Pulse2011

Network Topology Management and Root Cause Analysis: Today and Tomorrow

Mark Armstrong

Program Manager: Tivoli Network Management

Disclaimer

- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion

Agenda

- Networking challenges and IBM Network Management
- Network Manager Deep Dive
- Case Studies
- Futures

Customer Challenges

- *The network is constantly changing*
  - We are struggling to keep on top of changes occurring in our networking environment.
  - Because we use multiple different vendors' networking equipment, we cannot see all the networking equipment that we have on any single screen.
  - It is very difficult to visualize how our "logical" (IP routing) network structure relates to our "physical" network equipment.
  - We are implementing a new networking technology which our current network management vendor does not support well (for example VoIP, MPLS, VPN, etc.)
- *The network 'is the problem'*
  - We sometimes do not know that something in the network has failed until users complain.
  - The users complaining – is it really the network ?
  - When something in the network stops working, we have to work across several different point management tools to figure out what has gone wrong, it is hard to understand the scope of impact for the outage, and it is sometimes very difficult to identify the "root cause" of the problem (we sometimes just have to guess).
- *Things are getting worse…*
  - Our best staff spend a high percentage of time fighting fires versus supporting new business initiatives.
  - Can I meet the latest service demand with my currently deployed network assets ?
  - We need to improve planning by ensuring that the "as is" state of our network matches provisioning or inventory systems.

Network Manager can help

- *Visualizing a changing environment*
  - Network Manager provides end to end visibility of heterogeneous networks
  - Network Discovery is dynamic, always active and event driven
  - Network Discovery grows with your business needs as you roll out new networking technologies or consolidate network operations
- *Ensure network availability*
  - Network Manager automatically determines root cause (actionable) events and their symptom events
  - Network Manager identifies where the problems lie, even identifying problems that originate in peered networks.
  - Network Manager ensures staff have meaningful, contextual information at their fingertips
- *Best utilizing staff and deployed network assets*
  - Accurate monitoring and root-cause analysis ensures staff don't waste time chasing symptom problems.
  - Comprehensive Network Discovery helps clients Optimize network asset utilization and extract the maximum return from existing investments
  - Centralized Open Network Data repository can drive data accuracy in off-line network design, inventory and provisioning systems

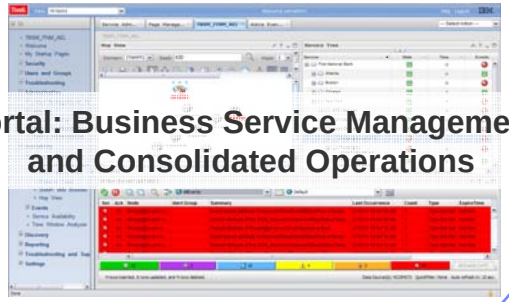
Network Manager for Netcool/OMNIbus customers

- Netcool/OMNIbus provides a single consolidation point for events from my complete infrastructure. All events – in a single pane of glass…

- How can I be confident I'm seeing all network problems ?
  - ITNM discovery helps identify business-critical network devices and verify your collecting events from these devices
  - ITNM active monitoring automatically monitors network devices for availability – don't wait for the network to tell you there's a problem (if it even tells you !)

- How can I focus operations on resolving the network problems and not their symptoms ?
  - ITNM automatically enriches events with network device configuration and status information to ensure staff has meaningful, contextual information at their fingertips
  - ITNM root cause analysis automatically correlated alarms identifying alarms that require operator action (root cause alarms) and filter out events that can be ignored (their symptomatic alarms)
  - ITNM compliments Netcool/OMNIbus' event correlation to further reduce the noise

Service Management and Network Management



Portal: Business Service Management and Consolidated Operations

Monitor service quality and prioritize work based on service impact

Automate configuration tasks, manage network change proactively, ensure compliance

Monitor KPIs, identify performance bottlenecks and remediate before they affect network service

Increase operational efficiency through event enrichment and automation

Service Quality, SLA and Customer Experience Management

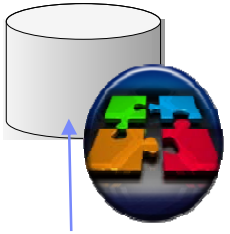
Market-leading integrated network availability management

Fault/Event Management

Performance Management

Configuration Management

Enrichment & Automation



Discovery & Data Collection

Radio Access
LTE, UMTS, GPRS,GSM, CDMA, EVDO, WiMax

Wired Access

Core
Mobile (PS,CS), Wireline, IP, NGN

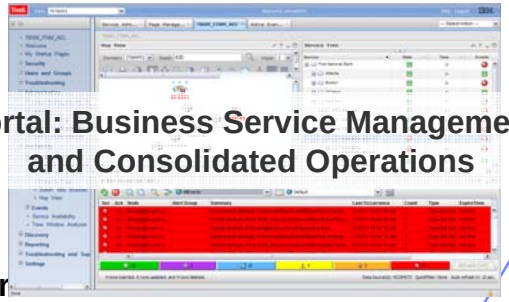
VAS
Multimedia, IMS

IT Resources and Applications

Consolidated view of your entire infrastructure including configuration and dependency information

…All aligned to <u>your</u> service management goals

Service Management and Network Management



Portal: Business Service Management and Consolidated Operations

Tivoli Business Service Manager
Service Quality Manager
Customer Experience Manager

Tivoli Netcool Performance Manager
Tivoli Netcool Performance Flow Analyzer

Tivoli Netcool Configuration Manager (formerly Intelliden)

Netcool/Impact

Service Quality, SLA and Customer Experience Management

OMNIbus and Network Manager

Fault/Event Management

Performance Management

Configuration Management

Enrichment & Automation

Discovery & Data Collection

Radio Access
LTE, UMTS, GPRS,GSM, CDMA, EVDO, WiMax

Wired Access

Core
Mobile (PS,CS), Wireline, IP, NGN

VAS
Multimedia, IMS

IT Resources and Applications

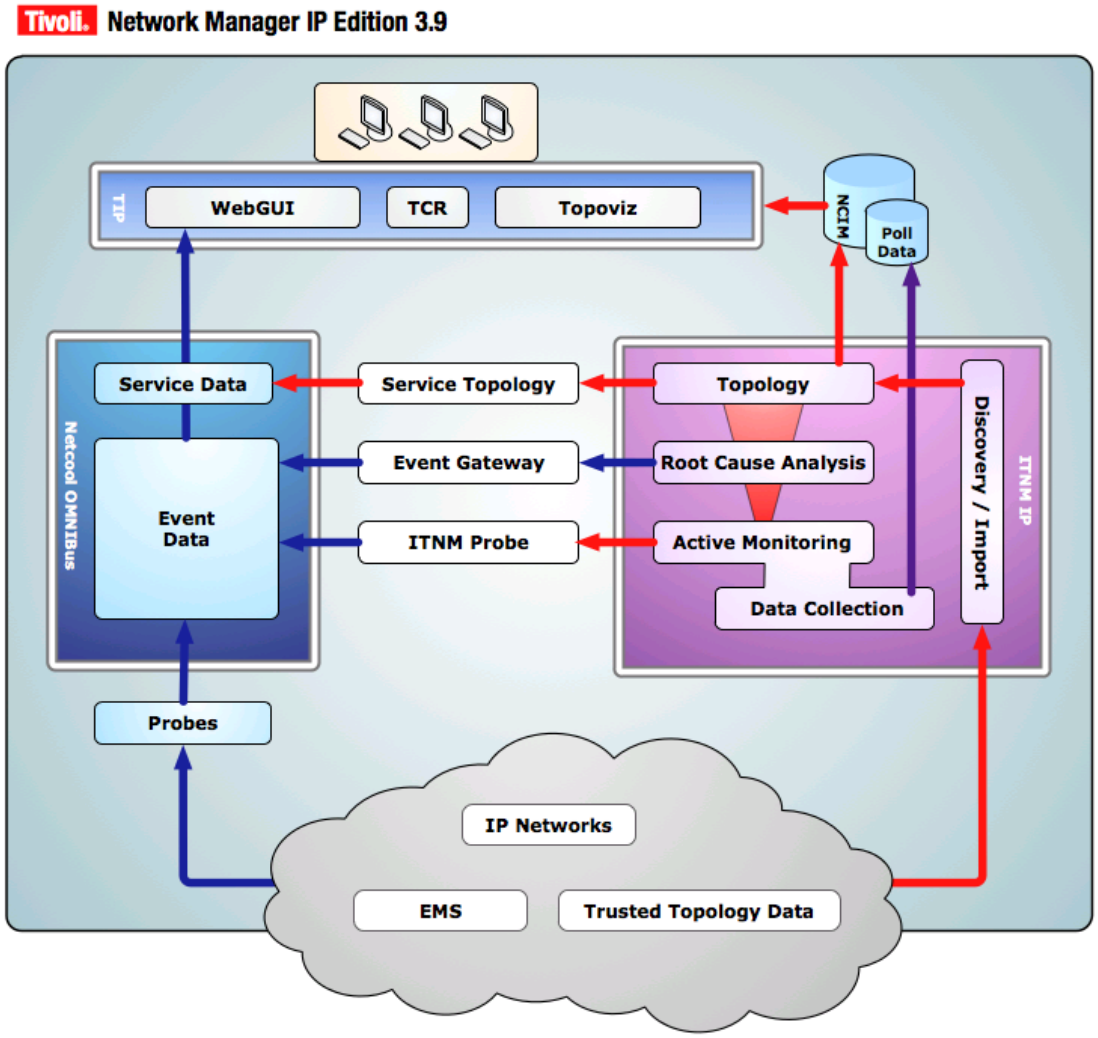
Tivoli Change and Configuration Management Database

