

CPNI VIEWPOINT 03/2007

HOSTED VOICE OVER IP

AUGUST 2007

Abstract

Voice over IP (VoIP) is the term used for a set of technologies that enable real time voice or video conversations to take place across IP networks. VoIP devices and networks may interface with the Public Switched Telephone Network (PSTN). Enterprise VoIP, described in Viewpoint 02/2007, encompasses systems deployed by larger organisations that would traditionally run internal telephony services. This Viewpoint discusses the special case of Hosted VoIP, in which the corporate VoIP telephony system is hosted and managed by a third party network operator or service provider. Internet VoIP, which involves peer-to-peer telephony via the public Internet, is described in Viewpoint 01/2007.

CPNI Viewpoints

CPNI Viewpoints are intended to provide a management level overview of emerging risks. A Viewpoint may not necessarily offer mitigation advice; other CPNI products are available for this purpose.

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

KEY POINTS

- Organisations considering VoIP should carry out a full risk assessment to understand the value of voice communications to their business, and enable an adequate approach to providing security measures.
- VoIP allows shared physical media to be used for voice and data; this enables savings on infrastructure and operating charges but can bring new risks to business critical communications.
- If the business wishes to maintain the level of confidentiality available on current voice systems, logical or physical separation of voice and data will be required on internal networks.
- Internet and data network performance can have a critical impact on the reliability of VoIP services.
- Risk mitigation measures need to be built in at the design stage and cannot easily be added later.
- An organisation can reduce capital expenditure by outsourcing the control and management of its corporate VoIP infrastructure to a network operator or service provider who will 'host' the control elements.
- Hosted VoIP infrastructure can be dedicated to one customer or shared amongst many. There are cost and security trade-offs to make when choosing between the two approaches.
- Retaining an emergency telephony capability in the event of power loss, or the interruption of access to the service provider, will require planning and investment.
- Some local Public Switched Telephone Network capabilities can be maintained to provide service backups in failure or emergency conditions.
- It is possible that the components that make up a Hosted VoIP service are not all UK based, which could have legal and policy implications.

INTRODUCTION

The traditional Public Switched Telephone Network (PSTN) infrastructure, and voice telephony in general, is in transition from a Time Division Multiplex (TDM) based, circuit-switched architecture; to an Internet Protocol (IP) based, packet-switched architecture, commonly referred to as Voice over IP (VoIP). One of the fundamental properties of the VoIP implementations is the use of common media for speech, signalling and control data.

The use of a common medium for carrying both voice and data traffic is seen as an advantage in that users and providers can make great savings on capital expenditure (capex) and operating costs (opex). The use of a common medium also brings a number of risks to business communications that should be balanced against the cost savings in any proposed or planned implementation, and actively managed.

The convergence of voice and data into IP based communications allows VoIP adopters to implement applications (for example contact centres) that integrate voice and data in a very flexible manner.

Telephony networks are mission critical to an organisation and it is therefore vital to understand the potential security risks a move to VoIP could expose, and to ensure any implementation minimises those risks.

Enterprise VoIP is the term given to VoIP implementations that provide facilities equivalent to the corporate telephone exchange systems that would normally be deployed by large companies.

Hosted VoIP is the term given to a type of Enterprise VoIP in which a third party VoIP provider remotely hosts the systems that support the VoIP-based subscriber equipment on the user's desk.

