IEN - 197

A Host Monitoring Protocol

Benjamin M. Littauer
Andrew J. Huang
Robert M. Hinden

Bolt Beranek and Newman Inc.

September 1981

Table of Contents

1 Introduction..... 1
2 Protocol Operation..... 2
2.1 Unsolicited Messages..... 3
2.2 Status Messages..... 4
2.3 Statistics Messages..... 4
3 Header Formats..... 6
3.1 IP Headers..... 6
3.2 Monitor Header..... 7
4 Monitor Message Formats..... 9
4.1 System Type 1: General Messages..... 9
4.1.1 Message Type 1: Polling Message..... 9
4.1.2 Message Type 2: Error in Poll..... 11
4.2 System Type 2: IMP..... 13
4.2.1 Message Type 1: IMP Trap..... 13
4.2.2 Message Type 2: IMP status..... 16
4.2.3 Message Type 3: IMP Modem Throughput..... 20
4.2.4 Message Type 4: IMP Host Throughput..... 23
4.3 System Type 3: TAC..... 26
4.3.1 Message Type 1: TAC Trap Message..... 26
4.3.2 Message Type 2: TAC Status..... 29
4.3.3 Message Type 3: TAC Throughput..... 32

A Host Monitoring Protocol

1 Introduction

The Host Monitoring Protocol (HMP) is used to collect information from hosts in various networks. At present the protocol aims at collecting information from ARPANET IMPs and TACs in an internet environment. It is designed to be extensible to other monitoring functions (e.g. hosts, gateways, local nets) while its addressing and control structures allow it to operate as well within a single network. In implementation it is a portion of a larger system, the Network Operations Center (NOC).

The monitoring algorithm relies on polling for messages; the Host Monitor (HM) periodically sends a polling message to the host being monitored, requesting a specified report. The host then creates the report and sends it to the HM. Missing reports are detected as unanswered polls and duplicate polls are sent to have the report retransmitted. Some messages cannot be polled for and these are sent to the HM spontaneously. Checksums calculated on the data portions of all messages assure their integrity.

The HMP implements a password scheme in order to restrict access to monitoring information. The monitored hosts check each

poll message for a valid password before responding; this helps prevent unauthorized use of the monitor system. The HMP is not intended to be a highly secure protocol.

2 Protocol Operation

The HMP is designed to operate reliably in the internet environment. To gain this measure of reliability it uses polling. The HM sends polling messages requesting reports to the monitored hosts. A host, upon receiving the poll, verifies the message and, if it is acceptable, sends the appropriate report to the poll source. The HM, after transmitting the poll, awaits the corresponding report. If it is not received within a reasonable interval, another poll is sent assuming that either the previous poll or the answering report was lost. If after a number of repeated polls no response has been received, it can be reasonably concluded that the host is unreachable and the polling frequency is reduced to a background level. This minimizes traffic but, since polling continues, a poll will reach the host once it becomes reachable. When a report is received the normal poll frequency is resumed.

The most important reason for choosing polling over other methods of detecting lost messages is that it centralizes control

of monitoring in a dedicated HM, rather distributing it throughout the network of monitored hosts. This frees resources in the monitored systems and also allows the HM to regulate the flow of monitoring messages to prevent overloading of the HM's resources.

There are three classes of data with which the monitoring protocol is concerned. These are (1) reports of unexpected changes of status or error conditions, (2) reports of the current state of the host, and (3) reports of statistics and throughput data. These three kinds of data are handled in different ways by the HMP as described below.

2.1 Unsolicited Messages

These are reports of unexpected changes of status or error condition reports (traps) which the monitor should be informed of as they occur. They are not polled, but are instead sent directly to a particular HM. If the address of the HM must be changed for unsolicited messages, it will be done by external means (e.g. packet core protocol).

2.2 Status Messages

These are reports of the current state of a system; they contain any kind of information which is not cumulative. The HM will poll for these on a periodic basis. When a monitored host receives a poll for a status message, it assembles a message with the current data pertaining to its status. Since this is an instantaneous "picture" of a system, it is not critical if any particular status report is lost.

2.3 Statistics Messages

These messages, also called throughput messages, contain data collected on a periodic basis. The information will be collected in a monitored machine using a double buffering system. At the end of each collection period, a message will be assembled and the counters will be cleared. During the next collection period, any HMs polling for a statistics message will be sent this message.

The collection frequency for statistics messages from a particular host must be relatively long compared to the average round trip message time between the HM and that host to allow the HM to re-poll if it does not receive an answer. With this restriction it should be possible to avoid missing any statistics messages in most cases. Each statistics message will contain a

field giving the (local) time when the data was collected, and the time at which the message was sent (*). This will allow the HM to schedule its polling so that the poll arrives near the beginning of each collection period. This is done to ensure that if a message is lost, the HM will have sufficient time to try again to get the statistics message for that period. Sequence numbers will be used to detect the loss of a message for a period, and also to eliminate duplicate messages.

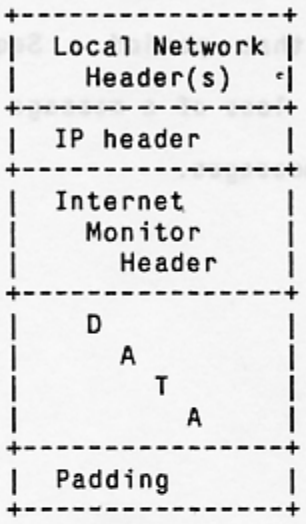
---

* The units of the local time should be large enough to guarantee a rollover time of at least one hour.

