



Practical Network Management in Ethernet-based Access Networks



Pál Varga



MUSE Autumn School 2006
(October 19-20, Bilbao)

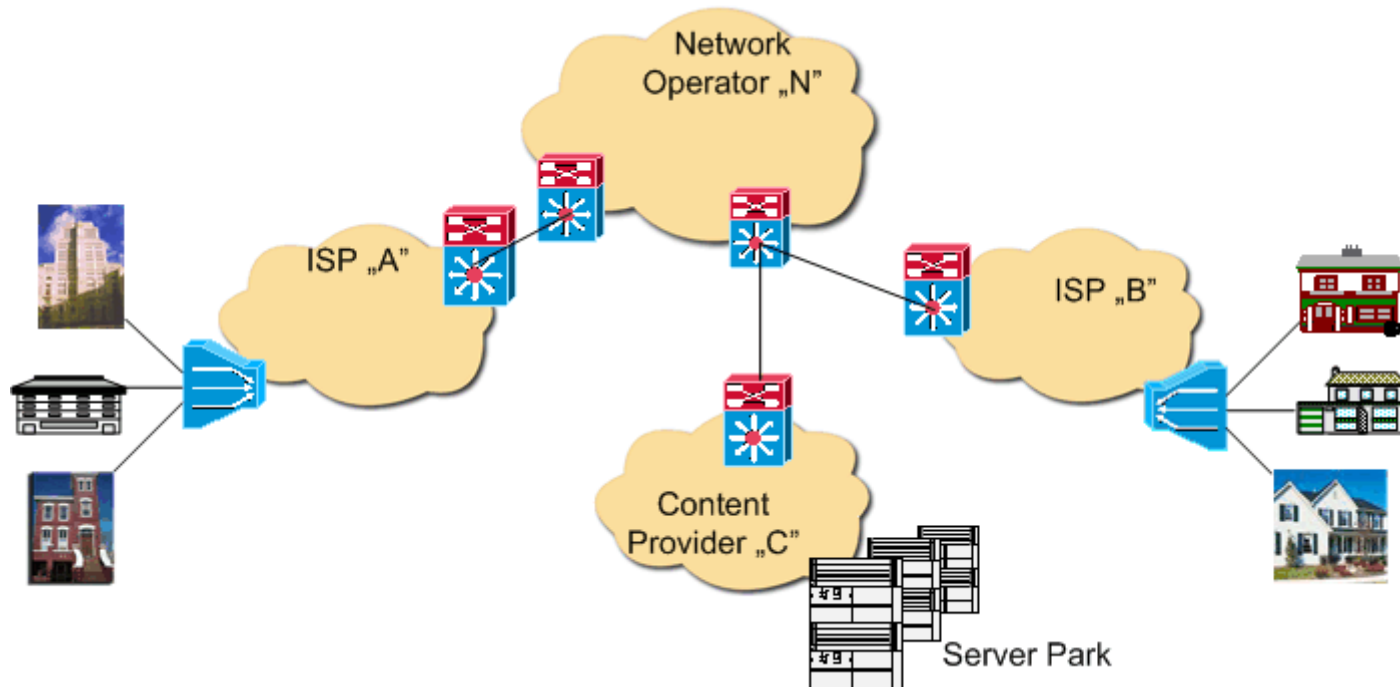
- > Inter-connected Multi-provider Ethernet networks
- > User expectations vs. network provider views of QoS
- > Network and Service Management
 - FCAPS Model
 - eTOM
- > Service Assurance for Ethernet Services
 - Connectivity Fault Management (CFM)
 - Performance Management (PM)
 - Service Level Specification (SLS) validation
 - ...
- > Service Assurance Framework for End-to-End Ethernet Services
 - Event Collection, Event Processing, Root Cause Analysis, Advice...
 - Data-driven RCA model
 - Examples

The global, end-to-end view of networking services

The user is satisfied with the service if

- ☑ his/her requests are **served**,
- ☑ the **quality** of the received service is satisfactory,
- ☑ temporary problems (if any) are **solved** fast.

The user does not want/need to know which service providers and network operators were involved during the process.



Expectations against service quality



Requirements ➤ Service ↗	Bandwidth	Delay	Loss	Other
Interactive speech and video (conf.)	A: small V: HUGE	Minimal	Best Effort	Low jitter
Off-line streaming audio and video	A: small V: HUGE	Best Effort	Best Effort	Low jitter
Client-server apps	small	Low	Low	
Downloads	HUGE	Low	Best Effort	
Potentially alicious traffic	controlled	Best Effort	Best Effort	Isolation suggested
Gaming	Variable	Minimal	Minimal	
Other (E-mail, ...)	small	Best Effort	Best Effort	

