



A Monitoring and Measurement Architecture for Traffic Engineered IP Networks

A. (Hamid) Asgari, S. Van den Berghe, C. Jacquenet, P. Trimintzios, R. Egan, D. Goderis, L. Georgiadis, E. Mykoniati, P. Georgatsos, and D. Griffin

Presented by:

Hamid Asgari

**THALES Research Limited, Worton Drive, Reading RG2 0SB, UK.
Email: Hamid.Asgari@uk.thalesgroup.com.**



- Introduction
- TEQULA System Architecture
- Monitoring Requirements for TE Networks
- Scalability of Monitoring Architecture
- Monitoring & Measurement Architecture
- Conclusion



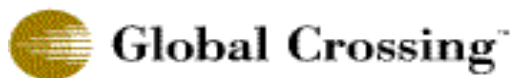
Introduction

- TEQUILA Consortium
- Traffic Engineering
- Differentiated Services
- Service Level Specifications

Traffic Engineering for QQuality of service in the Internet, at Large scale

TEQUILA Consortium

Industrial Partners



Universities



NTUA



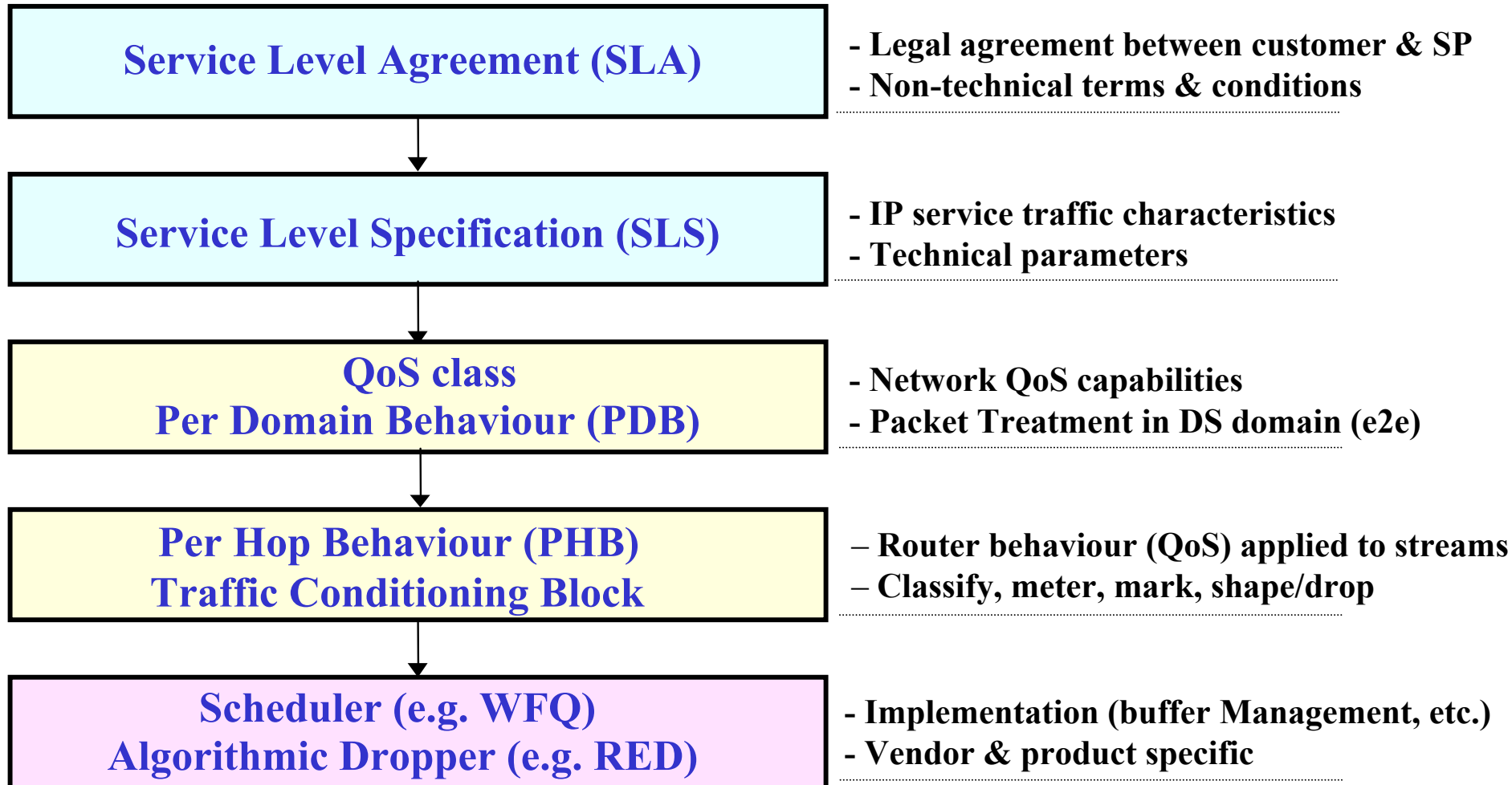
UniS

Research Institutes

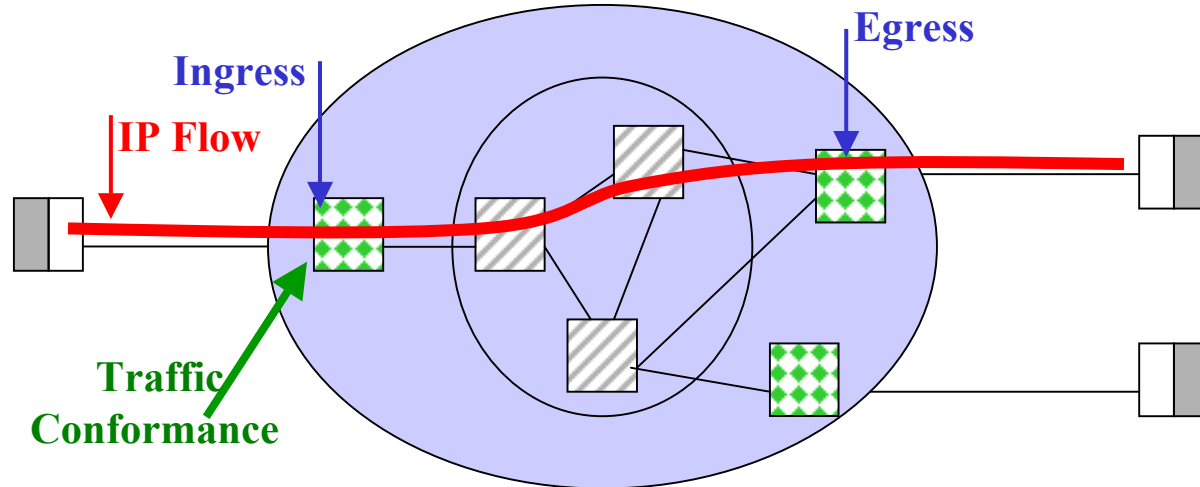


- TE is described as:
 - A collection of techniques allowing SPs to use network resources efficiently, according to the different quality levels associated with services they offer.
- TE is aimed at:
 - Accommodating as many customer requests as possible,
 - Satisfying the customer demands QoS requirements.
- TE is achieved through:
 - Capacity management by optimising the use of network resources,
 - Routing management by calculating, selecting, and installing of a set of routes and queue management parameters, throughout the network.
- TE Techniques used:
 - MPLS: By setting up explicit LSPs - LSPs are not explicitly associated with BW
 - IP-based: By setting up QoS-enabled IP routes - Hop-by-hop routing, OSPF-based, link-weights Assignment, BW reservations in the network per PHB.

From PHB to value-added IP services: a layered service model for DiffServ



- A set of technical parameters and their values, defining the service, offered to a traffic stream by a DiffServ domain.
 - **Traffic Conformance:** Set of actions to identify in/out of profile packets e.g., token bucket.
 - **IP Flow:** Stream of IP packets sharing at least one common characteristic - Source, destination, DSCP, application information.
 - **Scope:** Geographical limits over which the SLS is to be enforced - Ingress, Egresses
 - **Performance Guarantee:** delay, jitter, loss, throughput. Excess : drop | shape | re-mark

