SLA Monitoring in Next Generation Networks

Charles Barry

CEO, Brilliant Telecommunications

ITSF, London, November 2007

Outline

Prelude

- SLA Monitoring in Legacy Networks
- Next Generation Networks use similar principles

Basis of SLA Monitoring in Next Generation Networks

- IP Backhaul Requirements
- Packet network performance protocols
- Active Monitoring
- End-to End and Segment Monitoring, Metrics

Data Collection and Analysis

- Network Management Stations
- Deployment of timing clients (multi-purpose)

Concluding Remarks

- Managing performance of Next Generation Networks

Legacy Networks

Legacy (circuit-switched) SLA monitoring is *indirect*

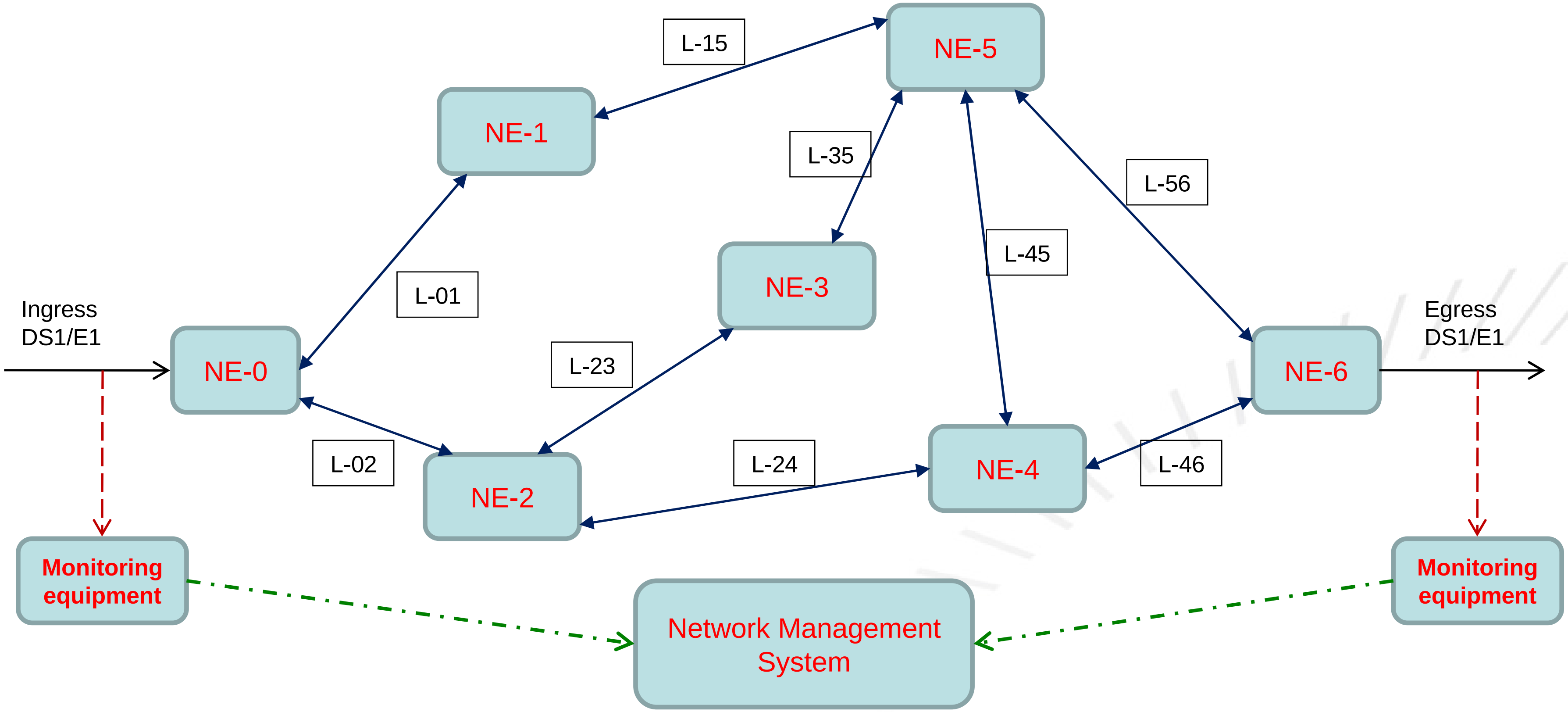
- Connections viewed as *pipes* – bandwidth availability is by design. Path is fixed and constant.
- SLA based primarily on *up time* –
  - Is channel is functioning and the bit-error-rate acceptable?
  - Network Synchronization addresses *slips* and *pointer movements.*
- Trunk fabric meeting requirements is equivalent to SLA conformity for all constituent channels.

Legacy SLA monitoring is achieved by monitoring all trunk segments

- Multiplexing format includes error checking.
- Pointer activity provides information regarding service clock stability.
- Major Alarms (LOS, LOF, etc.)