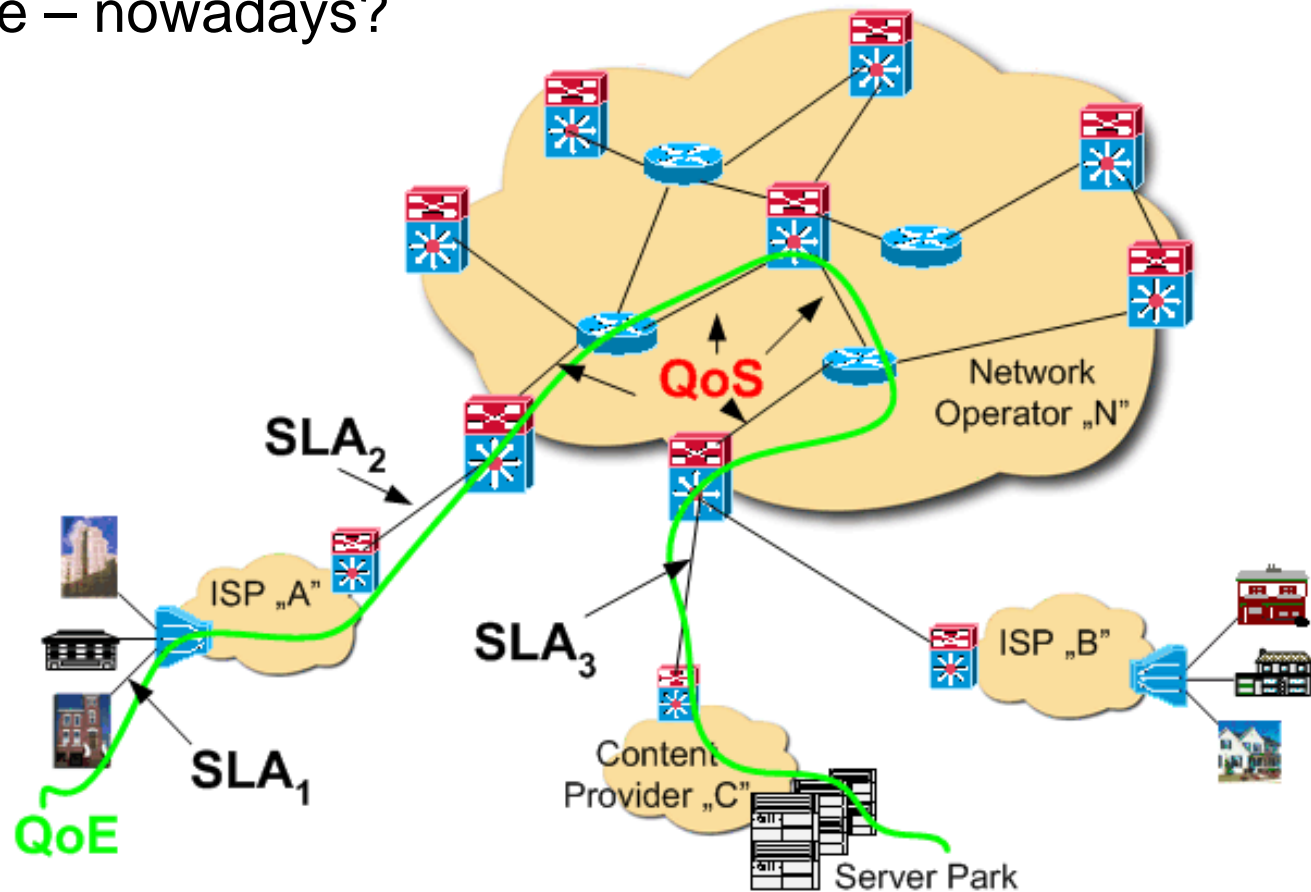


- > SLA: Service Level Agreement
 - The contract itself
 - among service providers and network operators
 - the provider of the **access network** and the subscriber

- > SLS: Service Level Specification – the „**concrete**” part of the SLA
 - The technical parameters describing service quality
 - bandwidth - [kbps]
 - (delay)
 - (jitter)
 - (data loss rate)
 - ... as well as non-technical parameters...
 - service availability time (in the ratio of complete billing time)
 - time constraints of solving service problems

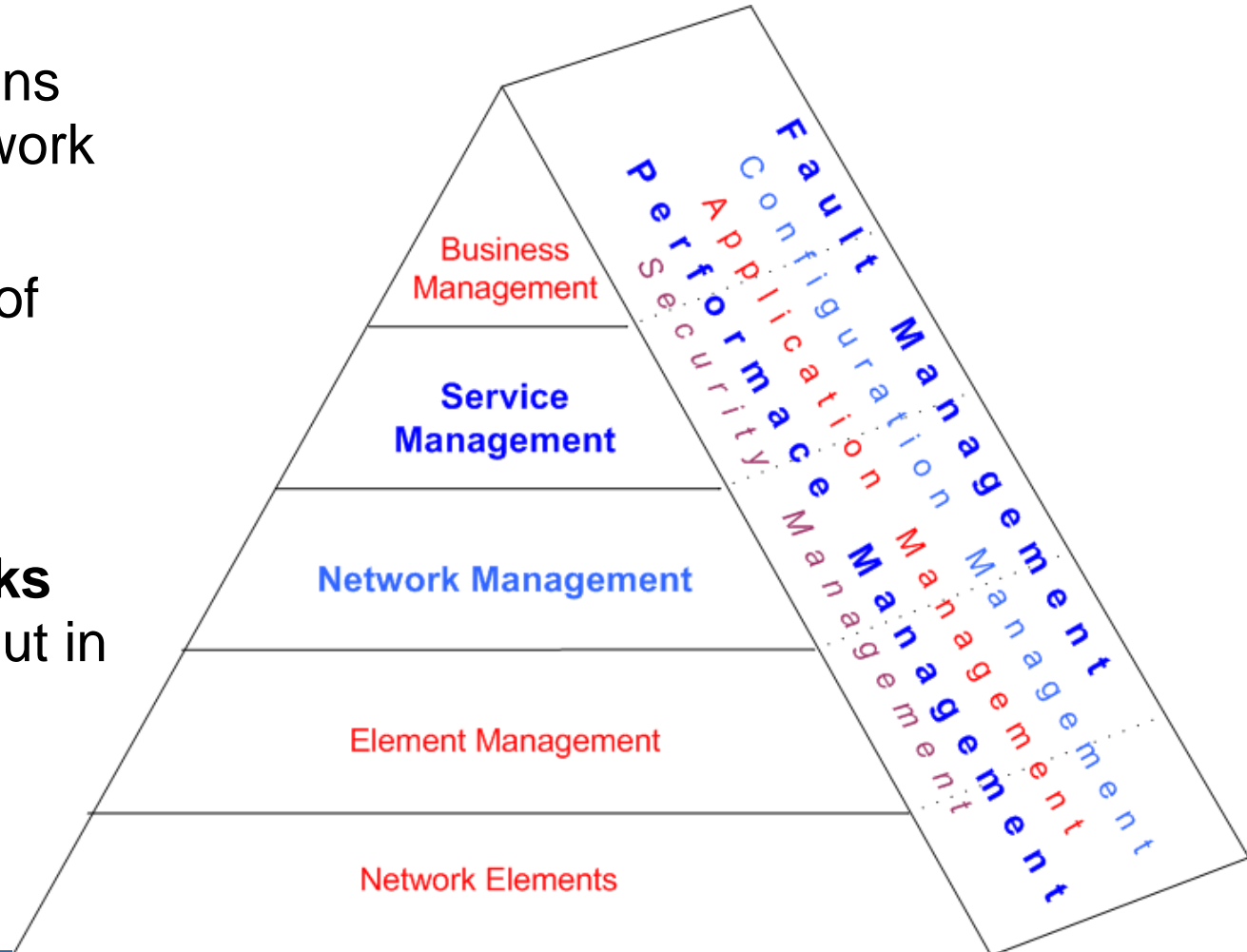
> Is there a real correlation between these – nowadays?

- ❑ If there is no..., then operators cannot rely on the network nodes in service quality assurance & management.
- ❑ There is a need for a constantly working network/service/fault management system.

