

CMCC PERFORMANCE MEASUREMENT MESSAGE FORMATS

IEN 157

David Flood Page

Bolt, Beranek and Newman Inc.

50 Moulton Street

Cambridge, Massachusetts 02238

(617)491-1850

26 September 1980

## TABLE OF CONTENTS

	Page
1. PREFACE	1
2. INTRODUCTION	2
3. MESSAGE FORMATS	3
3.1 CPU Idle Time - report type 8	4
3.2 Packet delay - report type 9	4
3.3 Gateway to gateway delay - report type 10	5
3.4 Bit Throughput - report type 11	7
3.5 Queue occupancy - trap type 3	8

1. PREFACE

TABLE OF CONTENTS

This document describes the message formats for the performance measurement reports and traps which are to be added to the ARPA CMCC gateway monitoring messages. It is an addendum to the Gateway Monitoring Protocol described in IEN 131, which should be consulted first. Processing for the new reports and traps will be added to the CMCC, and a document describing their use will be issued later.

3	MESSAGE FORMATS	3
4	3.1 CPU Idle Time - report type 8	3.1
4	3.2 Packet delay - report type 9	3.2
5	3.3 Gateway to gateway delay - report type 10	3.3
7	3.4 Bit Throughput - report type 11	3.4
8	3.5 Queue occupancy - trap type 3	3.5

## 2. INTRODUCTION

The message types described here will be used in two ways: either experimentally, in conjunction with message generators used to load the Catenet until something breaks, or regularly as are the other report types, to show how the Catenet is behaving at any time.

In evaluating Catenet performance, message generators will be required to load the gateways with traffic until packets are dropped, the delays start to rise steeply, or the throughput saturates. These conditions indicate that the limit of some resource has been reached. These message generators, whose implementation is yet to be defined, can be located in either the gateways, the CMCC program, or in other internet hosts. When both the CMCC program and the gateways implement the new message types, and message generators are defined and implemented, the CMCC will be able to find out how much traffic the gateways were processing, where the bottlenecks lie in the Catenet, and what the accompanying delays were.

All the measures described here are cumulative from the time the gateway started. The CMCC will, by keeping suitable histories of the measures, be able to show shorter term values as required.

### 3. MESSAGE FORMATS

All gateway monitoring messages consist of an Internet header followed by a monitoring header, and then the message data. A monitoring header, as described in IEN 131, has the following format:

Bits	Contents
0	0 - Report or trap. 1 - Negotiation message.
1	0 - Report. 1 - Trap.
2-3	For a negotiation message: 0 - DO 1 - DONT 2 - WILL 3 - WONT For a report or trap: zero.
4-7	Reserved.
8-15	Report or trap type.
16-31	For a negotiation message: report identifier. For a regular report: Sequence number. For a trap: data depending on trap type, i.e. this field is not part of the header for a trap message.

The five new message types are:

- o CPU idle time (which gives a measure of how heavily the gateway is loaded).
- o Packet delay across a gateway.
- o Gateway to gateway delay (round trip time).
- o Throughput (bits).

- o Queue traps (which signal when the occupancy of a queue goes above or below a certain threshold value).

### 3.1 CPU Idle Time - report type 8

CPU idle time gives an idea of the amount of time the gateway machine is not doing useful processing. The purpose of this is to find out when the CPU becomes saturated, which will be the case if the proportion of idle time becomes very small. The report consists of two 32-bit counts following the monitoring header:

1. The amount of CPU idle time since the gateway started, in milliseconds.
2. The time since the gateway started, in seconds.

### 3.2 Packet delay - report type 9

Packet delay refers to the length of time a packet stays in the gateway. The measurement of this delay and of gateway to gateway delay are related: measurement of one begins where the other ends. The model used here assumes that gateway processing takes place in three parts: network I/O, queuing and routing. Implementation considerations will affect just where the packets can be timestamped on their way through the gateway, so that for some gateways it may be possible to stamp a packet at the network I/O level, while for others it may not be possible until the

packet enters the routing processing. This specification therefore does not define where the boundary should lie, but it is important that together the measures account for all the delay that a packet will experience as far as the gateway is concerned. It is recommended that the packet delay be made to refer to as large a fraction as possible of the time the packet spends in the gateway. The report consists of two 32-bit counts and two 16-bit counts. All delays are in milliseconds. The format is:

1. The total number of packets processed since the gateway started (32 bits).
2. The total delay for all packets processed (32 bits).
3. The minimum delay experienced by a single packet (16 bits).
4. The maximum delay experienced by a single packet (16 bits).