3 Header Formats

[Note: Any field labeled "unused" is reserved for later extensions and must be zero when sent.]

Monitor messages have the following format:



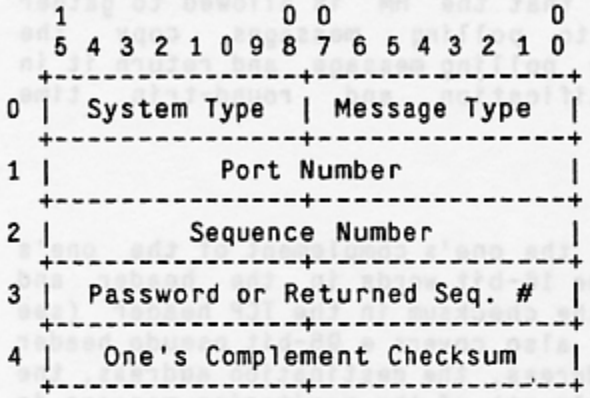
The local header(s) depend on the local network, and do not concern us here.

3.1 IP Headers

HMP messages are sent using the version 4 IP header as described in IEN-128 (RFC-760). The HMP protocol number is 20 (decimal). The time to live field should be set to the maximum value. All other fields should be set as specified in IEN-128.

3.2 Monitor Header

The monitor header format is:



HMP FIELDS:

System Type
Message Type

The combination of system type and message type determines the format of the data in the monitoring message.

The system types which have been defined are:

System Type	Meaning
1	General Messages
2	IMP
3	TAC

Message types are defined for each system type according to the needs of that system. Message types and their formats for each system are defined below.

Port Number

The Port Number field is presently unused. It can be used to multiplex similar messages from/to different processes in one host.

Sequence Number

Every message contains a sequence number. The sequence number is incremented when each new message of that type is sent.

Password or Returned Sequence Number

The Password field of a polling message from an HM contains a password to verify that the HM is allowed to gather information. Responses to polling messages copy the Sequence Number from the polling message and return it in this field for identification and round-trip time calculations.

Checksum

The Checksum field is the one's complement of the one's complement sum of all the 16-bit words in the header and data area. As with the checksum in the TCP header (see IEN-129), the checksum also covers a 96-bit pseudo header containing the source address, the destination address, the protocol (20), and the length of the monitoring message in bytes. The fields of the pseudo header are as defined for the IP header.

4 Monitor Message Formats

4.1 System Type 1: General Messages

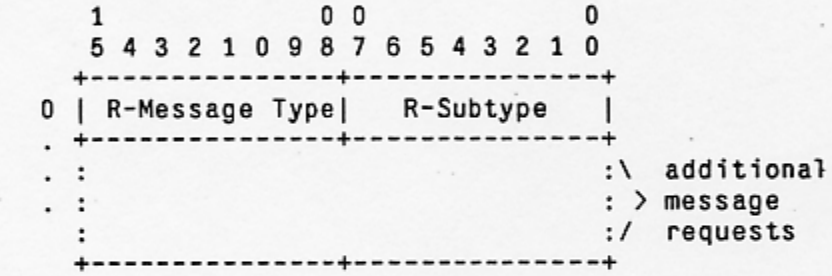
4.1.1 Message Type 1: Polling Message

Description

The HM will send polls to the machines it is monitoring according to its polling algorithm. Multiple requests can be combined in a single message, but each request is still considered a separate poll.

The polled machine will return a message of each type requested; it will only answer a poll with the correct system type and password. It will return an error message (System Type 1; Message Type 2) if it receives a poll for the wrong system type or an unsupported message type.

A polling message has the following form:



HMP FIELDS

System Type

General Messages = 1

Message Type

Polling Message = 1

Port Number

Unused

Sequence Number

The sequence number identifies the polling request. An HM will have separate sequences for each host it monitors. The sequence number is returned in the response to a poll; the

HM will use this information to associate polls with their responses and to determine round trip times.

Password

The monitoring password.

POLL FIELDS

R-Message Type

The message type requested.

R-Subtype

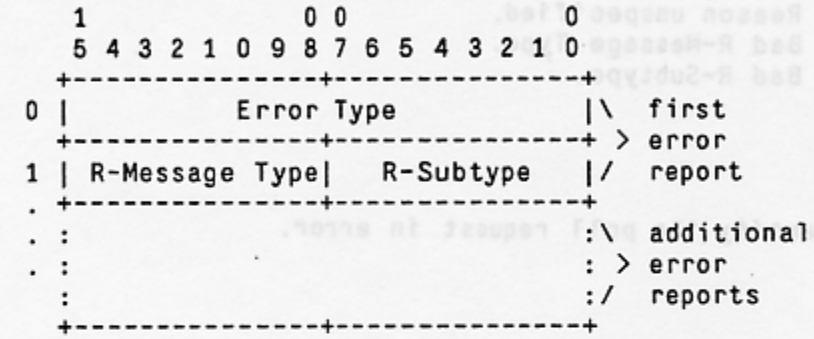
Presently unused, this field might later be used to specify options or include additional data in a polling message.

