Voice over IP

Voice over Internet Protocol (Voice over IP, VoIP) is one of a family of internet technologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms frequently encountered and often used synonymously with VoIP are IP telephony, Internet telephony, voice over broadband (VoBB), broadband telephony, and broadband phone.

Internet telephony refers to communications services — voice, fax, SMS, and/or voice-messaging applications — that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream.[1]

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. The codec used is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs.

Protocols

Voice over IP has been implemented in various ways using both proprietary and open protocols and standards. Examples of technologies used to implement Voice over IP include:

- H.323
- IP Multimedia Subsystem (IMS)
- Media Gateway Control Protocol (MGCP)
- Session Initiation Protocol (SIP)
- Real-time Transport Protocol (RTP)
- Session Description Protocol (SDP)

The H.323 protocol was one of the first VoIP protocols that found widespread implementation for long-distance traffic, as well as local area network services. However, since the development of newer, less complex protocols, such as MGCP and SIP, H.323 deployments are increasingly limited to carrying existing long-haul network traffic. In particular, the Session Initiation Protocol (SIP) has gained widespread VoIP market penetration.

A notable proprietary implementation is the Skype protocol, which is in part based on the principles of Peer-to-Peer (P2P) networking.
Adoption

Consumer market

A major development that started in 2004 was the introduction of mass-market VoIP services that utilize existing broadband Internet access, by which subscribers place and receive telephone calls in much the same manner as they would via the public switched telephone network (PSTN). Full-service VoIP phone companies provide inbound and outbound service with Direct Inbound Dialing. Many offer unlimited domestic calling for a flat monthly subscription fee. This sometimes includes international calls to certain countries. Phone calls between subscribers of the same provider are usually free when flat-fee service is not available.

A VoIP phone is necessary to connect to a VoIP service provider. This can be implemented in several ways:

- Dedicated VoIP phones connect directly to the IP network using technologies such as wired Ethernet or wireless Wi-Fi. They are typically designed in the style of traditional digital business telephones.
- An analog telephone adapter is a device that connects to the network and implements the electronics and firmware to operate a conventional analog telephone attached through a modular phone jack. Some residential Internet gateways and cablemodems have this function built in.
- A softphone is application software installed on a networked computer that is equipped with a microphone and speaker, or headset. The application typically presents a dial pad and display field to the user to operate the application by mouse clicks or keyboard input.

PSTN and mobile network providers

It is becoming increasingly common for telecommunications providers to use VoIP telephony over dedicated and public IP networks to connect switching stations and to interconnect with other telephony network providers; this is often referred to as "IP backhaul". Smartphones and Wi-Fi enabled mobile phones may have SIP clients built into the firmware or available as an application download. Such clients operate independently of the mobile telephone phone network and use either the cellular data connection or WiFi to make and receive phone calls.

Corporate use

Because of the bandwidth efficiency and low costs that VoIP technology can provide, businesses are gradually beginning to migrate from traditional copper-wire telephone systems to VoIP systems to reduce their monthly phone costs.

VoIP solutions aimed at businesses have evolved into "unified communications" services that treat all communications—phone calls, faxes, voice mail, e-mail, Web conferences and more—as discrete units that can all be delivered via any means and to any handset, including cellphones. Two kinds of competitors are competing in this space: one set is focused on VoIP for medium to large enterprises, while another is targeting the small-to-medium business (SMB) market.

VoIP allows both voice and data communications to be run over a single network, which can significantly reduce infrastructure costs.
The prices of extensions on VoIP are lower than for PBX and key systems. VoIP switches may run on commodity hardware, such as PCs or Linux systems. Rather than closed architectures, these devices rely on standard interfaces.[7]

VoIP devices have simple, intuitive user interfaces, so users can often make simple system configuration changes. Dual-mode cellphones enable users to continue their conversations as they move between an outside cellular service and an internal Wi-Fi network, so that it is no longer necessary to carry both a desktop phone and a cellphone. Maintenance becomes simpler as there are fewer devices to oversee.[7]

Skype, which originally marketed itself as a service among friends, has begun to cater to businesses, providing free-of-charge connections between any users on the Skype network and connecting to and from ordinary PSTN telephones for a charge.[8]

In the United States the Social Security Administration (SSA) is converting its field offices of 63,000 workers from traditional phone installations to a VoIP infrastructure carried over its existing data network.[9][10]

**Benefits**

**Operational cost**

VoIP can be a benefit for reducing communication and infrastructure costs. Examples include:

- Routing phone calls over existing data networks to avoid the need for separate voice and data networks.[11]
- Conference calling, IVR, call forwarding, automatic redial, and caller ID features that traditional telecommunication companies (telcos) normally charge extra for, are available free of charge from open source VoIP implementations.

