



IP Networking for Video Surveillance



Version 4.3, June 1, 2018



Table of Contents

Class 1 – Bandwidth	3
Class 2 - Network Addressing	6
Class 3 - Network Hardware	12
Class 4 - PoE, VLANs and QoS	17
Class 5 - Network Cabling	23
Class 6 – Protocols	27
Class 7 – Installation	31
Class 8 - Remote Network Access	33
Class 9 - Network Security	36
Class 10 - Hacking	39
Class 11 – Wireless.....	40



Class 1 – Bandwidth

Data, in its rawest form, is comprised of 1's and 0's.

A 'bit' is the most fundamental unit of bandwidth and storage on an IP surveillance network.

Bandwidth and network speeds are commonly measured in bits per second (bps or b/s). Bits are represented with a small 'b'.

8 bits is equal to 1 Byte. Bytes are represented with a capital 'B'.

10 Bytes equals 80 bits (10 Bytes * 8 = 80 bits). 800 bits equals 100 Bytes (800 bits / 8 = 100 Bytes).

IP video requires LOTS of bits. Thousands, millions, even billions of bits could be needed.

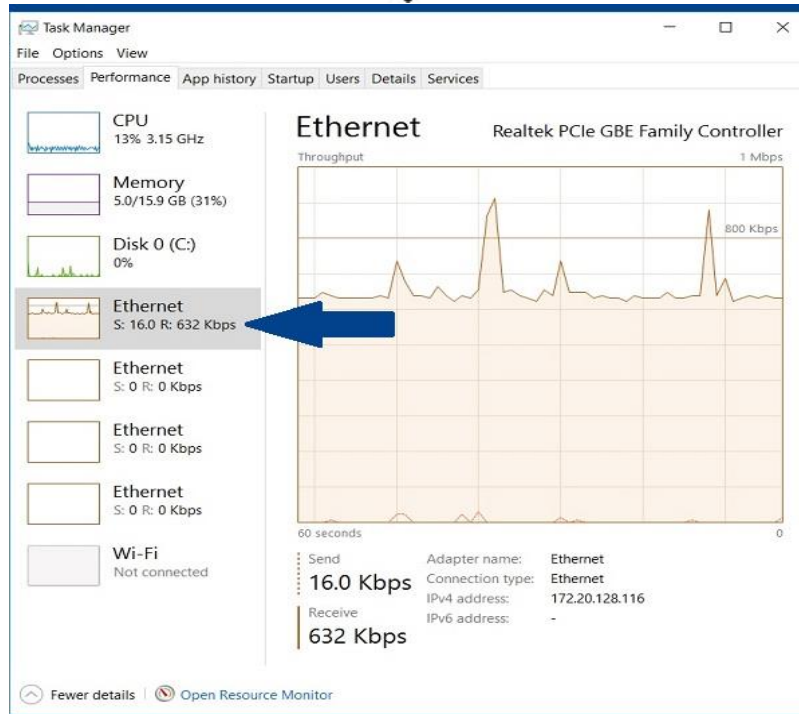
1,000 bits equals 1 Kilobit (also referred to as 1Kb). Not common with today's IP HD megapixel cameras as they typically require at least 1 Megabit or higher.

1,000,000 bits equals 1 Megabit (also referred to as 1Mb). 1,000 Kilobits also equals 1 Megabit. This is the most common measurement for today's IP HD megapixel cameras. An individual HD / MP video stream tends to be in the single digit megabits (e.g., 2Mb/s or 4Mb/s or 8Mb/s are common ranges).

1,000,000,000 bits equals 1 Gigabit (also referred to as 1Gb). 1,000 Megabits also equals 1 Gigabit. One rarely needs more than a gigabit of bandwidth for video surveillance unless one has a very large-scale surveillance system backhauling all video to a central site.

Bandwidth is measured in bits per time (i.e. bits per second or bps)

Knowing how to measure bandwidth is a key component to understanding overall system architecture and requirements. In Windows 8 (for example) the ability exists to measure bandwidth on the NIC using Task Manager, more specifically, the Performance tab in Task Manager. The following image illustrates this tool



All video data from an IP surveillance camera is compressed. It is not feasible to transmit RAW (uncompressed) data across traditional cable mediums.

Total bandwidth consumption is determined by adding up the bandwidth required per camera. For example, if you have a total of 4 cameras, with Camera 1 requiring 2 Mb/s, Camera 2 requiring 3Mb/s and cameras 3 and 4 requiring 7 Mb/s, you need to add these values together ($2 + 3 + 7 + 7 = 19$). This means that these 4 cameras will require 19 Mb/s total.

