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. Right-click the fields on the tab for context-sensitive help.

{button ,KL(`Interface tab')} Things you can do on the Interface tab

The Interface Table lists the interfaces defined for your workstation. The display columns are:

- **Enabled**: yes indicates the active interface.
- **Interface Label**: an optional name for the interface.
- **Type**: whether the interface is Ethernet, Token-Ring, FDDI, or serial.
- **IP Address**: the IP address of the interface, such as `192.168.34.22`.
- **Subnet Mask**: the subnet mask for the interface, such as `255.255.255.0`.
- **Broadcast**: the optional broadcast address for the interface, such as `192.168.34.255`.

Click the New button to create an interface.

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

Click the Delete button to remove the selected interface.

New or Modify Interface Dialog Box

The New or Modify Interface dialog box lets you configure a network interface.

{button ,AL(`Interface dialog box')} Things you can do with the Interface Dialog Box

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

Choose the type of network interface (Ethernet, Token-Ring, serial, or FDDI).

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.

Enter your site's subnet mask for the interface. If you are not sure of your subnet mask, ask your network administrator.

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

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

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.

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

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

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

Click the Cancel button to quit the dialog box and abandon any changes 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. Right-click the fields on the tab for context-sensitive help.

{button ,KL(`Routing Tab')} Things you can do with the Routing Tab

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

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

Click the New button to add routes to the routing table.

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

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

The Routing Method group determines how Cisco TCP/IP Suite routes packets.

Click Default Route and enter the IP address to which Cisco TCP/IP Suite is to direct packets when there is no specific route for the destination host or network in the routing table.

Click Router Discovery to make your workstation broadcast 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.

Click Router Information Protocol (RIP) to have your workstation listen for packets sent by routers that are regularly broadcasting their IP address. Cisco TCP/IP Suite uses this information to build and dynamically update a routing table. Your routers must broadcast RIP information to use this type of routing.

Check Listen For Default Route Only to have RIP build 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.

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. Right-click the fields in the dialog box for context-sensitive help.

{button ,AL(`Route dialog box')} Things you can do with the New or Modify Route Dialog Box

Enter the destination address, which is the IP address of the remote host or network you want to reach.

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

Click Host if the destination for this route is a host; Network if it is a network.

DNS Tab

The DNS (Domain Name System) tab lets you configure the domain name service for your workstation. Right-click the fields on the tab for context-sensitive help.

{button ,KL(`DNS tab')} Things you can do with the DNS Tab

The DNS Server IP Address table lists all DNS servers used by your workstation. 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 query times out.

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

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

Click the New button to add an entry to the DNS Server IP Address table.

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

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

The Search Order group controls the search order for name resolution (the order in which host names are resolved). Click the Set button to change the current search order:

- **DNS only**: resolve host names only with DNS
- **DNS then Host Table**: resolve host names with DNS and if the host name is not found, use the host table
- **Host Table then DNS**: resolve host names with the host table and if the host name is not found, use DNS
- **Host Table only**: resolve the host name only using the host table

Set Search Order Dialog Box

The Set Search Order dialog box lets you change the current search order for host name resolution. Right-click the fields in the dialog box for context-sensitive help.

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.

{button ,AL(`Set Search Order dialog box')} Things you can do with the Set Search Order dialog box

The Name Resolution group controls how host names are resolved.

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

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 in its own host table to resolve host names to IP addresses.

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

Click Host Table only to make your workstation look only to its own host table to resolve 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. Right-click fields in the dialog box for context-sensitive help.

{button ,AL(`DNS Server dialog box')} Things you can do with the New or Modify DNS Server dialog box

Enter the IP address (in dotted-decimal format) 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 workstation can resolve names even if your DNS server is unavailable. Right-click fields on the tab for context-sensitive help.

{button ,KL(`Host Table tab')} Things you can do with the Host Table tab

The host table lets you store host-name-to-IP-address translations on your workstation. By storing translations locally, you ensure that your workstation 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:

- **Name:** 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.

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

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

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. Right-click fields in the dialog box for context-sensitive help.

{button ,AL(`Host dialog box')} Things you can do with the New or Modify Host dialog box

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

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

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

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.

