KINETICS *LAN Ranger*
User Guide

About This Guide

The LAN Ranger is a monitoring program for internetworks that include Kinetics Fastpath gateways. After the internet is set up, you can use the LAN Ranger from any Macintosh Plus, Macintosh SE, or Macintosh II on the network to review the internet topology, monitor gateway configuration and performance, and run various tests.

This guide is intended for the network manager or the person who is responsible for maintaining the internet. It tells how to install and use the features of the LAN Ranger. It is not intended as a tutorial on network management issues or techniques.

Chapter 1 introduces the LAN Ranger, describes what you will need, and tells how to start the program.

Chapter 2 describes how to use the LAN Ranger to review your internet. It tells how to view the internet topology, read the Event Log, and display information about network zones.

Chapter 3 tells how to find out what network hardware and software services are available on a specific network or in a specific zone.

Chapter 4 describes how to monitor the performance of any Kinetics gateway on the internet.

Chapter 5 tells how to run various tests to evaluate how well the internet is functioning.

Appendix A provides information about gateway statistics that are displayed when you monitor a gateway's performance.

Manual Revision History

Manual Revision	Date	Summary of Changes
A	1-16-89	Initial Release Publication No. 4200119-00
B	3-6-89	First Revision Publication No. 4200119-00

Contents

Chapter 3: Identifying Network Services

Chapter 4: Monitoring Gateway Performance

Chapter 5: Running Tests

Appendix A: Gateway Statistics

Index

Chapter 1
Getting Started

The LAN Ranger is a powerful network management tool that lets you view, monitor, and test an internet that includes Kinetics FastPath gateways. Use the LAN Ranger on any Macintosh Plus, Macintosh SE, or Macintosh II on the network to perform these management tasks:

- View the internet topology.

- View a log of important network events (such as network failures) that is automatically maintained by the LAN Ranger.

- Monitor gateway traffic, transmission errors, and general gateway performance.

- Find network hardware or software services on a selected network.

- Test a gateway to make sure it has accurate zone information.

- Run an echo test on a gateway or any other node.

- Display RTMP packets.

Requirements

To use the LAN Ranger version 1.0, your internet must include Kinetics FastPath gateways. The LAN Ranger relies on connectivity information provided by Kinetics gateways to display the internet topology. This information is not currently provided by bridges and gateways from other vendors.

Note: As network management standards are developed for gateways and bridges, future versions of the LAN Ranger will be able to monitor all types of gateways and bridges.

The LAN Ranger runs on any Macintosh Plus, Macintosh SE, or Macintosh II connected to the internet. We suggest that you dedicate one Macintosh to network management, however, this is not required. The LAN Ranger automatically reinitializes the AppleTalk driver when you quit the program. You may need to reestablish some network services (such as mounted AppleShare volumes) in order to use them after quitting the LAN Ranger. Other network programs (such as HostAccess) may require that you restart your Macintosh. Since the LAN Ranger works in the background under MultiFinder, you may want to leave it running while you work on other applications.

The LAN Ranger is meant to be used by the network manager. If more than one person is using the LAN Ranger, gateway statistics and test results could be biased by the additional traffic that is created by other LAN Ranger users. If you plan to monitor statistics or run tests, you must send a message to other LAN Ranger users asking them to quit the program.

The LAN Ranger is configured to run with System versions 4.2 through 6.0.3. When Apple introduces a newer System version, you must reconfigure the LAN Ranger by using a utility that is provided for this purpose (see "Updating the LAN Ranger" in this chapter for detailed information).

The "Responder" INIT (provided with the LAN Ranger) must be installed in the System folder of all Macintoshes on the network in order for the LAN Ranger to identify and display them.

Starting the LAN Ranger

Follow these steps to start the LAN Ranger:

1. Insert the LAN Ranger disk and open it.

   The contents of the disk appear on the desktop.

Figure 1-1. Files contained in LAN Ranger disk

2. If you are running the LAN Ranger from a hard disk, copy the contents of the LAN Ranger disk to your hard disk.

   If you are running the LAN Ranger from a floppy disk, make a backup copy of the LAN Ranger disk. Store the original disk in a safe place and use the copy. Make sure the copy is unlocked.

3. Double-click the LAN Ranger icon to start the application.

The Save Event Log dialog box appears. The LAN Ranger records significant network events (such as network failures) in the Event Log. If you do not save the Event Log, you can only review it on the screen as long as the LAN Ranger is in use. When you quit the LAN Ranger, the Event Log is lost.

Note: If you are using a System version that is not recognized by the LAN Ranger, a message appears asking you to call Kinetics. Before you can start the LAN Ranger you must configure it for this System version (see "Updating the LAN Ranger" in this chapter).
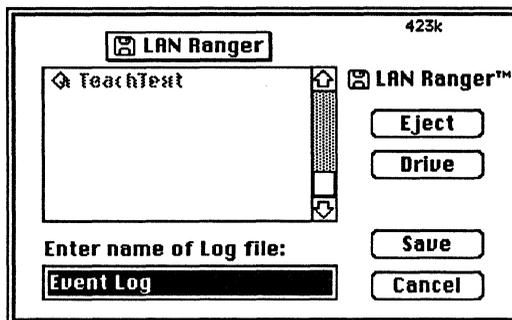
Figure 1-2. **The Save Event Log dialog box**

4. If you want to save a copy of the Event Log, type a file
    name and select the folder and disk where you want the
    file to be saved. Then click **Save**.

    If you do not want to save the Event Log, click **Cancel**.

    The Internet window appears. After a pause of up to ten
    seconds, the internet topology drawing is displayed and
    you are ready to begin working (see Chapter 2,
    "Viewing the Internet," to learn how to use the Internet
    window).

    Note: If the internet topology drawing does not appear,
    the gateways connected to your network are not
    functioning or your Macintosh is not connected to your
    network.
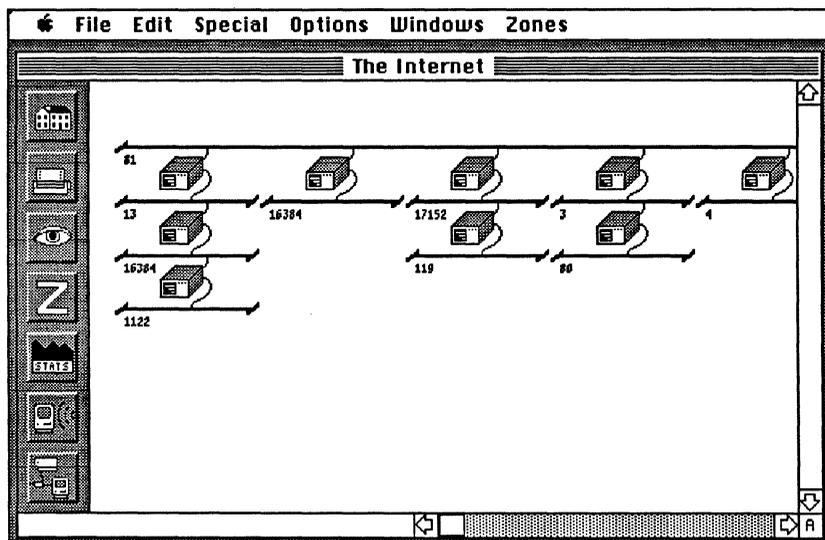
Figure 1-3.   The Internet window

Sending a Message to Other LAN Ranger Users

More than one person can run the LAN Ranger on the internet. If you plan to use the LAN Ranger to monitor gateway statistics or to run tests (such as the Echo test), the additional network traffic generated by other users will bias your test results. You will want to send each of the other users a message asking them to quit the program. The message will appear on their screen.

Follow these steps to send a message to other LAN Ranger users:

1. Choose **Find LAN Ranger Users** from the **Special** menu.

    The LAN Ranger searches the internet for other LAN Ranger users. This may take up to a minute, depending on the number of zones on your internet. You will hear a beep if other users are found.

2. Choose **Send Message to** from the **Special** menu and choose the user to whom you want to send a message from the pop-up menu that appears.

    A dialog box appears in which to enter your message.

    Note: If there are currently no other LAN Ranger users, the command **Send Message to** is dimmed.

3. Type your message and click **Send** in the dialog box to send the message.

    Click **Cancel** if you decide not to send a message.

Updating the LAN Ranger

You need to update the LAN Ranger if you are using a System version later than 6.0.3. (System versions earlier than 4.2 cannot be used with the LAN Ranger.) If the LAN Ranger is not configured for your System version, when you try to start the program a message appears advising you to call Kinetics at (800) 433-4608. A technical support person will tell you the number you need to enter to update the LAN Ranger for your System version and Macintosh type.

When you have the number, follow these steps to update the LAN Ranger:

1. Make sure that the LAN Ranger application and the Update LAN Ranger utility are in the same directory on an unlocked disk. Also check that the LAN Ranger application has not been renamed. It should appear as **LAN Ranger** ™ on the desktop.

2. Double-click the **Update LAN Ranger** utility icon.

   The Update dialog box appears. The System version you are using appears in the System Version box.

   ```
   ┌──────────────────────────────────────┐
   │  ┌────────────┐                       │
   │  │     OK     │   System Version 6.02 │
   │  └────────────┘                       │
   │  ┌────────────┐              ┌──────┐ │
   │  │    Quit    │   Offset     │      │ │
   │  └────────────┘              └──────┘ │
   └──────────────────────────────────────┘
   ```
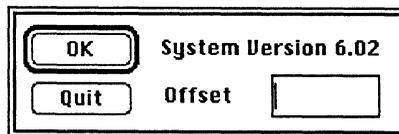
   Figure 1-4. The LAN Ranger Update dialog box

3. Type the number you received from Kinetics in the Offset Number box and click **OK**.

   The LAN Ranger is now configured properly for your System version. You are ready to start the LAN Ranger.

Quitting the LAN Ranger

To quit the LAN Ranger, choose **Quit** from the **File** menu.

Chapter 2
Viewing the Internet

When you start the LAN Ranger, it automatically polls all Kinetics gateways for connectivity information and draws the current internet topology in the Internet window. It also begins recording important network events, such as network failures, in another window called the Event Log. Both the Internet window and the Event Log remain open as long as you are running the LAN Ranger. This chapter describes how to use these windows to view the internet and monitor its status.

Using the Internet Window

The Internet window graphically displays the internet topology. It automatically shows the networks and interconnecting Kinetics gateways that are operating. Non-Kinetics gateways and bridges are also shown if you have entered connectivity information for them (see "Entering Information for Non-Kinetics Gateways and Bridges" later in this chapter).

