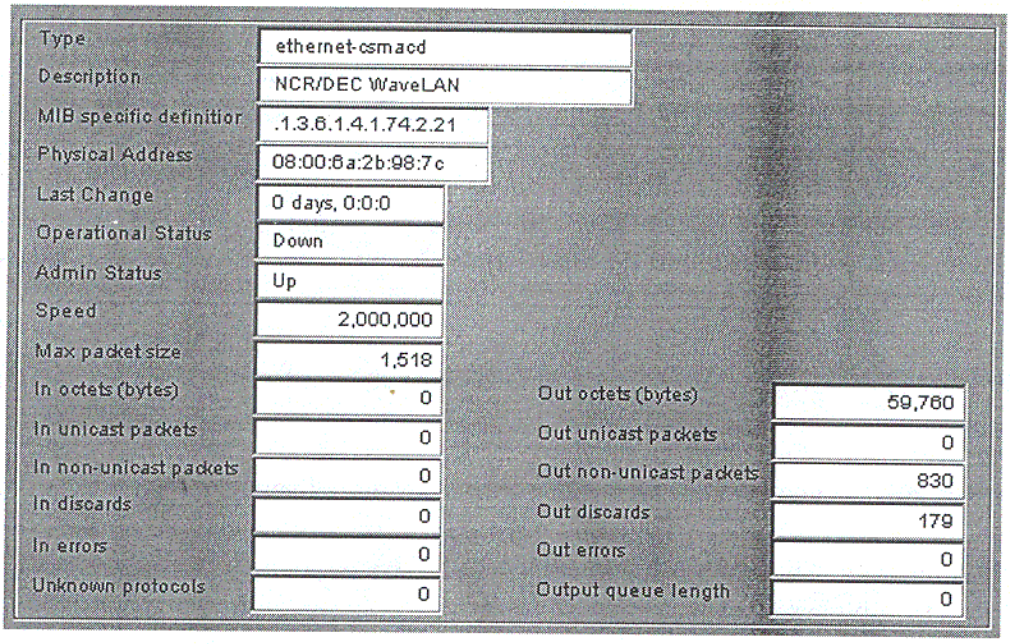
Interface Monitor

The interfaces table contains information on the unit's interfaces. Each interface is thought of as being attached to a 'subnetwork'. Note that this term should not be confused with 'subnet' which refers to an address-partitioning scheme used in the Internet suite of protocols.



Type	ethernet-csmacd		
Description	NCR/DEC WaveLAN		
MIB specific definitior	.1.3.6.1.4.1.74.2.21		
Physical Address	08:00:6a:2b:98:7c		
Last Change	0 days, 0:0:0		
Operational Status	Down		
Admin Status	Up		
Speed	2,000,000		
Max packet size	1,518		
In octets (bytes)	0	Out octets (bytes)	59,760
In unicast packets	0	Out unicast packets	0
In non-unicast packets	0	Out non-unicast packets	830
In discards	0	Out discards	179
In errors	0	Out errors	0
Unknown protocols	0	Output queue length	0

Type - The type of interface, distinguished according to the physical-link protocols immediately below the network layer in the protocol stack. The possible types are: other, regular1822, hdh1822, ddn-x25, rfc877-x25, ethernet-csmacd, iso88023-csmacd, iso80024-tokenbus, iso88025-tokenring, iso99026-man, starLan, proteon-10Mbit, proteon-80Mbit, hyperchannel, fddi, lapb, sdlc, ds1, e1, basicISDN, PrimaryISDN, propPointToPointSerial, ppp, softwareloopback, eon, ethernet-3Mbit, nsip, slip, ultra, ds3, sip, frame-relay.

Description - A textual string containing information about the interface. This string should include the name of the manufacturer, the product name, and the version of the hardware interface.

MIB specific definator - A reference to MIB definitions specific to the particular media being used to realize the interface. For example, if the interface is being realized by an Ethernet, then the value of this object refers to a document defining objects specific to the Ethernet. If this information is not present, its value will be set to 0.

Physical Address - The interface's address at the protocol layer immediately below the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.

Last Change - The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last reinitialization of the local network-managment subsystem, then this object contains a value of zero.

Operational Status - The state of the interface. The testing state indicates that no operational packets can be passed. Up - ready to pass packets; Down - cannot pass packets; testing - in some test mode.

Admin Status - The desired state of the interface. The testing state indicates that no operational packets can be passed.

Speed - An estimate of the interface's current bandwidth in bits per second. For interfaces which do not vary in bandwidth or whose bandwidth can't be accurately estimated, this object should contain the nominal bandwidth.

Max packet size - The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces used for transmitting network datagrams, this is the size of the largest network datagram that can be sent on the interface.

In octets (bytes) - The total number of octets (bytes) received on the interface, including framing characters.

In unicast packets - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

In non-unicast packets - The number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.

In discards - The number of inbound packets to which were chosen to be discarded even they were deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.

In errors - The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Unknown protocols - The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.

Out octets(bytes) - The total number of octets (bytes) transmitted out of the interface, including framing characters.

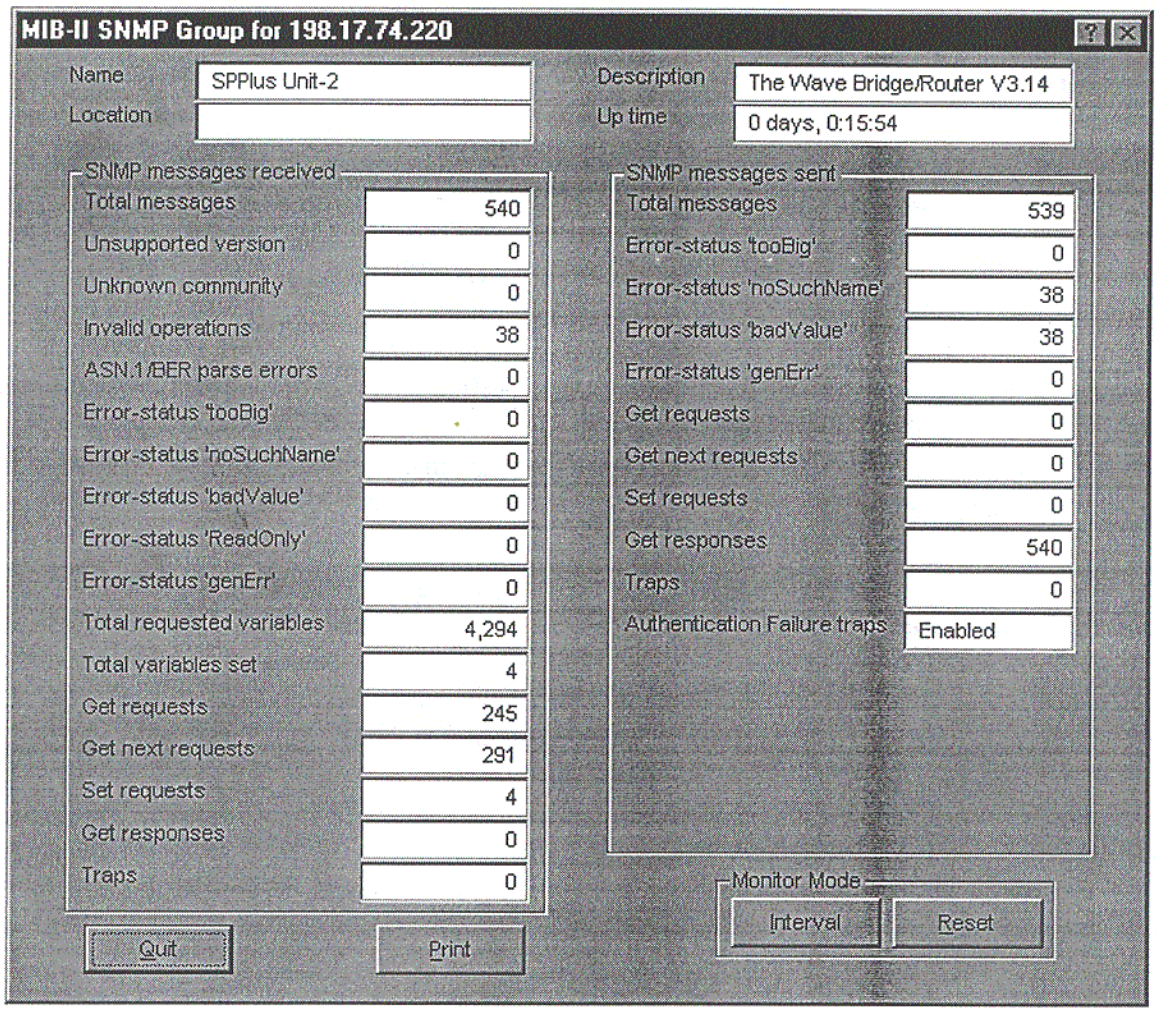
Out unicast packets - The total number of packets that higher-layer protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Out non-unicast packets - The total number of packets that higher-layer protocols requested be transmitted to a non-unicast (i.e. a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.

