Packet Networks White Paper

November 2015

Contents

1 - Introduction, the PNWG

The UTC Packet Network Working Group (PNWG) is focused on the deployment and operation of packet-based networks in the utility and critical-infrastructure environment. In parallel with technology and service-delivery capability, additional processes involving network security, management and operational support must also develop to form a complete migration model. The UTC PNWG exists to document these steps and to provide a roadmap for other members.

This is the first of several whitepapers to be drafted by the PNWG and focused utility network modernization and deployment of packet-based network technology. In preparing this inaugural document, the consensus among contributors is to focus on current-state and issues to be addressed when planning for a future network migration. Current members of the PNWG have direct experience in migrating utility networks and can speak to the challenges directly related with such an initiative.

Many utility networks continue to use what is becoming *legacy* switching technology - SONET, SDH, TDM, and ATM. All of these technologies are declining - some more than others - in new deployment in favor of packet-based alternatives. Exact statistics may not exist to specifically show the extent of TDM or SONET/SDH technology decline within specific regions or utilities, but the consensus among most utility network planners is that it is happening. With that being the case, the number of network migration projects and adoption of packet-based technologies is sure to increase.

As with the development of the global Internet, packet-networking is the core technology for next generation networks. All modern utility equipment has some form of packet-based communication. This common network functionality makes deployment of packet networking for next generation utility networks the best technical choice. The common network functionality also aligns with serving the Information Technology (IT) needs of an organization, regardless of whether an organization has converged IT and Operational Technology (OT) functions.

Lastly, nearly all services utilizing existing wide-area networking and telecom technology have a packet-network migration path. Utilities today demand increased access to a seemingly exponential large ecosystem of devices. SCADA, Emergency or Private Voice, Mobile - PTT Radio, Video Surveillance, PMU/Synchrophasor and even Metering systems all rely on protocols designed around packet transport. Even Teleprotection systems, whether based on proprietary protocols or using IEC-61850 protocols, are moving towards packet network interfaces.

2 - Current State of Utility Networks

2.1 - Drivers for Change

The need to migrate to packet-based technologies is based on a number of evolving factors. The foremost of which is the need for more packet-based services in the field - substations, telecom sites, and field offices. The majority of new services require packet-network technology. The second driver is *increased network utilization* - more services, in more locations. Where legacy services using n x 64 kbps of TDM-based traffic used to be sufficient, modern network services need service in the hundreds of kbps or even Mbps. The rigid bandwidth granularity of TDM and SONET/SDH systems is not sufficiently scalable or flexible for transport of packet based services, resulting in inefficient use of available bandwidth. Furthermore, the sheer quantity of devices capable of communicating on utility networks is also growing exponentially, as seen with such concepts as the *Internet of Things (IoT)*. Next-generation

utility network users demand service where and when it is needed, without significant overhead. Rapid service deployment with both low-speed and future high-speed capability is desired.

Many traditional network services are migrating to packet-based protocols. The following table demonstrates common services and protocols and their packet-based evolution:

Service	Legacy Protocol	Next-generation or Packet-based Protocol	Adoption Rate (estimated, among utilities)
Teleprotection	Analog tone (4W), Serial Data (RS-232, G.703, C37.94, X.21, etc)	IEC-61850, vendor proprietary	Low
SCADA	DNP3 Serial, MODBUS RTU	DNP3-over-IP, MODBUS TCP	Medium
Voice	2W, 4W E&M backhaul	VoIP	High
Video Surveillance	MPEG-2, transport over T1, Fractional-T1	MPEG-4, H.264 AVC, H.265 HEVC	Medium
Mobile Radio	2W, 4W E&M backhaul	VoIP backhaul, Over-the-air VoIP	Medium
Synchrophasor	Macrodyne PMU (as an example), other proprietary protocols (serial, RS-232)	IEEE C37.118 - Synchrophasor over Ethernet	High
Metering	Standard serial (terminal session), dial-up modem	IP - MV90 polling over packet	High
Remote Substation Access	Dial-up, Frame Relay, Leased Line	Private WAN, IP Routing	High
Corporate Network Access (from field)	Dial-up, Serial (terminal Server), T1	Private WAN, IP Routing	High

Looking more specifically at network transport evolution, it is clear from the perspective of vendor equipment availability and equipment cost, that legacy TDM and SONET/SDH equipment is either plateauing or declining in industry deployment. It is thought that moving toward higher capacity Ethernet technology is largely driven by the commercial carrier / cellular markets and their large capital investment in packet-based technologies incorporated within HSPA and LTE network deployments. The reality is that utility investment in telecom equipment purchases from common manufacturers is a small fraction of what large carriers will purchase in a given year, hence the manufactures focusing on where their customers are going - and penalizing to some degree those that fail to keep up.

