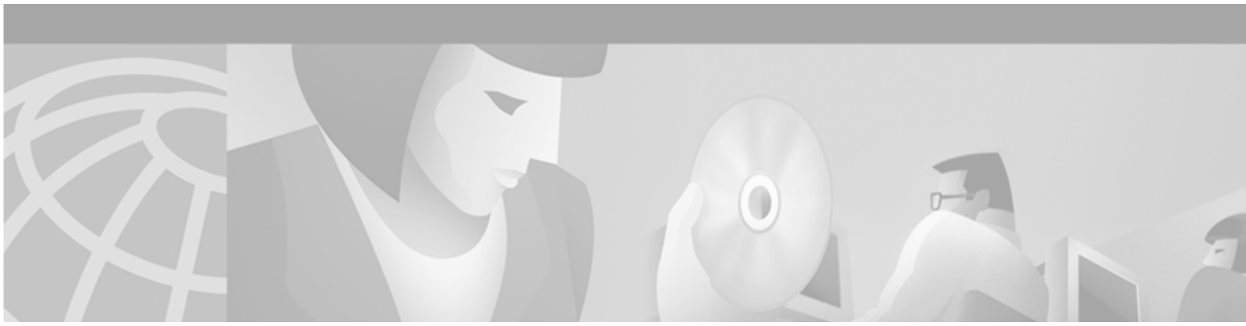


Managed Multiservice Networks and Packet Voice VPNs

Version Number	Date	Notes
1	7/20/2001	This document was created.

Managed Mutliservice (MMS) networks are enterprise networks that are owned and operated by service providers (SPs). The SPs then contract with enterprise customers that require voice and data services but do not want to maintain their own WAN and customer premises equipment (CPE). Instead, the enterprise customers use the SP WAN as a virtual WAN. MMS networks enable SPs to offer inexpensive voice and data services to their enterprise customers, which can then focus on their core business responsibilities.

This document discusses two classes of hosted voice networks:

- Peer-to-peer MMS networks
- Packet voice virtual private networks (PV-VPNs)

MMS networks are VoIP, VoFR, or VoATM networks that are intended for enterprise customers that want dependable, inexpensive voice service between two or more sites. A virtual private network (VPN) is an MMS with more advanced features and functionality. We will discuss the differences between the two types of networks in this document.

Note Packet voice VPNs should not be confused with traditional data VPNs. Although both types of VPN enable enterprise customers to outsource their information technology (IT) responsibilities to SPs, data VPNs use technologies such as Multiprotocol Layer Switching (MPLS), Layer 2 tunneling (L2F, L2TP, PPTP), and encryption (IPSec and MPPE) to enable geographically dispersed sites to communicate securely over a shared backbone.

Packet voice VPNs are MMS networks that include devices such as gatekeepers and route servers. These devices provide additional network intelligence and support advanced voice features such as overlapping dial plans, digit manipulation, priority routing, load balancing, and multiple-stage dialing.

SPs can offer Packet voice VPN services in conjunction with or independent of a data VPN.

In this document we will explain how MMS and packet voice VPN solutions can be designed, the features and elements of the solution, and how to configure a packet voice VPN.

This document focuses only on the voice functionality of an H.323 MMS network service offering. ATM AAL5-based and AAL2-based MMS solutions will not be covered here. In addition, data managed services and data VPNs that are assumed to be a necessary precursor to an MMS are not explicitly discussed.

This document contains the following sections:

- Managed Multiservice Networks, page 2
- Peer-to-Peer MMS Networks, page 3
- Packet Voice VPNs, page 8

Managed Multiservice Networks

A managed multiservice network is essentially an enterprise network that is *hosted* by an SP on its shared backbone. The customer premises equipment (CPE) and features are the same as the enterprise would use to create its own network, but instead they are managed and sometimes owned by the SP. Instead of maintaining its own WAN, the enterprise uses the SP backbone, which is shared by many different enterprises, as a virtual WAN.

A managed multiservice network has the same configuration, features, and performance issues as any enterprise network. Additionally, security, billing, network management, compliance with service level agreements (SLAs) including traffic policing and shaping, and voice quality issues must be considered.

A managed multiservice network has the following characteristics:

- Combined services. In addition to managing data traffic between multiple sites for the enterprise customer, an overall solution managed and deployed by the SP includes voice services.
- Tandem/Class 4 replacement. SPs offer business connect services that replace those that would ordinarily connect an enterprise telephony equipment to the IXC Class 4 switch.
- Not a local services solution. MMS solutions do not support the features required to address the residential market (Class 5).

Evolution of Managed Voice Networks

Managed voice networks began with the advent of circuit-switched telephone solutions. Following are a few of the significant developments that have occurred:

- Mid-1980s—Sprint USA implemented a time-division multiplexing (TDM) voice VPN to compete against AT&T private line PBX networks.
- Early 1990s—U.S. long distance companies such as AT&T, and several international companies such as SITA-Equant, started providing managed router services over FrameRelay.
- Early 1990s—50 international carriers ratified the circuit switched voice VPN as an international standard.

Today, SPs like AT&T and MCI offer feature-rich, worldwide voice VPN services to enterprises.

The following pressures are driving the industry toward packet-based solutions:

- Competitive pressure to duplicate existing circuit-switched services on packet networks.

- Desire to provide advanced, revenue-generating services that can be deployed only over packet-based networks.
- New entrants want to complement existing packet-based voice services with voice VPNs.
- Mobile carriers want to interconnect mobile and PBX networks with voice VPNs.

Now that data VPNs have matured and become commoditized, enterprises can switch relatively easily between different SP offerings, which are often competitively priced. By adding voice and other value-added services to their existing data managed service offerings, SPs can maintain a competitive edge with differentiated services.

MMS Solution Market Drivers

The following factors were the original market drivers for MMS networks:

- To leverage the convergence of data and voice over packet networks, the traditional data providers needed to upgrade their offerings to be multiservice.
- To increase revenue, SPs wanted to attract more traffic onto their packet backbone.

However, as we will see, just transporting voice traffic is no longer a cutting edge service. The industry is moving toward value-added services and applications leveraging a combined infrastructure, particularly packet voice VPNs. The factors driving this market include the following:

- As competitive pressures force enterprise customers to focus on their own business plans, the customers are increasingly turning to SPs for network outsourcing.
- Enterprise customers are comfortable with VPNs, because both voice VPN (circuit-switched) and data VPN services are mature technologies.
- VPNs offer cost-effective communication with remote offices and business partners.
- For large, multisite enterprises, internal voice traffic typically is greater than external traffic.

The following enterprise customers are ideally suited for MMS network solutions:

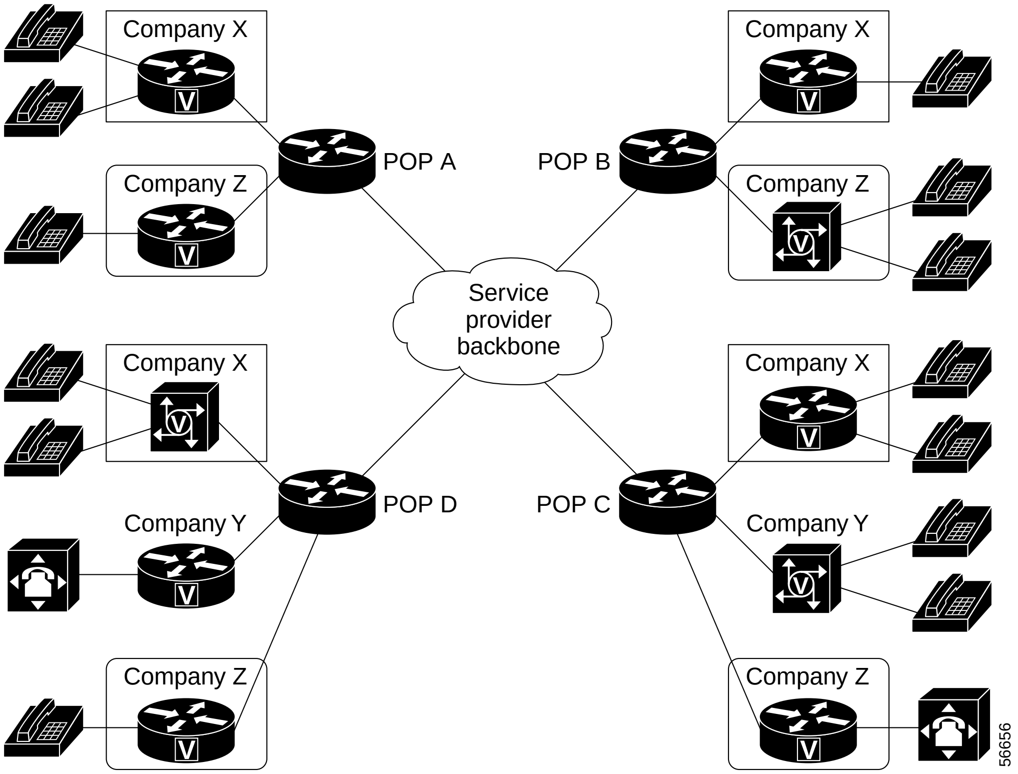
- Larger enterprise customers that want to interconnect multiple sites (a more important goal than Internet access or e-business connectivity, although these are often secondary goals).
- Customers with the need to integrate existing dial plans, PBXs, and key systems.
- Customers that would prefer to outsource management of their WAN.
- Customers that need to improve the efficiency and reduce the overall cost of their networks.

Specifically, retail and financial enterprises have benefited from MMS networks.

Peer-to-Peer MMS Networks

A peer-to-peer MMS network is a network that has the same architecture used by the older data-only networks, as shown in Figure 1. Each customer has data and voice traffic coming in from edge CPE devices resident at their various sites.

Figure 1 Peer-to-Peer MMS Network Architecture



This architecture is primarily designed for customers outsourcing their enterprise WANs. Note that the traffic on the network is from one Company X location to another Company X location. A peer-to-peer MMS network is not as well suited to SP value-added services (such as voice VPNs or Unified Messaging services) offered on common or shared equipment accessed by multiple end customers. In contrast, there is additional secure traffic on a voice VPN between different customers, and traffic from customers to shared servers that provide services such as Unified Messaging or web applications.

