Cisco Systems

White Paper

Hosted Business
IP Telephony

Table of Contents

Table of Figures

Cisco Systems

White Paper

Hosted Business **IP Telephony**

The adoption of data applications in the business environment has meant the demand for data services has exploded. In many service providers the volume of data traffic has overtaken voice traffic. This fundamental change in traffic profiles has made the case to converge voice and data networks even more compelling.

At the same time the service provider's customers, the enterprise, the small business and even the home worker have deployed voice over IP. This means the end users need IP telephony services to connect their applications over the wide area and access the PSTN. These multiple drivers, and the new opportunities arising from voice over IP can change the way people work and live and the resulting change in network architecture cannot be ignored.

This white paper provides an overview of the components and architectures involved in deploying new and existing voice services in the business environment using voice over IP.

1 Introduction

Hosted business telephony offers tremendous new revenue opportunities for service providers. Data traffic now rivals the volume of voice traffic, and data traffic is expected to continue to grow at a much faster rate than voice. Some estimates suggest that data traffic could grow by as much as 100% per year, while voice traffic may only see growth in the range of 5% per year.

At the same time, voice traffic continues to be the source of the bulk of service provider's profits and revenue. The Public Switched Telephone Network (PSTN) has evolved over the last hundred years to optimise the transmission of voice traffic over a switched network infrastructure. This has resulted in operators being faced with the challenge of managing the explosive growth of data traffic whilst maintaining the quality of voice traffic on a network that was never designed for the transmission of data. This resulted in operators having to have separate infrastructure for voice and data networks, the consequence of which has been increased complexity and cost for the service provider.

Packet networks have now facilitated the convergence of voice and data traffic. Rather than trying to run data traffic on a circuit switched network optimised for voice, or running disparate infrastructure to support voice and data requirements, service providers now have the option of delivering data and voice services over a single infrastructure optimised for all the applications running over it, including voice. Some of the clear advantages provided by convergence are:

- A network optimised to support the phenomenal growth in data traffic, but which supports the sensitivities and requirements of a variety of applications, including voice.
- A vastly superior efficiency in the delivery of voice, data and multimedia services resulting in significant cost reductions in the delivery of these services.
- Allowing the 'tight' integration of voice, data and multimedia services as they all run on a common network infrastructure.
- Allows the rapid development of applications and services as the network is built around the open standards that have come from the development of the Internet.
- It increases customer loyalty as critical voice and data applications can now be delivered by one service provider.

The case for convergence is particularly clear in providing business voice services. Analysts suggest that over the next three to five years that approximately 20% of business voice traffic will be carried over packet based networks. When combined with the booming demand for data services driven by business, the opportunities presented by providing business services over a common infrastructure are immense.

The revenue opportunities for service providers expand considerably when the operator moves from providing simple access via a converged network to delivering a range of hosted business services. The importance of hosted services is borne out by a study released in June 2001 by Allied Business Intelligence Inc that shows the value of hosted solutions growing at a compound annual growth rate of 137 percent over the next six years. This represents a tremendous market opportunity for the service providers that recognise the need to differentiate their service offerings in a market where competition for basic transmission continues to drive prices down making bandwidth a commodity.

The advantages of Hosted Business IP Telephony are numerous and apply differently to the various types of service providers:

- Internet Service Providers (ISPs) providing data only can broaden their service offering to include telephony and advanced VPN services.
- Telephony service providers that are moving their backbone networks to IP can extend IP to their customers and provide them with the benefits of end-to-end IP Telephony services. A Hosted Business IP Telephony network is complimentary to the existing TDM network and it is easy to extend the new services to reach all customers.
- Greenfield service providers can start with next generation technology and immediately deliver both voice and data services over a converged IP network.

In offering these services each service provider can then choose how to price the services. Telephony can be provided based on lower telephony (per minute) charges, free calls between IP-based sites, or combined pricing with data connectivity. In addition IP technology, particularly when hosted by service provider reduces operational and capital expenditure costs for businesses associated with running their own PBX and data network. When expansion is necessary, or reduction of services, the hosted model is also more beneficial as the capacity can be reallocated to or from other customers.

The most popular hosted services are:

- PSTN Access.
- Voice and Data VPNs.
- Business telephony services.
- Value Added Services such as Unified Messaging and Voice Portals.

Whilst these are the most common services, the distributed nature of the IP network and the 'shortest route' properties of the IP voice path mean that it is a flexible and scalable solution. Cisco Systems has developed an end-to-end Hosted Business IP Telephony reference architecture based on open standards. This makes it easy to add new services, offer unique functionality and increase revenues.

This document is a technical overview designed to explain the services that can be offered and to provide details of the Cisco components that can be used to deliver them. It contains the following sections:

Section Overview	
Section 2 Services Summary	An overview of the services Hosted Business IP Telephony can deliver.
Section 3 - 6 Technical Description	A detailed look at the functionality and the components used.
Section 7 IP Telephony Quality of Service	A how and why section for Quality of Service.
Section 8 Customer Premises Telephony	An explanation IP Telephony (VoIP to the Phone) as a 'resale', managed and hosted service.
Section 9 Customer Access	A description of the equipment that can be used at the customer premise to allow the services to be connected to existing PBXs.
Section 10 Contacts and References	
Section 11 Glossary of Terms	

It is suggested that section 2 be read in its entirety and then sections 3 to 6 can be read selectively depending on the services that are of interest.

2 Services Summary

The ability to offer complete communications solutions to business customers is going to be essential in the race to gain and maintain market share. A Hosted IP model enables the creation of new services fully integrating voice, data and video. With an IP base, services can be rapidly deployed to open new revenue streams ahead of competition in a modular fashion.

Access to the PSTN is a vital component in any solution; nearly all customers will want to talk to all the other PSTN users worldwide. Cisco's PGW 2200 PSTN Gateway provides a variety of incoming and outgoing call revenue opportunities. Today, data has already overtaken voice in terms of volume yet voice still makes up the majority of service provider revenue.

After PSTN access, Voice VPNs are high on the importance list to multi-site companies. These companies need the means to interconnect sites cost effectively. The VPN section looks at the benefits of a Voice VPN from a functionality perspective and the cost savings that are achieved through improved traffic routing control.

Traditionally, VPNs are based on the assumption that each site has a local PBX, which can be expensive. IP provides a cost effective alternative to outsource call control to a service provider. Traditionally, the alternative has been known as Centrex but has too many limitations for most customers. IP Centrex offers complete integration within the VPN without the need for local PBXs and is described in the IP Centrex section. This section explains why Centrex on an IP core addresses the limitations that have prevented the widespread use of TDM Centrex in Europe.

A Voice over IP network architecture also allows easy addition of many new Value Added Services. The section on Value Added Services shows how only a small incremental cost can provide additional revenue streams from services such as Voice Portals and Unified Messaging.

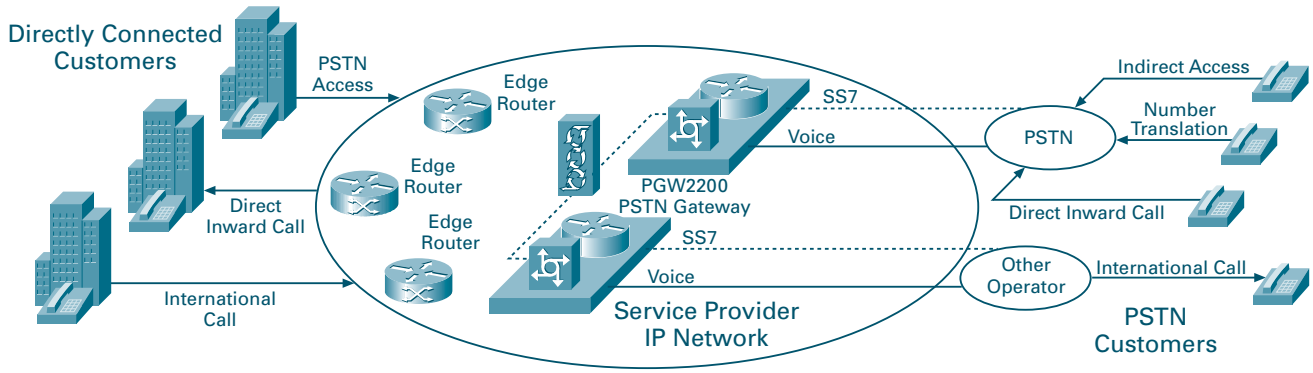
The remainder of this section gives an overview of the core services followed by an explanation and a summary of the benefits offered by each service. For an in-depth or technical understanding please read the specific sections as well.

2.1 PSTN Access

Even as the level of voice traffic carried over IP increases, until everything is IP there will be a requirement to connect to the TDM based PSTN. PSTN access requirements will continue to grow until something like 50% of the world's traffic is VoIP. In addition interconnection between operators is still predominantly TDM based with SS7 or PRI signalling. It is therefore essential that Business IP Telephony provide integration with existing TDM networks.

In providing a connection between Voice over IP and the TDM PSTN a new door is opened to provide many services, some traditional, such as Indirect Access, Free-phone and other non-geographic number as well as new VoIP based services that will provide additional revenue streams. A number of associated services are described below, but for a more technical description of Cisco's PSTN Access solution please refer to Section 3.

Figure 2-1: PSTN Access using PGW 2200



The diagram in Figure 2-1 shows how the PSTN Gateway (PGW 2200) is the interface between the IP network on the left and the TDM network on the right. Calls can originate from and terminate on either side of the PSTN Gateway.

Basic call types can be split into three groups - directly connected customers, indirectly connected customers and special services.

Local Number Portability:
To ensure customers have a fair and equal choice of service provider, it is common for national regulators to enforce Local Number Portability (LNP). This obliges service providers to allow customers to transfer their existing number to a new service provider if they request it.

There are two main mechanisms for LNP:

- Onward Donor Network Routing

This works by the original network (the owner of the number range) re-routing the call to the new network.

- All Call Query

For every call the originating or transit network checks a database to determine if the number is ported and should be routed differently

Cisco's PGW 2200 PSTN Gateway supports both of these mechanisms using internal lookup tables or INAP queries to an SCP.

2.1.1 Directly Connected Customers

2.1.1.1 PSTN Access

The most basic service the PSTN Gateway provides is outgoing calls to the PSTN for directly connected customers. In general the offering to the customer is a lower call tariff for all or some destinations. For example, a service provider may offer lower cost international or long distance calls and maintain margin by taking advantage of its own IP backbone network and/or interconnects with competitive wholesale VoIP or TDM carriers.

2.1.1.2 Direct Dial Inward (DDI)

The PSTN Gateway also supports calls in the other direction such as incoming calls to customers' direct dial number ranges. This is particularly advantageous in countries where Local Number Portability (LNP) has been imposed by the regulator allowing customers' to keep their existing number ranges. The service provider will then receive revenue from other operators for delivering the calls to the customer.

PSTN Access and Direct Dial for directly connected customers can be combined with other hosted IP Telephony services such as VPN or IP Centrex. This combination of PSTN access with enhanced features allows the service provider to offer a complete telephony solution to a business customer.

2.1.2 Indirectly Connected Customers

Indirect Access (IDA) allows customers to use the services of a network they are not directly connected by dialling an access number. A service provider offering Indirect Access collects call charges from the customer and pays a portion of this back to the customer's 'direct' service provider for the access leg of the call.

There are two main types of Indirect Access; Call by Call, where the user dials a prefix on an individual call to select the indirect access service provider and Pre-Selection, where the subscriber has arranged for all calls to be routed via a particular indirect access service provider. Business customers often use customer premises equipment or program their PBXs to add the indirect access prefix to ensure all traffic is routed via the cheapest route.

Indirect Access, enabled by the Cisco PGW 2200, provides a route for new service providers to generate revenue without the cost of building an extensive national network to get to their customers. It is also useful to complement other services and to extend a service provider's reach, allowing access to customers not within the service provider's network footprint.

2.1.3 Special Services

A service provider with a PSTN Gateway can offer a variety of special call services to PSTN customers based on Number Translation Services (NTS). Number translation is normally applied to non-geographic numbers such as Local Rate, National Rate, Premium Rate and Free Phone numbers. When calls are placed to these numbers they are charged at the same rate for each caller. The actual cost of the call will vary according to the geographic destination of the call and the difference will be either be paid or collected from the destination.

Examples of this include:

2.1.3.1 Free Phone

Free Phone or '800' calls are free to the caller but are paid for by the destination. This is commonly used to encourage customers to call the particular company.

2.1.3.2 Local Rate

Local Rate calls allow the caller to dial a number that charges them only at the local rate regardless of where the destination is. Call centres commonly use Local Rate, particularly for Utilities and ISPs where they want to imply a local presence but actually may route the calls elsewhere for their benefit such as to a central call centre.

The amount the caller pays for the call may cover the cost of the call, if not the destination has to contribute.

2.1.3.3 National Rate

National Rate is similar to Local Rate except the caller is charged for a national call. As the caller is paying more than Local Rate the destination may receive an income from each call or contribute to each call depending on the locations involved.

2.1.3.4 Premium Rate

Premium Rate calls are charge to the caller at rates above that of a normal call in order to be able to pay the called party for the call. Examples of these services include chat lines, recorded announcements, tele-voting download of ring tones and logos for mobile phones. In many countries there are multiple types of Premium-Rate numbers enabling different rates to be charged.

2.1.3.5 Personal Numbering Services/Personal Call Routing

Service providers can also offer customers the ability to route or handle calls based on rules such as the identity of the caller, the time of day, whether they are busy etc. and route the call to the appropriate destination. This service is often combined with a Unified Messaging/Communications service. Unified Messaging is discussed in more detail in Section 6.

MGCP:
The Media Gateway Control Protocol (MGCP) is designed to interface between a media gateway controller (or call agent) and a media gateway. It is a master/slave protocol and uses other protocols in addition, for example session description protocol to describe the media aspects of the call.

MGCP allows the separation of the call control intelligence and the media end-point by a standard interface. This potential separation means that the end points for the call can be remotely located from a centralised media gateway controller unlike existing TDM circuit switches.

MGCP is specified in RFC2905 (IETF) while the ITU has proposed H.248.

The PGW2200 uses MGCP to control Cisco's media gateways such as AS5400 and MGX8850.

