White Paper

Technical Overview: The Complete Lifecycle Management of Cisco Unified MPLS for Mobile Transport System

What You Will Learn

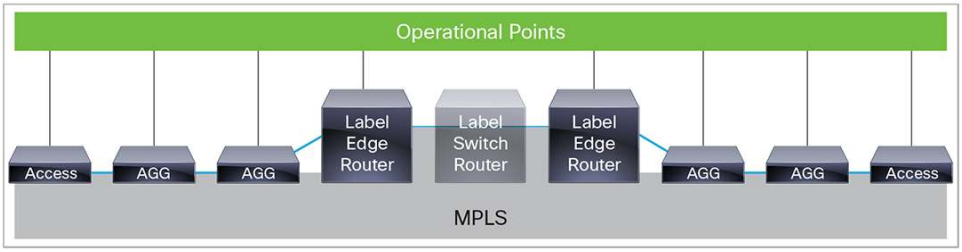
This white paper provides a complete service lifecycle management overview using the Cisco Prime™ Carrier Management solution for the provisioning and ongoing management of Cisco® Unified MPLS Mobile Transport (UMMT) System. A description of the solution is provided along with a phased approach to UMMT resource management, service provisioning, and service assurance.

Challenge: A Cost-Effective Transition from Legacy to 4G/LTE Networks Is Not Easy

In the transition to fourth-generation/Long-Term Evolution (4G/LTE) networks, mobile service providers are gaining much greater throughput capabilities and maximizing their return on investment with transport virtualization that can support multiple services. During the 4G/LTE transition, Multiprotocol Label Switching (MPLS) has emerged as the preferred technology to support virtualization and transport of legacy time-division multiplexing (TDM)- and Asynchronous Transfer Mode (ATM)-based networks.

One area of mobile networks that has presented a particular challenge as traffic volumes have grown dramatically in recent years is mobile backhaul. A variety of technologies have been added to the radio access network (RAN) to provide greater scalability and efficiency for mobile backhaul. This has led to a highly complex environment where every service must be configured on every network element through operational points. The majority of deployments require concurrent legacy second- and third-generation (2G, 3G) and newer (4G/LTE, Wi-Fi) backhaul support along with virtualization of the packet transport to deliver multiple services together. The Cisco UMMT System integrates all of these operational points over MPLS islands to deliver highly scalable, simple-to-operate MPLS-based IP RAN backhaul (Figure 1). UMMT therefore simplifies the end-to-end architecture, eliminating the control and management plane translations inherent in legacy designs.

Figure 1. Multiple Operational Points in Mobile Backhaul Networks



MPLS over IP is a desirable solution for RAN backhaul because:

- The MPLS pseudowire is the industry choice for support of legacy ATM and TDM traffic

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

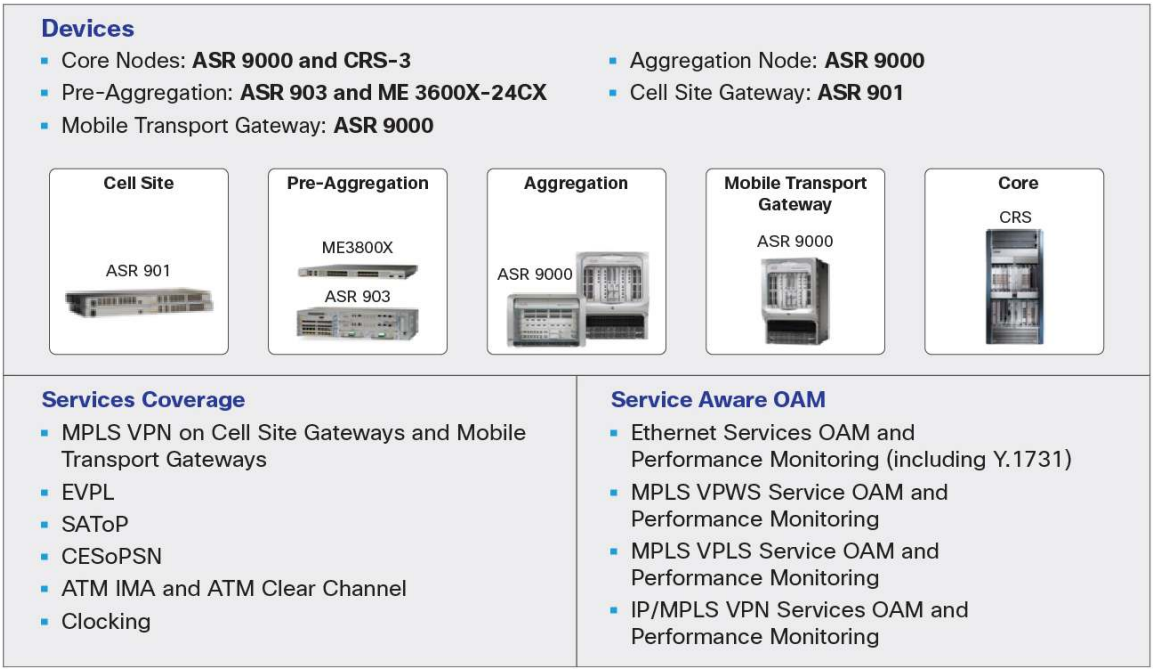
- Layer 3 MPLS VPNs in the backhaul facilitate virtualization of the transport infrastructure, which provides greater cost efficiency, scalability, and agility for wholesale transport and uses the RAN backhaul for transport of other services for business and residential customers

UMMT resolves several challenges that operators have faced with legacy environments, including scaling MPLS to support tens of thousands of end nodes and support of complex technologies such as traffic engineering fast reroute (TE-FRR) to meet transport service-level agreements (SLAs). It provides simplified carrier class operations with end-to-end operations, administration, and management (OAM), performance monitoring, and seamless loop-free alternate free reroute (LFA-FRR) protection.

UMMT Architecture Overview

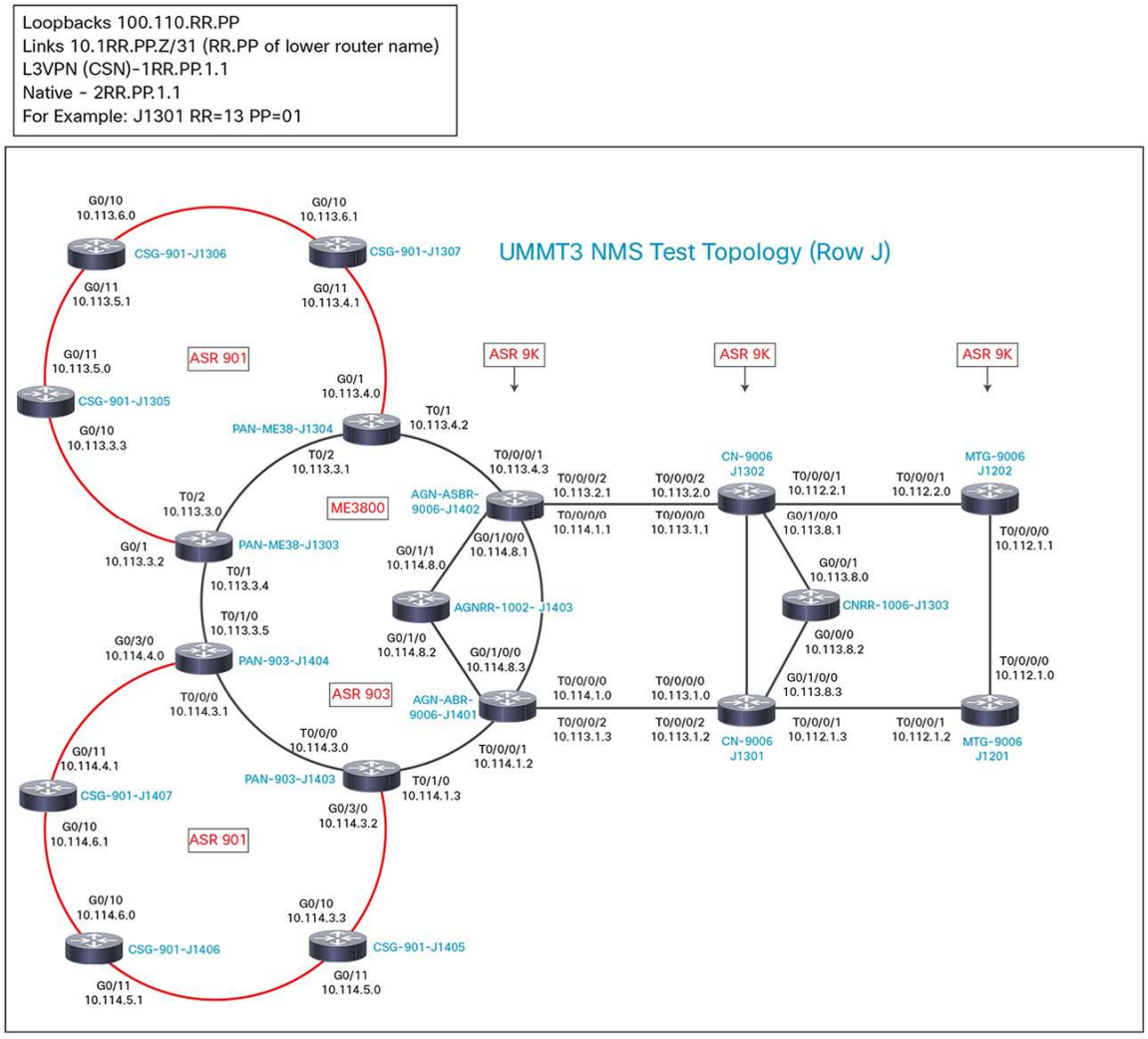
The Cisco UMMT System includes the Cisco ASR 901 Aggregation Services Router as the cell site gateway (CSG) and the Cisco ASR 9000 Series Aggregation Services Router as the mobile transport gateway (MTG). The services supported by UMMT between the CSG and MTG include MPLS VPN and clocking. UMMT provides simplified carrier class operations with end-to-end OAM and performance monitoring. (See Figures 2 and 3.).

