RFC - 869

A Host Monitoring Protocol

Robert M. Hinden

BBN Communications Corporation

December 1983

Table of Contents

RFC-869 December 1983
Replaces IEN-197

A Host Monitoring Protocol

1 Introduction

The Host Monitoring Protocol (HMP) is used to collect information from hosts in various networks. A host is defined as an addressable Internet entity that can send and receive messages; this includes hosts such as server hosts, personal work stations, terminal concentrators, packet switches, and gateways. At present the Host Monitoring Protocol is being used to collect information from Internet Gateways and TACs, and implementations are being designed for other hosts. It is designed to monitor hosts spread over the internet as well as hosts in a single network.

This document is organized into three parts. Section 2 and 3 contains a general description of the Host Monitoring protocol and its relationship to other protocols. Section 4 describes how it operates. Section 5 and 6 contain the descriptions and formats of the HMP messages. These are followed by appendices containing the formats of messages sent by some of the hosts that use the HMP to collect their monitoring information. These appendicies included as examples only and are not part of the HMP protocol.

This document replaces the previous HMP document "IEN-197, A Host Monitoring Protocol."

2 General Description

The Host Monitoring Protocol is a transaction-oriented (i.e., connection-less) transport protocol. It was designed to facilitate certain simple interactions between two internet entities, one of which may be considered to be "monitoring" the other. (In discussing the protocol we will sometimes speak of a "monitoring host" and a "monitored entity".) HMP was intended to be a useful transport protocol for applications that involve any or all of the following three different kinds of interactions:

- The monitored entity sometimes needs to send unsolicited datagrams to the monitoring host. The monitoring host should be able to tell when messages from the monitored entity have been lost in transit, and it should be able to determine the order in which the messages were sent, but the application does not require that all messages be received or that they be received strictly in the same sequence in which they were sent.

- The monitoring host needs to gather data from the monitored entity by using a query-response protocol at the application level. It is important to be able to determine which query is being answered by a particular response, and to determine whether successive responses are duplicates of previous ones.

- The monitoring host must be able to initiate certain control functions in the monitored entity, possibly including the setting of parameters in the monitored entity. The monitoring host needs to know if the control function has been carried out.

In addition, we assume that a given monitoring host may be monitoring several different types of entities simultaneously, and may be gathering several different types of data from a given

type of monitored entity. Several different monitoring hosts may be monitoring a given entity, and several processes on the same host may even be monitoring the same entity.

Messages from the monitoring host to the monitored entity are called "polls". They need to contain enough information to allow the monitored entity to make the following determinations:

- The monitored entity must be able to determine that this message is in fact a poll from a monitoring host. The "system type," "message type," and "password" fields in the HMP header have been defined to meet this need.

- The monitored entity may need to be able to identify the particular process on the monitoring host that sent this poll, so it can send its response back to the right process. The "port number" field in the HMP header has been defined to meet this need.

- The monitored entity must be able to indicate to the monitoring host, in its response, precisely which query is being answered by a particular response. The "sequence number field" has been defined to meet this need.

- The monitored entity must be able to determine just what kind of action the monitoring host is requesting. That is, the HMP transport protocol must provide some way of multiplexing and demultiplexing the various higher-level applications which use it. The "R-message type" and "R-subtype" fields of the polling message have been defined to meet this need.

Messages from the monitored entity to the monitoring host need to contain enough information to enable the monitoring host to make the following determination:

- The monitoring host must be able to route this message to the correct process. The "port number" field meets this need.

- The monitoring host must be able to match up received messages with the polls, if any, that elicited them. The "returned sequence number" field in the HMP header has been defined to meet this need.

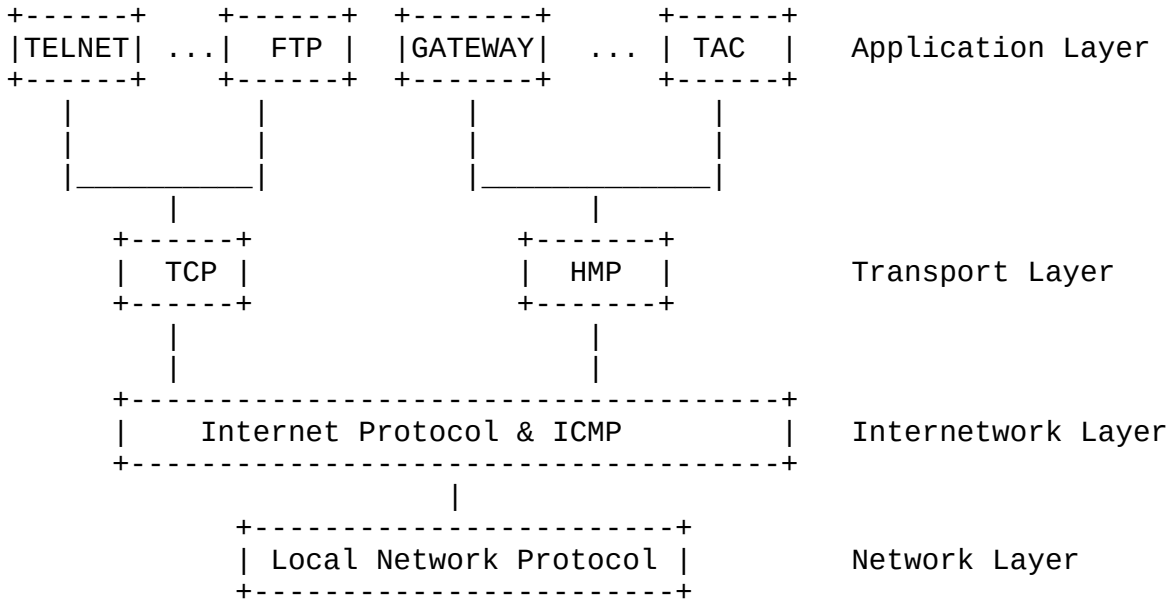
- The monitoring host must be able to determine which higher level application should receive a particular message. The "system type" and "message type" fields are used for this purpose.

- The monitoring host must be able to determine whether some messages of a given type were lost in transit, and whether messages have arrived out of sequence. Although this function, strictly speaking, belongs to the application and not to the transport layer, the HMP header contains a "sequence number" for this purpose.

In addition, a simple one’s complement checksum is provided in the HMP header to detect data corruption during transmission.

3 Relationship to Other Protocols

The Host Monitoring Protocol is a transport protocol designed to fit into the layered internet protocol environment. It operates on top of the Internet/ICMP protocol and under applications that require its services. This relationship is illustrated in the following diagram:



If internetwork services are not required it should be possible to run the HMP without an Internetwork layer. As long as HMPs' service requirnments (addressing, protocol demultiplexing, and occasional delivery) are met it should run over a variety of protocols.

4 Protocol Operation

The HMP is built around the idea that most of the intelligence needed to monitor a host should reside in a monitoring center, not in the host. The host should be required only to collect data and send it to the monitoring center, either spontaneously or on request from the monitoring center. The host is not responsible for insuring that the data arrives reliably (except that it checksums the data); instead, the monitoring center is responsible for ensuring that the data it requests is received correctly.

Consequently, the HMP is based on polling hosts for messages. When the monitoring center requires a particular type of data (e.g., throughput data), it sends a poll to the host requesting that type of report. The host, upon receiving the poll, responds with its latest set of collected data. If the host finds that the poll is incorrect (e.g., if the poll was for throughput data and the host is not collecting throughput data), it responds with an error message. The monitoring center waits a reasonable length of time for the host to answer its poll. If no response is received, it sends another poll for the same data. In this way, if either a poll or the response is lost, the correct data is still collected.

The HMP is used to collect three different classes of data:

- o Spontaneous Events (or Traps)
- o Current status
- o Statistical data collected over time

These classes of data allow a host to send data in a manner best suited to the data. For instance, the host may quickly inform the monitoring center that a particular event has happened by sending a trap message, while the monitoring center is reliably collecting the host's throughput and accounting data.

Traps report spontaneous events, as they occur, to the monitoring center. In order to insure their prompt delivery, the traps are sent as datagrams with no reliability mechanisms (except checksums) such as acknowledgments and retransmissions. Trap messages usually contain an identifier to indicate which event is being reported, the local time in the host that the event occured, and data pertinent to the event. The data portion is intended to be host and event specific.

Status information, the second type of data collected by the Host Monitoring Protocol describes the current state of the host. Status information is useful at one point, but it does not have to be collected cumulatively over a certain period of time. Only the latest status is of interest; old status provides no useful information. The monitoring center collects status information

by sending a poll for status to a host. Upon receiving the poll, the host responds with its latest status information, always creating a new status message. If the monitoring center does not receive a response to its poll, it sends another poll. The monitoring center can decide if the host is up or down based on whether the host responds to its polls.

The third type of data collected by the HMP is statistical data. These are measurements taken over time, such as the number of packets sent or received by a host and the count of packets dropped for a particular reason. It is important that none of this type of data be lost. Statistical data is collected in a host over a time interval. When the collection time interval expires, the current data is copied to another area, and the counters are cleared. The copied data is sent to the monitoring center when the host receives a poll requesting statistical information. If another poll is received before the collection time interval has expired, the data in the buffer is sent again. The monitoring center can detect duplicate messages by using the sequence number in the header of the message, since each type of statistical data has its own sequence number counter.