…All aligned to <u>your</u> service management goals

Agenda

- Networking challenges and IBM Network Management
- Network Manager Deep Dive
- Case Studies
- Futures

Network Manager - Architecture



Visualization

- Tasked-based navigation combining widgets from Network Manager and OMNIbus
- Tivoli Integrated Portal / Tivoli Common Reporting
- Topology Maps / Event Views / Device Deep Dive / Administration

Network Availability / Event Management

- Leverage out-of-the-box integration with OMNIbus
- Augment with monitoring and RCA from Network Manager

Discovery

- Heterogeneous layer 2 / layer 3 network technologies including IP, Ethernet and MPLS
- Open for data retrieval / manipulation / reporting

Functional Overview

- Discovery

- Visualization

- Monitoring

- Root Cause Analysis

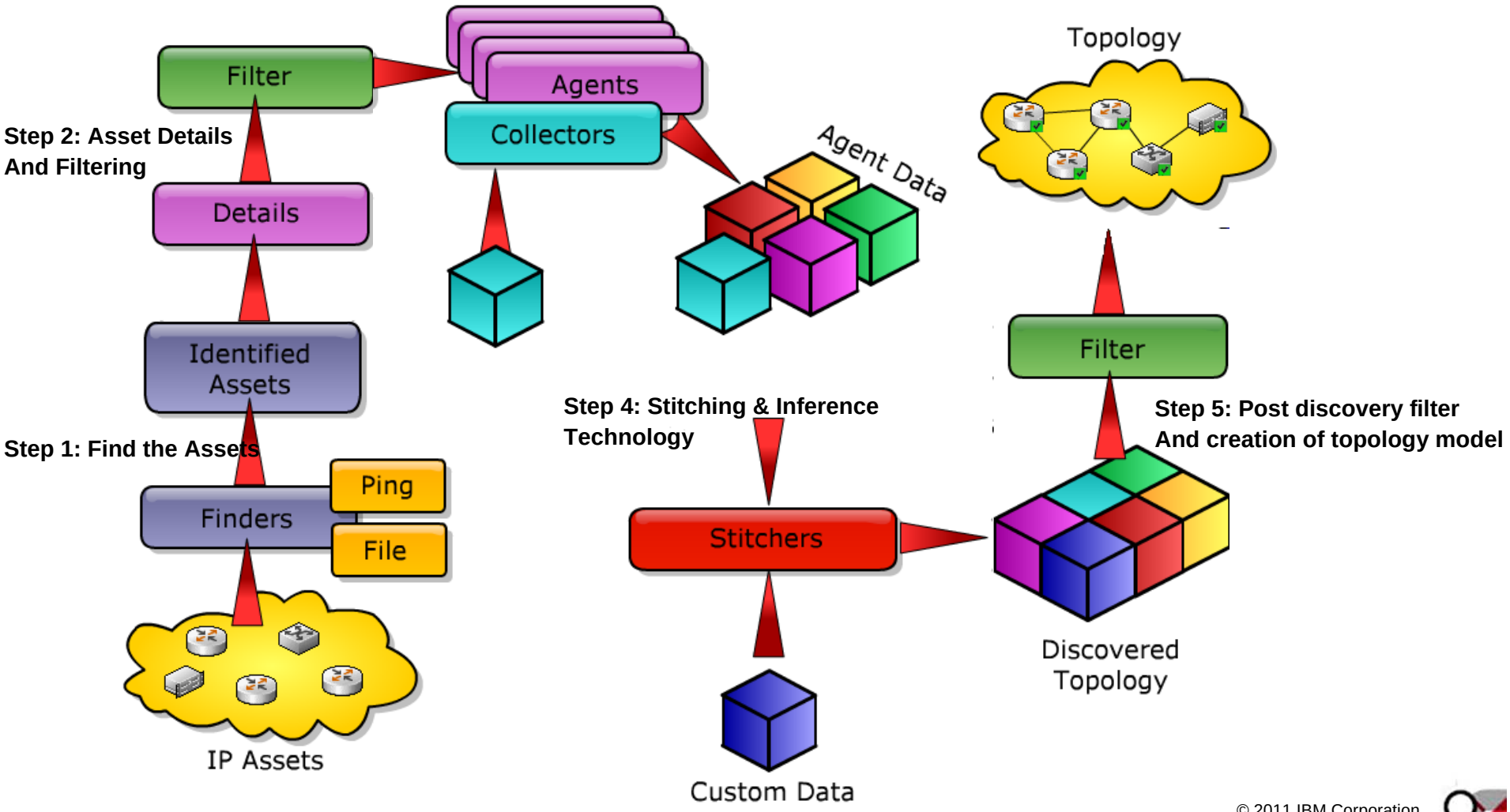
- Network Services and Event Correlation