ARP Tab

Address Resolution Protocol, or ARP, maps IP addresses to hardware addresses. This mapping is almost always performed dynamically by communications 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. Right-click the fields on the tab for context-sensitive help.

{button ,KL(`ARP tab')} Things you can do with the ARP tab

The ARP table contains IP and hardware address pairs for quick lookup. The columns are:

- **Host Address:** the IP address 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) for the IP address.
- **Translation:** whether the ARP table entry is using proxy or publish translation. 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.

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

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

Click the Delete button to delete the selected mapping 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. Right-click fields in the dialog box for context-sensitive help.

{button ,AL(`ARP Table Entry dialog box')} Things you can do with the New or Modify ARP Table Entry dialog box

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

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.)

The Translation group determines how the local host responds to ARP requests on behalf of other hosts. Check Proxy to have the local host respond to an ARP request as if it were the target host. 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.

{button ,KL(`LM Host Table tab')} Things you can do with the LM Host Table tab

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

The NBT Name Registration/Resolution dialog box lets you determine the order in which broadcast messages and WINS servers should be used for registering your workstation on the NetBIOS network, and resolving NetBIOS names to IP addresses. Right-click fields in the dialog box for context-sensitive help.

{button ,AL(`NBT Name Registration Resolution dialog box')} Related Topics

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.

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.

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.

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. Right-click fields in the dialog box for context-sensitive help.

{button ,KL(`NBT tab')} Things you can do with the NBT tab

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

The NBT Settings group controls how NetBIOS applications run over TCP/IP.

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

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

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.

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.

Select 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.

Check Enable NBT DNS to have 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.

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.

Global Tab

The Global tab features settings that affect more than one aspect of the TCP/IP stack. Right-click fields on the tab for context-sensitive help.

{button ,KL(`Global tab')} Things you can do with the Global tab

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

Enter your organization's 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.

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

The Desktop Options group controls the behavior of the cheetah icon.

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

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

To create a LAN network interface:

1 Choose the Interface tab in the Configuration Utility.
2 Click the New... button.
3 Enter the interface label and a LAN interface type (anything but serial).
4 If you want to use dynamic configuration, check Dynamic Configuration. The IP address, subnet mask, and broadcast address are determined dynamically.
5 If you do not use dynamic configuration, enter the IP address for the network interface card, the subnet mask, and the broadcast address (if required by your site).
6 Check Enable Interface if you want this interface to be the active one.

Tips:

- Obtain the interface type, IP address, subnet mask, and broadcast address from your network administrator.
- The interface is not activated until you restart Windows.
- 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. Your network administrator handles this.

{button ,KL(`Interface tab')} Related Topics

To create a serial interface for use with Dialer:

1 Choose the Interface tab in the Configuration Utility.
2 Click the New... button.
3 Enter the interface label.
4 Select Serial for the interface type.
5 Check Enable Interface if you want this interface to be active. Serial interfaces can be enabled at the same time as LAN interfaces.

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.

{button ,KL(`Interface tab')} Related Topics

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.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Interface tab')} Related Topics

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.
4 Enter the new interface label.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Interface tab')} Related Topics

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.
4 Select the new interface type provided by your network administrator.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Interface tab')} Related Topics

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... button.
4 Enter the IP Address provided by your network administrator.

Tips:

- The change is not complete until you restart Windows.
- Make sure the new IP address is registered in DNS (via a DNS server) or in the host tables on other computers.

{button ,KL(`Interface tab')} Related Topics

To modify the 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.
4 Enter the subnet mask provided by your network administrator.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Interface tab')} Related Topics

To modify the 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.
4 Enter the broadcast address provided by your network administrator.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Interface tab')} Related Topics

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.
4 Check Dynamic Configuration to enable dynamic configuration; clear the check box to disable it.

Tips:

- The change is not complete until you restart Windows.
- If your network administrator gave you a specific IP address for your workstation, disable dynamic configuration and fill in the IP address, subnet mask, and broadcast address fields.

{button ,KL(`Interface tab')} Related Topics

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.
4 Check Enable Interface to enable the interface; uncheck it to disable the interface.