The Internet window automatically draws the "backbone network" at the top of the screen. The backbone network is defined as the one that has the most gateways connected to it. A gateway appears as a box, and a network appears as a bold, horizontal line. The network number appears on the left, below the line.

You can select a specific gateway or a network by clicking on its icon or number. (Clicking on a selected icon or number deselects it.) The menu commands at the top of the Internet window and the buttons on the left side of the Internet window let you change the internet display, and review, monitor, and test a selected gateway or network.

Click the **Home** button to display and highlight your local network.

Network number.

A network appears as a bold line.

Gateways.

Click the **Print** button to print the internet topology drawing.

Click the **View** button to redraw the internet topology with a specified network at the top of the screen.

Click the **Zone** button to check gateway zone information.

Click the **Statistics** button to monitor the performance of a selected gateway.

Click the **Echo** button to perform an echo test on a selected gateway.

Click the **Network Services** button to find hardware and software services available on a selected network.

Status message.

You can scroll the internet topology display.

é File Edit Special Options Windows Zones

The Internet

81
13   16384   17152   3   4
16384   119   30
1122

Engineering Gateway

Figure 2-1. The Internet Window

If your internet topology is very large, you may not be able to see the entire internet on the screen at once. Use the scroll bars to scroll the rest of the internet into view.

If the Auto Verify option is turned on, the LAN Ranger constantly updates the internet topology drawing. When a network fails, it is immediately removed from the drawing; when a new network begins operating it is added to the drawing. If Auto Verify is turned off, the drawing is only updated when you redraw the Internet Window using the Redraw command. The letter "A" appears in the lower right corner of the Internet window when Auto Verify is turned on. It flashes when the LAN Ranger receives an RTMP packet from a gateway. The letter "N" appears when Auto Verify is turned off (see "Setting the Auto Verify Option" later in this chapter).

Changing the Internet View

You can change the current internet topology view so that it is redrawn from the perspective of any selected network. The selected network (or "root") appears at the top of the internet topology.

Follow these steps to change the internet view:

1. Click on the network you want to become the root.

2. Click the **View** button.

    The internet topology is redrawn with the selected network at the top.

Or

1. Make sure that no network is selected, then click the **View** button.

A dialog box appears asking you to enter the network you want to become the new root. The number of the backbone network is automatically entered as the root.

2. To change the root network, type the number of the network you want and click OK.

    The internet topology is redrawn with the specified network at the top.

Selecting Your Home Network

Your home network is the network connected to your Macintosh. Click the **Home** button to automatically select your home network. The LAN Ranger scrolls the internet topology to display your home network, if it has been scrolled out of view, and then selects it.

Redrawing the Internet Window

To redraw the internet topology when the Auto Verify option is turned off, choose **Redraw Internet** from the **Special** menu. When Auto Verify is turned off, the LAN Ranger does not automatically update the Internet window to reflect changes in the internet topology (see "Setting the Auto Verify Option" later in this chapter).

Identifying Gateways that Connect Three or More Networks

If a gateway connects three or more networks, the LAN Ranger displays the gateway more than once in the Internet window to show all the network connections to it. The diagram in Figure 2-2 shows a gateway connecting three networks. Figure 2-3 shows how these connections are shown in the Internet window.
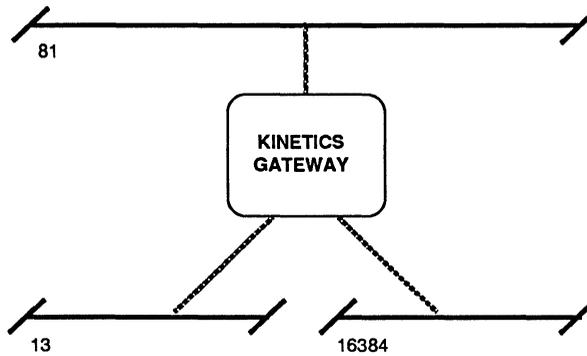
Figure 2-2. A gateway connecting three networks
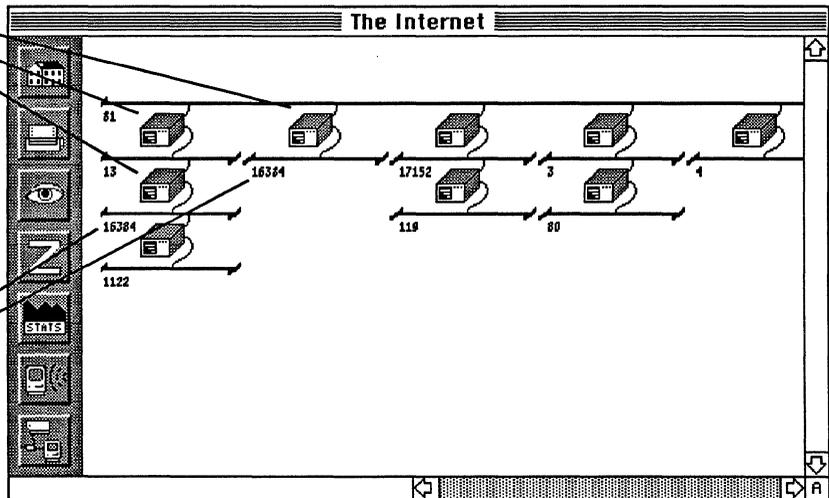
Figure 2-3. Internet window with gateway connecting three networks

Note: Although the gateway and connected networks appear near each other in the internet drawing in Figure 2-3, this is not always the case.

Entering Information for Non-Kinetics Gateways and Bridges

A non-Kinetics gateway or bridge will not appear in the Internet window unless you enter the following connectivity information for it:

- The gateway type (for example, "Hayes Interbridge").

- The name assigned to the gateway (for example, "Engineering").

- The network number of each network connected to the gateway.

- The gateway's node number on each of the networks to which it is connected.

Note: Non-Kinetics gateways and bridges include all those produced by other vendors and Kinetics gateways using non-Kinetics download code or a PROM version earlier than 4.1.

You must update connectivity information whenever it changes. For example, if a non-Kinetics gateway fails, a different node number may be assigned to the gateway when it resumes operation. You will need to change the node number you have entered for this gateway. The LAN Ranger cannot display a non-Kinetics gateway if the connectivity information you have entered is not accurate.

Note: If you do not know a FastPath gateway's node number, use the appropriate version of the *FastPath Manager* application to find out what the node number is.

Follow these steps to enter, change, or delete information for a non-Kinetics gateway:

1. Choose **Open Bridge File** from the **File** menu.

   The Other Bridges dialog box appears.

Other Bridges:

◉ FastPath 3.0   ○ Alisa UMSBridge
○ Shiva NetBridge   ○ Infosphere Liaison
○ Hayes Interbridge ○ Tridata Netway1000
○ P. Ingeniere Intertalk ○ Cayman Gatorbox
                          ○ Other
Name: [   ]

Net#   Node #   FastPath3.0 Engineering
                  Hayes Marketing
[   ] [   ]

[   ] [   ]

[   ] [   ]

[Exit]   [New] [Replace] [Delete]

If information has already been entered for a non-Kinetics bridge, the name of the bridge appears here.
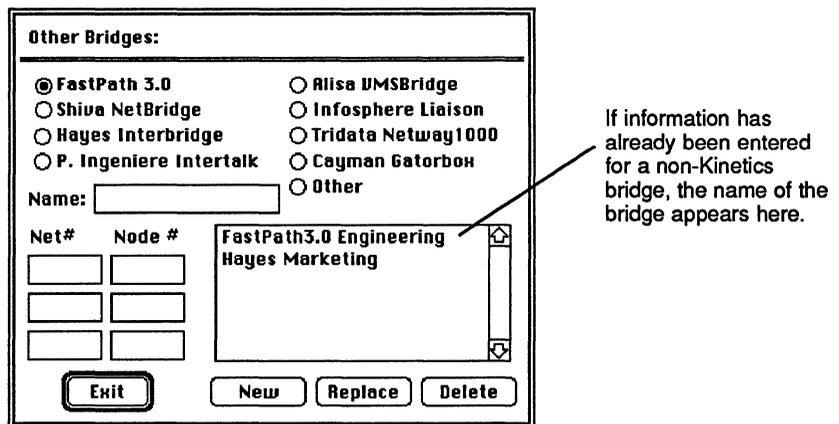
Figure 2-4. The Other Bridges dialog box

2. To enter information for a gateway for the first time, follow these steps:

   a. Click the **Radio** button to indicate the gateway type.

   b. Type the name of the gateway in the Name box.

      For example, "Marketing."

   c. In the Net # box, type the number of each network connected to the gateway.

d. In the Node # box opposite each network number you entered, type the node number used by the gateway on that network.

e. Click **New** when you have finished entering information.

   The name of the gateway appears in the list box.

To change existing information for a gateway, follow these steps:

a. Click on the gateway in the list box.

   The current information for the selected gateway appears.

b. Select any entry you want to change and type the new information.

c. Click **Replace** when you have finished changing information.

   The new information you typed replaces the old information in the file.

To delete information for a gateway, click on the gateway in the list box. Then click **Delete**.

Displaying
Isolated Networks

If you have not entered the required connectivity information for a non-Kinetics gateway or bridge, or if the information you entered is no longer accurate, the networks connected to this gateway or bridge will not appear in the internet topology drawing. Such networks are called "isolated networks."

Note: Non-Kinetics gateways include all gateways and bridges produced by other vendors and Kinetics gateways using non-Kinetics download code or a PROM version earlier than 4.1. To enter or revise connectivity information for a non-Kinetics gateway, see "Entering Information for Non-Kinetics Gateways and Bridges" earlier in this chapter.

You can display an isolated network separately if you know its network number.

Follow these steps to display an isolated network:

1. Make sure that no network is selected (to deselect a network, click on it). Then click the **View** button.

    The Change View dialog box appears.

```
Enter the network number you
want to become the new root:

[81      ]   ( OK )   ( Cancel )
```
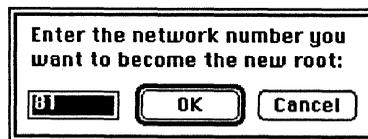
Figure 2-5. The Change View dialog box

2. Type the number of the isolated network you want to see.

   The LAN Ranger draws the network as shown in the following figure.

