



Are Managed Services Right for Your Business



Customer Information



Index

| | |
|---|----|
| The Expanding Role of the Network in Business Success | 4 |
| What Are Managed Services? | 4 |
| Scenario 1: Customer Owns Network and Shares Management Responsibility | 5 |
| Scenario 2: Service Provider Owns the CPE; Customer Can Share Equipment Management with Service Provider | 6 |
| Scenario 3: Service Provider Owns Equipment in its Own Facility; Customer Monitors Service Provider's Management of the Equipment | 6 |
| Would Your Business Benefit from Managed Services? | 7 |
| The Business Case for Managed Services | 8 |
| HIS Communications Services | 9 |
| FW. Honerkamp | 10 |
| Sims Hugo Neu | 11 |
| Outback Steakhouse, Inc. | 12 |
| Identifying the Managed Services That Are Right for Your Business | 13 |
| Managed IP VPNs | 13 |
| Managed IP Communications | 14 |
| Managed Security | 16 |
| Selecting a Managed Services Provider | 18 |
| Define Your Business Requirements | 18 |
| Evaluate Service Providers | 19 |
| Align SLAs with Your Business Requirements and Operations | 20 |
| The Cisco Powered Program | 21 |
| Further Information | 23 |



Managed services delivered by a service provider is an increasingly popular and preferred alternative to internal management of network-based services. This primer explains when managed services are beneficial, how managed services reduce costs, and factors to consider when choosing a managed services provider.

- The Expanding Role of the Network in Business Success
- What Are Managed Services?
- Would Your Business Benefit from Managed Services?
- The Business Case for Managed Services
- Identifying the Managed Services That Are Right for Your Business
- Selecting a Managed Services Provider
- The Cisco® Powered Program

The Expanding Role of the Network in Business Success

All business has become global. Companies of any size can now market products and services worldwide over the Internet. At the same time, competition has intensified because customers can investigate global competitors with a few clicks of a mouse.

To compete effectively in a global market, companies need new capabilities:

- Global procurement and sales 24 hours a day
- Integrated internal and external business processes
- Up-to-the-minute access to sales, order processing, production, and other business critical information required for informed decision making
- Flexible processes that can adapt dynamically to changes in the business climate

Meeting these challenges requires a fast, reliable, and secure IP network. However, maintaining the IP network requires regular, ongoing investments in networking infrastructure and IT staff training. Many companies find it expensive to keep up with new technologies—or simply prefer to devote IT resources to the core business rather than ongoing network management.

Managed services bridge the gap by giving companies access to leading network technologies and management expertise without requiring high initial capital expenditures (CapEx) or ongoing investments in technology upgrades.

What Are Managed Services?

When a company subscribes to a managed service, a service provider manages the network equipment and applications on the customer premises according to the terms of a service-level agreement (SLA) established to meet the company's unique business needs. Some managed services are also hosted, meaning that the service provider hosts the equipment in its facility instead of the customer's, and delivers services to company employees over the WAN.

For small and medium-sized businesses (SMBs), managed services provide enterprise class capabilities for a predictable monthly fee—without requiring a large, initial capital investment. Companies that out-task enjoy high levels of network support and availability, enable internal IT staff to focus on strategic activities instead of network support, and pay only for those networking services that they need.

Key Benefits of Managed Services

- Reduces costs, including traditional service fees, hardware, IT operations, and transport
- Eases adoption of new business processes
- Increases levels of support and network availability without additional staff
- Makes the IT budget more stable and predictable
- Provides access to the latest technology with limited risk
- Provides access to an enhanced skills base
- Makes it easier to adapt to changing business conditions
- Enables the IT group to focus on the core business

Managed services generally include software, hardware, and other IP networking services. The service provider's highly experienced technical experts focus exclusively on providing the network services and support that their customers need to meet their business requirements.

Companies have the option to out-task some or all of their network management and monitoring tasks and retain control of the rest—even if the equipment is physically located at the provider's site. Following are typical scenarios for deploying managed services.

