IP Over Direct Links: IP Over Sonet

October 27, 2008

Abstract

The explosive growth in Internet traffic has created the need to transport IP on high-speed links. In the days of low traffic volume between IP routers, bandwidth partitions over a common interface made it attractive to carry IP over a frame relay and/or an ATM backbone. As the traffic grows, it is becoming more desirable to carry IP traffic directly over the synchronous optical network (SONET), at least in the core backbone with very high pairwise demand. Currently, the focus of IP transport continues to be data-oriented. However, a significant trend in the industry, with the emergent demand for the support of real-time IP services (e.g., IP telephony), is the development of routers with sophisticated quality of service (QoS) mechanisms. We see details of IP Transport over SONET and give an overview of the protocol and performance considerations that need to be taken into account. Then scalability and performance considerations for transport protocols and outline for functions of protocols that can be used to transport IP on very-high-speed links are discussed. Finally, the solutions to improve Quality of Service (QoS) for VoIP services are discussed.

1 Introduction

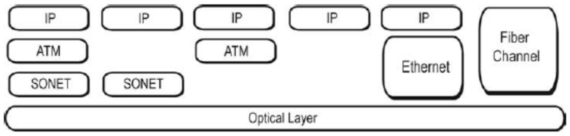
With telecom companies offering higher speed bandwidth to meet new demand, the need for scalable, integrated, and compatible testing equipment is set to increase. After a long time, carriers are shifting from 10-gigabit synchronous optical networking/synchronous digital hierarchy (SONET/SDH) to 40-gigabit bandwidth. It is no longer feasible to use four 10-gigabit bandwidth cables for the new applications, and 40 gigabit is fast becoming the standard. This also poses technological challenges such as integration for the test equipment vendors. Integrated test solutions need to offer a better price-to-performance ratio, especially for the installation and maintenance market. Another driver for the test equipment market is the installation of multi-service SONET provisioning platforms (MSPPs).

"The overall growth in Ethernet is also driving the bandwidth expansion in SONET/SDH, whether it is traditional, next generation, or optical transport network (OTN), as Ethernet requires SONET/SDH as a carrier," notes the analyst of this research. "In IP/Ethernet access, emerging applications such as video and 3G-4G play a key part." With Ethernet slowly emerging as a primary access technology, SONET/SDH and OTN will find greater deployment as the transport mechanism for the core of the network. In fact, the maturity and reliability of the SONET/SDH technology will ensure its continued deployment and consequently, enhance the market for the test equipment.

SONET/SDH Rollout in Eastern Europe and Asia Pacific to Boost the Market for Test Equipment

Countries such as Russia, China, and India are witnessing massive traditional SONET/SDH deployments due to the proven reliability of the technology. Service providers and network equipment manufacturers (NEMs) have established or are in the process of setting up bases in these countries. This factor is set to boost the market for test equipment in these regions. Local equipment manufacturers too have come up in the Asia Pacific region, generating more demand for test equipment. The shift toward next-generation SONET is greater in Europe than in North America, where companies are adopting a wait-and-watch strategy. The Eastern European market is set to grow the fastest as traditional SONET/SDH deployments do not require large investments.

"The Asia Pacific region offers the most opportunities for test equipment vendors of SONET/SDH," notes the analyst. "In Japan, there are requirements for next-generation SONET and it is also actively deploying OTN." China and India, on the other hand, continue to increasingly use traditional SONET/SDH. At present, there is not much need for next-generation SONET/SDH in China and India. Today different layered approaches are being used in optical networks, summarized in Figure 1.



Source: Cisco Systems, Inc.

Figure 1: Different Layered Approaches Used in Optical Networks Today

2 IP Over SONET

IP Over SONET or Packet over SONET/SDH (PoS) was first deployed in 1996 at 155 Mb/s, and has since become a key protocol standard for building large internet protocol (IP) backbones. Networks worldwide now carry PoS traffic at line rates of 10

Gb/s and 40 Gb/s to accommodate the explosion in internet traffic. PoS is often referred to as a ‘Layer 2 protocol’, in other words, a formal set of rules and conventions that governs how routers exchange information over a network medium. ‘Layer 2’ refers to the Open Systems Interconnects (OSI) conceptual 7-layer model that describes the process of transferring applications across a network. PoS hardware processing is mainly limited to the first three layers (Figure 2), beginning at layer 1, the physical layer. This is the media (usually fiber), physical connectors, as well as the signal characteristics carried on the medium – SONET or SDH for PoS. Layer 2, the data link layer, is responsible for reliable transit of data across the physical network link. Finally, Layer 3, the network layer, looks after the topology of the network, that is, routing and related functions that enable multiple data links to be combined into an internetwork. Layer 3 and above accounts for the software component of PoS.

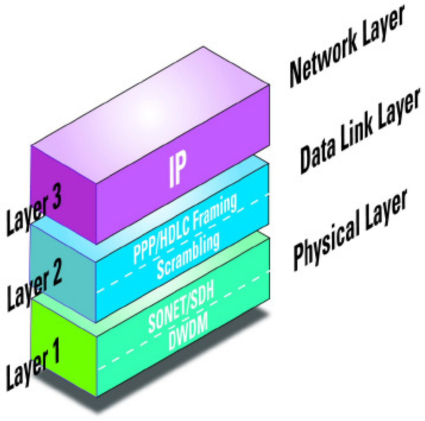


Figure 2: PoS Hardware Processing layers

2.1 Working

The layer 2 protocol used by PoS technology offers a standardized way for mapping IP packets into SONET/SDH payloads. Figure 3 gives an pictorial overview of IP over Sonet process. Data is first segmented into an IP datagram that includes a 20-byte IP header. This datagram is encapsulated via Point-to-Point Protocol (PPP) packets and framing information is added with High-level Data Link Control (HDLC) – framing. Gaps between frames are filled with flags, set to value 7E. Octet stuffing occurs if any flags or resultant escape characters (of value 7D) are found in the data. The resulting data is scrambled, and mapped synchronously by octet into the SONET/SDH frame.

