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

Positioning

Issues

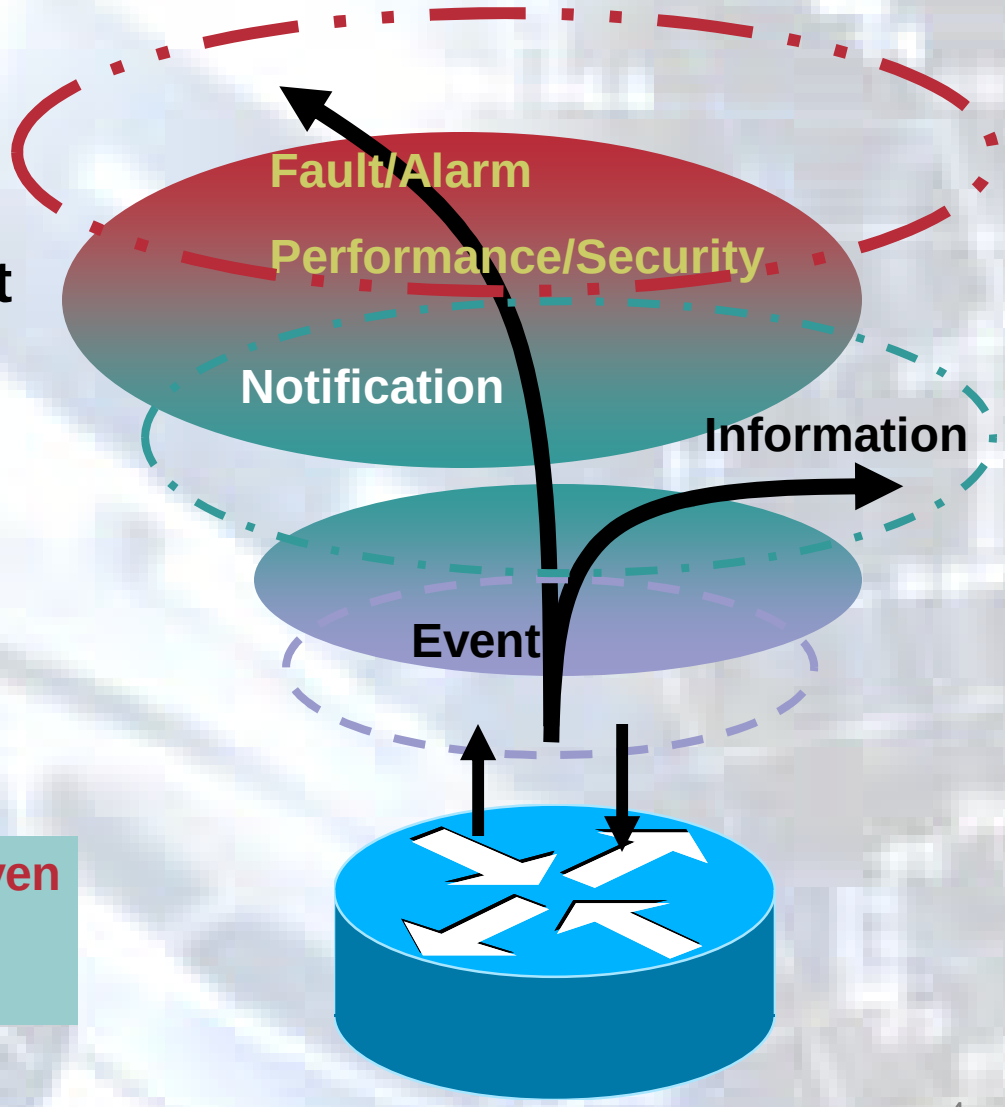
- Event definition
- Event transport
- Event processing
- Business-driven events