4.1.2 Message Type 2: Error in Poll

Description

This message is sent in response to a faulty poll and specifies the nature of the error.

An error message has the following form:



HMP FIELDS

System Type

General Messages = 1

Message Type

Error Message = 2

Port Number

Unused

Sequence Number

A 16 bit number incremented each time an error message is sent.

Returned Sequence Number

The Sequence Number of the polling message which caused the error.

ERROR MESSAGE FIELDS

Error Type

This field specifies the nature of the error in the poll. The following error types have been defined.

1 = Reason unspecified.
2 = Bad R-Message Type.
3 = Bad R-Subtype.

R-Message Type
R-Subtype

These fields identify the poll request in error.

4.2 System Type 2: IMP

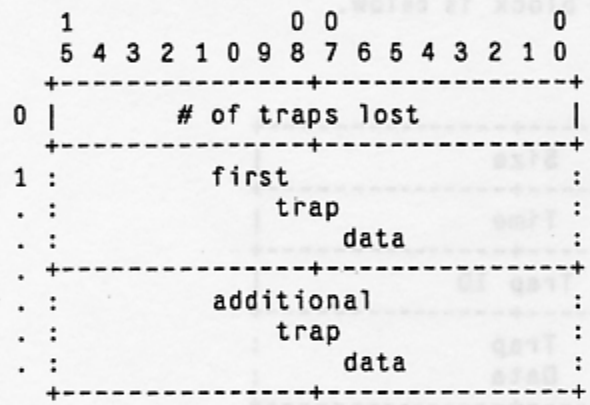
4.2.1 Message Type 1: IMP Trap

Description

When a trap occurs, it is buffered in the IMP and sent as soon as possible. Trap messages are unsolicited. If traps happen in close sequence, several traps may be sent in one message.

Through the use of sequence numbers, it will be possible to determine how many traps are being lost. If it is discovered that many are lost, a polling scheme might be implemented for traps.

A IMP trap message has the following form:



HMP Fields

System Type

IMP = 2

Message Type

IMP Trap Message = 1

Port Number

Unused

Password

Unused

Sequence Number

A 16 bit number incremented each time a trap message is sent so that the HM can order the received trap messages and detect missed messages.

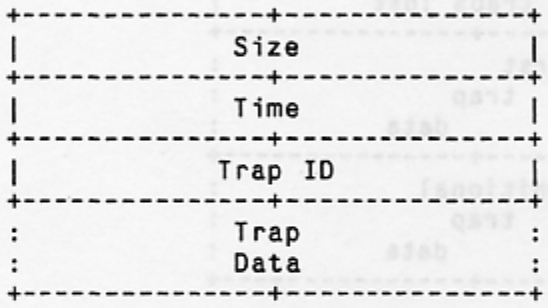
IMP TRAP FIELDS

# of traps lost

Under certain conditions, an IMP may overflow its internal trap buffers and be unable to save traps to send. This counter keeps track of such occurrences.

Trap Reports

There can be several blocks of trap data in each message. The format for each such block is below.



Size

Size is the number of 16 bit words in the trap, not counting the size field.

Time

The time (in 640 ms. units) at which the trap occurred. This field is used to sequence the traps in a message and associate groups of traps.

Trap ID

This is usually the program counter at the trap. The ID identifies the trap, and does not have to be a program counter, provided it uniquely identifies the trap.

Trap Data

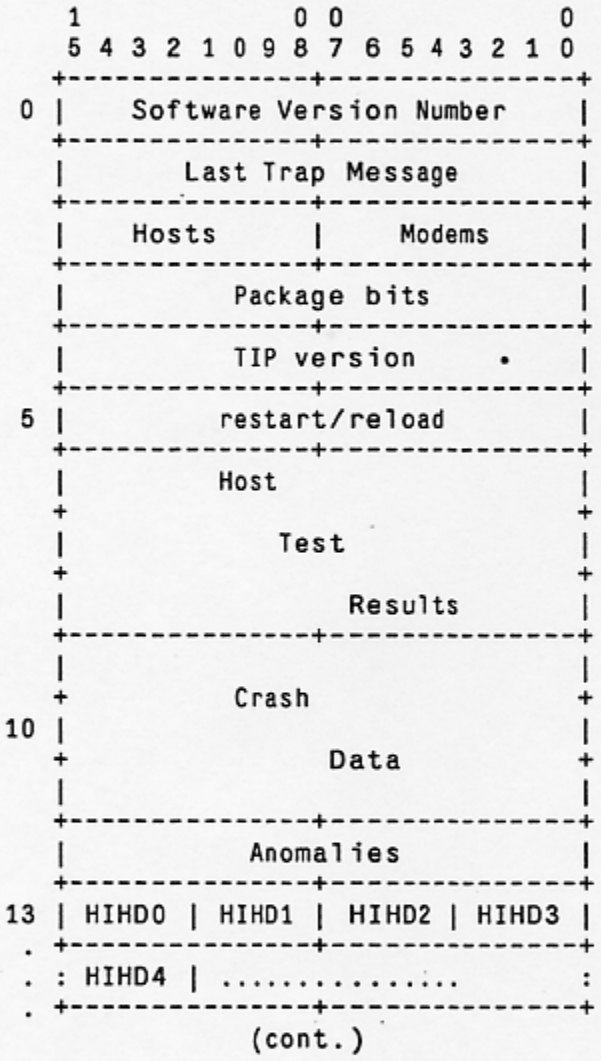
The IMP returns data giving more information about the trap. There are usually two entries: the values in the accumulator and the index register at the occurrence of the trap.