- Reporting

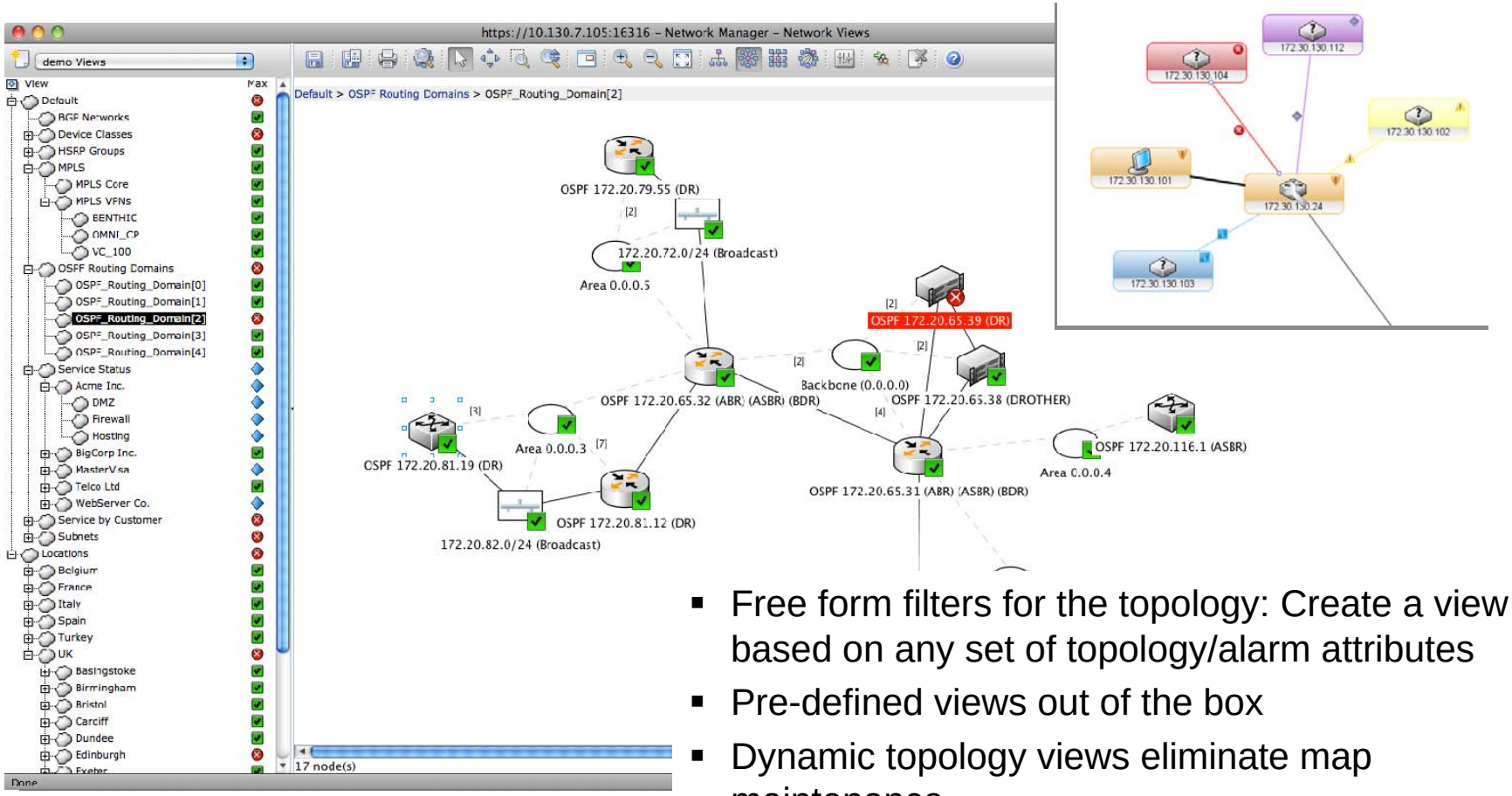
- Integrations

Discovery

- Network Topology Model is standards-based and can be hosted on Informix, DB2, MySQL and Oracle.
- Discovery Library Adapter can export network data to TADDM, TBSM and other data consumers.



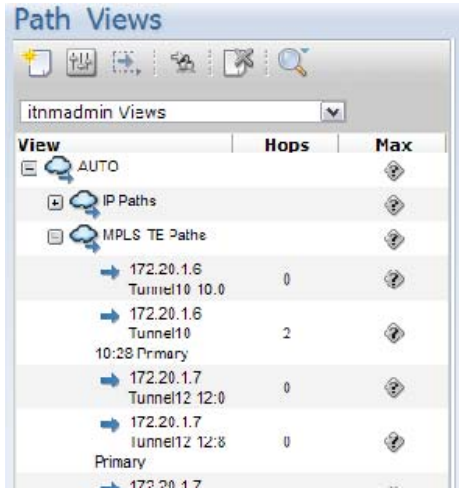
Visualisation – Network Views

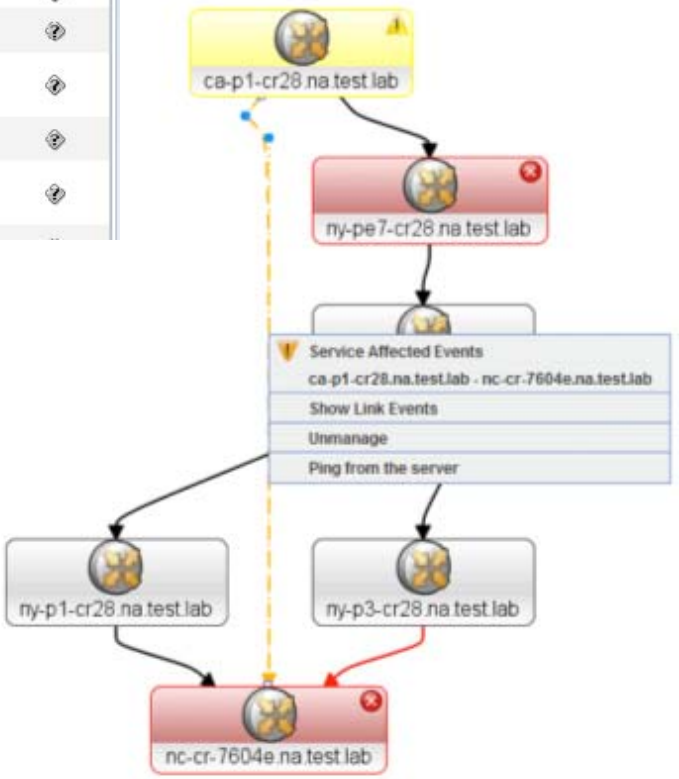


- Free form filters for the topology: Create a view based on any set of topology/alarm attributes
- Pre-defined views out of the box
- Dynamic topology views eliminate map maintenance
- Technology specific views, per user views
- *All alarming from OMNIbus*

Visualisation – Network Path Views

- Monitor, visualize and verify complex network paths used by critical business and network services
- Models MPLS-TE tunnels at discovery time
- Discover IPv4 network paths on-demand through use of an intuitive ‘right-click’ tool from selected network devices
- Leverages service modeling and event correlation to identify when a discovered network path, and subsequently a service, is affected by events occurring in the network

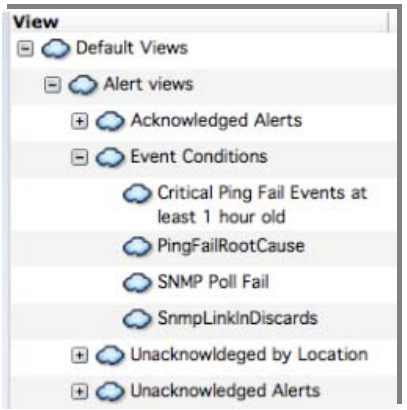




- Significantly increases the amount of information available to operators for troubleshooting purposes allowing them to identify the point along a network path that is subject to error conditions, and remediate the problem
- Discovered network path information can be used by engineers to verify network configuration in complex IP networks

Monitoring – Scoping polls…

1. Class-based polling
   - Classify devices based on any topology attributes
   - Differential polling per class (or per device/interface level within a class)
2. View-based polling
   - Assign poll policies to network views or SmartSets
   - Network View membership can be based on topology data and OMNIbus event fields
   - Poll devices on a custom topology field (location, customer name, etc.)
   - Poll devices based on event attributes (escalation, severity, etc.)
3. Adaptive Polling: Can be used to adopt polling to specific conditions i.e.
   - Failure conditions - ping 'poll failed' devices more frequently
   - Threshold conditions - adopt polling frequency when CPU is high
   - View Membership - poll all devices in a VPN with a specific set of polls