The collection frequency for statistics messages from a particular host must be relatively long compared to the average round trip message time between the monitoring center and that host inorder to allow the monitoring center to re-poll if it does

not receive an answer. With this restriction, it should be possible to avoid missing any statistics messages. Each statistics message contains a field giving the local time when the data was collected and the time at which the message was sent. This information allows the monitoring center to schedule when it sends a poll so that the poll arrives near the beginning of each collection period. This ensures that if a message is lost, the monitoring center will have sufficient time to poll again for the statistics message for that period.

The HMP also includes a provision to send data to and read parameters in hosts. The data may be used to set switches or interval timers used to control measurements in a host, or to control the host itself (e.g. a restart switch). The format of the data and parameters is host specific.

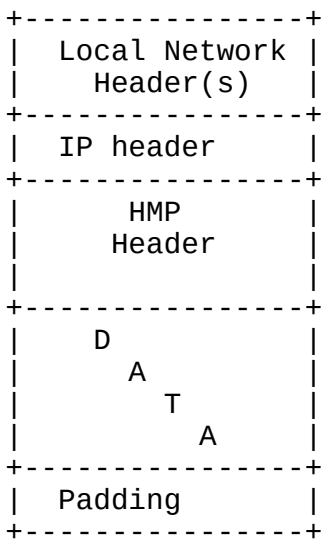
To send data to a host, the monitoring center sends the host a poll for a control-acknowledgment message. This poll message includes the type of the data and the data being sent. When the host receives this poll, it processes the data and responds with a control-acknowledgment message.

To read parameters in a host, the monitoring center will send a poll for parameters to the host. This poll includes the type of the parameters being read. When the host receives this poll, it will send the parameters of the requested type to the

monitoring center in a parameters message.

5 Header Formats

Host Monitor Protocol messages have the following format:



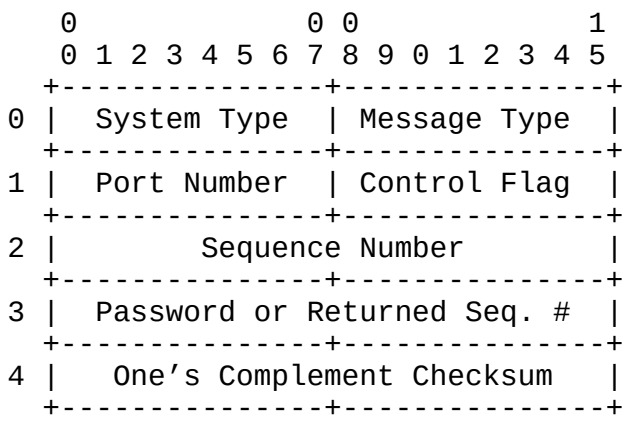
5.1 IP Headers

HMP messages are sent using the version 4 IP header as described in RFC-791 "Internet Protocol." The HMP protocol number is 20 (decimal). The time to live field should be set to a reasonable value for the hosts being monitored.

All other fields should be set as specified in RFC-791.

5.2 HMP Header

The HMP 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	Monitoring Host
2	IMP
3	TAC
4	Gateway
5	SIMP
6	BBN VAX/C70 TCP
7	PAD
8	Reserved
9	TIU
10	FEP
11	Cronus Host
12	Cronus MCS

Message types are defined and used for each system type according to the needs of that system. The message types currently defined are:

Type	Description
1	Trap
2	Status
3	Thruput
4	HTM - Host Traffic Matrix
5	Parameters
6	Routing
7	Call Accounting
100	Poll
101	Error
102	Control Acknowledgment

Port Number

This field can be used to multiplex similar messages to/from different processes in one host. It is currently unused.

Control Flag

This field is used to pass control information. Currently Bit 15 is defined as the "More bit" which is used in a message in responce to a poll to indicate that there is more data to poll for.

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 monitoring center contains a password to verify that the monitoring center 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.

6 HMP Monitoring Center Message Formats

6.1 Message Type 100: Polling Message

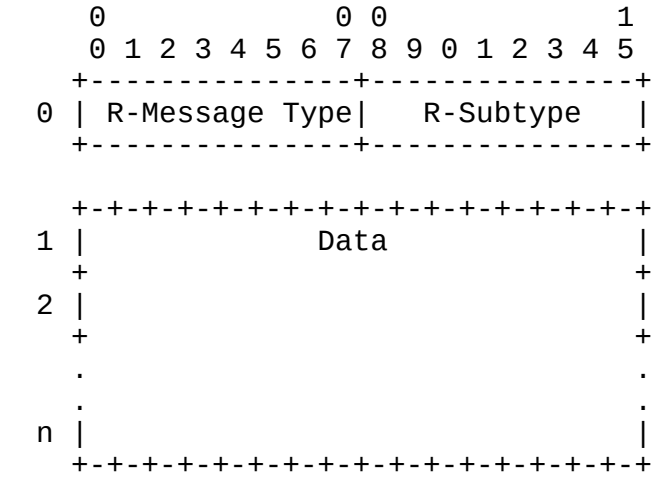
Description

The monitoring center will send polls to the hosts it is monitoring to collect their monitoring data. When the host receives a poll it will return a message of the type requested. It will only answer a poll with the correct system type and password and will return an error message (Message Type 101) if it receives a poll for the wrong system type or an unsupported message type.

The Poll message includes a facility to send data to a monitored host. The poll message to send data consists of a poll for a Control Acknowledgment message (type 102) followed by the data. The R-Subtype specifies the type of the data that is being sent. When the monitored host receives a Poll for a Control acknowledgment, it processes the data, and then responds with an Control acknowledgment message. If the monitored host can not process the data, it should respond with an error message.

A poll to read parameters consists a poll for a Parameters message. The R-Subtype specifies the type of parameters being read. When the monitored host receives a poll for a Parameters message, it responds with a Parameters message containing the requested information.

A polling message has the following form:



HMP FIELDS

System Type

The type of machine being polled.

Message Type

Polling Message = 100

Port Number

Unused

Control Flag

Unused

Sequence Number

The sequence number identifies the polling request. The Monitoring Center will maintain separate sequence numbers for each host it monitors. This sequence number is returned in the response to a poll and the monitoring center 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

This field is used when sending data and reading parameters and it specifies the type of the data being sent or parameters being read.

Data

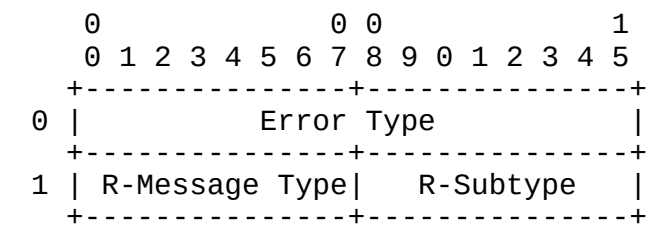
When the poll is requesting a Control Acknowledgment message, data is included in the poll message. A poll for any other type of message does not include any data . The contents of the data is host specific.

6.2 Message Type 101: 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

The type of machine sending message.

Message Type

Error Message = 101

Port Number

Unused

Control Flag

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.
4 = Unknown parameter
5 = Invalid parameter value
6 = Invalid parameter/value format
7 = Machine in Loader

R-Message Type
R-Subtype

These fields identify the poll request in error.

6.3 Message Type 102: Control acknowledgment

Description

This message is sent in response to a poll for this type of message. It is used to acknowledge poll messages that are used to set parameters in the monitored host.

The Control acknowledgment has no fields other than the HMP header.

HMP FIELDS

System Type

The type of the system sending the message.

Message Type

Control acknowledgment = 102

Port Number

Unused

Control Flag

Unused

Sequence Number

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

Returned Sequence Number

The Sequence Number of the polling message which requested this message.

A Appendix A - IMP Monitoring

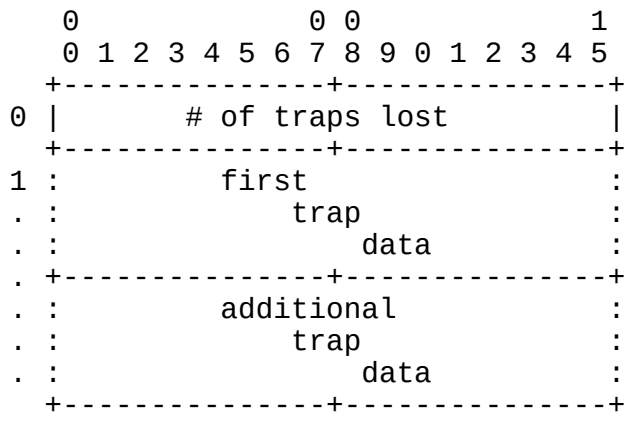
A.1 Message Type 1: IMP Trap

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

Control Flag

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.