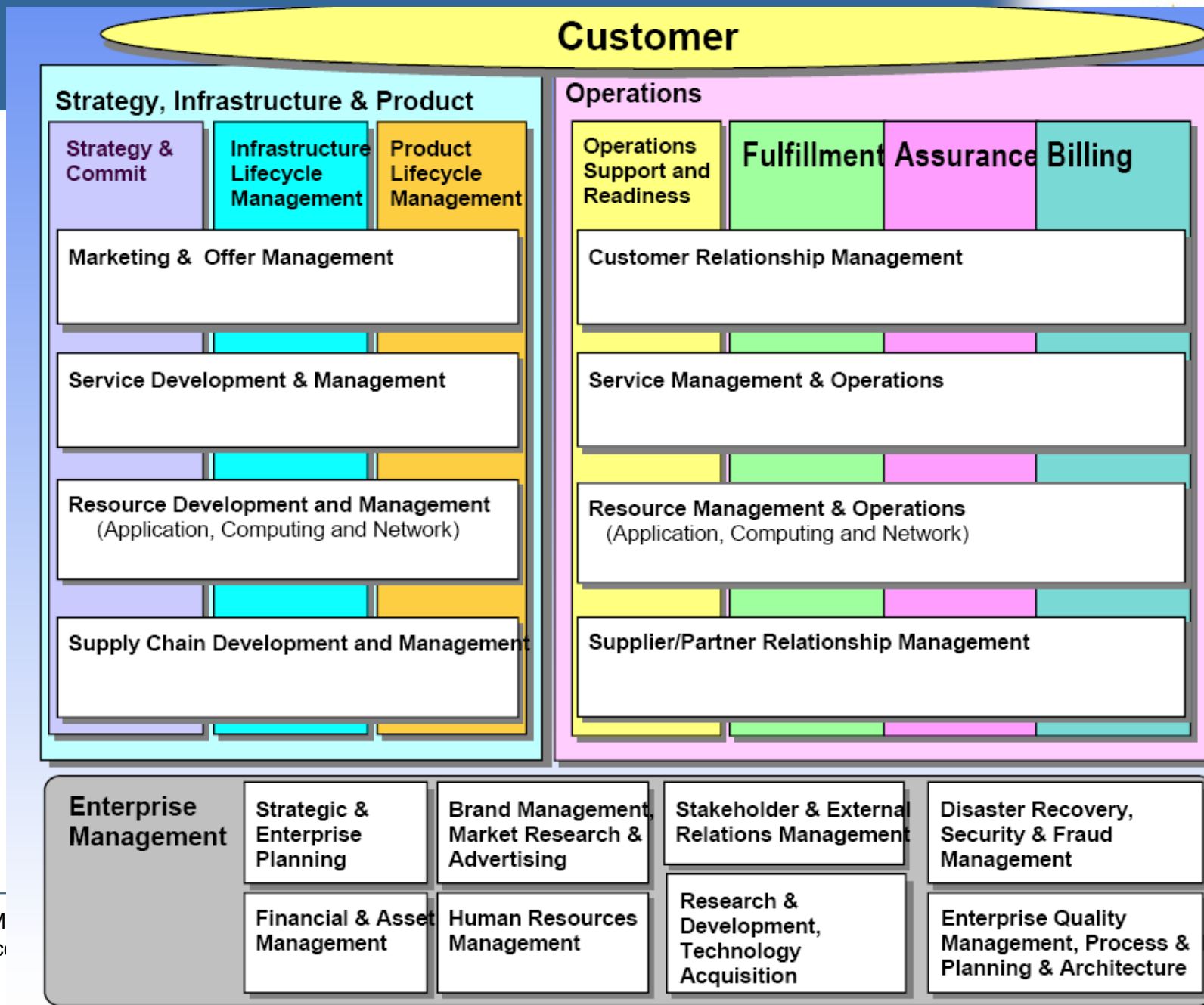


The TMN logical model

- > TMN – Telecommunications Management Network
- > Separated **levels** of management
- > **Similar types of management tasks** are to be carried out in various levels.

