bsia
british security industry association

a user guide to the use of **internet protocol (IP)** in the security industry

June 2007

For other information please contact:

British Security Industry Association
t: 0845 389 3889
f: 0845 389 0761
e: info@bsia.co.uk
www.bsia.co.uk

Contents

1. Introduction

Security systems are changing at an ever-increasing pace and are making more use of standard Information Technology (IT) products running over a Local Area Network (LAN) or Wide Area Network (WAN) e.g. across the Internet, where they can be remotely monitored and controlled. As a result of using Internet Protocol (IP), the opportunity has arisen for manufacturers to develop new generations of equipment from control panels, cameras, and door controllers, to fully integrated systems combining fire, access control, CCTV, intruder and building control systems. These "integrated" systems are often called security management systems as they bring together the management of all aspects of an organisation's security.

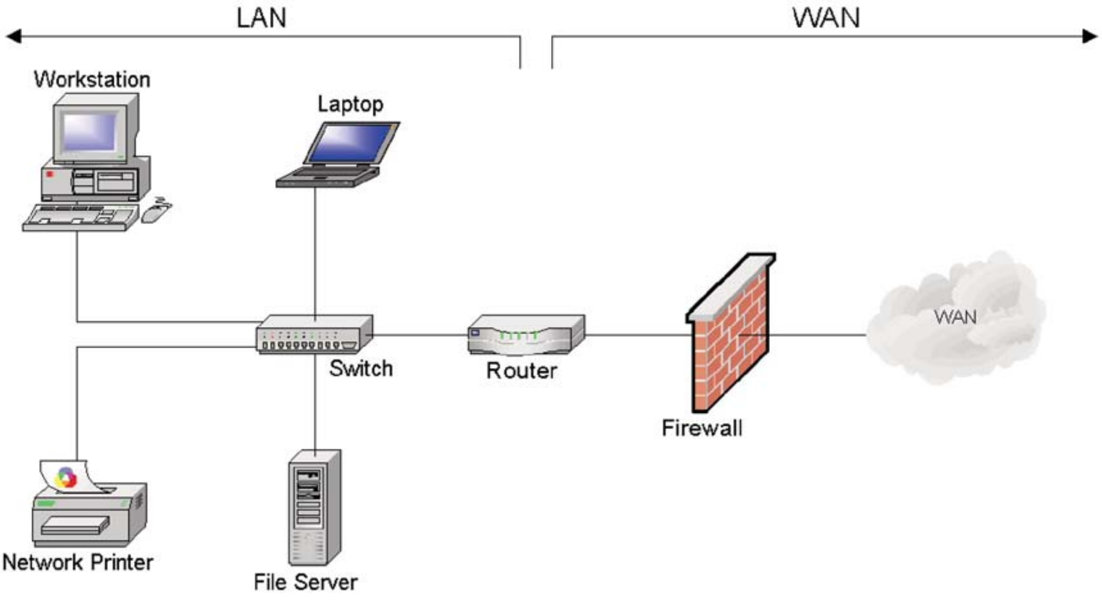
This brief document will explain most of the security opportunities for LAN / WAN use from a simple IP-based system, to an integrated solution incorporating multiple systems. It is directed towards an end user at an entry level to provide guidance on the use of IP technology in the Security Industry.

Note: There is a glossary of terms & definitions at the end of this document to assist in understanding the terminology associated with IT and IP working in the security Industry.

2. Using a network for security applications

a. What is a network?

