EUROCONTROL

ATNP/WG2/WP524
17/3/99

AERONAUTICAL TELECOMMUNICATIONS NETWORK PANEL

WORKING GROUP TWO

Naples, Italy 18.5.99 – 20.5.99

# ATN Performance Management Requirements Analysis

**Presented By Tony Whyman**

**Prepared by Tony Whyman**

SUMMARY

This paper is concerned with the derivation of Performance Management Requirements for the ATN Internet. A top down analysis is presented, first identifying the objectives for Performance Management and then going on to look at how these objectives are met, from which system and tool requirements can be derived.

It should be noted that this analysis does not attempt to determine how difficult or costly each identified requirement is to implement.

# TABLE OF CONTENTS

# 1. Introduction

## 1.1 Scope

This paper is concerned with the derivation of Performance Management Requirements for the ATN Internet. A top down analysis is presented, first identifying the objectives for Performance Management and then going on to look at how these objectives are met, from which system and tool requirements can be derived.

It should be noted that this analysis does not attempt to determine how difficult or costly each identified requirement is to implement.

## 1.2 Purpose of Document

This document has been prepared as a discussion document for use within Eurocontrol and in projects implementing Systems Management services.

## 1.3 References

| | | |
|---|---|---|
| 1. | ICAO DOC9705 | ATN SARPs |
| 2. | ATNP/WG2/WP438 | Performance Management Requirements for the ATN Internet Communications Service |
| 3. | Version 1.4 | ACI and ProATN: Convergent MIB |
| 4. | ATNP/WG2/WP-478 | Preliminary Draft Version 1.0 ATN Systems Management – Concept of Operations |
| 5. | ADSP/4-WP/53 | Draft ICAO Manual of Air Traffic Services (ATS) Data Link Applications |

# 2. Performance Management Objectives

ISO/CCITT defines performance management as follows:

> *Performance management enables the behaviour of resources in the OSIE and the effectiveness of communication activities to be evaluated. Performance management includes functions to*
>
> 1. *gather statistical information;*
> 2. *maintain and examine logs of system state histories;*
> 3. *determine system performance under natural and artificial conditions; and*
> 4. *alter system modes of operation for the purpose of conducting performance management activities.*

In an ATN context, there are three basic purposes for which the above procedures will be conducted:

1. The end-to-end performance will need to be measured in order to ensure that the operational requirements are being met.

2. Users will wish to monitor the performance of Internet Service Providers (ISPs) and subnetwork providers, and, in particular, to assess their compliance with service level agreements (this could be for both Operational and Financial reasons).

3. ISPs will wish to monitor the performance of the network, to ensure that they are maintaining service level agreements, to ensure that the network capacity will match future requirements (Capacity Planning), and to ensure that the service that users require, is being provided in the most cost effective manner.

It should be noted that the end-to-end service may be provided by many ISPs operating in serial.

In order to determine the Performance Management Objectives, it is thus necessary to look at each of the above purposes, to identify the performance monitoring points, and to consider the different relationships between ISPs. In particular, service agreements will relate to path segments though the ATN Internet and a given path segment may be maintained by more than one ISP in series. The performance management models that result from scenario this need also to be considered.

## 2.1 Performance Monitoring Points

Figure 2-1 Illustrates the various performance monitoring points (PMPs) that are required.

1. The **End to End Service** measures the end-to-end service provided to an application. Performance monitoring is required here in order to verify that the end to end service meets the operational requirement.

2. **End System Monitoring** is required to determine the part of the end to end overhead attributable to the End System itself. This should be a small component of the overall end-to-end figure, but this still needs to be demonstrated.

3. **Path Segment Monitoring** is required to monitor the performance of ISPs and to measure the contribution of the end-to-end overhead of the routers and subnetworks operated by an End User.

4. **Router Performance Monitoring** is required to measure the performance of individual routers and to determine their contribution to the end-to-end overhead.

5. **Subnetwork Performance Monitoring** is required to monitor the compliance of subnetwork providers with performance level agreements and to measure the contribution of each subnetwork to the end-to-end overhead.

