

Industrial Challenges in Working with Events

Prof. Dr. Petre DINI, Senior Technical Leader, NMTG Manageability

Cisco Systems, Inc.

pdini@cisco.com
petre@iaria.org

The Road Ahead

Cisco.com

Positioning

Issues

- Event definition
- Event transport
- Event processing
- Business-driven events

2009 Athens

Positioning

Cisco.com

- Layered event process architecture
 - Issuing events
 - Processing events
 - ? Performance
- Information bus
 - Publishing events
 - Subscribing to events
 - ? Access/ transport
- Towards autonomic event processing
 - Network smartness vs. network management

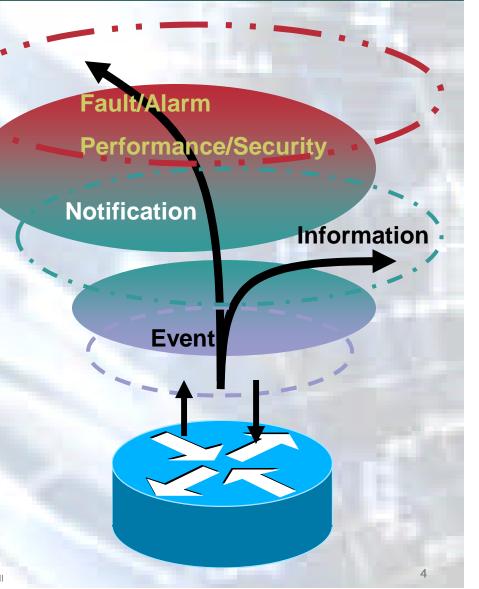
Get the infrastructure behavior

Cisco.com

- Act (pre-emptive, proactive, reactive,...)
- Correlate (diagnostic, troubleshooting, impact, root cause, ...)
- Get status (push/poll)

All operations can be policy-driven

- top-down
- bottom-up



Bottom-up vs. Top-down

Cisco.com

- Domain Manager enriches with domain information
- EMS enriches with multidevice information
- Notification Engine collects OS notifications

Third level (Domain Manager)

Second level (Element Manager)

First Level (Mgd Elemt)

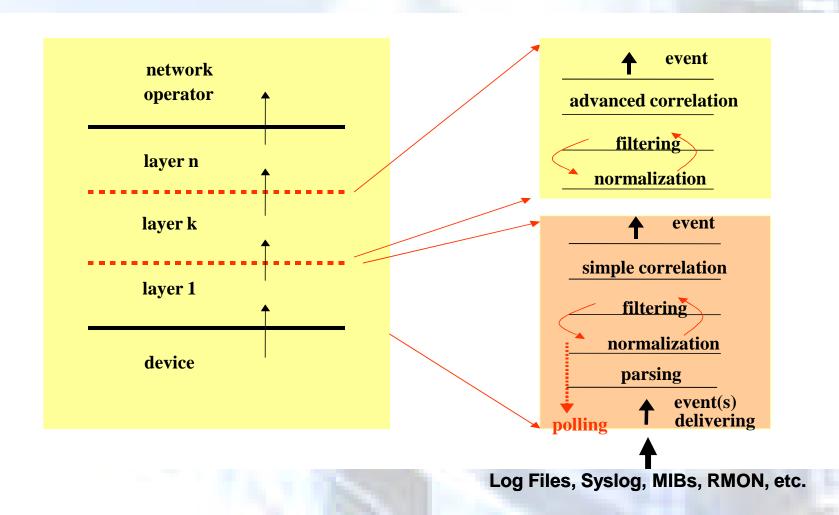
➤ Event
Information +
 Device
Information +
 Domain
Information

