Outsourcing Managed Network Services
Is the decision right for your network?

Introduction
Business success today often depends on having the right information at the right time. The Internet has gone a long way toward helping connect more easily with each other, customers, and suppliers, regardless of location. As Web users become more sophisticated, and networks more complex, however, getting the information to the right user at the right time has become more difficult than ever.

For example, today Web users are conducting business interactively on Web sites, querying multiple databases, exploring streaming video, customizing and personalizing applications, and engaging in real-time messaging. Network managers are facing increasing user demand for mission-critical systems deployed on corporate networks that are already bandwidth constrained. The cost of bandwidth is declining, encouraging businesses to deploy more intranets, create new distribution channels through e-commerce, and to integrate their networks with suppliers, partners and customers. Additionally enterprise networks are challenged to scale networks in real time and still ensure reliability of the data, so that it is secure and performance is not compromised.

Time to market is also important. It's not just the big companies who win in this new world economy, it is the companies whose ability to move fast in response to business needs are the ones who stand a better chance at capturing market share and succeeding.

Industry analysts have estimated that more than 40 percent of all customers who experience errors while visiting a Web site never return. With the pace of today's complex environment, business-to-business e-commerce is expected to reach a trillion dollars in the next few years and Internet infrastructure spending to surpass $55.7 million by 2004 according to IDC. This data shows that traffic is getting richer and the means to handle it more sophisticated. But if the network is not managed properly, companies who use these networks are at risk.

How do network management teams respond to this situation with enough resources to keep up with existing services, train technical staff, implement new technologies, deal with the increasing dilemma of how to manage and secure these networks, and the constant pressure to keep critical data moving forward? Besides the operational challenges, costs to meet these challenges can be prohibitive.

Many businesses respond by outsourcing business applications and network services to service providers who offer managed services. Outsourcing can help meet the challenges to reduce capital expenditures, mitigate network risk and do this at an accelerated pace (remember time to market) in order to handle growth. IT managers are looking for service providers who can deliver all these benefits, and also provide a scalable solution with reliable performance, and network security.

How can a business be assured that a service provider will provide the level of service that is promised? Many businesses turn to Service Level Agreements (SLAs) to give them a guarantee of the quality of service they can expect from a service provider.

The purpose of this paper is to describe what an SLA is and to outline reasonable expectations in negotiating SLAs with a service provider. Additionally this paper defines SLA best practices guidelines and shows how these guidelines can help you determine
Outsourcing Managed Network Services
Is the decision right for your network?
practical things to look for when considering outsourcing your company’s business applications.

The Benefits of Outsourcing
Choosing a reliable service provider who can deliver these services instead of going to the expense and risk of building complex networks to handle network services that are not necessarily part of your core business has significant benefits. Below is a list of benefits that can be realized by outsourcing:

Tangible benefits to outsourcing:
- Lower network management cost
- Reduced complexity of in-house networks
- Access to the latest technologies
- Dedicated and reliable resources due to their focused experience
- The ability to focus on your core business
- Ability to customize some services based on demand requirements
- Security
- Convenience
- Ability to grow the network without major overhaul of environment
- Ability to scale and add new services (time to market)
- Lower network management cost
- Reduced complexity of in-house networks
- Reduced infrastructure and maintenance costs
- Savings on manpower, technical staff and technical training

Performance isn’t just how fast your data gets to its destination, it’s about how well your network is managed and performs end-to-end. Businesses are looking to service providers for solutions that increase reliability, reduce operational overhead, and have the ability to scale to meet their customer’s demands. The enterprise wants this guarantee regardless of the application or the transport technology. Does the service provider offer imbedded service assurance agents that generate measurements end-to-end and track behavior or monitor different aspects of the network? Can the network send secure traffic not only across its own equipment, but manage priority traffic across other service provider networks?