Out errors - The number of outbound packets that contained errors preventing them from being transmitted via this interface.

Output queue length - The total number of octets (bytes) waiting to be transmitted via this interface.

SNMP Monitor



SNMP Messages Received

Total Messages - The total number of SNMP messages received.

Unsupported Version - The total number of SNMP messages which were delivered to the SNMP protocol entity and were for an unsupported SNMP version.

Unknown Community - The total number of SNMP messages delivered to the SNMP protocol entity which used an SNMP community name not known to the unit.

Invalid Operations - The total number of SNMP messages delivered to the SNMP protocol entity which represented SNMP operations not allowed by the SNMP community named in the message.

ASN.1/BER parse errors - The total number of ASN.1 or BER errors encountered by the SNMP protocol entity when decoding received SNMP messages.

Error-status 'too big' - The total number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field was 'too big'.

Error-status 'noSuchName' - The total number of SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field was 'noSuchName'.

Error-status 'badValue' - The total number of SNMP PDUs delivered to the SNMP protocol entity for which the error-staus field was 'badValue'.

Error-status 'ReadOnly' - The total number of valid SNMP PDUs delivered to the SNMP protocol entity for which the value of the error-status field was 'ReadOnly'. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value 'ReadOnly' in the error-status field; use this field to detect incorrect implementations of SNMP.

Error-status 'genErr' - The total number of SNMP PDUs delivered to the SNMP protocol entity for which the error-status field was 'genErr'.

Total requested variables - The total number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.

Total variables set - The total number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid Set-Request PDUs.

Get requests - The total number of SNMP Get-request PDUs accepted and processed by the SNMP protocol entity.

Get next requests - The total number of SNMP Get-next PDUs accepted and processed by the SNMP protocol entity.

Set requests - The total number of SNMP Set-request PDUs accepted and processed by the SNMP protocol entity.

Get responses - The total number of SNMP Get-response PDUs accepted and processed by the SNMP protocol entity.

Traps - The total number of SNMP Trap PDUs accepted and processed by the SNMP protocol entity.

SNMP Messages Sent

Total Messages - The total number of SNMP messages passed from the SNMP protocol entity to the transport service.

Error-status 'tooBig' - The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field was 'tooBig'.

Error-status 'noSuchName' - The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field was 'noSuchName'.

Error-status 'badValue' - The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field was 'badValue'.

Error-status 'genErr' - The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field was 'genErr'.

Get requests - The total number of SNMP Get-request PDUs generated by the SNMP protocol entity.

Get next requests - The total number of SNMP Get-next-request PDUs generated by the SNMP protocol entity.

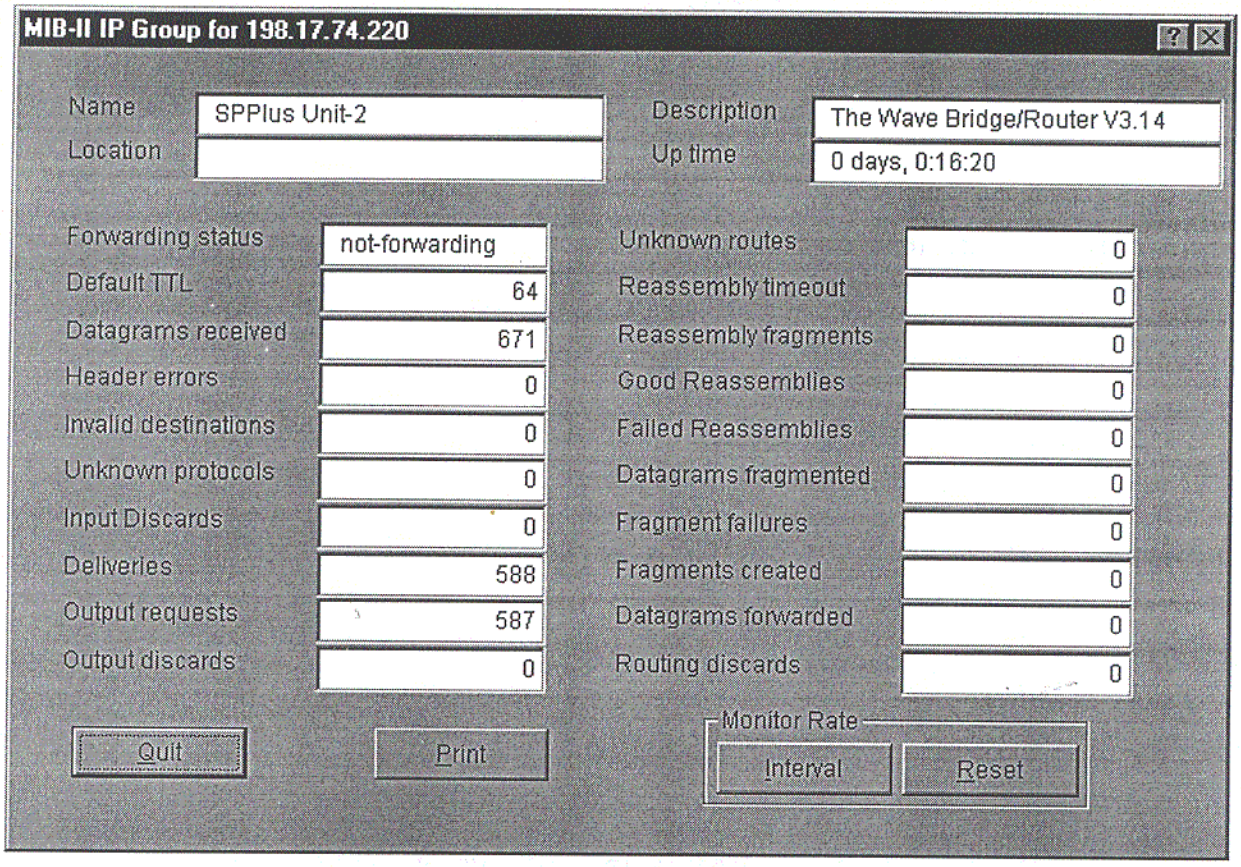
Set requests - The total number of SNMP Set-request PDUs generated by the SNMP protocol entity.

