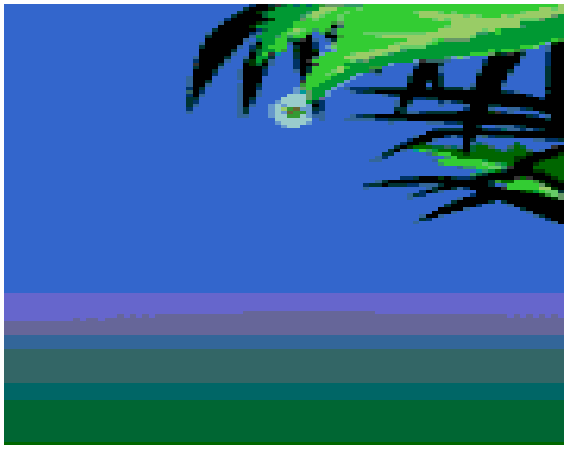
Root Cause Analysis

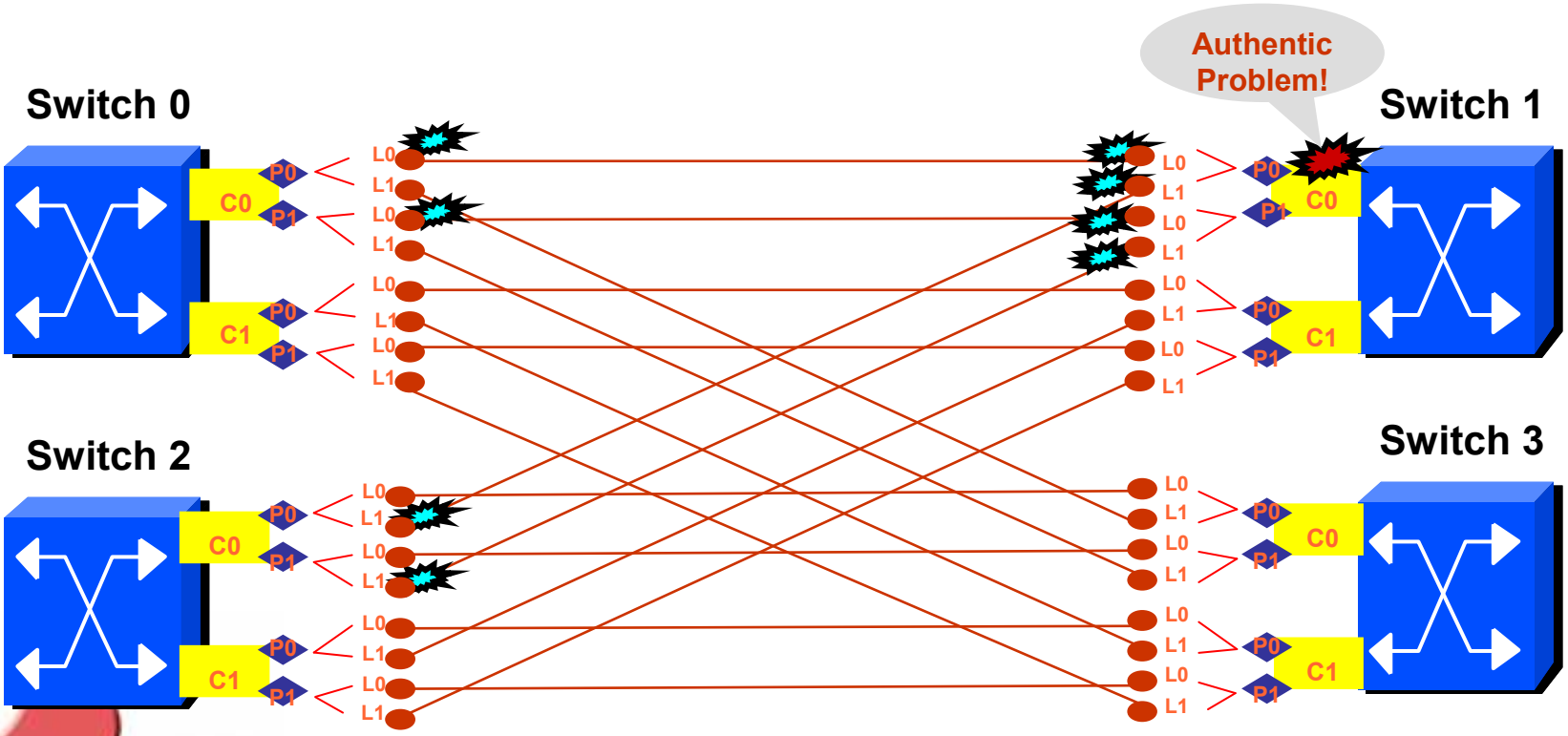
What you always wanted to know but were too afraid to ask

Dr Yuri Rabover
EMC Smarts

In Search of Root Cause….



Problem Scenario



RCA Challenges

- Problems can start in any logical or physical object in the network, attached systems, or applications.
- A single problem often causes many symptoms in many related objects.
- The absence of particular symptoms is as meaningful as the presence of particular symptoms.
- Different problems can cause many overlapping symptoms. For example, the operationally down status of logical port 0 over physical port 1 in Card 0 of Switch 1 could be caused by a failure in any one of the following components:
  - Switch 1
    - Switch 1 Card 0
    - Switch 1 Card 0 Port 1
    - Switch 1 Card 0 Port 1 Logical Port 1
  - Switch 2
    - Switch 2 Card 0
    - Switch 2 Card 0 Port 1
    - Switch 2 Card 0 Port 1 Logical Port 1
  - The trunk connecting Port 1 in Card 0 in Switch 1 with Port 1 in Card 0 in Switch 2.

RCA Challenges – cont.

- Symptoms can propagate across related components. In our example, a symptom propagated from a card to its ports and from a port to a peer port. This makes it necessary to examine *all the symptoms* across related elements in order to identify the root cause.
- Problems are not always observable in the object where they originate. For example, if the switch does not generate card failure traps, the card failure would have no direct (local) symptoms.
- Problems can occur in objects that do not generate any observable events. For example, there is no event and/or trap associated with a trunk.

Conventional approach – write rules

"If all the logical ports that are layered over the physical ports in S1C0 report as operationally down, and all the logical ports that are their peers in connected switches also report as operationally down, then the S1C0 failure is the root-cause problem generating all these symptoms."

