Integrated Services Architecture: The Next-generation Internet

The integrated services architecture is a response to the growing variety and volume of traffic experienced in the Internet and intranets. It provides a framework for the development of protocols such as RSVP and RTP, to handle multimedia/multicast traffic and provides guidance to router vendors on the development of efficient techniques for handling a varied load. ISA is already influencing router and Internet design, and will have a greater impact over the next few years. Copyright © 1999 John Wiley & Sons, Ltd.

By William Stallings*

Historically, the Internet and other IP-based internets (such as corporate intranets) have been able to provide a simple best-effort delivery service to all applications. Although the Internet Protocol (IP) header is equipped with fields that can specify precedence and type of service, this information has generally been ignored by routers, in both the selection of routes and the treatment of individual packets.

But the needs of users have changed. A company may have spent millions of dollars installing an IP-based internet designed to transport data among LANs, but now finds that new real-time, multimedia, and multicasting applications are not well supported by such a configuration. The only networking scheme designed from day one to support both traditional data traffic and real-time/multimedia traffic is ATM. However, reliance on ATM means either constructing a second networking infrastructure for real-time traffic or replacing the existing IP-based configuration with ATM, both of which are costly alternatives.

Thus, there is a strong need to be able to support a variety of traffic with a variety of quality-of-service (QoS) requirements, within the TCP/IP architecture. One response to this need has been the development of new networking protocols, of which the three most important are IPv6, the Resource ReserVation Protocol (RSVP), and the real-time transport protocol (RTP).

However, the fundamental requirement is to

William Stallings is a consultant, lecturer, and author of over a dozen books on data communications and computer networking. This article is based on material in the author’s latest book, High-Speed Networks: TCP/IP and ATM Design Principles (Prentice Hall, 1997). His home in cyberspace is http://www.shore.net/welcome.html

*Correspondence to: William Stallings, 845 Satucket Road, P.O. Box 2405, Brewster, MA 02631, U.S.A. Email: ws@shore.net
add new functionality to routers and a means for requesting QoS-based service from internets. To meet this requirement, the IETF is developing a suite of standards under the general umbrella of the Integrated Services Architecture (ISA). ISA, intended to provide QoS transport over IP-based internets, is defined in overall terms in RFC 1633, while a number of other documents are being developed to fill in the details. Already, a number of vendors have implemented portions of the ISA in routers and end-system software. This article provides an overview of ISA.

Internet Traffic

Traffic on a network or internet can be divided into two broad categories: elastic and inelastic. A consideration of their differing requirements clarifies the need for an enhanced internet architecture.

—Elastic Traffic—

Elastic traffic can adjust, over wide ranges, to changes in delay and throughput across an internet and still meet the needs of its applications. This is the traditional type of traffic supported on TCP/IP-based internets and is the type of traffic for which internets were designed. Applications that generate such traffic typically use TCP or UDP as a transport protocol. In the case of UDP, the application will use as much capacity as is available up to the rate that the application generates data. In the case of TCP, the application will use as much capacity as is available up to the maximum rate that the end-to-end receiver can accept data. Also with TCP, traffic on individual connections adjusts to congestion by reducing the rate at which data are presented to the network.

Applications that can be classified as elastic include the common Internet-based applications, such as file transfer, electronic mail, remote logon, network management, and web access. But there are differences among the requirements of these applications. For example:

- E-mail is generally quite insensitive to changes in delay.
- When file transfer is done on-line, as it frequently is, the user expects the delay to be proportional to the file size and so is sensitive to changes in throughput.
- With network management, delay is generally not a serious concern. However, if failures in an internet are the cause of congestion, then the need for network management messages to get through with minimum delay increases with increased congestion.
- Interactive applications, such as remote logon and web access, are quite sensitive to delay.

So, even if we confine our attention to elastic traffic, a QoS-based internet service could be of benefit. Without such a service, routers are dealing evenhandedly with arriving IP packets, with no concern for the type of application and whether this packet is part of a large transfer element or a small one. Under such circumstances, and if congestion develops, it is unlikely that resources will be allocated in such a way as to meet the needs of all applications fairly. When inelastic traffic is added to the mix, matters are even more unsatisfactory.

—Inelastic Traffic—

Inelastic traffic does not easily adapt, if at all, to changes in delay and throughput across an internet. The prime example is real-time traffic, such as voice and video. The requirements for inelastic traffic may include the following:

The purpose of ISA is to enable the provision of QoS support over IP-based internets.

- Throughput: A minimum throughput value may be required. Unlike most elastic traffic, which can continue to deliver data with perhaps degraded service, many inelastic applications absolutely require a given minimum throughput.
- Delay: An example of a delay-sensitive application is stock trading; someone who consistently receives later service will consistently act later, and with greater disadvantage.
- Delay variation: The magnitude of delay variation is a critical factor in real-time appli-
cations. The larger the allowable delay, the longer the real delay in delivering the data and the greater the size of the delay buffer required at receivers. Real-time interactive applications, such as teleconferencing, may require a reasonable upper bound on delay variation.