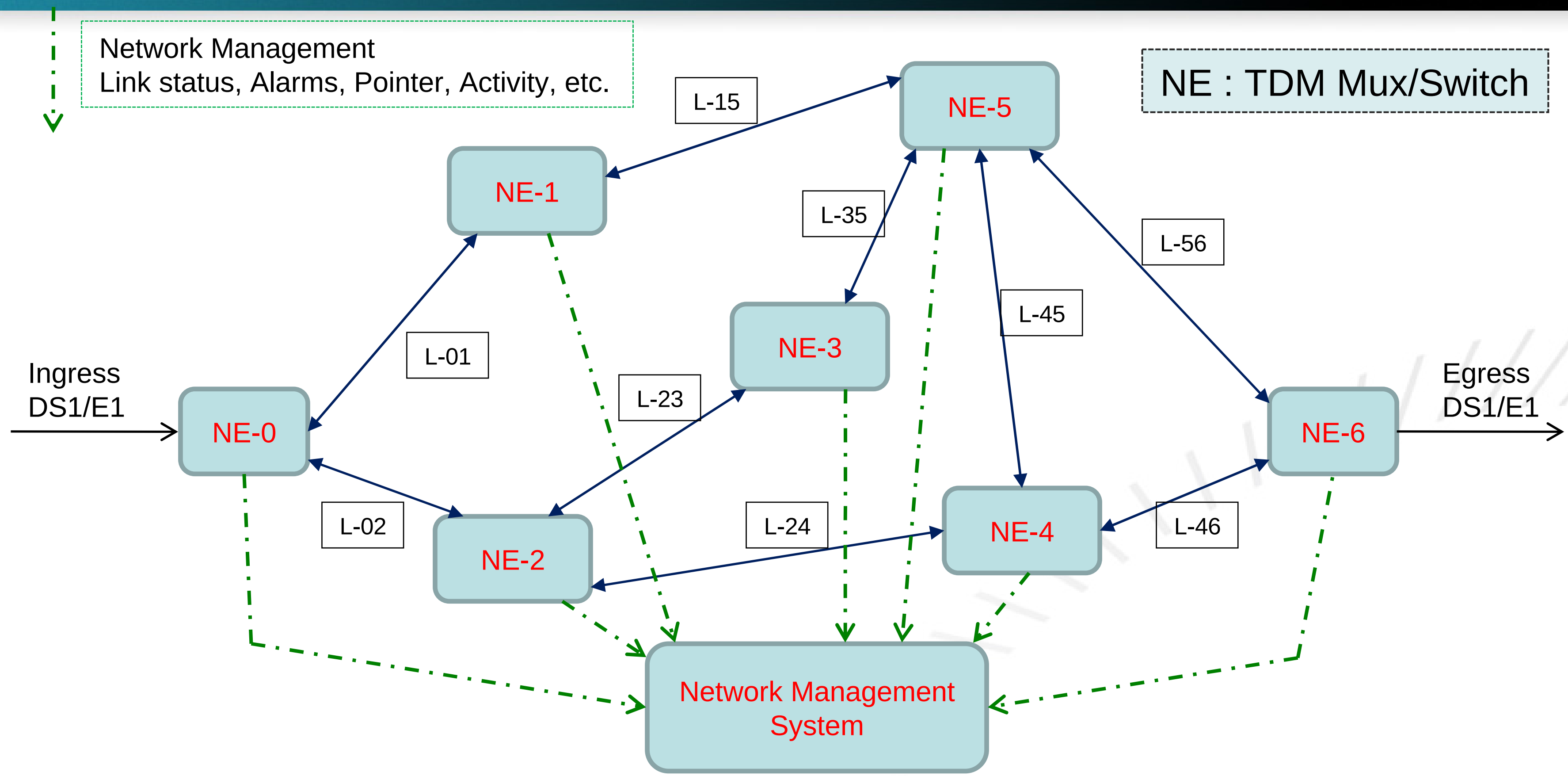
SLA monitoring in Next Generation Networks is based on the same *principles*

Monitoring Options – 1 (Legacy)



