Grid Communications Protocol Interoperability on Converged Virtual IP networks

Eruch Jal Kapadia
Sr. Solutions Architect, Cisco Systems Inc.
Agenda

- Architecture
  - Reference Model
  - Building a Converged Architecture

- Converging on IP

- Architecture Discussion
  - Converged WAN
  - Transport MPLS-TP

- Protocol Interoperability
The Legacy Approach to Grid Apps
Promotes Multiple Silo’ed Networks/Systems
Building a Converged Architecture

A Converged Communications Architecture Is One which Brings Together a Diverse Set of Functions to Share a Common Set of Resources, Driving Down Cost, and Synergistically Creating New Efficiencies by Increasing Interaction Between Them.

Traditional View + New Interpretation

**Transport Convergence**
- Using the same underlying transport to meet communications requirements for multiple types of traffic

**Protocol Convergence**
- Allowing elements talking diverse protocols to communicate with each other

**Technology Convergence**
- Multiple technologies (voice, data etc.) over the same underlying infrastructure

**Intelligence**
- Allow elements (including apps) to analyze information, make collaborative decisions and exercise control cutting across domains to which they belong

**Services**
- A uniform set of service (such as security) policies spread across the environment adhering to overall business objectives

**Design**
- Architectural development in a manner which allows modularity as well as architectural leverage across networks
Converging on IP
IP is not just a protocol but an architecture

- Architecture

- Seeking a *global* optimum *NOT Local* excellence
- Jack of everything but not optimized for anything
WAN – Converge with IP/MPLS
Converged WAN
Virtual Segmentation in the Core
WAN Architecture: MPLS Single Core

Model Characteristics

• **Single core, Layer 2 & 3 VPN services**

  • **Segmentation**: Layer 3 VPN offers layer 3 controlled policy based segregation enabling multiple zones. Layer 2 VPN to provide layer 2 transport for utility applications e.g. 61850

  • **Convergence**: MPLS TE with fast reroute to achieve <50 ms link failure recovery in core and sub-second recovery for node failure
WAN Architecture: Regionalized Domains

Model Characteristics
- Extends the single core Model
- Regionalized MPLS Core w/ Layer 2 and Layer 3 VPN services

Segmentation:
- Multiple utility domains based on service level or regional boundaries.
- Domain can be IP or IP/MPLS
- Shared resources like Control or Data Centers are directly connected to inner Core.

QoS
- Defined at the edge and for the MPLS domain. MPLS QoS for all domains is similar to assure transport of the QoS parameters through the MPLS core
WAN Edge Segmentation with VRFs

Virtual Router A
Virtual Router B
Virtual Router C
Virtual Router D
Virtual Router E

Substation
- Employee and Vendor Engineering Access
- Video and Access Control
- Serial/IP RTU and IEDs
- Feeders with Reclosures and Switches
- AMI

VRF-Lite to WAN Mapping
IP/MPLS perception Corrected

- IP/MPLS may take too long to converge to meet the requirements of utility operational requirements.
- Solution: Use the Fast Reroute capability to achieve <50 ms Link failure recovery and sub-second recovery times for node failures.

**Node Protection**

**Link Protection**

![Node Protection Diagram](image1)

![Link Protection Diagram](image2)
Transport
SONET perception

- SONET is the only preferred transport choice for utilities due to its resiliency, convergence, and OAM (management).

Reality:


- Forcing packets into Sonet/SDH framing is an inefficient means of transport; operators had no other choice but to transport packets over Sonet/SDH to use its management, resiliency, and reliability functions.

- MPLS-TP and OTN incorporate the OAM, resiliency and are more scalable.

- In addition, there is tremendous momentum around 100G transport as the next-gen core transport rate. Yet, the Sonet/SDH standards have been capped at 40G rates (256 VC-4 in SDH or 768 STS-1-SPE in SONET).
Transport and IP convergence

- MPLS-TP
  - MPLS-TP OAM
  - Path Protection
  - 50ms Switchover
  - Alarm and monitoring
  - Static Provisioning

- PW

- GMPLS

- IP/MPLS
  - PHP
  - ECMP
  - MP2MP
  - IP
## Take the Best of Both World

<table>
<thead>
<tr>
<th>Connection mode</th>
<th>TDM Transport</th>
<th>Packet Data Network</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Connection oriented</td>
<td>Connectionless (except TE)</td>
</tr>
<tr>
<td>OAM</td>
<td>In-band OAM</td>
<td>Out-of-band (except PW, TE)</td>
</tr>
<tr>
<td>Protection Switching</td>
<td>Data Plane Switching</td>
<td>Control plane dependency</td>
</tr>
<tr>
<td>BW efficiency</td>
<td>Fixed Bandwidth</td>
<td>Statistical multiplexing</td>
</tr>
<tr>
<td>Data Rate Granularity</td>
<td>Rigid SONET hierarchy</td>
<td>Flexible data rate</td>
</tr>
<tr>
<td>QoS</td>
<td>One class only</td>
<td>QoS treatment</td>
</tr>
</tbody>
</table>