   Note: If the network has Kinetics gateways connected to it, displaying the isolated network will cause the entire subinternet to be drawn.
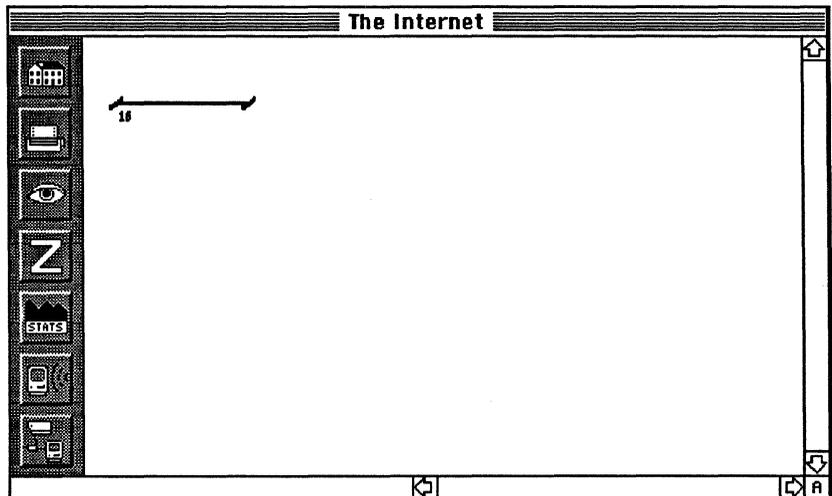
Figure 2-6. An isolated network

3. To return to the original internet drawing, click the **Home** button.

Printing the Internet Topology Drawing

You can print the internet topology drawing on a LaserWriter or ImageWriter for later review. If the internet is very large, it may be printed on several pages.

Follow these steps to print the internet topology drawing:

1. Click the **Printer** button on the left side of the Internet window.

   The Page Setup dialog box appears.

2. Specify the page setup options you want in the dialog box and click **OK** to display the Print dialog box.

   Click **Cancel** if you do not want to change page setup options.

3. Specify the print options you want in the dialog box and click **OK** to print the internet topology drawing.

   Click **Cancel** if you decide not to print.

Setting the Auto Verify Option

If the Auto Verify option is turned on, the LAN Ranger updates the internet drawing automatically to reflect changes in the internet topology. If you turn off Auto Verify, the LAN Ranger will update the internet drawing only if you choose **Redraw Internet** from the **Special** menu. To turn Auto Verify on or off, choose it from the **Options** menu. A check mark appears next to the option when it is turned on.

Reading the Event Log

The Event Log records important network events that have occurred since the program was started. The Event Log window always appears on the screen and cannot be closed. To make the Event Log window active, choose **Event Log** from the **Windows** menu or click on its window. Events are numbered sequentially and stamped with the date and time of their occurance. If the sound alert option is turned on, an alert sounds for events that could require your immediate attention (see "Setting the Sound Alert Option" later in this chapter). In the Event Log, an asterisk indicates those events that sounded an alert.

The Event Log is lost when you quit the LAN Ranger unless you save it to a file by choosing **Save Event Log to a File** from the **Special** menu. If you save the Event Log, the information is saved to an ASCII text file that you can edit and print using any word processing program.

The Event Log window display has a limited amount of memory available for its use. When this memory is exhausted, new event entries overwrite old ones, beginning with the first entries in the Event Log window.

The Event Log file is limited only by the amount of space available on the disk. If this space is exhausted, new event entries are lost—they do not overwrite old entries. You will be alerted if disk space is exhausted.

Here is an example of an Event Log containing entries:
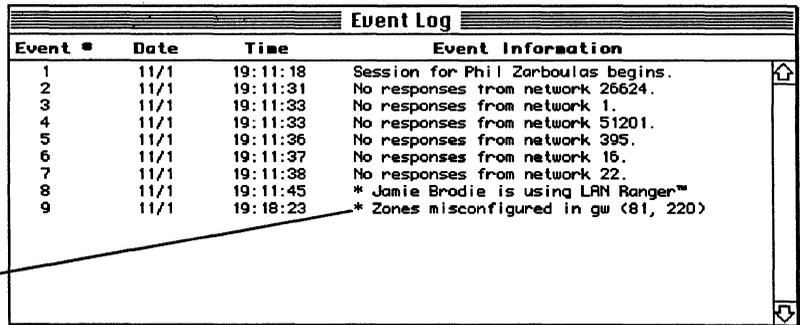
```
═══════════════════════════ Event Log ═══════════════════════════
Event #    Date       Time              Event Information
   1       11/1     19:11:18    Session for Phil Zarboulas begins.        ⬆
   2       11/1     19:11:31    No responses from network 26624.
   3       11/1     19:11:33    No responses from network 1.
   4       11/1     19:11:33    No responses from network 51201.
   5       11/1     19:11:36    No responses from network 395.
   6       11/1     19:11:37    No responses from network 16.
   7       11/1     19:11:38    No responses from network 22.
   8       11/1     19:11:45    * Jamie Brodie is using LAN Ranger™
   9       11/1     19:18:23    * Zones misconfigured in gw (81, 220)

                                                                          ⬇
```

An asterisk indicates
an event that
sounded an alert.

Figure 2-7. The Event Log

The following table lists event messages and what they mean. An asterisk indicates events that sound an alert.

Event message	Significance
*X at Y% (TH: Z%)	In the Gateway Statistics window, statistic X was at Y% load and exceeded the threshold Z% you set for it in a graph.
No response from network X	The gateway (or gateways) on network X is not responding to the LAN Ranger and will not appear in the internet topology drawing. The gateway may have failed, or network X may be isolated by a non-Kinetics gateway. (A non-Kinetics gateway is any gateway from another vendor or a Kinetics gateway that uses non-Kinetics software or a PROM version earlier than 4.1.)
*X is using LAN Ranger	Your test results and statistics will be biased if others are using the LAN Ranger. Before testing, ask other users to quit the program.
*Network X has come up	Network X has resumed operation.
*Network X has gone down	Network X has failed.
*RTMP traffic has stopped	The gateway (or gateways) connected to your local network are not operating, or the cables to your Macintosh have been disconnected.

Event message	Significance
Bad Echo data in node (X, Y)	The Echo test indicates bad data integrity for node Y on network X.
Zone misconfigured in	Gateway node Y on network X gateway (X,Y) has a mis-configured zone. You may need to reconfigure zones for this gateway (see the appropriate *Kinetics FastPath Gateway Installation Guide* for instructions on configuring FastPath gateways).
*X has quit using the LAN Ranger	X is no longer using the LAN Ranger.

Saving the Event Log to a File

If you chose not to save the Event Log to a file when you started the LAN Ranger, you can change your mind and save it at any time while you are using the LAN Ranger. The Event Log is saved to an ASCII text file that can be printed using a word processing program.

Follow these steps to save the Event Log to a file:

1. Choose **Save Event Log to a File** from the **Special** menu.

   Note: If the Event Log is already being saved to a file, **Save Event Log to a File** appears dimmed and cannot be chosen.

   A Save As dialog box appears.

2. Type the name of the file and select the folder and disk where you want the file saved. Then click **Save**.

Setting the Sound Alert Option

By setting the Sound Alert option, you control whether the LAN Ranger alerts you when an event occurs that might require your immediate attention. You can also determine how many times the alert will sound. To set this option, choose **Sound Alert** from the **Options** menu and choose the setting you want from the menu that appears.

Displaying Zone Information

The **Zones** menu lists the AppleTalk zones on the internet. To see a heirarchical menu that lists the networks located in a specific zone, hold the mouse button down on the zone in the **Zones** menu, as shown below.
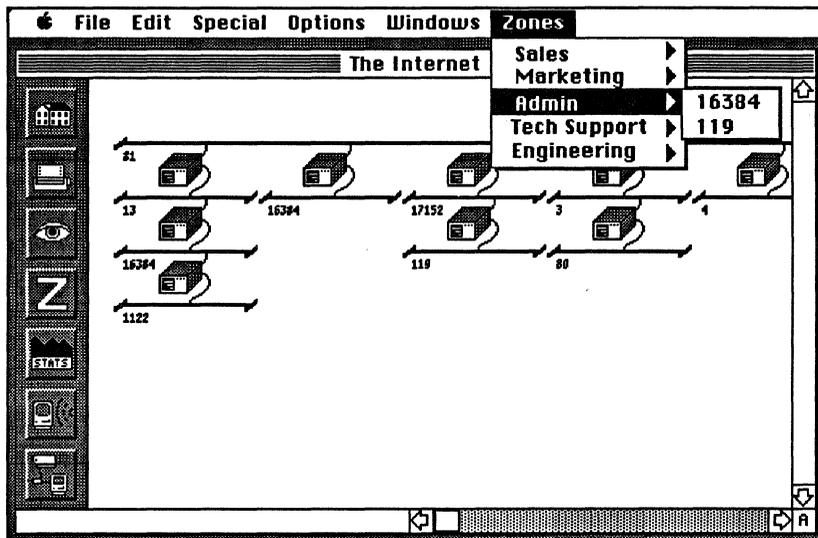
Figure 2-8. Displaying the Zones pop-up menu

Saving Zones to a File

You can save zone information to a file that can be printed using a word processing program. Zone information may change if the internet topology is redrawn. You may want to resave zone information whenever this happens.

Follow these steps to save zone information to a file:

1. Choose **Save Zones to a File** from the **Special** menu.

   A Save As dialog box appears.

2. Type the name of the file and select the folder and disk where you want the file saved. Then click **Save**.

Chapter 3
Identifying Network Services

A network service is any hardware device (such as a printer, Macintosh, or modem) or software application (such as Tops or QuickMail) that uses the network to communicate.

Use the LAN Ranger to find out what network services are available on a network or in a zone. You can look up a specific service by its user name (such as Marketing LaserWriter), look up a type of service (such as all LaserWriters), or find all available services.

Looking Up Services on a Network

To look up services on a network, you must first display the Network Services window. The LAN Ranger automatically shows the following services as icons in the window. You can then look up services that are running on a selected icon or look up services by their name and type.

- Macintosh Plus
- Macintosh SE
- Macintosh SE/30
- Macintosh II
- Macintosh IIx
- QuickMail Server
- Imagewriter
- Login Server
- FastPath K-Star IP Gateway

- AppleShare Server
- Apple IIe
- Apple IIGS
- Shiva NetModem
- LaserWriter
- FastPath DECnet Router
- InterMail Server
- IBM PC
- Login Server (K-Talk UNIX host)

Note: In order for the LAN Ranger to display a Macintosh, the Macintosh must have an INIT file called Responder in its system folder.

The node number of a service appears next to its icon in the Network Services window. Figure 3-1 shows how these services appear:

Click **Print** to print a copy of the network services drawing.

The node number.