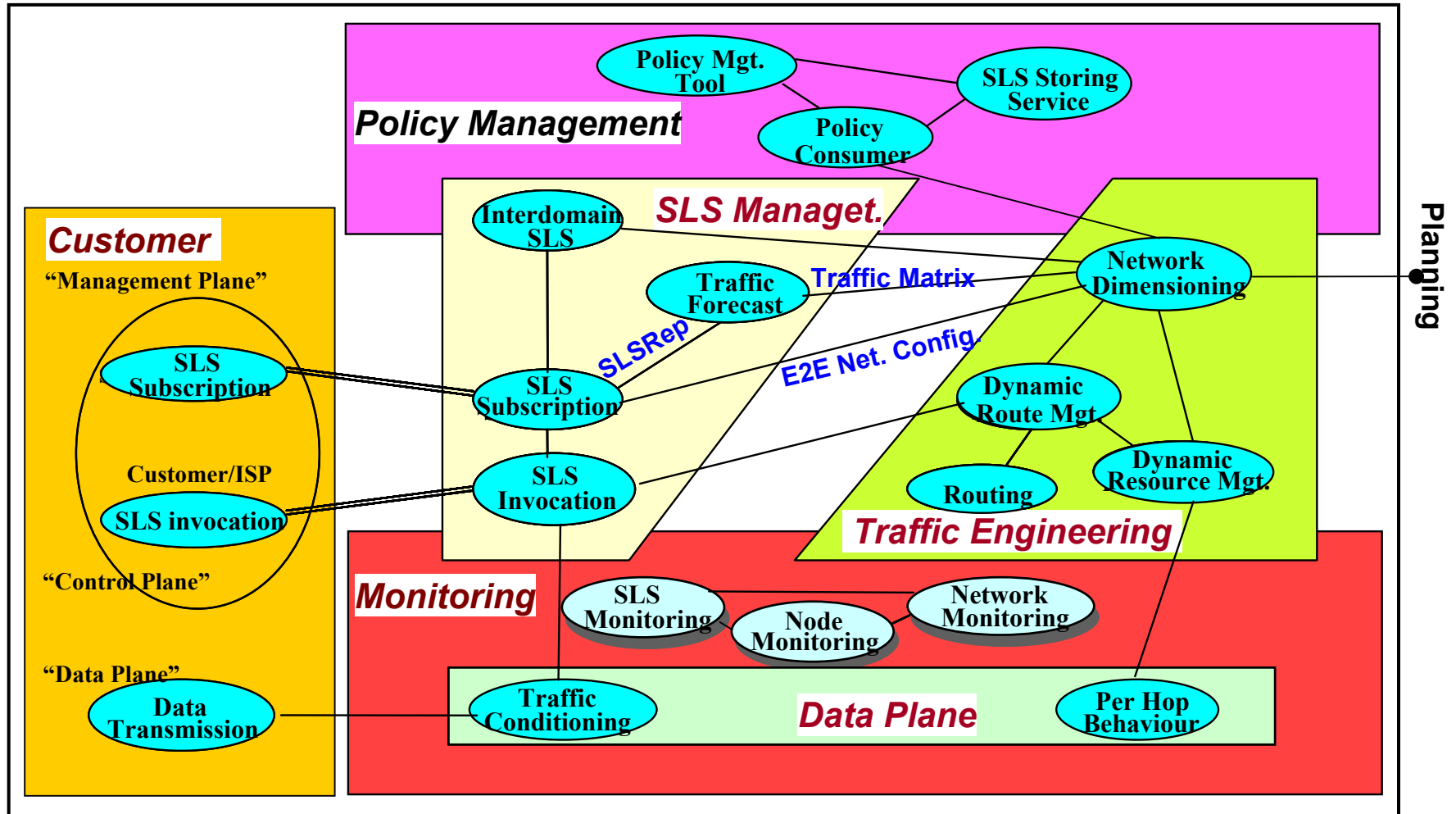




TEQUILA System Architecture

As A Traffic Engineered IP Management System

TEQUILA's objective is to specify, develop, and validate a system capable of dynamically negotiate, invoke, and provision the resources associated to the deployment of QoS based IP service offerings over the Internet. TEQUILA system provides service guarantees through planning, dimensioning and dynamic control of traffic management techniques based upon the DiffServ architecture in a flexible policy-driven manner.



Planning



Monitoring Requirements for Traffic-Engineered Networks and Services

- Why to Monitor/Measure?
- Assist Traffic Engineering & Perform Service Auditing

Functionality: *diagnostic* monitoring

- Basic monitoring functionality available for decades
- Data are used for management purposes (e.g. for failure detection, passive analysis, etc.)
 - *Ping*: Link/node failure, calculates RTD and loss
 - *SNMP/MIBs*: adds counters etc. to NEs to passively monitor link traffic

Functionality: *operational* measurement

- One step beyond: Monitoring results are used by management entities for their proactive action or automated reaction.
 - Policy based monitoring: if <event> then <action>

Assist Traffic Engineering:

- in efficient allocation of resources (e.g., to queues & paths),
- in proactive/reactive control of the network (e.g., traffic forecasting & dimensioning).

Perform Service Monitoring: Does the network provide the requested service?

- QoS enabled networks (DS) attempts to offer several service types.
- Monitoring is becoming important for providing e2e QoS and service assurance for multiple classes.
- A single measurement is not adequate for explaining traffic belonging to different services.
- As a result, network needs to be monitored in finer granularity (per service types).

