Solution Paper

Network Migration for Utilities

Teleprotection over Packet

RAD
data communications
The Access Company

Abstract

Teleprotection signals from protective relays are among the most critical data transmitted across utility networks and therefore must be assured immediate delivery when problems are detected. This complexity involved in ensuring protection performance is compounded when moving from legacy SDH/SONET to non-deterministic, packet-based networks.

This paper reviews the performance requirements that are unique to protection systems and explains how these challenges are met in a next generation packet environment.

Contents

Introduction

Teleprotection signals from protective relays are among the most critical data transmitted across utility networks, as they help manage the power grid load, as well as to protect equipment within the power network from severe damages resulting from faulty HV lines. By enabling load-sharing, grid adjustments and immediate fault clearance, Teleprotection has a decisive role in ensuring uninterrupted power supply and therefore requires special attention with regards to network performance and reliability. Specifically, protection commands must be assured immediate delivery when problems are detected, so that faulty equipment can be disconnected before causing a system-wide damage.

The complexity involved in meeting such targets is compounded when moving from legacy SDH/SONET to non-deterministic, packet-based networks. This paper reviews the performance requirements that are unique to protection systems and explains how these challenges are met in a next generation packet environment.

1. Utilities Communications: Network in Transition

The prevailing utility communications networks have been based on SDH/SONET; however, legacy infrastructure and substation devices are being phased out to make way for Ethernet transport and IP/packet-based networks. The move towards Smart Grids is a key driver for this change, as packet transport's high capacity and lower OpEx are required to handle the amount of bursty traffic generated by the advanced grid applications envisioned in intelligent power networks. Next-generation SCADA systems, wide area situation awareness (WASA) synchrophasor measurements and IP-based video surveillance are examples of new applications that mandate the use of packet switched networks. In addition, recent developments in substation automation (SA), such as the IEC 61850 standard, also require Ethernet capabilities throughout the transmission and distribution (T&D) grids.

1.1 Migration challenges

Utility companies, most of which operate self-owned, private networks, adopt a cautious approach to IP transformation. Traditionally a conservative segment, utility operators have been reluctant to migrate to IP without proper mechanisms to ensure SDH/SONET-level reliability for mission-critical applications. Their migration challenges can be broadly described as either business- or technology-related.

The economical challenge relates primarily to utilities' need to eliminate CapEx hikes and to avoid overburdening operations when introducing new devices and communications technologies, especially when the chosen migration path involves continued co-existence of SDH/SONET and next generation networks.

From a technical perspective, the implementation of smart communications over packet-based networks translates to the need for reliable service assurance tools to ensure low end-to-end delay, High Availability and resiliency when running mission critical applications in a PSN environment. For Teleprotection, the need for ultra-fast and reliable transmission is translated to extremely low, symmetrical delay and minimal delay variation ("jitter") – both of which not inherent to packet switched networks' behavior. Nonetheless, Ethernet technology has matured enough so that it now includes various mechanisms to overcome such impairments and ensure appropriate performance, as described below.

Today, typical implementations for transmitting TDM traffic (such as Teleprotection signals) over packet use pseudowire emulation (See Appendix for an explanation on the various methodologies of pseudowire encapsulation). Other methods, including direct mapping of payload to the Ethernet connection – thereby eliminating the TDM processing and pseudowire encapsulation phases – are expected to become available in the future.

