Tru64 UNIX Best Practice

Reconfiguring Your Primary Network Interface

February 2001

Product Version: **Tru64 UNIX Version *4.0x, 5.0, and 5.0A***

This Best Practice describes how to reconfigure the host name and IP address of Tru64 UNIX Version 4.0*x*, 5.0, and 5.0A systems that contain a single network interface and are running the Common Desktop Environment (CDE).

Compaq Computer Corporation
Houston, Texas

Contents

Reconfiguring Your Primary Network Interface

Reconfiguring Your Primary Network Interface

This Best Practice describes how to reconfigure the host name and IP address of Tru64 UNIX Version 4.0*x*, 5.0, and 5.0A systems that contain a single network interface and are running the Common Desktop Environment (CDE).

Once you use the Network Configuration application or the SysMan Menu to configure your network services on these systems for the first time, CDE becomes network-dependent, and it might function inconsistently if network services become unavailable as a result of further changes.

On systems with multiple active network interfaces, you can use the Network Configuration application or the SysMan Menu to change the host name and IP address, because the system can use other active interfaces to maintain communication with the network while the primary network interface is being reconfigured. However, on systems with a single network interface, you must not change the host name or IP address with the Network Configuration application or the SysMan Menu. Instead, follow the procedure in this Best Practice to avoid problems.

See the Tru64 UNIX Best Practices Web page for more information about Best Practices documentation.

Is This Best Practice Right for You?

Not all Best Practices apply to all configurations, so you must be sure that it is appropriate for your system and circumstances. To use this Best Practice, you must meet the requirements described in the following table:

Requirement	Description
Operating System	Tru64 UNIX Version 4.0*x*, 5.0, or 5.0A. The procedure in this Best Practice is unnecessary on Tru64 UNIX Version 5.1 and higher. Use the SysMan Menu utility to reconfigure all network interfaces on these systems.
Windowing System	Common Desktop Environment The procedure in this Best Practice is unnecessary on systems where the XDM login manager is running or where no windowing system is running.
System Configuration	An applicable system for this Best Practice: • Contains a single network interface, or only one active interface • Has a static or server-assigned IP address • Is not a node in a cluster
Impact on Availability	You must reboot the system after changing its host name or address; it will be unavailable during this process. If your system is a server of any kind (for instance, if your system provides DNS, NIS, Mail, or other services), you need to inform your users of the change well in advance because they will lose their connections with the server as a result of this change.
Skill Level	You must have basic UNIX administration skills.

If you do not meet the previous requirements, see *Alternative Practices* for information.

Before You Begin

Before you apply the Best Practice for *Reconfiguring Your Primary Network Interface*, you must understand some background information and perform some preliminary tasks.

Related Documentation

You might find it helpful to have the following documentation available while completing the procedure described in this Best Practice:

- The online or hardcopy reference pages, particularly `rcmgr`(8), `ifconfig`(8), `hostname`(8), and `wall`(1)
- The *Network Administration* guide

Obtaining a New Host Name and IP Address

To obtain a new host name and/or IP address, you need to contact the network administrator for your site. Depending on the network configuration at your site and site policies, you will be asked for the following information, or a subset thereof:

- Previous host name and IP address — The host name and static IP address you were using before this change. Static IP addresses are in high demand in some larger networks; therefore, if you are changing your IP address, the network administrator will want to reclaim the old address for future use.
- Media Access Control (MAC) address — The address that was assignned to your network interface card (NIC) when it was manufactured. Appears in the format *XX-XX-XX-XX-XX-XX*. You can obtain this address by entering the `netstat -i` command, as follows:

```
# netstat -i
Name  Mtu   Network     Address                 Ipkts Ierrs     Opkts Oerrs    Coll
lo0   4096  <Link>                           8206472     0    8206472     0       0
lo0   4096  loop        localhost            8206472     0    8206472     0       0
sl0*  296   <Link>                                0     0          0     0       0
tu0   1500  <Link>      08:00:2b:73:9e:84  3122976778     0 3122976776     2 8512910
tu0   1500  DLI         none               3122976778     0 3122976776     2 8512910
tu0   1500  state-net   hampshire          3122976778     0 3122976776     2 8512910
```

  In this case, the MAC address is `08:00:2b:73:9e:84`.

