Click the ARP Table button, or choose ARP Table from the Display menu, to display the contents of the ARP (Address Resolution Protocol) cache.

Reading the ARP Table Statistics

The ARP Table lists the contents of the ARP (Address Resolution Protocol) cache.

By viewing the contents of the ARP cache and comparing information displayed with the known IP and hardware address pairs, you can be sure that one system on the network is not using another system's IP address. Checking the ARP cache is useful when the workstation frequently loses connection when communicating with another host on the network.

The ARP Table contains these columns:
- **Host Network Address** identifies the IP address of the hosts with which your workstation is communicating.
- **Hardware Address** identifies the hardware address of each host.
- **Arp Flags** identifies whether an entry is temporary or permanent in the ARP cache.

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

Click the Buffer Statistics button, or choose Buffer Statistics from the Display menu, to see the amount of RAM space available for temporary data storage.

Reading the Buffer Statistics

The Buffer Statistics indicate the amount of RAM (random access memory) space available for temporary storage of IP data.   The Buffer Statistics identify the number of buffers in use, the percentage of buffers in use, and the number of denied memory requests.

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

Click the Connection Table button, or choose Connection Table from the Display menu, to list the workstation's current TCP/IP connections.

Reading the Connection Table Statistics

The Connection Table lists the workstation's current TCP/IP connections.   The Connection Table contains these columns:

- **Proto** identifies the networking protocol being used for each connection.
- **Rcv-Q** identifies the number of bytes waiting to be processed.
- **Snd-Q** identifies the number of bytes waiting to be sent to the remote host.
- **Local Address (Port)** identifies the IP address and port of the workstation being used for each connection.
- **Foreign Addr (Port)** identifies the address and port being used on the remote host.
- **State** identifies the status of the connection.

{button ,KL(`connection table statistics')}   <u>Related Topics</u>

Click the Interface Table button, or choose Interface Table from the Display menu, to display information about all interfaces on the workstation.

Reading the Interface Table Statistics

The Interface Table displays information about all interfaces on the workstation.

Double-click an entry in the table to get more information about the entry.

The Interface Table contains these columns:

- **Name** identifies each interface by name.
- **MTU** identifies the MTU (Maximum Transmission Unit) for the interface.   MTU path discovery determines the maximum-sized TCP packet that can be sent through the network.   By determining the largest, most efficient packet size possible with the hardware at each hop, performance is improved.   This feature is described in RFC-1191.
- **Network** identifies the network number for the interface or the interface status.   If the network is shown as `****DOWN****`, ensure that the interface is enabled with the Cisco TCP/IP Suite Configuration Utility.   If the device is an Ethernet device, a SLIP interface cannot be running simultaneously.
- **Address** identifies the IP address of the interface.
- **IPkts** identifies the number of incoming packets.
- **Ierrs** identifies the number of incoming errors detected.
- **Opkts** identifies the number of outgoing packets.
- **Oerrs** identifies the number of outgoing errors.
- **Collis** identifies the number of detected collisions.

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

Interface Display Window

The Interface display window shows additional information about an interface entry.   Right click the fields on the window for information on each item.

{button ,KL(`interface table statistics')}   <u>Related Topics</u>

Flags shows any flags in effect for the interface.

IP Address shows the IP address of the interface.

IP Sub-Net Mask shows the subnet mask for the interface.

IP Broadcast Address shows the broadcast address for the interface.

Click the Close button to close the window.

Click the Help button to display online help.

Click the Protocol Statistics button, or choose Protocol Statistics from the Display window, to get detailed networking statistics for all current connections.

Reading the Protocol Statistics

The Protocol Statistics list the number of packets sent and received for each TCP/IP protocol.

{button ,KL(`protocol statistics')}   <u>Related Topics</u>

Click the Routing Table button, or choose Routing Table from the Display menu, to identify the hosts or networks with which the workstation is communicating and the routes being used.

Reading the Routing Table Statistics

The Routing Table identifies the hosts or networks with which the workstation is communicating and the routes being used.

The Routing Table contains these columns:

- **Destination** is the IP addresses of hosts or networks with which the workstation is communicating.
- **Gateway** is the IP address of the default route.
- **Flags** are any flags in effect for the route.
- **Refcnt** (reference count) is the number of applications currently using each route.
- **Use** is the total number of times each route has been used.
- **Interface** is the IP address of the interface using the route.
- **MTU** is the maximum transmission unit for each route.   MTU path discovery determines the maximum-sized TCP packet that can be sent through the network.   By determining the largest, most efficient packet size possible with the hardware at each hop, performance is increased.   This feature is described in RFC-1191.

{button ,KL(`routing table')}   <u>Related Topics</u>

Click the Refresh button, or choose Refresh from the Display menu, to update the statistics appearing in a table.

Click the Save button, or choose Save As from the File menu, to save Monitor statistics to a file.

Click the Print button, or choose Print from the File menu, to print Monitor statistics.

Click the Exit button, or choose Exit from the File menu, to exit the Monitor application.

Choose Program to set a refresh rate and determine how hosts are identified in the statistics.

Check Toolbar to display the button toolbar below the menu.

