Management of Dynamic Networks and Services
Correlation-Based Solutions

Gabriel Jakobson

DSOM 2001
October 15, 2001
Nancy, France

Introduction: Some Thoughts About Dynamics and Intelligence
(hopefully relevant to network and services management)

- The Dynamic, Dynamic, Dynamic World
- How Much Intelligence We Need?

What Makes Systems Dynamic?

Dynamic System:

- Changes its Entity (parameters, configuration, states, etc.)
- Consumes (and Redistributes) Resources
- Interacts with the World

Living (Biological) System:

- Has a Lifecycle (Note: Lifespan for Events!)
- And Reproduction Capability (Note: Reproduction of Abstract Automata,…and Machine Learning!)

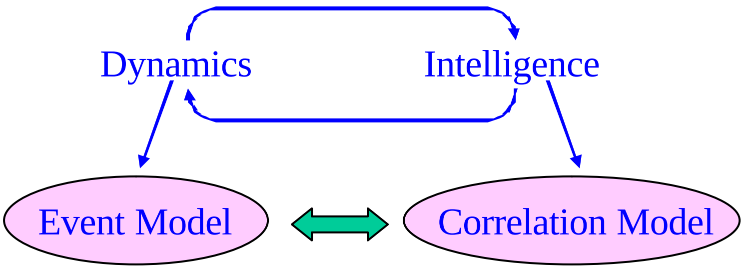
What Makes Things Intelligent?

Intelligent System:

- Reflects (Interprets, Models) the World
- Organizes its Behavior (For survival and Achieving Goals)
- Learns (Discovers, Improves Skills)
- Communicates (with others; forms collectives, federations, cooperations under different organizational paradigms)
- Explains its Behavior (Results)

Synergy Between System Dynamics and Intelligence

- Dynamics is Pre-Requisite for Intelligence
- Intelligence Gives Dynamics Purposeful Behavior



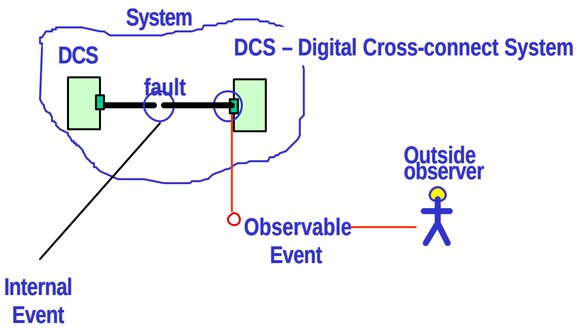
From Static Convenience To Dynamic Reality

- Many aspects of dynamic systems are often perceived as static
- "Living" in the real dynamic world, the systems are subjects for many internal dynamic transformations, such as:
  - changing the system internal states
  - dynamic system re-configuration
  - changes in the functionality of the nodes
  - transformations of link semantics
  - dynamic adjustment of behavioral goals and agreements
  - on-fly selection of system optimization criteria
  - dynamic re-specification of system interfaces
- Observation of these system aspects as dynamic entities, could lead to more adequate modeling of reality with significant rewards

Dynamic Systems: Basic Notions

- State - a set of system parameter values
- Dynamic System - a system, which changes its states over time
- Fault - a state with pre-defined abnormal parameter values
- Event – an act of transition of a system from state to state
- Informational Event - manifestation of an event via time-stamped piece of information
- Alarm – an informational event; external manifestation of a fault

