

# Providing VoIP Long Distance Services Over a Shared Data Virtual Private Network



With the deregulation of the telecommunications industry, barriers to entry have been significantly reduced and competition from new market segments such as long distance, video and data services has increased dramatically. As competition between start-up providers and incumbent carriers intensifies, service providers of all types continue to seek ways to attract and keep new customers. Building IP networks that can support many new services now and in the future becomes imperative to the Service Provider's survival.

Enterprise customers face many challenges of their own. It is nearly impossible to keep up with the rapid technological advances required to maintain and grow a network, let alone provide the capital investments required. Balancing between sufficient IT staffing to maintain their network versus focusing resources on their core business competencies creates a strategic dilemma. To a growing number of businesses, the answer is to turn to a Service Provider for a managed virtual private network (VPN) for data and in increasing frequency, voice services as well.

The Cisco Multiservice over VPN 1.0 Reference Architecture, (available as of June, 2001 with Cisco IOS release 12.2(1a)) bridges the gap between the worlds of data and voice connectivity and provides one integrated solution deliverable via a single Service Provider. Service Providers will find value in this solution as the best method to attract and maintain new and existing customers. As Service Providers expand their networks they seek new ways to fully utilize the large infrastructure investments they have made. Data traffic alone is no longer enough to maximize their return on investments. With the addition of the Cisco Multiservice over VPN 1.0 Reference Architecture to existing infrastructures, New World Service Providers are able to increase the traffic on their networks—with voice traffic, data traffic, and the ability to add new IP-based applications. Service Providers can now differentiate themselves in the increasingly commoditized marketplace.



## Cisco Multiservice over VPN 1.0 Reference Architecture Features and Benefits

The Industry's First Class-4 PBX Interconnect Solution Fully-Tested for Carrier-Class Reliability

The Cisco Multiservice over VPN 1.0 Reference Architecture is the industry's first Class-4 private branch exchange (PBX) interconnect solution that allows Service Providers to offer their multi-site Enterprise customers a managed, packet-based VPN service for both voice and data. It is the first of a series of Cisco solutions which provides fully-tested Reference Architectures for robust and profitable integrated voice and data managed IP services. Service Providers and their Enterprise customers alike are ready to take advantage of cost savings and New World applications that a unified IP infrastructure provides. This existing functionality, along with the prospect of multiple revenue-generating and cost-saving IP services, are only possible through the convergence of voice and data infrastructures into a single IP network.