This move to adopt packet technologies as the industry-standard provides incentive for manufacturers to discontinue their legacy TDM, SONET/SDM platforms and push customers towards mainstream offerings. The result, for utilities, is declining product availability and increasing costs for those products from the manufacturers still willing to produce and sell them.

In parallel with the shift in market offering, is the need for ever-increasing bandwidths. SONET/SDH evolved to a point where development appears to have halted - SONET OC-768/SDH STM-256 for

example - beyond that networks transition to 40GigE or 100GigE Ethernet. Capacities continue to expand, but for Ethernet-only - 100GigE and now 400GigE is possible.

Lastly, the workforce skillsets available to utility network operators are increasingly focused on packet-based technologies. This makes the skills needed to continue to operate and support legacy networks a dying breed. New staff - and in particular entry-level staff coming out of technical college or university - are trained in packet networks and expect to work using those skills in operational networks. This increases risk to network operators that the skills necessary to support existing legacy networks may not be available when needed.

2.2 - Utility Adoption

In this initial discussion and in future whitepapers, you will notice that simplicity or consistency is not mentioned as a specific benefit of packet-based network technology. It is a fact that Ethernet offers a common connection medium by which any and all devices may connect to the network. However, maintaining traffic separation, priority, and security of individual or specific services are additional factors that must now be considered when addressing deployment by a utility. All utility networks are different, with different environments, service expectations, and evolutionary paths.

Considering the uptake of packet-based technologies into utility networks, it can be assumed that technology migration will take a common form - the Innovation Adoption Lifecycle - as shown below.

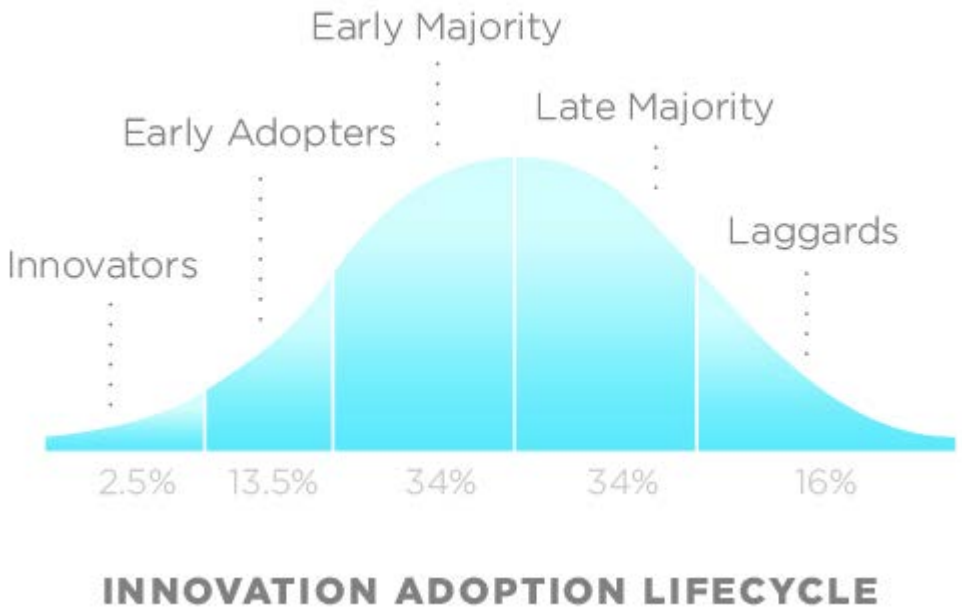

Figure 1 - Innovation Adoption Lifecycle
Reference: https://en.wikipedia.org/wiki/Technology_adoption_lifecycle