2. Teleprotection Connectivity

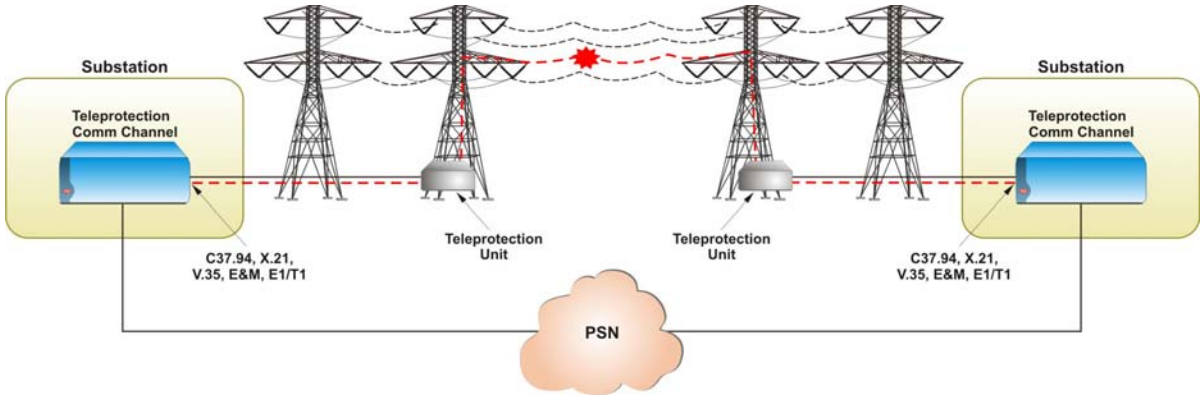

Figure 1: Teleprotection Connectivity over Packet

The most common schemes for power system protection, specifically for protecting HV transmission lines, use either distance (impedance) protection, current differential protection, or a combination of both. The former typically uses impedance measurements to trip the breakers when results vary from those taken under normal conditions, while the later measures the current entering and leaving the protection zone; if the measured results are not equal in several consecutive samples, the faulty part of the line is disconnected. This requires communication between the relays on both ends of the zone. Modern implementations of protection relays use a fiber optic communication channel based on the IEC C37.94 standard.

Pilot-aided distance protection uses a communications channel between the local and remote relays to improve fault localization and fault clearance performance with various command systems, such as overreach/underreach transfer trips. In addition to traditional communications channels, such as copper-based pilot-wires and PLCs (power line carrier), other solutions that use microwave radio and optic fibers are now available, either for a direct connection or for multiplexing multiple communication channels. Specific performance criteria depend on the protection equipment, network elements and topology, as well as on traffic volume, however some generalities can be drown for key parameters.

2.1 Teleprotection Communications Performance Criteria

The key criteria for measuring Teleprotection performance are command transmission time, dependability and security. These were defined by the IEC standard 60834 as follows:

Transmission time: The time between the moment of change of state at the transmitter input and the moment of the corresponding change of state at the receiver output, excluding propagation time. Overall operating time for a Teleprotection system includes the time for initiating the command at the transmitting end, the propagation time over the communications link and the selection and decision time at the receiving end, including any additional delay due to a noisy environment.

Dependability: The ability to issue and receive valid commands in the presence of interference and/or noise, by minimizing the probability of missing command (Pmc). Dependability targets are typically set for a specific bit error rate (BER) level.

Security: The ability to prevent false tripping due to a noisy environment, by minimizing the probability of unwanted commands (Puc). Security targets are also set for a specific bit error rate (BER) level.

Additional key elements that impact Teleprotection performance include bandwidth rate utilized by the Teleprotection system and its resiliency for recovering from failures. Of the above criteria, transmission time, bandwidth utilization and resiliency are directly linked to the communications equipment and the connections that are used to transfer the commands between relays.

2.1.1. Latency Budget Considerations

Delay requirements for utility networks tend to vary depending on a number of parameters, such as the particular protection equipment in use. Most power line equipment can withstand shortage or irruption faults up to approximately five power cycles before sustaining irreversible damage or affecting other segments in the network. In 50Hz lines, this translates to total fault clearance time of 100ms. As a safety precaution, however, actual operation time of protection systems is limited to 70-80 percent of this period, including fault recognition time, command transmission time and line breaker switching time. Some system components, such as large electromechanical switches, require particularly long time to operate and take up the majority of the total clearance time, leaving only a 10 ms window for the communications part of the protection scheme. Given the sensitivity of the issue, new networks pose requirements that are even more stringent: IEC standard 61850 limits the transfer time for protection messages to ¼-½ cycle, i.e., 5-10 ms (for 50Hz power lines) or 4-8 ms (for 60Hz lines) for the most critical messages.

