Keyur Parikh
Junius Kim

TDM services over IP networks

1. ABSTRACT

Time Division Multiplexing (TDM) circuits have been the backbone of communications over the past several decades. These circuits which provide reliable and low-delay services for voice, data and video transport, are migrating towards Internet Protocol (IP) based packet switched networks. The primary reason for the migration of these circuits is to reduce the cost of transport and management by having a converged network for all services. Due to the sheer magnitude of the installed legacy TDM equipment, this migration to "end-to-end IP" will go through a transitional phase where some services will continue to use legacy equipment, while the core network moves towards IP. In this transitional phase, there is a need for technology allowing seamless transmission of TDM services across the packet switch networks. The Internet Engineering Task Force (IETF) and International Telecommunication Union (ITU) provide specifications for interoperability to emulate TDM circuits over IP networks. These emulated services can be implemented using a gateway device that provides for inter-working function (IWF) between TDM and IP networks. The primary challenge of the gateway device is to provide the equivalent level of reliability and security of traditional TDM networks. To that extent, the gateway device must be able to achieve an equivalent level of synchronization of TDM circuits across the IP network and cope with packet impairments of the underlying IP network. In addition, the gateway can provide value added services such as echo cancellation, multicasting and IP security.

The remainder of this paper explores the architecture of a Gateway device such as Harris's NetXpress, which can facilitate a smooth transition for legacy TDM applications as the core network is migrating from TDM circuit switched to IP based packet switched networks.

2. NETWORK EVOLUTION

Over the years, TDM based Wide Area Networks (WANs) have enabled transport of a multitude of user applications including: basic telephony, trunked radio, low to medium rate data services and studio to transmitter links for broadcast audio and video. Figure 1 shows a basic model for an end to end TDM system.

Figure 1 End to End TDM Network

The TDM network dedicates a circuit with a fixed amount of bandwidth for the duration of a session, regardless of its actual usage. For voice applications, these networks have performed well, however for emerging data intensive applications, these networks do not scale effectively. As a result, IP based WANs are deployed to allow for cost efficient expansion of capacity and statistical multiplexing gain for new emerging applications. In addition, IP based WANs are built on open standards allowing inter-operability of equipment from different vendors. To allow for a smooth migration of legacy equipment, the IP WANs will be required to support legacy TDM applications in a seamless manner. The convergence of TDM traffic into the IP networks has to be well managed for maintaining the performance level of the TDM applications.

For transporting voice across IP networks, Voice over IP (VoIP) technology has emerged at the forefront. While this technology provides the most flexible way of routing telephony calls, it is very complex. The complexity of protocol inter-working between TDM and IP call processing may not be suitable and needed for many applications.

Alternatively, Circuit Emulation Service (CES) technology has emerged as an option to transport TDM trunks containing legacy applications across managed IP networks. This technology is sometimes referred to as pseudo-wire, as it emulates the TDM circuit across a packet network using virtual IP tunnel or path. The primary benefit of this technology is the cost and simplicity of deployment to support all types of legacy TDM applications without the need for complex protocol inter-working.

Figure 2 shows a reference diagram for supporting Legacy TDM applications over IP networks using CES.

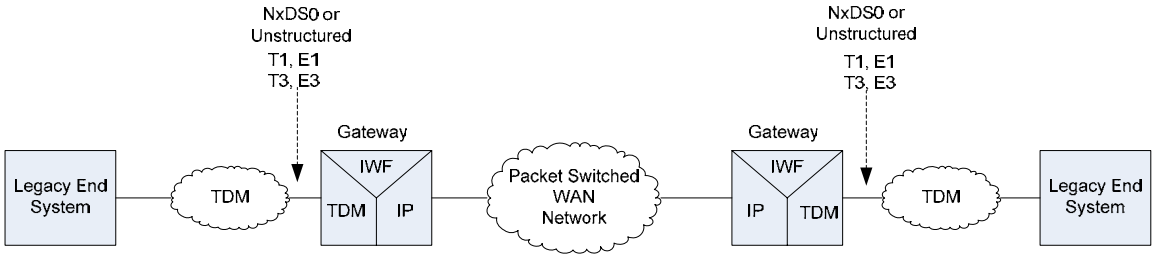

Figure 2 Reference model for CES over IP

In the figure above, the Gateway device supports CES by providing an Inter Working Function (IWF) between TDM and IP. Among standard bodies and working groups, the IETF's pseudo wire (PWE3) working group provides a standard framework for emulating structured and unstructured T1, E1, T3 and E3 circuits across IP networks. This framework provides specifications for traffic encapsulation and functions that are required for successful emulation of TDM circuits across IP networks. Figure 3 shows one such possible protocol encapsulation at the Gateway.

