

# Voice Trunking and Toll-Bypass Trunking Using Cisco MPLS DiffServ-Aware Traffic Engineering

## Service Description

### Challenge

Service providers need to integrate their packet- and circuit-switched infrastructures to save costs and offer data and voice services. One attractive service is the ability to carry voice traffic from central offices of facilities-based competitive local exchange carriers (CLECs). Trunking voice traffic using a data infrastructure is less expensive than using dedicated circuit-switched infrastructure that may be underutilized.

Today's enterprise customers are also responding to voice and data convergence by actively seeking solutions that are both robust and low cost. These customers are increasingly using data networks to trunk voice traffic between sites for intracompany communications over virtual private networks (VPNs). Instead of using separate dedicated circuits for voice and data, enterprise customers can now use a single data network to carry their voice traffic, avoiding long-distance charges.

With increasing adoption of voice over IP (VoIP), the landscape for deployment is rapidly changing. Service providers are often driven by the need to provide a high grade of service to their customers to carry voice traffic across the network.

## Cisco MPLS DiffServ-Aware Traffic Engineering Solution

Today's multiservice packet networks rely on IP-based packet switching. However, IP by itself is simply a best-effort service, not sufficient enough to provide the strict delay, jitter, and bandwidth guarantees required for voice over IP (VoIP) and other real-time traffic. Cisco IOS® quality of service (QoS) is ideal for this situation. Using the IETF Differentiated Services model (DiffServ) for QoS, the network treats VoIP traffic appropriately. Although bandwidth is fairly inexpensive today, fiber resources are relatively scarce. Adding DWDM trunks can be an expensive proposition without a real need. Even for networks with ample bandwidth, an "insurance policy" is essential to ensure guaranteed quality for voice traffic, regardless of the overall network traffic load. Thus, service providers must extract the maximum profit benefit from every bit of bandwidth available. While the DiffServ model provides for this, a service provider must:

