# Manage (Synchronisation Performance) …..or Die?

ITSF 2005

Greg Mason

Issue 1 IEE delivery

# Introduction

- Why manage synchronisation?
- What should management deliver?
- What is synchronisation performance monitoring?
- Who should be involved?
- When should we monitor?
- How should we monitor?
- Where should we monitor?
- Case studies to demonstrate the return on investment
- Converged network monitoring considerations

# Why manage synchronisation?

- Part of the business case! (due diligence)
- To reduce overall cost of ownership by:
  - reducing service downtime
    - increase business confidence - contract renewal
  - understanding network performance
    - efficient use of synchronisation equipment
    - minimise expenditure
  - reduce resource chasing faults
  - automating processes > evidence based SLA

# What should management deliver?

- Overall view of the network status (health)
- Control network & service
- Performance, logged - evidence
- Activity levels
- Input to assessing operational cost
- Centralised, efficient functionality
- Fault finding tool

# What is synchronisation performance monitoring?

- Act of observing (& recording) digital data flow!
- QoS measure similar to packet loss or BER
- An integral part of network management
- A tool to maintain the network (evidence for decisions)……but
  - …..need an up to date view of synchronisation & service network topology & connectivity……&
  - good relationship with network operations

# Who should be involved?

- Owner
  - wants to see right value (performance Vs cost)
  - … but your champion
- First line support (alarm management)
- Second line support
  - Business As Usual action management > processes
  - supplier (contract support) management
  - escalation > 3rd line & owner
- Third line support (buck stops here)
  - network design, process & procurement support

# Synchronisation performance monitoring – when?

- Assessing new network equipment/service
- Commissioning/acceptance
  - new network, or extension -
- Business as usual monitoring
  - set alarm thresholds -
- Problems
  - confirm synchronisation at fault?
  - or confirm synchronisation NOT at fault

# How (performance measurement)?

- Integrated SSU function
  - Permanent (static) network/service monitoring
  - By unused input reference port – NOT ENABLED!
  - For faulting (if within reach!)
- Dedicated synchronisation test equipment
  - Possibly for network/service monitoring
  - Largely for commissioning/remote faulting

# Where is performance monitored?

- At source – case study 1
- At network architecture confluence
- At distribution point
  - SSU
  - significant items of infrastructure >
- Service Access Point (SAP)
  - sample (not everywhere)
  - know what the customer is getting
  - remote from key building - most difficult

# Case study 1

- Objective : Importance of monitoring the network synchronisation source
- GPS (PRN 23) failure January 1, 2004
- BT’s multiple Caesium feeds at PRCs show GPS failure
- 50+ SSU’s internal oscillator performance threshold also reject GPS feeds

# Case study 1: Benefits_1

Performance monitoring:-

- clearly identified the root cause as being a GPS problem
- indicated the magnitude of the problem
- showed SSU had switched away from GPS source
- showed good SSU performance was maintained

# Case study 1: Benefits_2

Underlying point, performance monitoring:-

- knowing the alarm cause enabled the OS staff to concentrate on other work – no additional support teams (£)
- provided confidence in the network operation
- demonstrated clear benefit of performance monitoring (confirms strategy)
- confirms the need to monitor the source

# Case study 2

- Objective : importance of performance monitoring when bringing new network infrastructure into service
- Example: large narrowband switch
- Prior successful model synchronisation test

# Case study 2_1

- New switch introduction: perceived synchronisation fault
- First Office Application
  - Manifestations:
    - Network wide (but not all) signalling problems reported
    - Reported framing failures
    - Reported poor service quality
    - Reported interconnect problems

# Case study 2_2

- Switch supplier immediately (& incorrectly) pointed to synchronisation performance failure
- Reports symptomatic of a synchronisation failure
- Other factors:

  difficulty establishing absolute facts!
- Prove it was not a synchronisation failure!

# Case study 2_3

- Permanent monitoring strategy in place:
- MRTIE logging proved switch synchronisation good, i.e. that the deviation (transfer performance) from what the SSU was delivering was minimal
- SSU performance evidence from ‘downstream SSUs’ good 🗐 SSU not the problem

# Case Study 2_4

- Monitored a voice concentrator theoretically locked to switch, indeterminate?
- Switched voice concentrator synch source to old switch, performance appeared to improve
- Problem something to do with new switch?
- What was the real cause?

  - eventually discovered to be signalling

# Case Study 2: Benefits

- Underlying point, performance monitoring:-
  - Prevented investigation pursuing false trail
  - Hence:
    - speeded up finding real fault: a frame processing oversight in new switch silicon DSP = £ saving
    - prevented waste of resource = £ saving
    - maintained confidence in the synchronisation network
- Confirmed the need to performance monitor new network segments as they come into service
- Demonstrated benefit of investment

# Case Study 3

- Objective : Importance of performance monitoring significant items of service network infrastructure
- Private circuit (TDM) network

# Case Study 3_1

- Network wide frame slip reports
- SSU performance good SSU not the problem
- Architecture indicated likely place……
- But no equipment alarms?

# Case study 3_2

- Permanent ‘sample’ monitoring was in place on adjacent switch……no problems
- Moved SSU monitoring to likely switch via DDF –

  – poor performance indicated
- Experienced support switched to standby clock
- Network alarms cleared –
- Cause : failing oscillator – but no equipment alarms!

# Case Study 3: Benefits

- Underlying point, monitoring:-
  - Showed where it wasn't…
  - Directed resource to the vicinity of likely area…
  - Hence:
    - speeded up finding real fault: = £ saving - customer
    - prevented waste of resource = £ saving – business
    - maintained confidence in the synchronisation network
- Demonstrated benefit of investment

# Converged network monitoring strategy?

- Same principles apply – but more so?
  - Potentially more complex structure
  - Greater degree of software control
- Why?
  - The packet generation rate is created by the edge device clock
  - If the ingress rate different to PIG clock
    - > buffer overflow & packet Loss

# Converged network monitoring strategy?

- Services affected
  - Real time services
    - Voice
    - Video streaming & conferencing [protocol sensitivity]
    - Application may drop ‘exceeded time to live packets’
    - Secure links, financial transfers?

# So Where?

- Where flow rate controlled/generated?
- In principle:
  - PSTN  IP Gateway (PIG)
  - Media servers
  - Critical edge devices controlling packetisation
  - Large Routers with future ‘Synchronous Ethernet’  interfaces
  - Where TDM interfaces persist
    - Large Routers with SDH interfaces
    - SDH VC4 switches for specific QoS dependent services

# Summary

- We have discussed….
- What, why, where, when, who…..
- Case studies to demonstrate the benefits
- The principles of applying a monitoring strategy to a converged network

# End

- Thank you, questions?