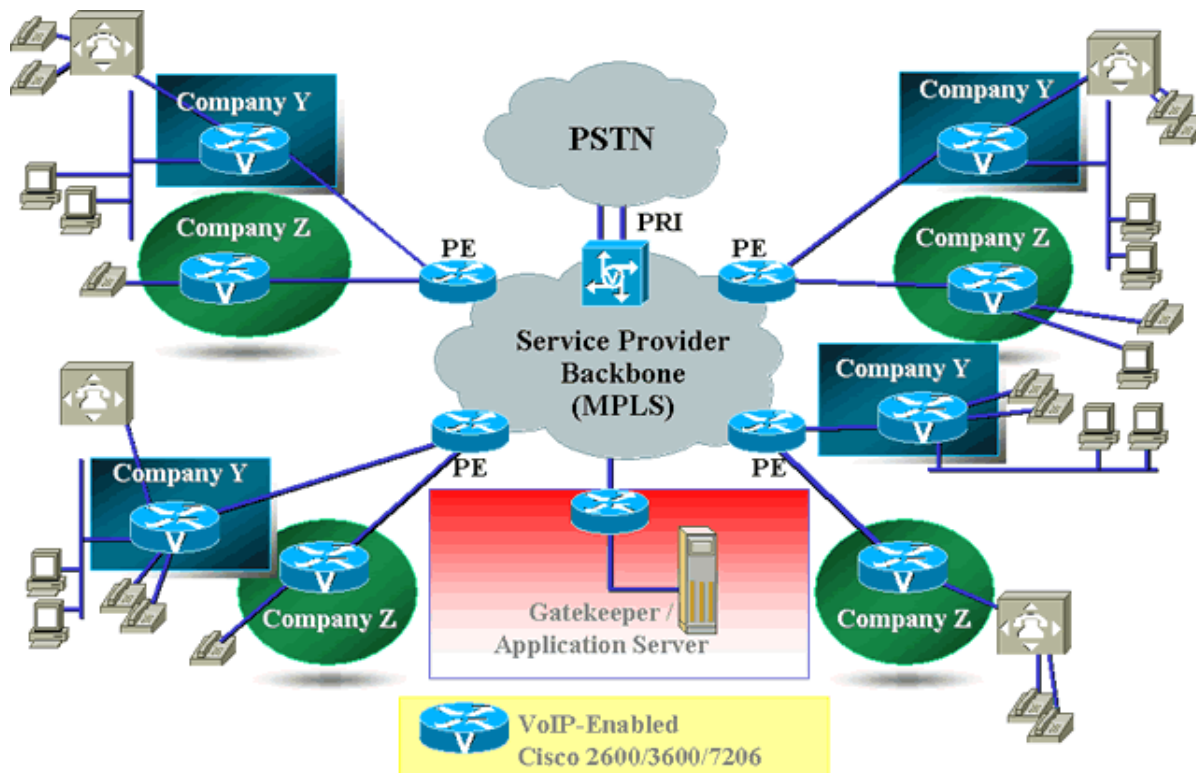
The Cisco Multiservice over VPN 1.0 Reference Architecture environment is H.323-based to leverage the most commonly deployed and feature-rich VoIP protocol available today. Features include on-net to on-net and on-net to off-net and off-net to on-net (via primary rate interface [PRI] to public switched telephone network [PSTN]), voice and fax connectivity, integrated voice response (IVR)-based calling card applications, multiprotocol label switching (MPLS) or backbones, least-cost routing functionality, and concurrent VPN data support. A third-party Cisco Ecosystem partner provides the VoIP VPN call control mechanism/gatekeeper to complete the Multiservice over VPN 1.0 Reference Architecture.

Supported customer premises equipment (CPE) include the Cisco 2600, Cisco 3600, and Cisco 7206 Series. The Cisco 5300 and/or the Cisco 3660 function as the trunking gateway for off-net interconnection.

Multiservice over VPN 1.0 Reference Architecture for Service Providers



Figure 1 Cisco Multiservice over VPN 1.0 Reference Architecture



#### Voice Overlay Provides Secure VoIP

One of the unique characteristics of the Cisco Multiservice over VPN 1.0 Reference Architecture is the voice overlay, which allows for overlapping dial plans on top of the data VPN infrastructure. Multiple Enterprise customers can now have the same short dialing patterns and co-exist on the same shared Service Provider backbone as if it were the Enterprise's own private network. The result is that the transition onto the network can be accomplished with little to no impact to the end-user's dialing plan, or existing legacy Enterprise equipment.

#### IntraNet Calling Delivers Secure, Cost-Reduced Site-to-Site Calling

The Cisco Multiservice over VPN 1.0 Reference Architecture includes a variety of call flows, supported on a per-customer basis. These call flows include On-Net to On-Net, On-Net to Off-Net and Off-Net to Off-Net.

#### On-Net to On-Net

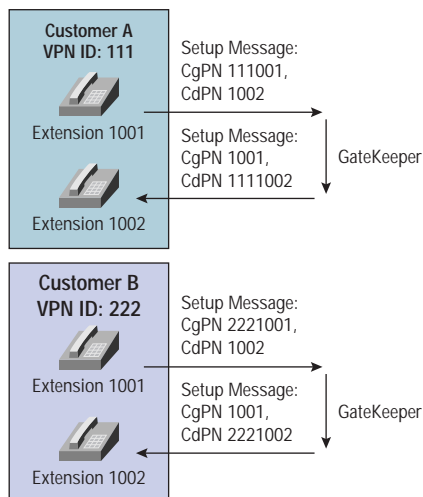
The most basic call flow is On-Net to On-Net as shown in Figure 2. This flow is the communication between two Enterprise branch offices over the shared network.