System Internal Events and Observable External (Informational) Events



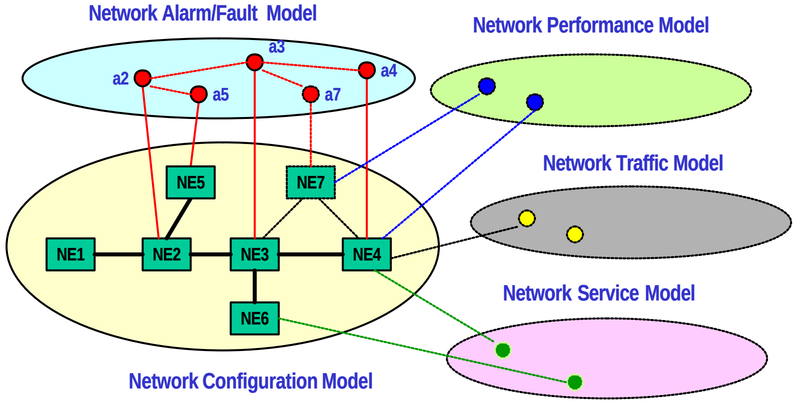
Event Types

- Event types by their source of origin
  - Base events - external events originated outside the correlation process
  - Derived events - events generated by the correlation process
- Event types by their function
  - Fault alarms
  - Clear messages
  - Status messages
  - Clock events
- Event types by their method of origination
  - Natural events, i. e. equipment faults
  - Artificial events, i.e performance events

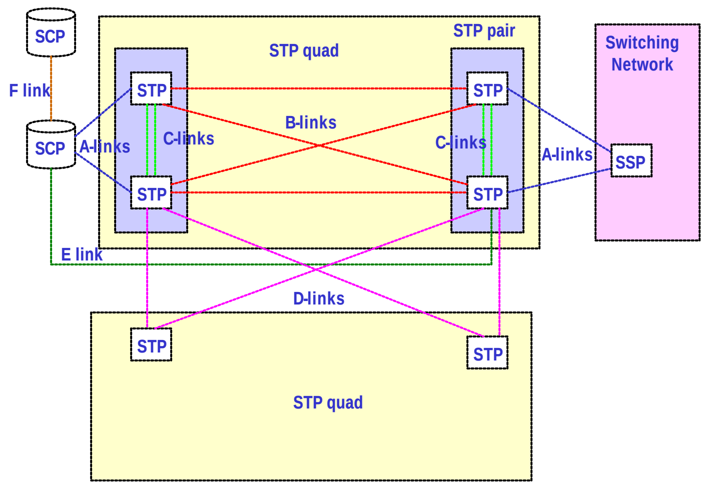
Dynamic Networks

- Traditionally network topology is considered as a static component in network management tasks
- Models of dynamic networks
  - Dynamically re-configurable networks
  - Active (programmable) networks
  - Dynamic VPN
  - Network updates during the management process
  - Mobile and survivable defense networks
  - Reconfigurable cellular networks (e.g. dynamic channel allocation)
- Dynamic network topology models
  - Real-time construction of network topology models

