Managed Services: Taking Advantage of Managed Services in the High-End Enterprise

What You Will Learn
This document explores the challenges and solutions for high-end enterprises using managed services. Two key reasons for a large enterprise to adopt managed services follow:

- Consistent and reliable services with a global reach
- Operational cost reductions

Cisco® has a successful track record with both enterprises using managed services and services providers offering managed services. This document provides an overview of the key challenges and solutions for the high-end enterprise using managed services.

Introduction
Service providers have offered their business customers managed services for broadband connections, VPNs, security services, and IP communications for years. These services are attractive to smaller businesses that do not have dedicated IT resources. Larger businesses have dedicated IT staff and usually purchase only broadband connections from service providers.

Recently large businesses are realizing their IT staff is a valuable strategic resource that they can use to improve profits in many ways. However, the IT staff is often allocated to running the network and maintaining the equipment to support the network and the employees. One way to free the IT staff is to outsource some of the network operation and take advantage of managed services. Figure 1 shows how enterprises can reduce costs of running their network by using managed services.

The shift to managed services is especially challenging for the high-end enterprise because managed services entail additional complexities. The following sections explore some of the unique challenges large enterprises need to address while shifting to managed services.
Before discussing the challenges of shifting network operations out of the enterprise, some background on typical managed service offerings and benefits is needed. The basic managed services that high-end enterprises use follow:

- Broadband connection that includes the physical layer (T1/E1, DS-1, DS-3, etc.) and the data link layer (Ethernet, Frame Relay, ATM, etc.)
- VPNs that tunnel the enterprise’s traffic over the shared network from the service provider: The VPN is dedicated to the enterprise, and it can be customized in a variety of ways to meet the needs of the enterprise. VPNs can extend out to remote employees, and they can be secured from unauthorized access. The performance of the VPN and the priority of the traffic carried by the VPN are specified in the service-level agreement (SLA) between the enterprise and the service provider.
- Security services that include firewalls to protect internal addressing, control access to enterprise resources, authenticate users of the enterprise network, and control access to router ports: Most security services also include monitoring for intrusions to the enterprise network and preventing intruders from accessing the network. Additionally, the service provider offers vulnerability assessments and up-to-date information about protecting the enterprise network.
- IP communications for voice, multimedia, and collaboration inside and outside the enterprise: Call processing, unified messaging, presence, video communications, collaboration, mobility, and soft clients are included in this service.

Figure 2 shows how these basic services support more advanced services such as collaboration and shared business applications. The figure also shows the typical large enterprise places in the network: headquarters, branch office, and remote access.
In addition to the basic service offerings, a managed service offers the following:

- Remote monitoring for all customer premise equipment (CPE) allocated to the service
- Remote configuration and troubleshooting
- An SLA between the service provider and the enterprise
- A term of contact for a year or more
- CPE title held by the service provider or the enterprise

In summary, a managed service is an IT service such as broadband, VPN, security service, or IP communications that a service provider offers an enterprise in compliance with a SLA. The following sections discuss some of the challenges for an enterprise in using managed services.

**Getting Consistent Managed Services Globally**

Most large enterprises have the following network elements:

- One or more regional or headquarter campus locations where most of the information technology resources are located (refer to
- Many remote branch locations that usually do not have information technology staff
- Secure remote employee access from public broadband facilities
- A data center for central servers and applications that employees and authorized customers and partners must be able to access
- WAN to connect the sites and provide optimized traffic routing

Additionally, the enterprise network elements are deployed globally.
Figure 3 shows a typical high-end enterprise campus network that is deployed in the headquarters or large regional office. Managed services from the service provider come in through the WAN or the Internet. Some high-capacity data-center services such as storage area networks have dedicated Fiber Channel access to transfer huge amounts of data quickly.

**Figure 3.** Regional Campus or Headquarters Campus in a Large Enterprise

Figure 4 shows the wide variety of branch offices that the enterprise IT staff has to manage remotely. Often these branches are located in a different country from the headquarters. For both diversity and cost savings, the enterprise uses multiple service providers for WAN connectivity and managed services. Employees in the branch offices need to have the same IP communications services and collaboration tools as the employees in the headquarters office. The branch-office employees also need access to corporate resources in the data center. Finally, because the branches are sending and receiving traffic over service provider networks, access security and data encryption are needed to prevent unauthorized use and protect confidential information.

