



White Paper

Optimizing Enterprise WAN Efficiencies Using Classes of Service

Executive Summary

The move to converge data, voice, and video onto a common network, coupled with the widespread adoption of IP VPNs, brings a new challenge to enterprises. A converged, common network can now meet the performance requirements of an increasingly broad mix of applications, but low-priority traffic can easily bog down bandwidth resources that are also needed for critical applications. To get the best returns on investment for network-based business applications, enterprise IT teams must be able to evaluate and optimize the behavior of these applications across all points in the corporate WAN, and to understand the network traffic that affects overall application efficiency.

This white paper explains the basics of a service-class-oriented structure that helps ensure optimal application performance across an enterprise WAN. A class-of-service (CoS) scheme is discussed as it relates to an end-to-end quality-of-service (QoS) solution for an enterprise, today and in the future. Recommendations to enterprise IT managers are provided for evaluating the class offerings from service providers, so that enterprise and service provider classes mesh transparently, without compromising the business requirements for the enterprise.

“CoS is rapidly becoming a major selling point for all service providers, as well as network resource engineering.”


– Henning Dransfeld and Stephen Young, January 2005, Ovum

VPNs and Application Optimization

IP VPNs are becoming commonplace in today's enterprise WANs. Compared to Frame Relay, IP networks offer simplified application deployment for enterprise resource planning (ERP), e-learning, hosting, telephony, centralized application services, and video services. These mission-critical and time-sensitive applications require QoS. Frame Relay, as a Layer 2 transport with no knowledge of higher-layer traffic, can provide QoS only per permanent virtual circuit (PVC). IP VPNs on Multiprotocol Label Switching (MPLS)-enabled networks can provide QoS on a per-packet basis, enabling rapid, enterprisewide application deployment compared to Frame Relay environments.

Other benefits offered by IP VPNs include:

- Reduced costs and the ability to introduce new productivity-enhancing IP-based applications through convergence of previously disparate data, voice, and video networks
- Delivery of consistent services to all users
- A foundation for deploying enhanced services (voice, for example)
- Enhanced network connectivity to geographically dispersed branch offices, remote users, teleworkers, and business partners, and the ability to share information among distributed teams
- Improved scalability with the ability to support both small and large deployments, and reduced time for adding sites and users



IP VPNs on MPLS-enabled networks provide additional benefits to the enterprise with other built-in abilities, including traffic engineering, security and privacy features, scalability, and the flexibility to support thousands of sites and users.

Traffic that traverses the public Internet typically does not receive different levels of service for different packet types. As networks consolidate, traffic types become more intermixed in a converged network – e-mail and games are sending packets alongside packets from videoconferencing applications, ERP report-generation programs, and IP phones. Networks must be able to identify traffic in terms of the application that it services. IP technology includes provisions for defining the type of service (ToS) requested for each packet. ToS must be recognized, and QoS established, to allow the delivery precedence of traffic associated with a complex mix of enterprise applications.

Meeting Application Requirements on IP VPNs

Meeting application demands in an enterprise WAN and on IP VPNs requires QoS practices to be incorporated by the enterprise and the service provider. QoS is the network's ability to deliver the end-to-end service characteristics an application needs in order to meet the requirements of a enterprise customer. One particular QoS category – the definition and implementation of service types – addresses application performance issues by classifying traffic into distinct classes of service. Today, enterprises and service providers deploy as few as two or three, or up to a dozen, classes of service.

Without classes in the enterprise environment, enterprises and service providers have traditionally solved the problem by provisioning more bandwidth. This approach can be cost-prohibitive and wasteful, if only one or two applications require stringent guarantees to operate satisfactorily. Implementing multiple classes of service on the network, each with a different performance guarantee, does not negate the need for proper capacity planning. It does, however, enable the network's capacity to be used by the classes for which it was intended. This becomes most apparent when considering voice traffic; the end-to-end delay for voice packets needs to be less than 150 ms for a satisfactory user experience. In a network that does not differentiate between traffic types, overall network capacity must be built in to meet that delay requirement for all traffic. In a network that does differentiate between traffic, bandwidth and queuing can be optimized to meet the required delay characteristics for voice traffic.

