Avoiding Traps and Pitfalls When Designing SMPTE 2059-2 Networks

Thomas Kernen – Staff Architect
Mellanox Technologies
Timing accuracy for ST 2110 networks

- IEEE 1588 Precision Time Protocol
  - SMPTE 2059-2 PTP Profile
- Slave to GrandMaster offset
  - Max +/- 500ns
- Well disciplined Endpoints
  - PTP stack stability
  - Filters, control loops
- Well designed networks
  - PTP aware devices
  - Boundary, Transparent Clocks
What could possibly go wrong?

- Deadlines
- Planning, lack of PTP experience
- Lack of in-depth testing
- Quality of project gate reviews
- Hardware/software limitations
- Efficiency of fixes/workarounds
- Unscheduled personnel events (reality check)
- “Other urgent project” that needs taken care of

The clock is ticking
Timing strategy

- PTP message rates
  - Don’t underestimate the impact of changing these rates
  - Must be consistent across the whole PTP domain
  - If changing defaults, test and validate corner cases, and test again!

- Managing the GM hierarchy (BMCA dataset)
  - Priority1, Clock Class, Clock Accuracy, Clock Variance, Priority2, Port ID
  - Setting P1 is like using a sledgehammer, P2 is generally more appropriate

- Where to connect the GMs? (Spine or leaf)
  - It depends, but really it shouldn’t make a difference (port cost/availability)

Network design

- PTP aware vs. non aware
- Transparent Clock, Boundary Clock?
- IPv4, IPv6 transport (Link Local Addresses)
- Multicast, Mixed Mode, Unicast messaging?
- PTP message path selection (in-band, mgmt)
- PTP traffic isolation using VRF/LAG/VLAN
- Management TLV messages (behaviour)
Basics: Securing all hosts

- Authentication, Authorization and Accounting (AAA)
  - Connection attempts, timestamp, username, IP address, commands used
- Access Lists (ACLs) to limit who can reach the device, on all interfaces
- Only use TLS encrypted transports (SSH, HTTPS, ...) for all sessions
- No unprotected interfaces! Unauthenticated GM web interface
- Don’t forget the physical ports too! Console, serial, auxiliary
- Disable unused services, interfaces, protocols
- Threat modeling

Securing the PTP network

- Traceable time sources
  - Source diversity, frequency & time traceable
- Acceptable Master Table (AMT)
  - Prevent remotely connected device from attempting GM role takeover
- “Forced master”
  - Prevent locally connected device from attempting GM role takeover
- Threat modeling (again)
Monitoring

- Broadcast/Network Controller PTP dashboard
  - Realtime visibility and overview of PTP health
- 1pps signal comparison between GM & SLAVE
  - Out of band signal validation at specific points
- Packet analysis of PTP messages (online/offline)
- PTP message counters for all nodes (trigger alarms)
- Slave port monitoring
  - Transfer slave information to monitoring node
  - Standardized in upcoming IEEE 1588 v2.1

Diversity & Failure testing

- Design for diversity
  - ST 2110 with ST 2022-7 for media
  - PTP redundancy != standard feature
  - Stack specific implementations
  - Different designs = different results
- Test for partial and total failure
  - Define key metrics
  - Recovery time (media and PTP)
  - What is gating this?
  - Is it important to reduce?
Vision vs. reality = Compromise

• Do your research
  – Vendor inputs, not just the datasheet
  – Presentations of existing projects
  – Industry publications, reference designs

• Cross check information
  – Early days, limited experience, inaccuracies

• You will need to compromise
  – Common feature baseline & operating model

Decision tree = Methodology

• Make a plan and stick to it!
  – Uncertainty will just make things worse

• Test & validate:
  – your design methodology
  – your vendors announced capabilities
  – end to end with all vendor equipment interconnected, including failure scenario

• Work with your vendors around their limitations, constructive process

• Schedule the fixes, enhancements, feature requests and deal breaker deadlines

• Finally, mitigate implementation limitations once everything else has been done
Plan, test, rinse, repeat

• All PTP networks are equal
  – Some more than others
• Your network will always be unique
  – Slight differences = big impact
• Plan ahead, mitigate limitations, think again
• Test again, again, and again, and some more

Thank you

Thomas Kernen, Mellanox Technologies
tkernen@mellanox.com