**Executive Summary**

This paper discusses Quality of Service (QoS) and the mechanisms QoS uses to manage congestion on a network to ensure that applications have sufficient network resources to communicate effectively and appropriately for the variety of traffic they use.

Using QoS, a network can be configured for stable and predictable end-to-end performance, and network services marketed so that the prices charged are tailored to the ‘end-users’ desired service level and price point.

This white paper has the following sections:

**A. Introduction**
Introduction QoS.

**B. How Does QoS Work?**
Provides a technical description of how QoS works and how levels of service work.

**C. Implementation of QoS in Allied Telesis Products**
A detailed look at how Allied Telesis Layer 3+ switches implement QoS to the best advantage and references real world case studies.
## Contents

A. INTRODUCTION 3
   What is QoS? 3

B. HOW DOES QoS WORK? 6
   QoS Mechanisms 6
   QoS at Layer 2 - 802.1 7
   QoS at Layer 3 - the Type of Service Field 7
   Architectures for QoS 8
   IntServ 8
   DiffServ 9
   QoS and Queuing 10
   On-going standardisation 10

C. IMPLEMENTATION OF QoS IN ALLIED TELESIS PRODUCTS 11
A. Introduction

What is QoS?

To demonstrate the world's first telephone in 1875 Alexander Graham Bell employed the clever tactic of using Hamlet's soliloquy, a passage familiar to the listeners in another room, to ensure that the listeners could themselves fill in any gaps caused by imperfections in the communication channel. 128 years later, communication systems have advanced at such an incredible rate that Professor Bell's telephone is unrecognisable in comparison, but the properties of two-way speech have not changed. Delays in communication, echo, and degradation of voice quality caused by missing information, can seriously impair the quality of speech, and render two-way communication impossible. Users of modern communications do not have the luxury of pre-empting spoken words.

The Internet is based around a 'best effort' concept where all packets are treated identically and share congested conditions. What began as an experimental best effort data network has grown in concept to a multimedia network that provides significant economic benefits to network providers and enterprises by minimising the investment required in network assets. In integrating voice and other media, such as video, data, and gaming onto a single network, however, the diversity and uniqueness of each traffic type must be managed to ensure acceptable service quality.

Today's network communication performance buzzwords include: Latency, Jitter, Bandwidth and Packet Loss. Bandwidth is the 'data clocking' rate of the system, typically expressed in bits per second. Latency refers to delay, caused by the physical characteristics of the transport media, packet reassembly and delay, processing delay and queuing delay. Jitter is the variation of delay over time, and is caused by latency variations.

Table 1 summaries:

- the characteristics of the type of network traffic
- the requirements for networks to deliver the traffic, and
- the requirements of applications to deliver the media to the user.
## Traffic Type

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Network Requirement</th>
<th>Application Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Voice</strong></td>
<td>Two way conversation comprises bursts or talk spurts. Must be delivered with minimal delay (less than 100 milliseconds), all packets in order, without jitter; but can tolerate some packet loss.</td>
<td>Route packets from source to destination with minimal delay. Priority must be given to these packets, and congestion managed to ensure they are not delayed at all. Provide appropriate Layer 4 support that facilitates this.</td>
</tr>
<tr>
<td><strong>Data</strong></td>
<td>Bursty, with some very large continuous transmissions. Some delay can be tolerated. Packet loss cannot be tolerated.</td>
<td>Route packets from source to destination with appropriate error checking protocol support at Layer 4. Emphasis is on correct delivery, not so much on rapid delivery.</td>
</tr>
<tr>
<td><strong>Video</strong></td>
<td>Continuous. Packet loss cannot be tolerated, as it causes visible degradation. For multicast and unicast video some small delay is acceptable (a few seconds), except for real-time applications, such as video conferencing, where the acceptable delay is similar to that of voice.</td>
<td>For multicast and unicast, route packets from source to destination accurately. Emphasis is on correct delivery, not so much on rapid delivery, although error checking and re-transmission is impractical for multicast applications.</td>
</tr>
<tr>
<td><strong>Gaming</strong></td>
<td>Bursts of data, voice, and continuous video. Must be delivered in real-time with some very minor packet loss tolerated.</td>
<td>Route packets from source to destination with minimal delay. Priority must be given to these packets, although not as high as voice, depending on the application. Appropriate Layer 4 support must be provided to ensure this.</td>
</tr>
</tbody>
</table>

Table 1
In this paradigm the network is responsible for the reliable delivery of traffic, and the higher Layers, including the Application Layer, are responsible for presentation of the traffic in a meaningful form to the user. This network architecture is a natural consequence of Moore’s law, where increasing intelligence at the end-points of the network (user sites) enables more powerful user applications to perform critical functions.

Devices connected to the network are free to use whatever application they require, and free to choose a protocol suitable for the particular purpose, such as TCP or UDP perhaps in combination with the Real-Time Protocol (RTP). The IP Layer in a network (Layer 3) simply routes packets with appropriate priority to ensure timely delivery from one end-point to another, with Layer 4 providing the necessary protocols on top of this.

