IP Phone Overview

Basics

A VoIP phone or IP Phone uses Voice over IP (Voice over Internet Protocol - VoIP) technologies for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional public switched telephone network (PSTN).

Digital IP-based telephone service uses control protocols such as the Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP) or various other proprietary protocols.

The overall hardware may look like a telephone or mobile phone. A VoIP phone has the following hardware components.

- Speaker/ear phone and microphone
- Key pad/touch pad to enter phone number and text (not used for ATAs).
- Display hardware to feedback user input and show caller-id/messages (not used for ATAs).
- General purpose processor (GPP) to process application messages.
- A voice engine or a digital signal processor (DSP) to process RTP messages. Some IC manufacturers provides GPP and DSP in single chip.
- AD and DA converters: To convert voice to digital data and vice versa.
- Ethernet or wireless network hardware to send and receive messages on data network.
- Most IP phones have an Ethernet port for a PC. This allows your computer and phone to share one data connection, routed through the phone and to the computer.
- Power source might be a battery or AC source. Some VoIP phones receive electricity from Power over Ethernet.
- Some VoIP phones include an RJ-11 port to connect the phone to the PSTN.

Common functionality and features:

- Caller ID
- Encrypted communications
- Dialing using name/ID (differs from speed dial in that no number is stored on the client)
- Locally stored and network-based directories
- Conference and multiparty call
- Call park
- Call transfer and call hold
- Applications like weather report, Attendance in school and offices, Live news etc.

Technology issues

- Requires Internet access to make calls outside the local area network (LAN) unless a compatible local private branch exchange (PBX) is available to handle calls to and from outside lines.
- VoIP phones and the routers depend on mains electricity for power, unlike PSTN phones, which are supplied with power from the telephone exchange. However, this can be mitigated by installing a UPS. The Power over Ethernet interface simplifies this immensely since power can be "injected" at any connector (especially in passive mode where all devices are drawing the same voltage) or at the router. This is a major reason the dominant call center and PBX VoIP systems rely on PoE exclusively, but UPS and PoE are only helpful if the upstream Internet provider also has reliable backup power.
- IP networks, particularly residential Internet connections are easily congested. This can cause poorer voice quality or the call to be dropped completely. As commercial grade routers begin to incorporate "managed" or "carrier" QoS features, this is less of an issue, but such features typically require expert configuration.
- VoIP phones, like other network devices can be subjected to denial-of-service attacks as well as other attacks especially if the device is given a public IP address;[1] This is especially significant as an issue with wireless devices using 802.11 protocols.
- Due to the latency induced by protocol overhead and other factors they do not work as well on satellite Internet, analog cell ("edge" networks) and other high-latency Internet connections. Extremely latency sensitive applications (music, remote device control) as of 2012 simply cannot exploit VoIP protocols.
- Proprietary vendors such as Skype and Google Voice focus on improving call quality between their own users to grow their user base, which to some degree competes and conflicts with the goal of better connections from Skype to Google Voice, or from either to the existing PSTN and cellular networks. The best codecs tend to be proprietary and not licensed to competitors, retarding the growth of the industry and causing incompatibility.

(http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701)

Quality of Service (QoS) is vital for the success of VoIP since few will use it if VoIP can not deliver at least the same voice quality as traditional telephone network. The QoS for VoIP is mainly affected by latency, jitter (delay variation) and packet loss.

Latency in VoIP refers to the time it takes for a voice transmission to go from its source to its destination. The ITU-T recommendation G.114 establishes a number of time constraints on one-way latency. The upper bound for domestic calls is 150 ms for one-way traffic. This time constraint limits the amount of security that can be added to a VoIP network. In the worst cases, there is only 20-50 ms left for security implementation since encoding and traveling might take 100-130ms.

Jitter refers to non-uniform packet delays. Introducing discontinuity in audio stream, jitter is more detrimental to QoS than the actual delays themselves. Jitter is often caused by low bandwidth situation in VoIP.