Get responses - The total number of SNMP Get-response PDUs generated by the SNMP protocol entity.

Traps - The total number of SNMP Trap PDUs generated by the SNMP protocol entity.

Authentication Failure Traps - Indicates whether the SNMP agent process is permitted to generate authentication-failure traps.

IP Monitor



The SPEEDLAN brouter keeps the standard SNMP MIB II statistics on IP type protocols as follows:

Forwarding Status - Indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to this enitity. IP gateways forward datagrams, and IP hosts do not (except those source-routed via the host). Note that for some managed nodes, this object may take on only a subset of the possible values.

Default TTL - The default value inserted into the Time-To-Live field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport-layer protocol.

Datagrams received - The total number of IP datagrams received by the host.

Header errors - The number of input datagrams discarded due to errors in their IP headers, including bad checksum errors, version-number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.

Invalid destinations - The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address for this entity to receive. This count includes invalid addresses (i.e., 0.0.0.0) and addresses of unsupported classes (i.e., Class E). For entities which are not IP gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.

Unknown protocols - The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

Input Discards - The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded anyway (e.g., for lack of buffer space). Note that this counter does not include any datagrams discarded while awaiting re-assembly.

Deliveries - The total number of input datagrams successfully delivered to IP user-protocols.

Output requests - The total number of IP datagrams which user-protocols (including ICMP) supplied to IP in-requests for transmission. Note that this counter does not include any datagrams counted in **Datagrams forwarded**.

Output discards - The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded anyway (e.g., for lack of buffer space). Note that this counter would include datagrams counted in **Datagrams forwarded** if any such packets met this (discretionary) discard criterion.

Unknown routes - The number of IP datagrams discarded because no route could be found to transmit them to their destination. Note that this counter includes any packets counted in **Datagrams forwarded** which meet this 'no-route' criterion, as well as any datagrams which a host cannot route because all of its default gateways are down.

Reassembly timeout - The maximum number of seconds that received fragments are held while they are awaiting reassembly at this entity.

Reassembly fragments - The number of IP datagrams received which needed to be reassembled at this entity.

Good Reassemblies - The number of IP datagrams successfully reassembled.

Failed Reassemblies - The number of failures detected by the IP reassembly algorithm (for whatever reason - timed out, errors, etc.). Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

Datagrams fragmented - The number of IP datagrams that have been successfully fragmented at this entity.

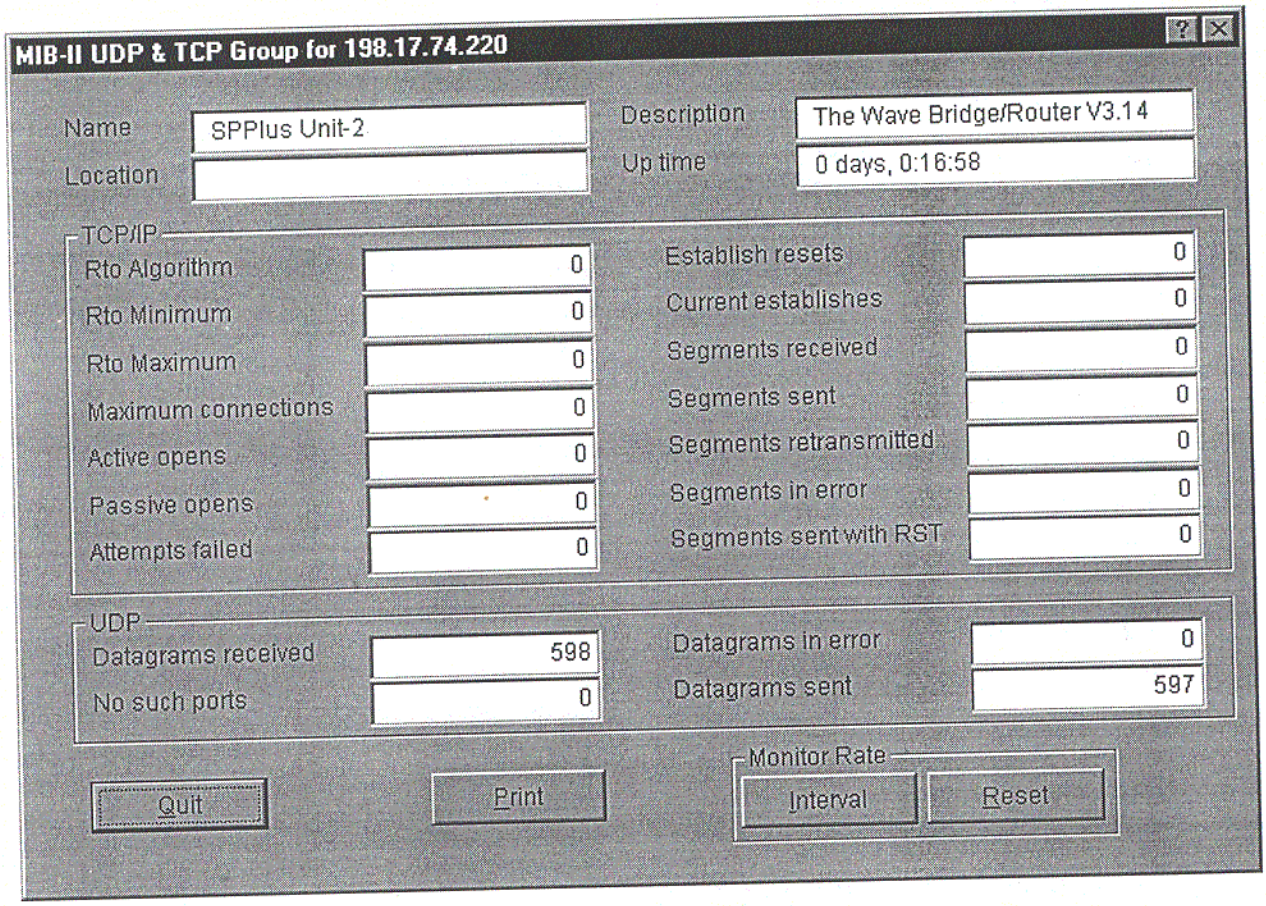
Fragment failures - The number of IP-datagram fragments that have been discarded because they needed to be fragmented at this entity but could not be because the datagram's "don't fragment" flag was set.

Fragments created - The number of IP-datagram fragments that have been generated as a result of fragmentation at this entity.

Datagrams forwarded - The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP gateways, this counter will include only those packets which were Source-Routed via this entity, and for which Source-Route option processing was successful.

Routing discards - The number of routing entries which were chosen to be discarded even though they were valid. One possible reason for discarding such an entry could be to free up buffer space for other routing.

IP/TCP/UDP Monitor



TCP

Rto Algorithm - The algorithm used to determine the timeout value used for retransmitting unacknowledged octets, which can be: "other" - none of the following; "constant" - a constant rto; "rsre" - MIL-STD-1778, Appendix B; "vanj" - Van Jacobson's algorithm.

Rto Minimum - The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is "rsre", an object of this type has the semantics of the LBOUND quality described in RFC 793.

Rto Maximum - The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre, an object of this type has the semantics of the LBOUND quality described in RFC 793.