Just as Moore’s law has given rise to an increase in the power at the end points of a network, and greater and more varied utilisation of a network, so it has enabled the required increase in functionality of networking devices themselves. This increase in functionality includes the ability to forward packets at wire-speed, and thereby reduce network congestion, and of particular interest in this paper, the ability to, at wire-speed, give priority treatment to packets and thereby provide quality of service to network users.

---

1 The increasing density of transistors on integrated circuits - for the past 3 decades the number of transistors on a silicon chip has doubled approximately every 18 months to 2 years, leading to greater and greater computational capability on a single chip. In turn this leads to far greater intelligence at the end-points of networks. Hence user workstations, for example, can run far more complex applications, leading to far more demand on the IP network and requirement for it to specialise in routing in order to forward packets at the increasing volumes and service demands.
B. How Does QoS Work?

**QoS Mechanisms**

Perhaps the simplest and most obvious way of providing a high service level without congestion is by over-provisioning a network. This involves adding resources to a network to ensure it can meet the current and future demand of applications, traffic, and its diverse nature. This approach has several disadvantages:

1. It almost invariably cannot account for future use of the network.

2. It is uneconomical to build a network from the outset that is designed to cope with all traffic, now and in the future. A company often wants to build a network incrementally, as demand increases, to reduce the upfront capital investment and resulting risk.

3. Many companies already own, or have access to, existing communications infrastructure, such as existing fibre optical cables, and it would be uneconomical to replace these.

4. Without QoS capabilities, it is impossible for a service provider to offer service differentiation to customers, where service expectations, and actual service provided, are linked to the amount paid for the service. This is a very important reason for QoS, and indeed forms one of the bases by which traffic congestion can be managed - working symbiotically with a service provider’s desire to differentiate product offerings to its customers. QoS means that a network can be segmented into a number of performance levels, with access priced at each level.
**QoS at Layer 2 - 802.1p**

One of the first attempts to give priority to packets is the IEEE-802.1P, or user priority field. This involves the addition of a user priority field to the IEEE-802.1Q VLAN (Virtual Local Area Network) header, as illustrated in the packet header depicted in Figure 2. The three bit field gives 8 levels of priority (one is reserved). 802.1P offers a simple QoS mechanism at Layer 2 for Layer 2 switches. Traffic classes can be assigned priority fields, with high priority traffic classes shifting any side effects of an overloaded router onto the traffic classes with lowest priority.

However, if the load from all traffic classes of elevated priority is so great that it in itself exceeds the entire capacity of the switch or router, then all other classes are denied access altogether; and even the priority class traffic will suffer service degradation. To counter this issue requires a more complex solution than 802.1p, and more of an architectural solution that considers the entire network. That said, 802.1p does offer a very simple and inexpensive QoS solution for simpler networks.

![Figure 2: Packet structure illustrating the 802.IP user priority field in the VLAN header](image)

**QoS at Layer 3 - the Type of Service Field**

An early attempt to introduce QoS into IP (Layer 3) was the TOS (Type of Service) field, again a simple priority field, although never really used on a large scale, mainly because of lack of demand around the time it was introduced. It has now been superseded by the DiffServ model.
The TOS methodology of providing QoS by signalling a simple priority has been superseded by more complex QoS architectures.

Architectures for QoS

The simple priority field methods, although useful in simple networks where congestion is not a major issue, do have shortfalls, and alone are not satisfactory for large and complex networks carrying large volumes of traffic of varying types. To properly support multimedia real-time applications it is necessary to go to an architecture that actively controls traffic entering a network and the Layer 3 switches in that network. The two methods developed for IP networks are Integrated Services (IntServ) and Differentiated Services (DiffServ).

IntServ

Integrated Services essentially defines an end-to-end pathway through a network for each application's packets, and in this respect is similar to Asynchronous Transfer Mode (ATM). It does this using the Resource Reservation Protocol (RSVP), which dynamically maintains a path for each application's packets through a network, using the resources (Layer 3 switches) with the lightest load. This state is maintained as a flow, with an associated policy for admitting traffic to the network, and pre-determined packet handling characteristics at each hop.
**DiffServ**

The IntServ methodology was found to be complex and demanding of processing requirements in network switches, so most network providers prefer to use the differentiated services model. In the DiffServ model traffic is classified into flows, although per flow resource reservation is not required. The IP packets are marked, using the DiffServ field. This field uses the same bits as the TOS field, although each bit has a different meaning (see Figure 3). The fundamental advance provided by DiffServ over and above TOS is that it applies an admission control mechanism at the entry point (ingress) of a network. At the ingress, a Layer 3 switch will determine the service to be applied to packets and the amount of traffic admitted within each service class. The typical functions performed in a DiffServ network are as follows:

1. Traffic entering a DiffServ network is classified into flows.

2. At the entry to the network a policy is applied to the classified flows. This shapes the traffic to meet the requirements of the particular flow. If excessive traffic enters the network, then packets in the low priority flows are discarded.