Tips:

- The change is not complete until you restart Windows.
- You must enable one of your interfaces to use TCP/IP communications. The currently active interface is indicated by a yes in the Enabled column of the interface table.
- You can only enable one LAN interface at a time (Ethernet, Token-Ring, or FDDI). However, you can enable serial interfaces and LAN interfaces together.

{button ,KL(`Interface tab')} Related Topics

To add a route to the routing table:

1 Choose the Routing tab in the Configuration Utility.
2 Click the New... button.
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.

Tips:

- After you save the changes to the routing table, you must restart Windows before the routing changes become active.

{button ,KL(`Routing tab')} Related Topics

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.
4 Change the routing properties as desired.

Tips:

- After you save the changes to the routing table, you must restart Windows before the routing changes become active.

{button ,KL(`Routing tab')} Related Topics

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.

Tips:

- After you save the changes to the routing table, you must restart Windows before the routing changes become active.

{button ,KL(`Routing tab')} Related Topics

To choose a routing method for your workstation:

1 Choose the Routing tab in the Configuration Utility.

2 Click the radio button corresponding to the routing method you want to use. For the default route method, enter the IP address of the default route in the edit box. For the RIP method, if you want to listen only for a default route, check Listen for Default Route Only.

Tips:

- Cisco TCP/IP Suite requires a routing method to route packets. Cisco TCP/IP Suite defaults to the default route method.
- You can only use router discovery if router discovery is enabled on your routers. Ask your network administrator for more information.
- After you save the changes to the routing table, you must restart Windows before the routing changes become active.
- The change is not complete until you restart Windows.

{button ,KL(`Routing tab')} Related Topics

To add a DNS server to the DNS server address table:

1 Choose the DNS tab in the Configuration Utility.
2 Click the New button.
3 Enter the IP address of a DNS server.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`DNS tab')} Related Topics

To change the IP address of a DNS server in the DNS server 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.
4 Change the IP address as required.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`DNS tab')} Related Topics

To delete a DNS server from the DNS server 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.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`DNS tab')} Related Topics

To change the priority order for DNS servers when using more than one:

1 Choose the DNS tab in the Configuration Utility.
2 In the DNS Server IP Address table, select the entry you want to move.
3 Click the Up or Down button to position the entry either upwards or downwards as desired.

Tips:

- DNS servers are accessed from top to bottom. If a DNS server does not answer a name request, subsequent servers are tried until the name is resolved or there are no more servers to try. If the name is not resolved by DNS, your host table is tried, if you have set up Cisco TCP/IP Suite to access your host table after trying DNS.
- The change is not complete until you restart Windows.

{button ,KL(`DNS tab')} Related Topics

To set the order in which DNS servers and host tables are accessed:

1 Choose the DNS tab or the Host Table tab in the Configuration Utility.
2 Click the Set... button in the Search Order group.
3 Choose the order in which you want Cisco TCP/IP Suite to use DNS servers and host tables to resolve host names. You can use DNS or host tables exclusively, or you can have Cisco TCP/IP Suite try one before resorting to the other.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`DNS tab')} Related Topics

To add an entry to the host table:

1 Choose the Host Table tab in the Configuration Utility.
2 Click the New... button.
3 Enter the name and IP address of the host.
4 Optionally, add a description of the host (for example, the name of the person who uses the machine, or the machine's location).
5 If desired, enter aliases for this host in the Aliases box and click the Add button. To remove an unwanted alias, select it and click the Delete button.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Host Table tab')} Related Topics

To merge host tables, or add several entries to the host table at once:

1 Edit the hosts file in the Cisco TCP/IP Suite installation directory.

2 Add your preformatted entries to the file.

Formatting Requirements for Host Table Entries

If you add entries to the host table by editing the file, the entries must follow this format (starting in the first column of each line):

```
IP-address   host-name   alias1 alias2 etc     # optional comments
```

You must separate the IP address, host names, aliases, and comments by spaces. Put no more than one IP address on each line.

Check that you are not duplicating entries. Only the first match to a host name is used in resolving the host name to an IP address.