IF
S1C0P0L0 *down* **AND**
S1C0P0L1 *down* **AND**
S1C0P1L0 *down* **AND**
S1C0P1L1 *down* **AND**
S0C0P0L0 *down* **AND**
S0C0P1L0 *down* **AND**
S2C0P0L1 *down* **AND**
S2C0P1L1 *down*
THEN CONCLUDE S1C0 *failure*

What's Missing?

Display

No built-in analysis — ongoing rules-writing required

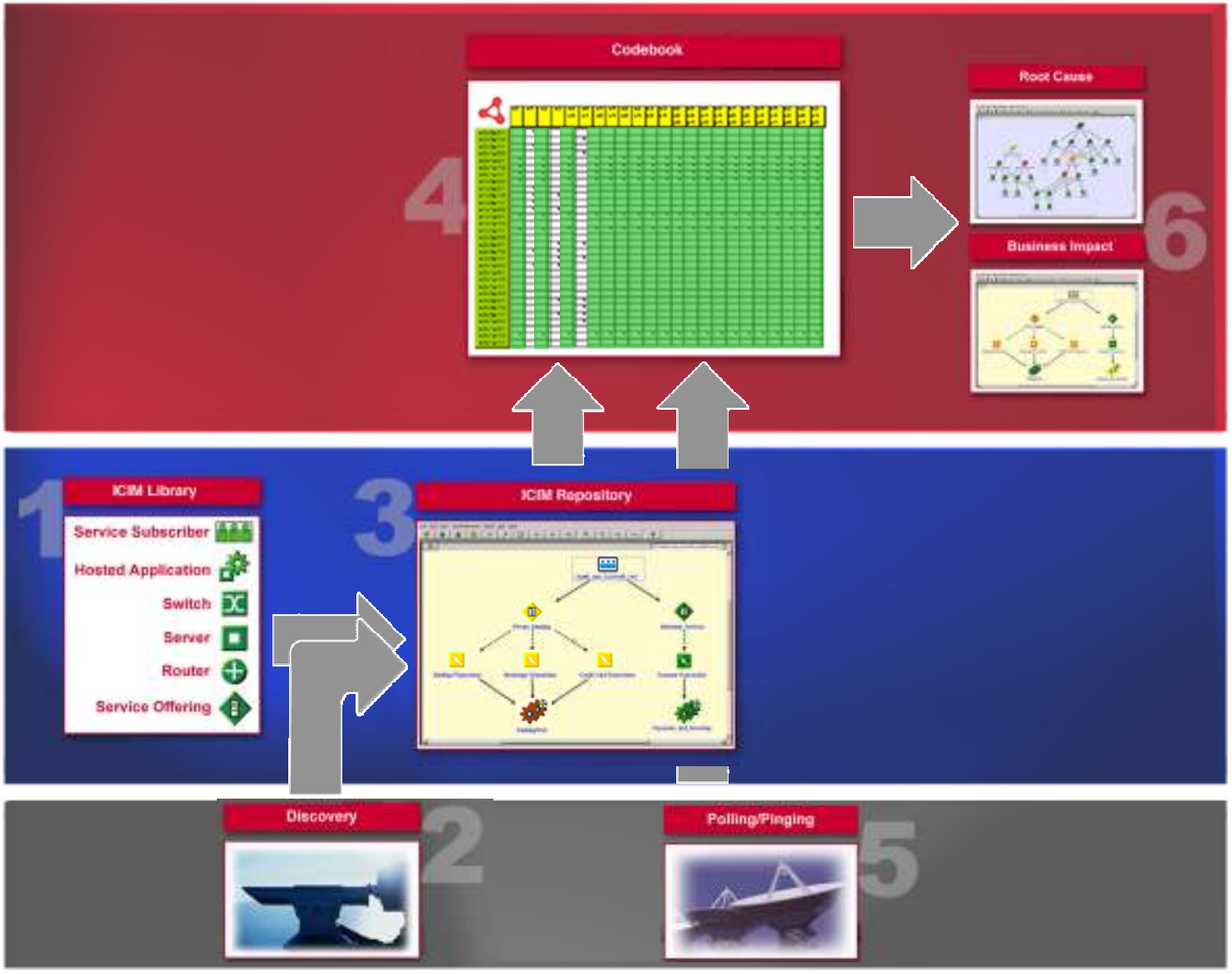
Data & Event Collection

How SMARTS works

Analysis

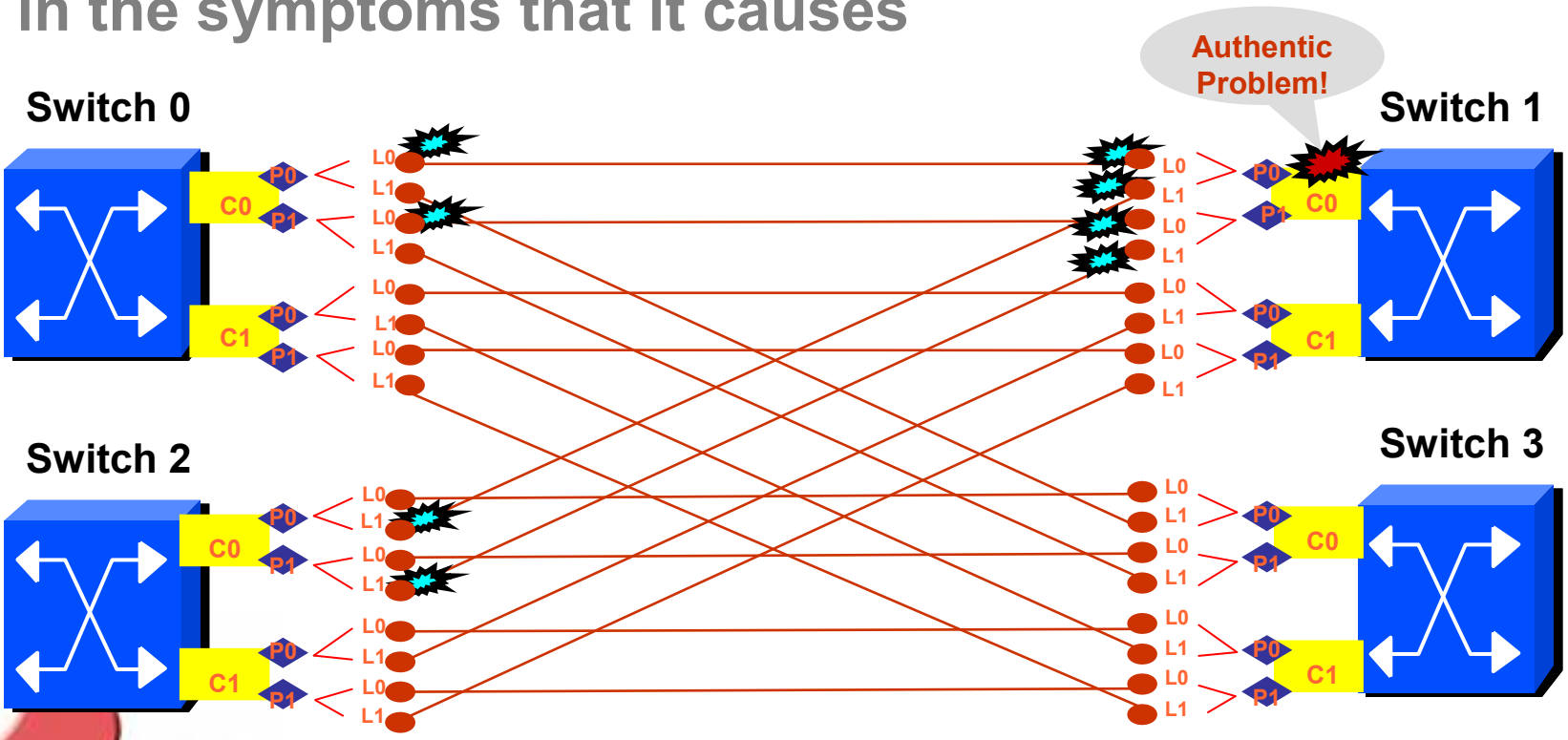
Context

Collection



Problem Signatures

Each instance of problem has a unique *signature* in the symptoms that it causes



Codebook

Problems

Symptoms

	s0	s1	s2	s3	s0 c0	s0 c1	s1 c0	s1 c1	s2 c0	s2 c1	s3 c0	s3 c1	s0 c0 p0	s0 c0 p1	s0 c1 p0	s0 c1 p1	s1 c0 p0	s1 c0 p1	s1 c1 p0	s1 c1 p1	s2 c0 p0	s2 c0 p1	s2 c1 p0	s2 c1 p1	s3 c0 p0	s3 c0 p1	s3 c1 p0	s3 c1 p1	
s0c0p0l0		1			1		1						1				1												1
s0c0p0l1					1						1		1												1				1
s0c0p1l0		1			1		1							1				1											1
s0c0p1l1					1						1			1												1			1
s0c1p0l0		1				1		1							1				1										
s0c1p0l1						1						1			1												1		
s0c1p1l0		1				1		1								1				1									
s0c1p1l1						1						1				1													1
s1c0p0l0	1				1		1						1				1												1
s1c0p0l1			1				1		1								1				1								
s1c0p1l0	1				1		1							1				1											1