Choosing a service provider to outsource critical network services is a big step, but it is one that can benefit your business greatly if the proper planning and relationships are in place. Enterprise businesses must look at a Service Level Agreement (SLA) from the standpoint of what is really important to its business. SLAs are a powerful tool for business to use to enable more efficient use of outsourced resources with a significant return on investment. The key is to find a service provider who will meet your needs and through well-prepared-for SLA negotiations, becomes your partner in meeting your corporate networking goals.
Outsourcing Managed Network Services
Is the decision right for your network?

Service Level Agreement Definition
A Service Level Agreement (SLA) is a contract between a business and a service provider that sets standards for network availability, reliability, and security. In other words, it is the service provider’s effort to distill the complexity of telecom services into a simple set of metrics that are acceptable and affordable to the business. As service providers seek to differentiate themselves from the competition, more of them are offering more comprehensive SLAs to meet business demands. When choosing to outsource any network service one must consider the following:

- Reliability, performance and cost savings
- Minimum acceptable performance of the particular application or network connection
- The business cost and customer satisfaction cost if the network or server hosting your application goes down or does not perform
- Assurance that best practices and open standards are being used
- The ability to cancel your SLA contract and the ease of migration from one service provider to another should the service provider not meet your company’s needs

Finding a credible service provider that supports your business goals requires a well-thought-out, informed decision.

Quality assurance is a key factor that must be considered, but the dilemma is how to confirm the vendor you choose is delivering on its promise? With the evident maturity of the telecom industry and the sophistication of new technologies, service providers are now able to answer a business's need for service guarantees with SLAs.

What Service Level Agreement Should Cover?
At a minimum SLAs must cover the activity of all the routers, switches, path, and points of presence (PoPs) across multiple vendors. A service provider who truncates the SLA based on the extent of its network is not telling customers the entire story as to what service is being delivered nor can the quality of the service be guaranteed. Customers do not care about the physical medium relating to how the service is delivered; they care what service is delivered in the area of reliability, performance and security. An SLA for a virtual private network (VPN) service might specifically determine minimum quality standards covering network availability (99.999%-100%), packet loss thresholds (.05% - 1%)m and latency guarantees to enable a business to retain a certain level of performance that they and their customers can rely on.

The SLA typically gives a business re-payment if the service provider fails to deliver on the level of service agreed to in the SLA contract. The form of re-payment is typically in the form of a credit for network service time or cash back (credits) on the fees charged to deliver the SLA. The SLA guarantees can be automatic or not. An automatic credit is a regular (agreed upon) report that automatically issues the credit when service levels fall below the agreed thresholds as appropriate. Automatic credit is common in the satellite industry and is quickly becoming standard with the larger, more stable service providers. A by-request credit usually sets an agreed time frame that the enterprise has to identify any down time, report, and request the credit. Some companies boldly claim 100% availability and the small print on the contract states by-request credits only with a time...
Outsourcing Managed Network Services
Is the decision right for your network?

limit in which to claim the credit. This adds a layer of administrative management that should be considered when negotiating the SLA.

Table 1 shows a few examples of ISP guarantees offered by service providers as of July 2000.

Table 1: Sample ISP Guarantees, July 2000

<table>
<thead>
<tr>
<th>ISP</th>
<th>Latency</th>
<th>Maximum Outage</th>
<th>Maximum Credit</th>
<th>Credit rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cable and Wireless Commun.</td>
<td>70 ms</td>
<td>3+ hours</td>
<td>9 days</td>
<td>Request</td>
</tr>
<tr>
<td>Concentric Network</td>
<td>80 ms</td>
<td>30 hours</td>
<td>30 days</td>
<td>Automatic</td>
</tr>
<tr>
<td>Epoch Internet</td>
<td>85 ms</td>
<td>8+ hours</td>
<td>1 month</td>
<td>Request</td>
</tr>
<tr>
<td>Qwest Communications</td>
<td>75 ms</td>
<td>30 hours</td>
<td>30 days</td>
<td>Request</td>
</tr>
<tr>
<td>Sprint</td>
<td>70 ms</td>
<td>27 hours</td>
<td>30 days</td>
<td>Request</td>
</tr>
<tr>
<td>UUNet</td>
<td>85 ms</td>
<td>30 hours</td>
<td>30 days</td>
<td>Request</td>
</tr>
</tbody>
</table>