When asking where the current states of utility networks are on this lifecycle, in 2015 it is assumed to be in the Early-Majority segment. However, this is moving towards the crest of the curve (Majority) as packet-technology is becoming common in utility networks. In North America, and as real-world examples, utilities such as AltaLink (Alberta, Canada) and Idaho Power (Western USA) began testing and deployment several years ago, making them part of the Innovator and Early Adopter segments. Europe and Africa are speculated (based on feedback from workgroup members) to be slightly behind North America in terms of packet network adoption putting them in between the early-adopter and early-majority segments. Now that packet-based network services and architectures are mature and field-proven, and available on numerous hardware platforms, more utilities are following and adoption rates are increasing.

In speaking with many utilities - most of which are members of UTC globally - three (3) common themes emerge when speaking about packet migration scenarios - 1. Maintain the Status Quo / Overbuild Packet Network (minimal migration), 2. Partial Migration - Non-critical services only, and 3. Full-scale migration. There are pros and cons to each of these but generally-speaking all utilities considering deployment of packet-based technology will adopt one of the three scenarios:

1. Maintain the Status-Quo/Overbuild Packet Network - only deploy packet-networking where justified and on top of the traditional TDM / SONET / SDH infrastructure. [Risk - Medium, Cost - Low, Staff Development - Low, Complexity - Low, Able to transport new services - Low]
   Pros: Minimal capital requirements, minimal upgrading for staff, proven technology.
   Cons: Minimal network support: May depend on legacy technology (e.g. Frame Relay). Delays upgrading until *absolutely* necessary - increasing risk of a forced upgrade due to obsolescence. Not a scalable paradigm. Complexity of support - multiple technologies and equipment models.

2. Partial Migration - plan to migrate all services with TDM-to-Packet roadmap over to packet technology *except* critical applications like Teleprotection (TPR). [Risk - Low, Cost - High, Staff Development - Medium, Complexity - High, Able to transport new services - Medium-High]
   Pros: Minimizes risk by not carrying critical traffic, allows slower migration process - time to learn new technology. Allows for services to operate in parallel prior to having legacy services shut down.
   Cons: Requires building and operating two networks - one legacy, one packet (new). Capital costs to build and operate one new network whilst maintaining existing TDM services will be higher than building new and carrying out a full migration (e.g. more site visits, construction, outages, etc.). Still require critical services to be migrated at a later date - delaying architecture, design, standard development until required. Requires transport network to be split in order to carry legacy TDM as well as the packet network - may lead to bandwidth constraints. Complexity of support - multiple technologies and equipment models.

3. Full Migration - plan to migrate all services with TDM-to-Packet roadmap over to packet technology *including* critical applications like Teleprotection (TPR). [Risk - High, Cost - Medium, Staff Development - High, Complexity - Medium/High, Able to transport new services - High]
   Pros: Allows for standard migration planning - move all services to new network and salvage of old network - one project, migrate and done. New services, new capabilities, new network service models all possible. Moves utility from legacy model to next-generation model. New network is scalable, packet-based, and ready for deployment of current and future services. Simplicity of support - likely to have less types of technology and models of equipment to support.
   Cons: Requires significant up-front effort to plan for the migration. Capital costs for new network, possibly including packet transport, training, and construction all higher than other two options. Highest risk for new users of packet technology - something may go awry and cause outages. Need to complete audits of current network and requirements in order to ensure all requirements are met. Need to train and prepare staff to support new network technologies. May require some form of corporate reorganization. Need to convince other utility staff of the benefits and to clarify and mitigate perceived risks to some applications, e.g. teleprotection engineers.

When looking at how new packet-based services are able to support existing utility services, the core service architecture is the same - connection-oriented communication. The fact that the terminal devices have not changed often requires that the service interfaces cannot change either. Only the method by which communication is provided from source to destination may change. This means that if a service was a point-to-point service in the TDM world, it will remain a point-to-point service in the packet environment - they are both connection-oriented protocols. What are different are the options for new services on packet-based transport. Point-to-multipoint service architectures and the flexibility and control

offered by traffic engineering capabilities offer new controls, monitoring, and capabilities not seen in the legacy environment.