Peer-to-Peer MMS Network Elements

A peer-to-peer MMS network has a relatively simple architecture consisting of the following components:

- CPE routers

  These routers are typically Cisco 2600 series routers, 3600 series routers , or MC3810 concentrators. The customer's data traffic enters the SP network through this router, which is typically connected by an Ethernet or Token Ring LAN on the customer side, and a Frame Relay, ATM, or IP connection on the SP side.

  The customer PBX, phone sets, and key system are also connected to this router and are responsible for originating and terminating the voice traffic. Earlier incarnations of MMS networks frequently used Voice over Frame Relay (VoFR) and Voice over ATM (VoATM) technologies. Many carriers that currently offer VoFR or VoATM solutions are now planning or considering VoIP-based services, either to replace or augment their existing services.

A variation on CPE voice traffic that is also under consideration is IP telephony. In this architecture, the CPE router does not originate or terminate the voice, but IP phones, softphones, and other H.323 endpoints originate and terminate VoIP traffic and the CPE router only aggregates and routes the traffic destined for the SP backbone. There are more challenges with this design (billing, security, call admission control, and so on) than with traditional telephony equipment connecting via the CPE router (which also acts as the voice gateway).

- SP POPs

  These are geographically dispersed aggregation points of CPE traffic that typically use Frame Relay or ATM connectivity.

- SP backbone

  The backbone carries traffic between the POPs, usually using an ATM-based, high-speed network (FrameRelay is more often used as a CPE access technology).

- Network management

  The premise of an MMS network is that it can be managed. SPs run elaborate Network Operations Centers (NOCs) where the status of the network is monitored and alarms are raised when outages occur. SPs can use Cisco management platforms such as CiscoWorks and Cisco WAN Manager, or they can write their own applications and use various products as elements in their network management scheme.

  There is also a Network Management overlay network, typically using a separate PVC to the CPE equipment, and separate IP addressing, to carry SNMP and remote-access traffic to allow the SP to gather the information necessary to manage the network.

- Billing

  This function is key to the ability of the SP to charge accurately for services rendered. Peer-to-peer MMS networks tend to use a relatively simple, flat-rate basis for billing, such as CPE access bandwidth or CIR.

Peer-to-Peer MMS Network Features and Characteristics

Peer-to-peer MMS networks are relatively simple and straightforward. They do not include call agents, gatekeepers, or any other type of server-based call control or call assistance. Because of this lack of high-level network intelligence, these networks typically have the following voice characteristics:

- On-net to on-net calls only between sites belonging to the same customer.
- No on-net to on-net calls between different customers.
- On-net to off-net traffic possible (although not typical, because of IP security risks).
- No off-net to on-net traffic (DID/DDI functionality).
- Relatively small number of customer sites (10 to 20 maximum) because the flat dial peer architecture does not scale well.
- One customer per gateway. Peer-to-peer MMS networks cannot support multitenant gateways shared among multiple customers—for example, a Cisco 3660 gateway in a building with different customers on different floors of the building.

Peer-to-peer MMS networks have been in operation for several years and were the first networks to be deployed with combined data and voice services. However, advanced call features, such as those discussed in more detail later in this document, are typically not yet offered. The primary purpose of these networks is to make and receive on-net calls across a shared packet backbone between sites belonging to the same customer. Advanced call features such as contact centers, on-net and off-net routing of calls, digit manipulation, VPN services, and time-of-day routing require more intelligence in the network than peer-to-peer dial plans allow.

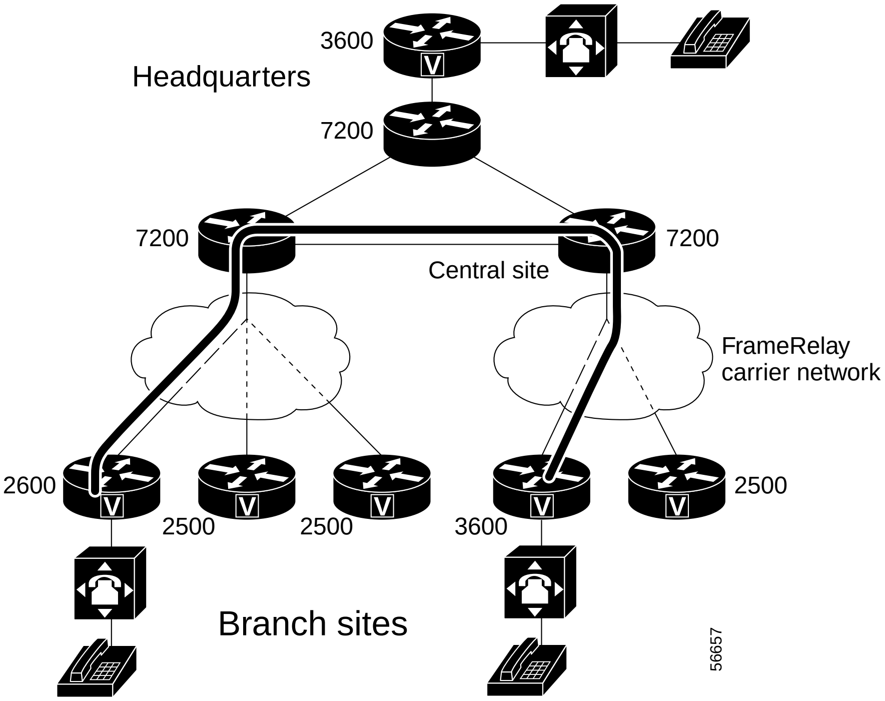
Peer-to-Peer MMS Network Customer Dialing Plans

The voice dial plan for a peer-to-peer MMS network is created as a flat direct dial-peer architecture, where every Company X site has a dial peer pointing to every other Company X site. Calls between Company X and Company Y are not possible by way of the packet network because no dial peers are entered for such calls.

In H.323 VoIP-based peer-to-peer MMS networks, the dial peers for each customer are fully meshed between the customer sites, precluding scalability to a large number of sites. In VoFR and VoATM-based networks, the tandem switching function provides a certain measure of centralization of some of the dial plan in the POPs or aggregation points in the network, simplifying the CPE configuration and easing the deployment of slightly larger networks.

Customer dial-plans in peer-to-peer networks *can* overlap—Company X has an extension 2211, as does Company Y—but often do not. Overlapping dial plans can be supported because there visibility or connectivity is between the voice networks of Company X and Company Y. An exception to this, shown in Figure 2, is the VoFR/VoATM tandem switching functionality in the SP network, which either precludes overlapping dial plans or forces the tandeming to be performed by a device dedicated to a particular customer. For example, all of the branch office CPE equipment of Company X could tandem the VoFR/VoATM calls through a Cisco 7200 CPE device at the headquarters of Company X or a large site location. SPs that have deployed VoFR tandeming have typically opted to not support overlapping dial plans and perform digit manipulation at the CPE to make the dial plan unique.

Figure 2 VoFR Tandem Switching



In summary, peer-to-peer dial plans tend to have the following characteristics:

- Fully meshed between sites belonging to a particular customer
- On-net to on-net calling only—within the same customer
- Nonoverlapping—each site, regardless of customer, has a unique phone number or range prescribed by the SP rather than fitting in with the custom dialing plan that the company may already have impleneted on its PBX.

Peer-to-Peer MMS Network Call Routing Characteristics

In peer-to-peer MMS networks, call routing is determined exclusively through the flat dial-peer plan configured on the CPE gateways, and through the IP routes they use. There are no database lookups, network-based address translation, call servers or any other intelligence in the network to aid with call setup, routing, admission decisions, or billing information.

On-Net to On-Net Calls

Calls between sites belonging to the same customer are fully supported. Calls between sites belonging to different customers are typically not supported. These calls must be placed by using the PSTN. Because of the flat dial plan, this functionality would require visibility of Company X’s IP addressing from Company Y’s network, which is insecure.

It is technically possible to implement intercustomer calling by making all voice calls from all customers share the same IP addressing plane—separate from the per-customer data IP addressing space. Yet there is still risk because currently there is no control point, such as a gatekeeper, to authenticate calls between different customers. If the H.323 voice traffic originates on the CPE voice gateway, the security concern is negligible. But if the traffic originates on the LAN segment behind the CPE router the IP addresses of the destinations are visible to end users, which is insecure.

On-Net to Off-Net Calls

It is technically possible to support calls from customer locations to PSTN destinations by using common, SP-owned PSTN gateways, but typically this functionality is not offered. Each customer gateways would have a dial peer pointing PSTN destination patterns to this shared PSTN-entry gateway, called a hopoff. Because this gateway destination IP address is visible to all end customers networks, there is also a security risk.

Off-Net to On-Net Calls

Off-net to on-net DID calls—calls from the PSTN to a customer location—are typically not supported. These calls usually terminate through existing PSTN connections to the customer PBX. Although such calls can be supported, they cause complexities in routing and dial plans.

Peer-to-Peer MMS Network Billing Features

First generation peer-to-peer MMS networks are typically billed at a flat rate. For data service, the customer pays for a given amount of bandwidth on the SP network access link. For voice connectivity, the customer usually pays for a certain maximum number of allowed simultaneous calls. The actual use of network bandwidth for voice calls is monitored by the SP, butis not charged.

As peer-to-peer MMS networks evolve toward value-added services such as Unified Messaging and voice VPNs, where off-net calling should be charged only for actual calls made, usage-based billing models become much more important. For voice traffic, usage-based billing means call detail recording (CDR) information collected from the network with details and accurate information on the parameters of the call.