{button ,KL(`Host Table tab')} Related Topics

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 delete.
3 Click the Delete button.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Host Table tab')} Related Topics

To change the host name for a host table entry:

1 Choose the Host Table tab in the Configuration Utility.
2 In the host table, select the entry whose name needs to be changed.
3 Click the Modify... button.
4 Enter the new host name provided by your network administrator.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Host Table tab')} Related Topics

To change the IP address for a host table entry:

1 Choose the Host Table tab in the Configuration Utility.
2 In the host table, select the entry whose IP address needs to be changed.
3 Click the Modify... button.
4 Enter the new host IP address provided by your network administrator.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Host Table tab')} Related Topics

To change the description for a host table entry:

1 Choose the Host Table tab in the Configuration Utility.
2 In the host table, select the entry whose description you want to change.
3 Click the Modify... button.
4 Change the description in the Description field.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Host Table tab')} Related Topics

To change an alias in a host table entry:

1 Choose the Host Table tab in the Configuration Utility.
2 In the host table, select the entry whose alias you want to change.
3 Click the Modify... button. The Aliases group lists the current aliases.
4 To change 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.

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`Host Table tab')} Related Topics

To add an entry to the ARP table:

1 Obtain a host address, an Ethernet, Token-Ring, or FDDI 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.
4 Enter the host IP address and corresponding hardware address for the Ethernet, Token-Ring, or FDDI controller.
5 Check Publish to publish a translation on another host's behalf, or Proxy if you need to create a proxy translation.

Tips:

- The new mapping takes effect when you restart Windows.
- 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.

{button ,KL(`ARP tab')} Related Topics

To delete an entry from the ARP table:

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.

Tips:

- The new mapping takes effect when you restart Windows.
- Deleting entries in the ARP table can seriously affect communications. Do not delete ARP table entries unless you are sure of their effects on your network.

{button ,KL(`ARP tab')} Related Topics

To change the host IP address for an entry in the ARP table:

1 Choose the ARP tab in the Configuration Utility.
2 In the ARP table, select the ARP table entry whose IP address you want to modify.
3 Click the Modify... button.
4 Enter the host's IP address provided by your network administrator.

Tips:

- The new mapping takes effect when you restart Windows.
- 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.

{button ,KL(`ARP tab')} Related Topics

To change the hardware address for an entry in the ARP table:

1 Choose the ARP tab in the Configuration Utility.
2 In the ARP table, select the ARP table entry whose hardware address you want to change.
3 Click the Modify... button.
4 Enter the hardware address provided by your network administrator.

Tips:

- The new mapping takes effect when you restart Windows.
- 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.

{button ,KL(`ARP tab')} Related Topics

To make an ARP translation 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.
4 Check Proxy or Publish, as required by your network administrator.

Tips:

- The new mapping takes effect when you restart Windows.
- 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.