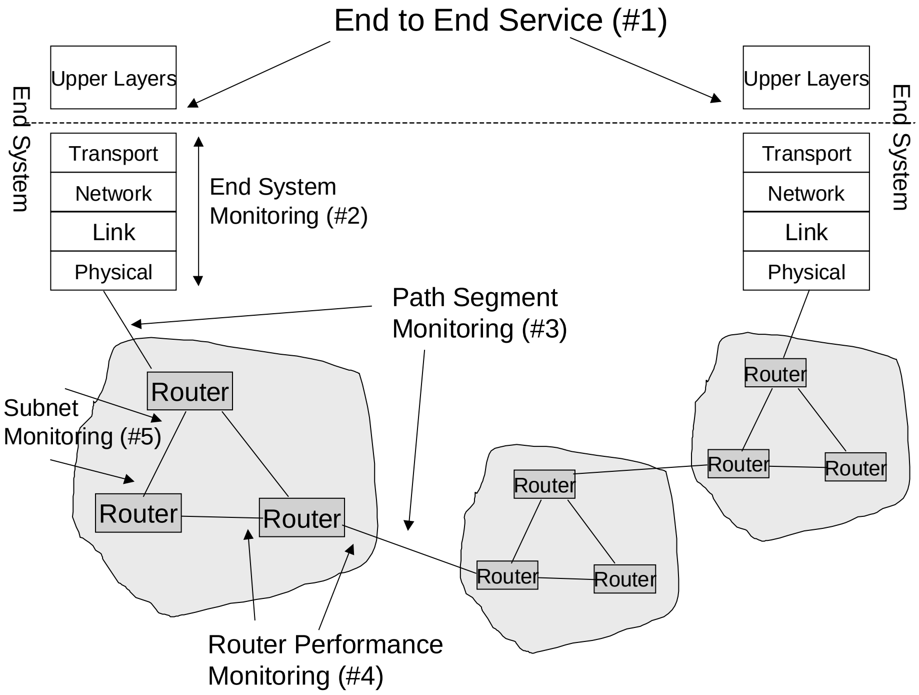

**Figure 2-1 Performance Monitoring Points**

## 2.1.1 End to End Service Monitoring

An end user of the ATN (typically a CAA or Airline) is interested in ensuring that the required end-to-end Quality of Service is being maintained. At the same time, they will also have an Accounting Management objective to monitor the cost of using the ATN, and, whilst this is a different subject, the data capture requirements will be similar.

The end-to-end quality of service can be broken down into the following parameters:

1. **Availability**: "The ability of a system to perform its required function at the initiation of the intended operation. It is quantified as the proportion of the time the system is available to the time the system is planned to be available".[1]

2. **Reliability**: "The probability that the system will deliver a particular message without errors."

3. **Continuity**: "The probability of a system to perform its required function without unscheduled interruptions during the intended period of operations."

4. **End-to-End Transfer Delay**: "The period elapsed from the time at which the originating user initiates the triggering event until the time the transmitted information has been

1.

[1] The definitions for availability, Reliability, Continuity, Transit Delay and Integrity are taken from the draft ADSP Manual.

received by the intended recipient." *Note that this can vary according to message priority, and ATSC Class.*

5. **Integrity**: "The probability that errors will be mis-detected. This may be when a correct message is indicated as containing one or more errors, or when a message containing one or more errors is indicated as being correct."

6. **Throughput: "**The quantity of data (e.g. measured in characters) that can be sent during a given period."

7. **Connection Establishment Delay:** "The time from initiating an end-to-end connection to its successful establishment (i.e. when messages can be sent)."

The end user's objective is to be able to measure each of the above Quality of Service metrics on an end-to-end basis i.e. for a dialogue with each other end user of the ATN with which they communicate. **[Objective 1]**

### 2.1.2 End System Monitoring

End Users typically own and operate the End Systems that form the first part of the chain of end to end communications. They will also need to monitor the internal performance of these systems. This is so that the performance of these systems can be monitored and hence so that the actual performance provided by the ISP(s) used for end-to-end communications can be calculated. **[Objective 2]**

### 2.1.3 Subnetwork Service Monitoring

*Note: An ATN ISP or end user may also operate subnetworks and hence wish to monitor their internal operation. However, the internal monitoring of subnetworks is outside of the scope of this paper.*

An ISP or End User will need to monitor the operation of each subnetwork they use in order to ensure that the expected/required Quality of Service is being maintained. **[Objective 3]**

The Quality of Service metrics to be measured are very similar to those for the end-to-end service and will always include: Availability, Reliability, Continuity, Transit Delay, Integrity and throughput. In addition, there will be subnetwork specific metrics. A connection mode subnetwork (e.g. X.25) will have a connection setup delay metric, while a Frame Relay circuit has only a maximum guaranteed throughput, with the possibility of data loss, and hence the data loss rate will need to be monitored and compared with offered traffic load.

### 2.1.4 Path Segment Monitoring

An ISP or End User will need to monitor the overall performance of each path through their segment of the ATN Internet **[Objective 4]**. The metrics measured will be those specific to a connectionless service i.e. Throughput, Reliability, Integrity and Transit Delay.

Performance achievement will also need to be measured against the theoretical maximum so that excess capacity can be removed **[Objective 5]**. Trend analysis will also need to be performed so that future growth can be predicted and hence future capacity growth planned and installed when needed **[Objective 6].**

ISPs and End Users may also wish to manage their capacity dynamically. This make take the form of bringing on additional capacity to meet busy hour requirements, according to a defined schedule, or simply be reacting to reports of congestion by opening up new circuits. **[Objective 7]**

### 2.1.5 ATN Router Performance Monitoring

General ATN Router performance may be considered in two separate parts: forwarding and route updates. There are also special considerations for Air/Ground Router Performance.