s1c0p1l1			1				1		1									1				1							
s1c1p0l0	1					1		1							1				1										
s1c1p0l1			1					1		1									1				1						
s1c1p1l0	1					1		1								1				1									
s1c1p1l1			1					1		1										1				1					
s2c0p0l0									1		1										1				1				
s2c0p0l1		1					1		1								1				1								
s2c0p1l0									1		1											1				1			
s2c0p1l1		1					1		1									1				1							
s2c1p0l0										1		1											1				1		
s2c1p0l1		1						1		1													1						
s2c1p1l0										1		1												1					1
s2c1p1l1		1						1		1										1				1					
s3c0p0l0			1						1		1										1				1				
s3c0p0l1	1				1						1		1												1				1
s3c0p1l0			1						1		1											1				1			
s3c0p1l1	1				1						1			1												1			1
s3c1p0l0			1							1		1											1				1		
s3c1p0l1	1					1						1			1												1		
s3c1p1l0			1							1		1												1				1	1
s3c1p1l1	1					1						1				1												1	1

Application Logic

Logical Port

Problem *Down* Causes *OperationallyDown, ConnectedPortDown*

Local symptom *OperationallyDown*

Propagated symptom *ConnectedPortDown* **To** *Connected Logical Ports Down*

Physical Port

Problem *Down* Causes *PortDown*

Propagated symptom *PortDown* **To** *Logical Ports Layered over the Port are Down*