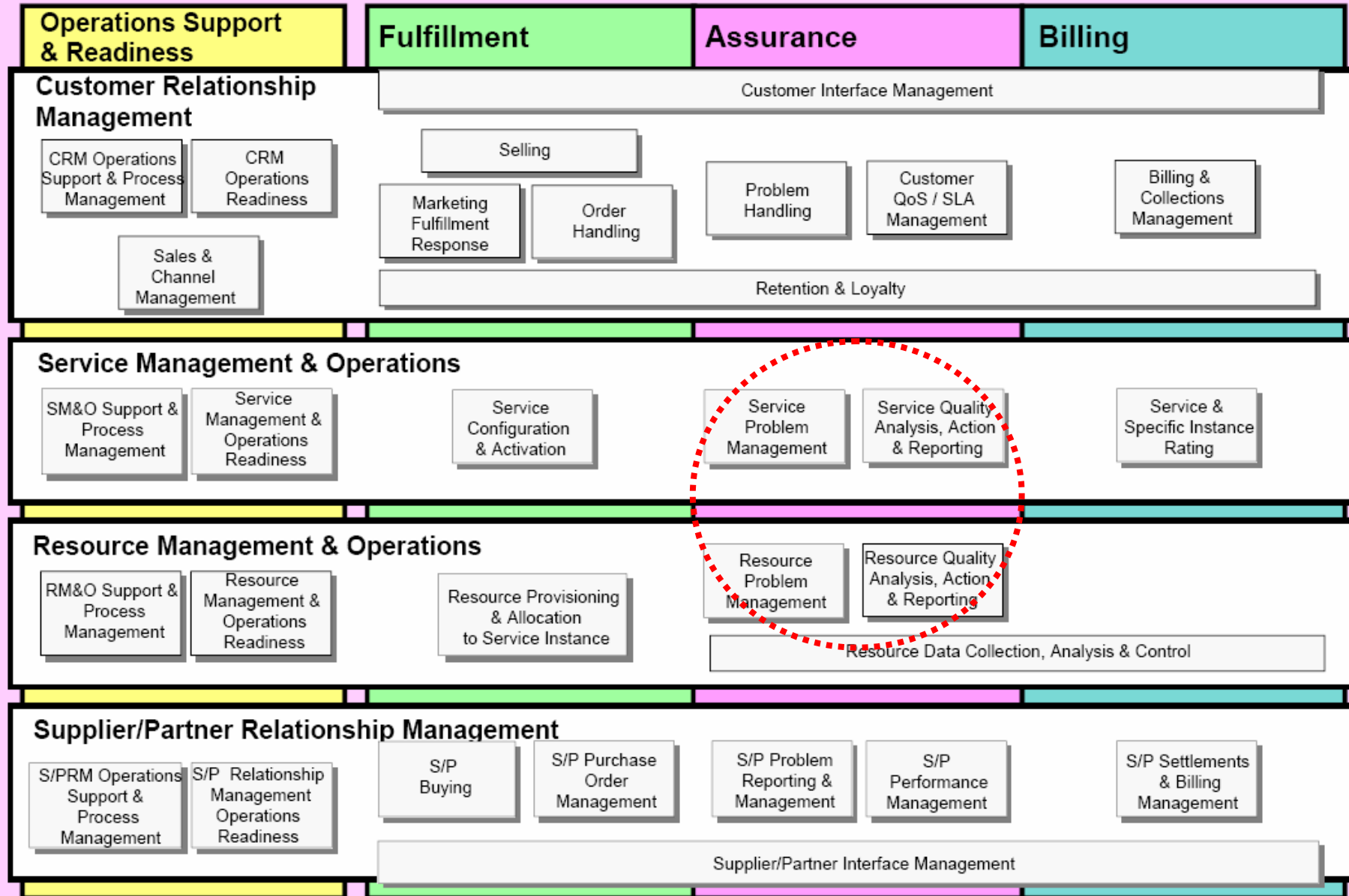


eTOM - Enhanced Telecom Operations Map

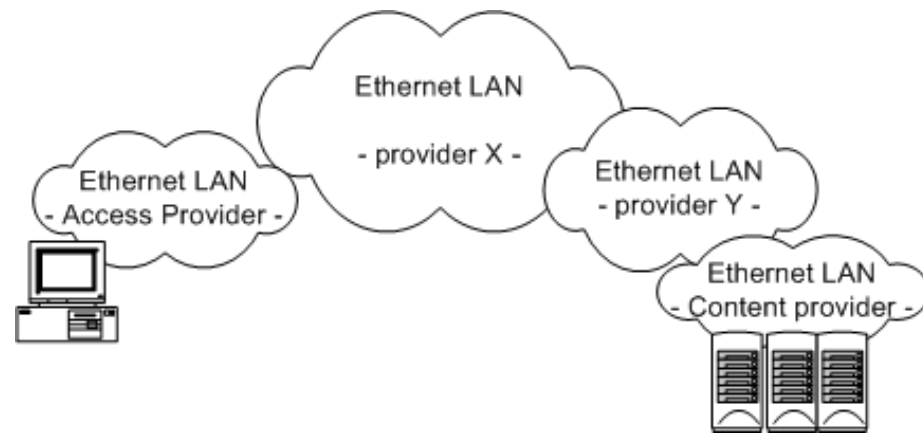


eTOM – The „Operations” area

Operations



- > Service Assurance approach: **end-to-end**
- > **Service Level Agreements (SLAs)**
 - between end-users and access-providers
 - between the service providers/network operators
- > SLA violation: which provider/operator is responsible???
- > What happens if
 - inter-provider SLAs are all OK, but
 - end-to-end SLA is NOT OK ?
- > How to measure „SLA” ?
- > Metrics of SLA: described in **Service Level Specification (SLS)**



> Network and Service Level Management

- **F**ault Management
- **C**onfiguration Management
- **A**ccounting Management
- **P**erformance Management
- **S**ecurity Management

and/or

eTOM

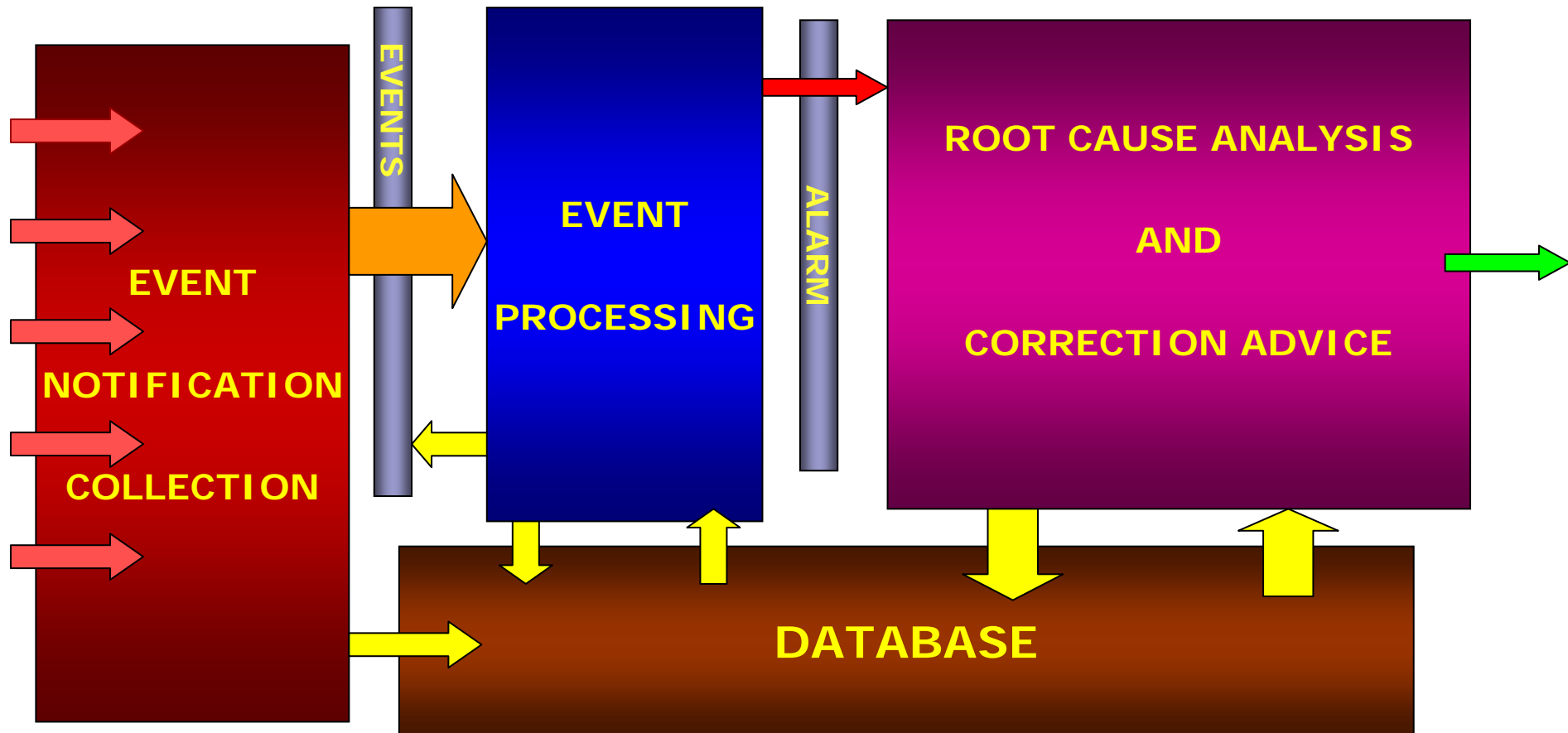
> Ethernet Network Management under Standardization

- Connectivity Fault Management (CFM)
- Performance Management (PM)