#### 2.1.5.1 Packet Forwarding

An ISP or End User will need to monitor the following packet forwarding metrics **[Objective 8]**:

1. Packets successfully forwarded during a given measuring period (e.g. per second)

2. Percentage of packets discarded.

As the service level requirements can vary by both ATSC Class and priority, these metrics will need to be broken down by both ATSC Class and priority.

Key parameters of the router that affect forwarding need also to be measured. These include the size of the Forwarding Information Base (FIB). **[Objective 9]**

#### 2.1.5.2 Routing Updates

An ISP or End User will need to monitor the route convergence rate. That is the time taken from a change in the network topology to this change being reflected in all affected routing tables **[Objective 10]**.

This metric is important in the maintenance of Availability, Reliability and Continuity targets as packet loss can occur during this period. The target convergence rate may be derived empirically or from simulation models.

#### 2.1.5.3 Air/Ground Routers

Ground/Ground Routers typically support a limited number of fixed adjacencies. However, Air/Ground Routers will support a large and variable number of adjacencies with aircraft, with each adjacency supported by one or more virtual circuits. The performance of the router may be affected by the number of such adjacencies maintained, and performance will thus need to be measured against the adjacencies and virtual circuits supported. It will thus be necessary to monitor the number of air/ground virtual circuits supported at any one time, and the number of IDRP adjacencies. **[Objective 11]**.

## 2.2 Performance Management

Service guarantees will need to be put in place to ensure that the end-to-end Quality of Service required to meet the operational requirements is achieved. When this service is provided vai multiple ISPs in serial, there are two possible models for maintenance of the end-to-end Quality of Service:

1. The end user(s) have separate service level agreements with each ISP that support (in serial) the end-to-end path.

2. The end user(s) have a single service agreement with one ISP who is also responsible for the service provided by any other ISP en route.

### 2.2.1 Separate Service Level Agreements

Whilst this model is, on first appearances, easier for the ISPs to operate, it pushes the complexity onto the end user, who has to be aware of the paths that their data takes, and who is required to negotiate with each ISP en route. This potentially makes for many small contracts between users and ISPs. It may thus be more costly to implement because of this contractual overhead.

In this model, each ISP will need to be able to demonstrate to an End User that they are meeting the service requirement for the path segment under their control. It will thus be necessary to monitor incoming packets from either users or other ISPs and analyse them by sending end user. Similarly, the ISP will need to analyse traffic at each exit point. **[Objective 12]**

Analysis of traffic by source is potentially a very costly exercise as each packet has to be metered.

### 2.2.2 Single User Service Agreements

This model can be operated in two different ways, which can be labelled as microscopic or macroscopic. In the microscopic view, one ISP simply becomes the “agent” of an end user, and organises the separate contracts with each other ISP en route. In order to monitor compliance, each data flow will still need to be identified as above, and the end user’s agent will collate the information together and monitor the overall performance, as above

In the macroscopic view, an ISPs will aggregate together the traffic from all of their users and thence identify the traffic volumes it will exchange with each other ISP. On the basis of agreed traffic volumes, the ISPs may then guarantee minimum service levels to each other. A given ISP may then offer a service guarantee to its end user, and base this guarantee on the knowledge of which ISPs lie on the route and by summing the guaranteed minimum service levels.

The macroscopic view is simpler to achieve because it requires only that each ISP monitors its own part of the ATN Internet (as in 2.1.4 above). However, it will probably need to be co-ordinated through an industry forum that will also receive, collate and monitor the overall service provided to end users. [**Objective 13]**

# 3. Fulfilment of Objectives

As presented below, there is a general requirement to log events locally for later, offline, analysis **[Req 1]**. Unless stated explicitly, all requirements to log or record events given below imply a local log.

## 3.1 Objective 1: End User QoS Measurement

The end user will need to be able to monitor each of the QoS metrics identified in 2.1.1 above.

### 3.1.1 Availability

In order to determine the percentage availability according to the above definition, the end user will need to record each successful attempt to use the service **[Req 2]** and each failed attempt **[Req 3]**. Analysis of such a record can then determine the percentage availability. **[Req 4]**

### 3.1.2 Reliability

In order to determine the probability that a message is delivered without errors it will be necessary to record both the number of messages sent to a given destination **[Req 5]** and those received with errors by that destination, analysed by sender **[Req 6]**. Comparison of these two records may then determine the percentage reliability. **[Req 7]**

### 3.1.3 Continuity

In order to determine the continuity, it will be necessary to record each service interruption and each corresponding resumption of service **[Req 8]**. For the end-to-end service, a service interruption event can be equated to the uncommanded loss of a transport connection, and service resumption to the successful re-establishment of such a transport connection. Analysis of this log can determine the continuity level achieved. **[Req 9]**

### 3.1.4 End-to-end Transit Delay

End-to-end transit delay could be measured by recording the transmission time of each message, and the reception time of each message, at each end of the connection. Comparison of these two records can then determine the actual transit delay provided that both end users have synchronised clocks.

