TELEMETRY AND SERVICE CONVERGENCE IN MIXED PROTOCOL TEST RANGE NETWORKS

Bob Kovach
Director, Access Products
Terawave Communications
Hayward, California

ABSTRACT

In the past few years, an evolution has been occurring in test range network topologies. With the proliferation of IP-based networks at the desktop, range officers are seeking ways to extend IP-based networks to the test range, to derive the cost and operational benefits offered with IP technology. This transition is not without its own set of problems. The operational transition from the traditional, ATM-based ranges to IP-based ranges must be addressed. In many cases, it is desired to maintain the ATM range, and add IP capabilities as time and budget permits. The net result is that frequently a mixed protocol network emerges. Terawave Communications has been developing telemetry transport solutions for both ATM and IP-based networks, along with technology to enable convergence of additional services such as video, voice, and data across test ranges. Terawave has developed a solution for various network topologies from ATM-only and IP-only to mixed protocol implementations, which supports end-to-end interworking of telemetry, video, and additional services over mixed protocol networks. In this paper, Terawave will detail the implementation decisions made in the course of application development, and share a framework for enabling seamless intra- and inter- range communication of telemetry and mixed services.

KEYWORDS

Packet Encapsulation, Source Selection, Quality of Service (QoS), Switched Virtual Circuit (SVC)

INTRODUCTION

The staff at Terawave has developed a platform that supports the aggregation of multiple services for transport over broadband networks. Among the traffic types supported are telemetry, video, voice, and data. The traditional broadband network implementation has been ATM-based, with the physical layer implementation being DS3 or SONET-based. However, with the emergence of the use of IP-based networks at both the edge and in backbone, the issues with making the transition from ATM-based to IP-based networks must be addressed.

In this paper, Terawave will present a framework for identifying design decisions and tradeoffs in the design of a network that will successfully transport multiple types of traffic in ATM, IP and mixed networks. A number of proposed solutions will also be presented.

NETWORK ARCHITECTURES

For the purposes of discussion, two basic network topologies will be presented. The network types will be classified by the type of mechanisms used to implement layers 2 and 3 of the ISO protocol stack. In this paper, only IP and ATM type networks will be considered.

The first type of network is the uniform topology. Uniform networks are distinguished by the fact that all elements in the network share the same media access and network layer mechanism. Two sub-types of uniform networks will be discussed; uniform IP network, consisting of IP-based elements only, and a uniform ATM network, consisting of ATM-based network elements only.

The second type of network topology will be called a mixed topology, and will allow the interconnection of both IP-based and ATM-based network elements. An additional network element is required to effect the interworking function where a protocol conversion between IP and ATM packets is performed.

DESIGN PARAMETERS

A number of design parameters have been identified that define the scope of effort required to support seamless traffic transport in a mixed network environment. These are:

- Encapsulation
- Connection Management
- Multicast Support
- Quality of Service

At all points in the network, standards-based solutions will be used in order to allow the maximum amount of connectivity options.

ENCAPSULATION

The encapsulation mechanism is the method by which the payload is converted from a traffic stream to a series of packets for transmission across the network. The goal of is to define a method to encapsulate traffic so that seamless transport across mixed networks is possible. After the traffic stream is broken up (or segmented) into packets, additional information is added that is used by the network to support packet routing, reassembly and error handling. In ATM networks, the traffic stream is converted into a series of packets that are all 53 bytes in length. In IP networks, packets can be from 64 to 1518 bytes in length. The goal of is to define a method to encapsulate traffic so that seamless transport across mixed networks is possible.

A standard exists that defines a mechanism for carrying IP traffic over ATM networks. This standard, RFC 2684, defines an encapsulation method for IP traffic for subsequent transmission over ATM networks. Figure 1 shows the method by which the traffic is converted into IP packets, and the mechanisms by which conversion between IP packets and ATM cells is accomplished.

Three conversion elements are defined to facilitate operation across all network topologies:

IP Convergence—This is a bi-directional function. In the forward direction, the source traffic stream is converted to IP packets. In the reverse direction, IP packets are converted back into the source traffic stream.

RFC 2684 IP to ATM Convergence—In this mechanism, native IP packets are converted to ATM cells according to the RFC 2684 standard.