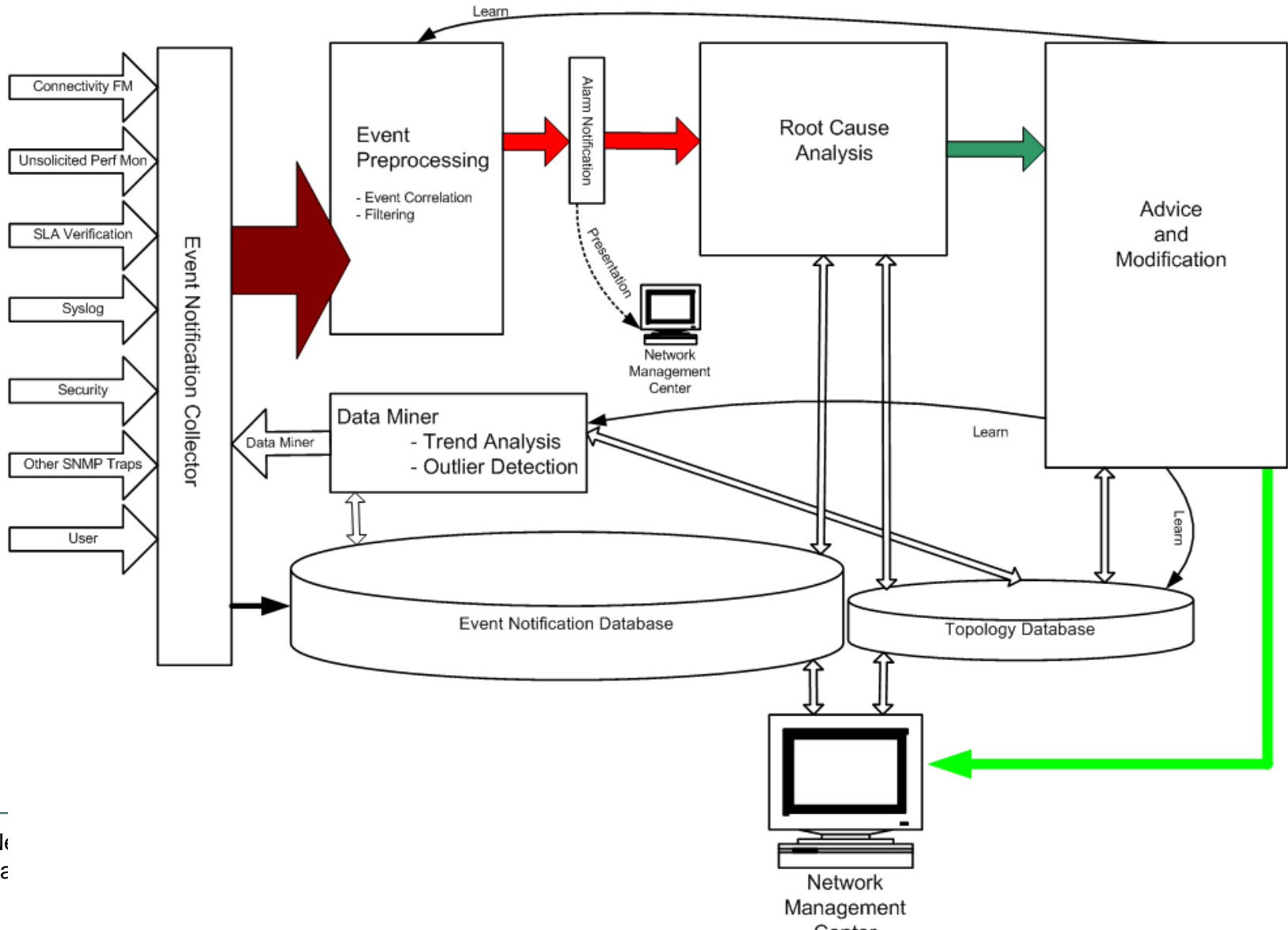
> No standardization body covers

- SLS validation and other event sources of service degradation,
- **How to find the responsible network/service provider?**
 - **Event Processing**
 - **Fault Localization / Root Cause Analysis**

A useful Fault Management framework



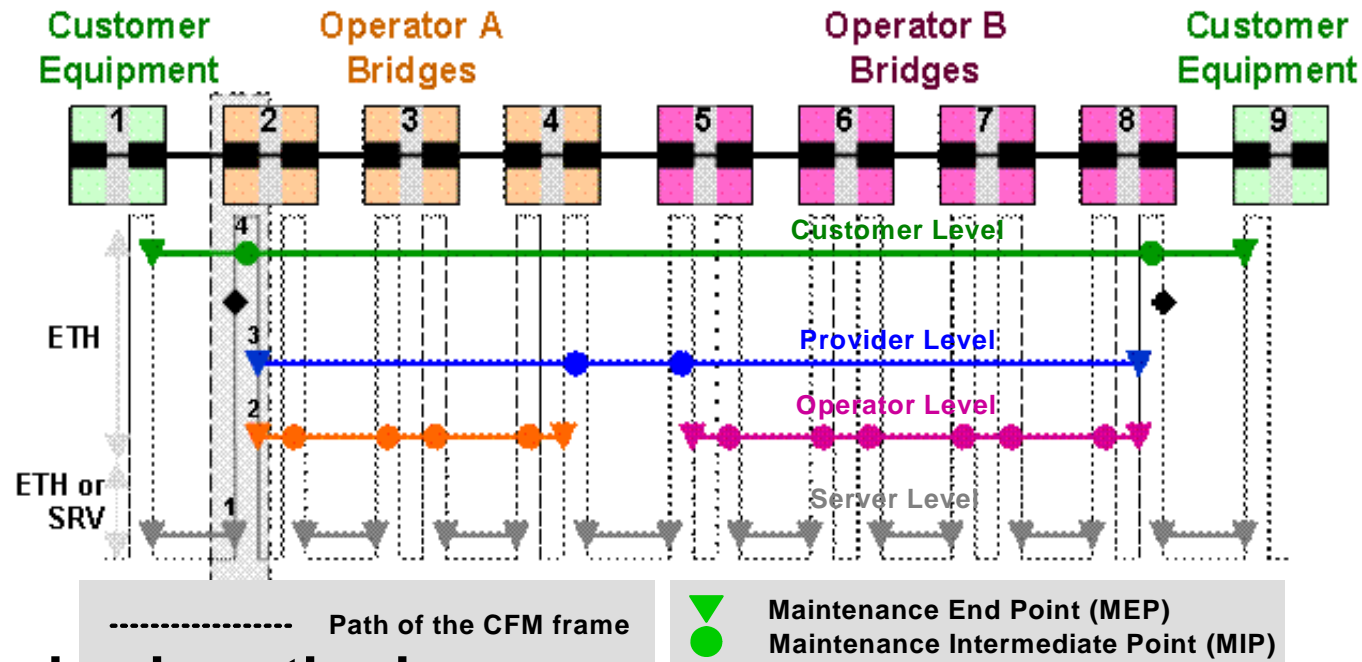
Fault Management for Ethernet Services



> Standardization: **802.1ag** (IEEE) and **Y.1731** (ITU-T)

> CFM key entities

- Maintenance Intermediate Points (**MIPs**)
- Maintenance End Points (**MEPs**)



> CFM uses active check methods

- **Connectivity Check** (periodic hello multicast by MEPs)
- **Loopback** (MEP pings MIPs)
- **Linktrace** (trace route from MEP to MEPs/MIPs)

> Y.17ethoam (ITU-T) defines various metrics

- Frame Loss Ratio
- Frame Delay
- Frame Delay Variation
- Availability
- Errored Frame Seconds
- Service Status
- Frame Throughput
- Frame Tx, Frame Rx Drop Number
- Unavailable Time

...the field is open to measure any other metrics...