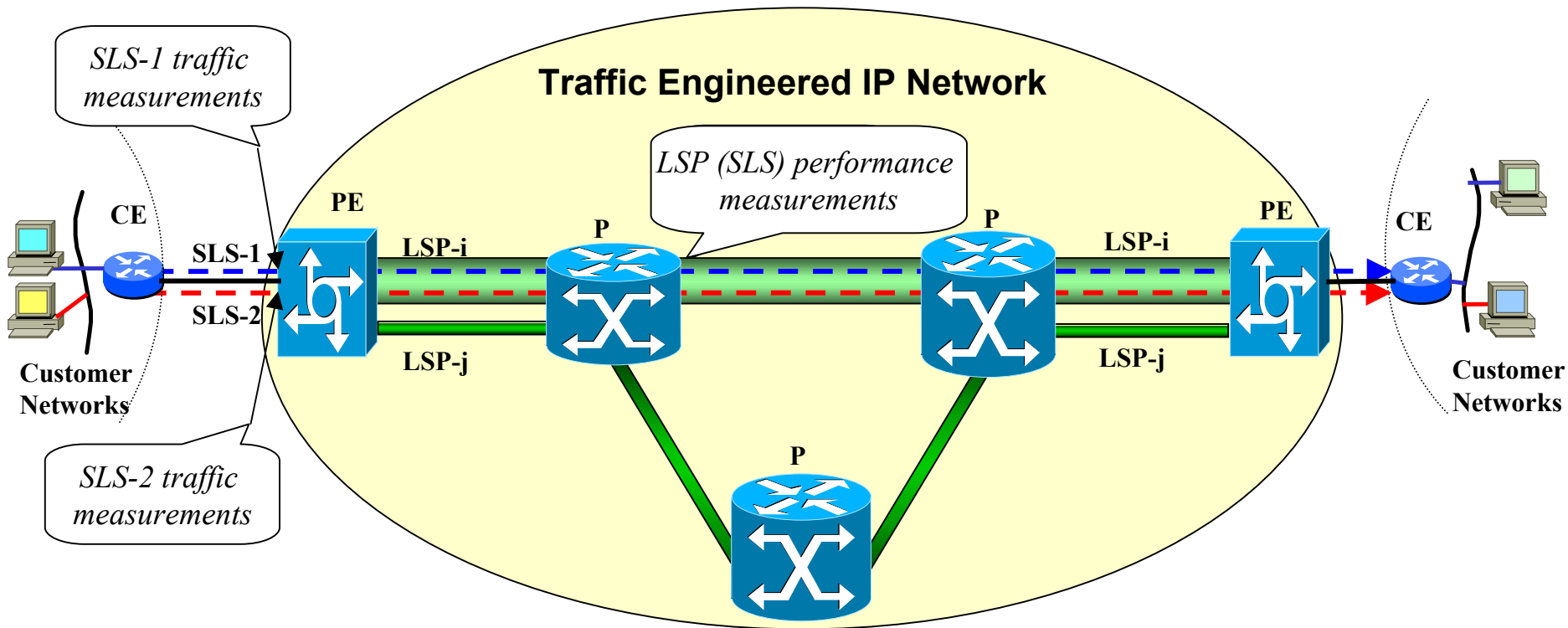


Scalability of the Monitoring Architecture

The architecture must scale with the size & speed of the network as it evolves.

- Defining the monitoring process granularity
 - LSPs/IP routes are used for the routing of QoS-enabled traffic flows.
 - Measurement methodology functions at the level LSPs/PHBs.
- Minimising the measurement transmission overhead by processing the raw data close to the source
 - Data capturing must be performed without degrading network performance and without generating a large amount of data.
 - Processing the raw data efficiently close to its source, which necessitate a distributed data collection system.
 - Condensing the collected data at the source by using event notification and statistics summarisation.

- Using aggregate performance measurements combined with per SLS traffic measurements
 - Monitoring every customer SLS is scalable and feasible if:

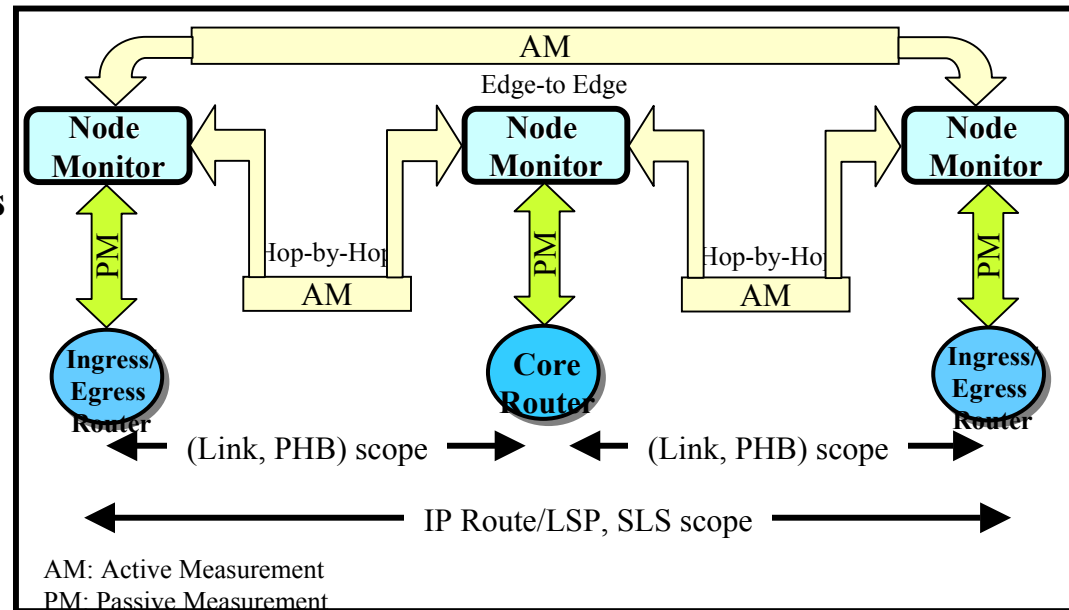


- Controlling the amount of active test traffic injection into network

Test Traffic Requirements:

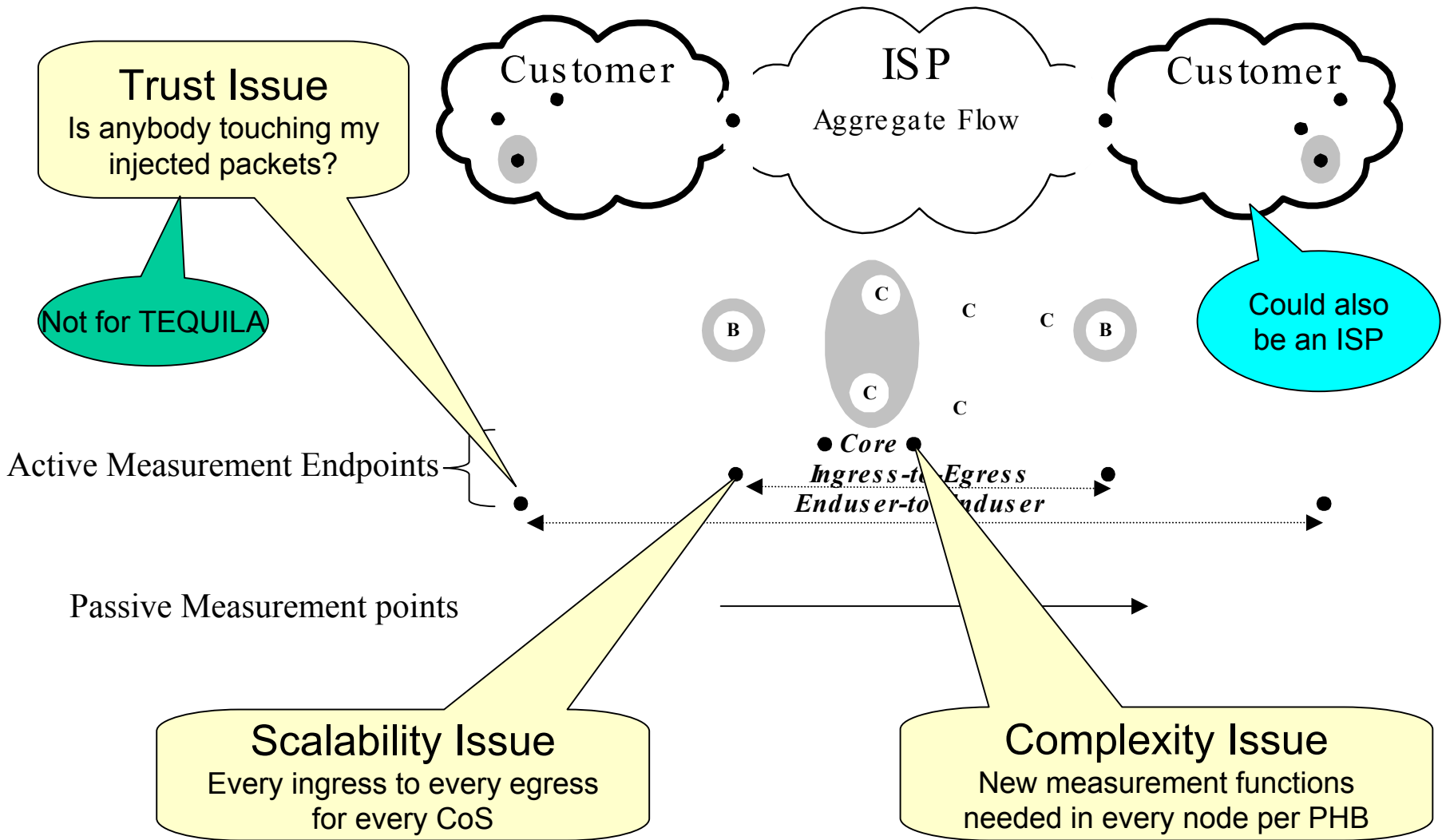
- Test traffic load should be small compared to the network load.
- Sampling intervals should be small enough to study fluctuations in the performance of the network.
- A trade-off between these two requirements needs to be made.
- The amount and type of test traffic should be configured.
- Test packets should be randomly distributed to prevent event synchronisation.

- *Edge-to-edge vs Hop-by-hop active measurements*
 - Measurements are performed between either two edge or two neighbouring nodes.
- *Edge-to-edge:*
 - Might not scale well if there are a huge number of LSPs