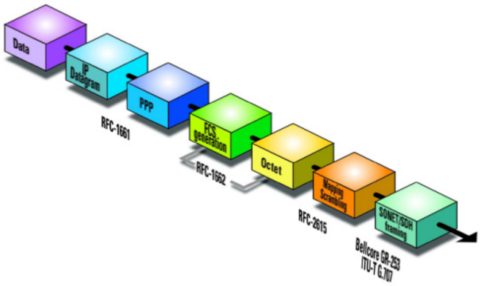


Figure 3: Working of IP/Sonet

2.2 Main Components

The main components of an IP/Sonet system are described in the following paragraphs.

2.2.1 IP Datagram

The internet protocol is a network layer (layer 3) protocol that contains addressing information and some control information that enables datagrams to be routed through a network to their destination. The role of POS is to package these IP datagrams efficiently. It is important to note that IP datagrams are not POS specific and can be transported by other means such as ATM or Ethernet. POS, therefore, can be thought of as a ‘high-speed WAN transport that leaves LAN traffic in its native format’. It is worth mentioning that the IP datagram contains a header and an information (data) field. The IP header contains the addressing and control information. The datagram can vary in length up to 65,535 octets, and although all values are possible, it is more common to have many packet sizes with few variations. For example, it is not uncommon for minimum length (40 octets) IP packets containing Transmission Control Protocol (TCP) acknowledgements to represent 40% of the traffic. Processing these small packets at wireline speeds is a serious challenge for POS hardware as it maximizes the rate of frame check sequence (FCS) calculations and stresses the HDLC framing.

2.2.2 Point-to-point protocol

Since Sonet is a layer 1 protocol and IP is a layer 3 protocol, a data link layer was additionally required, RFC 1619 selected PPP for this purpose. PPP is the encapsulation protocol (Figure 4) used by POS to transfer multi-protocol datagrams over point-to-point communication links. It carries the network layer in its information field and uses a 16-bit protocol field to identify which network layer protocol is being carried. It is important to note that this protocol field could contain different values relating to different protocols, for example, Xerox, AppleTalk, DECnet. POS uses only a small subset of these values to identify whether it is an IP packet or a PPP control protocol.

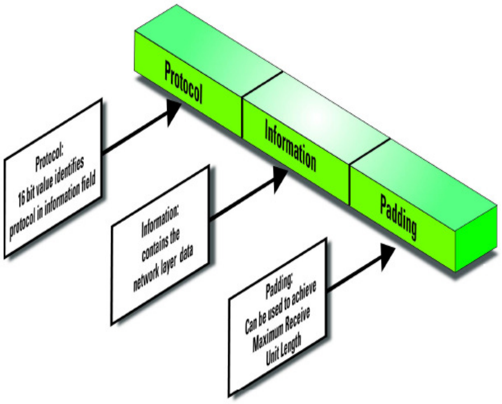


Figure 4: PPP Protocol

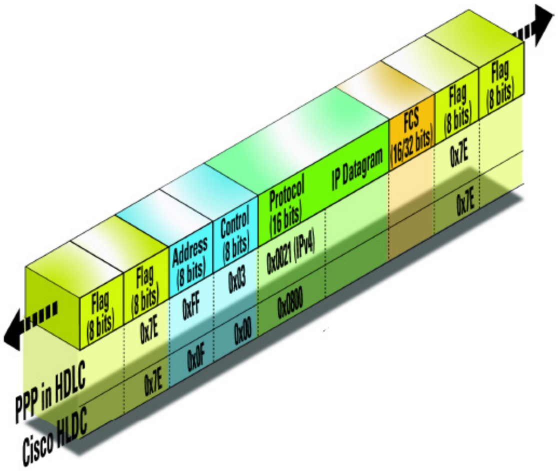


Figure 5: PPP in HDLC Framing

2.2.3 PPP in HDLC framing

PPP encapsulated packets are mapped into frames (Figure 5). HDLC framing is used to delineate the packet boundaries so that the receiver can extract them from the SONET/SDH frame. Gaps between packets are filled with standard HDLC flags of value 7E. The HDLC frame includes address, control, and protocol fields, followed by the encapsulated IP datagram. The address field is set to 0xFF for standard HDLC and 0x0F for Cisco HDLC. The control bits are set to 0x03 for standard HDLC and 0x00 for Cisco HDLC. A 16-bit or 32-bit FCS, acting as a CRC checksum, protects the entire frame and gives an idea of traffic integrity. The preference is for 32-bit FCS, however, 16-bit FCS may be used at the lowest speeds in the SONET/SDH hierarchy. The FCS field is calculated over all bits of the address, control, protocol and information fields. It does not include the flag fields or the FCS field itself.

2.2.4 HDLC and Stuffing

Octet Stuffing and Destuffing - Packets do not necessarily arrive at a router at fixed intervals. Indeed, the interval between packets varies depending on the volume and distribution of traffic between routers. A mechanism is therefore required to indicate the start and end of a frame. The octet value 7E is used for this. 7E is known as a 'flag' and is used whenever there are no packets occurring between frames. Clearly, 7E must not occur in the data, so an escape sequence is used to replace any 7E-octet value with 7D-5E. The 7D character is considered to be the 'escape' character so it too needs to be replaced. 7D is converted to 7D-5D. The entire process is reversed at the receiver. The example below shows how the bandwidth could increase dramatically if many replacements occurred.

