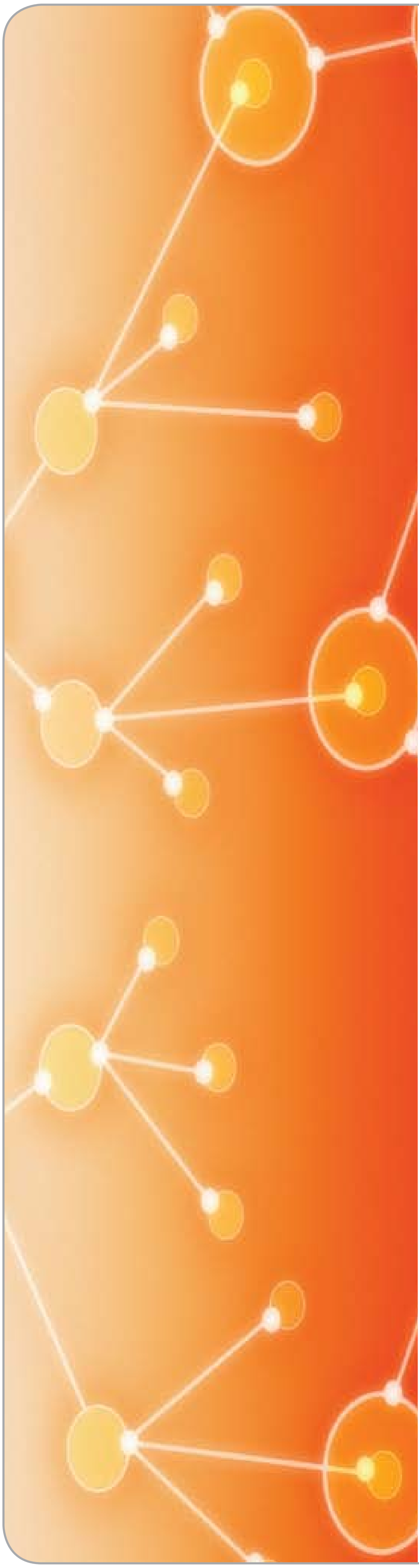
WHITE PAPER



Navigating Circuit to Packet Network Migration

ADC KRONE

Navigating Circuit to Packet
Network Migration

KRONE

Executive Summary

Navigating the migration of circuit switched to packet switched networks is a complex affair. In pursuit of improving overall network efficiency and making advanced data services available, service providers must simultaneously protect existing TDM revenue while investing in new packet-based technologies.

The good news is that the circuit switched architecture, which accounts for the bulk of service provider revenues, is highly reliable. The bad news is that this massive centralized processing network is neither fully depreciated nor built for packet switching. Taken together, the migration to a more efficient, distributed packet switched network will be an evolutionary process that will require integration with the TDM network.

The emerging hybrid network of TDM and packet-based assets is the precursor to a unified platform for transport of voice, data, and multimedia services. This paper will examine why a hybrid network is inevitable and explore the challenges that service providers face in deploying packet both at the edge and in the core of the network. In addition, this paper will show that a key reason for the exceptional reliability and 99.999% availability of TDM services can be traced to the arena of products that connect, protect, and manage cables. It is this foundation of connectivity that will also play an important role in creating efficient, reliable, and high performance packet switched networks, too.

Migration Promises a Hybrid Network for Some Time

The benefits of migrating to packet technology are compelling—new and higher margin services, better network performance, improved capacity, savings in transport, and cost reductions in operations. All of these benefits are embedded in the main differences between circuit switch and packet switch technologies.

The packet based network routes small units of data called packets through the network based upon a destination address contained in each packet. The network provides diverse paths for movement of data packets. Unlike circuit-switched networks that require a dedicated circuit for the duration

of a connection, packet switched networks share the same path among many users in the network while decisions on how data is routed are made farther out in the distributed network.

Yet traditional packet routing causes delay that makes voice over packet difficult, at least for those customers who expect the same highly reliable, high quality voice services as available through circuit switched networks.