Peer-to-Peer MMS Network Configuration

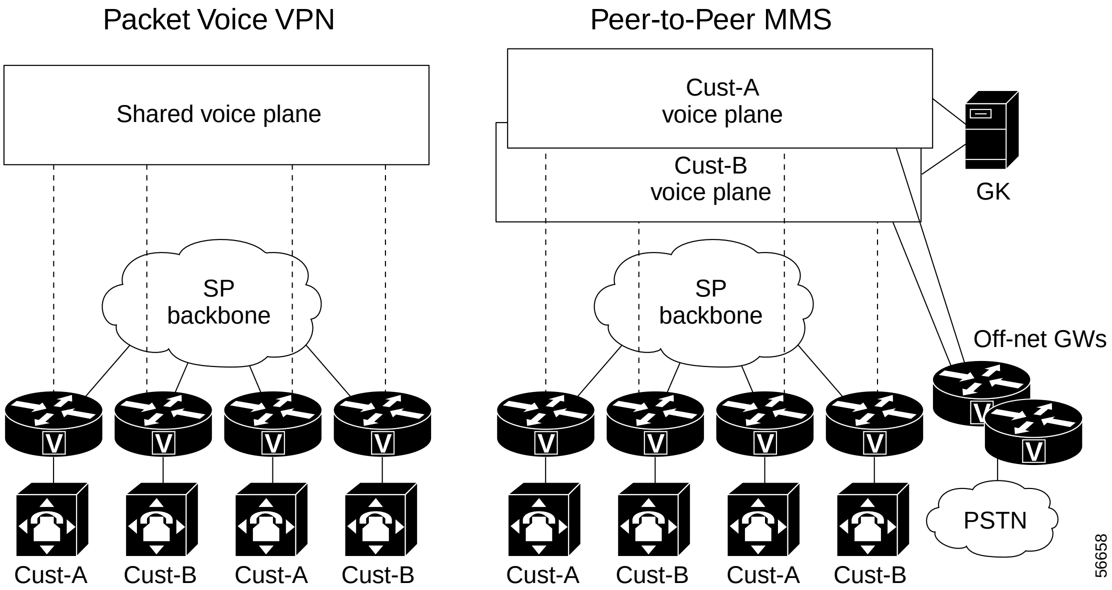
Peer-to-peer MMS networks are relatively easy to configure because they do not have gatekeepers. To configure a peer-to-peer MMS network, configure your gateways for standard VoIP.

Packet Voice VPNs

Packet voice VPNs are voice networks with a packet-based backbone that offer end-user features similar to traditional circuit-switched voice VPNs. These voice features may be offered by an SP entirely independent of data VPN offerings such as MPLS, IPSec, and other tunneling and security technologies.

Figure 3 illustrates the difference between a peer-to-peer MMS voice network and a packet voice VPN where each customer has a separate voice network customized to the individual company needs.

Figure 3 Peer-to-peer voice MMS versus a packet voice VPN



The key differences between the two voice architectures are described in Table 1.

Table 1 Differences between peer-to-peer MMS Networks and PV-VPNs

Peer-to-Peer MMS Voice Networks	PV-VPNs
Shared dial plan	Custom dial plan per customer
Typically no gatekeepers or servers	Gatekeepers, call routing servers, and call agents

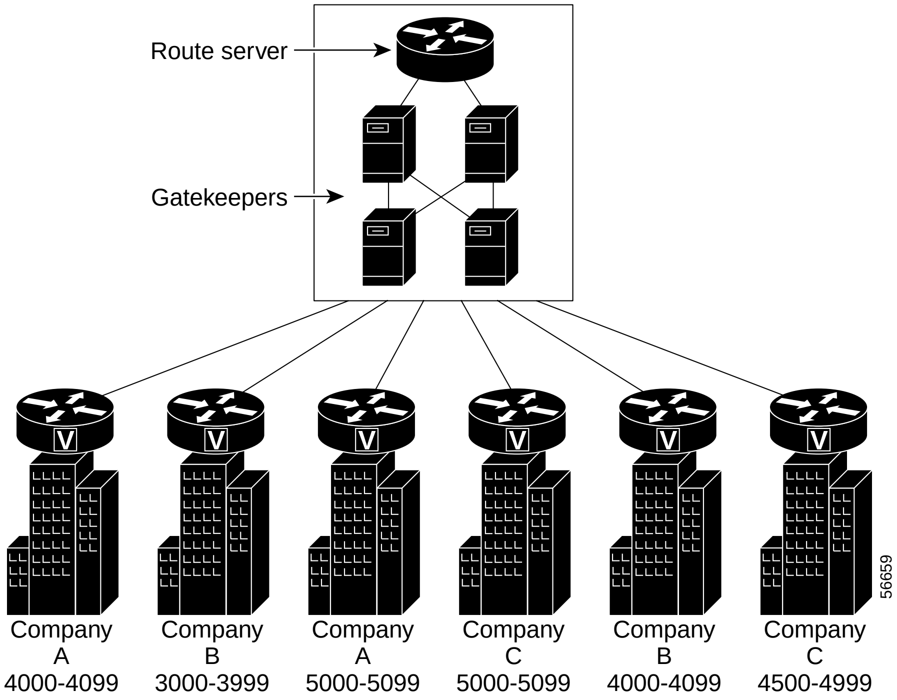
Table 1 Differences between peer-to-peer MMS Networks and PV-VPNs

Peer-to-Peer MMS Voice Networks	PV-VPNs
Point-to-point “pipes” between customer sites	Switched calls between any endpoints
Primarily on-net calling only	On-net and off-net calling, and any combination of these
CPE is the voice gateway	Voice source can be the CPE, or a voice gateway behind the CPE, or LAN-based voice deviced
Basic calling	Feature-rich calling

Packet Voice VPN Architecture

A packet voice VPN has the same elements as a peer-to-peer MMS network, with the addition of gatekeepers and route servers to add intelligence to the network for the purpose of controlling call routing and authentication. PV-VPNs can also include several other application servers to offer various additional features and applications. This equipment can be either physically centralized or dispersed. The servers provide services to the network and can be connected at any point where it makes logistical and geographical sense. Figure 4 gives a high-level view of a VPN.

Figure 4 PV-VPN Architecture



The architecture is designed to offer advanced voice features in addition to simple outsourcing of an enterprise WAN. It is scalable and extendable, and provides the basis for value-added applications such as Unified Messaging and call center outsourcing.

VPN Elements

A VPN has all the elements of a peer-to-peer MMS network to provide for the core infrastructure of the network. In addition, it includes the following elements:

- Advanced call servers and services

  Many potential pieces of equipment are in this category, and the number of these devices you deploy in your solution will depend on the features and applications offered in the VPN. Any or all of these servers can accomplish digit manipulation functions. The different types of servers include the following:

  - Gatekeepers, which are used both in the infrastructure of the network to improve dial plan scalability, and in applications that implement call routing to specific destinations such as a shared database or applications built on an API into the gatekeeper.
  - Call agents. These appear in MGCP-based networks and implement the core call control logic, which is centralized in an MGCP architecture rather than distributed as in an H.323 architecture.
  - Call route servers. These work in conjunction with a gatekeeper to control call routing decisions such as least-cost routing and time-of-day routing. You can implement a call route server as a database access by the gatekeeper, or as a peer application communicating with the gatekeeper.
  - Proxies. These are deployed for reasons such as security (to hide IP addresses), scalability (to hide the complexity of the rest of the network), and feature invocation (to invoke QoS features on behalf of an end-station that is not capable of QoS).
  - Specialized application servers. These include Unified Messaging, call center applications, customized announcement servers, IVR applications, speech recognition servers, and Follow-Me applications.

- OSP connectivity (optional)

  An off-net call termination capability includes at least interconnectivity with the traditional PSTN. To offer lower-cost alternatives to off-net destinations not served directly by the SP POPs, the SP may use an OSP clearing house to hand off calls to other low-cost, packet-based carriers to lessen the traditional long-distance PSTN charges of off-net calls.

- Enhanced billing services

  Billing systems for VPNs are more complex than those for peer-to-peer MMS network offerings, because per-usage-based billing is an important value-added VPN feature. Consolidated billing for off-net and business-to-business on-net calls is also necessary for VPNs.

Packet Voice VPN Characteristics and Features

Simple packet voice VPNs can be implemented today using Cisco and NetSpeak gatekeepers and NetSpeak route servers. Cisco and its partner vendors are still developing more advanced features.

Currently, SP packet voice VPN networks include one or more of the following features:

- Intrabusiness on-net calling (on-net to on-net calls, same customer). This functionality includes the following features to connect the different sites belonging to the same customer:

  - Private dialing plan—Private or custom number plan for intracompany voice and fax. Dialing plans can overlap; therefore, customers can keep the dialing plan already implemented on their PBX private network, and can have the same numbers as other customers.

  - On-net calling—Inter-PBX extension calls using the private dialing plan.
  - Virtual On-net—Expands VPN coverage of the dial plan to sites not connected to the packet network. An on-net number is assigned to the off-site location, and when this number is dialed, the network connects the call to the PSTN number. To the end user, the number appears to be for an on-net location.
  - Private network interface—The physical connection (such as E1 PRI, T1 CAS) between the PBX and the VPN CPE.
  - Forced on-net—If an off-site, PSTN number is dialed to an on-net location, the servers in the network convert this to an on-net call.
- Interbusiness on-net calling (on-net to on-net calls, different customers). This functionality includes various value-added features to connect different customers that each contract their packet voice VPN service from the same SP. These calls would otherwise traverse the PSTN, but because both enterprises are connected to the same physical SP network, the SP can provide better rates and services to these customers for business-to-business calling.
- PSTN access (on-net to off-net). This functionality includes the following features to route calls that originate on the VPN but terminate on the PSTN:
  - Off-net calling—Calls routed from the VPN to worldwide PSTN destinations. Calls are carried on-net as long as possible and use the closest or least-cost remote POP to connect to the destination local PSTN or other carriers.
  - Dedicated termination overflow—If trunks on the VPN to the distant PBX are blocked or fail, calls are allowed to overflow via the PSTN.
- Off-net access to VPN (off-net to on-net). This functionality includes the following features to route calls that originate on the PSTN but terminate on the VPN:
  - Calling card access—Employees at remote locations have access to the VPN by way of a toll-free or local PSTN number and a personal identification number (PIN).
  - Toll-free VPN access—Allows for end users to have a toll-free access number for customers and other services.
  - Off-net access—Allows small branch offices, telecommuters, and home locations to have PSTN access into the enterprise VPN with automatic number identification (ANI) authorization.
  - Customer care—Allows for customer care toll-free services to terminate on the SP network and the calls to be routed over the on-net network to the appropriate end customer call center location.

All of the features described are capable of performing sophisticated digit manipulation at various points in the network.

