Are Managed Network Services the Way to Interconnect Grid Sites?

What Role will Web Services Play in Managed Networks?

Alan J Weissberger
aweissberger@sbcglobal.net

I. Introduction

With the maturing of the enterprise grid market, it is surprising that there has been so little discussion (and even less press coverage) detailing how enterprise grid sites will be inter-connected. Many questions arise. How will the objective of true virtualization of computing and storage resources be realized? Will the connections be based on dedicated private lines or private networks, optical channels on demand, Layer 2 (FR, ATM, or Ethernet) VPNs, IP-VPNs, IP-MPLS VPNs, or some other new network technology? Will the network scale to accommodate a lot more users and more interconnected grid sites? What access network will remote users/ satellite sites use to "dial-in" to access the grid computer complex? Who will manage such a network, what will be managed, and what are the relevant Service Level Agreement (SLA) parameters between customer and the service provider? What role, if any, will web services play in service level management, especially the provisioning and monitoring of SLAs?

The generic answer to all of the above might be a set of "**managed network services**." While service providers continue to focus intently on growing revenues while cutting costs, end-user adoption of managed services continues to rise as the benefits to those users become apparent. Companies in a variety of industries are realizing business improvements, productivity gains, and cost reductions—as a result of out-sourcing some network services to service providers and focusing instead on their core business strengths.

Service providers are deploying several types of managed services now, especially different types of virtual private networks (**VPNs**), while developing integrated-services (e.g. data, voice, video, storage) capabilities to meet growing end-user requirements beyond site-to-site connectivity. These developments continue to have significant implications in terms of service-provider profitability, customer loyalty, and differentiation in the market. At the same time, the underlying carrier infrastructure is evolving toward a **Next-Generation Network (NGN)*** with more intelligence and better user control. This is creating a multitude of new service opportunities in the small business and enterprise markets

*** Please refer to the Webtorials article, "In Search of the NGN," published January 2005**

http://www.webtorials.com/main/newsletters/dcti/NGN-article.pdf

Definition: What's Being Managed in the Managed Network?

The Service Provider (SP) offering a managed network service will manage either the CPE, the network services itself, or both. For a managed network service, levels of performance/QOS, security, availability, and reliability may be specified as part of a **"Service Level Agreement" (or SLA).** For that reason, many refer to "managed services" as being SLA based. At this time, each SP defines his own service dependent set of SLAs (the DMTF Utility WG is chartered to work on definition of SLAs, but this work item is on hold at this time, in deference to work on server provisioning and virtualization.).

II. Highlights of Cisco Webinars on Managed Services and IP/MPLS Update:

A. Types of Network Services

Cisco defines **four classes of network services**, of which the latter three are managed in some way. They see a huge revenue potential in the Integrated (VPN) type of service.

-**Connectivity Service**: basic transport/ connectivity of end points. Examples include DS1/E1, DS3/E3 private lines, Frame Relay virtual private lines, dedicated IP private network, or a broadband access network (xDSL, PON, WiMAX, etc).

-**Provisioned Service**: managed CPE; connectivity + design, installation, monitoring. Examples include SONET/SDH or metro Ethernet Private Lines, Layer 2 (FR, ATM) VPN, Layer 3 (IP or IP-MPLS) VPN, Ethernet Private LAN/ VLAN.

-**Integrated Service**: selectively tailored to a class of customers; provisioning might include bundled services and/or partner apps. Examples include an IP VPN with built-in: security features, IP telephony, and/or IP video streaming; storage and computer-to-computer high speed data transfers over the same managed network.

-**Customized Service**: most complex; tailored to each customer; integration of services that meet customer's specific needs. An example here might be a wireless voice/ data service used to control or reconfigure a broadband wire-line service (e.g. boost the bandwidth).

-**Cisco's Managed Services Strategy is to maximize SP revenue opportunity through network and CPE based managed services.** The managed network based services include managed connectivity (traditional L1-L3), managed value add services (L4-L7), fully managed application services, and business process outsourcing.

B. Survey Results- What types of network services have end customers deployed?

Cisco conducted an **"Enterprise-Service Provider Connect"** survey and found that:

-Packet based technologies are growing in popularity for connectivity (assume these technologies to be IP and Ethernet, as Frame Relay is almost 15 years old).

-Redundancy for connectivity is not nearly as widespread as expected. Less than 28% in the commercial segment had a redundant (e.g. back-up/ standby) WAN connection.