Problems of jitter and latency that make QoS difficult to administer for voice over packet switched networks are being overcome with new technologies. Still, voice revenues from circuit switched networks are enormous and will likely continue to dwarf revenues generated from faster-growing packet-based networks for years to come. Service providers are surely motivated to invest in packet switch technology, but not at the expense of current monthly bill business. With capital limited and overbuilding taboo, service providers continue to seek ways to leverage the existing circuit switched network in delivery of voice, data, and multimedia services. Migration to next generation networks will therefore be evolutionary, not revolutionary. The end game may someday be a converged network. In the meantime, efficient delivery of services is going to require connections to TDM network assets.

It is common to refer to packet networks as "connectionless". From a data transmission perspective, this is an accurate description because packet switching does not require a dedicated circuit. However, "connectionless" is misleading. In the emerging hybrid TDM/IP network as well as in pure packet switched networks of the future, connections are everywhere. Wherever cables meet network elements or handoffs occur between networks or network segments, there will always be connections and cables to manage.

In the data world, issues of operational efficiency and standard craft practices for rearrangements and physical rerouting have never been high on the list of priorities. Yet as the data network grows and pressures for reliability and operational efficiency mount, frequent rebuilding of the network will not be an option. The focus on efficiency and craft practices that have contributed to the reliability and availability of the circuit switched network will play a central role in driving reliability and 99.999% availability into emerging packet networks.

Deploying Packet Data Services in a Hybrid Network

In today's network, basic data services remain viable service offerings. Yet as voice and data networks converge and evolve, service providers are finding new opportunities to expand the portfolio with value-added data services. As compared to selling pipes, value-added data services not only create differentiation in the marketplace but also justify a premium price for such value-added services as virtual LANs, storage area networks, virtual private network services, desktop video conferencing, and wavelength services. Businesses that place a value of guaranteed data availability, such as financial institutions and healthcare organizations, are demanding these new data services.

With forecasts for double-digit growth for value-added data services, service providers face the challenge of offering packet services on networks largely built upon circuit switched technology. Economics dictate that building an overlay network may not be cost-effective, which means the installed base of equipment, cables, and network elements must be put to good use. The overriding factor is overcoming bandwidth allocation issues that degrade time-sensitive services such as voice and video. In addition, packet services come in multiple protocols, adding even more complexity to offering seamless data services.

There are many paths to the marriage of circuit and packet technologies for transport of advanced data services. The first choice is packet over traditional SONET. On the positive side, the legacy network works with SONET—so well that SONET reliability is exceptional. But there are several downsides to packet over today's SONET network. Data services must often be backhauled all the way to the POP where intelligent routers are located for making decisions on routing of data packets. Because the TDM network is designed for switching at the core, packet over SONET fails to take advantage of a packet network's key strength—distributed intelligence. In addition, packet over SONET requires a dedicated circuit, making it expensive to deploy. With packet over SONET, bandwidth utilization is poor and services cannot scale on demand. Finally, SONET can be very difficult and labor intensive to provision and requires a fair amount of expensive equipment.

With the advent of new **multi-service platforms (MSP)**, however, deploying data services over next generation SONET gains more appeal. MSPs are network elements that enable voice and data services over a converged network, concentrating multiple transmission methods and transporting them over a single pipe downstream. By combining TDM voice, ATM, Frame Relay, and IP services into one network element, MSPs reduce the number of elements and cables to be managed, creating operational efficiencies for service providers. In addition, MSPs provide integrated transport with switching, circuit grooming, and more efficient use of bandwidth. The multi-service platform can also provision services dynamically. For example, for customers who want more bandwidth, the MSP automatically allocates more bandwidth on the customer's pipe. MSPs help negate the arduous provisioning normally required with SONET while greatly improving bandwidth utilization.

To reduce latency and improve reliability, MSPs and other IP/ATM platforms sometimes use **MPLS**, or Multiprotocol Label Switching. MPLS adds a small header to each packet that gives such information as destination, preferred route, service level, and how intermediate equipment should route. It expedites packets to reduce latency, helping messages move faster to the destination. With MPLS, packets are routed at the edge (layer 3) and switched at the core (layer 2), which allows switches to operate faster than using look-up tables. MPLS is truly multi-protocol, working with IP, ATM, and Frame Relay protocols. It provides a ready technique for achieving QoS for voice and video traffic over packet switched networks.