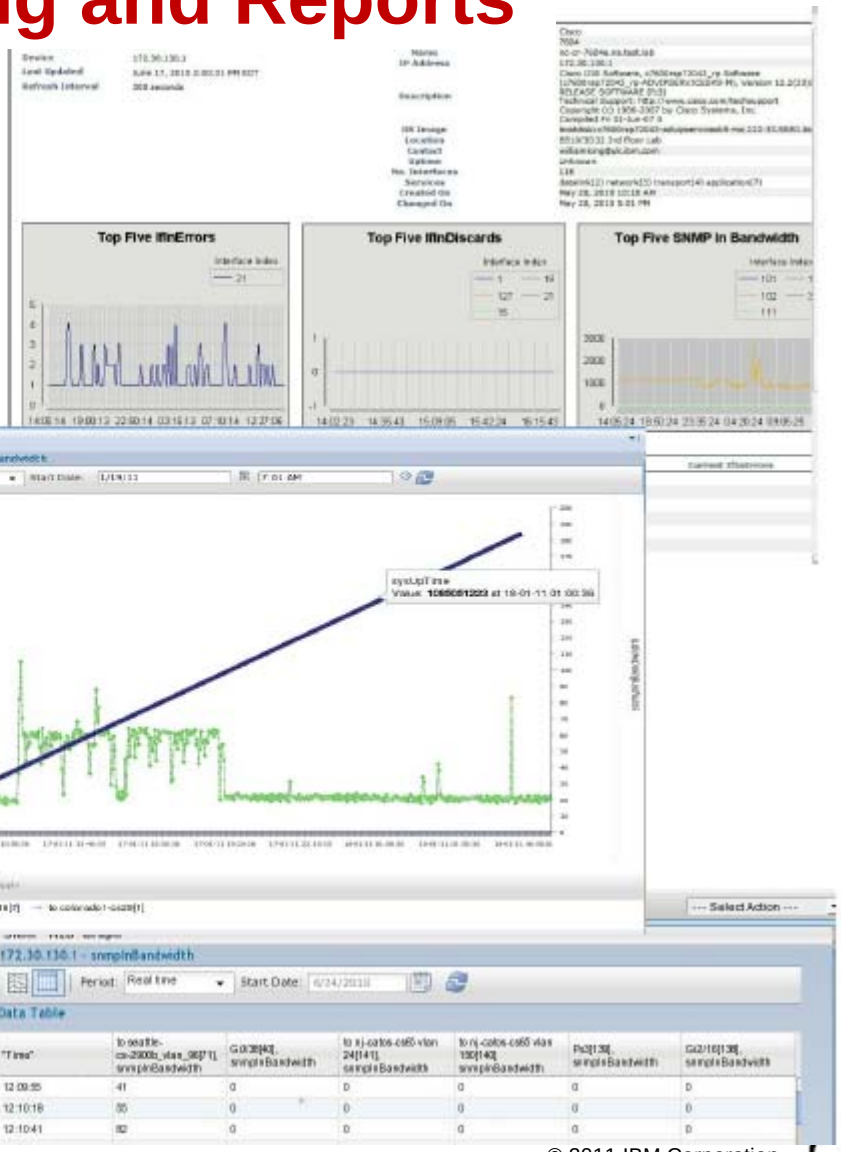
Real-time MIB Graphing and Reports

New Network Health Summary Reports

Help network operations quickly diagnose network health and take corrective action

1. Network Availability Summary
2. Device Inbound Traffic Health Summary
3. Device Outbound Traffic Health Summary

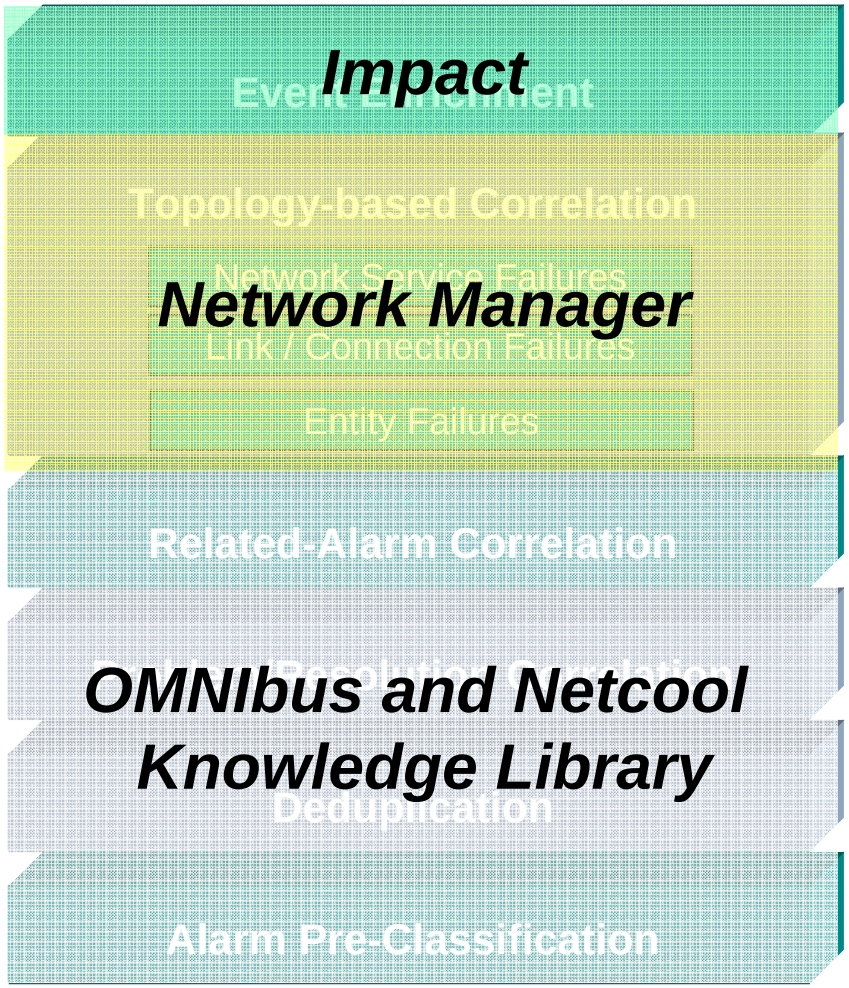
In addition the Router Health Summary was updated to use industry-standard SNMP variables supporting devices from many vendors



Usability improvements to SNMP MIB Grapher to speed time to resolution

- Graphing of two MIB variables/expressions
- Support large counter values including Float
- TIP Portlet: supports launch in context and dashboard mode.
- Graph is fully re-sizeable
- Switch between Real Time and historical view of data: Real time, 1 hour, 12 hours, 1 day or 7 days
- Table format View for sorting and filtering
- Data point value tool tips
- Faster access to data: Real time option is always available. Optionally, historical graphs can be presented initially when recent data available.

Tivoli Multi-layer Event Correlation

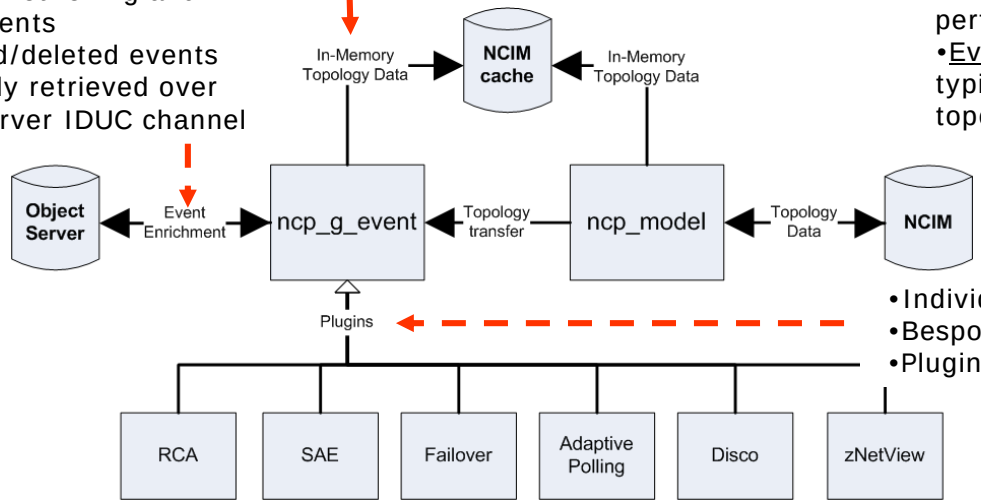


- **Multi-pass event correlation**
  - Can be optimised for different types of problem
- **Combines model-based & rule-based correlation**
  - Different correlation techniques address different classes of problems
- **Supports inclusion of information from external systems and databases**
- **Techniques are independent of technology & alarm source**
- **Uses open, extensible and customisable models & rules**
  - Users can extend to support evolving business processes & management
  - Supports auditing & traceability

Network Manager: Event Enrichment (and Correlation)

- Bi-directional event gateway to OMNIbus
  - Can enrich alarms with any network topology model information (either discovered or imported)
  - Access to any OMNIbus (ObjectServer) event table – not just the main alerts table
  - Plug-in infrastructure, facilitating integration with external products, and enabling rapid prototyping
  - Reduced load on OMNIbus as all event data passes via a single bidirectional channel

•At initialization, the gateway re-synchronizes with the ObjectServer, retrieving and filtering all events
•New/updated/deleted events are periodically retrieved over the Object Server IDUC channel



•Topology lookup is performed entirely by the event gateway before passing the event on to plugins
•Gateway matches events to network entities and performs standard event enrichment
•Event maps determine how an event is handled: typically match the event to an entity in the topology; Pass the event to interested plugins