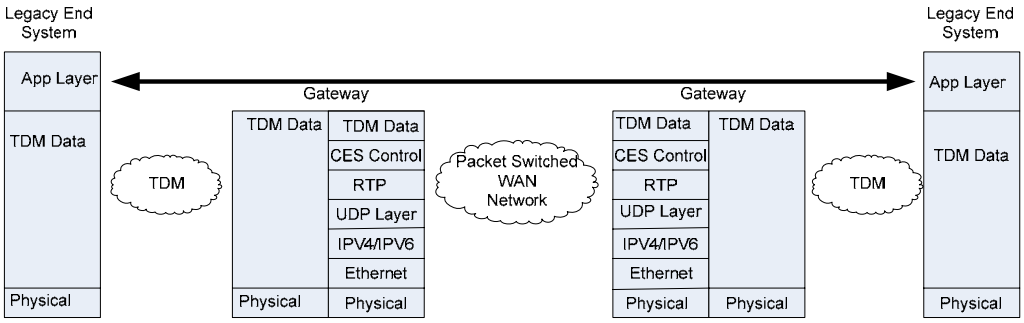

Figure 3 CES protocol encapsulation

The IWF at the Gateway accepts the TDM data from the attached circuit. This data is either in NxDS0 or unstructured format. The IP side encapsulation of the TDM data is done by adding the following layers to the payload.

CES Control Word: This layer is used to convey the status of the attached TDM circuit to the far end for re-generation of alarms and status.

RTP Layer: This layer is used for providing sequence numbers for in-order delivery and conveying synchronization information.

UDP Layer: This layer, along with the IP layer provides de-multiplexing information to the far end so that the incoming payload can be properly switched to the local TDM circuits.

IP Layer: Provides for de-multiplexing and routing across IPV4 or IPV6 networks.

Besides providing for the IWF, the Gateway's architecture must provide functionalities to overcome various challenges introduced by the IP network. The next section describes the challenges that must be overcome within the Gateway.

3. CHALLENGES

There are numerous technical challenges that arise from emulating circuit switched services across connectionless IP networks. The performance of the emulated circuits is expected to be the same as that of current TDM networks. As a result, the Gateway must be architected to overcome challenges posed by the underlying IP network to maintain the same quality of service.

3.1 Achieving Synchronization

A TDM circuit must establish the same TDM clock frequency on both endpoints of the network. A Plesiochronous Digital Hierarchy (PDH) network used to transport circuit emulated services such as T1, has built-in mechanisms, using bit stuffing techniques for transporting timing across the PDH network.

Within a packet network, there is no inherit transport of timing information and packets are discontinuous in time. In a CES application, the Gateway device must also transport timing, establishing the same frequency. The consequence of a long term mismatch in frequency is that the packet queue of the Gateway device at the egress of the network will either fill-up and overflow or empty and underflow. The direction depends on whether the regenerated clock is slower or faster than the original. This will cause loss of data and degradation of service.

One way to achieve synchronization is to provide a local same frequency clock to the Gateway devices at the endpoints of the circuit emulation. This can be done via GPS receivers, or by linking the Gateway devices to other network devices that recovers a clock traceable to the network clock strata. The disadvantage of such a method is the cost and complexity of this additional equipment.

A variation on the local clock method is for the Gateway device to use Network Time Protocol (NTP). NTP is an IP protocol used for synchronizing the clocks of hosts to servers over packet networks. NTP accounts for variable latency packet networks and is designed particularly to resist the effects of variable latency (Jitter). A disadvantage of NTP is the requirement of having NTP servers available to the Gateway devices.