Additionally, for customers who do not prefer traditional SONET, MSPs can be employed to transmit native Ethernet rings. RPR, or Resilient Packet Ring technology, is a network topology for fibre rings that allows Ethernet-based metro networks to carry packet data and voice traffic with the reliability of SONET. RPR adds several features to Ethernet and IP that are missing over SONET transport. The configuration is still a ring, using two fibres per ring. However, rather than dedicating one ring to protection and one to work, it uses bi-directional technology, which is control on one ring and traffic on the other. This eliminates the problem of SONET bandwidth waste.

A packet data service that is growing in popularity and is made possible by multiservice platforms and RPR is transparent LAN services. Also known as virtual LAN, LAN extension, and virtual private LAN services, this typically gigabit Ethernet data service allows the service provider to interconnect customer LANs in a geographic area, such as a LATA, and transport the customer's native Ethernet over the service provider network. Instead of providing high-speed data service over multiple protocols over the LAN and WAN, transparent LAN provides layer 2 switching of native Ethernet from LAN to WAN, reducing jitter and latency that can often occur from multiple protocol conversions and lookups in layer 3 routers.

Traditional data services are usually limited by T1 or OC-XX access issues, which then require additional equipment to step-down service for users. By comparison, transparent LAN can provide up to 10 Gbps in 1 Mbps increments—greatly expanding the menu of bandwidth options available. Besides improved bandwidth management features, Ethernet services can be increased or decreased in hours—without a service call and without reconfigurations that can add up to weeks or months that it often takes for additional T1 service. Ethernet transparent LAN is also deployed on less equipment and less expensive equipment, making the cost per bandwidth a fraction of the cost of traditional DS1 or DS3 service.

An upgrade for MSPs is packet over DWDM, or dense wavelength division multiplexing. This technology allows multiple wavelengths or channels of data to be transmitted over a single fibre. Different data formats at different data rates can be multiplexed onto the same fibre, including data from IP, SONET, and ATM. Using DWDM more than 150 wavelengths, each carrying up to 10 Gbps, can travel over a single fibre. This technology greatly expands the capacity of installed fibres and, in the long run, will spawn more optical switching devices in the network.

Services such as transparent LAN predict a trend in network design. With more optical services and more distributed intelligence in the network, more equipment is required at the edge of the network. For example, multi-service platforms could be deployed on a customer site instead of in the POP. Or a fibre ring could extend into basement of a building, placing the customer directly on the ring. In these examples, there are still a lot