RFC 2684 ATM to IP Convergence—In this mechanism, IP-bearing ATM cells are converted to native IP packets.

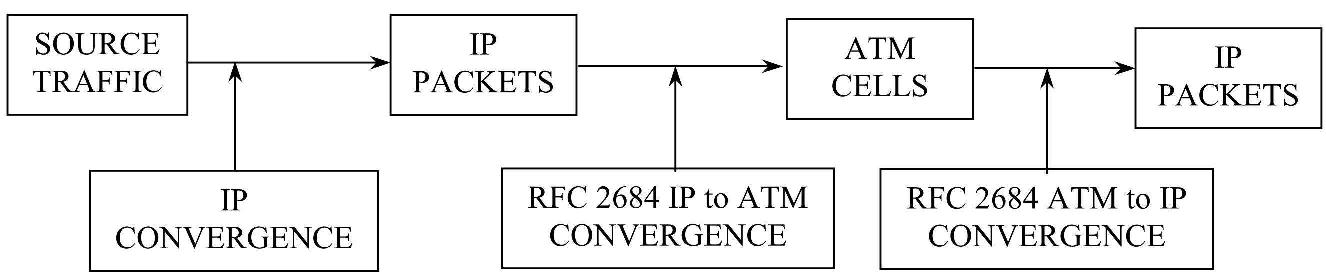

Figure 1--Packet and Cell Encapsulation

The operation is as follows.

In uniform IP networks, the source traffic is transported as IP packets, and the IP Convergence function is the only required conversion element.

In uniform ATM networks, the source traffic is converted to IP packets. At the ingress to the ATM network, the IP packets are converted to ATM cells via the RFC 2684 IP to ATM Convergence function. At the egress from the ATM network, the ATM cells are converted back to IP packets via the RFC 2684 IP to ATM Convergence function, prior to the conversion of IP packets back to the source traffic stream.

In mixed networks, transition between IP and ATM is effected by the RFC 2684 conversion element to perform interconnection between IP and ATM networks.

CONNECTION MANAGEMENT

Connection management is the means by which connections are provisioned and maintained. The goal is to maintain connectivity across mixed networks and to automatically propagate connectivity across uniform and mixed networks.

Two modes of operation are considered. In the first mode, all connections are statically provisioned. All of the ATM connections are provisioned with VBR traffic parameters. The IP connections are provisioned as typical best effort service. The aggregate bandwidth of the individual connections is configured such that it is less than the network bandwidth, minus an additional amount of bandwidth to accommodate bursts in traffic. In effect, quality of service is implemented using available bandwidth. This has the following advantages:

- Simplicity of configuration
- Minimal requirements on outer and inter-network equipment

Static configuration has the following disadvantages:

- Potential traffic corruption in bursty conditions
- Configuration must be manually adjusted when network changes

For this reason, it is desired to implement an automatic mechanism for the provisioning of connections. In uniform ATM networks, the ATM Forum has defined a mechanism for generating connections across the network using Switched Virtual Circuits (SVC). Using this scheme, connections are automatically propagated across ATM networks via a signaling method, but the intervening ATM switches must support the SVC signaling protocol to implement end-to-end connectivity.

In mixed networks, the ATM to IP transition must be supported by the intervening router that performs the following functions:

- ATM address to IP address resolution
- Forwarding of packets and cells to appropriate subnets or ATM network

These functions are implemented in routers compliant to RFC 2225, the IETF document that defines the routing interworking functions for IP and ATM networks.

MULTICAST SUPPORT

Multicast provides a means for traffic to flow from a source to multiple destinations. The goal is to provide seamless support for multicast traffic across mixed networks.

In uniform ATM networks, point-to-multipoint support is implemented using SVC type connections. In this implementation, a point-to-multipoint SVC call will provide the needed functionality, presuming that the ATM switch supports SVC operation.

In uniform IP networks, multicast support is a native mode of operation. To implement multicasting, the Layer 2 and Layer 3 addresses must conform to the IETF requirements for multicast addressing as defined in IETF documents RFC 1112 and RFC 1122.

In mixed networks, again the IP-to-ATM routing functionality must support multicast traffic. The support of multicast traffic is defined in RFC 2225.