-QOS WAN connections are not widely deployed (despite years of hype about IP QOS). Only 33% in the commercial segment had implemented QOS mechanisms over their WAN infrastructure.

-Security needs to be built in to the underlying managed service, rather than being an "add-on" service

-End customers are interested in using additional managed services, but Service Providers (SPs) need to build up a level of trust and partnership with them.

-Cost effectiveness is cited as one of the common reasons for choosing the various types of managed network services to deploy from the SP.

-**IP VPN was by far the most widely deployed managed service** (but not the most profitable for SPs!). Cisco reports that 74.5% of Small Business, 66% of Mid Enterprise, and 67% of Large Enterprises have deployed some form of IP VPN (IP Sec, IP MPLS, etc). A much lower percentage of users have deployed Metro Ethernet, Managed Security, or Managed Voice services.

-Carriers are using **IP VPNs as the foundation managed service** and then layering additional services on top of that service. For example, **security, storage, IP telephony, IP video would overlay an IP VPN** (Cisco did not specifically mention if the IP VPN was based on IP-MPLS as per RFC 2547bis, so we assume that it could be either IP-MPLS or an IP Sec VPN).

-In answer to a question from a caller on the Webinar, Cisco stated that **SONET/SDH private lines and metro Ethernet were the most profitable managed services for the SP.** *However, there was no mention of what is being managed, e.g. availability, time to restore service after an outage, guaranteed bit error rates, etc.*

C. Cisco's views on the necessary ingredients for a successful managed service:

-**QOS is critical** to providing the guarantees that are an integral part of a managed service. However, only one in three enterprise customers has deployed QOS based WAN connections. It was said that some business customers need 6 or 7 levels of QOS to support their apps.

-QOS interoperability across carrier domains is a huge unresolved issue**- this problem needs to be solved for wider deployment of "long haul" managed services.** In

particular, connecting grid sites in different countries with a VPN would require inter-carrier QOS. *Please see* **D. Key Messages from March 16th IP/MPLS Update** *below, for Cisco statement on "inter-provider solutions."*

-Security should be part of an "**integrated services VPN**." SLAs should specify the various types and levels of security. This might include: firewall, authentication, authorization, identity management, encryption, intrusion detection and prevention, anti-virus, anti-worm, etc.

-In their vision of the IP NGN, Cisco suggests collapsing the 7 layer OSI protocol stack into three layers. From top to bottom, these are:

L3 **Application layer**: Converged applications including comm., storage, mobile apps, **web services**, and an IP contact center/ help desk.

L2 **Service Control layer**: Authentication, personalization, privacy, identity, policy, and billing might be included here.

L1 **Secure Network layer**: Transport, access aggregation, intelligent edge, and a multi-service core make up this layer.

-Cisco's Integrated Services Router (ISR) product line was touted as "the delivery vehicle for managed services." It includes a "1 touch" provisioning capability, which accelerates service provider time to revenue. By speeding up provisioning time, provider gets services to market faster and realizes revenue sooner. ISR provides embedded security, voice/IP telephony, high availability and resiliency, and upward compatibility.

-Monitoring capabilities are important- not only bandwidth utilization measures, but the usage pattern of applications which are running on the managed network. Cisco did not say who would provide such monitoring capabilities.

-Cisco says they are partnering with service providers (like BT) to realize their vision of managed services within Next Generation Networks (NGNs). They say that BT is first among the carriers with a "tighter systems integration approach with the Applications layer." Cisco is also partnering with IT outsourcing firms like IBM, HP, and Accenture to better deliver managed services that involve applications and system integration.

- Cisco Summary: managed services help SPs move up their customer's value chain, decrease churn, and increase ARPU. They are of sizable interest to end users, but require network intelligence (e.g. QOS, integrated services VPN, etc) that does not exist yet in today's networks for the vision to be realized.

D. Key Messages from March 16th IP/MPLS Update webinar

1. Over the past year, Cisco has delivered several new leading IP/MPLS technologies: Virtual Private LAN Service (VPLS), IP/MPLS Management, EIGRP (optimal path routing) support over MPLS VPNs.
2. Market requirements are pushing IP/MPLS based inter-provider solutions.
3. An inter-provider enables SPs to extend their global footprint with minimal investment. This increases service value, while reducing CapEx/ OpEx.
4. Cisco is delivering industry leading technologies (e.g. multicast, traffic engineering, load balancing, inter-provider network management, etc).