Tier-1 companies like AT&T, Cable and Wireless, Genuity, and UUNet offer SLAs that are very similar to each other. Other companies are steering away from the use of SLAs in favor of implementing customer satisfaction guarantees that offer 10-25 percent in monthly service rebates if the customer is unhappy for any reason. A good SLA will help set minimum thresholds on latency and availability of the network. Does latency and availability guarantees alone help make a buying decision? The answer is it depends. If you are playing with the larger service providers mentioned above, the answer is probably not, but if you choose a smaller perhaps more local service provider you should look more closely at these guarantees to ensure that the resources are in place to protect your company’s interests. There is more to an SLA than latency and availability guarantees and the prudent network team will look closely at the options offered before choosing.

How do you measure performance?
First, one must understand the kind of traffic that is being considered for outsourcing. There is a significant difference between 60 milliseconds and 120 milliseconds of round-trip latency if you’re supporting voice over IP or multicast video streams, but that difference in latency may not be that important if you’re supporting Internet or company email. It is up to the enterprise IT manager to decide based on the company’s business requirements.

As we discussed previously, SLAs typically offer credits for failure to deliver on their promise, but do you really want the credit? The down time and the credit back certainly won’t recover lost revenue and customer disappointments that occur due to a downtime event. If you are negotiating service credits and your business model supports virtual private networks (VPN), which requires 99.999-100 percent availability with less than 1 percent packet loss and latency under 60 milliseconds, then it is important to make sure your SLA contract motivates the service provider to deliver this high quality of service and that they have the infrastructure and expertise in place to deliver. This question leads to how do you choose a service provider and what to look for in their environment.

How to Choose a Service Provider
To choose a service provider you must first understand your environment and what level of service you are looking for. Do you need pure network connectivity for Internet applications or are you considering outsourcing more complex solutions that include a
Outsourcing Managed Network Services
Is the decision right for your network?

key business application or VPN and network connectivity that is beyond a point-to-point situation? Before you start looking for a service provider it is a good idea to do your homework and be prepared. The right preparation will make your search more efficient and most of the tasks to consider are basic common sense that any network team should already have in place. Although each situation is unique to the enterprise business a few basics are listed below. Additionally, a data center checklist that can also be helpful for this task is located as an addendum to this white paper is at the end of this document.

1) Document your site
   a. Provide accurate records of the infrastructure and its purpose
   b. Provide accurate and detailed network diagrams that you can share with the service provider
2) Label your equipment
   a. Label IP addresses and domain names on the racks, network equipment, and servers to make support issues easier when dealing with a help desk
3) Know your software release levels and upgrade where necessary
   a. Track and share any changes with your service provider
   b. It is important to formalize updates and the process used is communicated to all involved.
4) Know what equipment you own and what equipment you may want to lease from the service provider
5) Review your facility’s security
6) Understand how information is currently shared in your network
7) Understand your backup and recovery methodology
8) Understand the geographical reach needed and whether your service local, regional or global

Once you have done your homework it's time to start having discussions with well-referenced service providers that you determine may be able to meet your needs. When you determine that the service provider offers the managed network services you need and you want to consider partnering with them, you need to visit their Network Operations Center (NOC).

When considering a more complex out-sourcing situation, it is important to look at the data center services offered in respect to your company’s goals as well.

**Data Center Services to Consider**

The data center of today is a multi-tiered, secure facility constructed of thick concrete walls and ceilings reinforced with steel, with no external glass, and with redundant power such as diesel generators. Other amenities that need to be considered are electrical, cooling, fire suppressant systems, floor-load capacity, security; alternate pathways to the service provider’s distribution center and the type of network operations support levels.