Propagated symptom *ConnectedPortDown* **To** *Layered over Logical Ports*

Card

Problem *Down* Causes *PortDown*

Propagated symptom *PortDown* **To** *Physical Ports in the Card are Down*

Propagated symptom *ConnectedPortDown* **To** *Physical Ports in the Card*

Switch

Problem *Down* Causes *ConnectedPortDown*

Propagated symptom *ConnectedPortDown* **To** *Cards in the Switch*

Application Logic

Network Device

Problem ***Congested*** **Causes** Degradation

Propagated symptom Degradation **To** Layered over Sessions are Degraded

Session

Problem ***Degraded*** **Causes** DegradedService

Propagated symptom DegradedService **To** ConnectedTo Applications are Slow

Application

Problem ***Slow*** **Causes** SlowResponseTime, DegradedService

Event SlowResponseTime

Propagated symptom DegratedService **To** Layered over Services Degraded

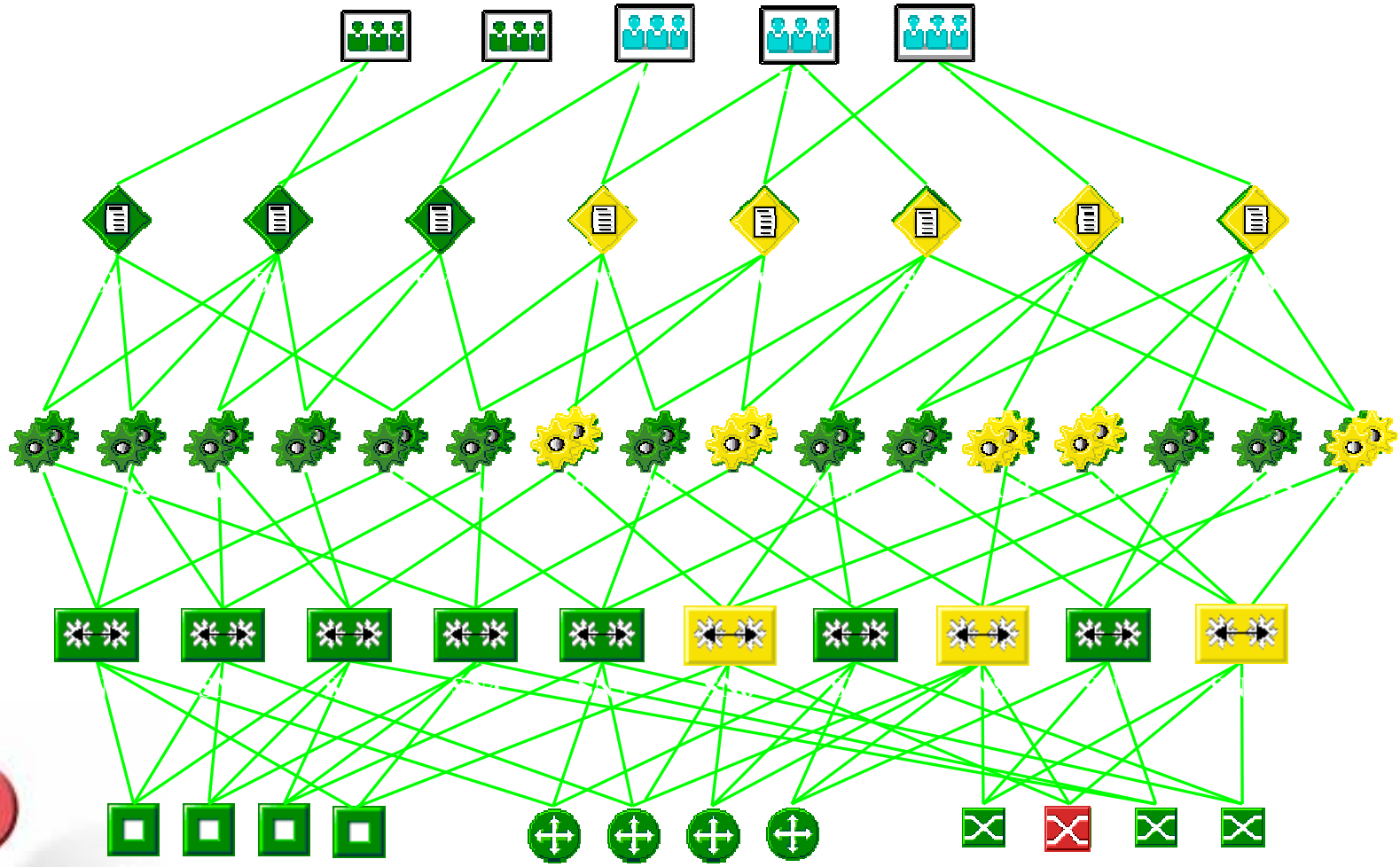
Service

Problem ***Degraded*** **Causes** SlowTransaction, Impact

Event SlowTransaction

Propagated symptom Impact **To** Subscribed Users

Authentic Problem Signature



Codebook

Problems

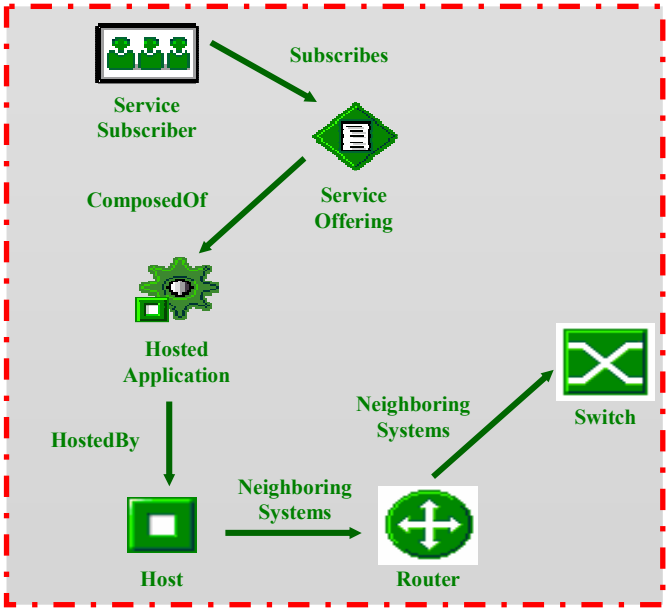
Symptoms

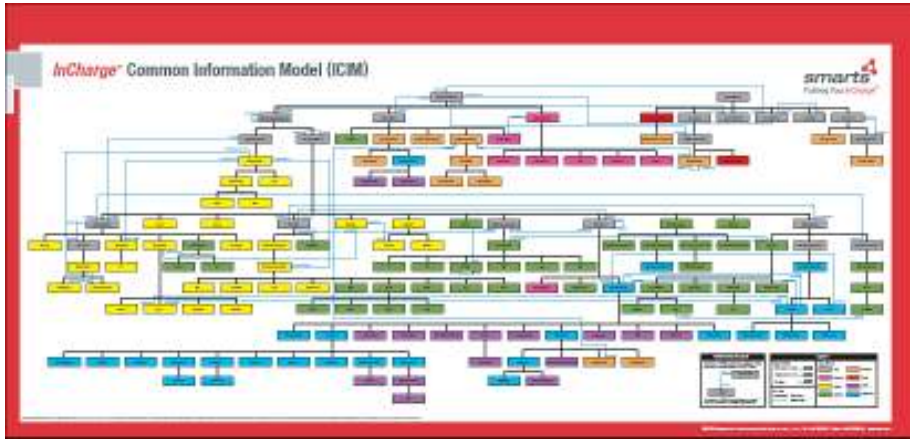
		HH1	HH2	HH3	HH4	RR1	RR2	RR3	RR4	SS1	SS2	SS3	SS4	SSN1	SSN2	SSN3	SSN4	SSN5	SSN6	SSN7	SSN8	SSN9	SSN10	AA1	AA2	AA3	AA4	AA5	AA6	AA7	AA8	AA9	AA10	AA11	AA12	AA13	AA14	AA15	AA16	SSV1	SSV2	SSV3	SSV4	SSV5	SSV6	SSV7	SSV8	
		Cong	Cong	Cong	Cong	Cong	Cong	Cong	Cong	Cong	Cong	Cong	Cong	Degr	Degr	Degr	Degr	Degr	Degr	Degr	Degr	Degr	Degr	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Slow	Degr	Degr	Degr	Degr	Degr	Degr	Degr	Degr	
A1	SRT	1	1	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A2	SRT	1	1	0	1	1	1	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A3	SRT	1	1	1	0	0	1	0	0	0	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A4	SRT	1	1	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A5	SRT	1	0	1	0	1	1	0	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A6	SRT	1	1	1	1	0	1	0	0	0	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A7	SRT	1	1	1	1	0	0	1	0	0	1	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A8	SRT	0	0	1	0	1	1	1	1	0	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A9	SRT	0	1	1	0	0	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A10	SRT	0	0	0	1	1	0	1	1	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A11	SRT	0	0	1	0	1	1	0	1	1	0	1	1	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
A12	SRT	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
A13	SRT	0	0	0	1	0	0	1	0	1	1	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
A14	SRT	0	0	0	0	1	0	1	1	1	0	1	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
A15	SRT	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
A16	SRT	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
SV1	ST	1	1	1	1	1	1	0	0	0	0	1	1	1	1	0	1	1	0	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
SV2	ST	1	1	1	1	1	1	0	0	0	0	1	0	1	1	1	1	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
SV3	ST	1	1	1	1	0	1	0	0	0	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
SV4	ST	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
SV5	ST	1	1	1	1	0	1	1	1	1	1	1	0	0	1	1	1	0	1	0	1	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
SV6	ST	0	1	1	1	1	1	1	1	1	1	1	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0
SV7	ST	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0
SV8	ST	0	0	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1