2.3 - What to consider - Precursor to Packet Migration

Consider the following, at a minimum, when considering a migration from legacy TDM transport and services to packet-based technology:

- ❏ Service architecture, characterization, and topology - what kinds of services are required and what protocols, bandwidth, tolerance to latency, tolerance to jitter, and tolerance to packet loss and out of sequence packets do the required services have?
- ❏ Deployment timeframe - timeline to in-service requirement?
- ❏ Physical interface types (analog, serial, etc.) - how do the terminal devices physically communicate?
- ❏ Typical service constructs - point-to-point, point-to-multipoint, substation-to-substation, substation-to-control center, etc.
- ❏ Network performance (bidirectional latency, jitter, bandwidth consumption)
- ❏ Service symmetry - any specific tolerance or limits on service asymmetry
- ❏ Service failover or restoration time - any specific requirements for service failover to backup paths (e.g. service restoration after failure detection in <50ms)
- ❏ For native packet-based services, are there any specific MTU requirements
- ❏ Network reliability and availability *objectives* - e.g. 99.9% availability - these will influence hardware and service architecture, and the need for alternate routes and failover options.
- ❏ Network quality of service - How does one service rank in priority versus all others? Which are most important and which can be restricted if congestion occurs?
- ❏ Network monitoring and alerting - How will you monitor, manage and report on the service to prove it is compliant with desired objectives?
- ❏ Network capacity - How much bandwidth is currently being used and what is the future growth potential?
- ❏ Underlying transport media - What media (i.e. fiber, microwave radio, DWDM, leased lines) will be used at layer 1 for the network?
- ❏ Cyber security - securing the data, control, and management planes cannot be overlooked.

Answering the above questions lays the foundation for performing a formal network audit and taking a snapshot of current, real-world network operation. Often the above information is not known and services must be researched to obtain a complete understanding. Ultimately, the information determined here sets the baseline for expectations and forms the basis for network evolution.

3 - Network Services

3.1 - Circuit Emulation Services

TDM networks typically have streaming services such as E1, E3, DS1, DS3 and the SONET/SDH family of interfaces. Streaming services are those in which the data flows continuously and without the concept of pausing or stopping - data is sent on a continuous basis whether useful or not. Packet networks typically implement legacy streaming service types by emulating the service. This is termed Circuit Emulation Services, or CES.

In general, CES works by encapsulating legacy service data in Ethernet frames at the transmit end and reassembling the data at the receive end. Two common formats exist - CESoPSN (Circuit-Emulation Service over Packet Switched Network) and SAToP (Structure-Agnostic TDM-over-Packet). CESoPSN adapts the TDM frame to a packet stream while maintaining the payload organization. This allows for

individual DS0 data to be visible to intermediate nodes, to be tracked and mapped as it crosses the packet network. SAToP adapts the entire TDM frame to packet, agnostic to the individual DS0 payload within. SAToP assumes the entire TDM frame will be reassembled for playback at the destination (e.g. A complete T1 or E1 frame).

The circuit emulation process does introduce additional transit delay to the service when compared to traditional TDM due to the encapsulation process. This is due to time needed to assemble the service frame (TDM to Packet) and the playout or jitter buffer at the destination (Packet to TDM). Another general effect of encapsulation is an increase in bandwidth used to transport a service over a packet network. The excess bandwidth of an encapsulated service is generally configurable and is inversely proportional to the desired latency, i.e. low latency encapsulated services requires a higher transport bandwidth.

3.2 - Network Synchronization

Circuit emulation services (CES) require disciplined network synchronization for clean, error free, operation, just as the TDM networks they replace. Conversely, network synchronization is not required if circuit emulation is not used on the packet network.

Traditional TDM and SONET networks have robust synchronization distribution methods built into their operating interfaces and protocols. Transport synchronization allowed network nodes separated by large distances to maintain synchronism to upstream references and provide error-free service. Maintaining links to those references was a requirement as legacy networks relied on robust sync distribution methods to form a complete synchronization distribution hierarchy. Despite changes in synchronization technology and transition to packet-based networks, the goal remains the same - to provide stable synchronization references in the support of clean, error-free, circuit emulation services.