**Flexibility**

VoIP can facilitate tasks and provide services that may be more difficult to implement using the PSTN. Examples include:

- The ability to transmit more than one telephone call over a single broadband connection.
- Secure calls using standardized protocols (such as Secure Real-time Transport Protocol). Most of the difficulties of creating a secure telephone connection over traditional phone lines, such as digitizing and digital transmission, are already in place with VoIP. It is only necessary to encrypt and authenticate the existing data stream.
- Location independence. Only a sufficiently fast and stable Internet connection is needed to get a connection from anywhere to a VoIP provider.
- Integration with other services available over the Internet, including video conversation, message or data file exchange during the conversation, audio conferencing, managing address books, and passing information about whether other people are available to interested parties.
- Unified Communications, the integration of VoIP with other business systems including E-mail, Customer Relationship Management (CRM), and Web systems.
Challenges

Quality of service

Communication on the IP network is inherently less reliable in contrast to the circuit-switched public telephone network, as it does not provide a network-based mechanism to ensure that data packets are not lost, or delivered in sequential order. It is a best-effort network without fundamental Quality of Service (QoS) guarantees. Therefore, VoIP implementations may face problems mitigating latency and jitter.

By default, IP routers handle traffic on a first-come, first-served basis. Routers on high volume traffic links may introduce latency that exceeds permissible thresholds for VoIP. Fixed delays cannot be controlled, as they are caused by the physical distance the packets travel; however, latency can be minimized by marking voice packets as being delay-sensitive with methods such as DiffServ.

A VoIP packet usually has to wait for the current packet to finish transmission, although it is possible to preempt (abort) a less important packet in mid-transmission, although this is not commonly done, especially on high-speed links where transmission times are short even for maximum-sized packets. An alternative to preemption on slower links, such as dialup and DSL, is to reduce the maximum transmission time by reducing the maximum transmission unit. But every packet must contain protocol headers, so this increases relative header overhead on every link along the user's Internet paths, not just the bottleneck (usually Internet access) link.

ADSL modems provide Ethernet (or Ethernet over USB) connections to local equipment, but inside they are actually ATM modems. They use AAL5 to segment each Ethernet packet into a series of 53-byte ATM cells for transmission and reassemble them back into Ethernet packets at the receiver. A virtual circuit identifier (VCI) is part of the 5-byte header on every ATM cell, so the transmitter can multiplex the active virtual circuits (VCs) in any arbitrary order. Cells from the same VC are always sent sequentially.

However, the great majority of DSL providers use only one VC for each customer, even those with bundled VoIP service. Every Ethernet packet must be completely transmitted before another can begin. If a second PVC were established, given high priority and reserved for VoIP, then a low priority data packet could be suspended in mid-transmission and a VoIP packet sent right away on the high priority VC. Then the link would pick up the low priority VC where it left off. Because ATM links are multiplexed on a cell-by-cell basis, a high priority packet would have to wait at most 53 byte times to begin transmission. There would be no need to reduce the interface MTU and accept the resulting increase in higher layer protocol overhead, and no need to abort a low priority packet and resend it later.

This doesn't come for free. ATM has substantial header overhead: 5/53 = 9.4%, roughly twice the total header overhead of a 1500 byte TCP/IP Ethernet packet (with TCP timestamps). This "ATM tax" is incurred by every DSL user whether or not he takes advantage of multiple virtual circuits - and few can.

ATM's potential for latency reduction is greatest on slow links, because worst-case latency decreases with increasing link speed. A full-size (1500 byte) Ethernet frame takes 94 ms to transmit at 128 kb/s but only 8 ms at 1.5 Mb/s. If this is the bottleneck link, this latency is probably small enough to ensure good VoIP performance without MTU reductions or multiple ATM PVCs. The latest generations of DSL, VDSL and VDSL2, carry Ethernet without intermediate ATM/AAL5 layers, and they generally support IEEE 802.1p priority tagging so that VoIP can be queued ahead of less time-critical traffic.

Voice, and all other data, travels in packets over IP networks with fixed maximum capacity. This system may be more prone to congestion and DoS attacks[12] than traditional circuit switched systems; a circuit switched system of insufficient capacity will refuse new connections while carrying the remainder without impairment, while the quality of real-time data such as telephone conversations on packet-switched networks degrades dramatically.