0
0
0
0
0
1
0
1
1
0
1
1
0
0
1
0
0
1
1
1
1

ICIM: The InCharge Common Information Model

- Based on DMTF CIM, extended with rich semantics for integrating and automating management applications
- Comprehensive
  - Models network, systems, applications, services, business entities
  - 100+ classes, 50+ relationships
  - Infinitely extensible via inheritance
- Models the complex web of relationships in the real world:
  - Within entities, across entities
- Models cross-domain relationships
  - Key to service management, end-to-end view
  - Pieces together information from heterogeneous sources
- Abstract
  - To scale to networks of unlimited size and complexity through multiple levels of abstraction
  - To decouple management application logic from the specifics of an ever-increasing stream of vendor products
- Efficient
- Open

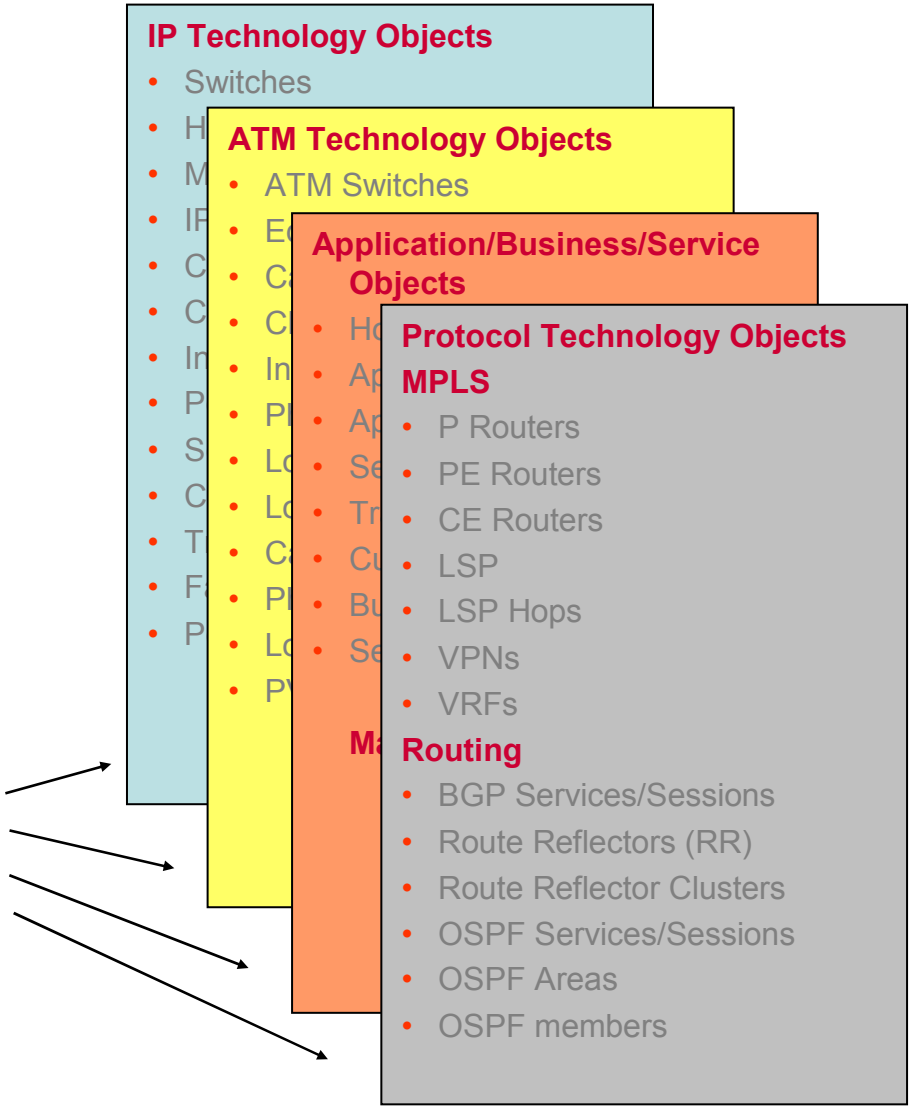




ICIM: The InCharge Common Information Model

- **Attributes**
  - Stored or instrumented – this is transparent to applications
- **Relationships**
  - 1-1, 1-many, many-1, many-many
- **Behaviors**
  - Specific extensions for each type of FCAPS application, e.g., problems for fault, constraints for configuration
- **Constraints**
  - Assure consistency of assigned values, e.g., speed match at both end of a circuit
- **MODEL: Managed Object DEfinition Language**
  - Based on CORBA IDL syntax