Maximum connections - The limit on the total number of TCP connections the entity can support. In entities where the maximum number of connections is dynamic, this object should contain the value -1.

Active opens - The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.

Passive opens - The number of times TCP connections have made a direct transition to SYN-SENT state from the LISTEN state.

Attempts failed - The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.

Establish resets - The number of times TCP connections have made a direct transition to the closed state from either the ESTABLISHED state or the CLOSE-WAIT state.

Current establishes - The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.

Segments received - The total number of segments received, including those received in error. This count includes segments received on currently established connections.

Segments sent - The total number of segments sent, including those on current connections but excluding those containing only retransmission octets.

Segments retransmitted - The total number of segments retransmitted -- that is, the number of TCP segments transmitted containing one or more previously transmitted octets.

Segments in error - The total number of segments received in error (i.e., with bad TCP checksums).

Segment sent with RST - The number of TCP segments sent containing the RST flag.

UDP

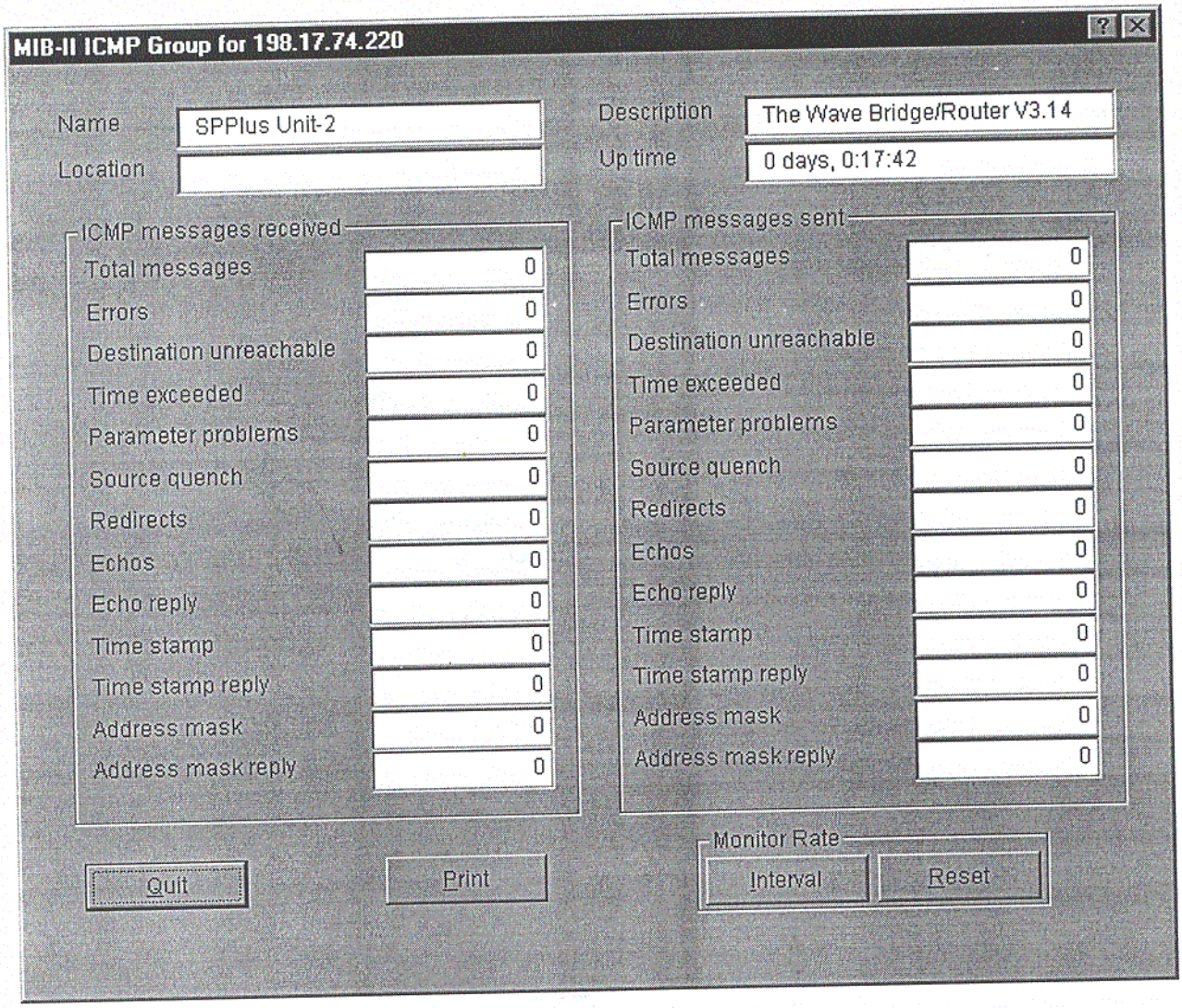
Datagrams received - The total number of UDP datagrams delivered to UDP users.

No such port - The total number of received UDP datagrams for which there was no application at the destination port.

Datagrams in error - The number of received UDP datagrams that could not be delivered for a reason other than the lack of an application at the destination port.

Datagrams sent - The total number of UDP datagrams sent from this entity.

ICMP Monitor



ICMP Messages Received

Total messages - The total number of ICMP messages which the entity received. Note that this counter includes all those counted by received **Errors**.

Errors - The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad checksums, bad length, etc).

Destination unreachable - The number of ICMP Destination Unreachable messages received.

Time exceeded - The number of ICMP Time Exceeded messages received.

Parameter problems - The number of ICMP Parameter Problem messages received.

Source quench - The number of ICMP Source Quench messages received.

Redirects - The number of ICMP Redirect messages received.

Echoes - The number of ICMP Echo (request) messages received.

Echo reply - The number of ICMP Echo Reply messages received.

Time stamp - The number of ICMP Timestamp (request) messages received.

Time stamp reply - The number of ICMP Timestamp Reply messages received.

Address mask - The number of ICMP Address Mask (request) messages received.

Address mask reply - The number of ICMP Address Mask Reply messages received.

ICMP Messages Sent

Total messages - The total number of ICMP messages which this entity attempted to send. Note that this counter includes all those counted by ICMP out **Errors.**

Errors - The number of ICMP messages which this entity did not send due to problems discovered within ICMP, such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of errors which contribute to this counter's value.

Destination Unreachable - The number of ICMP Destination Unreachable messages sent.

Time exceeded - The number of ICMP Time exceeded messages sent.

Parameter problems - The number of ICMP Parameter Problem messages sent.

Source quench - The number of ICMP Source Quench messages sent.

Redirects - The number of ICMP Redirect messages sent.

Echoes - The number of ICMP Echo (request) messages sent.

Echo Reply - The number of ICMP Echo Reply messages sent.

Time Stamp - The number of ICMP Time Stamp (request) messages sent.