**Packet Transport**
MPLS-TP Enabled Cloud

- Connection Oriented, pre-configured working path and protect path
- Transport Tunnel 1:1 protection, switching triggered by in-band OAM
- Phase 1: NMS for static provisioning

![Diagram of MPLS-TP Enabled Cloud]

**Sub station**

**Client node**

**PE**

**Working LSP**

**Protect LSP**

**NMS for Network Management Control**

**MPLS-TP LSP (Static or Dynamic)**

**Pseudowire**

**In-band OAM (e2e or per-segment)**

**Client Signal**
Connection Oriented Ethernet
Transport Evolution to MPLS-TP

- Multiprotocol Label Switching – Transport Profile
- Based on IETF Standards
- Service Flexibility/Scalability of MPLS
- No forwarding dependence on IP routing protocols
- Graceful extension of IP/MPLS Core into Access & Aggregation

Benefits to the Utility

- Transport operational model, Connection Oriented, Deterministic, Point & Click Mgmt.
- SONET/SDH like OAM&P (operations, administration, maintenance & provisioning)
- Highly Scalable (10G/40G/100G, Statistical Multiplexing)
- Support for Legacy TDM Interfaces (DS1, DS3), Synchronized Ethernet (1588, SynchE)
SONET Aggregation Solution - Today

Existing SONET Aggregation

- Fixed BW Assignment
- No Statistical Multiplexing
- No Multi-point Support
- Capped at 2.5G or 10G

TDM + IP/Ethernet Core

Data Hub DWDM Core

Class A Substations OC-48 SONET

Class B Substations OC-3/12 SONET & Microwave

Legacy TDM
Packet Transport Aggregation Solution

Next Gen Transport
- Ethernet over SONET to MPLS-TP
- Scale to 10G and Beyond
- Legacy Interfaces via DWDM/Circuit Emulation over Packet (CEoP)
- SONET like Operational Model
Substation Transport Evolution

**Current**
- IP with SONET Transport

**Phase 1**
- Extend DWDM Footprint

**Phase 2**
- End to End Packet Transport

---

**Data Hub**
- SONET ADM
- OC-3/12/48

**Class A Substation**
- SONET ADM
  - Utility Mux
  - SCADA Power Control
  - Admin/IT
  - DS-x
  - 10/100

**Phase 1**
- SONET ADM
- N x 10G DWDM
- 15454 DWDM

**Phase 2**
- N x 10G/40G/100G DWDM
- CPT Enabled DWDM
  - GE/10GE/DS1

**Multi-Service Router**
- Video Surveillance
- VOIP
- Mobility
- Smart Meter (AMI)
- SS Automation

**Class B/C Substation**
- CPT Enabled DWDM
- GE/10GE/DS1

**Class B/C Expansion**
- Low Latency

---

Grid Interop 2011
All rights reserved by the author
Eruch J. Kapadia
System Control Network – IP MPLS

The System Control Network interconnects substations with each other and with control centers. It is designed to support teleprotection via very low latency (under 5 msec) and high reliability architecture.

This network does NOT go through or use an enterprise core.
Protocol and IP interoperability
IEC 61850 GOOSE and SV over the WAN
Challenges and Solutions
CRAS, distance tele-protection, WAMS require sending GOOSE and SVs between substations and to control Center.

- The raw data sample values (SV) type 4 and GOOSE type 1 messages are time critical and mapped to Ethernet.

**Issues Inside Substation:**
- Inefficient Multicast Traffic Distribution
- Cyber security
- Scaling broadcast domain

**Issues outside the Substation**
- Ethernet is NOT routable and not built for WANs.
- Large Ethernet bridge domains can cause instability
IEC 61850-90-1 Solution to Carry GOOSE/SV over the WAN

- **Tunnel. Example**
  - Layer 2 Tunneling Protocol (L2TP / L2TPv3) – RFC 3931
  - Generic Routing Encapsulation (GRE) Tunneling - RFC 2784

- **Gateway**
  - Example Proxy Gateways
  - GWs Must Terminate Protocols
  - GWs must Understand Applications and configuration changes in the application
  - Latency and Jitter addition, especially when GWs are implemented in software

- **Tunneling or Encapsulation is the more realistic option**
  - MPLS, VPLS, PWs are examples of Encapsulation technologies
Problem: Layer 2 GOOSE / SV over the WAN – Implications on Scaling, Security, Replication, Flooding, etc

Issues:
- Intra Substation Replication
- Inter Substation Replication
- Information Leakage – Security Implications
- Wasted Bandwidth
- Limited Scale

VPLS: Packet replication and the amount of address information are the two main scaling concerns for the provider edge device. When packets need to be flooded (because of broadcast, multicast, or destination-unknown unicast address), the ingress provider edge needs to perform packet replication. As the number of provider edge devices in a VPLS increases, the number of packet copies that need to be generated increases.