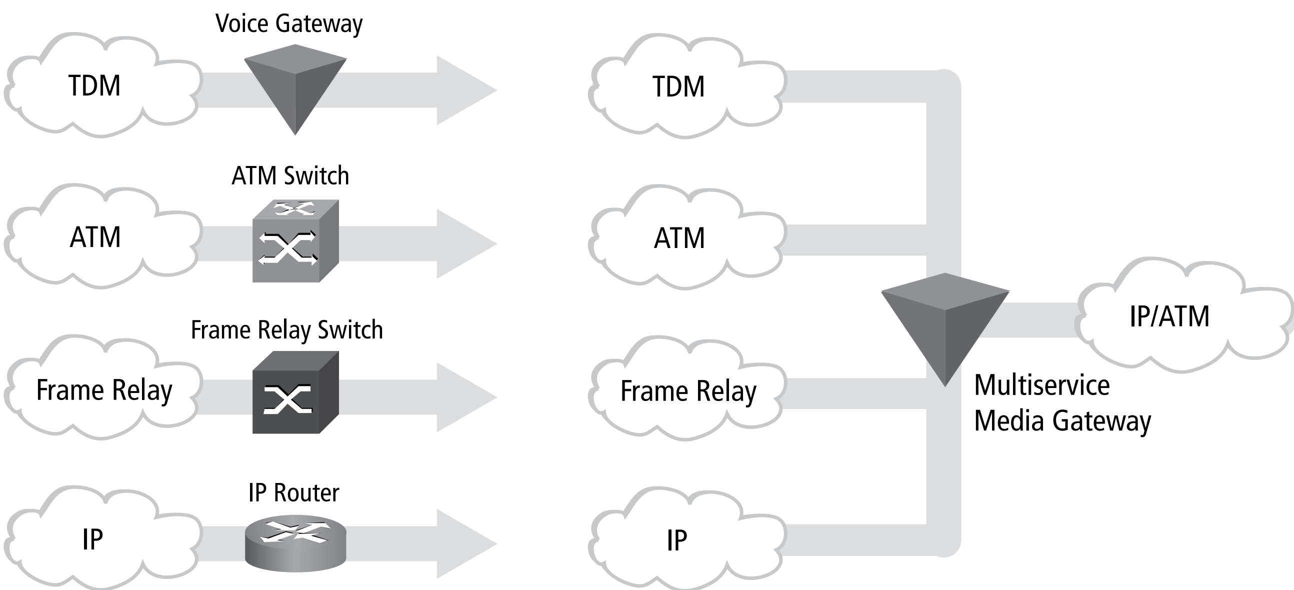


Figure 1. Multiservice Platforms

Deploying Packet in the IP/ATM Core

of connections to be made and cables to manage as the network evolves to packet-based technologies.

Today, SONET is optimized for steady streams of information, but doesn't offer granular scaling of services very well. In addition, tying-up a circuit for SONET is not efficient for the bursty nature of packet transmission. ATM over SONET has been used in the core since the early 1990s to provide bandwidth management while some short haul applications may just use ATM.

Packet switching offers advantages in making better utilization of bandwidth in the core. Rather than tie up a circuit, traffic may be switched at transport sites and at any nodes on the network. In Figure 2, the diagram shows normal layer 3 core packet traffic flow following the dotted arrow. The network element on left side of the diagram could be a router or multiservice platform such as a media gateway. The intelligent device notes the different priorities for certain packets, such as time dependency for voice or video transmission. When the element senses that traffic on that route is near exhaustion, the router or MSP eases congestion by automatically switching lower priority packets, such as e-mail, down a different path in the network, shown here as the dashed arrow. This traffic engineering capability—the ability to differentiate packets and provide QoS—is what gives the intelligent network element its multi-service capability.

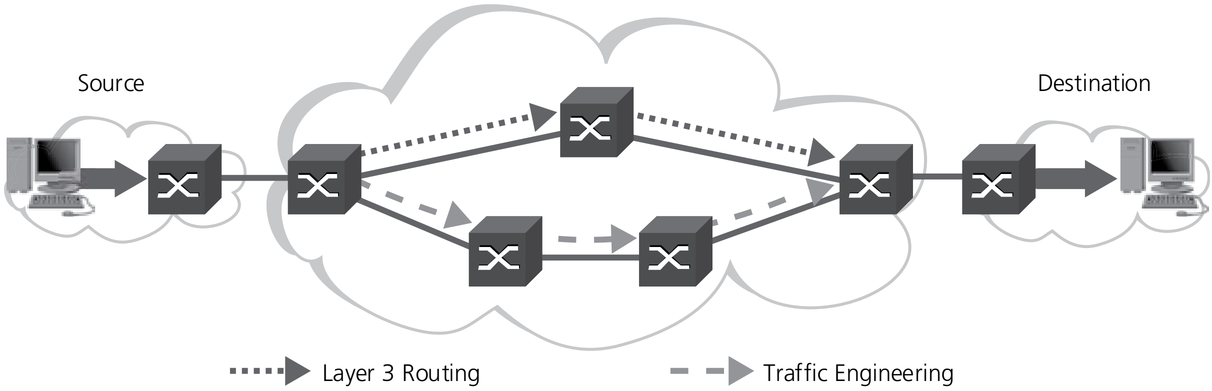


Figure 2

Another technology that is helping in the core is MPLS. For example, while ATM can assign priorities to individual packets, traditional IP cannot. MPLS, through software embedded in routers, enhances IP in the core by adding a small header in each packet that provides more detailed routing information. In IP/ATM routing, each router in the transmission path spends processing time assessing packet priorities and destinations. Employing MPLS enables routing at the edge and switching at the core by providing a pre-engineered path for each data packet so that only edge routers spend time in lookup tables. In this way, MPLS speeds core processing and enables IP traffic engineering with QoS and congestion management.

