San Jose, CA 95134-1706
USA

1 408 526 7209
1 800 553 2447

May 2013 Printed in United States of America