TEQUILA presentations/demonstrations

- **Overview of the TEQUILA System**
  - David Griffin, UCL

- **Demo 1: Traffic Engineering**
  - Panos Trimintzios, Paris Flegkas, UniS

- **Demo 2: Resource Provisioning Cycle, Network Configuration, Service Negotiation and Monitoring**
  - Steven Van den Berghe, IMEC
  - Takis Damilatis, Algonet
  - Charalampos Charalampous, NTUA

- **UK Testbed: Monitoring Results**
  - Richard Egan, Global Crossing
• Overview of the TEQUILA System
  – David Griffin, UCL
  – Panos Trimintzios, Paris Flegkas, UniS

• Demo 2: Resource Provisioning Cycle, Network Configuration, Service Negotiation and Monitoring
  – Steven Van den Berghe, IMEC
  – Takis Damilatis, Algonet
  – Charalampos Charalampous, NTUA

• UK Testbed: Monitoring Results
  – Richard Egan, Global Crossing
Service Level Specification
- topological scope
- QoS characteristics
  - schedule
  - etc.
- How to configure the network to accommodate all demands and...
- Meet SLS requirements...
- Meet operational objectives of provider
- How to configure the network to accommodate all demands and...
- Meet SLS requirements...
- Meet operational objectives of provider
- With a given physical infrastructure
Configure LSPs

Configure PHBs

Map addresses to LSPs

Configure Traffic Conditioning

… to allow SLSs to be realised
Resource Provisioning Cycle (RPC)
- background operational cycle to *pre-configure* network
- map traffic predictions to network configuration
- based on aggregate repository of subscribed SLSs and predictions for next cycle
- order of days/weeks/months
Dynamic Traffic Engineering
- tune network configuration according to monitored operational conditions
  - between RPC cycles
  - according to constraints set by network dimensioning
  - order of minutes/hours
SLS Subscription Epoch

- SLS negotiation with customer
- accepts/rejects SLS based on Resource Availability Matrix
- configures mapping to (pre-existing) LSPs
- does not require new RPC
Monitoring
Policy Management
SLS Management
SLS Invocation Epoch
- dynamic admission control based on network state
- configures traffic conditioning
Traffic Engineering
Data Plane
SLS Invocation Epoch
- dynamic admission control based on network state
- configures traffic conditioning
Demonstration

Traffic Engineering Algorithms

Simulation and Policy-based Extensions
• **Overview of the TEQUILA System**  
  – David Griffin, UCL

• **Demo 1: Traffic Engineering**  
  – Panos Trimintzios, Paris Flegkas, UniS

  Configuration, Service Negotiation and Monitoring
  – Steven Van den Berghe, IMEC
  – Takis Damilatis, Algonet
  – Charalampos Charalampous, NTUA

• **UK Testbed: Monitoring Results**  
  – Richard Egan, Global Crossing
TEQUILA presentations/demonstrations

• Overview of the TEQUILA System
  – David Griffin, UCL

• Demo 1: Traffic Engineering

• Demo 2: Resource Provisioning Cycle, Network Configuration, Service Negotiation and Monitoring
  – Steven Van den Berghe, IMEC
  – Takis Damilatis, Algonet
  – Charalampos Charalampous, NTUA
  – Richard Egan, Global Crossing
• Overview of the TEQUILA System
  – David Griffin, UCL

• Demo 1: Traffic Engineering
  – Panos Trimintzios, Paris Flegkas, UniS

• Demo 2: Resource Provisioning Cycle, Network Configuration, Service Negotiation and Monitoring
  – Steven Van den Berghe, IMEC
  – Takis Damilatis, Algonet

• UK Testbed: Monitoring Results
  – Richard Egan, Global Crossing
UK Testbed: Monitoring

Steven Van den Berghe

Richard Egan
Hamid Asgari
Mark Irons

Global Crossing™
Presentation Outline

• Monitoring Architecture & Design
• Monitoring Scalability
• Overview of UK Testbed
• Results of Monitoring Tests
• Conclusions
Network Monitoring