However, synchronised clocks can be an impractical requirement, and logging the transmission of each message is expensive and will result in large log files. Fortunately, there is a more readily available metric from which end-to-end transit delay can be estimated. This is the round trip delay.

The connection mode transport protocol (TP4) can readily measure the round trip delay from transmission of a TPDU to reception of the corresponding AK TPDU. Simply dividing this figure in two gives an estimate for the transit delay.

In practice, a user message (TSDU) may be split into several TPDUs, and transmitted with overlapping acknowledgements. However, the transit delay for the total message can still be estimated by measuring the delay from the transmission of the first TPDU of the TSDU to the reception of the AK TPDU for the last TPDU making up the TSDU (a TSDU equating to a user message), and then subtracting from this the estimated transit delay for a single TPDU. The result is the estimated transit delay for the whole message.

This is an estimate and each estimation is subject to an error. However, the errors should balance out over several messages. The transport protocol should record the estimated transit delay for each message, transmission time and the size of each message **[Req 10]**. Later analysis of the record can then provide an accurate estimate of the achieved end-to-end transit delay, analysed by message size, and transmission time **[Req 11]**.

### 3.1.5 Integrity

By definition, integrity cannot be measured by the ATN Internet because to measure it implies that the Internet can detect its own mistakes - in which case it can then correct them. Integrity has to be measured by the end user either by comparing messages sent and received at each end of the communications path, or by adding an additional message integrity check on transmission and recording, on reception, the number of messages received correctly and the number received with errors. In the former case, analysis requires access to logs at both end of the communications path while, in the latter case, access is required to only one log.

In practice, it is expected that there will be a data recording requirement for CPDLC messages and possibly messages sent by other applications. This requirement will be for a circular log on an aircraft recording the last two hours of messages. However, this will be sufficient to take a view on integrity. Routine analysis of messages logs can thus be used to provide the integrity metric. **[Req 12]**

Security requirements are also expected to require the use of digital signatures for authentication purposes. A digital signature also provides a high quality integrity check. In practice the most likely reason for authentication failure is an undetected network error. When implemented, authentication failures should be logged as well as numbers of messages successfully received **[Req 13].** The integrity achieved can then be computed from such a record - assuming that a security violation has not taken place **[Req 14]**.

### 3.1.6 Throughput

Throughput achieved can be simply measured provided that a log of each message sent (size and time of transmission) over each communications path is maintained **[Req 15]**. Throughput achieved can therefore be determined by analysis of the log **[Req 16]**.

### 3.1.7 Connection Establishment Delay

In the ATN, there are two possible measures of connection establishment delay. One is the time taken to establish a transport connection, and the other is the time taken to establish a connection using the Dialog Service. The second may be significantly longer than the former, as it usually requires an exchange of messages after the transport connection has been established - although this can be avoided in some cases.

The time taken to establish a transport connection is the proper measure for the performance of the ATN Internet. However, the end user only sees dialog service connection establishment time. On the other hand, the problem of using this as a metric is that it includes the response time of the remote application. It therefore is not a correct estimate of the performance of the ATN Internet.

Arguably, both metrics need to be recorded and analysed. Therefore, an ATN End System will need to log both dialog service D-STARTs **[Req 17]** and transport connection connect requests **[Req 18]**, and the time at which the request was made. Similarly, an ATN End System needs to log the time at which the connection was successfully established **[Req 19]**. Later analysis can then determine the mean for both logs **[Req 20]**.

## 3.2 Objective 2: End System Monitoring

In order to monitor End System Performance and to quantify the performance of ISPs, the operator of an End System will need to know:

1. At the Internet level, the number and size distribution (mean and max) of packets sent and received, analysed by priority and ATSC Class **[Req 21]**. When the End System is connected to multiple ISPs, the above will need to be broken down by ISP as well.

2. The transit delay of a packet through the End System (incoming and outgoing) **[Req 22]**. *Note that this need not be measured all the time, but could be measured during system testing and then taken as a system characteristic.*

This information will enable the computation of the traffic load on the End System and the load applied to each ISP **[Req 23]**. The per packet transit delay needs to be subtracted from the end-to-end transit delay in order to compute the ISP transit delay.

## 3.3 Objective 3: Subnetwork Service Monitoring

It is not possible to deal with all aspects of subnetwork monitoring without considering each type of subnetwork. This paper seeks only to establish the generic requirements. Specific subnetwork monitoring requirements will need to be determined on a case by case basis.

### 3.3.1 Availability

In order to determine the percentage availability of a subnetwork, the subnetwork user will need to record each successful attempt to use the service and each failed attempt **[Req 24]**. Analysis of such a record can then determine the percentage availability **[Req 25]**.

### 3.3.2 Reliability

In order to determine the probability that a packet is delivered without errors it will be necessary to record both the number of packets sent and received over a subnetwork **[Req 26]**. Comparison of these two records may then determine the percentage reliability **[Req 27]**.