2.1.4 PSTN Gateway for Transit Traffic

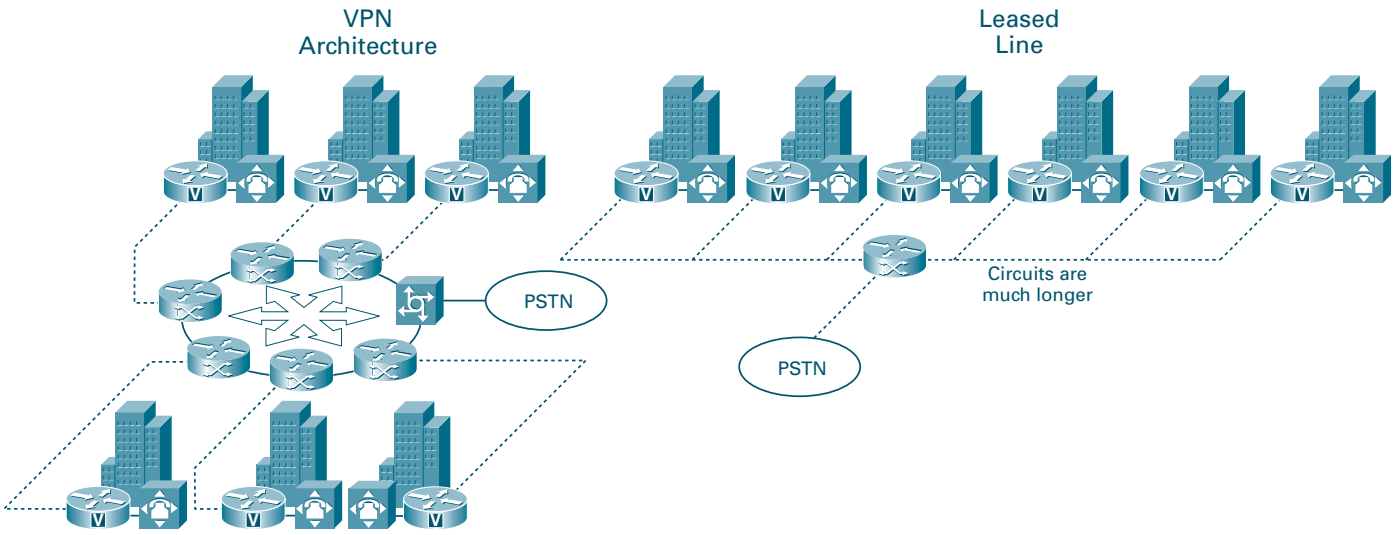
Regardless of which of the above reasons justified a PSTN Gateway deployment, service providers can use the same gateways to carry voice over their IP backbone. Voice is transited between any two PSTN Gateways and this is therefore known as Transit. This service is useful to service providers currently using a TDM network for their voice traffic as it allows expansion without further investment in TDM equipment and makes better utilisation of their bandwidth. The PSTN Gateway's ability to support multiple services means that any gateway can be used to access the PSTN. The routing is configured so each service will use the most appropriate gateway for each call, sharing capacity and reducing the cost. The savings can either be retained or used to expand to provide greater coverage. Transit, which involves routing the call to the best gateway, is also sometimes referred to as a Virtual Trunking Solution. Trunking on the other hand is simply replacement of point-to-point links.
Support for H.323, SIP as well as TDM interconnects using SS7 or PRI makes the PGW 2200 an important asset in interfacing VoIP and TDM networks. In many cases service providers with a TDM network will deploy PSTN Gateways themselves but new service providers may simply choose to buy service or capacity on a shared basis from others service providers either directly or via a Clearing House.

2.2 Voice VPN

Any business with more than one site normally communicates between sites with both voice and data. Within a single company sites are traditionally interconnected in one of two ways. For data, point-to-point leased lines are most common but ISDN is also used. Separate leased lines or the PSTN is commonly used for voice.

There is a big difference between leased lines and using a public network, the most important point being leased lines are charged according to distance and speed while the PSTN is charged primarily on a per minute of use basis. Users therefore make a choice based on their expected usage, between the PSTN and leased lines based on which is most cost effective (for them).

Figure 2-2: VPN versus Leased Line Architecture.



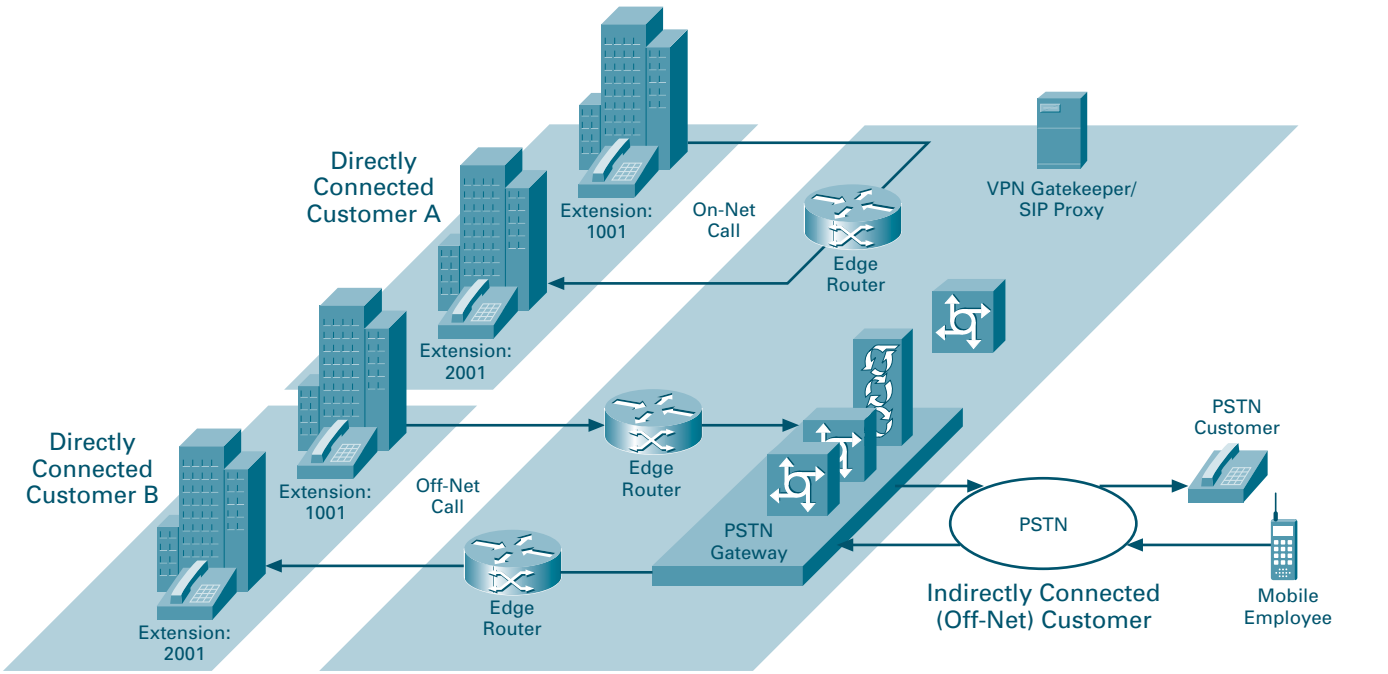
In many cases leased lines will be most cost effective, in others cases the PSTN will win. As always the cost is only one consideration and other factors such as security and increased functionality may also make a leased line approach more attractive.

There is a third option that combines the advantages of both. Service provider based Virtual Private Networks or VPNs as they are commonly known allows each site to connect at a point near to them to a shared core, whilst maintaining the same connectivity provided by the leased lines. Connecting to a local point significantly reduces the cost of the leased lines (distance based charging). The core of the VPN then provides the switching. Where multiple companies share the core to further reduce costs the service provider segregates each companies data. As shown in the following diagram, providing switching in the core also reduces access costs as each site can talk to each other over a single connection rather than having a hub and spoke or multiple connections.

VPNs are not a new concept and many service providers provide them today, although most are for data only. Where voice VPNs are provided they are normally separate and TDM based.

From the customer's point of view, the increasing demand for businesses to improve operational efficiency and continual restructuring results in a 'do more with less, (with greater flexibility)' attitude. Add to this increasing demand for new services such as 'Video on Demand' based training and collaborative working to improve efficiency create an even greater demand on connectivity. This results in a real opportunity for service providers to provide an integrated Voice and Data VPN.

Figure 2-3: Voice VPN.



2.2.1 Voice VPN Overview

In their simplest form, a Voice Virtual Private Network (VPN) provides a business with a cost effective means of routing voice calls between sites. This is normally achieved by creating a private dial plan where each site can dial another site by dialling a site code and extension. Alternatively, a consistent numbering plan is used where an extension number is unique within the company and the VPN knows where they are located. The VPN may also allow access directly to and from the PSTN as well.

The diagram above shows the basic call types that can be made using a VPN. Terms such as On-Net and Off-Net are used to refer to customers directly connected to the VPN and those connected via the PSTN.

Various functions in addition to basic calls are normally supported. The diagram in Figure 2-3 shows some of the call types that are normally supported:

1. Calls between sites of a single company are known as On-Net to On-Net calls.
2. Calls from any site to the PSTN are known as Off-Net calls.
3. For calls from the PSTN two options are available. An access number can be used that allows the caller to authorise themselves and then route within the VPN, this is known as Off-Net to On-Net or DISA (Direct Inward Station Access). Alternatively Direct Inward Dialling (DID/DDI) can be used.

Convenience for users is a major benefit but normally VPNs focus on providing significant cost savings. A VPN keeps calls on the service provider's converged network and uses least cost routes for calls to the PSTN. Some service providers offer use of the VPNs on a cheaper per minute call charge basis while others offer unlimited On-Net calls for a fixed fee, emulating the cost structure of a leased line based network.

A service provider that chooses to provide a Voice VPN based on IP has a number of advantages over a traditional TDM Voice VPN. A major advantage is the ability to offer the combined delivery of both voice and data significantly reducing the cost of access, often a large component of the running costs. Other advantages include the ability to dynamically allocate bandwidth between all services reducing the total bandwidth required. In addition to the ability to reduce costs, a service provider can add value in terms of providing management and administration and allowing use of shared components, with security between customers.

Cisco's Hosted Business IP Telephony VPN Service allows a service provider to offer VPN Services to multiple customers; each of which will have what appears to them as their own independent and fully configurable VPN. As this is a hosted solution, the customer gains all the benefits of a VPN without the capital expense and operational expense of maintaining the network. Combining a VPN with some of the other options explained in this document allows a service provider to build an integrated solution, offering a complete service without the cost of a PBX on every site.

Voice VPN Services	
PSTN Dial Plan	This includes options for access codes and routing restrictions. This covers basic break out to the PSTN but can also be used to give different users different privileges for international or long distance calls.
Private Dial Plan	Every customer can define their own private dial plan to meet their specific needs for location and extension numbers. Each private dial plan is independent of the others so it is possible to have the same number in more than one customer. This is known as overlapping dial plans.
Mobile Dial Plan	This extends the private dial plan to include employees' mobile phones. This can be done as a simple translation to the mobile's PSTN number or in collaboration with a mobile service provider.
Digit Manipulation	Digits can be deleted, replaced or added based on any call parameter. This can be used to ensure Calling Party numbers are always valid and meaningful even when calls are routed between public and private networks.
Least Cost Routing	Routing selection can be based on least cost routing lists. These can be set up by the service provider to route the call over their own backbone network or using the cheapest wholesale carrier for each call. Depending on the service provider's pricing package, these savings may or may not be passed on to the Customer.
Time of Day Routing	Routing selection can be based on the time of the call. This can be used to take advantage of off-peak rates or to route calls to different geographic locations to match working hours across different time zones.
Mandatory Services	Special call types can be defined to handle Emergency Calls or Information Services such as Directory Enquiries.
Caller/Calling Party ID	Called and Calling Party IDs are fully supported VPN Specific CDRs can be generated to improve cost allocation.

2.2.2 Voice VPN Services

One of the key advantages of a hosted Voice VPN service is that it allows easy configuration of the services from a central location. It is possible to develop a VPN solution that exactly meets a customer's specific requirements with the confidence that it will be simple to maintain as their requirements evolve. Whilst there are many different configurations possible, the main building blocks for most Voice VPN customers are as follows:

2.3 IP Centrex

A Centrex service provides similar features to a customer premises based PBX but is delivered from the service provider's central exchange. Rather than having customer premise equipment providing call transfer, call hold and conferencing, these functions are delivered by the service provider.

One benefit of centralising these functions is the enterprise is freed from the complexities and cost of managing their own voice services. Instead of making capital investments and having to maintain PBXs, the enterprise is delivered a flexible business telephony service where users can be added as required on a per line rental basis.

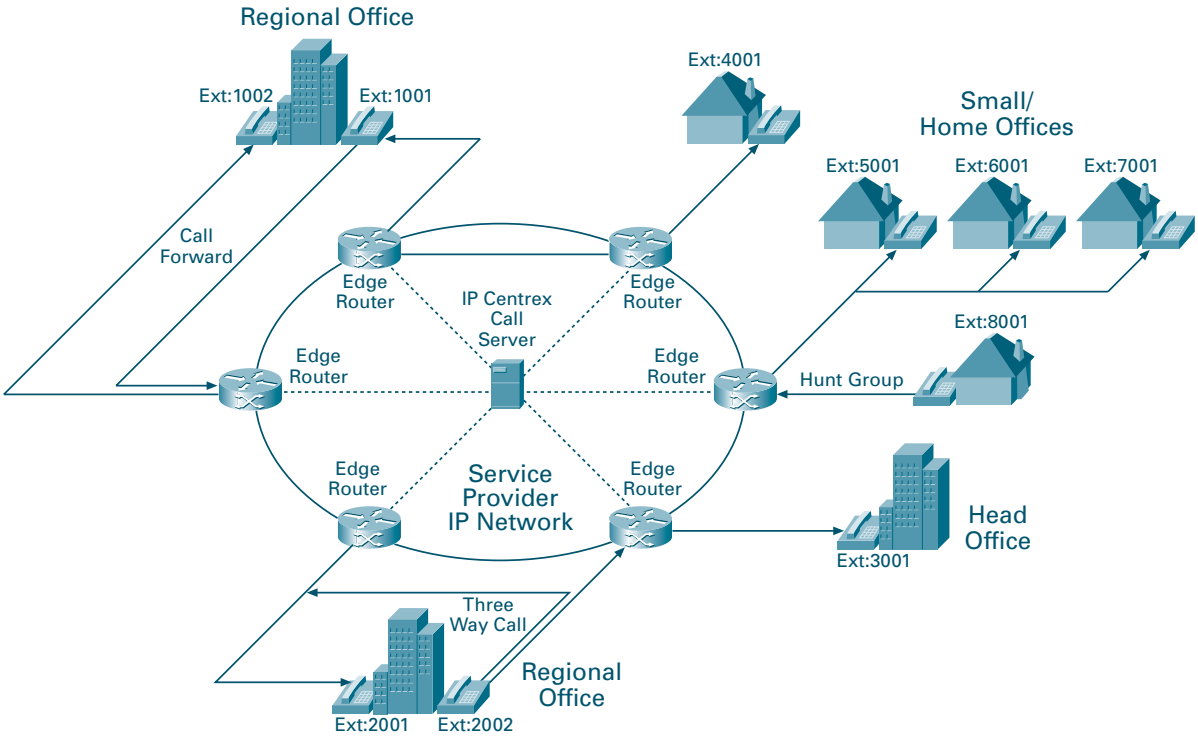
Despite the compelling business advantages of outsourcing the enterprise's telephony requirements via Centrex, the service has never been broadly accepted in Europe. Originally marketed as a managed service to large enterprises, Centrex has gained a larger level of acceptance with small to medium business customers.