4.2.2 Message Type 2: IMP status

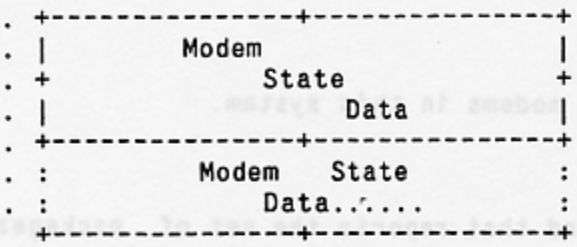
Description

The status message gives a quick summary of the state of the IMP. Status of the most important features of the IMP are reported as well as the current configuration of the machine.

The format of the status message is as follows:



Imp Status (cont.)



HMP FIELDS

System Type

IMP = 2

Message Type

IMP status message = 2

Port Number

Unused

Sequence Number

A 16 bit number incremented each time a status message is sent.

Password

The password contains the sequence number of the polling message to which this message responds.

IMP STATUS FIELDS

Software Version Number

The IMP version number.

Last Trap Message

Contains the sequence number of the last trap message sent to the HM. This will allow the HM to detect how many trap messages are being lost.

Hosts

The number of configured hosts in this system.

Modems

The number of configured modems in this system.

Package Bits

This is a bit encoded word that reports the set of packages currently loaded in the system. The table below defines the bits.

Bit (octal)	Package
1	VDH
2	TIP
4	experimental
10	Cumulative Statistics
20	Trace
40	TTY
100	DDT
200	Store and Forward statistics
400	End-to-end Statistics
1000	Level measurements

TIP version

The TIP version number if a TIP is loaded or zero if not.

Restart/Reload

This word reports a restart or reload of an IMP.

Value	Meaning
1	restarted
2	reloaded

Host Test Results

These three words report the result of the host test, if any. If a test is running, the first word will contain the host number, the second and third will contain the number of NOPs sent and received, respectively. If no test is running, the first word will contain a -1.

Crash Data

Crash data reports the circumstances surrounding an

unexpected crash. The first word reports the location of the crash and the following two are the contents of the accumulator and index registers.

Anomalies

Anomalies is a collection of bit flags that indicate the state of various switches or processes in the IMP. These are very machine dependent and only a representative sampling of bits is listed below.

Bit (octal)	Meaning
1	Sense Switch 1 ON
2	Sense Switch 2 ON
4	Sense Switch 3 ON
10	Sense Switch 4 ON
20	Override ON
200	Trace ON
2000	Message Generator ON

HIHD0 - HIHDn

Each four bit HIHD field gives the state of the corresponding host.

Value	Meaning
0	UP
1	ready line down
2	tardy
3	non-existent
4	VDH host not initialized

Modem State Data

Modem state data contains four byte fields of data. The first field indicates the line speed in a machine dependent fashion; the second field is the number of line protocol ticks covered by this report; the third is the neighbor on the line, and the fourth is a count of missed protocol packets over the interval specified in the second field.

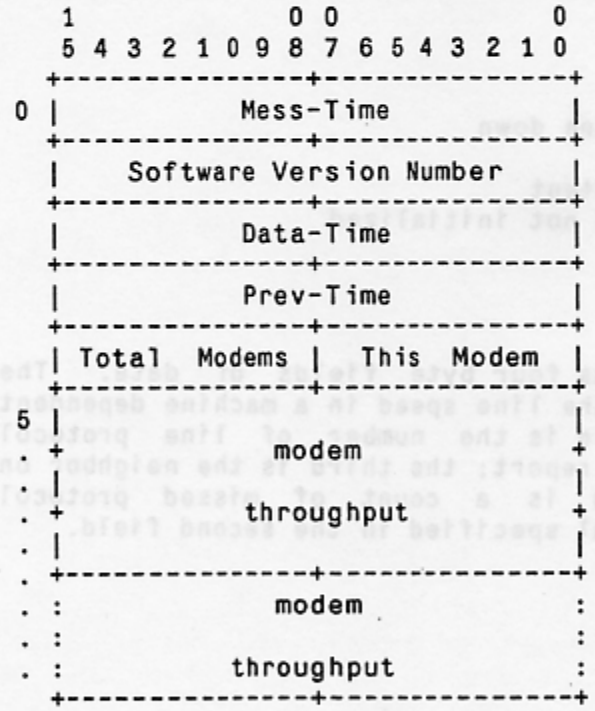
4.2.3 Message Type 3: IMP Modem Throughput

Description

The modem throughput message reports traffic statistics for each modem in the system. The IMP will collect these data at regular intervals and save them awaiting a poll from the HM. If a period is missed by the HM, the new results simply overwrite the old. Two time stamps bracket the collection interval (data-time and prev-time) and are an indicator of missed reports. In addition, mess-time indicates the time at which the message was sent.

The modem throughput message will accommodate up to fourteen modems in one packet. A provision is made to split this into multiple packets by including a modem number for the first entry in the packet. This field is not immediately useful, but if machine sizes grow beyond fourteen modems or if modem statistics become more detailed and use more than three words per modem, this can be used to keep the message within a single ARPANET packet.