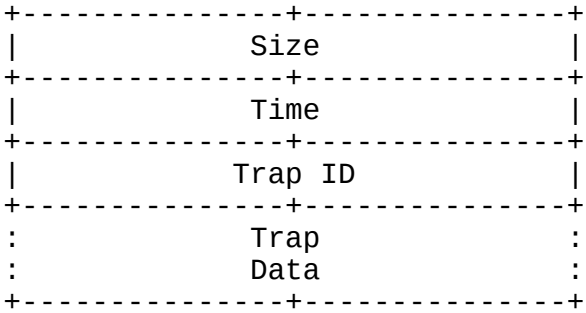
IMP TRAP FIELDS

# 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

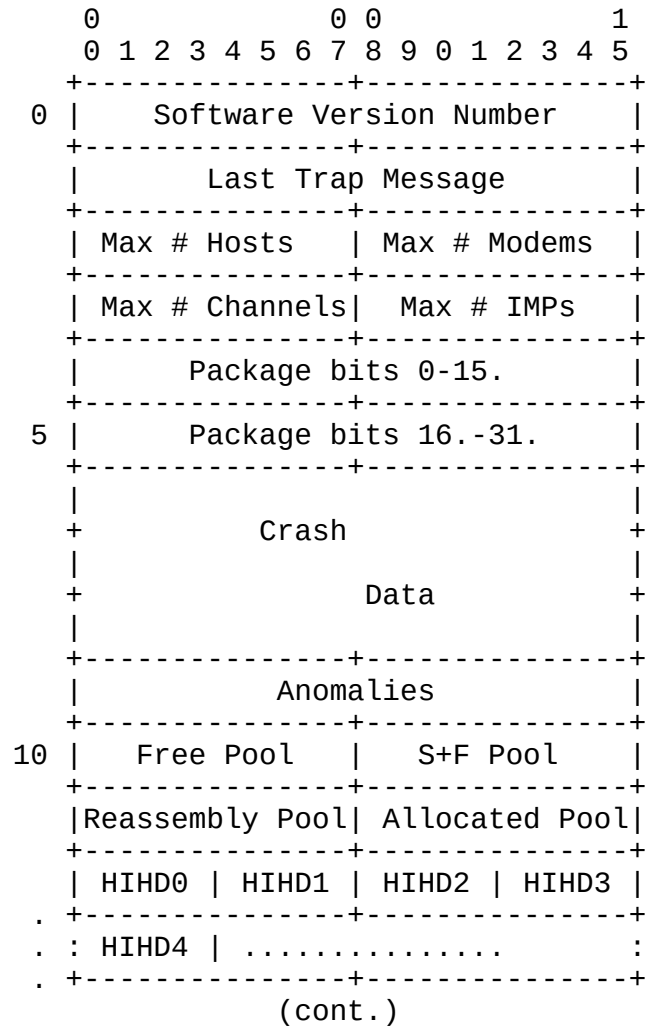
The IMP returns data giving more information about the trap. There are usually two entries: the values in the accumulator and the index register at the occurrence of the trap.

A.2 Message Type 2: IMP status

Description

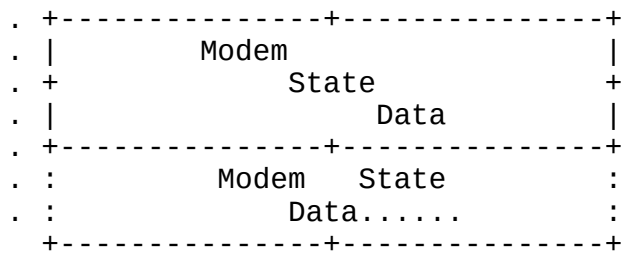
The status message gives a quick summary of the state of the IMP. Status of the most important features of the IMP are reported as well as the current configuration of the machine.

The format of the status message is as follows:



(cont.)

Imp Status (cont.)



HMP FIELDS

System Type

IMP = 2

Message Type

IMP status message = 2

Port Number

Unused

Control Flag

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.

Channels

The maximum possible number of IMP-IMP channels in this system.

IMPs

The maximum possible number of IMPs 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
(1st Word)	
1	VDH
2	Logical address tables
4	Mezmode
10	Cumulative Statistics
20	Trace
40	TTY
100	DDT
200	HDLC
400	HDH
1000	Cassette Writer
2000	Propagation Delay Measurement
4000	X25
10000	Profile Measurements
20000	Self Authenticating Password
40000	Host traffic Matrix
100000	Experimental/Special
(2nd Word)	
1	End-to-end Statistics
2	Store and Forward statistics

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
20	Override ON
200	Trace ON
1000	Statistics ON
2000	Message Generator ON
4000	Packet Trace ON
10000	Host Data Checksum is BAD
20000	Reload Location SET

Buffer Pool Counts

These are four bytes of counters indicating the current usage of buffers in the IMP. The four counters are: free buffers, store-and-forward buffers, reassembly buffers and allocated buffers.

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

Modem State Data

Modem state data contains six fields of data distributed over four words. The first field (4 bits) indicates the line speed; the second field (4 bits) is the number of the modem that is used by the neighboring IMP on this line; the third field (8 bits) is the number of line protocol ticks covered by this report; the fourth (1 bit) indicates line down(1) or up(0); the fifth (7 bits) is the IMP number of neighbor IMP on the line; and the sixth (8 bits) is a count of missed protocol packets over the interval specified in the third field.

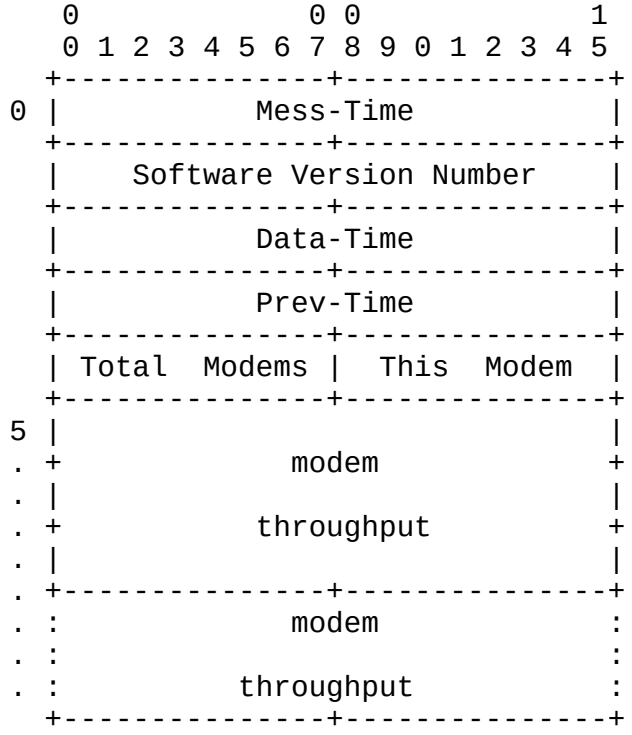
A.3 Message Type 3: IMP Modem Throughput

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

Control Flag

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.

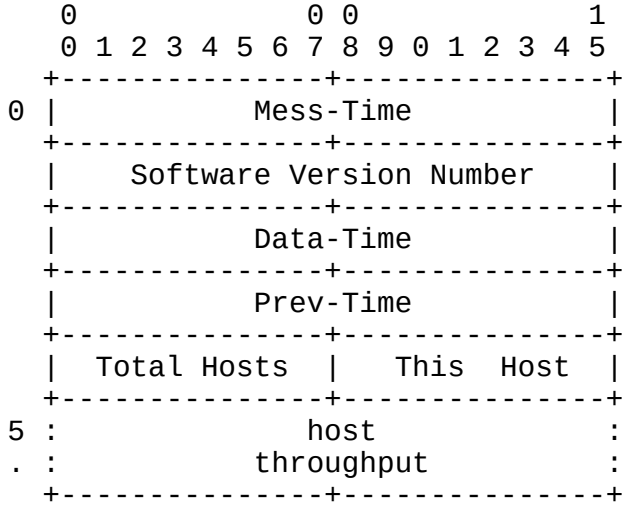
A.4 Message Type 4: IMP Host Throughput

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

Control Flag

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.

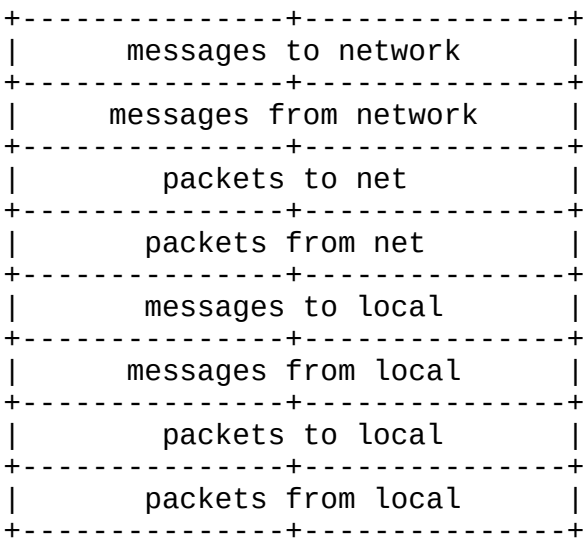
This Host

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 eight 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.

B Appendix B - TAC Monitoring

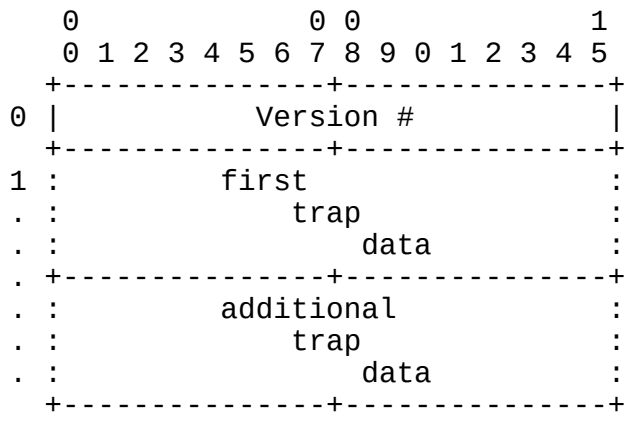
B.1 Message Type 1: TAC Trap Message

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

Control Flag

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

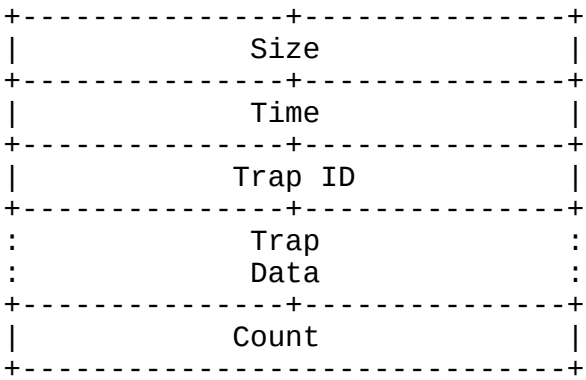
Version #

The version # of the TAC Software.