The Cisco Multiservice over VPN 1.0 Reference

Architecture allows for these calls to be placed through the customer PBX with short digit dialing (typically an escape digit + extension). To further expand on this function, it is quite typical that multiple Enterprise customers sharing the same Service Provider backbone will have identical extensions and short digit dialing plans. By leveraging the overlapping dial plan functionality of the solution gatekeeper, customers sharing similar dial plan schemes can reside on the same shared network, thus providing the same ease-of-use for voice that they experienced with legacy infrastructures.



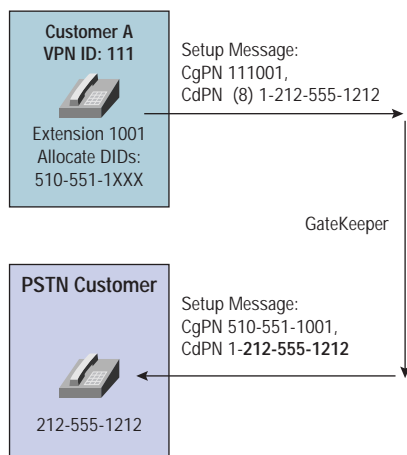
Figure 2 On-Net to On-Net Calls



### On-Net to Off-Net

The second most significant flow is the ability for On-Net users to place calls to Off-Net locations as shown in Figure 3. This functionality is accomplished via the use of a hop-off gateway, a Cisco AS5300 or Cisco 3660. The enterprise user will dial a special hop-off escape sequence triggering the gatekeeper to route the call to the PSTN. The gatekeeper routes the call to the appropriate hop-off gateway depending on the preference-based routing capabilities that have been configured.

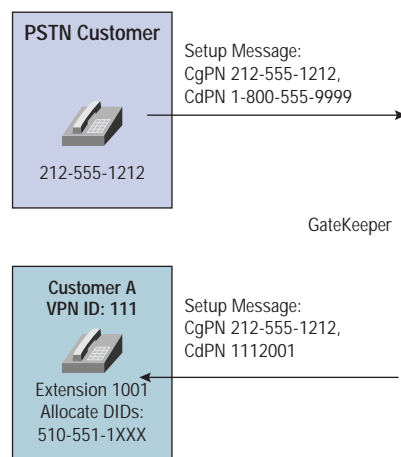
Figure 3 On-Net to Off-Net



### Off-Net to On-Net/Off-Net

The Cisco multiservice Over VPN 1.0 Reference Architecture enables the use of a hop-on gateway to accomplish the Off-Net to On-Net and Off-Net to Off-Net flows. In the basic Off-Net to On-Net flow, a customer sitting within the PSTN will dial the toll-free number of a local hop-on gateway. This gateway will perform authentication and collect the destination pattern for that VPN customer. If the customer is on the VPN, the gatekeeper can route the call to the correct site and thus completing the Off-Net to On-Net call. If, however, that number is another PSTN number, the gatekeeper has the flexibility of performing least-cost routing functions and terminating the call at a different hop-off gateway. This call will be billed back to the appropriate authenticated VPN customer. For an example of this flow refer to Figure 4.

Figure 4 Off-Net to On-Net/Off-Net



### Multiple Fax Protocols Supported for Multiservice Functionality

Although all of the above examples refer to PBX interconnection, it is important to note that the Cisco Multiservice over VPN 1.0 Reference Architecture also includes support for fax transmissions over this network as well. For Cisco 2600 and Cisco 3600 CPE, both Cisco Proprietary fax and T.38 fax are supported end-to-end. At the time testing was completed for phase 1.0, the Cisco 7206 does not have support for T.38 fax and therefore must rely on the Cisco Proprietary fax functionality.



### Least-Cost Routing Reduces Long Distance Calling Costs

Least-cost routing is available for call routing in the Cisco Multiservice over VPN 1.0 Reference Architecture.

Least-cost routing is the ability to place calls over the Service Provider backbone with the least possible cost to the Service Provider and thus to the end customer. This situation arises in several cases.

The first scenario is a VPN customer placing a call to an E.164 number that does not reside on the Service Provider backbone. The gatekeeper can use a predefined cost model to determine which of its hop-off gateways and/or hop-off partners will provide the best possible rates to this PSTN extension. Again, the Enterprise customer would see no difference in the call cost over any other call placed on the Service Provider backbone but the Service Provider would be able to control its own costs for terminating the call.