This is thought to be because TDM Centrex has sometimes failed to provide all of the features that an advanced PBX can provide and has suffered from the lack of per customer administration functions. TDM Centrex also requires dedicated circuits to be connected to the customer site from the service provider for each line, although in some cases concentrators are used. This increases the cost and also almost eliminates a competitive offering from providers not owning the 'last mile' access to business customers.

IP Centrex builds on the benefits of the TDM Centrex solution but adds additional functionality and improved administration and management control. Most importantly IP Centrex delivers the benefits of data and telephony integration all the way to the desktop allowing a single circuit to support multiple services and multiple users.

Figure 2-4: IP Centrex

The diagram below shows a typical IP Centrex configuration with some basic call features:



The diagram shows how the call control is based in a central location so that it can control the gateways that will carry the voice calls. Examples are shown of a call being forwarded, a three-way call being set up and a single call initiating a hunt group search for an available line. All of these functions are under the control of the IP Centrex Call Server. This centralised configuration also allows easy administration of the services. Depending on the customer requirements there can be a number of different levels of administration. These can range from the user activating features such as call forward through to department or company wide definition of hunt groups and conference calling facilities.

The advantages of IP Centrex are:

- Support for native IP-endpoints (e.g. Cisco 7960 IP phones) so businesses no longer have to install and support separate cabling plants for their voice and data networks.
- Moves, adds and changes are greatly simplified and are in the control of the user. Changes in user profiles, class of service, addition/deletion of users can all be controlled by the business directly, for example, through a secure web page. This reduces operating expense costs for the service provider.
- Feature rich user experience by delivering data content directly to an IP phone. Services such as dynamic user directories, stock prices, web portal access to frequently used services can all be presented to the IP phone. Features are simple to invoke through IP phone soft keys and integration with PC productivity applications, such as calendaring, email, and contact management software is easy. Features are invoked by pressing soft keys that can be dynamically changed through out the call rather than through complex 'star' commands used in traditional Centrex services.
- Features can be customised either by the end user or by the service provider. Customisation by the service provider can be sold as a value added service to end users or market segments.

2.3.1 IP Centrex Services

The IP Centrex service can deliver call features at any stage of a call, from call set-up, during the speech phase through to call clearing. The following are examples of the most popular IP Centrex features:

IP Centrex features:	
Set-up Stage Actions	Call Forward (unconditional, no reply, busy and rules based – time of day or caller ID).
Call In Progress Actions	Call Waiting, Call Hold, Call Transfer, Call Park and Pick Up.
Multi-Party Calls	Conference, Three Way Calling.
Network Services	Ring Back When Free.
Follow Me Services	Hot Desk and Remote Forwarding.
Hunt Groups/ACD	Sequential, random, simultaneous automatic call distribution (ACD).

A detailed description of the IP Centrex service can be found in Section 5.

2.4 Value Added Services

One of the key advantages of using an IP Network to deliver hosted services is the ease with which new services can be added. Cisco's hosted solutions use open standard protocols to further enable the rapid development of advanced applications. The general term for the functionality that these new applications provide is Value Added Services. The following diagram shows how new applications can be added and provides some examples:

Figure 2-5: Value Added Services

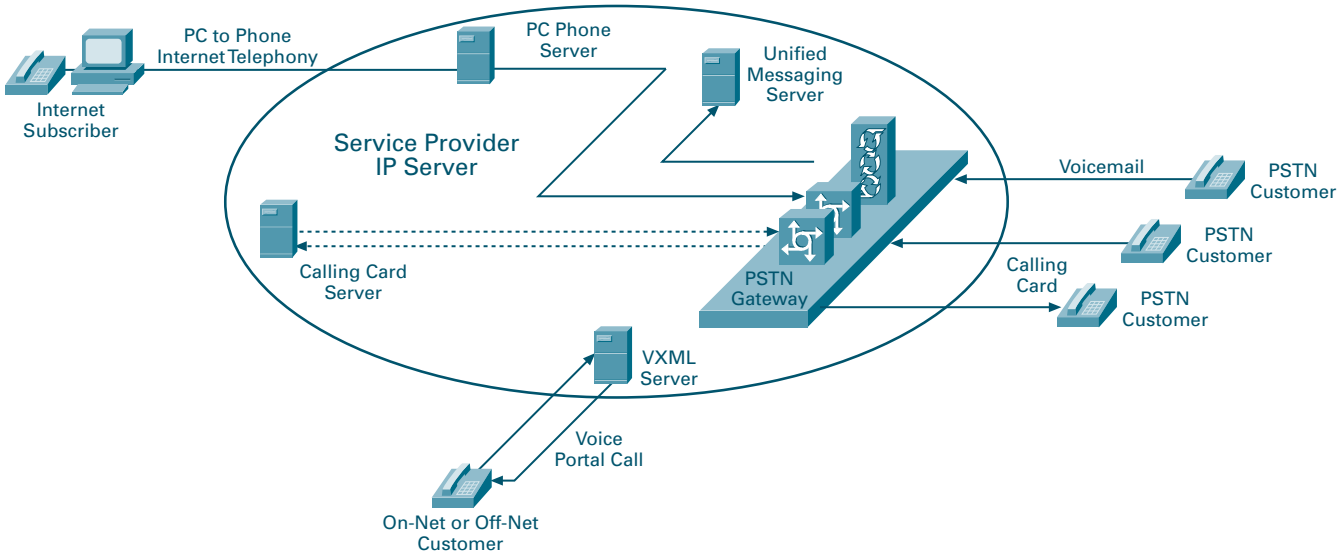


Fig 2-5 shows how new services can be added by deployment of the appropriate server within the service providers core IP network. The server, which may be an H.323 Gatekeeper or a SIP Proxy Server depending on the configuration, is used to perform authentication and call control functions. Some examples of these services are as follows:

2.4.1 Unified Messaging

Unified Messaging (UM) provides voicemail-type features but allows storage and retrieval not only of voice messages, but also email and fax. Notification of messages waiting can be via SMS to a mobile phone or by a message-waiting indicator on a fixed phone. Messages can be retrieved using a phone, email or a web browser on a PC or from a mobile device. This offers genuine multimedia communication storage, with choices for notification and retrieval. Being based on IP technology, UM can add enhanced applications such as personal calendar notifications, paging notification for urgent messages, or other services enabled via web, voice and IP data integration. It also has the significant advantage of being location independent via the Internet.

2.4.2 Voice Portals

VoiceXML can be used to transport a combination of text and audio information between devices. This enables the creation of Voice Portals that can receive requests from voice band data (tones or voice recognition) and perform audio actions such as the playing of voice scripts. VoiceXML is often described as the voice equivalent of the HTML used by web browsers. It is particularly suitable to mobile users who either can't access the web browser services on the small screen of a mobile phone or are using a mobile phone in a car with a hands-free kit.

Service providers can generate revenue by hosting Voice Portals to provide interactive services on behalf of business customers. For example, they could host voice activated bank services or a ticketing service for cinemas, or location based directory services, such as finding the local branch of a national restaurant chain.

2.4.3 Calling Card Platform

A Calling Card Platform can be used to provide authorisation and usage information for both post and pre-paid calling card services. Customers connect to the service provider via the PSTN Gateway and after authorisation the customer can make calls either to a Corporate VPN or to the PSTN using the service provider's backbone network to benefit from reduced call charges. This can be offered as part of a hosted Voice VPN service to give the customer a corporate calling card that provides the employee with access to the corporate voice VPN and long distance services.

SIP:

Session Initiation Protocol (SIP) is a relatively new protocol designed to integrate voice into the data environment. For example, email or URLs can be used for addressing calls in addition to E.164 numbers. SIP is specified in RFC 2543.

SIP end points are known as User Agents. Routing decisions and billing is typically implemented in proxy servers. The proxy server function is analogous to the gatekeeper in H.323 signalling. User Agents therefore send setup messages (known as 'Invites') to the proxy server for routing to its destination.

Cisco's VoIP gateways including the AS5000 range and IP phones support SIP. Also, the PGW2200 media gateway controller supports SIP signalling which allows media gateways using MGCP such as the MGX8850/VISM to terminate calls from SIP end points.

2.4.4 PC to Phone Internet Telephony

A service provider can use their connectivity to the Internet and their PSTN Gateway to offer Internet users the ability to make Internet Telephony calls outgoing through the PSTN Gateway. A gatekeeper can be used to perform authentication and record call usage. This service can be targeted at business customers with a mobile workforce who can use the service to make cheap international telephony calls from their laptop PCs for the cost of a local Internet call. Home users accessing the Internet with both Broadband and Dial-up are starting to use these services as well. Examples include Net2Phone and Microsoft's Messenger service MSN. As ISP's are currently making wireless broadband connectivity available in Internet café's, airport lounges and hotels using technology such as Cisco's Aironet® solution, PC to Phone Internet Telephony is becoming truly location-less and mobile.

These examples demonstrate some of the possible Value Added Services that a service provider can offer based on an IP core network. Unified Messaging and Voice Portals are discussed in more detail in Section 6.

2.5 Overall Solution

By delivering these services using an IP core network, the service provider can combine and add functionality to a network that is based on next generation technology. The following diagram shows how the different elements can be combined.

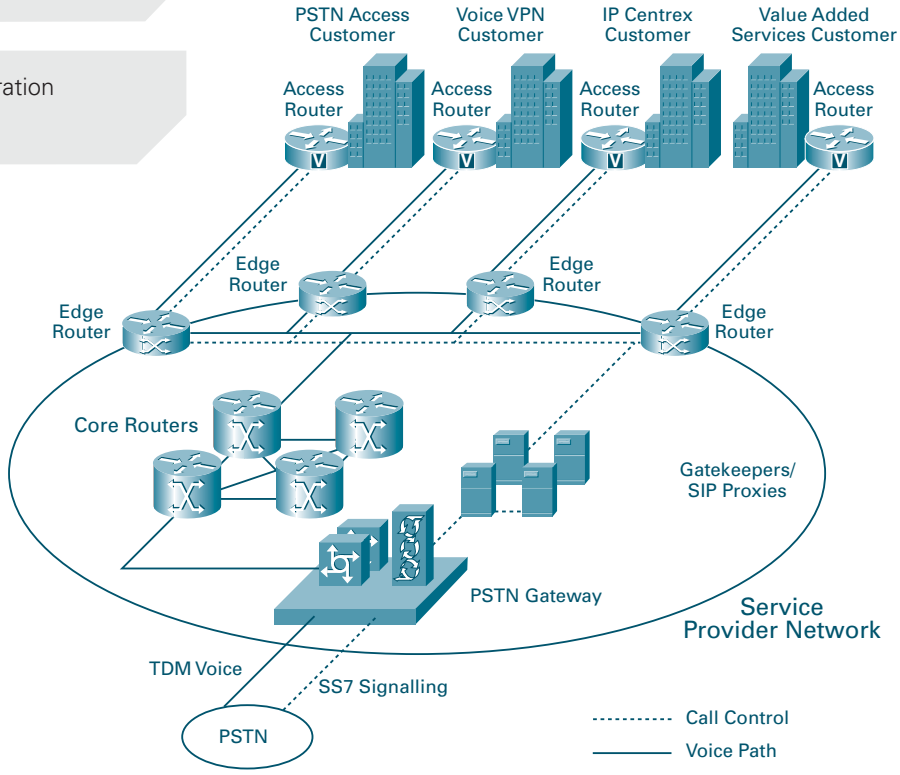


Figure 2.6: Configuration Summary

H.323 Overview:
H.323 is an umbrella recommendation from the ITU-T that defines the delivery of audio, video and data over a packet-based network. It defines the entities, their functionality and the interfaces between them. It includes the packetisation and compression of audio and video along with the call control and signaling. Version 1 was approved in 1996 and version 2 was approved in 1998. The H.323 family of recommendations includes the following areas, amongst many others:

- H.225 Call Signalling Protocols and Media Stream Packetisation.
- H.245 Multimedia Signalling.
- H.235 Security and Encryption.
- H.450 Supplementary Service.

H.323 Elements: H.323 defines the following key elements that together make up an H.323 Zone.

- **Gatekeeper:** Terminals are registered with the Gatekeeper which then looks after the Address Translation to and from E.164 and IP. It also looks after call control and routing.
- **Gateway:** The Gateway provides media and signaling conversion between packet and circuit switched elements (PCM to RTP).
- **Terminals:** This is the user end-point and can be an H.323 IP Phone or an H.323 compliant PC Client.

H.323 Call Stages: There are three main stages that enable a voice call to be completed. These are all completed over separate channels meaning that the call control is completely separate from the media channel.

Registration: The terminal or end-point registers with the Gatekeeper when it joins the network. RAS (Registration, Admission Control and Status) Signalling is used as defined in H.225.

Call Establishment: The terminal or end-point requests the call setup. The call may be requested via the Gatekeeper or directly between the end-points.

Media Negotiation: The two end-points use H.245 to negotiate the media characteristics and then the call is transported using RTP. RTCP can be used to measure the quality of service.

The Hosted Business IP Telephony solution has all the advantages of a distributed IP network in that it can be scaled at a component level. Gatekeepers, PSTN Gateways, Access Gateways and core routers are all individually scalable to meet increases in customers and traffic.

2.5.1 Cost Benefits

As well as generating new revenue streams through value added services there are also capital and operational cost benefits from IP Telephony networks.

Reduced Bandwidth: The integration of voice and data and the efficiencies of a packet switched network result in an overall reduction in capital costs compared with an equivalent TDM network.

Reduced Size and Power: IP network elements tend to be physically smaller than TDM network elements so there are further cost savings in terms of floor space, power consumption and air conditioning.

Modularity: IP network elements tend to be more modular than TDM network elements so it is easy to scale the network gradually to meet revenue-generating opportunities rather than the over-provisioning that is often associated with large TDM switch equipment.

2.5.2 Quality Of Service

There are now many techniques available to ensure that voice carried over IP maintains a high quality of service. These include packet labelling and classification, weighted priority queuing and provisioning methodologies. Further details of these can be found in Section 7.

2.5.3 Security

Security of both data and voice information can be ensured by a number of methods to prevent data interception and falsification. MPLS can provide network wide security ensuring that separate customers only have access to their own voice and data. IPSec can be used to encrypt data sent on a point-to-point basis. Further details of these can be found in Section 7.

2.5.4 Billing

IP Telephony components provide call usage information that can be fed to a mediation platform in the same way as TDM switches do. This provides identification of the caller, destination and the relevant timing information. In addition to this, IP Telephony components can also provide additional information such as the type of service invoked. In a converged, multimedia environment this can be used to build innovative pricing models that differentiate service types to maximise revenues.