Businesses today also need the ability to monitor and manage traffic associated with individual applications or categories of applications. This demand for traffic monitoring is necessary to measure the overall efficiency and productivity achieved with each application, and also to identify problems with the underlying network infrastructure such that user and application disruptions can be minimized. With the proper network management tools, businesses can also proactively monitor and manage their networks to help ensure that overall business efficiencies related to network and application usage are fully met.

Planning for Classes of Service in Enterprise WAN Networks

As part of an end-to-end QoS solution, the class capability helps ensure that time-sensitive traffic is given the appropriate priority over the network, and that stringent latency requirements can be met. To define the requirements for each class, enterprises must first identify the applications that are running on the network, and be able to address the unique network metrics required for these applications:

- Which applications will be running over the WAN?
- Are voice, video, and high-priority data applications supported today, or will they be in the future?
- How does/will the voice and video traffic affect the other applications?

An audit of the current applications should be performed to establish benchmarks for today's traffic patterns, and to identify the most important performance metrics for delay-sensitive applications. These metrics will be identified in terms of data loss, delay, and delay variation.

“The Yankee Group thinks there will be a bigger cost to enterprises if they do not invest time to audit. There is the risk that the network implementation will not be optimally designed. In addition, there is the need to return to the negotiating table with a supplier to revisit requirements. So keeping tabs on equipment deployments, network connections, and applications usage is not only good housekeeping, but also good business.”

– From “Navigating the IP VPN Market: A Decision-Making Guide for European Businesses,” by Camille Mendler and Amy Rodger, May 2003, The Yankee Group

Requirements for Consolidated Data, Voice, and Video Traffic

Enterprise IT managers must be familiar with the characteristics and requirements for the three types of network traffic:

- **Voice** – Voice traffic is smooth, benign, drop-sensitive, and delay-sensitive, and is typically User Datagram Protocol (UDP)-based. Bandwidth per call depends on the particular codes adopted, sampling rate, and Layer 2 media employed. Voice quality is directly affected by all three QoS quality factors (loss, delay, and delay variation).
- **Video** – Video traffic is bursty, bandwidth-greedy, drop-sensitive, and delay-sensitive. IP-based videoconferencing has some of the same sensitivities as voice traffic.
- **Data** – This category of traffic is much more varied. It can be smooth or bursty, benign or greedy, or drop- and delay-insensitive, and involves Transmission Control Protocol (TCP) for send/receive acknowledgment and retransmit. Traffic patterns vary by application, and data classes must support several different priorities or application categories.


Delay, Packet Loss, and Jitter Tolerances for Multiservice Traffic

Data traffic is typically handled with multiple classes, where each class can be defined and given the appropriate support based on the priority requirement of the application that is generating the traffic. In general, enterprises should restrict themselves to about five main traffic classes, such as:

- **Mission-critical and real-time** – Transactional and interactive applications with high business priority; in some cases, real-time traffic such as voice over IP (VoIP) can be subdivided into a separate class
- **Transactional/interactive** – Client-server applications, messaging applications (typically foreground activities that directly affect employee productivity)
- **Business or bulk** – Large file transfers, e-mail, network backups, database synchronization and replication, and video content distribution (background activities that do not directly affect employee productivity and are generally time-insensitive)
- **Best-effort** – Default class for all unassigned traffic; typically at least 25 percent of bandwidth is reserved for best-effort traffic
- **Scavenger (optional)** – Peer-to-peer media sharing applications, gaming traffic, and entertainment traffic

For voice traffic, three parameters are essential:

- **Loss** – Causes voice clipping and skips. The industry-standard algorithms implemented by most digital signal processors (DSPs) can typically correct for up to 30 ms of lost voice with the use of concealment algorithms. The loss of two or more consecutive 20-ms voice samples will result in noticeable degradation of voice quality.
- **Delay (latency)** – Causes voice-quality degradation if it is above 150 ms one way.
- **Delay variation (jitter)** – The adaptive jitter buffers within most IP telephony devices can usually compensate for 20–50 ms of jitter. These jitter buffers are dynamically adaptive; there is no defined and absolute limit for jitter that will hold true for all circumstances. However, most testing shows that when jitter consistently exceeds 30 ms, voice quality degrades significantly.