The second scenario is the Off-Net to Off-Net call. In this case, the Enterprise customer places a toll-free call to the closest hop-on gateway to the Service Provider's VPN backbone. After authentication, the user can dial their chosen E.164 number and traverse the Service Provider backbone to the final destination. This call would be billed by the Service Provider at the standard contractual rate but the VPN customer has acquired the advantage of not having the need to place a 100% PSTN routed long distance call. The advantages associated with least-cost routing can produce extra traffic for the Service Provider and simultaneously reduce costs to the Enterprise end customer.

### Time-of-Day Routing Gives Enterprises Control Over Call Routing and Destination

In addition to Least-Cost Routing via third party Gatekeeper, Time-Of-Day Routing will also be available within the Cisco Multiservice over VPN 1.0 Reference Architecture. Time-of-Day Routing is the ability to change the destination of the dialed number dependent on the time of day at which the call is placed. The basic example for this functionality is an internal support service for a large Enterprise customer. During the hours of 8:00am to 8:00pm PST, this Enterprise customer would like to route all calls to extension 5-5555 to their main facility thus substituting the dialed extension for a number at this facility. During the other twelve hours of

the day, these calls could be routed to the same company's alternate facility in for coverage. The advantage of Time-of-Day Routing is that it allows for automatic switchover of calls without user intervention based on the time of call setup.

### Applications Server Support Provides Endless Call Routing Solutions

There are virtually a limitless number of call routing options that a Service Provider can offer. When the gatekeeper has an attached application servers, the Service Provider can program their own functionality into the network for all routing applications. This could include functions such as near-end hop-off, far-end hop-off, call blocking based on number of calls to a specific location. All of this functionality can exist on top of the base infrastructure provided by the Cisco Multiservice over VPN 1.0 Reference Architecture.

### MPLS or IPsec: Cisco Multiservice over VPN 1.0 Reference Architecture Operates with Either IP-VPN Infrastructure

The foundation of the Cisco Multiservice over VPN 1.0 Reference Architecture is the VPN backbone. The Cisco Multiservice over VPN 1.0 Reference Architecture is compatible only on MPLS-based infrastructures. IPsec-based VPNs are being developed for a future phase.

When using MPLS, the architecture is structured such that no encryption of data will occur. The security of the data is ensured through the use of VRF tables within the provider edge (PE) routers. These VRF tables can be set up such that no other Service Provider customer on the backbone has access to the data/voice flow.

Future phases of Cisco Multiservice over VPN Reference Architecture will be compatible with IPsec-enabled Service Provider backbones. IPsec creates tunnels across the Service Provider backbone to provide secure encrypted data in the shared space. The security for voice on these backbones is still dependent upon the overlapping dialing support of the associated gatekeeper.

### Carrier-Class Network Management

A critical part of any solution deployment is the network management support. In the Cisco Multiservice over VPN 1.0 Reference Architecture, network management is achieved in several ways. The core VPN option is to use the Cisco VPN Solution Center 2.0, a carrier-class



management tool for either MPLS or IPSec-based VPNs. The Cisco VPN Solution Center provides provisioning, service auditing, accounting, and service-level agreement (SLA)/performance measurement to the Service Provider—all within the same solution. This eliminates the need for custom management interfaces. These custom systems, although still a possible solution, require the management platform to query and filter information from the individual routers' management information base (MIB) in order to collect the required information rather than the integrated solution provided with the Cisco VPN Solution Center.

Quality of Service (QoS) Allows the Service Provider to Prioritize Voice and Data Traffic Resulting in Higher Service Quality to the End Customer

The Cisco Multiservice over VPN 1.0 Reference Architecture has verified various QoS features and scenarios to help ensure our customers' success. There are three main sections to consider when evaluating these QoS issues including the Customer Edge (CE), Provider Edge, and the Service Providers' core network. In a converged IP network, QoS is essential because mission critical, time-sensitive applications such as voice need the appropriate level of prioritization throughout the network. Without implementing QoS, voice or any

time-sensitive traffic would be treated as any other data packet, thus resulting in reduced quality for time-sensitive traffic. Depending upon the network element being evaluated, the QoS mechanisms implemented will change. The first point in the network where the data and voice traffic will converge is at the CE. The CE requires the most significant attention to bandwidth utilization and prioritization due to the prevalence of lower speed links and bandwidth contention. Queuing mechanisms are therefore used for bandwidth allocation to the Service Provider's network. The most common technique implemented at the CE is policing combined with weighted random early detection (WRED) (with the DiffServ code point marking) used to control congestion toward the PE. On top of the congestion control mechanisms, LLQ will be deployed for the purpose of bandwidth assurance within the SLA traffic profiles.

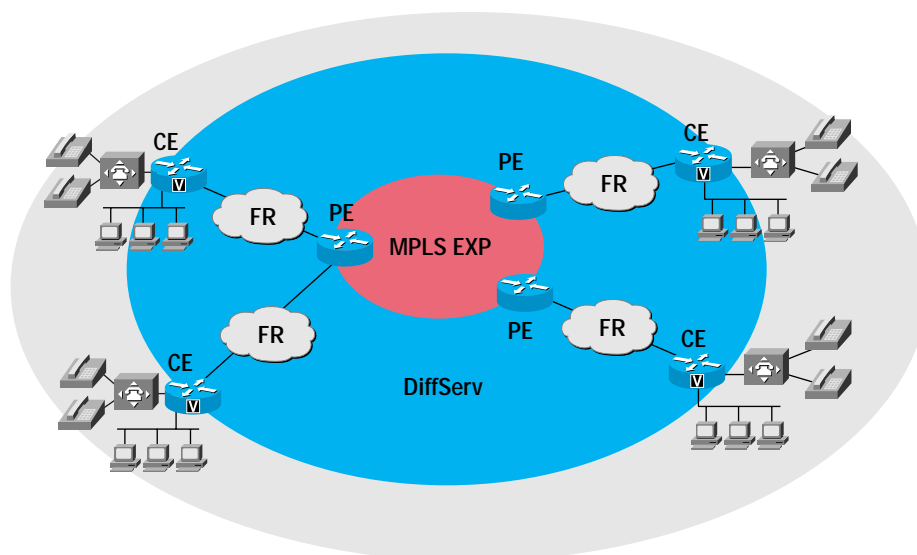
At the PE, the issues are quite similar. At the PE egress, facing the CE, it is important to pay great attention to the policing and prioritization of traffic over these slower links. At the Core egress, it is assumed there is sufficient bandwidth, therefore QoS will be less of an issue, and the primary function of the PE will be to appropriately transfer the DiffServ code points into MPLS Exp bits for

prioritization across the core. Note that after traversing the MPLS code the traffic flows will once again be policed to the SLA profile towards the CE from the PE to ensure that aggregate traffic from different CEs does not violate the profile.

The final component is the Service Provider core. In the Multiservice over VPN 1.0 Reference Architecture the assumption is made that the core is over-provisioned for the expected aggregate traffic flows from all included CE/PE combinations. The result of this assumption is that no Call Admission Control (CAC) mechanisms are deployed in the Core.



Figure 5 Multiservice over VPN 1.0 Reference Architecture QoS



Although the aforementioned QoS strategy is the primary technique deployed in the Multiservice over VPN 1.0 Reference Architecture, alternate strategies may be more appropriate depending on the specific customized networks.

Cisco Multiservice over VPN 1.0 Reference Architecture is the Service Provider's Path to Customer Acquisition and Retention. Due to increased competition and commoditization of services, Service Providers must look for new ways to add advanced services to their networks. By using the Cisco Multiservice over VPN 1.0 Reference Architecture, Service Providers can rapidly deploy voice VPN services on top of their existing data VPN service, or deploy an entirely new network to include new multiservice IP-based functionality.

With this new tested and validated architecture in place, the possibilities for enhanced services are unlimited. In an effort to retain customers, Service Providers can offer differentiated service in addition to their basic data services. These include, but are not limited to:

- Least Call-Routing functionality to further reduce the end customers' long distance charges.
- Video Applications

- LAN telephony
- Integration
- Content Delivery

With further innovation with the industry, the number of additional services that can be offered is growing rapidly. The Cisco Multiservice over VPN 1.0 Reference Architecture provides a validated architecture on which to build new IP-based services, and by which the Service Provider can attract and retain new customers.