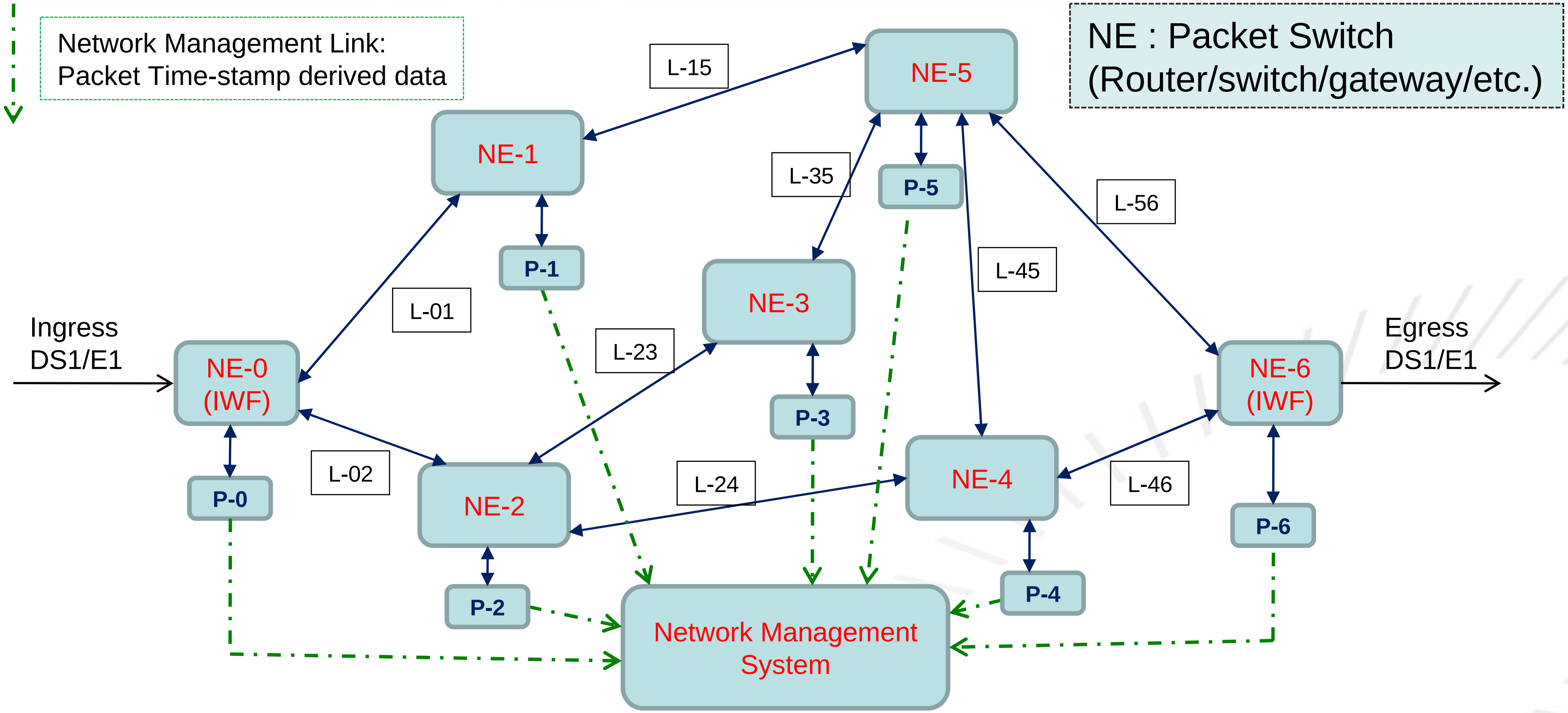
- End-point monitoring establishes SLA compliance for that particular private line circuit.
- Provides information related to other private line circuits that follow the same path.
- No guidance on problem source.
- Legacy monitoring does not include absolute delay (assumed to be within specifications).

Monitoring Options – 2 (Legacy)



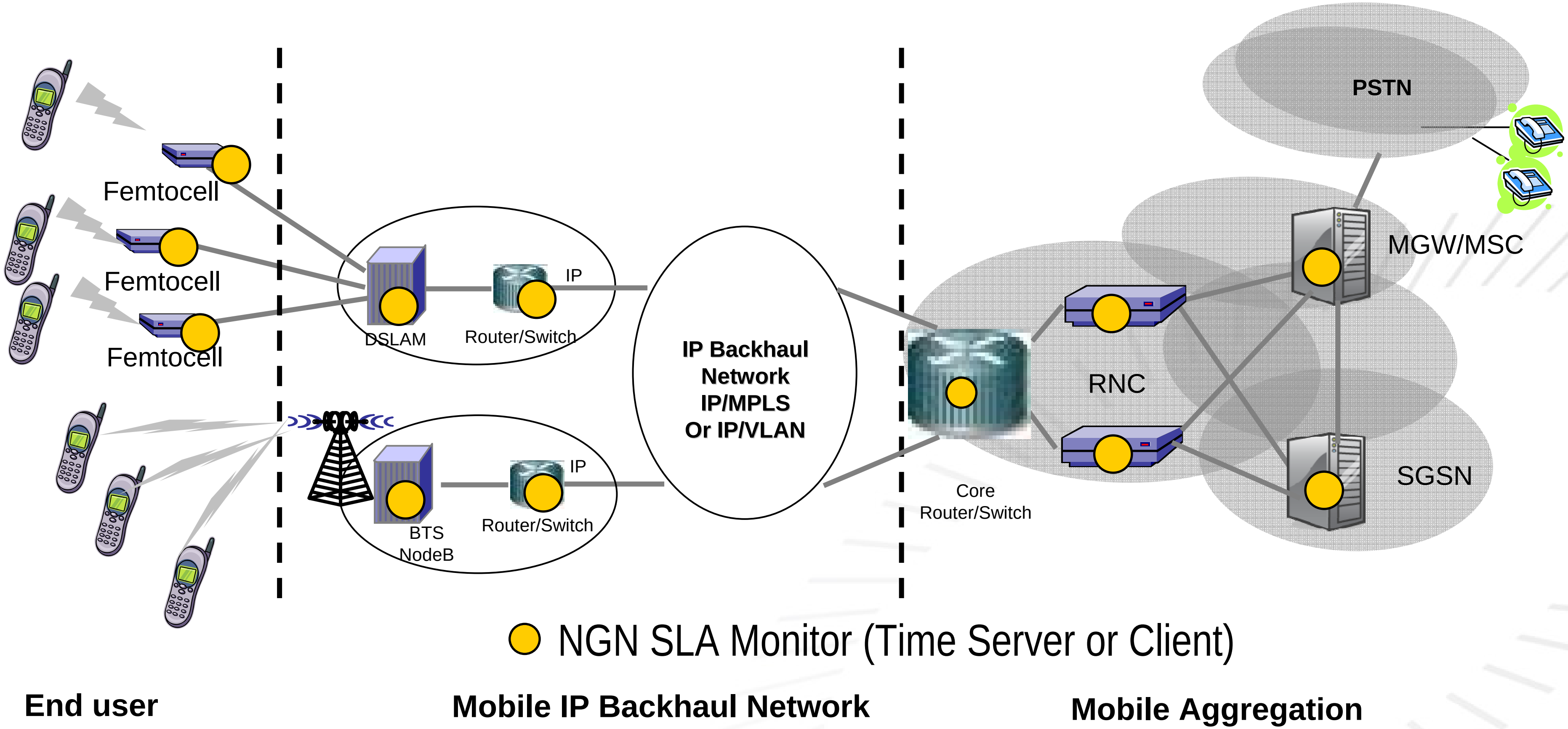
- Link monitoring provides information regarding all private line circuits carried over that link.
- NE status provides information related all private line circuits that traverse that NE.
- Problem links/NEs can be identified (and signals re-routed).
- Legacy monitoring does not include absolute delay (assumed to be within specifications).

