



White Paper

The Business Case for Out-Tasking Multiservice IP VPN Management

Businesses of all sizes worldwide are deploying their voice and video applications over the same IP networks they use for data applications, with the twin goals of cutting IT costs and improving productivity. Out-tasking IP VPN service management reduces risk, avoids the need to hire and train staff members with specialized expertise, and often proves the more economical option because it reduces operational and maintenance costs and makes costs more predictable.

The Cisco® Powered Network QoS Certification for Multiservice IP VPNs Indicates that the Service Meets the Needed Quality of Service for Delay-Sensitive Traffic.

Executive Summary

Before adopting a converged network, companies want to ensure that their networks deliver adequate quality of service (QoS) to support delay-sensitive voice and video traffic. Deploying a multiservice IP VPN can help ensure a business that its networks provide the needed QoS. Their next choice is whether to design, build, and manage the network in house or out-task service management to a provider.

This white paper is intended for business decision makers in businesses of all sizes that are considering deploying voice or video applications over the same IP networks they now use for data. The paper begins by explaining the business advantages of a converged network and summarizing the network capabilities needed to deliver high-quality voice and video over IP. Next it describes the components of QoS. The paper concludes with the advantages of out-tasking IP VPN network management and reasons for choosing a provider whose service has earned the Cisco Powered Network Multiservice designation with QoS certification.

Business Need

Traditionally, companies have developed and maintained separate networks for their data, voice, and video traffic. To reduce capital expenditure and operational costs, many now deploy a single, converged network that supports multiservice traffic. A converged network also helps increase productivity by supporting applications such as voice over IP (VoIP), unified messaging, videoconferencing, and customer service applications that provide access to real-time audio and video using a Web interface.

To deploy a multiservice IP VPN, companies want assurance that the end-to-end network delivers the quality and reliability to meet business expectations. This requires applying QoS techniques to assign priority to real-time voice and video applications. A network with end-to-end QoS transports delay-sensitive and mission-critical traffic across the WAN ahead of lower-priority traffic, such as e-mail, so that network performance remains consistent and predictable.

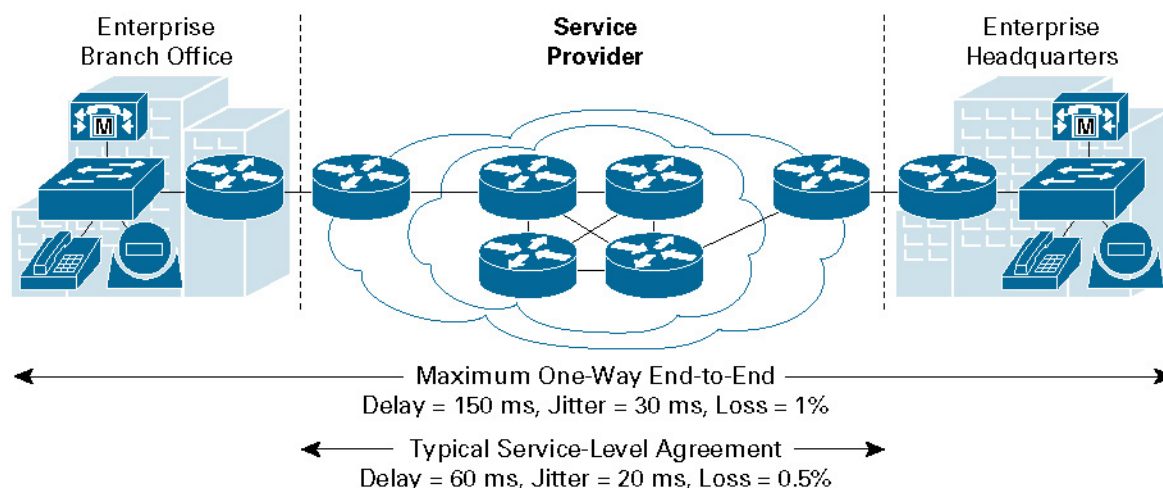
What is Required for Quality of Service?

To provide business-class voice and video services end to end, an IP-based VPN must meet the following requirements (see Figure 1):

- End-to-end delay, or the aggregate of the delay in each node and link along the path, less than 150 milliseconds (ms)
- End-to-end variation (jitter) less than 30 ms
- End-to-end packet loss less than 1 percent

Figure 1

Required Network Characteristics for Time-Sensitive Applications



To deliver QoS, the multiservice IP VPN performs the following steps:

Step 1: Classification and marking. Classification and marking tools mark each packet according to how it should be treated – for example, high priority for voice and best-effort for e-mail.

Step 2: Policing. Policers determine whether packets conform to the traffic rates that the network administrator has defined. If they do not conform, the policers take an action such as remarking or dropping the packet(s). This practice helps ensure that the network consistently achieves the desired traffic pattern and thresholds.