Fixed delays cannot be controlled as they are caused by the physical distance the packets travel. They are especially problematic when satellite circuits are involved because of the long distance to a geostationary satellite and back;
delays of 400-600 ms are typical. When the load on a link grows so quickly that its switches experience queue overflows, congestion results and data packets are lost. This signals a transport protocol like TCP to reduce its transmission rate to alleviate the congestion. But VoIP usually uses UDP not TCP because recovering from congestion through retransmission usually entails too much latency. So QoS mechanisms can avoid the undesirable loss of VoIP packets by immediately transmitting them ahead of any queued bulk traffic on the same link, even when that bulk traffic queue is overflowing.

The receiver must resequence IP packets that arrive out of order and recover gracefully when packets arrive too late or not at all. Jitter results from the rapid and random (i.e., unpredictable) changes in queue lengths along a given Internet path due to competition from other users for the same transmission links. VoIP receivers counter jitter by storing incoming packets briefly in a "de-jitter" or "playout" buffer, deliberately increasing latency to improve the chance that each packet will be on hand when it's time for the voice engine to play it. The added delay is thus a compromise between excessive latency and excessive dropout, i.e., momentary audio interruptions.

Although jitter is a random variable, it is the sum of several other random variables that are at least somewhat independent: the individual queuing delays of the routers along the Internet path in question. Thus according to the central limit theorem, we can model jitter as a gaussian random variable. This suggests continually estimating the mean delay and its standard deviation and setting the playout delay so that only packets delayed more than several standard deviations above the mean will arrive too late to be useful. In practice, however, the variance in latency of many Internet paths is dominated by a small number (often one) of relatively slow and congested "bottleneck" links. Most Internet backbone links are now so fast (e.g. 10 Gb/s) that their delays are dominated by the transmission medium (e.g. optical fiber) and the routers driving them do not have enough buffering for queuing delays to be significant.

It has been suggested to rely on the packetized nature of media in VoIP communications and transmit the stream of packets from the source phone to the destination phone simultaneously across different routes (multi-path routing).[13] In such a way, temporary failures have less impact on the communication quality. In capillary routing it has been suggested to use at the packet level Fountain codes or particularly raptor codes for transmitting extra redundant packets making the communication more reliable.

A number of protocols have been defined to support the reporting of QoS/QoE for VoIP calls. These include RTCP Extended Report (RFC 3611), SIP RTCP Summary Reports, H.460.9 Annex B (for H.323), H.248.30 and MGCP extensions. The RFC 3611 VoIP Metrics block is generated by an IP phone or gateway during a live call and contains information on packet loss rate, packet discard rate (because of jitter), packet loss/discard burst metrics (burst length/density, gap length/density), network delay, end system delay, signal / noise / echo level, Mean Opinion Scores (MOS) and R factors and configuration information related to the jitter buffer.

RFC 3611 VoIP metrics reports are exchanged between IP endpoints on an occasional basis during a call, and an end of call message sent via SIP RTCP Summary Report or one of the other signaling protocol extensions. RFC 3611 VoIP metrics reports are intended to support real time feedback related to QoS problems, the exchange of information between the endpoints for improved call quality calculation and a variety of other applications.

Layer-2 quality of service

A number of protocols that deal with the data link layer and physical layer include quality-of-service mechanisms that can be used to ensure that applications like VoIP work well even in congested scenarios. Some examples include:

- IEEE 802.11e is an approved amendment to the IEEE 802.11 standard that defines a set of quality-of-service enhancements for wireless LAN applications through modifications to the Media Access Control (MAC) layer. The standard is considered of critical importance for delay-sensitive applications, such as Voice over Wireless IP.
- IEEE 802.1p defines 8 different classes of service (including one dedicated to voice) for traffic on layer-2 wired Ethernet.
• The ITU-T G.hn standard, which provides a way to create a high-speed (up to 1 gigabit per second) Local area network using existing home wiring (power lines, phone lines and coaxial cables). G.hn provides QoS by means of "Contention-Free Transmission Opportunities" (CFTXOPs) which are allocated to flows (such as a VoIP call) which require QoS and which have negotiated a "contract" with the network controller.

Susceptibility to power failure

Telephones for traditional residential analog service are usually connected directly to telephone company phone lines which provide direct current to power most basic analog handsets independently of locally available power.

IP Phones and VoIP telephone adapters connect to routers or cable modems which typically depend on the availability of mains electricity or locally generated power. Some VoIP service providers use customer premise equipment (e.g., cablemodems) with battery-backed power supplies to assure uninterrupted service for up to several hours in case of local power failures. Such battery-backed devices typically are designed for use with analog handsets.