VoIP is intolerant of packet loss. VoIP packets are very small, containing a payload of only 10-50 bytes, which is approximately 12.5-62.5ms. Therefore, occasional one packet loss is not so significant. That's one reason why VoIP packets are transmitted by UDP instead of TCP. Even with less than 150ms of latency, a packet loss of 5% caused VoIP traffic encoded with G.711 to drop below the QoS levels of the PSTN, even with a packet loss concealment scheme. "Tolerable loss rates are within 1-3% and the quality becomes intolerable when more than 3% of the voice packets are lost"

Security

(http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701)

Security Guidelines for VoIP

1. **Develop appropriate network architecture**: It is a good practice to separate voice and data on logically different networks if feasible due to their different QoS requirements. At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network. Use strong authentication and access control on the voice gateway system, as with any other critical network component A mechanism to allow VoIP traffic through firewalls Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. USE IPsec or Secure Shell (SSH) for remote management and auditing access. If performance is a problem, use encryption at the router or gateway, to provide IPsec tunneling.
2. **VoIP-ready firewalls and other appropriate protection mechanisms should be employed.** Because of the inherent vulnerabilities of operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. “Defense in depth”. VoIP-ready firewalls are essential components in the VoIP network and should be used. If permitted, state-of-the-art intrusion detection and prevention systems should also be installed.
3. **Do not use Softphone system:** In practical, “softphone” system, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern. Worms, viruses and other malicious software are extraordinarily common on PCs connected to the internet and very difficult to defend against. If mobile units are to be integrated with the VoIP system, use products implementing WiFi protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).
4. **Tighten physical security control:** Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially tap into telephone conversions. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis or compromise the systems. Adequate physical security should be in place to restrict access to VoIP components.
5. **Implement power back up system:** Sufficient backup power should be available for the office VoIP switch, desktop instrument. There should be enough electrical power to maintain UPS battery charge. Backup power system should be periodically checked to make sure that they are ready when power is out.
6. **Maintain current patch levels:** Vulnerability in the operation system, software, and servers are the targets of attackers. Patching all the systems in the network is not easy.
7. **Install anti-virus system and update it regularly**: Viruses and worms are still the top concerns for computer security. The viruses might break down the system and disable the service.
8. **Apply encryption selectively:** Encryption is necessary to defeat eavesdropping attack. Transport layer security and IPsec are two main encryption methods. TLS is an alternative to IPsec and is based off the SSL protocol. Many different algorithms can be used such as DES, 3DES, AES, RC4 and RC5. The simpler encryption results in better performance.

(http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/do_business_better/how_to_protect_your_voice/index.html)

VoIP risks extend beyond toll fraud, voicemail hacks, and eavesdropping. IP phones can be entry points into your business network. VoIP calls and voicemail messages are data, susceptible to data network attacks.

Whether you use a hosted IP phone service or an onsite VoIP system, protecting the voice network is much like protecting the data network. The security policies and technologies can be complex, depending on your goals (including compliance requirements), users' applications and locations, and the IP phone system you're using, whether onsite or hosted. Fortunately you can engage VoIP experts to strengthen and simplify your company's security.

Suggestions:

- Configure Dial Plans and User Profiles
- Take advantage of features on your VoIP system that enable security. Essentially:
- Control voice network access by device certificate and/or user name and password.
- Restrict the types of calls allowed on the network, by device, user, and other criteria, such as time of day.
- Set up a firewall and intrusion prevention system (IPS) to monitor and filter authorized and unauthorized VoIP traffic, and track unusual voice activities.
- Lock voice servers physically, and logically for administration. Centralize administration and use domain restrictions and two-factor authentication for administrative access, including to credentials, signaling data, and configuration files.
- Regularly install OS updates, and limit software loading on phones.
- Use VLANs to Segment Voice Traffic and Separate It from Data Traffic
- Apply encryption by segment, device, or user; encrypting indiscriminately can result in excessive network latency or introduce operational overhead and complexity.
- Encrypt the signaling at your Internet gateway with Session Initiation Protocol (SIP) over Transport Layer Security (TLS); your service provider's switch fabric may do this.
- Encrypt the media (packets) with protocols such as SRTP.
- Use VPNs for network connections by remote phones. This is especially important when HTTPS or SRTP is unavailable.
- Implement Strict Security Policies with Users:
    - Communicate your phones' built-in security features to users.
    - Apply strong passwords to access the voicemail inbox. Immediately change the default password to a strong password, then change it as often as your company's policy dictates for changing login and email passwords.
    - Delete sensitive voicemail messages as soon as users have listened to them. Not storing voicemails is the easiest and most effective way to protect them.