When considering how to transition to packet-based technology and services, be aware that not all equipment is created equal especially when it comes to synchronization distribution and protocol compatibility. New packet-based transport equipment (microwave radio and fiber optic) may not support synchronization distribution within their Layer-1 protocols, forcing usage of Layer-2 and Layer-3 protocols such as IEEE 1588 - Precision Time Protocol. Additional, high-quality Stratum-1 primary reference source clocks (PRS) may be necessary to provide synchronization references at points throughout the network. In some cases, synchronization distribution using legacy TDM interfaces on transport equipment may be the necessary (e.g. T1-cards on packet based microwave radios).

This topic is mentioned so the reader is aware of the need for a comprehensive sync plan as part of any deployment of packet-based technology, and can incorporate synchronization planning into current or future network upgrade projects. Deployment of Circuit Emulation Services cannot be successful without proper network synchronization. Many current teleprotection schemes with legacy interfaces - in particular G.703 and C37.94 - require the use of Circuit Emulation Services. A robust synchronization plan is of paramount importance to their successful operation.

4 - Application Requirements

4.1 - Service Audit

Every utility needs to perform a complete assessment of the services currently being transported in their network. Often after many years of service some documentation will be lost or become inaccurate. The objective of this service audit is to gain a complete understanding of what services are being provided to the business, including the physical interfaces and the required topologies.

The performance objectives for a packet transport network may be set after the service assessment. Which services are mission critical, business critical and best-effort types of traffic? What services have low bandwidth requirements versus high bandwidth requirements? What services require low transit-latency? These are the questions which define how a utility wants its packet transport network to perform. The results develop into a comprehensive Quality of Service (QoS) strategy.

An audit of existing network services should follow a similar audit assessment as previously specified in section "**What to consider - Precursor to Packet Migration"** on page 6.

4.2 - Cyber Security

The Utility's security strategy may be driven by regulatory standards, the utility's own security policy, and industry best practices or by a combination of all three approaches. Ultimately the goal of the security strategy is to protect the availability, integrity and confidentiality of the organization's services and resources. Any new packet-based network must support the implementation of this strategy in its design, operation and management. It is equally imperative to communicate this security strategy to all relevant stakeholders and staff. Traditionally, the security of the TDM communications infrastructure may not have needed to be a priority amongst support staff. However, with the advent of packet-based technology and its associated security threats, such a mind-set must be changed.

It also should be noted that regulatory standards are at different stages of development on the different continents. Aside from such regulations, utilities must pursue security policies that adequately protect their services and resources. All concepts, plans or potential projects must include a cyber-security review at every step in the deployment process. Discussing and identifying the cyber security requirements up-front may impact technology selection and will result in a more complete, successful project in the future.

4.3 - Hardened Equipment

Packet network equipment complying with IEEE-1613 "Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations" and IEC 61850-3 "Communication networks and systems for power utility automation - Part 3: General requirements" are highly desirable for obvious reasons. This is not new. However, mandating compliance with these standards in a future project may limit the selection of potential equipment available. The tradeoff between technical capability and what can be done using a hardened platform is a question that many utilities will face. What features, protocols, and interfaces are available on the hardened platform? Does using the hardened platform require the use of additional equipment and hardware? How do the network management systems function and relate?

As an alternative, many utilities have chosen equipment not compliant with these standards and instead mitigated the situational risks using a controlled environment, dedicated communications system battery, good grounding practice, and optical isolation.

4.4 - Incorporating Leased / 3rd-party Packet Services

We are all aware of the ongoing discontinuation of traditional analog four wire (4W) leased-line services from commercial service providers. We also know that availability of traditional TDM services - T1/E1/T3/T3 /OC3/STM1 etc. are starting to decline in favor of packet-based service alternatives. The inevitable next question is how best to incorporate these new, packet-based replacement services into a next-generation network.

The short answer is to consider them as an extension of the utility packet-based network. Ethernet-based transport can be used in the same manner as legacy analog four wire or low-speed serial data links in

years past. In fact, native Ethernet transport for last-mile connections may make service access simpler as fewer protocol conversions are required. Higher speeds are also possible, making not just last-mile links but also managed network transport links possible. High-capacity (GigE, 10GigE) managed services may be used in parallel with the native internal utility network to add resiliency and backup paths to critical locations.