> **Unsolicited measurements (regular, periodic)**

> **Solicited measurements (upon request)**

Source	Measure	Type	Note
CFM	Connectivity Check	Unsolicited	MEP Fault alarm notification
	Loopback Link Trace	Solicited Solicited	initiated by elementary checks initiated by elementary checks
PM	Frame Loss Ratio	Unsolicited	notification by SNMP
	Frame Delay measurement Frame Delay Variation measurement	Solicited Solicited	initiated by elementary checks initiated by elementary checks
	Availability Errored Frame Seconds Service Status Frame statistics Unavailable time	Statistics Statistics Statistics Statistics Statistics	statistics are usually gathered into MIBs, otherwise collected with proprietary methods
	Frame Loss Ratio	Unsolicited	notification by SNMP
	Frame Delay measurement Frame Delay Variation measurement	Solicited Solicited	initiated by elementary checks initiated by elementary checks
SLS Validation	Availability Errored Frame Seconds Throughput at egress Offered Load at ingress Frame Rate at egress and ingress	Statistics Statistics Statistics Statistics Statistics	all these PM measurements are taken on a per-path or per-SLS basis
	Spanning Tree bridge traps VLAN notification traps RMON traps	Unsolicited Unsolicited Unsolicited	topology change, new root creation, deletion, membership monitoring of MIB values
	MIB Query	Solicited	query of statistical MIBs
	System messages	Unsolicited	notification by Syslog service
	MAC security Storm Control Unauthorized access attempts Intrusion Detection System	Unsolicited Unsolicited Unsolicited Unsolicited	notification by SNMP notification by SNMP notification by Syslog service proprietary (e.g., SNORT uses Syslog)
Firewall Statistics	Statistics	SNMP or proprietary	
User	Complaints	-	phone/mail



- > Service Endpoints should be managed similar to as MEPs
- > „Services” should be separated by source/destination addresses + protocols (5-tuple,... n-tuple)
- > PM measurements should be carried out on a
 - per SLS basis
 - is a specific SLS met in the specified area?
 - per path basis
 - are the various SLSs met in the path?
- > A database that associatiates endpoints, services and SLSs must be available for the Service Assurance system

- > Alarm vector
- > Rule-based reasoning
- > Case-based reasoning
- > Model-based
- > Fuzzy
- > Neural networks
- > Causal networks (e.g. Bayesian)
- > Distributed, voting-based
- > **Data-driven model**

Alarm vector



	link not avail.	route not avail.	"interface down"	node not responding	high load	high jitter
Link x faulty	1	1	0	1	0	0
Link x overloaded	0	1	0	0	1	1
"interface misconfig"	1	1	1	1	0	0
xy hardware fault	0	1	0	1	1	0
xy route overloaded	0	0	0	0	0	1
...
...

Between t1 and t2 moments in time:

1	1	1	0	0	0
----------	----------	----------	----------	----------	----------	-----	-----



- > Its foundation is a **knowledge base**, describing
 - in **what cases**
 - **what kind** of „complex” alarm describes the
 - incoming, **atomic events** best.
- > The knowledge base stored the relations according to Bool rules
- > In case the relation-value is true, then the operation corresponding to that rule is executed
- > This method is
 - simple,
 - rules can be changed flexibly
 - evaluation of the rules is fast enough.

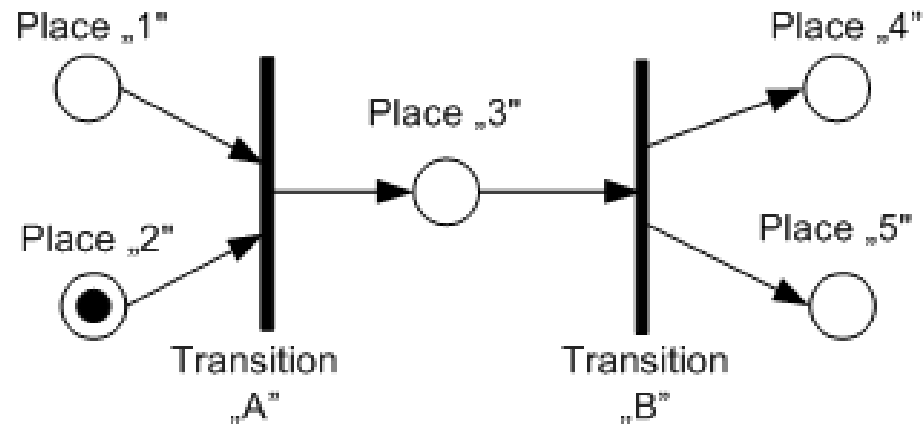
```
{2; a104 || a302; 3; ;Host=<IP addr>; Kind=6; Prio=2; Code=602;  
Parameter="TOO MANY CALLS FINISH UNEXPECTEDLY"}
```

- > **Follows** the working „habits” of fault-localization **experts**
- > Based on the parameters of the alarm
- > **Initiating active checks** while looking for possible (typical) fault causes
- > Once the satisfactory types of **input data of a check is** available, that checking test is immediately initiated
- > **Depending on the results**, more and more other checks are initiated
- > Execution of such test is **parallel**

> The most well-known implementation of the data-driven computing model are the Petri nets.

> Basic elements:

- Transitions
- Places
- Tokens



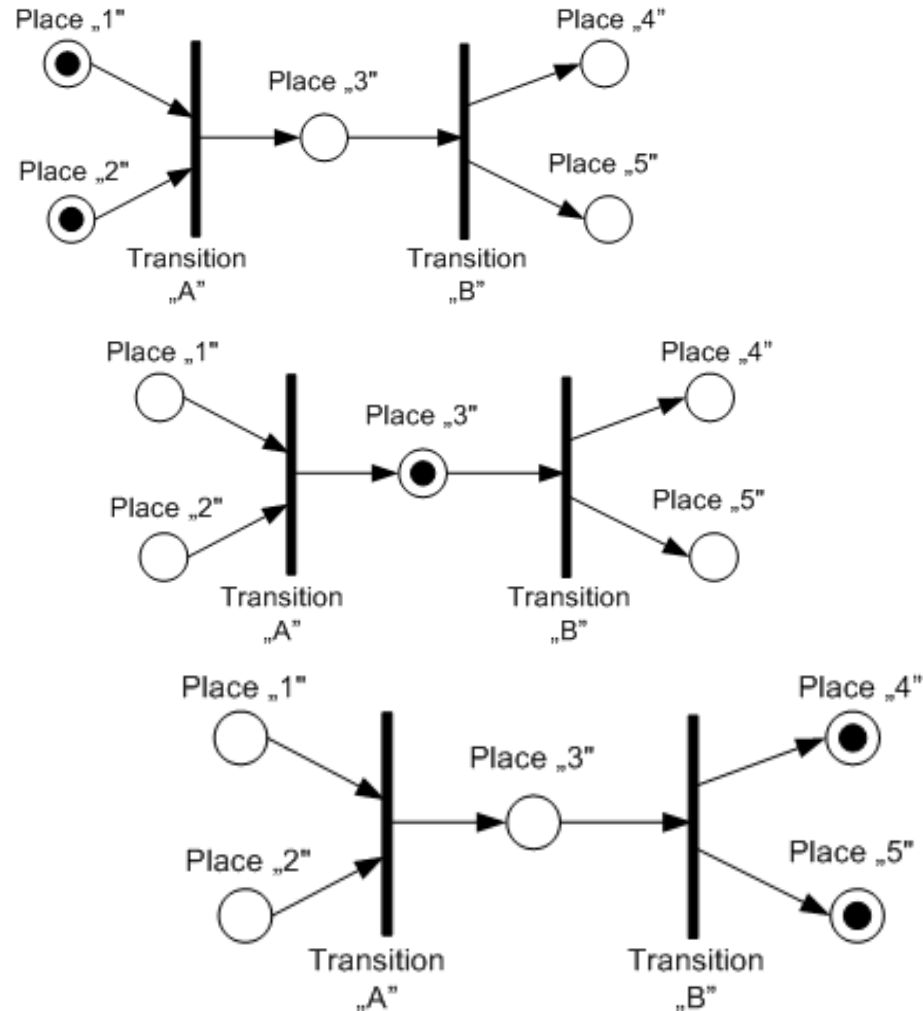
> A Transition „fires“ if all of its Places are Tokened.