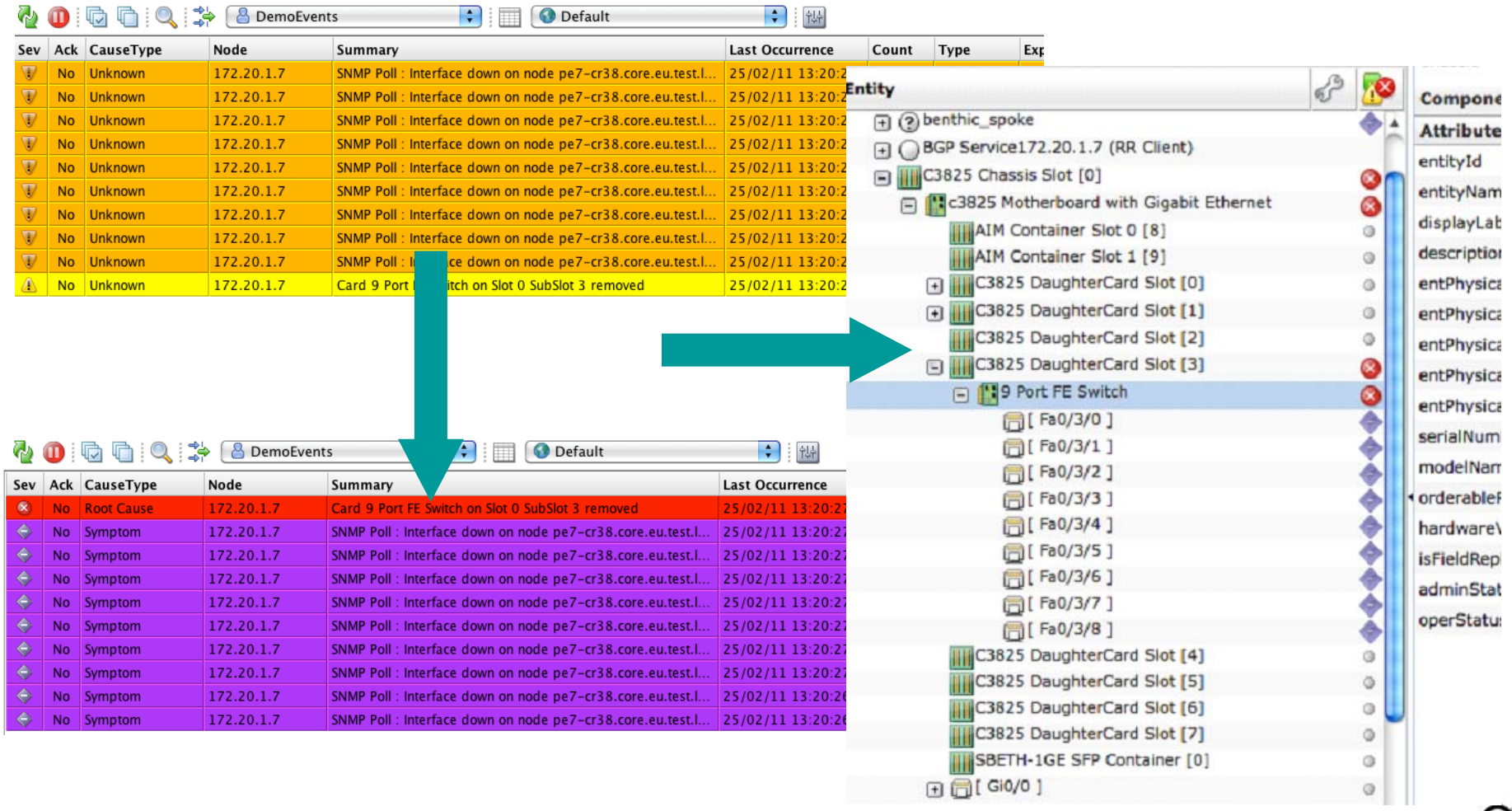
•Individual plugins register interest in specific event maps
•Bespoke plugins can be dropped in upon demand
•Plugins run concurrently, not sequentially

- Dedicated Root Cause Analysis (RCA) engine…

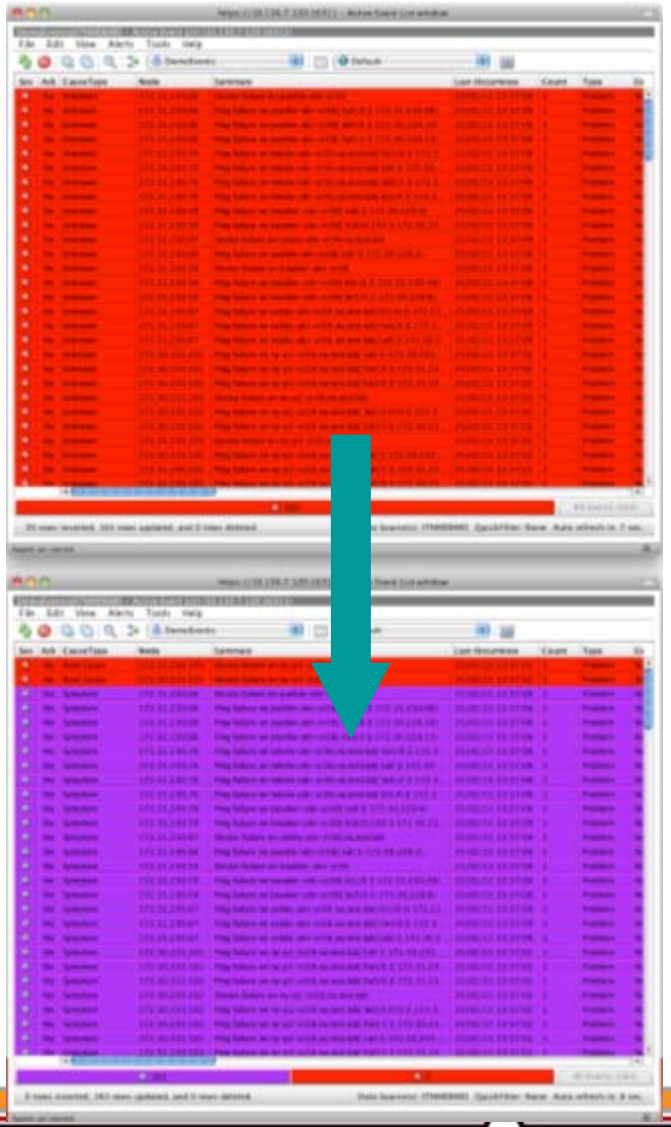
Topology-based Root Cause Analysis

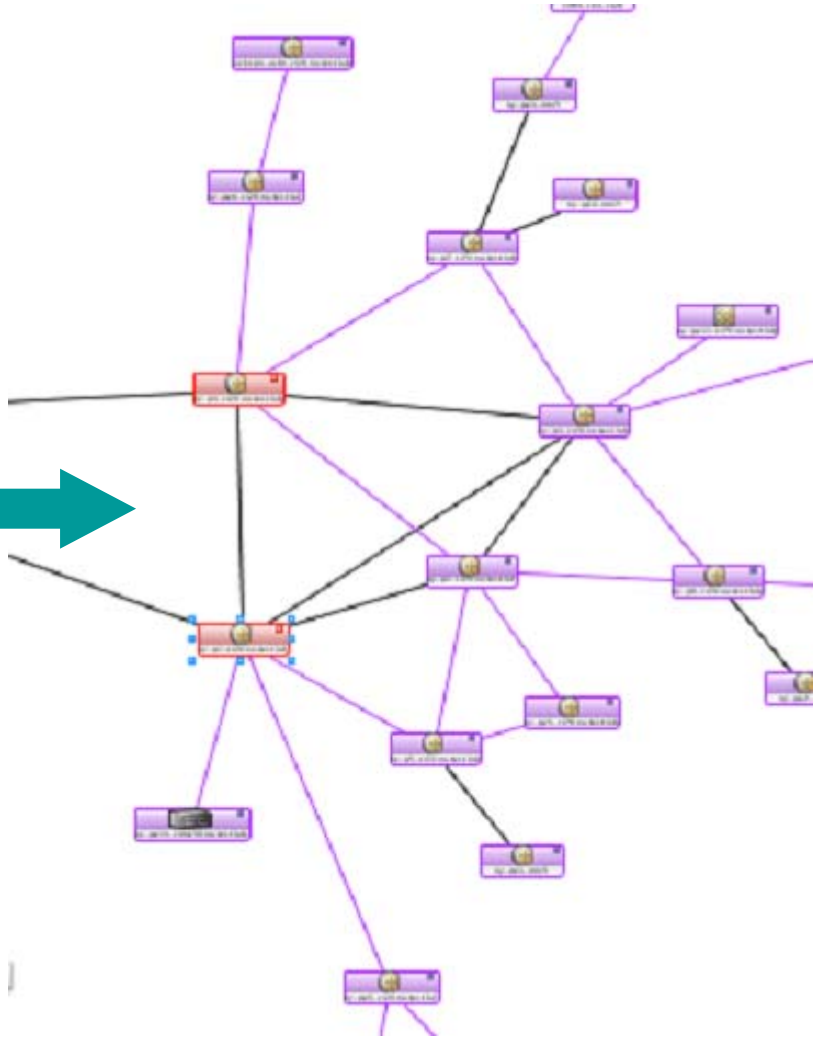
- Provides concise event reduction to focus operations on problems that need to be resolved
- Analyses events in the context of the topology
  - Any event source - passive (traps, syslog) and active (ITNM, other EMS, PM tool)
  - Regardless of the topology source (discovered or imported)
- Prioritise events based on the impact they have (updating the events in OMNIbus)
- Generic policies
  - No administration associated with network changes
  - Root cause is constantly re-evaluated as new events arrive
  - Updated set of RCA rules that are user-friendly and can be more easily customized by system integrators and network administrators (uses the discovery stitcher language)
  - Choose to only correlate events that occur within a defined time-window
- RCA policies handle…
  - Events on the same entity
  - Events on contained entities, connected entities, isolated entities
  - Events on unknown interfaces (identify for discovery)