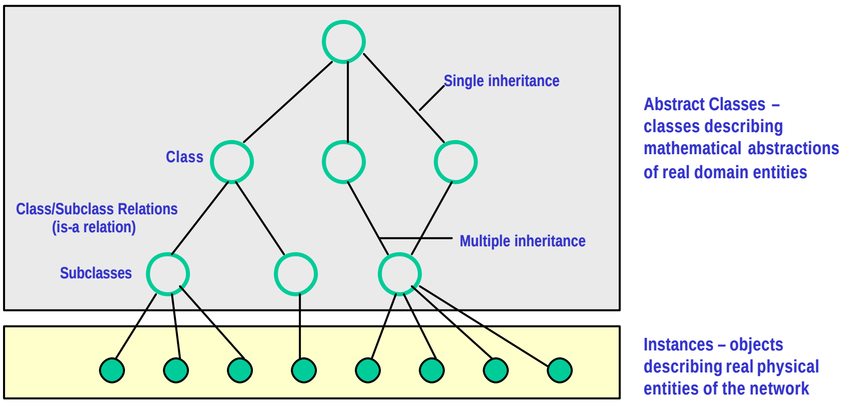
Dynamic Network Modeling



Network Topology: Signaling Network



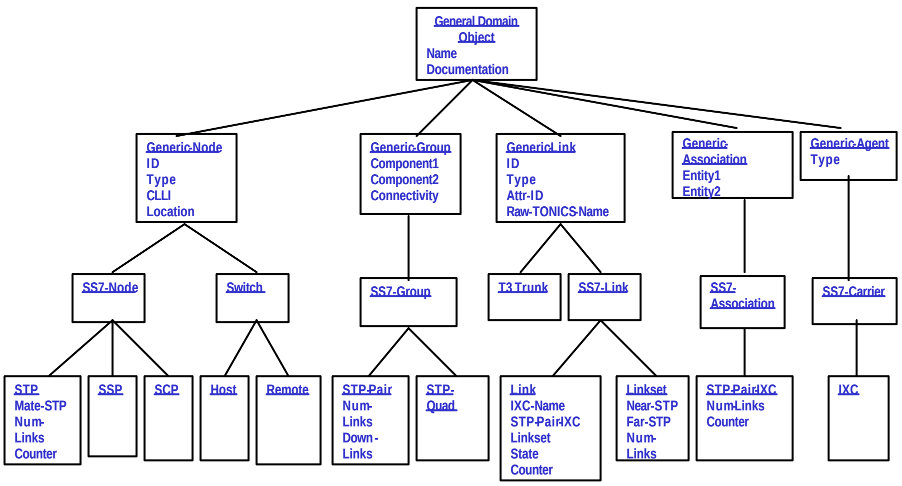
Network Topology: Domain Class Hierarchy



Network Topology Elements

- Network Element (NE) class specifications
  - Name
  - Type
  - Parents, children
  - CLLI code
  - Etc.
- NE instances descriptions
- Inter-NE relations
  - Class relations (is-a relations)
  - Connectivity relations
  - Containment relations
  - Part-of relations
  - Other domain-specific relations

NE Class Hierarchy: Example



Domain Classes:Examples

Generic-Domain-Object
- Parent
  - Basic-NE
- Children
  - Generic-Node
  - Generic-Group
  - Generic-Link
  - Generic-Association
  - Generic-Agent
- Attributes
  - Name
  - Documentation
- Methods

Generic-Node
- Parent
  - Generic-Domain-Object
- Children
  - SS7-Node
  - Switch
- Attributes
  - ID
  - Type
  - CLLI
  - Location

SS7-Node
- Parent
  - Generic-Node
- Children
  - STP
  - SSP
  - SCP
- Attributes

STP-Node
- Parent
  - SS7-Node
- Attributes
  - Mate-STP-CLLI
  - Num-Links
- Methods
  - GetNumLinks
  - SetNumLinks

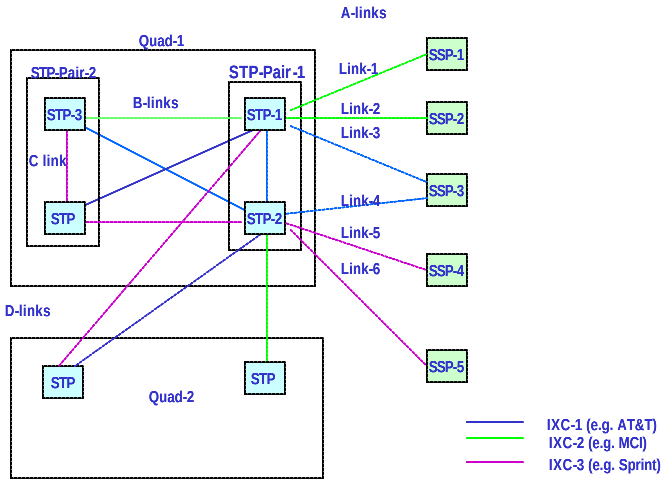
STP Class Specification in XML: Example

```
<DomainClass Name="STP-Node" Documentation="A class describing all STPs">
   <DomainClassParents>
       <DomainClassLink Name="Generic-Node"/>
   </DomainClassParents>
   <DomainClassSlots>
      <DCStringSlot Name="Mate-STP-CLLI"/>
      <DCIntegerSlot Name="Num-Links"/>
   </DomainClassSlots>
</DomainClass>
```