3 Technical Description – PSTN Access

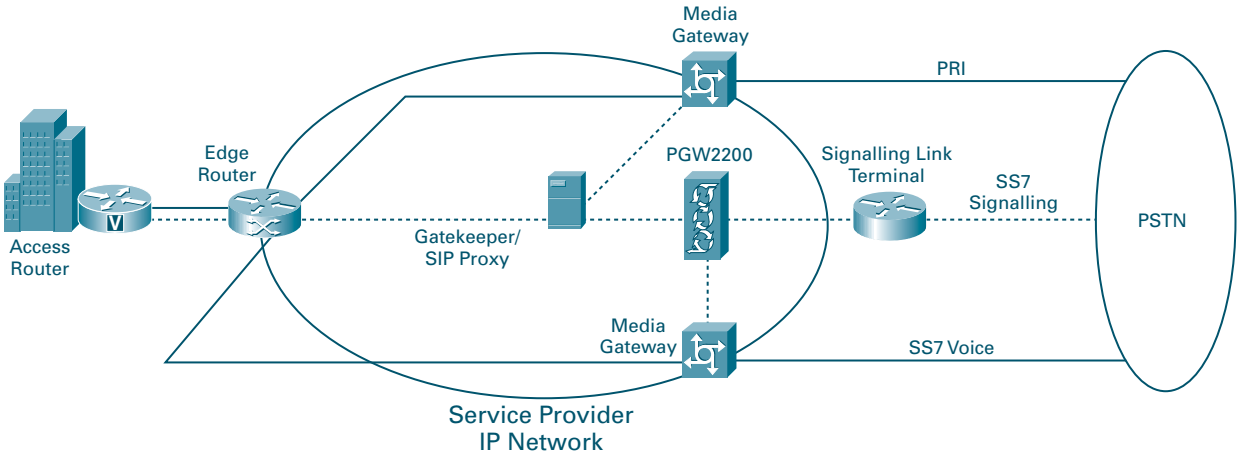
Interconnection with the PSTN enables a service provider to offer incoming and outgoing telephony services across VoIP and PSTN network domains. The Cisco PGW 2200 PSTN Gateway solution bridges these network domains by interworking voice, signalling and routing functions.

Voice channel interworking involves providing a TDM based interface such as an E1/T1, packetising the voice and then passing this out over an IP interface. Optionally, the voice may be reformatted or compressed using codecs and application of echo cancellation where necessary. Class of service parameters are also set here to ensure that the packetised voice is given the necessary priority over data across the IP network.

Signalling channel conversion involves mapping information to and from PRI or SS7 to the equivalent parameters in H.323 or SIP. The PGW 2200 can also handle PSTN to PSTN calls and VoIP to VoIP calls allowing it to act as common element for management, security and billing.

The following diagram shows a high level VoIP network architecture using a PSTN Gateway.

Figure 3-1: PSTN Gateway Components



PRI vs SS7 Interconnect:
The incumbent operator usually offers PRI as a retail service as PRI is aimed at connecting PBXs to the PSTN. Where deregulation is not yet complete it provides a quick and cost effective method to connect to the PSTN. However, call tariffs are usually higher than using SS7.

SS7 (CCS7 or C7) is usually offered as a wholesale service and where deregulation has taken place it is usually mandatory that the incumbent operator offers SS7 interconnects to license holders. Interconnects usually require specific PSTN functionality such as CLI delivery and restriction, malicious call identification and emergency call handling to be provided by the interconnecting operator.

3.1 SS7 Interconnect

The PGW 2200 PSTN Gateway provides full SS7 interconnect functionality. It consists of a Media Gateway Controller combined with one or more Media Gateways and Signalling Link Terminals. The Media Gateways perform all of the voice conversion functions and are controlled by the Media Gateway Controller using Media Gateway Controller Protocol (MGCP). The Signalling Link Terminals handle layers one and two (MTP1& MTP2) of the SS7 signalling and pass layer three and above to the Media Gateway Controller.

Since the Media Gateway Controller can manage multiple Media Gateways and SLTs, this configuration is extremely efficient for use at multiple Points of Presence (PoPs). The Media Gateway Controller can be located in a central location and only the media gateways and SLTs need to take up valuable footprint in the PoPs.

Media gateways that can be controlled by the PGW 2200 include AS5350, AS5400, AS5850, and the MGX 8000 Series including the MGX8850 and MGX8230.

3.2 PRI Interconnect

PRI, (Q.931) can be terminated by the PGW 2200 PSTN Gateway, the signalling being back-hauled from the media gateway to the Media Gateway Controller over IP.

If SS7 interconnection is not required, PRI, CAS, R2 and QSIG circuits can be terminated directly on Cisco Media Gateways without requiring PGW 2200 control. Media gateways supporting this include the Cisco 2600 series, 3600 series, AS5350, AS5400 or AS5850. As the same gateways can be used under control of the PGW 2200, they can continue to be used if the service provider chooses to migrate from PRI to an SS7 interconnect.

The PGW 2200 interoperates with Gatekeepers and SIP Proxies in H.323 and SIP environments which can control access to IP endpoints and can enable further applications in the VoIP network. Customer Premises Equipment and the Customer Access configuration are discussed in more detail in Sections 8 and 9.

SS7 Interconnect Testing:
Interconnecting with service providers with significant market share is usually highly regulated and most countries enforce a strict approval process that must take place before traffic can be carried over a regulated interconnect.

Typically, this will involve an approval stage where lab testing is carried out on a product basis to check that it meets the functional requirements. A subset of these tests is then carried out on site for every new circuit that will be brought into service. The aim is to ensure that calls can be handled in a consistent manner and that universal service requirements are met.

The PGW 2200 supports over 80 SS7 protocol variants, and has completed SS7 approval testing in many countries. This greatly reduces the time to deploy, since only basic interconnect testing is required for deployments in approved countries.

The PGW 2200 is also fully compliant with the ETSI, ITU and ANSI ISUP standards that are the predominant protocols for international carrier to carrier interconnect.

3.3 PGW 2200 PSTN Gateway

As well as performing the core gateway functions of signalling and bearer conversion, the PGW 2200 must be able to carry out analysis and routing functions specified by interconnect requirements. The PGW 2200 has a local analysis and routing ability equivalent to a TDM switch. Number analysis permits modification and analysis of A and B party numbers, as well as other parameters such as time of day and cause codes. Ultimately the call destination is determined along with an associated route list and trunk groups.

3.3.1 Calling Line Identifier

The interconnect agreement between operators for connection to the PSTN specifies the requirements for the handling of the Calling Line Identifier (CLI). In particular, some countries have strict rules to ensure that the CLI is not sent to the destination if the caller does not want it to be sent. For example, in the UK the caller can use the '141' prefix to restrict the sending of their CLI. These services are referred to as Calling Line Identifier Restriction (CLIR) and Calling Line Identifier Presentation (CLIP). It is also necessary for the PSTN Gateway to translate any internal CLI that may be generated by a PBX to the CLI that is meaningful in the PSTN. This is particularly important for calls to the Emergency Service and for Malicious Call tracing.

3.3.2 Number Portability

When a service provider has directly connected customers with their own number range there is usually a requirement from the national regulator that the customers are able to keep the same number range even if they change to a different service provider. This same regulation will enable an IP Telephony service provider to provide telephony services to an enterprise business without the inconvenience of changing their number range. The PGW 2200 can implement the two main number portability mechanisms (Onward Donor Network Routing and All Call Query Number).

3.3.3 Emergency Calls

Emergency calls must be given special treatment to ensure that they are routed to the nearest Emergency Call Centre and that accurate information is provided about the originator. Digit analysis on the PSTN Gateway can identify the emergency numbers (112, 999, 911 etc.) and digit manipulation can be used to add a location identifier prefix or suffix if required. The call can then be routed on a dedicated trunk to ensure call completion to the emergency service.

3.3.4 Malicious Call Handling

The PSTN Gateway provides the capability to terminate and originate Malicious Call Identifier requests when required by PSTN interconnect regulations.

3.3.5 Supplementary Services/Feature Transparency

Supplementary services such as call redirect are mapped through from SS7 to VoIP signalling (H.323 or SIP). The PGW 2200 supports ISUP transparency between multiple PGW nodes across an IP network. This is particularly important for PSTN transit applications over IP. The PGW 2200 fully supports regulatory and interconnect requirements at the network boundary.

Universal Port:
A Gateway that supports universal port architecture has the ability to answer voice, fax and Internet dial calls by simply running different algorithms on the DSPs within the box.

A universal port gateway, also known as UP, ASAP (Any Service Any Port) or universal DSP is therefore much more cost effective in a mixed environment.

3.3.6 Signalling Link Terminals (SLT)

Signalling Link Terminals are used to terminate the physical SS7 links. The SLT is based on the Cisco 2611 or 2651 modular router platform and supports the following physical interface options:

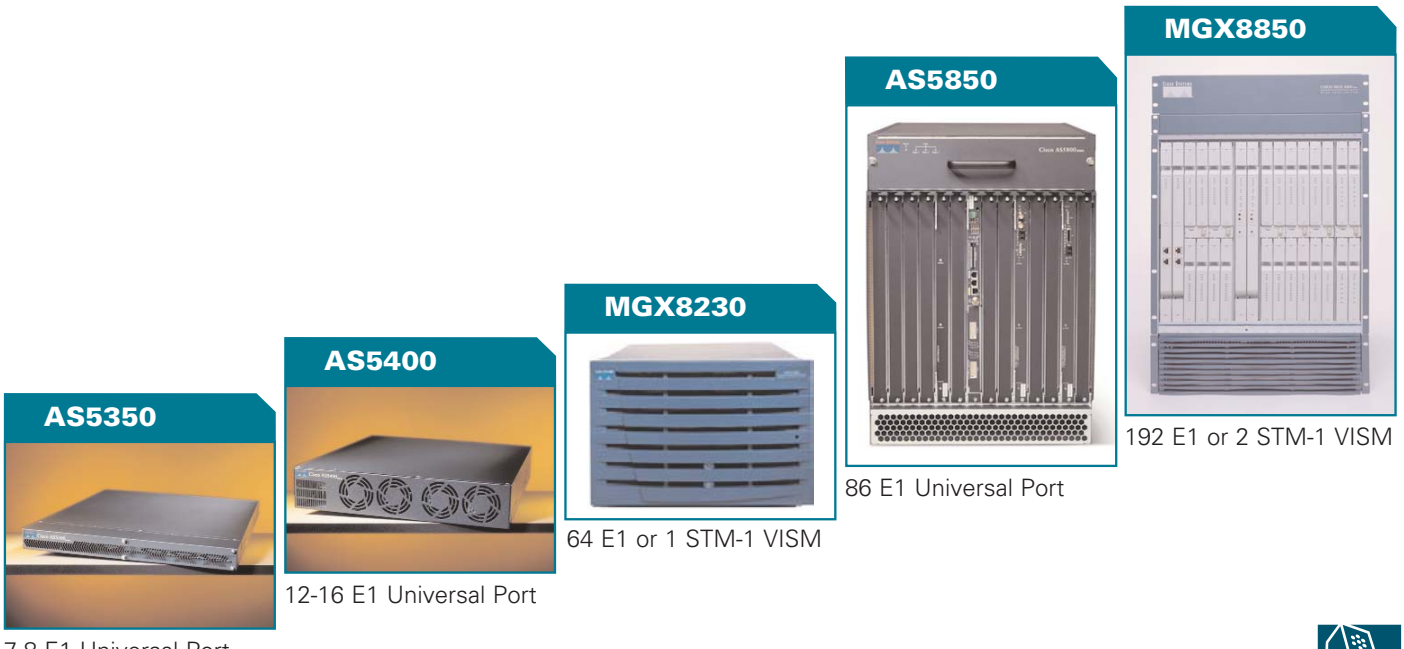
- E1
- T1
- V.35
- RS-449
- RS-530

The SLT can support two (2611 platform) or four (2651 platform) 64kbs/56kbs links carried over any of the above physical interfaces. The SLT terminates the physical layer (MTP 1) and layer 2 (MTP 2) of the SS7 protocol stack and only send layer 3 (MTP 3) and above protocol data units over IP to the PGW 2200. This is both efficient in terms of bandwidth and processing but also provides redundancy as well. In many countries the signalling is embedded as a channel in the voice trunks, where this is the case the SLT separates the voice and signalling at the local media gateway site.

3.4 Media Gateways

Cisco offers a range of media gateways varying in size, performance levels to meet the requirements of each site or point of presence. At the lower end of density/capacity scale are the gateways used for deployment on a per customer, on premises basis. As you move to the core of the network the capacity/density requirements increase, these gateways are used to connect to the PSTN and are often termed trunking gateways.

Figure 3-2: Cisco Media Gateways



Cisco's larger gateways fall into two categories, those with local call control capability and those requiring a call agent such as the PGW 2200. Gateways such as the AS5350, AS5400 and AS5850 can handle PRI signalling directly and interface to SIP and H.323. These gateways can also be controlled by the PGW 2200 using MGCP and have universal port capability enabling termination of dial up data connections and voice services on the same port. The MGX8230 and MGX8850 work in conjunction with the PGW2200 to provide higher capacity for large voice-only applications.

3.4.1 AS5350, AS5400 and AS5850

The Cisco AS5xxx family of Media Gateways use a Universal Port architecture. This allows the gateways to deliver what is known as Any Service Any Port (ASAP). The universal port architecture supports voice, ISDN dialup, Modem dialup and a number of voice services such as IVR and VoiceXML on a call by call basis.

The only difference between the gateways within this family is the capacity and redundancy of each product. The smallest, the AS5350 supports between one and 8 E1/T1 interfaces in a modular 1RU (44.5mm/1.75" high) unit. The AS5400 is 2RU high and provides 7 modular slots compared to 3 in the AS5350. This allows the AS5400 to support more E1/T1 interfaces or the higher density CT3. The exact capacity depends on the configuration but a 16 E1/T1 configuration supporting 480/496 simultaneous calls is commonly used. The AS5400 with its higher capacity can also be configured with redundant power supplies and AC and DC power is supported across all the gateways.

The AS5850 is the largest universal port gateway in the AS5000 family and supports up to 86 E1/T1 interfaces or multiple CT3 interfaces. Some service providers prefer the larger capacity of the AS5850 chassis while others prefer to use groups of AS5350 or AS5400s. The AS5850 is 14 RU high and can be configured with redundant power and control logic to provide very high availability for up to 2688 simultaneous calls.

3.4.2 MGX 8230 and MGX 8850

The Cisco MGX 8230 and MGX 8850 are chassis based wide-area edge switches represents the next generation in high-capacity edge switches and can support variety of interfaces. For voice, the most interesting is the VISM described in the next paragraph but other WAN and LAN, ATM and Ethernet interface cards are supported. This enables large-scale multi-service Points of Presence (POPs) to be built. Whilst the MGX series are very flexible they are often deployed as a voice only gateway and can support up to 192 E1s in the MGX 8850 or 64 in the MGX 8230, channelised STM voice interfaces are also supported allowing 63 E1s per STM-1 to be presented directly from the SDH network without the need for Add/Drop Muxes.

