



White Paper

Quality of Service for Managed Multiservice VPNs: Network Requirements and Out-Tasking Options

Businesses of all sizes worldwide are exploring the benefits of 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. But before adopting a converged network, companies need to have confidence that it will deliver adequate quality of service (QoS) to support delay-sensitive voice and video traffic.

The Cisco Powered Network QoS Certification Indicates That a Managed IP VPN Service Meets QoS Requirements for Delay-Sensitive Traffic

Executive Summary

To support delay-sensitive voice and video traffic, businesses need an IP virtual private network (VPN) that meets specific service levels for delay, variability, and packet loss. Enabling technologies include classification, prioritization, and link optimization.

An organization can choose between designing, building, and managing an IP VPN in house or out-tasking to a service provider. Out-tasking can reduce risk, avoid 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.

This white paper is for technical staff members in small and midsize businesses and large enterprises that are considering deploying voice or video over the same IP networks they now use for data. The paper begins by briefly reviewing the business need for converged networks. Then it explains the network capabilities needed to deliver high-quality voice and video over IP and the advanced technologies used to achieve these goals. The paper concludes with the advantages of out-tasking and reasons for selecting a service provider whose IP VPN service carries the Cisco® Powered Network designation with QoS certification, which means its service is delivered over a network built end to end with Cisco Systems® hardware and software, and meets Cisco best practices and standards for QoS.

Business Need

More and more companies are deploying corporate networked resources or applications on converged networks that support not only data but also real-time traffic such as voice and video. Primary motivations are to cut costs by maintaining and managing one network instead of two or more and to gain productivity advantages from applications such as voice over IP (VoIP), unified messaging, videoconferencing, and customer-service applications that provide access to real-time audio and video via a Web interface.

To deliver voice and video over a managed multiservice IP VPN, service providers need to ensure that quality and reliability meet enterprise expectations. Simply planning to add bandwidth is neither cost effective nor practical because accommodating growth would require continual capital outlays, and bandwidth provisioning delays might cause quality problems. The more practical, proven approach is to imbue the multiservice IP VPN with QoS so that real-time voice and video traffic flows are properly classified and prioritized to support VoIP applications. The technical challenge is to manage this time-sensitive traffic across the WAN with end-to-end QoS so that network performance remains consistent and predictable.

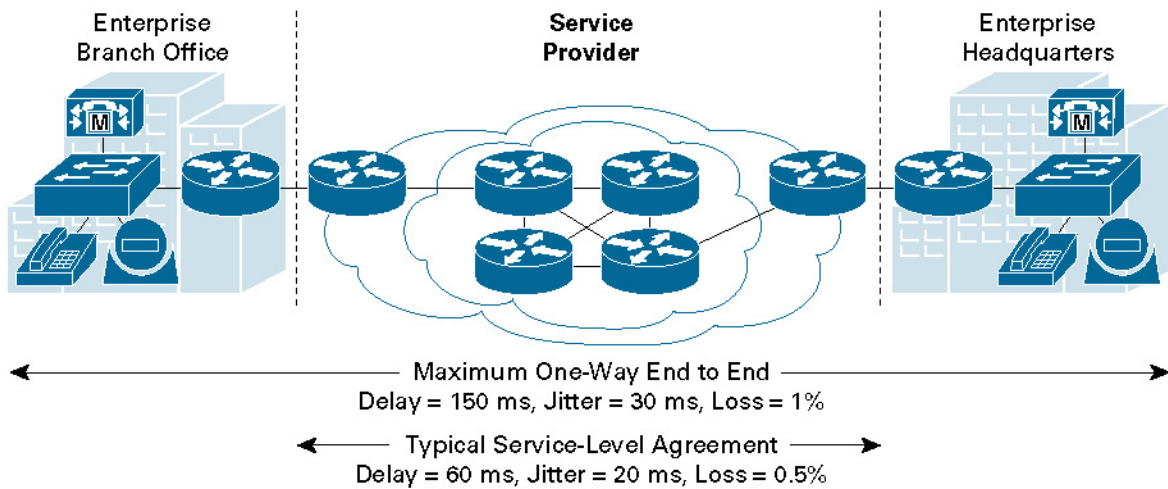
Technical Requirements for QoS-Enabled Networks