{button ,KL(`ARP tab')} Related Topics

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. Microsoft includes a sample LMHOSTS file called LMHOSTS.SAM. You can copy this file to lmhosts and use it as the basis for your LM host table. 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
```

Read the LMHOSTS.SAM file in the Windows installation directory for more information on formatting these entries, and to see more examples.

{button ,KL(`LM Host Table tab')} Related Topics

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. The registry key for NullSessionShares is HKEY_LOCAL_MACHINE\system\currentcontrolset\services\lanmanserver\parameters\nullsessionshares.

{button ,KL(`LM Host Table tab')} Related Topics

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 To have NetBIOS applications also search DNS servers, check Enable NBT DNS on the NBT tab.

Tips:

- 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 workstation's NetBIOS name is registered with the WINS servers when you use NetBIOS.
- If it exists, 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.

{button ,AL(`NBT Name Registration Resolution dialog box')} Related Topics

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.

Tips:

- 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.

{button ,AL(`NBT Name Registration Resolution dialog box')} Related Topics

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.

Tips:

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

{button ,KL(`NBT tab')} Related Topics

To make your workstation a WINS proxy server:

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

Tips:

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

{button ,KL(`NBT tab')} Related Topics

To disable your WINS proxy server:

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

Tips:

- The change is not complete until you restart Windows.

{button ,KL(`NBT tab')} Related Topics

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.

Tips:

- 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.

{button ,KL(`NBT tab')} Related Topics

To set a LAN adapter (LANA) number:

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

Tips:

- 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.

{button ,KL(`NBT tab')} Related Topics

To set the host name for your computer:

1 Choose the Global tab in the Configuration Utility.

2 Enter the name of your computer in the PC Host Name field. Do not include the domain name

Tips:

- 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 DNS or their own host tables 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.
- The change is not complete until you restart Windows.

{button ,KL(`host name')} Related Topics

To set the domain name for your computer:

1 Choose the Global tab in the Configuration Utility.

2 Enter your local domain name in the Local Domain Name field. Do not include your host name.

Tips:

- 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 domain name is appended to 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.
- The change is not complete until you restart Windows.

{button ,KL(`Global tab')} Related Topics

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.

Tips:

- The change is not complete until you restart Windows.
- You must also install the Client for Microsoft Networks using the Network Properties control panel, if the client is not already installed. Ask your network administrator for your Microsoft Networking workgroup name (defined on the Network Properties Identification tab) and Windows NT domain (defined in the Client for Microsoft Networks properties).
- 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.

{button ,KL(`NetBIOS over TCP/IP,')} Related Topics

To enable or disable IP packet 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.

Tips:

- 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.

{button ,KL(`IP forwarding,')} Related Topics

To control the behavior of the cheetah icon:

1 Choose the Global tab in the Configuration Utility.

2 Check Cheetah Icon Visible When Active if you want the icon to appear in the Windows taskbar when the Cisco TCP/IP Suite stack is working.

3 If you are having the icon appear when the Cisco TCP/IP Suite stack is working, you can also check Cheetah Icon Animated if you want the cheetah on the icon to run while the stack is working.

Tips:

- The change is not complete until you restart Windows.

What is the Address Resolution Protocol (ARP)?

The Address Resolution Protocol (ARP) defines the mapping of Internet Protocol (IP) addresses to hardware (physical) addresses. Before hosts can communicate with each other, the sending host on the same network as the receiving host must discover the hardware address of the receiving host. ARP discovers the hardware address that corresponds to a specific IP address and stores the mapping in the sending host's memory.

Hardware addresses, which are assigned by interface board manufacturers or network administrators, 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 are assigned by network administrators and can be used by other computers on other physical networks because they identify a unique host machine on the Internet.

When a router 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 corresponds to the information in the stack configuration for a machine, 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 temporary mappings are deleted from the ARP cache automatically after a short time. Permanent mappings (as entered using the ARP tab in the Configuration Utility) are not deleted.

{button ,KL(`ARP tab')} Related Topics

Understanding How Hardware Addresses are Assigned

“Hardware addresses” or “physical addresses” 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.

{button ,KL(`ARP tab')} Related Topics