- Immediately report anomalies. You may not know a phone has been hacked until an employee reports an odd occurrence, such as a saved voicemail message that has been deleted or forwarded to an unusual number.

Vulnerabilities

(http://www.sans.org/reading-room/whitepapers/voip/voip-security-vulnerabilities-2036)

(http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701)

- **Confidentiality threats**: Confidentiality means that the information can not be accessed by unauthorized parties. The confidential information of end users includes private documentation, financial information, security information like password, conversion content, conversion history or pattern, etc. The confidential information for network components includes operation systems, IP addresses, protocols used, address mapping, user records, etc. Leak of this information might make attackers' jobs easier.
    - **Eavesdropping of phone conversation:** Conventional telephone eavesdropping requires either physical access to tap a line, or penetration of a switch. With VoIP, opportunities for eavesdroppers increase dramatically because of the large number of nodes in the path between two conservation entities. If the attacker compromises any of theses nodes, he can access the IP packets flowing through that node. There are many free network analyzers and packet capture tools that can convert VoIP traffic to wave files. Theses tools allow the attackers to save the conversation into the files and play them back on a computer. VoMIT (Voice over Misconfigured Internet Telephones) is an example of such a tool. Ethreal can also be used to record SIP packets and retrieve voice message in wav file format.
      Countermeasures: Encryption of voice message packets can protect against eavesdropping. IPSec can be deployed to encrypt whole packets. SRTP can provide confidentiality, message authentication and replay protection for audio and video streams.
    - **Unauthorized access attack:** Unauthorized access means that the attacker(s) can access resources on a network that they do not have the authority. Shawn Merdinger reported multiple undocumented ports and services in certain VoIP phones. There are also vulnerabilities due to implementation issues. There are systems for call control, administration, billing and other voice telephone functions. Repositories in these systems may contain passwords, user identities, phone numbers, and private personal information. Lots of gateways and switches are shipped with default well-known passwords. If these passwords are left without changes, the attackers can easily break in. Some switches still use TELNET for remote access. The clear-text protocol exposes everything to anyone who can sniff the network traffic. Some of the gateways or switches might have a web server interfaces for remote control. The attacker might sniff the HTTP traffic in local network to steal sensitive information. Attackers can also use ARP cache poisoning to forward all traffic through their machines to capture network traffic.
      Countermeasures: To better protect gateways and switches, they should use SSH instead of ther clear-text protocols as remote access protocol. If web-based interface is provided, HTTPS should replace HTTP. In addition, all default passwords should be

changed before the system is plugged into the network. A up-to-date intrusion detection system might detect ARP poisoning and other types of attacks.

- **Integrity Threats:** Integrity of information means that information remains unaltered by unauthorized users. A legitimate user may perform an incorrect or unauthorized operations function and may cause delirious modification, destruction, deletion or disclosure of switch software and data. An intruder may masquerade as a legitimate user and access an operation port of the switch.
    - **Caller Identification spoofing**: Caller ID (Caller Identification) is usually a service provided by most telephone companies that tell users the phone number of an incoming call. Caller Identification spoofing is setting the Caller ID on the outgoing calls to a 10 digit number of the caller's choice. Several websites provide Caller ID spoofing service eliminating the need for any special hardware.
      The caller ID service relies on the "From" header to supply the identity. Call-ID contains a globally unique identifier for this call and has nothing to do with Caller ID. If the attacker can control the gateway server, he can arbitrarily change "From" header to anything that he wants. The recipient will send back acknowledgment to this proxy server, which is the same as "via" field. The proxy server can then forward the acknowledgment to Alice since it knows the real IP address of Alice's phone. The popular proxy server software Asterisk is open source and very flexible to customize. This only makes things worse.
      Countermeasures: Unfortunately, there is no effective way to prevent caller ID spoofing. The best solution so far is not to trust caller ID at all.
    - **Registration hijacking**: Registration hijacking happens when an attacker replace the legitimate registration of the victim with his address. The attack causes all incoming calls for the victim to be sent to the attacker's address. Registration is normally performed using UDP, which make it easy to spoof registration requests. For example, Alice wants to register her address at registrar using SIP protocol. The "REGISTER" message looks like the following:

      ```
      REGISTER sip:alice@atlanta.com SIP/2.0
      Via: SIP/2.0/UDP 192.168.2.10;branch=z9hG4bK776asdhds
      Max-Forwards: 70
      To: Alice <sip:alice@atlanta.com>
      From: Alice <sip:alice@atlanta.com>;tag=1928301774
      Call-ID: a84b4c76e66710@192.168.2.3
      CSeq: 314159 INVITE
      Contact: Alice <sip:alice@192.168.1.11:5061>;expire=60
      Content-Type: application/sdp
      Content-Length: 142
      ```

      In this message, the "To" and "From" fields use the same user information. The "contact" field contains a SIP URI that represents a direct route to the device. In this example, it is IP address 192.168.1.11 and the port is 5061. "expires=60" means that the registration will expire in 60 seconds. Another REGISTER request should be sent to

refresh the user's registration.
The attacker can construct a similar REGISTER message with modified "contact" header.
Countermeasures: Stronger authentication schemes are the solutions to registration spoofing, proxy impersonating and call hijacking. To mitigate this type of attacks, software patching is crucial to fix any known vulnerabilities. VoIP vulnerability scanning tools are strongly suggested.

- **Proxy Impersonation**: Proxy impersonation attack tricks the victim into communicating with a rogue proxy set up by the attacker. Once an attacker impersonates a proxy, he has complete control of the call. Figure 8 illustrates proxy impersonation. The attacker tricks Alice to communicate with the rogue proxy server instead of the legitimate proxy server. The UAs and proxies normally communicate using UDP and do not require strong authentication to communicate with another proxy. The attack can work by several means, including DNS (Domain Name Service) spoofing, ARP (Address Resolution Protocol) cache spoofing, DHCP spoofing, or changing proxy address for a SIP phone.
  Countermeasures: Stronger authentication schemes are the solutions to registration spoofing, proxy impersonating and call hijacking. To mitigate this type of attacks, software patching is crucial to fix any known vulnerabilities. VoIP vulnerability scanning tools are strongly suggested.
- **Call redirection or hijacking**: Call redirection occurs when a call is intercepted and rerouted through a different path before reaching the destination. Possible methods include proxy impersonation and registration spoofing. The attacker can also spoof the response from the recipient and trick the requestor to talk with the attacker. Call redirection or hijacking enables the attacker to eardrop even encrypted voice conversation. The attacker also can tamper the voice message sent both ways. They can also carry out replay attacks.
  Countermeasures: Stronger authentication schemes are the solutions to registration spoofing, proxy impersonating and call hijacking. To mitigate this type of attacks, software patching is crucial to fix any known vulnerabilities. VoIP vulnerability scanning tools are strongly suggested.

- **Availability threats:** Availability refers to the notion that information and services are available for use when needed. VoIP network is susceptible to denial of service attacks since DoS attacks can degrade QoS quickly to unacceptable level. Traditional DoS attacks against data networks are still very dangerous. However our focus is about VoIP specifics DoS attacks.
  - **VoIP Signaling DoS Attacks**: The attackers can abuse signaling protocol to conduct denial of service attacks. In first case, the attackers can create large number of call setup requests that consume the processing power of proxy server or terminal. One example is shown in Figure 10(a) where Tim sends way too many "invite" requests to Bob and Bob can not take request from Alice. This type of DoS attack does not have same LAN requirement. It only needs large volumes of requests to flood the victim. The attackers can also launch distributed DoS to cover trace and aggregate requests. In the second case, the attackers use cancellation of pending call set up signals including sending a CANCEL, GOODBYE or PORT UNREQACHABLE message. This causes the phone not being

able to complete calls or hang up. This type of attacks is aided by the complexity of the signal protocols. University of Oulu in Finland has developed simple SIP and H.323 protocol test suites and run them against several implementations. The results were "alarming", indicating that virtually all of the testbed components failed [20]. Figure 10(b) shows an example where CANCEL message is spoofed by the attacker to prevent call setup. Figure 10(c) gives an example where spoofed GOODBYE message tear down the established connections. One correctly crafted packet can tear down the call. However, this attack does require the attacker to be able to fill certain headers of the message correctly. The attacker can gather network data to extract this information.
Countermeasures: To mitigate VoIP signaling and media DoS attacks, strong authentication is the key. VoIP components need to make sure that they are communicating with legitimate counterparts. VoIP firewall should also be implemented to monitor streams and filter out abnormal signals and RTP packets. Media and signal rate limits can be set by observing normal traffic patterns.