The format of the modem throughput message is as follows:



HMP FIELDS

System Type

IMP = 2

Message Type

IMP Modem Throughput message = 3

Port Number

Unused

Sequence Number

A 16 bit number incremented at each collection interval (i.e. when a new throughput message is assembled). The HM will be able to detect lost or duplicate messages by checking the sequence numbers.

Password

The password contains the sequence number of the polling message to which this message responds.

IMP MODEM THROUGHPUT FIELDS

Mess-time

The time (in 640ms. units) at which the message was sent to the HM.

Software Version Number

The IMP version number.

Data-Time

Data-time is the time (in 640ms. units) when this set of data was collected. (See Description.)

Prev-Time

Prev-time is the time (in 640 ms. units) of the previous collection of data (and therefore, is the time when the data in this message began accumulating.)

Total Modems

This is the number of modems in the system.

This Modem

This Modem is the number of the first modem reported in this message. Large systems that are unable to fit all their modem reports into a single packet may use this field to separate their message into smaller chunks to take advantage of single packet message efficiencies.

Modem Throughput

Modem throughput consists of three words of data reporting packets and words output on each modem. The first word counts packets output and the following two count word throughput. The double precision words are arranged high order first. (Note also that messages from Honeywell type machines (316s, 516s and C30s) use a fifteen bit low order word.) The first block reports output on the modem specified by "This Modem". The following blocks report on consecutive modems.

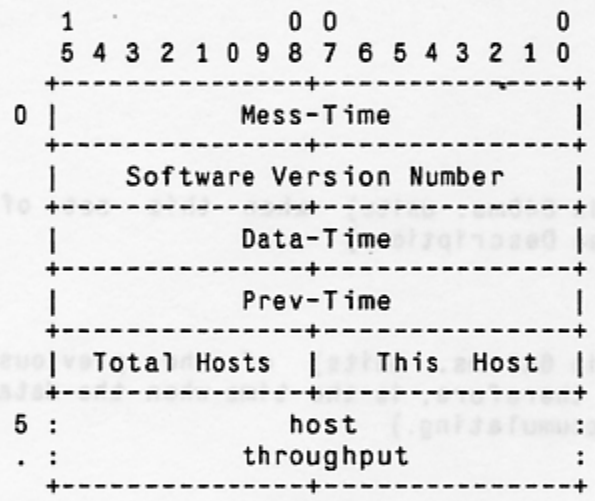
4.2.4 Message Type 4: IMP Host Throughput

Description

The host throughput message reports traffic statistics for each host in the system. The IMP will collect these data at regular intervals and save them awaiting a poll from the HM. If a period is missed by the HM, the new results simply overwrite the old. Two time stamps bracket the collection interval (data-time and prev-time) and are an indicator of missed reports. In addition, mess-time indicates the time at which the message was sent.

The host throughput format will hold only three hosts if packet boundaries are to be respected. A provision is made to split this into multiple packets by including a host number for the first entry in the packet.

The format of the host throughput message is as follows:



HMP FIELDS

System Type

IMP = 2

Message Type

IMP host Throughput message = 4

Port Number

Unused

Sequence Number

A 16 bit number incremented at each collection interval (i.e. when a new throughput message is assembled). The HM will be able to detect lost or duplicate messages by checking the sequence numbers.

Password

The password contains the sequence number of the polling message to which this message responds.

IMP HOST THROUGHPUT FIELDS

Mess-time

The time (in 640ms. units) at which the message was sent to the HM.

Software Version Number

The IMP version number.

Data-Time

Data-time is the time (in 640ms. units) when this set of data was collected. (See Description.)

Prev-Time

Prev-time is the time (in 640 ms. units) of the previous collection of data (and therefore, is the time when the data in this message began accumulating.)

Total Hosts

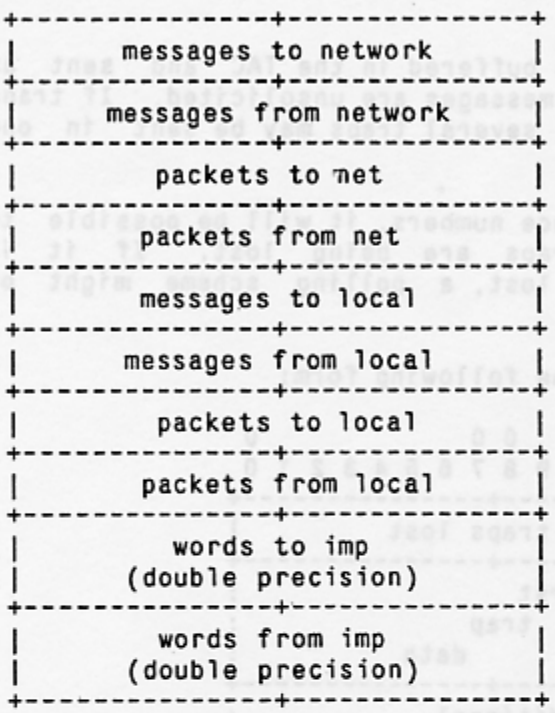
The total number of hosts in this system.

This Host

This host is the number of the first host reported in this message. Large systems that are unable to fit all their host reports into a single packet may use this field to separate their message into smaller chunks to take advantage of single packet message efficiencies.