RCA – Card Failure

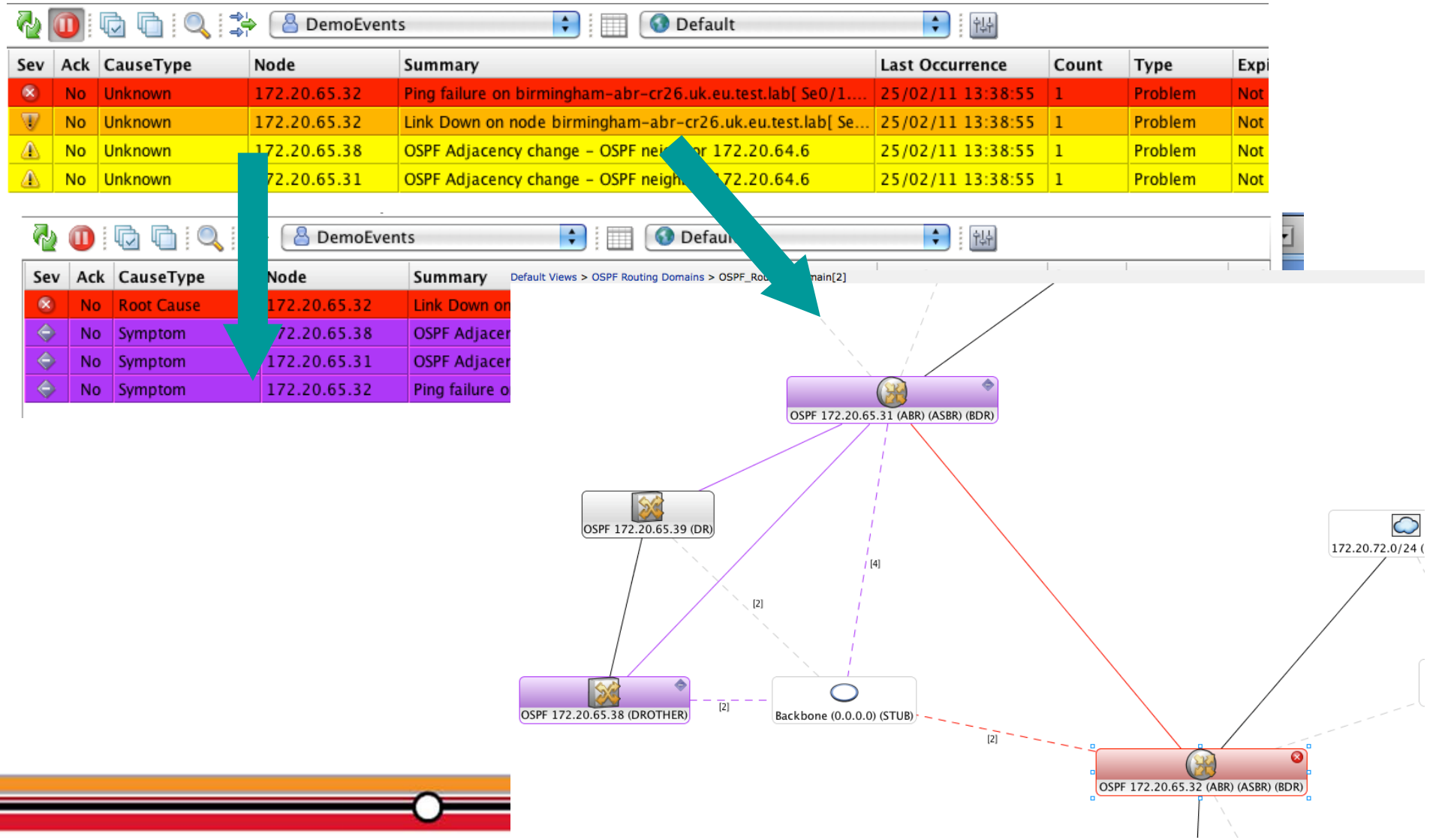


RCA – Core Device Failure





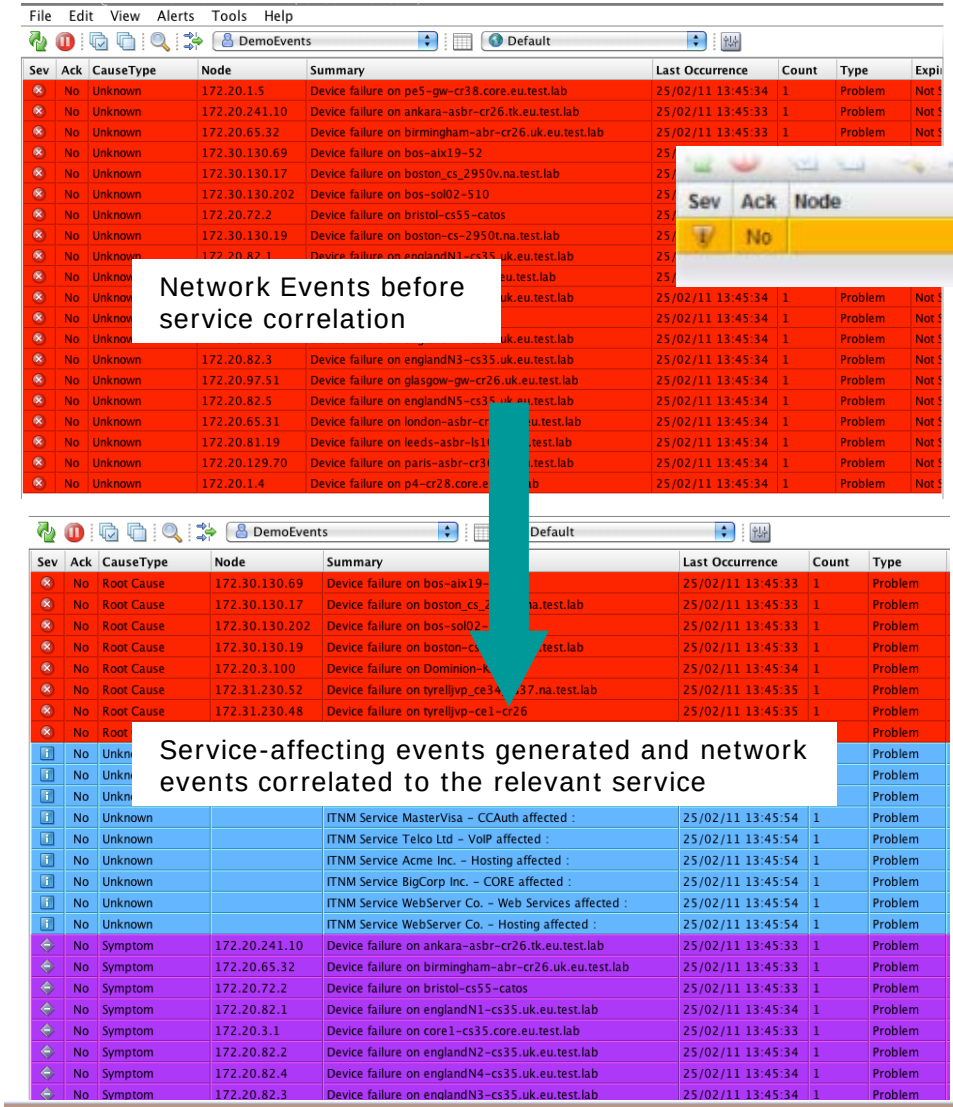
RCA – Logical (OSPF Failure)