- **VoIP Media DoS Attacks:** Attackers can flood gateway, IP phone and other media processing VoIP components with large number of RTP packets. If the target is forced to drop RTP packets, the voice quality will degrade. Furthermore, the attacker might knock key components like gateway offline. A failure in one of these devices could bring the entire voice network to a halt. Since RTP is encapsulated in UDP, it is easy to craft.
  Countermeasures: To mitigate VoIP signaling and media DoS attacks, strong authentication is the key. VoIP components need to make sure that they are communicating with legitimate counterparts. VoIP firewall should also be implemented to monitor streams and filter out abnormal signals and RTP packets. Media and signal rate limits can be set by observing normal traffic patterns.
- **Physical DoS Attacks:** These attacks include power outrage and physical damage to network components. Traditional telephone operate on 48 volts supplied by the telephone line itself and can operate smoothly during a power failure. VoIP can not operate without power supply. Also, an attacker with physical access to any key components of VoIP network can disrupt its normal operations easily. He can plug out the power cord or network cable.
  Countermeasures: To mitigate physical DoS attacks, strict physical security schemes should be implemented with restricted areas, access control, locks, guard, etc. To guarantee continuous power supply, backup power generation system should be available.

(http://arstechnica.com/security/2013/01/hack-turns-the-cisco-phone-on-your-desk-into-a-remote-bugging-device/)

Among other things, the hack allows attackers to monitor phone calls and to turn on the phone's microphone in order to eavesdrop on conversations within earshot and stream them over the network.

Codecs

(https://askozia.com/voip/what-is-a-codec/)

A codec defines how audio (and video) is transported over a network and the quality of the voice. If the speech quality is too low it might make sense to try a different codec. A common reason for bad audio quality when using Voice over IP is insufficient bandwidth of the internet connection.

Generally, we differentiate between codecs which use compressed and uncompressed data. We also differentiate between lossless and lossy compression. A codec is always a compromise between used bandwidth, required CPU power for the compression of voice data and the overall speech quality. Wideband codecs make voice transmission in hi-fi Quality possible. Narrowband codecs allow voice transmission even with poor bandwidth. Consequently, speech quality drops. We recommend a bandwidth of 100 kBit/s in both directions for good quality.

Audio Codecs for IP phone systems: Mean Opinion Score (MOS) is a measurement method for comparing codecs. A representative group evaluates how close speech quality of the codecs is to the human original. The scale is 1 (bad) to 5 (best). Everything better than 4 meets the speech quality of ISDN.

Codec Overview

Codec	Bandwidth	MOS-Score	Quality
G.711u-law	155 kBit/s	4,3	good (USA and Japan)
G.711A-law	180 kBit/s	4,4	very good (Europe)
GSM	60-90 kBit/s	3,8	satisfying
G.722	180 kBit/s	4,5	very good
G.723.1	60 kBit/s	3,8	satisfying
G.726 (AAL2)	100 kBit/s	3,8	satisfying
G.726 (RFC3551)	120 kBit/s	3,8	satisfying
G.729	70 kBit/s	3,92	satisfying
iLBC	80 kBit/s	4	satisfying
SpeeX	60-120 kBit/s	4	satisfying
ADPCM	16-64 kBit/s	-	-
16 bit Signed Linear PCM	64 kBit/s	4	satisfying
LPC10	2,4 kBit/S	-	-

Video Codecs for IP phone systems: H.261 is one codec for digital compression and decompression of video signals. Originally developed for video telephony via ISDN lines. H.261 was the first digital video standard codec. H.263 (from 1995) and H.264 (from 2001) are based on H.261. All standards are optimised for low data transfer rates. Constant data transfer rates are not defined. H.264, as the newest standard, can also handle high resolution images.