**Figure 4.** Branch-Office Architecture Variety
Figure 5 shows the WAN that connects the headquarters to the branch offices. In addition to traditional leased lines, enterprises use Frame Relay, ATM, and IP/Multiprotocol Label Switching (MPLS) to transport their traffic.

**Table 1.** WAN Transport Technology Differences: Ethernet Far Surpasses Other Alternatives

<table>
<thead>
<tr>
<th></th>
<th>Ethernet</th>
<th>FR</th>
<th>ATM</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scalability</strong></td>
<td>10M to 10G</td>
<td>56K to 45M</td>
<td>1.5M to 622M</td>
</tr>
<tr>
<td><strong>QoS</strong></td>
<td>Supported</td>
<td>Limited</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Service flexibility</strong></td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Protocol efficiency</strong></td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
</tr>
<tr>
<td><strong>IP optimized</strong></td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><strong>Provisioning</strong></td>
<td>Fast</td>
<td>Slow</td>
<td>Slow</td>
</tr>
<tr>
<td><strong>CPE: per-port-cost</strong></td>
<td>$</td>
<td>$$</td>
<td>$$$</td>
</tr>
<tr>
<td><strong>Cost/Mb</strong></td>
<td>4</td>
<td>$$</td>
<td>$$$</td>
</tr>
</tbody>
</table>

Table 1 summarizes some of the different WAN transport options. Ethernet and IP/MPLS technology usage is increasing, but in many locations leased line, ATM, or Frame Relay are the only options for WAN transport.

Table 1 shows many advantages of Ethernet over Frame Relay and ATM, but switching over to Ethernet incurs expense from tight budgets to provide the equivalent transport capabilities. However, for the enterprise that uses managed services from a service provider, the transport technology is less relevant to the network infrastructure. With a managed broadband service, the service provider can gracefully migrate the WAN transport to the higher-bandwidth Ethernet option.

The migration to Ethernet is a key step for high-end enterprises to take toward consistent managed-service capabilities in their global infrastructure. Because of the work of global standards bodies such as IETF, IEEE, ITU, and Metro Ethernet Forum (MEF), Ethernet services are evolving into ubiquitous offerings that network engineering teams understand.

VPNs services on top of the WAN transport can deliver further network service consistency for enterprises. VPNs provide tunnels between the different sites in enterprise networks, and they provide a tunnel from the remote employee to the enterprise. VPNs can be point-to-point, routed, or encrypted. With the VPN service, the enterprise has a standards-based toolkit to efficiently...
move traffic around the global enterprise. Further, the VPN service allows traffic to be classified and handled in a manner that best meets the needs of the enterprise.

What Is a Managed VPN Service and How Does It Benefit Enterprises?

When an enterprise uses a shared network to carry its traffic, the enterprise IT staff needs to be sure the traffic is delivered properly and without delay. Further, to comply with regulatory requirements and confidentiality requirements, the traffic must be segregated and often encrypted as it passes over the shared service provider network. The enterprise can choose to either manage the CPE or customer edge (CE) or allow the service provider to manage the CPE or customer edge. The network element at the edge of the service provider’s network is called the provider edge (PE). Figure 6 shows this arrangement.

Enterprises and service providers can use a few types of VPNs and configuration settings to meet the requirements of the high-end enterprise. Figure 7 shows the three basic kinds of VPN services. These example VPN configurations do not include support for encryption; they are simply ways to tunnel the enterprise data to and from the remote sites.

Most large enterprises require encryption of some or all of their traffic crossing a shared network. They configure and manage basic encryption with IP Security (IPsec) on a point-to-point basis.

To summarize, managed VPN services are of three basic types:

- Traditional Layer 2 VPN (L2VPN) using Frame Relay or ATM: Basic transport service for enterprise data
- Layer 3 VPN (L3VPN) using MPLS: Any-to-any transport for enterprise data
- L3VPN using the Internet: Similar to L3VPN using MPLS except the Internet is used for transport; this connection is usually a backup connection for the enterprise
Until recently these three types of VPNs were the only choices for enterprises to select for managed VPN service. However, these VPNs missed some key requirements such as enterprise network access from remote employees, support for multipoint encryption, and multicast support for multimedia support. Plus, for a large enterprise with hundreds of remote sites, management of the encrypted tunnels is a fairly complex task.