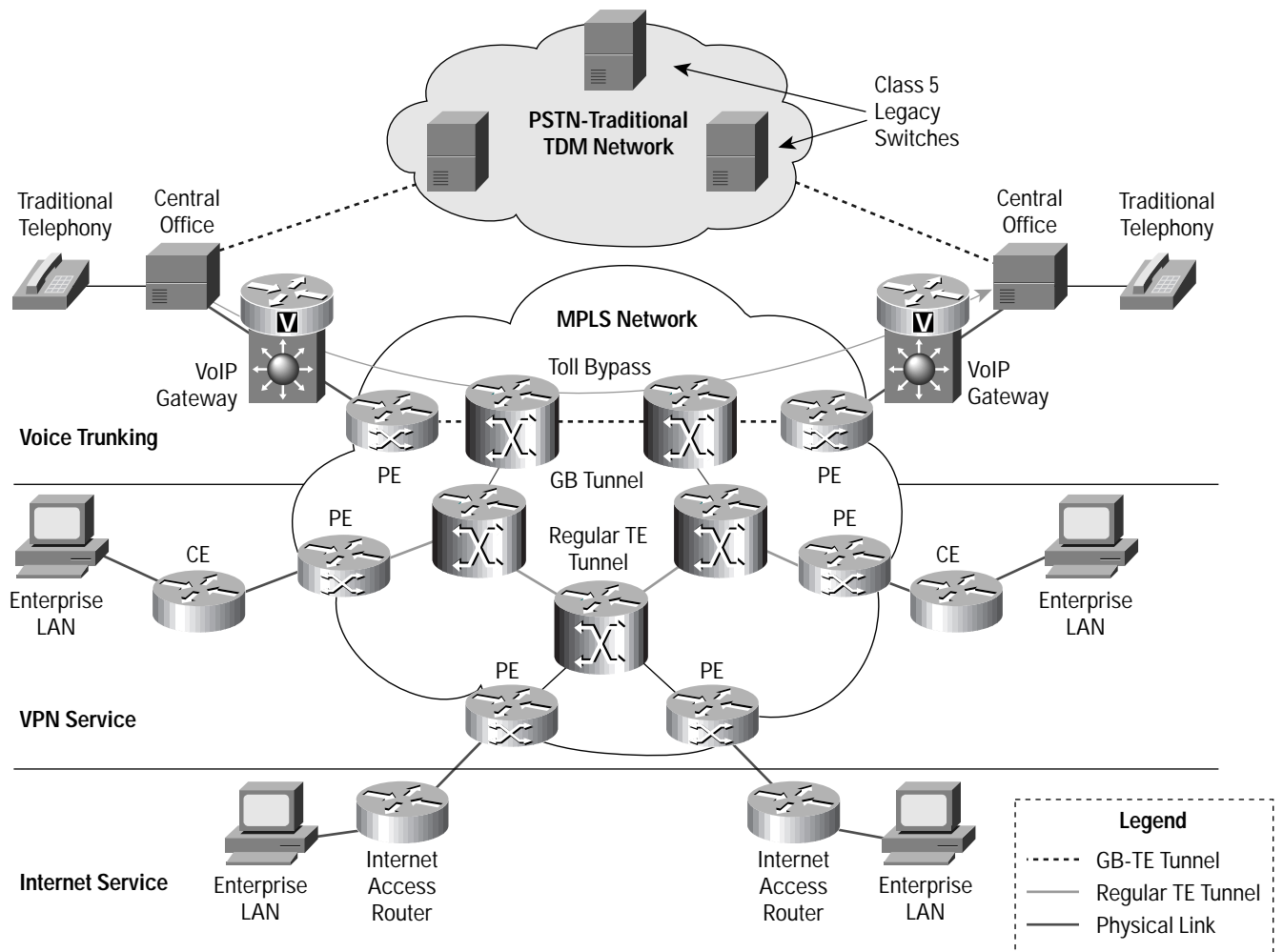
- Determine the path that IP routing takes for a particular customer's traffic
- Provision each router along the path for DiffServ
- Manually assure that not too many customers pass over that path, to avoid demand in excess of available bandwidth (the "over-subscription" scenario).



While this is feasible in a small network, a more scalable way to manage bandwidth is necessary to provide a point-to-point guarantee to the customer. Cisco DiffServ-Aware Traffic Engineering (DS-TE) is ideal for this situation. By automatically choosing a routing path that satisfies the bandwidth constraint for each service class defined (such as Premium, Gold, Silver, or Bronze), using DS-TE relieves the service provider from having to compute the appropriate path for each customer and each service class per customer.

A number of sites with various types of connectivity where voice trunking or toll-bypass trunking is required are shown in Figure 1. The enterprise customer infrastructure could be a Voice-over-IP or traditional telephone system.

Figure 1  
Comparison between guaranteed bandwidth TE tunnel and regular TE tunnel





## Service Characterization

Cisco IOS software enables service providers to implement the QoS capabilities they need to provide voice trunking capability on a data network.

The service provider has two choices:

1. Over-engineer the network so there is no congestion, under any circumstances
2. Enable QoS in the network for traffic and use other intelligent mechanisms such as DS-TE in MPLS to provide tighter QoS guarantees for bandwidth, delay, and jitter in the network

The first scenario is rarely the case, as bandwidth is price elastic—applications and users will soon utilize the available bandwidth. Thus, scenario 2 almost always applies: A network has either transient or persistent congestion.

The mechanisms a service provider chooses depend on how tight the QoS requirement is. For VoIP services or toll-bypass trunking, a service provider must deliver a very low-delay, low-jitter, and an assured amount of bandwidth.

## Requirements

**Bandwidth guarantees:** Toll-bypass trunking requires the equivalent of an emulated circuit, point-to-point, in the network, with bandwidth guarantees. The network devices must be capable of scheduling traffic so that voice traffic always receives its share of the link capacity under any (moderate or heavy) congestion conditions.