When you select a device, the user-assigned name and the device type appear here.
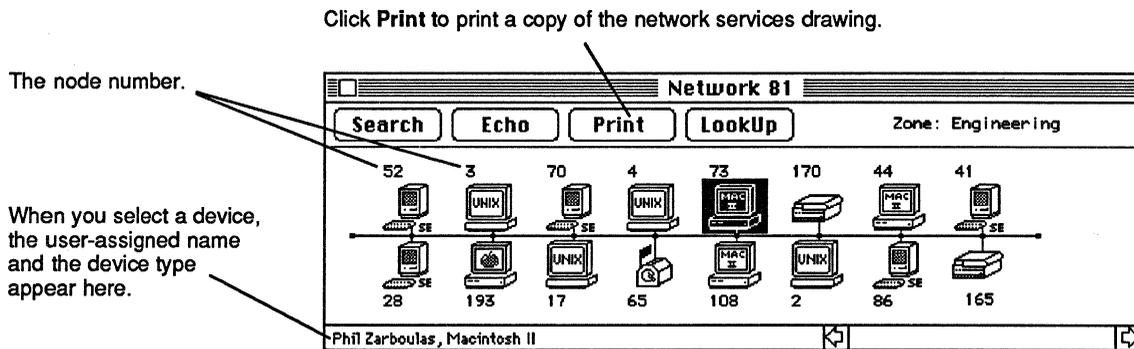
Figure 3-1. The Network Services window

Displaying the Network Services Window

Follow these steps to display the Network Services window:

1. Select the network in the Internet window.

2. Click the **Network Services** button, as shown in Figure 3-2.

   The Network Services window appears.

Click on a network to select it.

Then click the **Network Services** button.
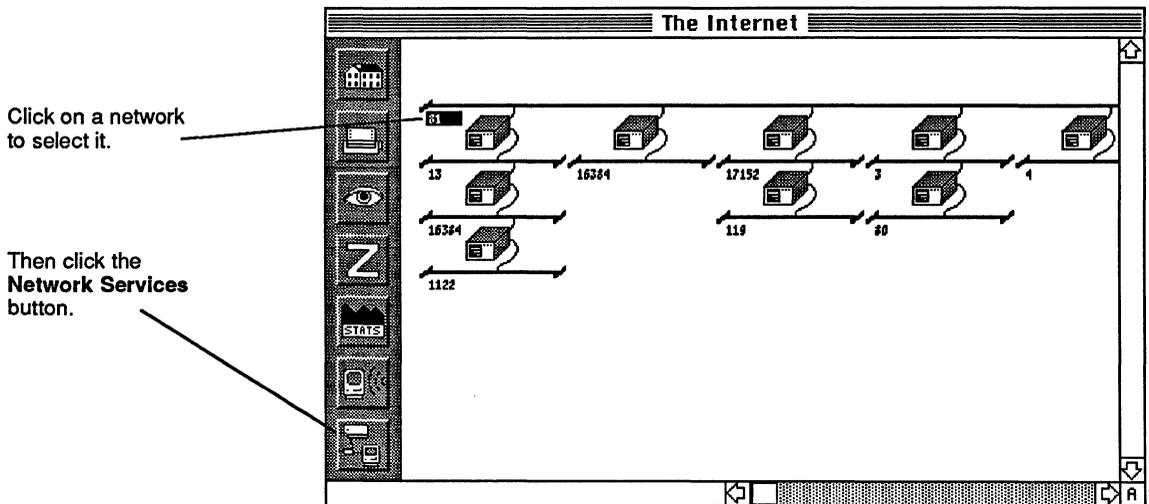
Figure 3-2. Displaying the Network Services window

3. Click **Search** in the Network Services window to search the network again. (Heavy network traffic may prevent the LAN Ranger from finding all existing services.)

   Any additional services are added to the Network Services window.

4. To find out if there are additional services running on a displayed device, see "Looking Up Services for a Selected Icon" later in this chapter.

To look for a service by its user name or service type, or to search for all available services, see "Looking Up Services by Name and Type" later in this chapter.

Looking Up Services for a Selected Icon

To display a list of network services that are running on a Macintosh or any other device shown in the Network Services window, select the icon and click **Lookup**. If additional services (such as QuickMail or Tops) are running on that device, a small window appears listing them. If there are no additional services, a message appears in the lower left corner of the window to inform you. To close the window, click the mouse button anywhere.

Clicking **Lookup** displays network services that are running on the selected device.
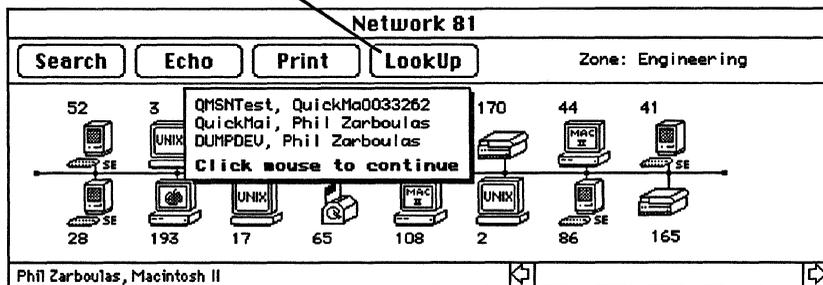
Figure 3-3. Looking up services running on a selected icon

Looking Up Services by Name and Type

You can also look up services on a network by specifying the name and type of service. The LAN Ranger searches the network and displays a list of the services you are looking for. By entering the wildcard symbol (=) for both the service name and type, you can display a list of all network services.

A service name is usually a user-assigned name (such as "Marketing Printer"), but in a few cases the name may be assigned by the software.

A service type is a word assigned by the vendor. It may differ slightly from the product name. For example, the service type for QuickMail is "QuickMai." Therefore, in order to find all QuickMail services, you must enter QuickMai as the service type. If you do not know the service type, look up all network services first to see how the service type appears.

Follow these steps to look up services by name and type.

1. Display the Network Services window for the network you want, if it is not already displayed.

   To display the Network Services window, see "Displaying the Network Services Window," earlier in this chapter.

2. Make sure that none of the icons are selected in the Network Services window. (Click a selected icon to deselect it.) Then click **Lookup**.

   The Service Lookup dialog box appears (Figure 3-4).

```
┌─────────────────────────────────────────────────────────────┐
│  Service Lookup:              ⟦ Find ⟧   ( Save )  ( Exit )  │
│                                                              │
│  Name  [=           ]   Retries [8    ]        Zone          │
│  Type  [=           ]   Interval[8    ]     [Marketing    ]  │
│  ┌──────────────────────────────────────────────────────┐⬆ │
│  │                                                      │   │
│  │                                                      │   │
│  │                                                      │   │
│  │                                                      │   │
│  │                                                      │   │
│  │                                                      │⬇ │
│  └──────────────────────────────────────────────────────┘   │
└─────────────────────────────────────────────────────────────┘
```
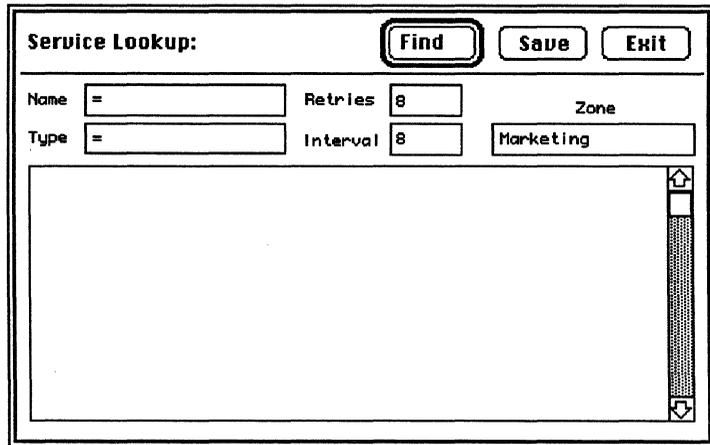
Figure 3-4. The Service Lookup dialog box

3. To look for a service by its name, type the name in the
    Name box and type an equal sign (=) in the Type box.

    To look for a type of service, type an equal sign (=) in the
    Name box and the service type (for example,
    "LaserWriter") in the Type box.

    To look for all network services, type an equal sign (=) in
    both the Name box and the Type box.

4. In the Retry box, type the number of times you want the
    LAN Ranger to search for services.

    Heavy network traffic may prevent the LAN Ranger
    from finding all services the first time it looks for them.

5. In the Interval box, type the number of ticks the LAN
    Ranger should wait between each retry. A tick is 1/60th
    of a second.

6. Click **Find** to begin the service lookup.

    The LAN Ranger searches for the service you are looking
    up and displays a list in the Service Lookup dialog box.
    Here's an example of how this list appears:
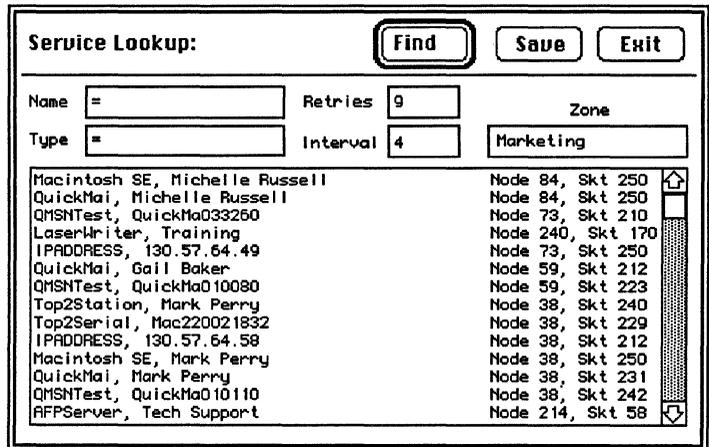
Figure 3-5. Services displayed in Service Lookup dialog box

7. If you want to save the contents of the Service Lookup
    dialog box, click **Save**.

8. Look up a different service or type of service, or click
    Exit to return to the Network Services window.

Looking Up Services in a Zone

You can also look up services in one zone or in all zones, rather than looking them up on individual networks. Looking up services in a zone takes much longer than looking up services on a network. If you are looking for a specific service and know what network the service is on, follow the steps described in "Looking Up Services on a Network," earlier in this chapter.

You look up services by specifying the name and type of service. The LAN Ranger searches the zone and displays a list of the services you are looking for. By entering the wildcard symbol (=) for both the name and type, you can display a list of all network services.

A service name is usually the user-assigned name (such as "Marketing Printer"), but in a few cases, the name may be assigned by the software.