In the hybrid TDM/IP network that will exist for the foreseeable future, softswitch technologies are being implemented to direct traffic across both TDM and IP networks. A softswitch is a software platform that resides on a server or multiple servers and interfaces with routers and ATM switches in the network. It performs intelligent call handling for media gateways. This provides a consistent call control structure across the service provider's network and brings voice switching capabilities to the packet network. Softswitch architecture promises to be less expensive, at least as compared to maintaining a Class 5 switch. The softswitch also offers operational savings by eliminating the use of bandwidth for sending voice silence and will enable new revenue opportunities and new services, such as VoIP.

Packet network signaling illustrates how softswitch technology can simplify the network and make it more cost effective to operate. On the left of Figure 3, the existing networks for voice and data services are shown. In all, three separate networks are engaged; voice, data, and SS7. On the right shows the configuration for a packet network with media gateways, which are closer to the edge, and softswitches. The result is significant network simplification with one network for signaling and traffic.

It is really the softswitch architecture that makes converged network signaling possible. By talking to different devices in call control and signaling, this architecture provides a seamless link to both new and old network assets. The very strength of the softswitch architecture and multiservice platforms is ability to interface with legacy assets.

As the network evolves and delays to time sensitive packets are eliminated, some edge voice traffic will evolve from Class 5 digital switches to VoIP and VoATM media gateways. Voice over packet is theoretically less expensive to provide because there is no dedicated circuit, which enables more voice calls per bandwidth—only when the challenges of delay are overcome.

An important application for voice over packet is long distance cost reduction. With MPLS implemented, VoIP and QoS can theoretically be achieved. There are numerous VoIP trials underway where entire metropolitan cities are carrying voice over IP. These trials are successful because the technology and the equipment are available today, especially in the core area, which allows cost-effective, high quality VoIP.

