Cisco TCP/IP Suite Online Help

Cisco TCP/IP Suite Configuration Utility Options

Configuration Procedures

Configuration Concepts

Cisco TCP/IP Suite Online Help

Interface Tab

TCP/IP network interfaces let you associate a physical network interface card or asynchronous connection with an IP address through software configuration. The Interface tab of the Cisco TCP/IP Suite Configuration Utility lets you configure multiple interfaces on the same machine.

The Interface tab contains controls that let you view all interfaces installed on the stack, add a new interface, modify an existing interface, or remove an interface. The tab is contains these fields and buttons:

Enabled
Yes indicates the enabled interface.

Interface Label
Shows the name of the interface, if you gave it a name.

Type
Shows the type of interface: Ethernet, serial, FDDI, or Token-Ring.

IP Address
Shows the IP address for the interface, such as `192.168.34.22`).

Subnet Mask
Shows the subnet mask for the interface, such as `192.168.34.255`.

Broadcast Address
Shows the broadcast address for the interface.

New button
Creates a new interface using the New Interface dialog box,

Modify button
Modifies the interface selected in the interface table.

Delete button
Deletes the selected interface.

Done button
Saves changes made to all tabs in the utility and exits the utility.

See Also:

- Configuring Network Interfaces
- Network Interface Concepts

◆◆◆

Interface Table

The Interface Table lists interface information in alphabetic order. The display columns are:

- Enabled: indicates whether the interface is enabled
- Interface Name: describes an optional name for the interface
- Interface Type: specifies whether the interface is Ethernet, serial, FDDI or Token-Ring
- IP Address: specifies the IP address of the interface, such as `192.168.34.22`
- Subnet Mask: specifies the subnet mask for the interface, such as `192.168.34.255`.
- Broadcast: lists the optional broadcast address for the interface, such as `191.87.255.255`

New Button

Click the New button to create an interface.

Modify Button

Click the Modify button to change information about the selected interface.

Delete Button

Click the Delete button to remove the selected interface.

Delete Dialog Box

The Delete Dialog box lets you confirm that you want to delete the selected item.

Interface Dialog Box

The New or Modify Interface dialog box lets you configure a network interface. The Interface dialog box contains these fields:

Interface Label

A descriptive name for the interface. This label is optional and can be up to 255 alphanumeric characters. For example, Sales Subnet.

Interface Type

The type of network interface: Ethernet, serial, FDDI, or Token-Ring.

IP address

The IP address, in dotted-decimal format, for the workstation (for example, `192.168.34.22`). If you are not sure of your IP address, ask your network administrator.

Subnet Mask

The subnet mask for the interface. If you are not sure of your subnet mask, ask your network administrator.

Broadcast Address

The broadcast address for the interface, if there is one. If you are not sure whether your site uses a broadcast address, ask your network administrator.

Enable Interface

Determines whether this interface active.

Dynamic Configuration (BOOTP/DHCP)

Determines whether you are using dynamic configuration for the interface. If you enable dynamic configuration, the IP address, subnet mask, and broadcast address are obtained dynamically as you use the network. Do not use dynamic configuration if you have been assigned an IP address.

Driver

Determines the interface driver for your network interface card: ODI, NDIS 2.0, or NDIS 3.0. If you are not sure of the correct driver, ask your network administrator.

See Also:

- Configuring Network Interfaces.

Interface Label

Enter a descriptive name for the interface.   This label is optional and can be up to 255 alphanumeric characters.   For example, Sales Subnet.

Interface Type

The Interface Type drop-down list lets you select an interface type.

IP Address

Enter the IP Address, in dotted-decimal format, for the workstation (for example, `192.168.34.22`). If you are not sure of your IP address, ask your network administrator.

Subnet Mask

The Subnet Mask edit box lets you add or change the subnet mask for the interface. Enter the subnet mask if your site uses one. If you are not sure of your subnet mask, ask your network administrator.

Broadcast Address

Enter the broadcast address for the interface.   If you are not sure whether your site uses a broadcast address, use the default broadcast address.

Enable Interface

Check Enable Interface to enable the interface.   The currently-enabled interface is indicated by a yes in the interface table.

Dynamic Configuration

Check Dynamic Configuration to enable dynamic configuration.   If you enable dynamic configuration, the IP address, subnet mask, and broadcast address are obtained dynamically from BOOTP or DHCP when you boot your system.   Do not use dynamic configuration if you have been assigned an IP address.

ODI

Choose ODI to designate an ODI driver. If you are not sure of the correct driver, ask your network administrator.

NDIS 2.0

Choose NDIS 2.0 to designate an NDIS 2.0 driver. If you are not sure of the correct driver, ask your network administrator.

NDIS 3.0

Choose NDIS 3.0 to designate an NDIS 3.0 driver. If you are not sure of the correct driver, ask your network administrator.

Configuration File Name Dialog Box

The Configuration File Name dialog box lets you specify the absolute location of either the ODI `NET.CFG` file or the NDIS2 `PROTOCOL.INI` file. Click the Browse button to locate the file on your disk drive.

Configuration File Name

Specify the absolute name of the configuration file.   If you do not know the location of the file, click the Browse button.

Driver Name Dialog Box

The Driver Name dialog box appears when the requested NDIS 3.0 driver has not been loaded.   Enter the name of the driver, which is supplied by the Ethernet or Token-Ring controller card (network interface) manufacturer.

Driver Name

Enter the name of the driver.   The driver name is supplied by the Ethernet or Token-Ring controller card (network interface) manufacturer.

File Name Dialog Box

The File Name dialog box appears when the requested ODI or NDIS 2.0 driver has not been loaded.   Enter the name of the driver, which is supplied by the Ethernet or Token-Ring controller card (network interface) manufacturer.

File Name

Enter the name of the driver.   The driver name is supplied by the Ethernet or Token-Ring controller card (network interface) manufacturer.

File Name Table

The File Name table displays the file names that match the file name pattern specified in the File Name edit box.

Browse Button

The Browse button opens the Browse dialog box to let you find the driver file.

Browse Dialog Box

The Browse dialog box lets you find a driver name.

File Name
The name of the driver.

File Name list
Displays all files in the current directory that are of the same type as shown in the List Files of Type drop-down list. To select a file from this list, click the file name and click the OK button.

List Files of Type
The type of files to display in the File Name list box.

Directories
The directory from which to choose a driver.

Drives
The drive for selecting the file.

File Name

The File Name edit box lets you enter a driver file name. A file name can contain up to eight characters and an extension of up to three characters. The Configuration Utility adds the extension you specify in the File As Type drop-down list.

Drives

The Drives drop-down list lets you select the drive for finding the file.

File As Type

The File As Type drop-down list lets you specify the file format for the file.

Directories

The Directories list box lets you select the file's directory.

Network Button

The Network button lets you connect to another network location and assign it a new drive letter.

Done Button

Click the Done button to close the Configuration Utility and save your changes in the configuration file.

Help Button

Click the Help button to view online help for the Configuration Utility.

OK Button

Click the OK button to save any changes you entered in the dialog box.

Cancel Button

Click the Cancel button to quit the dialog box and abandon any change you made.

Routing Tab

The Routing tab lets you define routes to remote hosts and networks and establish a default route. You only need to add specific routing information to the routing table if you do not have a default route, or your routers cannot correctly deliver information to a host or network. Normally, you only need to establish a default route, or specifiy that router discovery or RIP be used to route packets. Only add specific routes to the routing table to solve routing problems. The Routing tab contains these fields and buttons:

Destination Address
Shows the IP address of a remote host or IP network address of a remote network defined in the routing table.

Gateway Address
Shows the IP address of the local gateway router used to reach the destination address.

Address Qualifier
Shows whether the destination address is a host address or a network address.

New button
Adds routes to the routing table using the Route dialog box.

Modify button
Modifies the route selected in the routing table.

Delete button
Deletes the selected entry from the routing table.

Routing group
Controls how routing is done by your workstation:

Default Route
Indicates you are using the default route routing method. The default route method directs packets to the default route when a host has no specific route for the destination host or network in its routing table. Enter the IP address of the default route into the edit box.

Router Discovery
Indicates you are using the router discovery routing method. When using router discovery, your workstation broadcasts a message over the network requesting all routers to reply with their IP address. A routing table is then built with the router information received. Your routers must support ICMP router discovery to use this type of routing.

Routing Information Protocol (RIP)
Indicates you are using the Router Information Protocol (RIP) routing method. RIP listens for packets sent by routers that are regularly broadcasting their IP address. This information is used to build and dynamically update a routing table. Your routers must broadcast RIP information to use this type of routing.

Listen for Default Route Only
Determines whether RIP builds a routing table only from default route broadcasts, rather than all router information broadcasts. This is useful if there is only one router on your network, but the router advertises several routes, which can unnecessarily consume memory on your workstation.

Done button
Saves changes made to all tabs in the utility and exits the utility.

See Also:

- Configuring Routing
- Routing Concepts

Routing Table

The Routing table lets you store destination and gateway address information for remote hosts and networks. The display columns are:

- Destination Address: specifies the IP address of a remote host or IP network address of a remote network
- Gateway Address: specifies the IP address of the local gateway router used to reach a destination address
- Address Qualifier: specifies whether the destination address is a host address or a network address

New Button

Click the New button to add a route to the routing table.

Modify Button

Click the Modify button to change information about the selected route.

Delete Button

Click the Delete button to delete the selected route from the Routing table.

Default Route

Click Default Route to choose the default route routing method. The default route method directs packets to the default route when a host has no specific route for the destination host or network in its routing table. If you choose default route, you must enter the IP address of the default route into the Default Route edit box.

Router Discovery

Click Router Discovery to choose router discovery as your routing method. When using router discovery, your workstation broadcasts a message over the network requesting all routers to reply with their IP address. A routing table is then built with the router information received. Your routers must support ICMP router discovery to use this type of routing.

Router Information Protocol (RIP)

Click Router Information Protocol (RIP) to choose RIP as your routing method. RIP listens for packets sent by routers that are regularly broadcasting their IP address. This information is used to build and dynamically update a routing table.   Your routers must broadcast RIP information to use this type of routing.

Listen For Default Route Only

Check Listen For Default Route Only to have RIP build a routing table only from default route broadcasts, rather than from all router information broadcasts. This is useful if there is only one router on your network, but the router advertises several routes, which can unnecessarily consume memory on your workstation.

New or Modify Route Dialog Box

The New or Modify Route dialog box lets you add a route to the Routing table or change information about an existing route.   The dialog box contains these fields:

Destination Address
The IP address of the remote host or IP network address of a remote network you want to reach.

Gateway Address
The IP address of the local gateway router you want to use to reach your destination. The gateway must be on the same subnet as your workstation.

Address Qualifier
Determines whether the destination address is a host address or a network address.

See Also:

- Configuring Routes

Destination Address

Enter the IP address of the remote host or IP network address of the remote network you want to reach.

Gateway Address

Enter the IP address of the local gateway router you want to use to reach your destination. The gateway must be on the same subnet as your workstation.

Host

Click Host to indicate that the destination address for this route is for a host.

Network

Click Network to indicate that the destination address for this route is for a network.

DNS Tab

The DNS (Domain Name System) tab lets you configure the domain name service for your workstation. The DNS tab contains these fields and buttons:

DNS Server IP Address
Lists all DNS servers that your workstation uses to resolve host names to IP addresses.

Up button
Moves the selected IP address up in the DNS server table. The server at the top of the list is queried first, and if it does not respond, the subsequent servers are queried until an answer is returned, or the request times out.

Down button
Moves the selected IP address down in the DNS server table.

New button
Adds the IP address of a DNS server to the DNS server table, using the DNS Server IP Address dialog box.

Modify button
Changes information about the DNS server selected in the DNS server table.

Delete button
Deletes the selected DNS server from the DNS server table.

Search Order group
Controls the order in which DNS servers and host tables are used to resolve host names to IP addresses. Click the Set button to select one of these settings:

DNS only
Resolve host names only with DNS servers, do not use host tables.

DNS then Host Table
Resolve host names with DNS servers; if the host name is not found, use the host table.

Host Table then DNS
Resolve host names with the host table; if the host name is not found, use DNS servers.

Host Table only
Resolve the host name only using the host table.

Done button
Saves changes made to all tabs in the utility and exits the utility.

See Also:

- Configuring DNS
- DNS Concepts

DNS Server IP Address Table

The DNS Server IP Address table lists all DNS servers that your workstation uses to resolve host names to IP addresses.

Up Button

Click the Up button to move the selected DNS server IP address up one line in the DNS Server IP Address table.

Down Button

Click the Down button to move the selected DNS server IP address down one line in the DNS Server IP Address table.

New Button

Click the New button to add a DNS server to the DNS server table.

Modify Button

Click the Modify button to change information about the selected DNS server.

Delete Button

Click the Delete Button to delete the selected DNS server IP address from the DNS Server IP Address table.

Set Button

Click the Set button to change the current search order for host name resolution.

Set Search Order Dialog Box

The Set Search Order dialog box lets you change the current search order for host name resolution.   The dialog box contains these settings:

DNS only
Resolve host names only with DNS servers: do not use host tables.

DNS then Host Table
Resolve host names with DNS servers; if the host name is not found, use the host table.

Host Table then DNS
Resolve host names with the host table; if the host name is not found, use DNS servers.

Host Table only
Resolve the host name only using the host table.

Note:

- The search order you select affects how names are resolved within the stack regardless of whether you set the search order from the DNS tab or the Host Table tab.

DNS only

Click DNS only to make your workstation only look to the domain name server for resolving host names to IP addresses.

DNS then Host Table

Click DNS then Host Table to make your workstation look to the domain name server first and, if the name is not found, then look to its own host table for resolving host names to IP addresses.

Host Table then DNS

Click Host Table then DNS to make your workstation look to the host table first and, if the name is not found, then look to the domain name server for resolving host names to IP addresses.

Host Table only

Click Host Table only to make your workstation look only to its own host table for resolving host names to IP addresses.

New or Modify DNS Server IP Address Dialog Box

The New or Modify DNS Server IP Address dialog box lets you add or change DNS (Domain Name System) server IP addresses. Enter the IP address of a DNS server that is available to your workstation for resolving host names to IP addresses.

DNS Address

Enter the IP address of a DNS server.

Host Table Tab

The Host Table tab lets you store host-name-to-IP address translations on your workstation. By storing translations locally, you ensure that your host can resolve names even if your DNS server is unavailable. The Host Table tab contains these fields and buttons:

Name
Shows the host names entered in the host table.

Aliases
Shows the alternate names that you can use instead of the associated host name. Aliases are optional.

IP Address
Shows the IP address for the host.

Description
Shows an optional description of the host table entry.

New button
Adds an entry to the host table using the New Host dialog box.

Modify button
Changes information about the entry selected in the host table.

Delete button
Deletes the selected entry from the host table.

Search Order group
Controls the order in which DNS servers and host tables are used to resolve host names to IP addresses. Click the Set button to select one of these settings:

DNS only
Resolve host names only with DNS servers: do not use host tables.

DNS then Host Table
Resolve host names with DNS servers; if the host name is not found, use the host table.

Host Table then DNS
Resolve host names with the host table; if the host name is not found, use DNS servers.

Host Table only
Resolve the host name only using the host table.

Done button
Saves changes made to all tabs in the utility and exits the utility.

See Also:

- Configuring Host Tables
- Host Table Concepts

Host Table

The host table lets you store host-name-to-IP-address translations on your workstation. By storing translations locally, you ensure that your host can resolve names even if your DNS server is unavailable. Depending on your environment, you can use a host table in addition to or in place of a DNS server. The display columns are:

- Names: the host name
- Aliases: the optional alternate names for the host name
- IP Address: the IP address for the host
- Description: an optional description of the host table entry

New Button

Click the New button to add a new host to the host table.

Modify Button

Click the Modify button to change information about the selected host.

Delete Button

Click the Delete Button to delete the selected host from the host table.

New or Modify Host Dialog Box

The New or Modify Host dialog box lets you add a host to the Host table or change information about an existing host.   The dialog box contains these fields and buttons:

Host Name
The name of a host you want to add to the host table.

IP Address
The IP address for the host.

Description
An optional description of the host table entry.

Aliases
Alternate names you want to use for this host instead of the host name.   For example, you might want to create a short name for a host that has a long or difficult to remember name.   Enter the alias in the edit box and click the Add button.   To delete an alias, select the alias in the list box and click the Delete button.

See Also:

- Configuring Host Tables
- Host Table Concepts

Host Name

Enter the name of the host you are adding to the host table (for example, `daisy`).

IP Address

Enter the IP address of the host you are adding to the host table (for example, `192.168.128.184`).

Description

Enter any descriptive information you would like to associate with the host.   For example, you might want to indicate who uses the host.

Aliases

The aliases are a list of alternate names, or aliases, associated with the host. Add aliases for the host by typing the new alias into the edit field and clicking the Add button. Remove an alias by selecting the alias and clicking the Delete button. Modify an alias by selecting the alias, changing the text in the edit field, and clicking the Add button.

Add Button

Click the Add button to add aliases to the host. To add an alias, type the new alias into the edit field and click the Add button.

Delete Button

Click the Delete button to remove the selected alias from the alias list for the host.

ARP Tab

Address Resolution Protocol, or ARP, maps IP addresses to hardware addresses. This mapping is almost always performed dynamically by communication between hosts on the same subnet. However, some devices do not respond to ARP requests. The ARP tab lets you manage the ARP table, which stores IP and hardware address pairs for quick lookup. The ARP tab contains these fields and buttons:

Host Address
Shows the host IP addresses that are entered in the ARP table.

Hardware Address
Shows the hardware addresses (also called physical network addresses or Ethernet addresses) that are associated with the host addresses.

Translation
Whether the entry is using proxy or publish translations, or neither. Proxy translation indicates that the local host responds to an ARP request as if it were the target host, in which case the hardware address is not used. Publish translation indicates that the local host responds to an ARP request, supplying the hardware address on behalf of another host.

New button
Adds an entry to the ARP table using the ARP Table Entry dialog box.

Modify button
Changes information about the entry selected in the ARP table.

Delete button
Deletes the selected entry from the ARP table.

Done button
Saves changes made to all tabs in the utility and exits the utility.

See Also:

- Configuring ARP
- ARP Concepts

ARP Table

The ARP table contains IP and hardware address pairs for devices that do not respond to ARP requests. The columns are:

- Host Address: the IP addresses for creating a map between an IP address and a hardware address.
- Hardware Address: the hardware address (also known as physical network address or Ethernet address).
- Translation: whether the ARP table entry is using proxy or publish translation.

New Button

Click the New button to add mappings to the ARP table.

Modify Button

Click the Modify button to change the selected mapping in the ARP table.

Delete Button

Click the Delete button to delete the selected entry from the ARP table.

New or Modify ARP Table Entry Dialog Box

The New or Modify ARP Table Entry dialog box lets you add an IP and hardware address pair to the ARP table or change information about an existing address pair. The dialog box contains these fields:

Host Address
The IP address of a host.

Hardware Address
The physical network address for the host, for example, `00:DD:A8:13:48:C5`. (For Ethernet, this string of six hexadecimal numbers is assigned to the Ethernet controller card. For Token-Ring, this address is assigned by your network administrator.)

Translation group
Whether the entry is using proxy or publish translations, or neither. Proxy translation indicates that the local host responds to an ARP request as if it were the target host, in which case the hardware address is not used. Publish translation indicates that the local host responds to an ARP request, supplying the hardware address on behalf of another host.

Host Address

Enter the IP address of the host, for example, `192.168.34.22`.

Hardware Address

Enter the physical network address of the host, for example, `00:DD:A8:13:48:C5`. (For Ethernet, this string of six hexadecimal numbers is assigned to the Ethernet controller card. For Token-Ring, this address is assigned by your network administrator.)

Proxy

Check Proxy to have the local host respond to an ARP request as if it were the target host, in which case the hardware address is not used.

Publish

Check Publish to have the local host respond to an ARP request, supplying the hardware address on behalf of another host.

LM Host Table Tab

The LM Host Table tab lets you create a LAN Manager Hosts file. This file, named LMHOSTS, contains entries that map NetBIOS names to IP addresses, and is only used if you are using NetBIOS applications over a TCP/IP network. Use the NBT tab to enable NetBIOS over TCP/IP.

See Also:

- Configuring NetBIOS over TCP/IP
- Creating an LM Host Table
- Understanding NetBIOS over TCP/IP

LM Host Table

The LM host table is used to resolve NetBIOS names to IP addresses. Each record contains these fields:

- IP Address: the IP address of the machine with the associated NetBIOS name.
- Name: the NetBIOS name.
- Flags: optional switches that determine how the entry is processed. For example, #DOM indicates the entry is a domain controller, and includes the name of the LAN Manager domain that you want to log into. #PRE indicates that you want the entry preloaded into the NBT cache, so that a frequently used name can be resolved to a IP address quickly.
- Description: an optional description of the entry, preceded by the # character.

NBT Name Registration/Resolution Dialog Box

The NBT Name Registration/Resolution dialog box lets you determine the order in which NetBIOS name resolution resources should be searched when resolving a NetBIOS name into an IP address.   You can select one of these:

Use broadcasts to resolve names (b-node)

Indicates that you want to use broadcast messages but not WINS servers to announce your workstation's NetBIOS name to the network, and that you only want to use broadcasts to find other users workstations.   This is known as a b-node.

Use WINS to resolve names (p-node)

Indicates that you want to use WINS servers but not broadcast messages to register your workstation's NetBIOS name on the network, and that you only want to use WINS servers to learn of other user's workstations.   This is known as a p-node.

Use broadcasts first, then WINS to resolve name (m-node)

Indicates that you want to register your workstation with the WINS server, but you want to use broadcast messages before using WINS servers to resolve NetBIOS names to IP addresses.   This is known as an m-node.

Use WINS first, then broadcasts to resolve names (h-node)

Indicates that you want to register your workstation with the WINS server, and you want to use WINS servers before using broadcast messages to resolve NetBIOS names to IP addresses.   This is known as an h-node.

See Also:

- Configuring NetBIOS over TCP/IP

Use Broadcasts To Resolve Names

Click Use broadcasts to resolve names if you want to use broadcast messages but not WINS servers to announce your workstation's NetBIOS name to the network, and you only want to use broadcasts to find other user's workstations.   This is known as a b-node.

Use WINS To Resolve Names Radio Button

Click Use WINS to resolve names if you want to use WINS servers but not broadcast messages to register your workstation's NetBIOS name on the network, and you only want to use WINS servers to learn of other user's workstations.   This is known as a p-node.

Use Broadcasts First, Then WINS To Resolve Names Radio Button

Click Use broadcasts first, then WINS to resolve names if you want to register your workstation with the WINS server, but you want to use broadcast messages before using WINS servers to resolve NetBIOS names to IP addresses.   This is known as an m-node.

Use WINS First, Then Broadcasts To Resolve Names Radio Button

Click Use WINS first, then broadcasts to resolve names if you want to register your workstation with the WINS server, and you want to use WINS servers before using broadcast messages to resolve NetBIOS names to IP addresses.   This is known as an h-node.

NBT Tab

The NBT tab lets you configure Cisco TCP/IP Suite so that you can run NetBIOS applications over a TCP/IP network. The tab contains these fields and buttons:

Enable NetBIOS over TCP/IP (TDI)
Determines whether you can use NetBIOS applications over a TCP/IP network.

Primary WINS server address
The IP address of the primary WINS server you are using to resolve NetBIOS names to IP addresses.

Secondary WINS server address
The IP address of the secondary, or backup, WINS server you are using to resolve NetBIOS names to IP addresses.

NetBIOS Scope ID
The NetBIOS scope name if your workstation is part of a NetBIOS scope. This is usually blank. If you enter a scope, you are only able to communicate to hosts that belong to this scope when using NetBIOS applications.

LANA Number
The LAN Adapter (LANA) number that NetBIOS should use. Windows assigns LANA numbers dynamically, so leave this field blank unless a NetBIOS application you use requires a specific LANA number.

Enable NBT DNS
Determines whether NetBIOS applications use DNS servers to resolve NetBIOS names to IP addresses. DNS servers are only checked after broadcast messages, WINS servers, and LM host tables are checked, if you use them.

Enable WINS Proxies
Determines whether your workstation acts as a WINS proxy for your network. Ask your network administrator if your workstation should be a WINS proxy server.

Name Registration/Resolution group
Controls how NetBIOS applications learn about your workstation and how TCP/IP resolves NetBIOS names to IP addresses. Click the Set button to change the order in which broadcast messages and WINS servers are used for name registration and resolution.

See Also:

- Configuring NetBIOS over TCP/IP
- Understanding NetBIOS over TCP/IP

Enable NetBIOS over TCP/IP (TDI)

Check NetBIOS over TCP/IP to enable NetBIOS over TCP/IP.

Primary WINS Server

Enter the IP address of the primary WINS server you are using to resolve NetBIOS names to IP addresses.

Secondary WINS Server

Enter the IP address of the secondary, or backup, WINS server you are using to resolve NetBIOS names to IP addresses.

Enable WINS Proxies

Check Enable WINS Proxies to make your workstation act as a WINS proxy for your network. Ask your network administrator if your workstation should be a WINS proxy server.

NetBIOS Scope

Enter the NetBIOS scope name if your workstation is part of a NetBIOS scope. This is usually blank. If you enter a scope, you are only able to communicate to hosts that belong to this scope when using NetBIOS applications.

LANA Number

Enter the LAN Adapter (LANA) number that NetBIOS should use.   Windows assigns LANA numbers dynamically, so leave this field blank unless a NetBIOS application you use requires a specific LANA number.

Set Button, Name Registration/Resolution Group

The Name Registration/Resolution group displays the current setting for how NetBIOS applications learn about your workstation and how NetBIOS resolves NetBIOS names to IP addresses.   Click the Set button to set or change this registration and search order.

Enable NBT DNS

Check Enable NBT DNS to indicate whether NetBIOS applications should use DNS servers to resolve NetBIOS names to IP addresses.   DNS servers are only checked after broadcast messages, WINS servers, and LM host tables are checked, if you use them.

Global Tab

The Global tab features settings that affect more than one aspect of the TCP/IP stack. The Global tab contains these fields:

PC Host Name
The host name for your workstation. For example, if your fully-qualified host name is `willow.yoyodyne.com`, the host name is `willow`.

Local Domain Name
Your organizations domain name. This name does not include your host name. For example, if your fully-qualified host name is `willow.yoyodyne.com`, the domain is `yoyodyne.com`. If you do not know the name for your domain, ask your network administrator.

Time Zone
Your time zone.

Enable IP Forwarding
Determines whether your machine is a gateway router between networks if you are using a serial and LAN interface simultaneously. If you enable IP forwarding, your machine can then forward IP packets between the networks to which you are connected, as if it were a dedicated router.

Desktop Options group
Controls the products icon. Check Cheetah Icon Visible When Active to have the icon appear on the desktop when TCP/IP is active. Check Cheetah Icon Animated to make the cheetah on the icon run when TCP/IP is accessed. If the cheetah is set for animation and is moving, the movement generally indicates that TCP/IP is working correctly.

See Also:

- Configuring Global Parameters
- Global Parameters Concepts

PC Host Name

Enter the host name of your workstation.   For example, if your fully-qualified host name is `willow.yoyodyne.com` (on the yoyodyne.com domain), your host name is `willow`.

Local Domain Name

Enter your organizations domain name. This name does not include your host name. For example, if your fully-qualified host name is `willow.yoyodyne.com`, the domain is `yoyodyne.com`. If you do not know the name for your domain, ask your network administrator.

Time Zone

Select the time zone in which your workstation resides.

Enable IP Forwarding

Check Enable IP Forwarding to make your machine a gateway router between networks if you are using a serial and LAN interface simultaneously.   Your machine can then forward IP packets between the networks to which you are connected, as if it were a dedicated router.

Cheetah Icon Visible When Active

Check Cheetah Icon Visible When Active to display the cheetah icon on your Windows desktop when TCP/IP is accessed.

Cheetah Icon Animated

Check Cheetah Icon Animated to make the cheetah on the icon run when TCP/IP is accessed.

Cisco TCP/IP Suite Online Help

Configuring Network Interfaces

Use the Interface tab to add, change, or delete Ethernet or Token-Ring network interface card information.

Before starting, obtain the interface label, Interface Type, IP address for the network interface card, the subnet mask, the broadcast address, and the driver type from your network administrator.

If you have not installed a network driver, you must also know the path and file name of the driver so that it can be installed.

Use the Interface tab in the Cisco TCP/IP Suite Configuration Utility to:

- Create a new LAN interface
- Create a new serial interface
- Modify an existing interface
- Delete an interface

You can also:

- Change an interface label
- Change an interface type
- Change the interface subnet mask
- Change the interface broadcast address
- Enable or disable dynamic configuration
- Enable or disable an interface
- Change the interface driver

Creating a New LAN Interface

To create a new LAN network interface:

1. Obtain the interface label, Interface Type, IP address for the network interface card, the subnet mask, the broadcast address, and the driver type from your network administrator. If a network driver is not installed on your system, you need the driver name. If your workstation uses ODI or Windows 3.1, you also need the path and file name of the driver.
2. Choose the Interface tab in the Configuration Utility.
3. Click the New button. The New Interface dialog box appears.
4. Enter the interface label and Interface Type.
5. If you want to use dynamic configuration, check the Dynamic Configuration check box. If you use dynamic configuration, the IP address, subnet mask, and broadcast address edit boxes are all grayed. There is no need to enter anything in these edit boxes.
6. If you do not use dynamic configuration, enter the IP address for the network interface card, the subnet mask, the broadcast address (if required by your site).
7. Check Enable Interface.
8. Choose the driver type (ODI, NDIS2, or NDIS3) that your system uses for this network interface.
9. To add the network interface, click the OK button. To abandon the network interface changes, click the Cancel button. If the Configuration Utility does not detect a network interface driver in memory, it asks if you would like to install one.
10. To install a driver now, click the Yes button. To install the driver at a later time, click the No button.
11. Either select the desired network driver or enter the path and file name of the driver as requested. The new interface appears in the interface table.
12. To exit, click the Done button. Changes take effect the next time Windows starts.

Note

If other hosts need to reach your computer by host name, your host name and IP address must be registered in DNS (via a DNS server) or in the host tables on other computers.

Creating a New Serial Interface for Use With Dialer

To create a new serial network interface:

1. Choose the Interface tab in the Configuration Utility.
2. Click the New button. The New Interface dialog box appears.
3. Enter the interface label
4. Choose serial for the Interface Type.
5. Check Enable Interface.   Serial interfaces can be enabled at the same time as LAN interfaces.
6. Choose the driver type (ODI, NDIS2, or NDIS3) that your system uses for this network interface.   If the driver is not already on your system, you must add it now.
7. To exit, click the Done button. Changes take effect the next time Windows starts.

Tips:

- Most interface information for serial interfaces must be defined in Dialer when you configure Dialer's manual interface or when you create Dialer profiles.   In Dialer, you define the IP address, subnet mask, and broadcast address for the interface, as well as the information for the modem and modem port.   If you do not use dynamic configuration to obtain an IP address for serial interfaces, obtain the IP address, subnet mask, and broadcast address from your network administrator.   If you use dynamic configuration, use the Dialer defaults for these attributes.
- Serial interfaces do not use the information defined on the DNS and Routing tabs.   You must define this information in the Dialer manual configuration and Dialer profiles.   In general, use your workstation as the default route for serial interfaces.
- Serial interfaces do not use the host name and domain name defined on the Global tab. You must define this information in the Dialer manual configuration and Dialer profiles. If you are using dynamic configuration, you do not need to specify a host name for your system.   Defining the domain name is also optional: however, if you do not define the domain name, you must use fully-qualified host names to connect to other hosts using Telnet, FTP Client, or any other application.
- If you are connecting to more than one network at the same time, for example, a LAN network and a serial connection, you can have your workstation act as a router between the networks by enabling IP forwarding.
- The interface is not activated until you restart Windows.

Modifying an Existing Interface

To modify an existing network interface:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to modify.   If you are changing the network driver, you need the new driver name. If your PC uses ODI or Windows 3.1, you also need the path and file name of the driver.
3. Click the Modify button. The Modify Interface dialog box appears.
4. Modify the required parameters.
5. To add the network interface, click the OK button. To abandon the network interface changes, click the Cancel button.   If the Configuration Utility does not detect a network interface driver in memory, it asks if you would like to install one.
6. To install a driver now, click the Yes button. To install the driver at a later time, click the No button.
7. Either select the desired network driver or enter the path and file name of the driver as requested. The new interface appears in the interface table.
8. To add the network interface, click the OK button. To abandon the network interface changes, click the Cancel button.
9. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Deleting an Interface

To remove a network interface from the interface table:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to remove.
3. Click the Delete button. The Configuration Utility asks you to confirm the operation.
4. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Changing the Interface Label

To modify an existing interface label:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to modify.
3. Click the Modify... button. The Modify Interface dialog box appears.
4. In the Interface Label edit box, enter the new interface label provided by your network administrator.
5. To save your changes, click the OK button. To abandon changes, click the Cancel button.
6. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Changing an Interface Type

To modify an existing interface type:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to modify.
3. Click the Modify... button. The Modify Interface dialog box appears.
4. In the Interface Type drop-down list, select the new interface type provided by your network administrator.
5. To save your changes, click the OK button. To abandon changes, click the Cancel button.
6. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Changing the Interface IP Address

To change the IP address of a network interface:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to modify.
3. Click Modify.... The Modify Interface dialog box appears.
4. In the IP Address edit box, enter the IP Address provided by your network administrator.
5. To save your changes, click the OK button. To abandon changes, click the Cancel button.
6. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.
7. Make sure the new IP address is registered in DNS (via a DNS server) or in the host tables on other computers.

Changing the Interface Subnet Mask

To modify an existing subnet mask:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to modify.
3. Click the Modify... button. The Modify Interface dialog box appears.
4. In the Subnet Mask edit box, enter the subnet mask provided by your network administrator.
5. To save your changes, click the OK button. To abandon changes, click the Cancel button.
6. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Changing the Interface Broadcast Address

To modify an existing broadcast address:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to modify.
3. Click the Modify... button. The Modify Interface dialog box appears.
4. In the Broadcast Address edit box, enter the broadcast address provided by your network administrator.
5. To save your changes, click the OK button. To abandon changes, click the Cancel button.
6. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Enabling and Disabling Dynamic Configuration

To enable or disable dynamic configuration:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to enable or disable.
3. Click the Modify... button. The Modify Interface dialog box appears.
4. To enable dynamic configuration, check Dynamic Configuration.
5. To disable dynamic configuration, clear Dynamic Configuration.
6. To confirm the change, click the OK button. To abandon the change, click the Cancel button.
7. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Enabling and Disabling Interfaces

To enable or disable an existing network interface:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to enable or disable.
3. Click the Modify... button. The Modify Interface dialog box appears.
4. To enable the interface, check Enable Interface.   To disable the interface, clear Enable Interface.
5. To confirm the change, click the OK button. To abandon the change, click the Cancel button.
6. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Tip:

- Only one LAN interface can be enabled at the same time.   However, you can enable serial interfaces with LAN interfaces.

Changing the Interface Driver

To change the network driver:

1. Choose the Interface tab in the Configuration Utility.
2. In the interface table, select the interface you want to enable or disable.
3. Click the Modify button. The Modify Interface dialog box appears.
4. In the Driver Group, choose the driver type.
5. To add the network interface, click the OK button. To abandon the network interface changes, click the Cancel button.   If the Configuration Utility does not detect a network interface driver in memory, it asks if you would like to install one.
6. To install a driver now, click the Yes button. To install the driver at a later time, click the No button.
7. Either select the desired network driver or enter the path and file name of the driver as requested. The new interface appears in the interface table.
8. To exit the Configuration Utility, click the Done button. Changes take effect the next time Windows starts.

Interface Type

Interface types are Ethernet, serial, FDDI, and Token-Ring. Your network administrator provides the type of interface supported by your network interface card.

Interface Label

A text string that you or your network administrator chooses to identify the network interface card. The string can be up to 256 characters long.

Driver Type

The type of network driver used by your Ethernet or Token-Ring network interface card to interact with the network operating system. If your system uses Novell NetWare, an ODI (Open Data-Link Interface) driver is required. If your PC uses Windows for Workgroups and your network interface card provides an NDIS (Network Device Interface Specification) 3 driver, specify this type. Otherwise, if your PC uses LAN Manager, Banyan Vines, or the NDIS version of Pathworks, specify the NDIS 2 driver.

Configuring Routes

Use the Routing tab to add, modify, or delete routes in the routing table.   Before adding or changing an entry, obtain routing information from your network administrator.

Use the Routing tab in the Cisco TCP/IP Suite Configuration Utility to:

- Add new routes
- Modify existing routes
- Delete routes
- Choose a routing method

You can also:

- Change the destination address
- Change a gateway address
- Change the address qualifier

Adding New Routes

To add a new route to the routing table:

1. Choose the Routing tab in the Configuration Utility.
2. Click the New... button. The New Route dialog box appears.
3. Enter the IP address of the destination host or network.
4. Enter the IP addresses of the gateway through which the destination can be reached.
5. Specify the type of destination in the Address Qualifier group.
6. To add the new route, click the OK button. The new route appears in the routing table.
7. To exit the Configuration Utility, click the Done button. The new route takes effect the next time Windows starts.

Modifying Existing Routes

To modify an existing route in the routing table:

1. Choose the Routing tab in the Configuration Utility.
2. In the routing table, select the route you want to modify.
3. Click the Modify... button. The Modify Route dialog box appears.
4. Enter the IP address of the destination host or network.
5. Enter the IP addresses of the gateway through which the destination can be reached.
6. Specify the type of destination in the Address Qualifier group.
7. To add the modified route, click the OK button. The modified route appears in the routing table.
8. To exit the Configuration Utility, click the Done button. The new route takes effect the next time Windows starts.

Deleting Routes

To delete a route from the routing table:

1. Choose the Routing tab in the Configuration Utility.
2. In the routing table, select the route you want to delete.
3. Click the Delete button.
4. When prompted, click the OK button to confirm the delete operation. The route no longer appears in the routing table.
5. To exit the Configuration Utility, click the Done button. The new route takes effect the next time Windows starts.

Choosing a Routing Method

Cisco TCP/IP Suite requires a routing method to route packets.

To choose a routing method for your computer:

1. Choose the Routing tab in the Configuration Utility.
2. Click the radio button corresponding to the routing method you want to use.
3. If you choose to use a default route, enter the IP address of the default route in the Default Route edit box.
4. If you choose RIP and you want to listen only for a default route, check the Listen for Default Route Only check box. Router Discovery must be enabled on your routers to use RIP.
5. To exit the Configuration Utility, click the Done button. The new route takes effect the next time Windows starts.

Changing a Destination Address

To change the existing destination address in the routing table:

1. Choose the Routing tab in the Configuration Utility.
2. In the routing table, select the route you want to modify.
3. Click the Modify... button. The Modify Route dialog box appears.
4. Enter the IP address of the destination host or network.
5. To add the changed address, click the OK button. The changed route appears in the routing table.
6. To exit the Configuration Utility, click the Done button. The new route takes effect the next time Windows starts.

Changing a Gateway Address

To change the existing gateway address in the routing table:

1. Choose the Routing tab in the Configuration Utility.
2. In the routing table, select the route you want to modify.
3. Click the Modify... button. The Modify Route dialog box appears.
4. Enter the IP addresses of the gateway through which the destination can be reached.
5. To add the changed address, click the OK button. The changed route appears in the routing table.
6. To exit the Configuration Utility, click the Done button. The new route takes effect the next time Windows starts.

Changing the Address Qualifier

To change the existing address qualifier in the routing table:

1. Choose the Routing tab in the Configuration Utility.
2. In the routing table, select the route you want to modify.
3. Click the Modify... button. The Modify Route dialog box appears.
4. Specify the type of destination in the Address Qualifier group.
5. To add the changed address, click the OK button. The changed route appears in the routing table.
6. To exit the Configuration Utility, click the Done button. The new route takes effect the next time Windows starts.

Configuring DNS

Use the DNS tab to add, change, or delete DNS (Domain Name System) information. Cisco TCP/IP Suite DNS acts as a resolver, which means that each time you specify a computer by name in a TCP/IP application, Cisco TCP/IP Suite sends requests to the first computer listed in the DNS Server IP Address table to translate the name to an IP address. While TCP/IP applications accept either computer names or IP addresses, the network only understands IP addresses. Your network administration provides the DNS server IP addresses and the order in which they are listed in the table.

Use the DNS tab in the Cisco TCP/IP Suite Configuration Utility to:

- Add a new IP address to the DNS Server IP Address table
- Change an existing IP address
- Delete an IP address from the DNS Server IP Address table
- Set the order in which DNS servers are accessed for name resolution
- Specify whether DNS and Host tables are accessed together or exclusively

Adding a New DNS Server IP Address

To add a new IP address to the DNS Server IP Address table:

1. Choose the DNS tab in the Configuration Utility.
2. Click the New button.   The new DNS server IP address dialog box appears.
3. Enter the IP address of a DNS server.
4. To add the IP address, click the OK button. To abandon the add operation, click the Cancel button. The new DNS server appears in the DNS Server IP Address table.
5. To exit the Configuration Utility, click the Done button. The change takes effect the next time Window starts.

Modifying a DNS Server IP Address

To change an existing IP address in the DNS Server IP Address table:

1. Choose the DNS tab in the Configuration Utility.
2. In the DNS Server IP Address table, select the entry you want to modify.
3. Click the Modify button. The Modify DNS Server IP Address dialog box appears.
4. Position the cursor on the section of the IP address to change, or select the full number and replace the value with a new number.
5. To confirm the change, click the OK button. To abandon the change, click the Cancel button. The modified DNS server IP address appears in the DNS Server IP Address table.
6. To exit the Configuration Utility, click the Done button. The change takes effect the next time Window starts.

Deleting a DNS Server IP Address

To delete an IP address from the DNS Server IP Address table:

1. Choose the DNS tab in the Configuration Utility.
2. In the DNS Server IP Address table, select the entry you want to delete.
3. Click the Delete button.
4. When prompted, confirm the delete operation by clicking the OK button. The DNS server no longer appears in the DNS Server IP Address table.
5. To exit the Configuration Utility, click the Done button. The change takes effect the next time Window starts.

Positioning an IP Address

To position an IP address in the DNS Server IP Address table:

1. Choose the DNS tab in the Configuration Utility.
2. If the DNS Server IP Address table contains more than one entry, select the entry in the table.
3. Click the Up or Down button to position the entry either upwards or downwards as required. Servers are queried from top to bottom. If a server does not answer a name request, subsequent servers are tried until an answer is received or the request times out.
4. To exit the Configuration Utility, click the Done button. The change takes effect the next time Window starts.

Setting the DNS and Host Table Search Order

To change the relationship between DNS and host tables so that either DNS or host tables are accessed first or exclusively:

1. Choose the DNS tab in the Configuration Utility.
2. Click the Set... button in the Search Order group. The Set Search Order dialog box appears.
3. Select the preferred radio button.
4. To save the search order, click the OK button. The current search order appears in the Current Setting indicator window.
5. To exit the Configuration Utility, click the Done button. The change takes effect the next time Window starts.

Configuring Host Tables

Use the Host Table tab to add, modify, or delete a host table entry. A host table contains one or more entries that map the name of a computer to its IP address. A host table entry specifies a computer name, its IP address, any optional aliases that reference the computer name, and an optional description. You can also change the search order so that host tables are used with DNS or exclusively. Before adding or changing an entry, obtain host table information from your network administrator. Ensure that any other computers you need to access are also listed in your host table.

Use the Host Table tab in the Cisco TCP/IP Suite Configuration Utility to:

- Add a new host table entry
- Change an existing host table entry
- Remove an existing host table entry
- Change the search order

You can also:

- Change the computer name
- Change an IP address
- Change an alias
- Change a host table description

Adding Hosts to the Host Table

To add a new host table entry:

1. Choose the Host Table tab in the Configuration Utility.
2. Click the New... button. The New Host dialog box appears.
3. Specify the host name and IP address of the host you want to add to the host table.
4. If desired, enter a description of the host.
5. If desired, enter aliases for this host in the Aliases combo box and click the Add button. To remove an unwanted alias, select it and click the Delete button.
6. To save the new host table entry, click the OK button. The new entry appears in the host table.
7. Click the Set... button in the Search Order group. The Set Search Order dialog box appears.
8. Make sure that the DNS Only option is not selected.
9. If you want Cisco TCP/IP Suite to use DNS if the host table fails to resolve names, choose Host Table then DNS (you must add DNS servers to the DNS Server IP Address table on the DNS tab to take advantage of this option).
10. To save the search order, click the OK button.
11. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Modifying the Host Table

To modify an existing host table entry:

1. Choose the Host Table tab in the Configuration Utility.
2. In the host table, select the entry you want to modify.
3. Click the Modify button. The Modify Host dialog box appears.
4. Modify the name and IP address of the host table entry.
5. If desired, modify the description of the host.
6. If desired, enter aliases for this host in the Aliases combo box and click the Add button. To remove an unwanted alias, select it and click the Delete button.
7. To save the modified host table entry, click the OK button. The modified entry appears in the host table.
8. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Deleting Hosts from the Host Table

To delete an existing host table entry:

1. Choose the Host Table tab in the Configuration Utility.
2. In the host table, select the entry you want to modify.
3. Select the host table entry you want to delete.
4. Click the Delete button.
5. When prompted, confirm the delete operation by clicking the OK button. The entry no longer appears in the host table.
6. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Setting the Search Order for Name Resolution

To change the search order between host tables and DNS:

1. Choose the Host Table tab in the Configuration Utility.
2. In the host table, select the entry you want to modify.
3. Click the Set... button in the Search Order group. The Set Search Order dialog box appears.
4. Make sure that the DNS Only option is not selected.
5. If you want Cisco TCP/IP Suite to use DNS if the host table fails to resolve names, choose Host Table then DNS (you must add DNS servers to the DNS Server IP Address table on the DNS tab to take advantage of this option).
6. To save the search order, click the OK button.
7. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Changing the Host Name

To modify an existing host name:

1. Choose the Host Table tab in the Configuration Utility.
2. In the host table, select the entry you want to modify.
3. Click the Modify... button. The Modify Host dialog box appears.
4. Enter the new host name provided by your network administrator.
5. To save the changed host table entry, click the OK button. The changed entry appears in the host table.
6. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Changing the Host IP Address

To modify an existing host IP address:

1. Choose the Host Table tab in the Configuration Utility.
2. In the host table, select the entry you want to modify.
3. Click the Modify... button.   The Modify Host dialog box appears.
4. Enter the new host IP address provided by your network administrator.
5. To save the changed host table entry, click the OK button. The changed entry appears in the host table.
6. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Changing a Description for the Host

To modify an existing host description:

1. Choose the Host Table tab in the Configuration Utility.
2. In the host table, select the entry you want to modify.
3. Click the Modify... button.   The Modify Host dialog box appears.
4. Change the description in the Description edit box.
5. To save the changed host table entry, click the OK button. The changed entry appears in the host table.
6. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Specifying Host Aliases

To change an existing alias in the host table:

1. Choose the Host Table tab in the Configuration Utility.
2. In the host table, select the entry you want to modify.
3. Click the Modify... button.   The Modify Host dialog box appears.   The Aliases group lists the current aliases.
4. To modify an existing alias, select the alias you want to change and either edit the alias name or click the Delete button to remove the alias.
5. To enter a new alias, enter the alias and click the Add button.
6. To save the modified alias list, click the OK button.
7. To exit the Configuration Utility, click the Done button. The host table changes take effect the next time Windows starts.

Configuring ARP

Use the ARP tab to add, modify, or delete ARP table entries. ARP maps an IP address to the hardware address of an Ethernet or Token-Ring controller. Entries listed in the ARP table indicate that your computer can receive ARP requests from other computers.

The contents of the ARP table can provide useful diagnostic information. For example, if two machines have the same IP address, the ARP table may include conflicting entries for these machines.

Before adding or changing an entry, obtain ARP table information from your network administrator.

Warning!

> Adding or modifying entries in the ARP table can seriously affect communications. Do not create or change ARP table entries unless you are sure of their effects on your network.

Use the ARP tab in the Cisco TCP/IP Suite Configuration Utility to:

- Add a new ARP table entry
- Modify an existing ARP table entry
- Remove an existing ARP table entry

You can also:

- Change a host address
- Change a hardware address
- Select a proxy or publish translation

Adding a New ARP Table Entry

To add a new ARP table entry:

1. Obtain a host address, an Ethernet or Token-Ring hardware address, and an optional translation status (proxy or publish) from your network administrator.
2. Choose the ARP tab in the Configuration Utility.
3. Click the New... button. The New ARP Table Entry dialog box appears.
4. Enter the host IP address and corresponding hardware address for the Ethernet or Token-Ring controller.
5. To publish a translation on another host's behalf, or if you need to create a proxy translation, check the appropriate check box in the Translation group.
6. To save the new mapping, click the OK button. The new entry appears in the ARP table.
7. To exit the Configuration Utility, click the Done button. The new mapping takes effect the next time Windows starts.

Modifying an ARP Table Entry

To modify an ARP table entry:

1. Choose the ARP tab in the Configuration Utility.
2. In the ARP table, select the ARP table entry you want to modify.
3. Click the Modify... button. The Modify ARP Table Entry dialog box appears.
4. Modify the host IP address or its hardware address.
5. To publish the translation on another hosts behalf, or if you need to create a proxy translation, check the appropriate check box.
6. To save the modified mapping, click the OK button. The new entry appears in the ARP table.
7. To exit the Configuration Utility, click the Done button. The new mapping takes effect the next time Windows starts.

Deleting an ARP Table Entry

To delete an ARP table entry:

1. Choose the ARP tab in the Configuration Utility.
2. In the ARP table, select the ARP table entry you want to delete.
3. Click the Delete button.
4. When prompted, confirm the delete operation by clicking the OK button. The entry no longer appears in the ARP table.
5. To exit the Configuration Utility, click the Done button. The new mapping takes effect the next time Windows starts.

Changing an ARP Host Address

To change an existing host address:

1. Choose the ARP tab in the Configuration Utility.
2. In the ARP table, select the ARP table entry you want to modify.
3. Click the Modify... button.   The ARP Table Entry dialog box appears.
4. In the host address edit box, enter the host IP address provided by your network administrator.
5. To save the new mapping, click the OK button. The new entry appears in the ARP table.
6. To exit the Configuration Utility, click the Done button. The new mapping takes effect the next time Windows starts.

Changing an ARP Hardware Address

To change an existing hardware address:

1. Choose the ARP tab in the Configuration Utility.
2. In the ARP table, select the ARP table entry you want to modify.
3. Click the Modify... button.   The Modify ARP Table Entry dialog box appears.
4. In the Hardware Address edit box, enter the hardware address provided by your network administrator.
5. To save the new mapping, click the OK button. The new entry appears in the ARP table.
6. To exit the Configuration Utility, click the Done button. The new mapping takes effect the next time Windows starts.

Selecting an ARP Proxy or Publish Translation

To change a proxy or publish translation:

1. Choose the ARP tab in the Configuration Utility.
2. In the ARP table, select the ARP table entry whose proxy or publish translation you want to modify.
3. Click the Modify... button. The Modify ARP Table Entry dialog box appears.
4. Check or clear the Proxy and Publish check boxes as described by your network administrator.
5. To save the new mapping, click the OK button. The new entry appears in the ARP table.
6. To exit the Configuration Utility, click the Done button. The new mapping takes effect the next time Windows starts.

Publish

Normally, Cisco TCP/IP Suite uses the ARP table to quickly obtain the hardware address of other hosts. You can configure Cisco TCP/IP Suite to publish ARP translations in response to ARP requests by checking the Publish option in the ARP Table Entry dialog when adding or modifying ARP table entries. If the Publish option is disabled, the mapping is only used by your Cisco TCP/IP Suite host; other hosts on the network cannot take advantage of the mapping. Enable the Publish option to provide ARP translations on behalf of other hosts that are unable to respond to ARP requests.

Proxy

You can configure Cisco TCP/IP Suite to respond to ARP requests with the hardware address of a local network interface by verifying the Proxy translation option is checked when adding or modifying the ARP table entry.

Using proxy ARP translations for routing purposes allows the remote host to appear to be on the same network segment as the network adapter, eliminating the need for additional subnets.

Configuring NetBIOS Over TCP/IP

Use the NBT and LM Host Table tabs to configure NetBIOS over TCP/IP. NetBIOS over TCP/IP allows you to use NetBIOS applications over a TCP/IP network.

Use the NBT tab to enable NetBIOS over TCP/IP and identify any WINS servers you want to use, or a LANA number, if one of your NetBIOS applications requires a specific number.

Use the LM Host Table tab to create and manage a LAN Manager Host table, which is used for NetBIOS to IP address resolution if you are not using WINS servers, or if the NetBIOS name can not be found in the WINS server.

Use the NBT and LM Host Table tabs in the Cisco TCP/IP Suite Configuration Utility to:

- Set up NetBIOS over TCP/IP
- Create an LM Host Table

See Also:

- Understanding NetBIOS over TCP/IP

Setting Up NetBIOS Over TCP/IP

Use the NBT tab to:

- Enable or disable NetBIOS over TCP/IP
- Identify WINS Servers for NetBIOS name resolution
- Make your workstation a WINS proxy server
- Set the search order for NetBIOS name resolution
- Enable NetBIOS to use DNS servers to resolve NetBIOS names to IP addresses
- Set a NetBIOS scope for your workstation
- Set a LAN adapter (LANA) number

See Also:

- Creating an LM host table
- Understanding NetBIOS over TCP/IP

Enabling or Disabling NetBIOS Over TCP/IP

To enable or disable NetBIOS over TCP/IP:

1. Choose the NBT tab in the Configuration Utility.
2. Check NetBIOS over TCP/IP (TDI) to enable it, uncheck it to disable it.

Notes:

- The change is not complete until you restart Windows.
- NetBIOS over TCP/IP lets you encapsulate NetBIOS or NetBEUI packets in IP packets. This lets you use Windows peer networking with your TCP/IP network.
- If you are enabling NetBIOS over TCP/IP, you also need to set up NetBIOS-name-to-IP-address name resolution.   You can use WINS servers (defined on the NBT tab), LM host tables (LM Host Table tab), or the DNS servers used to resolved TCP/IP host names to IP addresses, if your NetBIOS names are the same as your host names (DNS tab).
- Ask your network administrator if your workstation is part of a NetBIOS scope, or if any of your applications require a specific LANA number.

Identifying WINS Servers for NetBIOS Name Resolution

To identify WINS servers for NetBIOS name resolution:

1. Choose the NBT tab in the Configuration Utility.
2. Enter the IP address of the primary WINS server in the Primary WINS server address field.
3. If there is a backup WINS server (in case the primary is not available), enter its IP address in the Secondary WINS server address field.

Notes:

- Ask your network administrator for the IP addresses of the WINS servers you should use.
- The change is not complete until you restart Windows.

Making Your Workstation a WINS Proxy Server

To make your workstation a WINS proxy server:

1. Choose the NBT tab in the Configuration Utility.
2. Check Enable WINS Proxies.

Notes:

- Ask your network administrator if you should define your machine as a WINS proxy server.
- The change is not complete until you restart Windows.
- To disable your proxy server, uncheck Enable WINS Proxies.

Setting the Search Order for NetBIOS Name Resolution

To set the search order for NetBIOS name resolution:

1. Choose the NBT tab in the Configuration Utility.
2. Click the Set button.
3. Select the order in which you want broadcast messages and WINS servers to be searched when Cisco TCP/IP Suite tries to resolve a NetBIOS name into an IP address.
4. Click the OK button.
5. To have NetBIOS applications also search the LM host table, check Enable LM Host Table on the LM Host Table tab.
6. To have NetBIOS applications also search DNS servers, check Enable NBT DNS on the NBT tab.

Notes:

- This search order is only used if NetBIOS over TCP/IP is enabled on the NBT tab.
- This search order is not related to the TCP/IP host name search order set on the Host Table or DNS tabs.
- If you use WINS servers, your workstations NetBIOS name is registered with the WINS servers when you use NetBIOS.
- If you use it, the LM host table is only searched after broadcast messages and WINS servers are searched (if used). However, any entries in the LM host table that you preload are searched before broadcast messages are issued or WINS servers are searched.
- If you use DNS servers, they are only searched after all other NetBIOS name resolution resources that you have activated are searched.
- The change is not complete until you restart Windows.

Enabling or Disabling NetBIOS Use of DNS Servers for Name Resolution

To enable or disable NetBIOS use of DNS servers for name resolution:

1. Choose the NBT tab in the Configuration Utility.
2. Check Enable NBT DNS to have NetBIOS use DNS servers to resolve NetBIOS names to IP addresses. Uncheck it to disable use of DNS servers.

Notes:

- If you use DNS servers, they are not used until broadcast messages, WINS servers, and the LM host table are searched (if you use these resources).
- The DNS servers searched are the ones defined on the DNS tab.
- The change is not complete until you restart Windows.

Setting a NetBIOS Scope for Your Workstation

To set a NetBIOS scope for your workstation:

1. Choose the NBT tab in the Configuration Utility.
2. Enter the scope name in the NetBIOS Scope ID field.

Notes:

- If you enter a NetBIOS scope, you can only use NetBIOS to communicate with other machines that use the same scope identifier. Ask your network administrator if you are not certain if you need to use a NetBIOS scope. The scope is normally blank.
- The change is not complete until you restart Windows.

Setting a LAN Adapter (LANA) Number

To set a LANA number:

1. Choose the NBT tab in the Configuration Utility.
2. Enter the required LANA number.

Notes:

- Windows dynamically assigns LANA numbers, so usually you do not need to set a LANA number. The only time you need to set a LANA number is when you are using a NetBIOS application that requires a specific number. Check the documentation for your NetBIOS applications, or check with your network administrator, to determine if you need to set a LANA number.
- The change is not complete until you restart Windows.

Creating an LM Host Table

Use the LM Host Table tab to:

- Add or modify entries in the LM host table
- Use a shared LM host table

See Also:

- Setting up NetBIOS over TCP/IP
- Understanding NetBIOS over TCP/IP

Adding or Modifying Entries in the LM Host Table

The LM host table is used to resolve NetBIOS names to IP addresses, if you have enabled NetBIOS over TCP/IP. The LM host table is only used after broadcasts and WINS servers are searched, if you use them. However, any entries that you preload in the NBT cache from the LM host table are found before broadcasts are issued or WINS servers are searched, which can help performance for accessing frequently-used hosts.

You can create an LM host table or modify an existing one by using a text editor, like NotePad or WordPad, or by using the LM Host Table tab in the Configuration Utility. An editor is easier to use than the LM Host Table tab if you are adding or modifying several entries.

The file name for the LM host table is LMHOSTS. It resides in the directory in which you installed Windows. When you save the file, be sure to save it as a plain text file with no file extension.

WINS servers are an easier way to resolve NetBIOS names to IP addresses. Check with your network administrator to find out if WINS servers are available on your network. Use the NBT tab to identify these servers to Cisco TCP/IP Suite.

Ask your network administrator for the NetBIOS-name-to-IP-address mappings that you should have in your LM host table.

Record Format for LM Host Table Entries

Each record in the LM host table has this general format:

```
IP-Address    NetBIOS-name    #Flags    #Description
```

IP Address

The IP address (dotted decimal) of the machine you want to contact using NetBIOS over TCP/IP.

NetBIOS name

The NetBIOS name of the machine that has the associated IP address. If the NetBIOS name includes special characters, like an undisplayable hexadecimal number in the last position of the name (sixteenth character), you must enclose the name in parentheses, include all spaces between the last character of the name and the special character, and use hexadecimal notation to indicate the special character. For example, an entry for a NetBIOS name with spaces and a special character might look like this:

```
        appname        \0x14
```

The \ character is an escape character, and indicates that the following characters count as one character. There are 8 spaces between the 7 character `appname` and the 1 special character, which makes the NetBIOS name 16 characters.

#Flags

Any of these keywords, which are used for special processing. (These keywords are optional, and you can use #PRE and #DOM on the same entry.)

#PRE

Include this flag if you want this entry preloaded into the NBT cache when you boot your workstation. The NBT cache is the first place Cisco TCP/IP Suite looks when resolving NetBIOS names to IP addresses, so preloading frequently-used entries can help performance.

#DOM:*LAN-Manager domain*

If the entry is for a NetBIOS domain controller, used to log into a LAN Manager domain, include #DOM and enter the name of the NetBIOS domain into which you want to log.   The sequence of entries for domain controllers is significant.   Windows attempts to log into the first domain controller it comes to in the LM host table.   If it cannot log into the first domain, it tries to log into the next domain it finds in the LM host table.   Ask your network administrator for more information about the LAN Manager domain controllers on your network.

#BEGIN_ALTERNATE, #INCLUDE, #END_ALTERNATE

These three flags are used to include one or more shared LM host tables.   These flags stand alone: they do not include an IP address or NetBIOS name in the same record, although they can take a description.

#Description

An optional description of the entry.   The # character indicates the beginning of the description.   You can also use # to put comment lines in the LM host table.   NetBIOS over TCP/IP ignores anything that comes after the # character, although it does recognize the previously mentioned special flags.

Examples

Here are some examples of LM host table entries:

```
192.168.240.56     Dogwood     #PRE  #DOM:marketing  #domain controller
192.168.240.57     Daisy                             #second machine
```

Using a Shared LM Host Table

If your site has a centralized LM host table, you can use it by including the #INCLUDE flag in the LMHOSTS file in the Windows installation directory. Adding or Modifying Entries in the LM Host Table explains how to create and edit the LMHOSTS file, and explains the format of entries in the file.

The #INCLUDE statement has this format:

```
#INCLUDE unc-filename
```

where ***unc-filename*** is the name of the shared LMHOSTS file in the universal naming convention. The universal naming convention identifies the machine, drive, directory, and file name of the shared LM host table. For example, to include the LMHOSTS file on the server named desktop, volume named sys, directory named public, use:

```
#INCLUDE \\desktop\sys\public\lmhosts
```

If your site keeps more than one LMHOSTS file, and these files are copies of each other, you can conditionally load the LMHOSTS file that is on the first available server. This allows you to account for a server being unavailable when you try to use a NetBIOS application. Use the #BEGIN_ALTERNATE, #INCLUDE, and #END_ALTERNATE flags to create a structure like this one:

```
#BEGIN_ALTERNATE
      #INCLUDE \\desktop\sys\public\lmhosts
      #INCLUDE \\marketing\sys\public\lmhosts
#END_ALTERNATE
```

In this example, the LMHOSTS file on desktop is used unless desktop is unavailable, in which case the marketing server is tried.

You can include comments on these statements. The comment must follow the statement, remain on the same line as the statement, and be preceded by the # character.

The entries in LMHOSTS are processed from the top down. For example, if your #INCLUDE statements are near the top of LMHOSTS, the shared LMHOSTS files are searched before the remainder of your LMHOSTS file is searched. Once a match is found, the search stops.

Additional Requirements for Using Shared LMHOSTS Files

In order for #INCLUDE to be processed correctly, you must ensure that:

- Any server used in an include statement has an entry in the LM host table preceding the #INCLUDE statement that references it. The entry must also be preloaded (the #PRE flag indicates this). In the example above, there would need to be entries for the NetBIOS names `desktop` and `marketing` prior to the #INCLUDE statements.
- The directory that contains the shared LMHOSTS file must be in the LAN Manager Server list of NullSessionShares in order for the client machines to read the file. This must be done by your network administrator.

Configuring Global Parameters

Use the Global tab to add, modify, or delete global parameter values. Global parameters affect other configuration activities and TCP/IP communications.

Use the Global tab in the Cisco TCP/IP Suite Configuration Utility to:

- Specify the name of your computer
- Specify the domain name for your organization
- Enable or disable IP forwarding
- Specify the status of the cheetah icon

Specifying a Host Name for Your PC

Many TCP/IP applications access the Cisco TCP/IP Suite stack to obtain the name of your computer. For example, mail readers and FTP servers include the host name in messages they send to other hosts. Naming your computer does not automatically affect the name by which it is known across the network; ultimately, other hosts use their own host tables or DNS to resolve your computer name to an IP address. To avoid confusion, however, your local host name should match the name by which other hosts know it. Ensure that your network administrator is apprised of your name choice.

To name your computer:

1. Choose the Global tab in the Configuration Utility.
2. Enter the name of your computer in the PC Host Name edit box.   Do not include the domain name.
3. To exit the Configuration Utility, click the Done button. The new host name takes effect the next time Windows starts.

Specifying a Local Domain Name

If DNS is configured for your network, you need to specify the local domain for your organization, for example YOYODYNE.COM. This name is provided by your network administrator. The name you specify is appended onto the name of your computer to create what is known in DNS as the fully-qualified domain name. TCP/IP applications, such as mail readers, use the local domain name to identify your machine in the network.

To specify your local domain name:

1. Choose the Global tab in the Configuration Utility.
2. Enter your local domain name in the Local Domain Name edit box.   Do not include the host name.
3. To exit the Configuration Utility, click the Done button. The new local domain name takes effect the next time Windows starts.

Enabling or Disabling IP Forwarding

To enable or disable IP forwarding:

1. Choose the Global tab in the Configuration Utility.
2. Check Enable IP Forwarding if you want your machine to act as a gateway router for IP packets when connecting to networks over different interfaces.   Uncheck it to disable IP forwarding.
3. To exit the Configuration Utility, click the Done button.   Your change to IP forwarding takes effect the next time Windows starts.

Notes:

- IP forwarding only happens if you are connected to two interfaces (serial and LAN) simultaneously.   IP packets sent to your workstation are forwarded between the networks to which you are connected.
- IP forwarding might be a security violation at your company.   Check with your network administrator before enabling IP forwarding.

Specifying Desktop Options

Select options for the appearance of the Cisco TCP/IP Suite cheetah icon.

To add or change a desktop option:

1. Choose the Global tab in the Configuration Utility.
2. To specify that the Cisco TCP/IP Suite cheetah icon be visible, when the stack is running, check the Cheetah Icon Visible When Active check box. To disable this feature, clear this check box.
3. To specify that the Cisco TCP/IP Suite cheetah icon be animated (so that the cheetah appears to be running), check the Cheetah Icon Animated check box. To disable this feature, clear this check box.
4. To exit the Configuration Utility, click the Done button. This change takes effect the next time Windows starts.

Cisco TCP/IP Suite Online Help

Cisco TCP/IP Suite Configuration Utility Commands

Configuration Procedures

Configuration Concepts

- ARP
- Domain Name System (DNS)
- Global Parameters
- Host Tables
- Network Interfaces
- Routing
- NetBIOS Over TCP/IP

ARP

The Address Resolution Protocol, or ARP, defines the mapping or translation of Internet Protocol (IP) addresses to hardware (physical) addresses. Before hosts can communicate with each other, the sending host must discover the hardware address of the receiving host. ARP provides the discovery functions that find the hardware address that corresponds to a specific IP address and that dynamically bind the hardware address to the IP address.

Topics available in this section discuss the Address Resolution Protocol in detail, explain how ARP keeps translation tables up to date, describes how hosts with ARP capabilities can assist in providing translation information for hosts that are incapable of using ARP, and suggests some methods of using ARP to troubleshoot network problems.

The following topics are available:

- Understanding ARP
- How ARP maintains IP translations
- How hosts can assist with translations
- Troubleshooting connectivity problems with ARP
- For More Information

Understanding ARP

ARP is a low-level protocol that lets administrators assign IP addresses to machines on a network as they see fit. There is no need to match the addresses to those on the physical network; ARP handles this dynamically.

This section describes ARP in detail and includes the following topics:

- The differences between hardware and IP addresses
- How hardware addresses are assigned
- How IP addresses are assigned
- Understanding ARP mappings

The Differences Between Hardware and IP Addresses

Since the purpose of ARP is to map IP addresses to hardware or physical addresses on the network, it is important to understand the differences between the addresses and the purpose of each address. Hardware addresses, which are assigned by interface board manufacturers, provide a fast and efficient way to deliver data (packets) on a physical network. Each machine on the physical network must have a unique address. IP addresses, however, can be assigned by network administrators. IP addresses are easily recognized by other computers on other physical networks because they identify a unique host machine on the Internet.

When a host receives data for a local IP address (an IP address on that physical network), it broadcasts an ARP request to all machines on the local network segment. This request message asks all machines if the IP address belongs to them. If the IP address to a host on the local network segment, the machine adds its hardware address to the packet and returns the packet to the sender. The sender   stores the mapping and uses it each time it sends data to that host.

How Hardware Addresses Are Assigned

Hardware addresses or physical address get their name from the method of assigning addresses to Ethernet boards. Each address is unique, starting with a board code from the manufacturer in the first three octets (the complete address is 48-bits). The IEEE assigns hardware addresses to manufacturers in blocks. Hardware addresses provide a data delivery mechanism for physical networks.   A hardware address resembles `00:DD:A8:13:48:C5`.

Network administrators assign hardware or physical addresses to Token-Ring boards.

How IP Addresses Are Assigned

IP addresses provide a data delivery mechanism from one host to another, regardless of the number of networks the message must cross to reach the target host. IP addresses are unique 32-bit addresses assigned by network administrators. An IP address is generally expressed in dotted-decimal format, such as `192.168.34.22`. Administrators, in turn, request an Internet Protocol Network Number from InterNIC Registration Services (HOSTMASTER@INTERNIC.NET) and derive individual host addresses from this number.

Understanding ARP Mappings

When a host receives data for a local IP address (an IP address on that physical network), it broadcasts an ARP request to all machines on the local network segment. This request message asks all machines if the IP address belongs to them. If the IP address to a host on the local network segment, the machine adds its hardware address to the packet and returns the packet to the sender. The sender   stores the mapping and uses it each time it sends data to that host.

Old mappings are deleted from the ARP cache automatically after a period of time specified by the network administrator. Old mappings are also deleted when they no longer work (that is, when new, correct mappings become available). If desired, the cache can be flushed (emptied) manually by a network administrator.

How ARP Maintains IP Translations

Cisco TCP/IP Suite maintains the ARP cache by deleting out-of-date temporary entries several minutes after they are received or added to the ARP table.   This ensures that no out-of-date entries remain for long in the ARP cache.

How Hosts Can Assist With Translations

Cisco TCP/IP Suite supports two types of ARP translation assistance for machines not directly connected to networks with ARP capabilities. These are: Proxy translations, which let a machine on the physical network advertise its hardware address as that of another host; and publish translations, which advertise the IP address and hardware address of a machine on a physical network that does not use ARP.

The following topics are available in this section:

- Understanding proxy translations
- Understanding publish translations

Understanding Publish Translations

Publish translations advertise the IP address and hardware address of a machine on a physical network that does not use ARP. The host that does not use ARP must be connected to the same network as the host supplying the publish service.

The publish translation is manually entered; proper discovery of the IP and physical addresses are the responsibility of the user.

Understanding Proxy Translations

A proxy ARP translation lets a machine on the physical network advertise its hardware address as that of another host.

Proxy translations require manual entry of IP address information and manual entry of hardware address information if another interface (not the active interface on the machine) will handle the proxy translation and services.

Troubleshooting Connectivity Problems with ARP

One of the common uses for ARP is checking address mappings and ensuring they work as planned. For example, a common delivery problem such as regularly lost information can be investigated by checking IP address assignments.

Use ARP to find address mappings for all machines on the network by having each machine send data to your machine. Scan the list for the hardware address of the host with the delivery problem. If the host with a delivery problem does not appear in the table, it is possible that another host is using the IP address for that host. You can then reconcile the IP address problem without changing the hardware.

For More Information

Recommended Reading

For an excellent conceptual overview of TCP/IP networking concepts, we recommend the following books:

Comer, Douglas E., **Internetworking with TCP/IP**, Volumes I and II, Prentice Hall

Black, Uyless D., **TCP/IP and Related Protocols**, McGraw-Hill

Recommended books for users of all levels.

Relevant RFCs

For more information on the ARP and RARP specifications, including packet formats and programming information, consult the following RFCs:

ARP	RFC 826
RARP	RFC 903

Learn how to get RFCs.

DNS Concepts

In its simplest form, DNS (Domain Name System) maps a host (computer) name to its IP address. When you specify a host by name, Cisco TCP/IP Suite uses DNS or host tables to map the host name to its IP address. The host name can be local to your organization or anywhere in the world, if your site is connected to the Internet. TCP/IP applications use DNS to convert host names to IP addresses, and vice versa. This conversion is called resolving.

Cisco TCP/IP Suite DNS acts as a simple resolver; that is, when you specify a computer name, it sends a request to another computer, called a DNS server to resolve the name into an IP address. Similarly, when an IP address is specified, a request is sent to the DNS server to resolve the IP address into a name.

You can specify one or more IP addresses of DNS servers with which Cisco TCP/IP Suite DNS can resolve requests. An IP address is entered as a series of four number groups, such as `192.168.224.42`.

DNS does not control IP routing, however.

The following topics provide information on DNS:

- How DNS works
- Domains
- DNS servers
- DNS and host tables
- For More Information

How DNS Works

DNS centralizes information about computer names and their IP addresses in a distributed database.   Computers called servers store the information so that your computer or any TCP/IP applications you use can access the information.   If your computer needs information that is not on the current server, the server automatically requests the information from other DNS servers.

Your computer acts as a type of simple DNS resolver.   A resolver understands how to ask DNS servers for information on converting computer names to IP addresses.   The Cisco TCP/IP Suite DNS resolver has two mechanisms for making requests: either your computer sends the server a computer name and the server sends an IP address, or your computer sends an IP address and receives a host name.

Domains

In DNS terminology, a domain is a hierarchical grouping of computers within the Internet. The domain administrator determines what computers are in the domain group. A domain name describes a domain and consists of words separated by dots. For example, `yoyodyne.com`.

Domain names are assigned by the Internet naming authority (InterNIC). Your domain can create subdomains for its domain. Domain names can pertain to a site, an organization, or to types of organizations.

The right-most word in the domain name is the top-level domain, which determines the function of an organization or specifies a country name code. In the example name, `yoyodyne.com`, `.com` means an organization engaged in commerce. The top-level domain can also indicate the country, such as .CA for Canada. The name of the organization is to the left of the top-level domain, such as `yoyodyne`. Any words to the left of the top-level domain are called subdomains. The left-most word in the domain name is the host name. For example, in the name `oak.yoyodyne.com`, `oak` is a host in the `yoyodyne.com` organization.

Domains and subdomains are analogous to a tree structure. Subdomains are set up and maintained by the domain administer or by each organization.

The root domain in DNS is expressed as a dot. You can think of domains as being analogous to directories, and subdomains as subdirectories.

Top-level domains such as .ORG, .COM, and .EDU are typically used in the United States. Other countries group their domain names below their two-letter country code. In the United States, .US is occasionally used instead of another top-level domain name, such as `palo-alto.ca.us`.

DNS Servers

A DNS server is any computer running DNS software that lets it communicate with other DNS servers and store (cache) address information for later retrieval. DNS servers are also called name servers. Your network administrator provides the IP address of the name server on your network.

Name servers come in these varieties:

Root Name Server

A root name server is a primary name server for the start or base of the domain name tree. A root name server usually handles domains just below the root, such as top-level domains. An example of a top-level domain is .COM or .EDU, or .US, .CH, and other country codes. A root name server delegates authority to other primary name servers for subdomains, such as `yoyodyne.com` or `cern.ch`.

A root name server is usually run by the InterNIC, the group responsible for naming domains on the Internet

Primary Name Server

A primary name server has authority over one or more subdomains. A primary name server reads information about the domain from the zone file, which describes the domain and hosts in that domain.

A primary name server is authoritative for a domain, and also caches information.

Secondary Name Server

A secondary name server for a domain receives information updates from the primary name server for that domain at regular intervals and stores this information on disk. A secondary server is also authoritative for the domain, and also caches information.

Caching-Only Name Server

A caching-only name server caches (stores) domain information in memory for faster retrieval later. A caching-only name server is not authoritative for any domain. If a caching-only name server cannot resolve a request from memory, it forwards the request to an authoritative name server for that domain.

Resolver

A resolver sends requests for resolution to another server. Any name server that can handle the request returns the answer. By default, Cisco TCP/IP Suite includes a DNS resolver. Resolvers do not cache DNS-related information.

DNS and Host Tables

The DNS (Domain Name System) software quickly maps host names to IP addresses.   DNS maintains a distributed repository of information that your computer can access without having to keep a private copy on its local disk. If DNS is configured on your network, you should use DNS.

If DNS is not configured on your network, you can configure Cisco TCP/IP Suite host tables. Host tables also map host names to IP addresses and IP addresses to host names.   However with host tables, the information is stored in your computer and must be updated frequently. With host tables, every host name you specify while running TCP/IP applications must have an IP address listed in the host table.   Whenever a change occurs on the network, such as when a new computer is added that you want to access by a name, you must add the information to your private host table.

In some rare cases, if you are using DNS, you may also want to use host tables.   This is useful for adding temporary changes such as when a new computer is added to the network, but has not been added to the DNS repository.

Depending on how you use DNS and host tables, ensure that the Search Order section of the DNS tab is set so that host tables or DNS are accessed in the order you require.

For More Information

Recommended Reading

For an excellent conceptual overview of TCP/IP networking concepts, we recommend the following books:

Comer, Douglas E., ***Internetworking with TCP/IP***, Volumes I and II, Prentice Hall

Black, Uyless D., ***TCP/IP and Related Protocols***, McGraw-Hill

Recommended books for users of all levels.

Relevant RFCs

For more information on the Domain Name System and host tables, consult the following RFCs:

DNS structure	RFC 1591
Host Tables	RFC 952

Learn how to get RFCs.

Global Parameters

Once you establish IP connectivity for your computer, you will find that many network applications require common configuration information, such as name of your host (your computer name). Cisco TCP/IP Suite allows you to configure the following global parameters so that any application can access them:

- PC Host Name
- Domain Name
- IP Forwarding
- For More Information

PC Host Name

Some WinSock applications require the name of your PC so that they can provide useful information to remote users. For example, some mail programs include the PC host name in mail message headers to indicate which host sent the mail. Similarly, FTP server applications often display the name of the host when remote users log in to access files.

Domain Name

Domains are used to provide a hierarchical grouping of hosts within the Internet.
Domain names are assigned by the Internet naming authority and can pertain to your site, your organization, or the type of organization in which you participate.
A domain name normally consists of at least two words, separated by a dot, such as `yoyodyne.com`.

Understanding IP Forwarding

If you use a serial and LAN connection simultaneously, it is possible for your machine to act as a gateway between the networks to which you are connected.   For example, if you are connected to your companys network over an Ethernet line, you might also dial into another network over a serial line.   You can choose whether packets that are sent directly to your system through one interface are forwarded out the other interface.   This is called IP packet forwarding.

If you enable IP packet forwarding, your machine becomes a gateway between the networks to which you are connected.   This can allow unwanted and insecure traffic from one network into another network.   Thus, enabling packet forwarding might be a security violation at your company.   In general, you only want to enable packet forwarding if you can trust the traffic on both networks, and if you specifically need your machine to act as a gateway between the networks.

For More Information

Recommended Reading

For an excellent conceptual overview of TCP/IP networking concepts, we recommend the following books:

Comer, Douglas E., ***Internetworking with TCP/IP***, Volumes I and II, Prentice Hall

Black, Uyless D., ***TCP/IP and Related Protocols***, McGraw Hill

Recommended books for users of all levels.

Relevant RFCs

For more information on host names and domain names, consult the following RFCs:

Host Tables	RFC 952
Domain Name System	RFC 1136

Learn how to get RFCs.

Host Tables

Host tables map computer names to IP addresses.   When using TCP/IP applications, it is easier to remember a computer by its name rather than its IP address.

An alternative to host tables is DNS, which is easier to configure but requires that your network administrator has configured other computers to map computer names to IP addresses.

When you configure a host table entry, you can specify the following:

- A domain name as a series of words separated with dots, such as **oak.yoyodyne.com**. Your network administrator can provide the computer names that you enter for each entry.
- An IP address as a series of four number groups, such as `192.168.224.42`. Your network administrator can provide the IP addresses of the hosts that you need to access.
- One or more optional alternative names for computer, called aliases. For example, if a computer is named **oak.yoyodyne.com**, you can specify aliases such as **oak**. Then you can specify the computer name as **oak** instead of **oak.yoyodyne.com**.
- An optional description to describe the entry.

When you add host table entries using the Cisco TCP/IP Suite Configuration Utility, ensure that the Search Order section of the Host Tables tab is set so that host tables are either accessed exclusively or after DNS.

See Also:

- For More Information

For More Information

Recommended Reading

For an excellent conceptual overview of TCP/IP networking concepts, we recommend the following books:

Comer, Douglas E., ***Internetworking with TCP/IP***, Volumes I and II, Prentice Hall
Black, Uyless D., ***TCP/IP and Related Protocols***, McGraw Hill

Recommended books for users of all levels.

Relevant RFCs

For more information on host tables, consult RFC952.

Learn how to get RFCs.

Network Interfaces

Network interfaces let systems communicate with one another on physical networks. Network interfaces typically include a network interface board that is installed in the system and a device driver that provides the communication link between the operating system and the network interface board. Together, the interface card and the device driver are responsible for all hardware details of communicating on the network.

Once the interface board and device driver are installed, the TCP/IP stack must be configured so that it knows which interface to use for network communications.

These topics are available:

- Supported Network Drivers
- Network interface parameters
- Dynamic Configuration Protocols
- For More Information

Supported Network Drivers

Cisco TCP/IP Suite includes drivers for many popular network interface cards.

Cisco TCP/IP Suite supports the following driver types:

ODI drivers Used by Novell NetWare clients, ODI drivers typically consist of an `LSL.COM` file and a network adapter driver, typically `*.COM`, both of which must be running before Cisco TCP/IP Suite starts.

NDIS3 drivers Used by Microsoft Windows for Workgroups, NDIS 3.0 drivers are VxD-based, and provide the best performance of the three driver types that Cisco TCP/IP Suite supports.

NDIS2 drivers Used by Microsoft LAN Manager and Banyan Vines, NDIS 2.0 drivers are TSR-based, and should only be used if no other driver is available or if you are running another network protocol that requires NDIS 2.0 drivers.

Of the three types of drivers, ODI uses more DOS memory than NDIS 2.0 or NDIS 3.0. NDIS 3.0 uses no conventional memory. In most cases, we recommend ODI over NDIS 2.0.

What is a VxD?

A VxD, or Virtual Device Driver, is a 32-bit multiplexing device driver that manages data exchanges between Windows applications and system services.

A VxD delivers a number of benefits. A VxD works the same way as the operating system itself, delivering the same potential degree of service, in terms of available memory, speed of operation, and number of applications it can support. In practical terms, a VxD makes the maximum amount of memory available for other programs, particularly those that run in a DOS box. That means you can do more with the Windows workstation.

Applications that use VxD services should run faster because the VxD has the ability to control its own operation more effectively, in cooperation with the operating system.   A VxD takes advantage of the full 32-bit architecture of future Windows versions which allows for greater performance and greater service, opening up the possibility of moving a greater range of information, including sound and pictures, at speeds acceptable to people using the machine.

Why Use a VxD and Not a TSR?

Because a TSR (terminate and stay resident) program occupies real mode DOS memory, it limits the use of other programs, including Windows itself, if the TSR is big enough. Most often, the impact of a TSR is felt when the user attempts to use one or more programs in a DOS box in Windows and finds the machine does not have enough memory to run the program. A VxD needs little or no real mode DOS memory.

Using a TSR also requires a mechanism for communicating data between the TSR, which loads into memory and becomes active before Windows starts, and any Windows program. This mechanism necessarily incurs a reduction in performance, though this can be minimized. This TSR-to-Windows mechanism also introduces a complexity that can be a critical point of failure in the system.

VxDs are fully integrated into Windows, eliminating the need for this communication mechanism.

Running Cisco TCP/IP Suite With Other Protocols

Cisco TCP/IP Suite can run concurrently with another protocol such as NetWare if one of the following is true:

- The other protocol uses a network interface driver that does not conflict with the driver used by Cisco TCP/IP Suite.
- The other protocol runs over a different network interface.

If you must run multiple protocols on your PC, refer to the following table to determine whether Cisco TCP/IP Suite and the other protocols can run over the same network interface card.

Protocol	**Drivers for Windows**	**Drivers for Windows for Workgroups**
Novell NetWare	ODI	ODI
LAN Manager	NDIS2	NDIS2 or NDIS3
PathWorks	NDIS2	NDIS2 or NDIS3
Vines	NDIS2	NDIS2 or NDIS3

Note

Only NDIS2 and NDIS3 drivers can run concurrently over the same network interface.

Example 1

If NetWare is configured over an ODI driver for an Ethernet card, you can run Cisco TCP/IP Suite over the same ODI driver, but not over an NDIS2 driver.

Example 2

If LAN Manager is configured over an NDIS2 driver for an Ethernet card, you can run Cisco TCP/IP Suite over an NDIS3 driver for the same Ethernet card.

Network Interface Parameters

For each network interface connecting your PC to your network, Cisco TCP/IP Suite requires the following information:

- Interface Label
- Interface Type
- Interface Driver Type
- IP Address
- Subnet Mask
- Broadcast Address

Interface Label

Cisco TCP/IP Suite uses network Interface labels so that interfaces are easy to identify in the Interface table in the Configuration Utility. Interface labels are limited to 255 alphanumeric characters.

Cisco TCP/IP Suite does not interpret the interface label, so you can assign interface labels that describe an interface or assign random numbers.

For example, **Sales Subnet** and **Sales123** are both valid interface labels.

Interface Type

For each network interface card over which Cisco TCP/IP Suite provides TCP/IP service, you must specify the type of network (Ethernet, Serial, FDDI, or Token-Ring) to which the network interface card is connected. Specifying the correct interface type lets Cisco TCP/IP Suite condition and interpret application data sent across the network.

Interface Driver Type

For each network interface card over which Cisco TCP/IP Suite provides TCP/IP service, you must specify the type of network driver configured for the interface card.

For example, if you have an SMC Ethernet card and are running an ODI driver, you must configure Cisco TCP/IP Suite to use the ODI driver.

IP Address

The Internet Protocol uses IP (Internet Protocol) to identify hosts or interfaces on an internet. IP addresses consist of four sets of numbers known as bytes or octets (because they are eight bits long) and they are generally expressed in dotted-decimal format.

An IP address consists of two parts:

- A network number that identifies the network segment to which the host is connected. The administrator must first obtain an Internet Protocol Network Number from InterNIC Registration Services (`HOSTMASTER@INTERNIC.NET`) or your Internet service provider (ISP) before creating specific IP addresses.
- A host number that distinguishes the system from all other systems connected to the network segment.

The Internet Protocol (IP) provides two mechanisms for determining which portion of an IP address defines the network number:

- Network classes
- Subnet Mask

IP requires each network segment to have a unique network number, but all network numbers at the same site must begin with the network number for that site. For example, no two network segments can have the network number `192.168`, but if they are part of the same network, they must have network numbers that begin with `192.168`, such as `192.168.35` and `192.168.34`. This allows hosts on either network segment to appear as though they are on the same network.

Each host must have a host number that is unique on its network segment.

IP Network Classes

The Internet Protocol (IP) defines network classes which contain ranges of IP addresses. These classes, labeled A through C, imply how many bits in the IP address constitute the network number. The actual network number is determined by the subnet mask, which can break a class A or B network into smaller networks.   Classes are defined as follows:

Class A networks
Identified by a number from 1 to 127 in the first byte, such as `10.1.1.1`.

Class B networks
Identified by a number from 128 to 191 in the first byte, such as `172.16.1.1`.

Class C networks
Identified by a number from 192 to 223 in the first byte, such as `192.168.32.1`.

The network class indicates the size of the network.   A class A network can have 16,777,216 hosts, while a class B network can have 65,536 hosts, and a class C network can have 256 hosts.

Notes

- The actual network number is determined by the combination of the IP address and the subnet mask.   The network number is usually represented with 0 in the host name position, for example, `192.6.123.0`.
- An organization can have more than one class A, B, or C network.
- Cisco TCP/IP Suite also supports class D addresses, which are used by applications that use IP multicasting.   Class D addresses are handled dynamically: there are no configuration considerations for enabling IP multicasting.

Subnet Mask

Subnet masks allow you to create networks consisting of multiple network segments while maintaining a single network address for the entire site. Subnet masks state explicitly which bits in an address for a host correspond to the network address. Without this information, hosts cannot reach hosts on other subnets.

Subnet masks specify the bits in the IP address for your host that comprise the network address, and override the network address implied by address classes. For example, class B networks have 16-bit network addresses, but to accommodate 8 network segments, each of which must have a unique network address, they require 3 more address bits. The subnet mask tells the host to use 3 of the 16 host address bits, and reduce the number of hosts on each subnet from 216 to 213.

For example

`255.255.255.0` indicates that all bits in the first three octets define the network address. If you have a class B address, in which the first two octets define the network address, the third octet specifies one of 256 possible network segments. You do not have to use an entire octet for the subnet number; a subnet mask of `255.255.224.0` indicates that only the highest three bits of the third octet specify a subnet, of which there can be 8.

Note

Increasing the number of subnets reduces the number of hosts that each subnet can accommodate.

Broadcast Address

A system uses a broadcast address to broadcast information or a request to all hosts on a local network.

The default IP broadcast address has all bits in the host portion of the IP address set to binary one. For example, for a class B network with no subnet, the IP broadcast address is `nn.nn.255.255` (such as `172.16.255.255`).

If the network contains subnets, the broadcast address is relative to the local subnet. For example, host `128.44.12.1` with a subnet mask of `255.255.255.0` has an IP broadcast address of `128.44.12.255`.

Dynamic Configuration Protocols

Dynamic configuration lets a system get its configuration information, such as IP address, subnet mask, host name, and broadcast address, from another computer on the network when it boots up. This is useful for systems that do not have a local hard disk to store that information (such as a printer), for networks that have more systems than IP addresses (such as a computer laboratory), environments where central control is preferred (where the network administrators assign and manage all IP addresses instead of users), or for systems that are used temporarily, like portable computers, when you do not want to permanently use up an IP address for each network to which the portable might connect.

Cisco TCP/IP Suite can use two different dynamic configuration protocols: Bootstrap Protocol (BOOTP) or Dynamic Host Configuration Protocol (DHCP). Although DHCP is a more powerful protocol than BOOTP, the differences between these protocols are mostly transparent to end users.

For More Information

Recommended Reading

For an excellent conceptual overview of TCP/IP networking concepts, we recommend the following books:

Comer, Douglas E., ***Internetworking with TCP/IP***, Volumes I and II, Prentice Hall

Black, Uyless D., ***TCP/IP and Related Protocols***, McGraw Hill

Recommended books for users of all levels.

Relevant RFCs

For more information on Internet protocols, consult the following RFCs:

Internet Protocol	RFC 791
Broadcasting	RFC 919, RFC 922
Subnetting	RFC 950
IP over Ethernet	RFC 894

Learn how to get RFCs.

Routing

Routing is the process of selecting the route that data, in the form of IP packets, must take to reach its destination. Routers forward packets to other routers or networks. When the packet for a host is received on the destination network, it is forwarded directly to the host.

Routing can be as simple as delivering packets to another host on the same network (direct routing) or it may involve forwarding packets to routers on its way to the destination network. This section helps you understand the basics of IP routing and how routing works in Cisco TCP/IP Suite in the following topics:

- Understanding IP routing
- Error and Status Reporting Through ICMP
- For More Information

Understanding IP Routing

IP routing forwards packets to a destination network. When the router receives the packet, it forwards the packet to the appropriate host. When a router forwards a packet to a local host (a host on the same network), routing is direct; if the packet must be forwarded to one or more routers to reach its destination, the route is indirect.

This section discusses the following indirect routing concepts:

- Static routing, default routes, router discovery, and RIP
- Understanding routing tables
- Subnet Routing
- Broadcast Addresses

Static Routing, Default Routes, Router Discovery, and RIP

When your host must forward packets to one or more routers before the packet reaches its destination, the route is indirect. Cisco TCP/IP Suite supports these methods of providing the necessary information for indirect routing :

- Static routing is a table-driven system of Internet network address and router address pairs.
- Default routes
- Router Discovery
- Routing Information Protocol (RIP)

Understanding Routing Tables

Routing tables store information about the routes that hosts can use to reach other hosts on the network or Internet. Routing tables can be static or dynamic.

All routing information in the routing table is based on local addresses only. The routing table is designed to supply the next hop address (which is always local) for data bound for other networks. The routing table never contains information about routers beyond the local network, nor does it contain information about how to reach individual host addresses (although it can contain host-specific entries that specify which local router to use when data is bound for a specific host address). Routers always forward data to other routers until the destination network is the local network. When the data arrives at the router on the destination network, it is sent to the appropriate host.

Host-specific routes are special routing table entries that specify which router to use when data is bound for a specific remote host.   Host-specific routes are frequently used to test new routers or to immplement network security.

Subnet Routing

Subnet routing allows network administrators of class A, B, and C networks to create smaller networks from single class A, B, or C host addresses. These smaller, internal networks are called subnets. Subnet masks inside the class A or class B network are not exposed to the rest of the Internet; all changes to accommodate the additional addresses are handled internally. This simplifies routing information to the Internet and minimizes the amount of information the network must advertise on the Internet.