3.4.3 Voice Interworking Service Module (VISM)

The Cisco Voice Inter-working Service Module (VISM) is the high-performance voice module for the MGX 8000 series. The module delivers toll-quality voice, fax, and modem transmission over both ATM and IP with built in echo-cancellation, voice-compression, and silence-suppression techniques. In conjunction with a call agent such as the PGW 2200 the VISM supports incoming and outgoing voice interconnections with TDM networks. The VISM card, like the other gateways supports echo cancellation, Continuity Testing (COT) and voice/fax handling while the PGW 2200 deals with the signalling and call control and provides bearer control commands to the VISM using MGCP.

Each VISM supports 8 E1/T1 circuits and these can be either SS7 or PRI controlled. For PRI the VISM passes the PRI D-channel traffic to the PGW 2200 call agent over the IP network.

3.5 Billing

Call usage information can be provided in a number of different ways from the PSTN Access solution. This enables easy integration with existing mediation systems.

A Radius server can be used to collect call usage details from media gateways such as the AS5000 series or from the Gatekeeper/SIP Proxy. Where media gateways are used for access from client sites or networks, the call usage information that they provide can be used to charge as calls enter the service provider network. This is in line with a typical TDM network.

The Gatekeepers and SIP Proxies can also provide call usage information to a mediation system. This method provides information for all calls set up by the Gatekeeper/SIP Proxy irrespective of where they originate.

The PGW 2200 can also be configured to generate full call usage information for every call type that routes through the PSTN Gateway. The PGW 2200 generates Binary Call Detail Blocks (CDBs) which can be converted by the Billing And Measurement Server (BAMS) to a common format such as BellCore AMA Format (BAF). These files can then be read by an existing mediation system. The BAMS is a fully redundant system with active and standby units to ensure billing integrity.

IP networks can provide many more details than just basic call parameters. For example, it can include service type information that can be used to get a more detailed understanding of what services are being used and to allow revenue generation from specific service provision. This could be applied in areas such as video conferencing services and content delivery.

3.6 Security

Security of the PSTN Gateway service is required to ensure that unauthorised users are not able to access the service. This is essential to protect service revenues and to maintain a high quality service for customers.

There are two main mechanisms to provide overall security, application level security and IP level security. At an application level, all users of the service must be registered with the gatekeeper/proxy. The gatekeeper/proxy knows which users are allowed to register and only authorises these recognised users. In addition to this, the gatekeeper/proxy performs a second level of screening every time that a call is placed. These application level checks ensure that only valid users gain access to the service.

In addition to this application level security, there are also IP level mechanisms that protect both the service provider but also the user. Firewalls at the customer premises can be configured to only accept VoIP communications from the validated service provider gatekeepers. Network Address Translation (NAT) also acts as a screening mechanism so that the customer's IP network cannot be addressed directly from the Internet. Intrusion Detection Systems (IDS) provide a further level of security on the customer premises.

The use of MPLS technology in the Service Provider's network is another method of controlling access between the service provider and customer networks. MPLS enables the service provider network to perform as a private network from the customer's point of view. Even though the service provider is operating a shared network, individual customers are completely separated from each other to ensure their complete security.

3.7 Element Management

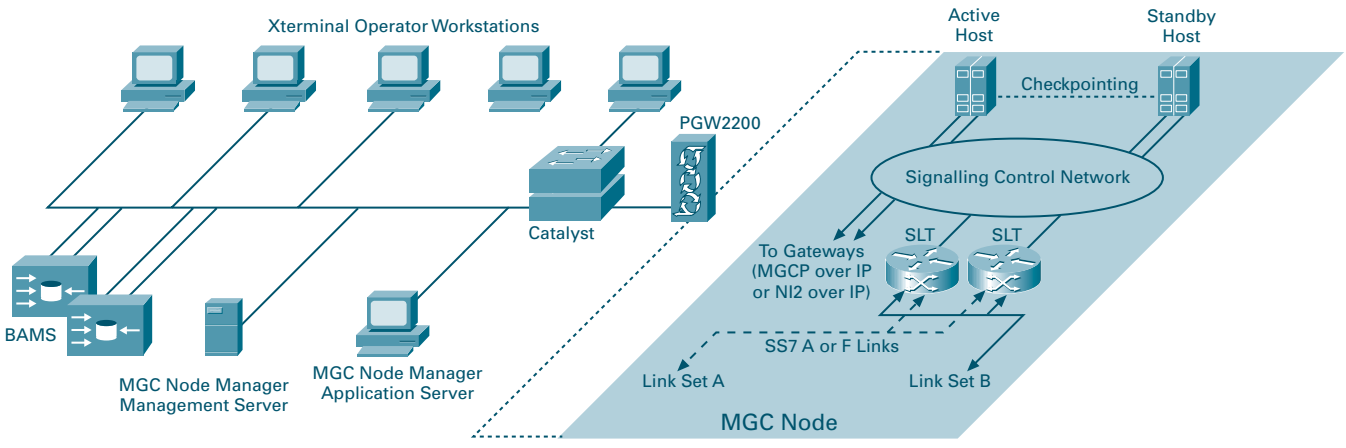
The Cisco Media Gateway Controller Node Manager (CMNM) provides a single interface for Fault, Configuration, Performance and Security management (FCPS) for all elements in the PGW 2200 including the Billing And Measurement Server (BAMS).

The Cisco MGC Node Manager comprises three major components: the management server, the presentation server and the X-terminal operator stations.

- **Management server:** This server is the control centre for the fault, configuration, performance, and security management provided by the Cisco MGC Node Manager. It contains the database for inventory, connectivity, alarm, performance and user access records. It controls all surveillance functions associated with alarm collection and configuration synchronisation, as well as the periodic collection of performance statistics.
- **Presentation server:** This server provides multi-user capability on the Cisco MCG Node Manager. It may include a high-resolution display for a local operator and it operates as a host for up to ten operators.
- **End-user X-terminal:** This terminal is an operator workstation that provides the graphical user interface (GUI) access to all Cisco MGC Node Manager capabilities. X-terminal stations may be network connected to the presentation server to provide Cisco MGC Node Manager access for operators using a generic X-terminal workstation or a PC-based X-terminal emulator such as Reflection X.

Figure 3-3: CMNM Configuration

The following diagram illustrates the relationship between CMNM and the PGW 2200 host.



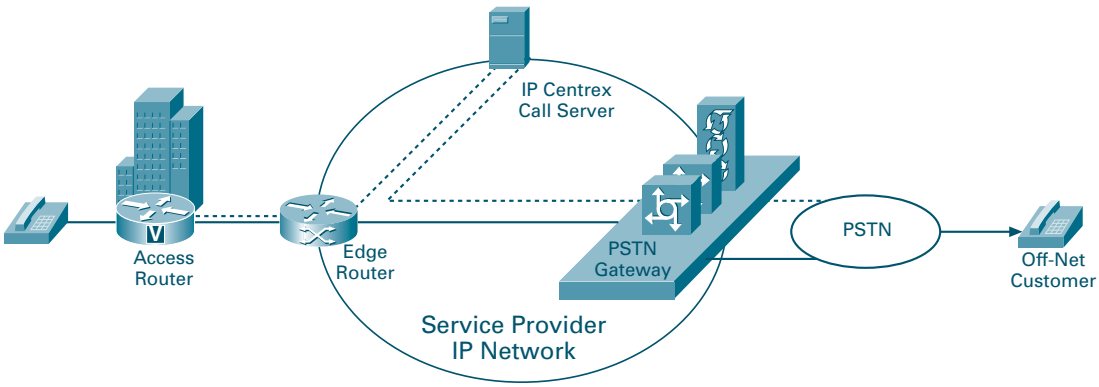
4 Technical Description – Voice VPN

Hosted Business IP Telephony combines the most exciting next generation services to offer a complete business communications package that covers the full range of multimedia services. Not only does this include reliable and high quality voice, video and data transport but also the advanced applications that perform the seamless integration that drives business efficiency. Service providers with hosted services can genuinely differentiate themselves from competitors resulting in significant customer growth and increased revenues.

Multi-service VPNs delivers business customers with complete connectivity between sites, encompassing voice, data and video. This section provides a technical description of how the voice VPN connectivity is achieved within this multi-service environment.

The Voice VPN provides multiple customers with their own multi-site private dial plan over a secure managed network. It has a centralised topology; this is easily scaled and simplifies network wide configuration and maintenance. The Voice VPN often provides users with a web interface to define their own personal options for call diverts and integration with Unified Messaging. The following diagram shows the components required for a hosted Voice VPN service:

Figure 4.1: VPN Components



The component dealing with the routing of calls in the Voice VPN is the VPN Gatekeeper or SIP Proxy. This handles call control, routing, digit manipulation, CLI management and screening for all VPN calls across the network. It analyses the requested destination address and then sets up the call to the appropriate gateway. The Gatekeeper/Proxy also provides call usage information that can be used for billing and cost allocation for different companies, locations or departments.

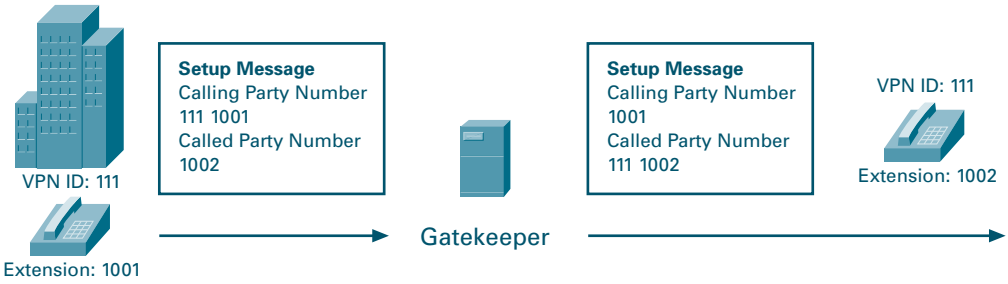
The details of each of the components are described in other sections. For customer premises and the customer access technology options please see Sections 8 and 9 and Section 3 for the PSTN Gateway.

4.1 Functionality

4.1.1 On-Net to On-Net

On-Net to On-Net calling is the basic VPN functionality. Users on the VPN network can dial other users on the network using either the extension by itself or by using an extension preceded by a location code. The following diagram shows how the originating access router prefixes the Calling Party Number with the VPN ID to convert a potentially duplicated extension number to a number that is unique across the network. This means that many different customer groups can have overlapping private dial plans within the same system. The Gatekeeper/Proxy uses this VPN ID to identify the customer and uses the appropriate routing tables to route the call. In addition, the Gatekeeper manipulates the Calling Party Number into a format that can be presented to the far end, and prepends the VPN ID onto the Called Party Number to enable the network to uniquely route it to the destination site.

Figure 4.2: On-Net to On-Net Call



4.1.2 On-Net to Off-Net (PSTN access)

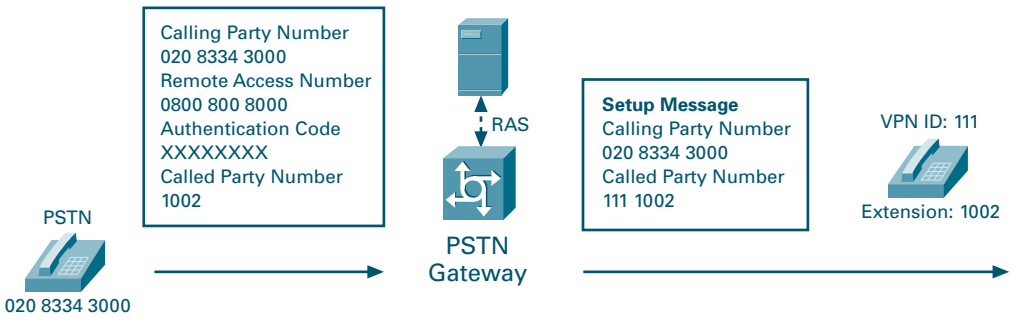
On-Net to Off-Net provides the members of the VPN with access to the PSTN. The Gatekeeper/Proxy selects the appropriate PSTN Gateway and if the originator is part of a Direct Dial Inward (DDI) number range it replaces the Calling Party Number with a DDI number that is valid for the PSTN. The following diagram shows the call flow:

Figure 4.3: On-Net to Off-Net Call

4.1.3 Off-Net to On-Net/Off-Net (Remote Access)

The VPN can be extended to users outside the corporate network by the using the Remote Access functionality of a PSTN Gateway or Access Router. A user with access to the PSTN can dial the PSTN Gateway or Access Router and can be validated by their Calling Party Number or by dialling an Authentication Code. They will then be able to make calls as part of the VPN. This can enable Off-Net to Off-Net calls with extension dialling or Off-Net to On-Net calls to make use of cheaper long distance tariffs.

Figure 4.4: Off-Net to On-Net Call



4.1.4 On-Net to Virtual On-Net

The use of location and extension dialling is not restricted to destinations on the corporate network. Extension numbers can also be assigned to PSTN numbers. This provides the customer with a consistent private dial plan covering all employees even if they are working from home or from a location that has not yet been connected to the network.

Figure 4.5: On-Net to Virtual On-Net Call

4.1.5 Mobile Extension

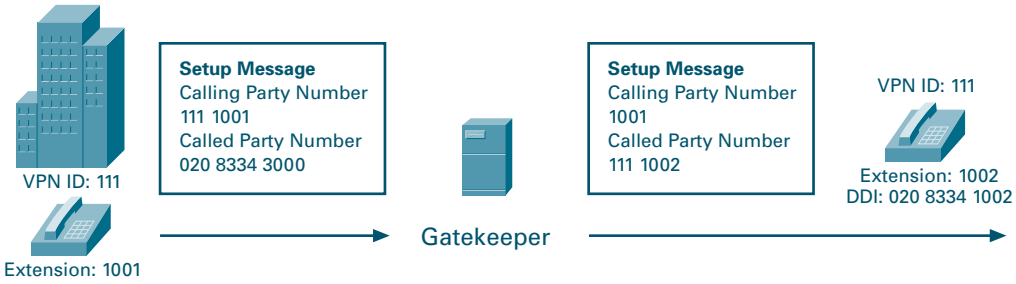
One very effective use of Virtual On-Net dialling is the Mobile Extension service where an On-Net call to a variation of the extension number can be routed to the same user's mobile number. For example, if the On-Net desk phone of an employee is 7 1001 (where 7 is the location and 1001 is the extension), then dialling 8 1001 will be translated by the VPN Gatekeeper and routed to the user's mobile phone via the PSTN Gateway.

A complimentary service for mobile users to use extension dialling to access On-Net can be deployed in collaboration with the mobile operator.