Figure 2. UMMT Devices, Services, and OAM



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 3. UMMT Network Management System (NMS) Test Topology

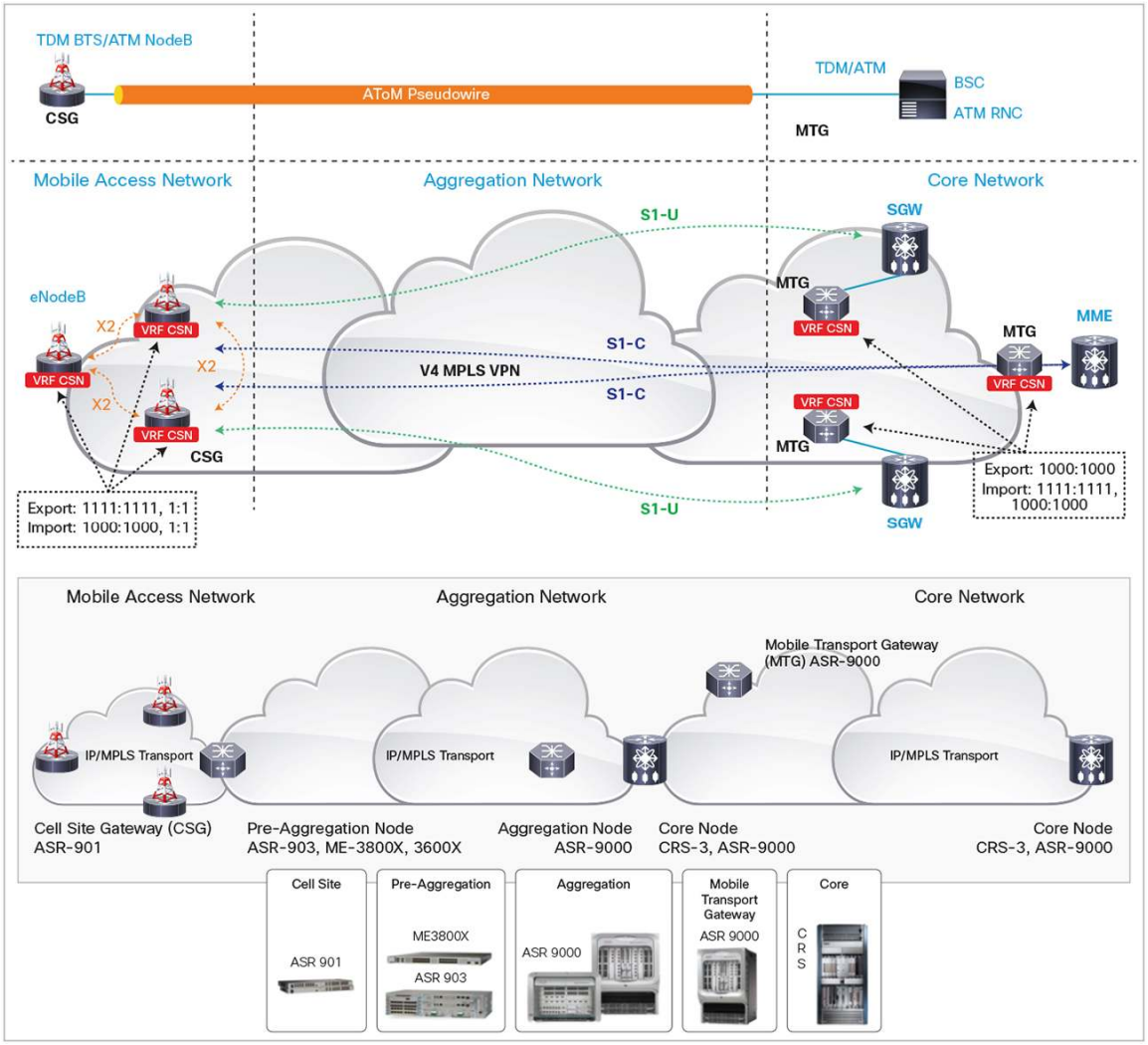


The UMMT architecture helps enable the flexible placement of the Layer 3 and Layer 2 transport virtualization function as required to support retail and wholesale backhaul for Global System for Mobile (GSM) communications, Universal Mobile Telecommunications Service (UMTS), and LTE. Different options are available for optimization of different topologies such as wireline residential and business, Layer 2 and Layer 3 VPNs, and IP services.

In this paper, the provisioning and management lifecycle of LTE MPLS VPNs between cell sites and the MTGs is presented. The LTE backhaul over the UMMT system assures a highly scalable MPLS VPN. It encompasses LTE S1 interfaces from all CSGs across the network along with LTE X2 interfaces per RAN access region (Figure 4).

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 4. UMMT Architecture for LTE MPLS VPN