Monitoring Options – 3 (NGN)

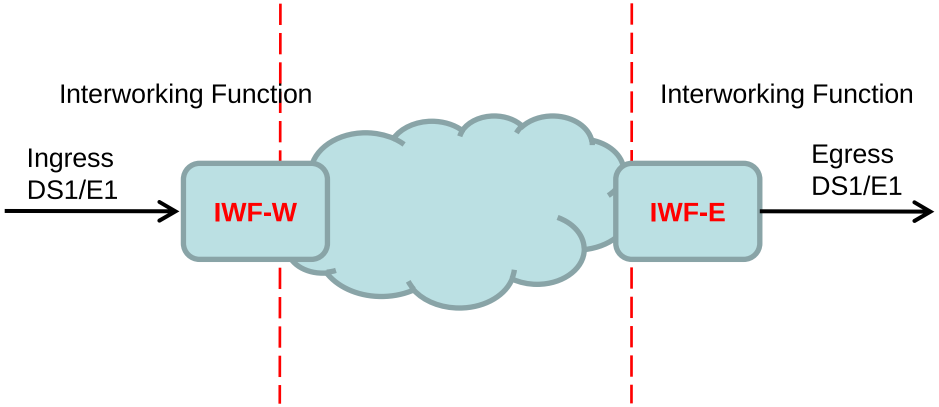


- Network can be logically partitioned into *segments*.
- Flow monitoring provides information regarding all packet flows between selected points.
- Problem links/NEs can be identified (and forwarding tables modified).
- Absolute delay and packet delay variation can be measured if time is tran

Carrier-Class IP Backhaul



IP Backhaul Network Objectives

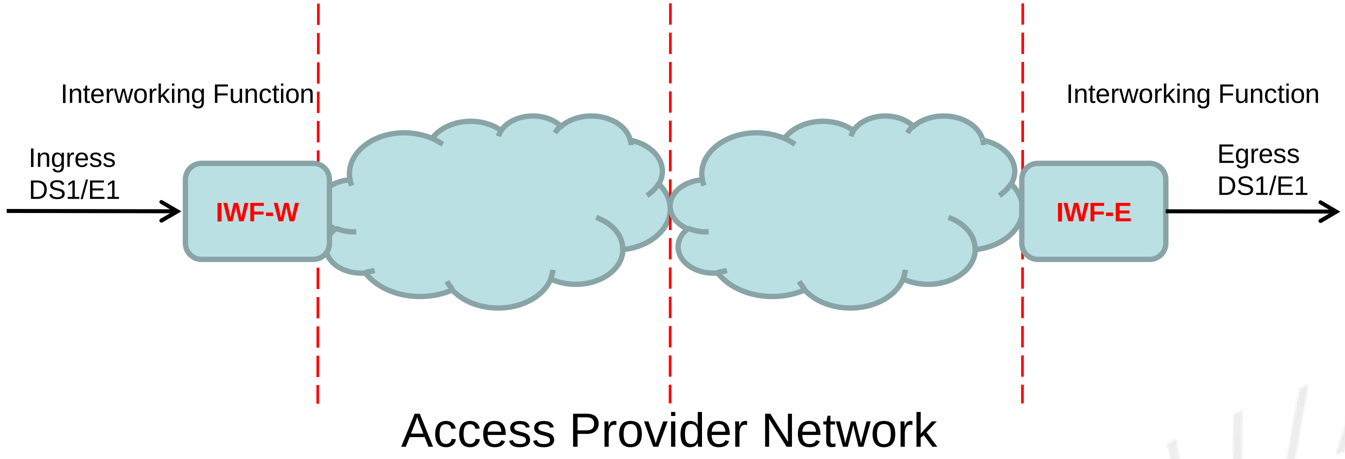


Access Provider Network

Key Performance Parameters	Network Objectives
One-way Frame Delay	< 8 ms
One-way Frame Delay Variation	< 2ms
Frame Loss Rate to support CES	5x10-7
Throughput	99.99%