Positioning

- **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

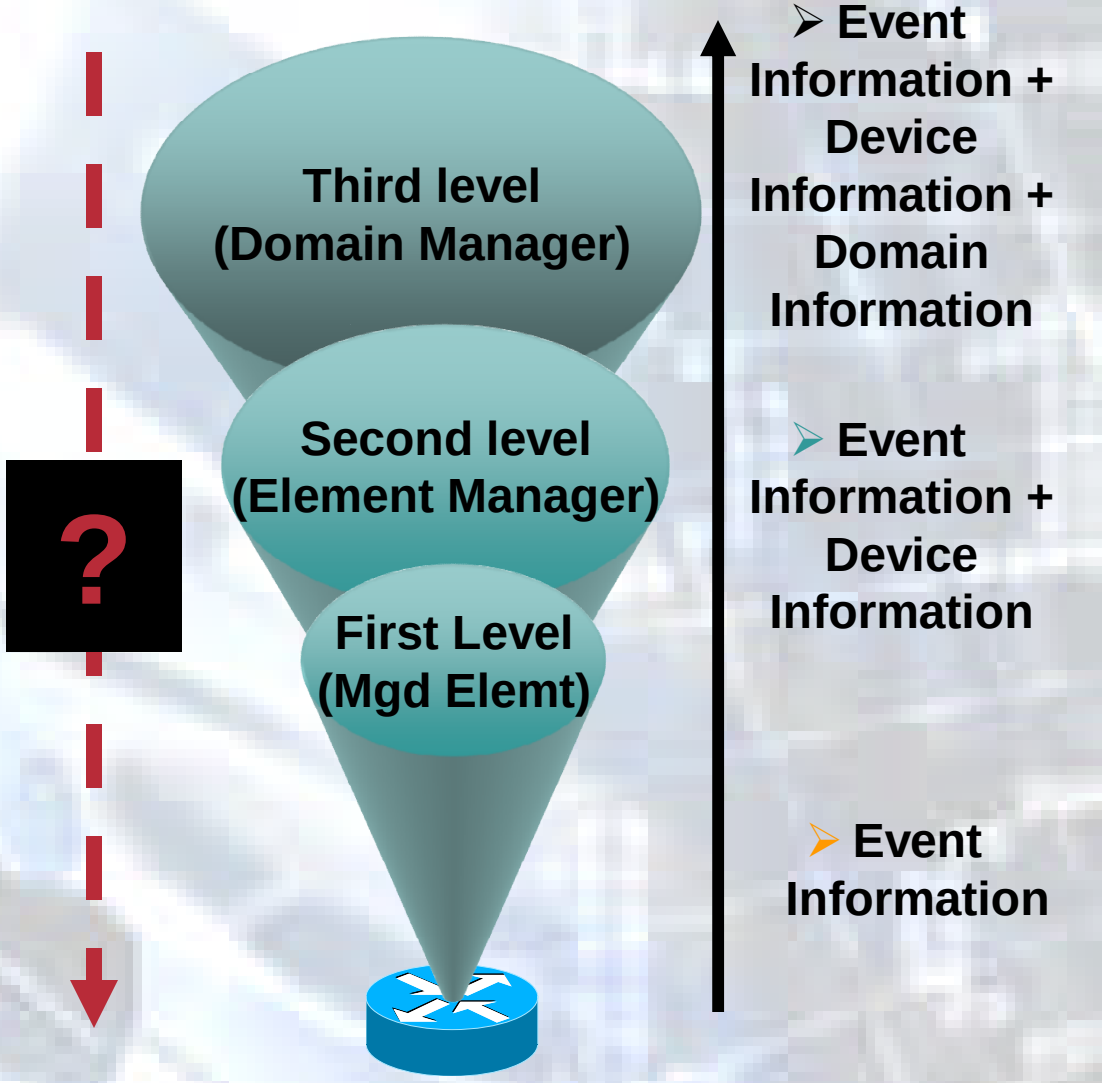
- Act (pre-emptive, proactive, reactive,..)
- Correlate (diagnostic, troubleshooting, impact, root cause, …)
- Get status (push/poll)



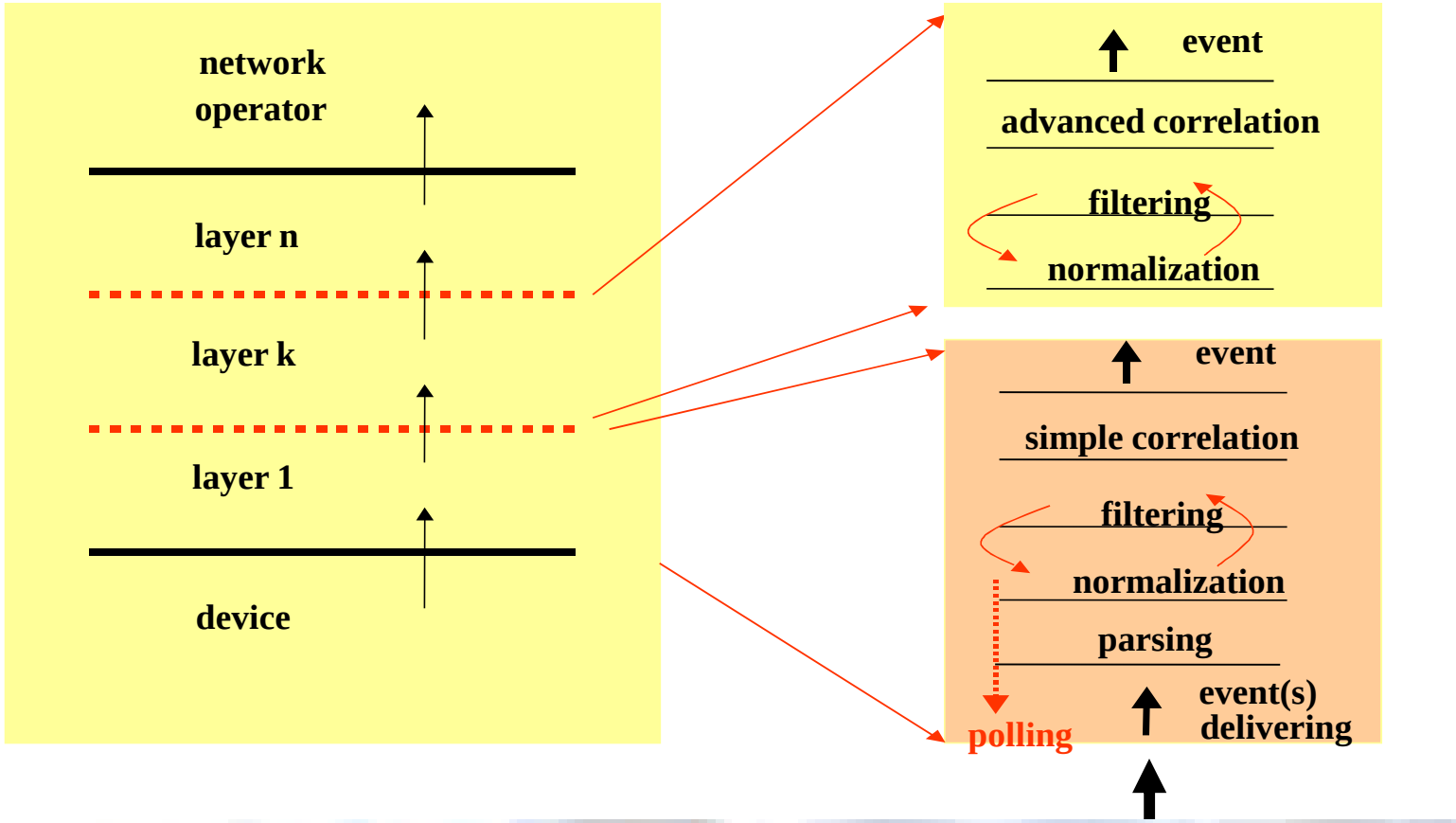
All operations can be policy-driven
- top-down
- bottom-up