4.1.6 Forced On-Net

The digit analysis and manipulation features of the VPN Gatekeeper can be used to override user's routing selections if they are not the most efficient. For example, if a user dials the full length E.164 number for another company site rather than using the VPN extension, the Gatekeeper can force the call to be routed on the network, rather than treating it as a PSTN destination

Figure 4.6: Forced On-Net Call



4.1.7 VPN Reference Architecture

Cisco has spent a significant amount of effort building a VPN Reference Architecture in conjunction with two large service provider partners. Working together, Cisco has duplicated the partners' network topologies and tested their specific services.

The VPN Reference Architecture supports both Cisco and third party Call Server/Gatekeeper platforms to provide the appropriate Voice VPN functionality and feature set. The Cisco solutions lab has tested with specific partners, to provide a tightly integrated end-to-end VPN service architecture.

4.1.8 Billing

Call usage information is provided directly from the VPN Gatekeeper or SIP Proxy Server. As it provides full details of the caller and the call type it can be used as the basis for billing records at a number of levels:

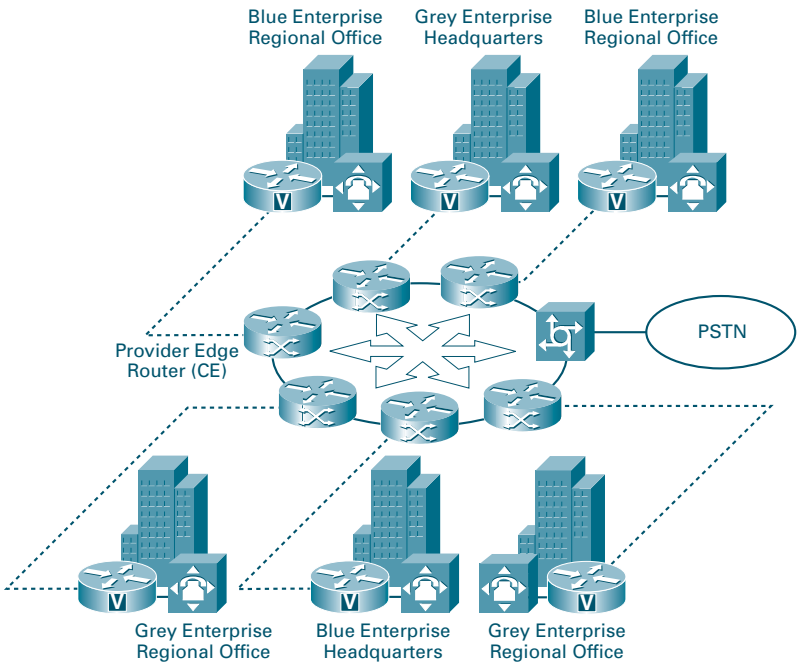
Billing Information	
Corporate Accounting	Provides centralised billing to a multi-site enterprise.
Location Accounting	Provides location specific billing. For example, by office, region, country.
Cost Centre Accounting	Provides a breakdown of calls and call types on a departmental basis for internal accounting.

4.1.9 Security

Security for the Voice VPN is provided at the call control level by ensuring that gateways accept calls only from known gatekeepers, and that gatekeepers only allow known endpoints to register. Mobile IP devices or PCs with softphone capabilities would first register with an authentication server, before being allowed to register with a gatekeeper for access to the Voice VPN.

It is important in a multi-service voice and data VPN environment, that security is maintained at the IP level. It is recommended that the service provider uses either MPLS in the core network or uses IPSec tunnels to provide security and control of access to IP VPN services. The following diagram illustrates how MPLS can be used to provide secure separated IP VPNs to multiple customers.

Figure 4.7: MPLS Network



4.1.9.1 MPLS

In the MPLS environment the Access Router at the customer premises is referred to as a Customer Edge router (CE). The router that the CE connects to in the core network is called the Provider Edge router (PE). A VPN consists of a group of CE routers connected to the core PE routers. Only the PE routers are aware of the VPN. The CE routers are not aware of the underlying network and perceive that they are connected to each other over a private network.

Each VPN is associated with a VPN Routing/Forwarding instance (VRF). A VRF defines the VPN membership of a customer site attached to a PE router. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table and a set of rules and routing protocol parameters that control the information that is included into the routing table.

Unlike traditional VPNs, MPLS VPNs do not rely upon encryption to provide security. Each VPN is separated by the MPLS IDs. The CE routers are not aware of any equipment, service or user that is not part of their own unique VRF. This prevents access to other company networks and ensures that all resources are secure.

The use of MPLS VPNs allows a new customer site to join an existing VPN and use routing advertisements of MBGP to introduce the new customer site into the existing VPN. In this fashion the addition of customer sites to the existing VPN is dynamic and scalable.

As well as providing security, MPLS also has the additional ability to reserve bandwidth and manage traffic.

4.1.9.2 IPSec

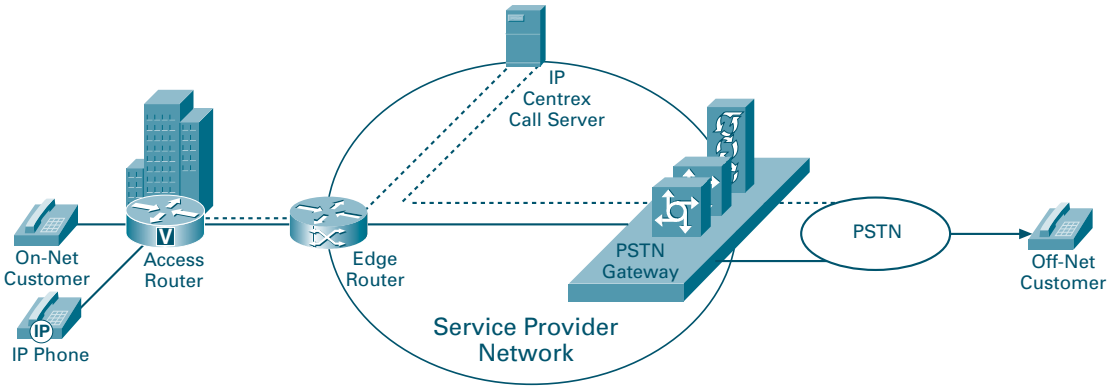
IPSec VPNs are an overlay type of network. They ride on top of any IP network. As an overlay technology, tunnels are established between sites, which can lead to a reduced efficiency network. Generally, there are two possible topologies: A hub-and-spoke configuration and a fully meshed configuration.

5 Technical Description – IP Centrex

An IP Centrex service provides end-users with advanced call features, typically PBX-like, irrespective of location. Typically features such as call forward, call transfer and conference facilities are available and are usually easily activated and administered by the end-user. As a hosted service, operated by the service provider, the end-user is provided with a reliable and easily scalable service without the complexity and cost of running their own PBXs on every site and is typically charged per line.

The key component of the IP Centrex service is the IP Centrex Call Server, located within the service provider's core IP Network. The following diagram shows the configuration:

Figure 5.1: IP Centrex Components



A PSTN Gateway is nearly always used as part of the configuration to extend the services out to the PSTN. The PSTN Gateway has already been discussed in Section 3. The remainder of this section describes the IP Centrex Call Server, the IP Phones that can be used with it and the associated services such as billing and administration.

5.1 IP Centrex Components

Perhaps the most important part of an IP Centrex solution is the call server, but alongside this, the right network components and architecture are vital for a reliable, high-performance, feature-rich service.

5.1.1 IP Centrex Call Server

The IP Centrex Call Server performs all of the call control functions for the IP Centrex services. Often configured as a cluster, all terminals register with the Call Server and both incoming and outgoing call control goes through it. During the registration process, the terminal informs the Call Server of its specification so that calls can be handled correctly and features can be activated by the appropriate method. For example, IP Phones have direct access to features through SIP or XML whereas analogue phones can activate features with key sequences and DTMF tones.

IP Phones such as the Cisco 7960 register directly with the Call Server. Analogue phones are connected through a voice gateway or IAD (Integrated Access Device) on the customer premises. This device performs the registration on behalf of the phones. Depending on the configuration, the call Server can use SIP, H.323, MGCP or other protocols such as Cisco's open SCCP Protocol (Skinny Client Control Protocol) to control the terminals and media gateways required to deliver the Centrex services.

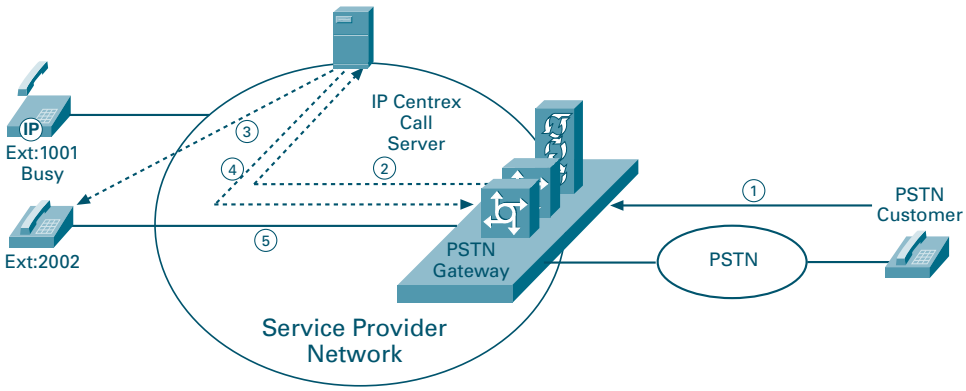
5.1.2 IP Phones

Whilst analogue phones can be used to access the majority of IP Centrex features, the use of IP Phones adds additional benefits. IP Phones can access information or services (e.g. Using XML) from the IP Centrex Call Server or other specified application servers. This information can be displayed on the IP Phone, or used to activate soft-keys on the phone providing additional call features. Many implementations do this dynamically to give information specific to the state of the call or calls. For more information on the specification of the Cisco 7960 IP Phone, refer to Section 8.

5.2 Functionality

An IP Centrex service can provide a wide variety of features both during call set-up and throughout the call. The Call Server is able to do this because it knows the status of all of the terminals registered with it. For example, when a call comes into the IP Network that is destined for a member of the Centrex group the call request is routed to the IP Centrex Call Server. The Call Server will check if the line is busy or if any call diverts are active at the time. Having done this and perhaps checking any personal details such as specific call handling by caller ID, it will pass on the request to the destination or to the appropriate line. The following diagram shows how a simple call-forward-on-busy feature works.

Figure 5.2: IP Centrex Functionality



In this example, the steps are as follows:

1. The call comes in from the PSTN via the PSTN Gateway.
2. The PSTN Gateway analyses the destination address (1001) and since it is a Centrex number, the call request is passed to the IP Centrex Call Server.
3. The Call Server knows that the destination line is busy and checks the feature tables for this line. Based on the call diverts set up by the user and other parameters such as the time of day, the Call Server tells the new device about the call and the phone will ring.
4. When the phone is answered the call server tells the PSTN Gateway to establish the media path to the IP address of 2002.
5. The PSTN Gateway and the alternative number (ext 2002) will then have a speech path between them. The signalling path, however, will normally still go via the call server.

Similar steps take place for features that are activated during the call or for features that are triggered when a call is cleared down. Call transfer is carried out when the Call Server receives an indication from one of the parties that they would like to transfer the call. The Call Server knows the status of the call and requests the new call path is established. Ring back when free, is a feature where the Call Server initiates a new call when it detects the end of another call. The signalling in each of these cases will be slightly different but the principle that the Call Server is at the centre of the network is the same for all features.

5.2.1 Billing

The IP Centrex Call Server can generate call usage information. This is normally fed to a mediation system for delivery to the billing system. Call and feature usage information can also be used to allocate costs to departmental cost centres. The centralised nature of the hosted IP Centrex service makes it easy to assess usage and costs across multiple sites so that the highest levels of service can be provided cost effectively.

5.2.2 Administration

A key feature of Hosted IP Centrex is the flexibility of administration. Multiple levels of administration can be set up to allow the appropriate level of control to users, departments, corporate and service provider administration. User level administration is via the IP phone or through a web browser interface although service providers will often use batch tools for bulk provisioning.

In addition to the flexibility and ease of administration, the centralised nature of the service means that large companies can maintain a consistent set of features across all of their sites. Colleagues from other offices will be familiar with the features and operation of facilities in every office they visit. IP Centrex is particularly useful in delivering big PBX features to small sites including single users where a PBX would be cost prohibitive.

6 Technical Description – Value Added Services

Due to the open standards used and the distributed nature of IP telephony, it is easy to add new resources to the network that can be accessed by all users or certain user groups. The resource may be a Unified Messaging platform or it may be a VXML Browser that will allow users to access Voice Portal services from their fixed or mobile phone. In either case the fact that they are based on an IP Network allows them to be integrated with other applications irrespective of geographical location on the network.

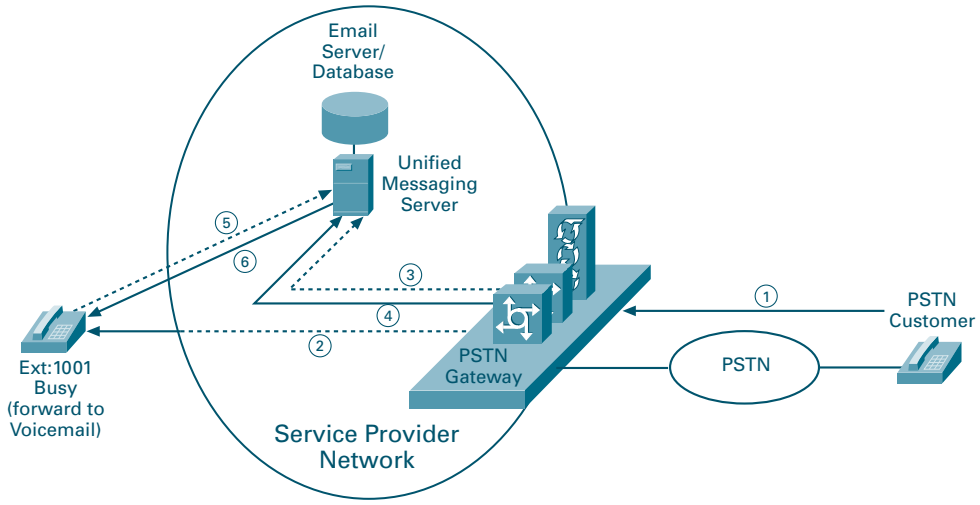
One of the most popular value added services is Unified Messaging and the next section will provide an overview of some of the configuration options available.

6.1 Unified Messaging

Voicemail has often used proprietary technology and interfacing it with other systems such as email or fax has been a difficult task. TDM networks have for many years had the ability to route voice to voicemail systems but the signalling used on the TDM interfaces is not ideally positioned to extend this to other resources such as email or directory servers that run on IP networks. Fortunately, service providers with an IP network have many more choices. VoIP protocols such as SIP and H.323 and web based protocols such as VoiceXML are much more easily interfaced directly to Unified Messaging platforms.

The following diagram shows how H.323 or SIP can be used to access a Unified Messaging system.