A service type is a word assigned by the vendor. It may differ slightly from the product name. For example, the service type for QuickMail is "QuickMai." Therefore, in order to find all QuickMail services, you must enter QuickMai as the service type. If you do not know the service type, look up all network services first to see how the service type appears.

Follow these steps to look up services for a zone:

1. Choose **Look Up Services** from the **Special** menu.

   The Service Lookup dialog box appears.

```
┌──────────────────────────────────────────────────────────┐
│  Service Lookup:              [ Find ]  [ Save ]  [ Exit ]│
│                                                           │
│  Name  [=          ]   Retries [8  ]        Zone          │
│  Type  [=          ]   Interval [8  ]   [*              ] │
│  ┌────────────────────────────────────────────────────┐▲ │
│  │                                                    │  │
│  │                                                    │  │
│  │                                                    │  │
│  │                                                    │  │
│  │                                                    │  │
│  └────────────────────────────────────────────────────┘▼ │
└──────────────────────────────────────────────────────────┘
```

Figure 3-6. The Service Lookup dialog box

2. To look for a service by its name, type the name in the Name box and type an equal sign (=) in the Type box.

   To look for a type of service, type an equal sign (=) in the Name box and the service type (for example, "LaserWriter") in the Type box.

   To look for all network services, type an equal sign (=) in both the Name box and the Type box.

3. In the Retry box, type the number of times you want the LAN Ranger to search for the service.

4. In the Interval box, type the number of ticks the LAN Ranger should wait between each retry. A tick is 1/60th of a second.

5. In the Zone box, type the name of the zone. Type an asterisk (*) if you want to specify your local zone (the zone in which your Macintosh is located).

6. Click **Find** to begin the service lookup.

   The LAN Ranger searches for the service you are looking up and displays a list in the Service Lookup dialog box. Here's an example of how this list appears:

```
┌─────────────────────────────────────────────────────────────┐
│  Service Lookup:                    ( Find )( Save )( Exit )  │
│ ┌───────────────────────────────────────────────────────┐    │
│  Name │F          Retry  │8              Zone            │    │
│  Type │=          Interval│8        │*                   │    │
│ ┌───────────────────────────────────────────────────┐        │
│ │IPADDRESS,  130.57.64.32        Net 81, Node 168, Skt 72 ⬆│  │
│ │IPADDRESS,  130.57.68.30        Net 13, Node 77, Skt 72   │  │
│ │Macintosh II, Virginia Zielinski Net 13, Node 77, Skt 251 │  │
│ │QuickMai, Virginia Zielinski    Net 13, Node 77, Skt 252  │  │
│ │QMSNTest, QuickMa033293         Net 13, Node 77, Skt 252  │  │
│ │LaserWriter, Engineering Annex  Net 13, Node 194, Skt 234 │  │
│ │AFPServer, Mac II in Computer Room Net 81, Node 193, Skt 253│ │
│ │QMServer, UNIX_MAIL             Net 81, Node 65, Skt 253  │  │
│ │QMServer, TEST                  Net 81, Node 65, Skt 253  │  │
│ │QMServer, MAIL_BOX1             Net 81, Node 65, Skt 253  │  │
│ │IPADDRESS,  130.57.68.21        Net 81, Node 89, Skt 72   │  │
│ │Macintosh SE, SystemBrad        Net 81, Node 89, Skt 252  │  │
│ │IPADDRESS,  130.57.68.14        Net 81, Node 37, Skt 72   │  │
│ │Macintosh SE, SystemLeyla       Net 81, Node 37, Skt 253 ⬇│  │
│ └───────────────────────────────────────────────────┘        │
└─────────────────────────────────────────────────────────────┘
```

Figure 3-7. Services displayed in Service Lookup dialog box

7. If you want to save the contents of the Service Lookup dialog box, click **Save**.

8. You can look up a different service or type of service, or click **Exit** to return to the Network Services window.

Chapter 4
Monitoring Gateway Performance

A Kinetics gateway maintains a statistical record of its performance. It keeps track of LocalTalk and Ethernet traffic and errors, Datagram Delivery Protocol errors, and the current status of gateway buffers. The LAN Ranger can monitor these gateway statistics and display them for you in a table. You can also graph the rates of a statistic (such as LocalTalk errors) to observe how they change over a period of time.

A gateway also maintains a Gateway Log where it records significant network events (much like the LAN Ranger's Event Log) as well as diagnostic messages regarding gateway malfunctions. Use the LAN Ranger to display the Gateway Log or save it to a file for later review.

Displaying the Gateway Statistics Window

Use the Gateway Statistics window to monitor the performance of a selected gateway. From the Gateway Statistics window, you can:

- View the gateway's configuration.

- Monitor gateway statistics.

- Graph selected statistics to see how they change over time.

- Display and save the Gateway Log.

Follow these steps to display the Gateway Statistics window:

1. Select the gateway you want to monitor in the Internet window.

2. Click the **Stats** button on the left side of the Internet window.

   The Gateway Statistics window appears. This window has two views—a graph view and a table view. You can change the view by clicking **Graph** or **Table** in the window. When you first display the window, the graph view appears.

The gateway configuration appears here.

The list box shows the statistics you can graph.

You can graph up to three statistics at a time. Each statistic is plotted in a separate graph.

Click **Table** to display the gateway statistics table.
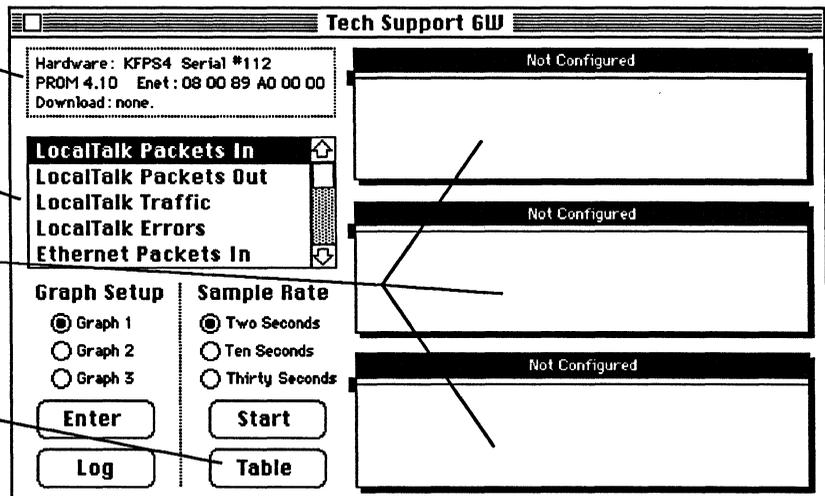
Figure 4-1. The Gateway Statistics Window (graph view)

The gateway configuration includes the gateway's serial number, the PROM version it is using, its Ethernet address, and the download code it is using (if any).

You can plot selected statistics in the graphs. For more information, see "Graphing a Statistic" later in this chapter.

3. Click **Table** to display the table view.

The graphs are replaced by the gateway statistics tables. Statistics are displayed in these tables when you monitor a gateway. For more information, see "Monitoring Gateway Statistics" in this chapter.

Monitored statistics are displayed in these four tables.

Click **Graph** to display the gateway statistics graphs.

Tech Support GW		
Hardware: KFPS4 Serial #112		
PROM 4.10 Enet: 08 00 89 A0 00 00		
Download: none.		

LocalTalk Statistics		Ethernet Statistics	
Packets In		Packets In	
Packets Out		Packets Out	
CRC Errors		CRC Errors	
Overruns		Overruns	
Underruns		Brdcst. Drops	
Bad Packets		Rsro. Errors	
Collsions		Algn. Errors	
Defers		Bad Transmit	
No Handler		Ovrsize Frame	

| LocalTalk Packets In |
| LocalTalk Packets Out |
| LocalTalk Traffic |
| LocalTalk Errors |
| Ethernet Packets In |

Graph Setup
- ◉ Graph 1
- ◯ Graph 2
- ◯ Graph 3

[Enter]
[Log]

Sample Rate
- ◉ Two Seconds
- ◯ Ten Seconds
- ◯ Thirty Seconds

[Start]
[Graph]

DDP Statistics		Buffer Statistics	
Bad Hop Count		Total	
Bad DDP Type		Free	
Bad Dest. Net		Ethernet Chip	
Too Long DDP		LocalTalk Rcv.	
Too Short DDP		Ethernet Rcv.	
Bad ATP Skt.		ARP	
Bad RTMP Skt.		Malloc	
Bad ZIP Skt.		General	
Bad KLAP Skt.		Dropped	

Figure 4-2. The Gateway Statistics Window (table view)

Clicking **Log** displays the Gateway Log. See "Reading the Gateway Log" later in this chapter for more information about this log.

Monitoring Gateway Statistics

Gateway statistics are a cumulative record of a gateway's performance since the gateway was started or the gateway memory was last cleared. When you monitor gateway statistics, the LAN Ranger retrieves the information from the gateway and displays it in a table in the Gateway Statistics window. It continues to monitor the gateway and update the statistics in the table as they change. You can temporarily stop the LAN Ranger from updating the table by clicking **Pause**. You may want to do this in order to make a note of statistics for later reference.

While you are monitoring statistics, you can also choose to graph certain statistics (such as LocalTalk traffic) to see how they fluctuate over time. See "Graphing a Statistic" later in this chapter for detailed instructions. When you have finished monitoring gateway statistics, just close the Gateway Statistics window.

Follow these steps to monitor gateway statistics:

1. In the Internet window, select the gateway you want to monitor.

2. Click the **Stats** button on the left side of the Internet window.

   The Gateway Statistics window appears.

3. Click **Table** in the Gateway Statistics window to display the table view.

4. To begin monitoring statistics, click **Start**.

The following figure shows how statistics appear in the Gateway Statistics window.
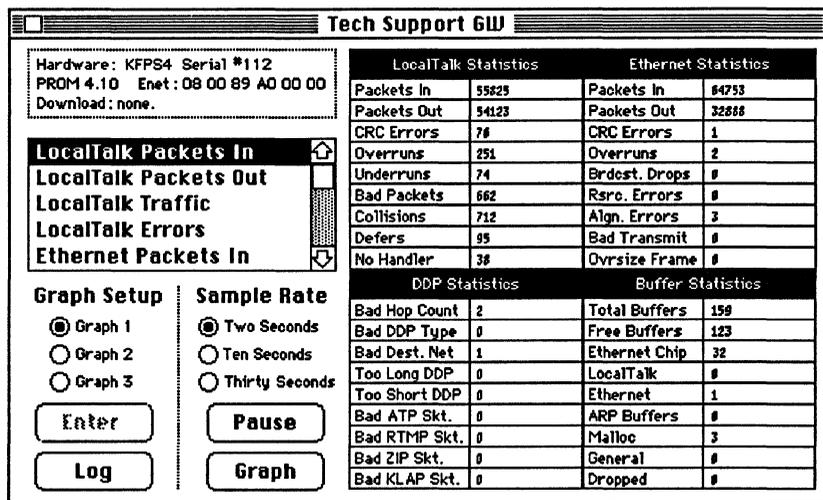
Figure 4-3. The Gateway Statistics window showing monitored statistics

The LAN Ranger monitors four kinds of statistics:

- **LocalTalk Statistics** include the total number of packets received and sent by the gateway on LocalTalk, and the occurrence of various types of LocalTalk transmission and reception errors.