Bottom-up vs. Top-down

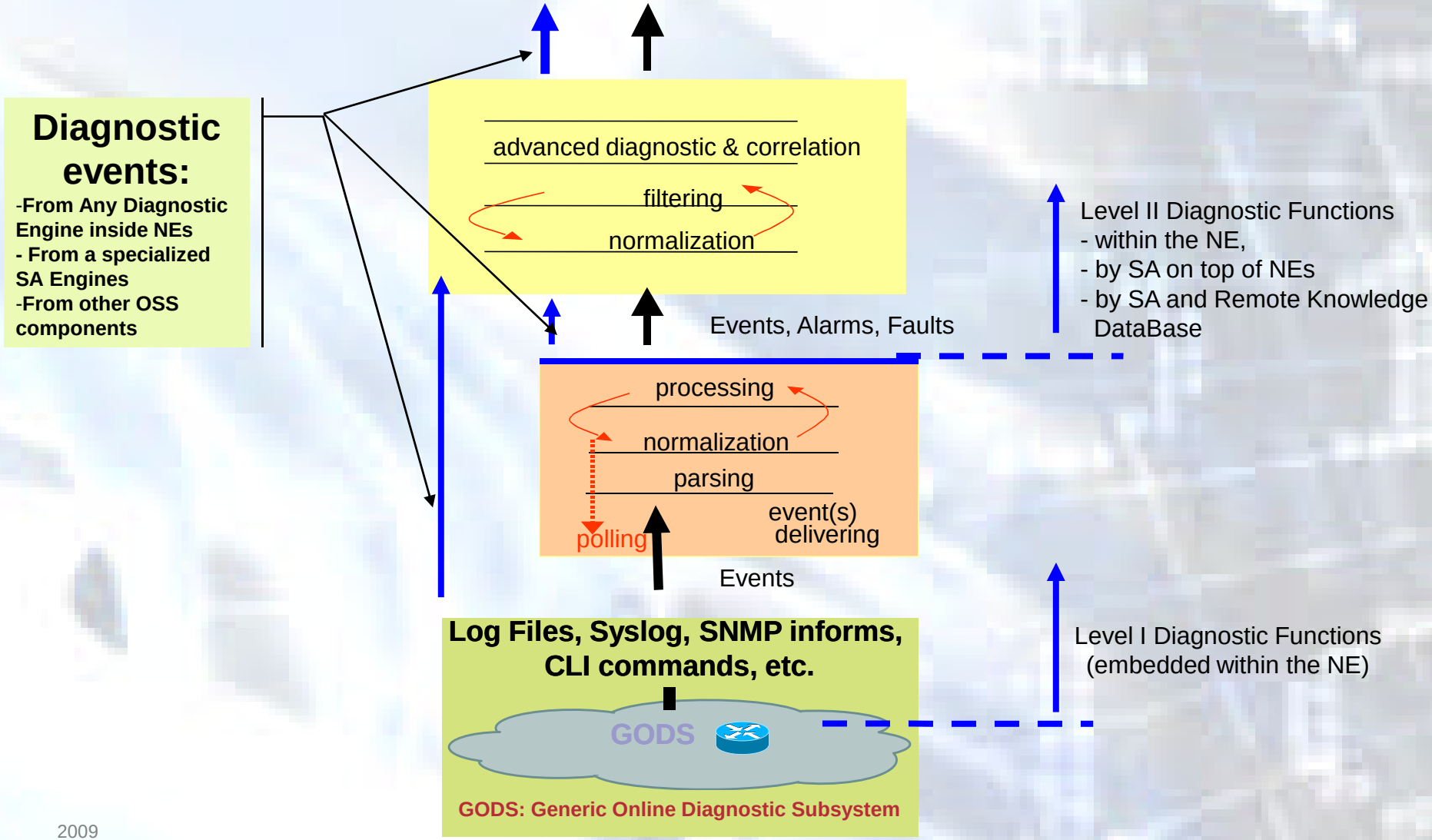
- Domain Manager enriches with domain information
- EMS enriches with multi-device information
- Notification Engine collects OS notifications