Therefore, the following additional types of managed VPNs are now being offered to address these requirements:

- Remote VPN using SSL: This VPN provides secure access for remote employees to the enterprise network and resources. Figure 8 shows how the remote employee’s tunnel is carried transparently across the service provider’s IP/MPLS network.

- Dynamic Multipoint VPN (DMVPN): This new type of VPN provides multipoint connections over an encrypted VPN. Note that standard encrypted VPNs can provide only point-to-point links. Figure 9 shows the additional dynamic encrypted tunnels that can be deployed with DMVPN.

- Group Encrypted Transport VPN (GETVPN): This type of VPN provides automatic allocation of encrypted tunnels for any-to-any connections. Additionally, multimedia applications such as Telepresence and video that require a multicast network are supported with packet replication. You can see the benefits of GETVPN by comparing GETVPN to a traditional encrypted VPN network in Figure 10.
Figure 8. Remote VPN

Figure 9. Dynamic Multipoint VPN

- = DMVPN Tunnels
- = Traditional Static Tunnels
- = Static Known IP Addresses
- = Dynamic Unknown IP Addresses
When the enterprise starts tunneling the traffic among its sites, two other key requirements surface: segregating latency-sensitive traffic such as voice to provide quality of service (QoS) and multiple virtual routers for separate VPNs to connect the branch locations (Virtual Route Forwarding [VRF]).

**Managed VPN: Success Depends on Quality of Service and Branch Routing**

QoS is usually managed with three, four, or five classes of service. The enterprise selects which kind of traffic is assigned to which class of service. The managed routers at each site must classify the traffic into appropriate classes of service. Note that the core routers in the service provider network expect the traffic to already be classified when it reaches them. Traffic is classified in the router using differentiated services code point (DSCP). Figure 11 shows an example of the classification of router traffic into four classes.
It is important that latency-sensitive traffic such as voice and video is handled before best-effort traffic such as Webpage downloads. The enterprise IT staff must be able to provide clear voice services to campus and branch-office employees. Therefore, the QoS parameters and contracted service levels are documented in the SLA between the enterprise and service provider.

Additionally, large branch offices have local routing requirements to segregate guest and partner traffic from that of the employees. Guests, partners, and employees also have different access privileges. Therefore, large branch offices need VPNs local to the branch, and these VPNs need to be carried over the service provider’s network. The ability for a CPE to route traffic from multiple VPNs locally and across the service provider’s network is called multiple VRF (multi-VRF). Figure 12 shows the value of this capability in a large enterprise.

**Figure 11.** Example of Traffic Classification into Four Classes

<table>
<thead>
<tr>
<th>Enterprise Application</th>
<th>Enterprise Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing</td>
<td>CS6</td>
</tr>
<tr>
<td>Voice</td>
<td>EF</td>
</tr>
<tr>
<td>Interactive Video</td>
<td>AF41→CS5</td>
</tr>
<tr>
<td>Streaming Video</td>
<td>CS4→AF21</td>
</tr>
<tr>
<td>Mission-Critical Data</td>
<td>AF31</td>
</tr>
<tr>
<td>Call Signaling</td>
<td>CS3→CS5</td>
</tr>
<tr>
<td>Transactional Data</td>
<td>Routing</td>
</tr>
<tr>
<td>Network Management</td>
<td>CS2</td>
</tr>
<tr>
<td>Bulk Data</td>
<td>AF11</td>
</tr>
<tr>
<td>Scavenger</td>
<td>CS1</td>
</tr>
<tr>
<td>Best Effort</td>
<td>0</td>
</tr>
</tbody>
</table>

**Figure 12.** Multiple VRFs in a Large Branch

Logical Separation Within Campus Through VLANs

Layer 3 Separation Within Customer Edge Through Multi-VRF Functions

Service Provider Carries Multiple VPNs for the Same Enterprise
Is an Encrypted VPN Enough Security?