Packet Voice VPN Customer Dialing Plans

One key feature that differentiates a VPN from a peer-to-peer MMS network is the support for customized dialing plans. Custom dialing plans imply overlapping, or nonunique, dial plans within the SP network. For example, both Company X and Company Y can have an extension 2211. Theoretically, peer-to-peer MMS networks can support custom overlapping dial plans, but they are difficult to manage. VPNs support overlapping dial plans with the following advanced features:

- Access rights for Company X extension 2211 that may be different from those of Company Y extension 2211.

- On-net calling access between Company X extension 2211 and Company Y extension 2211.
- Off-net to on-net (PSTN to on-net) calling for each of these extensions.

The interpretation of the dial plan is implemented by the gatekeepers and route servers in the network. The dialed string is not interpreted in isolation, but in conjunction with some indication of the enterprise customer (closed user group) to which the caller belongs. One method of accomplishing this identification is to assign each gateway to a specific customer. The combination of the originating gateway and the dial string then provides a unique identification of the VPN to which the call belongs. Another method is to use digit manipulation features such as number expansion, translation rules, and technology prefixes on the gateway to assign a unique “site ID” to the dialed number before attempting the call setup with the gatekeeper, then delete the site ID before the call exits the network to a PBX or the PSTN.

Custom dial plans provide two major benefits to enterprise customers:

- End-user transparency—Customers can maintain their preexisting private PBX dialing plans.
- Closed user groups—the establishment of user groups that have custom calling patterns between members of the group, with appropriate security and access rights restrictions (such as international dialing access) imposed by the network.

Custom dial plans provide the following benefits to SPs:

- The network is more manageable and economical.
- The SP can offer better service to ensure the loyalty of existing customers and to attract new customers.

Gateway Partitioning

In all currently deployable VPN offerings, the implementation of the overlapping dial plan still relies on the fact that gateways are not shared among customers. Often the nonunique dialing plan is resolved by associating the originating or terminating gateway with a particular customer in the gatekeeper and route server configurations. This association is transparent to the gateway: The gateway is only aware of its unique dial plan, while the gatekeeper and route server handle the overlapping portions of the dial plan. This means that if there are two or more extension 2211s in the network, each resides on a separate gateway.

Gateway partitioning is a concept that allows a single gateway to be partitioned between different customers. This enables an SP to offer VPN service to small offices sharing a common building—such as a downtown skyscraper, or shops in a mall—by putting a single gateway in the building and providing different T1/E1 trunks or analog connections to each customer. In this scenario, instead of gatekeepers associating customers with the originating gateway, the gateway will associate customers with the originating voice interface and then forward this information to the gatekeeper to decide on the proper routing.

Multiple-Stage Dialing

Multiple-stage dialing capability enables a caller to hear one or two additional dial tones and dial one or two additional numbers to access a VPN. The possible dialing scenarios as follows.

- Single-stage dialing

  The caller hears a dial tone, dials a string of digits, and the call is connected to the terminating point. If the call is an on-net call, it may be connected based on the exact digits dialed. For calls involving the PSTN, digit manipulation is usually required. For example, a user calls a friend in

U.K. by dialing 9.011.44.1582.845544. Because the hopoff gateway is in U.K., but not local to the 01582 area code, the number delivered to the U.K. PSTN is 01582.845544. This digit manipulation is transparent to the caller.

- Two-stage dialing

  The caller hears a dial tone, dials a number, hears another dial tone, then dials the terminating phone number. This can be used for several features—for example, the off-net access feature. A small or home office has a PSTN number to gain access to the VPN. The caller dials the PSTN number, hears a second dial tone supplied by a VPN gateway (authentication can be accomplished using ANI or CLID), and then dials the VPN destination.

- Three-stage dialing

  The caller hears a dial tone (or some type of tone) twice and dials three distinct numbers before the call is connected. An example application is calling card access to the VPN for traveling employees. The first number is a local or toll-free PSTN number terminating on the SP network. Next the caller dials an authorization number and PIN, and finally the VPN destination of the call. The sequence of the last two stages can be reversed depending on how the application is implemented.

Digit Manipulation

As mentioned in the previous sections, digit manipulation is a key feature in implementing packet voice VPN dialing plans, and every element of the network (PBXs, gateways, PoPs, gatekeepers, application servers, and the billing system) may manipulate the calling and called digits of every call. This is common practice in circuit-switched VPNs as well.

Packet Voice VPN Call Routing Characteristics

The design, implementation, and interpretation of dial plans are key elements in performing successful call routing in a packet voice VPN. Digit manipulation by various network elements is also important because it directs the decisions of the next element in the network to which a call is routed. In addition, the features discussed in the following sections are necessary to perform advanced call routing:

- Priority Routing
- Load Balancing and Fault Tolerance
- Gatekeeper Call Signaling Models

Priority Routing

If multiple paths exist to connect a call to its destination, some may be preferred over others due to cost, distance, quality, delay, partner hand-offs, traffic load, or various other considerations. The following priority routing features keep an updated list of possible routes and the preferences among these routes:

- Least-cost routing

  This is most useful for on-net to off-net and off-net to on-net calls. When multiple PSTN entry-points or OSP partners are available to deliver a call, or when a PSTN gateway has trunks to different PSTN carriers at different cost levels, least-cost routing will determine the least-expensive route for the call.

- Time-of-day routing

  This provides customized routing based on the time of day and day of the week. Situations where time-of-day routing is useful include the following:

  - Travel and roaming features
  - Call center call diversion during or after business hours
  - Technical support centers with 24/7 service offered by different locations and time zones
  - Call diversion for holidays or off-site meetings
  - Call diversion or announcements during outages

Load Balancing and Fault Tolerance

For traffic destined to destinations with multiple gateways (such as PSTN hopoff gateways, or gateways into a large customer site), load balancing is often required. The H.323 Resource Availability Indicator (RAI) feature is often part of this functionality. H323 RAI instructs gatekeepers to route calls to gateways only when they have adequate capacity available. For more information, see the *Call Admission Control* ISD at:

<<<CAC URL>>>

Gatekeeper Call Signaling Models

The call signaling model you choose for your network will influence the type of network topology and which call routing features you will be able to implement. The following two call signaling models are available:

- Directed call signaling

  In this model, both the H.225 and H.245 call signaling and the RTP media stream flow directly between the gateways. The only signaling passed to the gatekeeper—and therefore visible to the gatekeeper-based applications—is the H.225 RAS messaging.

  For many features this is suficint, and this call model scales well because the gatekeeper is not a bottleneck or a single point-of-failure for all call signaling in the network. A possible downside is that CDR information from the gatekeeper may not be accurate enough for billing purposes, and therefore CDRs must be drawn from the gateways in the network. Because there are many more gateways than gatekeepers in a network, this means more CDR traffic will be on the network.

- Gatekeeper-routed signaling

  In this model, only the RTP media stream passes directly between the gateways, while all call signaling passes through the gatekeepers. In some implementations, the RTP stream also passes through the gatekeepers.

  This call model does not scale as well as directed call signaling, particularly when the RTP stream is routed by way of the gatekeepers. It also introduces an additional point of failure in the network However, gatekeeper-routed signaling offers the most flexibility to gatekeeper-based applications. Billing information from the gatekeeper is also accurate, and often obviates the need to gather CDR information from the gateways.

Some third-party gatekeepers can operate in either mode; the mode you should choose will depend on the features and services required in your network.

Packet Voice VPN Billing Features

VPN billing can be quite sophisticated, and may include the following features:

- Single or multisite billing

- Consolidated PSTN (off-net) billing
- Volume discounts
- Interbusiness (Company X to Company Y) on-net call billing at different rates than either intrabusiness (Company X Site 1 to Site 2) on-net calling or off-net calling
- Account code billing

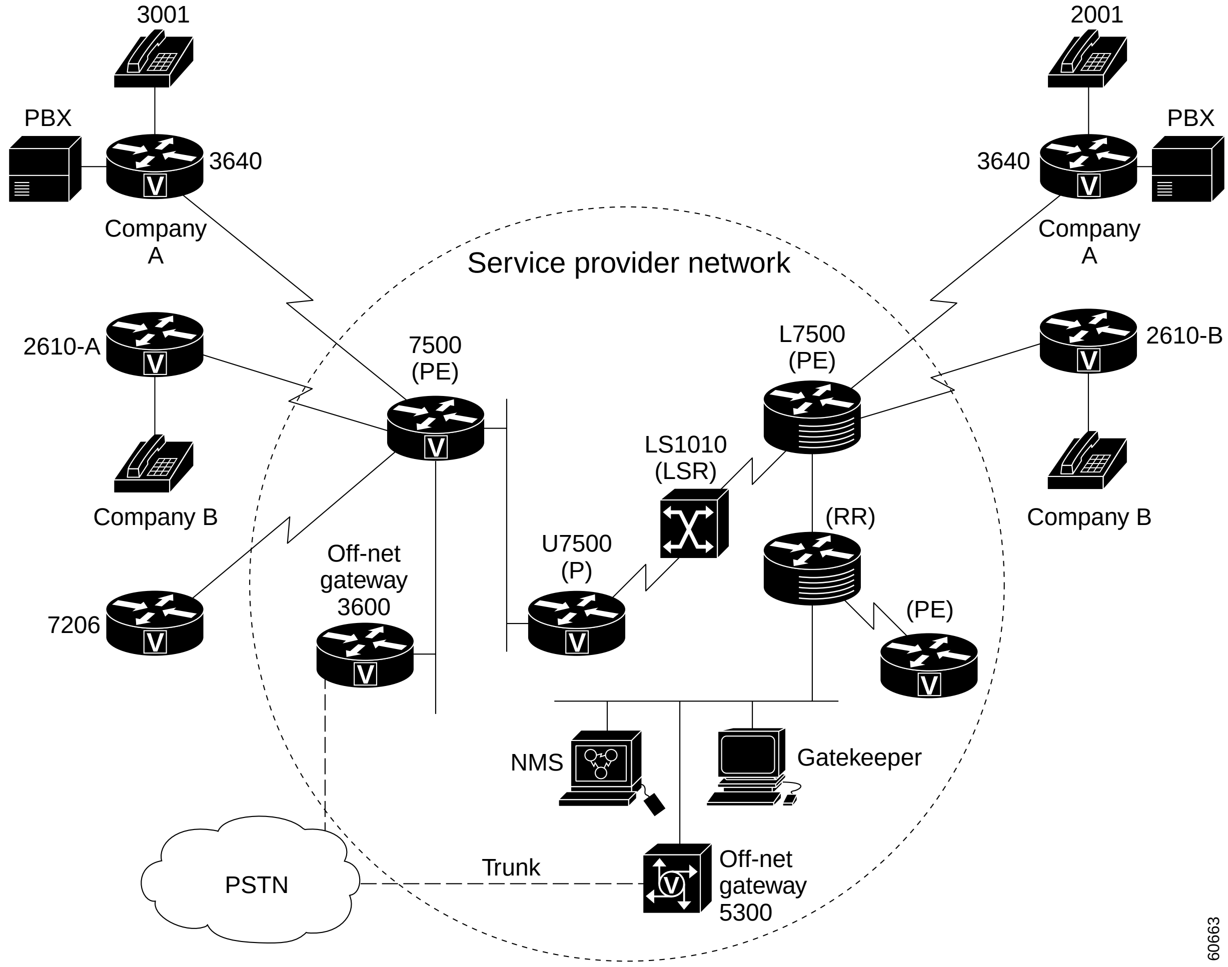
Third-party billing systems such as Mind-CTI, Belle, or Portal are generally used with Cisco networks. Some of the exact billing system features required for new VPN features may not be available yet, and you will need to evaluate billing criteria on a case-by-case basis. VSA extensions to RADIUS may be needed to support the information required by the billing system.