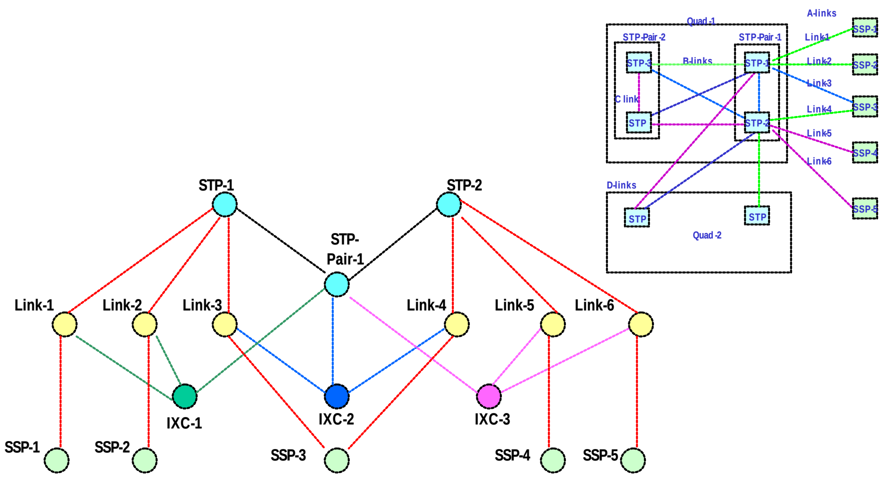
STP Object Specification in XML: Example

```
<DomainObject
     Name="dovrpaxd01w"
     Documentation="Description of the STP in Dover PA"
>
<Class>
     <DomainClassLink Name="STP-Node"/>
</Class>
<DomainObjectSlots>
     <DOSlot Name="ID" Value="1845888455"/>
     <DOSlot Name="NE-CLLI" Value="dovrpaxd01w"/>
     <DOSlot Name="NE-Name" Value="DOVER STP"/>
     <DOSlot Name="NE-Type" Value="dscstp"/>
     <DOSlot Name="Location" Value="Dover, PA"/>
     <DOSlot Name="Mate-STP" Value="yorkpaxm02w"/>
     <DOSlot Name="Num-Links" Value="9"/>
</DomainObjectSlots>
</DomainObject>
```

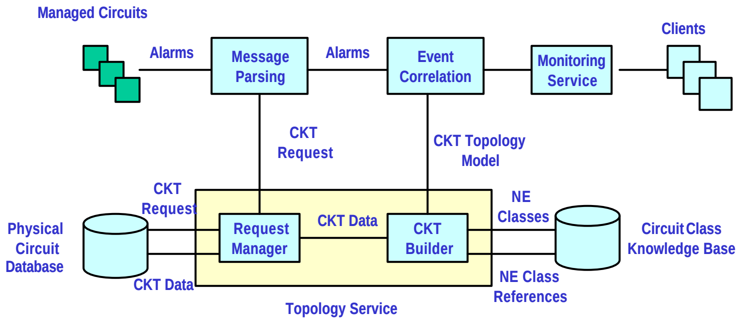
SS7 Network: A Fragment



Example: Fragment of a SS7 Network Topology Model



Dynamic Circuit Topology Building



Management of Dynamic IP Services

- Monitoring (in real-time) of services, SLAs, resources, and QoS is becoming a critical aspect of successful service provisioning
- Any fault or degradation of the network may result in violation of the SLAs or even halt the requested service
- Dynamic aspects of service management may include:
- - On-the-fly changes in service definitions
- - Dynamic re-specification of SLAs
- - Changes in resources
- - Requests for rapid near real-time deployment of new
- services

What is Event Correlation?

- Event Correlation is a real-time event analysis procedure, which, by using event pattern matching rules, assigns a new meaning to the events
- It is a critical process enabling the real-time fault diagnosis of complex networks and services
- It is Artificial Intelligence and Expert Systems technology based software, which is part of general Network/Service Management OSS

The Dual Role Of Event Correlation

- The traditional role of event correlation is to answer to the question: What did go wrong with the network?
- The new emerging role of event correlation is to answer to the question: How do understand the network situation?