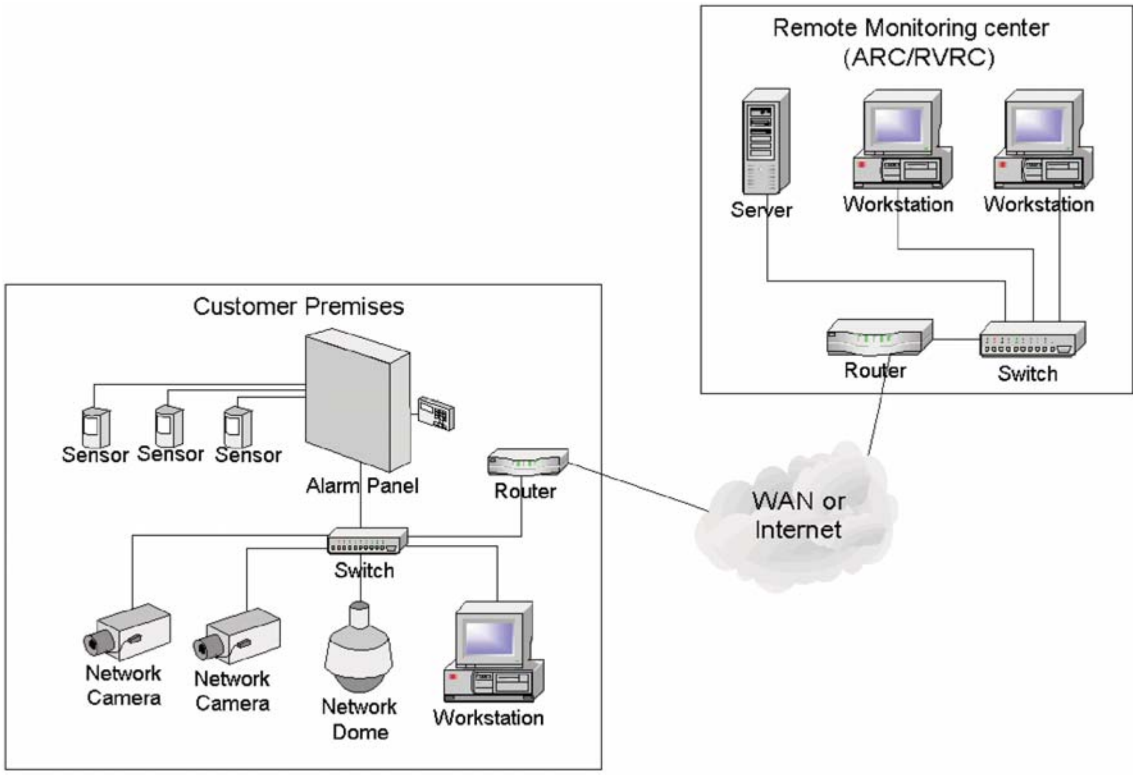
In simple terms, a network provides a means of communicating data between two or more computer-like devices. A network can be a LAN and can incorporate a Wireless element of networking (WLAN). Where the network has the need to communicate outside of a single LAN, a WAN is used. A WAN can connect LANs together to communicate with users and computers in other locations. The most well known example of a WAN is the Internet.



b. Why use an IP network?

Traditionally, many security systems have been linked to remote monitoring centres using modem type devices connected to a telephone line to exchange information. Using a network introduces many benefits, for example a substantial financial saving compared to dial up solutions. Additionally, the use of a network can improve quality of information and the time required to connect and exchange information.

Digital formats are being chosen by many industries such as music, telephone (voice over IP networks), TV, photography etc. With so many industries making use of IP technology, networks have become extremely robust. As a result, the use of a network can make the exchange of information between a security system and a remote monitoring centre more efficient.

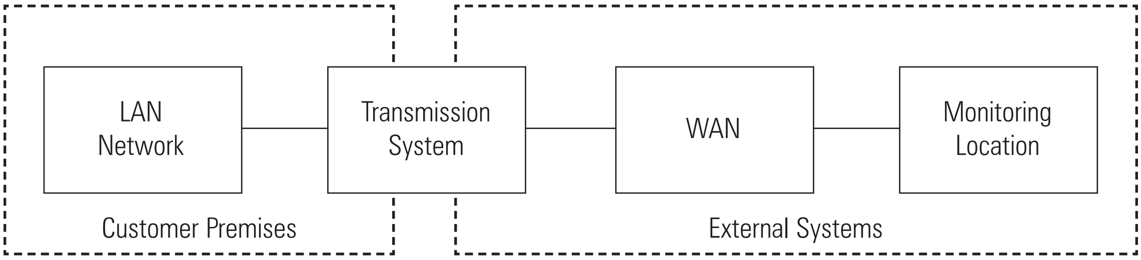


3. Considerations for IP systems

As with all technology, IP requires careful consideration. Good system design and communication between interested parties such as the installer, IT liaison, and the end user will pay dividends in the long term. However, it is worth outlining some key elements to consider as below:

a. Infrastructure

When considering IP as a means of security communication, there are two main areas of IP use. These are internal network communication and the external communication.



Communication within the customer's premises may use your existing IP network, a dedicated security system IP network, or be installed as a directly wired security system.