Figure 6.1: VoIP Based Unified Messaging



The example in Figure 6-1 shows a call coming into the network from the PSTN and being routed to a Unified Messaging Server to record a message. The owner of the mailbox then picks up this message. The steps are as follows:

1. The call is routed over the PSTN to the PSTN Gateway.
2. The PSTN Gateway attempts to route the call to the destination (ext.1001).
3. The extension is busy so the call is re-routed by the VoIP network to the Unified Messaging Server.
4. The Unified Message Server accepts the call and after playing the greeting, records the message.
5. Later, the owner of the mailbox calls the Unified Message Server.
6. The Unified Message Server accepts the call, plays the command menu and follows the commands selected by the user to play, forward or delete the message.

This example shows how the Unified Messaging Server can be accessed from anywhere on the IP voice network or PSTN. However, the Unified Messaging server also enables message retrieval via a web browser as well as message notification via email, SMS, Pager or fixed phone message waiting lamp.

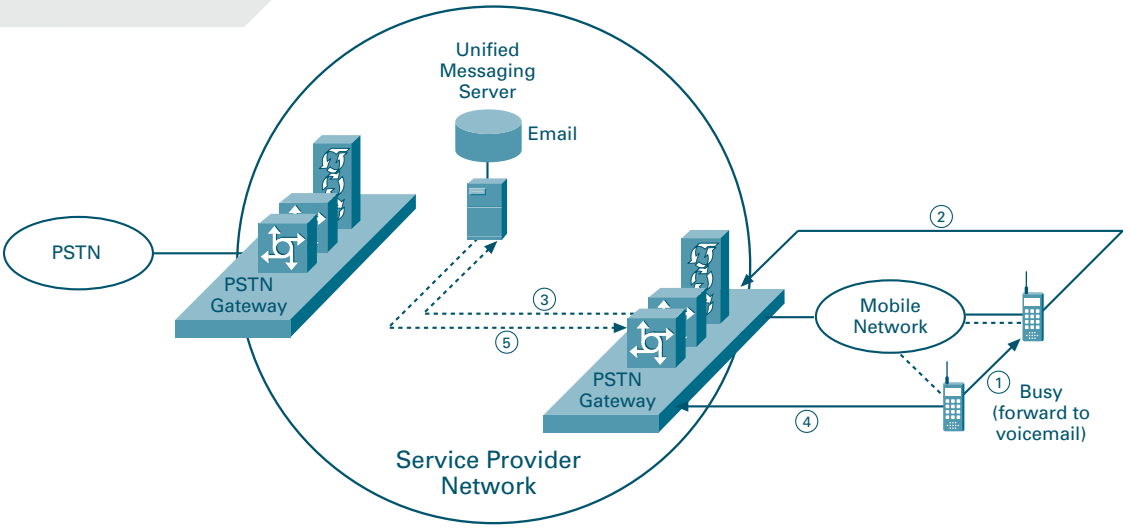
6.2 Voice Browsers

The VoiceXML protocol has been developed to provide a standardised interactive voice interface to web-based information and services. VoiceXML-enabled devices act as the voice equivalent to web browsers; VoiceXML requests are sent to a VoiceXML server, or portal, using HTTP and instructions or voice pages are returned that can contain information and menu choices. The voice equivalent of a web form can be created to collect and categorise information from the user using voice recognition or DTMF tones.

The VoiceXML protocol integrates easily with the web environment eg. HTTP, RTSP, SMTP, many Unified Messaging platforms now incorporate VoiceXML to standardise their Telephony User Interface (TUI).

The following diagram shows an example of how the VoiceXML browser capabilities of Cisco's IOS gateways are leveraged in this type of Unified Messaging environment. The example shows how message storage and retrieval can be offloaded from the PSTN or Mobile network.

Figure 6.2: VoiceXML Based Unified Messaging



In this example a call is placed from mobile to mobile. The call is diverted on busy to the Unified Messaging Server. When the gateway receives the call it asks the Unified Messaging Server what to do. The server returns a page, often created dynamically using the VoiceXML syntax to instruct the Cisco Gateway what to do.
Typically the PSTN Gateway will be told to play a greeting, and record a message. When the mailbox owner calls in to request the message be played back, it again uses VoiceXML. The steps are as follows:

1. The mobile phone call is attempted on the mobile network.
2. The destination phone is busy or switched off, so the mobile network diverts the call to the IP network.
3. The VoiceXML browser capability of the IOS Gateway communicates with the Unified Messaging Server application. The greeting is played, and the message is recorded and sent to the server.
4. Later, the owner of the mailbox calls his Unified Messaging service. The call is routed to the PSTN Gateway.
5. The VoiceXML Browser on an IOS gateway requests the mailbox information from the Unified Message Server and enables the caller to navigate through, and listen to the stored messages.

Text-to-speech engines allow email messages to be played (read out) over the voice interface. Faxes can be sent either to local fax machines for printing, or displayed using a web browser. The VoiceXML standard enables multiple applications to be accessed via VoiceXML browsers, so Unified Messaging can be one of a suite of Voice Portal services hosted on the service provider IP network, and accessible from either IP or TDM network domains.

7 IP Telephony Quality of Service

Quality of Service (QoS) is of critical importance in any voice network. Whilst some packet loss, delay and some variation in delay, known as jitter is normally acceptable for data transmission it is highly undesirable for a voice network. In general is does not matter if an email arrives 200ms late and if a packet is lost it is retransmitted; for voice these factors result in poor quality or unintelligible speech. There are of course some data applications that require the same QoS considerations as voice. The following sections look at the potential problems and how they are avoided by using the appropriate equipment and network design.

7.1 QoS Factors

There are a number of factors that affect the ability of a network to carry voice traffic and the resulting quality of the voice. These factors typically include Packet Loss, Packet Delay and Jitter.

7.1.1 Packet Loss

Packet loss can occur as a result of transmission errors or when a router discards them during congestion conditions. Packet loss causes voice clipping and skipping. The industry standard codec algorithms used in Cisco Digital Signal Processors (DSP) can correct for up to 30ms of lost voice. Voice over IP (VoIP) technology generally uses 20ms samples of voice payload per VoIP packet. In this case for the codec correction algorithms to be effective, only a single packet can be lost at a time. Avoiding packet loss due to transmission errors is not normally a problem in a digital infrastructure that is correctly provisioned and uses reliable and resilient equipment from end to end. Packet loss due to congestion can occur when buffers overflow. Often buffering causes delays first and by fixing delay by classifying and prioritising these packets, both problems are solved.

7.1.2 Packet Delay

Packet delay is caused by four main factors: transmission, switching, serialisation and congestion. If a long distance is involved or satellites are used then it takes a while for the data to cover the distance. Switching delay is the length of time a device may hold on to a packet to decide where to send it and assumes the packet does not get buffered due to congestion. The more hops a packet takes the more switching delays are accumulated. Where low speed circuits are used, consideration also needs to be given to the amount of time it takes to send a packet on to the wire. For example a 64kbps line can carry 8 kilobytes of data every second so if a packet 1kB in length is transmitted it will take 1/8th of a second from sending the first byte to get rid of the last. Perhaps the most important consideration though is the delay caused by congestion.
When a link is busy, traffic is held in a buffer until there is space on the link. The greater the congestion the longer the delay the packets experience. The backlog is cleared, or reduced every time the data arrival rate drops below the speed of the link, even if only for a few milliseconds.

Too much packet delay makes an interactive conversation harder as both speakers will start talking over each other. Two-way radios solve this by saying 'over' at the end of a transmission but this is not acceptable for telephony. In general networks should aim to minimise delay for voice with a target in the region of 150ms each way.

7.1.3 Jitter

When the delay is variable, a process runs at the receiving end of the connection that uses a buffer to ensure that the next packet has arrived before the previous one is completely processed. This is often known as the de-jitter buffer. The buffer works by storing enough packets to cover the variation in delay. This makes the end-to-end delay of the connection equal to that of the anticipated worst delay so that it never loses packets. Packets later than this are discarded and treated as lost. Minimising jitter therefore also minimises delay.

The mechanisms to resolve all of these QoS problems are detailed later in this section.

7.1.4 Echo

A fourth factor affecting the perceived quality of a connection is echo. This is not a specific VoIP issue and is the same in TDM networks. Echo is caused by the reflection of signals, typically from the terminating equipment but is generally only noticed where the delay before the echo is heard is more than 150ms. Echo cancellation is used in existing TDM networks to deal with this today. In an IP network this feature is built in to the VoIP gateways.

7.2 QoS Tools

Packet loss, delay and echo all contribute to degraded voice quality and whilst the weakest parts of the link will have the greatest impact the results are cumulative and so the whole network should always be considered. The QoS tools discussed here can be used to maintain high quality voice on data networks. In general they work by ensuring voice packets are given priority which means that delay and jitter and loss are minimised. These are the same tools that would be used to prioritise specific data connections as well if required.

QoS tools can be separated into three categories:

- Classification.
- Queuing.
- Network Provisioning.

7.2.1 Classification

Classification tools mark a packet or flow with a specific priority. The devices in the path then look at this classification to decide how to prioritise the flow. Accepting the authenticity of a marked packet in order to give a higher priority normally means a trust boundary is created where the classification occurs. Classification should take place at the network edge to ensure end-to-end voice quality but may be checked for validity elsewhere as well. Packets can be marked as important at different layers of the network. For example, this may be in the IP Precedence/Differentiated Services Code Point (DSCP) bits in the IP Type of Service (ToS) Byte of the IPv4 header. Alternatively, ATM, Frame Relay and MPLS also have classification mechanisms that can mark voice packets as high priority. Some of the key mechanisms are as follows:

- Frame Relay Traffic Shaping (FRTS) and Frame Relay Fragmentation (FRF12).
- Class Of Service (COS) with MPLS.
- Differentiated Services Code Point (DSCP) with MPLS.

The decision to classify can be based on the source or destination IP address, the arriving interface, the protocol used and content. It is also possible to classify according to an arrival rate policy.

7.2.2 Queuing

Queuing tools assign a packet to one of several queues based on classification. Queues are then transmitted according to their priority and packets are discarded according to the configured policy when high levels of congestion are reached. Typically a policy would discard low priority traffic in preference to high priority but may also be rate based.

Implementations that use a single queue for all traffic types, data, voice, and video, may discard or delay a packet from any stream without any concern on the impact of that stream. Cisco routers use multiple queues on outgoing and sometimes incoming interfaces to allow predictive queuing to be maintained.

Cisco Routers support a number of queuing mechanisms that help deliver QoS. Examples of these are:

- CBWFQ and LLQ with MQC for voice prioritisation.
- Class-Based Weighted Random Early Discard (CBWRED).
- Distributed Traffic Shaping (DTS).

Essentially all of these work by creating multiple queues, either by class or down to individual packet flows and then scheduling the emptying of the queue according to the configured policy.

7.2.3 Network Provisioning

No amount of classification and queuing can ensure high quality voice is transported over a badly provisioned network. If insufficient bandwidth is provided, queuing resulting in delay and eventually loss will occur. QoS simply ensures the losses and delay occur as configured. This means that you choose what is lost first. If there is still too much data for the capacity the mechanism will continue to discard according to policy but eventually will result in loss of the highest priority traffic.

Network Provisioning tools are available which accurately calculate the required bandwidth needed for voice conversations, data traffic, video applications and the necessary link management overhead such as for routing protocols. Tools are also available to monitor the proportion of each traffic type in a live network to ensure that the required bandwidth is maintained in each section of the network as demand changes.

8 Customer Premises Telephony

Earlier sections of this document have shown how by combining basic PSTN Access with Voice VPN and IP Centrex services, a service provider can offer a complete business telephony package to the customer. In some cases though, business customers may want to own and operate their own telephony system onsite.

When this is the case a service provider may want to resell the equipment (Resale) or provide the customer the equipment on site but operate it for them (Managed).

The options describe below can be deployed either as managed or resale.

8.1 Cisco IOS Telephony Service

Cisco IOS® Telephony Service delivers a small scale IP telephony solution based on access routers such as the Cisco 2600, 3600 controlling Cisco IP Phones or analogue phones. The router is used as both the IP access router and local call control server. The features provided are a subset of those provided by the Cisco Call Manager but are ideal as a leader for smaller companies that would previously have considered low end PBXs or keyswitches. All of the components involved can be re-used if migrating to Cisco Call Manager. The IOS Telephony Service platform can be integrated into a Cisco Call Manager network to maintain local site telephony services if connectivity to a centralised Call Manager system are temporarily unavailable. This is known as 'Survivable Remote Site Telephony'.

8.2 Cisco Call Manager

Cisco Call Manager is the software-based call-processing component of the Cisco enterprise IP telephony solution. Cisco Call Manager software delivers enterprise telephony features and capabilities to packet telephony network devices such as IP phones, media processing devices, Voice-over-IP (VoIP) gateways, as well as multimedia applications. Additional data, voice, and video services such as unified messaging, multimedia conferencing, collaborative contact centres, and interactive multimedia response systems can interact with the IP telephony solution through standardised protocols and Cisco Call Manager's open telephony application programming interfaces (APIs).

Cisco Call Manager provides a scalable, distributable, and highly available enterprise IP telephony call-processing solution by clustering servers so that they operate and are managed as a single entity. Cisco Call Manager clustering supports up to 10,000 users per cluster. By interlinking multiple clusters, system capacity can be increased significantly beyond this number.

By separating the call control from the actual switching, done at the IP level, Call Manager can support a number of different architectures and topologies. The most common are centralised call processing and distributed call processing.

8.2.1 Distributed Call Processing

In a Distributed Call-Processing model each site has its own phones, gateways and call control and can make all decisions without referring to any device outside the site. For two sites, two Call Manager clusters are deployed, for ten sites ten clusters etc. This is the traditional model for a TDM PBX where call processing, the telephone interface and the PSTN gateway are provide within one unit.

8.2.2 Centralised Call Processing

A Centralised Call Processing model differs in that a single call processing (Call Manager) cluster is used to control all the sites. This reduces the cost, as fewer clusters are required as well as having a number of other advantages such as the ability to provide number portability between sites, to allow users to log in as themselves in all offices etc.

When Centralised Call Processing is deployed obviously there is an increased dependence on the connectivity to the site containing the Call Manager cluster. Survivable Remote Site Telephony uses the IOS access router at a remote site to provide local fail-over which ensures IP Telephony continues in the event of WAN connectivity failure.

A service provider can provide a managed service offering for both the centralised and distributed designs, described above. In the centralised design, the service provider would normally host the Call Manager cluster at their own premises.

8.3 IP Phones

Cisco provides a range of IP phones from a basic set through to phones with large displays and multiple lines as well as a full duplex conference phone. These phones use standards based communication protocols for signalling and voice media. SIP and MGCP are supported as well as SCCP (Skinny Client Control Protocol) for use with Call Manager environments.

A number of the phones (7940 and 7960) have also been built with applications in mind. They have a large, pixel based, LCD display, driven via an eXtensible Markup Language (XML) interface.