Step 3: Queuing. Bottlenecks can occur if packets enter a device faster than they can exit, as happens when the incoming link has higher throughput than the outgoing link. Scheduling tools overcome this problem by defining how packets exit a device. Devices with buffers allow the network administrator to specify that higher priority packets, such as voice and video, can exit before lower priority packets.

Step 4: Link-specific QoS. Individual WAN or VPN links can employ additional QoS mechanisms to mitigate delays. These techniques are called link fragmentation and interleaving (LFI) and shaping.

Process for Deploying QoS-Enabled Network Services

Companies can follow a five-step process to deploy QoS:

1. Define business objectives:

- Identify mission-critical applications; the fewer that receive this classification, the better their end-to-end performance across the network
- Obtain endorsement on business requirements from executives
- Determine how many classes of traffic are required to meet objectives: more classes translates to more granular service guarantees (see Figure 2)

2. Analyze service-level requirements:

- Voice, which is affected by loss, delay, and delay variation
- Video, also affected by loss, delay, and delay variation
- Data, which varies according to the application

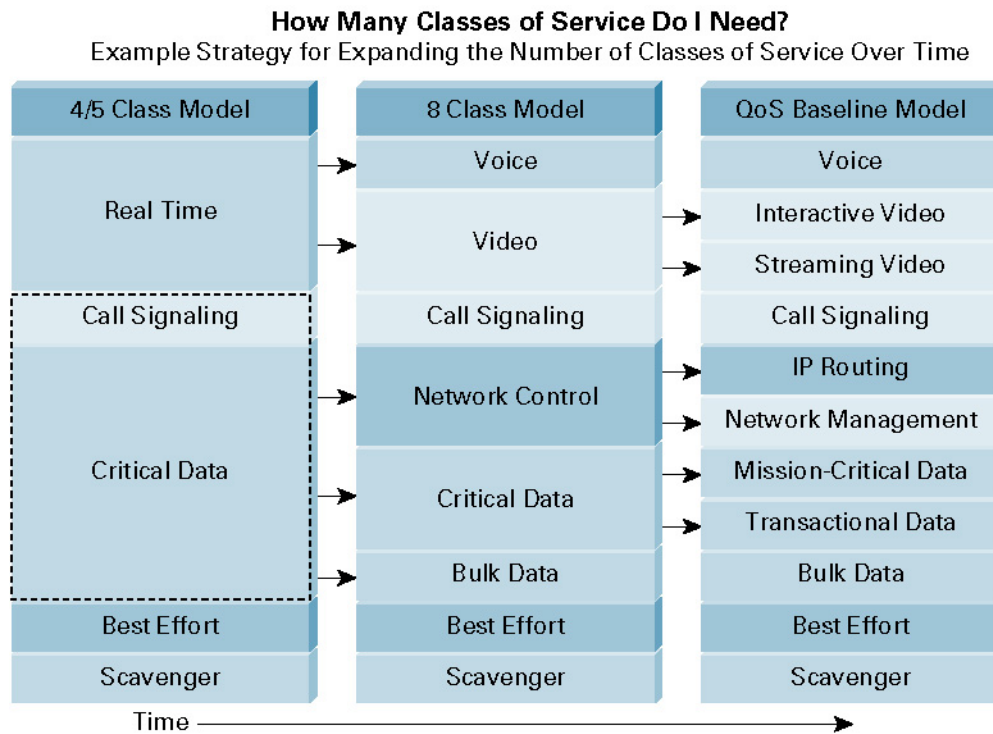
Different versions of the same application can have different traffic characteristics. Consider the Create Sales Order transaction in the SAP R/3 application. The transaction involves 14 KB of data, which requires 112 kbps for a response time of less than one second. If the enterprise provisions SAP as a mission-critical application that receives 25 percent of link capacity, then the link must be 512 kbps. If the enterprise runs a newer version of SAP R/3, then the same transaction might involve 490 KB of data, not 14 KB. If the enterprise did not change the bandwidth, transaction time would lengthen to 32 seconds. Therefore, in the case of increased data traffic, QoS requirements must be re-evaluated to accommodate required service levels.

3. Design and test QoS policies against business objectives and requirements

4. Roll out the QoS designs to production network in phases, during scheduled downtime

5. Monitor service levels to help ensure that objectives are met across the entire network

Figure 2
Models for Identifying Classes of Service



Why Out-Task to a Service Provider?