Host Throughput

Each host throughput block consists of twelve words in the following format:



Each host throughput message will contain several blocks of data. The first block will contain data for the host specified in First Host Number. Following blocks will contain data for consecutive hosts. All counters are single precision with the exception of the two word counters which are double precision. The double precision words are arranged high order first. Note also that messages from Honeywell type machines (316s, 516s and C30s) use a fifteen bit low order word.

4.3 System Type 3: TAC

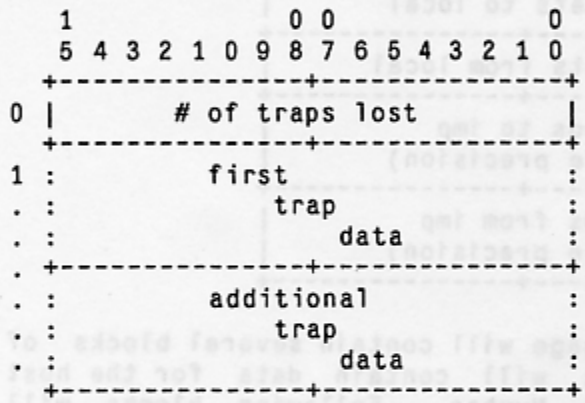
4.3.1 Message Type 1: TAC Trap Message

Description

When a trap occurs, it is buffered in the TAC and sent as soon as possible. Trap messages are unsolicited. If traps happen in close sequence, several traps may be sent in one message.

Through the use of sequence numbers, it will be possible to determine how many traps are being lost. If it is discovered that many are lost, a polling scheme might be implemented for traps.

A TAC trap message has the following form:



HMP FIELDS

System Type

TAC = 3

Message Type

TAC Trap Message = 1

Port Number

Unused

Password or Returned Sequence Number

Unused

Sequence Number

A 16 bit number incremented each time a trap message is sent so that the HM can order the received trap messages and detect missed messages.

TAC TRAP FIELDS

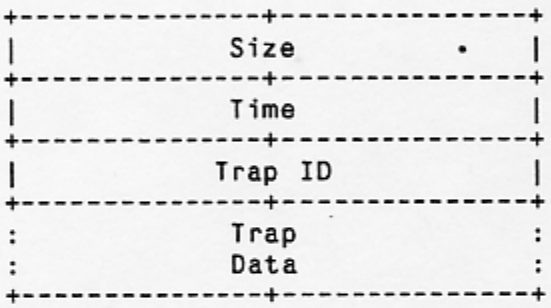
# of traps lost

Under certain conditions, a TAC may overflow its internal trap buffers and be unable to save traps to send. This counter keeps track of such occurrences.

Trap Reports

There can be several blocks of trap data in each message.

The format of the trap data is as follows:



Size

Size is the number of 16 bit words in the trap, not counting the size field.

Time

The time (in 640ms. units) at which the trap occurred. This field is used to sequence the traps in a message and associate groups of traps.

Trap ID

This is (usually) the program counter at the trap. The ID identifies the trap, and does not have to be a program counter, provided that it uniquely identifies the trap.

Trap Data

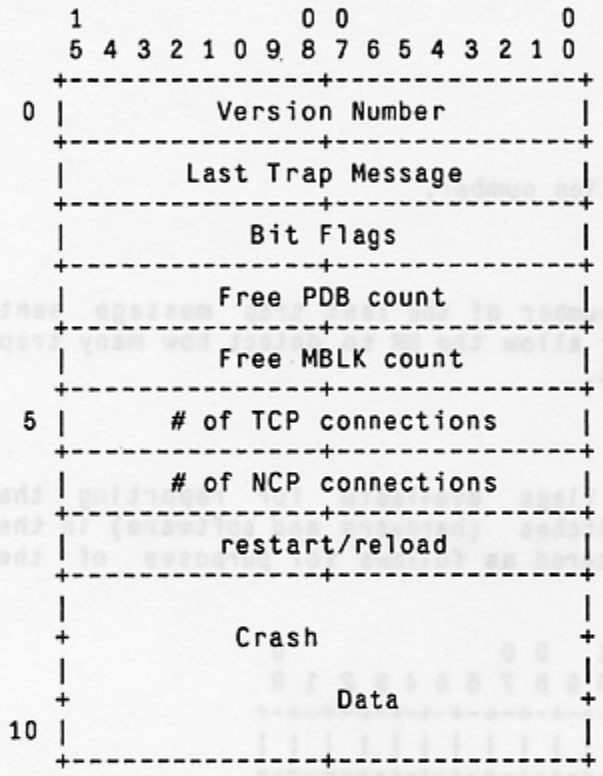
The TAC returns data giving more information about the trap. There are usually two entries: the values in the accumulator and the index register at the occurrence of the trap.

4.3.2 Message Type 2: TAC Status

Description

The status message gives a quick summary of the state of the TAC. Status of the most important features of the TAC are reported as well as the current configuration of the machine.

A TAC status message has the following form:



HMP FIELDS

System Type

TAC = 3

Message Type

TAC Status Message = 2

Port Number

Unused

Sequence Number

A 16 bit number incremented each time a status message is sent.

Returned Sequence Number

Contains the sequence number from the polling message requesting this report.