- Proposed new host name — A name that is unique to your site. It is best to provide more than one choice, in case one or more is already taken. Note that some companies have a site-wide naming convention. In this case, you will not be able to select your own host name.
- Subnet or segment — If your network is split up into several subnets, perhaps for different floors or buildings, you might need to specify your logical location in the network.

- CPU type and operating system — Some sites track this information for debugging purposes. If a specific system or other piece of hardware (like a printer) is not functioning correctly, this information can be helpful for locating it.
- Physical location — The office number or address where the system is located.
- Contact information — Your full name, email address, and phone number.

Migrating to or from Dynamic Addressing

If your system currently obtains a temporary IP address from a Dynamic Host Configuration Protocol (DHCP) server, and you need to switch to a static IP address, or vice versa, the procedure described in this Best Practice still applies to your system.

If you are migrating to static addressing, you need to follow the directions in *Obtaining a New Host Name and IP Address* to obtain a new IP address and, if necessary, a new host name, as if you were configuring your system for the first time. Then, follow the steps of the procedure for *Applying the Best Practice*.

If you are migrating to dynamic addressing (DHCP), do the following:

1. Contact your network administrator to check if dynamic addressing at your site is restricted by MAC address. If it is, the network administrator will need to add your MAC address to the access control list on the DHCP server. See *Obtaining a New Host Name and IP Address* for more information about the MAC address.
2. Follow the steps in the procedure for *Applying the Best Practice* to convert to dynamic addressing.
3. When you are convinced that dynamic addressing is working, inform your network administrator that your static address can be reclaimed for use by another system.

Migrating to a New Network or Subnetwork

If you are migrating to a new network or subnetwork, you must verify that your system is correctly configured for services on that network. These are just a few services to consider:

- Routing

You must update the routing tables on your system, otherwise, you will be unable to communicate with other systems on the new network.

You might need to manually update your `/etc/routes` file to reflect the new routes. But if routing information is distributed through RIP or another routing protocol in the new network, you can instead configure the appropriate daemon (`routed` or `gated`) to dynamically update your routing tables. Contact your network administrator to ask how routing information is maintained and distributed in the new domain, and make the appropriate changes.

For information about basic routing concepts, see the *Best Practice for Network Routing*.

- Domain Name System (DNS)

  If you use DNS for host name resolution, you might need to reconfigure your system for service in a new DNS domain. If necessary, you will need to supply a new domain name and a new list of DNS servers.

- Network Information Service (NIS)

  If you use NIS to obtain user information or Automount maps for your network, you might need to reconfigure your system for service in a new NIS domain. If necessary, you will need to supply a new domain name and a new list of NIS servers.

- Mail

  If you use your system to send and receive mail, you might need to specify a new Simple Mail Transfer Protocol (SMTP) server that your system will use as a mail relay. Furthermore, if you use POP or IMAP mail, you might need to specify new POP or IMAP servers from which you will collect your mail.

- Network File System (NFS)

  If you mount remote file systems via NFS, you might need to import these file systems from other servers within your new network. Furthermore, if you use Automount, you might need to update your local Automount maps.

- Network Time Protocol (NTP)

  If you synchronize time via NTP, you might need to specify a different list of time servers within your new network.

Contact your network administrator to obtain the necessary configuration information. Use it to reconfigure your system after you have changed your host name and IP address.

See the *Network Administration* guide and online help for more information about configuring these services.

If Your System is a Server

If your system is a server of any kind, it is imperative that you plan ahead for a host name and/or IP address change. Because you need to stop network services on your system and reboot to put the changes into effect, your system will be temporarily unavailable to client systems during the procedure for *Applying the Best Practice*. In addition, because you are changing your server's host name and/or IP address, client systems might not be able to communicate with the server even after the change.