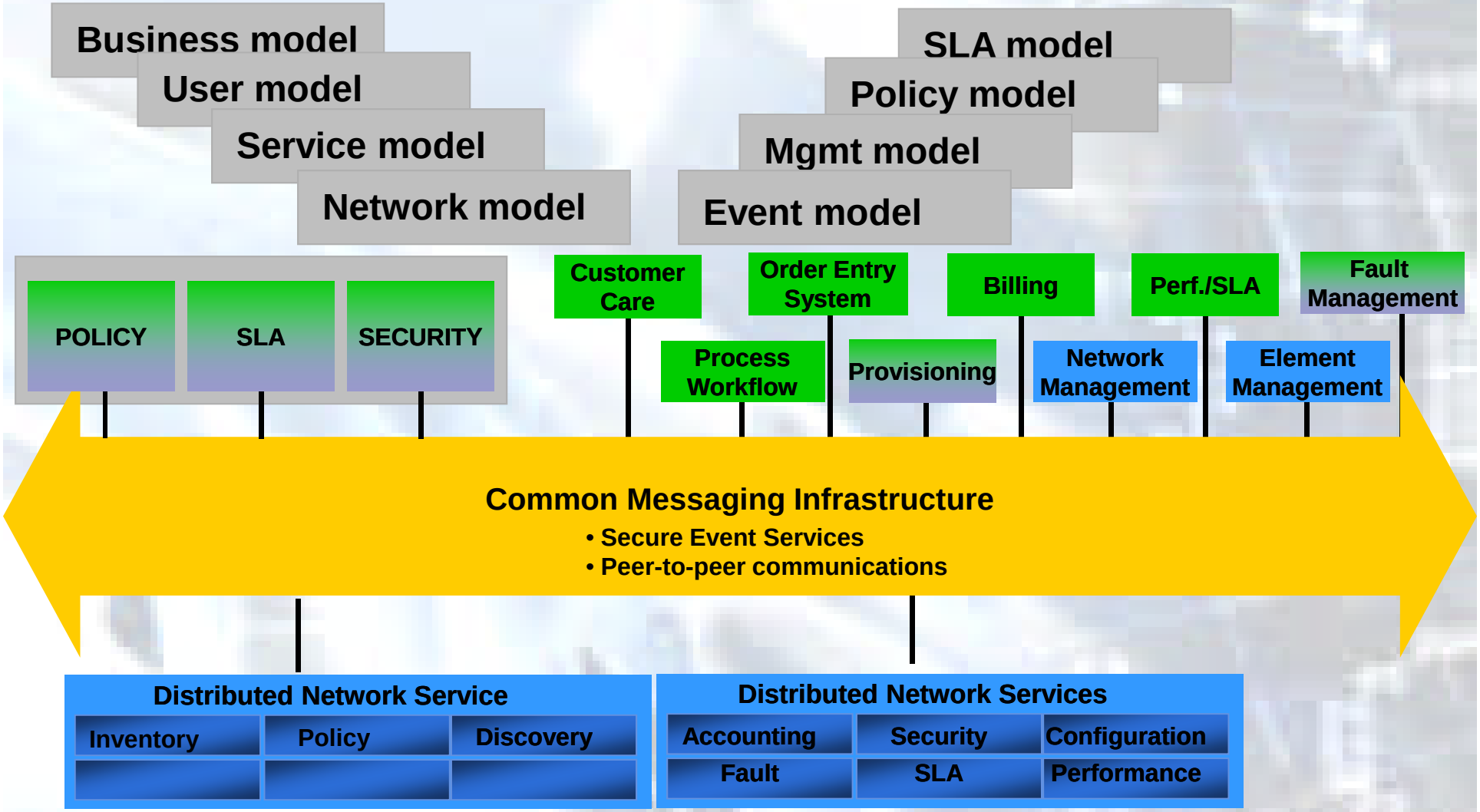
A Layered Processing View



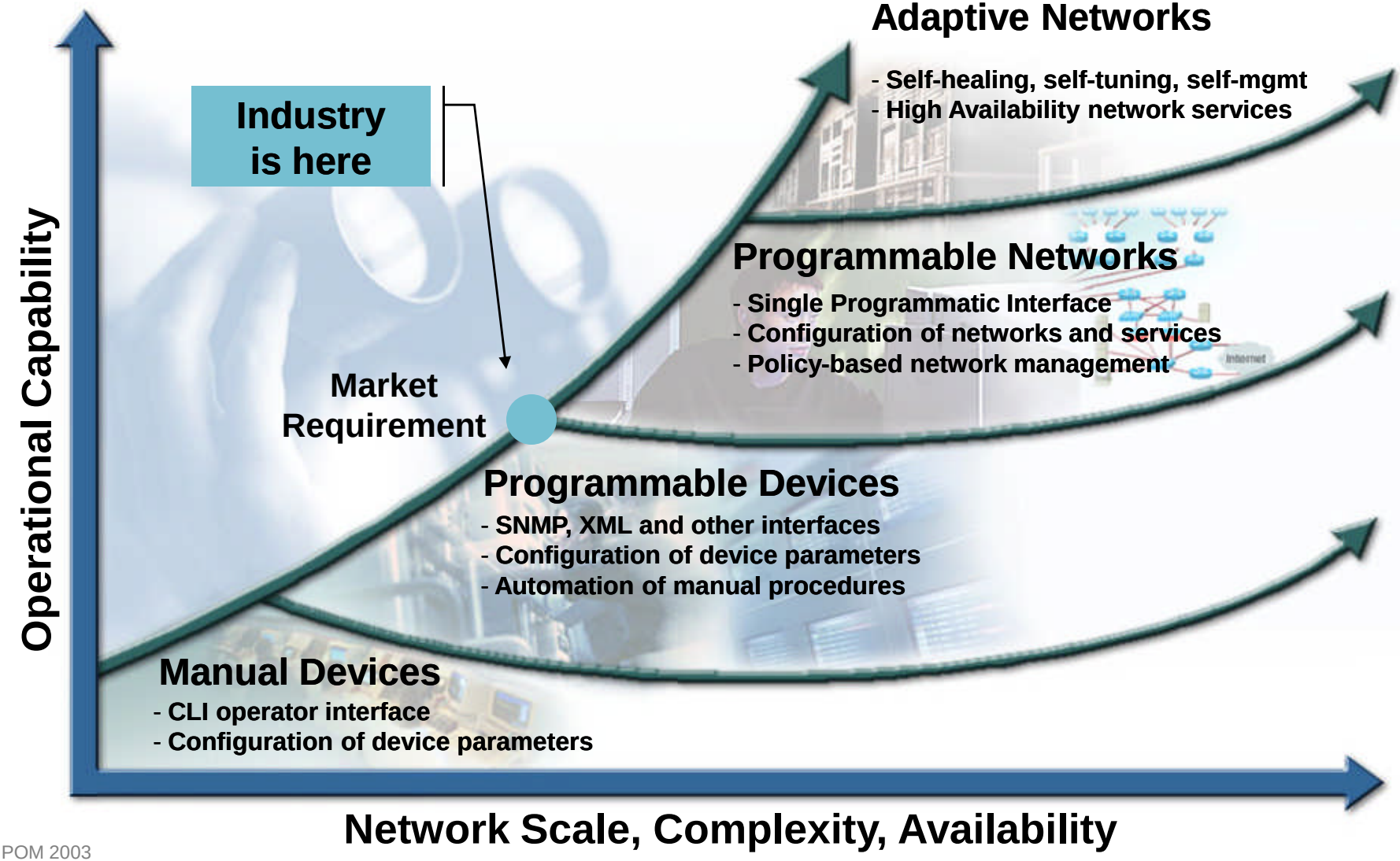
Multi-level diagnostic



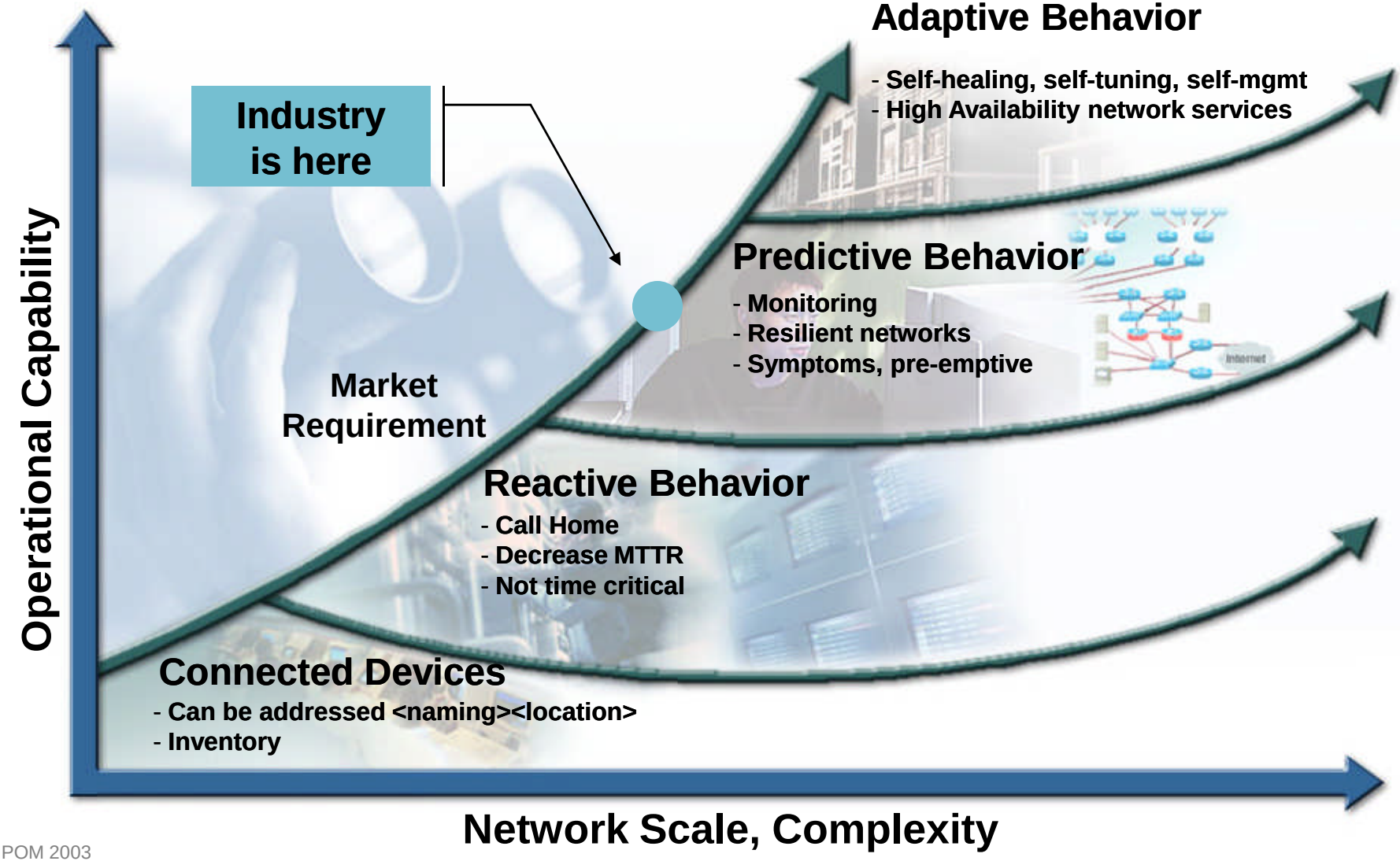
Communication Bus



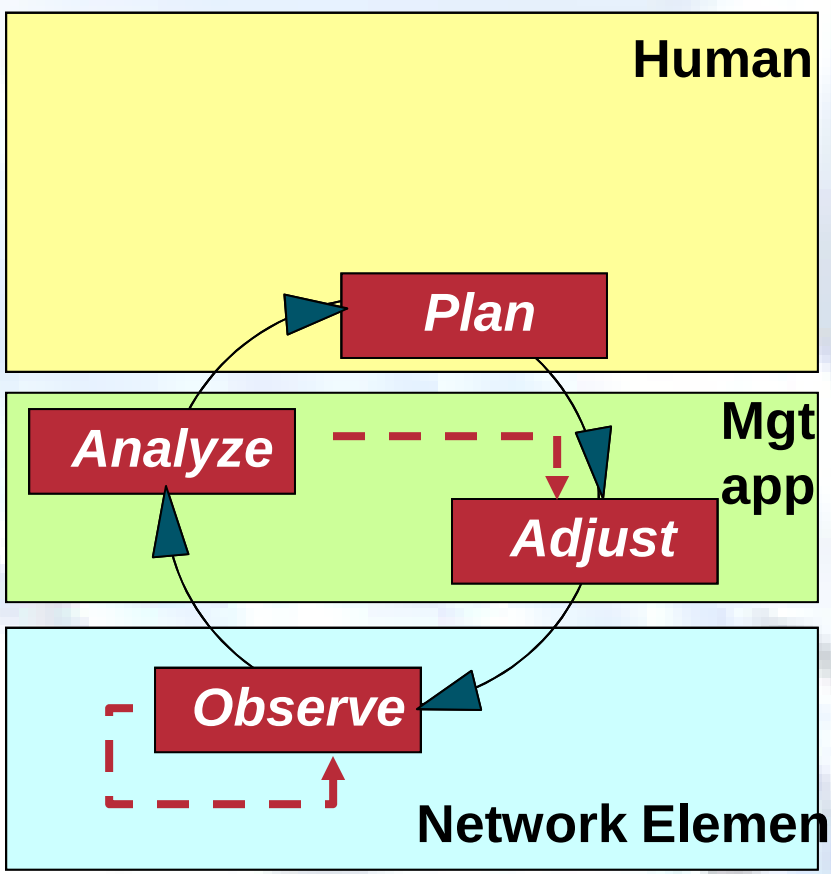
Evolution of Network Manageability

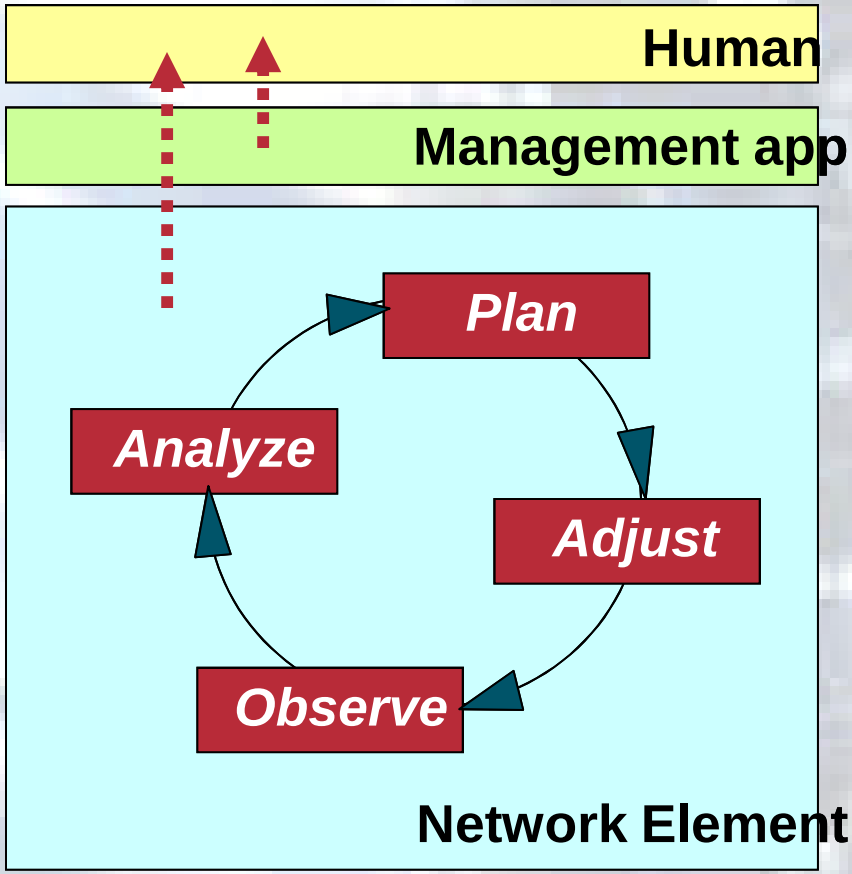


Evolution of Network Smartness



Autonomic Computing





(a) Typical management control loop