Enterprises Can Focus on Core Competencies While Reducing Costs

End user Enterprise customers of today are looking for ways to reduce their costs and the Cisco Multiservice over VPN 1.0 Reference Architecture is an easy way to accomplish this goal. Historically, Enterprise customers have deployed their own solution to perform toll-bypass and used the time-division multiplexing (TDM) world for their voice services. This can change with the Cisco Multiservice over VPN 1.0 Reference Architecture. Enterprise customers can reduce the number of expensive IT professionals by outsourcing their WAN and long distance services to a single managed multiservice SP partner. Enterprise customers can be freed from the constant challenge of keeping up with new technological advances in the communications sector. The value of the



Cisco Multiservice over VPN 1.0 Reference Architecture to the Enterprise end user is that they can significantly reduce their cost of ownership for voice and data services. Meanwhile the Enterprise can remain on the cutting-edge of technological advances by leveraging the Service Provider for setting up, maintaining and enhancing their voice and data service.

#### The Cisco Multiservice VPN Solution Components

The Cisco Multiservice over VPN 1.0 Reference Architecture utilizes the Cisco 2600, Cisco 3600, and Cisco 7206 Series routers for the Customer Premise Equipment, (only Frame Relay access links were validated for phase 1.0 of the Reference Architecture) the Cisco AS5300 and/or the Cisco 3660 for trunking gateway support and the Cisco 7200 and Cisco 7500 series routers as Provider Edge Equipment. This combination of products form the Cisco portfolio provides a robust and flexible solution for Service Providers' Multiservice over VPN 1.0 Reference Architecture needs.

#### Cisco 2600 Multiservice Router



The Cisco 2600 modular multiservice routers offer versatility, integration, and power to branch offices. With over 80 network modules and interfaces, the modular architecture of the Cisco 2600 Series easily allows interfaces to be upgraded to accommodate network expansion. The Cisco 2600 family is available in three performance levels and six base configurations: Cisco 2650 and Cisco 2651, Cisco 2620 and Cisco 2621, and Cisco 2610 through 2613.

Branch office networking requirements are dramatically evolving, driven by Web and e-commerce applications to enhance productivity and converging the voice and data infrastructure to reduce costs. In order to continue the

multiservice, content networking, VPN and bandwidth build-out, the Cisco 2600 Series delivers up to ten times the performance and capabilities of traditional small/medium branch office platforms.

The Cisco 2600 Series is a key member of the Cisco data/voice/video integration portfolio, delivering the industry's broadest range of end-to-end IP and Frame Relay-based packet telephony solutions.

The Cisco 2600 Series shares modular interfaces with the Cisco 1600, Cisco 1700, and Cisco 3600 Series, providing network managers and service providers a cost-effective solution to meet today's branch office needs such as:

- Internet/intranet access with Firewall security
- Multiservice voice/data integration
- Analog and digital dial access services
- VPN access
- Inter-VLAN routing
- Routing with Bandwidth Management

#### Cisco 3600 Multiservice Router



The Cisco 3600 Series is a family of modular, multiservice access platforms for medium and large-sized offices and smaller Internet Service Providers. With over 90 modular interface options, the Cisco 3600 family provides solutions for data, voice video, hybrid dial access, VPNs, and multi-protocol data routing. The high-performance, modular architecture protects customers' investment in network technology and integrates the functions of several devices into a single, manageable solution.

Cisco extended the successful Cisco 3600 Series with the Cisco 3660 multiservice access platform. The Cisco 3660 provides higher densities, greater performance, and more

expansion capabilities. The additional power and performance of the Cisco 3660 platform enables new applications, such as packetized voice aggregation and branch office ATM access ranging from T1/E1 IMA to OC-3.

The Cisco 2600 and Cisco 3600 Series of multiservice platforms has been greatly enhanced with many voice capabilities: added support for Voice over Frame Relay (VoFR) and Voice over ATM (VoATM-AALS) on the digital voice interfaces (T1 and E1). QSIG is also supported on all digital interfaces, including T1/E1 and basic rate interface (BRI). Other enhancements include Off Premise Extension (OPX), VoFR, and enhanced queuing functionality. In addition, a feature that works with Call Manager software makes these products perfect gateways for the PBX and PSTN for IP telephony, enabling applications like call transfers, holds, and conferencing.

Cisco 5300 Multiservice Routers



The award-winning Cisco AS5300 Universal Access server provides superior density, price, and performance. Utilizing the differentiated services delivered through Cisco IOS®, customers are offered best-of-breed scalability and investment protection via the broadest support of worldwide protocols such as Channelized E1 (R2), Channelized T1 (RBS), SS7, and VoIP.

Frequently, geographic concerns require a service provider to employ a large number of small Points of Presence (POPs) that are geographically dispersed in addition to the traditional large centralized POP. The high density 8 PRI AS5300, with its compact and cost effective design is the optimal choice for implementation in a dispersed or centralized dial infrastructure. With its four redundant high speed serial WAN ports and two redundant LAN interfaces, the Cisco AS5300 provides the maximum flexibility of deployment. Customers can utilize the serial ports for backhaul in a distributed

environment, thus removing the need for aggregation switches and routers. For a large centralized POP environment, the Cisco AS5300's Fast Ethernet LAN interface provides a high-speed data path for integration with other access servers.

A common application for the Cisco AS5300 is VoIP toll bypass. Corporations can now leverage their WAN infrastructure to provide long distance toll-bypass services. Using the Cisco AS5300 as the aggregation point, along with voice/fax network modules for the Cisco 3600 and Cisco 2600 routers, companies can significantly reduce their long distance telephone and fax charges by routing their intracompany voice and fax traffic over their existing IP networks, without compromising voice or fax quality.

In addition, by avoiding the need for expensive telephony switches, ISP's can offer long distance service to their subscribers at a fraction of traditional long distance rates while further utilizing their existing data networks. This allows ISP's to grow their business from plain dial access to multiservice access for subscribers and corporate outsource customers.

## Cisco 7200 Multiservice Router



The Cisco 7200 provides exceptional performance/price, density and availability. It also introduces industry-leading serviceability and manageability features. By leveraging the modularity of the Cisco 7200, customers have scalable solutions based on differing requirements for density, performance, and availability.

Benefits of the Cisco 7200 Series routers include:

- Accelerated services using PXF technology
- Flexible Modular Interfaces including OC-3, DS-3, Fast Ethernet and Gigabit Ethernet, Packet Over Sonet and more
- IP and ATM QoS/CoS
- Modular design and small 3U footprint
- MPLS VPN and Full L2TP Support
- Feature Rich IP services and PPP termination support

- Multiservice features support

## Cisco 7500 Multiservice Routers



The high-performance Cisco 7500 Series routers remain the market leader due to its breadth of advanced support for LAN/WAN services, redundancy, reliability, and performance.

A distributed architecture using Versatile Interface Processors (VIPs) is the key to the Cisco 7500's scalability. Each VIP has its own processor, which is capable of switching IP data packets and providing network services. This scenario allows the overall system performance of Cisco 7500 routers to scale up when they need to handle more high-speed network connections and more data packets. The RSP is still the master of the system. It runs routing protocols with other routers in the network to gather switching intelligence, which is then downloaded to the VIPs so that each can switch IP packets on its own.



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 Europe  
11, Rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9

France  
www.cisco.com  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

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 Australia, Pty., Ltd  
Level 9, 80 Pacific Highway  
P.O. Box 469  
North Sydney

NSW 2060 Australia  
www.cisco.com  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

**Cisco.com 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

All contents are Copyright © 1992-2001 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement. Printed in the USA. Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or 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. (0101R)

05/01 BW7270

In addition to performing packet switching, the VIPs can also provide a set of distributed IP network services, including access control, QoS, and traffic accounting (NetFlow). With the VIPs off-loading these IP switching and service functions from the RSP, the RSP can devote all its CPU cycles to handle other essential tasks. VIP distributed switching is the way to scale up system performance, and should be enabled where possible, to significantly reduce CPU utilization on the RSP.