Typical Wireless Service Provider Reqs for Delay, Jitter, Loss
One-Hop Network

IP Backhaul Network Objectives



Key Performance Parameters	Network Objectives (Per Hop)
One-way Frame Delay	< 4 ms
One-way Frame Delay Variation	< 1 ms
Frame Loss Rate to support CES	3x10-7
Throughput	99.99%

Typical Wireless Service Provider Reqs for Delay, Jitter, Loss Per-hop in Two-Hop network

Example Desired OAM&P Standards

brilliant

IEEE 802.3ah:

- **Link level diagnostics, management and monitoring**

IEEE 802.1ag/ITU Y.1731

- **Service level connectivity fault management**
  - **continuity check, intrusive and non-intrusive loopbacks);**
- **Service level performance management**
  - **Delay, delay variation, frame loss and availability).**

RFC4656:

- **One-way/Two-Way Active Measurement Protocol (OWAMP/TWAMP)**
- **One-way/Two-Way delay and loss**

RFC 2544:

- **Benchmarking Methods for Network Interconnect Devices**

Service Providers want fully integrated end-to-end solution

Active Monitoring

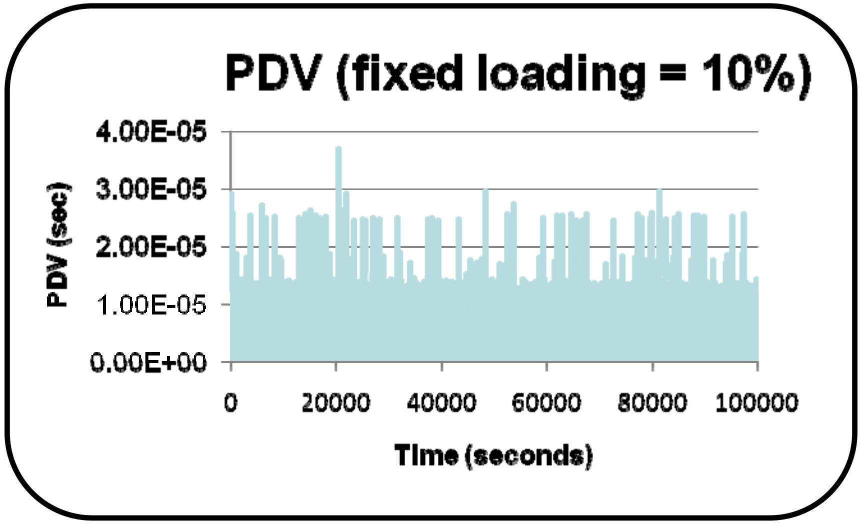
- Traditional clock-clients (e.g. NTP, PTP) can be adapted the basis for implementing active monitoring streams
  - Standard protocols and ***time-stamp aware***
- Client-server interaction provides all requisite information to establish transit delay (and derivative metrics) between the two entities
  - Multiple streams can address multiple QoS strata (streams can be segregated by class-of-service, VLAN, etc.)
- Fundamental requirements:
  - Need a “common” time reference independent of the measured flow.
  - Ability to monitor performance is directly related to accuracy of time-stamps and the stability of the measurement entities
  - Packets associated with this active measurement flow should not be misconstrued by other devices on the network.

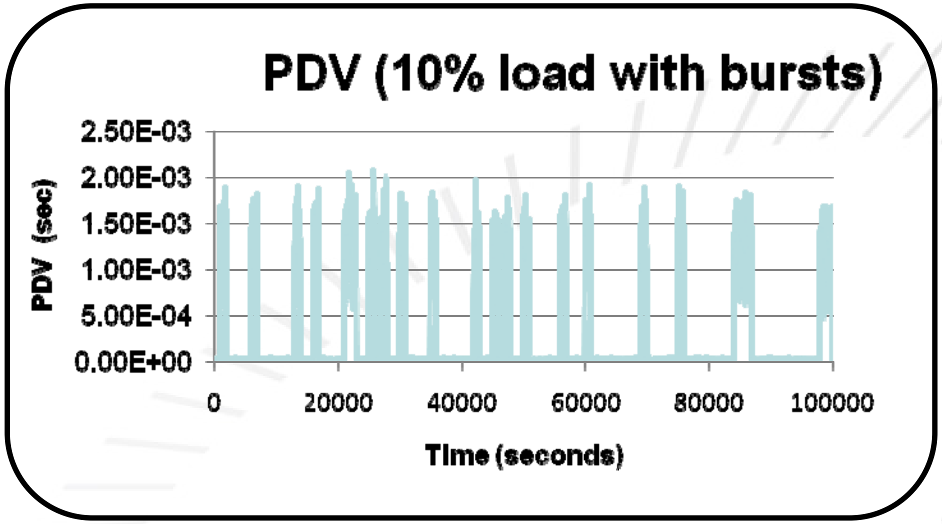
PDV Metrics

- Metrics that characterize PDV are computed from the sequence $\{x_k\}$:
  - Probability density function (pdf) or cumulative distribution function (cdf) or histogram. All provide the same information related to amplitude, including:
    - Minimum, x_{min} : largest value such that $x_k > x_{min}$ for all k.
    - Variance: $\sigma_x^2 = < x_k^2 > - < x_k >^2$ {< > is the average}
    - Maximum-95 , x_{max} : smallest value such that $P[x_k < x_{max}] > 0.95$
  - Spectral metrics (e.g. TDEV) address temporal distribution
    - Implied sampling interval = τ_0 (packet interval)
  - TDEV($\tau = n\tau_0$) = $\sqrt{\left(\frac{1}{6\cdot(N-3n-1)}\right)\cdot\left(\sum_{j=0}^{N-3n}\left(\frac{1}{n}\cdot\sum_{i=j}^{n+j-1}\left(x_{i+2n}-2x_{i+n}+x_i\right)\right)^2\right)}$