- **Ethernet Statistics** include the total number of Ethernet packets received and sent by the gateway, and the occurrence of various types of Ethernet transmission and reception errors.

- **Datagram Delivery Protocol Statistics** reflect how often various kinds of Datagram Delivery Protocol errors have occurred.

- **Buffer Statistics** tell you the total number of gateway buffers, how many buffers are free, and how many are in use.

Note: For a detailed description of individual statistics and what they indicate, see Appendix A.

Graphing a Statistic

While you are monitoring gateway statistics, you can plot any of the following statistics to see their rate of change over time.

- **LocalTalk Packets In** —packets coming into the gateway from LocalTalk.

- **LocalTalk Packets Out** —packets leaving the gateway on LocalTalk.

- **LocalTalk Traffic** —the sum of the number of packets coming into the gateway and leaving the gateway on LocalTalk.

- **Ethernet Packets In**—packets coming into the gateway on Ethernet.

- **Ethernet Packets Out**—packets leaving the gateway on Ethernet.

- **Ethernet Traffic** —the sum of the number of packets coming into the gateway and leaving the gateway on Ethernet.

- **LocalTalk Errors**—the sum of CRC errors, overruns, and underruns on LocalTalk.

- **Ethernet Errors**—the sum of resource errors, alignment errors, CRC errors, and overrun errors on Ethernet.

You can graph up to three statistics at a time. Follow these steps to graph a statistic:

1. Click **Graph** in the Gateway Statistics window to display the graphs view if it is not already displayed.

2. Click the graph you want to use to plot the statistic under Graph Setup.

   If you click a graph that is currently in use, it will be cleared to graph the new statistic you have chosen.

3. Click the sample rate you want under Sample Rate.

   Note: You can change the sample rate at any time while the statistic is being graphed by first clicking the graph in Graph Setup, then clicking a different sample rate.

4. Double-click the statistic you want to graph in the list box. Or select the statistic in the list box and click **Enter**.

5. Click **Start** to begin graphing the statistic.

   The following figure shows how graphed statistics appear.
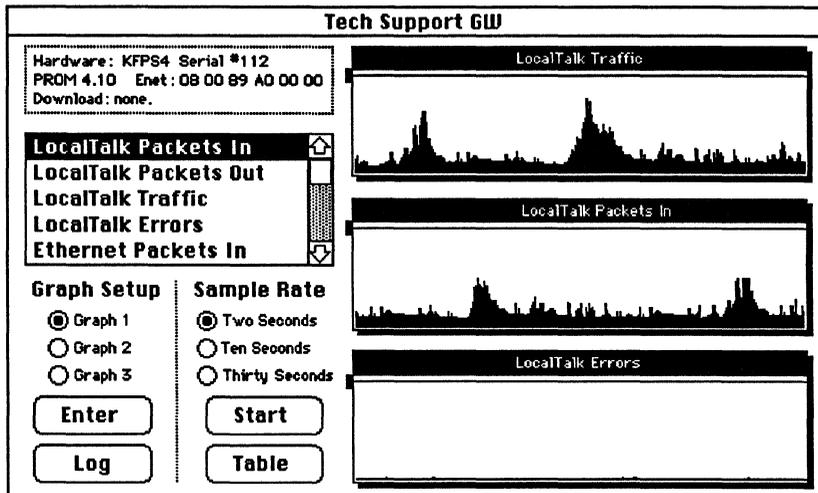
Figure 4-4. The Gateway Statistics window showing graphed statistics

Showing Information for a Selected Point

To display additional information about a point on a graph, place the cursor over the point and hold down the mouse button. A box appears containing the information, as shown in Figure 4-5. The following information is displayed:

- The percentage of the gateway's capacity that was being used.

- The actual number of packets per second represented.

- The time when the statistic was graphed.

Hold down the mouse button to display
additional information about a selected point.
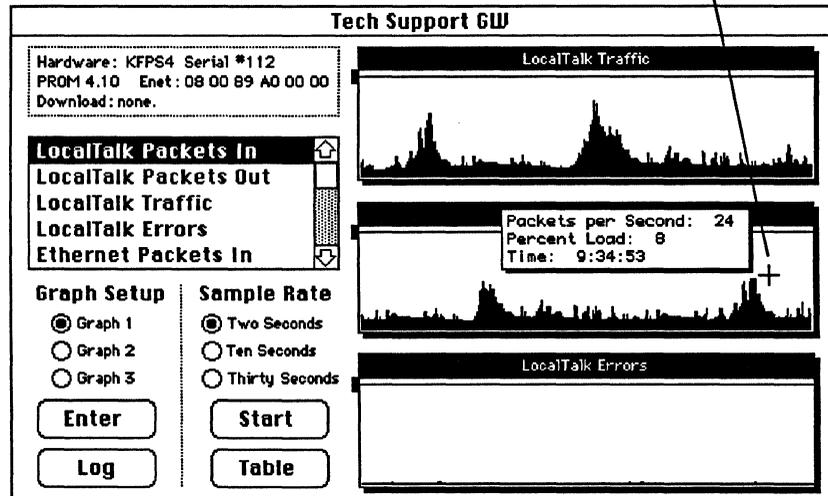
Figure 4-5. Displaying information about a selected point on a
graph

Setting a Threshold for a Graphed Statistic

You can also set a visual threshold for any statistic you are
graphing to cause the LAN Ranger to sound an alert whenever
the statistic exceeds the threshold. An alert message is posted in
the Event Log for your reference.

Follow these steps to set a threshold for a statistic you are
graphing:

1. Drag the handle on the left side of the horizontal line that
    appears at the top of the graph (see Figure 4-6).
    Move the handle up or down to set the threshold.

A small hand appears when you drag on the handle.

Drag on the handle...   ...to set the threshold for this statistic.

Tech Support GW

Hardware: KFPS4 Serial #112
PROM 4.10 Enet : 08 00 89 A0 00 00
Download: none.

LocalTalk Traffic

LocalTalk Packets In
LocalTalk Packets Out
LocalTalk Traffic
LocalTalk Errors
Ethernet Packets In

LocalTalk Packets In

Graph Setup | **Sample Rate**
⦿ Graph 1 | ⦿ Two Seconds
◯ Graph 2 | ◯ Ten Seconds
◯ Graph 3 | ◯ Thirty Seconds

LocalTalk Errors

[Enter]   [Start]

[Log]   [Table]
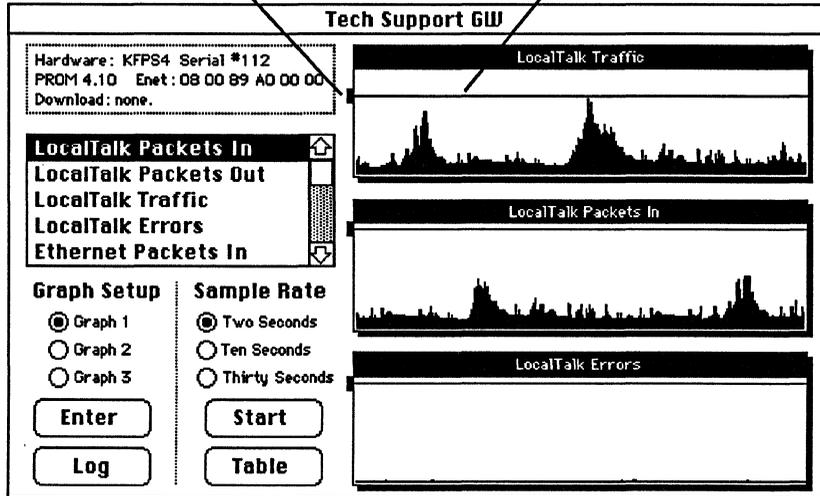
Figure 4-6. Setting a threshold for a graphed statistic

Saving Gateway Statistics to a File

While you are monitoring statistics, you can continuously save the gateway statistics table to an ASCII file. The file can be imported into a database or spreadsheet program, like Microsoft Excel, for later analysis.

Follow these steps to save gateway statistics to a file.

1. Choose **Save Statistics to a File** from the **File** menu.

    The Save As dialog box appears.

2. Type the name of the file and choose the folder and disk where you want the file saved.

3. Click **Save**.

Reading the Gateway Log

The Gateway Log records network events (such as network failures) and diagnostic messages that indicate when and why the gateway did not function properly. The Gateway Log is especially useful when you are tracking down a gateway or a network malfunction. For more information about diagnostic messages and suggestions about what action to take if any is needed, see Appendix F in the *Kinetics FastPath 4 Installation Guide*.

Follow these steps to display a Gateway Log:

1. Select the gateway in the Internet window and click the **Stats** button on the left side of the window.

   The Gateway Statistics window appears.

2. Click **Log** in the Gateway Statistics window.

   The Gateway Log appears. The following is an example of a Gateway Log.

```
┌──────────────────────────────────────────────────────────────┐
│  ┌─────────────┐  ┌─────────────┐                             │
│  │    Save     │  │    Exit     │                             │
│  └─────────────┘  └─────────────┘                             │
│  ┌──────────────────────────────────────────────────────┬──┐ │
│  │•Mismatched net numbers: local=81; 2001 reported on ETALK│⬆│ │
│  │•Mismatched net numbers: local=81; 2001 reported on ETALK│ │ │
│  │•Mismatched net numbers: local=81; 2001 reported on ETALK│ │ │
│  │•Mismatched net numbers: local=81; 2001 reported on ETALK│ │ │
│  │•Net 2000 went down                                      │ │ │
│  │•Net 2001 went down                                      │ │ │
│  │•Net 7 went down                                         │ │ │
│  │•Ethernet transmission error: 8060                       │ │ │
│  │•Ethernet transmission error: 8060                       │ │ │
│  │•Ethernet transmission error: 8060                       │ │ │
│  │•Ethernet transmission error: 8060                       │ │ │
│  │•Ethernet transmission error: 8060                       │ │ │
│  │•Ethernet transmission error: 8060                       │ │ │
│  │•Net 17152 went down                                     │ │ │
│  │•Net 119 went down                                       │ │ │
│  │•Net 1234 went down                                      │⬇│ │
│  └──────────────────────────────────────────────────────┴──┘ │
└──────────────────────────────────────────────────────────────┘
```

Figure 4-7. A Gateway Log

Saving the Gateway Log to a File

While the Gateway Log is displayed, you can save it to an ASCII file. The file can be printed using a word processing application, such as Microsoft Word.