2.2.5 Scrambling

Payload scrambling is implemented in hardware. It is transparent to the user and adds to network stability. The addition of payload scrambling occurs when the HDLC framed PPP packets are inserted into the SONET/ SDH frame. POS scrambling ensures that a malicious user cannot bring the network down by sending patterns which result in SONET/SDH layer low transition- density synchronization problems, emulating the SONET/SDH frame synchronous scrambler pattern, or replicating the SONET/ SDH frame alignment word. POS uses the $x^{43}+1$ self-synchronous scrambler (also used by ATM) to alleviate these potential security problems.

2.3 But how secure is it?

Predicting the output of the $x^{43}+1$ scrambler requires knowledge of the 43-bit state of the transmitter as the scrambling of a known input is begun. This requires knowledge of both the initial 43-bit state of the scrambler when it started, and every byte of data scrambled by the device since it was started. The odds of guessing correctly are 0.543, with the additional probability of 1 in 127 (due to the x^7+1 SONET/SDH scrambler) that a correct guess will leave the frame properly aligned in the SONET/SDH payload. This results in a probability of 9e-16 against being able to deliberately cause SONET/SDH-layer problems. With internet traffic, this level of security is crucial.

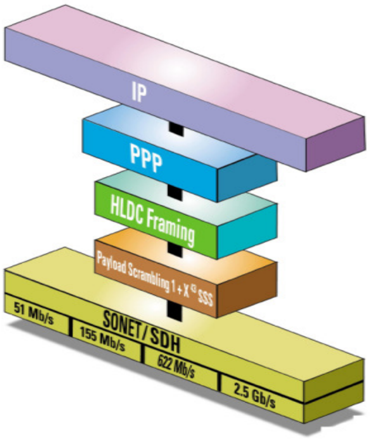


Figure 6: IP/Sonet working with PPP protocol, HLDC Framing and Payload Scrambling

3 Need for IP Over Sonet

Networks must have longevity and scalability with an initial low cost of ownership. A successful network must also use bandwidth efficiently. To achieve these goals, we must design networks based on the type of traffic it carries and choose between a connection-oriented and a connectionless network early in the design process. Choices will depend on the applications running on the network. If an IP-based network is selected because the true nature of the infrastructure is data-centric, then ample buffering must be seeded in the network to deal with the round-trip delays and packet bursts.

Packet-over-sonet technology implemented with new gigabit switch routers can meet these requirements. Consideration of IP over sonet when a business model is IP-centric is essential. Packet over sonet leverages existing sonet technology and delivers simple and efficient bandwidth use, Layer 3 QoS, and scalability. It can synchronize off existing sonet rings and support the required bytes in the sonet overhead for reliable, cohesive integration.

3.1 IP Quality of Service (QoS)

To deliver efficient network manageability and scalability, today`s data networks are based on a hierarchical architecture that includes the backbone as well as the service node layers. The major function of a router in the backbone is to provide performance and scalability, to switch millions of packets per second, and to scale to higher rates. At the service nodes or the distribution layer, the main goal of an edge router is to provide features such as security, access control, and support for differentiated services through class-of-service (CoS) offerings.

With telecommunications deregulation in full swing, incumbent local exchange carriers will need to ward off competitive risks within their regions by raising the bar on the level of service offerings and to focus on providing value-added services. Simply providing more bandwidth is not a competitive way of doing business. Service providers can up the ante by giving their customers guaranteed and differentiated services through Internet protocol-based quality of service (QoS) products, allowing the customers to rely on their network for their mission-critical applications and increase the revenue earning for the service providers.

High-end routers can support this level of service through Layer 3 QoS offerings. With the three precedence bits in the Internet protocol header (see table), it is possible to provide differentiated CoS by utilizing random early detection (red) and weighted red. As packets enter the network, their precedence is set by the edge routers; this precedence is used to determine the queuing of packets through the network.

3.2 Packet-over-Sonet applications

Internet protocol (IP)-powered networks can support a vast number of applications. With the right optics in place and support for various Synchronous Optical Network (sonet) overhead bytes--such as K1 and K2, which allow 4-fiber route diversification--network providers can literally eliminate the need for the intermediate sonet network elements. The primary application would be to light dark fiber to provide router-to-router connectivity, router-to-sonet/Synchronous Digital Hierarchy (SDH) connectivity, private peering and bypass of congested network access points, and wavelength-division multiplexing (WDM) connectivity for sharing fiber.

Carriers, utilities, and competitive local exchange carriers are the prime candidates for deploying such IP-powered transport platforms in their networks. The following application represents a traffic aggregation by backhauling packet-over-DS-3 (44.736 Mbps) to the Internet backbone and using metropolitan Sonet/SDK ring networks through high-speed channelized router connections.

In recent years, DS-3 has become the most common drop interface at the customer premises, replacing T1 services. The accompanying figure shows the data network as an overlay to the sonet interoffice transport facility. Today`s IP network elements (IPNES) enable the connection of these networks through high-speed channelized interconnects. The traffic that originates in the data network rides a specific Synchronous Transport Signal (STS), which traverses through the channelized OC-12 (622 Mbps) to the sonet transport local access and transport area. The sonet gateway node, or the digital cross-connect in the central office, peels off each STS and drops or passes it through the network as required. High-speed channelized optical interfaces on the routers efficiently connect the two networks. Depending on the distance and topology involved, the IPNES can light the dark fiber in order to bypass the telephone company interoffice sonet ring, or the network can be route-diversified by taking both the sonet telephone company path as well as direct private peering between the two IPNES.