PDV Monitoring

- Case 1 : 10% load (fixed)
- Case 2 : 10% with bursts of 95%

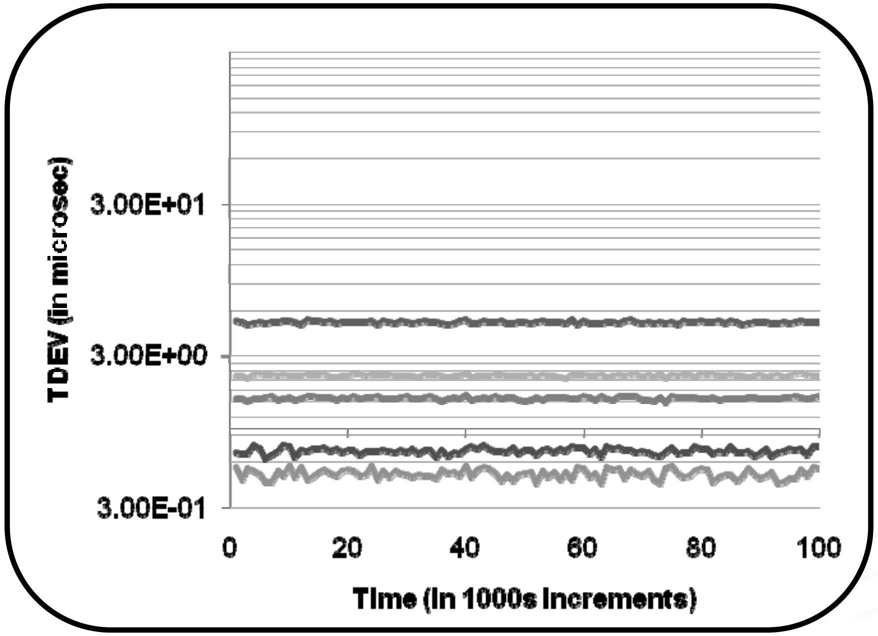




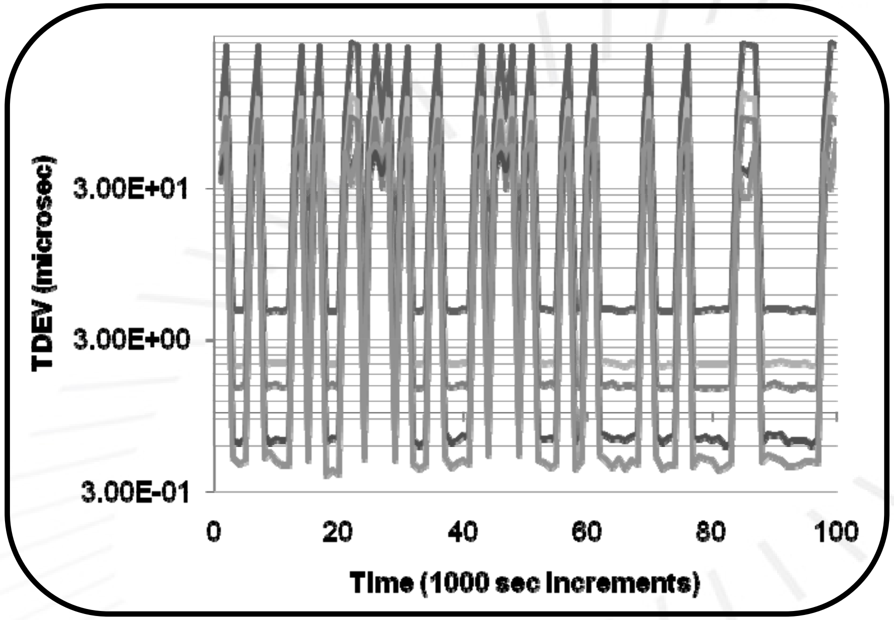
- Simulation methodology follows G.8261 guidelines
- Note difference in scale

TDEV Monitoring

- Short-term TDEV trajectory for the two cases
- Short-term TDEV identifies changes in load
- Historic records of TDEV can identify systemic changes in network loading

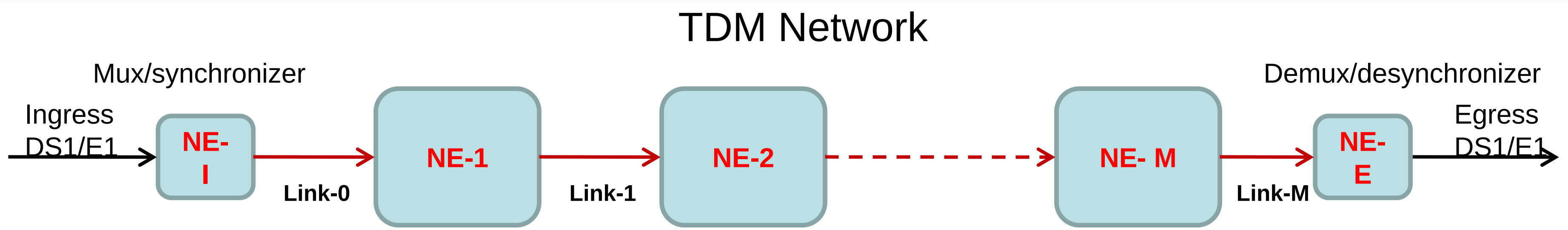


Fixed Load (10%)