### 3.3.3 Continuity

In order to determine the continuity, it will be necessary to record each service interruption and each corresponding resumption of service reliability **[Req 28]**. For connection mode subnetworks, a service interruption event can be equated to the uncommanded loss of a subnetwork connection, and service resumption to the successful re-establishment of such a connection. For connectionless subnetworks a service interruption can be equated to a transmission failure, with service resumption being the time of the next successful transmission attempt. (Note that on some connectionless subnetworks, it may not be possible to detect transmission failure).

Analyis of the logs can then determine the outage time and the period between outages and hence the continuity of service provided by the subnetwork **[Req 29]**.

### 3.3.4 End-to-end Transit Delay

There is no general purpose mechanism to measure transit delay over subnetworks. A connectionless network, such as an Ethernet, has no acknowledgement and transit delay can only be measured by using special link level test packets to “echo back” a response and thereby derive the transit delay from the round trip time.

On the other hand, a connection mode subnetwork, such as X.25, does provide an acknowledge, but this is not necessarily end-to-end across the subnetwork and has no real-time constraints. It is thus unsuitable for measurement of transit delay.

The CLNP Echo is potentially available to provide an estimate of round trip delay between a pair of Routers or a Router and an End System attached to the same subnetwork. However, the processing delay within the target system is potentially significant and will need to be independently measured and factored out. Furthermore, CLNP echo is of limited value when more than one subnetwork joins the same pair of systems, as it is not possible to guarantee which subnetwork is used to transfer the Echo packet.

A strategy for measurement of transit delay will need to be developed for each type of subnetwork. For connectionless subnetworks, or wide area networks involving multiple hops, this will need to be based on some kind of subnetwork specific echo packet. For single hop connection mode networks this may use the subnetwork's own acknowledgement procedures.

For example, in VDL Mode 2, the air/ground data link uses a connection mode variant of HDLC (the AVLC) which could be used to measure round trip time and hence to estimate transit delay.

### 3.3.5 Integrity

Data integrity problems can be measured by two ATN mechanisms: the CLNP Header Checksum and the Deflate checksum - when Deflate based compression is used. The Deflate checksum provides an integrity check over the entire packet and is therefore a very good check on integrity. The CLNP Header checksum only covers the CLNP header and its generation by a sending End System is not mandatory in the ATN SARPs. It is therefore of more limited value.

A record should be kept of the number of packets received over a subnetwork and those received with a failed CLNP Header checksum, or a Deflate checksum failure, when Deflate is used **[Req 30]**. Later analysis of the log can then estimate the subnetwork undetected error rate **[Req 31]**.

### 3.3.6 Throughput

Throughput achieved can be simply measured provided that a record of each packet sent (size and time of transmission) over each communications path is maintained **[Req 32]**. Offline analysis of this record may then be used to determine throughput. **[Req 33]**

### 3.3.7 Connection Establishment Delay

For connection mode subnetworks, the time at which each subnetwork connection is initiated and the time of successful establishment should be recorded **[Req 34]**. Later analysis of the record can then be used to determine the subnetwork connection establishment delay **[Req 35]**.

## 3.4 Objective 4: Measurement of Path Segment Performance

The requirements for measuring path segment performance are related to the performance management model adopted. They are hence discussed in 3.11 below.

## 3.5 Objective 5: Monitoring for Excess Capacity

Excess capacity occurs when there exist underused data links. These could potentially be removed or replaced by less performant and lower cost data links.

Two metrics are required to determine excess capacity: the actual throughput over each subnetwork (peak) and the available throughput. When the peak throughput is significantly lower than the available throughput then the data link may be eliminated if a suitable (and also underused) alternative exists. Alternatively, it could be replaced by a lower cost/capacity subnetwork. The throughput threshold when a lower cost/capacity subnetwork is realistic needs also to be known.

Subnetwork throughput is determined from subnetwork monitoring (see 3.3.6). The available throughput and the threshold for downgrading to a lower cost/capacity subnetwork are required to be known *a priori.* A monitoring tool should be available to monitor subnetwork utilisation and report on candidates for downgrading **[Req 36]**.

## 3.6 Objective 6: Planning Future Capacity

Capacity planning requires the development of a network design model **[Req 37]**. This will comprise the Routers, subnetwork interconnections and predictions of data flows through the internetwork, with both normal and busy hour profiles required. From this model, the capacity requirements of subnetwork connections and Routers can be predicted.

In the ATN, the Network Design Model is complicated by the existence of ATSC Class which restricts the options for data flow. It will also be necessary to use the model to predict behaviour during outages. For this reason, more than a simple static model may be required, in order to simulate the impact of subnetwork connection and Router loss, and to demonstrate that there is sufficient capacity to maintain the required Quality of Service to high priority applications during such failures.

The model will require good quality information on the expected traffic flows if it is to be useful. Furthermore, accurate predictions of future traffic levels will be necessary if it is to be used to plan the growth of the network. This requires capture of information on current network loading and analysis of historical network performance information in order to perform trend analysis and hence to predict future growth.