**Delay guarantees:** Bandwidth guarantees don't always ensure a proper delay or jitter guarantee. For example, satellite links may provide a bandwidth guarantee but will not meet the delay requirement for tight QoS-based services. So, applications such as voice trunking also require a delay guarantee.

**Jitter bounds:** Voice trunking applications require consistent and predictable network behavior. Network devices introduce jitter during traffic queuing and scheduling, regardless of how smooth the initial entry of traffic is. Providing low network jitter also reduces the requirement of large de-jitter buffers in the end nodes, resulting in smooth playback of voice at the receiving end.

For successful deployment, higher network availability and greater network resiliency must equal today's voice networks. Meeting these requirements provides a powerful alternative to circuit switching, at a fraction of the cost.

## Technology Components

Cisco IOS software delivers a powerful combination of industry-leading technology and features to build a voice trunking solution with the assumptions and characteristics described above. The following Cisco IOS MPLS features are the essential ingredients in building a profitable and highly robust voice trunking or toll-bypass trunking service.

### **Cisco MPLS Traffic Engineering (MPLS TE)**

Cisco MPLS TE automatically sets up Label Switched Paths (LSPs) that can assure, through appropriate aggregate QoS (across the LSPs), to meet the bandwidth, delay, and jitter constraints imposed by the toll-bypass or voice trunking application. Additionally, MPLS is the first step to set up these paths for carrying voice traffic in a diverse manner for better network utilization, over all throughput and resiliency in the network.



### **Cisco MPLS DiffServ-Aware Traffic Engineering (MPLS DS-TE)**

Traffic engineering treats all traffic in the same manner and does not differentiate among traffic types. To carry voice and data traffic on the same network, it may be necessary to separately account for the amount of voice traffic being transferred over the network to provide the necessarily stricter QoS guarantees. Cisco DS-TE not only allows the configuration of a global pool for bandwidth accounting, but also provides a restrictive subpool configuration for high-priority network traffic such as voice. Available bandwidth on the global pool and in the subpool are both advertised by IGP LSA or TLVs thus ensuring, each router tracks the available bandwidth when admitting new LSPs for voice or high priority traffic. In this manner service providers, depending on their service level agreement (SLA) requirements, can choose to overbook lower-priority classes or underbook higher-priority traffic to meet stringent QoS requirements. Obviously, they can charge a premium for that extra protection of voice traffic.

### **Cisco IOS QoS**

Cisco IOS software also provides a rich set of QoS features that are necessary to provide the minimum guarantees to TE tunnels. These mechanisms work with DS-TE to provide a point-to-point guarantee for each service class. At the network edge, traffic traveling into a tunnel is appropriately policed and colored. Coloring refers to marking the packets with the appropriate MPLS EXP bits. This color is then used in the core to identify the class to which the packet belongs. In the core, the Cisco Low-Latency Queuing (LLQ) scheme is deployed to ensure the minimum bandwidth for tunnels of a particular class. This allows a service provider to ensure strict priority and an assured amount of bandwidth for voice, while dividing the remaining bandwidth pie into slices, called Class-Based Weighted Fair Queuing (CBWFQ), for the other tunnels and data traffic.

### **Cisco MPLS Fast Reroute (MPLS FRR)**

Fast reroute is the ability to locally patch traffic onto a backup tunnel in case of a link or node failure with a failover time of 50 ms or lower, which is competitive with SONET APS (Automatic Protection Switching). Cisco FRR utilizes MPLS label stacking with RSVP signaling to create a backup tunnel around the link or node that needs protecting. On signal loss detection from the link, the MPLS FRR application in Cisco IOS software starts forwarding the traffic onto the backup tunnel transparent to end users or applications in 50 ms or less. Actual failover time may be greater or less than 50ms, depending on the hardware platform, the number of TE Tunnels and/or Network prefixes.