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.

Count

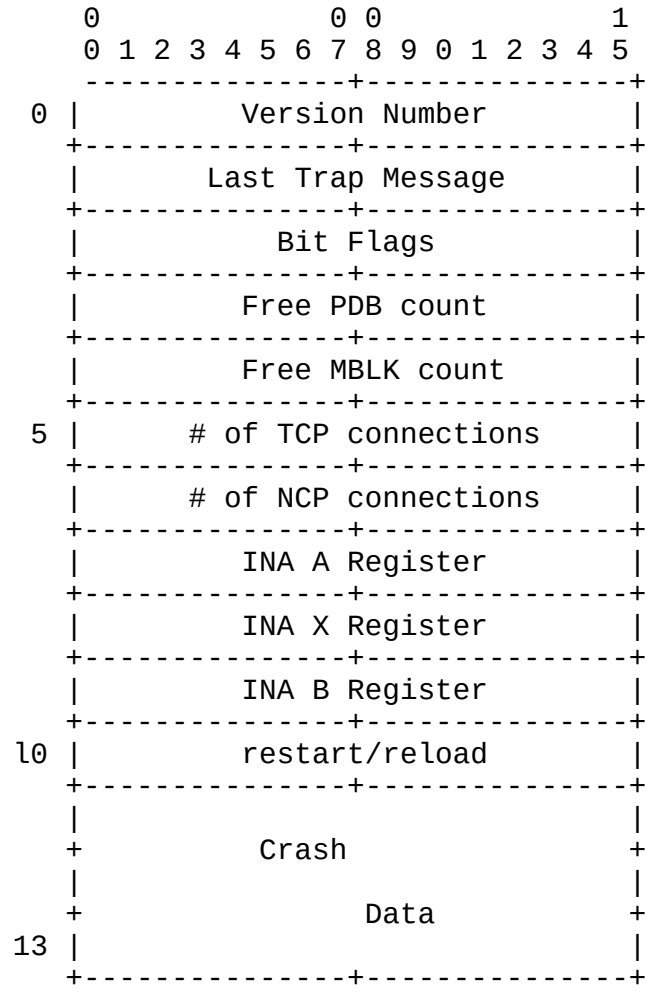
The TAC Counts repetitions of the same trap ID and reports this count here.

B.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

Control Flag

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

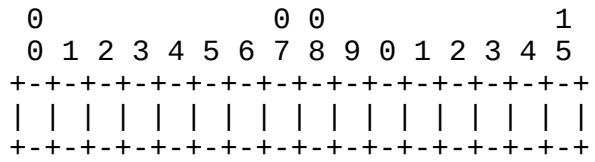
The TAC’s software version number.

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
15	0 => DDT override off; 1 => override on.
11-14	0 => Sense Switch n is off; 1 => SSn on.
10	0 => Traps to remote monitor; 1 => Traps to console.
9	1 => Message generator on.
0-8	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.

INA Report

These three fields report the values retained by an INA 1011 instruction in a C/30. This instruction returns micro-machine status and errors. In a #316, the fields are meaningless.

Restart/Reload

This word reports a restart or reload of the TAC

Value	Meaning
1	restarted
2	reloaded

Crash Data

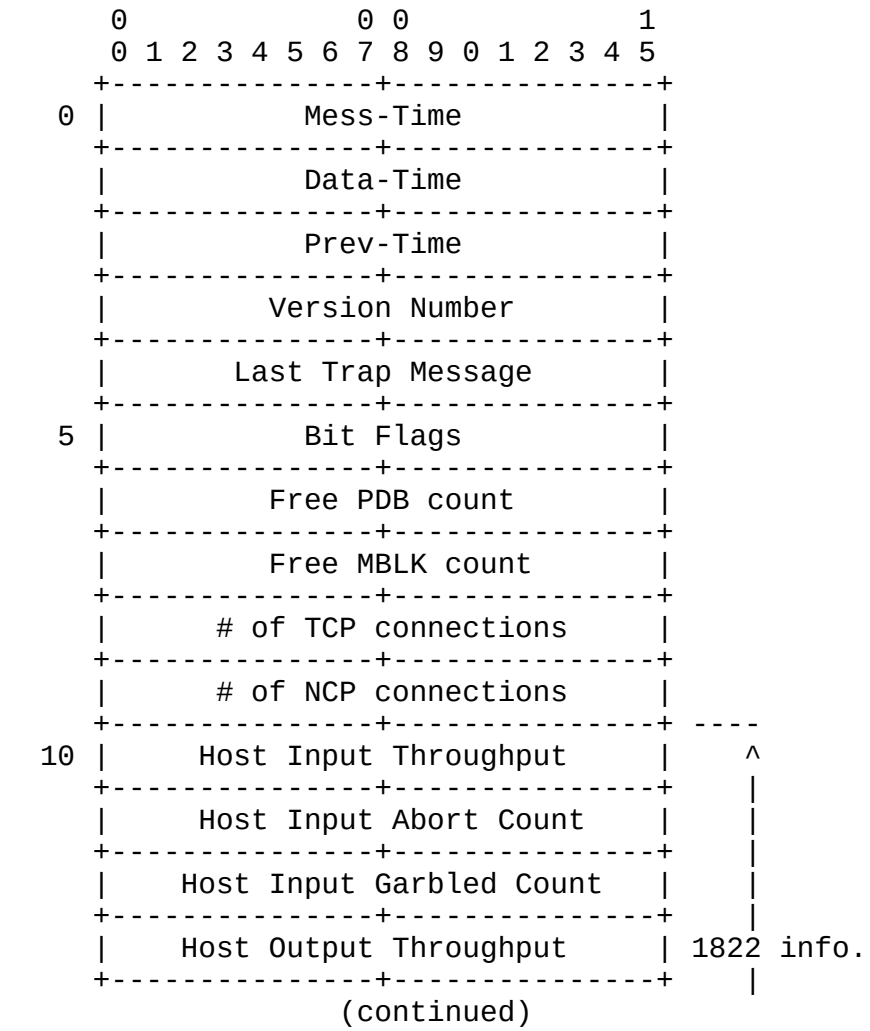
Crash data reports the circumstances surrounding an unexpected crash. The first word reports the location of the crash and the following two are the contents of the accumulator and index registers.

B.3 Message Type 3: TAC Throughput

Description

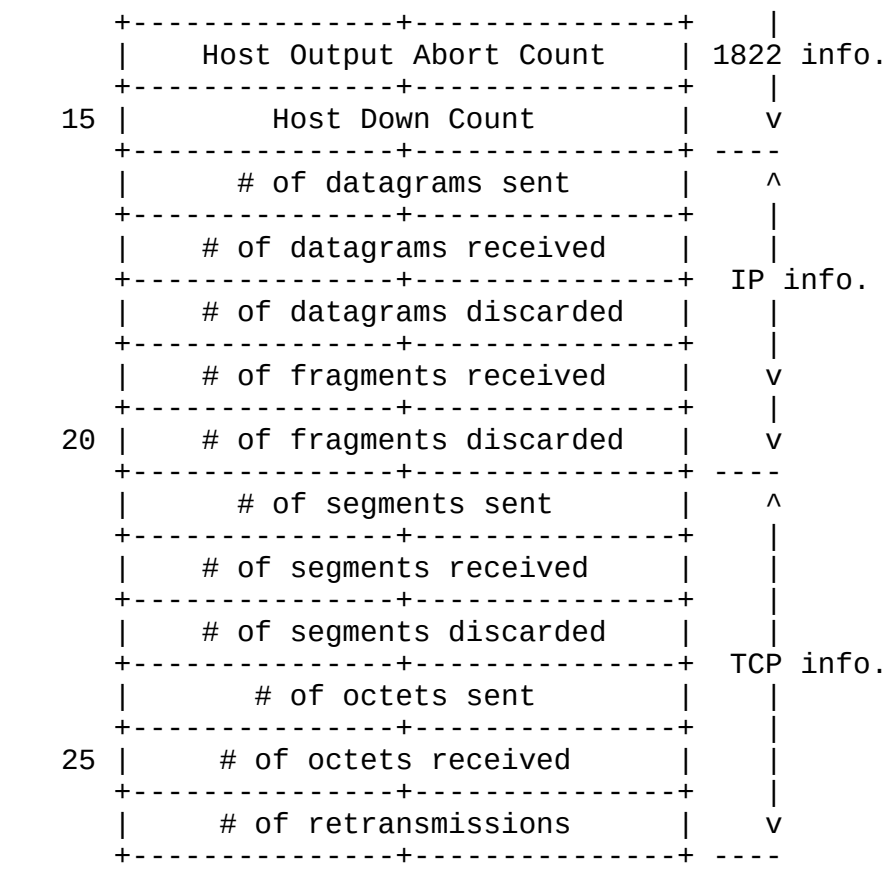
The TAC throughput message reports statistics for the various modules of the TAC. The TAC will collect these data at regular intervals and save them awaiting a poll from the HM. If a period is missed by the HM, the new results simply overwrite the old. Two time stamps bracket the collection interval (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

Control Flag

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

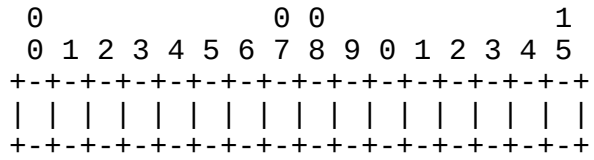
The TAC’s software version number.