Key benefits for the service providers in this application include bandwidth savings due to the use of channelization for interconnection, reliability through automatic protection switching support, lower cost due to the elimination of the intermediate sonet network elements.

4.0 Why not use ATM?

It's not as efficient as using IP over Sonet. The wide area circuits are the most expensive and for IP backbone networks, Internet service providers (ISPs) are increasingly turning to IP directly over SONET technology. The main reason given by most ISPs is that they cannot afford the ATM overhead "cell tax." The hubbing effect of the architecture shown results in highly utilized backbone links. It is well known that using ATM to transport IP adds a 10 percent ATM "cell tax" because of the overhead of the ATM header; however, that overhead percentage fails to take into account the distribution of packet sizes. Recent traffic studies have shown that nearly half of all packets are 40 or 44 bytes. Neither side can be encapsulated into a single ATM cell using the IP over ATM mapping described in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1483. The average ATM overhead across the entire distribution of packet sizes, seen in Internet backbones today, is roughly 25 percent. By comparison, the IP-over-SONET overhead tax on the same distributions is roughly 2 percent. Thus, ISPs planning IP over ATM backbones need to account for the 25 percent ATM cell tax when planning their networks.

Obviously, there is much more to the IP over ATM vs. IP over SONET debate than the overhead efficiency of each mapping. In particular, carrying IP directly over SONET uses up the whole SONET link bandwidth for traffic between a pair of routers even when the traffic volume requires a fraction of it. This breakage penalty needs to be weighed against the ATM overhead and the cost of operating ATM equipment. Another reason for mapping IP directly over SONET without the intervening ATM layer is the scalability of the solution. In 1998, Most ISPs backbone routers were operating with OC-3 (155 Mb/s) and OC-12 (622 Mb/s) links. With no slowdown in IP traffic growth expected, many ISPs are planning to upgrade their backbone router links to OC-48 (STS-48c) by the end of 1998. The ATM segmentation and reassembly (SAR) function (required for the IP-over-ATM mapping) becomes increasingly complex as the interface speed increases. Currently, interfaces up to OC-12 speed can use ATM SAR chips while OC-48C interfaces have begun to appear with direct SONET interfaces. Thus, IP over SONET was the first technology to the marketplace to meet ISPs' Internet backbone capacity expansion needs beyond OC-12 (622 Mb/s).

5 Advantages of IP over Sonet.

- Simple
- Bandwidth efficient
- Scalable
- Fault Tolerant (with Sprint's fiber network)
- 1:1 redudancy
- Only one infrastructure to manage
- Technology upgrade possible on link basis
- Supports 350ms BW delay product at 155Mbs.

Packet over Sonet places the IP layer directly above the sonet layer and eliminates the overhead needed to run IP over ATM over Sonet while offering Quality of Service guarantees. Packet over Sonet better accommodates fast growing Internet and intranet traffic and offers the first reliable way to create multiservice networks based on IP. Service providers such as GTE Internetworking, Qwest, Sprint and UUNet have already deployed it. The technology also is promising to eliminate intermediate Sonet add/drop muliplexers (ADMs).

Advances in IP switching speeds and economy and the development of IP-based voice and video products made this configuration possible last year. Underlying the shift toward packet over Sonet are the changing realities of business, network demand and applications. Meanwhile, a dramatic collapse of network Layers 2 and 3 is occurring through improved Sonet transport, digital cross-connect and routing integration. Sonet platforms are melting into the digital cross-connects. As difficult as it may seem, vendors are toying with the idea of supporting Layer 3 services in their ADM/cross-connect platforms, and major RHCs are implementing digital cross-connects with full Sonet ADM and ring functionality.

From the data side, low speed drops no longer exist. Demand for bandwidth has pushed major internetworking vendors to migrate to Sonet rates of OC-12 (622 Mb /s), OC-48 (2.5 Gb/s) , OC-192 (10 Gb/s) and OC – 768 (40 Gb/s). Vendors also have pushed the limits by supporting Sonet features such as automatic protection switching and the capability to interpret and provision various Sonet overhead bytes. With the right optics in place, who needs a plain vanilla Sonet box?

Finally, changes at the network edge make optimizing core switches, routers and backbones for IP increasingly important. Despite early hopes that ATM would provide service to the desktop, the network edge is dominated by Ethernet, which has proved to be the most scalable, economical and manageable LAN protocol. Ethernet also has data rates from 10 Gb/s to 100 Gb/s, port costs also costs very less, and network management tools and techniques familiar to most network managers.

Now that Ethernet accounts for more than 80% of the installed base of network ports and network interface cards, optimizing the network core makes sense. Efficiency matters - to grasp the benefits of packet over Sonet, it's necessary to compare it with the traditional ATM over Sonet architecture. ATM has a number of strengths: It can operate over Sonet links at speeds up to OC-48. It provides QoS guarantees suitable for voice and video and can accommodate multiple services and protocols. For telecommunication companies' networks carrying thousands of voice conversations, it's still the way to go.

Historically, IP could not operate at high speeds or provide QoS. But those shortcomings are a thing of the past. Packet over Sonet breaks through the old performance limitations of IP, scaling up from OC-3 to OC-192 today, with OC-768 (10 Gb/s) speeds becoming easily available. New IP QoS techniques easily can be delivered via packet over Sonet using the three precedence bits in the IP header, allowing deployment of voice, video and other isochronous services.

High-end routers such as the Cisco 12000 series that connect IP networks to Sonet rings eliminate expensive intermediate ADMs. By combining the support for Sonet automatic protection switching with long- and intermediate-reach optical interfaces, automatic protection switching protects against fiber cuts or module failure. Packet over Sonet builds an optimized infrastructure based on the dominant protocol. Other benefits depend on user and application, and that requires closely viewing different networking environments, users and common applications.