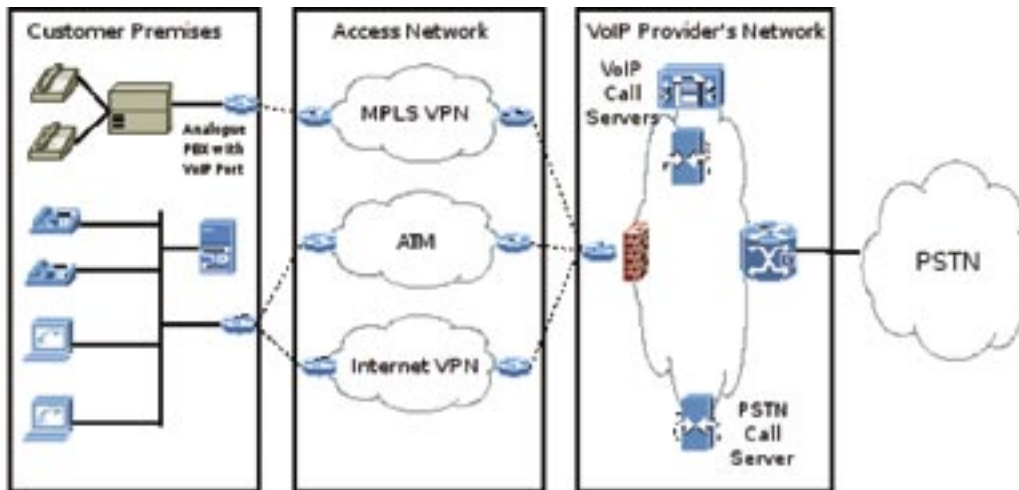
Organisations planning to implement a VoIP service should read this Viewpoint in conjunction with Viewpoint 02/2007, 'Enterprise VoIP'.

There are three distinct technology aspects involved in deploying Hosted VoIP, represented in Table 1 below.

Table 1. Technology Aspects

Customer Premises Equipment	Includes IP phones and soft phones, and any hardware devices supplied to the customer that support internal calls in the event of network failure. There may also be interfaces to legacy telephone exchange systems and phones.
Access Network	The access network links the customer network to the VoIP service provider. Many network technologies are used, depending upon the required bandwidth, reliability and cost.
VoIP Service Provider Network	The VoIP service provider will host all systems that support call setup, provision, billing and interfaces with the PSTN.

Figure 1. Hosted VoIP Overview



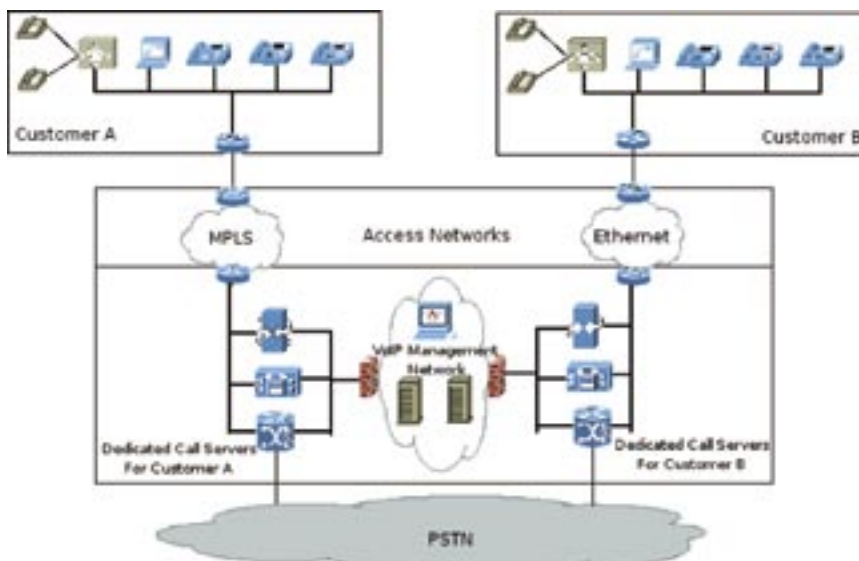
VoIP systems require Call Servers to provide all the facilities usually supplied by a local corporate telephone exchange. Call switching, messaging and feature services, call logging and billing, and the interface with the PSTN are all provided by various VoIP call servers. The degree to which a Hosted VoIP service provider shares these resources between customers influences not only the cost but also the security of the overall solution.

There are two types of Hosted VoIP; Multi-Instance and Multi-Tenancy Hosted VoIP.

Multi-Instance Hosted VoIP

In a Multi-Instance Hosted VoIP deployment the VoIP Provider employs separate call processing systems for each customer (see Figure 2). Cost benefits to the customer over a local Enterprise VoIP deployment come largely from leveraging the service provider's existing management resources, by sharing support services between multiple customers.