Scenario 1: Customer Owns Network and Shares Management Responsibility

Companies that already have an internal IP network can continue to manage it while out-tasking management of onsite equipment, usually known as customer-premises equipment (CPE), used for the managed service, such as a Cisco Unified CallManager system or a Cisco intrusion prevention system (Figure 1). Roles are as follows:

Service provider – Sets up, maintains, and administers the equipment needed for the managed service, including company-owned equipment such as servers

Company – Maintains and administers its internal network

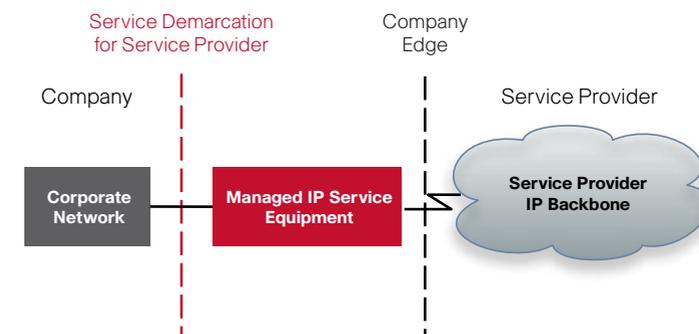


Figure 1 Service Provider and Customer Divide Responsibility for Customer's Network Infrastructure

Scenario 2: Service Provider Owns the CPE; Customer Can Share Equipment Management with Service Provider

Some companies do not own a LAN, either because the location is new or the company already out-tasks its LAN services. In this situation, the service provider can manage the equipment needed for the corporate network as well as the managed service. Many large enterprises like this arrangement because they can maintain physical control of the equipment while relying on the service provider for 24-hour network operational support. Roles are as follows:

Service provider – Sets up, maintains, and administers the equipment for the managed services as well as the corporate network (Figure 2)

Company – Monitors its corporate network through a Web interface provided by the service provider, receives regular reports on the network status and managed services, and is notified in case of a defined emergency

Scenario 3: Service Provider Owns Equipment in its Own Facility; Customer Monitors Service Provider’s Management of the Equipment

The difference between this scenario and the previous one is that most of the equipment is physically located in the service provider’s hosting facility instead of on the customer premises. Roles are as follows:

Service provider – Sets up, maintains, and administers the corporate network and related managed services; most of the network equipment is physically located in the provider’s computing center; the exceptions are the equipment for the LAN and network connections, as well as gateways for computers and IP telephony

Company – Monitors performance of its systems through a Web interface provided by the service provider, receives regular reports on the network status, and is notified in case of a defined emergency

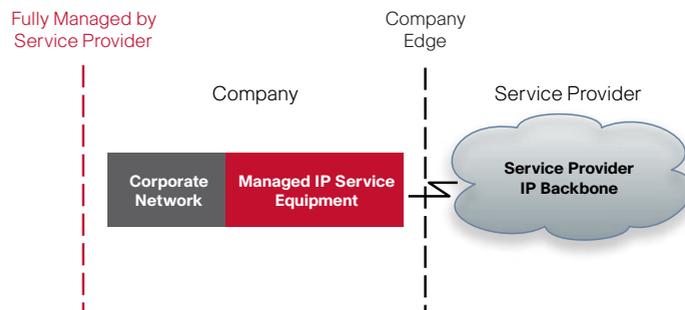


Figure 2 Service Provider Manages Customer Infrastructure as well as the Managed Service Equipment

Would Your Business Benefit from Managed Services?

Review the business needs in Table 1 to decide if managed services can provide benefits to your business. If you answer yes to any of these, it can indicate areas where managed services could assist.

Table 1 Are You a Candidate for Managed Services?

| |
|---|
| Our business is facing challenges: |
| <ul style="list-style-type: none"> ▪ Staffing IT professionals ▪ Staying up-to-date with evolving technologies and IT skill sets ▪ Managing and maintaining current infrastructure, hardware, and software ▪ Securing data, transactions, and communications ▪ Responding quickly to time-to-market demands ▪ Remaining flexible enough to maintain competitive position ▪ Reducing network overhead costs ▪ Operating in real time in order to meet 24-hour demand ▪ Delivering services to branch offices and remote workers |
| Our business is in transition: |
| <ul style="list-style-type: none"> ▪ We need to upgrade, refurbish, move, or relocate existing infrastructure. ▪ The scope or scale of current business operations is changing. ▪ A merger, partnership, or acquisition is altering operations. ▪ We need to increase the range and level of service. ▪ Our growth targets depend on implementing new technologies. ▪ We are expanding into new markets. |
| Our business wants to increase profitability: |
| <ul style="list-style-type: none"> ▪ We prefer to dedicate resources to our core competencies and mission-critical processes rather than network support activities. ▪ We view managed services as a good strategy for gaining efficiencies and reducing costs. ▪ We need to implement a global network service but lack internal global resources. ▪ We are concerned with our ability to keep up with the latest security threats and to meet privacy or security regulations. ▪ We are experiencing dynamic business growth while undergoing downsizing and hiring freezes. |