Consider if outsourcing is to pay off, *and it can in a substantial way*, whether this service provider would be able to support additional applications or services that your business may grow into. Does the service provider specialize only in specific areas? It is important that you not confuse data center services, Web hosting services, and application infrastructure providers (AIPs) with application service providers (ASPs) that may concentrate on specialized applications and may not provide network management services beyond the data-center services used for application support. It is important to

Delcina J Betts
Technical Business Development Manager,
Cisco Powered Networks
Outsourcing Managed Network Services

Is the decision right for your network?

know if the provider you choose is able and interested in supporting additional requirements not part of their specialization.

Now that you have determined your basic outsourcing requirements and have determined the depth of services you are looking for, it is recommended that you take your questions to the next level by assessing your network’s vulnerability. Vulnerability is possible not only in loss due to down time and latency issues, but also can be affected in multiple areas of your network.

Once you have thought through the physical and connectivity requirements it is important to look at how the service provider ensures that it will keep its commitments, and the type of network management that is available.

- Does the service provider offer a fully redundant network (intrinsic networks) that guarantee 5 9’s of availability?
- Has the service provider deployed quality of service (QoS) or DiffServ guarantees?
- Is the solution interoperable with other network offerings such as multi-protocol label switching (MPLS)?

There is often a disconnect between business managers, who do not view their bits as undifferentiated bits, and service providers who are interested in moving volumes of bits. A service provider who understands the use of QoS-enabled networking is able to add another level of performance and security and at the same time offer flexibility to the business to manage its response times and bit rates while reducing cost.

Typically, QoS refers to an aggregation of system performance metrics; the most important of these are availability, throughput, packet loss, latency and jitter. Availability ideally should be 100 percent (99.8 percent translates into about an hour and a half of down time per month). Throughput is the effective data-transfer rate measured in bits per second. Networks that are shared usually have a lower throughput realizable by any single user, as does the overhead imposed by the extra bits included in every packet used for identification purposes. Packet loss occurs when network devices such as switches and routers hold data packets in buffered queues. If a link is congested too long then the buffered queue overflows and packets (data) are lost. Latency is the time it takes for data to travel from the destination to the source. Lastly jitter is another way of saying latency variation or a variation in the processing of packets and the time it takes to re-assemble them on the receiving end. QoS can help set the priorities at network-aggregation points (routers, switches and multiplexes) to ensure adequate transport of specific data over a common infrastructure. Throughput, availability, packet loss, latency and jitter all must be spelled out in the SLA along with how each is to be measured and reported.

In today’s global environment where services for any particular company may be located all over the world, many service providers partner with one another and share the larger bandwidth on their core with those who offer services in a particular geographical areas, Business customers who want their mission critical data to reach its destination in the most optimum way will want to work with service providers who offer QoS, DiffServ and MPLS services that can support requirements in the area of content delivery networking, (distributed applications), voice over IP (VoIP) and VPN. QoS and MPLS work together in order for a service provider to truly offer options in traffic prioritization and be able to slice bandwidth and manage it so that your bandwidth doesn’t cross onto that of other

Delcina J Betts
Technical Business Development Manager,
Cisco Powered Networks
Outsourcing Managed Network Services
Is the decision right for your network?

customers. The next generation of services being offered are QoS trend services, in which you pay for a guaranteed path for critical data which may cost more than a typical point to point connection, such as a T1 type connection. The only true way to offer managed services across multiple networks is through technologies like QoS. If these technologies are not in place you should understand exactly how the service provider meets your global requirements and still ensures data performance and integrity.