The following data is thus required to be recorded during daily operations and kept for historical analysis:

1. Data volumes for each subnetwork on a point to point basis and during each sample period **[Req 38]**.

2. Data volumes (both bytes and packets) handled by each Router during each sample period **[Req 39]**.

The above needs to be analysed by priority and ATSC Class.

## 3.7 Objective 7: Dynamic Capacity Management

There are three requirements that flow from this. The first is a need for an indication that the packet flow rate over a given subnetwork has increased beyond some threshold that implies a need for additional capacity. The second is a corresponding indication that the additional capacity is no longer required, and the third is the means to bring on new capacity.

### 3.7.1 Indicating the need for Additional Capacity

The first indication that the applied load is reaching the limits of the subnetwork will be an increase in the queuing delay for packet transmission over that subnetwork. This could be measured as either the absolute queuing delay per packet, or, perhaps more easily, as the average queue length during a sample period. As queue length is proportional to queuing delay, this should be sufficient.

An alternative mechanism might be to measure the actual throughput over some period and compare it against the maximum achievable. However, this requires knowledge of the maximum achievable throughput and, as this is not necessarily a constant (if the subnetwork includes an element of statistical multiplexing), this can be difficult to predict accurately. This can be further complicated if more than one subnetwork is already used to support a router to router adjacency.

Average queue length is thus the preferred mechanism for determining when an event should be generated requesting additional capacity. As the quality of service requirements can differ by priority, there may need to be different reporting thresholds for different priority bands **[Req 40]**.

### 3.7.2 Indicating When Additional Capacity is no longer Needed

The inverse of the above may be readily adopted as the signal that indicates when capacity may be reduced i.e. when the average queue length drops below some threshold, However, the normal queue length (i.e. when load and capacity are in balance) will be between zero and one. Therefore, the measure of average queue length will have to be a real number if it is to be useful **[Req 41]**.

Alternatively, if throughput levels are used to determine when the additional capacity is to be withdrawn, then throughput monitoring should also be used to determine when the additional capacity is to be withdrawn.

### 3.7.3 Adding and Removing Additional Subnetwork Capacity

This is a need for Systems Management Actions to bring up new subnetwork connections or to remove existing subnetwork connections in response to the above events. While these actions could be invoked by a remote manager, the simplest implementation is probably to have a local response (i.e. within the Systems Management Agent) **[Req 42]**.

## 3.8 Objective 8: Router Forwarding Measurement

In addition to the data forwarded by a Router, as required above, a complete assessment of the Router's performance will also require that packet discards are recorded and analysed by discard reason **[Req 43]**.

If the reason for packet discard is "congestion", then this may be indicative of a lack of network capacity. There is thus a need to report, to a Network Manager, when the number of such discards exceeds a given threshold during a reporting period **[Req 44]**.

## 3.9 Objective 9: Router Key Parameters Measurement

The key parameters of the Router that affect forwarding must also be measured. This may include system specific parameters **[Req 45]** (e.g. memory utilisation) and the number of entries in the Forwarding Information Base (FIB) **[Req 46]**.

## 3.10 Objective 10: Measurement of Route Convergence Times

The measurement of Route Convergence Time requires that each Router records each routing event for collection and later analysis **[Req 47]**. Furthermore, so that routing events in different routers can be correlated, each must have a synchronised clock **[Req 48]**.

An offline tool will be required to perform the analysis. This will analyse the logs provided by each Router and correlate routing events between routers. This tool will be required to determine the time taken from each change in the network topology to a stable routing set being reached in every router, including the elimination of any false routes that may have been introduced as a consequence of the change.

Trend analysis of route convergence rates will also be necessary against historical data in order to predict the need for higher performance routers. This is so that the convergence rate does not increase to the point at which the end-to-end Quality of Service falls below acceptable levels **[Req 49]**.

## 3.11 Objective 11: Air/Ground Router Overhead Measurement

An Air/Ground Router will need to log:

1. Establishment and termination of adjacencies with Airborne Routers **[Req 50]**.

2. Establishment and termination of subnetwork connections with Airborne Routers**[Req 51]**.

A tool will be required to analyse such logs and thus to determine the numbers of such adjacencies and subnetwork connections at any one time and to compare this against the monitored performance of the router. The maximum number of adjacencies and subnetwork connections that can be maintained without significantly impacting performance can then be determined, and hence the need for future capacity planned **[Req 52]**.

## 3.12 Objective 12: Analysis of Data Stream Performance

*Note: The need for this objective depends upon the model for service level agreements developed by the industry.*

If the performance assessment mechanism adopted by the ISP requires that data flows are individually monitored, then the ISP will need to demonstrate compliance with Quality of Service metrics for a given user's data flows. In turn, this requires identification and metering of data flows on both entry to and exit from the ISP.

The metrics to be monitored are those appropriate to a connectionless internet i.e. Transit Delay, Integrity, Throughput and Reliability **[Req 53]**.