Another method of synchronization is for the Gateway device at the egress of the network to employ an adaptive timing recovery algorithm. This algorithm examines the timestamps of the incoming CES packets in relation to its own local reference clock. Based on the timestamps, the algorithm can measure and extract the far-end timing information and regenerate a local same frequency TDM clock. The regenerated clock is a plesiochronous representation of the original. The fidelity of the regenerated clock is impacted by several factors including the packet rate, the packet jitter and loss within the network, and the quality of the algorithm itself. The advantage of this method is the CES itself is the source of timing with no other overhead and no other equipment required.

3.2 Managing network jitter

The variation in the inter-packet arrival time at the receiving Gateway is caused by the network jitter. The jitter in the TDM networks is of a much smaller scale than that of IP networks. This is primarily because TDM networks provide for fixed end-to-end circuits for the duration of the session, while the paths in the IP Networks are connectionless and statistically multiplexed with other sessions. The amount of network jitter depends on how well the network is engineered and how many “hops” or routers must be traversed. A well engineered IP network can be designed to control the network variation, while an unmanaged network, such as the public Internet, can produce large amount of jitter.

The Gateway’s architecture absorbs this variation in the delay by providing a de-jitter buffer. The de-jitter buffer adds additional delay to the end-to-end service. Thus, the Gateway must provide for a flexible configuration of this parameter so that it can be optimally engineered to work in a variety of IP networks, from extremely well managed to public Internet.

4. MANAGING PACKETIZATION DELAY AND BANDWIDTH

One of the factors in the overall delay for CES is the transmit delay. The most important element of the transmit delay is packetization (or packet generation delay). The packetization is delay associated with the process of accumulating payload for the CES packet from the TDM circuit. The packetization parameter is configured in terms of number of TDM bytes from which to accumulate the packet payload. A higher number results in longer packetization delay and bigger payload size. In an NxDS0 or structured application, the lowest possible packetization is one TDM frame, which contains payload from one TDM frame and will have packet generation latency of 125 microseconds, resulting in 8000 packets/seconds.

The bandwidth utilization of CES is inversely proportional to the packetization delay. This is because each CES packet contains a fixed number of overhead bytes for protocol headers. Therefore, a bigger payload size in each packet will yield better bandwidth efficiency.

The tradeoff between bandwidth efficiency and overall service delay has to be done based on the latency tolerance of the underlying application. To this extent, the Gateway's architecture must support a wide range of packetization parameters to allow for maximum flexibility to engineer CES, based on the type of application transported and the network constraints.

5. SERVICES IMPLEMENTATION

This section discusses the value added functionalities that can be integrated in to the architecture of the Gateway to provide for a smoother transition.

4.1 Echo cancellation

The legacy telephony equipment that provide for a hybrid conversion between 2 and 4 wire circuits are a source of voice echo. In the scenario where the end-to-end delay is less than 25 msec, the echo may not be perceptible. When this application is transported across the IP network, the additional end-to-end delay may be severe enough where echo cancellation is desirable. Figure 4 shows a reference model for this application.

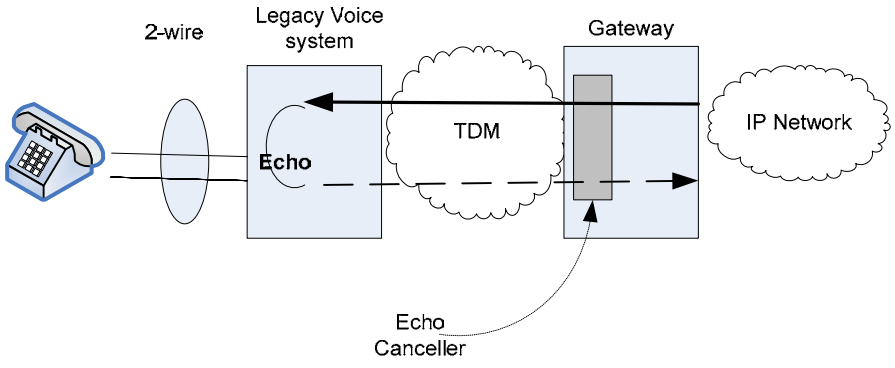

Figure 4 Integrated Echo canceller

For certain deployment cases, having an integrated Echo cancellation function within the Gateway that can be enabled based on the underlying TDM application will reduce both, the capital and operational cost of having external echo cancellation equipment.