It is important to be sure that the service provider understands your core business model and how the services they will deliver affects your network and your customer’s data. Questions to ask when developing an SLA with your service provider:

Does the service provider?
- Guarantee a service that goes outside of its network?
- Offer active monitoring?
- Monitor services across all of the vendor hardware installed in the network?
- Provide front-end connectivity/peering?
- Provide co-location or fully managed services?
  - Load balancing
  - Mirroring
  - Caching
  - Integrity and performance design reviews
  - Security
  - Backup and recovery procedures
- Provide 24x7x365 support?
  - Active monitoring
  - Second-tier support
  - Third-tier support
  - Guaranteed response time
  - Real-time, Web-based customer reporting
- What level of expertise is in-house?
  - Educational certifications for staff?
  - Number of CCIEs
  - Security expertise
- When adding a new service, how are the network services you purchase affected?
- What is the attitude of the service provider on the subject of SLAs? You want the relationship to be a partnership, not adversarial finger-pointing, but rather procedures for fixing issues if problem arise.
- Is the SLA adaptable as your network requirements evolve?
- Is the SLA measurable? Does it provide:
  - Built-in tools for tracking and measuring SLA performance data?
  - Performance criteria commitments?
  - A secure, Web-based interface to access your data so you can confirm that the provider is in compliance with the SLA agreement?
  - Business metrics, such as mean time to provision (MTTP) or mean time to repair (MTTR)?
  - Confidential reporting on performance and how often?
- Is the SLA enforceable?
  - Do penalties such as time/monetary credit units for down time apply?
Outsourcing Managed Network Services
Is the decision right for your network?

- Are the penalties active or non-active (enough to motivate a provider)
- Does the SLA cover all components?
  - The entire IT and networking infrastructure as an integrated unit
  - Multiple SLAs covering several components?

In Summary, when considering a more complex outsourcing situation, it is important to look at the total services offered in respect to your company’s business goals. If you prepare and invest some upfront time understanding your environment, current business needs and future company direction you will be better positioned to partner with a service provider who is best suited to deliver you quality services that meet your requirements. Moving forward as you focus on your core business and are able to more effectively leverage overall company resources the better positioned you will be to thrive in today’s complex economy.
Outsourcing Managed Network Services
Is the decision right for your network?

The figure below is in the form of a check list that contains basic examples of items to consider when reviewing the data center of a service provider you may be considering for managed services.

**Data Center Best Practices Checklist**

**Facility and Physical Requirements**

- Multiple physically separate connections to public power grid substations
- Continuous power supply with backup UPS systems
  - Adequate UPS capacity including air conditioning and lights
  - UPS systems tested at full load on monthly schedule
  - 48 Hours of fuel for UPS generators kept on premises and monitored for local environmental compliance
- Conform to or exceed applicable local structural building codes utilizing standards such as bullet proof glass, fire doors and reinforced walls and complying with disaster proof design
  - Comply with all local zoning ordinances
  - Certify not located in a hundred year flood plain
  - Earthquake and hurricane bracing on all racks and cable trays (where appropriate)
- Adequate multi-zone air conditioning, including a backup system for the multi-zone air conditioning
  - Climate control including humidity sensors and control
- Heat and smoke detectors that meet or exceed all local fire code regulations.
  - Very Early Smoke Detection Alarm (VESDA)
  - FM200 fire suppression system in data center and network operations center (NOC)
  - Separate detection/FM200 zone under raised floors
- Pre-action dry pipe system zoned to release water only where needed
- Easily removable access panels in raised flooring
- Flood sensors and monitoring under raised floors and in other critical areas

**Physical Security**

- Background checks on personnel with access to all critical areas
  - Servers
  - Network management systems
  - Equipment cages and applications.
- Written security policies readily accessible
  - Badge sharing / piggy back entry rules
  - All visitors must be admitted through reception, etc.
- Building access procedures
  - Limited number of building entrances in compliance with local fire ordinance
  - Provide access to limited and managed security policies for all facility entrances
  - 7 X 24 hour guards
Outsourcing Managed Network Services
Is the decision right for your network?