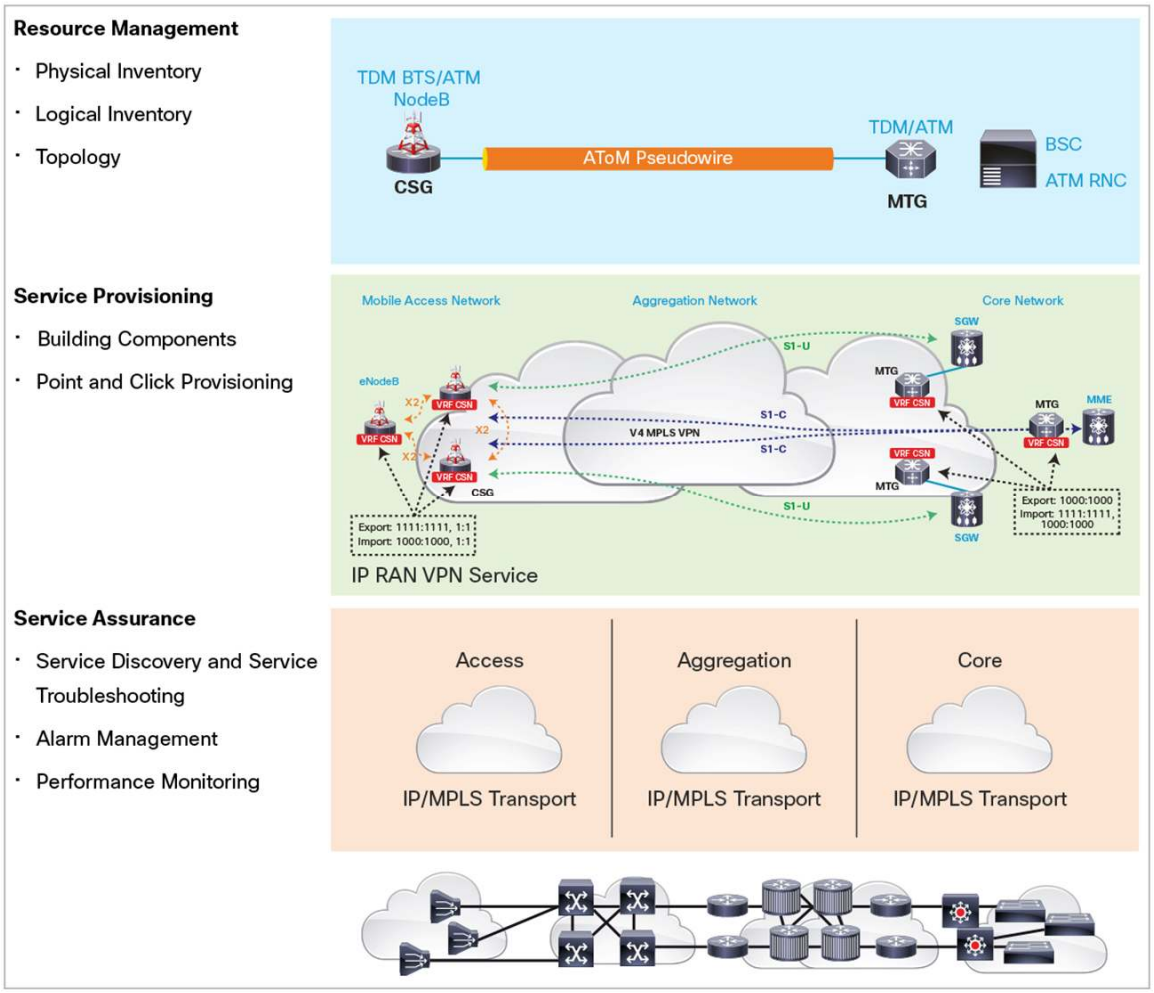


A single MPLS VPN per operator is built across the network with VPN routing and forwarding (VRF) instances on MTGs connecting the LTE Evolved Packet Core (EPC) gateways - including the serving gateway (SGW), packet data network gateway (PGW), and Mobility Management Entity (MME) in the mobile packet core. CSGs connect the eNode Bs in the RAN access layer. VPN prefix filtering with simple Multiprotocol Border Gateway Protocol (MP-BGP) Route Target (RT) import and export statements is provided on the CSGs and MTGs. Service provisioning is required only at the network edges.

The UMMT management lifecycle begins with resource management and proceeds to provisioning and service assurance. The Cisco Prime Carrier Management solution provides an integrated, workflow-based suite of tools that greatly simplifies all of these functions (Figure 5).

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 5. UMMT Management Lifecycle Phases



Cisco Prime Carrier Management

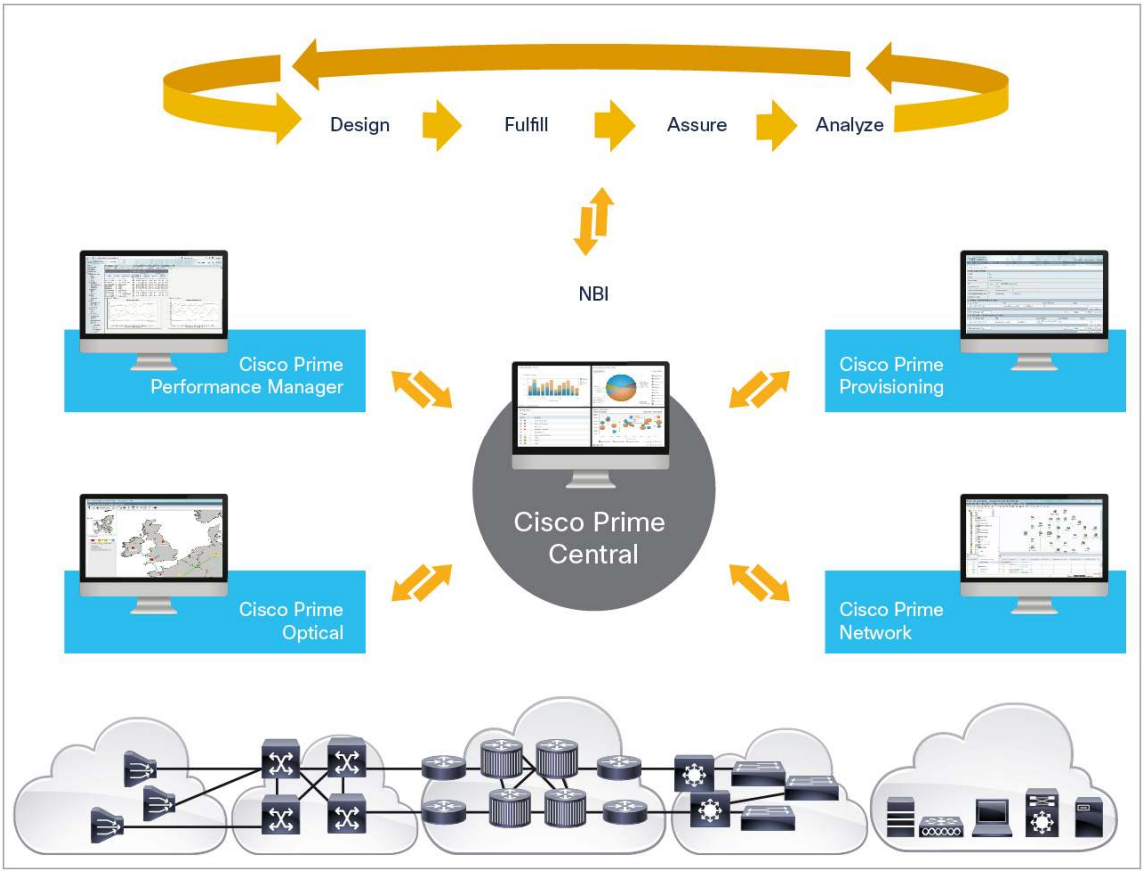
The Cisco Prime Carrier Management solution provides integrated lifecycle management through a suite of products that can be purchased individually on a standalone basis or as a complete suite for much greater functionality.

Cisco Prime is designed for lower startup and ongoing management costs with common architectural components, integrated workflow, and a common user experience. Used to provision and manage the Cisco UMMT System, the Cisco Prime Carrier Management solution provides visibility and automation to make management of UMMT simpler, faster, and less costly.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

There are five products within the suite, shown in Figure 6

Figure 6. Cisco Prime Carrier Management



- **Cisco Prime Central** provides one centralized interface with an inventory view of all components that span the network.
- **Cisco Prime Network** provides a simplified and automated approach to network device discovery, configuration, and change management plus fault monitoring and troubleshooting for the packet and IP domain.
- **Cisco Prime Optical** helps ease the TDM to 4G/LTE backhaul transition by simplifying management of the optical domain through the ability to use a GUI-based interface for provisioning of optical circuits and the fault, performance, and configuration management of TDM and Synchronous Digital Hierarchy (SDH) platforms.
- **Cisco Prime Provisioning** brings automation and GUI-based, policy-driven workflows to service provisioning, configuration, and functional audits from one end of the network to the other.
- **Cisco Prime Performance Manager** reveals the performance and reliability issues of Cisco and third-party network devices deployed across the network infrastructure in real time, including core, aggregation, and access layers.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Integrated Lifecycle Management for the Cisco UMMT System Using Cisco Prime Carrier Management

The major activities required for deployment and use of the Cisco UMMT System include resource management, service provisioning, and service assurance. The lifecycle management process using the suite follows.

Manage Network Resources

Network inventory management is an essential component of a robust network management architecture.