Packet over Sonet deployments - for telecommunication companies, competitive LECs, Internet service providers, campus LAN managers and others with dark or dim fiber, packet over Sonet offers considerable advantages over ATM. A widespread increase of this technology's deployment worldwide in the enterprise and service provider markets is occurring.

For example, Sprint deployed packet over Sonet using routers to boost its Internet backbone speed to 622 Mb/s in 1998. The carrier found it could increase bandwidth 400% by running live traffic over full line speed OC-12 connections, providing faster access to Web pages, real-time applications and file transfers for its customers worldwide. Among the most important applications for packet over Sonet is leveraging existing Sonet infrastructure for data services, lighting dark fiber and aggregating traffic from edge routers, and consolidating the multiservice and IP-optimized networks typically run in parallel by major carriers. Although this may seem to be a diverse set of applications, they all provided a rapid return on investment, as well as scalability, manageability and improved reliability.

Today's routers can connect data networks through the high-speed OC-12 channelized interconnect. The traffic that originates in the data network rides a specific synchronous transport signal, which traverses the OC-12 to the Sonet transport. The Sonet gateway node or the digital cross-connect in the CO peels off each synchronous transport signal and drops or passes it through the network, as required. High-speed channelized optical interfaces on the routers connect the networks. Benefits for service providers include:

- Bandwidth savings due to the use of channelization for interconnection
- Reliability through the automatic protection switching support
- Lower capital and operating costs by eliminating the intermediate Sonet elements.

One of the most important applications for packet over Sonet is lighting the dark or dim fibers available in many campuses and enterprises and in the rights of way owned by utilities. With packet over Sonet line cards, an ISP or enterprise network designer can scale the speed of interconnecting Sonet links without experiencing the overhead tax associated with other transmission methods.

Today's networks are not homogenous. The typical telco/ISP interworking includes both a multiservice and an IP-optimized network. The core gigabit switch router interfaces with the ATM cloud, routing digital subscriber line access multiplexer traffic to the Internet backbone. The IP traffic can traverse the fiber between the two core routers, at OC-12 and OC-48 optical rates with Sonet automatic protection switching. This ensures reliable private peering and bypasses the congested network access points. The data also can ride the interoffice Sonet ring and traverse the telco ring infrastructure to get to the Internet backbone.

Implementing packet over Sonet Packet over Sonet promises to offer significant advantages by providing efficient bandwidth use, higher performance and greater simplicity. But implementation details will determine whether it becomes widespread. To be successful, packet over Sonet implementations must provide support for Layer 3 switching, multicast/broadcast controls, traffic management and congestion control features that enable efficient network bandwidth use. They also must offer QOS that allows customers to support critical or delay-sensitive applications such as voice and video.

As data becomes the dominant part of the backbone payload and as routers scale up to higher rates, seamless integration with Sonet/SDH networks and equipment from multiple vendors becomes essential. Despite minor differences, interoperability between these standards remains vital to service providers. Clearly, network managers must optimize their networks for the dominant applications. Throwing bandwidth at the problem isn't enough. Despite competition between packet over Sonet and

ATM, with "net-heads" on one side and "Bell-heads" on the other, the two technologies can and should co-exist. It's still important to mark separate territories based on each technology's strengths and weaknesses.

Packet over Sonet uses existing Sonet infrastructure to better support IP and is optimized for the Ethernet infrastructure that now extends to millions of Web users. It offers scalability to allow IP traffic to grow, more efficient bandwidth utilization and support for new IP applications such as voice, multicast and video. As the light at the end of the tunnel-or fiber conduit-packet over Sonet unifies existing infrastructure with IP, supports richer set applications and delivers a dramatically cheaper ownership. For service providers, quality of service (QoS) brings the service differentiation offering that companies need. By selling the QoS, customers can hand off their critical services easily, and they can increase their revenues by selling differentiated services. Major data companies such as Cisco support Layer 2 and Layer 3 QoS.

Sonet's widespread acceptance in high-speed data transport lies partly in its ability to switch transport lines automatically when a problem is detected. The seamless traffic rerouting causes no noticeable data loss or service disruption on the network. This capability, automatic protection switching, is important in today's data- and time-sensitive environments and to the operating company as well as the end user.

Without it, the disaster scenarios of megabits of lost or corrupted data would read like a "Twilight Zone" script. Imagine the New York Stock Exchange, the NASDAQ or the World Bank transferring a major file between New York and Los Angeles. Suddenly, the fiber optic cable starts taking hits. A little scary, isn't it? This scenario is not restricted to global business deals. Joe the mechanic, with his ISDN line, could be on-line ordering parts for your car from a dealer or warehouse when the hits occur. Your new wheel covers become a trans-axle assembly. Sonet automatic protection switching is complex and robust, and automatic protection switching schemes are defined for various Sonet network architectures. Protection switching is provided from one fiber to another on a 1+1, 1-to-1 or 1-to-N basis. The following example looks at linear network architecture with a 1-to1 ratio of fibers because it’s easiest to view automatic protection switching principles there. Sonet technology uses two overhead bytes, K1 and K2, to initiate bridging and switching. Together, these bytes constitute the automatic protection switching channel.

Automatic protection switching implements a bit-oriented protocol for time-critical switching operations between two nodes. The nodes are the headend and tail end. The tail end asks for automatic protection switching action in response to incoming errors. The headend responds by executing a bridge between the working fibers and the protect fibers. Headend to tail end communications are accomplished through the automatic protection switching channel. Error detection occurs when the tail end recognizes a signal-fail or signal-degrade condition on the working transmit fiber from the headend.