2.1.2. Asymmetric Delay

In addition to minimal transmission delay, a differential protection communication channel must be synchronous, i.e., experiencing symmetrical channel delay in transmit and receive paths. As mentioned above, this requires special attention in jitter-prone packet networks. While optimally Teleprotection systems should support zero asymmetric delay, typical relays can tolerate discrepancies of up to 250 µs. The main tools available for lowering delay variation below this threshold are:

A jitter "buffer" at the multiplexers on each end of the line can be used to offset delay variation by queuing sent and received packets. The length of the queues must balance the need to regulate the rate of transmission with the need to limit overall delay, as larger buffers result in increased latency.

Traffic management tools ensure that the Teleprotection signals receive the highest transmission priority and minimize the number of jitter-inducing routing points passed en route.

Standard PSN-specific synchronization technologies, such as 1588-2008 Precision Time Protocol (PTP) and Synchronous Ethernet (Sync-E), help maintain stable networks by disciplining the communications elements to a highly accurate clock source. Additional details on Timing over Packet (ToP) tools are provided in section 3.4.

2.2 Latency Sources in Teleprotection

It is important to understand the impact of network constraints, as each element and processing stage in the protection system adds to the overall end-to-end delay:

Protection/Teleprotection equipment delay: This latency is inherent and includes the relay's fault identification, command initiation and decision time.

Substation multiplexer (TDM interface): Mux equipment delay is the result of functions such as reframe time following a loss of signal, drop and insert through-channel delay, DS0 and DS1 buffering, synchronization and de-synchronization delay, ring switchover time, and fault detection time. Multiplexer latency is minimized via optimal design of ICs and DS0 cross connect function, as well as via high-performance buffering and forwarding technology.

Pseudowire encapsulation and packetization delay: The process of converting TDM data into packets involves a fixed delay of 1-5ms, depending on packet size and the number of TDM frames each packet contains. Smaller packets increase bandwidth overhead, but reduce latency.

PSN network elements: Where protection equipment is connected over a packet network (rather than over a direct, back-to-back link), each element along the traffic path adds a mixture of fixed and variable latency in the form of processing and queuing delay, respectively. Variable delay poses a greater threat to Teleprotection performance due to the high level of uncertainty it introduces, and therefore needs to be dealt with via advanced traffic management. Further details are provided in section 3.2.

3 Additional Issues Relating to Teleprotection Connectivity

3.1 Resiliency

Given their mission-critical nature, Teleprotection systems must be ensured fail-safe operations in the event of malfunction in any of the system components. Many utilities are employing redundant protection methods, such as distance and line differential protection over different channels. From a communications perspective, resiliency can be achieved at a number of levels:

Hardware redundancy: Multiplexer resiliency should ideally be based on no single point of failure (NSPF) design with redundant, hot-swappable power supplies, as well as control plane card and switch fabric card redundancy.

Link redundancy: A 1+1 protection topology with automatic switchover between links when network or cable failures occur. Ethernet-based services employ a link aggregation group (LAG) scheme using IEEE 802.3-2005 LACP (link aggregation control protocol), in which parallel links are bundled to a single virtual link.

Path protection: Carrier Ethernet standards provide various tools to ensure High Availability. These include Ethernet Linear protection Switching (G.8031) – also called "EVC (Ethernet Virtual Connection) protection" and Ethernet Ring Protection Switching (G.8032 ERPS) to provide Five Nines (99.999%) availability via service resiliency and speedy restoration.

3.2 Traffic Management and Quality of Service

Advancements in Ethernet technology allow the use of sophisticated mechanisms to provide protection signals with the level of deterministic quality of service and priority they require. This is especially critical when traversing various switches and network elements and need to offset variable constraints, such as queuing delay. By managing bandwidth consumption and transmission priorities with CoS (Class of Service) granularity, multi-level hierarchical traffic management enables predictable latency and jitter performance across the service path. An advanced toolset includes the following:

Classification of incoming traffic into flows according to type and required QoS. Ethernet supports a wide variety of sorting criteria, such as VLAN-ID, P-bit marking, MAC/IP address and many more, to allow traffic identification in fine granularity.

Metering and policing is applied for each flow to regulate traffic according to pre-defined CIR (Committed Information Rate) and EIR (Excess Information Rate) bandwidth profiles. Rate limitation is performed so that traffic admitted into the network based on metered "color": Green (admitted frames), yellow ("best-effort" transmission), or red (discarded frames).

Hierarchical scheduling to define the order in which the various flows are forwarded, using a two-step scheduling mechanism so that each flow receives the desired priority. Advanced queue management techniques also serve to ensure minimal latency and jitter, even when a large amount of bursty traffic is sent over the same link.

Shaping to smooth out bursts and avoid buffer overruns in subsequent network elements.

Packet editing and marking to signal proper handling instructions for subsequent network elements

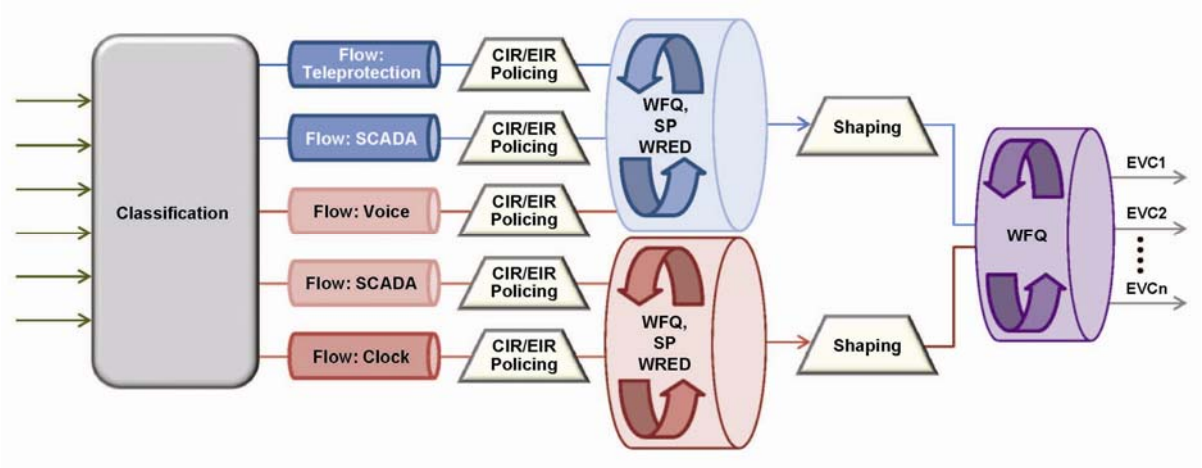

Figure 2: *Packet-based traffic management and hierarchical QoS tools*

3.3. Performance Monitoring and Testing

Carrier Ethernet offers a wealth of tools to test, monitor and troubleshoot the communications links operation. A comprehensive Ethernet OAM (operations, administration and maintenance) suite, delay, jitter, and packet loss measurement schemes, diagnostic loopbacks, and other means are available remotely and automatically conduct the following functionalities:

- Connectivity verification
- Stress testing
- Performance monitoring
- Fault detection and isolation
- Fault propagation and isolation

Remote testing, end-to-end visibility and proactive monitoring capabilities help utility network operators anticipate service degradation ahead of time, as well as to cut down truck-rolls and on-site technician calls, thereby ensuring consistent performance and lowering operational costs (OpEx).

3.4. Timing Synchronization over Packet

As mentioned above, packet switched networks were not designed with built-in synchronization mechanisms, requiring complementary clock transfer solutions to ensure a stable network with predictable performance – particularly for applications that are delay and jitter sensitive, such as protection and SCADA. Up until recently, the prevailing custom entailed the use of a GPS at each node/service point; however, the equipment costs involved are considerably high.

There are several methods in use today for ensuring synchronization in an all-packet environment. The most popular two are based on the ITU-T Synchronous Ethernet (Sync-E) methodology, which uses the Ethernet physical layer to accurately distribute frequency, and on the IEEE 1588-2008 Precision Time Protocol standard, which involves timestamp information exchange in a master-slave hierarchy to deliver frequency, phase and TOD (Time of Day) information. Another method, Adaptive Clock Recovery (ACR) is a frequency synchronization method in which the clock is distributed over the PSN as a Constant Bit Rate (CBR) TDM pseudowire stream and regenerated at the receiving end using the packet's time-of-arrival information, independently of the physical layer. The clock stream format is a standard TDM pseudowire (SAToP/CESoPSN) flow.

Due to their sensitive nature, power protection applications require a very high level of clock precision. IEC standard 61850 specifically addresses utility networks' needs in timing and synchronization over packet. It refers to IEEE C37.238 standard profile for use of IEEE Std. 1588 Precision Time Protocol in power system applications. The latter requires 1µs accuracy that is on par with GPS levels.

Teleprotection communication devices that support clock transfer enable substantive cost savings, as they eliminate the need for costly dedicated hardware or GPS installations.

3.5. Choosing the Right Packet Network

When migrating to next-gen networks, the decision on the type of technology to employ depends on such factors as the number of sites to be connected and their size, as well as on the ability of the selected solution to ensure consistent performance across the different access media available at each site.

Available options include MPLS (Multi-Protocol Label Switching) using VPLS (Virtual Private LAN Service) encapsulation, IP/MPLS or Ethernet end-to-end, or a combination of Ethernet access and an IP/MPLS core. While an end-to-end VPLS can provide the required resiliency for critical applications with a low-latency Fast Re-Route (FRR) protection mechanism, it has severe security issues, limited

built-in OAM tools for performance monitoring in the network and prohibitive per-port costs in large deployments. A combination of Layer 2 Ethernet access with an IP/MPLS core, on the other hand, offers lower cost per port, richer OAM and PM tools for native Layer 2 Ethernet connections and advanced protection mechanisms via Ethernet Ring Protection Switching (ERPS) and Ethernet Linear Protection Switching (ELPS). In addition, it allows utility network operators to maintain existing access media installed base, and an optimal fit for a large number of distributed sites with copper, fiber and wireless infrastructure.

4 Teleprotection over Packet Test Case

RAD's Megaplex-4100 multiservice access platform was successfully tested by a major energy utility, as part of a Teleprotection over packet proof of concept program. The testing consisted of converting TDM data received from protection units into packets. The encapsulated traffic was then transmitted over a Cisco MPLS network employing static routing to ensure path determinism, while meeting all Teleprotection performance required, such as extremely low delay.

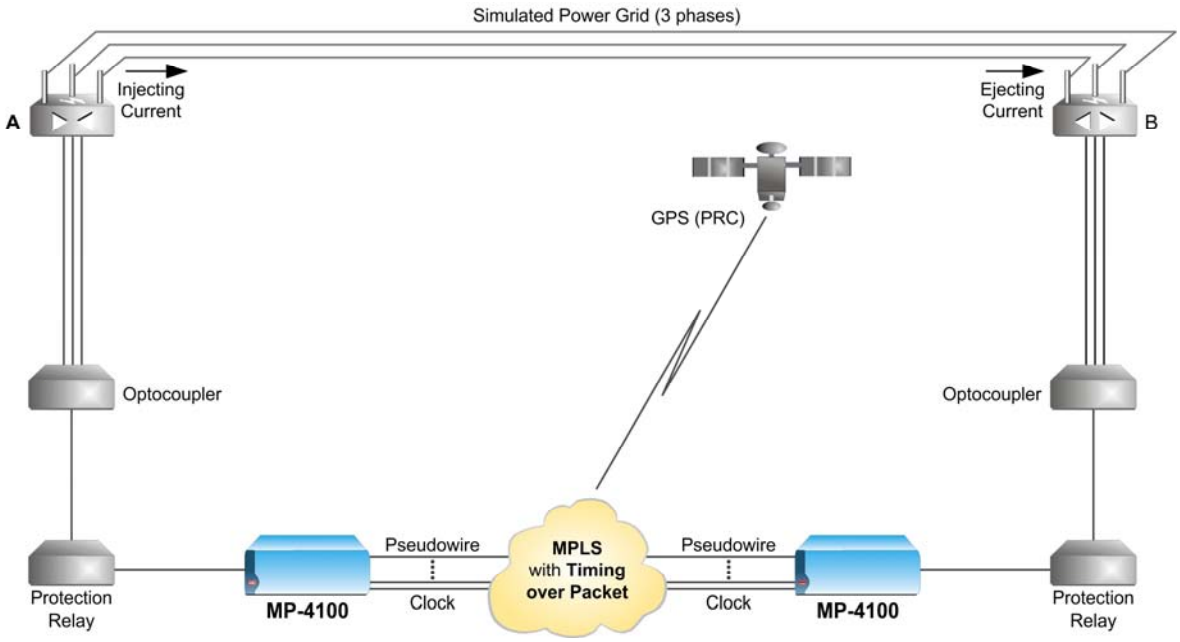

Figure 3: Testing Teleprotection performance over Ethernet and MPLS

The line differential protection equipment included devices from AREVA, ABB and Siemens, featuring a variety of TDM communications interfaces, including the following:

- G.703
- X.21
- RS-232
- E&M
- C37.94
- Native E1

Regardless of the specific device or interface used, the protection system required an end-to-end communications delay of 8-10ms in a packet network environment experiencing a jitter of 2.5ms. Additional requirements include symmetrical latency, with maximum tolerance of 100-250µs.

RAD's Teleprotection multiplexers have successfully met these constraints, experiencing a delay of up to 5ms and delivering the quality of service for signal priority via shaping and traffic engineering tools. In addition, they rigorously maintained clock accuracy throughout transmission and provided a high degree of resiliency through various protection schemes. One of these schemes included redundancy at a DS1 level, whereby two pseudowires are created to serve redundant DS1 ports over different paths in the MPLS network. In scenarios where an SDH/SONET network is kept for backup, DS1 redundancy can be used to transmit one link as a pseudowire over packet, while the other is connected over the TDM backup network.

5 RAD's Teleprotection over Packet Solutions

Megaplex

Multiservice Access Platforms

ETX-A

Carrier Ethernet over Fiber

IPmux

TDM Pseudowire Gateway

FCD

NG-ADM

RICi-GE

Ethernet over NG-SDH

Figure 4: *RAD's Teleprotection over packet solutions – enabling a safe transition*

RAD's best-of-breed, hybrid SDH/SONET and PSN access solutions for the energy market allow utilities to choose the migration path that best suits their needs. By combining carrier-grade Ethernet capabilities with extensive support for legacy services and interfaces, RAD's system solution offer the following benefits:

- Easy integration of Intelligent electronic devices (IEDs) and NG services and equipment over existing TDM infrastructure
- Service continuity for legacy applications and equipment, even after core networks are replaced to IP/MPLS
- Circuit emulation solutions without compromising service quality or latency levels
- Ensure deterministic QoS for NGN services and advanced grid applications over packet transport using multi-priority traffic management, end-to-end OAM and diagnostics, and performance monitoring

- Multi-standard timing over packet synchronization
- Multi-level redundancy options for Five Nines resiliency
- Future-proof solutions streamlined for Smart Grid communications and IEC61850 architecture, including reliable, low-latency Ethernet services between sites with real-time messaging, such as GOOSE/GSSE
- Help protect critical infrastructure and IP-based SCADA systems from malicious cyber attacks with cyber security and authentication protocols, such as SSH, SSL, SNMPv3, and RADIUS

Among the various options offered to utility network operators, RAD's hybrid solutions enable the use of a single device to migrate non-critical services to new packet environment, while protection and other vital traffic is kept over the legacy SDH/SONET network, thus allowing a phased transition without increasing the capital investment or operating costs involved in the process.

Conclusion

The move towards Smart Grids and next-generation networks in utility communications is already under way, however extremely critical applications as Teleprotection require special attention. Only solutions that meet the exacting performance criteria of minimal transmission time, reliability and security can be considered as viable alternatives to existing deployments. Specifically, extremely low, symmetrical delay together with robust clock accuracy, QoS assurance, resiliency, and on-going performance monitoring are "must have" elements for any Teleprotection over packet system. Furthermore, hybrid TDM/Packet solutions allow utility operators the freedom to choose the migration path that best suits their needs and budgets.

Appendix – Pseudowire Emulation

TDM-based traffic is transmitted in a new Ethernet/IP/MPLS environment using pseudowire emulation (PWE) – an encapsulation method that allows a seamless connection by creating logical links, or virtual tunnels, between two elements across the packet network. A pseudowire will emulate the attributes of a TDM service such as an E1, T1 or a fractional n x 64 service.

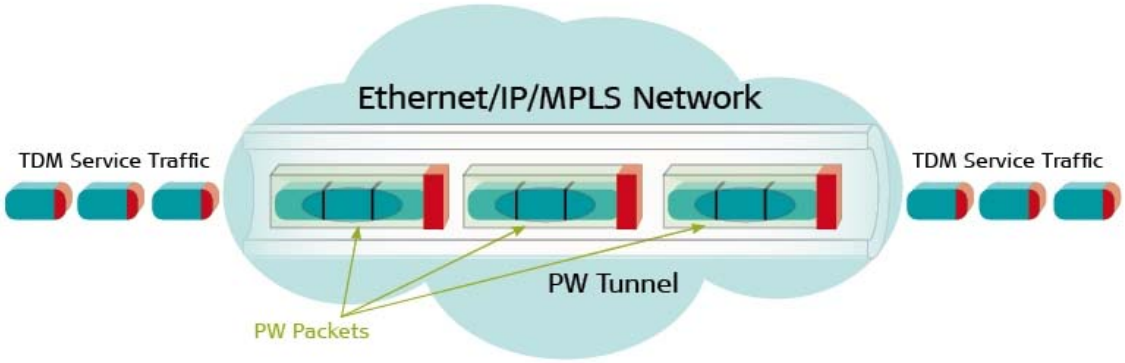

Figure 5: *TDM pseudowire emulation over packet networks*

The transmitted data streams are encapsulated in packets upon entering the network, and then reconstructed at the pseudowire egress, where clocking information is also regenerated. As a result, real-time traffic is delivered transparently without distortion, while avoiding the complexities of translating signaling data and ensuring that synchronization criteria are met. The latter issue is critical for legacy TDM devices, as they require a synchronized clock to function, however the packet switched network by nature is not synchronous. The pseudowire emulation mechanism must therefore regenerate the original TDM timing accurately across the packet network.

The most common methods of TDM pseudowire emulation are based on the following standard protocols:

The **SAToP** (Structure Agnostic TDM over Packet) service fits unframed E1/T1 streams as it treats the TDM traffic as a data stream and ignores framing segmentations or timeslots (DS0). It offers low bandwidth overhead, flexible packet sizes and low end-to-end delays; however, it is susceptible to frame loss and re-sequencing and therefore requires appropriate mechanisms to offset such risks. In addition, SAToP is not bandwidth-optimized, as it requires a full E1/T1 capacity to transfer even a few timeslots.

CESoPSN (Circuit Emulation over PSN) supports framed and channelized TDM services over PSN. The packetizing uses multiples of the TDM frame itself, which results in a lower delay when transporting several timeslots. A CESoPSN payload always corresponds to 125 µs of TDM data, or some multiple thereof.

TDMoIP (TDM over IP), a standardized method developed by RAD, encapsulates E1/T1 signals and supports framed, unframed and channelized services in a single protocol. However, the packetization of TDM data into n x 48 Byte frames may result in delay levels that are unacceptable for some services, such as when transmitting multiple timeslots of Teleprotection signals.

www.rad.com

International Headquarters
RAD Data Communications Ltd.
24 Raoul Wallenberg St.
Tel Aviv 69719 Israel
Tel: 972-3-6458181
Fax: 972-3-6498250
E-mail: market@rad.com
www.rad.com

North America Headquarters
RAD Data Communications Inc.
900 Corporate Drive
Mahwah, NJ 07430 USA
Tel: (201) 529-1100,
Toll free: 1-800-444-7234
Fax: (201) 529-5777
E-mail: market@radusa.com
www.radusa.com

RAD
data communications
The Access Company

Catalog no. 802491 Version 5/2011