Communication over the external systems from the transmission equipment to a remote monitoring location may also use IP but this will be hired from other providers, such as an Internet Service Provider (ISP).

b. Internet Service Provider (ISP)

The connection between your premises and the monitoring location may use an ISP to provide the service. When choosing an ISP, you should endeavour to establish the level of service being offered. Additionally, it may be prudent to have a second ISP link. The connection between your premises and the ISP is perhaps the weaker link so if you do have concerns, you should investigate an alternate means of communication from your premises into the ISP, i.e. GPRS, GSM (mobile service providers).

c. Cabling

A decision has to be made to either use an existing network or to install an independent network for security use. Some buildings make use of structured cabling, which is used for various purposes including networks. CAT 5/6 UTP cable is commonly used for networking and it is very important to use the right CAT cable for optimum signalling performance on high-speed networks.

It is important to discuss the proposals with the company IT manager before commencing installation. If an exclusive network is installed, all hardware should be installed in accordance with the network hardware manufacturer's guidelines. Manufacturers usually offer training courses for network products. Alternatively employ an installation company which has this expertise to install the network infrastructure.

d. Bandwidth

Bandwidth requirements (space on your network to operate) should be discussed with your IT manager. The bandwidth required to operate a CCTV system may be considerable. Your security system provider will be able to advise you on the bandwidth requirements. As a general guide, CCTV systems require considerable bandwidth to send video images over a network whereas access control, intruder alarm systems and visitor management systems that only send small amounts of data, do not require much bandwidth.

e. Physical security

It is generally well understood that the equipment installed to provide security on your premises needs to be installed in a secure manner. However if your security system is to make use of your existing network, it is important to ensure that network components are also treated as security system components. This may mean ensuring these components are installed in protected areas and ensuring that network connectors are labelled as being security connections (against inadvertent disconnection etc). Another consideration is backup power supplies. If your security system must have backup power supplies, then this may mean that some network components may also have backup power supplies.

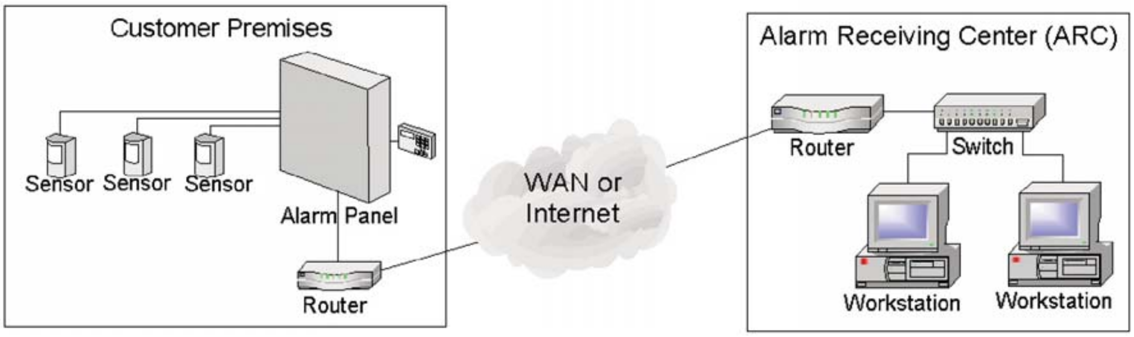
f. Company usage policies

You will also need to consider company policies relating to "what is allowed" to use an existing network. If the nature of your business dictates that the network shall only be used for specific applications, then this may immediately determine that a separate network must be installed for the security system.