The Business Case for Managed Services

Compared to managing network-based business requirements internally, out-tasking all or some functions to a managed services provider provides the following benefits:

- Reduces costs, including traditional service fees, hardware, IT operations, and transport
- Eases adoption of new business processes
- Increases levels of support and availability without additional staff
- Makes the IT budget more stable and predictable
- Provides access to the latest technology with limited risk
- Provides access to an enhanced skills base
- Makes it easier to adapt to changing business conditions
- Enables the IT group to focus on the core business

The following case studies help to illustrate the business case for managed services.

HIS Communications Services

Small Support Company Reduces Voice Costs with Managed IP Communications Service

Background: Located in Houston, Texas, HIS Communications Services provides telecommunications services support, including network management as well as sales and service for call centers and conferencing systems. The company has 15 employees and primarily serves customers in the oil and gas industry.

Challenge: Because customers call HIS Communications when they have network problems that need prompt resolution, the company wanted to ensure that callers did not receive a busy signal, and also wanted to make it easier for callers to reach employees. Limiting CapEx and ongoing telephony costs were important requirements.

Business Solution: HIS Communications subscribed to a Cisco Powered managed service from a provider that bundles local and long-distance nationwide calling, high-speed T1 Internet access, e-mail, and a Web-hosting service.

Business Results: HIS Communications enjoys telephone features typically available only in much larger companies. For example, the ability to easily set up spontaneous conference calls helps accelerate resolution of customer concerns. With virtually unlimited long-distance calling, HIS Communications is saving US\$250 to \$350 monthly, a 25 to 35 percent reduction—and a consolidated bill for all voice and data services simplifies administration.

“Cisco Unified CallManager Express and the [managed] service provide small companies like ours a reliable, flexible voice-and-data service.”

Brian Blanton, vice president of business administration,
HIS Communications

F.W. Honerkamp

Small Supply Company Improves Customer Service by Out-Tasking Voice System

Background: F.W. Honerkamp Company, Inc. distributes architectural plywood, such as laminates and veneers, to vendors ranging from small home-improvement companies to multi-million-dollar architectural millwork firms. The family-run business has 30 employees.

Challenge: F.W. Honerkamp's previous private-branch-exchange (PBX) system inhibited the company's competitiveness. If the incoming lines were jammed, callers received a busy signal. The company had a single phone number, which rang every phone. This setup inconvenienced callers, who had to wait to be transferred, and impaired the productivity of the company's salespeople, who were constantly answering phone calls intended for others. When the company acquired another distributor, employees could not easily collaborate because of their inability to transfer calls between offices and a lack of voicemail in the new office.

Business Solution: F.W. Honerkamp subscribed to a managed IP telephony service that also includes hosting. The only equipment the company needed to purchase were Cisco Unified IP phones and a Cisco router for each office. (The company already had Cisco Catalyst® switches and a firewall.) The service provider charges a fixed, monthly per-user fee that includes local- and long-distance calling and Internet access.

Business Results: The out-tasked phone system service is reliable and gives F.W. Honerkamp a competitive advantage with vendors because employees are easier to reach. The company estimates that productivity has increased by 25 percent because of telephony features such as direct dial, 4-digit transfers, and voicemail. In addition, F.W. Honerkamp no longer has to pay US\$200 for extension moves, adds, or changes.

"Given the choice between a distributor who charges a penny or two less per square foot and a distributor who is easy to reach, a vendor will often choose the latter. When vendors tour our facilities and see our advanced phone system—whose capabilities often exceed their own—it increases their confidence that we are positioned for long-term growth."

Jeff Honerkamp, chief operating officer, F.W. Honerkamp

Sims Hugo Neu

Global Recycling Company Increases Network Availability and Reduces Costs with a Managed VPN Service

Background: Sims Hugo Neu Corporation is the U.S. division of The Sims Group, a global metal recycler with 160 sites.

Challenge: The company calculates scrap metal weight and payment by weighing trucks as they enter and exit the yard and then sending the information over the network to a centralized application. If a network outage forces yard workers to calculate weight and payments manually, payment errors inevitably result. The company also wanted to deploy IP telephony and videoconferencing, so it needed quality of service (QoS).