Network inventory is an important business asset (regardless of the environment) that requires ongoing tracking and management.

The ability to access up-to-date network information is essential to high-reliability environments. Typical network operations rely on physical network management that identifies element failures. Network operators need to uniquely determine the exact location of a network element, along with the element's associated attributes, and navigate to specific network element information.

Most networks already employ network management systems for fault detection. However, network inventory management is often missing because of network complexity and a lack of integration time.

The network inventory function implemented in a network management application should provide automated device discovery to catalogue and to update what the network actually contains. This information should be available in a central database repository with GUI access and open APIs for northbound interface (NBI) integrations. The discovery should also be flexible to detect network elements and import asset information for all hardware, software, and infrastructure from any system in the network. This information should be gathered and updated regularly.

What most of the network management provides today is just physical inventory.

The Cisco Prime Carrier Management solution provides a common inventory and event/alarm management solution with automated device discovery to catalogue and update network inventory. Inventory features include:

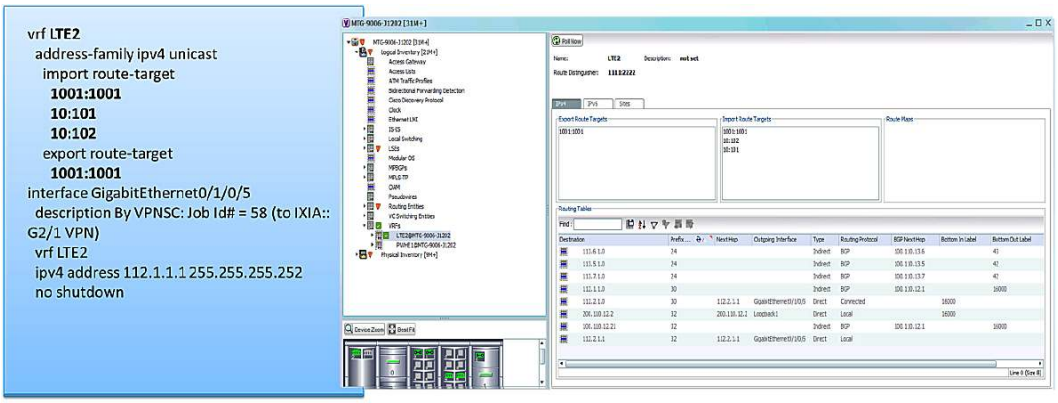
- **Physical Inventory** - Through a simple centralized GUI Cisco Prime Carrier Management provides automated device discovery that shows administrators the full physical inventory in the network. The information is available in a central database and it can be accessed through the GUI and through open APIs for NBI integration with operation support systems and business support systems (OSSs/BSSs). The discovery is flexible enough to detect network elements and import asset information for all hardware, software, and infrastructure from any system in the network. This information can be gathered and updated regularly.
- **Logical Inventory** - The logical inventory reflects additional data provided by the device configuration, such as pseudowires, label switching tables, tunnels, protocols, services, and so on. Every artifact created within device configurations can be modeled by the management system through a logical structure that identifies the relationships between items of configuration (for example, same service, depends on) and other physical and logical constructs. The physical assets are just the enablers: how they are connected and configured creates the services that customers rely on.

The Cisco Prime Carrier Management solution can also provide device configuration information and represent it in the device's user interface for easy access to the information for operators that may not be familiar with the details of the command-line interface (CLI).

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

For UMMT VPN services, for example, it can show the VPN VRF information defined on the MTG and CSG. The system gathers this information and it is available to the administrator in a GUI (Figure 7).

Figure 7. Logical Inventory Collection for UMMT: MTG



To accommodate mobile backhaul synchronization, UMMT implements a combination of synchronization distribution methods (TDM-based, Synchronous Ethernet, IEEE 1588v2 PTP) so monitoring the clocking is also important. Again, this information can be presented in a GUI. Administrators can see if the clocking function is working or if it hasn't been defined. The easy-to-use GUI available with the solution is an alternative to using a CLI for each endpoint, and it results in less time and less complexity.

Beyond the physical and logical inventories, a third major feature of the Cisco Prime Carrier Management solution in its use to provide resource management for UMMT is the ability to view and analyze the network topology.

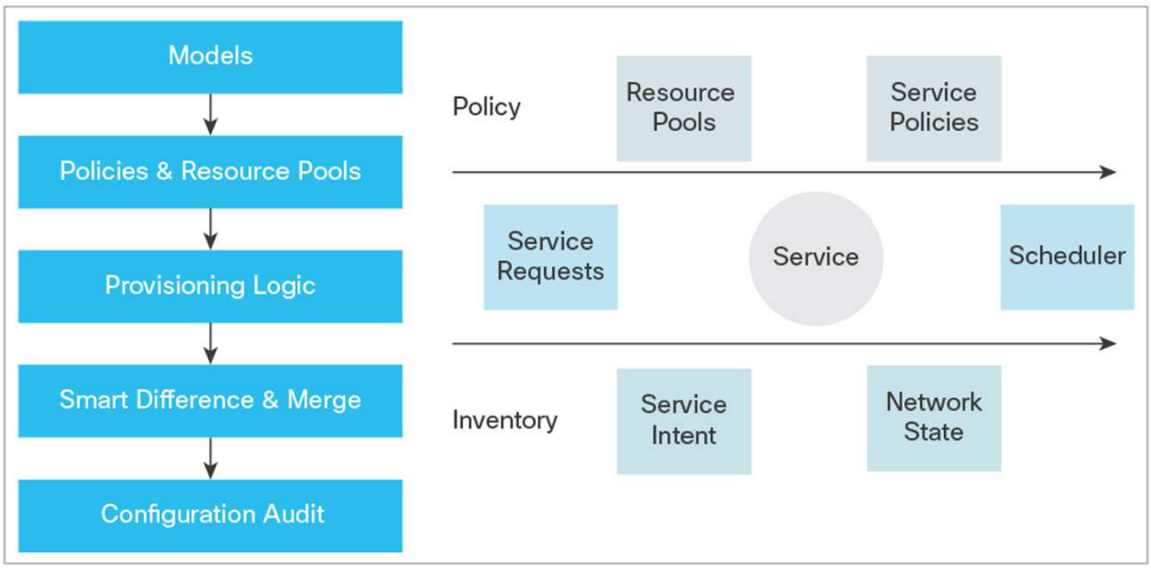
- **Topology** - With the physical inventory known along with details of the logical inventory of each device, the next step is to uncover the connections between the devices. This can be automatically retrieved by using the device genome, which can be identified by identifying the Layer 1 to Layer 3 protocol stacks used by the device, the routing information available in the routing table (accessible through CLI and part of the configuration of the device), and the termination point to the interfaces of the devices. Through this information the device behavior can be modeled, packet flow understood, and the device connections uncovered.

Perform Service Provisioning for UMMT

Service provisioning with UMMT begins with simple service requests or network orders. These must include user parameters, service policies, resource pools, route targets, and the templates that are models of different kinds of services (Figure 8). Additionally, the inventory should contain information about the devices, the network, the topology, and the interfaces. And the state of the network has to be aligned with that inventory. Then the services can be deployed and scheduled.