There are two main types of video applications – interactive video (such as videoconferencing) and streaming video (such as Cisco IP/TV[®] content, which may be either unicast or multicast).

For interactive video traffic:

- Packet loss should be no more than one percent.
- One-way latency should be no more than 150 ms.
- Jitter should be no more than 30 ms.
- For streaming video traffic:
 - Packet loss should be no more than two percent.
 - Latency should be no more than four to five seconds (depending on video application's buffering capabilities).
 - There are no significant jitter requirements.

Working closely with a service provider, enterprise IT managers can fine-tune specific requirements for delay, packet loss, and jitter parameters.

Defining Classes

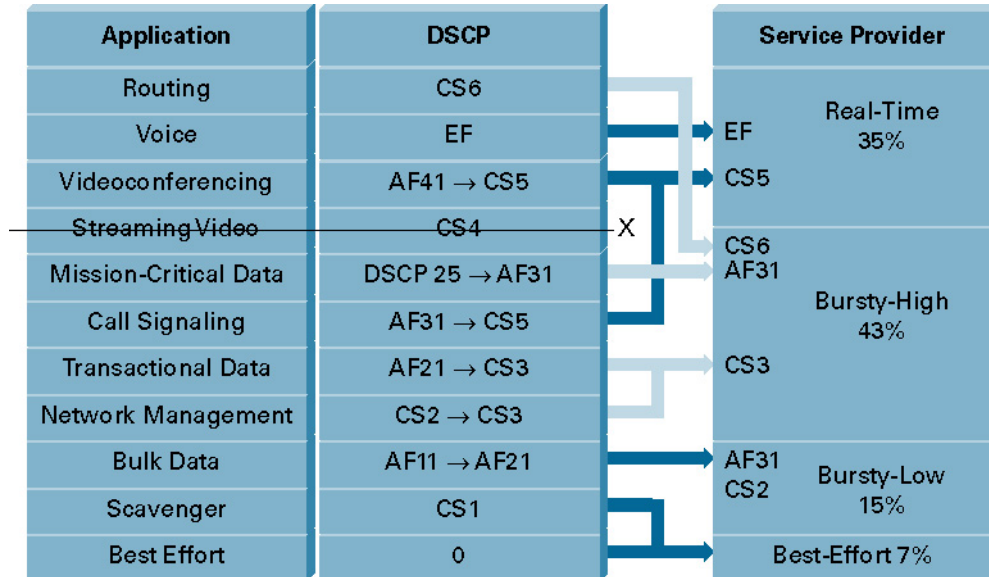
After auditing their present and future application requirements, enterprises can define the required classes for their environments and specify the network performance parameters that must be provided for each class. MPLS-based networks offer a broad range of class support, and enterprises can take advantage of inherent MPLS capabilities to implement traffic classification, priorities for traffic movement, and monitoring traffic classes.

Evaluating Service Providers and Class Offerings

Today, many enterprises implement in-house class schemes to optimize traffic on enterprise-owned-and-operated networks. Enterprises can also work with service providers and engage them to manage all or part of their WANs, to extend their networks, or to connect multiple networks. When working with a service provider, an enterprise must compare the in-house class requirements with the abilities of the service provider network. Service providers vary greatly in terms of the numbers of classes implemented on their networks, but a service provider need not offer the same number of classes that are defined within the enterprise network. This presents a challenge – the class markings and number of classes defined within the enterprise need to be mapped to the class offerings supported by the provider. QoS transparency allows enterprise class labels to be retained so that traffic going through the service provider network will translate back to the finer-grained class scheme of the enterprise network. The service provider only needs to make sure that the requirements for each of the defined enterprise classes can be met within the class levels that they do offer across the network. The Cisco Enterprise Solutions Engineering (ESE) team works with many enterprises to simplify the mapping between enterprise classes and service provider offerings (Figure 1).