Packet Voice VPN Configuration

This section describes how to configure PV-VPNs. The two main types of components in a PV-VPN are Cisco gateways and third party (either NetCentrex or NetSpeak) gatekeepers. If the PV-VPN is running on a network that also operates a data VPN, the PV-VPN is largely independent of and transparent to the data VPN.

The topology shown in Figure 5 shows an SP PV-VPN that supports two companies, which each have two sites.

Figure 5 PV-VPN Network Topology



Description of VPN Services

The gateways register with the gatekeeper using Registration, Admission and Status (RAS) messages. Each company is assigned a unique VPN ID. The different offices of the company are assigned unique site IDs. Therefore, all the sites within a company have the same VPN ID but different site IDs. Each office or location also has an escape digit, which the other offices need to dial along with the extension number to reach the particular office. The user thus dials the escape digit defined for the destination site and the extension desired. The escape digit instructs the gateway to route the call to the gatekeeper and use digit manipulation to add the VPN ID to the Site ID to the dialed extension number.

The gateways forward the call to an edge router, which in turn forwards it to the gatekeeper. The gatekeeper then attempts to match the called number to a number in its dialing plan that belongs to the same VPN. Once a match is determined, the gatekeeper strips off the VPN ID and site ID from the calling number and sends the call to the destination gateway.

In the current implementation of NetCentrex, the identification of the VPN is not based on the H.323 ID but on the VPN ID contained in the calling number. Although the H.323 ID is not used for determining the VPN, you should define a loopback interface on the Cisco gateway and bind the loopback IP address as the source address for all H.323 calls. Only this loopback address is routed over the SP backbone and is known to the NetCentrex Gatekeeper. Although all the managed companies share the same SP backbone, within any given company VPN, its routers have knowledge of only each other's loopback addresses.

Gateway Configuration Task List

To configure the Cisco gateways for the VPN, perform the steps described in the following sections at each participating managed CPE:

- Configuring the Loopback Interface
- Registering the Gateway with Its Gatekeeper
- Configuring the Translation Rules
- Configuring the Dial-Peers

Configuring the Loopback Interface

The H.323 source address should preferably be bound to a loopback address and not to one of the physical interfaces on the gateway, because if bound to a physical interface and the interface goes down, H.323 connectivity will also go down. Because the state of a loopback interface is always up on a router, binding the H.323 process to a loopback interface creates a more reliable network. The following configuration binds H.323 to loopback interface 0:

```
Interface loopback 0
!Assigns an IP address to the loopback interface
 ip address 10.22.22.13 255.255.255.255
!Defines the loopback as the H.323 interface
 h323-gateway voip interface
!Specifies the name and IP address of the Gatekeeper
 h323-gateway voip id NETCENTREX ipaddr 10.1.1.50 1718
!Defines the H.323 ID for the gateway
 h323-gateway voip h323-id Anjou
!Specifies the source IP address that will be used for all VoIP traffic.
 h323-gateway voip bind srcaddr 10.22.22.13
```

Note **NOTE:** The H.323 ID for the gateway must be unique. If two gateways have the same H.323 ID, they will be unable to register with the gatekeeper.

Registering the Gateway with Its Gatekeeper

After you have configured the loopback interface, you must explicitly register the gateway with its gatekeeper. Gateway registration is not mandatory when using NetCentrex gatekeepers. It is required for NetSpeak gatekeepers. To register the gateway, use the **gateway** global configuration command and the following interface configuration commands on the loopback interface:

```
interface Loopback0
 ip address 10.22.22.7 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id NETCENTREX ipaddr 10.1.1.50 1718
 h323-gateway voip h323-id captain
```

Once the gateway has registered, it will begin exchanging RAS messages with the gatekeeper. To verify that the gateway successfully registered with the gatekeeper, use the **show gateway** privileged EXEC command as foolows :

```
gateway# show gateway

 Gateway captain is registered to Gatekeeper NETCENTREX
```

Note The phone numbers configured on the FXS ports of the gateway must be unique, otherwise the gateway will be unable to register with the gatekeeper.

Configuring the Translation Rules

In order for the gatekeeper to be able to route calls properly, the gateway must add the VPN ID and the Site ID to dialed extension numbers. The following configuration adds the VPN ID 999 and the site ID 111 to all calls:

```
Translation-rule 1
 Rule 1  ^1  9991111
 Rule 2  ^2  9991112
 Rule 3  ^3  9991113
 Rule 4  ^4  9991114
 Rule 5  ^5  9991115
 Rule 6  ^6  9991116
 Rule 7  ^7  9991117
 Rule 8  ^8  9991118
 Rule 9  ^9  9991119
```

Configuring the Dial-Peers

Dial peers are configured to handle the incoming and outgoing voice calls. The following configuration enables a POTS dial peer to handle calls to and from controller 2/0 connected to a PBX:

```
!Instructs the POTS dial peer to handle calls from extensions 2100 to 2199.
Dial-peer voice 1 pots
 Destination-pattern 21..
 Port 2/0:15
 Direct-inward-dial
 Forward digits all
!
Dial-peer voice 2 voip
!Configures the escape digit 2 and the destination number 31.
 Destination-pattern 231..
!Applies the translation rules to all outgoing calls.
 Translate-outgoing calling 1
 Session target ras
 no vad
```

To configure the originating gateway to make CAS calls, you must configure another POTS dial peer. Before you configure the dial peer carrying the POTS wild card number 21, configure a POTS dial peer as follows:

```
Dial-peer voice 1 pots
 Destination pattern 2101
 Port 2/0:15
 forward digits all
```

Without this dial peer, the wild card number 21.. would be recognized as an extension beginning with 21, and the gateway would convert it to 99911121.., which the gatekeeper will not recognize. This additional dial peer instructs the gateway to recognize the calling number as 2101 instead of 21..

NetCentrex Gatekeeper Configuration

NetCentrex gatekeeper configuration information was unavailable at the time of publication of this document.

NetSpeak Gatekeeper Configuration

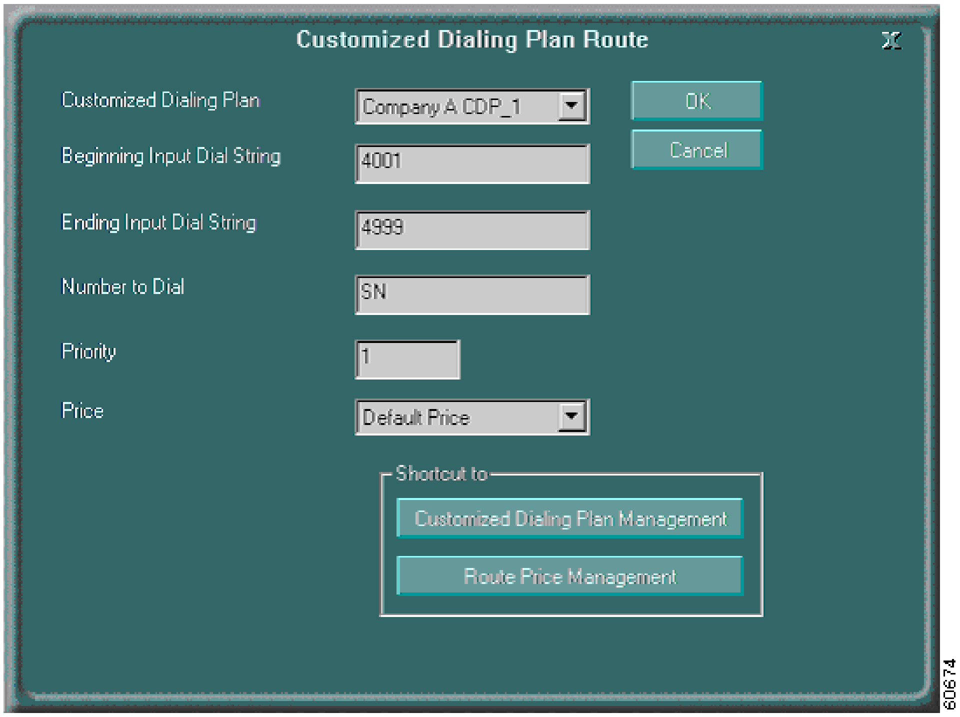
NetSpeak gatekeepers are configured using the NetSpeak Control Center. The following sections show screen captures of NetSpeak Gatekeeper/RouteServer version 3.2 running on Windows 2000:

- Creating VPN Dial Plans
- Assigning VPN Dial Plans to Gateways
- Creating Exchange Sets

Creating VPN Dial Plans

For each company VPN, create a route set defining the numbering plan used to place calls with the company as shown in Figure 6. Multiple CDP routes can be created and added to the route set to provide complete coverage of intracompany usage. Multiple route sets can be used to capture situations where multiple gateways are used along with multiple CDP configurations.

