

снарте 2

Getting Started with CDS Video Navigator

This chapter explains how to perform the initial configuration tasks needed to get CDS Video Navigator running. Read the following sections and perform the initial configuration tasks in this order:

- 1. Configuring Terminal Emulation Software, page 2-1
- 2. Connecting Cables to the CDE110, page 2-1
- 3. Configuring the CDE110 Ethernet Interfaces, page 2-3
- 4. Configuring CDS Video Navigator, page 2-5
- 5. Configuring the Apache Web Server, page 2-5
- 6. Starting CDS Video Navigator and Verifying Status, page 2-6

In addition, the "Information on CDE110 Hardware" section on page 2-10 contains some notes on the hardware components and configuration used with CDS Video Navigator.

This chapter assumes that the Cisco CDE110 hardware has been installed as described in the *Cisco Content Delivery Engine 110 Hardware Installation Guide*, including connecting cables and connecting power.

Configuring Terminal Emulation Software

The RJ-45 serial ports on the Cisco CDE110 front and back panels can be used for administrative access to the CDE110 through a terminal server. Terminal emulation software must be configured as follows:

- Bits per second: 9600
- Data bits: 8
- Parity: none
- Stop bits: 1
- Hardware flow control: ON

Connecting Cables to the CDE110

The following cable connections are used on the Cisco CDE110:

• For the four Ethernet interfaces on the back of the Cisco CDE110, use Category 5 UTP cables to connect the following:

- One CDE110 Ethernet interface to the network that includes the set-top boxes that CDS Video Navigator will service
- One CDE110 Ethernet interface to connect to the network used for management and back-office communication
- If a terminal server is used, the RJ-45 cable from the terminal server is connected to an RJ-45 serial port on the front or back of the Cisco CDE110. Only one serial port can be used because it is one shared serial port.
- If a PC is directly connected to the CDE110 serial port, the cable from the PC is connected to an RJ-45 serial port on the front or back of the Cisco CDE110. Only one serial port (front or back) can be used because it is one shared serial port. The PC end of the cable connected to the CDE110 serial port varies depending on the type of ports supported by the PC.

Note

The serial port is used for the system console. A system console is typically used rather than a monitor, keyboard, and mouse directly attached to the Cisco CDE110.

• If a monitor, keyboard, and mouse are used, the cables for the devices are connected to the appropriate connectors on the Cisco CDE110.

For the location of connectors on the Cisco CDE110 front and back panels, see the *Cisco Content Delivery Engine 110 Hardware Installation Guide*.

L

To configure the CDE110 Ethernet interfaces for CDS Video Navigator, follow these steps:

Step 1 Press the front panel power switch to power on the Cisco CDE110.

The operating system boots.

- **Step 2** Log in as root with the password rootroot.
- **Step 3** So that your system password for root is not the default password, use the **passwd** command to change the password used for root.
- Step 4 For the Ethernet interfaces that will be used for CDS Video Navigator (eth0 and eth1), use a text editor to modify the two appropriate /etc/sysconfig/network-scripts/ifcfg-eth# files (where # is the number of the Ethernet interface, such as ifcfg-eth1) and do the following:

Configuring the CDE110 Ethernet Interfaces

This section explains the initial Ethernet interface configuration tasks needed for a Cisco CDE110 that will run CDS Video Navigator software. The explanation assumes that the needed software for Red Hat Linux and CDS Video Navigator has been pre-installed on the Cisco CDE110. For Red Hat Enterprise Linux 3.0 AS/ES Update 9 documentation, go to the following web site:

http://www.redhat.com/docs/manuals/enterprise/

For software configuration, the RJ-45 NIC (Ethernet) ports on the Cisco CDE110 back panel are specified as eth0, eth1, eth2, and eth3 as shown in Figure 2-1.





On the back panel, the NIC ports labeled 1, 2, 3, and 4 are, respectively, for interfaces eth0, eth1, eth2, and eth3.