- Visitor-logging procedure
- Card-key, biometric, or similar entry locks
- ID-badge system for all employees and visitors
- Staff and visitors must wear badges at all times on premises

**Equipment locations**
- Video surveillance and motion sensors for entrances, interior doors, equipment cages, and critical equipment locations within the building
- Locked cages with ceilings; locking cabinets with climate control for those wanting more privacy
- Secure rooms available
- Managed Firewall services with 24X7 monitoring available

**Network Security**

- Written network access security policies readily accessible
  - Password policies (not sharing/lengths/forced renewal/aging)
  - Acceptable use (ISP not allowed to run programs that are illicit/illegal, use of sniffers or cracking/hacking programs)
  - User responsibilities on security
  - Asset protection
- Network security infrastructure in place
  - Perimeter protection (firewalls, filtering router)
  - Intrusion detection
  - Authentication & Authorization (passwords, RADIUS/TACACS, Secure ID’s)
  - Backup & Recovery Systems (to restore after a problem) (load balancing, fail-over protection)
  - Regular on going assessment of network infrastructure
  - Assessment of network expansions or additions

**Operations**

- Database of all installed equipment and configurations
- Toll free telephone support
- Supported monitoring
  - 24x7 monitoring of dedicated servers and network equipment (note both frequency and method, e.g., ping, SNMP)
  - 24 x 7 monitoring of the health of the equipment with alarms and pager alerts for network failure/failovers
- Alternate NOC available
- Second-tier support personnel located nearby

**Trouble tickets**
- Created and logged for all unusual or unexpected events
- Automated case escalation procedures in place including escalation time frames

Delcina J Betts
Technical Business Development Manager,
Cisco Powered Networks
Outsourcing Managed Network Services
Is the decision right for your network?

- Reporting that provides trending statistics on trouble tickets and minutes (above) to facilitate quality / customer reports
- Performance reporting and End-User impact monitoring
- Periodic and exception reports provided to customers (including usage and problem reports)

- Spare equipment on site for key networking equipment available in case of hardware failure
- Business Continuity Plan
  - Daily Site Backups
  - Tape vaults or other secure storage facilities on site in case of natural disaster
  - Onsite and Off-site storage available

**Backbone connectivity**

- Multiple direct connections to Tier 1 Internet carriers.
- BGP-4 routing
- Class C Internet Address blocks available
- Each carrier has a secure termination area, and location supported via the NOC or via the carrier providing the termination
- Fiber enters the data center through diverse conduits/routes (example if a backhoe cuts though conduit, will the design re-route to minimize loss of service)
- Aggregate bandwidth sufficient to scale the network to meet customer's service demands
- Describe policy on facility utilization or over-subscription
- Provider must have private facilities connecting to other data centers, and a documented process

**Gateway/WAN Edge layer**

- High end routers in a redundant configuration
- Hot Standby Router Protocol (HSRP) implemented
- BGP4 implemented
- Adequate total packet-per-second capacity for peak customer load
- Firewalls in place
- Provider has a network security team
- Remote firewall management offered

**Core layer**

- High-end switches deployed
- Switching and links entirely redundant with no single points or paths of failure
- Web cache redirection implemented
- Content and TCP offloading implemented via Reverse Proxy caching
- HSRP implemented for fail-over protection
- Intrusion detection implemented
- Automatic notification of intrusion attempts in place
Outsourcing Managed Network Services
Is the decision right for your network?

**Distribution layer**

- High to mid range switches deployed
- Switching and links entirely redundant with no single points or paths of failure
- Caching systems implemented
- Server load balance implemented
- Server content routing implemented if multiple data centers
- Caching implemented

**Access layer**

- Mid range switches deployed
- All servers dual-homed

**Cabling**

- All cable runs located under raised flooring and appropriately marked
- All cable runs physically protected from damage via tie-downs or where appropriate in conduit
- All cabling designed to Category 6 specifications (to support 1Gb/s data rates)

End figure