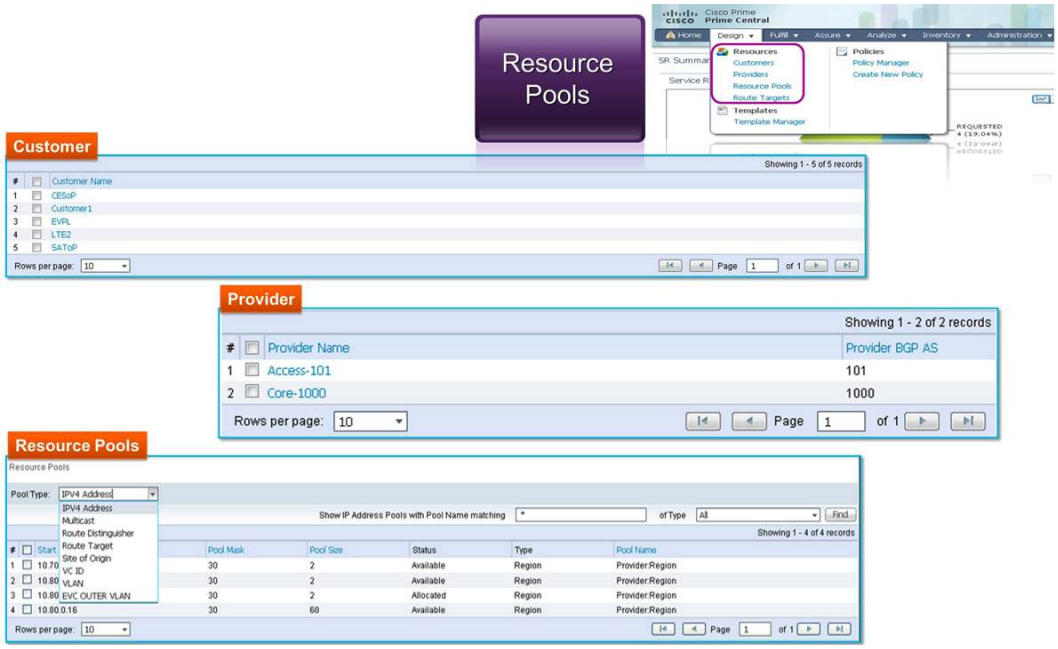
© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 8. Service Provisioning for UMMT: Process Steps



For UMMT, the administrator creates models of Layer 3 VPNs to define many different attributes for the different kinds of Layer 3 VPNs that may be created (Figure 9). Defining the service requires designating the customers and site with its associated devices. The provider is designated as an autonomous system and there can be multiple providers associated with a service. Finally, various resource pools are defined. With UMMT, for example, there are address pools for the provider to customer edge subnet on the Layer 3 VPN, virtual LAN (VLAN) pools, bridge domain pools, route target pools, and virtual circuit identification (VCID) pools. Resource pools contain attributes that can change from one service.

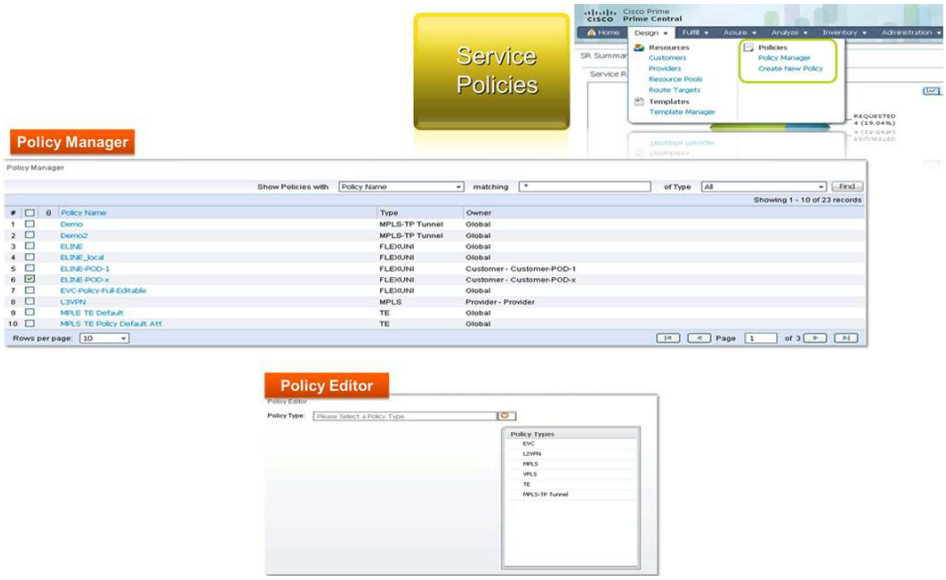
Figure 9. Service Provisioning for UMMT: Resource Pools



© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Policies provide defaults for resource pool attributes that can be used to simplify provisioning for the Layer 3 VPN (Figure 10). Using the policy editor, the defined resource pool attributes that draw resources from specific pools to provision the service are selected. There are built-in checks within this process. The configuration provisioning logic can determine if an interface's IP address is invalid, for example, and will create an alternate configuration to fix the problem with a valid IP address.

Figure 10. Service Provisioning for UMMT: Policy Editor



Each service configuration is the sum total of many little templates that contain attributes that would be extremely time-consuming to create and maintain manually. With Cisco Prime Carrier Management, the process is automated and relies on checking the configurations against the actual network inventory and topology in real time. The solution maintains models of different kinds of services, which makes it easier for multiple administrators to work on service creation.

Here is an example of steps for the provisioning of Layer 3 VPN services as part of UMMT:

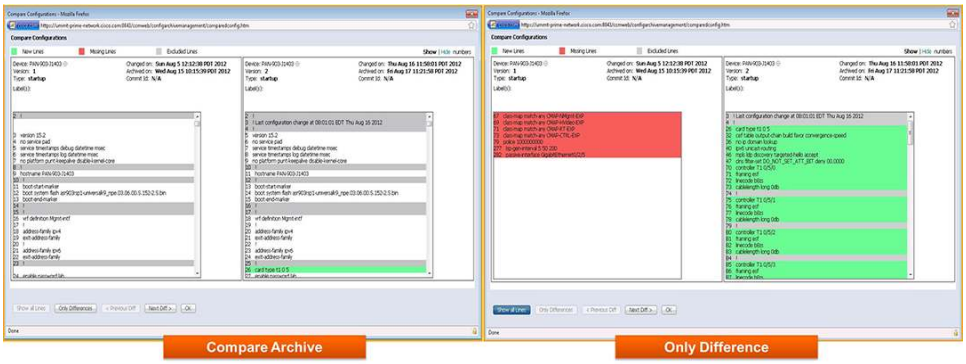
1. Create a Layer 3 VPN service from a main menu, then predefine, customize, or choose existing policies for the service in the policy editor (or use point-and-click provisioning).
2. Input the user information for the service.
3. Using resource pooling, associate a set of resources to deliver the Layer 3 VPN service (for example, a predefined range of VLAN IDs, IP addresses, route distinguishers, VCIDs, route targets, and so on). These are taken from resource pools when the service is provisioned and returned when the service is decommissioned.
4. Associate service policies to the Layer 3 VPN service. Policies can be predefined or customized using the policy editor, and templates can be used to capture CLI configuration or specific customer information (for example, quality of service [QoS] or IP SLA information) to further customize policies.
5. Provision the service by selecting the Layer 3 VPN service, creating a service request, validating specific attributes of the service, and deploying it. The Service Scheduler allows users to schedule when the service should begin running.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

6. A Configuration Audit (Figure 11) lets the administrator validate that the service is running as intended on the network. It will show any discrepancies in configuration in a log so that the configuration can be easily fixed if necessary.

An archive in Cisco Prime Carrier Management is maintained of the Layer 3 VPN configuration. Every configuration can be monitored and compared with changes made over time. Filters can display only differences, if desired. Administrators may choose to revert to previous configurations or to update configurations with more up-to-date ones. Every time a new device is added, the configuration for the device can be quickly uploaded, greatly simplifying and speeding up resource management and provisioning.

Figure 11. Service Provisioning for UMMT: Configuration Audit



Using Cisco Prime Carrier Management, a service model for a Layer 3 VPN can be created that contains many different attributes. The customer and provider are defined upfront. Then, using predefined policies in flexible templates and an easy-to-use GUI-based policy editor instead of a complex CLI, administrators can easily apply or modify policies. Resources can then be quickly assigned from resource pools. Predefined services pulled from a service pool let operators avoid conflicting information. The whole process is highly intuitive, easy, and fast. And configuration audits let administrators monitor, update, correct, and compare every configuration, simplifying resource management.

Perform Service Assurance for UMMT

The ability to uncover the configuration information of devices that was used in the resource management phase can be extended to investigate what services and newly configured technologies are in use. This service assurance process is possible with top-down and bottom-up approaches.