### 3.3 Gateway to gateway delay - report type 10

The measurement of this delay and of packet delay are related: see the first paragraph in the previous section.

This report could be something of an interim measure, provided the gateways obtain radio synchronizing equipment for measuring the one-way delay directly. However, currently only the round trip delay can be determined. The report assumes that gateways will use some kind of tagged echo packets to find the

round trip delay to each of their neighbors, the tagging being used to identify specific packets.

The report format is a table ordered by internet address considered as a 32-bit unsigned integer. Each table entry consists of an internet address followed by two 32-bit counts and two 16-bit counts. The internet address is the neighbor address for which this delay applies. Of the 32-bit counts, the first is the cumulative total of the echo packets returned by the neighbor since this gateway started, and the second is the total delay experienced by those returned packets, in milliseconds. The two 16-bit counts are the minimum and maximum delays, in milliseconds, for a single packet sent to the neighbor. There will be one table entry for each neighbor address, so that if a gateway is a neighbor on two networks then it will have two table entries. There will be an entry for each such address for each neighbor that replies to the echoes, whether or not that neighbor is a routing gateway. The table size may grow as new neighbors come up while a gateway is running, but it may not shrink; the entry for a gateway that stops replying will simply remain unchanged.



The report format is therefore:

```

Internet address of first neighbor,
  lowest network number
Total of echo packets returned by this neighbor
  (32 bits)
Total delay experienced (32 bits)
Minimum delay to this neighbor (16 bits)
Maximum delay to this neighbor (16 bits)
.
.
Internet address of last neighbor,
  highest network number
Total echo packets returned (32 bits)
Total delay (32 bits)
Minimum delay for this neighbor (16 bits)
Maximum delay for this neighbor (16 bits)

```

#### 3.4 Bit Throughput - report type 11

In contrast with the packet throughput report type, which has its emphasis on the number of packets a gateway can process, the bit throughput report type focuses on how fast a gateway's network connections can accept or deliver data. The report is a table of pairs of 32-bit counts ordered by interface; the first count in each pair is the cumulative total of bits processed coming in at that interface, and the second is the output count. Interfaces are ordered as in the gateway description message, report type 0. There are two extra 32-bit counts at the end of the message: the first is the total of bits dropped, and the second is the time since the gateway started, in seconds. The counts for the interfaces include all traffic at that interface, including control traffic and messages originating at the

gateway.

The format of the message is therefore:

```
Input count for first interface
Output count for first interface
.
.
Input count for nth interface
Output count for nth interface
Dropped count
Time since gateway up
```

### 3.5 Queue occupancy - trap type 3

This is a trap message which is sent by the gateway whenever a queue length exceeds a threshold percentage specified in the trap request message, or when the occupancy falls below that threshold after having been above it for some time. If a queue is loaded such that the threshold occupancy is continually being passed in each direction, a large number of these traps would be generated in a short time. To avoid this, there should be some minimum time interval between successive trap messages. It is left up to the individual gateway implementors to decide what this time interval should be; experience with using this trap type will probably suggest a reasonable value.

Note that this replaces the earlier Queue full trap described in IEN 131. I believe that a percentage occupancy trap is more useful because if a queue becomes full, the gateway is

probably already dropping packets and the message is not useful as an early warning. In any case, a queue full trap is just a 100% percentage occupancy trap.

The DO TRAP message for this trap type requires an extra piece of information: the percentage occupancy of the queue which is to trigger the trap. This is expressed as an integer in a single byte following the report id field in the DO TRAP message. A gateway should only use one value of this threshold at a time, so that a second DO TRAP message will supersede the previous one if the threshold value is different.

The DO TRAP message for this trap type has the format:

Bits	Contents
0	1
1	1
2-3	0
4-7	0
8-15	3
16-31	report identifier
32-39	occupancy threshold

The trap message has the following format:

Bits	Contents
0-7	Interface number of Queue.
8-11	Input(0) or output(1) queue.
12-15	Above(0) or below(1) the specified occupancy.
16-23	The occupancy percentage used as a trigger.