



Changing the IP Address and Host Name for Cisco Unified Communications Manager Release 7.1(2)

Published: May 13, 2009

Revised: April 2, 2010

This document provides the steps to change the IP address or host name on a Cisco Unified Communications Manager server. You may want to change this IP address for a variety of reasons, including moving the server from one segment to another or resolving a duplicate IP address problem.

This document contains the following main sections:

- [Readiness Checklist, page 1](#)
- [Changing the Cluster IP Addresses for Servers That Are Defined by IP Addresses, page 3](#)
- [Changing the Cluster IP Addresses for Servers That Are Defined by Host Names, page 7](#)
- [Changing the Host Name for Servers in a Cluster, page 12](#)
- [Post-Change Task List, page 16](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 18](#)

Readiness Checklist

Perform the following tasks to ensure that your system is prepared for a successful IP address change.



Note

If you do not receive the results that you expect when you perform these tasks, do not continue with this procedure until after you resolve any problems that you find.

Procedure

Step 1

List all servers in the cluster and note whether the nodes are defined by using IP addresses or host names.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2009 - 2010 Cisco Systems, Inc. All rights reserved.

- From Cisco Unified Communications Manager Administration on the first node, navigate to **System > Server** and click **Find**. A list of all servers in the cluster displays.
- Capture this list of servers for later reference.

Step 2 Ensure that you have saved an inventory of both the host name and IP address of each node in your cluster.

Step 3 Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.

- To check by using RTMT, access Alert Central and check for ServerDown alerts.
- To check by using the CLI on the first node, enter the following command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 4 Check the DB replication status on all the Cisco Unified Communications Manager nodes in the cluster to ensure that all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that is shown in the following example:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :
```

```
    - Perf class (Number of Replicates Created and State of Replication)
has instances and values:
  ReplicateCount -> Number of Replicates Created    = 344
  ReplicateCount -> Replicate_State                  = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- 1—Replicates have been created, but their count is incorrect.
- 2—Replication is good.
- 3—Replication is bad in the cluster.
- 4—Replication setup did not succeed.

Step 5 To check network connectivity and DNS server configuration, enter the CLI command that is shown in the following example:

```
admin: utils diagnose module validate_network
Log file: /var/log/active/platform/log/diag1.log
```

```
Starting diagnostic test(s)
=====
test - validate_network      : Passed
```

```
Diagnostics Completed
admin:
```

Step 6 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, refer the *Disaster Recovery System Administration Guide* for your release:

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Step 7 For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the Certificate Trust List (CTL) file.



Note All IP phones that support security always download the CTL file, which includes the IP address of the TFTP servers with which the phones are allowed to communicate. If you change the IP address of one or more TFTP servers, you must first add the new IP addresses to the CTL file, so the phones can communicate with their TFTP server.



Caution

To avoid unnecessary delays, you must update the CTL file with the new IP address of your TFTP servers before you change the IP address of the TFTP servers. If you do not perform this step, you will have to update all secure IP phones manually.

For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, refer to *Cisco Unified Communications Manager Security Guide Release 7.1(2)*.

You can find this document at the following URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Changing the Cluster IP Addresses for Servers That Are Defined by IP Addresses

This section describes how to change the cluster IP addresses for servers that are defined by IP addresses. For information about changing cluster IP addresses for servers that are defined by host names, see the “[Changing the Cluster IP Addresses for Servers That Are Defined by Host Names](#)” section on page 7.



Caution

Changing the IP address on any node in a Cisco Unified Communications Manager cluster can interrupt call processing and other system functions. Also, changing the IP address can cause the system to generate certain alarms and alerts, such as ServerDown and SDLLinkOSS, and automatic failover to a backup server may not operate. Because of this potential impact to the system, you must perform IP address changes during a planned maintenance window.

This section contains the following procedures:

- [Changing the Cluster IP Addresses for Subscriber Servers That Are Defined by IP Addresses, page 3](#)
- [Changing the Cluster IP Address for the Publisher Server That Is Defined by IP Address, page 5](#)

Changing the Cluster IP Addresses for Subscriber Servers That Are Defined by IP Addresses

Use this procedure to change the IP address of a subscriber server if your cluster servers are defined by IP address. To successfully change the IP address, you must complete all steps in this procedure.



Note

To define subscriber servers on the Cisco Unified Communications Manager publisher server or to determine how a subscriber server is defined, navigate to **System > Server**. For more information, see the *Cisco Unified Communications Manager Administration Guide*.