Check Bubble Help to display bubble help for toolbar buttons when moving the cursor over the buttons.

Check Status Bar to display the status bar at the bottom of the screen.

Program Dialog Box

The Program dialog box lets you specify a refresh rate and how hosts are identified in the statistics.

{button ,KL(`Program dialog box')}   Things you can do with the Program dialog box

Enter the refresh interval, which is the number of seconds that should elapse before Monitor updates the information in the table.

Check Save Settings on Exit to save the values set in this dialog box for the next time you use the Monitor application.   If you do not check this, your changes only apply to the current session.

The Symbolic Display group determines how hosts are identified in the statistics.

Click None to have Monitor identify hosts by IP address.

Click Host Table to have Monitor identify all hosts by their host names as defined in the workstation's host table.

Click DNS to have Monitor identify all hosts by their host names as defined in DNS (Domain Name System).   This can generate many queries to DNS servers, which can make Monitor run more slowly.

Click the OK button to close the dialog box and save your changes.

Click the Cancel button to close the dialog box without saving your changes.

To display ARP statistics:

▶   Click the ARP Table button.

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

To display buffer statistics:

▶ Click the [Buffer Statistics button](#).

{button ,KL(`buffer table statistics')}   <u>Related Topics</u>

To display the connection table:

▸ Click the Connection Table button.

{button ,KL(`connection table statistics')}   <u>Related Topics</u>

To display the interface table:

▶ Click the Interface Table button.

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

To display the protocol statistics:

▶   Click the Protocol Statistics button.

{button ,KL(`protocol statistics')}   Related Topics

To display the routing table:

▶   Click the Routing Table button.

_____

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

To change the frequency at which statistics are updated (the refresh rate):

1 Select the Program option from the Options menu.
2 Change the refresh interval in the Refresh Interval box (the rate is in seconds).
3 To save the refresh interval for the next time you use Monitor, check the Save Settings On Exit check box.

To determine whether host names or IP addresses are displayed:

1 Select the Program option from the Options menu.
2 In the Symbolic Display field, click None, Host Table, or DNS.
3 To save your changes for the next time you use the Monitor, check the Save Settings On Exit check box.

To save statistics in a file:

1 Click the Save button or select Save As... from the File menu.
2 Enter the name and location of the file you want to use.

To print Monitor statistics:

1 Click the Print button or select Print... from the File menu.
2 Select the desired printer.

To exit the Cisco TCP/IP Suite Monitor:

▶ Click the Exit button.

Diagnosing a Failing Connection to a Network Resource

You might find that a connection to a network resource such as a printer or workstation is failing even though it had been working fine.   For example, you might suddenly find that you can no longer print on your network printer.

This might indicate that another machine on the network has taken over the IP address for the machine that is causing problems.

To check out a bad network connection:

1 If you can, check the machine to ensure that it is turned on and working properly.   If the machine is not working properly, fix it and retry your connection.

2 Start MultiNet Tools and use Host Lookup to check the DNS listing for the machine's host name.   Make note of the IP address.   If there is no entry for the machine, it may no longer be on the network.   Contact your network administrator.

3 Ping the machine.   If the machine does not respond, then there might be something wrong with it. Contact the person responsible for managing the machine.

4 Start MultiNet Tools and use Traceroute to determine where the failure occurs.

5 If the machine does not respond to Ping, Traceroute did not help, and you are familiar with the hardware network cards and their hardware addresses (also called media access control (MAC) addresses), look at the entry for the machine in the ARP table in Monitor.   If the hardware address is not within the expected range given the hardware manufacturer for the machine you are expecting at that address, then the IP address is probably being used by a different machine.   (Your hardware manufacturer can tell you the hardware addresses that they use.)   In order to restore the connection to the machine, the network administrator must find the machine that has taken over the IP address and change its configuration to use a new, unique IP address.

If you have a network sniffer, or a UNIX or MultiNet for OpenVMS system that can run a TCP dump in promiscuous mode, you can also check for ARP problems by watching for ARP replies.   You should see only one response for an ARP request. If you see two or more responses, they will be from different hardware addresses.   Only one system will have the correct hardware address.

6 If you still cannot determine the problem, contact the network administrator, who might be able to examine a TCP dump or call service for help in isolating the problem.

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

Determining Why You Cannot Connect to a System

Occasionally you might find that you cannot connect to a particular system.   Often this is due to heavy network activity for the target machine (for example, a popular Web site).   If you know the system is popular, you might simply try reconnecting later.

If your problems connecting to the system are regular, or if the system is critical to you, you can follow these steps to determine if there is another problem besides the system just being too busy to respond:

1 ![icon]   Start MultiNet Tools and use TraceRoute to trace the route between your machine and the target, unresponsive machine.   If the trace makes it to the unavailable system, the system is may be too busy at this time to respond to your attempted connection.   This does not mean there is no other problem, however.   Try your connection again, and if the problem persists, contact your network administrator.

2   If the trace stops before making it to the remote system, then the network connection is broken at that last location.   If the location is within your company, or is provided as a service for which your company is paying, call the owner of the resource.   (Whois in MultiNet Tools can help you locate a contact if you do not know who to call, or call your help desk or network administrator.)