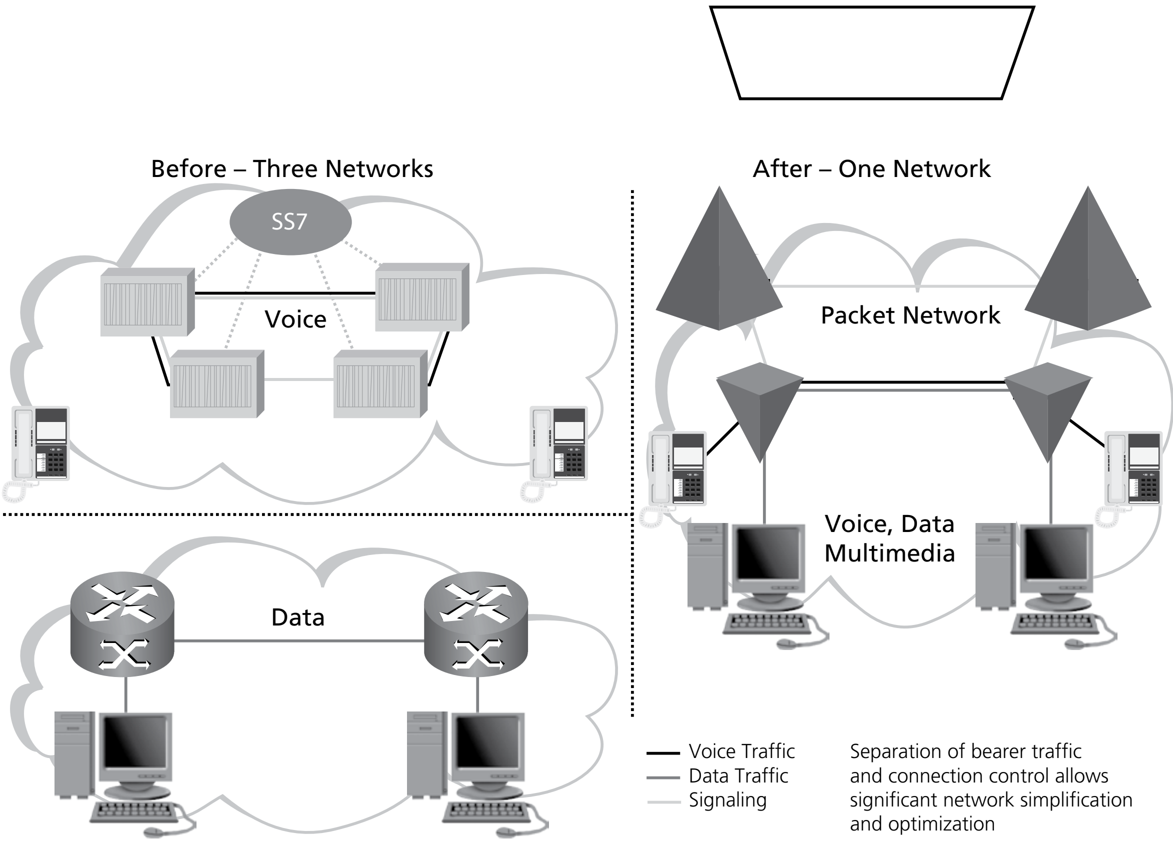


Figure 3

Managing the Hybrid Network with a Foundation of Connectivity

What do circuit switched networks have that packet networks have not? For starters, circuit switched networks have a huge legacy plant in place—an access, switching, and transmission plant connected by copper and fibre cables that today generates well over 90% of services revenue for most service providers. Combined with today's capex constraints, the reality is that the legacy plant isn't going away any time soon. Driven to protect existing revenues, service providers will employ a hybrid TDM/IP network to deliver voice and data services for years to come.

Another feature that the TDM plant has that so far eludes packet switched networks is decades of exceptional reliability and 99.999% availability. Of course, technology promises to bring packet switched networks up to par on these measures. However, there is much more than the latest technology behind the reliability and performance of the circuit switched network. In fact, a large part of exceptional TDM network performance is due to a foundation of connectivity.

Proper connectivity is a design philosophy combined with highly functional products for terminating, patching, accessing, and managing cables around active equipment. With a proper foundation of connectivity, craft practices are centralized around a common set of connectivity interfaces that remain constant despite changing technologies. As a result, reconfigurations are conducted on the connectivity work interface instead of in the backplanes of active equipment. Creating a foundation of connectivity facilitates growth and change without disrupting service—yielding operational efficiency that reduces costs, improves network reliability, and contributes to profit improvement.

A foundation of connectivity helps connect, protect, and manage cables from the core to the edge of the network using products and techniques that are field proven in carrier class operations around the world. These products offer more reliable connections and add density that delays capital expenditure for additional floor space. The design criteria for a proper foundation of connectivity include the following:

- Provide a centralized location for making changes in the network.
- Create a cable management platform that provides bend radius protection, smart cable routing paths, functional access to cables, and both on-frame and off-frame physical protection for cables.
- Place passive monitoring ports at all critical junctions of the network for unobtrusive test access and monitoring.
- Create craft efficiency by providing a standard technical interface.

The products to build a proper connectivity foundation are available from ADC—the market leader in solutions that connect, protect, and manage copper and fibre cables.

To understand what connectivity is, it is important to understand that connectivity is not direct connection of network elements. With direct connect, network elements are "hard wired" together so that technicians are forced to work on active elements and equipment cables. Simple maintenance and reconfigurations require taking circuits out of service, working in sensitive back planes, and re-terminating and testing equipment cables. Direct connect looks great on paper. In practice, it is a nightmare for Operations and a formula for unreliable, interrupted service.

In a foundation of connectivity, a cross-connect architecture provides flexibility and efficiency. All outside plant cables (OSP) and equipment patch cords are connected to the rear of the frame or bay and, once terminated and tested, never have to be touched again. All reconfigurations occur on the front of the bay or frame using cross-connect patch cords. Now equipment patch cords and OSP cables are less vulnerable to damage during rearrangements and routine maintenance, emergency service restoration is simplified, and access to network elements through simple patching greatly increases technician efficiency.