The Cisco IP Phone Productivity Services (PPS) provide a good example of the types of business efficiency services that can be developed for the graphical phone interface. These XML based applications let you check your e-mail, voice mail, calendar, and personal contact information using the LCD display and by dynamically changing the functions of the soft keys on the phone.

Figure 8.1: Cisco 7960 IP Phone

Other possible IP phone services include:

- Conference room scheduler.
- Flight status.
- Transit schedules.
- E-mail and voice-mail messages list.
- Daily and weekly schedule and appointments.
- Personal address book entries.
- Company news.

In fact any web style service.

8.3.1 Cisco IP Softphones

The Cisco IP Softphone is a PC-based, software implementation of the 7960 IP phone. This can be used in two modes: either standalone as a replacement for the phone, or in combination with the Cisco IP Phone handset. In both modes a variety of features such as LDAP3 directory integration and virtual conference room can provide improved business efficiency. In combination mode, the user has an IP phone handset for voice but the advantages of CTI control to dial and deal with inbound calls directly from a screen-based application.

8.4 Other features

There are many other features unique to an IP solution such as a Web based operator console, with the ability to see a real-time view of the state of each line on the system. Web-based provisioning of call handling and diversion information is enabled by IP, as well as personal assistant, IP base IVR services and a host of new applications that are being added by Cisco and Cisco AVVID partners every day.

9 Customer Access

Access to the business customer site can be achieved in a number of ways; traditional TDM (E1/T1) circuits are obviously used when the service provider has centralised gateways. This is normally expensive and the cost increases with distance, additionally the circuit is normally dedicated to a single service – Voice.

Deploying over an IP access network has a number of advantages, perhaps the most important being that IP is a layer 3 protocol and so is media independent. This is the reason IP can run over fibre, SDH and SONET, DSL, leased lines, frame relay, X.25, SMDS, ATM, Ethernet, dialup PPP etc. In addition to being common to so many media types IP can also carry multiple traffic types.

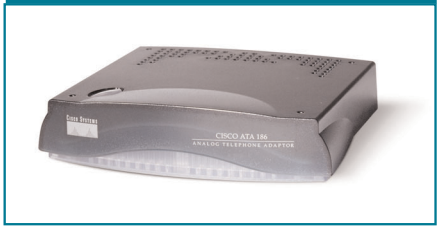
In summary IP can normally be deployed more cheaply, over a choice of media and can carry voice and data simultaneously and more efficiently than a TDM circuit.

The Internet also uses IP allowing voice traffic to be sent over the Internet, as well as over private networks. Whilst many will be sceptical about Internet use there are many commercial services using the Internet and considerably more using carriers that provide QoS guarantees over their network which is also part of the Internet.

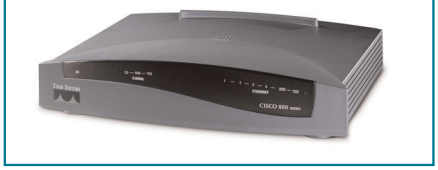
With a TDM connection each voice channel is given a fixed bandwidth for the duration of a call. At the end of the call the bandwidth sits idle waiting for another call. One of the reasons IP is more efficient is it allows dynamic allocation of bandwidth based on usage. If a channel is not in use the bandwidth can be used by other services. IP also supports compression and other bandwidth reduction techniques. While the bandwidth requirements are relatively low for a voice call, jitter and packet loss need to be managed by implementing the Quality of Service (QoS) mechanisms discussed in Section 7.

Having decided the access method, the customer's telephony side interface must be considered. For traditional TDM PBXs, digital E1 PRI or BRI trunks are preferred running either Q.931 (ISDN) or QSIG signalling but equally CAS and R2 signalling can also be used. For analogue connections a choice of FXO, FXS and E&M are available to match PBX, phone and exchange line interfaces.

Cisco ATA 186

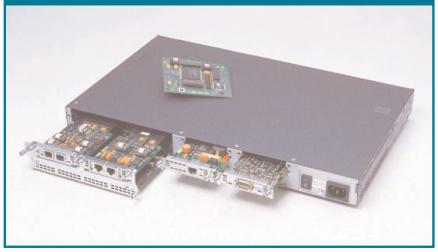


Cisco 800 Series



Cisco 1700 Series

Cisco 2600 Series



9.1 Cisco CPE Voice Enabled Access Routers

Cisco provides a range of voice enabled Access Routers supporting the various telephony and WAN interfaces with built in advanced Quality of Service (QoS), security and network integration features essential to both enterprise and service provider networks.

9.1.1 Cisco ATA 186

The ATA 186 is a two port fixed configuration voice gateway. It is equipped with two voice ports allowing a user to connect regular telephones to a VoIP network. The ATA is targeted for residential, small office and home workers as well as where one or two analogue ports are required i.e. lobby phones and fax machines in enterprises using IP phones elsewhere in the building.

9.1.2 Cisco 800 Series Access Routers

The low-cost, fixed configuration Cisco 800 Series is ideal for very small offices and telecommuters. It supports DES encryption for VPN functionality, includes models equipped with ISDN, serial and DSL. Models with integrated Ethernet hub and analogue phone ports increase the applications even more. The Cisco 827 router for example offers support for business class ADSL and VoIP, with the ability to add software based firewall and encryption.

9.1.3 Cisco 1700 Series Access Routers

The Cisco 1700 Series allows modular WIC and VIC interface cards to be installed in three slots at the rear of the unit. This allows the 1700 series to interface to telephones, the PSTN and PBXs from a telephony point of view and to Serial, ISDN and DSL services on the data side. The software goes on to provide additional features such as DHCP, firewall, VPN and encryption. The performance and capacity of the 1700 series is such that it is commonly deployed at small branch offices and small to medium sized businesses.

9.1.4 Cisco 2600 and 3600 Series Access Routers

The Cisco 2600 and 3600 series are modular in nature. Both series share the same modules and scale from small, to quite large deployments.

The models in the range provide increasing processing power and slots to accept network modules. The variety of network modules available includes analogue and digital voice ports, ATM, serial, frame relay, analogue and digital modems, ISDN and additional Ethernet/Fast Ethernet ports. Depending on the modules installed, the 2600/3600 series meet a wide variety of applications.

The 2600 range has only a single network module slot but includes additional built-in ports to meet the needs of common applications. Depending on the model, one or more WAN, Ethernet or Fast Ethernet ports are built in while the network module slot allows for expansion.

Cisco 3600 Series

The largest model in the series, the 3660 also includes two built-in Fast Ethernet ports allowing it to support up to 12 E1s or 360 channels for voice.

For CPE deployments the 2600/3600 series are often deployed with spare capacity giving the flexibility to add or swap modules as requirements change.

For high performance applications requiring lots of processing power the 2600/3600 Series supports one or two Advanced Integration Module (AIM) slots. AIM slots allow hardware assistance to be added to off-load tasks such as high-speed data compression, encryption, voice processing and ATM with minimal impact on the performance of the router.

Cisco 7100/7200 Series

9.1.5 Cisco 7100 and 7200 Series Access Router

The Cisco 7100 and 7200 Series routers offer higher performance than the 3600 series and use Port Adaptors (PAs) rather than Network Modules. PAs are common across the whole of the 7000 range including the 7100, 7200 and 7500.

The 7100 is a high-end, full-featured, integrated VPN with plenty of processing power. The Cisco 7100 Series is normally used for VPN, tunnelling, data encryption, security, firewall, advanced bandwidth management, and service-level validation.

The 7200 builds on the 7100s performance with additional slots enabling it to handle a greater mix of interfaces and therefore applications.

Like the 3600 the 7000 series also supports 12/30/60 channel digital voice cards, up to a total capacity of 24 E1s or 720 simultaneous calls. Analogue is not supported on the 7000 range.

10 Contacts and References

10.1 Standards Organisations

10.1.1 ETSI

The European Telecommunications Standard Institute (ETSI) is a non-profit organisation devoted to creating standards for telecommunications within Europe and beyond.

10.1.2 IETF

The Internet Engineering Task Force (IETF) is an international community of network designers, operators, vendors and researchers concerned with the evolution the Internet architecture and the smooth operation of the Internet.

10.1.3 ITU

The International Telecommunications Union (ITU) is an international organisation that coordinates global telecom networks and services for government and the private sector.

10.1.4 VoiceXML Forum

The VoiceXML Forum is an industry organisation, and chartered with establishing and promoting the Voice Extensible Mark-up Language (VoiceXML), a specification to enable Internet content and information to be accessible via voice and telephone.

10.1.5 Standards

H.323	H.323 is an umbrella recommendation that sets standards for multimedia communications over IP Networks.
H.225	H.225 specifies call signalling (Q.931 subset), RAS, multimedia transport (RTP/RTCP).
H.450	H.450 specifies supplementary services. Transfer, Diversion, Hold, Park & Pickup, Call Waiting, Message Waiting Indication, Name Identification, Call Completion on Busy.
H.235	Security, encryption, authentication.
H.245	Multimedia signalling.
H.GCP	Proposed Recommendation Gateway Control Protocol.
H.323 Annex E	Call Signalling over UDP.
H.323 Annex F	Single Use Audio Device (SUD).
H.225 Annex G	Interzone communication. Extended to include not only address resolution but also pricing information exchange, access authorisation, and usage reporting.

11 Glossary of Terms

ADSL	Asynchronous Digital Subscriber Line.
AMA	Automatic Message Accounting – The process that generates information from which customers and carriers are billed for their use of network services and capabilities.
ANSI	American National Standard Institute.
ATM	Asynchronous Transfer Mode.
C7	Signalling System 7 (SS7) used between PSTN Voice switches.
CAS	Channel Associated Signalling.
CCS	Common Channel Signalling.
CDR	Call Detail Record – Call Detail Record files consist of several CDBs.
CLI	Calling Line Identifier.
CPE	Customer Premises Equipment.
CPS	Calls per second.
CRTP	Compressed RTP.
DDI	Direct Dialling Inward.
Diffserv	Differentiated Services.
DS0	A 64kpbs digital TDM channel used for carrying a single POTS call.
DSP	Digital Signal Processor.
E.164	ITU Standard for the format of PSTN Numbers.
E-ISUP	Extended-ISUP – Originally a subset of Q.761 ISUP. It is expanding in to a superset of ITU and ANSI ISUP. In addition, it supports the delivery of SDP parameters via generic digits. E-ISUP runs over IP and therefore uses IP addresses instead of point codes.
ETSI	European Telecommunications Standards Institute.
FR	Frame Relay.
Gatekeeper (GK)	An H.323 entity that provides address translation, control access, and sometimes bandwidth management to the LAN for H.323 terminals, Gateways, and MCUs.
Gateway (GW)	An H.323 entity which provides real-time, two-way communications between H.323 terminals on the LAN and other ITU terminals on a WAN, or to another H.323 Gateway.

H.245 Logical	A channel carrying information streams between two Channel H.323 endpoints.
H.323 Entity	Any H.323 component, including terminals, Gateways, Gatekeepers, MCs, MPs, and MCUs.
H.323	ITU umbrella standard covering a number of standards enabling VoIP.
IAD	Integrated Access Device.
IETF	Internet Engineering Task Force.
IP	Internet Protocol.
ISDN	Integrated Services Digital Network.
ISP	Internet service provider.
ISUP	ISDN User Part – Used to set up and tear down all circuits used for data or voice calls in the Public Switched Network. Telephone (PSTN).
ITU	International Telecommunication Union.
IVR	Interactive Voice Response.
LNP	Local Number Portability.
Local Area Network	A shared or switched medium, peer-to-peer communications network, which may include inter-networks, composed of LANs connected by bridges or routers.
MBGP	Multi-Protocol Extensions for BGP.
MG	Media Gateway. The emerging industry standard generic term for a gateway.
MGC	Media Gateway Controller. The emerging industry standard generic term for softswitches such as the Cisco PGW 2200.
MGCP	The Media Gateway Control Protocol – A merging of the IPDC and SGCP protocols.
MPLS	Multi-Protocol Label Switching.
MTP	Message Transfer Part – Layers 1 (physical), 2 (data), and 3 (network) of the SS7 signalling protocol.

OLO	Other Licensed Operators.
POI	Point of Interconnection.
POP	Point of Presence. A location where two service providers (e.g. an ISP and a LEC) co-locate and interconnect equipment.
POTS	Plain Old Telephony Service.
PRI	Primary Rate Interface (Q.931).
PSTN	Public Switched Telephone Network.
PTO	Public Telecom Operator, also referred to as PTT.
Q.931	Call signalling protocol for set-up and termination of calls.
Quality of Service (QoS)	Guarantees network bandwidth and availability for applications.
RAS Channel	A channel used to convey the Registration, Admissions and Status messages and bandwidth changes between two H.323 entities.
RTP/RTCP	Real-Time Protocol/Real-Time Control Protocol (RTP/RTCP): IETF specification for audio and video signal management. Allows applications to synchronise and spoil audio and video information.
Resource Reservation Protocol	(RSVP) Reservation Set-up Protocol – IETF Protocol specification. Allows applications to request dedicated bandwidth.
RUDP	Reliable User Data Protocol.
SDH	Synchronous Digital Hierarchy.
SG	Signalling gateway. A gateway that supports only signalling traffic (no bearer traffic.) For example, a gateway that terminates SS7 A-links is a signalling gateway.
SIP	Session Initiated Protocol.
SLT	Signalling Link Terminal – A Cisco 2611 router used to terminate MTP2 and provide backhaul support of MTP3 to the PGW 2200.
SNMP	Simple Network Management Protocol. A set of protocols to manage complex networks by sending messages called protocol data units (PDUs) and getting responses from SNMP agents that store information about them.
SVC	Switched Virtual Circuit.

TCP	Transmission control protocol. A reliable networking layer on top of IP.
TDM	Time Division Multiplexing. The transmission scheme employed by all manners of digital circuits in the PSTN.
Terminal	An endpoint that provides for real-time, two-way communications with another Terminal, Gateway, or MCU. A terminal must provide audio and may also provide video and/or data.
UDP	User Datagram Protocol. An unreliable networking layer, which sits at the same level of the networking stack as TCP.
URL	Universal Resource Locator (Internet Address).
VISM	Voice Interworking Service Module.
VoATM	Voice over ATM. The ability to carry normal telephony-style voice over an ATM-based network with POTS-like functionality, reliability, and voice quality.
VoIP	Voice over IP. The ability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality.
VPN	Virtual Private Network.
WAN	Wide Area Network.
WAP	Wireless Application Protocol.
xDSL	Generic Term for all variations of DSL.
Zone	A collection of all Terminals, Gateways, and MCUs managed by a single Gatekeeper. A zone must include at least one Terminal and may include LAN segments connected using routers.

UK Office
Cisco Systems, Inc.
11 New Square
Bedfont Lakes
Feltham
Middlesex
United Kingdom

Tel: +44 208 824 1000
Fax: +44 208 756 8099

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.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe