Understanding the Basics

Networking

The Back Bone for Security Systems

The electronic security industry has moved into the IT space, with IP technologies growing in significance and application. Most CCTV, access control, intruder detection and intercom systems now offer IP network interfaces, allowing devices or control panels to communicate over an IP infrastructure.

This trend towards IP based security systems is firmly established. The trend is away from **analog-based video systems that run over coaxial-cabling systems and toward IP-based systems running over twisted-pair and/or fibre-optic cabling systems.** This transition from Analog to IP based security systems is also true for other end points like Sensors and Intelligent Building Management Systems.

By utilising an IP network, these technologies can work together using the same communications protocol and perform as a complete solution. This enables the security requirements of the network to be considered as a whole.

The massive amount of data that is collected, transformed, and delivered across the network requires a state-of-art network. Not only does the system need to support current data requirement, but it must also accommodate the future volumes of data as the organization grows.

The role of the network is very important, as it is critical to the performance of the overall Security System.

Basic Elements of the Network

Passive Components

- Wall outlets – to which the end points (cameras, readers etc) are connected
- Patch panels and Cabinets
- Horizontal: Cat 6 / 6a/ 7 UTP cable – medium between the end point and the main cross connect
- Vertical (backbone): Fibre optic cable; WiFi – not quite passive

Active Components

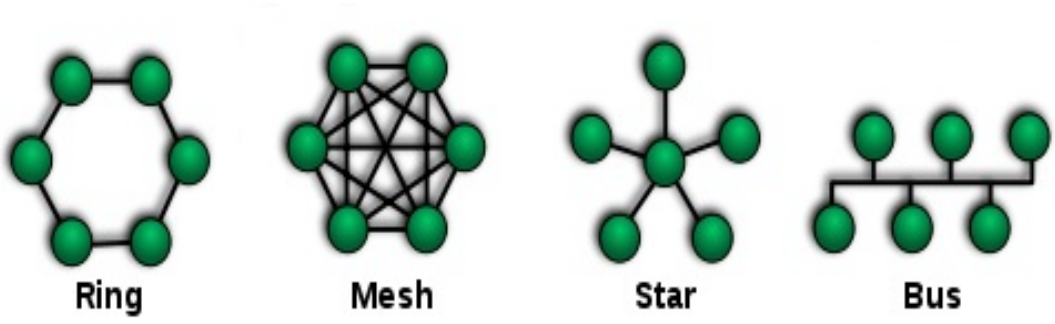
- **Hub aka repeater**: This broadcasts the same data to all its ports. Hubs do not manage any traffic coming through them; they only broadcast or repeat packets from an incoming port to all other ports.

- **Switch**: This is more sophisticated than a hub. It forwards data only to those devices that the data is intended for, as it uses MAC addresses to forward data to the correct destination. A switch is considered a Layer 2 device operating at the data link layer. Switches use packet switching to receive, process and forward data.

- **Router**: A router is a more sophisticated device than a switch. It connects computer networks, for example, connecting a campus network with the Internet. They connect LAN's with WAN's. Routers transfer packets of data between networks to establish and sustain communication between two nodes in an internetwork. Routers operate at Layer 3 (network layer) of the OSI model; a router uses the destination IP address in a data packet to determine where to forward the packet.
  In addition, routers often perform (a) network address translation (NAT), which allows all devices on a sub-network (e.g., all devices in a campus) to share the same public IP address and (b) sometimes include built-in firewalls to improve the network's security.

Although the two names are mistakenly interchanged**, switches and routers are not the same!**

Network Topologies



Bus Topology

This topology is typically deployed where a backbone of optical fiber cable runs around the perimeter of a premise so as to connect all the devices/cameras to the network. This is the simplest way to design the network of a Security System.

Ring Topology

This is an arrangement of cameras/ security devices in a ring - creating a closed logical loop in the network. Every device receives the signal first and then transmits it further to the other device.

Star Topology

This topology is generally used when the premise is small and all the security devices are networked to a central hub or a core switch. In this case network failure for one device does not affect the other devices.

Mesh Topology

Mesh Topology is generally used in 'wireless city surveillance applications'. In this topology, all the security devices are connected to each other, **giving a lot of redundancy to the network.**

TCP/IP & Ethernet

TCP/IP stands for **Transmission Control Protocol**/Internet Protocol, which is a set of networking protocols that allows two or more computers to communicate. The Defence Data Network, part of the Department of Defence, developed TCP/IP, and **it has been widely adopted as a networking standard.**
TCP is responsible for the data delivery of a packet. **IP** is responsible for the logical addressing.
IP obtains the address and **TCP** guarantees delivery of data to that address.

Ethernet is a local area technology, a protocol for the Network Layer within the TCP/IP stack.

Power over Ethernet (PoE)

Cameras need power. Power over the network cable eliminates the need for additional power cabling for the cameras.