Figure 6 Creating VPN Dial Plans

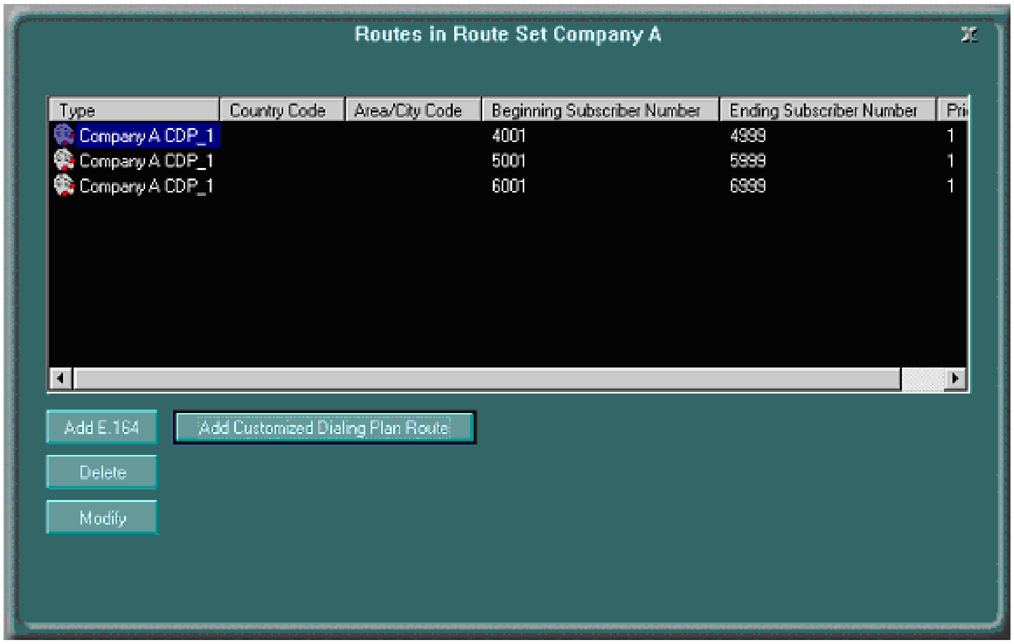


Customized Dialing Plan Route

Customized Dialing Plan: Company A CDP_1
Beginning Input Dial String: 4001
Ending Input Dial String: 4999
Number to Dial: SN
Priority: 1
Price: Default Price

Figure 7 displays the dial plan for Company A that is configured on the NetSpeak gatekeeper.

Figure 7 Displaying VPN Dial Plans



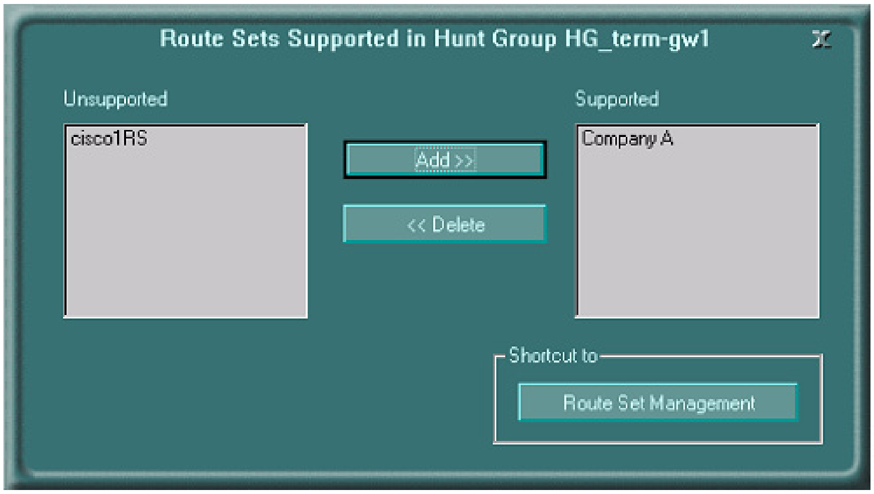
Routes in Route Set Company A

Type	Country Code	Area/City Code	Beginning Subscriber Number	Ending Subscriber Number	Pri
Company A CDP_1			4001	4999	1
Company A CDP_1			5001	5999	1
Company A CDP_1			6001	6999	1

Assigning VPN Dial Plans to Gateways

Assign the company-specific route set to gateways that will receive calls matching the CDP route characteristics as shown in Figure 8.

Figure 8 Assigning VPN dial Plans to Gateways



Route Sets Supported in Hunt Group HG_term-gw1

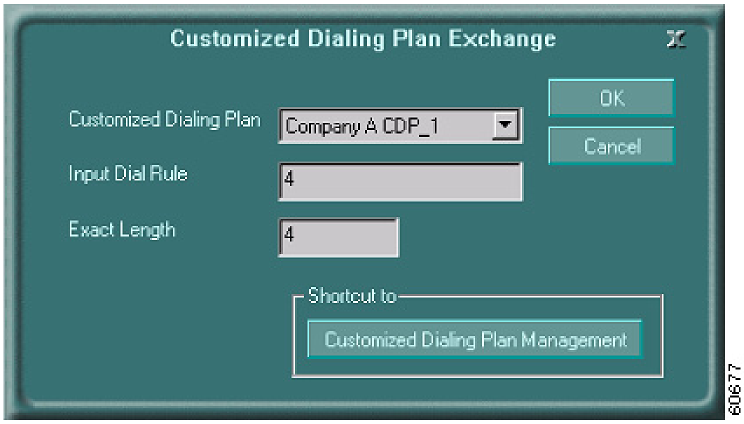
Unsupported: cisco1RS

Supported: Company A

Creating Exchange Sets

Create exchange sets for each company that describe the nature of the dialing plan and are associated with the CDPs of Company A as shown in Figure 9.

Figure 9 Creating Exchange Sets



Customized Dialing Plan Exchange

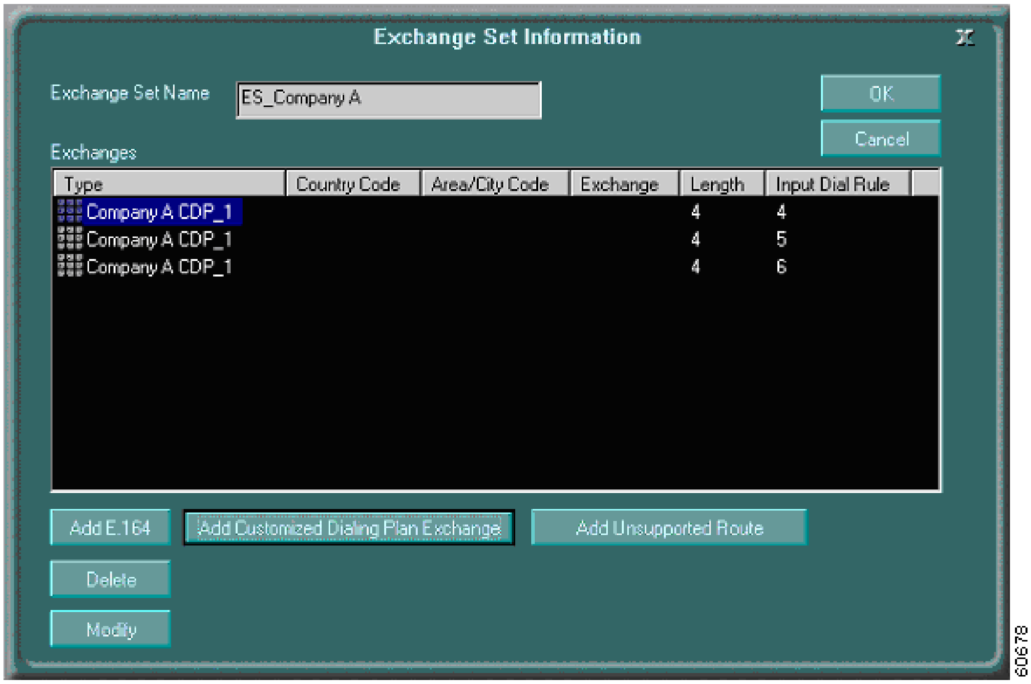
Customized Dialing Plan: Company A CDP_1

Input Dial Rule: 4

Exact Length: 4

Figure 10 displays the exchange set for Company A that is configured on the gatekeeper.