- **Packet loss**: Real-time applications vary in the amount of packet loss, if any, that they can sustain.

These requirements are difficult to meet in an environment with variable queuing delays and congestion losses. Accordingly, inelastic traffic introduces two new requirements into the internet architecture. First, some means is needed to give preferential treatment to applications with more demanding requirements. Applications need to be able to state their requirements, either ahead of time in some sort of service request function, or on the fly, by means of fields in the IP packet header. The former approach is preferable: it provides more flexibility in stating requirements, and it enables the network to anticipate demands and deny new requests if the required resources are unavailable. This approach implies the use of some sort of resource reservation protocol.

A second requirement in supporting inelastic traffic in an internet architecture is that elastic traffic must still be supported. Inelastic applications typically do not back off and reduce demand in the face of congestion, in contrast to TCP-based applications. Therefore, in times of congestion, inelastic traffic will continue to supply a high load, and elastic traffic will be crowded off the internet. A reservation protocol can help control this situation by denying service requests that would leave too few resources available to handle current elastic traffic.

### ISA Approach

The purpose of ISA is to enable the provision of QoS support over IP-based internets. The central design issue for ISA is how to share the available capacity in times of congestion.

For an IP-based internet that provides only a best-effort service, the tools for controlling congestion and providing service are limited. In essence, routers have two mechanisms to work with:

- **Routing algorithm**: Most routing protocols in use in internets allow routes to be selected to minimize delay. Routers exchange information to get a picture of the delays throughout the internet. Minimum-delay routing helps to balance loads, thus decreasing local congestion, and helps to reduce delays seen by individual TCP connections.
- **Packet discard**: When a router’s buffer overflows, it discards packets. Typically, the most recent packet is discarded. The effect of lost packets on a TCP connection is that the sending TCP entity backs off and reduces its load, thus helping to alleviate internet congestion.

These tools have worked reasonably well, but are inadequate for the variety of traffic now coming to internets.

ISA is an overall architecture within which a number of enhancements to the traditional best-effort mechanisms are being developed. In ISA, each IP packet can be associated with a flow. RFC 1633 defines a flow as a distinguishable stream of related IP packets that results from a single user activity and requires the same QoS. For example, a flow might consist of one transport connection or one video stream distinguishable by the ISA. There can be more than one recipient of a flow (multicast).

ISA makes use of the following functions to manage congestion and provide QoS transport:

- **Admission control**: For QoS transport (other than default best-effort transport), ISA requires that a reservation be made for a new flow. If the routers collectively determine that there are insufficient resources to guarantee the requested QoS, then the flow is not admitted. The protocol RSVP is used to make reservations.
- **Routing algorithm**: The routing decision may be based on a variety of QoS parameters, not just minimum delay.
- **Queuing discipline**: A vital element of the ISA is an effective queuing policy that takes into account the differing requirements of different flows.
- **Discard policy**: A queuing policy determines which packet to transmit next if a number of packets are queued for the same output port. A separate issue is the choice and timing of packet discards. A discard policy can be an
An important element in managing congestion and meeting QoS guarantees.

**ISA Components**

Figure 1 is a general depiction of the implementation architecture for ISA within a router. Below the thick horizontal line are the forwarding functions of the router; these are executed for each packet and therefore must be highly optimized. The remaining functions, above the line, are background functions that create data structures used by the forwarding functions.

The principal background functions are:

- **Reservation Protocol**: This protocol is used among routers and between routers and end systems to reserve resources for a new flow at a given level of QoS. The reservation protocol is responsible for maintaining flow-specific state information at the end systems and at the routers along the path of the flow. The reservation protocol updates the traffic control database used by the packet scheduler to determine the service provided for packets of each flow.

- **Admission Control**: When a new flow is requested, the reservation protocol invokes the admission control function. This function determines if sufficient resources are available for this flow at the requested QoS. This determination is based on the current level of commitment to other reservations and/or on the current load on the network.

- **Management Agent**: A network management agent is able to modify the traffic control database and to direct the admission control module in order to set admission control policies.

- **Routing Protocol**: The routing protocol is responsible for maintaining a routing database that gives the next hop to be taken for each destination address and each flow.

These background functions support the main task of the router, which is the forwarding of packets. The two principal functional areas that accomplish forwarding are the following:

- **Classifier and Route Selection**: For the purposes of forwarding and traffic control, incoming packets must be mapped into classes. A class may correspond to a single flow or to a set of flows with the same QoS requirements. For example, the packets of all video flows or the packets of all flows attributable to a particular organization may be treated identically for purposes of resource allocation and queuing discipline. The selection of class is based on fields in the IP header. Based on the packet’s class and its destination IP address, this function determines the next-hop address for this packet.
Packet Scheduler: This function manages one or more queues for each output port. It determines the order in which queued packets are transmitted and the selection of packets for discard, if necessary. Decisions are made based on a packet’s class, the contents of the traffic control database, and current and past activity on this outgoing port. Part of the packet scheduler’s task is that of policing, which is the function of determining whether the packet traffic in a given flow exceeds the requested capacity and, if so, deciding how to treat the excess packets.