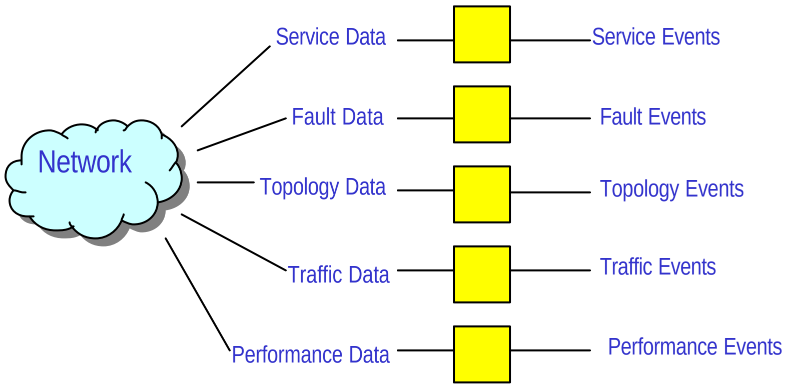
The Role of Time in Event Correlation

- Models of time
  - Interval
  - Point time
  - Event duration and lifespan
- Temporal aspects of event correlation
  - Temporal constrains
  - Temporal reasoning
- (Hard) real time processing
  - Synchronous and asynchronous events
  - Performance
- Natural delays, event masking, event racing, non-deterministic system behavior

Examples of Time –Dependent Correlation Functions

- Monitoring of Event Lifespan
  - For garbage collection purpose
  - For taking account of domain-specific event duration, e.g. “generator
    provides power for 2 hours (until fuel lasts)”
- Managing Correlation Time Window
  - E.g. “correlate 3 alarms during 5 seconds”
- Scheduling Time Dependent Actions
- Managing Time Relations Between Events

Event Sources



Generalized Event Correlation Model

- Generalized (Abstract) Event Model

$$e = < dS, t>, \; e \in E; \; t \in T, \; T = \{0, 1, 2, 3, \ldots \}$$

e - event, E - set of all events, dS - system state change, T - time

- Generalized (Abstract) Event Correlation Model

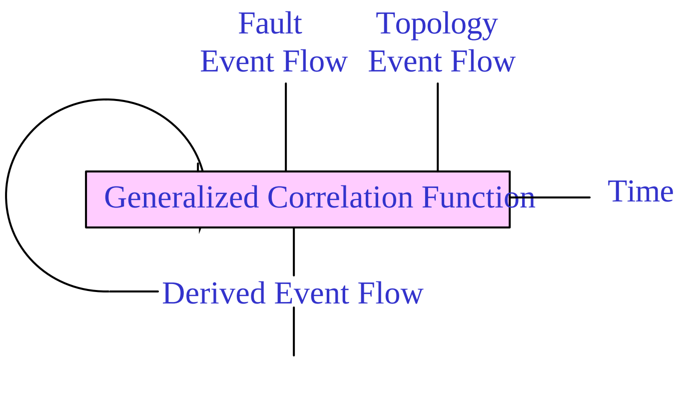
$$S = (E, CF), \quad CF: E^{*} \times T — E$$

CF – correlation function, E^{*} - set of all subsets of E

Generalized Event Correlation Model (cont.)

- Generalized event is mathematical abstraction of specific event types, such as
  - Topology events
  - Performance events
  - Service events
  - Traffic events
  - Fault events

Generalized Correlation Model (Cont.)