QUALITY OF SERVICE

In order to support robust delivery of traffic across the network, a set of mechanisms must be implemented to ensure successful transmission of the telemetry packets across the network. These mechanisms collectively are called Quality of Service or QoS. The goal in mixed network implementations is to support the migration of QoS across the different networks.

In uniform ATM networks, QoS is implemented via reservations-based system. ATM provides QoS by supporting mechanisms to differentiate traffic and classify packets based upon their service category. ATM provides a number of service categories; CBR, rt-VTR, nrt-VBR, ABR, and UBR. Each Virtual Channel (VC) traversing the network can specify the required service category. A VC requiring a particular service category can additionally specify its traffic characteristics using explicit parameters.

ATM provides dynamic signaling and routing protocols for setting up resource reservations. Signaling protocol is “hard state", meaning that a reservation state is explicitly set up and torn down. In an ATM network, each network node implements intelligent queuing mechanisms to ensure received packets are processed according to the resource reservation made for them. ATM also provides admission control mechanisms that ensure QoS integrity by not allowing a new VC to be set up which will impact the QoS of existing connections.

In uniform IP networks, a number of QoS mechanisms are proposed. One type of QoS is a relative priority mechanism, which makes use of the default interpretation of the 802.1p priority classes.

802.1q (Virtual Bridged LANs Working Group) defines changes to Ethernet frames that will enable them to carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

Four bytes have been added to the Ethernet frame for this purpose, causing the maximum Ethernet frame length to increase from 1518 to 1522 bytes. In these 4 bytes, 3 bits allow for up to eight priority levels and 12 bits identify one of 4,094 different VLANs.

Layer 2 priority can be bestowed upon a traffic stream by using the VLAN priority field, layer 3 priority is controllable by using TOS. Switches and routers which the stream must traverse should be configured to respect these priorities.

In mixed networks, QoS can be supported across network boundaries using a mapping mechanism where ATM traffic categories are mapped into the 802.1p relative priority mechanism. The following features must be supported:

- The IP switch must support the Layer 2/802.1p priority mechanism
- A mapping mechanism must be designed to map the ATM traffic classes into the Layer 2 service classes

RESULTS

An implementation of the mechanisms discussed is shown in Figure 2. This network is designed to terminate input telemetry traffic from two encoders, E1 and E2, located in IP Attached Subnet 1. The traffic can then be transmitted and targeted to a mixed network, with different decoder implementations on the far end of the network.

All TM traffic coming from the IP Attached Subnet 1 is coded as IP packets by TM encoders E1 and E2. The IP traffic is configured as multicast.

The IP packets then are connected to router R1 via the IP backbone. Router R1 performs the following actions:

- IP to ATM conversion function per RFC 2684
- Mapping of multicast IP traffic to ATM connections via SVC calls per RFC 2225

The traffic, now as ATM traffic flows across the ATM backbone to two ATM attached network elements, NE1 and NE2.

In ATM Attached Subnet 1, the decoder is implemented in NE1, and is ATM-based. In this case, the decoding of the TM stream is from ATM cells to the native TM stream.

In ATM Attached Subnet 2, NE2 performs the conversion from ATM cells to IP packets. by performing the ATM to IP conversion function per RFC 2684.

In this fashion the TM traffic can be propagated across mixed networks, and can be targeted to an IP-based decoder or an ATM-based decoder. As the source traffic in this example is multicast across the network, the decoder nodes can both decode the same source TM stream.