4.2 Mitigating packet loss

Unlike TDM networks, the IP networks are prone to packet loss caused by various events within the network. The amount of packet loss and jitter are two key attributes of the underlying network and varies based on the network, with the worst case being the public Internet. There are two options for handling packet loss: error concealment or error recovery. The error concealment option is media-dependent and generally does not incur additional delay. This option is best suited for real-time TDM applications. The error recovery is an option that is suited for applications that are more sensitive to packet loss than delay. The Gateway should integrate an interoperable error recovery scheme that works in a media independent manner in a low or high packet loss network. One option is to use TCP as oppose to UDP for transport. This provides retransmission capabilities. However, using TCP has several disadvantages:

- It increases the end-to-end delay and use of system resources.
- It does not work with multicast application.
- Has bandwidth throttling mechanisms incompatible with real time data applications.

IETF's RFC 2733 provides the framework for a forward error correction (FEC) that operates at packet level, as shown in figure

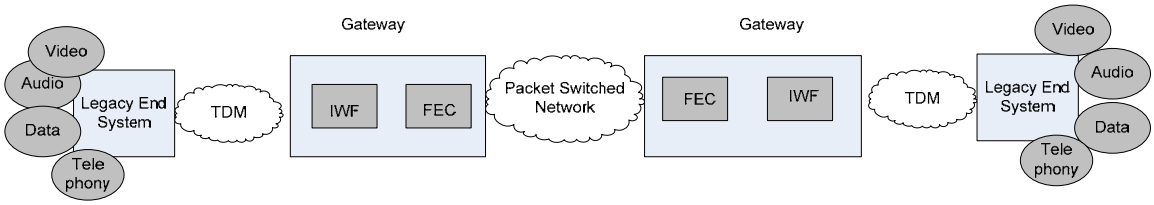

Figure 5 Integrated Forward Error Correction

The FEC operates at the application layer by grouping original data packets and sending a parity packet along with the original data packets. At the receiver, the parity packets are discarded if the original data packets are received without error, otherwise the lost data packets are attempted to be recovered from the received data packets within the group and the corresponding parity packet. The RFC specifies multiple modes of FEC operation, where each mode provides for a different degree of protection from packet loss. The FEC modes that provide higher levels of packet loss protection incur more delay and system resources, hence the Gateway must provide for a flexible configuration to allow the user to adequately engineer the FEC protection based on the network condition through which the TDM trunks are transported.

4.3 Multicasting

TDM networks provide only point-to-point connection. When legacy TDM applications require point to multipoint connections, the user has to setup and manage multiple physical TDM connections from the source to each destination. For example consider the example of Figure 6. The contribution site needs to send the content to multiple radio distribution sites.