### **Cisco MPLS AutoBandwidth Allocator**

Cisco IOS software supports another first: An MPLS Traffic Engineering feature, called Cisco AutoBandwidth allocator, to ease constant monitoring and provisioning of the network. The AutoBandwidth feature constantly keeps track of average use of the MPLS Traffic Engineering tunnel. It can resize TE tunnel bandwidth to suite the traffic flow, efficiently utilizing the available network bandwidth and maximizing profits for service providers. The average duration of monitoring is configurable, providing better control of network resources.

### **Advantages**

By using Cisco's technology, MPLS guaranteed bandwidth services can be used to construct voice trunking and toll-bypass trunking applications, offering an alternative approach in the multi-billion dollar market for long-haul voice networking equipment.



Service providers benefit in the following ways:

Offering new premium services for high-priority traffic, such as voice traffic or online transaction processing with tight guarantees for throughput, delay, and more.

Increasing bandwidth utilization by load balancing traffic on alternate traffic engineered paths.

Achieving higher network availability by using Cisco MPLS FRR to use alternate traffic engineered paths quickly—in 50 ms or less (actual failover time may be greater or less than 50ms, depending on the hardware platform, the number of TE Tunnels and/or Network prefixes).

Simplifying network manageability and reducing costs with the Cisco MPLS AutoBandwidth allocator to take advantage of available tunnel bandwidth while providing guarantees for high-priority traffic.

Preventing service theft with policing. An important requirement for maintaining bandwidth guarantees is the ability to police traffic to check if the traffic is in profile. Service providers can do so using the policing feature in Cisco IOS software. Policing allows each user of a guaranteed bandwidth tunnel to gain a fair share of its allocated capacity. No overall degradation occurs due to heavy usage of one application/user, and theft of resources is avoided.

With Cisco IOS QoS, the following can help reduce and prevent service theft:

- Policing and traffic shaping (smoothing) at the network edge (customer edge or provider edge)
- Reexamining the markings and possible remarking
- Increasing the probability of packet drop when the network becomes congested because a customer is transmitting over a purchased “guaranteed”/assured bandwidth link. (specifically, use RED & WRED features)