- *Hop-by-hop:*
 - Scale well by adding the hop-by-hop results and calculating e2e results
 - Significant reduction of test traffic in the network
 - Introducing inaccuracy due to:
 - non-synchronised individual hop-by-hop measurements
 - concatenating discrete values to estimate per-route e2e results
 - Appropriate for estimating the route performance of low profile services (BE)



Monitoring & Measurement Architecture (in TEQUILA)

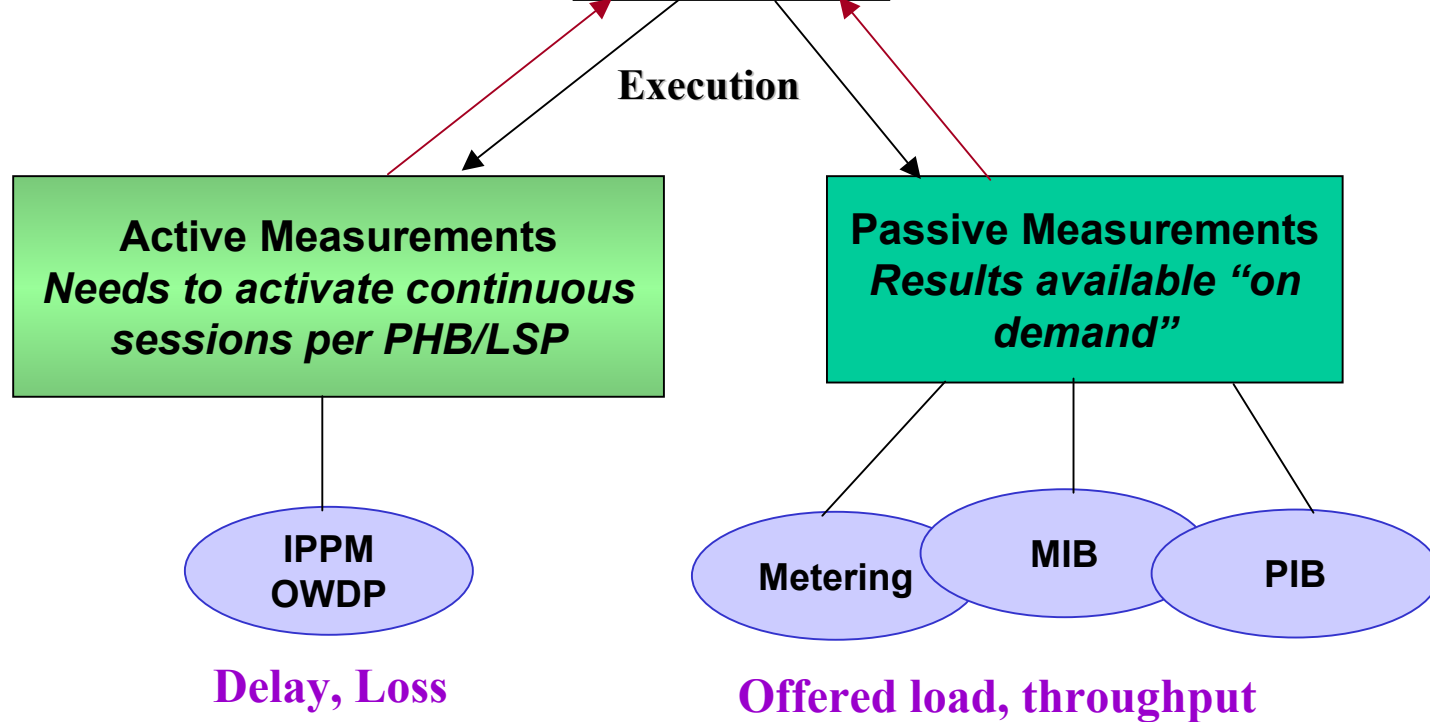
- Where to Monitor/Measure?
- How to Organize Measurements?
- Monitoring & Measurement Architecture
- Measurement Feedback
- Engineering Challenge