Protocols

(http://www.sans.org/reading-room/whitepapers/voip/security-issues-countermeasure-voip-1701)

VoIP needs two types of protocols: signaling protocol and media protocols. Signaling protocols manage call setup and teardown. Examples of signaling protocols include H.323, SIP, MGCP, Megaco/H.248 and other proprietary protocols like UNISTIM, SCCP, Skype, CorNet-IP, etc. Media protocols manage the transmission of voice data over IP networks. Examples of media protocols include RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol), SRTP (Secure Real-time Transport Protocol) and SRTCP (Secure RTCP). A diagram of VoIP protocols is shown in Figure 5. Signaling protocols are generally transported by TCP for the benefit of reliability. Media protocols are always transmitted by UDP.

(http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/4_0_1/ccmsys/a08procl.html)

- **H.323 Protocol**: The International Telecommunications Union (ITU) developed the H.323 standard for multimedia communications over packet networks. As such, the H.323 protocol is a proven ITU standard and provides multivendor interoperability. The H.323 protocol specifies all aspects of multimedia application services, signaling, and session control over an underlying packet network. Audio is standard on H.323 networks, but networks can be scaled to include both video and data. The H.323 protocol can be implemented in large enterprise networks or can be deployed over an existing infrastructure, which makes H.323 an affordable solution.
  The basic components of the H.323 protocol are terminals, gateways, and gatekeepers (which provide call control to H.323 endpoints). Similar to other protocols, H.323 applies to point-to-point or multipoint sessions. However, compared to MGCP, H.323 requires more configuration on the gateway.
- **Media Gateway Control Protocol (MGCP):** MGCP provides a powerful, flexible and scalable resource for call control. MGCP is used to control media on the telephony interfaces of a remote gateway and to deliver messages from a remote gateway to appropriate devices.
  MGCP enables a call agent (media gateway controller) to remotely control and manage voice and data communication devices at the edge of multiservice IP packet networks. Because of its centralized architecture, MGCP simplifies the configuration and administration of voice gateways and supports multiple (redundant) call agents in a network. MGCP does not provide security mechanisms such as message encryption or authentication.
  MGCP controls call processing and routing and provides supplementary services to the gateway. The MGCP gateway provides call preservation (the gateway maintains calls during failover and fallback), redundancy, dial-plan simplification (the gateway requires no dial-peer configuration), hookflash transfer, and tone on hold. MGCP-controlled gateways do not require a media termination point (MTP) to enable supplementary services such as hold, transfer, call pickup, and call park.
- **Skinny Client Control Protocol (SCCP)**: SCCP uses proprietary messages to communicate between IP devices and the call manager. SCCP easily coexists in a multiple protocol environment. The IP Phone is an example of a device that registers and communicates with the call manager as an SCCP client. During registration, an IP phone receives its line and all other

configurations from the call manager. Once it registers, it is notified of new incoming calls and can make outgoing calls. The SCCP protocol is used for VoIP call signaling and enhanced features such as Message Waiting Indication (MWI).

- **SIP**: The Internet Engineering Task Force (IETF) developed the SIP standard for multimedia calls over IP. ASCII-based SIP works in client/server relationships as well as in peer-to-peer relationships. SIP uses requests and responses to establish, maintain, and terminate calls (or sessions) between two or more end points.
- **QSIG**: The QSIG protocol is a series of international standards that define services and signaling protocols for Private Integrated Services Networks (PISNs). These standards use ISDN concepts and conform to the framework of International Standards for Open Systems Interconnection as defined by ISO/IEC. The QSIG protocol is a variant of ISDN D-channel voice signaling. It is based on the ISDN Q.921 and Q.931 standards and is a worldwide standard for PBX interconnection. The integration of QSIG protocol support with voice over IP (VoIP) enables voice switching services to connect to PBX's, key systems, and central office (CO) switches that communicate by using QSIG protocol. Devices can route incoming voice calls from a private integrated services network exchange (PINX) device across a WAN to a peer device that can transport the signaling and voice packets to a second PINX device. PINX devices can be PBXs, key systems, or other nodes that support QSIG protocol.
  In a network that supports QSIG protocol, a user in a PINX can place a call to a user that is in a remote PINX. The called party receives the caller's name or number as the call rings. If the called party is not available, the call forwards to another destination or to a voice-messaging system. All the features that are available as a PBX user operate transparently across the network. QSIG protocol provides supplementary and additional network features, as defined for PISNs.

(http://www.protocols.com/pbook/voipfamily.htm): This link includes a list of all protocols used by VoIP.