Some VoIP service providers implement services to route calls to other telephone services of the subscriber, such a cellular phone, in the event that the customer's network device is inaccessible to terminate the call.

The susceptibility of phone service to power failures is a common problem even with traditional analog service in areas where many customers purchase modern telephone units that operate with wireless handsets to a base station, or that have other modern phone features, such as built-in voicemail or phone book features.

Emergency calls

The nature of IP makes it difficult to locate network users geographically. Emergency calls, therefore, cannot easily be routed to a nearby call center. Sometimes, VoIP systems may route emergency calls to a non-emergency phone line at the intended department. In the United States, at least one major police department has strongly objected to this practice as potentially endangering the public.

A fixed line phone has a direct relationship between a telephone number and a physical location. If an emergency call comes from that number, then the physical location is known.

In the IP world, it is not so simple. A broadband provider may know the location where the wires terminate, but this does not necessarily allow the mapping of an IP address to that location. IP addresses are often dynamically assigned, so the ISP may allocate an address for online access, or at the time a broadband router is engaged. The ISP recognizes individual IP addresses, but does not necessarily know to which physical location it corresponds. The broadband service provider knows the physical location, but is not necessarily tracking the IP addresses in use.

There are more complications since IP allows a great deal of mobility. For example, a broadband connection can be used to dial a virtual private network that is employer-owned. When this is done, the IP address being used will belong to the range of the employer, rather than the address of the ISP, so this could be many kilometres away or even in another country. To provide another example: if mobile data is used, e.g., a 3G mobile handset or USB wireless broadband adapter, then the IP address has no relationship with any physical location, since a mobile user could be anywhere that there is network coverage, even roaming via another cellular company.

In short, there is no relationship between IP address and physical location, so the address itself reveals no useful information for the emergency services.

At the VoIP level, a phone or gateway may identify itself with a SIP registrar by using a username and password. So in this case, the Internet Telephony Service Provider (ITSP) knows that a particular user is online, and can relate a specific telephone number to the user. However, it does not recognize how that IP traffic was engaged. Since the IP address itself does not necessarily provide location information presently, today a "best efforts" approach is to use an available database to find that user and the physical address the user chose to associate with that telephone number—clearly an imperfect solution.
VoIP Enhanced 911 (E911) is a method by which VoIP providers in the United States support emergency services. The VoIP E911 emergency-calling system associates a physical address with the calling party's telephone number as required by the Wireless Communications and Public Safety Act of 1999. All VoIP providers that provide access to the public switched telephone network are required to implement E911, a service for which the subscriber may be charged. Participation in E911 is not required and customers may opt-out of E911 service.

One shortcoming of VoIP E911 is that the emergency system is based on a static table lookup. Unlike in cellular phones, where the location of an E911 call can be traced using Assisted GPS or other methods, the VoIP E911 information is only accurate so long as subscribers are diligent in keeping their emergency address information up-to-date. In the United States, the Wireless Communications and Public Safety Act of 1999 leaves the burden of responsibility upon the subscribers and not the service providers to keep their emergency information up to date.

**Lack of redundancy**

With the current separation of the Internet and the PSTN, a certain amount of redundancy is provided. An Internet outage does not necessarily mean that a voice communication outage will occur simultaneously, allowing individuals to call for emergency services and many businesses to continue to operate normally. In situations where telephone services become completely reliant on the Internet infrastructure, a single-point failure can isolate communities from all communication, including Enhanced 911 and equivalent services in other locales. However, the internet as designed by DARPA in the early 1980s was specifically designed to be fault tolerant under adverse conditions. Even during the 9/11 attacks on the World Trade Centers the internet routed data around the failed nodes that were housed in or near the towers. So single point failures while possible in some geographic areas are not the norm for the internet as a whole.

**Number portability**

Local number portability (LNP) and Mobile number portability (MNP) also impact VoIP business. In November 2007, the Federal Communications Commission in the United States released an order extending number portability obligations to interconnected VoIP providers and carriers that support VoIP providers. Number portability is a service that allows a subscriber to select a new telephone carrier without requiring a new number to be issued. Typically, it is the responsibility of the former carrier to “map” the old number to the undisclosed number assigned by the new carrier. This is achieved by maintaining a database of numbers. A dialed number is initially received by the original carrier and quickly rerouted to the new carrier. Multiple porting references must be maintained even if the subscriber returns to the original carrier. The FCC mandates carrier compliance with these consumer-protection stipulations.