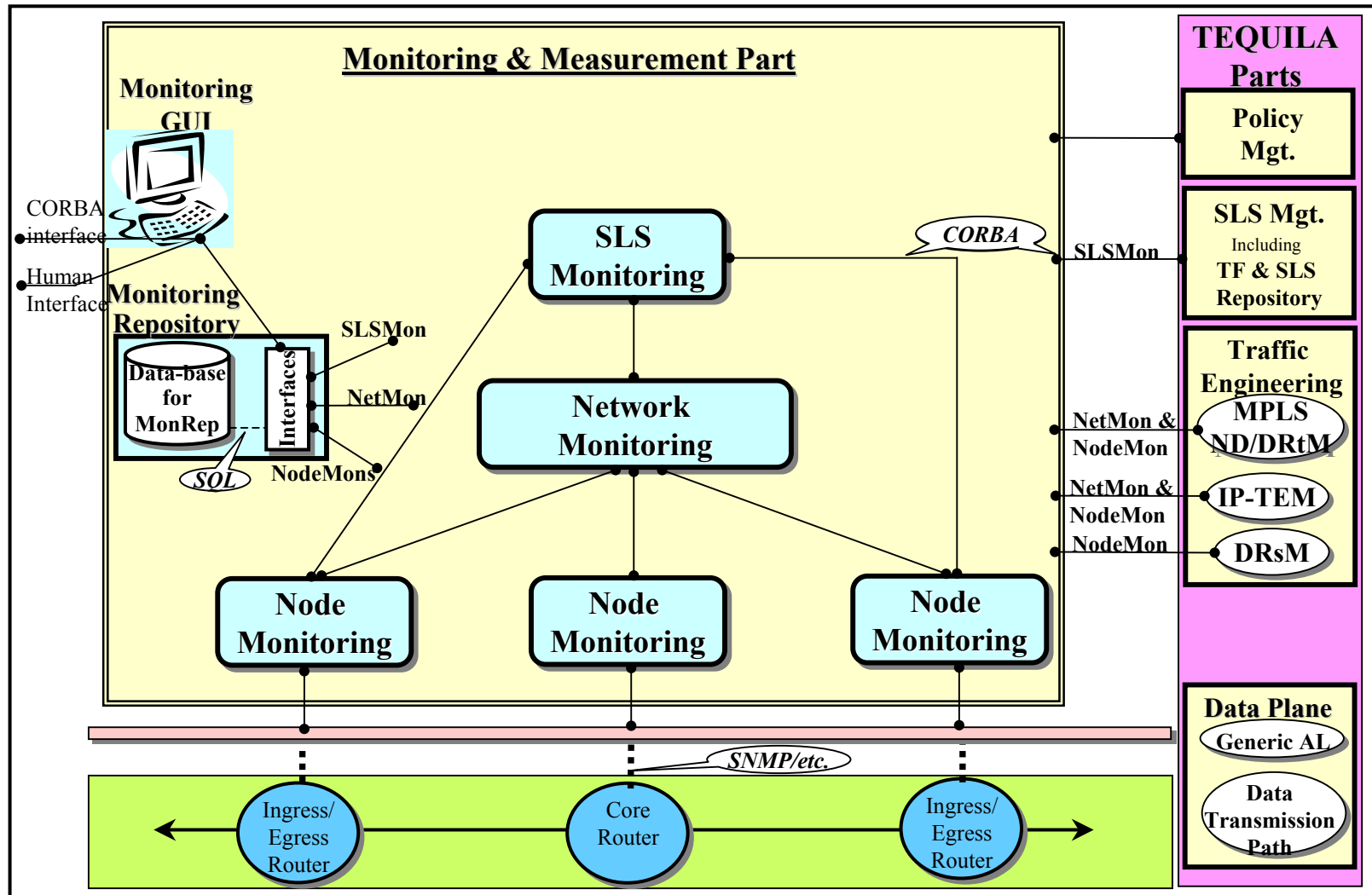
Organise



Methods

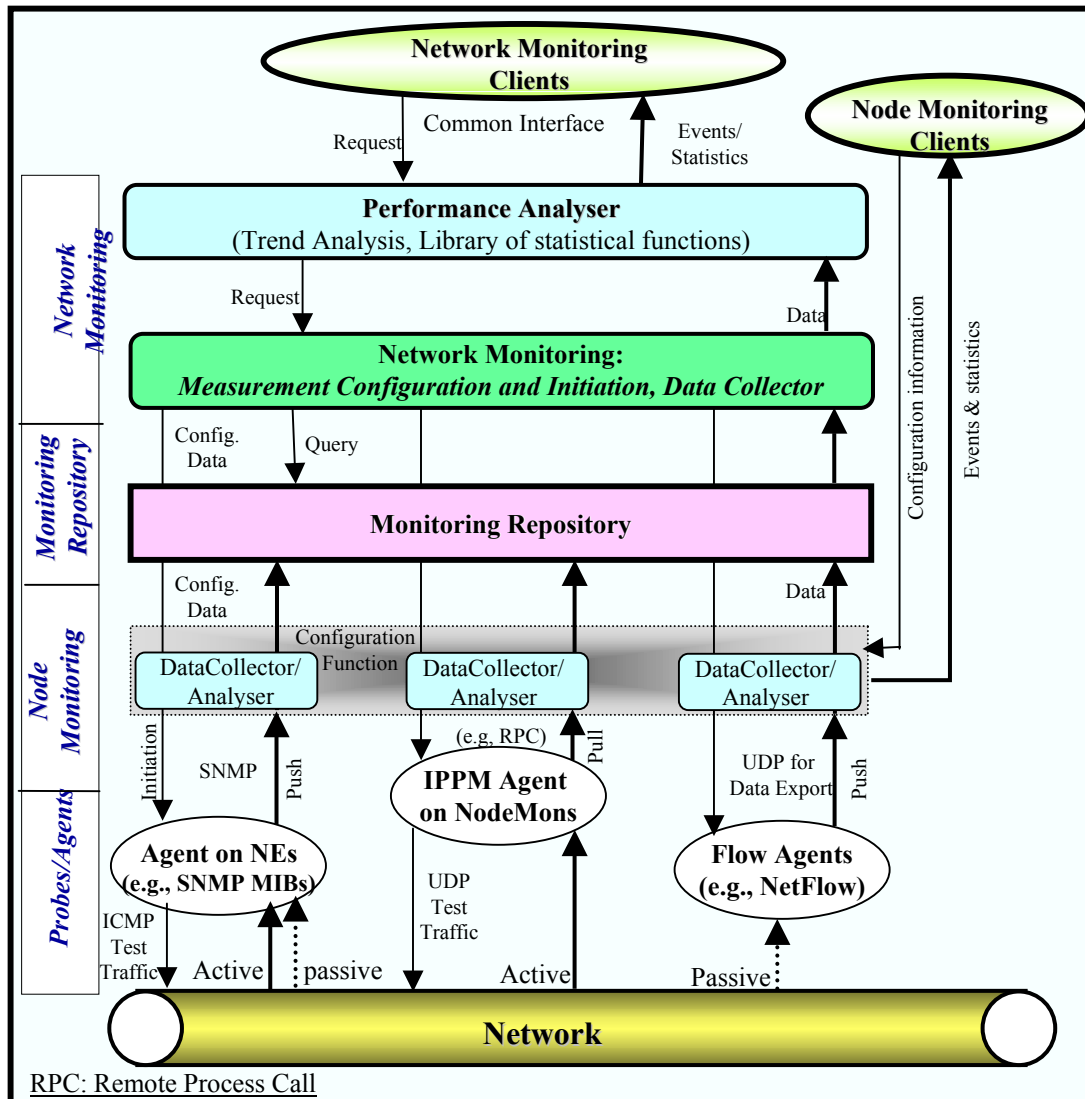


Network Layer Measurements

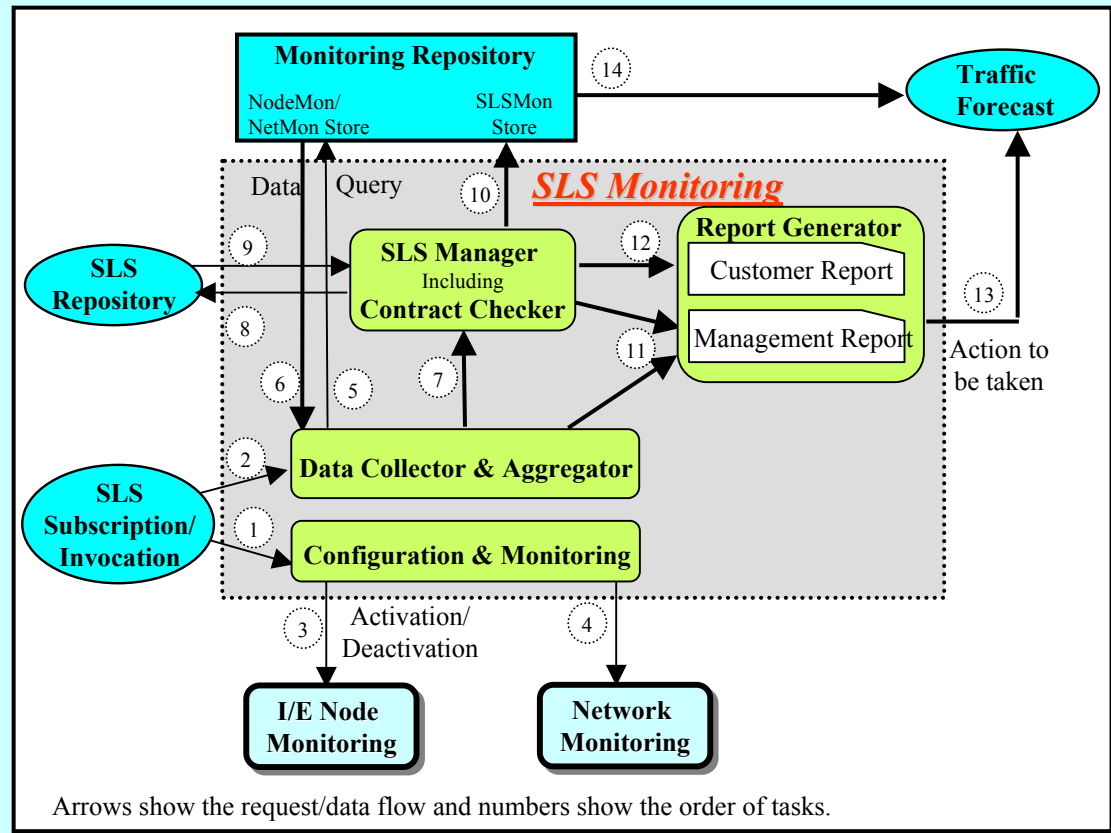


- Distributed component located on nodes
- Performs and organizes performance measurements
 - *Active*: with its neighbouring or ingress-egress nodes
- Performs and organizes traffic measurements
 - *Passive*: at the ingress/egress for end-to-end traffic measurements
 - *Passive*: on the node it resides
- Performs some basic functions
 - Events on thresholds
 - Apply statistical functions

- Centralized
- Gets notification if ND activates new state
- Configures node monitors
- Processes the measurements gathered by node monitors for links, nodes, PHBs, and routes
- Builds up a physical and logical network view
- Performs longer term, more complex traffic analysis



- Centralized
- Configures edge NodeMons for traffic related measurements
- Processes traffic related measurements gathered by edge NodeMons for SLSs
- Processes end-to-end performance for SLSs
- Service monitoring and auditing
- Reporting to customer and Management