Power over Ethernet (PoE) is a technology for wired Ethernet LANs (local area networks) that enable the electrical current, required for the operation of 'IP end points', to be carried by the data cables rather than by a separate power cable.
This reduces the number of wires that must be installed. The result is lower cost, less downtime, easier maintenance, and greater installation flexibility than with traditional wiring.
The electrical current is fed to the data cable at the power-supply end and comes out at the device end (the IP end point - camera), in such a way that the current is kept separate from the data signal so that neither interferes with the other. The current enters the cable by means of a component called an injector. This uses two twisted pairs in a standard TIA-568B CAT5/6 RJ-45 Ethernet cable connection to carry DC power to a PoE-enabled device.
PoE is a safe and reliable way to transmit power to the IP end points such as phones, cameras, monitors, access points, readers and other IP devices.

Switch types

As explained earlier a switch is more sophisticated than a hub as it forwards data only to those devices that the data is intended for. It uses MAC addresses to forward data to the correct

destination. A switch is considered a Layer 2 device operating at the data link layer. Switches use packet switching to receive, process and forward data.

Fixed Configuration Switches
These switches have a fixed in their configuration. It is not possible to add features or options to the switch. It will not be possible to add additional ports when required.

Modular Switches
Modular switches offer more flexibility in their configuration. They typically come with different sized chassis that allow for the installation of different numbers of modular line cards which contain the ports. The larger the chassis, the more modules it can support.

Unmanaged Switch
Unmanaged network switches are often deployed in home networks, small companies and businesses.

Managed Switch
These switches can be customized to enhance the functionality of a certain network. They offer some features like QoS (Quality of Service), Simple Network Management Protocol (SNMP) and so on. These types of switches can support a range of advanced features designed to be controlled by a professional administrator.

PoE Switch

PoE Gigabit Ethernet switch is a network switch that utilizes Power over Ethernet technology. When connected with multiple other network devices, PoE switches can support power and data transmission over one network cable.

Industrial Switches
These are similar in function to the switches described above except that **they are specifically designed to stand up to extreme temperature, vibration and shock.**

OSI model

OSI stands for Open Systems Interconnection. It has been developed by ISO – 'International Organization of Standardization'.

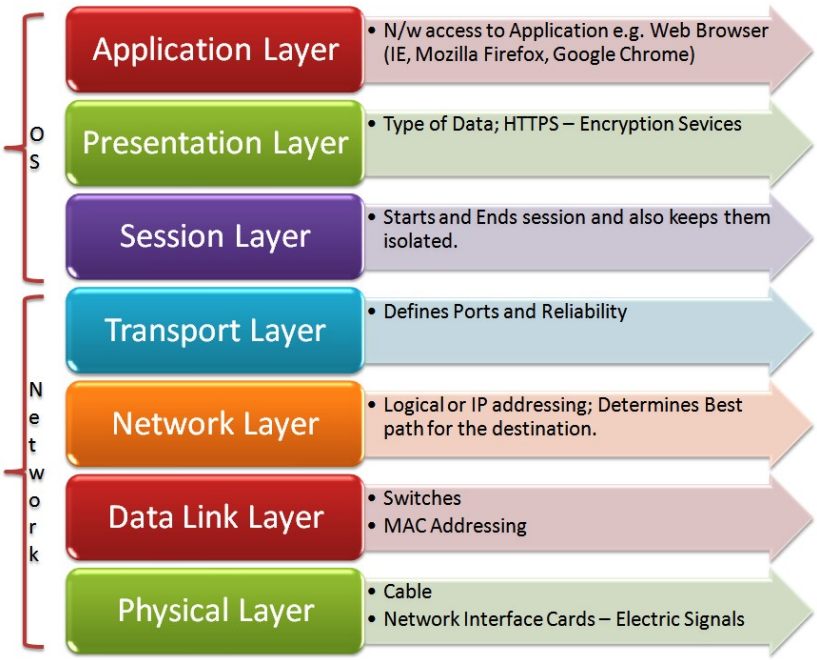
This has 7 layers with each layer having specific functionality. All these 7 layers work collaboratively to transmit the data from one person to another.

Layer 1 - Physical Layer
The lowest layer of the OSI reference model is the physical layer. **It is responsible for the actual physical connection between the devices.** The physical layer contains information in the form of bits.

Layer 2 - Data Link Layer (DLL)
The data link layer **is responsible for node to node delivery of the message**. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Layer 3 - Network Layer Network layer **works for the transmission of data from one host to the other host located in different networks**. The sender & receiver's IP address are placed in the header by network layer.

It also selects the optimum route, the shortest path to transmit the packet, from the number of routes available.



OSI model

Layer 4 - Transport Layer

Transport layer **provides services to application layer and takes services from network layer**. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End delivery of the complete message. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

Layer 5 - Session Layer

This layer **is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.**

Layer 6 - Presentation Layer also called the **Translation layer**

The **data from the application layer is extracted here and manipulated as per the required format** to transmit over the network.

Layer 7 - Application Layer

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also **serves as a window for the application services to access the network and for displaying the received information to the user.**