4. Capabilities of IP in security applications

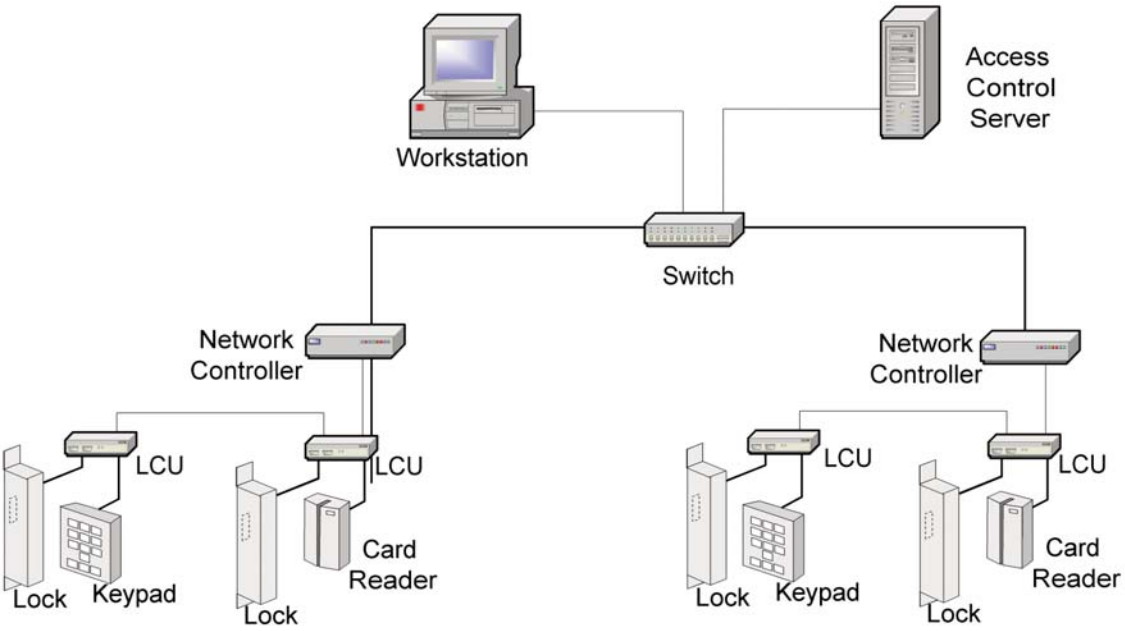
a. Alarm systems

IP has already been proven to be an effective communication method accepted in this field with capabilities at least equal to the best conventional solution on the market today. When linked to building management systems, the efficiency of a building can be monitored and adjusted such as heating, lighting, ventilation etc.



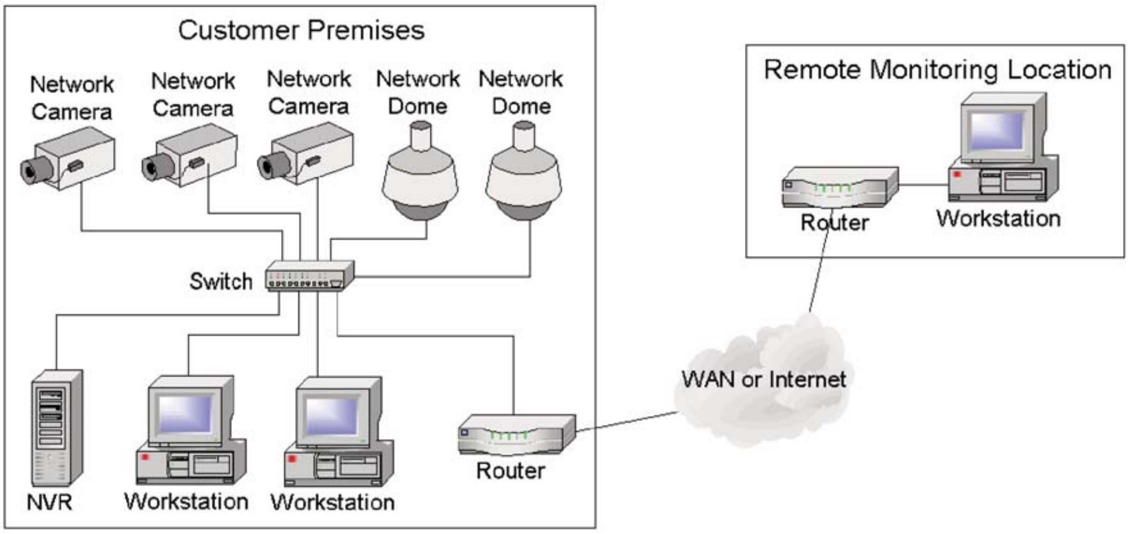
b. Access control systems

Using an IP network to link together other access control systems such as barrier control, time and attendance systems, lift & visitor management, payroll systems etc, can all benefit from a single IP network.