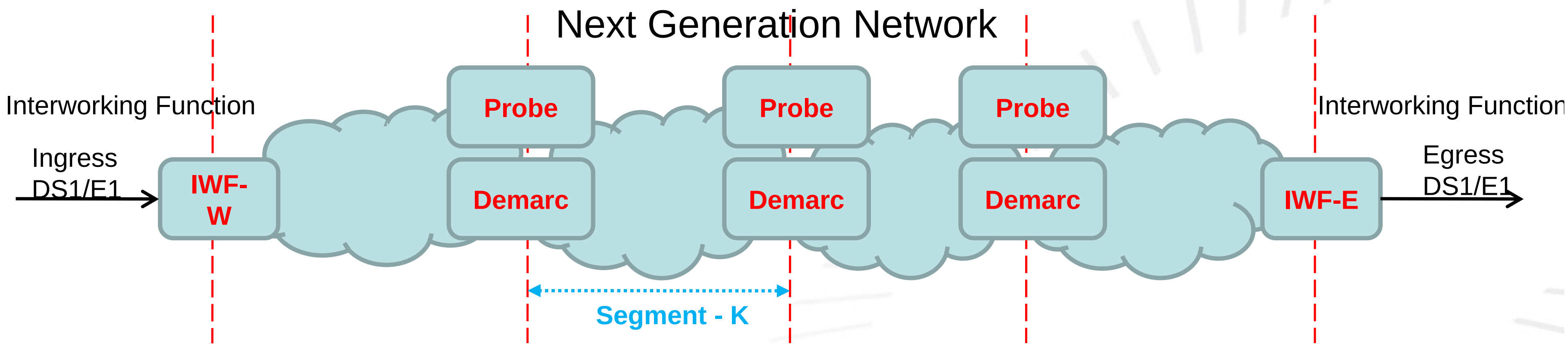


Variable load (10% + bursts)

E1/DS1 Private Line



- E1/DS1 Private Line circuit is built using a particular path of Links (e.g. STM-N/OC-N) and NEs
- SLA compliance guaranteed if path is "up" –
  no alarms; bit-errors within limits; pointer activity within limits



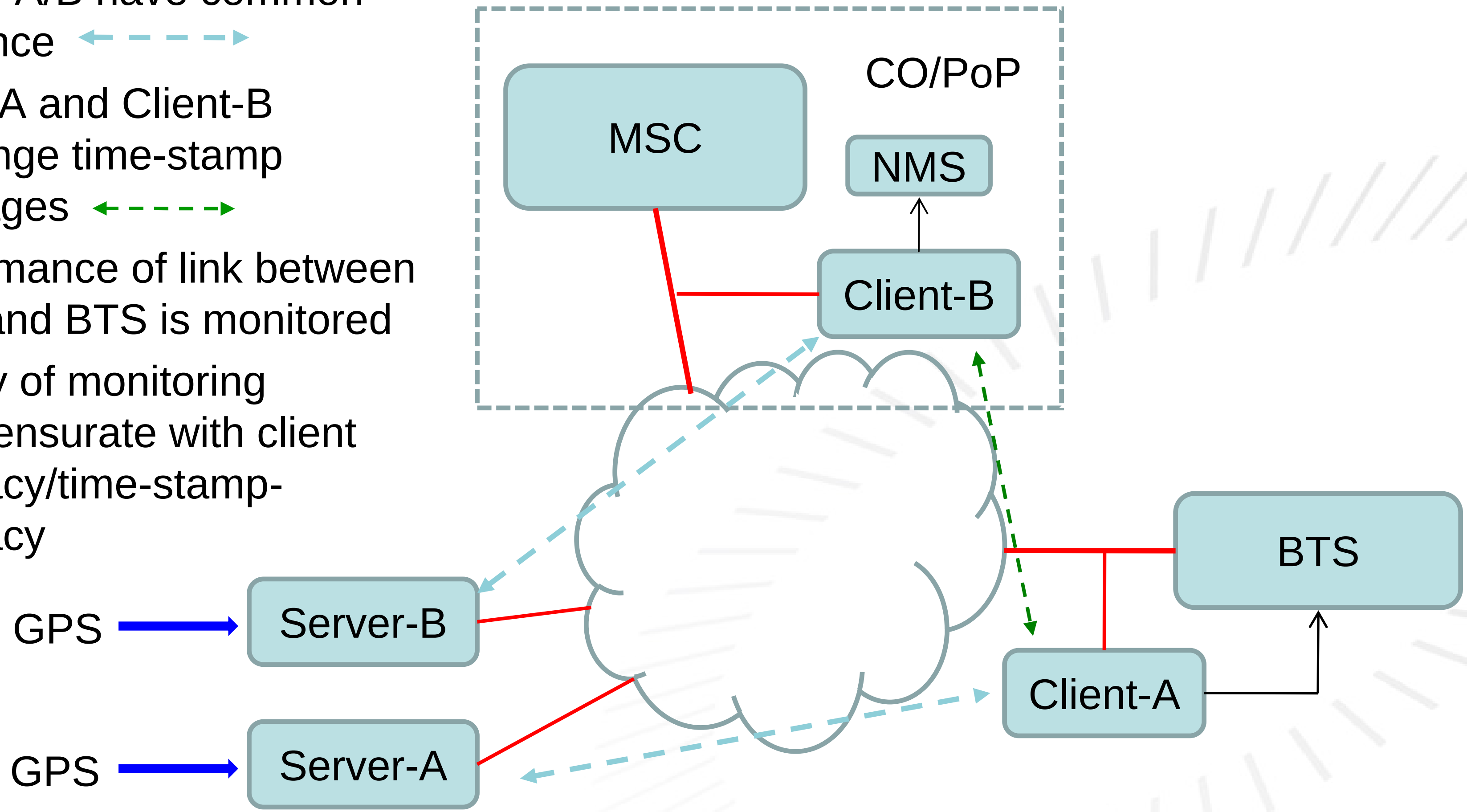
- E1/DS1 CES (Circuit-emulation-service) between IWFs can have multiple paths (quasi-static)
- SLA compliance requires each segment of the path meet requirements –
  continuity, acceptable packet-loss, acceptable delay, acceptable delay-variation