• **Purpose:**
  – to provide in-service verification of customer services
  – to assist Dynamic TE (MPLS & IP) to adapt to congestion / under-utilisation

• **Two primary components**
  – **Node Monitor**
    • contains the distributed active/passive measurement agents
  – **Network Monitor**
    • centralised component builds a physical & logical network view

• **Relevant Metrics**
  – **Active** - OneWayDelay, OneWayLoss
  – **Passive** - PHB BW Usage, PHB Packet Discard, Throughput
Monitoring Architecture

Monitoring GUI

Monitoring Repository

SLS Monitor

Network Monitor

Node Monitor

Node Monitor

Node Monitor

Node Monitor

PMA Passive Monitoring Agent
AMA Active Monitoring Agent

I/E

C

C

I/E

Premium IP - Cluster Meeting & Review, 15 May, 2002,
Maastricht, The Netherlands
Creating an Active Monitor

- Node Monitor
- Active Monitoring Agent
- Synthetic Source
- Monitor Holder
- Synthetic Reporter

Connections:
- Reg -> Node Monitor
- Create -> Active Monitoring Agent
- Get Port -> Result -> Monitor Holder
- Result -> Synthetic Reporter
- R <-> R
Scalability

- SLS Monitor uses Network Aggregate Measurements
  - Per LSP monitoring is more scalable than per SLS
  - Combine with per-SLS Ingress/Egress measurements
    - throughput / offered load

- Use Hop by Hop Measurements
  - Reduce volume of synthetic traffic
  - Aggregate hop measurements to get E2E measurement

AM: Active Measurement
PM: Passive Measurement
<table>
<thead>
<tr>
<th>Node</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>TEQ. 0011</td>
</tr>
<tr>
<td>194.166.11.33</td>
<td></td>
</tr>
<tr>
<td>195.166.11.45</td>
<td></td>
</tr>
<tr>
<td>194.166.11.125</td>
<td></td>
</tr>
<tr>
<td>L2.128/30</td>
<td></td>
</tr>
<tr>
<td>3/0:0</td>
<td></td>
</tr>
<tr>
<td>4/0</td>
<td></td>
</tr>
<tr>
<td>1/0</td>
<td></td>
</tr>
<tr>
<td>PE1</td>
<td>SX/12 (1)</td>
</tr>
<tr>
<td>PE2</td>
<td>SX/12 (2)</td>
</tr>
</tbody>
</table>

**Node Descriptions**
- **P1**: TEQ. 0011
- **PE1**: SX/12 (1)
- **PE2**: SX/12 (2)
- **PE3**: SX/12 (1)
- **PE4**: SX/12 (2)

**Networks**
- 194.166.11.33
- 195.166.11.45
- 194.166.11.125

**Links**
- E1 Link
- X.21 Serial Link
- Fast Ethernet/Ethernet
- G703-X.21 Converter
Synchronisation

- Achieves client synchronisation accuracy of < 1ms
Accuracy Test Set-up

- **Objective**
  - verify accuracy of active delay and loss measurements
- **Method**
  - compare Node Monitor result with SmartBits result (delay)
  - compare Node Monitor result with SX/12 (loss)
One Way Packet Loss

Accuracy Test for Edge-to-Edge One-Way Packet Loss (5 minutes intervals)

Time of Day

02-May-07-16:48:00.000 02-May-07-19:12:00.000 02-May-07-21:36:00.000 02-May-08-00:00:00.000 02-May-08-02:24:00.000 02-May-08-04:48:00.000 02-May-08-07:12:00.000 02-May-08-09:36:00.000

% Packet loss

0.0 1.0 2.0 3.0 4.0 5.0 6.0 7.0 8.0 9.0 10.0

% Packet Loss Measured: 3.28%
Mean Loss Measured: 3.10%
Mean Loss Introduced: 3.10%