Figure 10 Displaying Exchange Sets



Exchange Set Information

Exchange Set Name: ES_Company A

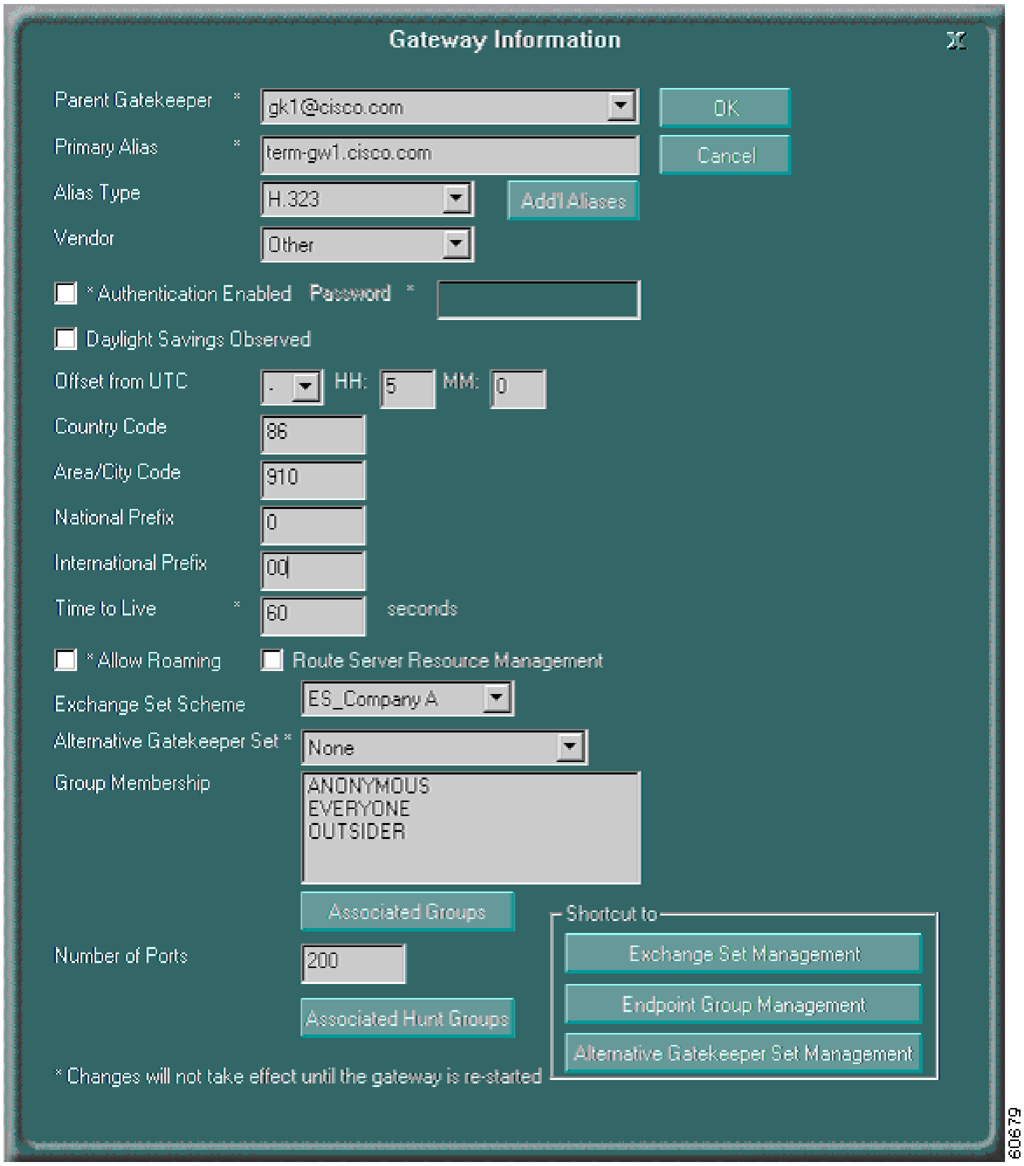
Exchanges

Type	Country Code	Area/City Code	Exchange	Length	Input Dial Rule
Company A CDP_1				4	4
Company A CDP_1				4	5
Company A CDP_1				4	6

Configuring the Gateways

Configure the individual gateways that report to the gatekeeper as shown in Figure 11. Assign the company-specific exchange set to gateways that will originate calls matching the exchange set routing characteristic.

Figure 11 Configuring Gateways



Gateway Information

Parent Gatekeeper * gk1@cisco.com

Primary Alias * term-gw1.cisco.com

Alias Type H.323

Vendor Other

□ * Authentication Enabled Password *

□ Daylight Savings Observed

Offset from UTC - HH: 5 MM: 0

Country Code 86

Area/City Code 910

National Prefix 0

International Prefix 00

Time to Live * 60 seconds

□ * Allow Roaming □ Route Server Resource Management

Exchange Set Scheme ES_Company A

Alternative Gatekeeper Set * None

Group Membership
ANONYMOUS
EVERYONE
OUTSIDER

Number of Ports 200

* Changes will not take effect until the gateway is re-started

Complete Configuration Files

Complete device configurations are provided in the following sections:

- Gateway Configurations
- Hopoff Gateway Configuration
- SP Edge Router Configuration

Gateway Configurations

The following configuration is for a Cisco 3640 gateway connected over a Frame Relay link to the SP network:

```
!
version 12.2
no service single-slot-reload-enable
no service timestamps debug uptime
no service timestamps log uptime
no service password-encryption
!
hostname right-gateway
!
enable password cisco
!
voice-card 2
!
ip subnet-zero
!
!
no ip finger
ip telnet source-interface Loopback0
no ip domain-lookup
!
no ip dhcp-client network-discovery
!
class-map match-all VOICE
  match access-group 102
!
!
policy-map LLQ
  class VOICE
    priority 75
class class-default
fair-queue
 !
frame-relay switching
isdn switch-type primary-qsig
call rsvp-sync
voice call send-alert
!
voice service voip
 h323 call start fast
!
!
controller E1 2/0
 pri-group timeslots 1-31
!
controller E1 2/1
 pri-group timeslots 1-31
!
translation-rule 1
 Rule 0 ^0 9991110
 Rule 1 ^1 9991111
 Rule 2 ^2 9991112
 Rule 3 ^3 9991113
 Rule 4 ^4 9991114
 Rule 5 ^5 9991115
 Rule 6 ^6 9991116
 Rule 7 ^7 9991117
 Rule 8 ^8 9991118
 Rule 9 ^9 9991119
```

```
!
interface Loopback0
 ip address 10.22.22.7 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id NETCENTREX ipaddr 10.1.1.50 1718
 h323-gateway voip h323-id right-gateway
 h323-gateway voip bind srcaddr 10.22.22.7
!
!
!
interface Serial1/0
 description *** To gatekeeper ***
 ip address 10.32.32.2 255.255.255.0
 encapsulation frame-relay
 load-interval 30
 clockrate 1000000
 no arp frame-relay
 frame-relay class CRTP
 frame-relay traffic-shaping
 frame-relay map ip 10.32.32.1 32 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
 frame-relay ip rtp header-compression
!
!
interface Serial2/0:15
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn protocol-emulate network
 isdn incoming-voice voice
 no isdn T309-enable
 isdn T310 60000
 no cdp enable
!
interface Serial2/1:15
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn protocol-emulate network
 isdn incoming-voice voice
 no isdn T309-enable
 isdn T310 60000
 no cdp enable
!
router bgp 101
 no synchronization
 bgp log-neighbor-changes
 network 10.22.22.7 mask 255.255.255.255
 network 10.32.32.0 mask 255.255.255.0
 network 10.19.173.0 mask 255.255.255.192
 network 10.10.10.0
 neighbor 10.32.32.1 remote-as 65001
 neighbor 10.32.32.1 send-community extended
 no auto-summary
!
ip classless
no ip http server
!
map-class frame-relay CRTP
 no frame-relay adaptive-shaping
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output LLQ
frame-relay fragment 640
access-list 10 permit 10.33.33.2
access-list 102 permit udp any range 16384 32727 any range 16384 32727
!
voice-port 2/0:15
!
voice-port 2/1:15
!
voice-port 3/0/0
 echo-cancel coverage 32
!
voice-port 3/0/1
!
voice-port 3/1/0
!
voice-port 3/1/1
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
destination-pattern 21..
direct-inward-dial
port 2/0:15
forward-digits all
!
dial-peer voice 2 voip
 destination-pattern 23...
 translate-outgoing calling 1
 session target ras
 no vad
!
dial-peer voice 3 pots
 destination-pattern 2001
 port 3/0/0
!
dial-peer voice 4 voip
 destination-pattern 0041227076006
 translate-outgoing calling 1
 session target ras
!
dial-peer voice 5 pots
 destination-pattern 2002
 port 3/0/1
!
dial-peer voice 6 pots
 destination-pattern 201.
 direct-inward-dial
 port 2/1:15
 forward-digits all
!
dial-peer voice 7 voip
 destination-pattern 0041227083001
 translate-outgoing calling 1
 session target ras
!
gateway
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
 password cisco
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
line vty 5
 login
!
end
```

The following configuration is for a Cisco 3640 gateway connected over a Frame Relay link to the SP network:

```
!
version 12.2
no service single-slot-reload-enable
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname left-gateway
!

enable password cisco
!
voice-card 2
!
ip subnet-zero
!
no ip finger
ip telnet source-interface Loopback0
no ip domain-lookup


!
no ip dhcp-client network-discovery
!
class-map match-all VOICE
  match access-group 102
!
!
policy-map LLQ
  class VOICE
    priority 75
class class-default
fair-queue

isdn switch-type primary-qsig
isdn voice-call-failure 0
call rsvp-sync
voice call send-alert
!
voice service voip
 h323 call start fast
!
controller T1 2/0
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
 description *** Connected to T1Callgen ***
!
controller T1 2/1
```

```
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
 description *** Analog1 ***
!
translation-rule 1
 Rule 0 ^0 9992220
 Rule 1 ^1 9992221
 Rule 2 ^2 9992222
 Rule 3 ^3 9992223
 Rule 4 ^4 9992224
 Rule 5 ^5 9992225
 Rule 6 ^6 9992226
 Rule 7 ^7 9992227
 Rule 8 ^8 9992228
 Rule 9 ^9 9992229
!
!
interface Loopback0
 ip address 10.22.22.6 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id NETCENTREX ipaddr 10.1.1.50 1718
 h323-gateway voip h323-id left-gateway
 h323-gateway voip bind srcaddr 10.22.22.6
!
interface Serial0/0
 description *** To gatekeeper ***
 ip address 10.33.33.2 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 load-interval 30
 clockrate 1000000
 no arp frame-relay
 frame-relay class CRTP
 frame-relay traffic-shaping
 frame-relay map ip 10.33.33.1 33 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
 frame-relay ip rtp header-compression
!
!

!
interface Serial2/0:23
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn protocol-emulate network
 isdn incoming-voice voice
 no isdn T309-enable
 isdn T310 4000
 no cdp enable
!
interface Serial2/1:23
 no ip address
 no logging event link-status
 isdn switch-type primary-qsig
 isdn protocol-emulate network
 isdn incoming-voice voice
 no isdn T309-enable
 no cdp enable
!
!
```

```
router bgp 102
 no synchronization
 bgp log-neighbor-changes
 network 10.22.22.6 mask 255.255.255.255
 network 10.33.33.0 mask 255.255.255.0
 network 10.10.10.0
 neighbor 10.33.33.1 remote-as 65001
 neighbor 10.33.33.1 send-community extended
 no auto-summary
!
ip local policy route-map LOCAL-POLICY
ip classless
no ip http server
!
!
map-class frame-relay CRTP
 no frame-relay adaptive-shaping
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output LLQ
frame-relay fragment 640
!
access-list 10 permit 10.32.32.2
access-list 102 permit udp any range 16384 32727 any range 16384 32727
!
!
voice-port 2/0:23
!
voice-port 2/1:23
!
voice-port 3/1/0
 timeouts ringing 10
!
voice-port 3/1/1
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 destination-pattern 31..
 direct-inward-dial
 port 2/0:23
 forward-digits all
!
dial-peer voice 2 voip
 destination-pattern 12...
 translate-outgoing calling 1
 session target ras
 no vad
!
dial-peer voice 3 pots
 destination-pattern 3001
 port 3/1/1
!
dial-peer voice 4 pots
 destination-pattern 30..
 direct-inward-dial
 port 2/1:23
 forward-digits all
!
```

```
dial-peer voice 5 pots
 destination-pattern 3002
 port 3/1/0
!
gateway
!
line con 0
 exec-timeout 0 0
 password cisco
 transport input none
line aux 0
 exec-timeout 0 0
 password cisco
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
ntp clock-period 17179862
ntp server 10.22.22.7
end
```