If a leased public network is being used as a primary traffic path, then the resilience must be carefully designed both physically and logically. In particular, for circuits carrying critical services, the details of the last mile redundancy in terms of full path diversity from the site must be specified and verified.

Prior to incorporating leased services into the new network, the same traffic and performance evaluation must be completed before using the new leased services. Third-party transport performance and capability must be known and profiled. Latency, bandwidth, maximum MTU size, packet delay variation (PDV), and even ping-time across the leased service must be tested and known. Service tests such as IETF RFC-2544 or ITU-T Y.1564 may be performed and results compared to the service-provider Service Level Agreement.

At the application-level, another consideration is what traffic will be permitted to transit across the leased service and what traffic must be excluded? When will the leased service be used and in what priority? What traffic classifications may use the leased service, avoid the lease service entirely, or only use in case of emergency? Traffic engineering around the use of the leased service must be considered. Network usage policy must be developed and incorporated in advance of the leased service integrating into the larger network to avoid a scenario where critical traffic is running across a link not approved for that purpose.

Lastly, the impact of evolving security standards and policies must be considered. How will new policies such as NERC CIPv6 (North America) impact the use of managed services? How will evolving cyber security standards in other regions of the world align with existing policies? Is the network technology planned for deployment able to adapt to remain compliant? With the leased service not under direct control of the utility, it must be considered to be ‘untrusted’. Therefore, end-to-end encryption and/or some other form of embedded traffic security or message authentication process should be deployed where necessary. Future cyber security policies may mandate encryption over any transport network outside of the defined security perimeters, adding additional complexity to an evolving network ecosystem.

5 - Technology Options

5.1 - Technology Variants

There are two main variants when it comes to packet network transport technologies: Carrier Ethernet (CE) and Multi-Protocol Label Switching (MPLS). These are in addition to traditional routed-IP networks utilizing layer-3 routers to move IP packets across the network. Both CE and MPLS use Ethernet as their basic building block and work by encapsulating service traffic inside an Ethernet frame. Service traffic is inspected at transport network ingress and identifiers added to the traffic stream. This identifier is additional information added to the transport Ethernet frame and used in the network core to switch the packet to its destination. How this identifier is generated and provisioned defines the majority of the differences between Carrier Ethernet and MPLS. Traffic engineering is a core part of both Carrier Ethernet and MPLS.

Carrier Ethernet is primarily targeted for transporting native Ethernet services. This is not to say Carrier Ethernet does not have the ability to transport other legacy and TDM services - product offerings vary in the interfaces supported.

MPLS product offerings can also transport multiple traffic types including TDM and legacy services in addition to native Ethernet services. Product offerings vary in the interfaces supported. MPLS is further subdivided into two variants, IP-MPLS and MPLS-TP.
The older, original variant of MPLS uses Internet Protocol for the control plane, hence the name IP-MPLS. IP-MPLS leverages existing Internet Protocol technologies in the control plane to make the network self-aware and reduce reliance on network management systems. This reduces human time needed to provision new services, automatically heal services upon network failures, and allow networks to be scaled to proportions difficult to otherwise attain. IP/MPLS was developed to further enhance the functionality of pure IP routing. In particular, it allows the logical isolation of different services to be achieved in a flexible manner through the use of MPLS VPNs that can be provisioned in minutes. It also supports sub-100ms convergence speeds and the ability to configure pre-determined explicit end-to-end paths similar to SDH/SONET.

The newer variant of MPLS is called MPLS-TP, where the TP stands for Transport Profile. MPLS-TP is mostly a simplified version of IP-MPLS with much of the control plane automation removed. MPLS-TP operates using the same architectural principles of layered networking used in legacy transport network technologies like SDH, SONET and OTN. MPLS-TP may not have a control plane at all, requiring all provisioning and network awareness to be managed elsewhere. While simpler in function, this puts all provisioning, and perhaps more importantly, rerouting decisions, in the hands of the Network Management System.

Many utility telecom staff will find Carrier Ethernet and MPLS-TP attractive because of the resemblances to SONET/SDH. Although perhaps not as well-known and understood, IP-MPLS has the same static provisioning abilities as Carrier Ethernet and MPLS-TP, but gives an organization the additional options to static provision some traffic (e.g. teleprotection) and automate the rest. Using one combined, multi-service network technology may save operational time and expense.