For the configuration examples in this section, Figure 2-2 shows the IP addresses for the following interfaces:

- Interface eth0 connects to the network used for management and back-office communication
- Interface eth1 connects to the network containing the set-top boxes (STBs)

Figure 2-2 IP Addresses for CDS Video Navigator Configuration Examples



-eth1) and do the following:

Cisco CDS Video Navigator Application User Guide, Release 2.1

- Change ONBOOT to yes
- Add IPADDR=ip_address_of this_system_eth#
- Add NETMASK=netmask_for_eth#_network

As an example, for the eth1 interface, the /etc/sysconfig/network-scripts/ifcfg-eth1 file would include the following after the modifications:

ONBOOT=yes IPADDR=11.2.10.2 NETMASK=255.255.255.0

Step 5 To bring the Ethernet interfaces up, issue the **ifup** command for eth0 and eth1. For example:

[root@system]# ifup eth1

- **Step 6** Verify that the eth0 and eth1 interfaces are configured correctly and up and running.
 - Use the **ifconfig** *interface* command to verify that each Ethernet interface is up and running and the IP address and netmask for each are set correctly. The following example is for eth1:

[root@system]# ifconfig eth1

```
eth1 Link encap:Ethernet HWaddr 00:0E:0C:C6:F3:0F
inet addr:11.2.10.2 Bcast:11.2.10.255 Mask:255.255.255.0
inet6 addr: fe80::20e:cff:fec6:f30f/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:3 errors:0 dropped:0 overruns:0 frame:0
TX packets:36 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:192 (192.0 b) TX bytes:2700 (2.6 KiB)
Base address:0x3000 Memory:b8800000-b8820000
```

• Use the **ip link show eth**# command (where # is the Ethernet interface number) to check that the link is up. The following example is for eth1:

[root@system]# ip link show eth1

```
eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
link/ether 00:0e:0c:c6:e4:fe brd ff:ff:ff:ff:ff
```

• Use the **ping** command to check that the Cisco CDE110 can reach the devices directly connected to the Ethernet interfaces (for example, a directly connected router):

[root@system] # ping device_IP_address

Step 7 Use a text editor to modify the /etc/hosts file and add a line with the IP address for eth0 and the associated hostname. For example:

11.2.9.2 starfire-iptv

Step 8 Save and close the /etc/hosts file.



For the host system IP address, using the IP address of the Ethernet interface that points to the management network and video back office is recommended.

Step 9 Use a text editor to modify the /etc/sysconfig/network file and change HOSTNAME to the hostname of this system. For example:

HOSTNAME=starfire-iptv

Step 10 Save and close the /etc/sysconfig/network file.



The changes to the files /etc/hosts and /etc/sysconfig/network do not take effect until the system is rebooted in the Step 11.

Step 11 To restart the system, issue the following command:

[root@system]# init 6

The operating system restarts.

Configuring CDS Video Navigator

CDS Video Navigator is a web application and requires minimal configuration. To configure CDS Video Navigator, follow these steps:

Step 1	Log in	with the	user name	isa and	password	calypso
--------	--------	----------	-----------	---------	----------	---------

Step 2 Change the working directory as follows:

\$ cd /home/isa/MIDAS/config

Step 3 Use a text editor to modify the backoffice.properties file.

- a. Search for the TandbergWSAddress and CatalogFetchUrl parameters in backoffice.properties.
- Enter the IP address of the Tandberg OpenStream platform in these two parameters as follows: TandbergWSAddress=http://Tandberg_IP_address:6070/OSVod CatalogFetchUrl=http://Tandberg_IP_address:6070/Catalog

For example:

TandbergWSAddress=http://192.168.100.200:6070/OSVod CatalogFetchUrl=http://192.168.100.200:6070/Catalog

Step 4 Save and close the backoffice.properties file.

Configuring the Apache Web Server

You must configure the Apache web server to work with multiple IP addresses. Typically, two CDE110 Ethernet interfaces are configured with IP addresses. One Ethernet interface is for the set-top box client-facing VLAN, and the other Ethernet interface is for the management- and back-office-facing VLAN.