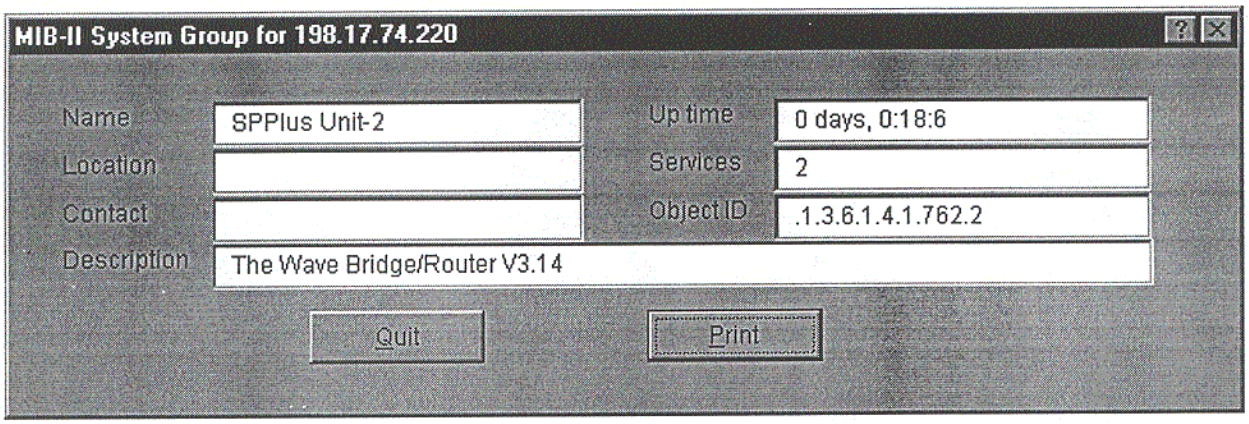
Time Stamp Reply - The number of ICMP Time Stamp Reply messages sent.

Address mask - The number of ICMP Address Mask (request) messages sent.

Address mask reply - The number of ICMP Address Mask Reply messages sent.

TABLES

System Information



The brouter keeps the standard SNMP MIB II statistics on system-related information as follows:

Name - An administratively-assigned name for this managed node. By convention, this is the node's fully-qualified domain name.

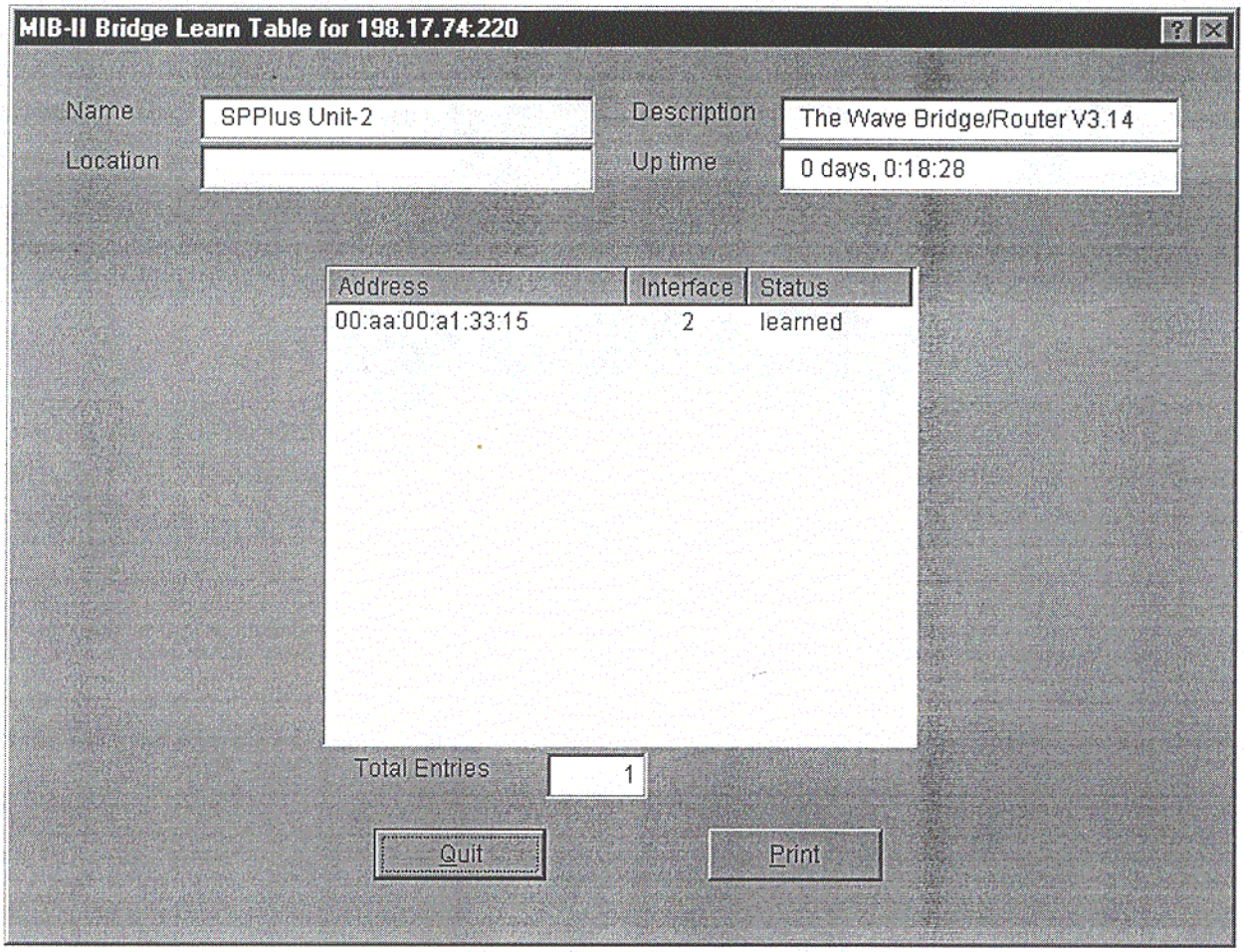
Location - The physical location of this node (e.g., 'telephone closet, 3rd').

Contact - The name/position of the contact person for this managed node, together with information on how to contact this person.

Up time - The time since the network-management portion of the system was last re-initialized.

Description - This value contains the full name and version identification of the system's hardware type, software operating system, and network software.

Bridge Learn Table



This table contains information about unicast entries for which the brouter has forwarding and/or filtering information. This information is used by the transparent bridging function to determine how to propagate a received frame.