(b) Closed management control loop in autonomous network

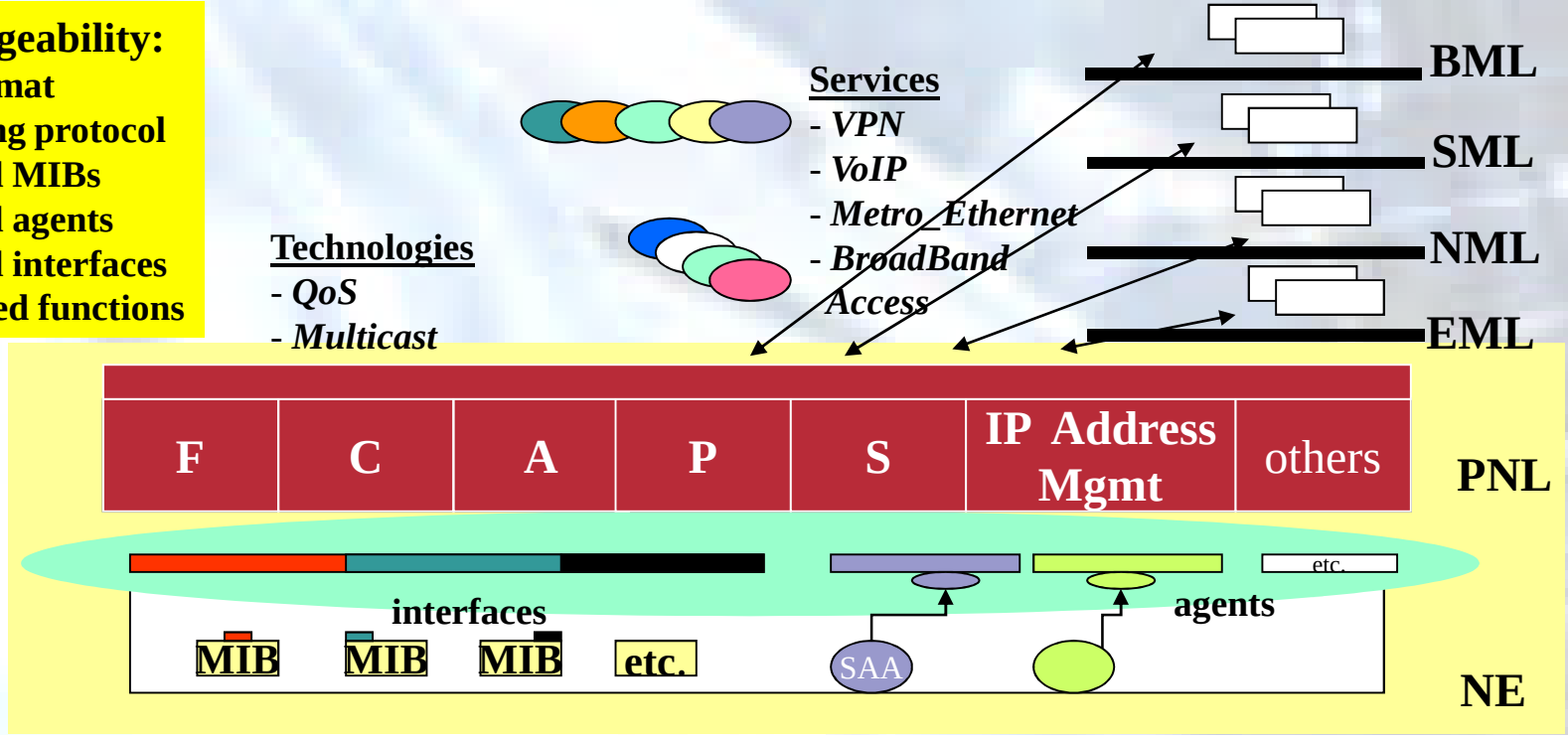
Challenging Issues

Too Many

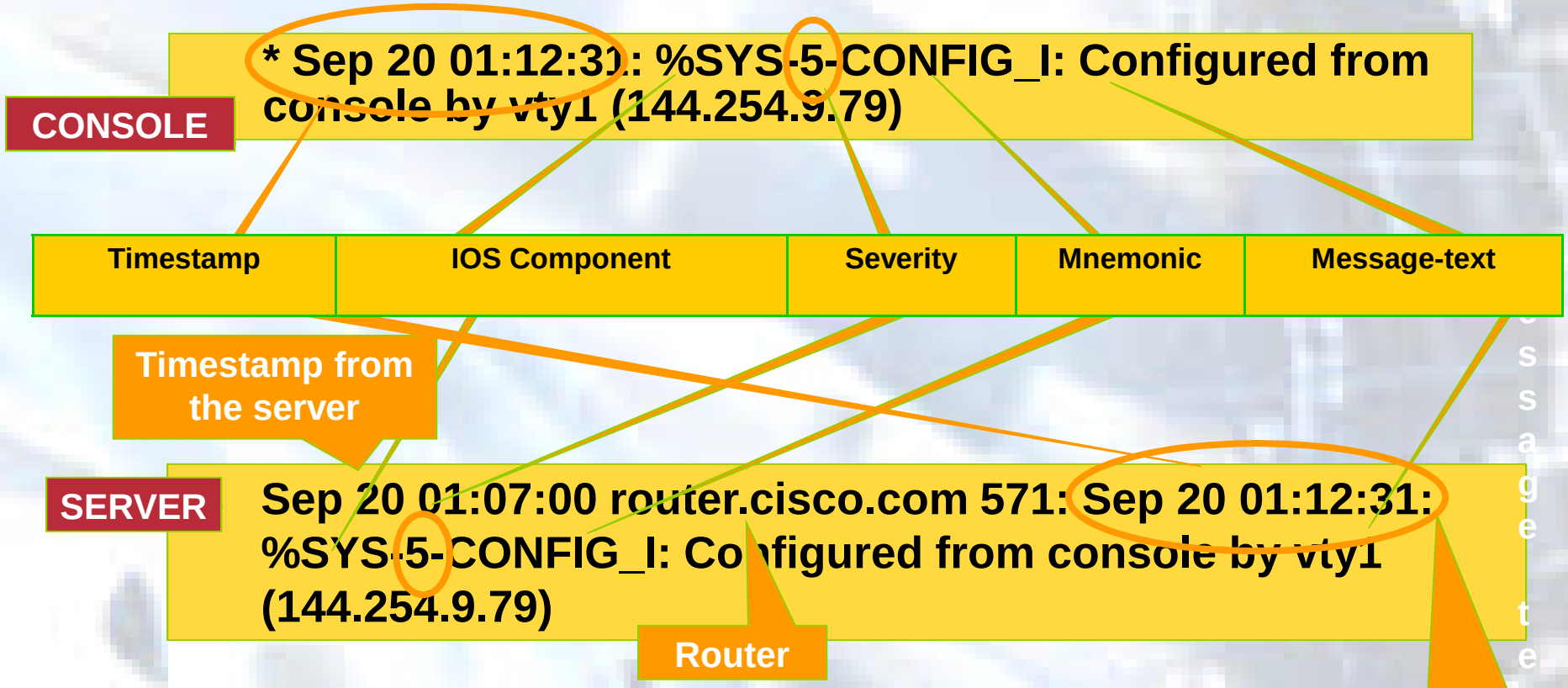
Syntax Issues

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

NE Manageability:
- ? data format
- ? conveying protocol
- ? required MIBs
- ? required agents
- ? required interfaces
- ? embedded functions