III. The role of Web Services in Managed Networks and Applications Sharing

A. Use of Web Services for Service Level Management (SLM) of NGN Services

This editor (and at least two SPs) believe that Web Services (WSs) can be effectively used by SPs to manage NGN services, totally independent of the specific service or network technology. We refer to this capability as **Service Level Management (SLM)**, because the service -rather then the underlying network technology- is being managed.

Verizon refers to this SLM capability as "command and control" and has implemented over 70 applications on a WS platform. **BT** is using web services for control of many of their 21st Century Network Services. Other carriers may be using web services in a similar manner, but have not disclosed this for fear of losing their competitive edge.

Note that the use of WSs for SLM is independent of its use in building grid infrastructures, as per the Global Grid Forum (GGF) specifications (see IV. below).

Web Services – specifically, distributed services that process XML-encoded **SOAP** messages, sent over **HTTP** transport, and described using Web Services Description Language (**WSDL**) - are being deployed broadly. Web Services are used in a range of application integration scenarios: from simple, ad hoc, behind-the-firewall, data sharing to very large-scale Internet retailing and stock market trading. Increasingly, Web Services are being applied in grid computing scenarios that are being standardized by the Global Grid Forum (GGF). **Web Services provide interoperability between software components that can communicate between different companies and can reside on different infrastructures.** This solves one of the most critical problems that customers, software developers, and partners face.

The benefits of WS's for use in SLM include:

-Much faster provisioning with fewer telco resources engaged in the process,
-Modularity and extensibility of service level management without dependence on the underlying network technologies,

-Structured software interfaces between the SP network management system (NMS) and ISV/ OSS vendors (vs proprietary interfaces that are time consuming to orchestrate and are very difficult to maintain/ modify),
-Simpler interactions with ISPs and other service providers that have endorsed the "WS infrastructure" paradigm.

B. Web Services can provide SLM Functions within Managed Networks

Specifically, we are suggesting the use of Web Services technology for four distinct functional blocks of SLM+:

1. Provisioning of NGN services (e.g. multi-site grid interconnection, MPLS or optical VPNs, Ethernet virtual private line/ virtual private LAN, point to multipoint video distribution, residential video services, enhanced web phone, etc). This includes a subscription management protocol with ability to specify and negotiate SLA parameters.

2] End to end performance monitoring/measurement/compliance assessment of SLA parameters (by the SP or a 3rd party). Performance management reports may be scheduled or obtained via user query, asynchronous alerts or event notifications may be requested when specific SLA parameters are not met by the SP.

3] Other service level management functions of interest (eg. service advertisement by SP and service discovery by end user, access to distributed directories or service registries to find a desired network service and associated SP, re-negotiation of SLA parameters at service activation time as well as once the service is operational, etc.)

4] OSS integration and structured software interfaces between EMS-NMS and between NMS-OSS. This would include evolution of OSS vendor platforms (e.g. billing, CRM, inventory management, etc) to a web services based infrastructure.

+ Please contact the author directly for more information about a related research project which involves the use of WS's for NGN SLM.

C. AT&T Web Service Connect: Creating an On-Line Extranet Environment to facilitate eBusiness Services

In November 2004, AT&T introduced an Internet-based business services network that dramatically reduces the cost, risk and complexity of integrating the "networked enterprise" across suppliers, partners and customers, enabling true interoperability and collaboration. **AT&T WebService Connect** uses Web Services to help companies and government agencies easily and securely connect, create, share and manage business processes and applications with their suppliers and customers. The service creates an environment based on a service-oriented architecture, where applications can be

developed by enterprises or third parties, incorporated into a business process, and then shared on demand across the extended enterprise. [Editors Note: this is the essence of eBusiness on-demand, as promoted by IBM.]

AT&T **WebService Connect** is a comprehensive solution that delivers a fully secure, managed platform for businesses to share their critical services and information with partners and customers to drive additional revenue and efficiencies in their businesses. Because the service is based on open standards, companies can easily and securely share information, regardless of the diverse systems and applications used by their suppliers and customers.

"By leveraging our investments, infrastructure and expertise, businesses and government agencies can lower their total cost of ownership to integrate applications, data and critical business processes across their extended enterprise," according to Eric Shepcaro, AT&T Vice President, Application Networking. Thomson Financial, an operating unit of The Thomson Corporation and leading provider of information and technology solutions to the worldwide financial community, is one of the first customers of the new AT&T service. Jeff Scott, chief information officer at Thomson Financial states, "Using AT&T WebService Connect, we will be able to deliver even greater value because this open, standards-based platform puts our customers in the driver's seat. They can use our services and applications on demand--in the format and on the systems of their choice."