A voice call originating in the VoIP environment also faces challenges to reach its destination if the number is routed to a mobile phone number on a traditional mobile carrier. VoIP has been identified in the past as a Least Cost Routing (LCR) system, which is based on checking the destination of each telephone call as it is made, and then sending the call via the network that will cost the customer the least. This rating is subject to some debate given the complexity of call routing created by number portability. With GSM number portability now in place, LCR providers can no longer rely on using the network root prefix to determine how to route a call. Instead, they must now determine the actual network of every number before routing the call.

Therefore, VoIP solutions also need to handle MNP when routing a voice call. In countries without a central database, like the UK, it might be necessary to query the GSM network about which home network a mobile phone number belongs to. As the popularity of VoIP increases in the enterprise markets because of least cost routing options, it needs to provide a certain level of reliability when handling calls.

MNP checks are important to assure that this quality of service is met. By handling MNP lookups before routing a call and by assuring that the voice call will actually work, VoIP service providers are able to offer business subscribers the level of reliability they require.
**PSTN integration**

E.164 is a global FG_numbering standard for both the PSTN and PLMN. Most VoIP implementations support E.164 to allow calls to be routed to and from VoIP subscribers and the PSTN/PLMN. VoIP implementations can also allow other identification techniques to be used. For example, Skype allows subscribers to choose “Skype names” whereas SIP implementations can use URLs similar to email addresses. Often VoIP implementations employ methods of translating non-E.164 identifiers to E.164 numbers and vice-versa, such as the Skype-In service provided by Skype and the ENUM service in IMS and SIP. Echo can also be an issue for PSTN integration. Common causes of echo include impedance mismatches in analog circuitry and acoustic coupling of the transmit and receive signal at the receiving end.

**Security**

VoIP telephone systems are susceptible to attacks as are any internet-connected devices. This means that hackers who know about these vulnerabilities (such as insecure passwords) can institute denial-of-service attacks, harvest customer data, record conversations and break into voice mailboxes.

Another challenge is routing VoIP traffic through firewalls and network address translators. Private Session Border Controllers are used along with firewalls to enable VoIP calls to and from protected networks. For example, Skype uses a proprietary protocol to route calls through other Skype peers on the network, allowing it to traverse symmetric NATs and firewalls. Other methods to traverse NATs involve using protocols such as STUN or ICE.

Many consumer VoIP solutions do not support encryption, although having a secure phone is much easier to implement with VoIP than traditional phone lines. As a result, it is relatively easy to eavesdrop on VoIP calls and even change their content. An attacker with a packet sniffer could intercept your VoIP calls if you are not on a secure VLAN. However, physical security of the switches within an enterprise and the facility security provided by ISPs make packet capture less of a problem than originally foreseen. Further research has shown that tapping into a fiber optic network without detection is difficult if not impossible. This means that once a voice packet is within the internet backbone it is relatively safe from interception.

There are open source solutions, such as Wireshark, that facilitate sniffing of VoIP conversations. A modicum of security is afforded by patented audio codecs in proprietary implementations that are not easily available for open source applications; however, such security through obscurity has not proven effective in other fields. Some vendors also use compression, which may make eavesdropping more difficult. However, real security requires encryption and cryptographic authentication which are not widely supported at a consumer level. The existing security standard Secure Real-time Transport Protocol (SRTP) and the new ZRTP protocol are available on Analog Telephone Adapters (ATAs) as well as various softphones. It is possible to use IPsec to secure P2P VoIP by using opportunistic encryption. Skype does not use SRTP, but uses encryption which is transparent to the Skype provider. In 2005, Skype invited a researcher, Dr Tom Berson, to assess the security of the Skype software, and his conclusions are available in a published report.

The Voice VPN solution provides secure voice for enterprise VoIP networks by applying IPsec encryption to the digitized voice stream.

**Securing VoIP**

To prevent the above security concerns government and military organizations are using Voice over Secure IP (VoSIP), Secure Voice over IP (SVoIP), and Secure Voice over Secure IP (SVoSIP) to protect confidential and classified VoIP communications. Secure Voice over IP is accomplished by encrypting VoIP with Type 1 encryption. Secure Voice over Secure IP is accomplished by using Type 1 encryption on a classified network, like SIPRNet. Public Secure VoIP is also available with free GNU programs.
**Caller ID**

Caller ID support among VoIP providers varies, although the majority of VoIP providers now offer full Caller ID with name on outgoing calls. In a few cases, VoIP providers may allow a caller to spoof the Caller ID information, potentially making calls appear as though they are from a number that does not belong to the caller. Business grade VoIP equipment and software often makes it easy to modify caller ID information. Although this can provide many businesses great flexibility, it is also open to abuse.