1. Fault in the Vlan spread across Substations
2. Traffic flooding inside the substation vlan
3. Info security leak

1. Multicast Replication Inefficiently done. Replication per Tunnel.
2. Blind flooding of Ethernet Multicast traffic wastes BW in the WAN and in the other substations
3. Tunnel Scaling of the solution is limited
4. Inefficient forwarding of traffic in the WAN (due to tunnel encapsulation)
5. Higher MTTR as the tunnel has to do live ness checks, to detect tunnel failures
6. Weaker Security – Flooding sends data to unneeded/unwanted places… information leakage
Solution: IEC 61850 with IPv4/v6 profile provides - Scalability, Security, etc

GOOSE/SV on IPv4/v6 routable protocol
- Scalable
- Low (in usecs) Latency – All HW forwarding Path
- Low (in usecs) Jitter
- Cyber Security benefits
- Easy to trouble shoot and manage over WAN – proven model
- ...

GOOSE or SV Messages are NOT Flooded in the WAN.
- Saves bandwidth
- Reduces latency due to replication inefficiency
- Reduce inter packet jitter
- Enables stricter applications like Tele protection, primary bulk power protection, CRAS, etc
- Improves security and information leaks
- Reduces the window for Denial of Service attacks (limit the traffic and subnets from which GOOSE traffic is accepted)

Packet replication at most optimal points in the network

Green traffic contained to Green substations

WAN (Utility or SP owned)
IP profiles for all 61850 messages!!!

- IEC 61850-90-1 extended the 61850 beyond the substation but did not address the challenges of extending tele-protection controls beyond the sub-station.
- IEC 61850-90-5 for PMUs is working on a 61850 profile to carry GOOSE / SV over TCP/IP[v4v6] stack
- IP profiles being developed above must Not only be restricted to PMUs, but also to other all relays and applications!!!!
## Protocols Communication Architecture

<table>
<thead>
<tr>
<th>Feature</th>
<th>60870-5-101</th>
<th>60870-5-104</th>
<th>DNP3</th>
<th>60870-6-TASE.2</th>
<th>61850</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>SCADA</td>
<td>SCADA</td>
<td>SCADA</td>
<td>Control Center to Control Center</td>
<td>Substation automation, Substation to Control Center and other domains</td>
</tr>
<tr>
<td>Communication</td>
<td>V.24/V.28 or X.24/X.27</td>
<td>TCP/IP over ethernet 802.3 or X.21</td>
<td>V.24/V.28 or X.24/X.27; TCP/IP over Ethernet or X.21</td>
<td>TCP/IP and OSI over Ethernet 802.3 or X.21</td>
<td>TCP/IP and OSI over Ethernet 802.3 or X.21; Ether-type for GOOSE and SV</td>
</tr>
<tr>
<td>Layering</td>
<td>3 layer</td>
<td>7 layer (TCP/IP)</td>
<td>4 layer (serial) or 7 layer (TCP/IP or UDP/IP)</td>
<td>7 layer and Object library</td>
<td>7 layer (TCP/IP and OSI) and logical node and object library</td>
</tr>
<tr>
<td>Routing</td>
<td>N/A</td>
<td>IP</td>
<td>IP (TCP or UDP)</td>
<td>IP, OSI NP</td>
<td>IP, OSI NP</td>
</tr>
<tr>
<td>Transport Protocol</td>
<td>N/A</td>
<td>TCP</td>
<td>Pseudo Transport over serial, TCP or UDP over IP</td>
<td>TCP, OSI TP</td>
<td>TCP, OSI TP</td>
</tr>
<tr>
<td>Open support for encoding (XML etc.)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>HTML and XML coded messages products</td>
</tr>
<tr>
<td>Open Service support (HTTP, CORBA, SOAP etc.)</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>IEC 61400-25-4 defines a webservice protocol for IEC 65180-7-2</td>
</tr>
</tbody>
</table>
Thank you.
MPLS-TP Encapsulation

SONET/SDH
- VT1.5 SPE
  - STS-1/Nc SPE
  - VC-3/4 SPE
- DS1 Service
  - E1 Service
- VT1.5 Muxed into STS-1
- VT1.5 approximately Equivalent to Pseudowire

Ethernet Mapping
- Network Identifier
  - STS/VC number
- STS-N/VC-3/4 approximates an LSP

GFP-F/HDLC
- STS-1/Nc SPE
  - VC-3/4 SPE
- SONET SDH over DWDM

MPLS-TP
- Pseudowire Encap
- MPLS Label Switched Path (LSP)
- Circuit Emulation 1588v2
  - Generic Associated Channel (G-Ach)
  - for Inband MPLS-TP OAM

Pseudowire Muxing Function
- MPLS Label Switched Path (LSP)
- Ethernet Service
- 802.1Q, 1ad
  - PVC3 Encap

MPLS Label
- Network Identifier
  - MPLS Label
- G-Ach