Understanding Proxy and Publish 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.

- **Proxy translations** let 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. 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.
- **Publish translations** advertise the IP address and hardware address of a machine on a physical network that cannot respond to ARP requests. The host that does not use ARP must be connected to the same network as the host supplying the publish service. Publish translations are entered manually; proper discovery of the IP and physical addresses are the user's responsibility. If you are not publishing ARP translations, the entries in your ARP table can only be used by your machine; other hosts on the network cannot take advantage of the mapping.

{button ,KL(`ARP tab')} Related Topics

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.

{button ,KL(`ARP tab')} Related Topics

For More Information about ARP

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

{button ,JI(`glossary.hlp',`Recommended_Books_on_TCP_IP_Connectivity')} List of recommended books

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

{button ,JI(`glossary.hlp',`How_to_Get_Internet_RFCs')} How to get RFCs

Understanding the Domain Name System (DNS)

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 resolution.

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 DNS server, the server automatically requests the information from other DNS servers. You can specify one or more IP addresses of DNS servers with which Cisco TCP/IP Suite DNS can resolve requests.

Your computer acts as a 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.

Tip:

- DNS does not control IP routing.

{button ,KL(`DNS tab')} Related Topics

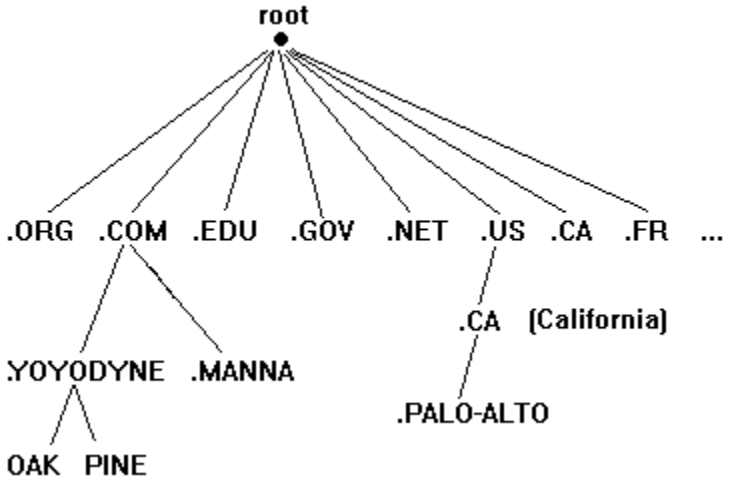
Understanding Domains

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`.

{button ,KL(`DNS tab')} Related Topics

Understanding 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 can provide 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 DNS 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 caches DNS 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. Cisco TCP/IP Suite provides a DNS resolver. Resolvers do not cache DNS information.

{button ,KL(`DNS tab')} Related Topics

Understanding the Relationship Between 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 own 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 the 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.

{button ,KL(`DNS tab')} Related Topics

For More Information about DNS, Host Tables, and the Global Parameters

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

{button ,JI(`glossary.hlp',`Recommended_Books_on_TCP_IP_Connectivity')} List of recommended books

Relevant RFCs

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

DNS structure	RFC 1591
Host Tables	RFC 952

{button ,JI(`glossary.hlp',`How_to_Get_Internet_RFCs')} How to get RFCs

Understanding the PC Host Name

The host name is the machine name for your workstation. 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.

For example, if the full name of your workstation is **willow.yoyodyne.com** (on the yoyodyne.com domain), your host name is **willow**.

{button ,KL(`Global tab')} Related Topics

Understanding IP Forwarding

If you use a serial and LAN connection simultaneously, it is possible for your machine to act as a gateway router between the networks to which you are connected. For example, if you are connected to your company's 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 router 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 router between the networks.

{button ,KL(`IP forwarding,')} Related Topics

Understanding NetBIOS over TCP/IP (NBT or TDI)

NetBIOS is a network transport originally developed by IBM for small networks. NetBIOS, 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.

{button ,KL(`NetBIOS over TCP/IP,')} Related Topics

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.

{button ,KL(`NetBIOS over TCP/IP,')} Related Topics

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 WordPad or NotePad, or the LM Host Table tab. The file is named LMHOSTS, and resides in the directory in which you installed Windows. Microsoft includes a sample LM host table named LMHOSTS.SAM. 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 WordPad, make sure you save the file as a plain text document.

{button ,KL(`NetBIOS over TCP/IP,')} Related Topics

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 resource's 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.

{button ,KL(`NetBIOS over TCP/IP,')} Related Topics

Understanding the Changes Made During NBT Configuration

If you enable NetBIOS over TCP/IP, the Configuration utility adds NBT settings to the `Hkey_Local_Machine\System\CurrentControlSet\Services\VxD\MSTCP` key in the registry. See **Microsoft Windows 95 Resource Kit,** Microsoft Press, 1995, for more information about TCP/IP and NetBIOS over TCP/IP registry entries, how to edit the registry, and other parameters you can set for TCP/IP in the registry.

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.

{button ,KL(`NetBIOS over TCP/IP,')} Related Topics

For More Information About NetBIOS over TCP/IP

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

{button ,JI(`glossary.hlp',`Recommended_Books_on_TCP_IP_Connectivity')} List of recommended books

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

{button ,JI(`glossary.hlp',`How_to_Get_Internet_RFCs')} How to get RFCs

Understanding Host Tables

Use the Host Table tab to add, modify, or delete host table entries. A host table contains one or more entries that map the name of a computer (a host name) to its IP address. When using TCP/IP applications, it is easier to remember a computer by its name rather than its IP address.