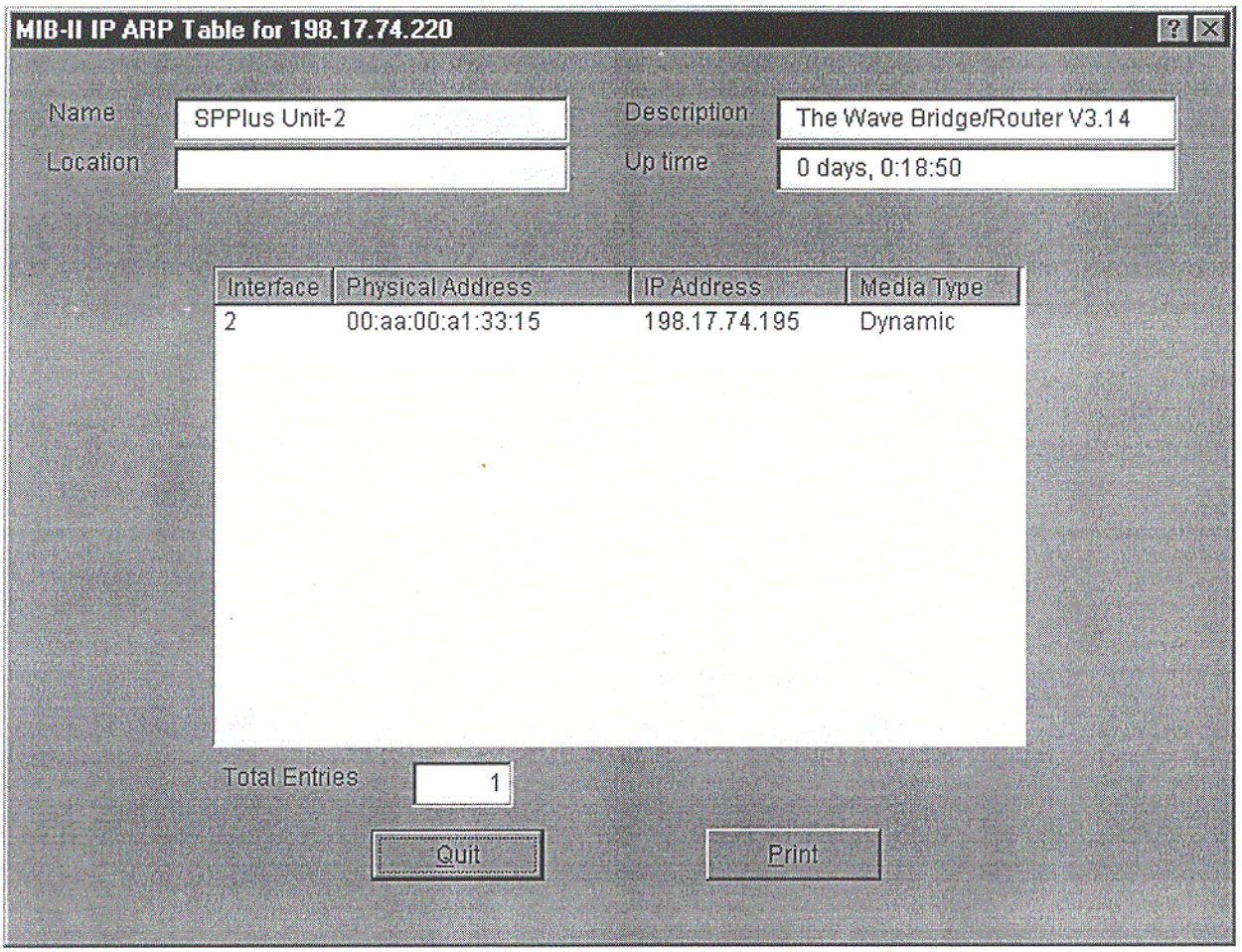
Address - A unicast MAC address for which the brouter has forwarding and/or filtering information.

Interface - Either the value 0 (zero), or the interface number on which a frame has been seen. A value of 0 (zero) indicates that the interface number has not been learned but the the brouter does have some forwarding/ filtering information about this address.

Status - The status of this entry. The meanings of the values are:

other	-	None of the following.
invalid	-	This entry is no longer valid, but has not been flushed from the table yet.
learned	-	This entry was learned, and is being used.
self	-	This entry represents one of the brouter's addresses. The interface value indicates which of the brouter's interfaces has this address.
mgmt	-	This entry is also the value of an existing instance in the static table.

IP ARP Table



The IP ARP Table contains the IP-Address-to-'physical'-(MAC)-Address equivalences.

Interface - The interface on which this entry is effective.

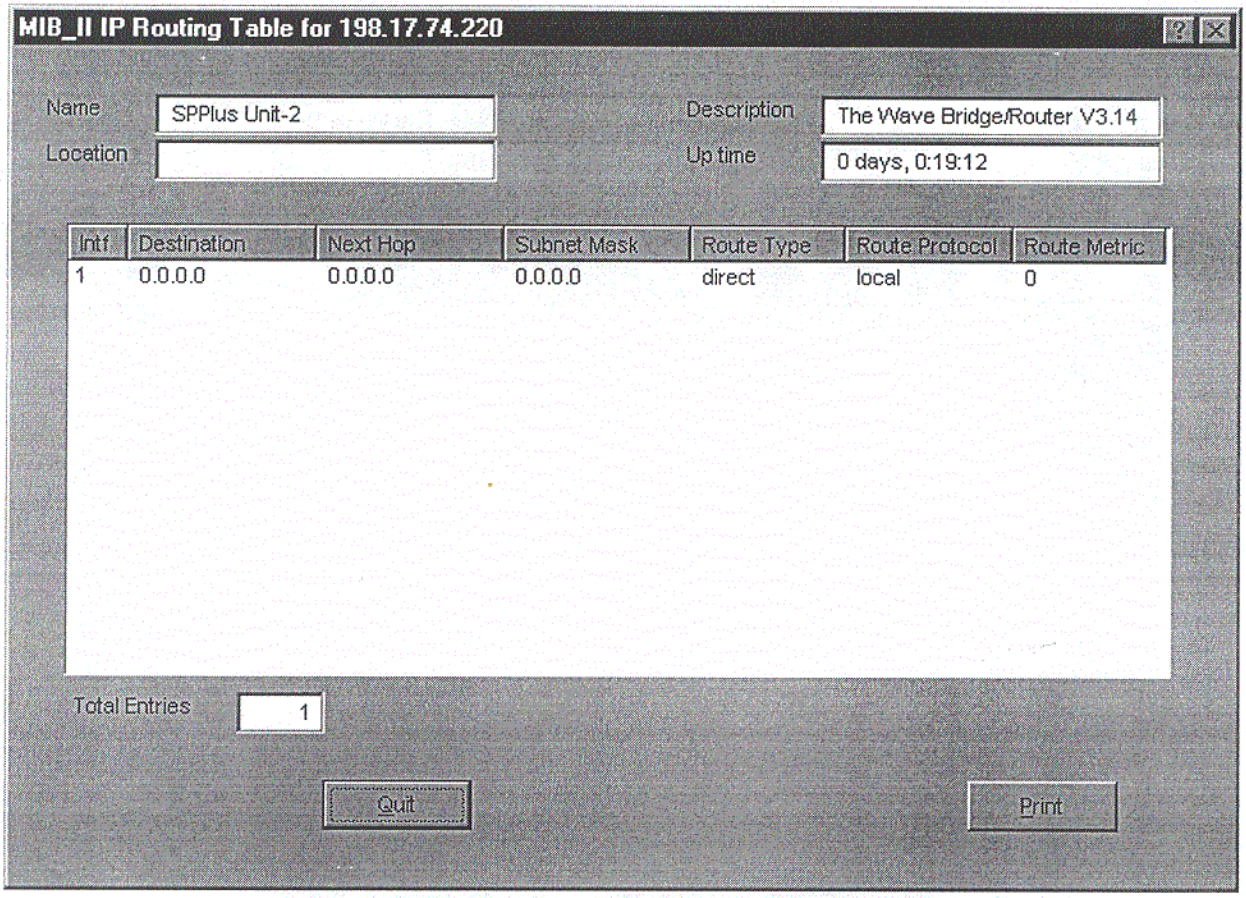
Physical Address - The media-dependent 'physical' (MAC) address. An example would be the MAC address of the Ethernet interface.

IP Address - The IP address corresponding to the media-dependent 'physical' (MAC) address.

Media Type - The type of mapping:

other - none of the following
invalid - an invalidated mapping
dynamic - a mapping that can change with circumstances
static - a mapping which does not change

IP Route Table



The brouter keeps the standard SNMP MIB II statistics on the IP routing table, which contains an entry for each route presently known.

Intf - The local interface through which the next hop of this route should be reached.

Destination - The destination IP address of this route. An entry with a value of 0.0.0.0 is considered a default route. Multiple routes assigned to a single destination can appear in the table, but access to such multiple entries is dependent on the table-access mechanisms defined by the network-management protocol in use.

Next Hop - The IP address of the next hop of this route.

Subnet Mask - Indicates the mask to be a logical-ANDed with the destination address before being compared to the value in the **Destination** field. For systems that do not support arbitrary subnet masks, an agent constructs the value of the **Subnet Mask** by determining whether the value of the correspondent **Destination** field belongs to a Class A, B, or C network.

Route Type - Type of route. This can be:

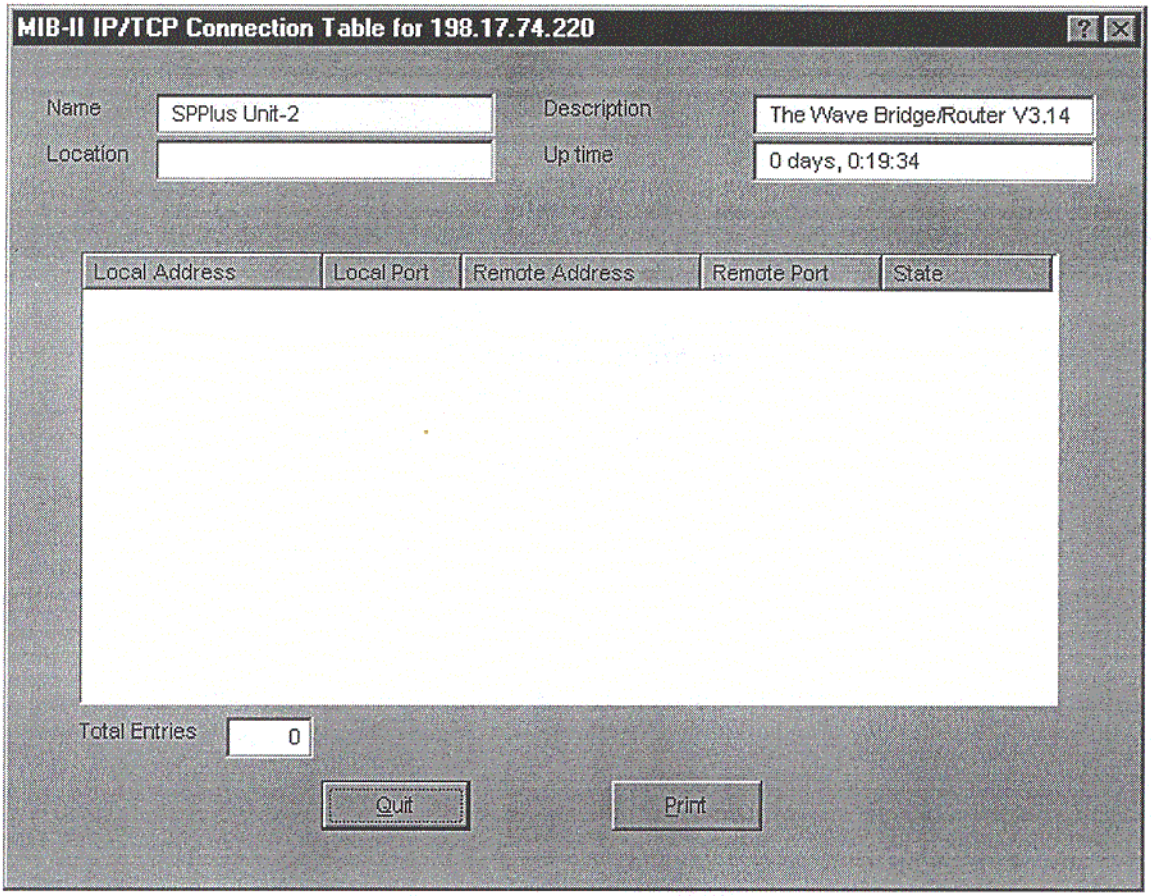
other	-	none of the following
invalid	-	an invalidated route
direct	-	route to directly connected (sub-)network
indirect	-	route to a non-local host/network/subnetwork.

Route Protocol - The routing mechanism by which this route was learned. Inclusion of values for gateway-routing protocols is not intended to imply that hosts should support those protocols. The values are as follows:

other	-	none of the following
local	-	non-protocol information
netmgmt	-	entries set via a network-management protocol
icmp	-	obtained via ICMP (e.g., ICMP 'redirect')
egp	-	all gateway-routing protocols
ggp	-	all gateway-routing protocols

Route Metric - The primary routing metric for this route. The semantics of this metric are determined by the routing protocol specified in the route's **Route Protocol** value. If this metric is not used, its value should be set to -1.

IP/TCP Connection Table



This table reports the states of the TCP connections and contains the following fields:

Local Address - The local IP address for this TCP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.

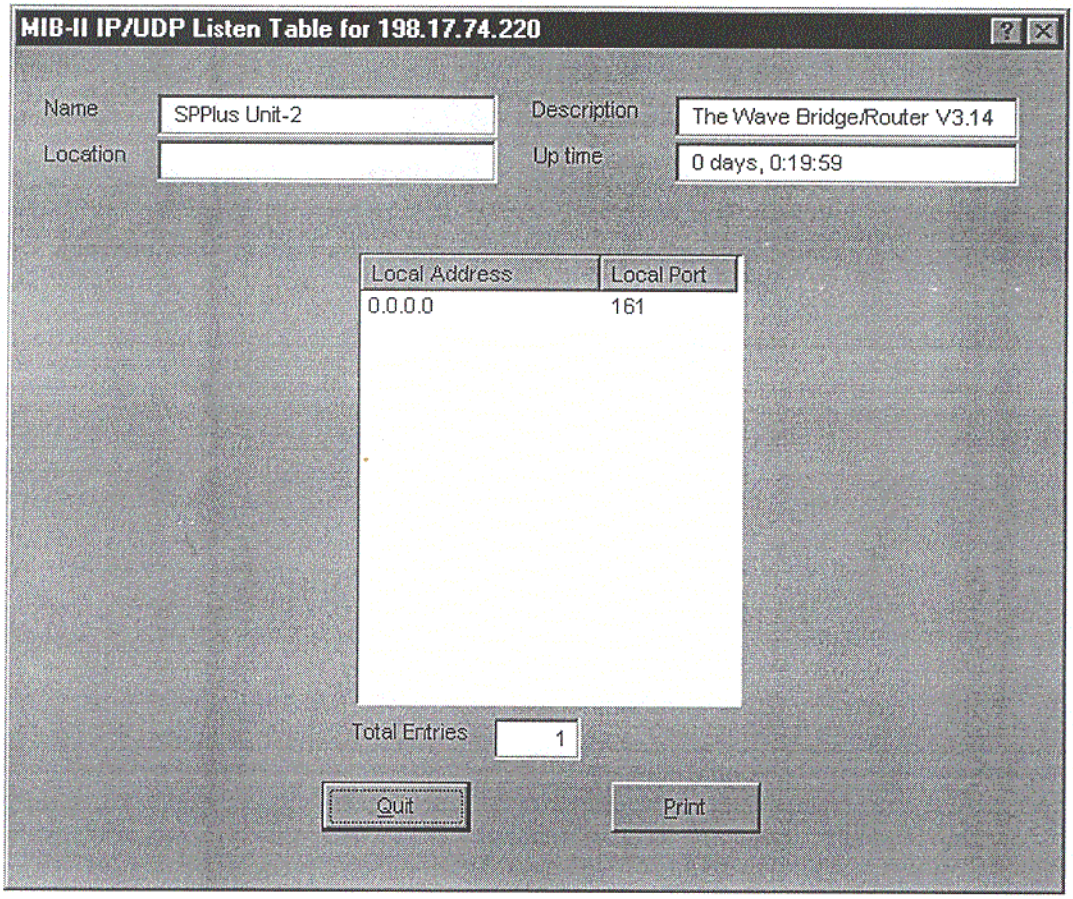
Local Port - The local port number for this TCP connection.

Remote Address - The remote IP address for this TCP connection.

Remote Port - The remote port number for this IP connection.

State - The state of this TCP connection, which can be one of the following: closed, listen, synSent, synReceived, established, finWait1, finWait2, closeWait, LastAck, closing, timeWait, deleteTCB.

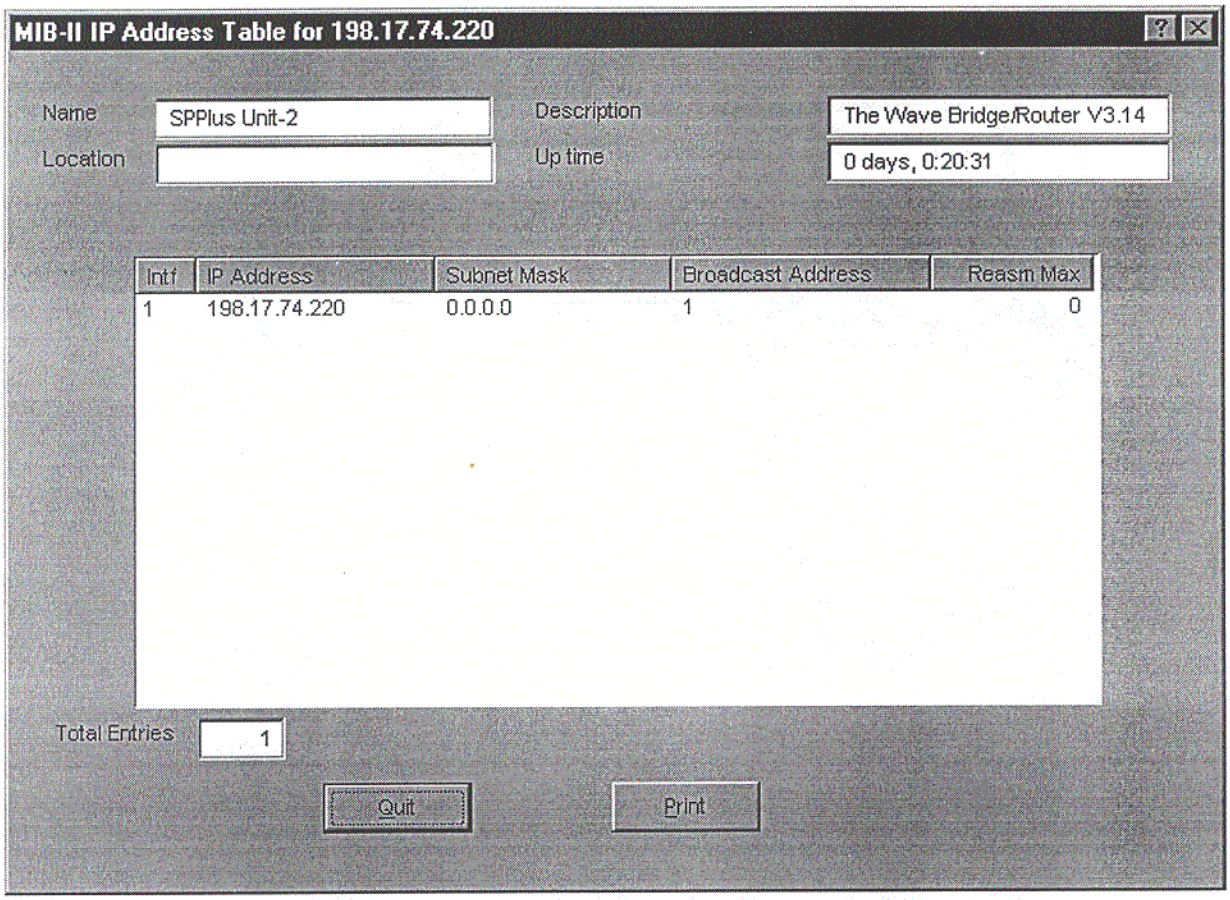
IP/UDP Listener Table



Local Port - The local port number for this UDP connection.

Local Address - The local IP address for this UDP connection. In the case of a connection in the listen state which is willing to accept connections for any IP interface associated with the node, the value 0.0.0.0 is used.

Local IP-Address Table



The table of addressing information relevant the this entity's IP addresses.

Intf - The interface to which the entry is applicable.

IP Address - The IP address to which this entry's addressing information pertains.

Subnet Mask - The subnet mask associated with the IP address of this entity. The value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0.

Broadcast Address - The value of the least-significant bit in the IP broadcast address used for sending datagrams on the logical interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value will be 1. This value applies to both the subnet- and network-broadcast address used by the entity on this logical interface.

Reasm Max - The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

APPENDIX

COMMON ETHERNET PROTOCOLS

This table contains the protocols that can be specified in SPEEDLAN's "Ethernet Protocol Menu".

* 0600	Xerox NS IDP
0601	XNS Address Translation (3Mb only)
* 0800	DOD Internet Protocol (IP)
0801	X.75 Internet
0802	NBS Internet
0803	ECMA Internet
* 0804	CHAOSnet
0805	X.25 Level 3
* 0806	Address Resolution Protocol (ARP) (for IP and for CHAOS)
0807	XNS Compatibility
081C	Symbolics Private
0888-088A	Xyplex
0900	Ungermann-Bass network debugger
0A00	Xerox IEEE802.3 PUP
0A01	Xerox IEEE802.3 PUP Address Translation
* 0BAD	Banyan Systems
0BAF	Banyan VINES Echo
1000	Berkeley Trailer negotiation
1001-100F	Berkeley Trailer encapsulation for IP
1234	DCA - Multicast
* 1600	VALID system protocol
1989	Artificial Horizons Aviator dogfight simulator on Sun
3C00	3Com NBP virtual circuit datagram (like XNS SPP) not registered
3C01	3Com NBP System control datagram not registered
3C02	3Com NBP Connect request (virtual cct) not registered
3C03	3Com NBP Connect response not registered
3C04	3Com NBP Connect complete not registered
3C05	3Com NBP Close request (virtual circuit) not registered
3C06	3Com NBP Close response not registered
3C07	3Com NBP Datagram (like XNS IDP) not registered
3C08	3Com NBP Datagram broadcast not registered
3C09	3Com NBP Claim NetBIOS name not registered
3C0A	3Com NBP Delete NetBIOS name not registered
3C0B	3Com NBP Remote adapter status request not registered
3C0C	3Com NBP Remote adapter response not registered
3C0D	3Com NBP Reset not registered
4242	PCS Basic Block Protocol
4321	THD - Diddle
6000	DEC unassigned, experimental
6001	DEC MOP Dump/Load Assistance
6002	DEC MOP Remote Console
6003	DECnet Phase IV, DNA Routing
6004	DEC Local Area Transport (LAT)
6005	DEC diagnostic protocol (at interface initialization?)
6006	DEC customer protocol
6007	DEC Local Area VAX Cluster (LAVC SCA)
6008 & 6009	DEC unassigned