Inside the network, the administrator determines how to reallocate addresses by choosing how many bits of the host portion of each address are used as a subnet address and how many bits are used as the host address. The administrator uses a subnet mask to divide the existing addresses into network and host portions. The subnet mask identifies how much of the existing address can be used as the network portion. The underlying physical network must also be divided into smaller, physical subnets when using a subnet mask to create subnets.

Example:

The following example illustrates how to create several subnets from a class B address. The example also illustrates how traffic is received and how the addresses appear to other hosts and routers on the Internet.

An administrator wants to create two subnets from a class B address. The class B address `172.16.0.0` can be divided by masking the first 24 bits of the 32-bit IP address using the netmask `255.255.255.0`. The class B network will accept all traffic bound for any IP address beginning with the 16-bit network portion `172.16`. Therefore, the administrator can create the networks `172.16.224.0` and `172.16.225.0`. Valid addresses on the internal network such as `172.16.224.42` and `172.16.225.12` can be reached from anywhere on the Internet; final delivery is handled by the individual physical subnets that contain the nodes associated with the addresses.

Broadcast Addresses

Broadcast addresses are used to send information to all hosts on a network. Packets addressed to the network's broadcast address are transmitted to every host with the same broadcast address on the local network.   Broadcast packets are routinely used by the network to share routing information, field ARP requests, and send status and informational messages.

Routing Information Protocol (RIP)

RIP is a dynamic routing protocol. Routers using RIP broadcast their routing tables to the network at regular intervals. Machines on the network, including other routers, receive these broadcasts and update their routing tables as necessary. If a particular router fails to broadcast its routing table after a specified period of time, the other machines on the network remove that router from their routing tables, thus updating their routing tables dynamically.

Router Discovery

Router discovery is a method of finding a router when no default route entry exists in the routing table. When booting, a host using router discovery broadcasts a message asking for available routers. The available routers reply with a message indicating its address. The host adds the information to its routing table.

Router Discovery requires that Router Discovery be enabled on the routers.   See your routers documentation for information on enabling Router Discovery.

For More Information

Recommended Reading

For an excellent conceptual overview of Internet routing (and a complete discussion of TCP/IP networking concepts), we recommend the following books:

Comer, Douglas E., ***Internetworking with TCP/IP***, Volumes I and II, Prentice Hall

Black, Uyless D., ***TCP/IP and Related Protocols***, McGraw Hill

Recommended books for users of all levels.

Relevant RFCs

For more information on Internet routing protocols, consult the following RFCs:

Routing Information Protocol (RIP)	RFC 1388 (updates RFC 1058)
Border Gateway Protocol (BGP)	RFC 1267 & RFC 1268
Exterior Gateway Protocol (EGP)	RFC 904
Open Shortest Path First (OSPF)	RFC 1247
Internet Control Message Protocol (ICMP)	RFC 792
Router Discovery	RFC 1256

Learn how to get RFCs.

NetBIOS Over TCP/IP

NetBIOS over TCP/IP lets you run NetBIOS applications (like the Windows ClipBook) over TCP/IP networks.   This section helps you understand the basics of NetBIOS over TCP/IP in the following topics:

- Understanding NetBIOS Over TCP/IP
- Understanding NetBIOS to IP Name Resolution
- Understanding the LAN Manager Hosts (LM Hosts) File
- Understanding the Windows Internet Naming Service (WINS) Server
- Understanding Changes Made During NBT Configuration
- For More Information About NetBIOS Over TCP/IP

Understanding NetBIOS Over TCP/IP

NetBIOS is a network transport originally developed by IBM for small networks. It, and an extension of it called NetBEUI, are the transport layer used by Windows. These two transports have a limitation that they cannot deliver packets over a router, because they rely on broadcast messages, which are not forwarded by routers.

NetBIOS over TCP/IP, also called NBT or TDI, solves that problem by encapsulating the NetBIOS or NetBEUI packets in IP packets. It converts between IP addresses and NetBIOS names, so that both TCP/IP and NetBIOS applications get the information in the expected format. Because IP packets can be forwarded by routers, you can use the NetBIOS applications over a router.

If you want to use NetBIOS applications (for example, the Windows ClipBook), you should enable NetBIOS over TCP/IP.

When you use NetBIOS over TCP/IP, you must tell Cisco TCP/IP Suite how to attempt to resolve NetBIOS names to IP addresses. You can use broadcast messages, WINS servers, a LAN Manager hosts file (LM Hosts), DNS servers, or any combination of these. What you use depends on what your network administrator has configured for your network.

Understanding NetBIOS to IP Name Resolution

There are several ways in which a NetBIOS name can be resolved to an IP address.   Which way you use depends on what facilities your network administrator has created for you.   You might be required to create some of these resources yourself.

The first place NetBIOS looks to resolve a name to an IP address is the NBT cache on your workstation.   This cache contains information about recently used NetBIOS names, and any entries from the LM host table that you preloaded into the NBT cache.   You determine which entries are preloaded when you create or modify LM host table entries from the LM Host Table tab.   (The NBT cache is automatically created and maintained for you.)

If NetBIOS cannot find the name in the NBT cache, it either issues a broadcast message to the network, asking for the machine that uses the name to respond with its IP address, or it looks in the WINS servers that you have identified on the NBT tab.   You can set the sequence in which WINS servers and broadcast messages are used from the NBT tab.

If the NetBIOS name is still not found, NetBIOS searches your LM host table on the workstation, if you have enabled it.

Finally, if the name is still not found, NetBIOS searches the DNS servers you defined on the DNS tab, if you have enabled NetBIOS use of DNS on the NBT tab.   In this case, the NetBIOS name must be the same as the TCP/IP host name for NetBIOS to find a match.

Understanding the LAN Manager Hosts (LM Hosts) File

The LAN Manager Hosts (LM Hosts) file is similar to the TCP/IP host table: both are files on your workstation that map IP addresses to names. In the case of the LM Hosts file, the name mapped to an IP address is a NetBIOS name.

Build the LM Hosts file using a text editor such as Write or NotePad, or the LM Host Table tab. The file is named LMHOSTS, and resides in the directory in which you installed Windows. As with the TCP/IP host table, only include key NetBIOS name mappings in the LM Hosts file. If you are not using WINS servers, include all NetBIOS names that are not on your local network segment in the LM Hosts file.

If you make any typing mistakes when creating the LM Hosts file, it can prevent you from using NetBIOS communications with the target machine. Also, you must ensure that this file correctly reflects any changes made to the network that involve the machines for which you have entries.

Tip:

- If you create the LMHOSTS file using an editor that can create non-text formats, such as Word or Write, make sure you save the file as a plain text document.

Understanding the Windows Internet Naming Service (WINS) Server

A WINS name server is similar to a DNS server, except that WINS servers return the IP address of a network resource based on the resources NetBIOS name. When a workstation or other network machine needs to use TCP/IP to deliver NetBIOS packets, it can ask a WINS server for the IP address that belongs to the NetBIOS name of the target machine.

WINS servers build their IP address-to-NetBIOS name mappings automatically from these sources:

- Windows NT-based DHCP servers, which inform the WINS server of all mappings in their databases
- Client machines that are using a WINS server register with the server when they are started
- Broadcast messages on the local network segment

Because WINS servers can gather and maintain these mappings automatically, they require little maintenance while being reliable. Thus, they are a good choice for name resolution when using NetBIOS over TCP/IP.

Normally, there should be a WINS server on every segment of the network for WINS to work well. However, instead of having a WINS server on each segment, you can define your workstation as a **WINS proxy**. If your workstation acts as a WINS proxy, it redirects NetBIOS name queries to a WINS server, and stores the responses in its local NBT cache. Your workstation can then respond to subsequent requests for the NetBIOS name.

Check with your network administrator to find out the address of your WINS server, if you have one. Your network administrator can also help you determine if your workstation should act as a WINS proxy server.

Understanding Changes Made During NBT Configuration

If you enable NetBIOS over TCP/IP, the Configuration utility adds the following drivers to the `transport=` line in the `[386Enh]` section of SYSTEM.INI:

drive:\path\vtdi.386
drive:\path\vnbt.386
drive:\path\vmntdi.386

where the drive and path are the ones where Cisco TCP/IP Suite is installed.

The following settings may also be added the to the `[NBT]` section in the SYSTEM.INI file, depending on what selections you make in the Configuration utility. Some of these settings are configurable through the Configuration utility, or have defaults that you can override by adding these settings to SYSTEM.INI.

The configuration utility does not set all of these parameters. If you want to change a parameter not set through the utility, you must edit the registry directly.

`BroadcastAddress=`_address-in-hexadecimal-format_
The broadcast address for NetBIOS name broadcasts. The default broadcast address is calculated from the local IP address and subnet mask, and is not necessarily the same as the broadcast address entered in the Configuration utility.

`BcastNameQueryCount=`_integer_
The number of times a NetBIOS broadcast is sent. The default is 3 times. This is not set by the Configuration utility.

`BcastQueryTimeout=`_milliseconds_
The length of time a NetBIOS broadcast is sent. The minimum length is 100. The default is 750. This is not set by the Configuration utility.

`CacheTimeout=`_milliseconds_
The length of time that a NetBIOS name and IP address mapping is stored in the NBT cache. The minimum is 60000 (1 minute). The default is 360000 (6 minutes). This timeout does not apply to entries preloaded from the LM host table, which do not time out. This value is not set by the Configuration utility.

`DnsServerPort=`_port-number_
The port number used by the DNS server. The default is 53. This value is not set by the Configuration utility.

`EnableDNS=0` _or_ **`1`**
Whether NetBIOS should use DNS servers to resolve NetBIOS names to IP addresses. 0 disables use of DNS, 1 enables it. The default is 0. This is set on the NBT tab in the Configuration utility.

`EnableProxy=0` _or_ **`1`**
Whether your machine should act as a WINS proxy server on the local network. 0 prevents your machine from being a proxy server, 1 enables it. The default is 0. This is set on the NBT tab in the Configuration utility.

`InitialRefreshT.O.=`_milliseconds_
The length of time between sending WINS name refresh messages. The minimum is 960000 (16 minutes); the maximum is 0xFFFFFFFF (about 50 days). The default is 960000. This value is not set by the Configuration utility.

`LANABASE=`_LAN-Adapter-number-in-decimal_
The LAN Adapter number base. The first LANA number will have this value, and

subsequent LANAs are calculated by incrementing by 1 (e.g. if you specify 2, the first LANA is 2, the next one is 3, then 4, and so on). The minimum value is 0, the maximum is 4. This is set on the NBT tab in the Configuration utility.

LMHostFile=_path-and-filename_

The full drive, path, and file name of the LM host table. The default is %windows%\lmhosts. This is set on the LM Host Table tab in the Configuration Utility.

LmHostsTimeout=_milliseconds_

The length of time that NBT waits before searching through the lmhosts file. The minimum is 1000 (1 second). The default is 10000 (10 seconds). This value is not set by the Configuration utility.

NameServer1=_IP-address_

NameServer2=_IP-address_

The IP addresses of the WINS servers you want to use for resolving NetBIOS names to IP addresses. These are set on the NBT tab in the Configuration utility.

NameServerPort=_port-number_

The port number used by the WINS server. The default is 137. This value is not set by the Configuration utility.

NameSrvQueryCount=_integer_

The number of times that NetBIOS attempts to resolve a name using WINS. The minimum is 1. The default is 3. This value is not set by the Configuration utility.

NameSrvQueryTimeout=_milliseconds_

The length of time before NetBIOS marks a query as having timed out. The minimum is 100 (1/10th second). The default is 750 (3/4ths seconds). This value is not set by the Configuration utility.

NameTableSize=_integer_

The maximum number of NetBIOS name and IP address pairs that can be stored in the cache. The minimum is 1, the maximum 255. The default is 17. This value is not set by the configuration utility.

NodeType=_integer_

The type of node for the workstation for NetBIOS name resolution. The possible node types are:

1 b-node (use only broadcast messages to resolve names).
2 p-node (use only WINS servers to resolve names).
4 m-node (use broadcast first, then WINS servers).
8 h-node (use WINS first, then broadcast).

The default is 1, unless you specify a WINS server, in which case the default is 8. This is set on the NBT tab in the Configuration utility.

ScopeId=_NetBIOS-scope-name_

The NetBIOS scope ID for the workstation. The default is blank (no scope ID). This is set on the NBT tab in the Configuration utility.

SessionKeepAlive=_seconds_

How often to send session keepalive packets for active sessions. The minimum is 60 (1 minute). The default is 3600 (1 hour). This value is not set by the Configuration utility.

SessionTableSize=_integer_

The maximum number of NetBIOS sessions in the session table. The minimum is 1, the maximum 255. The default is 255. This value is not set by the Configuration utility.

For More Information About NetBIOS Over TCP/IP

Recommended Reading

For an excellent conceptual overview of Internet routing (and a complete discussion of TCP/IP networking concepts), we recommend the following books:

Comer, Douglas E., ***Internetworking with TCP/IP***, Volumes I and II, Prentice Hall

Black, Uyless D., ***TCP/IP and Related Protocols***, McGraw Hill

Recommended books for users of all levels.

Relevant RFCs

For more information on NetBIOS over TCP/IP, consult the following RFCs:

NetBIOS over TCP/IP concepts	RFC 1001
NetBIOS over TCP/IP details	RFC 1002

Learn how to get RFCs.