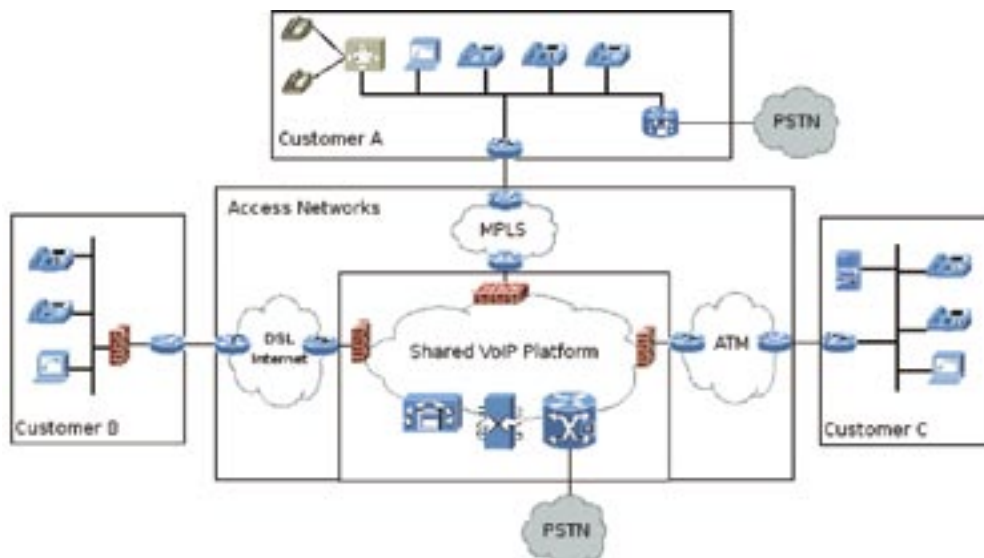
Figure 2. Multi-Instance Hosted VoIP



Multi-Tenancy Hosted VoIP

Multi-Tenancy hosted VoIP deployments use the same call processing systems to handle multiple customers (see Figure 3). Multi-tenancy systems are usually considerably cheaper and quicker to provision than Multi-Instance systems.

Figure 3. Multi-Tenancy Hosted VoIP



Multi-Tenancy Hosted VoIP systems are frequently described as 'IP Centrex' systems, a reference to traditional Centrex services that provide corporate telephone exchange type facilities on central switches belonging to the network operator. Some systems use VoIP to provide customer connectivity, and continue to use a traditional Digital Local Exchange for network functions. Others provide a pure VoIP switching platform (often called a 'Soft Switch') and only interface with the PSTN when required.

Hosted VoIP services can provide significant capex and opex savings, by reducing the amount of technology requiring local deployment, and the need to hire specialised support staff. Some capital investment may, however, be required to enhance the internal network infrastructure, as the VoIP protocols are less tolerant to network congestion than desktop PC applications.

PLANNING

The deployment of any VoIP system requires careful consideration. From a functional point of view a VoIP system appears similar to a traditional corporate telephone exchange/PSTN based solution, but the use of the data network as the voice transport can impact existing data network facilities considerably. It is important to ensure that both voice and data network support staff work together with the Hosted VoIP provider to ensure that a reliable and secure solution is deployed.

A formal risk assessment of a Hosted VoIP deployment is strongly advised. To facilitate such a risk assessment, the importance of the use of voice across the business with regards to confidentiality, integrity and availability should be understood.

The support for encryption in VoIP devices varies between manufacturers, and due to the shared nature of call servers in Multi-Tenancy configurations, is more likely to be offered in Multi-Instance scenarios. If encryption of VoIP traffic is going to be a requirement, the capabilities of potential Hosted VoIP service providers should be checked.

In order to accept an incoming VoIP call, a network connection must be accepted from the caller. With a Hosted VoIP scenario, inbound connections will originate from the service provider. Allowing network connections into an IP network from an external source is not generally considered to be desirable from a security point of view. When implementing Hosted VoIP CNI organisations must either;

- Trust the Hosted VoIP service provider to allow only genuine connections into the corporate network, in which case the security the provider has in place must be understood in detail, or
- Implement additional firewall or proxy systems to control inbound calls.

The service provider may supply customer premises equipment for installation on the client site. Such systems may be used to give backup access to the PSTN in the event of network failure, or provide local call switching for VoIP calls that do not need to go off the local network. The method used to manage such devices should be examined, as this may require remote network access by the service provider.

