Chapter 4

Monitoring and Maintaining Your Network

Chapter 3 described how to configure your network. This chapter describes how to monitor and maintain your network. The TALnet software allows you to monitor and maintain your network at two levels:

- Using TALnet commands
- Using standard Simple Network Management Protocol (SNMP) MIB-II variables

This chapter describes both of these methods.

4.1 TALnet Monitoring Commands

The TALnet software provides the following methods of monitoring your network:

- Display network and configuration statistics.
- Test connectivity of other systems.
- Trace the route IP datagrams travel.
- Analyze the received signal strength (RSS) of packets from neighboring transmitters.

The following subsections describe these methods.

4.1.1 Displaying Statistics

The commands in Table 4-1 allow you to display statistics about your configuration. Enter the commands at the service console or through a remote Telnet connection.

Table 4-1 TALnet Monitoring Commands

Command	Function
arp	Displays the current contents of the Address Resolution Protocol (ARP) cache.
device show {*device-name* | **all**} [**verbose**]	Displays the configuration and some statistics about devices.

Table 4-1 TALnet Monitoring Commands

Command	Function
domain cache clean	Displays whether or not expired Domain Name System (DNS) records are discarded.
domain cache list	Displays the DNS cache.
domain cache only	Indicates the state of "ignore Domain.txt."
domain cache size	Displays the memory size for the DNS cache.
domain cache wait	Displays the time in seconds between DNS cache file updates.
domain list	Displays the DNS server list.
domain retry	Displays the number of retries.
domain suffix	Displays the local domain-name suffix.
hop maxttl	Displays the current maximum time-to-live used by the traceroute facility. In other words, this command displays the maximum number of hops a traceroute will follow when testing the route a datagram travels.
hop maxwait	Displays the current length of time a host will wait for a response during a traceroute.
hop queries	Displays the current number of queries sent to each router during a traceroute.
hop trace	Displays whether hop-trace checking is on or off.
icmp echo	Displays whether Internet Control Message Protocol (ICMP) echoing is on or off.
icmp status	Displays the status of ICMP.
iface show {*iface-name* | **all**} [**verbose**]	Displays the configuration and some statistics about interfaces.
ip address	Displays the current Internet Protocol (IP) address.
ip pool	Displays the current pool of IP addresses that are available for dynamic assignment.
ip rtimer	Displays the current IP retransmission timer in seconds.
ip status	Displays statistics about IP.
ip ttl	Displays the current maximum time to live for locally created IP datagrams.
log [[**-f**] **console** | [**-f**] **session** | *filename*]	Displays logging and debugging information, either directly on the service console, in a separate session, or in a file.
memory	Displays system memory and packet buffer usage.
memory freelist	Displays the storage allocator freelist.
memory ibufsize	Displays the current size of the interrupt buffer.
memory sizes	Displays a history of requested storage allocator sizes.
memory thresh	Displays the current memory threshold size in bytes.
rip merge	Displays whether or not the Routing Information Protocol (RIP) is set up to merge redundant entries.

Table 4-1 TALnet Monitoring Commands

Command	Function
rip status	Displays the RIP counters and the RIP neighbor table.
route	Displays the routing table.
snmp community show {*community* | **all**}	Displays information about the specified community or about all defined communities.
snmp syscontact	Displays the currently named system contact.
snmp syslocation	Displays the current description of the system location.
talk show neighbors [**verbose**]	Displays all remote Wireless Routers to which the router can transmit or from which the router can receive.
talk show radio	Displays currently configured radio parameters (radio model, channel number, frequency, default and per-link power settings, and pseudorandom noise [PN] code).
talk show rss [*talk-address*]	Shows the accumulated results of the received signal strength (RSS) analysis.
talk show timers	Displays information about the timing values the TALtalk protocol is currently using.
talk show debug	Displays which parts of the TALtalk protocol are currently generating debugging information.
tcp ceiling	Displays the current maximum round-trip time in milliseconds.
tcp floor	Displays the current minimum round-trip time in milliseconds.
tcp irrt	Displays the current value in milliseconds for the initial round-trip time to be used for Transmission Control Protocol (TCP) connections.
tcp limit	Displays the current window size limit in bytes.
tcp mss	Displays the current segment size in bytes that will be sent on all outgoing TCP connection requests.
tcp status	Displays the status of TCP data sent and received.
tcp syndata	Displays whether or not SYNs and data can travel together in the same packet.
tcp window	Displays the current window size.
time	Displays the current time on the Wireless Router.
udp status	Displays statistics relating to the User Datagram Protocol (UDP).
uptime	Displays the amount of time since the Wireless Router last rebooted.
user show {*name* | **all**} [**verbose**]	Displays the user table.
version	Lists the current version of TALnet software.
who	Lists users who are currently logged on to the Wireless Router.

For more information about these commands, see Appendix A, “TALnet Command Reference.”

4.1.2 Testing Connectivity of a System

You can test whether a system is alive and reachable using the Packet Internet Groper (ping) facility. When you issue a ping, you send an ICMP *Echo Request* datagram to the system you are querying. If the remote system, or host, is alive and reachable, it will return an ICMP *Echo Reply* datagram. The result of a ping is the IP address of the host you are querying and the delay time (round-trip time) between when the local host sent the *Echo Request* datagram and received the *Echo Reply* datagram.

To test the basic connectivity of a system, use the **ping** command. You can issue the following variants to this command:

- To send a single ping to a host, use the following command:

  ping *hostid*

- By default, the data portion of an ICMP Echo Request is 16 bytes. You can change this to contain up to 1472 bytes of data. In general, you would change this to test the round-trip time for longer datagrams. This helps you identify routes that cannot handle longer datagrams. To change the length of the data packet, use the following **ping** command:

  ping *hostid length*

- When testing connectivity to a host, you should issue repeated pings to the server to determine an average response time. To send multiple pings, you must specify the interval in milliseconds to wait between each ping. Use the following **ping** command:

  ping *hostid length interval*

  Note that you must specify the length of the data packet in addition to specifying the interval to wait. If you perform repeated pings to a host, the initial ping might take longer than subsequent pings. This is usually because the initial ping is trying to resolve DNS name and IP address, or if the destination's physical address is not in the ARP cache. To end the series of pings, use the **reset** command.

4.1.3 Testing the Route a Datagram Travels

You can test the route a datagram travels using the traceroute facility. When you invoke the traceroute facility, you send an IP datagram with a time to live (TTL) of 1; this indicates that the datagram can only travel one hop to its destination. When a router receives a datagram with a TTL of 0 or 1, it must not forward that datagram. Instead, it sends a "time exceeded" message to the source host. The source host then increments the TTL to 2, and resends the datagram. In this way, it determines the path the datagram is taking. It also calculates the round-trip time for each hop. Keep in mind, however, that even consecutive datagrams might not follow the same path to a destination. You can invoke and configure the traceroute facility using the following **hop** commands:

- To test the route an IP datagram travels, use the **hop check** command:

  hop check *hostid*

  The DNS name and IP address of each router displays, along with the TTL and the round-trip time of the response. The first round-trip time usually is longer than others because the router must do an ARP exchange.

- To alter the TTL field and thereby change the maximum number of routers a datagram will pass through, use the **hop maxttl** command. The default TTL is 30.

  hop maxttl *number*

- To change the amount of time in seconds that the source router will wait for a reply before timing out, use the **hop maxwait** command:

  hop maxwait *number*

4.1.4 Analyzing the RSS of Neighboring Routers

The TALnet software allows you to analyze the received signal strength (RSS) of packets from neighboring transmitters. By analyzing the signal strength of packets that come in from a neighbor over a period of time, you can determine whether you should adjust the power from the neighboring transmitter to the Wireless Router you are analyzing.

Analyzing the RSS is a two-step process:

1. Configure the receiving Wireless Router to gather data on the RSS. To do this, use the **talk radio analyze** command:

   talk radio *iface-name* **analyze rss on**

   Where:

   - *iface-name*—Represents the symbolic name of the wireless interface you are analyzing. This name is the one you assigned with the **talk radio address** command.

   You can turn off this feature with the command **talk radio** *iface-name* **analyze rss off**. You can view whether this feature is turned on or off with the command **talk radio** *iface-name* **analyze rss**.

2. View the resulting data using the **talk show rss** command:

   talk show rss [*talk-address*]

   Where:

   - *talk-address*—Is the TALtalk link-layer address of the neighboring transmitter. If you do not specify a neighbor, this command shows the average RSS for all neighbors that you analyze.

Ideally, your signal quality should be high enough to allow an average bit error rate (BER) of 10^{-6} or lower. Table 4-2 shows the digital RSS value that appears in the output of the **talk show rss** command, and relates that value to the signal quality. Note that exact values might vary.

Table 4-2 Received Signal Strength (RSS)

DC Voltage at the RSS Test Point	Digital RSS Value in Decimal	Signal Quality (Average BER)	RSS in dBm (Interference Free)
7.5	192	$<10^{-10}$	>-70
7.0	179	$<10^{-10}$	>-70
6.5	166	$<10^{-10}$	>-70
6.0	154	$<10^{-10}$	-70

Table 4-2 Received Signal Strength (RSS)

DC Voltage at the RSS Test Point	Digital RSS Value in Decimal	Signal Quality (Average BER)	RSS in dBm (Interference Free)
5.5	141	$<10^{-10}$	-88
5.0	128	10^{-7}	-94
4.5	115	10^{-6}	-95
4.0	102	10^{-5}	-98
3.5	90	10^{-4}	-100
3.0	77	10^{-3}	-101
2.5[1]	64	10^{-3}	-102
2.0[1]	51	10^{-2}	-103
1.5[1]	38	10^{-2}	-105

1. Occasional sync loss

If you determine that the power for a particular neighbor should be reconfigured, use the **talk radio neighbor MW** subcommand within the configuration file for that Wireless Router. See Chapter 3, “Configuring the TALnet Software,” for more information.

4.2 SNMP

You can gather statistics about your router using the Simple Network Management Protocol, Version 1 (SNMPv1).

The TALnet software supports the standard MIB-II as specified in RFC 1213, “Management Information Base for Network Management of TCP/IP-based internets: MIB-II.” TALnet also provides a proprietary MIB that allows you to gather statistics on the radio interfaces. This section provides a background on SNMP and describes basic SNMP-related tasks. See Appendix B, “TAL Proprietary Management Information Base (MIB),” for the TALnet-proprietary MIB.

4.2.1 Overview of SNMP

SNMP is an application-layer network management protocol that allows you to send queries to or set variables on network devices such as routers. SNMP consists of three elements:

- SNMP manager—A network management client program that requests or sets information. SNMP managers run on Network Management Stations (NMSs).
- SNMP agent—A software module on a managed network device, such as a router. The agent contains information the manager can monitor or change, and sends traps to the manager that alert the manager when network conditions change.
- Management Information Base (MIB)—A repository on the managed network device that contains performance and administrative information about that device. The MIB defines variables maintained by the agent that the manager can request or set. (The term MIB also refers to the document that describes the information that can be read or set on a managed device.)

SNMP supports the following operations:

- Get-request—The SNMP manager sends a request to the agent, asking for a value from a specific variable.
- Get-next-request—The SNMP manager sends a request to the agent, asking for a value of the variable following the named variable. Get-next requests are useful for traversing entire branches of a MIB database.
- Set-request—The SNMP manager sends a value for a specific variable to the agent to store.
- Get-response—The SNMP agent replies to the Get or Get-next request.
- Trap—The SNMP agent sends an unsolicited message to the manager, alerting the manager that a condition on the network has changed.

Note The current version of the TALnet software does not support trap operations. Set operations are only valid for the current session. In addition, the software does not support SNMPv2 get-bulk-request operations.

4.2.2 Supported MIBs

The following Requests For Comments (RFCs) describe SNMP and MIB standards:

- RFC 1155, “Structure and Identification of Management Information for TCP/IP-based Internets”
- RFC 1212, “Concise MIB Definitions”
- RFC 1213, “Management Information Base for Network Management of TCP/IP-based internets: MIB-II”
- RFC 1354, “IP Forwarding Table MIB”
- RFC 1443, “Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)”
- RFC 1573, “Evolution of the Interfaces Group of MIBs”
- RFC 1724, “RIP version 2 MIB Extensions”

The TALnet software provides support for the following MIB-II standard object identifiers:

- System
- Interfaces
- Address translation
- IP
- ICMP
- TCP
- UDP
- SNMP

4.2.3 Configuring Your Router to Support SNMP

You must configure your router to support SNMP:

1. Define at least one community string for your Wireless Router.

   SNMP messages contain community strings, which determine access to an SNMP agent. You can define communities with either read-only access or read-write access to the agent. Enter the following in the configuration file:

   snmp community add *community access*

   Where:

   - *community*—Specifies the community name, and must be a single word that can use uppercase and lowercase letters and numbers.
   - *access*—Indicates the level of access members of that community have, and can be either **read-write** or **read-only**.

2. Enable the SNMP agent on the router. Enter the following in the configuration file:

   start snmp

3. Limit access to the router.

   To provide additional access restrictions, define IP packet filters. For more information, see Section 3.10, “Establishing IP Packet Filters.”

4. Make sure the NMS you use can access the TAL-proprietary MIB.

4.2.4 Sending SNMP Requests

As a network manager, you monitor routing statistics from a network management station (NMS). This station acts as the SNMP manager. To send SNMP requests from the NMS, enter the IP address of the router you are querying and provide the community string (defined with the **snmp community add** subcommand in the configuration file). The conventions you use to send SNMP requests depend on your SNMP client software.