TAC STATUS FIELDS

Version Number

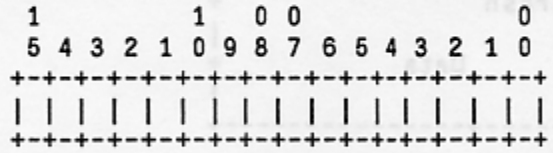
The TAC's software version number.

Last Trap Message

Contains the sequence number of the last trap message sent to the HM. This will allow the HM to detect how many trap messages are being lost.

Bit Flags

There are sixteen bit flags available for reporting the state of various switches (hardware and software) in the TAC. The bits are numbered as follows for purposes of the discussion below.



The bit flags report the status of the following:

Bit	Meaning
0	0 => DDT override off; 1 => override on.
1-4	0 => Sense Switch n is off; 1 => SSn on.
5	0 => Extended DDT not enabled; 1 => Extended DDT enabled.
6	0 => Traps going to console; 1 => Traps going to remote monitor.
7-15	unused

Free PDB count

The number of PDBs on the free queue.

Free MBLK count

The number of MBLKs on the free queue.

# of TCP connections
# of NCP connections

The number of open connections for each protocol.

Restart/Reload

This word reports a restart or reload of the TAC

Value	Meaning
1	restarted
2	reloaded

Crash Data

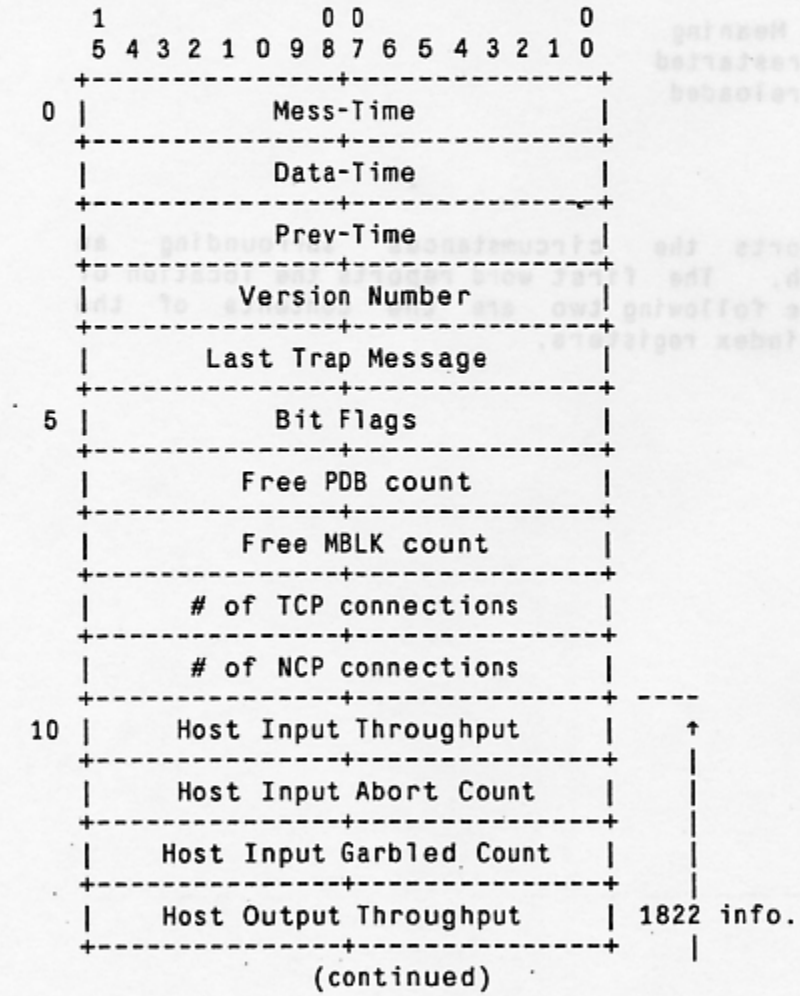
Crash data reports the circumstances surrounding an unexpected crash. The first word reports the location of the crash and the following two are the contents of the accumulator and index registers.