In general, to make a VoIP call, signalling traffic for call set-up will traverse the access network to the service provider, even to set up calls between internal users. Voice traffic between internal extensions will not traverse the access network, but voice traffic to off site destinations will.

The access network linking the VoIP switching systems operated by the service provider to the client site can be implemented using a variety of transport technology with the required bandwidth, latency and cost. The security measures provided by the access network should be assessed for suitability. For example, if the confidentiality of voice conversations were considered important, the use of the Internet as an access network without any encryption would not be appropriate.

The hosting service provider will be responsible for sizing their access networks accordingly, but it may also be necessary to upgrade internal LANs to guarantee acceptable service. Service providers may offer site survey services to check that internal LANs can provide adequate performance.

As the service provider hosts much of the call processing capability remotely, it is important to consider the business impact that any loss of connectivity to that provider would cause. Many services give the option of customer premises equipment that implement 'survivable proxies', which enable internal VoIP communications to continue in the event of link failure to the central systems. It may also be possible to specify the provision of backup PSTN circuits to support off network calls in the event of access network failure.

Some providers may be able to offer multiple access points with diverse routing in their access networks, thereby reducing the risk of loss of the voice service.

The service provider should be asked whether they operate a regular maintenance schedule for their systems, and what the likely effect maintenance will have on your telephony access.

If the access network is not dedicated to the Hosted VoIP service, care must be taken to ensure the

full implications of the loss of the shared connection are understood. For example, when planning for downtime on an Internet connection, one would not traditionally expect the loss of telephony service during the outage, but this would be the case if the same Internet connection were being used as the access network to a VoIP provider.

Inbound Internet VoIP (often called inbound SIP calling) could open the organisation's telephony service to attacks such as SPIT or denial of service. The potentially low cost of Internet VoIP should therefore be balanced against the increased risk of attack. The service provider should be asked if they permit inbound Internet VoIP calls into their environment and if so, what controls are placed on such calls. Internet VoIP is discussed in Viewpoint 01/2007.

Many service providers give their customers access to web based provisioning and billing systems. Even when private access networks are used for VoIP connectivity, the web provisioning and billing systems will usually be accessed via the Internet. It is important to ensure the provider pays adequate attention to securing such systems, and that access is limited to only those people that require it.

It is important to know the physical locations of the systems used by the Hosted VoIP service provider. If systems are used that are not operated in the UK, it is possible that important information like call records and billing data may be subject to regulatory and legal provisions other than those imposed in the UK. The transfer of data outside of the EU may also expose corporate information, and increase the risks to confidentiality, integrity and availability of the data.

EMERGENCY CALL HANDLING

PSTN 999 calls are delivered by service providers under a Universal Service Obligation (USO), as determined by the industry regulator, Ofcom. Facilities such as caller ID and location information, as well as service survivability in the event of power failure are all catered for. Hosted VoIP systems add some additional functionality that can complicate the provision of caller ID and location information. It may be necessary to carefully update any web based self-service system to ensure a correct map of extension and location information is maintained.

VoIP endpoints may be unable to set-up emergency calls if access to the Hosted VoIP service is lost. One solution is to implement survivable proxies with local PSTN connections, which can handle emergency calls locally. This solution also solves some of the caller ID and location issues, allowing the building address to be identified, if not the caller.

Gaining emergency assistance in the event of conditions such as power failure may be difficult via VoIP systems, as network-switching equipment is not always resilient to power failure. It may be necessary to invest in a resilient infrastructure. Alternatively emergency procedures may need to be reviewed and external PSTN lines provided for emergency use. In this case staff must be made aware of which telephones can be used in emergency or power loss situations.

CONCLUSION

There are many ways in which Hosted VoIP systems can be implemented, potentially saving corporate users in both capex and opex. It is vital however to understand the security arrangements made by a potential service provider before subscribing to their service. When switching any service to new technology it is important to assess the risks that may be introduced and to mitigate against them where necessary. VoIP is potentially more susceptible to call interception and modification than a traditional corporate telephone exchange based-system, unless steps are taken to ensure that the VoIP signalling and media connections are secured. Even though the bulk of the service provision may be outsourced in a Hosted VoIP scenario, service levels can easily be compromised, and security risks can be introduced, by making inadequate internal network provision. As with any technology, security is cheaper and easier to build in during the planning phase, than it is to bolt on after deployment.