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
15	0 => DDT override off; 1 => override on.
11-14	0 => Sense Switch n is off; 1 => SSn on.
10	0 => Traps to remote monitor; 1 => Traps to console.
9	1 => Message generator on.
0-8	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 five fields report statistics which concern Internet Protocol in the TAC.

TCP info.

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

C Appendix C - Gateway Monitoring

C.1 Gateway Parameters

The gateway supports parameters to set Throughput and Host traffic matrix measurements. The type of parameters and the parameter and data pairs are as follows:

Throughput - Type = 3

Parm.	Description	Control Data Word
1	Start/Stop	0=Stop,1=Start
2	Collection Interval	Time in 1 minute ticks

Host Traffic Matrix - Type = 4

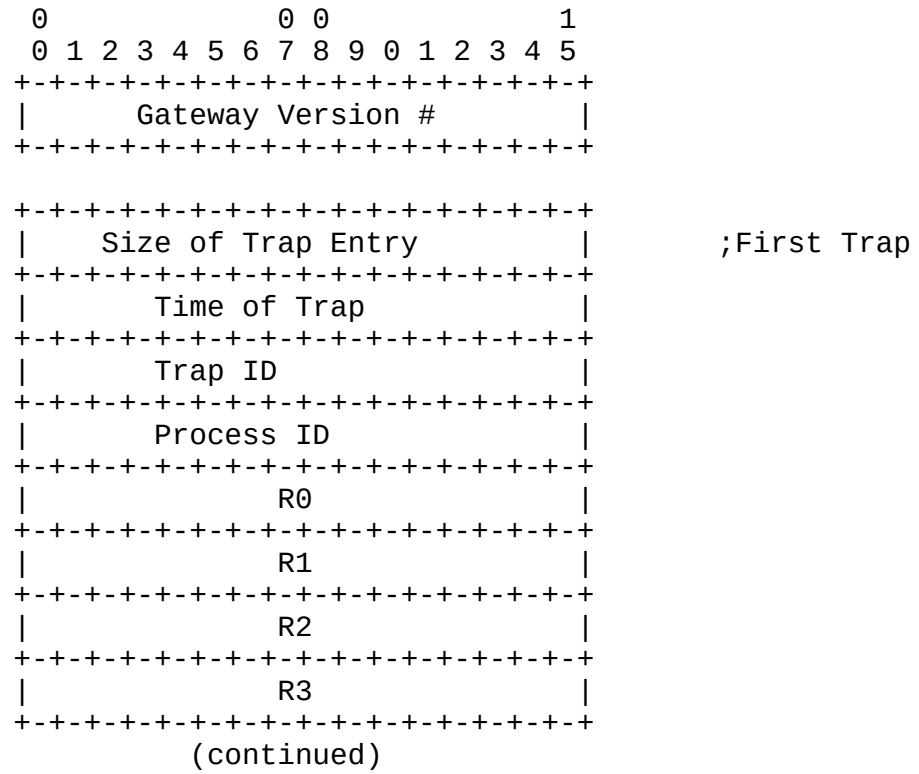
Parm.	Description	Control Data Word
1	Start/Stop	0=Stop,1=Start
2	Collection Interval	Time in 1 minute ticks
3	HTM Switch Control	Include Control Protocols

C.2 Message Type 1: Gateway Trap

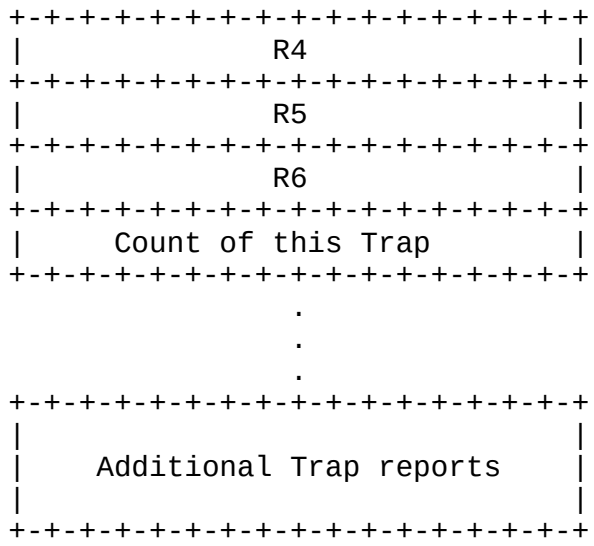
Description

When traps occur in the gateway they are buffered. At a fixed time interval (currently 10 seconds) the gateway will send any traps that are in the buffer to the monitoring center. The traps are sent as unsolicited messages.

A Gateway trap message has the following format:



Gateway Trap Message (cont'd.)



HMP FIELDS

System Type

Gateway = 4

Message Type

Gateway Trap Message = 1

Port Number

Unused

Control Flag

Unused

Password or Returned Sequence Number

Unused

Sequence Number

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

GATEWAY TRAP FIELDS

Gateway Version #

The software version number of the gateway sending the trap.

Trap Reports

The remainder of the trap message consists of the trap reports. Each consists of the following fields:

Size of Trap Entry

The size in 16-bit words of the trap entry, not including the size field.

Time of Trap

The time in (in 1/60 sec. ticks) at which the trap occurred.

Trap ID

The number of the trap which is used to identify the trap.

Process ID

The identifier of the process that executed the trap.

R0-R6

The registers of the machine at the occurrence of the trap.

Count of this Trap

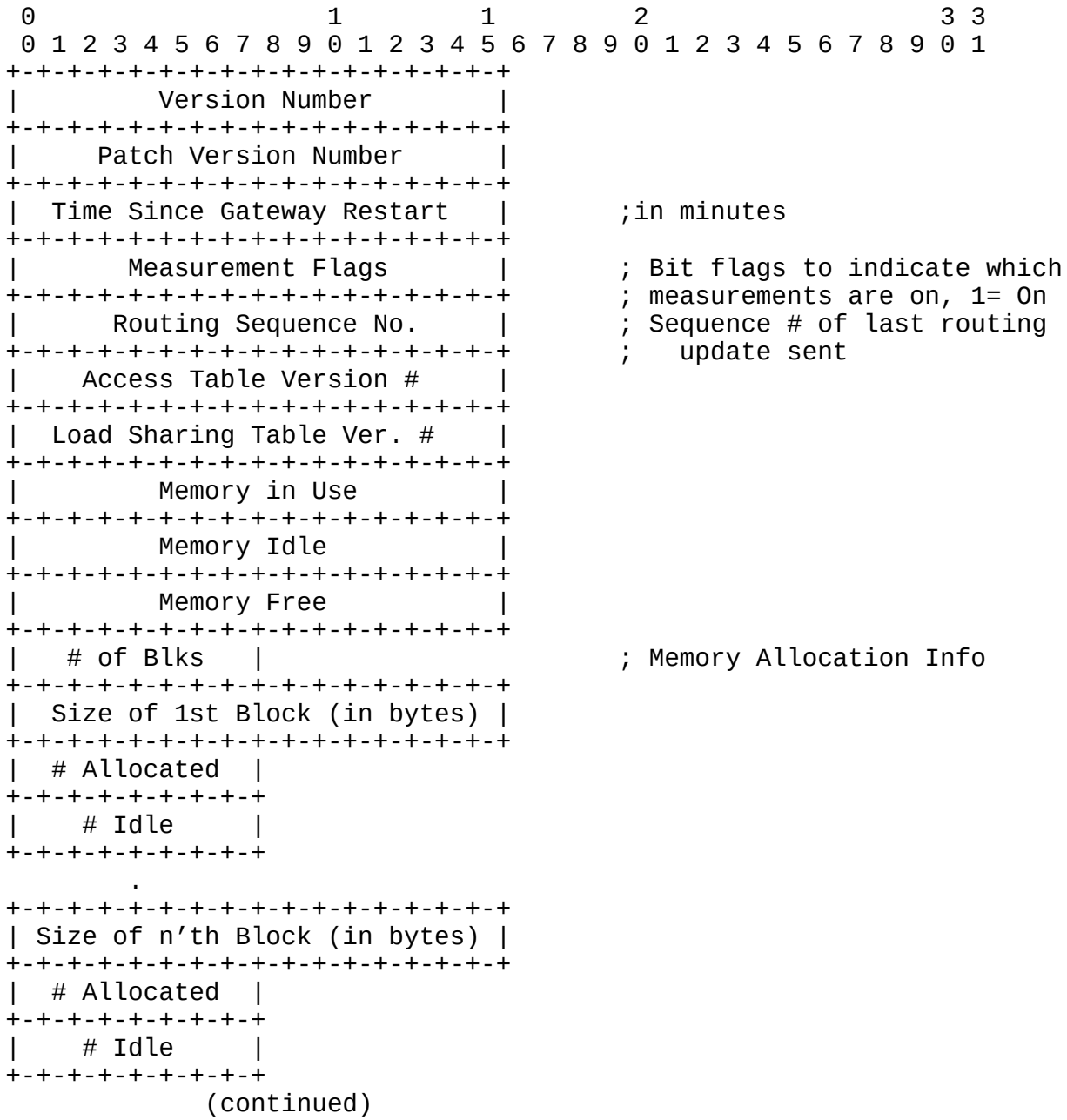
The number of times that this trap occurred.