Business Solution: Sims Hugo Neu subscribed to a managed Multiprotocol Label Switching (MPLS) VPN service from a Cisco Powered program member after realizing that building an internal VPN would require hiring highly trained personnel. The service provider set up four classes of service to give priority to the most important or latency-sensitive traffic: IP telephony, then video, then the weighing-scales application, then all other traffic.

Business Results: The managed VPN service meets the company's needs for availability and low latency, uninterrupted operation of the mission-critical weighing-scales operation, and IP telephony and videoconferencing. In addition, bandwidth costs per gigabit have dropped from \$13,636 monthly to \$5,143.

"The availability, high bandwidth, and low latency of our MPLS VPN service has improved corporate efficiency by enabling us to share resources and centralize our ERP [enterprise resource planning], preventive maintenance, HR, payroll, and other critical applications. The Cisco Integrated Services Routers and [managed VPN] service make us more competitive by improving our service levels and avoiding the costs of downtime."

David Gramblicka, IT director, Sims Hugo Neu

Outback Steakhouse, Inc.

International Restaurant Chain Positions Itself for Growth by Out-Tasking Network Connectivity

Background: Headquartered in Tampa, Florida, Outback Steakhouse operates more than 800 Outback Steakhouses as well numerous other restaurants in 50 U.S. states and 21 countries.

Challenge: Management wanted to provide each restaurant with a reliable, high-performance network connection to centralized corporate information and applications. The company also wanted to host its critical application servers in a secure site where they would remain available despite power outages and hurricanes.

Business Solution: Outback out-tasked network connectivity and data center hosting to managed services providers. The network service provider remotely monitors the network 24 hours a day to ensure high availability.

Business Results: Outback's new network is far more powerful and reliable, positioning the company for rapid growth while assuring high data availability. Outback has also reduced LAN costs and gained the ability to quickly add bandwidth capacity as needed to support growth.

“We looked hard at the total solution package and we knew with Cisco and [the managed services providers] we had a partnership. We were looking to work with companies that would treat it as a partnership.”

Dusty Williams, CIO, Outback Steakhouse

Identifying the Managed Services That Are Right for Your Business

Service providers offer a variety of options for managed services. This section describes three of the most popular managed services and their options to help you determine which services would be most useful for your company.



Managed IP VPN

Businesses gain both tactical and strategic advantages when adopting IP VPNs. In the short term, they benefit from cost-effective, secure network connectivity to branch offices and secure access to remote workers, teleworkers, and global partners. In the long term, they position themselves to take advantage of new value-added, IP-based applications and to support more users and applications at a lower cost.

Cisco commissioned the Yankee Group to describe the decision-making process that enterprises used to select one of three broad types of IP VPN managed services (Figure 3). You can use the decision tree to determine which of the three options for managed IP VPNs is most appropriate for your company:

- **Network-based IP VPNs** – Service provider provides complete management services
- **Managed CPE-based IP VPNs** – Service provider installs and manages the equipment on the customer premises and provides connectivity
- **“Do-it-yourself” IP VPNs** – Business installs and manages the equipment; service provider provides connectivity.