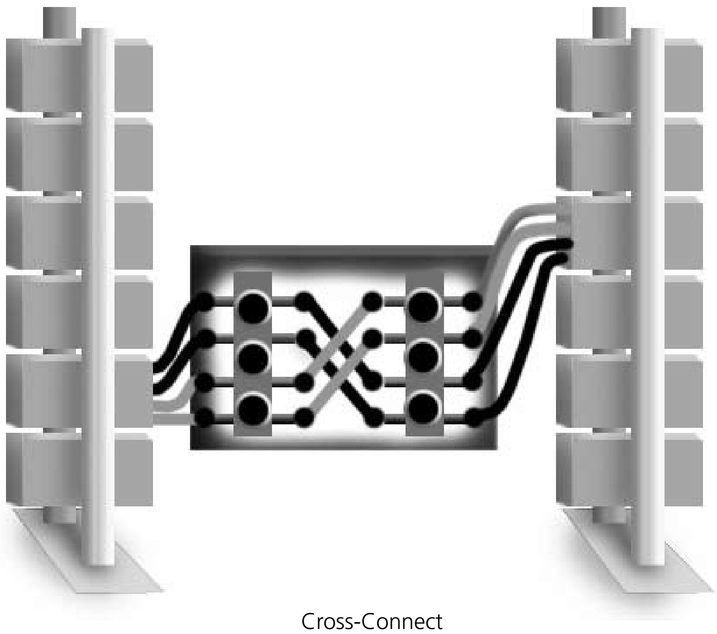
In addition, port count matching with this architecture eliminates port disparities between active elements. This craft friendly design supports cost-effective growth and change in the physical layer.

As network elements and higher speed pipes reach closer to the edge, the value of connectivity increases ten fold. Specifically, a proper connectivity enables the following:

- Rapid and transparent changes to the network.
- Non-intrusive testing and monitoring of circuits.
- Fast and accurate fault isolation.
- Quick circuit rerouting options.
- A common interface and methodology for craft.

Whether the task is performing maintenance or upgrades, creating demarcation points between carriers, patching around equipment failures, or segmenting the network for troubleshooting, a foundation of connectivity remains a critical design element for evolving networks. A foundation of connectivity is a proven solution in the physical layer that improves reliability and ensures maximum service availability.

In this way, proper connectivity minimizes the risks of lost customers, lost revenue, and lost profits as networks evolve to next generation packet-based architectures.



Cross-Connect

Conclusion

Packet switched networks are destined to be hybrid TDM/IP networks for years to come. Factors such as protecting substantial TDM-based revenue and capex limitations dictate an evolutionary, not revolutionary, migration to next generation packet switched services. In fact, the very strength of emerging technologies such as multiservice platforms and softswitches, as well as underlying technologies such as MPLS and RPR, is ready interface with legacy networks.

Circuit switched networks have a proven record of reliability and 99.999% availability—a record due in part to a foundation of connectivity. While technology is playing a role in achieving these same measures for packet-based services, a foundation of connectivity in emerging packet switched networks remains an essential element for cost-effective, highly reliable, and highly available services.

WHITE PAPER

Appendix: Definitions

Protocols

Ethernet is the de facto standard to connect computers, printers, terminals and other devices on LANs. It operates over twisted pair, fibre, or coax and accounts for about 80% of traffic today on corporate intranets. The most commonly installed Ethernet systems are 10Base-T providing speeds up to 10 Mbps. For LAN backbone systems as well as workstations, Fast Ethernet provides 100 Mbps (100Base-T) while Gigabit Ethernet delivers speeds up to one gigabit per second (1000Base-T).

Frame Relay is a service commonly used for discontinuous data transmission between LANs and between end points in a WAN. This technology puts data in variable-size units called frames that can be as large as 1000 bytes or more. It gains speed by depending upon end points to detect errors, drop frames with errors, and retransmit dropped frames. Frame Relay requires a dedicated virtual connection even though individual frames are sent through the network over various routes. Based upon older X.25 packet-switching technology, Frame Relay is a widely deployed data service today on fractional T1 or full T-carrier systems.