The metering of packets (both by number and size) on entry and exit can be used to assess both throughput and reliability. Note that as different service levels may apply to different priorities and ATSC class, data flows may require separate meters by priority and ATSC Class.

Throughput can then be measured by direct computation of the metered values. An assessment of reliability can be gained by comparing counts of packets that entered the ISP's network with those on exit **[Req 54]**.

Measurement of transit delay is not quite so straightforward. The "brute force" approach would be to log each individual packet on entry and exit and to record the time of entry and exit, using synchronised clocks. Offline analysis could then compute the transit delay for each packet and hence the average transit delay, etc.

However, this approach would be computationally expensive and is not readily justifiable. Instead two approaches are possible:

1. A sample of such packets is logged. The sampling procedure could use some algorithm based on the packet identifier in order to select packets for logging and this would guarantee the same packets were selected. The approach is basically the same as the brute force approach, but it does reduce the amount of data to be logged and processed.

2. Periodic echo packets are sent on the data flow. These can be used to directly compute the round trip delay and hence derive the transit delay.

As the computational effort is much lower, the use of periodic echo packets for transit delay monitoring is to be preferred. The echo packets will need to be sent at various ATSC classes and priorities in order to determine the service levels for each ATSC class and priority **[Req 55]**.

## 3.13 Objective 10: Monitoring of Service Provider Compliance by Aggregate Data Flows

*Note: The need for this objective depends upon the model for service level agreements developed by the industry.*

In the macroscopic view, the ISP is interested only in the total data flow at each entry and exit point. There is no analysis to the level of individual data flows. In general, this objective requires less computational effort than Objective 9 and hence this is why it may be preferred.

The metrics to be measured are still the same i.e. Throughput, transit delay and reliability. Again, they may need to be metered by ATSC Class and priority. However, the meters are on aggregate values and not on individual data flows **[Req 56]**.

Total throughput can be calculated from this information as can an overall assessment of reliability. Transit delay will have to be determined by use of periodic echo packets between all entry points and all exit points. The echo packets will need to be sent at various ATSC classes and priorities in order to determine the service levels for each ATSC class and priority **[Req 57]**.

# 4. Performance Management Requirements

The following requirements have been derived from the preceding analysis. It should be noted that there is also an implicit requirement to be able to selectively enable and disable each requirement to log an event.

## 4.1 General

1. All ATN systems are required to keep local event logs for the recording of designated systems management events. Some mechanism must also be provided to transfer these logs to an offline processor. **REQ 1**

2. All ATN Systems are required to log each successful and each unsuccessful attempt to establish a connection over a connection mode subnetwork. **REQ 24**

3. All ATN Systems are required to log the number of successful and unsuccessful attempts to send a packet over a connectionless subnetwork. **REQ 24**

4. All ATN Systems are required to log the number of packets sent and received over each subnetwork or subnetwork connection, and to count the volume of data sent and received, analysed by priority and ATSC Class. **REQ 25, REQ 32, REQ 38**

5. All ATN Systems are required to log the time of uncommanded loss of a subnetwork connection. **REQ 28**

6. When possible, ATN systems are required to log the time of each failure to transmit a packet over a connectionless subnetwork, and time of the next successful transmission attempt. **REQ 28**

7. All ATN Systems are required to keep a count of the number of packets received with a CLNP header checksum failure. **REQ 30**

8. When Deflate is implemented, ATM Systems are required to keep a count of the number of packets received with a Deflate checksum failure. **REQ 30**

9. On each connection mode subnetwork, an ATN system is required to log the time at which each connect request is sent and the time at which the connection is successfully established. **REQ 34**

10. All ATN Systems are required to monitor average queue length analysed by priority during each sampling period, and to generate a notification when the average queue length exceeds a set threshold (high watermark) or drops below another set threshold (low watermark). **REQ 40, REQ 41**

11. When subnetworks or subnetwork connections can be dynamically managed, Systems Management actions are required to be available to activate and deactivate them. **REQ 42**

## 4.2 End System

1. The user application is required to record, in a local log, each successful attempt to establish an end-to-end connection **REQ 2**

2. The user application is required to record, in a local log, each unsuccessful attempt to establish an end-to-end connection **REQ 3**

3. The transport layer is required to record, in a local log, the number and size of user messages sent on each transport connection **REQ 5, REQ 15**

4. The transport layer is required to record, in a local log, the number and size of user messages received on each transport connection **REQ 6, REQ 15**

5. The transport layer is required to record, in a local log, each connect request, and the time at which the connect request was issued. **REQ 17**

6. The transport layer is required to record, in a local log, the time of each successful connection establishment. **REQ 19**

7. The transport layer is required to record, in a local log, each uncommanded transport connection loss. **REQ 8**

8. The transport layer is required to record the measured round trip delay between transmission of a TPDU and its acknowledgement together with an indication of whether the TPDU marks the end of a TSDU. **REQ 10**