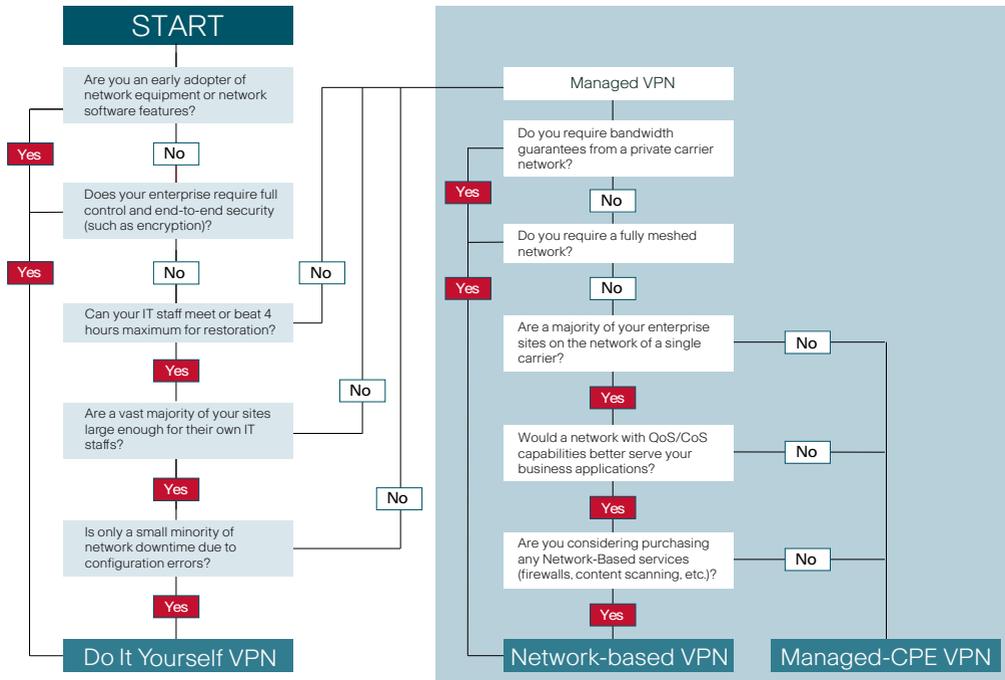


Figure 3 Decision Tree for Identifying the Right IP VPN Service

Managed IP Communications

Traditionally, companies have maintained separate networks for data and voice. With a converged voice-and-data network, companies reduce costs and gain productivity benefits such as 4-digit dialing between branches, intelligent call routing, and the ability to use IP phones instead of computers to access information and applications.

For many businesses, however, the cost of implementing and managing the IP communications solution internally is prohibitive. A more affordable option is to out-task IP communications to a managed services provider. This arrangement avoids initial CapEx and provides economies of scale because the service provider already owns the infrastructure and has the expertise and resources to implement managed IP communications services over a converged network.

You can choose from several options for managed IP communications services: management of the entire IP network, operational management of IP equipment, and provisioning of specific telecommunications services. Table 2 describes typical managed IP communications services offerings and how you can use them.

Table 2 Types of Managed IP Communications Services and Their Business Value

| |
|--|
| <p>Business IP Telephony Services</p> <p>Business IP telephony services are subscriber and group calling services. Companies that need sophisticated PBX features can use a managed IP telephony service based on the Cisco Unified CallManager system. Many small businesses can receive the services they require with a managed IP telephony service based on Cisco Unified CallManager Express software, which is included on certain Cisco routers.</p> |
| <p>Site-to-Site Voice</p> <p>This service is useful for companies with several branch offices that communicate regularly. A site-to-site voice service enables a business to call from one site to another using the service provider's voice-over-IP (VoIP) infrastructure, avoiding long-distance toll costs. Businesses that subscribe to site-to-site voice services can maintain a private dial plan, including support for 4-digit dialing.</p> |
| <p>Public Switched Telephone Network Access</p> <p>Access to the traditional circuit-switching public switched telephone network (PSTN) can be enabled centrally over the service provider's network. Central PSTN access provides economies of scale, which, in turn, reduce business costs.</p> |
| <p>Unified Messaging</p> <p>Unified messaging capabilities enable workers to retrieve and respond to voice, fax, and e-mail messages from any phone or PC within the organization. Employees can check any type of message from the same inbox—either the voicemail box, accessed from a phone, or the e-mail inbox, accessed from a computer. Capabilities such as rules-based call routing and speech recognition can further enhance service levels to your employees and other callers.</p> |
| <p>Voice over VPN</p> <p>A voice-over-VPN managed service can reduce toll charges for companies with telecommuters and mobile workers. Using an IP phone from home or softphone software on their laptop during travel, employees can make voice calls over the same, secure VPN connection they use to access business data and applications.</p> |
| <p>Enhanced Services</p> <p>Companies can increase productivity by delivering applications and information directly to employees' IP phones. As part of a managed IP telephony service, service providers can provide customized Extensible Markup Language (XML) applications for your business—for example, to access other employees' calendar information or read news stories relevant to the business.</p> |

Managed Security

In the networked business environment, security has become more critical—and also more complex. Today, network security requires constant monitoring and management of both internal and external network operations. Small businesses can no longer rely only on standard off-the-shelf virus programs, while all businesses experience vulnerability on an infrastructure that extends to local, regional, or global offices.

No matter what size your business is, service providers can create a comprehensive security offering that meets your needs and enables you to maintain the level of control you want. Service providers can manage some or all of your network security functions, giving you access to their sophisticated technologies, dedicated manpower, and 24-hour watchfulness, as well as routine maintenance and management of disaster operations.