Regardless of the technology chosen, carefully consider any offered products lines for the TDM and legacy interfaces your organization requires. Low-speed or legacy Interface support widely varies by manufacturer and product line.

5.2 - Control Plane and Management Plane

One of the key features of a next-generation, packet network is the ability to provision, control, and monitor traffic streams in real-time. Advanced network management tools offer visibility and granular control over services like never before.

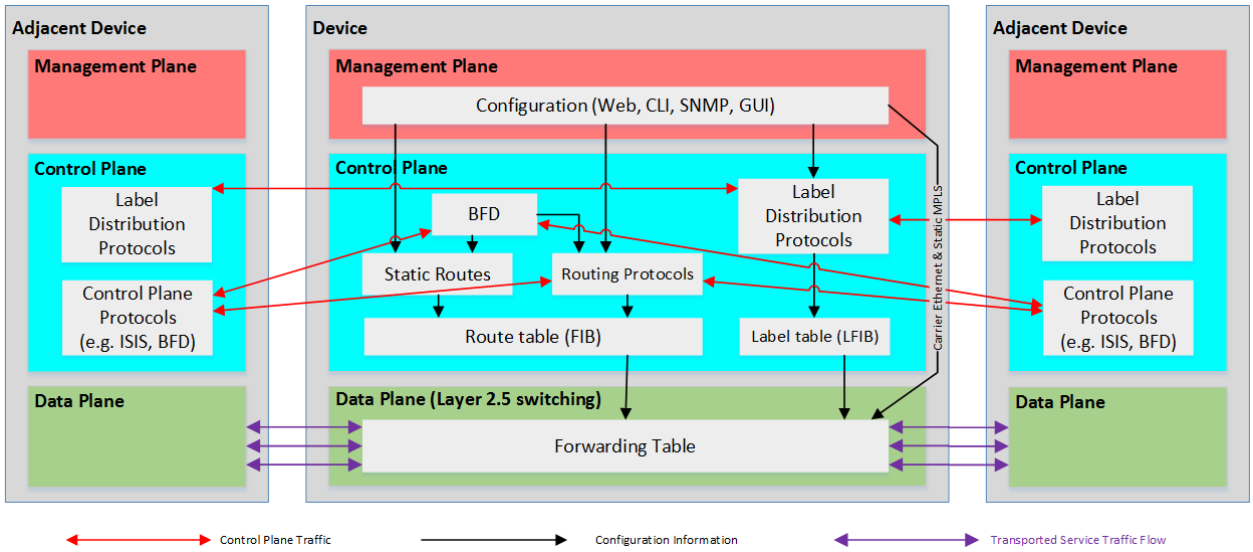

Figure 2 - Illustration of Device Planes

In discussing the various technology features and functions, it is critical to understand the difference between *control plane* and *management plane*, as all these technologies have some or all of them (the only one not described here is the *data plane*, where service traffic flows). A control plane involves communication sessions between network nodes. Routing protocols discover adjacent nodes and interfaces and exchange network information to build virtual network topologies. Interface statuses are monitored, reachability through the network is determined, and ultimately services are provisioned.

Within the management plane are user-interfaces and machine-to-machine interfaces facilitating communication between the user or network management software (NMS) and the individual nodes. If the control plane is not present on a node, then services are provisioned on a per-node or node-to-node basis using the NMS software. Likewise, the network topology is only known on the NMS software rather than the nodes themselves.

The implementation options associated with the control plane have pro's and con's - control planes with built-in routing protocols can create self-healing networks able to reconfigure and reroute around a network failure. But, the capability comes at a cost of additional processing time (routing protocols) for service to come to an operational state, complexity, and in some cases, security if not configured properly. Control planes with routing protocols do have the added benefit of near-autonomous operation. Once provisioned and built, the network will handle rerouting and restoring of services as needed, independent of any NMS tools.

A simple or non-existent control plane is simpler in architecture, typically running complex NMS software on a server infrastructure as a trade off to a control plane on the individual nodes. In this way, the node has minimal routing tables and route calculations to be performed, if any. This reduces CPU overhead within the network hardware itself. Having software running centrally versus distributed across the network can make upgrades and management simpler and fewer protocols to be exploited for potential vulnerabilities. The one question that remains is what happens if the connection from node to NMS is severed - how are services impacted?