➤ Event
Information +
Device
Information

Event
Information

A Layered Processing View

Cisco.com

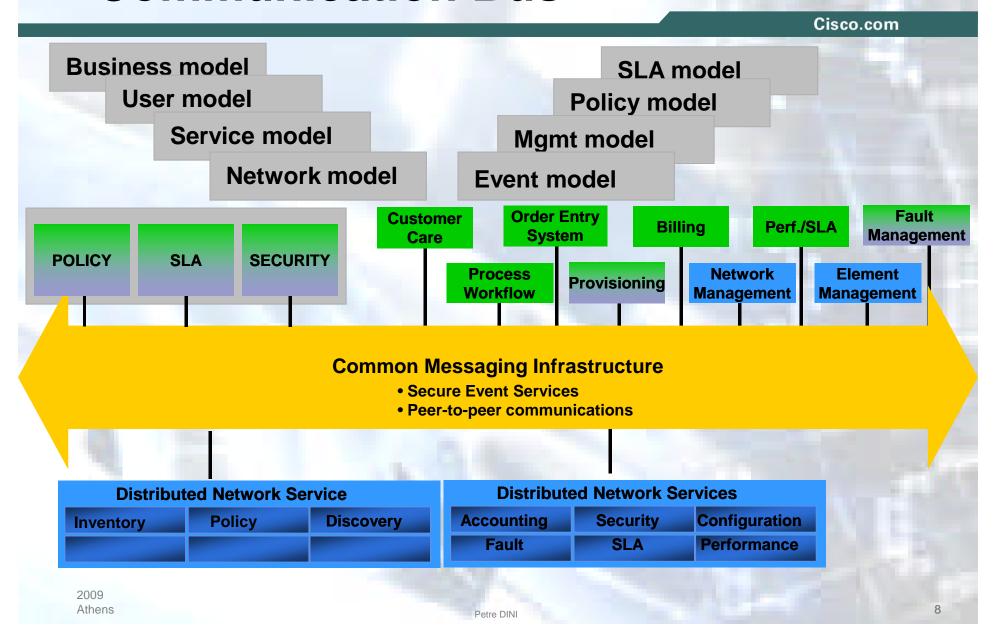


Multi-level diagnostic

Cisco.com **Diagnostic** advanced diagnostic & correlation events: filtering -From Any Diagnostic Level II Diagnostic Functions **Engine inside NEs** normalization - within the NE, - From a specialized - by SA on top of NEs **SA Engines** - by SA and Remote Knowledge -From other OSS Events, Alarms, Faults **DataBase** components processing normalization parsing event(s) delivering **Events** Log Files, Syslog, SNMP informs, Level I Diagnostic Functions CLI commands, etc. (embedded within the NE) **GODS: Generic Online Diagnostic Subsystem** 2009 Athens

Petre DINI

Communication Bus



Evolution of Network Manageability

Cisco.com

Operational Capability

Industry is here

Market Requirement

Adaptive Networks

- Self-healing, self-tuning, self-mgmt
- High Availability network services

Programmable Networks

- Single Programmatic Interface
- Configuration of networks and services
- Policy-based network management

Programmable Devices

- SNMP, XML and other interfaces
- Configuration of device parameters
- Automation of manual procedures

Manual Devices

- CLI operator interface
- Configuration of device parameters

Network Scale, Complexity, Availability

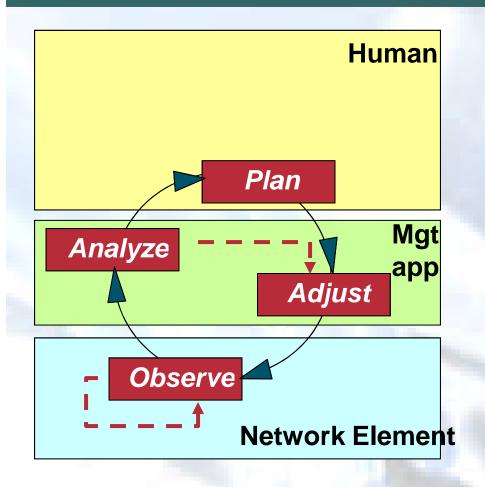
Evolution of Network Smartness

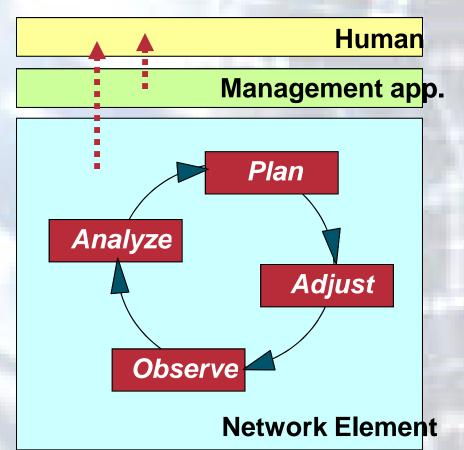
Cisco.com

Adaptive Behavior Self-healing, self-tuning, self-mgmt **Industry High Availability network services** is here **Operational Capability Predictive Behavior** - Monitoring - Resilient networks - Symptoms, pre-emptive Market Requirement **Reactive Behavior** - Call Home - Decrease MTTR - Not time critical **Connected Devices** - Can be addressed <naming><location> - Inventory

Autonomic Computing

Cisco.com





(a) Typical management control loop (b) Closed management control loop in autonomous network

Challenging Issues

Cisco.com

Too Many

2009 Athens

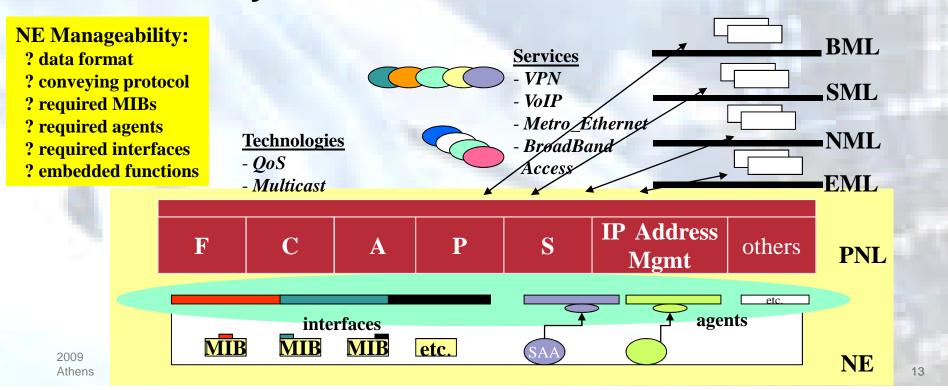
Petre DIN

Syntax Issues



Cisco.com

- Various formats
- Myriad of conversions needed
- Lack of syntax control



Syslog Message "Body" Format in the IOS

Cisco.com

* Sep 20 01:12:31: %SYS-5-CONFIG_I: Configured from CONSOLE CONSOLE (144.254.9.79)