3. The shaped traffic is then assigned a particular behaviour aggregate. The IP header DiffServ field is marked with the appropriate DiffServ Code Point (DSCP).

4. When it is passed through a DiffServ network the DSCP triggers a selected per-hop behaviour from the interior of the network.

For a network to support DiffServ every Layer 3 switch or router in the network must be able to respond to the service marking contained in the packet’s DSCP and to respond consistently with this DSCP. No further classification or profiling is required or performed inside the network. In this way the most intensive classification and profiling of traffic occurs near the edge of the network, with this function performed on ingress. The ability to classify traffic, apply policies and traffic shaping, and priority mark packets is particularly important near the edge of a network, with the core mainly required to support DSCP classification and priority treatment.

Allied Telesis Layer 3+ switches support the RSVP protocol and are eminently suitable for classifying traffic on a per flow basis and therefore able to support the IntServ methodology, but DiffServ is predominantly used and it is extremely well supported by Allied Telesis Layer 3+ switches.
QoS and Queuing

Queue management is fundamental to QoS. It enables bandwidth control (which is essentially admission control), and ensures that traffic is dealt with as its priority requires. To achieve this, two main queue types are required. They are:

1. Weighted fair bandwidth distribution

   This allocates bandwidth to applications based on their needs, and thereby sets maximum and minimum bandwidth limits. It ensures that applications, with lower priority for instance, cannot borrow bandwidth from other applications.

2. Priority

   This ensures that high priority traffic is always given priority over other traffic, and thereby suffers less delay. It does this by 'graceful' dropping of lower priority packets via the RED mechanism when severe congestion occurs, dropping progressively more and higher priority packets, until congestion is eased.

On-going standardisation

The standardisation of QoS has progressed substantially since the need for it was first recognised with the integration of multiple traffic types on to single networks. Although some very useful standards have been developed the standardisation effort by the IETF and ITU is on-going, particularly for core carrier networks. The advanced Allied Telesis QoS architecture within Allied Telesis Layer 3+ switches provides fundamental functions including classification and queuing. It is a flexible architecture that can accommodate numerous applications, and new standards as they emerge.
C. Implementation of QoS in Allied Telesis Products

Allied Telesis’ Layer 3+ products support the full QoS suite, from IEEE-802.1P within the IEEE-802.1Q tag at Layer 2, to the TOS field, RSVP (RFC 2205), IntServ Controlled Load Service Class (RFC2211), and the DiffServ architecture (RFC 2475). Allied Telesis high-end Layer 3+ switches provide full classification and re-marking capabilities based on the DiffServ Code Point (DSCP) as well as source and destination Layer 2 (MAC), Layer 3 (IP / IPX), and Layer 4 (TCP / UDP port) addresses. In addition classification can take place on the Ethernet encapsulation type and protocol, as well as VLAN source and destination addresses.

This very advanced classification capability operating in the data plane of Allied Telesis’ switches enables very advanced traffic classification based on the type of traffic, its source, and priority. This means that network providers can roll out different service levels to their customers based on service charge, as well as implement admission control, consistent with the overall DiffServ philosophy.

Operating on top of these, in the control plane is Allied Telesis’ full suite of routing protocols (OSFP, BGP4, RIPv1, RIPv2, and IS-IS). These protocols complement the extensive QoS capabilities of the switches and make them ideal for a wide variety of networks, from large to small.

Allied Telesis has implemented QoS in a wide range of network situations. It has enabled an important Telco to provide a video service that is broadcast quality, and jitter-free. Service providers rely on QoS network management functionality to prevent congestion and to manage traffic with a jitterless delivery mechanism. Hotel and hospital enterprises successfully use Allied Telesis devices to support multimedia services on the same network that provides standard data service. The network services that they provide are reliable, resilient and chargeable. For further information about this implementation, and others, see the case studies on www.alliedtelesis.com.

Operating above these is the Allied Telesis SNMP management system. The management system provides extensive set up capabilities for switches. It includes:

- The AlliedView™-EMS device management application, available in two versions.
- a powerful command line interface with scripts and triggers.
- an Graphical User Interface.

Traffic classification is complemented by extensive queuing capability, with eight priority queues at the output ports, supporting the full 8 802.1P TOS levels. The Random Early Discard (RED) curve features that are built into the queues enhance congestion control further and work extremely well in conjunction with the TCP suite, which "backs off" sending packets when it detects that packets have been discarded, and so automatically manages network congestion. To ease congestion, large packet buffering memory within the switches assists in ‘smoothing’ out peaks in traffic through the switch.

In the Allied Telesis QoS model, traffic is classified into flow groups and traffic classes, and policies are applied to these. Each policy has a weighted fair bandwidth distributor queuing mechanism that operates to guarantee minimum bandwidths, and enforce maximum bandwidths. The ability of Allied Telesis switches to provide min/max bandwidth guarantees means that a network provider can guarantee service levels to users. The queuing also acts to distribute bandwidth between the traffic classes, so as manage bandwidth across the switch. Hence, admission control can be effectively applied to users.