4.3.3 Message Type 3: TAC Throughput

Description

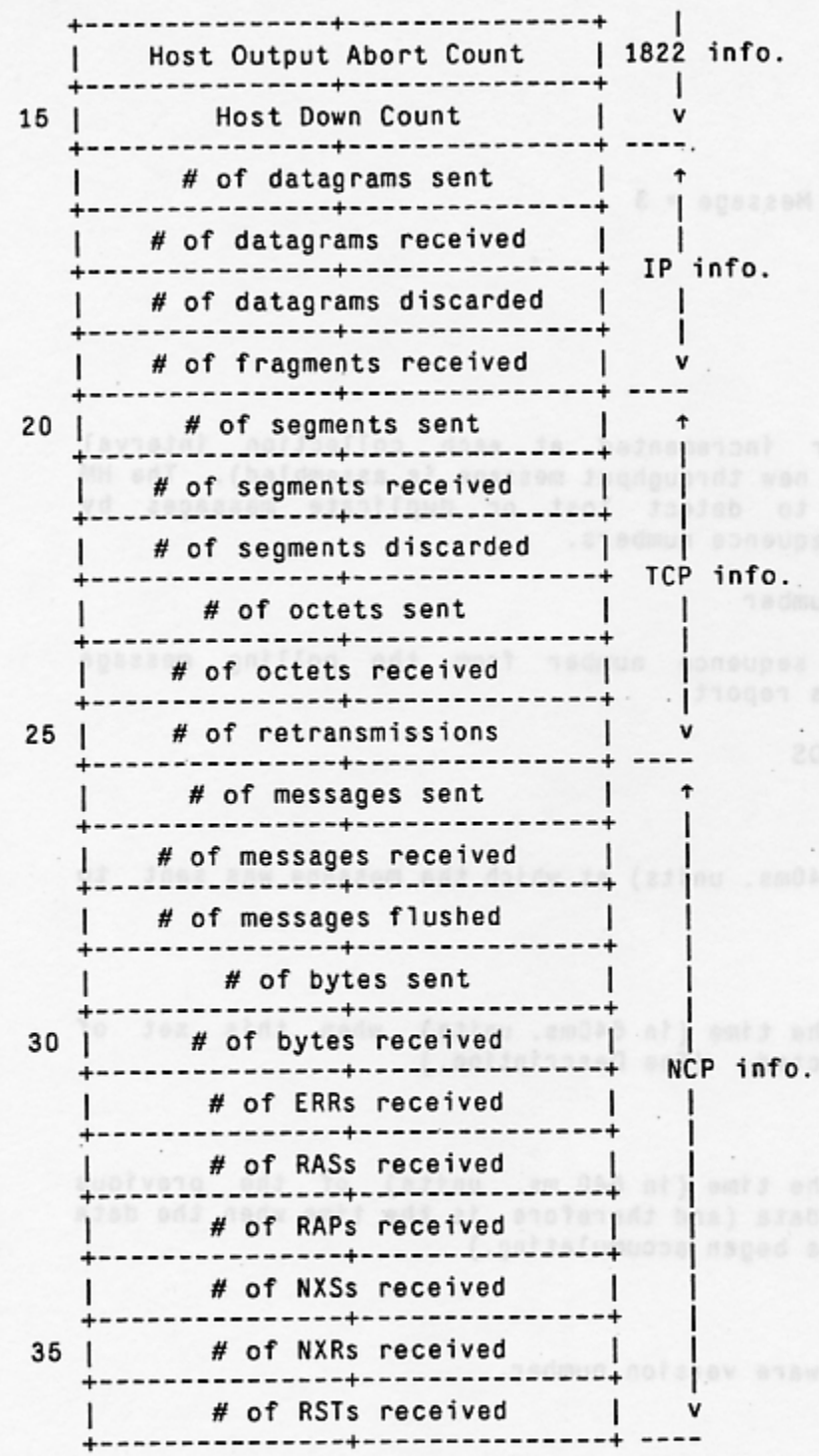
The TAC throughput message reports statistics for the various modules of the TAC. The TAC will collect these data at regular intervals and save them awaiting a poll from the HM. If a period is missed by the HM, the new results simply overwrite the old. Two time stamps bracket the collection interval (data-time and prev-time) and are an indicator of missed reports. In addition, mess-time indicates the time at which the message was sent.

A TAC throughput message has the following form:



(continued)

TAC throughput (cont.)



HMP FIELDS

System Type

TAC = 3

Message Type

TAC Throughput Message = 3

Port Number

Unused

Sequence Number

A 16 bit number incremented at each collection interval (i.e. when a new throughput message is assembled). The HM will be able to detect lost or duplicate messages by checking the sequence numbers.

Returned Sequence Number

Contains the sequence number from the polling message requesting this report.

TAC THROUGHPUT FIELDS

Mess-time

The time (in 640ms. units) at which the message was sent to the HM.

Data-Time

Data-time is the time (in 640ms. units) when this set of data was collected. (See Description.)

Prev-Time

Prev-time is the time (in 640 ms. units) of the previous collection of data (and therefore, is the time when the data in this message began accumulating.)

Version Number

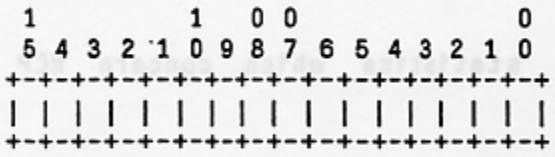
The TAC's software version number.

Last Trap Message

Contains the sequence number of the last trap message sent to the HM. This will allow the HM to detect how many trap messages are being lost.

Bit Flags

There are sixteen bit flags available for reporting the state of various switches (hardware and software) in the TAC. The bits are numbered as follows for purposes of the discussion below.



The bit flags report the status of the following:

Bit	Meaning
0	0 => DDT override off; 1 => override on.
1-4	0 => Sense Switch n is off; 1 => SSn on.
5	0 => Extended DDT not enabled; 1 => Extended DDT enabled.
6	0 => Traps going to console; 1 => Traps going to remote monitor.
7-15	unused

Free PDB count

The number of PDBs on the free queue.

Free MBLK count

The number of MBLKs on the free queue.

# of TCP connections
# of NCP connections

The number of open connections for each protocol.

1822 info.

These six fields report statistics which concern the operation of the 1822 protocol module, i.e. the interface between the TAC and its IMP.

IP info.

These four fields report statistics which concern Internet Protocol in the TAC.

TCP info.

These six fields report statistics which concern TCP protocol in the TAC.

NCP info.

These eleven fields report statistics which concern NCP protocol in the TAC.