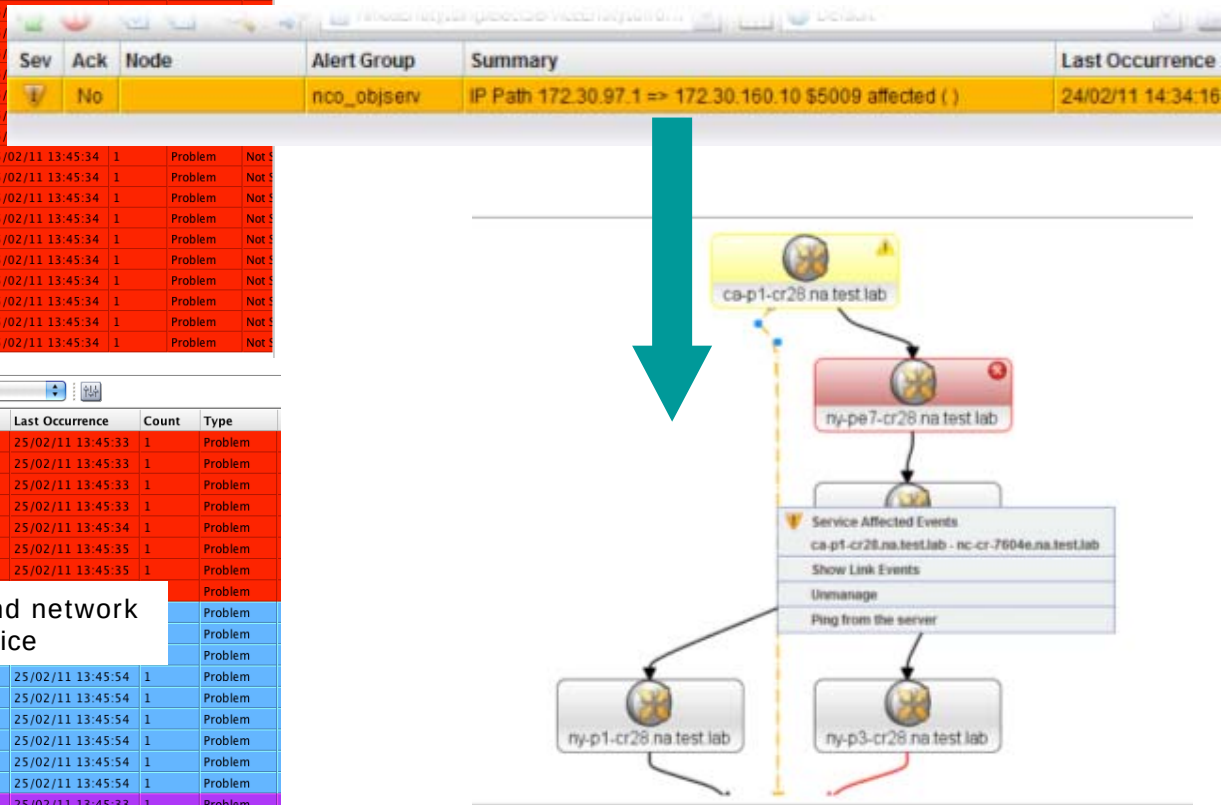
Network Services and Event Correlation

- Allows dynamic discovery and modelling of network services
  - Out of the box for MPLS VPNs, MPLS TE paths, On-demand IPv4 Paths
  - Customisable to any collection of discovered entities
    - Related (i.e. a set of devices in a location)
    - Unrelated (i.e. all the devices serving a specific service)
- Services can be visualised using the Network Views
  - VPN / VPLS Views - Status based on VPN health
  - Physical View - Status based on the event status
  - Service View - Status changes as service-affecting events are raised
- Allows complex sequence of network events to be seen within the context of a service
  - Generate service events for non-technical audiences
  - Display using filtered event lists or WebGUI maps
- Event list tooling links service affecting events to the underlying network events
- Complimentary to a Business Service Management (BSM) solution
  - The service-affecting events can be used as part of the overall service calculation
  - Automated discovery and monitoring removes the need to model complex network based services in the BSM solution - modelled services can be exported to Tivoli Business Service Manager

Network Services and Event Correlation

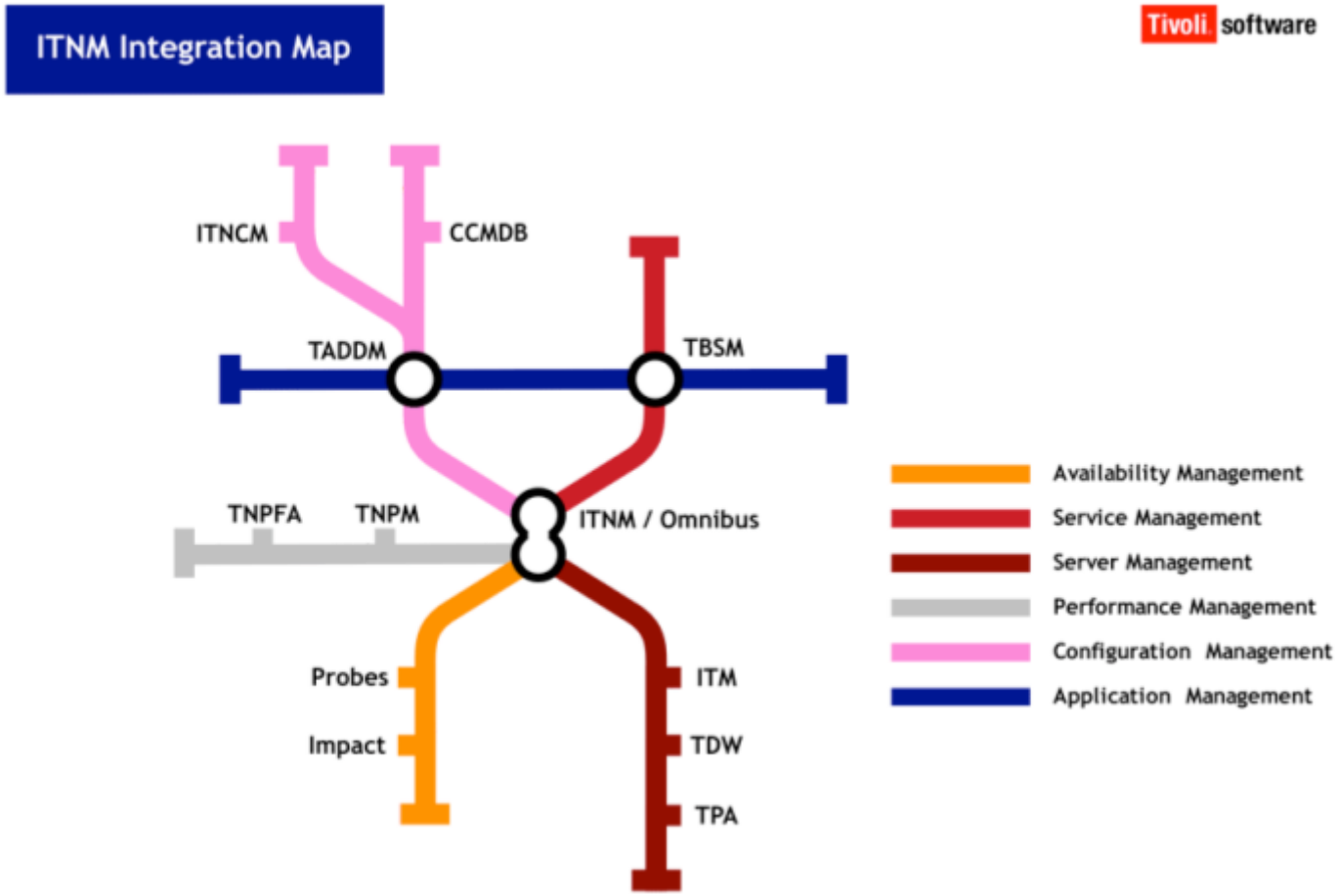


Interface alarms grouped to a higher-level IP V4 Path service-affecting event



IP V4 path view shows service-level event and devices supporting this path (and their alarm state)