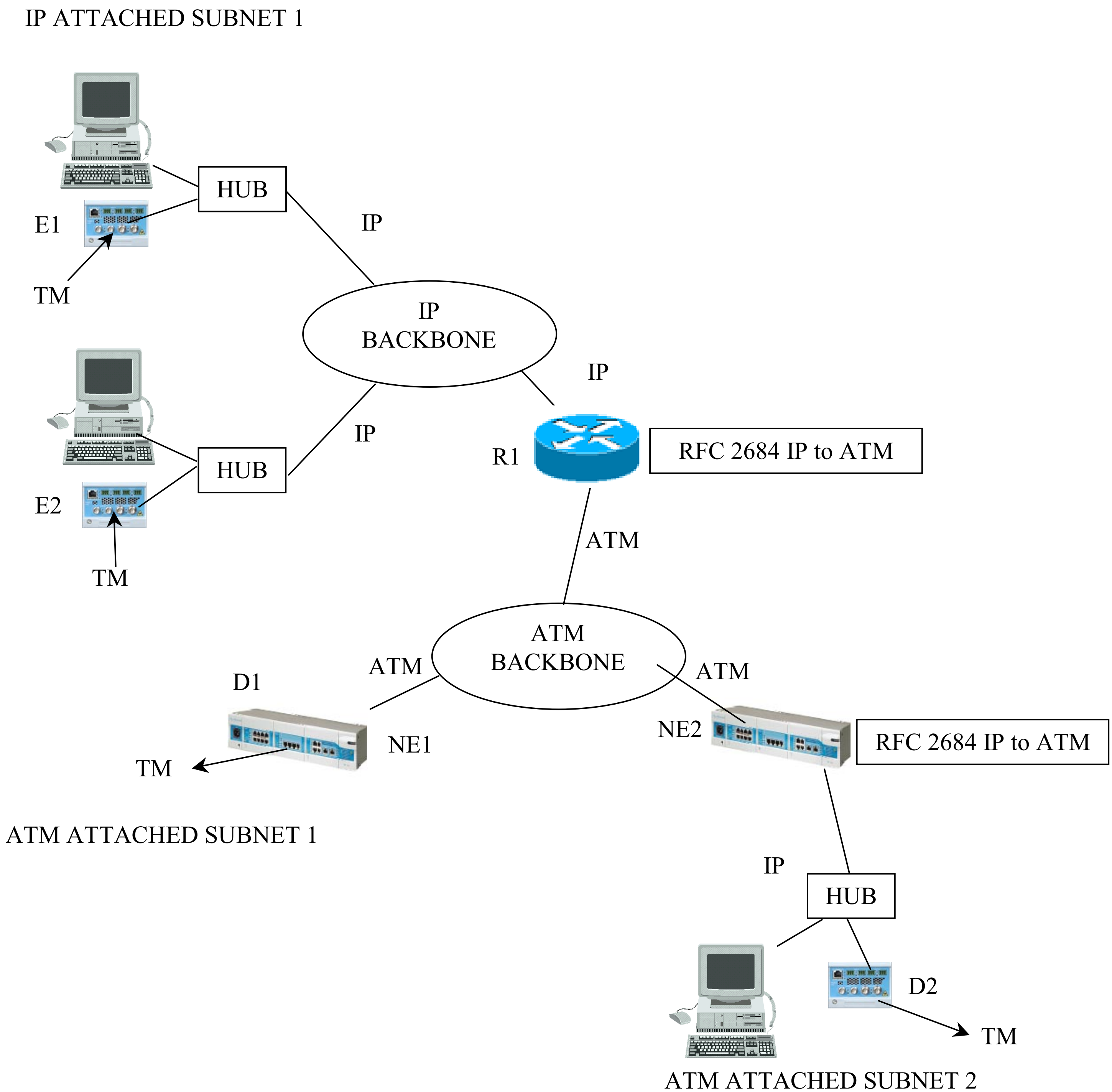

Figure 2--Mixed Network Test Scenario

CONCLUSION

As network topologies evolve from ATM to IP-based implementations, a growing number of ranges will be IP-based as well as a mixture of IP and ATM topologies. In this paper, a set of mechanisms was discussed to ease the transition from uniform ATM networks to uniform IP networks. The ability to support operation in mixed networks is seen as a way to ease the transition from ATM to IP networks. as well as to supply the user with a method to interoperate between ATM and IP networks.

REFERENCES

Braden, (editor), “Requirements for Internet Hosts – Communication Layers”, IETF Document RFC 1122.

Deering, S., “Host Extensions for IP Multicasting”, IETF Document RFC 1112.

Fenner, W., “Internet Group Management Protocol, Version 2, IETF Document RFC 2236.

Heinanen, J. and Grossman, D. and Heinanen, J., “Multiprotocol Encapsulation over ATM Adaptation Layer 5”, IETF Document RFC 2684.

Laubach, M., and Halpern, J., “Classical IP and ARP over ATM”, IETF Document RFC 2225.