Hopoff Gateway Configuration

The following configuration is for a Cisco AS5300 hopoff gateway and is used to connect to the PSTN:

```
!
version 12.2
no service single-slot-reload-enable
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Hopoff-gw
!
boot system flash:c5300-is-mz.122-1a
logging rate-limit console 10 except errors
aaa new-model
aaa authentication login default group radius local
aaa authentication login h323 group radius
aaa authorization exec h323 group radius
aaa accounting connection h323 start-stop group radius
enable password cisco
!
username cisco password 0 cisco
username 111 password 0 1234
!
!
resource-pool disable
!
call rsvp-sync
ip subnet-zero
no ip finger
no ip domain-lookup
ip host CALLGEN-SECURITY-V2 10.70.27.66 10.12.0.0
!
no ip dhcp-client network-discovery
isdn switch-type primary-qsig
!
!
!
```

```
!
!
fax interface-type vfc
mta receive maximum-recipients 0
!
!
controller T1 0
 framing sf
 clock source line primary
 linecode ami
!
controller T1 1
 framing esf
 clock source line secondary 1
 linecode b8zs
 pri-group timeslots 1-24
 description *** Connected to PSTN ***
!

interface Loopback0
 ip address 10.22.22.15 255.255.255.255
 h323-gateway voip interface
 h323-gateway voip id NETCENTREX ipaddr 10.1.1.50 1718
 h323-gateway voip h323-id hopoff-gw
 h323-gateway voip bind srcaddr 10.22.22.15
!
!
interface Serial1:23
 no ip address
 isdn switch-type primary-qsig
 isdn protocol-emulate network
 isdn incoming-voice modem
 no isdn T309-enable
 no cdp enable
!
interface FastEthernet0
 ip address 10.1.1.22 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
!
router bgp 110
 no synchronization
 bgp log-neighbor-changes
 network 10.22.22.15 mask 255.255.255.255
 neighbor 10.1.1.2 remote-as 65001
 neighbor 10.1.1.2 send-community extended
 no auto-summary
!
ip classless
no ip http server
!
tftp-server flash:enter_account.au
tftp-server flash:enter_pin.au
tftp-server flash:enter_destination.au
!
radius-server host 200.1.1.8 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
!
```

```
voice-port 1:D
 translate calling 1
!
dial-peer voice 1 pots
 application clid_authen_collect
 incoming called-number 1800
 destination-pattern 1800
 direct-inward-dial
 port 1:D
 forward-digits all
!
dial-peer voice 2 voip
 destination-pattern .T
 session target ras
!
dial-peer voice 3 pots
 destination-pattern 0041.T
 direct-inward-dial
 port 1:D
 forward-digits all
!
gateway
!
!
line con 0
 exec-timeout 0 0
 transport input none
line aux 0
 exec-timeout 0 0
 transport input all
line vty 0 4
 exec-timeout 0 0
!
ntp master
end
```

SP Edge Router Configuration

The following configuration is for a Cisco 7500 SP edge router and is used to connect to the various gateways over Frame Relay links:

```
!
version 12.2
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname l7500(PE2)
!

logging rate-limit console 10 except errors
enable password cisco
!
ip subnet-zero
no ip finger
no ip domain-lookup
!
!
ip vrf LAPD
rd 65001:30
export map Ex1
```

```
route-target import 65001:30
route-target import 65001:200
!
ip vrf NYPD
rd 65001:20
export map Ex
route-target import 65001:20
route-target import 65001:200
ip cef distributed
no ip dhcp-client network-discovery

frame-relay switching
!
class-map match-all VOICE
match access-group 102
!
!
policy-map LLQ
 class VOICE
  priority 75 30000
 class class-default
 fair-queue

policy-map SHAPED-LLQ
 class class-default
 shape peak 512000 2048 2048
 service-policy LLQ
!

!
!
interface Loopback0
 ip address 10.22.22.3 255.255.255.255
 ip router isis
!
interface FastEthernet1/0/0
 ip address 10.25.25.1 255.255.255.0
 ip router isis
 ip route-cache distributed
 full-duplex
 tag-switching ip
 isis circuit-type level-2-only
 isis metric 2000 level-2
!
interface ATM1/1/0
 ip address 10.24.24.2 255.255.255.0
 ip router isis
 ip route-cache distributed
 no atm ilmi-keepalive
 pvc 3/300
 protocol ip 10.24.24.1 broadcast
 protocol clns 49.0022.0022.0022.0002.00 broadcast
 encapsulation aal5snap
!
tag-switching ip
isis circuit-type level-2-only
isis metric 2000 level-2
isis priority 81
!
interface Serial2/0/0
 no ip address
 encapsulation frame-relay
 ip route-cache distributed
 no ip mroute-cache
 load-interval 30
 no fair-queue
 no arp frame-relay
 no frame-relay inverse-arp
 frame-relay lmi-type cisco
!
interface Serial2/0/0.1 point-to-point
 ip vrf forwarding NYPD
 ip address 10.32.32.1 255.255.255.0
 no ip mroute-cache
 no arp frame-relay
 frame-relay interface-dlci 32
 class CRTP
 frame-relay ip rtp header-compression
!
interface Serial2/0/1
 ip vrf forwarding LAPD
 ip address 10.38.38.1 255.255.255.0
 encapsulation frame-relay
 ip route-cache distributed
 clockrate 250000
 no arp frame-relay
 frame-relay map ip 10.38.38.2 38 broadcast
 no frame-relay inverse-arp
 frame-relay intf-type dce
 frame-relay ip rtp header-compression
!
interface Serial2/0/2
 ip vrf forwarding LAPD
 ip address 10.39.39.1 255.255.255.0
 encapsulation frame-relay
 ip route-cache distributed
 no ip mroute-cache
 no fair-queue
 frame-relay map ip 10.39.39.2 39 broadcast
 no frame-relay inverse-arp
!
interface Serial2/0/3
 description ***** Connected to Thebes ******
 no ip address
 encapsulation frame-relay
 no ip route-cache cef
 ip route-cache distributed
 no ip mroute-cache
 no fair-queue
 no arp frame-relay
 no frame-relay inverse-arp
 frame-relay lmi-type cisco
!
interface Serial2/0/3.1 point-to-point
 description *****
 ip vrf forwarding NYPD
 ip address 10.40.40.1 255.255.255.0
 no ip mroute-cache
 no arp frame-relay
 frame-relay interface-dlci 40
 class CRTP1
 frame-relay ip rtp header-compression
!
!
router isis
 redistribute connected metric 20 route-map LOOP
 net 49.0022.0022.0022.0003.00
 is-type level-2-only
 metric-style wide
 max-lsp-lifetime 65000
 lsp-refresh-interval 64000
!
router bgp 65001
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.22.22.4 remote-as 65001
 neighbor 10.22.22.4 update-source Loopback0
 neighbor 10.22.22.4 next-hop-self
 neighbor 10.22.22.4 send-community extended
 no auto-summary
!
address-family ipv4 vrf NYPD
 neighbor 10.32.32.2 remote-as 101
 neighbor 10.32.32.2 activate
 neighbor 10.32.32.2 send-community extended
 neighbor 10.32.32.2 default-originate
 neighbor 10.40.40.2 remote-as 110
 neighbor 10.40.40.2 activate
 neighbor 10.40.40.2 send-community extended
 neighbor 10.40.40.2 default-originate
 no auto-summary
 no synchronization
 network 10.32.32.0 mask 255.255.255.0
 network 10.40.40.0 mask 255.255.255.0
 exit-address-family
!
address-family ipv4 vrf LAPD
 neighbor 10.38.38.2 remote-as 108
 neighbor 10.38.38.2 activate
 neighbor 10.38.38.2 send-community extended
 neighbor 10.38.38.2 default-originate
 neighbor 10.39.39.2 remote-as 109
 neighbor 10.39.39.2 activate
 neighbor 10.39.39.2 send-community extended
 neighbor 10.39.39.2 default-originate
 no auto-summary
 no synchronization
 network 10.38.38.0 mask 255.255.255.0
 network 10.39.39.0 mask 255.255.255.0
 exit-address-family
!
address-family vpnv4
 neighbor 10.22.22.4 activate
 neighbor 10.22.22.4 send-community extended
 no auto-summary
 exit-address-family
!
ip kerberos source-interface any
ip classless
ip route 10.10.10.0 255.255.255.0 10.32.32.2
no ip http server
!
!
ip access-list standard Ex
 permit 10.22.22.16
 permit 10.22.22.7

ip access-list standard Ex1
 permit 10.22.22.14
 permit 10.22.22.13
```

```
ip access-list standard LOOP
 permit 10.22.22.3
!
map-class frame-relay CRTP
 no frame-relay adaptive-shaping
 service-policy output SHAPED-LLQ
 frame-relay fragment 640
!
access-list 102 permit udp any range 16384 32727 any range 16384 32727
 route-map Ex1 permit 10
 match ip address Ex1
 set extcommunity rt 65001:30 65001:101
!
route-map LOOP permit 10
 match ip address LOOP
!
route-map Ex permit 10
 match ip address Ex
 set extcommunity rt 65001:20 65001:101
!
line con 0
 transport input none
line aux 0
 password cisco
 login
 line vty 0 4
 password cisco
 login
!
end
```