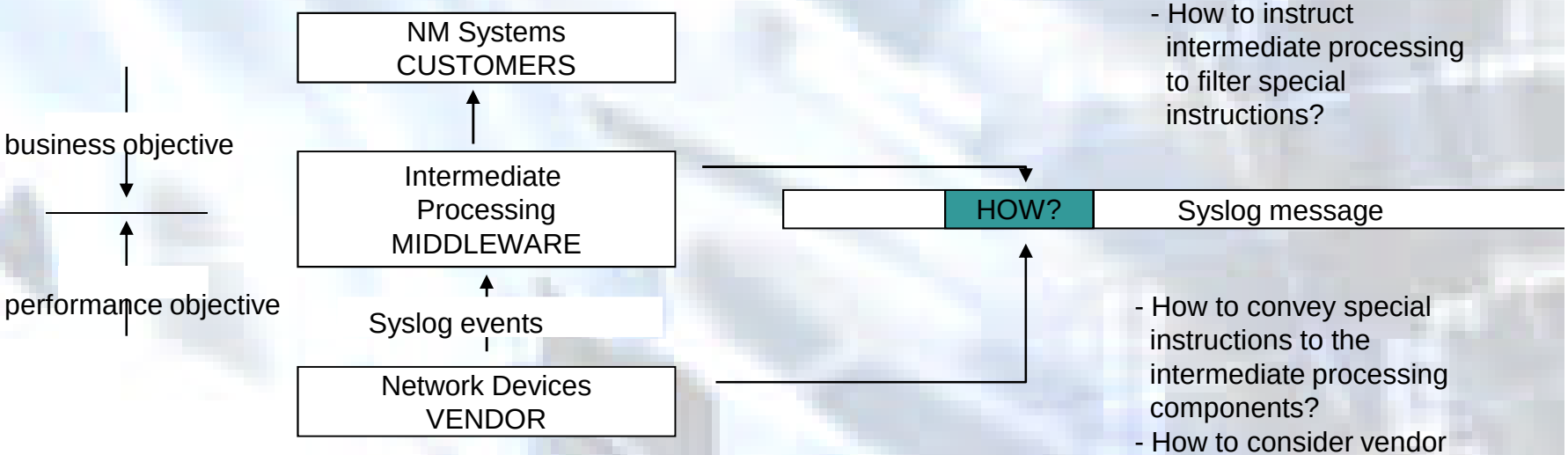
Syslog Message "Body" Format in the IOS



- NTP is needed!
- Header:level can be different than Body:severity

Semantic Issues

- **Naming**
- **Context-defined**
- **Smart events**



XML Tagging is Not Enough

% *versus* <XML>

: <<<a><b>><c>>

: (((a)(b)c))

1. <a> <b> <c>
   ? ? ?
2. <<a> --- r1 -- <b>> -- r2 -- <c>
   ? ?

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

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

?
Tag relationships

?
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.

Timestamps issues

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

Adding Security to Event Transport

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

Putting and End to Unreliability

- Reliable transport mechanism
- Partially reliable transport [weak link]

- ?

  - event itself [seq numbers]-based

  - window-based

  - context-based

Example: Syslog

[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

- 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]

Still to answer…

- 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 event-related requirements is MPLS OAM and all aspects related to MPLS VPN.

Network Management Technology Group