Metrics	Measurement Mechanism & Method (Active/Passive)	Events and Measurement Statistics for:				
		SLS Monitoring (SLS Types & Services)			SLS Mgt.	Traffic Engineering (ND, DRtM & DRsM)
		Real-time Services	Guarantee data Services	Olympic Services (Best-effort)		
<ul style="list-style-type: none"> Performance 		Per Route	Per Route	Per Route	Per Route	Per PHB & Route
One-way delay	IPPM (A)	▶	-	-	▶	▶
Jitter (end-to-end)	IPPM (A)	-	-	▼		
One-way packet loss	IPPM (A)	▶	▶	-	▶	▶
<ul style="list-style-type: none"> User Traffic Flow 		Per SLS	Per SLS	Per SLS	Per SLS	Per macro-flow
Throughput per SLS/flows at egress	Flow-based (P)	▶	▶	▶	▶	▶
Offered load per SLS/flows at ingress	Flow-based (P)	-	-	-	-	▶
<ul style="list-style-type: none"> Network's Workload 					Per LSP	Per PHB & LSP
Throughput per PHB per link	COPS-PIB/metering (P)					▶
Throughput per LSP	Flow-based (P)				▶	▶
Packet Discards per PHB per link	COPS-PIB/SNMP MIB (P)					▶
Link utilisation In/Out	SNMP MIB (P)					(Per Link) -
<ul style="list-style-type: none"> Availability Metrics 						
Link & device availability	ICMP (A)					▶

- Commercial (Cisco) & PC-based (Linux) routers in the testbeds
- Limited availability of required PM in commercial routers
- Estimating PHB-based delay by using hop-by-hop AM
- Finding the proper sampling intervals for test traffic injection, PM polling, Stats summarisation
- Monitoring the aggregated flow level of SLSs for use in load balancing
- Finding the address blocks of active/non-active flows for traffic flow re-mapping
- and so on.

Conclusion

- Summary and On-going work

Challenge:

- Dynamic engineering of the network, since the ND and routing management have significant implications on resource efficiency and user performance.
- Customer service level management

Proposed:

- An architecture for node, traffic-engineered network, and service monitoring.
- Methodologies for event monitoring and measurement statistics to be used for both network operation and in-service verification of offered services.

On-going work:

- TEQUILA system implementation for performance assessment tests
- Examining the practical effectiveness of monitoring on TE algorithms and TF.
- Investigating the monitoring architecture scalability in real-time data processing.



Thank you

For more information visit TEQUILA web site at:

“<http://www.ist-tequila.org/>”