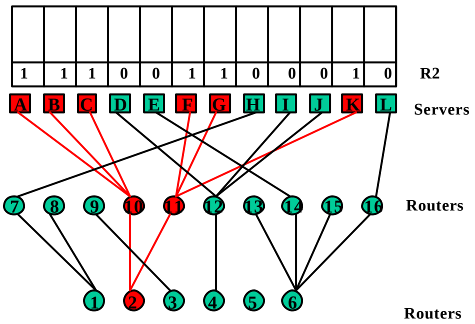
Pro-Active Network Fault Management

- Fault Propagation Model - Classical Model
  $FM = F_1$ (Root Cause)
- Primary Symptoms Model
  $FM = F_2$ (Primary Symptoms)
- Performance Model
  $FM = F_3$ (Performance Trends)

Approaches to Event Correlation

- Rule-based reasoning
- Case-based reasoning
- Binary coding
- Other methods
  - model-based reasoning
  - finite state machines
  - neural nets
  - database methods
  - hardcoded programs

Codebook Approach



1. Incoming events are coded as binary 0/1 vectors.
2. Each problem is presented by a unique binary code – signature composed from network element alarms and logical conditions
3. Correlation process - finding closest match between the incoming vector and a signature (uses Hamming distance calculation)

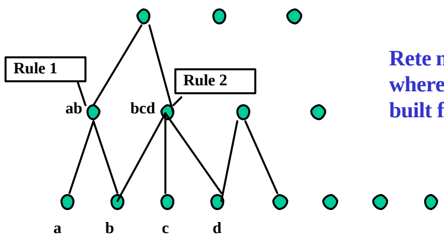
The Codebook method has been used in the InCharge product by SMARTS

Rete Algorithm

Very fast pattern matching algorithm
Rete algorithm takes advantage of two empirical observations:

Temporal Redundancy: The firing of a rule usually changes only a few facts, and only a few rules are affected by each of those changes.

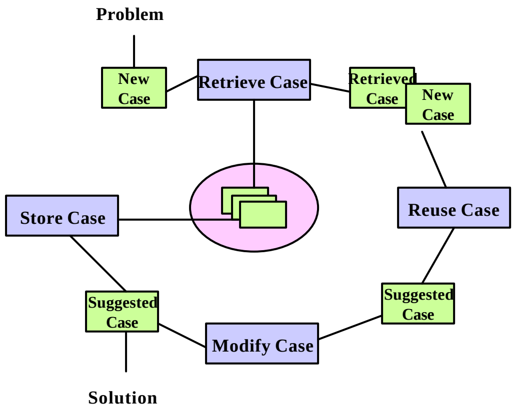
Structural Similarity: The same pattern often appears in the left-hand side of more than one rule.



Rete network, an acyclic graph, where nodes represent patterns built from input variables

Charles Forgy, "Rete: A Fast Algorithm for the Many Pattern/Many Object Pattern Match Problem", Artificial Intelligence,19, pp 17-37, 1982.

Case-Based Approach

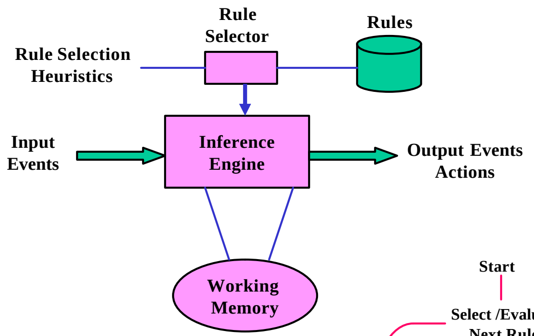


- Uses previous precedents (cases)
- Heuristics and indices to store and retrieve cases
- Modifies retrieved case to match new problems
- Contains some elements of learning

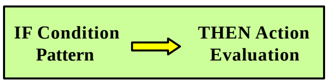
Rule-Based Approach

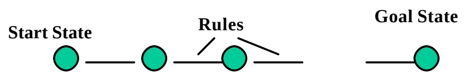
Planning RB Systems
- opportunistic planning
- agenda-based