> Upon „firing“ the Transition

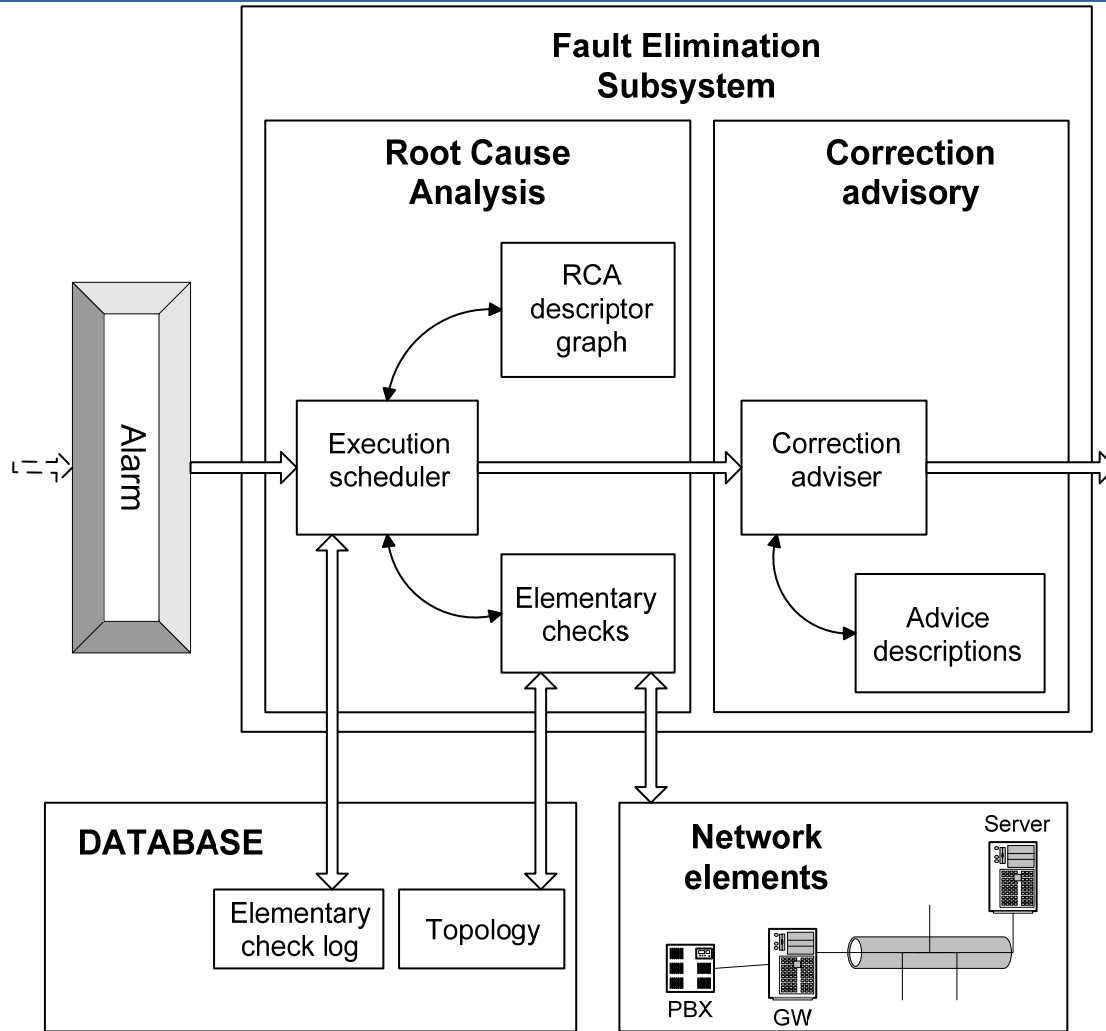
- takes all tokens from its input,
- executes its corresponding function, and
- puts tokens to all its output Places.

Data-driven models – Petri Nets (cont'd)

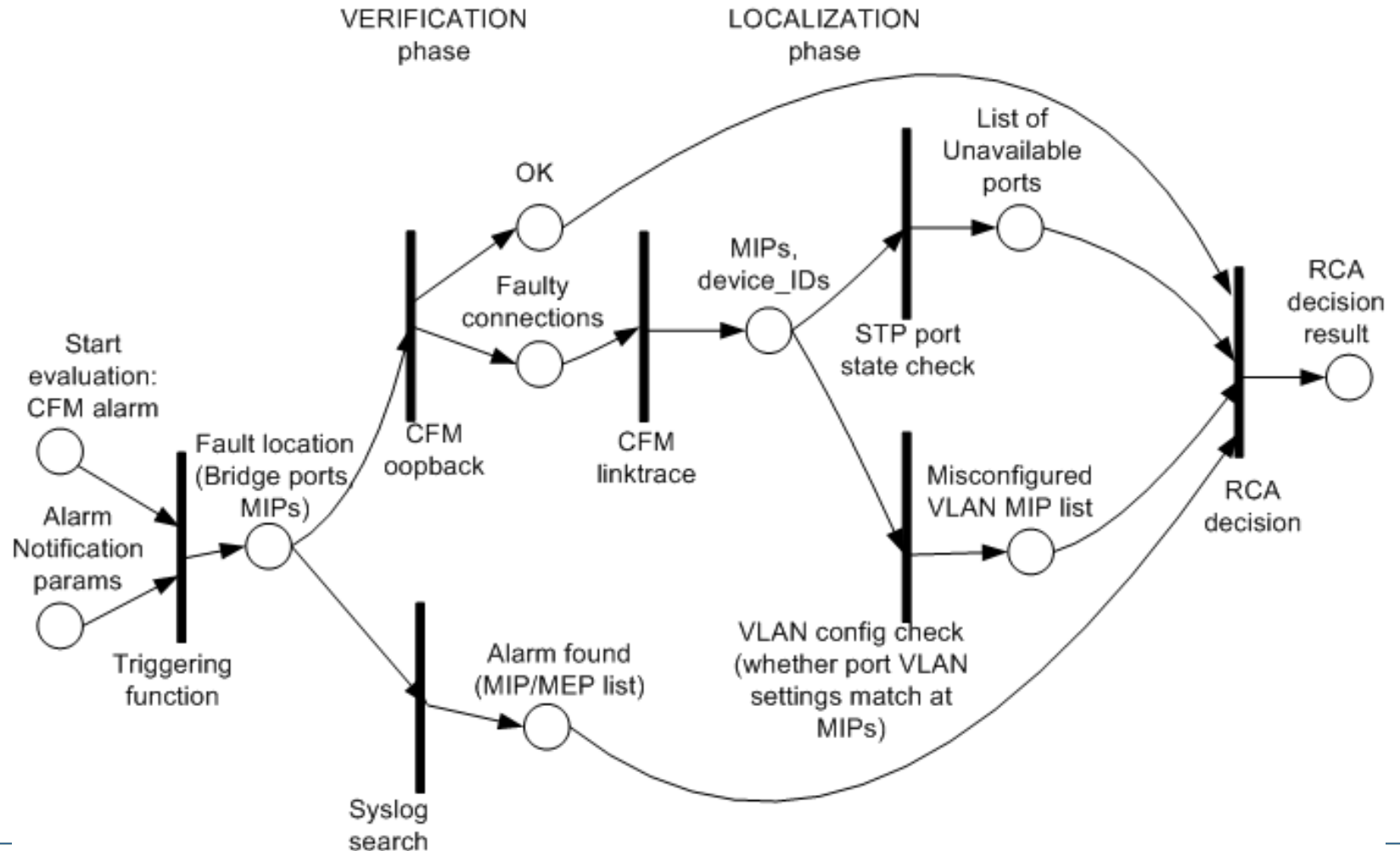
- > In the current fault management case:
 - Transitions are active, elementary checking routines
 - Places are input and output parameters of the active checks
 - Once an elementary check is finished and returns with results – new elementary checks will start up, using these parameters as input



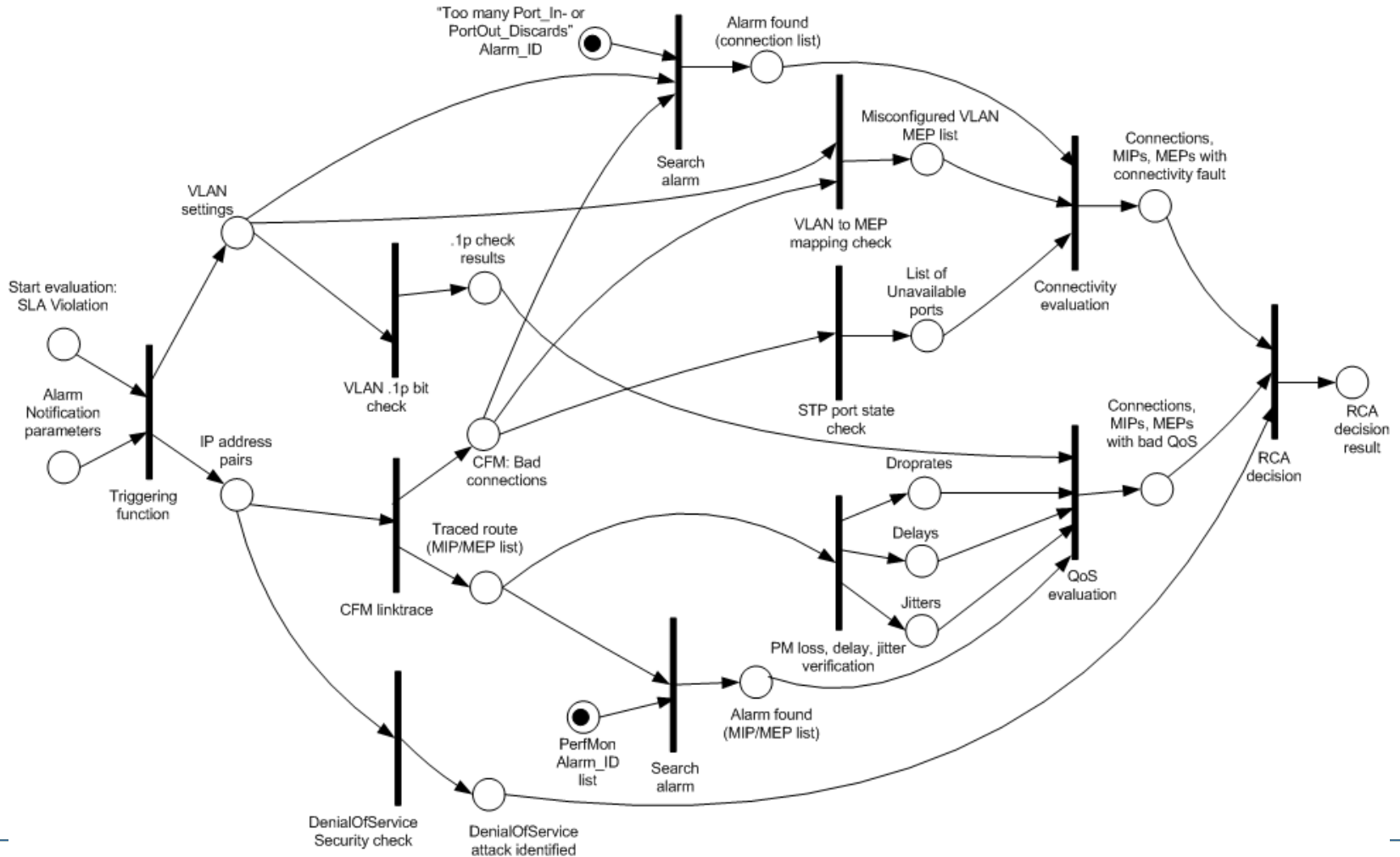
The modular view of data-driven Root Cause Analysis



Fault Localization steps of an Ethernet CFM alarm



Fault Localization steps of an SLA-violation alarm



- > Network and Service level mgmt in multi-provider Ethernet networks
- > Who is responsible for a fault???
 - Notification about faults „as fast as possible”
 - Finding out the root cause of a fault „automatically”
- > Ethernet Connectivity Fault Management – end-to-end solution
- > Performance Management
- > SLS Validation
- > Service Assurance Framework
 - Utilizing methods and metrics suggested by the standards
 - **Making the expert’s job easier**: easy-to-implement, **data-driven** fault localization methods with scheduled active checks
 - End-to-end QoE can be evaluated in the **Access Network** by standard FM procedures