ISA Services

ISA service for a flow of packets is defined on two levels. First, a number of general categories of service are provided, each of which provides a certain general type of service guarantees. Second, within each category, the service for a particular flow is specified by the values of certain parameters; together, these values are referred to as a traffic specification (TSpec). Currently, three categories of service are defined:

- Guaranteed
- Controlled Load
- Best Effort

An application can request a reservation for a flow for a guaranteed or controlled load QoS, with a TSpec that defines the exact amount of service required. If the reservation is accepted, then the TSpec is part of the contract between the data flow and the service. The service agrees to provide the requested QoS as long as the flow’s data traffic continues to be described accurately by the TSpec. Packets that are not part of a reserved flow are by default given a best-effort delivery service.

Before looking at the ISA service categories, one general concept should be defined: the token bucket traffic specification. This is a way of characterizing traffic that has three advantages in the context of ISA:

1. Many traffic sources can easily and accurately be defined by a token bucket scheme.
2. The token bucket scheme provides a concise description of the load to be imposed by a flow, enabling the service to determine easily the resource requirement.
3. The token bucket scheme provides the input parameters to a policing function.

A token bucket traffic specification consists of two parameters: a token replenishment rate \( R \) and a bucket size \( B \). The token rate \( R \) specifies the continually sustainable data rate; that is, over a relatively long period of time, the average data rate to be supported for this flow is \( R \). The bucket size \( B \) specifies the amount by which the data rate can exceed \( R \) for short periods of time. The exact condition is as follows: during any time period \( T \), the amount of data sent cannot exceed \( RT + B \).

Figure 2 illustrates this scheme and explains the use of the term bucket. The bucket represents a counter that indicates the allowable number of octets of IP data that can be sent at any time. The bucket fills with octet tokens at the rate of \( R \) (i.e. the counter is incremented \( R \) times per second), up to the bucket capacity (up to the maximum counter value). IP packets arrive and are queued for processing. An IP packet may be processed if there are sufficient octet tokens to match the IP data size. If so, the packet is processed and the bucket is drained of the corresponding number of tokens. If a packet arrives and there are insufficient tokens available, then the packet exceeds the TSpec for this flow. The treatment for such packets is not specified in the ISA documents; common actions are relegating the packet to best effort service, dis-
carding the packet, or marking the packet in such a way that it may be discarded in future.

Over the long run, the rate of IP data allowed by the token bucket is $R$. However, if there is an idle or relatively slow period, the bucket capacity builds up, so that at most an additional $B$ octets above the stated rate can be accepted. Thus, $B$ is a measure of the degree of burstiness of the data flow that is allowed.

--- Guaranteed Service ---

The key elements of the guaranteed service are:

1. The service provides assured capacity level, or data rate.
2. There is a specified upper bound on the queuing delay through the network. This must be added to the propagation delay, or latency, to arrive at the bound on total delay through the network.
3. There are no queuing losses. That is, no packets are lost due to buffer overflow; packets may be lost due to failures in the network or changes in routing paths.

One category of applications for this service is those that need an upper bound on delay so that a delay buffer can be used for real-time playback of incoming data, and that do not tolerate packet losses because of the degradation in the quality of the output. Another example is applications with hard real-time deadlines.

The guaranteed service is the most demanding service provided by ISA. Because the delay bound is firm, the delay has to be set at a large value to cover rare cases of long queuing delays.

--- Controlled Load ---

The key elements of the controlled load service are:

1. The service tightly approximates the behaviour visible to applications receiving best-effort service under unloaded conditions.
2. There is no specified upper bound on the queuing delay through the network. However, the service ensures that a very high percentage of the packets do not experience delays that greatly exceed the minimum transit delay (i.e. the delay due to propagation time plus router processing time with no queuing delays).
3. A very high percentage of transmitted packets will be successfully delivered (i.e. almost no queuing loss).

The integrated services architecture is a response to the growing variety and volume of traffic experienced in the Internet and intranets.

As was mentioned, the risk in an internet that provides QoS for real-time applications is that best-effort traffic is crowded out. This is because best-effort types of applications employ TCP, which will back off in the face of congestion and delays. The controlled load service guarantees that the network will set aside sufficient resources so that an application that receives this service will see a network that responds as if these real-time applications were not present and competing for resources.

The controlled service is useful for applications that do not require an a priori upper bound on the delay through the network. Rather, the receiver measures the jitter experienced by incoming packets and sets the playback point to the minimum delay that still produces a sufficiently low loss rate. Examples: video can adapt by dropping a frame or delaying the output stream slightly; voice can adapt by adjusting silent periods.

If you wish to order reprints for this or any other articles in the International Journal of Network Management, please see the Special Reprint instructions inside the front cover.