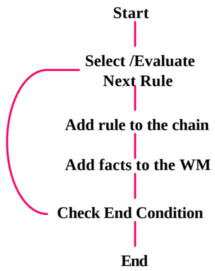
Non-Planning RB
- Rete network



IF-THEN Rule



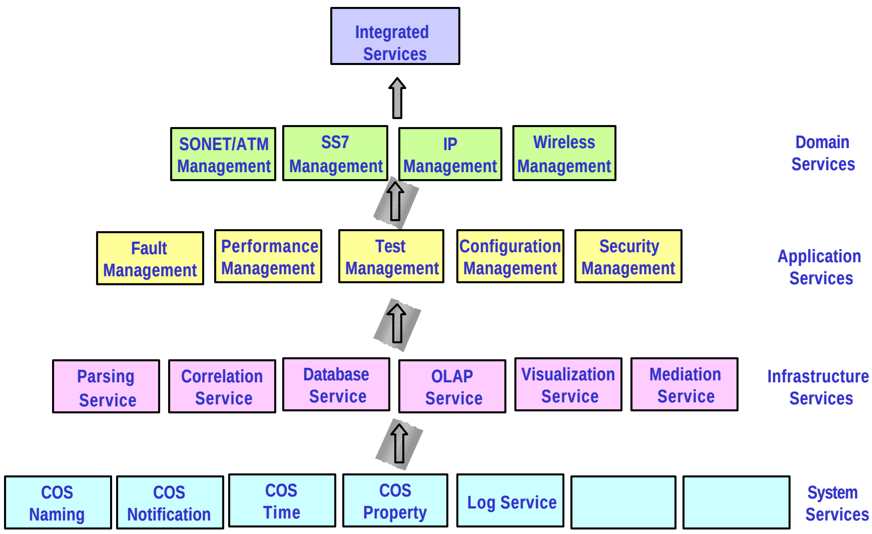




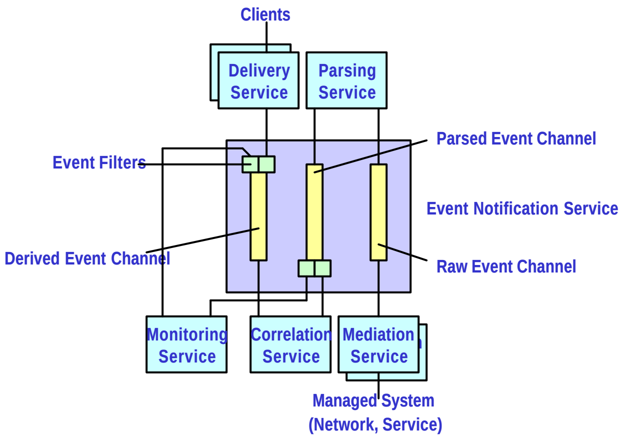
Distributed Service-Based Architecture

- A major paradigm shift in building network management systems in general, and event correlation systems in particular.
- The use of standard services and communication protocols allows the building of open, scalable, and customizable systems.
- Encapsulation of idiosyncrasies of components and easy addition, replication, and replacement of components allows effective construction of multi-paradigm, fault-tolerant, and high performance systems
- Various technologies are used for building the infrastructure of distributed network management systems, including CORBA, DCOM, and RMI