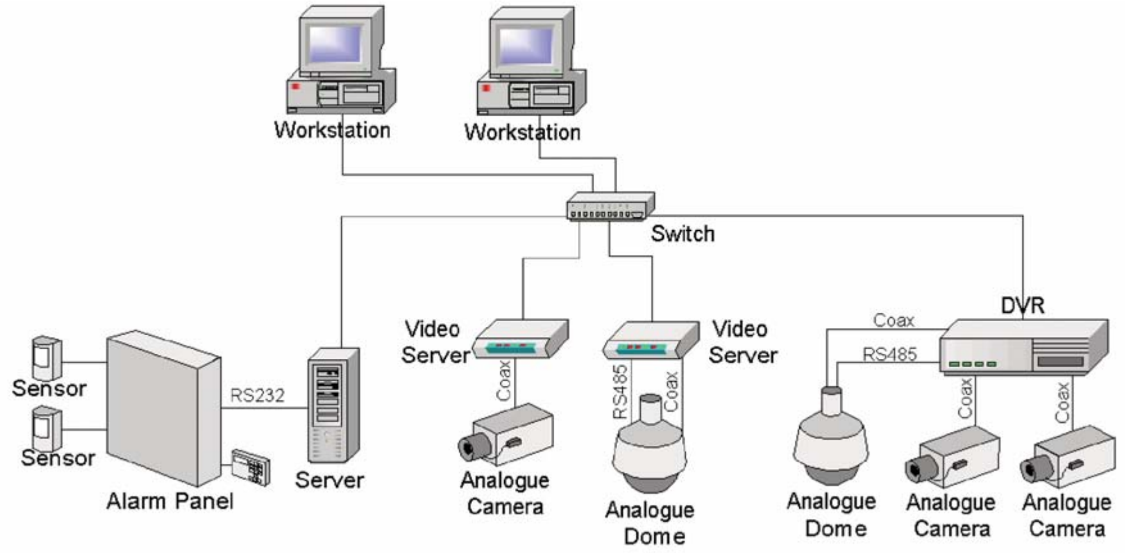
c. CCTV systems

Transmission of CCTV over an IP network both locally at the premises and remotely at another location is becoming increasingly commonplace with very high definition image recognition available. It is not possible to do this with analogue VCR's (video cassette recorders).



All the above share the same common benefit of reduced cost with excellent quality of product and results.

5. Integrating existing security with IP security solutions



Some products allow a mixture of analogue and digital security equipment to be combined, and this means that there is not always a need to move completely to an IP based system if an existing security system is in place. The 'hybrid' approach is more common where two or more security sub systems are combined to create an integrated solution.

The data in a hybrid system will usually come together at one or more PC's. Non-IP systems are often connected to a PC using a serial port, whereas IP systems will be connected over the network.

Some other benefits include:

- Intelligent management /maintenance-analysing system and alerts.
- Remote maintenance-improved user rights in management to configure and control.
- Scalability - to add additional equipment when ready to expand.
- Resilience in system - if one path is not available it will automatically take another path very quickly and easily.
- Preservation of previous capital investment.

6. Cost

System costs and potential savings will be dependent upon the intended use and scope of the system, and the degree of use of existing installed equipment and/or cabling.

a. WAN

WANs offer the most potential for security application cost savings and are often the catalyst for users and installers to change from PSTN and ISDN signalling solutions.

Users have often invested in IP systems to send emails and implement other business applications. The money has already been spent on a high-speed broadband connection, which can be used to replace most conventional connections.

Analogue lines cost around £160 per annum with a bandwidth of around 34Kbits per second and ISDN lines can cost twice that of analogue with a maximum bandwidth of 128Kbits per second. A Broadband circuit provides a bandwidth of up to 8Mbits per second downstream and up to 512K bits per second upstream, which is more than adequate to absorb these applications without affecting the business requirements of the system.

b. LAN

Many applications such as CCTV require large amounts of bandwidth and are well suited to operation over a LAN. Wide bandwidth requirements cause a dilemma for shared use with the business applications. However, a LAN solution within a building can be constructed to provide separate networks for business and security. Installation of IP CCTV cameras can often utilise existing wiring.

Different technologies can be brought together, such as access control, building management systems, CCTV and intruder systems, leading to an integrated solution. This can produce great savings at design stage or further down the line as new technology is introduced throughout the life of a building or application leading to more efficient maintenance and overall lower running costs.

In all cases it is important to look at the long-term cost of such a system, which is more flexible and where additions and/or alterations are often required.

c. WAN Radio (GPRS)

WAN radio offers a viable backup solution with GPRS and IP connectivity. Intruder alarm panels have for some time been operated over radio networks and with the advent of GPRS the solutions can be more cost effectively integrated. Cost effective GPRS SIM and airtime packages can be realised from around £25 per annum and are becoming more commonplace in other security applications.