3 If the trace does not stop, but at some point circles back on itself, look at the trace information to find the point at which the route is circling back.   The machine which is routing packets back needs to be fixed.

Determining Why You Cannot Connect Outside the Local Network

If you cannot connect outside your local network, you have a routing problem.   Look at the routing table.   You should have at least these three destinations:

- **0.0.0.0**

  This is the default route, and should be the IP address of a gateway.   It is defined in the Cisco TCP/IP Suite Configuration utility under Routing.   You can configure your workstation to use a specific route (supplying a specific IP address), or you can have your workstation find a route by specifically asking the network or by listening for routing information from the network.   In any of these cases, you should get an entry for 0.0.0.0 in the routing table.

- **127.0.0.1**

  This is your workstation's loop-back address.   If there is no entry for this address, your Cisco TCP/IP Suite configuration is incorrect.   Contact your network administrator to get the information you need and update the configuration using the Cisco TCP/IP Suite Configuration utility.   The information you need is the same information needed during Cisco TCP/IP Suite installation.

- **Subnet IP address**

  This is the IP address of the subnet that your machine is on.   The gateway address for this destination should be your machine's IP address.

{button ,KL(`routing table')}   <u>Related Topics</u>

Launch the Cisco TCP/IP Suite Configuration Utility

Determining Why a Network Connection is Getting Dropped

If you find that, when using an application like Telnet for FTP, your connection to the remote system is getting dropped more often than you deem reasonable, there might be a hardware problem somewhere on the network. Here are some things you can do to determine if there is a hardware problem somewhere on the network:

- Look at the protocol statistics.   These statistics are accumulated since the last time TCP/IP was started on the machine (typically during boot).   Some of these statistics cover "timeout" errors (for example, "dropped due to keepalive timeouts").

  In general, the ratio of timeout errors to TCP connections should be no more than 1 to 2 percent.   Anything more than 10 percent indicates a problem, and ratios between 2 and 10 indicate a possible problem.   (These ratios are rules-of-thumb; it is up to you to determine which ratios define what is, and is not, a significant problem.)

  An excessive number of connections dropped due to timeouts might indicate a faulty bridge on the network.

-    Ping the host that is timing out.   To make the ping useful, you must make it emulate the type of connections that are being dropped by the host.

  For example, if users typically Telnet to the host, set up Ping to resemble Telnet.   Use 1000 bytes for the data length.   Send a large number of packets so that the ping will last long enough to resemble a normal Telnet session.   (Specify 0 to have the Ping last until you stop it.)

  If you are emulating FTP connections, you might want a larger data length (like 1500 for Ethernet or 4352 for FDDI).   Send enough packets so that the Ping resembles the FTP sessions that are getting dropped.   The reason you want to send large packets is to determine if there is a router that is handling large packets incorrectly.

  Look at the %Loss figure when the Ping is finished.   A high packet loss might indicate a hardware problem on the network, either in the line itself or in a bridge, router, or other machine.

   Use MultiNet Tools TraceRoute to help isolate which machines are used in the connection.

{button ,KL(`protocol statistics')}   Related Topics

Finding Out Who is Responsible for a Problem Router

If you know which part of a network is failing, you also want to know who is responsible for fixing that part.   If the machine's owner has registered with a "white pages" server that you have access to, you can use Whois to look up contact information on full machine names, domain names, and IP addresses.

White pages only contain information about Internet hosts, not hosts internal to an organization's network.

 Start MultiNet Tools

Understanding TCP/IP Monitoring

Monitor provides detailed information about your workstation's TCP/IP communications.   When you click a toolbar button or choose a menu option, Monitor gathers the requested information and displays it in a table for your review.   Monitor lets you establish how frequently the information is updated and lets you determine if hosts should be identified by host name or IP address.   If desired, you can print the currently displayed statistics for later review.

ARP Cache

The ARP cache contains IP-to-hardware-address mappings for systems with which the workstation is communicating. By viewing the contents of the ARP cache and comparing the information displayed with known IP and hardware address pairs, you can be sure that one system on the network is not using another system's IP address.   Checking the ARP cache is useful when the workstation frequently loses connection when communicating with another host on the network.   To resolve network delivery problems, scan the ARP cache for the hardware address of the host with the delivery problem. If the correct hardware address does not appear in the ARP cache, another machine is using the target host's IP address.

Buffer Statistics

Buffer statistics indicate how much space is available for temporary storage of IP data being sent or received. To verify that all requests for memory are being honored, examine the workstation's buffer statistics. Occasionally, some requests for memory may be denied.   This is acceptable behavior.   However, if you consistently encounter denied requests for memory, contact your network administrator.

Interface Setup

The Interface table displays information about the workstation's interfaces and their configuration.   If desired, you can obtain more information about an interface entry by double-clicking the entry.

Protocol Statistics

The Protocol statistics table presents detailed networking statistics for all current connections.

Routing Table

The Routing table identifies the hosts or networks with which the workstation is communicating and the routes being used.

{button ,KL(`statistics,')}   Related Topics