Principles of Segment Monitoring

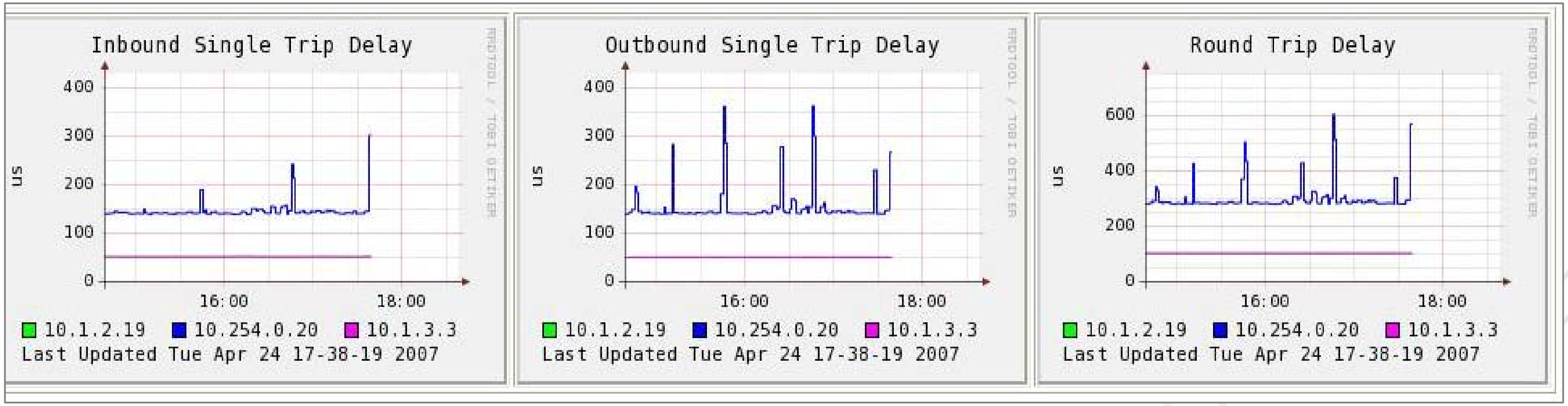
- End-to-end path constructed as concatenation of segments
- If δ_k is the transit delay across segment *k*, the end-to-end delay is $\Sigma\delta_k$
- Delay and delay variation in segment *k* affects all flows using segment *k*
- Segment monitoring to pinpoint network impairment, traffic overload, instabilities
  - Per hop (segment) delay and jitter requirements/alarms

SLA Monitoring Example

- Client-A/B derives time from Server-A/B (e.g. PTP, NTP); Server-A/B have common reference
- Client-A and Client-B exchange time-stamp messages
- Performance of link between MSC and BTS is monitored
- Quality of monitoring commensurate with client accuracy/time-stamp-accuracy



Real-Time SLA Monitor



- **Non-intrusive SLA measurement between end points over IP network**
  - Physical and Logical Segments and End-to-End
- **PDV/one-way delay and jitter with 10 microsecond accuracy**
- **Statistics per class of service, packet type and packet length with Threshold Crossing Alerts (TCA)**
- **Adjustable sampling rate as required by application**
- **Historical Views**
- **Integration with alarm management**

Concluding Remarks

- SLA (performance) monitoring in Next Generation Networks follows same principles as in legacy networks
- NGN SLA (performance) metrics include delay, delay variation, throughput and loss.
- Monitoring systems can utilize existing protocols (e.g. PTP, NTP) for time transfer, timestamps
- Monitoring using timing client/server communications – entities can assist multiple OAM&P functions
- Monitoring can be done on physical and virtual topologies and per class of service
- Monitoring efficacy depends upon with time-stamp accuracy and stability of the measuring entities