A host table entry includes a host name, its IP address, any optional aliases that you want to use instead of the host 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 computers you need to access are listed in your host table.

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

When you configure a host table entry:

- The host name can be just a host name (for example, `daisy`), or it can be fully qualified with a domain name (for example, `daisy.yoyodyne.com`).
- The IP address must be in dotted-decimal format (for example, 192.168.224.42).
- The aliases are any names you might want to use besides the host names. Aliases are optional. For example, if the host name is `daisy.yoyodyne.com`, a good alias would be `daisy`. Then you can use `daisy` whenever you need to refer to that machine by host name.
- The description is anything that will help you remember what the host is used for.

{button ,KL(`host table,')} Related Topics

What is a Network Interface?

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. Although Windows 95 manages the device driver independently of Cisco TCP/IP Suite, you still must identify the type of network to Cisco TCP/IP Suite (for example, Ethernet).

Understanding Interface Types

For each network interface card over which Cisco TCP/IP Suite provides TCP/IP service, you must specify the type of network (Ethernet, serial, Token-Ring, or FDDI) 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.

{button ,KL(`Interface tab')} Related Topics

Understanding IP Addresses

The Internet Protocol (IP) uses IP addresses to identify hosts or interfaces on an internet. This provides 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 numbers consisting of four sets of numbers known as bytes or octets (because they are eight bits long). They are generally expressed in dotted decimal format. On occasion, they appear in hexadecimal format (`C0.29.E4.0F`) or in octal format (`300.51.344.017`). The network administrator assigns these numbers to hosts.

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 Masks

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 `172.16`, but if they are part of the same network, they must have network numbers that begin with `172.16`, such as `172.16.35` and `172.16.34`. 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.

{button ,KL(`Interface tab')} Related Topics

Understanding IP Network Classes

The Internet Protocol (IP) defines network classes that contain ranges of IP addresses. These classes, labeled A through C, imply how many bits in the IP address constitute the network number. Classes are defined as:

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.

Note:

- The 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.

{button ,KL(`Interface tab')} Related Topics

Understanding 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.

{button ,KL(`dynamic configuration')} Related Topics

For More Information about Network Interfaces

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

{button ,JI(`glossary.hlp',`Recommended_Books_on_TCP_IP_Connectivity')} List of recommended books

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
Host Extensions for IP Multicasting	RFC 1112

{button ,JI(`glossary.hlp',`How_to_Get_Internet_RFCs')} How to get RFCs

Understanding IP Routing

IP 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 by the router on the destination network, it is forwarded directly to the host.

IP 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 (indirect routing). Indirect routing requires a routing table, the selection of a routing method, and can include subnets and broadcast addresses.

{button ,KL(`Routing tab')} Related Topics

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

{button ,KL(`Routing tab')} Related Topics

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.

{button ,KL(`Routing tab')} Related Topics

Understanding Subnet Routing and Subnet Masks

Subnet routing and subnet masks allow network administrators of class A, B, and C networks to create smaller networks from class A, B, and C host addresses, while maintaining a single network address for the entire site. 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, and overrides 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 reduces the number of hosts on each subnet from 2 to the power of 16 to 2 to the power of 13.

The underlying physical network must also be divided into smaller, physical subnets when using a subnet mask to create subnets. Increasing the number of subnets reduces the number of hosts that each subnet can accommodate.

Example 1:

The subnet mask `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.

Example 2:

This 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.

{button ,KL(`Routing tab')} Related Topics

Understanding Broadcast Addresses

Broadcast addresses are used to send information to all hosts on a local 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, send ARP requests, and send status and informational messages.

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 `172.16.12.1` with a subnet mask of `255.255.255.0` has an IP broadcast address of `172.16.12.255`.

{button ,KL(`Routing tab')} Related Topics

The Routing Information Protocol (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 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 messages indicating their addresses. The host adds the information to its routing table. Router discovery requires that router discovery is enabled on your routers.

For More Information about Routing Protocols

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

{button ,JI(`glossary.hlp',`Recommended_Books_on_TCP_IP_Connectivity')} List of recommended books

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

{button ,JI(`glossary.hlp',`How_to_Get_Internet_RFCs')} How to get RFCs