Figure 1

A Cisco ESE Design Map of an Enterprise's Service Levels to a Service Provider's Offering



Working with a service provider does not eliminate the application audit process that was previously described. Each enterprise should still fully explore current and future application situations, and fully define class requirements, based on its particular business needs.

With multiservice IP VPNs in particular, businesses are realizing the additional benefits of managed services. A service provider can handle part or all of an enterprise's need for installation, provisioning, management of network equipment, support of network transport, and network security. Managed VPN services offer enterprise customers immediate access to the benefits of an MPLS network, with network availability and security being managed by the service provider 24 hours per day. Service-level agreements (SLAs) can be established to define the required network performance, and to set metrics for monitoring and reporting actual performance against the requirements. Service providers can also deliver valuable support services – such as “follow-the-sun” help desks – that would require extensive staffing resources and budgetary support if implemented in-house.

Today, enterprises choose to work with service providers when they are:

- Facing challenges – Service providers can help enterprises with IT resources, infrastructure management, security, responding to market demands quickly with flexible and scalable networks, remaining competitive, and reducing costs.
- In transition – Enterprises often need assistance when it becomes necessary to upgrade or relocate infrastructures, change the scope or scale of operations, adjust for a merger or acquisition, or introduce new services to meet customer demands or company growth.
- Setting priorities to increase revenue – Service providers can help enterprises remain focused on mission-critical processes rather than day-to-day support and management of networking resources, and can help ensure secure communications and expand an enterprise WAN as business grows.

For more information about selecting and working with service providers, please visit: <http://www.cisco.com/go/managedservices>.

In addition to exploring service providers' abilities to support QoS transparency, enterprises should evaluate and compare service providers in terms of:

- Cost – What are the basic class bundles offered?
- Application certification – Some service providers offer services that are certified for specific applications. Application certification is relatively new; few service providers have started or completed it today, but each service provider should be evaluated in terms of their plans and commitment to certification for the applications that are most relevant to the enterprise.
- Numbers of class levels – While QoS transparency allows multiple enterprise class levels to be combined into fewer levels on a service provider network, a service provider that provides class levels that more closely match the enterprise levels may be a better fit.
- Measurement and monitoring tools – Which measurement and monitoring tools does the service provider make available to enterprise customers? Are these included in the basic service, or is there an extra cost?
- Reporting – Based on the enterprise requirements, can the service provider deliver real-time performance reports on schedule and with the desired information?
- Escalation procedure – What support teams and procedures are in place for identifying troublesome network behavior? Are notifications provided via e-mail or phone? Who will be the point of contact for the enterprise and for the service provider?
- SLA enforcement – What compensation is offered when an SLA is not met? How is a violation defined? Is the credit automatic?
- Security – What WAN access will be given to or required by the service provider?
- Use of existing equipment – Can the service provider support the existing equipment or must new equipment be purchased at the customer edge?
- Interprovider CoS – Today, multinational companies do not have many options if they require multiple service providers to interface with each other. Some providers are starting to explore interprovider CoS as an enhanced service; these solutions will allow service providers to team up and handle enterprise WANs that span multiple provider infrastructures. A service provider's commitment to tracking and implementing these emerging standards should be taken into consideration.