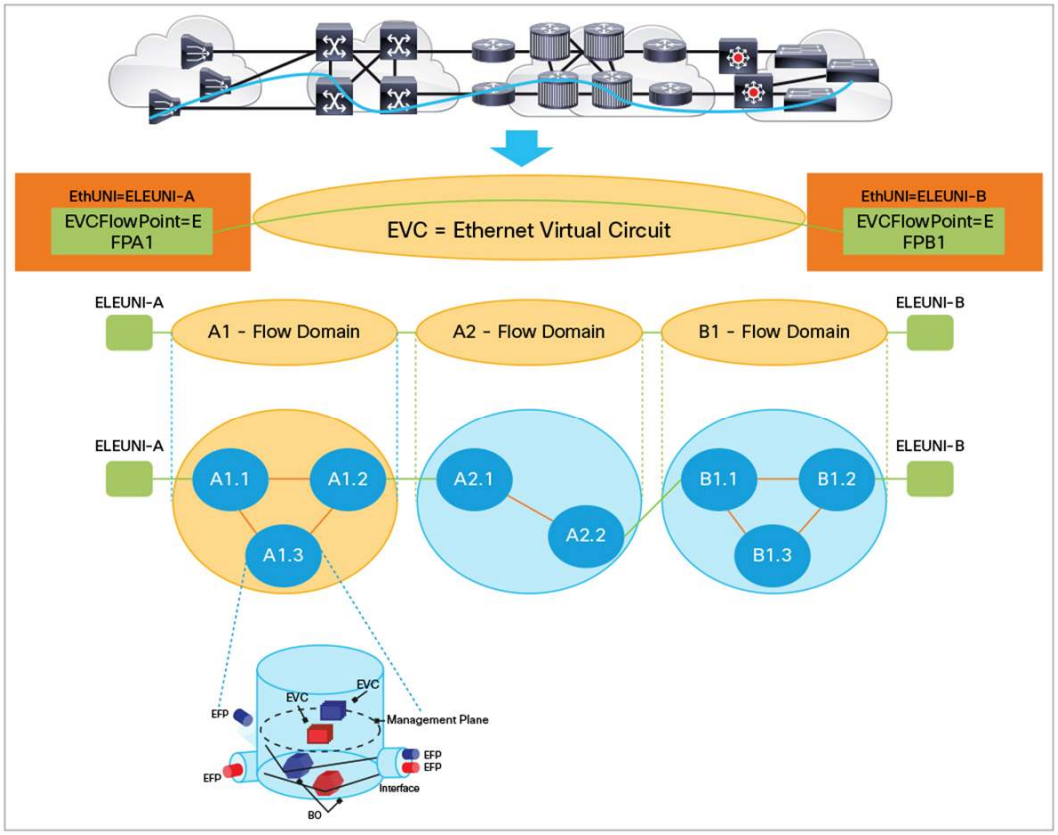
The top-down approach is used to analyze the technology from a standard point of view. The network layering concept involves looking at the logical separation of network resources that support transport for different types of information.

The bottom-up approach looks at flow domains or subnetworks. It involves partitioning a flow domain to describe the resources that are managed within the flow domain.

In the Ethernet Virtual Circuit (EVC) example in Figure 12, there may be multiple domains representing an EVC, including pseudowire and Virtual Private LAN Service (VPLS) domains. This represents the service layer, in this case running on a static, deterministic infrastructure that is represented by the LTE Layer 3 VPN. Analyzing the flow domain allows the administrator to describe the resources that are in the subnetwork and identify the building blocks that define the service. These building blocks may include Ethernet flow points (EFPs), VCIDs, VLAN tagging, VLAN Switching Element, VLAN Trunk Protocol (VTP), Spanning Tree Protocols (STP).

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

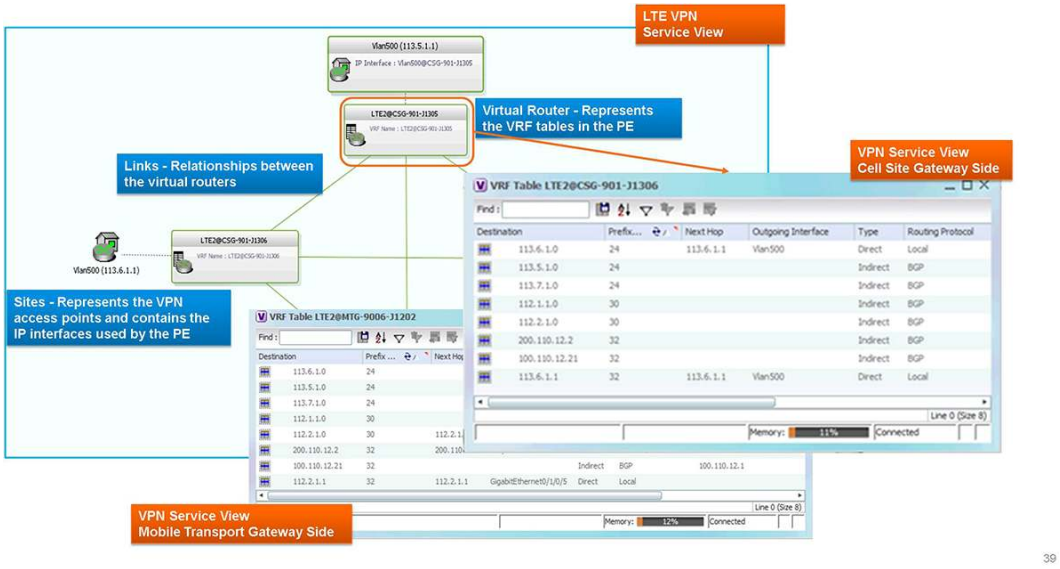
Figure 12. Service Assurance for UMMT: Multilayer Service Discovery



To monitor a service, the topology is displayed by Cisco Prime Carrier Management. In Figure 13, a hub-and-spoke VPN topology deployed in a full mesh is displayed. The individual links and how they are connected can be seen. The hub sites are visible and the administrator can navigate to see more information (for example, to see the route distinguishers, the import/export route targets, and routing tables). With this information, if one of those hub sites goes down, the administrator knows how the VPN is distributed, what users will be affected, and what hub sites and spokes will be affected. This view provides the kind of deep discovery that greatly enhances, simplifies, and speeds up service assurance. Cisco Prime Carrier Management can model all of the different UMMT services, including Layer 3 VPNs, VPLS, and Layer 2 VPNs.

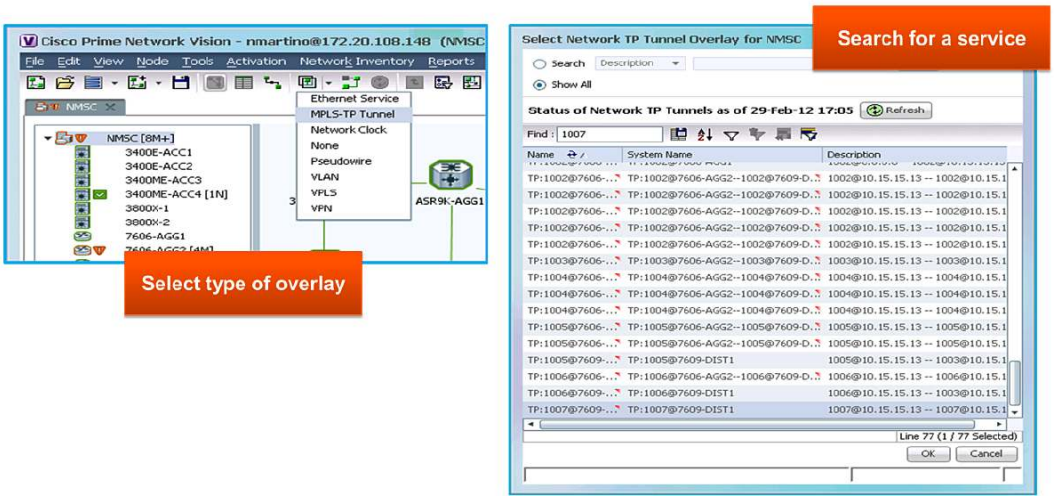
© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 13. Service Assurance for UMMT: LTE VPN Service View



Another tool in Cisco Prime Carrier Management that helps provide deep discovery for service assurance is the Service Overlay tool (Figure 14). It allows an administrator to see all of the services that have been provisioned on the network. Filtering can then be applied to search for a specific service. All devices and links that are part of a service are also displayed (for example, VPN, pseudowire, VLAN, MPLS-TP). As the output is displayed, the devices not providing the service are grayed out. Those that belong to the service are shown in color along with their links. All IP next-generation network (NGN) services can be seen with this tool.