C.3 Message Type 2: Gateway Status

Description

The gateway status message gives a summary of the status of the gateway. It reports information such as version number of the gateway, buffer memory usage, interface status and neighbor gateway status.

A Gateway Status message has the following format:


0 1 1 2 3 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Version Number
Patch Version Number
Time Since Gateway Restart
;in minutes
Measurement Flags
; Bit flags to indicate which
; measurements are on, 1= On
Routing Sequence No.
; Sequence # of last routing
; update sent
Access Table Version #
Load Sharing Table Ver. #
Memory in Use
Memory Idle
Memory Free
# of Blks
; Memory Allocation Info
Size of 1st Block (in bytes)
Allocated
Idle
.
Size of n'th Block (in bytes)
Allocated
Idle

(continued)

Gateway Status Message (cont'd.)

HMP FIELDS

System Type

Gateway = 4

Message Type

Gateway Status Message = 2

Port Number

Unused

Control Flag

Unused

Password or Returned Sequence Number

Unused

Sequence Number

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

GATEWAY STATUS FIELDS

Version Number

The version number of the gateway sending the Status message.

Patch Version Number

The patch version number of the gateway.

Time Since Gateway Restart

The time in minutes since the gateway was last restarted or reloaded.

Measurement Flags

Flags that, if set, indicate which measurements are turned on. Current values are:

```
Bit 0   =   Message Generator
    1   =   Throughput
    2   =   Host Traffic Matrix
    3   =   Access Control 1
    4   =   Access Control 2
    5   =   Load Sharing
    6   =   EGP in Gateway
```

Routing Sequence Number

The sequence number of the last routing update sent by this gateway.

Access Control Table Version #

The version number of the access control table.

Load Sharing Table Version #

The version number of the load sharing table.

Memory In Use

The number of bytes of buffer memory that are currently in use.

Memory Idle

The number of bytes of buffer memory that have been allocated but are currently idle.

Memory Free

The number of bytes of buffer memory that has not been allocated.

MEMORY ALLOCATION INFORMATION

The next part of the status message contains information on the buffer pools in the gateway. The fields are:

# of Blocks

The number of different buffer pools.

Size of Block

The size of this block in bytes.

Allocated

The number of blocks of this size that have been allocated.

Idle

The number of blocks of this size that are idle.

GATEWAY INTERFACE FIELDS

The next part of the status message are fields that provide information about the gateway's interfaces. The fields are:

# of Interfaces

The number of network interfaces that the gateway has.

Interface Flags

Flags that indicate the status of this interface. The current values are:

```
Bit 0  -  1=Up/0=Down
    1  -  1=Looped/0=Not Looped
```

Buffers

The numbers on this interfaces write queue.

Time Since Last Status Change

The time in minutes since this interface changed status (Up/Down).

# of Buffers Allocated

The number of buffers allocated for this interface.

Data Size for Interface

The buffer size required for this interface.

Interface Address

The Internet address of this interface.

NEIGHBOR GATEWAY FIELDS

The final part of the status message consists of information about this gateway's neighbor gateways. The fields are:

# of Neighbors

The number of gateways that are neighbor gateways to this gateway.

UP/DN Flags

Bit flags to indicate if the neighbor is up or down.

Neighbor Address

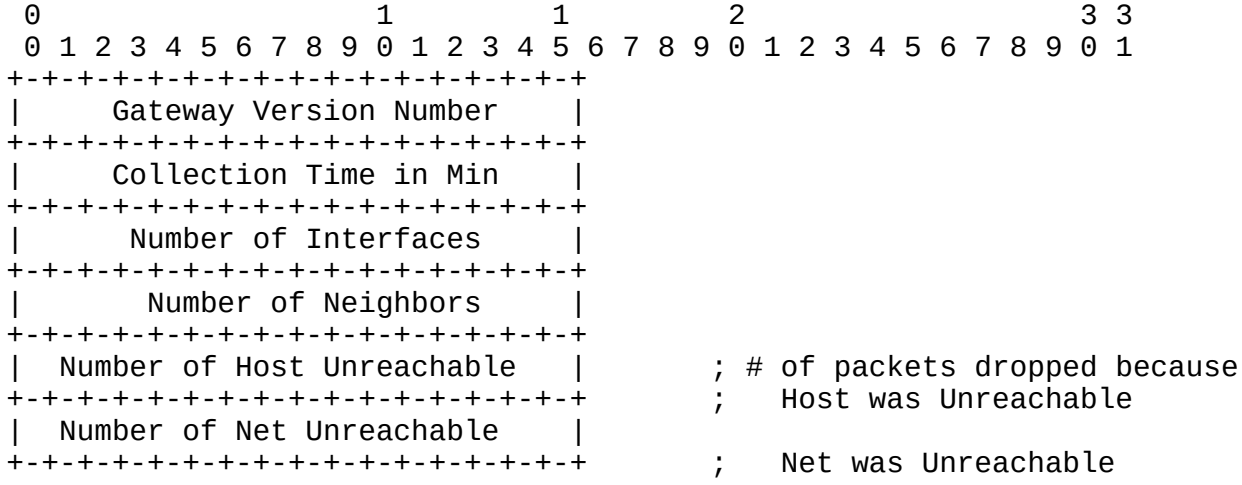
The Internet address of the neighbor gateway.

C.4 Message Type 3: Gateway Throughput

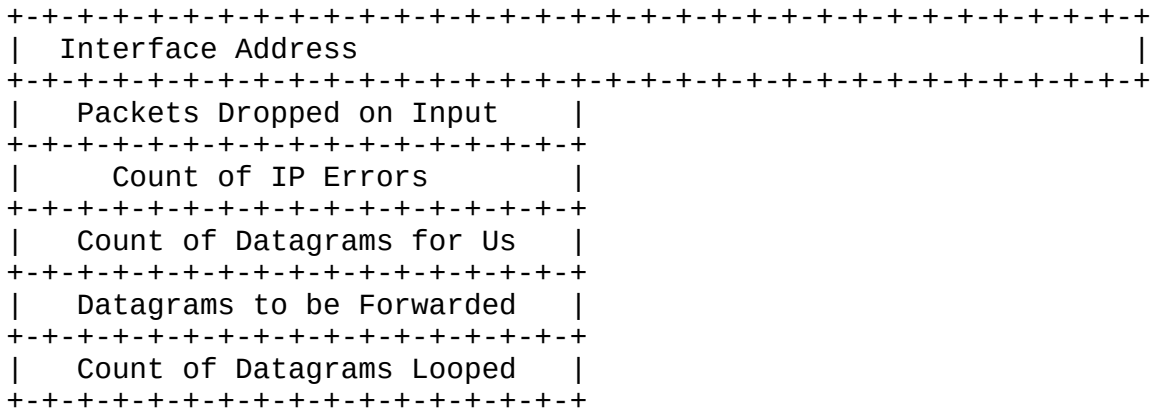
Description

The gateway collects throughput statistics for the gateway, its interfaces, and its neighbor gateways. It collects them for regular intervals and will save them for collection via a Poll message from the Monitoring host. If they are not collected by the end of the next interval, they will be lost because another copy will be put into the saved area.

A Gateway Throughput message has the following format:

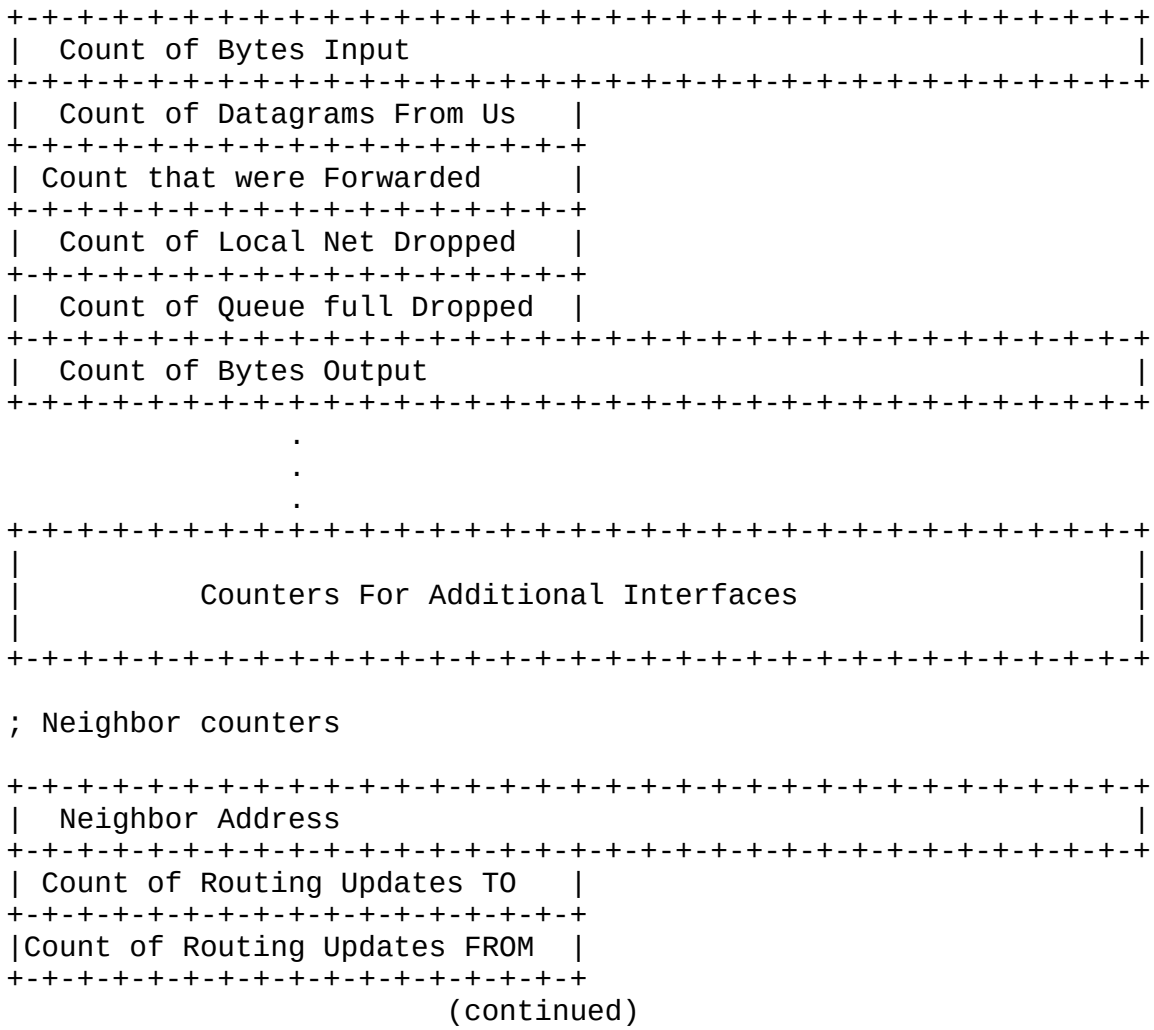


; Interface Counters



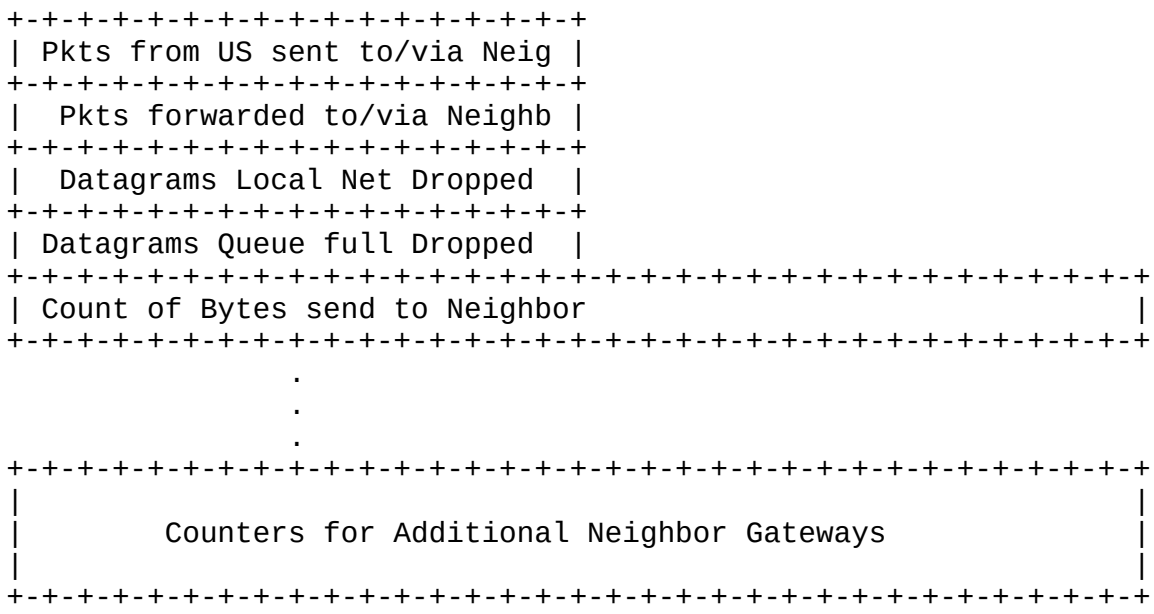
(continued)

Gateway Throughput Message (cont'd.)



(continued)

Gateway Throughput Message (cont'd.)



HMP FIELDS

System Type

Gateway = 4

Message Type

Gateway Throughput Message = 3

Port Number

Unused

Control Flag

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.

GATEWAY THROUGHPUT FIELDS

Gateway Version Number

The software version number of the gateway sending the trap.

Collection Time in Min.

The time period in minutes in which the throughput data is to be collected.

Number of Interfaces

The number of interfaces this gateway has.

Number of Neighbors

The number of neighbor gateways this gateway has.

Number of Host Unreachable

The number of packets dropped because the Host was unreachable.

Number of Net Unreachable

The number of packets dropped because the Network was unreachable.

INTERFACE COUNTERS

The next part of the Throughput message contains counters for the gateways interfaces. Each interface has the following fields:

Interface Address

The Internet address of this interface.

Packets Dropped on Input

The number of packets on input to this interface because there were not enough buffers.

Count of IP Errors

The number of packets received with bad IP headers.

Count of Datagrams for Us

The number of datagrams received addressed to this gateway.

Datagrams to be Forwarded

The number of datagrams were not for this gateway and should be sent out another interface.

Count of Datagrams Looped

The number of datagrams that were received on and sent out of this interface.

Count of Bytes Input

The number of bytes received on this interface.

Count of Datagrams From Us

The number of datagrams that originated at this gateway.

Count that were Forwarded

The number of datagrams that were forwarded to another gateway.

Count of Local Net Dropped

The number of packets that were dropped because of local network flow control restrictions.

Count of Queue full Dropped

The number of packets that were dropped because the output queue was full.

Count of Bytes Output

The number of bytes sent out on this interface.

NEIGHBOR COUNTERS

The last part of the Throughput message are counts for each neighbor gateway. The fields are:

Neighbor Address

The Internet address of this neighbor gateway.

Count of Routing Updates TO

The number of routing updates sent to this neighbor gateway.

Count of Routing Updates FROM

The number of routing updates received from this neighbor gateway.

Pkts from US sent to/via Neig

The number of packets from this gateway sent to or via this neighbor gateway.

Pkts forwarded to/via Neighb

The number of packets forwarded to or via this neighbor gateway.

Datagrams Local Net Dropped

The number of datagrams dropped to this neighbor gateway because of local network flow control restrictions.

Datagrams Queue full Dropped

The number of datagrams dropped to this neighbor because the output queue was full.

Count of Bytes send to Neighbor

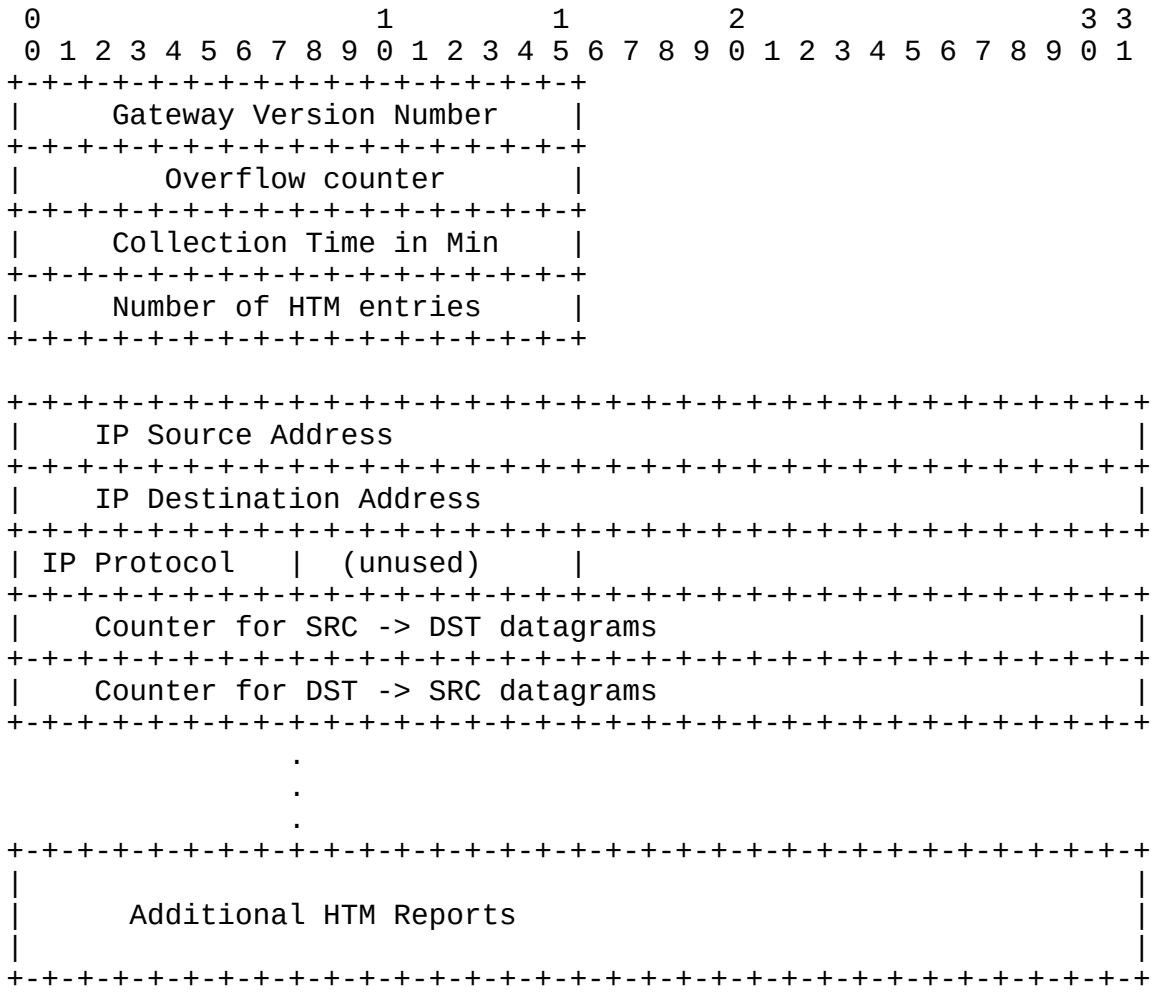
The number of bytes sent to this neighbor gateway.