The "Truth in Caller ID Act" has been in preparation in the US Congress since 2006, but as of January 2009 still has not been enacted. This bill proposes to make it a crime in the United States to "knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value ...".

**Compatibility with traditional analog telephone sets**

Some analog telephone adapters do not decode pulse dialing from older phones. They may only work with push-button telephones using the touch-tone system. The VoIP user may use a pulse-to-tone converter, if needed.

**Fax handling**

Support for sending faxes over VoIP implementations is still limited. The existing voice codecs are not designed for fax transmission; they are designed to digitize an analog representation of a human voice efficiently. However, the inefficiency of digitizing an analog representation (modem signal) of a digital representation (a document image) of analog data (an original document) more than negates any bandwidth advantage of VoIP. In other words, the fax "sounds" simply don't fit in the VoIP channel. An alternative IP-based solution for delivering fax-over-IP called T.38 is available.

The T.38 protocol is designed to compensate for the differences between traditional packet-less communications over analog lines and packet based transmissions which are the basis for IP communications. The fax machine could be a traditional fax machine connected to the PSTN, or an ATA box (or similar). It could be a fax machine with an RJ-45 connector plugged straight into an IP network, or it could be a computer pretending to be a fax machine. Originally, T.38 was designed to use UDP and TCP transmission methods across an IP network. TCP is better suited for use between two IP devices. However, older fax machines, connected to an analog system, benefit from UDP near real-time characteristics due to the "no recovery rule" when a UDP packet is lost or an error occurs during transmission. UDP transmissions are preferred as they do not require testing for dropped packets and as such since each T.38 packet transmission includes a majority of the data sent in the prior packet, a T.38 termination point has a higher degree of success in re-assembling the fax transmission back into its original form for interpretation by the end device. This in an attempt to overcome the obstacles of simulating real time transmissions using packet based protocol.

There have been updated versions of T.30 to resolve the fax over IP issues, which is the core fax protocol. Some newer high end fax machines have T.38 built-in capabilities which allow the user to plug right into the network and transmit/receive faxes in native T.38 like the Ricoh 4410NF Fax Machine. A unique feature of T.38 is that each packet contains a portion of the main data sent in the previous packet. With T.38, two successive lost packets are needed to actually lose any data. The data you lose will only be a small piece, but with the right settings and error correction mode, there is an increased likelihood that you will receive enough of the transmission to satisfy the requirements of the fax machine for output of the sent document.
Support for other telephony devices

Another challenge for VoIP implementations is the proper handling of outgoing calls from other telephony devices such as Digital Video Recorders (DVR) boxes, satellite television receivers, alarm systems, conventional modems and other similar devices that depend on access to a PSTN telephone line for some or all of their functionality. These types of calls sometimes complete without any problems, but in other cases they fail. If VoIP and cellular substitution becomes very popular, some ancillary equipment makers may be forced to redesign equipment, because it would no longer be possible to assume a conventional PSTN telephone line would be available in consumer's homes.

Legal issues

As the popularity of VoIP grows, and PSTN users switch to VoIP in increasing numbers, governments are becoming more interested in regulating VoIP in a manner similar to PSTN services.\[42\] Another legal issue that the US Congress is debating concerns changes to the Foreign Intelligence Surveillance Act. The issue in question is calls between Americans and foreigners. The National Security Agency (NSA) isn’t authorized to tap Americans’ conversations without a warrant—but the Internet, and specifically VoIP doesn’t draw as clear a line to the location of a caller or a call’s recipient as the traditional phone system does.\[43\] As VoIP’s low cost and flexibility convinces more and more organizations to adopt the technology, the surveillance for law enforcement agencies becomes more difficult.\[44\] VoIP technology has also increased security concerns because VoIP and similar technologies have made it more difficult for the government to determine where a target is physically located when communications are being intercepted, and that creates a whole set of new legal challenges.\[45\]

In the US, the Federal Communications Commission now requires all interconnected VoIP service providers to comply with requirements comparable to those for traditional telecommunications service providers. VoIP operators in the US are required to support local number portability; make service accessible to people with disabilities; pay regulatory fees, universal service contributions, and other mandated payments; and enable law enforcement authorities to conduct surveillance pursuant to the Communications Assistance for Law Enforcement Act (CALEA). "Interconnected" VoIP operators also must provide Enhanced 911 service, disclose any limitations on their E-911 functionality to their consumers, and obtain affirmative acknowledgements of these disclosures from all consumers.\[46\] VoIP operators also receive the benefit of certain US telecommunications regulations, including an entitlement to interconnection and exchange of traffic with incumbent local exchange carriers via wholesale carriers. Providers of "nomadic" VoIP service — those who are unable to determine the location of their users — are exempt from state telecommunications regulation.\[47\]