Use of VoIP systems may compromise the ability to make emergency 999 calls, and adequate provision must be made to compensate for this.

USEFUL LINKS

<p>www.voipsa.org</p>	<p>VoIP Security Alliance: A collaboration between vendors, service providers and industry leaders that aims to promote the adoption of VoIP by improving security research, education and awareness. In particular, see the 'VOIPSA Threat Taxonomy' dated 24 October 2005.</p>
<p>www.hackingvoip.com/sec_tools.html</p>	<p>An illustration that risk mitigation is an important activity during Enterprise VoIP implementation, this web page lists currently available tools discussed in a forth-coming book that can be used to compromise VoIP if sufficient controls are not implemented.</p>
<p>www.blueboxpodcast.com</p>	<p>A weekly roundup of VoIP security related issues produced by VOIPSA member Dan York.</p>
<p>www.cpni.gov.uk</p>	<p>A number of products giving advice on related subjects including: NISCC Technical Note 01/07 IPsec VPN Security Guide dated 4 January 2007 CPNI Viewpoint 01/2007 'Internet VoIP' dated August 2007 CPNI Viewpoint 02/2007 'Enterprise VoIP' dated August 2007 UK NSIE 'VOIP Security Considerations for Service Providers' dated July 2007</p>
<p>www.ofcom.org.uk</p>	<p>The telecommunications industry regulator: The Ofcom website contains a description of the telecommunications marketplace, including details of the Authorisation Regime.</p>

GLOSSARY

802.1Q	An IEEE standard that defines the use of Virtual LANs (VLANs)
802.1X	An IEEE standard that defines port based network access control.
ACL	Access Control List: In networking an access control list defines the communications permitted between specific source and destination locations.
Circuit switched	A circuit switched network is one that establishes a dedicated circuit between endpoints before any communication occurs. Each circuit created cannot be used by other callers until the circuit is released and a new connection is set up.
DHCP	Dynamic Host Configuration Protocol: Defined by the IETF standard RFC 2131, DHCP is used by networked systems to obtain IP addresses and other parameters to allow network operation.
DLE	Digital Local Exchange
DTMF	Dual-tone Multi-frequency: A line code used for signalling to and from the traditional telephone instrument.
DNS	Domain Name System: Defined in the IETF standards RFC 1034 and 1035, DNS provides a mechanism to resolve host names to IP address information.
Endpoint	Within this document the term 'Endpoint' is used to describe any device that initiates or terminates a VoIP session.
ETSI	European Telecommunications Standards Institute
Firewall	A logical barrier designed to prevent unauthorised or unwanted communications between sections of a computer network
H248	H.248, also known as the "Megaco" protocol, is the international standard for media gateway control.
H323	H.323 is an international standard defined by the ITU for multimedia communication over packet-switched networks.
IETF	Internet Engineering Task Force: The standards body for Internet protocols.
IP	Internet Protocol: a data-oriented protocol used for communicating data across a packet-switched network.
IP Address	Internet Protocol Address: a unique address that devices use in order to identify and communicate with each other on a computer network utilising the Internet Protocol standard (IP).
IP Phone	A VoIP endpoint that looks and works like a conventional analogue telephone, but usually with additional capabilities like video display.
ITU	International Telecommunication Union
Jitter	In packet-based networks jitter is the measure of variation in delay experienced by consecutive packets as they travel from source to destination. VoIP devices include buffers to smooth out the effects of jitter, but ultimately call quality will suffer if jitter becomes too high.
LAN	Local Area Network