Companies that deploy networked resources over WANs have the option to design, build, provision, support, and manage a multiservice IP VPN using in-house resources, or to selectively or totally out-task that responsibility to a service provider. The decision affects IT workload, capital expenditure, and ongoing operational expenses and it potentially can affect QoS, service availability, and network security. Out-tasking multiservice IP VPN management spares companies from devoting resources to:

- Plan, design, and implement the network in order to classify, prioritize, and optimize traffic flow as described earlier in this paper
- Monitor the network 24 hours a day to help ensure optimal performance

According to Gartner, most Fortune 1000 large enterprises are out-tasking or planning to out-task the management and support of their corporate networks. For medium-sized businesses in the United States and Canada, 41 percent and 23 percent, respectively, are planning to out-task; and for small businesses in the United States and Canada, 12 percent and 13.5 percent, respectively, will out-task network service management.¹

Following are the primary incentives for enterprises to out-task VPN service management:

¹ Gartner, Managed Services Uncovered: North America, July 2002

Free Resources to Focus on the Core Business

By working with a service provider that offers managed, multiservice IP VPN services, companies can delegate the routine tasks they do not see a compelling reason to control, such as daily monitoring, support, provisioning, transport, and router maintenance. At the same time, they free staff resources to focus on the core business as well as strategic initiatives.

Reduce Costs

Gartner reports that large enterprises in the United States that out-task network management to service providers cut their network costs by up to 25 percent, and small U.S. businesses can experience up to 15 percent cost reductions. In fact, access to the service provider's lower cost structure, the result of a greater economy of scale, is one of the most compelling tactical reasons for out-tasking, according to The Outsourcing Institute of Jericho, New York. The service provider can charge less than its customers would otherwise spend for operations, maintenance, service, equipment, and technology upgrades.

Companies that out-task network management not only reduce their costs, they also make recurring costs more predictable by shifting from a variable to a fixed-cost model. These businesses know their monthly costs in advance, as compared to businesses that need to find the budget for unexpected expenses related to network upgrades or outages. Out-tasking network management also permits more gradual investment, eliminating the need to overpurchase at the outset of service deployment to accommodate anticipated growth.

Gain Expertise and Support Not Available In House

Service providers often can provide networking skills not readily available within the enterprise. The value of this benefit increases as companies deploy more applications and users and as network management becomes more complex. Service providers have the resources to offer 24-hour monitoring, management, and support – capabilities not readily available in house to any but the largest enterprises. Service providers also can offer rapid deployment because of their deployment experience. Even for companies with large in-house staffs, service providers can fill critical resource gaps such as network security, which typically require special training and expertise.

Get the Right Service from the Right Provider

Choosing the right service provider when out-tasking the responsibility for your multiservice IP VPN can be critical. Since 1997, businesses have depended upon the Cisco Powered Network designation to find providers that deliver their services over a network built end to end with Cisco products and technologies and that meet Cisco standards for network quality. Today, that designation is even more important because providers that offer IP VPN services must now pass an objective assessment certifying that the service meets Cisco best practices and standards for QoS for the metrics shown in Table 1.

Table 1. QoS Requirements for Service Providers to Receive the Cisco Powered Network IP VPN-Multiservice Designation

QoS Metric	Allowed End-to-End	Allowed in Service Provider Core
One-way, end-to-end delay	<150 ms	<60 ms
Variation, or jitter	<30 ms	<20 ms
Packet loss	<1%	<0.5%

Certification Process

The process for awarding the Cisco Powered Network IP VPN-Multiservice designation is an objective one. A third-party consultant conducts an on-site assessment that verifies that the service provider follows best practices for delivering the recommended levels of delay, jitter, and packet loss. During the assessment, the third-party assessor interviews the service provider's technical staff, asking questions such as:

- Does the service provider track and monitor the end-to-end network?
- Can the service provider secure its own network traffic and manage priority traffic across other networks?
- What are the minimum thresholds for network latency and availability?
- How is performance measured?
- Do procedures exist for load balancing, mirroring, caching, integrity, and performance design reviews, security, backup, and recovery?
- Can the service provider's data center support enterprise requirements for physical and network security, capacity, availability, operations, and backbone connectivity?
- How quickly will the service provider respond as the enterprise customer's business grows or changes?

This ongoing, rigorous assessment provides objective validation of the service provider's qualifications and the performance you can expect from its IP VPN services. Services that display the logo in Figure 3 have passed the Cisco assessment and are certified by Cisco to employ the best practices necessary to deliver real-time voice and mission-critical applications over the IP VPN.

Figure 3

Cisco Powered Logo with QoS Descriptor



Conclusion

To deliver real-time voice and video applications end to end, companies need a QoS-enabled network. Because of the expertise required to develop and monitor such a network, out-tasking VPN service management to a service provider can dramatically reduce risk and is often the most economical choice.

New QoS certification requirements can help businesses locate providers of managed IP VPN services that meet Cisco best practices. Cisco works closely with service providers that have qualified for this designation to help ensure they are planning, designing, and deploying highly reliable networks and managed services to meet business needs.

To locate IP VPN services that have earned Cisco Powered Network designation and are certified by Cisco, visit: <http://www.cisco.com/cpn>.

To learn more about the value of managed services, visit: <http://www.cisco.com/go/managedservices>.

**Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco *Powered* Network mark, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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. (0502R)

DM/LW9321 09/05