Throughout the developing world, countries where regulation is weak or captured by the dominant operator, restrictions on the use of VoIP are imposed, including in Panama where VoIP is taxed, Guyana where VoIP is prohibited and India where its retail commercial sales is allowed but only for long distance service.\[48\] In Ethiopia, where the government is monopolizing telecommunication service, it is a criminal offense to offer services using VoIP. The country has installed firewalls to prevent international calls being made using VoIP. These measures were taken after the popularity of VoIP reduced the income generated by the state owned telecommunication company.

In the European Union, the treatment of VoIP service providers is a decision for each Member State's national telecoms regulator, which must use competition law to define relevant national markets and then determine whether any service provider on those national markets has "significant market power" (and so should be subject to certain obligations). A general distinction is usually made between VoIP services that function over managed networks (via broadband connections) and VoIP services that function over unmanaged networks (essentially, the Internet).

VoIP services that function over managed networks are often considered to be a viable substitute for PSTN telephone services (despite the problems of power outages and lack of geographical information); as a result, major
operators that provide these services (in practice, incumbent operators) may find themselves bound by obligations of price control or accounting separation. VoIP services that function over unmanaged networks are often considered to be too poor in quality to be a viable substitute for PSTN services; as a result, they may be provided without any specific obligations, even if a service provider has "significant market power". The relevant EU Directive is not clearly drafted concerning obligations which can exist independently of market power (e.g., the obligation to offer access to emergency calls), and it is impossible to say definitively whether VoIP service providers of either type are bound by them. A review of the EU Directive is under way and should be complete by 2007.

In India, it is legal to use VoIP, but it is illegal to have VoIP gateways inside India. This effectively means that people who have PCs can use them to make a VoIP call to any number, but if the remote side is a normal phone, the gateway that converts the VoIP call to a POTS call should not be inside India.

In the UAE and Oman it is illegal to use any form of VoIP, to the extent that Web sites of Skype and Gizmo5 are blocked. Providing or using VoIP services is illegal in Oman. Those who violate the law stand to be fined 50,000 Omani Rial (about 130,317 US dollars) or spend two years in jail or both. In 2009, police in Oman have raided 121 internet cafes throughout the country and arrested 212 people for using/providing VoIP services.

In the Republic of Korea, only providers registered with the government are authorized to offer VoIP services. Unlike many VoIP providers, most of whom offer flat rates, Korean VoIP services are generally metered and charged at rates similar to terrestrial calling. Foreign VoIP providers encounter high barriers to government registration. This issue came to a head in 2006 when Internet service providers providing personal Internet services by contract to United States Forces Korea members residing on USFK bases threatened to block off access to VoIP services used by USFK members as a way to keep in contact with their families in the United States, on the grounds that the service members' VoIP providers were not registered. A compromise was reached between USFK and Korean telecommunications officials in January 2007, wherein USFK service members arriving in Korea before June 1, 2007 and subscribing to the ISP services provided on base may continue to use their US-based VoIP subscription, but later arrivals must use a Korean-based VoIP provider, which by contract will offer pricing similar to the flat rates offered by US VoIP providers.[49]

**International VoIP implementation**

**IP telephony in Japan**

In Japan, **IP telephony** (IP電話 IP Denwa ) is regarded as a service applied by VoIP technology to the whole or a part of the telephone line. As of 2003, IP telephony services have been assigned telephone numbers. IP telephony services also often include videophone/video conferencing services. According to the Telecommunication Business Law, the service category for IP telephony also implies the service provided via Internet, which is not assigned any telephone number.

IP telephony is basically regulated by Ministry of Internal Affairs and Communications (MIC) as a telecommunication service. The operators have to disclose necessary information on its quality, etc., prior to making contracts with customers, and have an obligation to respond to their complaints cordially.

Many Japanese Internet service providers (ISP) are including IP telephony services. An ISP who also provides IP telephony service is known as a "ITSP (Internet Telephony Service Provider)". Recently, the competition among ITSPs has been activated, by option or set sales, in connection with ADSL or FTTH services.

The tariff system normally applied to Japanese IP telephony is described below:

- A call between IP telephony subscribers, limited to the same group, is usually free of charge.
- A call from IP telephony subscribers to a fixed line or PHS is usually a uniformly fixed rate all over the country.
Between ITSPs, the interconnection is mostly maintained at VoIP level.