The headend constantly receives K1 and K2 bytes from the tail end. When the tail end recognizes a signal-fail or signal-degrade condition, the next frame the tail end sends has the K1 and K2 bytes, which are coded in the Sonet line overhead to begin automatic protection switching action. The headend receives the K1 and K2 bytes from the tail end and establishes a bridge between the working transmit fiber and the protect transmit fiber. Dual or duplicate service is now transmitted across the working and protect transmit fibers. The headend codes K1 and K2 bytes in the Sonet line overhead to the tail end. These code messages are called reverse request. The tail end receives the K1 and K2 bytes and switches traffic from the working transmit fiber to the protect transmit fiber. The tail end also establishes a bridge between the working receive and protect receive fibers. The tail end again codes K1 and K2 bytes across the working-receive and the protect-receive fibers back to the headend. The headend receives the K1 and K2 bytes and bridges the two fibers. The headend switches all traffic from the working-receive fiber to the protect-receive fiber. Traffic now has been switched from the original working transmit and receive fibers to the protect transmit and receive fibers. This process began when the errors were first detected and completely bridged and switched in 50 milliseconds. About one second passed. If we were using Sonet transport at the OC-192 level of 9.95328 Gb/s, this would equate to 5376 DS-1s or 129,024 simultaneous operating channels. The automatic protection switching detected, bridged and switched all of this traffic, not once, but 20 times while we counted off one second.

6 Performance of IP Over Sonet Vs IP Over ATM

The crucial technical problem in supporting multimedia services over the current internet protocol is that real time traffic must reach its destination within a present delay and with some tolerance of jitter. This is complicated because the original IP that operates on a best effort basis permits dropping packets on the way to a destination. Alternatively, under IPv6, network hosts will be able to identify packets that belong to a particular traffic scheme.

6.1 Network Models

The following network topologies have been simulated to analyze the performance of both real-time and non real-time traffic in IPv4 network. The network performance study has been carried out by comparing the performance of those applications over point to point (PPP) and ATM. HTTP represents the non real-time applications while Voice over IP (VoIP) represents real time data. It is assumed that the packets arrived and queued in the buffer according to service rate. This will result in zero packet loss. The following figures 7 and 8 illustrate network models of HTTP over PPP and VoIP using ATM respectively.

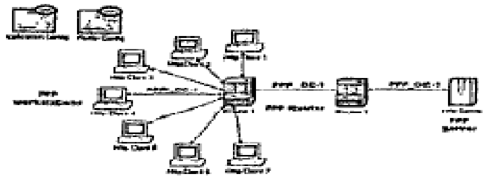


Figure 7 : Network Topology for HTTP

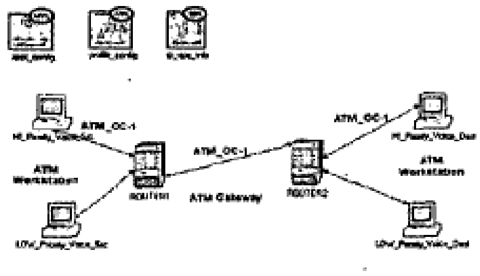


Figure 8: Network Topology for VoIP

6.2 Simulation Results

The following figures show the simulation results for both HTTP and VoIP using PPP and ATM in terms of end-to-end delay, throughput, link utilization and jitter. It can be seen in figure 9 that HTTP suffers less end-to-end delay using PPP compared to ATM as in figure 10. Thus it can be concluded that PPP provides better performance in transferring non real-time applications rather than ATM. The reason for that is because ATM is connection oriented protocol that requires virtual circuit to be setup for each flow. Besides that it consumes another layer of overhead in addition to the Sonet Overhead. The graphs in figure 3a also illustrate the graph of M/M/1 curve. This curve is obtained by manipulation of the basic formulae; $\rho = \lambda/\mu$ making HTTP/PPP comparable to the queuing theory.

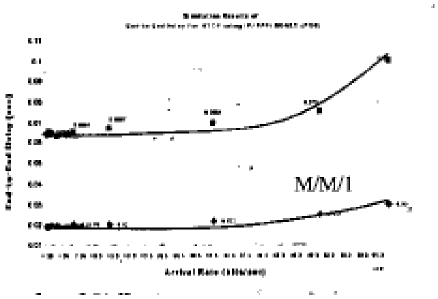


Figure 9 : Simulation Results of HTTP using PPP and M/M/1

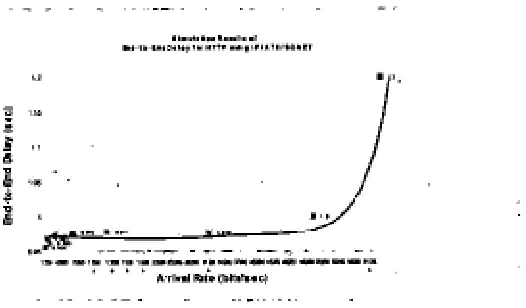


Figure 10: Simulation Results of HTTP using ATM

However, ATM seems to provide better performance for real-time application compared to PPP **as** illustrated in Figure 11. VoIP applied over the ATM produced less packet end-to-end delay compared to VoIP using PPP. ATM is a best choice when transmitting voice compared to PPP because its small, fixed length cells are well suited to transfer voice.