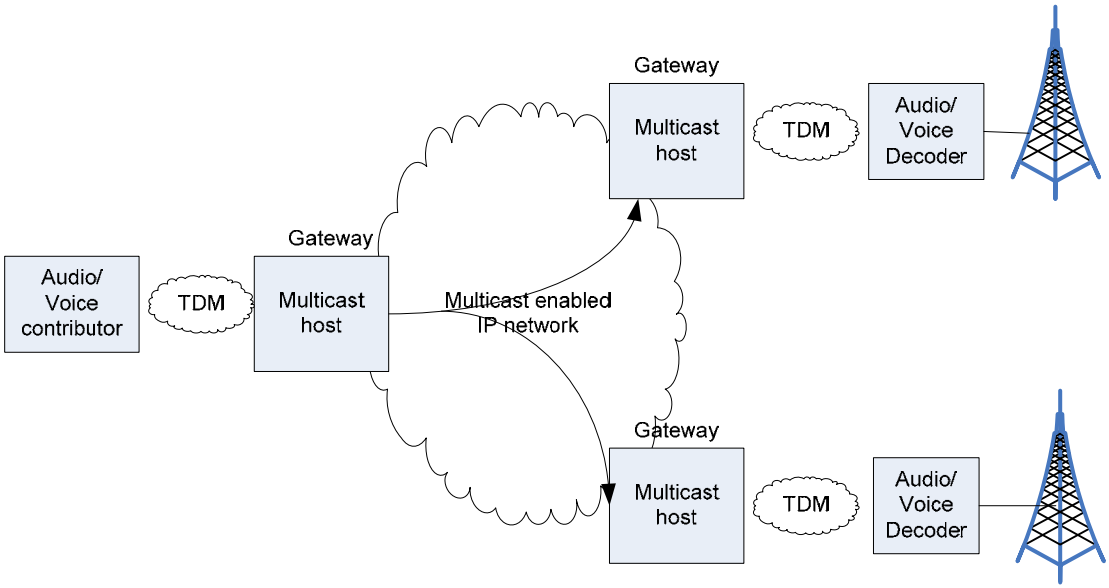

Figure 6 Integrated Multicast host

The Gateway at the contribution site performs the functions of a multicast source, while the Gateways at the distribution sites act as multicast listeners. By supporting multicasting, applications requiring point-to-multipoint connections can be easily created and managed.

4.4 Transport security

The TDM networks are perceived to be secure against eavesdropping due to their physical nature. Certain legacy TDM applications, such as tactical communications, are relying on this physical security to prevent unauthorized eavesdropping. When these applications are transported across IP networks, they become susceptible to security threats that were previously not present. The ubiquitous nature of the IP network is not only a threat for eavesdropping, but also for impersonation of a device's peer. Standard security protocols such as IP security (IPSEC) provide for secure IP transport using strong authentication and encryption schemes. Authentication provides protection against identity verification and strong encryption algorithms such as AES128 provide protection from eavesdropping. The Gateway's architecture integrates a security engine which allows any legacy TDM application to be securely transported to its destination across the IP network. Figure 7 shows a reference model for secure transport.

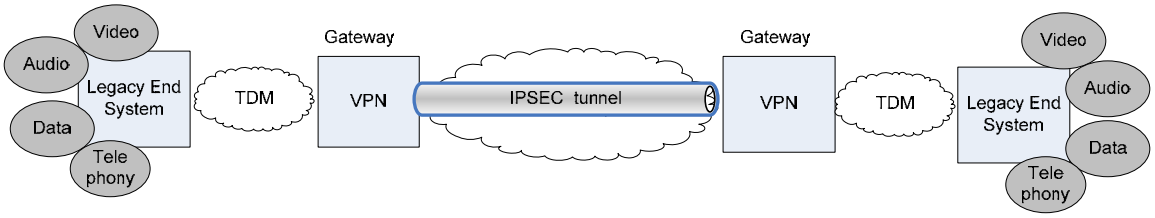

Figure 7 Integrated transport security

Having an integrated security engine not only provides for flexibility in configuring secure transport for TDM services but also reduces cost and risk of having an external equipment or outsourcing the service it to the network provider.

6. PLATFORM MANAGEABILITY

The management plane provides an important element in the operation of IP networks. The manageability of an IP device factors in to the overall operational cost of the IP network and therefore, to integrate within an existing network management scheme, the Gateway must support standardize interface for management.

The following lists some of the key management functions architected within the Gateway:

- Support of standard protocols such as SNMP and HTTP for configuration and status monitoring.
- Support of management plane security using SNMPv3 and HTTPs. These protocols provide for authentication and encryption of management messages.
- Support of protocols such as ICMP, FTP, Telnet for maintenance and trouble shooting.
- Support of user level access control and protection from common denial of service (DOS) attacks.

7. CONCLUSION

Circuit emulation services allow existing TDM based applications to be transported across packet switch networks, thus extending the life of legacy TDM equipment and providing for a smoother transition from TDM to packet based networks. The architecture of the CES Gateway provides for a critical element in maintaining equivalent performance and enabling appropriate IP services for legacy TDM applications.

8. REFERENCES

- IETF: draft-*ietf-pwe3-cesopsn-07*
- ITU-T Rec Y.1413: *TDM-MPLS Network Interworking*