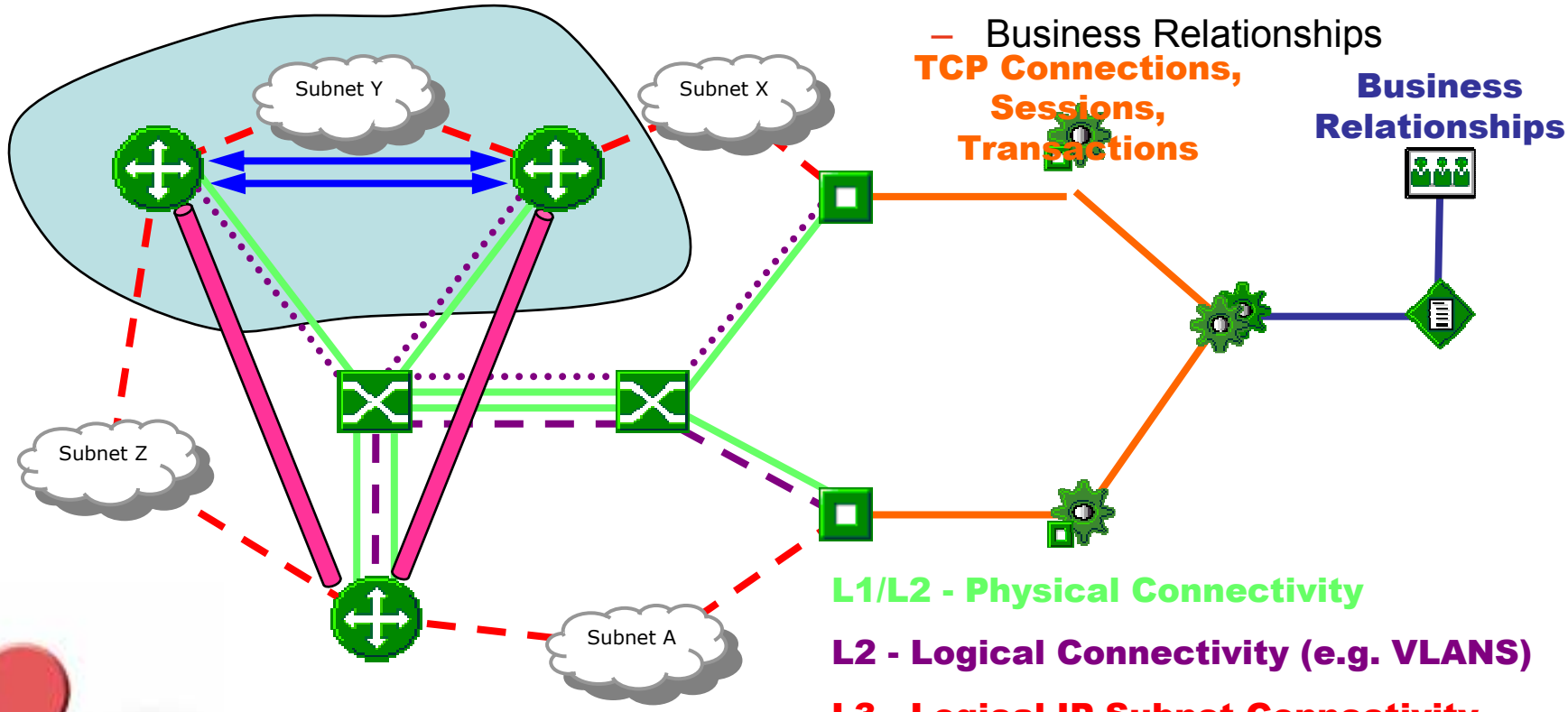
Relationship Types
- ConnectedVia/ConnectedTo
- ParentOf/ChildOf
- LayeredOver/Underlying
- SwappedFrom/SwappedTo
- NextHop/PreviousHop
- ImportedBy/Import



InCharge Common Information Model

Multi-Layered Relationships

- Intra-Domain Relationships
- Inter-Domain Relationships
- Business Relationships



L1/L2 - Physical Connectivity

L2 - Logical Connectivity (e.g. VLANS)