It is best to send several warning e-mail messages to users starting a few weeks before the change. In the messages, include any information that users need to reconfigure their client systems — like new server names and IP addresses.

In addition, shortly before you stop network services on the system, you can use the `wall` command to inform any users who are logged in to the system that they are about to lose their connection. You can send a message with the `wall` command by executing the following command:

```
# wall warning
```

Replace *`warning`* with the name of a file that contains the warning message for the users. See `wall`(1) for more information.

Note that only users currently logged in to the system will see the warning message. DNS, NIS, Mail and other service clients will not see it. As previously stated, you need to warn these users long before you make any changes.

Applying the Best Practice

Before you reconfigure your primary network interface, be sure to follow the recommendations in *Before You Begin*.

To change the IP address and host name of a system with a single network interface, follow these steps:

1. Log in as the root user at the system console.

2. Edit the /etc/hosts file and add a new entry to reflect the new hostname and the new IP address of your system. Do not remove the old entry yet; you will do that later in the procedure.

   For example, if you were changing the host name and IP address of your system to newname.ocean.corp.com (192.9.201.2), you would add the following entry in your /etc/hosts file:

   ```
   192.9.201.2    newname.ocean.corp.com      newname
   ```

3. Execute the following command to change the host name of your system in the /etc/rc.config file:

   ```
   # rcmgr set HOSTNAME new-host-name
   ```

   Replace *new-host-name* with the new host name. If you have configured DNS, use the fully-qualified host name, as in step 2. For example:

   ```
   # rcmgr set HOSTNAME newname.ocean.corp.com
   ```

4. Execute one of the following commands to change the IP address of your system in the /etc/rc.config file.

   - For a static IP address:

     ```
     # rcmgr set IFCONFIG_n IP-address netmask network-mask
     ```

     For example:

     ```
     # rcmgr set IFCONFIG_0 192.9.201.2 netmask 255.255.255.0
     ```

   - For a dynamic address (as assigned by DHCP):

     ```
     # rcmgr set IFCONFIG_n DYNAMIC
     ```

     For example:

     ```
     # rcmgr set IFCONFIG_0 DYNAMIC
     ```

   If there is only one network card in your system, the value for n is likely to be 0. However, it is best to view all of the IFCONFIG_*n* entries in the /etc/rc.config file to verify this before setting the new IP address and network mask with the rcmgr command.

5. The operating system uses the parameters in the /etc/rc.config file to configure your network interface at system startup. If you enter the parameters incorrectly, it will cause problems; therefore, verify the information you supplied by entering the following commands:

```
# rcmgr get HOSTNAME
# rcmgr get IFCONFIG_n
```

If there is an inconsistency, fix the problem before moving onto the next step.

6. Close any open connections (from `telnet`, `rlogin`, `ftp`, and other applications) to other machines. Save and close any open files, especially files in NFS-mounted file systems.

7. Execute the following commands to stop network services and close any open connections:

```
# rcinet stop
# ifconfig interface-ID down delete abort
```

You can determine the value for *interface-ID* by executing the following command, where *n* has the same value (probably 0) you determined in step 5:

```
# rcmgr get NETDEV_n
```

For example, a common interface ID is `tu0`. In this case, the `ifconfig` command string would appear as follows:

```
# ifconfig tu0 down delete abort
```

8. If necessary, reconfigure services on your system as specified in *Migrating to a New Network or Subnetwork*. See the relevant sections of the *Network Administration* guide for more information. If you moved the system into a new network or subnetwork, it is very likely to require changes.

Some utilities offer you the option to restart network services after configuration. It is best not to restart network services while you are following this procedure, especially if your system is a server. Otherwise, clients might reconnect to your system while it is in an inconsistent state.

9. Reboot the system to effect the changes, as follows:

```
# /usr/sbin/shutdown -r now
```

Watch the boot process carefully for any error messages. If the system is a server, verify each service it provides before announcing the system's availability.