After the physical network access is in place and the VPN service is established among the sites, the next area to address is security services. The most important on-premises security service for the large enterprise is firewall protection to hide internal addresses and control access to internal resources. The first level of firewall protection is to hide internal addressing -- otherwise known as obfuscation -- using Network Address Translation (NAT). Obfuscation prevents external attackers from guessing internal addresses and attempting to access addressing devices.

The next step is to control who can access what resource. Typically enterprise networks are divided into different zones, each with a different security level, so, for example, the inside of the network has the highest security level and the Internet the lowest security level. A typical firewall policy allows connections initiated from the inside of the network to the Internet, but not conversely. Users from both the inside network and the Internet should be able to access Web servers that sit on the DMZ, or network perimeter, which has a "medium" security level, that is, lower than the inside network but higher than the Internet. The DMZ should therefore not be able to initiate connections to the inside network. With this policy, then how does the return traffic get from the Internet to the inside network? A “stateful” firewall controls this traffic -- return traffic is allowed in only if an established connection is initiated from the inside network.

You can add stronger security by authenticating users and limiting their access -- one application would be split-tunnelling, whereby only authenticated users can gain access to the corporate network. Firewalls typically control the number of connections for a range of protocols. With protocol connections limits, access to resources can be limited, providing protection from denial-of-service (DoS) attacks.

Firewalls can also control which ports are allowed. Adding firewalls to stateful access control allows you to limit Web traffic. For example, port 80 can be opened between an inside host and a Web server for only a limited time.

The trend for firewalls today is in the direction of application firewalling, whereby there is deeper inspection into the packet to glean information about what is happening at the application level. For example, a firewall can inspect and control HTTP traffic, so that browsing Webpages is allowed but HTTP POST packets are blocked (POST packets are used to post data to insecure and untrusted servers).

How Can Managed Services Be Cheaper Than a Self-Managed Network?

Cisco has much information about the savings that you can obtain from managed services. Please refer to the references for links to relevant information. An example scenario has a midsize financial services firm with 2000 employees, 1000 of which work at its headquarters. The rest of the employees are distributed across 49 branch offices, averaging 20 employees in each office. These remote locations are small branch offices with financial specialists in each, and no IT capabilities at all. A managed-services solution brings headquarters-style applications, and the security of knowing that the applications and network run correctly. Without a managed-services solution, fixing problems could require travel.

The distributed routers, firewalls, and VPN sites are costly for the enterprise in this scenario to manage, given the number of network elements per employee. In this scenario, the financial services company can reduce its costs by more than 40 percent by shifting to managed services.
This case shows the benefit of managed services in the branch-office environment. These offices generally serve a smaller number of employees, and keeping IT resources in the office is often not economically feasible. Also, these offices are geographically dispersed, so problems require remote diagnosis and in the worst case, travel to resolve the problem. Figure 13 shows the monthly savings for this scenario.

Figure 13. A Comparison of Monthly Recurring Costs for Self-Managed Versus Managed Network Services

In addition to the savings from using managed services, enterprises can use other steps to minimize costs when adopting managed services:

- Partner with the managed services provider for the network design
- Develop a clear and measurable SLA with the managed services provider
- Use the minimum amount of network elements to reduce the number of devices to manage
- Select network equipment vendors with a track record of managed services and established relationships with managed service providers

Finally, using network equipment that meets the requirements of the high-end enterprise is mandatory for successful migration and usage of managed services.

Cisco Midrange Routers for Large Enterprises Using Managed Services: Cisco 7200 Series Routers

Cisco offers the industry’s most widely deployed universal services aggregation router for enterprises: Cisco 7200 Series Routers, which provide:

- Exceptional price-to-performance for aggregation services up to 2 Mpps
- A wide range of connectivity options and numerous features, including serviceability and manageability
- Increased VPN performance with the integrated Cisco VPN Services Adapter

Benefits of these proven routers in a managed service setting include the following:

- Award-winning QoS feature performance
- MPLS: Leading choice for managed VPN services
- IP Security (IPsec) VPN: Scalable to 5000 tunnels per chassis
- IP-to-IP gateway support to provide a network-to-network interface point for signaling interworking (H.323 and Session Initiation Protocol [SIP]), media interworking, address and port translations (privacy and topology hiding), billing and call-detail-record (CDR) normalization, and bandwidth management (QoS marking using type of service [ToS])
- Voice, video, and data integration: Time-division multiplexing (TDM)-enabled voice port adapters
- Modular design: One-rack-unit (1RU) footprint with broad range of flexible, modular interfaces (from DS-0 to OC-3)
- Flexibility: Support for Fast Ethernet, Gigabit Ethernet, Packet over SONET/SDH, and more

Cisco 7200 Series Routers extend services aggregation to enterprises and redefine best-in-class routing for secure, concurrent delivery of data, voice, and video.

Cisco Midrange Routers for Large Enterprises Using Managed Services: Cisco ASR 1000 Series Aggregation Services Routers

As enterprises expand globally while simultaneously integrating a new wave of applications, the WAN edge has become a critical gateway for business success. The Cisco ASR 1000 Series Aggregation Services Routers are ground-breaking routers that represent a dramatic advance in technology innovation based on Cisco’s understanding of evolving customer requirements. These routers set new expectations for industry-leading performance and scalability of embedded services atop a secure, resilient hardware and software architecture.

For the highest performance demands, the cutting-edge Cisco ASR 1000 Series Router is offered for:

- Higher-bandwidth requirements: The routers offer 10-Gbps throughput even with Firewall, Network Address Translation (NAT), QoS, generic routing encapsulation (GRE), or other services enabled. The routers offer 5- and 10-Mpps packaging options in a 2RU package. Additional performance benefits include the following:
  - Twenty thousand sessions per second for Firewall or NAT
  - Ten thousand sessions per second for IPsec site-to-site or remote tunnels
  - Sixty thousand IP Multicast groups
  - Less than 100 microseconds latency for high-priority applications
  - Up to 1 million IPv4 routes and 250,000 IPv6 routes
  - Up to 16,000 access control lists
- Embedded Session Border Controller (SBC) functions to handle next-generation voice and multimedia: Supporting up to 32,000 simultaneous voice or multimedia sessions, the Cisco ASR 1000 Series Router can process up to 10 Gbps of multimedia data, even while concurrently providing customized accounting, firewall, and QoS services to these sessions
- Highly available WAN infrastructure: The routers offer rapid failover without service disruption and platform redundancy
- Full WAN security for data protection and compliance: The routers offer network resiliency with a self-defending architecture
- Inspection of traffic flows at high speeds for attack prevention, policy enforcement, and application security
• Consistent service delivery with application intelligence: Enterprises need to meet demanding internal SLAs, with improved service delivery and application performance over the WAN

The Cisco ASR 1000 Series Routers have been crafted to meet and exceed the most exacting standards that rapidly evolving enterprise business requirements can demand.

Conclusion

Migrating from a self-managed network to managed services saves operational costs for large enterprises. When the managed services provider is experienced with the challenges of enterprises with multiple campuses, hundred of branches, and remote employees, the IT staff is freed to generate new profits for the enterprise. Installing a proven, scalable, and reliable router platform is required to use secure managed WAN services. Investing in a Cisco router platform implements the managed-services infrastructure that meets today’s demands as well as future service demands.

For More Information

For more information about the solutions and products mentioned in this document, please refer to:

• Cisco Powered Networks: http://www.cisco.com/cpn  
• Cisco ASR 1000 Series Routers: http://www.cisco.com/go/asr1000

Cisco Powered Networks

Service providers that display the Cisco Powered logo can help enterprises migrate to MPLS-based VPN services. These providers have earned the Cisco Powered designation by maintaining high levels of network quality and by basing their VPN services on Cisco equipment. An increasing number of Cisco Powered providers have earned the QoS Certification for VPN services, meaning that they have been assessed by a third party for the ability of their SLAs to support real-time voice and video traffic, and for their use of Cisco best practices for QoS.
Nearly 400 of the most successful service providers throughout the world offer services that have earned the Cisco Powered designation. These providers offer services such as Internet access and Web hosting as well as IP communications and multiservice VPNs.