To configure the Apache web server, follow these steps:

- **Step 1** Log in as root or use the **su** command to get root privileges.
- **Step 2** Change the working directory as follows:

cd /usr/local/apache2/bin

L

Step 3 Stop the Apache httpd daemon:

./apachectl stop

- **Step 4** Change the working directory as follows:
 - # cd /usr/local/apache2/conf
- **Step 5** Use a text editor to modify the httpd.conf file.
 - **a**. Search for the following section:

```
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
Listen 80
```

b. Replace Listen 80 with the following:

```
Listen xxx.xx.xx.xx:80
Listen yyy.yy.yy.980
```

In the preceding, xxx.xx.xx.and yyy.yy.yy.yy.yyy are the IP addresses that you configured for the two CDE110 Ethernet interfaces.

- c. Save and close the httpd.conf file.
- **Step 6** Change the working directory as follows:
 - # cd /usr/local/apache2/bin
- **Step 7** Start the Apache httpd daemon:
 - # ./apachectl start

Starting CDS Video Navigator and Verifying Status

The following system services are started automatically each time the CDE110 is powered on:

- sshd— Secure Shell daemon
- httpd—HyperText Transfer Protocol daemon (the Apache web server)
- tomcat5—Apache Tomcat application server

This section shows you how to do the following:

- 1. Manually start CDS Video Navigator when you start it for the first time
- 2. Verify that CDS Video Navigator is running correctly
- **3.** Configure CDS Video Navigator to start automatically when the CDE110 is powered on or is restarted in the case of a software failure

Note

The name "midas" appears in the CDS Video Navigator commands and directory names. The midas name was used for CDS Video Navigator when the commands were created.

To start CDS Video Navigator and verify that the needed processes are running, follow these steps:

- **Step 1** Log in with the user name isa and password calypso.
- **Step 2** To start CDS Video Navigator, issue the following command:

\$ start_midas

MIDAS not running starting MIDAS

Step 3 To verify that the CDS Video Navigator process is running, issue the following command:

```
$ check_midas
```

MIDAS (2.1.X.X) is running

If CDS Video Navigator is not running, the output will be MIDAS is not running.

Step 4 To test the set-top box Client-facing Web Services Interface, issue the following commands:

\$ cd /home/isa/MIDAS_IntegrationTest
\$ clientinterfacetest

The **clientinterfacetest** script does not verify the connection from CDS Video Navigator to the set-top box. It does verify that the Client-facing Web Services Interface of CDS Video Navigator is working correctly.

If the test is successful, the output is as follows:

Test successful

If the test is not successful, the output is as follows:

Step 5 To test the connection to and the Web Services interface on the Tandberg OpenStream, issue the following commands:

```
$ cd /home/isa/MIDAS_IntegrationTest
$ tandbergtest
```

The **tandbergtest** script tests fetching a web catalog from the Tandberg OpenStream. It also tests the Tandberg Web Services interface by querying the number of services and their corresponding offerings.

L

Some abbreviated example output from a successful test is as follows:

```
*****
   * Start testing fetching catalog from Tandberg. *
   Success: Fetched catalog information from Tandberg
   * Start testing Tandberg WS - Fetching available services and offerings. *
   Success: Number of services in Tandberg system = 8
   Service id = 0
   name = N2BB
   description =
   displayPrice = null
   pricename = 0
   type = mod
   Offering count of 4 for N2BB
   Offering id = 1
   Offering id = 3
   Offering id = 51
   Offering id = 103
   Service id = 255
   name = SOD
   description =
   displayPrice = null
   pricename = 599
   type = svod
   Offering count of 0 for SOD
   Service id = 203
   name = MAX
   description =
   displayPrice = null
   pricename = 299
   type = svod
   Offering count of 0 for MAX
   Service id = 0
  name = TVN
   description =
   displayPrice = null
   pricename = 0
   type = mod
   Offering count of 0 for TVN
   ... <Output omitted> ...
   Offering count of 1 for HOD
   Offering id = 301
Log in as root or use the su command to get root privileges.
```

Step 7 To verify the sshd process is running, issue the following command and look for output similar to that shown below.

```
# ps -ef | grep sshd
```