9. When authentication is implemented, authentication failures shall be logged. **REQ 13**

10. The Dialog Service is required to record, in a local log, each connect request, and the time at which the connect request was issued. **REQ 18**

11. The Dialog Service is required to record, in a local log, the time of each successful connection establishment. **REQ 19**

12. The number, average and maximum size of CLNP packets sent and received during a reporting period are required to be logged. These are to be analysed by ATSC Class and priority, and by each data link. **REQ 21**

13. The mean transit delay of packets through and End System shall be measured under various loading conditions. **REQ 22**

## 4.3 Router

1. ATN Routers are required to keep counts of packets forwarded and data volumes, analysed by priority and ATSC Class. **REQ 39**

2. ATN Routers are required to log packet discards by discard reason. **REQ 43**

3. When the number of packet discards due to congestion exceeds a defined threshold, then a notification shall be sent to a network manager. **REQ 44**

4. System specific parameters that affect forwarding performance should be logged **REQ 45**

5. Changes to the number of entries in a Router's FIB should be logged. **REQ 46**

6. ATN Routers are required to log each route received and each route advertised to another router, recording the time received/advertised. **REQ 47**

7. ATN Routers are required to maintain synchronised clocks for event logging purposes. **REQ 48**

8. An Air/Ground Router should log the establishment and termination of adjacencies with Airborne Routers **REQ 50**

9. An Air/Ground Router should log the establishment and termination of subnetwork connections with Airborne Routers **REQ 51**

10. Depending on the performance assessment model adopted, ATN Routers may be required to meter each data flow, counting number of packets and data volumes for each identified data stream, where a data stream is identified by a unique combination of source, destination, priority and ATSC Class. **REQ 53**

11. Depending on the performance assessment model adopted, ATN Routers may be required to meter the number of packets and data volumes received from each identified source and sent to each identified destination. Separate meters are required for each ATSC Class and priority. **REQ 56**

## 4.4 Offline Analysis Tools

1. A tool is required to process logs of connection establishment successes and failures in order to determine the service availability. **REQ 4**

2. A tool is required to process logs of messages sent and received on individual transport connection and to correlate the logs at both ends of the same transport connection, in order to determine reliability. **REQ 7**

3. A tool is required to analyse transport layer logs for uncommanded transport connection disconnects and the later successful re-establishment to the transport connection to the same destination, if any. This is to measure service continuity. **REQ 9**

4. A tool is required to analyse TPDU round trip delay logs in order to estimate the average transit delay per user message. **REQ 11**

5. A tool is required to analyse the user messages recorded by data recording equipment (both airborne and ground). The tool shall correlate individual messages and compare them for any loss of data integrity. **REQ 12**

6. A tool is required to analyse logs of security authentication failures in order to assess the data integrity achieved. **REQ 14**

7. A tool is required to analyse logs of messages sent and received by the transport protocol in order to determine the achieved throughput for each application. **REQ 16**

8. A tool is required to analyse End System Logs to determine the load place on the network by the End System. **REQ 23**

9. A tool is required to analyse subnetwork access logs in order to derive the percentage availability of each subnetwork. **REQ 25**

10. A tool is required to analyse subnetwork usage logs, to correlate the logs of all users of a given subnetwork, and hence to determine subnetwork **REQ 27**

reliability.

11. A tool is required to analyse subnetwork logs in order to determine the continuity of service. **REQ 29**

12. A tool is required to analyse packet received counts, and CLNP Header and Deflate checksum failures in order to assess subnetwork integrity. **REQ 31**

13. A tool is required to analyse logs of data volumes sent over each subnetwork in order to determine the achieved throughput. **REQ 33**

14. A tool is required to analyse subnetwork access logs to compute the connection establishment delay. **REQ 35**

15. A tool is required to analyse logs of subnetwork usage in order to compare achieved utilisation against available capacity and hence to identify where excess capacity may exist. **REQ 36**

16. A Network Design Model is required for capacity planning purposes. **REQ 37**

17. A tool is required to analyse router logs of packets forwarded and discarded and hence to assess router throughput **REQ 43**

18. A tool is required to measure route convergence rates and to predict future trends in route convergence rates **REQ 49**

19. A tool is required to analyse the impact on an Air/Ground Router of the number of Airborne Router adjacencies and subnetwork connections that it supports. **REQ 52**

20. Depending on the performance assessment model adopted, a tool may be required to analyse data stream meters in order to determine throughput and reliability as provided to each service user. **REQ 54**

21. A tool is required to generate echo packets in order to measure roundtrip delay and hence transit delay for each identified data stream. **REQ 55, REQ 57**

22. Depending on the performance assessment model adopted, a tool may be required to analyse meters at entry and exit points in order to determine throughput and reliability as provided by the Service Provider. **REQ 56**

## 4.5 Open Issues

1. A strategy is required on a per subnetwork basis to measure transit delay over that subnetwork.

2. Subnetwork specific monitoring criteria need to be developed.

3. There is the potential need for an industry group to collate together ISP performance statistics and to plan development of future capacity.