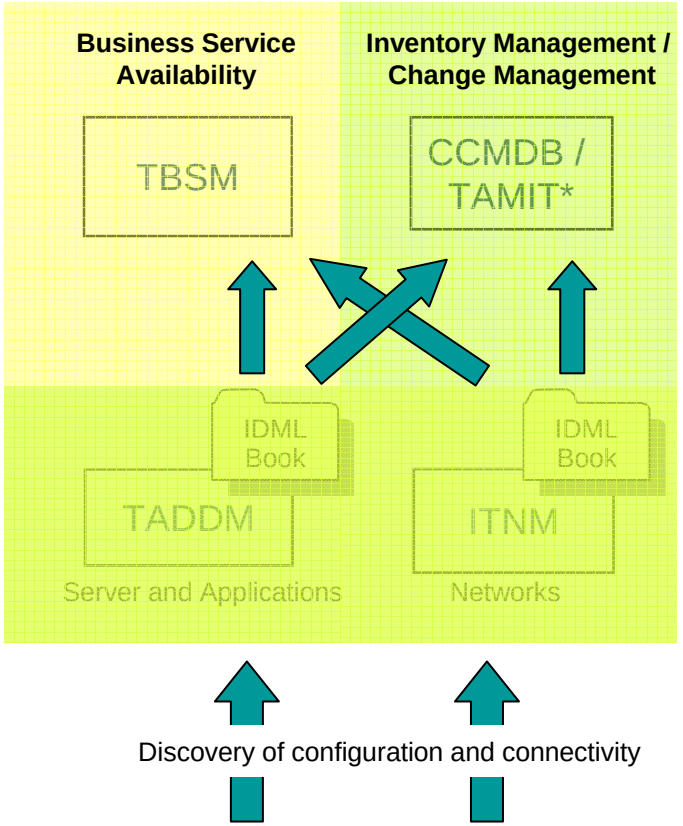
Integrations



Integration – Discovery Library Adapter

- Exposes the network information discovered by Network Manager in the Common Data Model (CDM) format. Two main uses cases…

1. Business service availability
   - Pre-populates service component repository with discovered network resources
   - Drill-down in context from business views to locate problems affecting the business service
2. Inventory / Change Management
   - Provide view of the as-built network assets
   - Drive inventory / change management from this as-built view
   - Reconcile against as-planned views of the network



- Filter export using a specific Network View or set of Views
- Physical inventory resources including Connectors, Chassis, Power Supply, Card, Fan, Sensor and Slot.
- Layer 2 connectivity
- Supports IPv4/IPv6 subnetting and addressing

Integration with Netcool Configuration Manager

IBM Tivoli Netcool Configuration Manager (ITNCM)

Formerly INTELLIDEN® An IBM Company

- Automate routine configuration management task
- Understand how network changes may affect service and your customers, and proactively manage the impact of these changes
- Improve adherence to corporate and regulatory standards through ongoing network policy enforcement
- Comprehensive provisioning of networks, servers, storage and applications

- Seed ITNCM discovery with it's network connectivity information (lowers the cost of ownership)
- Event Integration
  - ITNCM will detect configuration changes in the network and post a network change event to Netcool/OMNIbus and Network Manager.
  - ITNCM will detect when network device configurations are not compliant with pre-defined policies and will post an event to OMNIbus and Network Manager in the event of non-compliance.
  - These events can be correlated to other events in the cause where a configuration change has caused a problem in the network.
- From OMNIbus and Network Manager an operator can launch
  - in-context out of the box reports showing the configuration history of selected devices (including an audit of who made the changes)
  - into ITNCM to make a configuration change or revert to a previous compliant configuration

Agenda

- Networking challenges and IBM Network Management
- Network Manager Deep Dive
- Case Studies
- Futures

Customer Case Studies

IT Service Provider for Utility Industry

Challenges

- Business demanding more stringent LAN SLA
- Core network upgraded to MPLS

Benefits

- Dramatically increase availability and performance of critical business operations
- Enable the rapid identification of the root caused of network downtime
- Reduce meantime to repair (MTTR) so that problems can be addressed before they becomes full-fledged outages.
- Leverage real-time, centralized monitoring to consolidate network and IT operations and to boost efficiency.

Large European Cable Operator

Challenges

- Over 35 different network technologies
- Voice/Video/Data are separate and difficult to manage
- Departments using individual tools and information sources

Benefits

- Provided a central fault-management process across the company
- One front-end for monitoring and fault analysis simplifies work and reduces training efforts
- Root Cause Analysis reduces number of tickets and MTTR
- Automated network discovery reduces documentation effort and increases accuracy of inventory data
- Visualisation of customer VPNs enables customer service management

Large transportation / logistics provider

Challenges

- Complex and ever changing network requires automated / robust automation discoveries
- Advanced end2end visualization from layer 2 and 3
- Streamline existing network management tools to reduce gaps/redundancies
- Provide dual Data Center redundancy / high availability

Benefits

- Real-time in-depth network visibility
- Provide reports on devices found to other departments
- Collect and provide more data on each device/network technology (e.g. OSPF, BGP)
- Reduce MTTR through event enrichment and correlation

Agenda

- Networking challenges and IBM Network Management
- Network Manager Deep Dive
- Case Studies
- Futures

Network Manager Futures

Lower cost of ownership in large distributed environments

- Discovery / Polling workers deployed in multiple locations
  - Small footprint / headless deployment option
  - Localized discovery, modelling, monitoring and event correlation
  - All network tooling hosted locally
- Central Network Manager instance
  - Secure two-way communication with the remote workers
  - Centralized administration of remote workers
  - Rollout 'standard' remote worker images/installation
  - Centralized operator console providing end-to-end network visibility and control across multiple workers
  - End-to-end event correlation/reduction

Distributed deployment architectures are typically used in...

- Very large networks
- Distributed networks with clear geographical, ownership or security boundaries
- Managed Service Providers (MSP)
- Networks containing overlapping IP Address spaces

Network Manager Futures Cont.

- Advanced discovery as a shared component
  - Immediate feedback and monitoring as devices are first discovered
  - Just-in-time discovery
    - Real time for fast changing parameters (interface status)
    - Less dynamic for physical inventory
  - Leverage other discovery technologies including EMS integrations, L1 (transmission networks) discovery, provisioning tools
  - Import server/application data from Tivoli Application Dependancy Discovery Manager and Network Mapper (NMAP)

  - Reuse Network Manager discovery technology in
    - IBM System Technology Group
    - Netcool Configuration Manager
    - Tivoli Application Dependancy Discovery Manager
    - Tivoli Netcool Performance Manager
  - Resulting in a lower cost of ownership

- Performance, Scalability and High Availability
  - High-availability / clustering of web UI
  - Exploit 64bit platform options

Network Manager Futures
Network Technology Support

- Additional discovery and technology-enhanced visualization/reports
- Strategic network technologies including Carrier Ethernet, IP Multicast, LTE and CEE
- Enhanced monitoring and visualization of existing technology support
  - IS-IS, HSRP/VRRP, SMLT
- Optical network technology support
  - Extend core network topology model tables to support modeling optical technologies including cross-connects, termination points, circuits and lambdas
  - Leverage existing TL1 device support
  - Extend with additional transport device/technology support
- DataCenter, Virtualization and Cloud
  - Additional device support including Juniper, Brocade and Blade
  - Support discovery of virtual network devices, their connectivity with the VMs (hypervisor and physical host) and connectivity with the physical network
  - Apply RCA algorithms to connectivity between virtual infrastructure components

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list pricesand performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.