Monitoring Tools

Once the class scheme and requirements are defined, with the service provider selected and the classes implemented, the enterprise IT team must have the means to monitor the WAN and the applications to verify that the defined performance requirements are being met. Service providers will typically monitor and report on many performance metrics, to conform to the SLAs in place. They may also provide monitoring tools that allow the enterprise customer to independently monitor the SLAs. Two basic monitoring modes are last-mile performance monitoring for assessing the customer edge-to-provider edge (CE-PE) access link, and end-to-end performance monitoring (CE-CE). End-to-end performance monitoring provides more relevant information – it encompasses performance of the network from the origination CE, through the provider's network, to the destination CE. While a service provider may have deployed a highly robust core network, enterprise IT managers should not assume that the core supports infinite performance. In many instances, an end-to-end monitoring tool can provide a complete performance picture. The enterprise IT team should discuss one or both of these monitoring options with the service provider, along with details of the SLA metrics that they provide. SLA metrics include general metrics for availability, mean time to restore (MTTR), and per-class metrics, including latency, jitter (for voice or real-time traffic only), and packet loss.

Even if a service provider performs monitoring services, it is highly recommended that enterprises carry out independent end-to-end monitoring. Cisco IOS® IP SLA, a network performance measurement feature in Cisco IOS Software, provides a scalable, cost-effective solution for service-level monitoring. It eliminates the deployment of dedicated monitoring devices by including the “operation” capabilities in the routers. This tool collects real-time network performance information, including response time, one-way latency, jitter, packet loss, and Website download time. Cisco IOS IP SLA also provides a mechanism to monitor performance for different classes of traffic over the same connection. For more information about Cisco IOS SLA, please visit:

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper0900aecd8017530d.shtml.

Cisco Systems® offers several other tools for network monitoring. For more information about these tools, please visit:

<http://www.cisco.com/en/US/products/sw/netmgtsw/index.html#products>.

Enterprises can also take advantage of any tools offered by their service providers, and can acquire additional monitoring tools from a growing list of third-party vendors.

Security concerns may make it preferable to limit a service provider’s monitoring capabilities, so that they do not have access to the sensitive portions of the enterprise network. In this case, the enterprise must retain responsibility for end-to-end monitoring. Optionally, security measures should be discussed if the enterprise wishes the service provider to monitor the complete network.

Cisco Powered Network Program

Cisco awards the Cisco Powered Network designation to service providers that use Cisco equipment from end to end in their networks and that meet Cisco standards for network support. Look for the Cisco Powered logo to identify providers with these qualifications.




More than 350 of the most successful service providers around the world have earned the Cisco Powered Network designation. Situated in 62 countries, these providers offer a wide range of services over Cisco equipment for small and large businesses. From basic services such as Internet access and Web hosting to emerging services such as IP telephony and storage networking, Cisco Powered Network providers should be an enterprise’s first choice.

Cisco has recently raised the value of the Cisco Powered Network designation by certifying that service providers with the IP VPN–Multiservice designation meet industry standards for delay-sensitive voice and video traffic and mission-critical data traffic. Now, enterprise customers can find providers that offer the best practices for SLAs pertaining to delay, jitter, and packet loss (Table 1).

Table 1. Multiservice IP VPN Performance Requirements for 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 percent	<0.5 percent



Candidates for this designation undergo a Cisco assessment that reviews the following aspects of a service provider's operations:

- Does the service provider track and monitor the end-to-end network?
- Can the provider secure its own network traffic and manage priority 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, performance design reviews, maintenance, inventory, upgrades of QA certification, deployments, 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 network requirements as the enterprise customer's business grows or changes?

For a list of recommended service providers, visit the Cisco Powered Network Website: <http://www.cisco.com/cpn>.

For more information about managed services over end-to-end Cisco networks, please visit: <http://www.cisco.com/go/managedservices>.

This site includes regularly updated information about topics that include:

- Frame Relay to IP VPN migration
- Yankee Group Report on IP VPNs, "Navigating the IP VPN Market: A Decision-Making Guide"
- VPN service overview for IT managers
- MPLS VPN security

**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

Copyright © 2005 Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, the Cisco *Powered* Network mark, Cisco Systems, the Cisco Systems logo, and Cisco IP/TV 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) DMLW8843 07/05