10. Edit the `/etc/hosts` file and remove the old entry for your system.

Verifying Success

After you apply the Best Practice for *Reconfiguring Your Primary Network Interface*, you can verify whether it was successful, as follows:

- If you changed your system's host name, enter the following command to verify that the new host name is in effect:

  ```
  # hostname
  ```

  The host name of the system is returned.

- If you changed your system's IP address, enter the following command to verify that the new IP address is in effect:

  ```
  # ifconfig interface-ID
  ```

  Information about the specified adapter, including the IP address, is returned.

- Check the log files in the `/var/adm/syslog.dated/`*`date-time`* directory for error messages. Replace *`date-time`* with the directory in `/var/adm/syslog.dated` that has the most current time stamp.

If the Best Practice was not successful, see *Troubleshooting* for information about identifying and solving problems.

Troubleshooting

If you determine that the Best Practice was not successful, as described in *Verifying Success*, use the following table to identify and solve problems:

Problem	Possible Solutions
System startup takes longer than usual, system pauses when mounting remote file systems	Do the following: 1. Verify your physical connection to the network — cables, hubs, and other hardware. 2. Verify that the servers in your environment are up and running. 3. Verify the configuration of DNS, NIS, NFS, and other services on your system. Ensure that you are using the appropriate server and domain names, especially if you moved to a new network or subnetwork. Verify the spelling (and for some services, particularly NIS, the case) of all host and domain names. 4. Verify that the IP address for your system is not being used by another system. Your network administrator might have tools to check for this. 5. If you are using DHCP: a. Verify that the DHCP server is up and running. b. If DHCP usage at your site is restricted by Media Access Control (MAC) address, verify that your MAC address has been added to the access control list on the DHCP server. Contact your network administrator for more information.

Problem	Possible Solutions

CDE applications fail to start, and the system displays a `Can't open display` error	Follow these steps to diagnose the problem:
	1. Verify the new host name in the `rc.config` file by executing the following command:
	`# rcmgr get HOSTNAME`
	2. Verify the new host name in the running kernel by executing the following command:
	`# hostname`
	If the host name is incorrect in either place, follow the steps in the procedure for *Applying the Best Practice* to fix the problem.
	If the host name is correct in both places, it is likely that the new host name was not added to the X access control list, especially if you did not reboot the system after changing the name.
	Execute the following command to open X access to the local host:
	`# xhost +new-host-name`
	If you have configured DNS, replace *new-host-name* with the fully qualified host name of your system. For instance, use `newhost.domain.com` instead of `newhost`.

System cannot see the network, or network connectivity is intermittent.	Do the following: 1. Follow the steps under "System startup takes longer than usual..." 2. Verify that network services are running on your system.

If you cannot solve a problem by following the instructions in this table, see the *Network Administration* guide for more comprehensive network troubleshooting information.

Alternative Practices

Although this Best Practice is the recommended method for reconfiguring your primary network interface, if your system does not meet the requirements described in *Is This Best Practice Right for You?*, you can use an alternative method as described in the following table:

Configuration:	Action:
If you are running a version of Tru64 UNIX prior to Version 4.0...	You can reconfigure your network interface as you normally would. Because CDE was not introduced until Version 4.0, the procedure described in this Best Practice is not necessary for previous releases, but it will work.
If you are running Tru64 UNIX Version 5.1 or higher...	Use the SysMan Menu utility to reconfigure network interfaces on these systems. The procedure described in this Best Practice is not necessary on Tru64 UNIX Version 5.1 and higher, even if you have only one interface.
If the X Server is not running on your system...	You can reconfigure your network interface as you normally would. Because a windowing system is not running on your system, your login session is not network-dependent. The procedure described in this BP is not necessary, but it will work.
If your system is a node in a cluster...	If your cluster is running TruCluster Server Version 5.0A, see the Best Practice for *Changing the Cluster Name or IP Address in a TruCluster Server Version 5.0A Cluster*.

Comments and Questions

We value your comments and questions on the information in this document. Please mail your comments to us at this address:

best_practices@zk3.dec.com

Legal Notice