Finding the right security solution for your organization begins with establishing your priorities and becoming informed about alternatives. Table 3 describes typical managed security services and how you can use them.

Table 3 Types of Managed Security Services and Their Business Value

| |
|---|
| Managed Firewall |
| Firewalls protect internal and external networks by restricting the types of network protocols and traffic allowed on your network. Firewall appliances, which the service provider manages remotely, include dedicated hardware and software platforms located on your premises. |
| Managed Distributed Denial-of-Service Protection |
| This service involves protecting the network infrastructure and network-based resources from distributed denial-of-service (DDoS) attacks so that the business can operate without interruption. It also helps prevent worm propagation that can cause DDoS attacks. DDoS mitigation provides protection against emerging threats in public networks such as the Internet or extranets. |
| Managed Intrusion Prevention Systems |
| Intrusion prevention systems (IPSs) identify and stop inappropriate attempts to access the network, systems, services, applications, or data. Intrusion detection services (IDSs) rely on network-based or host-based monitors, and often match monitored traffic or activity against profiles of known attacks. |
| Managed Antivirus Protection |
| This service most often involves checking for viruses at the gateway or firewall as well as in e-mail messages, attachments, and file transfers. The service might include automatic updates to antivirus definition files. |
| Managed Endpoint Protection |
| This service detects and stops anomalous behavior on endpoint devices, such as desktops and servers. In this way, companies can prevent damage from “Day-Zero” security threats whose signature has not yet been identified. |
| Managed Authentication |
| Authentication refers to a group of processes and technologies used to verify the identity of a user attempting to gain access to systems or applications. |
| Managed Content Filtering |
| Filtering is used to isolate and block content deemed inappropriate according to internal policies or regulatory policies. |
| Vulnerability Assessment |
| Vulnerability assessment includes security risk assessments, network scanning, and probing to reveal vulnerabilities in the network, operating system, or applications that can be accessed from the Internet. |

Selecting a Managed Services Provider

Gaining the most business value from managed network services requires selecting the right provider—and the right services—for your business needs.

Define Your Business Requirements

To create a managed service that meets your unique business requirements, service providers need a clear understanding of your business and technology requirements. You can either perform a preliminary requirements assessment internally or work with a service provider that offers this service.

The most accurate requirements assessments are developed by a cross-functional team that includes management, technical staff, and end users. First, establish your business and financial objectives, including the factors shown in the left column of Table 4. Next, establish IT objectives and application requirements to meet those objectives, as shown in the right column of Table 4. If you do not have the internal expertise to determine the needed bandwidth requirements or QoS metrics, a managed services provider can help you define them.

Table 4 Assessing Your Business and IT Needs

| Business Needs | IT Objectives and Application Requirements |
|---|--|
| Security criteria | Number of sites |
| Risk management | Number of users |
| Budget resources | Target applications |
| Projected downsizing or growth | Bandwidth requirements |
| Merger and acquisition plans | Acceptable latency, jitter, and error levels |
| Strategic business and financial goals Macroeconomic and competitive factors | Support and help desk requirements |

Evaluate Service Providers

After defining your requirements, you can narrow your list of service providers to those that provide the needed technology expertise, transport infrastructure, geographic coverage, and price levels. It is important to understand the service provider’s core competencies. For example, some carriers focus primarily on network connectivity and operational excellence, whereas others have deep levels of IT and applications hosting expertise. Also consider the service provider’s size, financial resources, management team, greatest strengths, and expertise in your industry. Table 5 lists some questions to answer when choosing a service provider.

Table 5 Service Provider Evaluation Check List

| |
|---|
| 1. Does the service provider track and monitor the network end to end? |
| 2. Can the provider secure its own network traffic and manage priority traffic across other networks? |
| 3. What are minimum thresholds for network latency, packet loss, and jitter on the IP services? |
| 4. How is network performance measured? |
| 5. Are there procedures for trouble escalation, load rebalancing, network security assessments, and regular data backups? |
| 6. Can the provider’s data center support your requirements for physical and network security, capacity, availability, operations, and backbone connectivity? |
| 7. Does the service provider have a plan to adjust its service as your business needs change with time? How quickly can the service provider respond to changing needs? |
| 8. What are the terms if the network goes down or the level of agreed-upon service is not maintained? |
| 9. What measures does the service provider take to ensure continuous availability and high performance? |
| 10. Will the service provider provide you with real-time monitoring as well as regular, thorough reports on network performance? |

Align SLAs with Your Business Requirements and Operations

The SLA contract is intended to ensure that the managed service meets the specific needs of your critical business applications. Make sure that the SLAs include measurable, detailed criteria because a nonspecific SLA is difficult to enforce. Also establish SLAs that can evolve and adapt to accommodate the inevitable changes to the network, your applications, and the managed services relationship, such as additional services, changes caused by business growth, and evolving security policies.