Previously, two traditional approaches have been used by enterprises to share information and applications with partners: point-to-point connections or industry-specific communities. Over time, these approaches have proven to be both technically complex and cost prohibitive for today's any-to-any business integration model to be established and maintained. Web Services are much more adept at delivering eBusiness applications.

The Web-based business services network provides a framework for companies to rapidly and flexibly establish trusted connections with their diverse business units, partners and customers, without adding infrastructure. Connectivity to the network can be established with any application supporting Internet communications via the Simple Object Access Protocol (**SOAP**), version 1.1, the File Transfer Protocol (**FTP**), and the Electronic Data Interchange-Internet Integration (**EDIINT**) AS2 protocol.

In addition, the service provides Web service gateways for exchanging data via additional Internet protocols, including Hypertext Transfer Protocol (**HTTP**) and Simple Mail Transfer Protocol (**SMTP**). No particular brand of software is required to connect an application with the network as long as the application employs one of the supported open communication standards.

The intelligence in the network "translates" the differences in communications protocol, data format and security standards. As a result, the network enables customers to connect to applications that are controlled and managed by separate organizations.

Once a connection to the Web-based business services network has been configured, ongoing management of the business process is as simple as viewing a Web page. Administrators can view transaction histories, errors, usage and other detailed reports of the status and state of the integrations. These reports provide an end-to-end view over all the services involved in the integration, including those behind a partner's firewall, allowing administrators to view and understand errors across the entire integration.

By subscribing to the AT&T service, businesses benefit from a solution based on open standards, which lowers the total cost of ownership and allows them to communicate with all their partners and customers, regardless of their technical infrastructure.

IV. What else is needed in a Managed Network Service for Grids?

We think that the selection of network connectivity and managed services for grids decomposes into the following set of unanswered questions and issues:

-What network technology and associated SLA/QOS parameters will be used to interconnect the grid computer/storage sites to realize true virtualization? This means a combination of high bandwidth for computer interconnection, with low latency for storage and real time applications (e.g. simulations). The choices include: high capacity private lines (with managed firewall), IP-MPLS VPNs, Ethernet-MPLS VPNs/ virtual private LANs/ geographically dispersed VLANs, or optical channels on demand (via IETF/ITU specs for GMPLS or OIF UNI/NNI).

-What network technology and associated SLA/QOS parameters will be used for FIXED broadband access to the grid sites by remote offices and smaller, satellite sites. The choices here include business class- symmetric DSL (not very good in the US), fiber access PONs, or WiMax [We do not think that mobile or nomadic access to grid sites is a realistic issue at this time].

-What CPE should be managed and exactly what aspects of operation are managed? Who provides maintenance and hardware/ software upgrades?

-Can the SP adequately manage all aspects of the service? In particular, can the SP's security solution and intrusion detection capabilities be trusted? Is it sufficiently comprehensive and robust? What about identity management and federation?

-Who will monitor and mange the SLA parameters associated with the managed network service? Is SP monitoring of SLAs a conflict of interest? Who will assess penalties for non- compliance? What type of SLA reporting and alerting will be available to the end customers?

-What role will **Web Services** play in the managed network used to interconnect grid sites and provide access to remote site users? If the equipment is managed, will it have

web services capabilities for security and authorization, reliable messaging, policy, addressing, federated identity, equipment management, etc? If not, will the end customer be responsible for procuring and maintaining the WS middleware throughout the enterprise network? Does that imply that end point equipment running WS code is to be co-managed by the SP and customer? Can you envision the finger pointing that would result?

-Should Application layer routing be considered? Should a router be able to function as a WS intermediary in order to inspect or append WS/ SOAP headers, e.g. for WS reliable messaging and WS security?

V. Conclusions

- We believe that managed services, particularly those that use IP v6 addressing, together with metro optical Ethernet (a hybrid IP- Ethernet VPN?) offer the most potential for grid site interconnection and remote access to the grid computer complex.

- Performance, cost effectiveness and scalability will be key issues to consider by the SPs in selection of the network technology. SLA parameter selection, negotiation, and compliance assessment will be of paramount importance to end customers in their evaluation of managed services from a SP. Maintaining the SLA's when inter-networking between service providers should be carefully considered when one or more endpoints can not be reached by a single SP's network.

- The previously posed questions (in IV. above) must be worked out between the end customer and SP for the managed service to be effectively deployed.

Invitation: Please contact the author directly if interested in discussing any of these complex issues. Phone: 1 408 863-6042 or *aweissberger@sbcglobal.net*