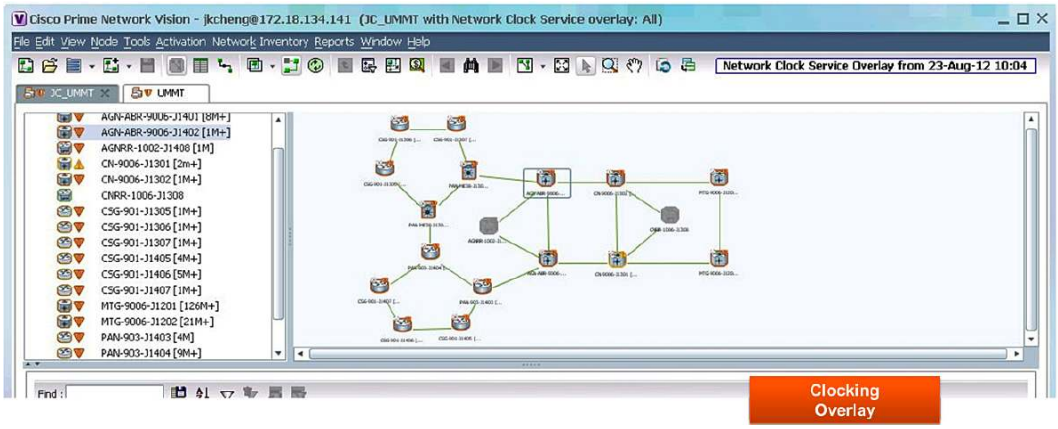
Figure 14. Service Assurance for UMMT: Service Overlay Tool



Another view shows a map of device clocking (Figure 15). Different options allow viewing one or many network clocks, and seeing which devices a clock has enabled. Again, a navigation menu provides more detailed clock information.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 15. Service Assurance for UMMT: Clocking Overlay

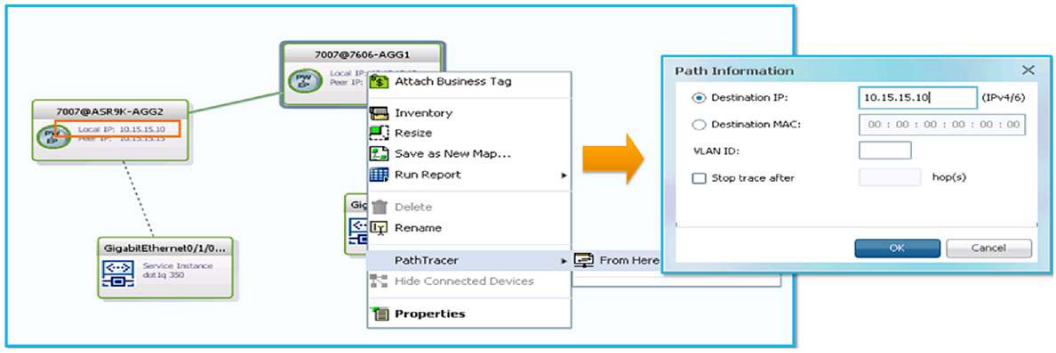


Another tool from Cisco that is useful in service assurance is the Path Tracer. Utilizing the network model displayed in Cisco Prime Carrier Management, the Path Tracer is used to define the health status of the network. The tool maps a service's path hop by hop and includes information from the multiple network layers. Devices in the route path are queried at a greater frequency to provide near real-time counter type statistics. The retrieved information contains network elements in the path, including all properties at Layer 1, Layer 2, and Layer 3, plus alarm information, counters, and more. With Path Tracer, multiple paths between the source and destination can be viewed from different points in the network. All of this information can be saved for use in troubleshooting.

Figure 16 is an example of the use of Path Tracer to uncover the health of a pseudowire tunnel used in UMMT. The Path Tracer can be launched from the service view. It can also be launched from a bridge, switching entity, Ethernet interface, Ethernet flow point, VLAN interface, ATM virtual circuit, data-link connection identifier (DLCI), or IP interface entry point.

The tunnel endpoint of the pseudowire is selected and traced to its peer IP address utilizing a Layer 3 VPN through the MPLS core. The dialogue box displays the full list of all devices that are potentially involved in this service.

Figure 16. Service Assurance for UMMT: Path Tracer

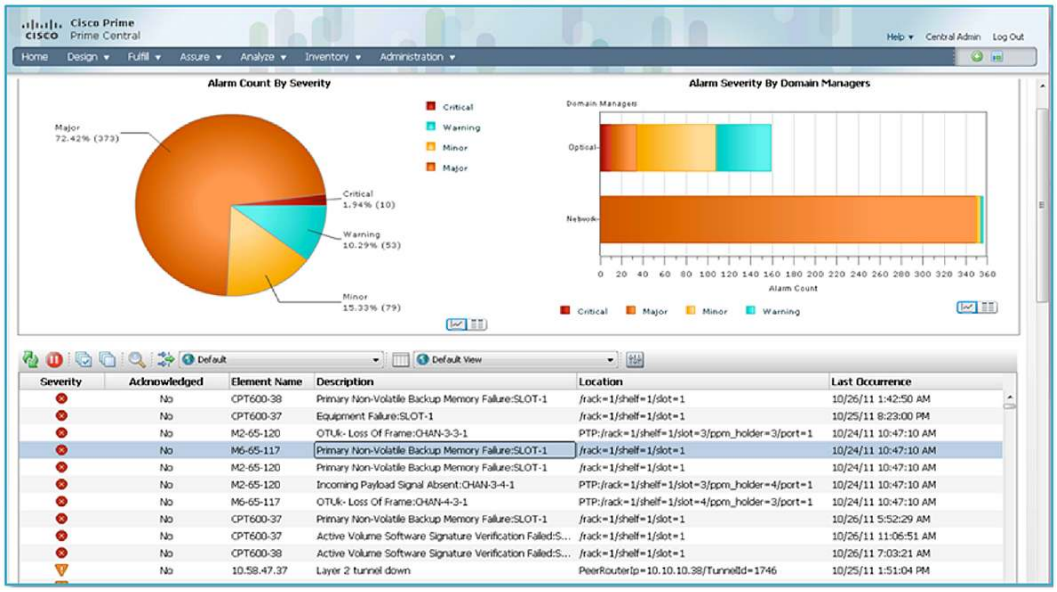


Cisco Prime Carrier Management features a centralized dashboard with a view of all of the combined alarms that are coming from the different domain managers (Figure 17). It is able to collect all the information coming from the domain managers (Cisco Prime Optical for optical devices, Cisco Prime Network for the IP routers and switches) that can send Simple Network Management Protocol (SNMP) traps, syslogs, and event notifications.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Administrators can navigate to see the alarm links from the combined IP and optical view. Since routers and switches can be very chatty based on network events it is important to reduce the number of alarms that are reported. Cisco Prime Carrier Management also conveys threshold-crossing alerts that have been defined and raised.