- Where the IP telephony is assigned normal telephone number (0AB-J), the condition for its interconnection is considered same as normal telephony.
- Where the IP telephony is assigned specific telephone number (050), the condition for its interconnection is described below:
  - Interconnection is sometimes charged. (Sometimes, it is free of charge.) In case of free-of-charge, mostly, communication traffic is exchanged via a P2P connection with the same VoIP standard. Otherwise, certain conversions are needed at the point of the VoIP gateway which incurs operating costs.

Since September 2002, the MIC has assigned IP telephony telephone numbers on the condition that the service falls into certain required categories of quality.

High-quality IP telephony is assigned a telephone number, normally starting with the digits 050. When VoIP quality is so high that a customer has difficulty telling the difference between it and a normal telephone, and when the provider relates its number with a location and provides the connection with emergency call capabilities, the provider is allowed to assign a normal telephone number, which is a so-called "0AB-J" number.

Voice over IP can be used together with static IP addresses so that one can talk to any computer just the way one uses internet, but instead he can access IP-address as definitive unique 'Internet VoIP'-phone number...

**Historical milestones**

- 1974 — The Institute of Electrical and Electronic Engineers (IEEE) published a paper titled "A Protocol for Packet Network Interconnection."[50]
- 1981 — IPv4 is described in RFC 791.
- 1985 — The National Science Foundation commissions the creation of NSFNET.[51]
- 1995 — VocalTec releases the first commercial Internet phone software.[52][53]
- 1996 —
  - ITU-T begins development of standards for the transmission and signaling of voice communications over Internet Protocol networks with the H.323 standard.[54]
  - US telecommunication companies petition the US Congress to ban Internet phone technology.[55]
- 1997 — Level 3 began development of its first softswitch, a term they coined in 1998.[56]
- 1999 —
  - The Session Initiation Protocol (SIP) specification RFC 2543 is released.[57]
  - Mark Spencer of Digium develops the first open source Private branch exchange (PBX) software (Asterisk).[58]
- 2004 — Commercial VoIP service providers proliferate.[2]

**Pronunciation**

The acronym VoIP has been pronounced variably since the inception of the term. Apart from spelling out the acronym letter by letter, vē'ō'ī'pē (vee-oh-eye-pee), there are three likely possible pronunciations: vō'ī'pē (vo-eye-pee) and vō'ip (vo-ipp), have been used, but generally, the single syllable vō'y'p (voyp, as in voice) may be the most common within the industry.[59]

**References**

Voice over IP

38


FCC.gov (http://www.fcc.gov/voip/). What are some advantages of VOIP?


FCC Consumer Advisory: "VOIP and 911 Service" (http://www.fcc.gov/cgb/consumerfacts/voip911.html).

Keeping your telephone number when you change your service provider — FCC (http://www.fcc.gov/cgb/consumerfacts/numbport.html).

Volpservice.com (http://www.volpservice.com/sip-trunking/)


"Examining Two Well-Known Attacks on VOIP" (http://www.cirleid.com/posts/examining_two_well_known_attacks_on_voip1/). CircleID. Retrieved 2006-04-05.


ICICNOS.org (http://paper.icicn.org/07_book/200706/20070610.pdf), Secure Voice-over-IP

SANS.org (http://www.sans.org/reading_room/whitepapers/voip/secure_voice_over_ip_322). SANS Institute InfoSec Reading Room


GDC4s.com (http://www.gdc4s.com/documents/D-VIPER-14-1007_p11.pdf), State-of-the-art voice over IP encryptor


Govtrack.us (http://www.govtrack.us/congress/billtest.xsd?/bill=xid=111-30), "Truth in Caller ID Act".

Oldphoneworks.com (http://www.oldphoneworks.com/antique-phone-parts/arts-and-pieces/pulse-to-tone-converters/)

Soft-Switch.org (http://soft-switch.org/foip.html), Faxing over IP networks
Voice over IP

[41] FaxSuperstore.com (http://www.faxsuperstore.com/ricoh-4410nf.html), Ricoh 4410NF
[47] FCC.gov (http://www.fcc.gov/voip/)
[49] Stripes.com (http://www.stripes.com/article.asp?section=104&article=41826&archive=true), Stars and Stripes: USFK deal keeps VoIP access for troops

External links
• Voice over IP (http://www.dmoz.org/Business/Telecommunications/Services/VoIP/) at the Open Directory Project