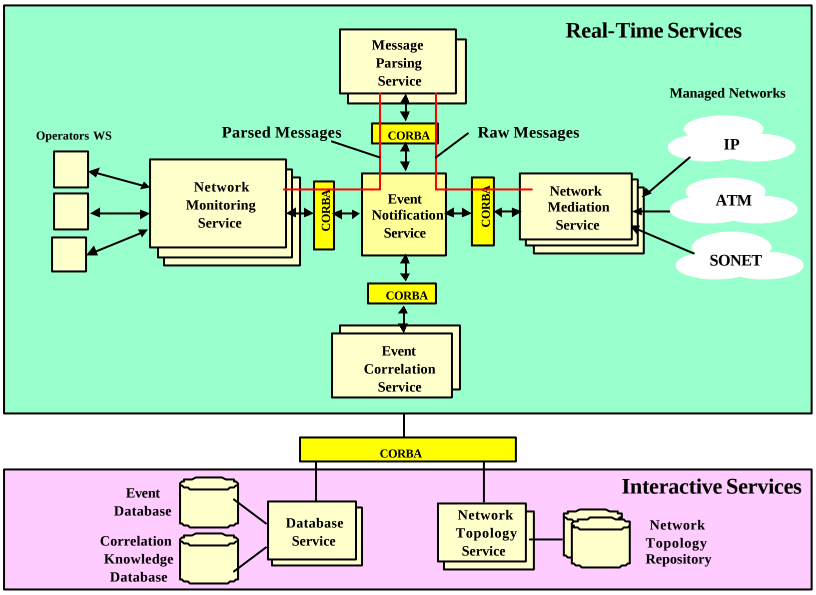
Component-Based Service Framework



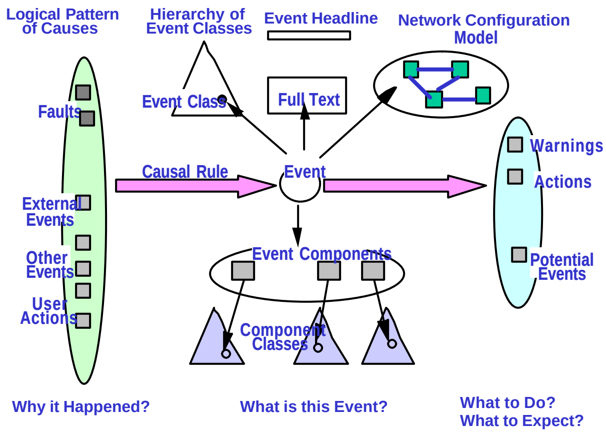
Event Notification Service



Distributed Event Management Architecture



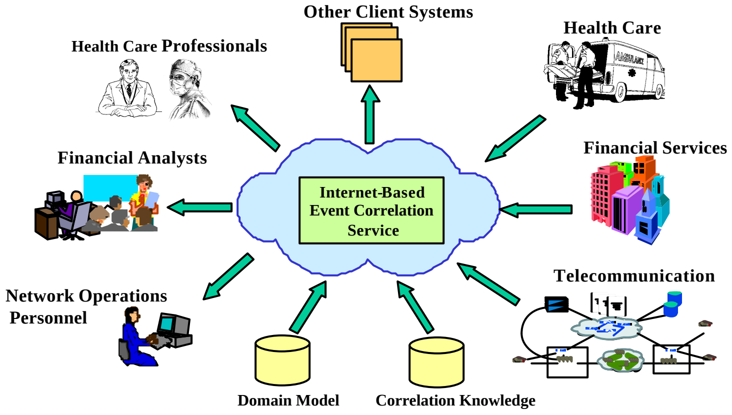
Event Explanation Process



Internet-Based Management

- The Internet is becoming a universal information transportation and service media.
- It will connect any business, home, device, transportation vehicle, process, living body or any other object - human or machine.
- Event correlation holds great potential for increasing the utility of information passed through the Internet.
- Provided as an Internet-based service to perform a variety of functions, e.g. stock market information correlation
- New opportunities will be open for customer-oriented event correlation, e.g. in the area of Customer Network management

Correlation DialTone: Internet-Based Event Correlation Service



Advanced Correlation Features

- Explanation of the content of the derived solutions and their logical reasons
- Discovery of correlation knowledge, e.g. learning correlation rules
- Extension of correlation paradigms with hypothetical reasoning
- Use of inexact (fuzzy) knowledge to estimate the possibility of derived solutions,
- Extensive use of the logic of time, space and action.

Multi-Paradigm Event Correlation

- Different solutions can be used to implement the same network management functionality, based on alternative reasoning paradigms.
- A paradigm will be selected based on the specificity of the tasks, the operational context, and the goals of the management process.
- While using multiple paradigms, the implementation, maintenance and support costs of parallel modules need to be evaluated

Event Correlation and Knowledge Discovery