Latency	Latency, or delays in the traffic paths, can cause voice quality degradation if it is excessive. The goal commonly used in designing networks to support VoIP is the target specified by ITU standard G.114 which states that less than 150 ms of one-way, end-to-end (from mouth to ear) delay provides user satisfaction for telephony applications. Delay is typically experienced through various components that make up VoIP connections, including encoding/decoding, network transport and routing and encryption/decryption.
Layer 2	The Data Link Layer. Ethernet is the most common data link protocol.
Layer 3	The Network Layer. IP operates at the Network Layer of the OSI seven-layer protocol stack.
MAC Address	Media Access Control Address: A 48-bit address used to uniquely identify systems on an Ethernet.
Media Gateways	Media Gateways provide conversion between traditional telephone circuits and voice content carried on VoIP networks. Gateway control protocols such as MGCP and H.248 (Megaco) are used to control set up of calls on Media Gateways in response to call management requests received in signalling messages.
MGCP	Media Gateway Control Protocol: Defined by the IETF in standard RFC 3435, MGCP is used between call processing systems and Media Gateways that link VoIP to the PSTN.
NIDS:	Network Intrusion Detection System: a system that tries to detect malicious activity by monitoring network traffic.
Packet Loss	Packet loss causes voice clipping and dropouts in conversation. Many codecs incorporate packet loss concealment techniques to mask the effects of lost or discarded VoIP packets. The packetisation interval determines the size of samples contained within a single packet. For a 20ms packetisation interval, the loss of two or more consecutive packets results in a noticeable degradation of voice quality. VoIP networks should be designed for zero packet loss in normal operation.
Packet switched	A data communications system in which packets (units of information carriage) are routed between nodes over data links shared with other traffic.
Patch	An update to a piece of software that fixes a defect in a formal release. Most often used in reference to operating systems.
PBX	Private Branch eXchange
Peer to Peer	A peer-to-peer system is a distributed system whose component nodes participate in similar roles, and are therefore peers to each other. There is usually some form of structure placed on peer-to-peer networks to enable individual nodes to locate each other.
Proxy	A proxy is a server that acts as an intermediary between a workstation user or local service and the Internet or remote service, so that an enterprise can control and administer security and provide a caching service.
PSTN	Public Switched Telephone Network
QoS	Quality of Service

Router	A router is a communications device that forwards data packets across a network toward their destinations, through a process known as routing. Routing occurs at Layer 3 (the network layer i.e. Internet Protocol (IP)) of the OSI seven-layer protocol stack.
RTP	Real-time Transport Protocol: Defined by the IETF standard RFC 3550, RTP is a standardised packet format for delivering audio and video over internet networks.
Signalling	Signalling protocols are used to manage all aspects of call set-up, acceptance and termination, as well as in call operations such as handling DTMF signalling to remote call systems. The signalling protocols also provide a transport for text based instant messaging functionality.
SIP	Session Initiation Protocol: Defined by the IETF standard RFC 3261, SIP is an application-layer control protocol for creating, modifying, and terminating sessions with one or more participants. These sessions include VoIP telephone calls, multimedia distribution, and multimedia conferences.
Soft Phone	A piece of software for making VoIP calls using a general-purpose computer, rather than using dedicated hardware.
SPIT	Spam over Internet Telephony: A theoretical method of exploiting the SIP protocol to distribute unsolicited voice messages and calls to VoIP users.
SRTP	Secure Real-time Transport Protocol: Defined by the IETF standard RFC 3711, SRTP provides encryption, message authentication and integrity, and replay protection to the RTP data.
Stateful Inspection	A method for keeping track of the state of network connections (such as TCP streams) travelling through a routing TCP/IP device (usually a firewall). The system is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed to pass.
Switch	A network switch is a networking device that performs transparent bridging (connection of multiple network segments with forwarding based on MAC addresses) at full wire speed in hardware.
TDM	Time Division Multiplexing: A transmission technique whereby several low speed channels are multiplexed into a high speed channel for transmission. Each low speed channel is allocated a specific position based on time.
TFTP	Trivial File Transfer Protocol: Defined by the IETF standard RFC 1350, TFTP is a very simple file transfer protocol which is useful for providing image and configuration data to relatively low powered network devices.
Toll Fraud	Any technique that allows a third party to make fraudulent calls by exploiting configuration weaknesses in telephony systems.
TLS	Transport Layer Security: A cryptographic protocol that provides secure communications on the Internet for such things as web browsing, e-mail, VoIP, and other data transfers.
VLAN	Virtual LAN: A method of creating independent logical networks within a physical network.
VoIP	Voice over Internet Protocol

VPN	Virtual Private Network: A VPN is a private communications network often used within an organisation, or shared by several organisations, to communicate confidentially over a publicly accessible network.
Wi-Fi	A brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks based on the IEEE 802.11 specifications.
Wire Tapping	The monitoring of telephone conversations by a third party, often by covert means.