C.5 Message Type 4: Gateway Host Traffic Matrix

Description

The Host Traffic Matrix (HTM) message contains information about the traffic that flows through the gateway. Each entry consists of the number of datagrams sent and received for a particular source/destination pair.

A Gateway HTM message has the following format:



HMP FIELDS

System Type

Gateway = 4

Message Type

Gateway HTM Message = 4

Port Number

Unused

Control Flag

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.

GATEWAY HTM FIELDS

Gateway Version Number

The software version number of this gateway.

Overflow counter

The number of HTM entries lost because the HTM buffer was full.

Collection Time in Min

The time period in minutes in which the HTM data is being collected.

Number of HTM entries

The number of HTM reports included in this message.

HTM ENTRIES

The remainder of the HTM message consists of the actual HTM entries. Each entry consists of the following fields:

IP Source Address

The source Internet address of the datagrams being counted.

IP Destination Address

The destination Internet address of the datagrams being counted.

IP Protocol

The protocol number of the datagrams.

Counter for SRC -> DST datagrams

The number of datagrams sent in the Source to Destination address direction.

Counter for DST -> SRC datagrams

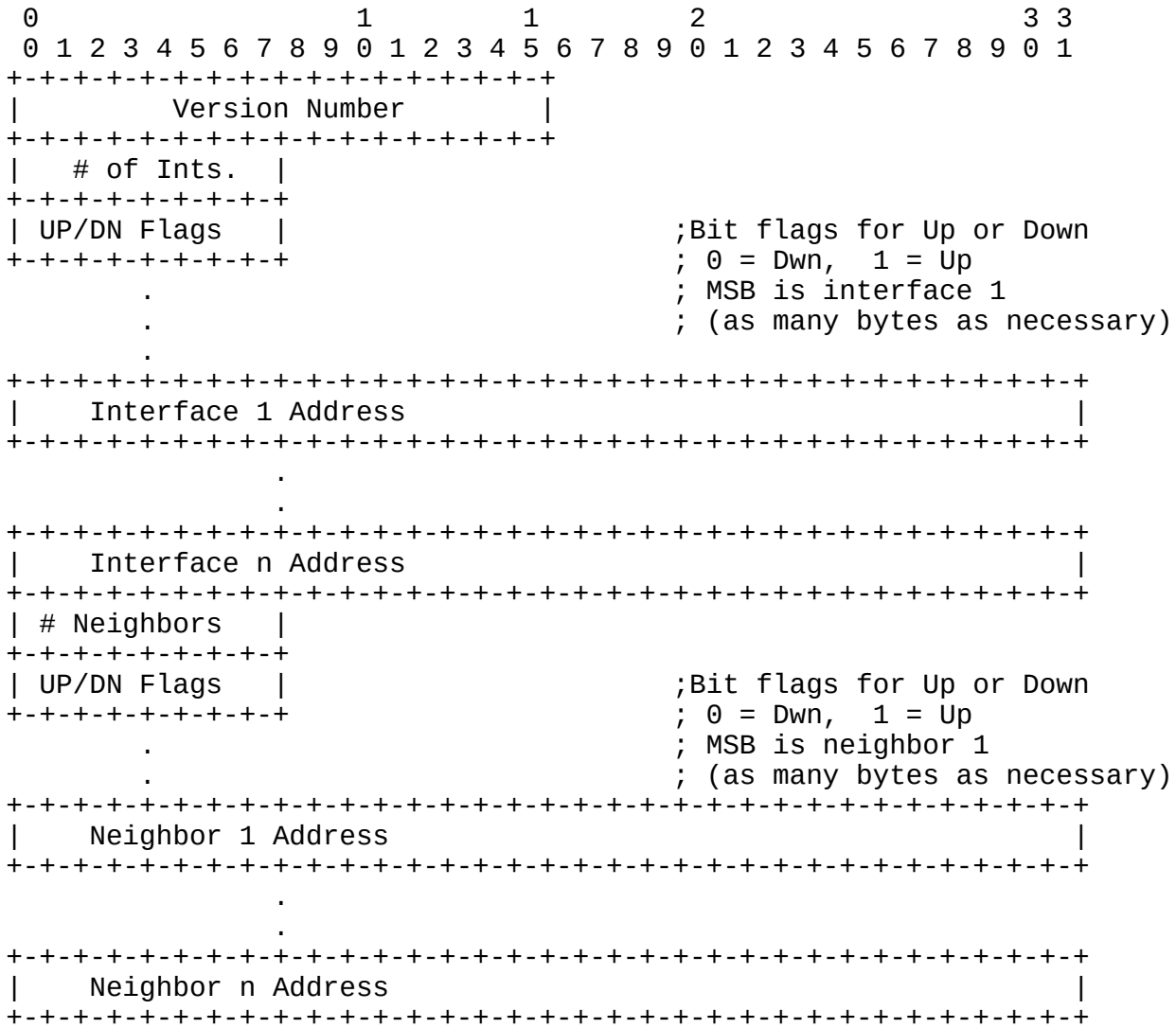
The number of datagrams sent in the Destination to Source address direction.

C.6 Message Type 6: Gateway Routing

Description

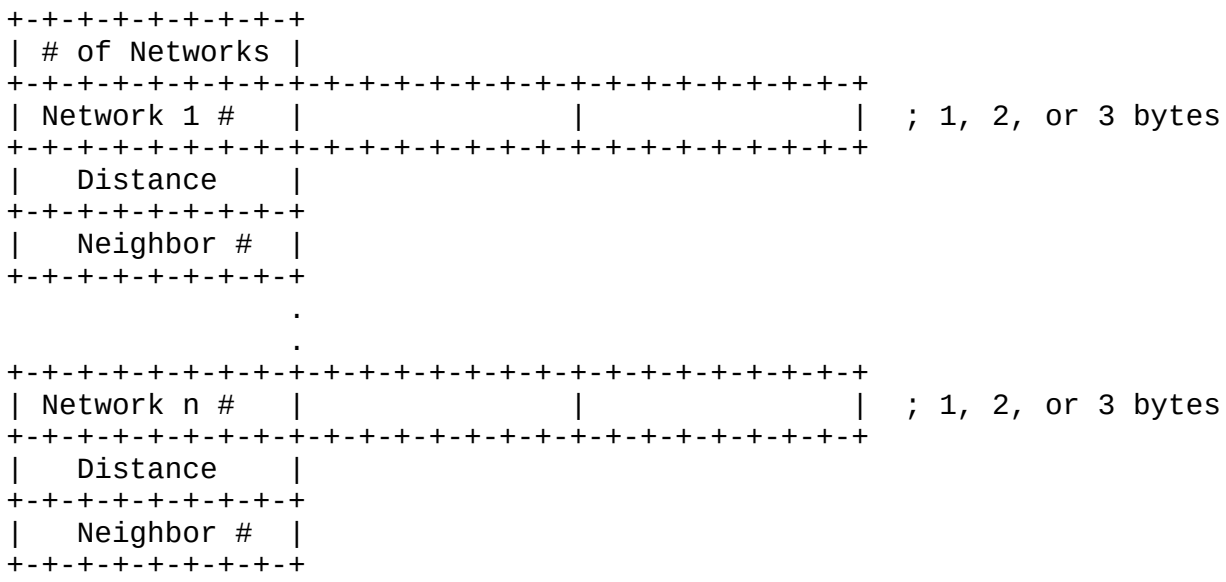
The Routing message contains information about routes the gateway has to the networks that make up the Internet. It includes information about its interfaces and its neighbor gateways.

A Gateway Routing message has the following format:



(continued)

Gateway Routing Message (cont'd.)



HMP FIELDS

System Type

Gateway = 4

Message Type

Gateway Trap Message = 6

Port Number

Unused

Control Flag

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.

GATEWAY ROUTING FIELDS

Gateway Version #

The software version number of the gateway sending the trap.

INTERFACE FIELDS

The first part of the routing message contains information about the gateway's interfaces. There is data for each interface. The fields are:

# of Interfaces

The number of interfaces that this gateway has.

UP/DN Flags

Bit flags to indicate if the Interface is up or down.

Interface Address

The Internet address of the Interface.

NEIGHBOR FIELDS

The next part of the routing message contains information about this gateway's neighbor gateways. The fields are:

# of Neighbors

The number of gateways that are neighbor gateways to this gateway.

UP/DN Flags

Bit flags to indicate if the neighbor is up or down.

Neighbor Address

The Internet address of the neighbor gateway.

NETWORK ROUTING FIELDS

The last part of the routing message contains information about this gateway's routes to other networks. This includes the distance to each network and which neighbor gateway is the route to the network. The fields are:

# of Networks

The number of networks that are reachable from this gateway.

Network #

The network number of this network. This is the network part of the Internet address and may be one, two, or three bytes in length depending on whether it is a Class A, B, or C address.

Distance

The distance in hops to this network. Zero hops means that the network is directly connected to this gateway. A negative number means that the network is currently unreachable.

Neighbor #

The neighbor gateway that is the next hop to reach this network. This is an index into the previous information on this gateway's neighbor gateways. This field is only valid if the Distance is greater than zero.