Procedure

- Step 1** From the Cisco Unified Communications Manager Administration window, perform the following tasks:
- a. Navigate to **System > Server**.
 - b. Change the IP address of the subscriber server to reflect the new IP address.

- Step 2** Ensure that the IP address change is replicated to the subscriber server database by entering the CLI command `run sql select name,nodeid from ProcessNode` on all nodes in the cluster. The following example shows the command output:

```
admin: run sql select name,nodeid from ProcessNode
name                nodeid
=====
EnterpriseWideData 1
10.3.90.21          4
10.3.90.5           2
```

- Step 3** If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the `set network gateway` CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
*** WARNING ***
This will cause the system to temporarily lose network connectivity

Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

- Step 4** Change the IP address of the subscriber server by performing the following tasks:

- a. Enter the CLI command `set network ip eth0 ip_address netmask` where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask.

The following output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0
*** WARNING ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
=====
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
=====
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

- b. Enter **yes** and press **Enter**.



Note You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings > IP > Ethernet**.

- Step 5** Reboot all other servers in the cluster, including the publisher node, to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.



Note These files get updated only during system startup, and the system needs to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures the proper update and service-restart sequence for the IP address changes to take effect.

Changing the Cluster IP Address for the Publisher Server That Is Defined by IP Address

Use this procedure to change the IP address of a publisher server if your cluster servers are defined by IP address.

Procedure

- Step 1** From the Cisco Unified Communications Manager Administration window, perform the following tasks:
- Navigate to **System > Server**.
 - Change the IP address of the publisher server.
- Step 2** Ensure that the IP address change is replicated to the subscriber server database by entering the CLI command `run sql select name,nodeid from ProcessNode` on all nodes in the cluster. The following example shows the command output:

```
admin: run sql select name,nodeid from ProcessNode
name                nodeid
=====
EnterpriseWideData 1
10.3.90.21          4
10.3.90.5           2
```

- Step 3** From the Cisco Unified Communications Operating System Administration window of each subscriber server in the cluster, perform the following tasks:
- Navigate to **Settings > IP > Publisher**.
 - Change the IP address of the publisher server.
- Step 4** If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the set network gateway CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
*** WARNING ***
This will cause the system to temporarily lose network connectivity
```

```

Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
    
```

Step 5 To change the IP address of the publisher server, perform one of the following tasks:

- To change the IP address from Cisco Unified Communications Operating System Administration
 1. Choose **Settings > IP > Ethernet**.
 2. Enter the new IP addresses.
 3. Click **Save**. The server reboots automatically.
- To change the IP address by using a CLI command

1. Enter the CLI command `set network ip eth0 ip_address netmask`

where *ip_address* specifies the new server IP address and *netmask* specifies the new server network mask.

The following output displays:

```

admin: set network ip eth0 10.3.90.21 255.255.254.0
***  W A R N I N G  ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
=====
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
=====
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
    
```

2. Enter **yes** and press **Enter**.

Step 6 After the publisher server reboots automatically, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.



Note These files get updated only during system startup, and the system needs to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures the proper update and service-restart sequence for the IP address changes to take effect.

Step 7 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, refer the *Disaster Recovery System Administration Guide* for your release.

Changing the Cluster IP Addresses for Servers That Are Defined by Host Names

This section describes how to change the cluster IP addresses for servers that are defined by host names. For information about changing cluster IP addresses for servers that are defined by IP address, see the “Changing the Cluster IP Addresses for Servers That Are Defined by IP Addresses” section on page 3.



Caution

Be aware that a DRS backup that you take from a server with a particular host name cannot be restored on a server (either a publisher or subscriber node) with a different host name, even after you reinstall that node.

This section contains the following procedures:

- [Changing the Cluster IP Addresses for Subscriber Servers That Are Defined by Host Name, page 7](#)
- [Changing the Cluster IP Addresses for Publisher Servers That Are Defined by Host Name, page 9](#)

Changing the Cluster IP Addresses for Subscriber Servers That Are Defined by Host Name

Use this procedure to change the IP address of a subscriber server if your cluster servers are defined by host name.

Procedure

- Step 1** Change the DNS record of the subscriber server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records. You must refresh your DNS cache to ensure that the records get correctly updated.



Note DNS servers comprise part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.

- Step 2** Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
```

```
admin:show tech network hosts
```

```
----- show platform network -----
```

```
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.
```

```
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
```

```
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 3 If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the `set network gateway` CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity

Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

Step 4 Change the IP address of the subscriber server by performing the following tasks:

a. Enter the CLI command `set network ip eth0 ip_address netmask`

where *ip_address* specifies the new server IP address and *netmask* specifies the new server network mask.

The following output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0
*** W A R N I N G ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
=====
Note: To recognize the new IP address all nodes within
the cluster will have to be manually rebooted.
=====
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
```

b. Enter **yes** and press **Enter**.