7. Security considerations

System costs and potential savings will be dependent upon the intended use and scope of the system, and the degree of use of existing installed equipment and/or cabling.

a. Network security

Your IT manager may suggest using specific software security features such as fixed IP addressing, VPN segmentation etc. Consideration should be given to setting up user rights and creating a separate area on the network for different departments i.e. HR, finance, managers etc. Consideration also needs to be given to external security; this can be achieved by using a Virtual Private Network (VPN), which uses encryption. firewalls/routers/switches and other security mechanisms are used to ensure that only authorised users can access the network and that the data cannot be intercepted.

The way in which the security system manages data communication and storage may be a little different to the traditional IT data processes. For example:

- The event databases may be encrypted and secured with additional security access and password protection. This means that the company IT database manager may not have ready access to the security databases, as he would for other databases within the company system.
- The data being transferred across the network may be heavily encrypted.

The security computer server may require more stringent user access controls in place. The computer may be 'locked down' more than other computers on the network.

It is worth noting that some security systems will require a secondary signalling path to satisfy the needs of security and other key stakeholders such as insurers.

b. Physical Security

Physical access to the network components, e.g. unsecured workstations, power failures, tampering with components and interconnections will need to be considered.

Note: The network is only as secure as the weakest link. You must ensure all these issues are discussed between your IT manager and your security provider.

8. Summary

Finally, ensure that you understand the capabilities of your computer network and most importantly, make sure you (and/or your IT provider) understand the requirements of any security system that will be connected to it. Time spent sorting out these requirements at design stage will save potential issues later. Also make sure you ask for a demonstration to ensure your system output equals your input. Ideally what is required is a good quality system that is flexible, easily upgraded and offers reliability that is well supported.

9. Acknowledgements

The BSIA would like to thank the IP Working Group for its contribution in the production of this guide.

Annex A

Terms & Definitions

Broadband

In networking terms, Broadband refers to communication using wider frequencies to provide higher bandwidth connections for WAN links.

CAT 5/6

Category of UTP cabling recommended for use for Ethernet networks. CAT5 is for 100Mb transmission, CAT6 for 1Gb.

Firewall

Security device designed to block unauthorised communications. Blocking is based on a set of rules that are based around IP and port address details of incoming (and outgoing) communications but do not examine the contents. Firewall will therefore not necessarily stop attacks such as viruses, which are attached to legitimate communications.

Hybrid

The combination of two or more security applications of differing technologies that are integrated to form one operational system.

Internet

Global public network accessed through Internet Service Providers (ISPs) running on network infrastructure provided by many telecoms companies. Biggest known example of a WAN.

ISP – Internet Service Provider

A business or organization that provides to consumers access to the Internet and related services.

IP Address

An address format that hosts use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard.

IP – Internet protocol

A data-oriented protocol used for communicating data across a packet-switched network. IP operates over diverse networks.

IT – Information Technology

Broad term covering the various disciplines relating to communications and computer-based information systems.

LAN – Local Area Network

A data network over which hosts 'local' to each other can communicate with each other. Typically considered to be limited geographically to within a building or group of buildings. Ultimately a LAN can be considered to be constrained by its implementation, operation and management by a single organisation.

Network Camera / Dome

Analogue or digital video cameras, plus an embedded video server having an IP address, capable of streaming a video signal (and sometimes, even audio).

NVR – Network Video Recorder

A device that records video in a digital format to a disk drive or other medium that also includes an embedded video server having an IP address, capable of streaming a video signal

Router

Inter-networking device that forwards data based on IP addressing usually linking LAN networks together.

Storage

Media on which information is held, such as DVD, USB stick, HD etc.

Switch

Networking device that transparently connects hosts or devices to each other as a LAN

Transmission system

A system that transmits a signal from one place to another.

VPN – Virtual Private Network

A private communications network often used by companies or organisations, to communicate confidentially over a public network

VPN Segmentation

VPNs segment a customer's network from other customers on the same carrier network or from the public Internet, often accomplished through the use of Virtual Routers

WLAN – Wireless LAN

The implementation of LANs using wire free communication devices. The most common form is based on "Wi-Fi" as defined by the IEE802.11 standard.

WAN – Wide Area Network

A computer network that allows the connection of LANs and other networks to allow users and computers to communicate from one location to another.

Workstation

A location where a computer terminal can be accessed by a user.