ATM, Asynchronous Transfer Mode, offers much higher speeds than Frame Relay-either 155 Mbps or 622 Mbps, with speeds up to 10 Gbps over SONET. This technology requires a dedicated connection, organizing data into 53-byte cell units. ATM earns its name because each cell is processed and transmitted at a different clock rate than related cells in a communication before bring multiplexed over the transmission path. This high-bandwidth, low delay service is suited for voice, data, and video.

IP, Internet protocol, delivers data from one host computer to another, each with its own unique IP address. This protocol divides messages into data packets and affixes the IP address of both the sender and receiver to each packet. Packets are then sent across the network through various gateways by different routes and are often received in a different order than originally sent. This addressing and forwarding protocol only delivers packets; it is up to another protocol, TCP, (Transmission Control Protocol) for reassembly of packets into the original message. While perfect for data, IP shows its weakness time-sensitive voice and video transmission due to jitter and latency that are introduced as packets traverse the network.

OSI

OSI, Open Systems Interconnection, is a standard for how messages should be transmitted between two points in a network. The standard defines seven layers of functions that take place at each end of a communication. These layers are divided into two groups. Layers 4 through 7 govern how messages are sent and received between host computers. Layers 1 through 3 concern functions of node-to-node communications, such as communication between routers, switches, and hubs. Each layer is described below:

• The **Application Layer**, layer 7, is not the application itself, but rather where hosts are identified, user authentication is reviewed, quality of service is assessed, and any constraints are identified. In this layer applications such as PC programs and FTP usually perform these functions.

• The **Presentation Layer** converts incoming and outgoing data from one format to another. For example, logging on to a secure site, inputting a credit card number, and encryption functions occur in this layer.

• Layer 5, the **Session Layer**, establishes a link between applications, coordinating exchanges between applications on each end, such as authenticating a user and logging on to a server.

• The **Transport Layer** is the last host-to-host layer. In this layer, messages from the application layer are cut into data packets, sent out, and reassembled on the other end. Here end-to-end message control and error checking is handled.

• The **Network Layer** handles routing and forwarding of data packets. This is the first of three node-to-node or communication between network elements layers. The IP protocol functions here.

• In the **Data Link Layer**, protocol knowledge and management is provided, as well as sychronization for the physical level. Frame Relay sends packets in this layer.

• Layer 1 is the **Physical Layer**. In concert with the Data Link Layer, this ensures data from element to element is sound in terms of such factors as transmission protocol and hardware links between devices including PCs and routers.

Hardware

A **hub** is a point where data converges from multiple directions and is forwarded out in multiple directions.

In many ways, a hub is like a splitter. It is a work-group level device that allows a large, logical Ethernet to be subdivided into multiple physical segments. This is a layer 1 element that offers no intelligent congestion control for data packets.

Bridges connects multiple elements in layers 1 and 2. These devices are used to connect network segments, such as different LANs, and forward packets between them. There is limited congestion control with simple filters that may keep certain packets within a LAN or region.

A **switch** establishes a transmission path between incoming and outgoing connections, taking an incoming signal and routing it to the proper channel going out. Switches are layer 1 and layer 2 devices that offer no congestion control or intelligence for routing packets. As such, a switch is a simpler and faster mechanism than a router and is perfectly suited for moving packets rapidly through the network. Cisco, Foundry Networks, and Extreme Networks all make Ethernet switches.

Routers are highly intelligence data switches that serve as the interface between two networks. Routers look at the network as a whole and makes decisions to route data packets based upon destination, address, packet priority, least-cost, delay, congestion level and other factors. These layer 3 devices are the work-horses of the data network. Major names in routers are Cisco, Foundry Networks, and Juniper.

ADC KRONE

CERTIFIED ISO9001 CERTIFIED

www.adckrone.com/in

Corporate Office and Factory: P.B. No. 5812. 10C II Phase, Peenya, Bangalore – 560058 INDIA
Tel: +91 80 28396101 Fax: +91 80 28396104
TOLLFREE: 1800 425 8232
OFFICE LOCATIONS: BANGALORE, NEW DELHI, MUMBAI, PUNE, CHENNAI, HYDERABAD

ADC Telecommunications, Inc., P.O. Box 1101, Minneapolis, Minnesota USA 55440-1101