Figure 17. Service Assurance for UMMT: Alarm Dashboard

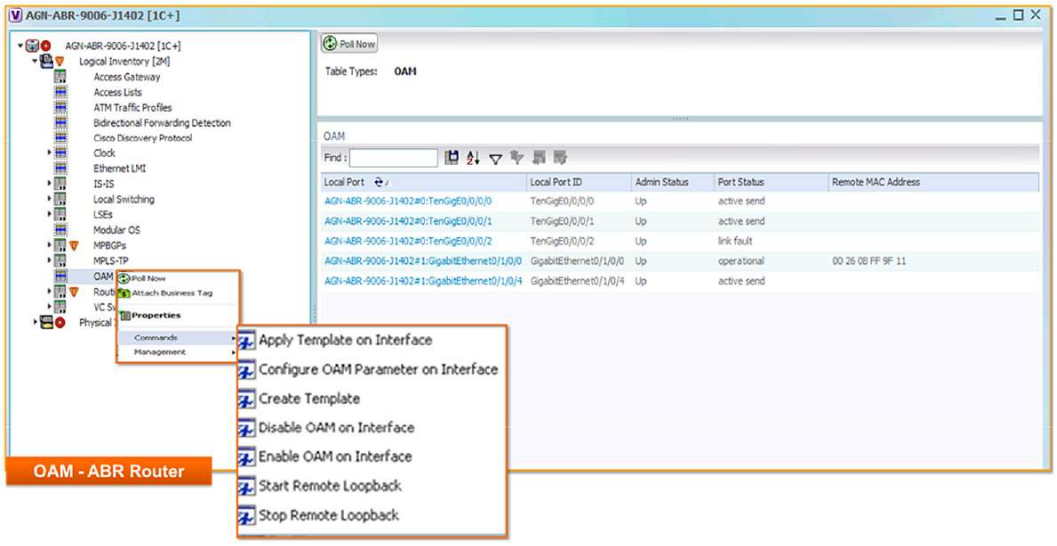


Through the modeling of the relationship between logical and physical inventory and the relationship between topology and services, Cisco Prime Carrier Management can help reduce the number of alarms and ultimately reduce the time required by administrators to identify the root cause triggering an alarm. One way to reduce alarms is removal of duplicate events. The MPLS network behaves differently from a transport network. Devices in UMMT networks are sending multiple traps and events. De-duplicating and associating these alarms can help in reducing the total count. The system can poll status to confirm suspicious alarms before notifying the operator that they are false alarms. Alarms are automatically correlated to identify causality without the need to develop a codebook or rules. There is local correlation (alarms emitted within a single network element) and topology-based correlation (alarms from multiple network elements). The modeling of the network relationships using these two types of event correlation allows for alarm reports to be included in the logical topology. They help identify the real root cause of a specific problem or suspected problem, which can be extremely useful in a UMMT network with 700 to 800 events happening simultaneously.

OAM functions can also be modeled to see which OAM functions are enabled on which interfaces (Figure 18). Administrators can configure OAM through predefined functions. This again is based on Cisco Prime Carrier Management's ability to model the network, providing operators with the tools to do troubleshooting without having to use a CLI with much simpler operational diagnostics.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 18. Service Assurance for UMMT: Configuring OAM



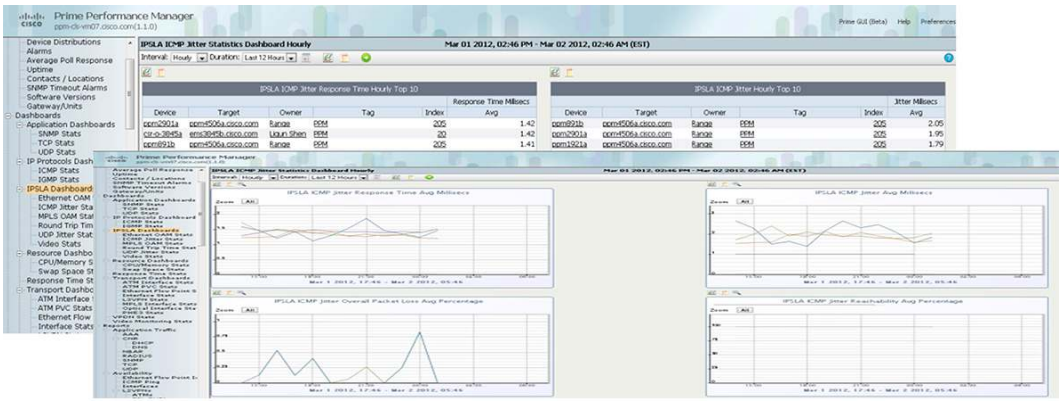
Cisco Prime Carrier Management helps enable the collection of more than thousands of different key performance indicators (KPIs), and this information is combined in a dashboard that can be used for performance monitoring. The dashboard can be customized to help enable an administrator to monitor only a part of a network, if desired. The dashboard features navigation menus in a tabular format. Thresholds, number of interfaces, and number of devices can all be displayed.

Different types of QoS and IP SLA reporting are also available, based on whether products are used in standalone or suite mode. In standalone mode, Cisco Prime Performance Manager discovers the network elements and starts collecting key performance statistics based on the device type and what reports have been enabled. In suite mode, Cisco Prime Performance Manager discovers the network elements as they are added and as Cisco Prime Central discovers them and adds them to the inventory. The integrated suite adds a lot of functionality related to device discovery and facilitates the ability to navigate into an interface and cross-launch directly into a utilization report for that interface without having to go through Cisco Prime Central.

Figure 19 shows custom dashboard views of performance monitoring for a pseudowire for a VLAN. Time intervals may be viewed, and it is possible to navigate in the dashboard display to look at ever smaller time intervals. Additionally, QoS and IP SLA policies may be viewed.

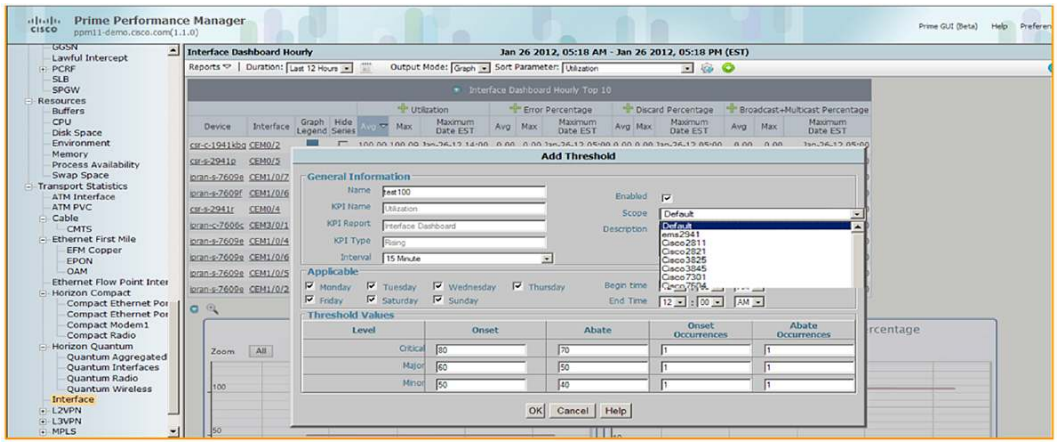
© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

Figure 19. Service Assurance for UMMT: Performance Monitoring



Cisco Prime Carrier Management provides the ability to navigate into an interface and associated device for a view in real time of the interface utilization over time along with many other details. Thresholds are rules or policies that determine whether a KPI has risen or fallen to a particular level and when an event should be forwarded. Within the service assurance reports, if a plus appears next to a particular KPI, such as utilization, error percentage, or discard percentage, clicking that button displays an “add threshold” window (Figure 20). This helps enable the administrator to set intervals for monitoring (for example, 5 minutes, 15 minutes, daily, hourly) and the onset and abate values and occurrences and abate occurrences. After three instances, the administrator may want to stop reporting on it so the scope and threshold for particular devices can be customized.

Figure 20. Service Assurance for UMMT: Threshold Crossing Alerts



Summary

The Cisco Prime Carrier Management solution helps to dramatically reduce the time and complexity required to deploy UMMT services by enhancing and simplifying the service lifecycle through resource management, service provisioning, and service assurance phases. The suite solution is feature rich, utilize easy-to-use GUIs and graphical representations, and eliminate the need to know and work with myriad device CLIs. Policies can be adapted to specific operational needs. The products include configuration management tools that monitor activity on the network and improve QoS and SLAs by using different troubleshooting tools. Operators gain a faster understanding of service impacts and reduced time for problem resolution, and the proactive monitoring features enhance customer loyalty.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.

About Cisco Prime

The Cisco Prime portfolio of IT and service provider management offerings empowers organizations to more effectively manage their networks and the services they deliver. Built on a service-centered foundation, Cisco Prime supports integrated lifeccle management through an intuitive workflow-oriented user experience, providing A-to-Z management for evolved programmable networks, mobility, video, cloud, and managed services.

For More Information

For more information on Cisco Prime for Service Providers, email ask-prime-sp@cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA C07-729494-00 10/13

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information.