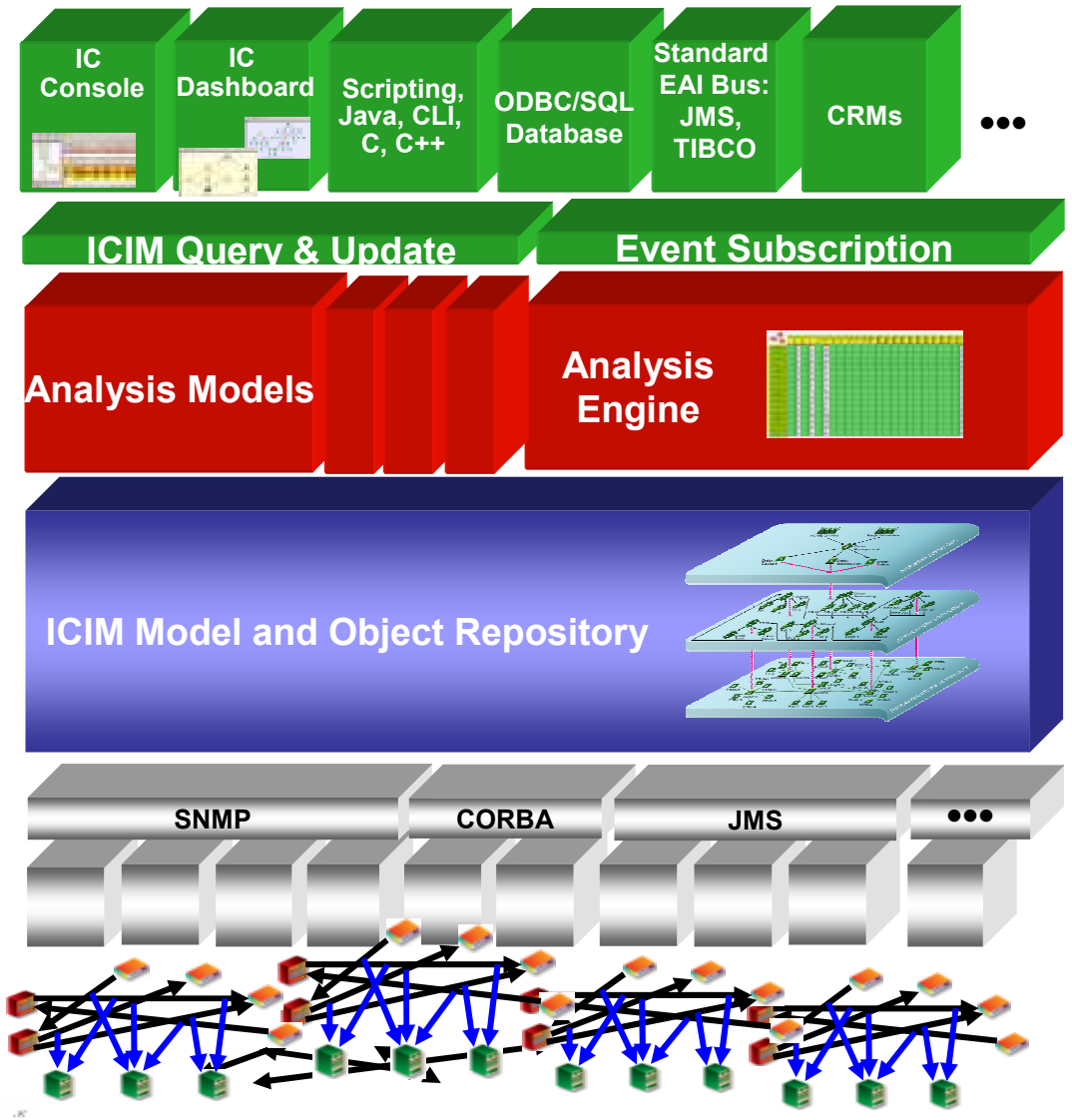
L3 - Logical IP-Subnet Connectivity

- MPLS LSP/LSP Hop/VFR/VPN

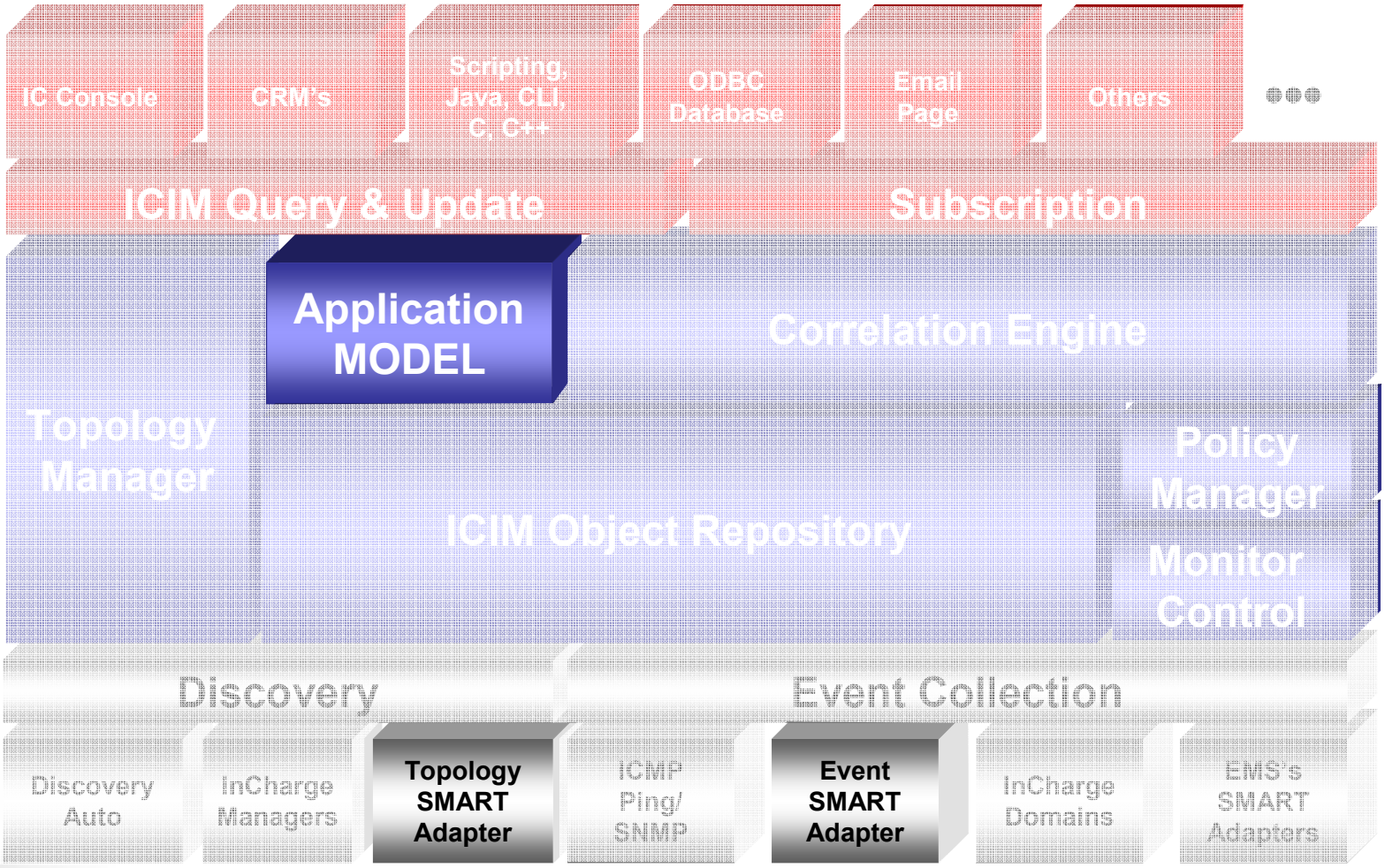
- OSPF/BGP Areas/Adjacencies

SMARTS InCharge Architecture

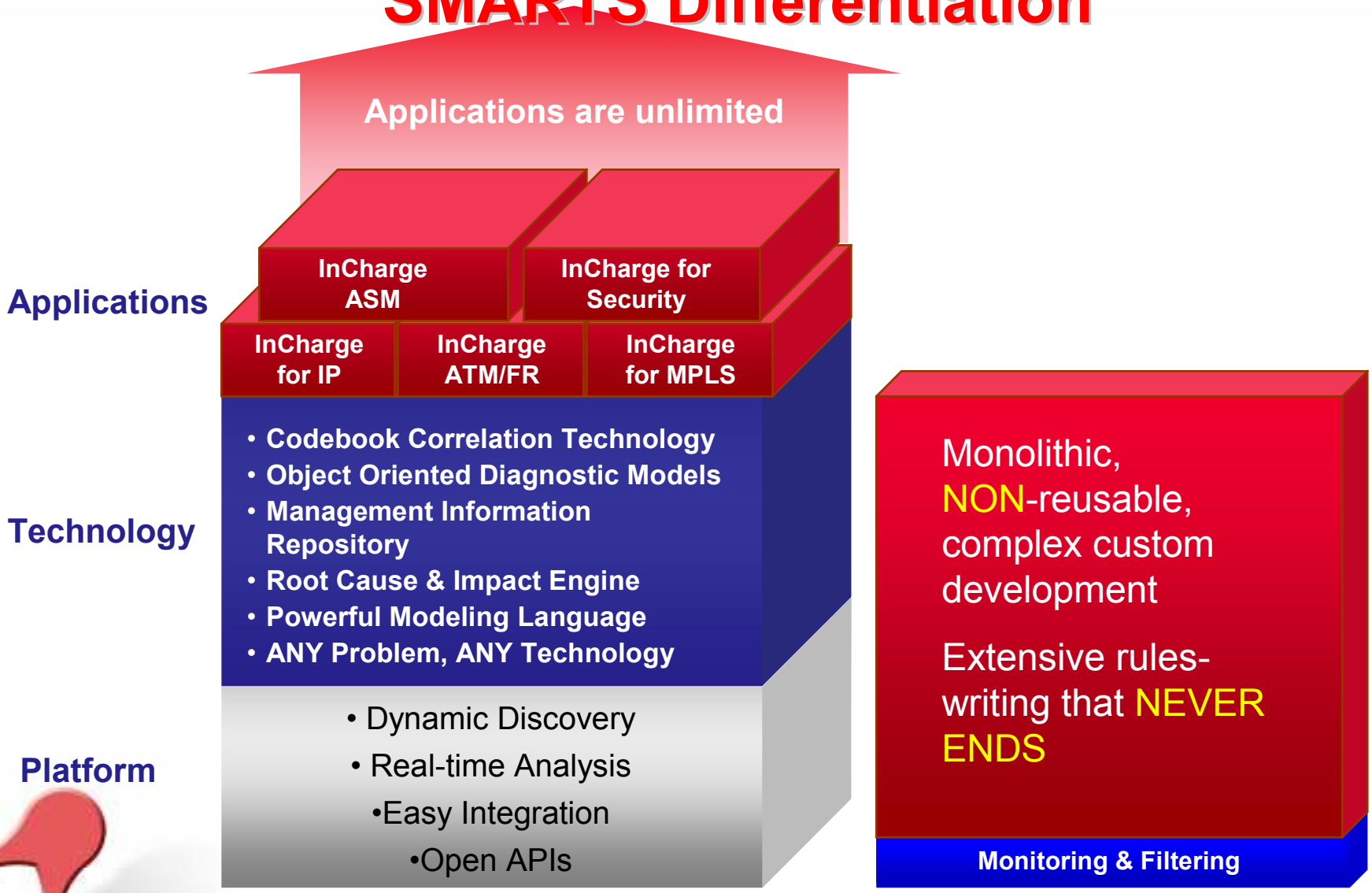
- InCharge Common Information Model
  - Unified data model
  - Rich – 50+ relationships
- InCharge automation engines:
  - Codebook Correlation Technology
- Auto - Discovery
  - Populate topology through mediation layer
  - De-coupled from ICIM and analysis
- Automatic adaptation to change
- Recursive distributed architecture
- Open extensible architecture
  - De-coupling of layers
  - Open-ended import/export APIs
  - Incremental product support
  - Add new classes and new automation engines



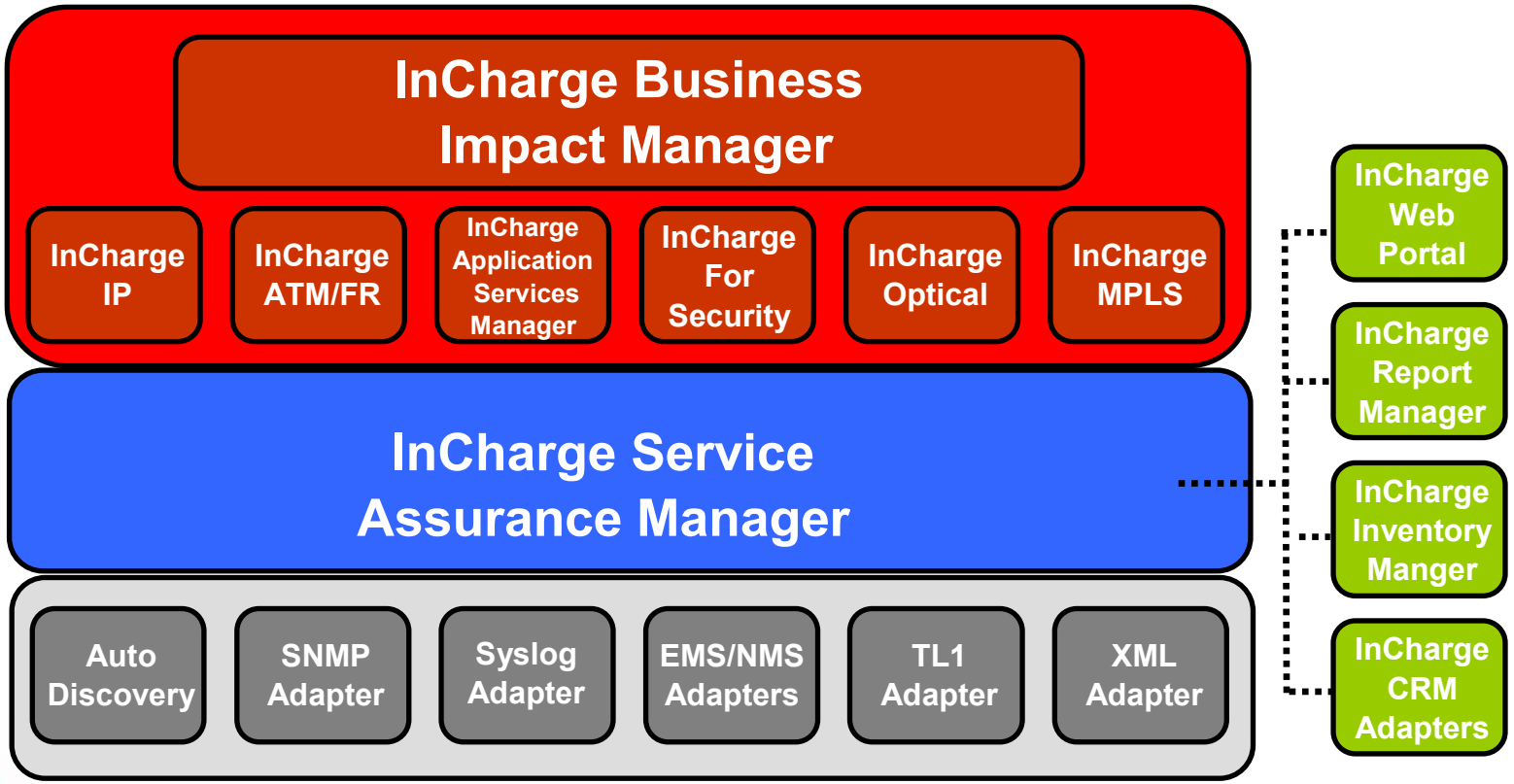
InCharge Architecture



SMARTS Differentiation



InCharge Solutions Architecture



Thank You!

Questions, Comments, Suggestions?