Premium IP - Cluster Meeting & Review, 15 May, 2002,
Maastricht, The Netherlands
Test Set-up

- **Objective**
  - Compare accuracy of edge2edge with hop by hop measurement

- **Method**
  - compare Node Monitor result with SX/12 (delay & loss)

\[
EE_{OWD} = \sum_{i=1}^{n} d_i \\
EE_{OWL} = (1 - \prod_{i=1}^{n} (1 - p_i))
\]
One Way Delay

**Hop-by-Hop & Edge2Edge One Way Delay (Test Pkt Length: 128)**

- **Hop 1 (SX12: 3 ms)**
- **Hop 2**
- **Hop 3 (SX12: 7 ms)**
- **Edge-to-Edge**
- **Hop-by-Hop**

![Graph showing One Way Delay](image-url)
One Way Packet Loss (EMA)

Hop-By-Hop & Edge-to-Edge Packet Loss

% Packet loss

Time of day

2002-05-08 14:24:00.000 2002-05-08 16:48:00.000 2002-05-08 19:12:00.000 2002-05-08 21:36:00.000 2002-05-09 00:00:00.000 2002-05-09 02:24:00.000 2002-05-09 04:48:00.000 2002-05-09 07:12:00.000 2002-05-09 09:36:00.000
Scalability

Edge-to-edge Synthetic Traffic Injection vs Hop-by-hop
(4 PPS injected for each LSP/Hop - Supported PHBs per interface <=8 )

Packet Per Second (PPS)

Number of LSPs crossing the link/Hop per interface

- PPS for LSPs crossing a link
- PPS for Hops crossing a link
Conclusions

• Good accuracy for both OWD and OWL
  – even with agents outside the routers
  – comparable E2E and hop by hop results
• Scalability claims for hop by hop are justified
• OWD results suitable for dynamic operation & SLS Monitoring
• OWL results suitable for SLS Monitoring
  – use passive monitoring of packet discards for dynamic mgt
• Need for accurate synchronisation of agents
  – higher cost for hop by hop approach
Enforcing an IP TE policy

Christian JACQUENET
christian.jacquenet@rd.francetelecom.com
Enforcing an IP TE policy

• Outline:
  – Configuration and testing environment
  – Enforcing an IP TE policy: an example
    • PRC instantiation
    • COPS-PR provisioning of the configuration information
    • Reporting the actions
    • Validation aspects
  – Current restrictions
  – Preliminary performance results
Configuration and testing environment

• Basic components:
  – An XML-based “OSS”
    • For populating the IP TE PIB, based on the manipulation of XML files
  – A PDP for making the decisions
    • E.g. modify a TE metric value on a given router interface
  – PEPs for applying the decisions
    • The PEP capability is currently outsourced from the routers
  – OSPF-TE-capable routers
    • Embed a CSPF computation algorithm
Development and testing resources

12 Linux-based routers (with TE extensions)

PIB

PDP

COPS-PR

CLI syntax

Proxy PEP
Access interfaces
• According to the IP TE PIB structure
  
  – *E.g.* modification of the `ospfTeMetricSubTlvMaxRsvBandwidth` value
COPS-PR provisioning of the configuration information

- By sending (unsolicited) DEC messages:
Reporting the actions

- By sending RPT messages towards the PDP:

Allows to check the (updated) configuration
Validation aspects

• Checking the router’s configuration:

“Show run” command result
Current restrictions

• Syntax correctness is not checked by the current PIB parser
  – Some syntax errors have been detected

• The PEP capability is external
  – Native PEP support available in June
Preliminary performance results

• On the benefits of the COPS-PR approach:
  – Manual configuration of the 12-router platform takes about 1 hour
  – COPS-PR configuration procedure takes less than 5 minutes

• On the support of the TE extensions to OSPF:
  – Negligible impact on the switching performances of the routers
    • Less than 5% on PC-based routers