Step 6

root 2835 1 0 Jul18 ? 00:00:00 /usr/sbin/sshd

Step 8 To verify the httpd process is running, issue the following command and look for output similar to that shown below.

```
# ps -ef | grep httpd
```

root	2880	1	0	Jul18	?	00:00:00 /usr/sbin/httpd
apache	4881	2880	0	04:03	?	00:00:00 /usr/sbin/httpd
apache	4882	2880	0	04:03	?	00:00:00 /usr/sbin/httpd
apache	4883	2880	0	04:03	?	00:00:00 /usr/sbin/httpd
apache	4884	2880	0	04:03	?	00:00:00 /usr/sbin/httpd
apache	4885	2880	0	04:03	?	00:00:00 /usr/sbin/httpd
apache	4886	2880	0	04:03	?	00:00:00 /usr/sbin/httpd
apache	4887	2880	0	04:03	?	00:00:00 /usr/sbin/httpd
apache	4888	2880	0	04:03	?	00:00:00 /usr/sbin/httpd

Step 9 To verify the tomcat5 process is running, issue the following command and look for output similar to that shown below.

ps -ef | grep tomcat5

root 2915 1 0 Jull8 ? 00:00:11 /usr/java/default/bin/java -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -Djava.util.logging.config.file=/usr/share/tomcat5/conf/logging.properties -Djava.endorsed.dirs=/usr/share/tomcat5/common/endorsed -classpath :/usr/share/tomcat5/bin/bootstrap.jar:/usr/share/tomcat5/bin/commons-logging-api.jar -Dcatalina.base=/usr/share/tomcat5 -Dcatalina.home=/usr/share/tomcat5 -Djava.io.tmpdir=/usr/share/tomcat5/temp org.apache.catalina.startup.Bootstrap start

- **Step 10** Do one of the following after checking that the sshd, httpd, and tomcat5 processes are running:
 - If these checks indicate that all processes are running, proceed to Step 11.
 - If any of these checks fail, restart the processes that are not running. As an example, to restart the tomcat5 process, use **service tomcat5 restart**. Then verify the processes are running and proceed to Step 11.
- **Step 11** Change the working directory as follows:

cd /etc

- **Step 12** To configure CDS Video Navigator to start automatically when the CDE110 is powered on or restarts in the case of a software failure, use a text editor to modify the rc.local file.
 - **a**. Uncomment the following line by deleting the # character:

#su - isa -c "cd /home/isa/MIDAS; ./run_midas >& /home/isa/MIDAS/midas_log&"

b. Save and close the rc.local file.

Information on CDE110 Hardware

This section has some brief notes on some of the hardware components and RAID configuration that are used for CDS Video Navigator models of the Cisco Content Delivery Engine 110 (CDE110).

- Flash Disk, page 2-10
- Hardware RAID and Disk Duplexing, page 2-10

Flash Disk

The Cisco CDS Video Navigator models of the CDE110 include a 4-GB flash drive. The 4-GB flash drive provides a more reliable boot mechanism in the event of hard-drive failure. The flash drive stores the software image used to boot the server and serves as a file system for failsafe booting as well as non-volatile storage for system configuration data.

Hardware RAID and Disk Duplexing

The Cisco CDS Video Navigator models of the CDE110 provide hardware RAID (redundant arrays of independent disks) on the motherboard. Hardware RAID includes the following three components:

- Intelligent Battery Backup Unit (IBBU)
- RAID Activation Key
- RAID MiniDIMM

On the Cisco CDS Video Navigator models of the CDE110, the three hard disk drives are configured, by default, to use RAID 1 disk duplexing. RAID 1 is an easy and highly efficient way to provide data redundancy and system availability.

By default, the two drives are configured for RAID 1, and the third drive is configured as a hot spare. If one hard disk in the disk-duplexed pair fails, all data is immediately available on the other without an impact on performance. With a hot spare drive, any disk failure will start an automatic rebuild of the data onto the hot spare drive. The hot spare automatically replaces the failed drive in the disk-duplexed pair.

With RAID 1, because all data is duplicated, only half of the total drive space can be counted as available space. Therefore, data capacity for the disk-duplexed pair of drives (two 146-GB drives) is approximately 146 GB total.