Note You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings > IP > Ethernet**.

Step 5 Reboot all other servers in the cluster, including the publisher server, to update the local name resolution files, such as `hosts`, `rhosts`, `sqlhosts`, and `services`.



Note These files only get updated during system startup, and you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures that the proper update and service-restart sequence for the IP address changes take effect.

Step 6 Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
----- show platform network -----

/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Step 7 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, refer the *Disaster Recovery System Administration Guide* for your release.

Changing the Cluster IP Addresses for Publisher Servers That Are Defined by Host Name

Use this procedure to change the IP address of a publisher server if your servers are defined by host name.

Procedure

Step 1 Change the DNS record of the subscriber server to point to the new IP address. Ensure that you correctly update both the forward (A) and reverse (PTR) records.



Note DNS servers comprise part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.

- Step 2** Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
----- show platform network -----

/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

- Step 3** From the Cisco Unified Communications Operating System Administration window (http://subscriber_ip_address/cmplatform) of each subscriber server in the cluster, perform the following tasks:

- a. Navigate to **Settings > IP > Publisher**.
- b. Change the IP address of the publisher server.

- Step 4** If you are moving the server to a different subnet that requires a new default gateway address, change the default gateway by using the `set network gateway` CLI command, as shown in the following example:

```
admin:set network gateway 10.3.90.2
*** W A R N I N G ***
This will cause the system to temporarily lose network connectivity

Do you want to continue ?

Enter "yes" to continue or any other key to abort
yes
executing...
admin:
```

- Step 5** Change the IP address of the publisher server by using the CLI by performing the following tasks:

- a. Enter the CLI command `set network ip eth0 ip_address netmask` where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask.

The following output displays:

```
admin: set network ip eth0 10.3.90.21 255.255.254.0
*** W A R N I N G ***
If there are IP addresses (not hostnames)
configured in CallManager Administration
under System -> Servers
```

```

then you must change the IP address there BEFORE
changing it here or call processing will fail.
This will cause the system to restart
=====
Note: To recognize the new IP address all nodes within
      the cluster will have to be manually rebooted.
=====
Do you want to continue?
Enter "yes" to continue and restart or any other key to abort
    
```

b. Enter **Yes** and press **Enter**.



Note You can also change the IP address of the default gateway and the server by using the Cisco Unified Communications Operating System. From Cisco Unified Communications Operating System Administration, choose **Settings > IP > Ethernet**.

Step 6 After the publisher server reboots automatically as a result of the **set network ip** command, reboot all subscriber servers to update the local name resolution files, such as hosts, rhosts, sqlhosts, and services.



Note These files only get updated during system startup, and you need to restart core network services, such as Cisco DB and Cisco Tomcat, after the files are updated. Restarting the servers ensures that the proper update and service-restart sequence for the IP address changes take effect.

Step 7 Ensure that local resolution of the subscriber node also resolves to the new IP address by running the **utils network host** and **show tech network hosts** CLI commands:

```

admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11

admin:show tech network hosts
----- show platform network -----

/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
    
```

Step 8 From the Cisco Unified Communications Manager Administration window, navigate to **System > Enterprise Parameters**.

Step 9 Under Phone URL Parameters, change all URLs that contain the old IP address to reflect the new IP address.

- Step 10** Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, refer the *Disaster Recovery System Administration Guide* for your release.

Changing the Host Name for Servers in a Cluster

The section provides procedures for changing the host name of publisher and subscriber servers.

Changing the Host Name of Subscriber Servers

Use the following procedure to change the host name of subscriber servers in a cluster.

Procedure

- Step 1** Change the DNS record of the subscriber server to point to the new IP address. Ensure forward (A) and reverse (PTR) records are updated correctly.



Note DNS servers comprise part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.

- Step 2** Perform one of the following tasks:
- If the servers are defined by IP address and you are only changing the host name of the server, skip to [Step 6](#).
 - If you are changing the IP address or the server is defined by hostname, continue with [Step 3](#).
- Step 3** From the Cisco Unified Communications Manager Administration window, perform the following tasks:
- a. Navigate to **System > Server**.
 - b. Change the host name and/or IP address of the server under Server Configuration.
- Step 4** Ensure that the host name or IP address change is replicated to all the nodes in the cluster by entering the CLI command `run sql select name,nodeid from ProcessNode`.
- Step 5** Repeat on all nodes in the cluster.
- Step 6** Change the host name of the server by performing one of the following tasks:
- To change the host name by using a CLI command
 1. Enter the CLI command `set network hostname hostname`.
 2. Enter **Yes** and press **Enter**. This will automatically reboot this server with the new host name.
 - To change the host name from Cisco Unified Communications Operating System Administration
 1. Navigate to **Settings -> IP -> Ethernet**.
 2. Change IP address and, if necessary, the default gateway to the new address.
 3. Click the **Save** button, which automatically reboots this server with the new changes.



Note Changing the host name triggers an automatic, self-signed Certificate Regeneration. After the server reboots automatically, secure connections to this server will fail until the CTL client is rerun and the CTL file is updated.

Step 7 If the IP address is changing along with host name and the server is moving to a new subnet, first change the server Default Gateway to the new address by using the `set network gateway ipaddress` CLI command.



Note When the default gateway is changing prior to the next step, ensure that the server is moved to the new subnet and has access to the default gateway prior to the next step. During Cisco Unified Communications Manager server startup, the Verify Network script checks whether the server can access the default gateway. If the server cannot communicate with the default gateway at the time of startup, the Verify Network script will fail, and startup may be delayed. If you are using Manual DHCP configuration and the DHCP server is not reachable or not giving out an IP address to the server, the system will not boot and instead continuously waits at the Verify Network startup phase.

Step 8 If you want to also change the IP address, change the IP address of the server by performing the following tasks:

- a. Enter the CLI command `set network ip eth0 ip_address netmask` where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask.
- b. Enter **Yes** and press **Enter**. This will automatically reboot this server with the new IP address.

Step 9 Reboot all other servers in the cluster, including the publisher, to update the local name resolutions files such as `hosts/rhosts/sqlhosts/service`.

These files only update during startup time, and core network services such as Cisco DB and Cisco Tomcat need to be restarted after the files are updated. A restart of the servers ensures the proper update and service restart sequence for the IP address changes to take effect.

Step 10 Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-sub-4
Hostname lg-sub-4 resolves to 14.86.13.11
```

```
admin:show tech network hosts
```

```
----- show platform network -----
```

```
/etc/hosts File:
```

```
#This file was generated by the /etc/hosts cluster manager.
```

```
#It is automatically updated as nodes are added, changed, removed from the cluster.
```

```
127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
```

admin:

You can also use the `utils diagnose module validate_network` command on all the cluster nodes. This diagnostics module checks that you configured DNS client services correctly, the server can connect to the DNS server, and Forward (A) and Reverse (PTR) records are present and match the server IP address and host name.



Note Do not proceed if the change has not propagated to all nodes.

- Step 11** From the publisher server, run `utils dbreplication reset all` to set up replication across the whole cluster again.

Changing the Host Name for the Publisher Server

Use the following steps to change the host name of a publisher server.

Procedure

- Step 1** Change the DNS record of the publisher server to the new host name. If the IP address is going to be changing at the same time, make sure that it is also reflected on the DNS servers. Ensure forward (A) and reverse (PTR) records are updated correctly.



Note DNS servers comprise part of the network infrastructure. Cisco Unified Communications Manager servers do not and cannot run DNS services.



Note Skip [Step 2](#) through [Step 5](#) if the servers are defined by IP address and you are only changing the host name of the server.

- Step 2** From the Cisco Unified Communications Manager Administration window, perform the following tasks:
- a. Navigate to **System > Server**.
 - b. Under Server Configuration, change the host name and/or IP address of the server.
- Step 3** Ensure that the host name or IP address change is replicated to all the nodes in the cluster by entering the CLI command `run sql select name, nodeid from ProcessNode`.
- Step 4** Repeat on all nodes in the cluster.
- Step 5** From the Cisco Unified Communications Operating System Administration window (http://subscriber_ip_address/cmplatform or http://subscriber_ip_address/iptplatform) of each subscriber server in the cluster, perform the following tasks:
- a. Navigate to **Settings > IP > Publisher**.
 - b. Change the host name and/or IP address of the publisher server.



Note You can use the following CLI commands to change the IP address and/or host name of the publisher server on the subscriber servers: `set network cluster publisher ip` or `set network cluster publisher hostname`.

- Step 6** On the publisher server, change the host name of the server by performing the following tasks:
- Enter the CLI command `set network hostname hostname`.
 - Enter **Yes** and press **Enter**. This will automatically reboot this server with the new host name.



Note Changing the host name triggers an automatic, self-signed Certificate Regeneration. After the server reboots automatically, secure connections to this server will fail until the CTL client is rerun and the CTL file is updated.

- Step 7** If the IP address is changing along with host name and the server is moving to a new subnet, first change the server Default Gateway to the new address by using the `set network gateway ip_address` CLI command.



Note When the default gateway is changing prior to the next step, you need to ensure that the server is moved to the new subnet and has access to the default gateway prior to the next step. During Cisco Unified Communications Manager server startup, the Verify Network script checks access to the default gateway. If the server cannot communicate to the default gateway at the time of startup, the Verify Network script will fail, and startup may be delayed. If you are using Manual DHCP configuration and the DHCP server is not reachable or not giving out an IP address to the server, the system will not boot and instead continuously waits at the Verify Network startup phase.

- Step 8** If the IP address is also changing, change the IP address of the server by performing the following tasks:
- Enter the CLI command `set network ip eth0 ip_address netmask`, where `ip_address` specifies the new server IP address and `netmask` specifies the new server network mask.
 - Enter **Yes** and press **Enter**. This will automatically reboot this server with the new IP address.

- Step 9** From the CLI or Cisco Unified Communications Operating System Administration, reboot all other servers in the cluster, including the publisher, to update the local name resolutions files such as `hosts/rhosts/sqlhosts/service`. You must reboot the whole cluster after you change each node.



Note These files only update during startup time, and core network services such as Cisco DB and Cisco Tomcat need to be restarted after the files are updated. A restart of the servers ensures the proper update and service restart sequence for the IP address changes to take effect.

- Step 10** Verify that the DNS change propagates to other nodes by using the `utils network host` and `show tech network hosts` CLI commands on all the cluster nodes:

```
admin:utils network host lg-pub-4
Hostname lg-pub-4 resolves to 14.86.13.11
```

```
admin:show tech network hosts
----- show platform network -----
```

```
/etc/hosts File:
#This file was generated by the /etc/hosts cluster manager.
```

```
#It is automatically updated as nodes are added, changed, removed from the cluster.

127.0.0.1 localhost
14.87.10.10 lg-pub-1.lindermangroup.cisco.com lg-pub-1
14.87.10.11 lg-tftp-1.lindermangroup.cisco.com lg-tftp-1
14.87.10.12 lg-tftp-2.lindermangroup.cisco.com lg-tftp-2
14.87.11.10 lg-sub-1.lindermangroup.cisco.com lg-sub-1
14.87.11.11 lg-sub-3.lindermangroup.cisco.com lg-sub-3
14.86.13.10 lg-sub-2.lindermangroup.cisco.com lg-sub-2
14.86.13.11 lg-sub-4.lindermangroup.cisco.com lg-sub-4
14.87.11.12 lg-sub-5.lindermangroup.cisco.com lg-sub-5
14.87.11.13 lg-sub-7.lindermangroup.cisco.com lg-sub-7
14.86.13.12 lg-tftp-3.lindermangroup.cisco.com lg-tftp-3
14.87.20.20 lg-cups1.heroes.com lg-cups1
14.86.13.13 lg-sub-6.lindermangroup.cisco.com lg-sub-6
admin:
```

Alternatively, you can use the `utils diagnose module validate_network` command on all the cluster nodes. This diagnostics module will ensure that, if DNS client services are configured, connectivity to DNS server is present, and Forward (A) and Reverse (PTR) records are present and matching with the server IP address as well as host name.



Caution

Do not proceed if the new host name does not resolve to the correct IP address.

- Step 11** From the publisher node, run `utils dbreplication reset all` to set up replication across the whole cluster again.

Post-Change Task List

After you finish changing the IP addresses of your cluster, complete the following tasks:

Procedure

- Step 1** For security-enabled clusters (Cluster Security Mode 1 - Mixed), update the CTL file.
- For detailed instructions on updating and managing the CTL file, including adding a new TFTP server to an existing CTL file, refer to the *Cisco Unified Communications Manager Security Guide Release 7.1(2)*.
- You can find this document at the following URL:
- http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- Step 2** After you finish updating the CTL file, restart all nodes in the cluster.
- Step 3** Ensure that all servers in the cluster are up and available by checking for any active ServerDown alerts. You can check by using either the Real Time Monitoring Tool (RTMT) or the Command Line Interface (CLI) on the first node.
- To check by using RTMT, access Alert Central and check for ServerDown alerts.
 - To check by using the CLI on the first node, enter the following command and inspect the application event log:

```
file search activelog syslog/CiscoSyslog ServerDown
```

Step 4 Check the DB replication status on all the Cisco Unified Communications Manager nodes in the cluster to ensure all servers are replicating database changes successfully. You can check by using either RTMT or a CLI command.

- To check by using RTMT, access the Database Summary and inspect the replication status.
- To check by using the CLI, enter the command that is shown in the following example:

```
admin: show perf query class "Number of Replicates Created and State of Replication"
==>query class :
```

```
    - Perf class (Number of Replicates Created and State of Replication)
has instances and values:
ReplicateCount -> Number of Replicates Created    = 344
ReplicateCount -> Replicate_State                 = 2
```

Be aware that the Replicate_State object shows a value of 2 in this case. The following list shows the possible values for Replicate_State:

- 0—Replication Not Started. Either no subscribers exist, or the Database Layer Monitor service is not running and has not been running since the subscriber was installed.
- 1—Replicates have been created, but their count is incorrect.
- 2—Replication is good.
- 3—Replication is bad in the cluster.
- 4—Replication setup did not succeed.

Step 5 In Cisco Unified Reporting, generate the Unified CM Database Status report. Look for any errors or warnings in this report.

Step 6 In Cisco Unified Reporting, generate the Unified CM Cluster Overview report. Look for any errors or warnings in this report.

Step 7 Reconfigure the netdump server and clients by using the `utils netdump` CLI commands. For more information, see Appendix A in the *Cisco Unified Communications Operating System Administration Guide*.

Step 8 Run a manual DRS backup and ensure that all nodes and active services get backed up successfully. For more information, refer the *Disaster Recovery System Administration Guide* for your release.



Note You must run a manual DRS backup after you change the IP address of a node, because you cannot restore a node with a DRS file that contains a different IP address or host name. The post-change DRS file will include the new IP address or host name.

Step 9 Update all relevant IP phone URL parameters.

Step 10 In Cisco Unified Communications Manager Administration under **System > Enterprise Parameters**, update all relevant IP phone services.

Step 11 Update IPsec tunnels that terminate to the Cisco Unified Communications Manager.

Step 12 Update RTMT custom alerts and saved profiles:

- RTMT custom alerts that are derived from performance counters include the hard-coded server IP address. You must delete and reconfigure these custom alerts.
- RTMT saved profiles that have performance counters include the hard-coded server IP address. You must delete and re-add these counters and then save the profile to update it to the new IP address.

Step 13 Update the DHCP server that runs on Cisco Unified Communications Manager.

Step 14 Check and make any required configuration changes to other associated Cisco Unified Communications components, including the following ones:



Note Consult the documentation for your product to determine how to make any required configuration changes.

- Cisco Unity
- Cisco Unity Connection
- Cisco Unity Express
- SIP/H.323 trunks
- IOS Gatekeepers
- Cisco Unified MeetingPlace
- Cisco Unified MeetingPlace Express
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- DHCP Scopes for IP phones
- SFTP servers that are used for Cisco Unified Communications Manager trace collection, CDR export, or as a DRS backup destination
- IOS hardware resources (conference bridge, media termination point, transcoder, RSVP agent) that are registered with Cisco Unified Communications Manager
- IPVC video MCUs that are registered or integrated with Cisco Unified Communications Manager
- Cisco Emergency Responder
- Cisco Unified Application Environment
- Cisco Unified Presence
- Cisco Unified Personal Communicator
- Associated routers and gateways

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Cisco Product Security Overview

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

Further information regarding U.S. export regulations may be found at

http://www.access.gpo.gov/bis/ear/ear_data.html

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco 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. (1002R)

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

© 2009 - 2010 Cisco Systems, Inc. All rights reserved.