Each type of managed service requires different SLA metrics. For example, SLA metrics for a managed IP VPN service include network delay, packet loss, jitter, and mean time to restore values. An SLA for network storage includes metrics for available storage levels, disk access speed, levels of Redundant Array of Independent Disks (RAID) redundancy, backup and archive frequency, and more. SLAs for a managed IP communications service include the quality of voice calls in terms of end-to-end latencies, voice bandwidth, echo levels, call setup time, call reroute time, and more. For any type of network service, you can enforce the SLA only if you have access to network performance information, so ask if the service provider provides regular and thorough reporting on network operations.

The type of SLA you need depends on your business model as well as financial factors. If your business requires high levels of uptime, for example, you should invest in a service with the highest possible SLAs for availability—typically 99.999 percent. If you have lower availability requirements, you might prefer to pay less for a somewhat lower SLA for availability.

Things to look for in your managed network service SLA:

- Metric and performance criteria that ensure end applications can perform as expected
- Good reporting on network performance, support response times, and other SLA components
- An easy-to-understand format and straightforward organization
- End-to-end metrics and performance goals that are relevant to the application

In addition to performance metrics, you can request an SLA that includes support services. You might also want to insert a clause requiring the provider to maintain a support staff and helpdesk team with a high level of professionalism and a positive, helpful attitude. Although this aspect of the SLA does not have metrics, it can help avoid a situation in which you receive acceptable network latency and jitter but the working relationship is unpleasant because your company and the service provider have different cultural values and work styles.

When possible, try to ensure that the contract gives your company the flexibility to expand or reduce the scale of the service if your business needs or budget change. For instance, if you anticipate upgrading bandwidth in your access lines, then obtain advance agreement about costs within the framework of the existing managed network services contract. It is nearly always better to arrive at costs for future growth or downsizing during initial vendor selection and service negotiation. Think ahead.

The Cisco Powered Program

Cisco understands that finding a provider that is a good fit for your business is critical—and that is why the company has developed the Cisco Powered program.

Cisco awards the Cisco Powered designation to a select group of service providers worldwide that offer their customers reliable, proven, and cost-efficient technologies and solutions. The Cisco Powered logo tells you that the service provider uses industry-leading Cisco solutions in its network and that Cisco recommends its managed services. Some providers have also undergone a third-party audit for IP VPN or Metro Ethernet managed services and are certified by Cisco as meeting Cisco QoS standards. Members of the Cisco Powered program receive comprehensive support from Cisco to ensure high-quality results, including security audits, troubleshooting, assessment, best practices, and training programs.





If you do not have a dedicated IT staff, you can feel confident knowing that qualified service providers that display the Cisco Powered logo will manage your network requirements professionally and reliably. If you do have an IT department, you can delegate nonstrategic network management areas to a trusted service provider partner, giving your team the time and resources to focus on core competencies or IT projects that directly affect resources and revenue.

Enjoy the peace of mind of working with a service provider that uses Cisco equipment in the delivery of its services; meets Cisco standards for network support; and achieves Cisco standards for interoperability, service reliability, and service quality.

More than 300 of the most successful service providers around the world offer one or more services that have earned a Cisco Powered designation. Located in 62 countries, these providers offer a wide range of services for small and large businesses alike.

For further information about finding the right service provider for your business requirements, visit <http://www.cisco.com/cpn>

Further Information

Managed Services for Small and Medium-Sized Businesses – Overview
www.cisco.com/go/ms4smb

Managed Services for Enterprises – Overview
www.cisco.com/go/ms4ent

Managed Services E-Tour (flash)
<http://www.cisco.com/go/mssmbetour>

Managed Services Technical Glossary
www.cisco.com/en/US/applicat/cpnfind/applications_glossary.html

Managed Services Success Stories for Small and Medium-Sized Businesses
www.cisco.com/en/US/netsol/ns458/networking_solutions_customer_success_stories_list.html



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.



©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0609R)