Figure 2  
Toll Bypass with Voice Network

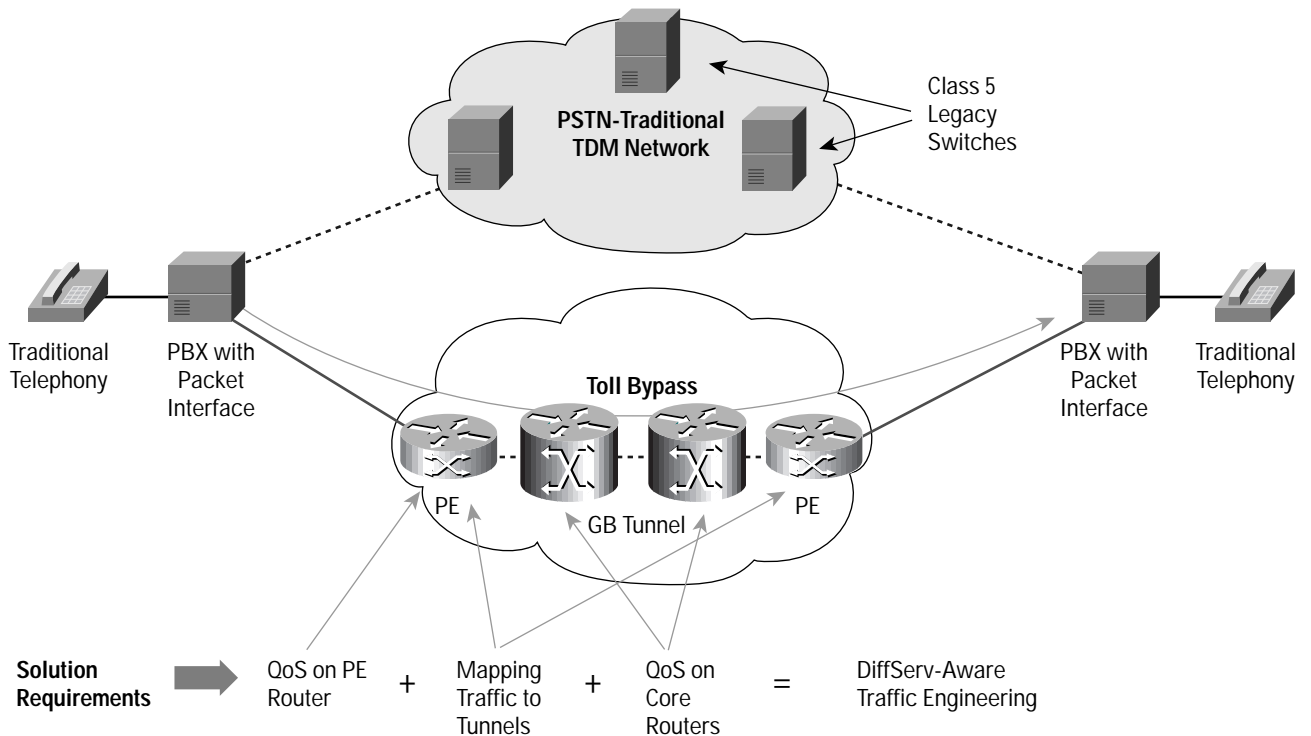




Figure 3  
Toll Bypass with Voice/Data Converged Network

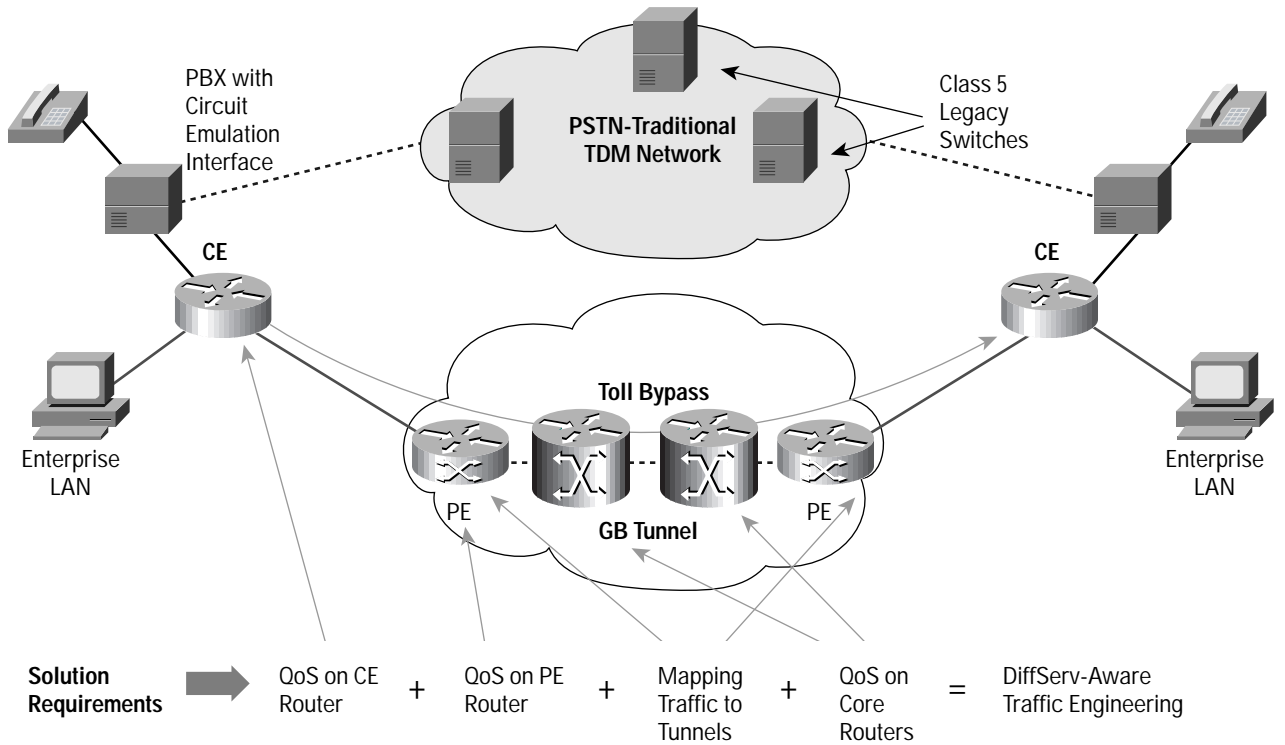
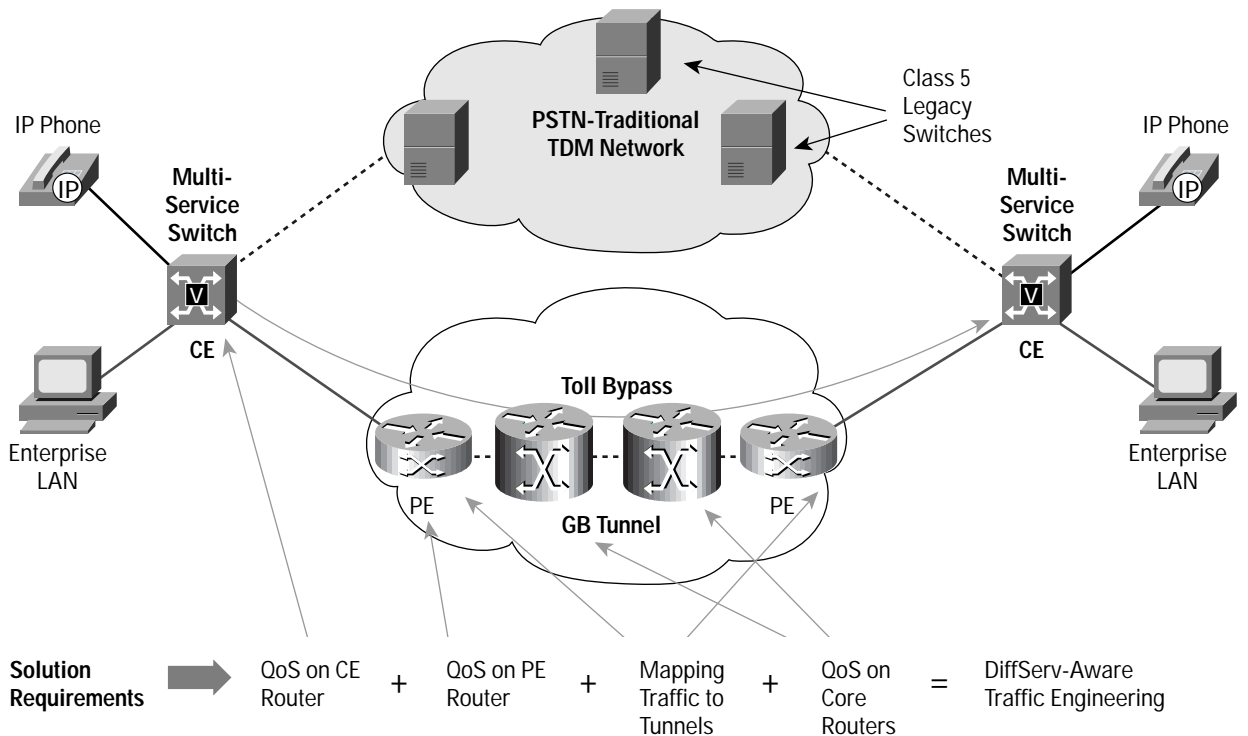


Figure 4  
Toll Bypass with VoIP Network



## For More Information

For more information about Cisco MPLS DS-TE, contact your  
Cisco account manager or global service manager.



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.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 317 7777  
Fax: +65 317 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 Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
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 © 1992–2002, Cisco Systems, Inc. All rights reserved. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.  
(0208R) xxxxxx/ETMG 9/02