To provide business-class voice and video support, IP-based VPNs must meet the following requirements (Figure 1):

- End-to-end delay less than 150 milliseconds; end-to-end delay is the aggregate of the delay in each node and link along the path
- End-to-end variation (jitter) less than 50 milliseconds
- End-to-end packet loss less than 1 percent

Figure 1

Required Network Characteristics for Time-Sensitive Applications



To achieve these recommended limits for delay, jitter, and packet loss, enterprises or their service providers employ a variety of technologies related to capacity, classification, prioritization, and link optimization. Note that enterprises can avoid learning and implementing these technologies by out-tasking multiservice VPN service management to a service provider with in house expertise.

Capacity

Capacity refers to the actual throughput, as opposed to bandwidth, across each link. The multiservice IP VPN needs adequate throughput at each link to avoid delay when enterprise traffic is at its peak rate.

Classification

To minimize delay and packet loss, the network must classify all traffic flows, especially real-time voice and mission-critical applications, according to its performance requirements. Classifications typically include high priority, low latency, or best effort. When the network is congested, traffic classified as critical will advance to the head of the queue so that it is not impeded by non-critical traffic. The enterprise is responsible for classifying its traffic at the enterprise edge, unless it out-tasks to a service provider, in which case the service provider assumes this responsibility. Note that many networks use Layer 2 link-layer technologies, such as Frame Relay and Ethernet, in addition to Layer 3 technologies. In this situation, to provide end-to-end IP QoS, Layer 2 and Layer 3 QoS classifications must match.

Prioritization

Prioritization ensures that delay-sensitive voice and video payload and signaling packets are forwarded in a timely fashion. When outbound traffic is congested, packets with higher priority, such as voice and video packets, are forwarded before data packets – even if the data packets arrive first.

Link Optimization

Link optimization techniques include link fragmentation and interleaving (LFI) and shaping:

- LFI – On access links between the enterprise edge and service provider edge under 768 kbps, large data packets can create delays that exceed acceptable levels. To prevent such delays, the enterprise or its service provider can fragment the data packet at the enterprise edge.
- Traffic shaping – While LFI helps ensure QoS when the network carries very large packets, traffic shaping helps ensure QoS when total traffic from all remote sites exceeds the bandwidth capacity at the central site. In effect, traffic shaping accommodates mismatches between access speeds and aggregated bandwidth.

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-size 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:

Free Resources to Focus on the Core Business

By working with a service provider that offers a managed multiservice IP VPN solution, 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

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 also permits more gradual investment, eliminating the need to overpurchase at the outset of service deployment to accommodate anticipated growth.

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

Gain Expertise and Support Not Available In House

Service providers can often 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 can also 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 requires special training and expertise.

Get the Right Service from the Right Provider

Choosing the right service provider when out-tasking the responsibility for a 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. Requirements for Service Providers to Receive the Cisco Powered Network 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

Cisco has established an objective process for awarding the Cisco Powered Network QoS Certification. A third-party consultant conducts an on-site assessment that verifies that the service provider follows best practices for delivering service-level agreements (SLAs) pertaining to delay, jitter, and packet loss. During the assessment, the third-party assessor reviews key aspects of the service provider's operations, 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 to changing networking requirements 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 2 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 2

Cisco Powered Logo with QoS Descriptor



Conclusion

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

Locating a managed IP VPN service to meet your business requirements has become straightforward, the result of the new requirements that Cisco uses to award QoS certification. Choosing a service that carries a Cisco Powered Network designation with QoS certification helps assure businesses that they are depending on highly reliable networks that will meet their business needs.

To locate a managed IP VPN service that has earned Cisco Powered Network QoS Certification, visit: <http://www.cisco.com/cpn>.

To learn more about 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/LW9319 09/05