Follow these steps to save the gateway log to a file:

1. Click **Save** in the Gateway Log (see Figure 4-7).

   A Save As dialog box appears.

2. Type the name of the file and select the folder where you want the file saved. Then click **Save**.

Chapter 5
Running Tests

Use the LAN Ranger to verify a gateway's zone information, run an Echo test to monitor a node's performance and local traffic conditions, or display RTMP packets to check on a non-Kinetics gateway.

Verifying a Gateway's Zone Information

For the internet to function properly, all gateways must have the same network zone information. When you first start the LAN Ranger or when a new network starts operation, it's a good idea to verify zone information for all gateways. You'll also want to verify zone information when you or another user cannot find a network service (such as a LaserWriter) that you know exists.

When you verify zone information, the LAN Ranger compares the zone information stored in the gateways. If there is a discrepancy, the LAN Ranger displays a message to let you know. A gateway that has incorrect zone information must be restarted and reconfigured.

Note: To reconfigure gateway zones, follow the appropriate steps described in "Launching the FastPath Manager II" and "Configuring a Gateway" in the *Kinetics FastPath 4 Installation Guide*. Be sure to tell other users not to use services on the internet while you are reconfiguring the gateway.

Follow these steps to verify a gateway's zone information:

1. To test zones for a specific gateway, select the gateway you want to test.

   To test zones for all gateways, make sure that no gateway is selected in the Internet window. (Clicking on a selected gateway deselects it.)

   Note: Testing zones for all gateways will take longer than testing zones for a selected gateway.

2. Click the **Zone** button in the Internet window (shown below).
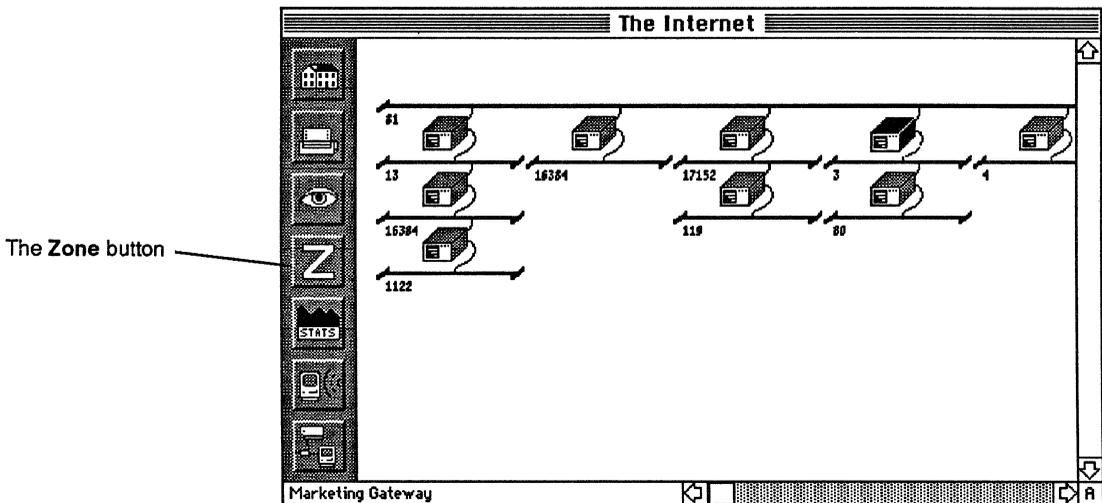
The **Zone** button ——

Figure 5-1. The Zone button in the Internet window

If the gateway's zones are configured correctly, a message lets you know.

If the LAN Ranger finds an error, a message tells you how this gateway's zone information differs from the information stored in your local gateway. See the appropriate *Kinetics Fast Path Installation Guide* for information about reconfiguring a gateway's zones.

If a gateway is missing zone information for a network, a message lets you know.

Using the Echo Test

You can perform an Echo test on any network node. The Echo test sends packets from your Macintosh to a specified network node and measures how long it takes for those packets to be returned (the delay time). The delay time is measured in "ticks." A tick is a sixtieth of a second.

The Echo test can reveal information about the following :

- The traffic load along the path to the selected network node.

- The distance from your Macintosh to the selected node.

- How well the node or gateway is performing—that is, how well it can receive and return packets.

- How well data integrity is being maintained.

The LAN Ranger checks data integrity when you run the Echo test if you set the Echo Data Check option on the **Options** menu to Hex AA or Hex 55. Setting this option to Hex AA causes the LAN Ranger to send packets that contain data in a 10101010 bit pattern. Setting it to Hex 55 causes the LAN Ranger to send packets in a 01010101 bit pattern. Setting it to None causes the LAN Ranger to send empty packets when you run the Echo test and data integrity is therefore not tested. To set the Echo Data Check Option, choose **Echo Data Check** from the **Options** menu and select the option you want.

The Echo test is started from the Echo dialog box. This is how information appears while you are running an Echo test.

The number of packets sent so far.

The number of packets received back.

The average time delay.

The number of the node you are testing.

The network on which the node is located.

The total number of packets you are sending.
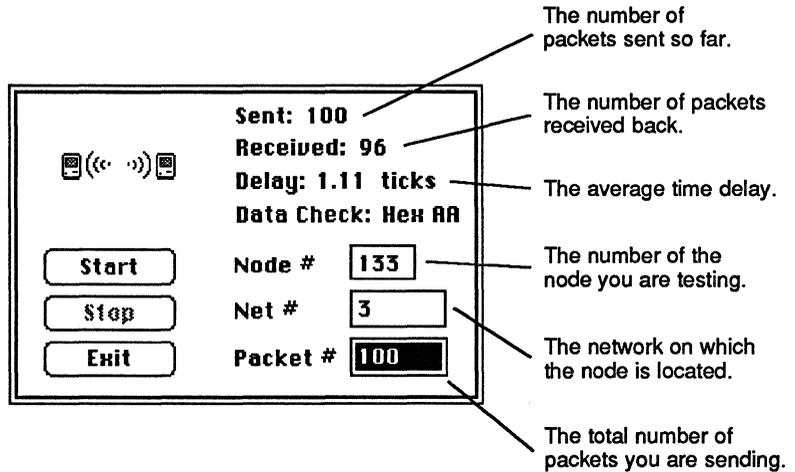
Figure 5-2. The Echo dialog box

Running the Echo Test on Gateways

To test a gateway, first display the Internet window.

1. If the gateway appears in the internet topology drawing, select the gateway to be tested, and click the **Echo** button.
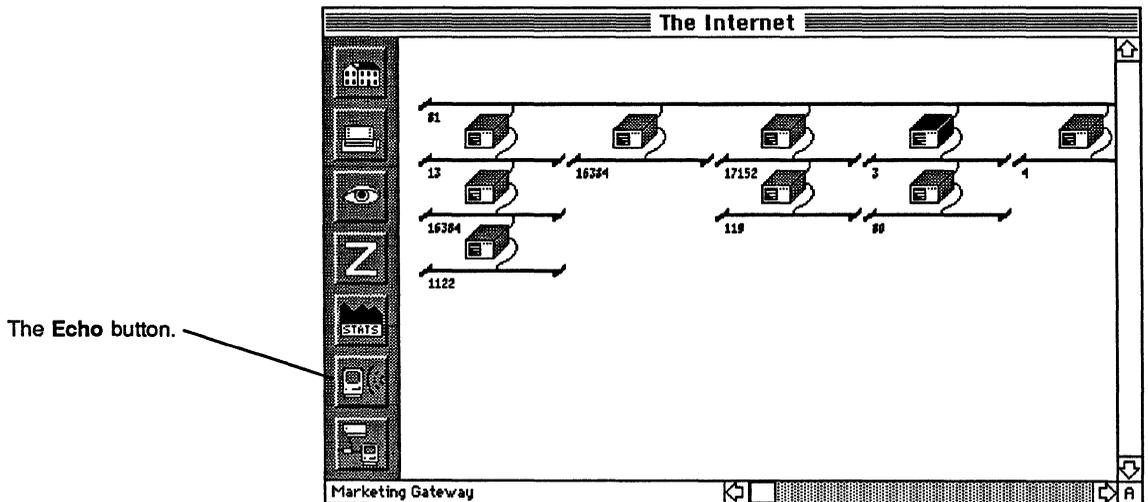
The **Echo** button.

Figure 5-3. The Echo button in the Internet window

If the gateway does not appear in the internet topology drawing, choose **Echo Test** from the **Special** menu.

The Echo dialog box appears.

2. If you selected a gateway from the Internet window, the node number and network number are entered for you.

If you choose Echo from the **Special** menu, type the node number and network number of the node you want to test.

3. The Packet box indicates the number of packets that will be sent. The number 100 is entered for you. To change this number, select the box and type a new number.

4. Click **Start** to start the test.

   While the test is running, the Echo dialog box shows how many packets have been sent and received. If a data integrity error occurs, a dialog box interrupts the test to inform you of the error. When the test is completed, the Echo dialog box shows the average delay time (see Figure 5-2).

Running the Echo Test on Other Network Nodes

To test a node that is currently displayed in the Network Services window, follow these steps:

1. Select the node and click **Echo** in the Network Services window.

   The Echo dialog box appears. The node number and network number are automatically entered for the node you selected.

2. Type the number of packets in the Packets box.

3. Click **Start** to begin the test.

If the node you want to test is not currently displayed in the Network Services window, follow these steps.

1. Choose **Echo** from the **Special** menu.

   The Echo dialog box appears.

2. Type the node number and network number of the node you want to test.

3. Type the number of packets in the Packets box.

4. Click **Start** to begin the test.

   While the test is running, the Echo dialog box shows how many packets have been sent and received. If a data integrity error occurs, a dialog box interrupts the test to inform you of the error. When the test is completed, the Echo dialog box shows the average delay time and any data integrity problems (see Figure 5-2).

Displaying RTMP Packets

RTMP (Routing Table Maintenance Protocol) packets are AppleTalk packets that are broadcast every 10 seconds by both Kinetics and non-Kinetics bridges and gateways on your local network. These packets contain routing information about the networks on the internet. When you display RTMP packets you can see which networks and local gateways are operating. This is useful for checking non-Kinetics gateways because these gateways may not appear in the Internet window.

Follow these steps to display RTMP packets:

1. Choose **Display RTMP Packets** from the **Special** menu.

   The RTMP Packets window appears. The window is blank.

2. Click **Start**.

   The LAN Ranger begins recording all RTMP packets that are broadcast on the network. It displays this information in the window, as shown in the following figure. If a network does not appear, you can assume that the corresponding gateway(s) is not operating.

The total number of RTMP packets received since Start was clicked.

A hop represents a packet's passage through a gateway.
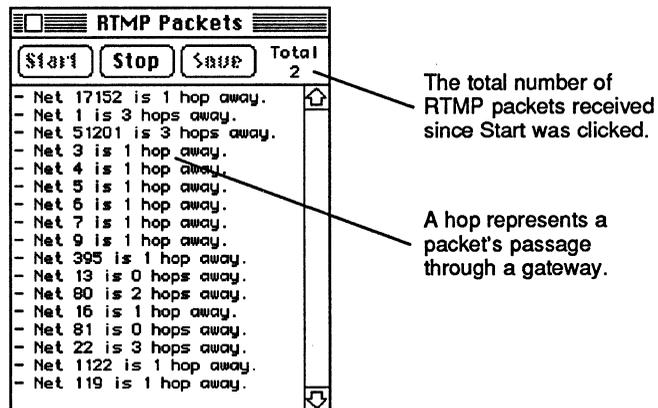
Figure 5-4. The RTMP Packets window

3. The LAN Ranger continues capturing RTMP packets until you click **Stop** to stop the test.

   Click **Save** to save the contents of the window to a file that can be printed.

4. When you have finished capturing RTMP packets, close the window.

Saving RTMP Packets to a File

After you have displayed RTMP packets, you can save the results of an RTMP packets test to a file that can be printed using any word processing application.

1. Click **Save** in the RTMP Packets window.

   A Save As dialog box appears.

2. Type the name of the file and select the folder and disk where you want the file saved. Then click **Save.**

Appendix A

Gateway Statistics

This appendix provides information about gateway statistics that appear in the table in the Gateway Statistics window (see Chapter 4, "Monitoring Gateway Performance").

LocalTalk Statistics

LocalTalk statistics measure LocalTalk traffic entering and leaving the gateway, and various transmission and reception errors.

Bad Packets   The number of packets that contained bad AppleTalk control information and therefore could not be identified by the gateway. Bad packets could be the result of a software error on the part of the sender.

Collisions   The number of times a node did not acknowledge receipt of an RTS packet that was sent by the gateway. Either the node was too busy to receive the packet, the node was turned off, or the packet collided with another packet.

Note: When a FastPath gateway is started up, the collision rate will initially be 620 because the node-finding packets are counted as collisions.

CRC   Cyclic Redundancy Check is a transmission error from any LocalTalk node that indicates corrupt data. Check for bad cabling, loose wires, or improperly terminated cables. When CRC statistics rise, it may be an indication that the network has too many nodes—traffic is increasing and there are more transmission errors.

Defers   The number of times a gateway attempted to send a packet but could not do so because traffic was too heavy. Defers are an indication of how much traffic there is on the line.

No Handler   The number of packets received that had an unknown ALAP protocol handler. This indicates a software error.

Overruns   The number of packets that came into the gateway faster than the gateway could process them. A node may be violating AppleTalk transmission specifications by sending data at too fast a rate.

                Note: Kinetics FastPath 1, 2, and 3 have slower processors than Kinetics FastPath 4 and therefore may have a higher Overrun error rate.

Packets in   The total number of packets received by the gateway since the gateway was last started up or since the gateway memory was last cleared. By comparing this statistic for a group of gateways, you can determine whether one gateway is receiving more than its share of traffic.

Packets out   The total number of packets sent by the gateway since the gateway last started up or since the gateway memory was last cleared.

Underruns   The number of packets that came into the gateway too slowly. This may indicate a bad driver in a node that may be violating AppleTalk transmission specifications by sending data at too slow a rate.

Ethernet Statistics

Ethernet statistics measure Ethernet traffic entering and leaving the gateway, and various transmission and reception errors.

Alignment Errors   The number of packets received that contained improperly aligned data. Alignment errors could be caused by bad cabling, or a node that is not functioning properly due to a bad Ethernet chip or bad software.

Bad Transmit   A bad transmit error is generated whenever the gateway has tried 16 times to send a packet and failed. Bad transmit errors probably indicate that there is too much traffic on the network.

Broadcast Drops   The number of times the gateway dropped a broadcast packet internally because the gateway was overloaded. Broadcast packets are information packets sent to all network nodes. These packets have the lowest priority for processing and are the first type of packet to get dropped when the gateway is overloaded. Some broadcast drops will always occur.

CRC   Cyclic Redundancy Check is a transmission error from some Ethernet node that indicates corrupt data. Check for bad cabling, loose wires, or improperly terminated cables. When CRC statistics rise, it may be an indication that the network has too many nodes—traffic is increasing and there are more transmission errors.

Overruns	The number of Ethernet packets that came into the gateway faster than the Ethernet chip could process them. A node may be violating Ethernet transmission specifications by sending data at too fast a rate.
Oversized Frame	The number of oversized packets received by a gateway. A network node is violating Ethernet specifications regarding packet length.
Packets in	The total number of packets received by the gateway since the gateway was last started up or since the gateway memory was last cleared. By comparing this statistic for a group of gateways, you can determine whether one gateway is receiving more than its share of traffic.
Packets out	The total number of packets sent by the gateway since the gateway last started up or since the gateway memory was last cleared.
Resource Errors	The number of packets dropped because the gateway CPU did not give the Ethernet chip a buffer to accept the packet. If resource errors are high, it indicates there is too much traffic for the memory resources allocated to the Ethernet chip. This statistic represents a hardware level packet drop.

DDP
Statistics

Datagram Delivery Protocol statistics measure high level software or protocol errors.

Bad Destination Network The number of packets containing a network destination the gateway did not recognize. These errors are generated when a network goes down while packets are still being transmitted to it from a gateway. Also could be caused by bad software—a node may be sending out packets that have incorrect destination information.

Bad ATP Socket The number of packets addressed to an unknown AppleTalk Transaction Protocol client. This statistic indicates bad application software.

Bad DDP Type The number of packets with an unknown DDP protocol handler.

Bad Hop Count The number of packets that passed a gateway more than 16 times in an attempt to reach their destination. Bad hop count will rise when a network goes down. Packets may be passed between gateways many times in an attempt to reroute them to their destination. Bad Hop Count is a measure of relative internet stability. If networks fail often, Bad Hop Count will be high.

Bad KLAP Socket The number of packets addressed to an unknown Kinetics Link Access Protocol client. This statistic indicates bad application software.

Bad RTMP Socket   The number of packets addressed to an unknown Routing Table Maintenance Protocol client. This statistic indicates bad application software.

Bad ZIP Socket   The number of packets addressed to an unknown Zone Information Protocol client. This statistic indicates bad application software.

Too Long DDP   The number of packets that exceeded the maximum length of the Datagram Delivery Protocol level.

Too Short DDP   The number of DDP packets whose length field says that the packet is longer than it is.

Buffer Statistics

Buffer statistics measure the number of total buffers, free buffers and dropped buffers, and the status of individual buffers.

ARP
The number of buffers filled with Address Resolution Protocol (ARP) packets.

Dropped
The number of times a buffer was needed but no buffers were free.

Ethernet Chip
The number of buffers allocated to the Ethernet chip for packet reception.

Ethernet
The number of buffers filled with Ethernet packets that are waiting to be processed by the gateway.

Free
The total number of free buffers.

General
The number of buffers being used for outgoing packets, such as LocalTalk packets, Ethernet packets, and Zone Information packets.

LocalTalk
The number of buffers filled with LocalTalk packets that are waiting to be processed by the gateway.

Malloc
The number of buffers required by the CPU for non-packet related functions.

Total
The total number of buffers, including free buffers and AppleTalk, Ethernet, ETQueue, ARP, Malloc, and General buffers.

Note: If the number of total buffers is not equal to the number of free buffers plus the number of buffers in use, you may be running bad download code on the gateway.

Index

N

network
   deselecting, 2-1
   failure of, 2-3
   selecting, 2-1
network manager, 1-2
network node, and echo test, 5-3/7
network number, 2-1, 2-9/10, 5-5/6
network service icons, 3-1
network services
   definition, 3-1
   identifying, 3-1/10
   looking up (name/type), 3-5/7
   looking up (network), 3-1/7
   looking up (selected icon), 3-4
   looking up (zones), 3-8/10
network services window, displaying, 3-1/4
network, in Internet window, 2-1
network zone information. See zone information
"No Handler," A-2
node number
   of a gateway, 2-6, 5-5/6
   of a network service, 3-2
non-Kinetics download code, 2-6
non-Kinetics gateways/bridges, 1-2, 2-1, 5-8
   and changing information, 2-8
   definition, 2-6, 2-14
   and deleting information, 2-8
   and entering information, 2-6/8

O

"Overruns," A-2, A-4
"Oversized Frame," A-4

P

"Packets in," A-2, A-4
"Packets out," A-2, A-4
packets, number of, 5-6, 5-7
pause, in statistics updating, 4-4
PROM version, 2-6, 2-9, 2-14

R

Redraw command, 2-3
"Resource Errors," A-4
Responder INIT, 1-2, 3-2
root (network), 2-3/4
Routing Table Maintenance Protocol packets. See
      RTMP packets
RTMP packets, 2-3
   definition, 5-8
   displaying, 5-8/9
   saving to a file, 5-9

S

sample rate, 4-7
scroll bars, 2-3
service name, definition, 3-5. See also network
      services
service type, definition, 3-5. See also network
      services
Sound Alert option, 2-12
   setting, 2-16
statistics. See gateway statistics; see also specific
      types of statistics
System folder, 1-2
System versions, 1-2, 1-4, 1-7

T

test results, biasing of, 1-2, 1-6, 2-14
tests, running, 5-1/9
threshold, for graphed statistics, 4-9/10
tick, definition, 3-7
"Too Long DDP," A-6
"Too Short DDP," A-6
"Total," A-7

U

"Underruns," A-3

W

wildcard symbol, and network services, 3-5, 3-6, 3-8, 3-9

Z

zone information
  displaying, 2-16/17
  saving to a file, 2-16/17
  verifying, 5-1/3
zones, and looking up services, 3-8/10