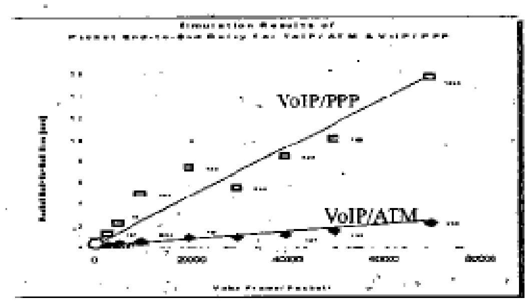


Figure 11: Packet End-to-End Delay for VoIP /ATM/SONET & VoIP/PPP/SONET

Throughput statistics represents the average 'number of bits successfully received by the receiver channel per unit time; in bits per second. When the delay gets higher, the throughput tends to become lower. This applies to both the network models. Recall from the above graphs that have been discussed, IP/PPP/SONET packet end-to-end delay is much lower when compared to IP/ATM/SONET, therefore its throughput is higher. This can be viewed from the graph in Figure 12.

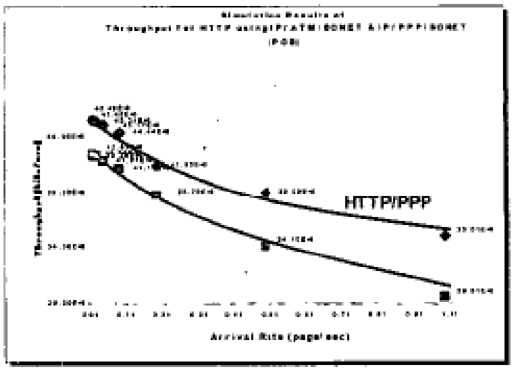


Figure 12: Throughput for IP/PPP/SONET & IP/ATM/SONET for HTTP Applications

As for the real time application, its throughput for IP/ATM/SONET is higher at the expense of **low** end-to-end delay as been discussed earlier. This is illustrated in Figure 13. For instance, the throughputs for sending one voice frame/packet in VoIP/ATM Network overshoot to 84,852 bits/second whereas only 29,652 bits/second when transmitting in VoIP/PPP/SONET. The reason behind this occurrence is that in IP networks, unlike ATM networks do not offer guaranteed *QoS,* they can he designed to support something more along the lines of GoS (Grade of Service) on a best-effort basis only. Besides that it is also due to the ATM network that able to handle different type of service required. The ATM services categories are used by the end system to identify the type of service required. Hence, ATM could provide better performance in terms of throughput in real-time traffic.

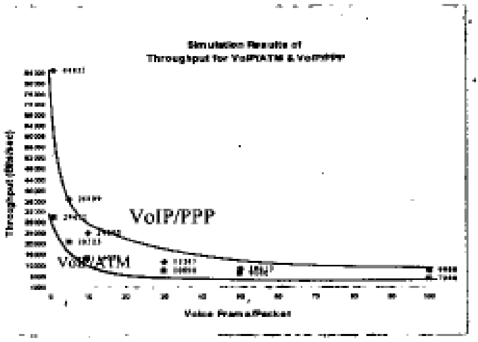


Figure 13: Throughput for VoIP/ATM/SONET & VoIP/PPP/SONET

Packet delay variation or better known as jitter is another factor that affects delay. Jitter occurs when there is a variation between when a voice packet is expected to be received and when it actually' is received, causing a discontinuity in the real-time voice stream. The larger the allowable delay variation, the longer the real delay in delivering the data and the greater the size of the delay buffer required at receivers. By analyzing Figure 14, it illustrates that jitter experienced by the VoIP/PPP/SONET is higher than VoIP/ATM/SONET. The jitter corresponds to the end-to-end delay.

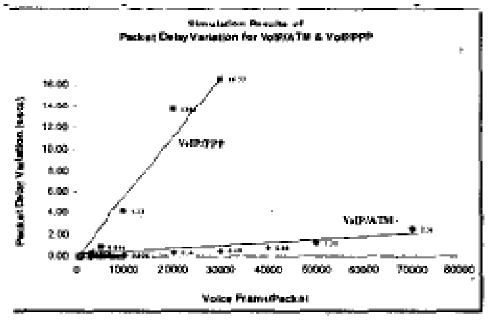


Figure 14: Packet Delay variation for VoIP/ATM/SONET & VoIP/PPP/SONET

Link utilization represents the percentage of the consumption of an available bandwidth channel. It corresponds to the throughput that was discussed in the above section. Higher throughput leads to higher utilization.

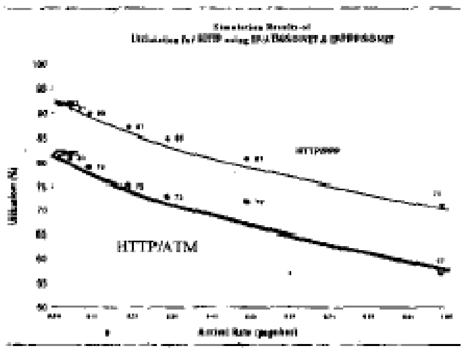


Figure 15: Link Utilization for HTTP using IP/PPP/SONET & IP/ATM/SONET

From Figure 15 it can be seen that PPP is a very efficient way to transport IP. IP can achieve up to 95% of the available line rate when running over PPP compared to 80% of the available line rate when running over ATM. The difference is the overhead or cell tax required to support ATM. The simulation results have shown clearly that transporting IP using PPP as the interface does not provide any quality of service especially for real-time application. Although ATM shows better performance for real-time traffic, implementing ATM could lead to higher overhead and it is not economically viable to bring ATM directly to the desktop. The performance of 1P service using PPP can be further improved by implementing various techniques in an IPv6 environment described in next Section.

7 QoS Improvement measures

The simulation results discussed in previous section have shown that IPv4, which is based on best effort routing, is insufficient in supporting QoS for real time applications. The IPv6 network with some refinements like IntServ, DiffServ and MPLS can provide QoS for particularly real time traffic such as voice and video.

7.1 Integrated Services (IntServ)

Integrated Services encompasses various types of service, including best-effort and real-time service, and allows for bandwidth reservations. It was concluded that using IntServ, .routers must be capable' of reserving resources in order to provide special QoS for specific user packet streams or flows. To reserve resources, IETF defined the resource reservation protocol (RSVP), a network-control protocol that lets IP-based applications request *QoS* treatment for their data flows. Host applications use RSVP to request the necessary *QoS* (such as guaranteed bandwidth) from the network for specific data flows. The QoS request is sent through all the routers along the path of the data flow on a hop-by-hop basis, and at each device the RSVP process attempts to establish and maintain a reservation state to provide the requested service. RSVP is receiver-oriented, meaning that the receiving host is responsible for requesting resource reservations and transmitting these, back to the sender. This way, a receiver can request a QoS that is tailored to its particular requirements. By being receiver-oriented, RSVP avoids the problem of a sending host transmitting a bigger-quality video stream than the receiver can handle.

7.2 Differentiated Services Architecture (DiffServ)

In DiffServ, traffic is divided into a small number of forwarding classes and resources are allocated on a per class basis. The desired performance levels are achieved through the proper mix of provisioning, prioritization and admission control. Simplicity is fostered by the fact that these flows are grouped into a relatively small number of aggregates that receive a limited number of differentiated treatments throughout the network. The IETF's DiffServ work is largely based on the type-of-service (ToS) and precedence field within the IPv6 header. The IP precedence field was first defined in IP to indicate a certain way by which a given IP datagram should be queued at routers or other network devices over an end-to-end connection.

7.3 Multi-Protocol Label Switching

One of the MPLS features that would be important in providing *QoS* is the ability to set up label switched paths for different type of services although it is found in that MPLS is more suitable for non real-time applications. A performance studies done in recent times have shown that the network using MPLS produced less end-to-end video packet delay compared to the network using normal IP routing. On top of that, MPLS technology has the advantages for both network administrator and the users. It provides network administrator with several tools for traffic engineering. Furthermore, MPLS offers QoS guarantees that are offered by data transport services such as Frame Relay and ATM without enquiring any dedicated lines. Network administrator can define a Label Switched Paths (LSPs) for example; real-time traffic such as voice will be routed though the most reliable and the highest performing sections of the network while less crucial traffic such as email is sent across the slower sections. MPLS based service provider edge equipment is designed to communicate with Customer Premises Equipment (CPE) in a standards-based environment. This is an advantage for the client, as the clients will not have to deploy new equipment. Furthermore, the implementation of MPLS is not only suitable for large-scale network operators but also can benefit a wide range of network users, from service providers, enterprise and any size of businesses with the growth in functionality and cost-effectiveness of data transport services.

The core function of MPLS is the generation of a short fixed-length label that acts as a shorthand representation of an IP packet's header. In MPLS, the IP packets are encapsulated with these labels by the first MPLS device that they reach as they enter the network. Label Edge Router (LERs) at the network's edges will analyze the IP header and selects the right label to encapsulate with the packet. The analysis process is totally different from normal IP routing where IP header just carries the destination address. At the subsequent nodes within the network, MPLS label is used to make the forwarding decision for the packet. Label Switch Routers (LSRs) will route the packets based on the instructions contain in the labels. Finally, another edge router will remove the labels once the MPLS labeled packets leave the network.

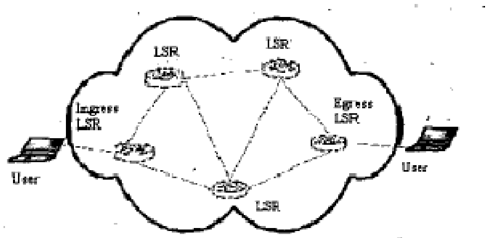


Figure 16: The MPLS Domain

8.0 Conclusion

IP backbone providers are seeking expedient, cost-effective solutions for providing high-capacity interconnection between gigarouters. IP-over-SONET technology is a leading solution to this need. Apart from some flaws with the early IP-over-SONET specification which have subsequently been fixed, IP directly over SONET using HDLC provides a robust, reliable, bandwidth-efficient solution for the transport of IP from 155 Mb/s to 10 Gb/s rates. Extensions to the specification will be necessary to extend the transmission range to beyond 10 Gb/s.

References

[1] Packet over SONET / SDH (PoS) – Technical Paper , Agilent Technologies.
[2] RFC 1619 – PPP over SONET/SDH
[3] RFC 1662 – PPP in HDLC Framing
[4] RFC 1661, The Point to Point Protocol (PPP)
[5] Optical Networks: DWDM and SONET 2003 – 2008, April 2003 , The Insight Research Corporation.
[6] BOGDAN JAKOBIK and PIERRE- YVES PAU - Ethernet over SONET delivers bandwidth efficiency to the IP World , Nortel Networks
[7]http://www.iec.org/online/tutorials/ip_int/topic08.html
[8]http://lw.pennnet.com/articles/article_display.cfm?article_id=34713
[9] http://en.wikipedia.org/wiki/SONET
[10] J. Manchester *et al.*, "PPP over SONET/SDH," Internet draft, <draft-ietf-pppsonet-00.txt>, Oct. 1997
[11] B. Doshi, S. Dravida, E. Hernandez-Valencia, and J. Manchester, "Scramblers for PPP over SONET/SDH: Performance Considerations and Analysis," T1X1.5/97-129, Dec. 1997.
[12] "Synchronous Optical Network (SONET) Transport Systems: Common Generic Criteria," Bellcore GR-253-CORE, issue 2, Dec. 1995.
[13] K. Thompson, G. J. Miller, and R. Wilder, "Wide Area Traffic Patterns and Characteristics," *IEEE Network*, Dec. 1997.