Timestamp IOS Component Severity Mnemonic Message-text

Timestamp from the server

SERVER

Sep 20 01:07:00 router.cisco.com 571: Sep 20 01:12:31: %SYS-5-CONFIG_I: Configured from console by vty1 (144.254.9.79)

Router

NTP is needed!

Timestamp from the router

Header:level can be different than Body:severity

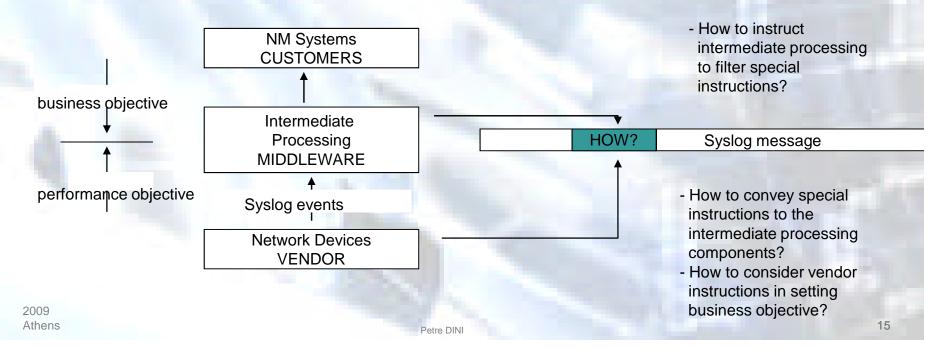
2009 Athens

Semantic Issues



Cisco.com

- Naming
- Context-defined
- Smart events



XML Tagging is Not Enough

Cisco.com

Tag table (??)
Tag List:
<name><semantics>

1. <a> <c> ? ? ?

Tag relationships

2. <<a> --- r1 -- > -- r2 -- <c>

e.g.,
<a> -- Interface (? OID)
 -- Port (? OID)
<c> -- Severity

Naming service required

- Despite the problems caused by its use:
- The messages don't have a standardized definition
- Priority is geared toward UNIX problems
- Priority is not used consistently
- Not reliable
- Not secure
- some key features, (i) ease of use for developers, (ii) familiarity, and (iii) ubiquity makes it a workable solution.

2009 Athens

Timestamps issues

Cisco.com

- Format
- Clock-free event sources
- Sources-destination timestamps
- Delay tolerant networks
- Localizing processing
 Local synchronization
 Wide synchronization
- Reliable timestamps

2009 Athens

Adding Security to Event Transport

Cisco.com

- Entity authentication
- Message Authentication
- Privacy
- Data integrity
- Signatures

2009 Athens

Putting and End to Unreliability

Cisco.com

- Reliable transport mechanism
- Partially reliable transport [weak link]
- ?
 - event itself [seq numbers]-based
 - window-based
 - context-based

2009 Athens

Example: Syslog

Cisco.com

[field1] % [field2] % [severity] % [priority]%[mnemonic] %[free form field]

Well identified fields

[timestamps]

[facility]

[severity]

[priority]

[mnemonic]

Free form field (the richest in semantic) [..English plain text..]

Field separator

Issues

- Number of fields varies
- Value space of the fields is is not uniform/standardized
- Semantic of timestamps is not uniform/or not defined
- Mnemonic is not modeled
- The English text is only humanly readable/useful
- Automation is difficult due to the "natural language processing" needs

Things started to get fixed

Cisco.com

- Syslog, SNMP/MIB: IETF
- Adaptive message format: IBM/Cisco
- Intrusion detection format: IETF
- Anomaly report format: OASIS
- Incident handling format: IETF
- NGN management : ITU-T [Focus group]

2009 Athens

Still to answer...

Cisco.com

- Concepts such utility-based computing, autonomic computing, diagnosis-in-the-box, diagnosis out-of-box, adaptable applications, self-adaptable applications, and reflexive environments require a new approach of formalizing events, architecting event-based systems, and integrating such systems.
- Additionally, GRID systems bring into the landscape the concept of intermittent and partial behavior related to resource sharing that may require a special semantic on SLA/QoS violation events.
- Events related to traffic patterns and the dynamics of performance and availability changes in such environments requires particular metrics and processing, as well [accounting, outage].
- Another hot area quite poorly covered in terms of eventrelated requirements is MPLS OAM and all aspects related to MPLS VPN.

2009 Athens

CISCO SYSTEMS



Network Management Technology Group