5.3 - Technology Lifecycle

Packet network lifecycles are more similar to IT type equipment than traditional telecommunications type equipment. Today's packet network transport equipment should be planned for replacement in five to ten

years; a challenge when large networks may take up to five years just to deploy. Part of the reason for this is a chosen equipment manufacturer may not support a product line much longer than five to ten years due to technology evolution or planned obsolescence or both. Good cyber-security practice dictates manufacturer-provided, active firmware support for these systems. This message needs to be understood by utility executives and accounting as it may not be in alignment with traditional tax depreciation cycles for telecommunications equipment. The days of deploying telecom assets and operating them for 20-30 years are now a thing of the past. Assets now more closely resemble IT assets with life spans less than ten years.

6 - What's Next

In this inaugural whitepaper prepared by members of the Packet Network Working Group, is meant to be a primer for topics related to assessing current state of utility networks and preparing them for migration to packet-based technology are presented. Discussion points on Network Services, Application Requirements and Technology Options are meant to assist the reader with items to be considered at the concept phase of a future network upgrade project. As discussed, this whitepaper should set a foundation for the future work of the group and to offer opportunity for discussion among readers and authors. UTC members are welcome to connect with the PNWG via the NetWorks Community portal and engage directly on this paper and the future topics. Subsequent whitepapers from the PNWG will discuss Project Planning and Implementation, Operational Skills and Staff Development, Business Process Development and Network Management and Control.

About the Authors

Principal Authors

Clinton Struth, M.Sc. P.Eng. [Clint@scinet.ca] – Clinton is currently Principal Engineer, SCI Networks Inc., an engineering consulting firm with specialty in telecom, networking, and cybersecurity for the utility, oil & gas, and pipeline sectors. Prior to 2014 Clinton was employed by AltaLink (Calgary, Canada) as Principal Engineer – Netcom, where he led the Telecommunications Engineering group and implemented the one of the first fully-converged IP/MPLS networks in a utility environment. Clinton holds a Bachelor of Science in Electrical Engineering (Power Systems) and Master of Science in Telecommunications Engineering, both from University of Manitoba.

Shaun Skidmore, B.Sc. EE PE [sskidmore@idahopower.com] has worked for Idaho Power Company for the last 20 years as an engineer in the Communications Engineering group. For the last 12 years he has served as Principal Engineer concentrating on architecture and planning. Recently, Shaun architected a fully converged IP/MPLS network to replace Idaho Power Company's entire time division multiplex transport network. He holds a Bachelor of Science degree in Electrical Engineering from a joint engineering program of the Boise State University and the University of Idaho. His areas of emphasis are network and transport engineering and information security. He is a registered Professional Engineer.

Cory Struth, B.Sc. CompSci [Cory@scinet.ca] - Cory is currently Principal Network Architect, SCI Networks Inc., an engineering consulting firm with specialty in telecom, networking, and cybersecurity for the utility, oil & gas, and pipeline sectors. Prior to 2014 Cory was employed by AltaLink (Calgary, Canada) as IP/MPLS Network Architect and Cyber-Security Lead - Netcom, where he developed and implemented the IP/MPLS network and service architecture for AltaLink's high-voltage transmission system. Prior to AltaLink, Cory worked in the oil & gas and service-provider industries implementing next-generation networks, Unix, and Cybersecurity programs. Cory holds a Bachelor of Science in Computer Science from the University of Manitoba.

Contributing Authors

Cormac Long - ESB [Ireland] <cormac.long@esb.ie>
Pascal Motsoasele - ESKOM [South Africa] <MotsoaPP@eskom.co.za>
Kamal Medjdoub - Hydro Quebec - [Canada] <Medjdoub.Kamal@hydro.qc.ca>
Peter Moray - UTC [UK] <Peter.Moray@utc.org>
Lamont Hill - Oncor [USA] <Kevin.Hill@oncor.com>
Ron Beck - Central Lincoln PUD [USA] <rbeck@cencoast.com>
Zwelandile Mbebe - ESKOM [South Africa] <MbebeZ@eskom.co.za>