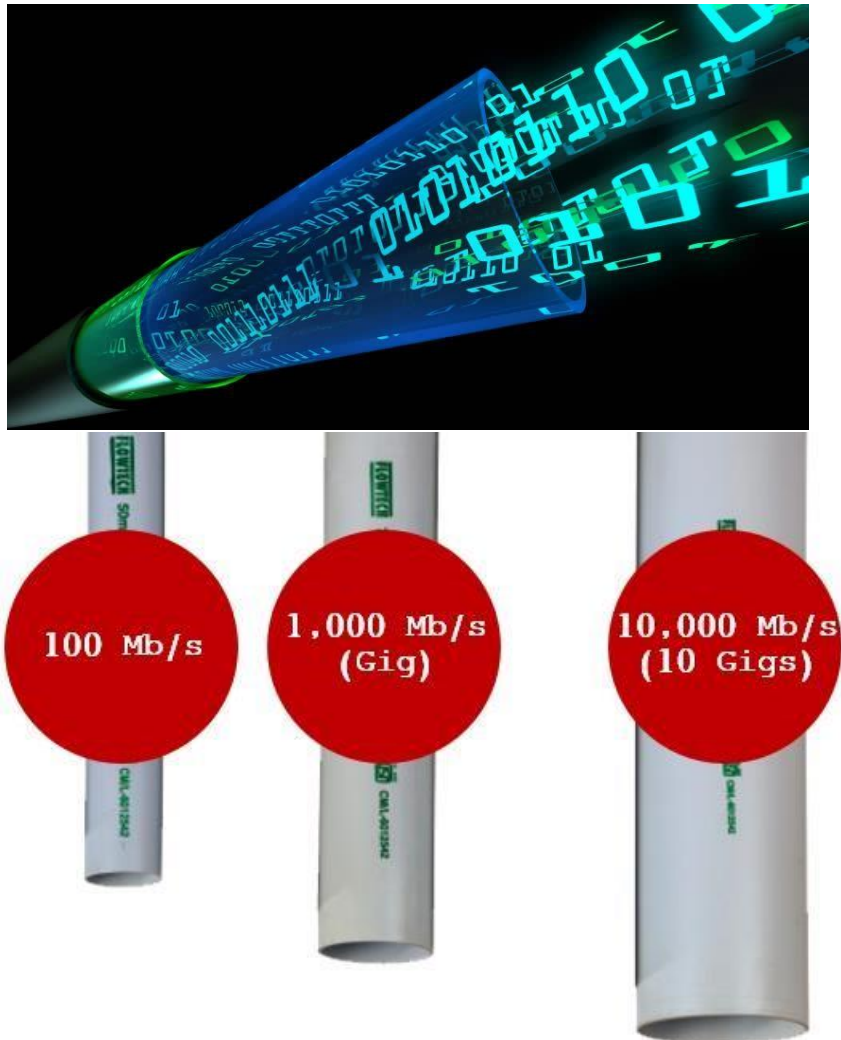
In traditional analog systems no bandwidth is required to transmit video as electrical signals are passing on a coax cable directly into the DVR (Digital Video Recorder), with bandwidth only required when remotely managing the DVR.

All IP networks require bandwidth. Most commonly in IP surveillance, bandwidth is used when transmitting data from a camera to a recorder (i.e. Video Management Server). Anytime data is traveling a network (like camera to VMS or VMS to Client software) bandwidth is used.

To break this down a bit further, bandwidth will be used when a VMS is recording data from a camera. In this case data is being sent over the network from a camera to the recorder, which will store it for retrieval later (if needed). Bandwidth will also be used when a viewing client is watching video live, or playing back video. In this case, the data is being sent over the network from the VMS to the client machine. If a camera is not sending data to the recorder (i.e. the VMS is recording on motion only, and there is no motion in the scene) or the server is not

sending data to a viewing client (i.e. No live or playback viewing is being done) then very little (if any) bandwidth will be used.

Bandwidth availability, or total 'speed' capabilities is sometimes referred to as a 'Pipe'. The 'larger' the pipe is, the more can be passed through it.



Higher speed capacities do not necessarily mean a physically bigger cable or medium. For example, Cat5e can handle up to 1 Gb/s. Cat6 can handle up to 10 Gb/s. Single mode fiber can handle up to 40 Gb/s, therefore is the biggest 'pipe' while being physically the smallest of the three examples.



Class 2 - Network Addressing

All managed IP network devices on a local network have an IP (Internet Protocol) address. These devices include cameras, managed switches, servers and many other types.

IP addresses should be unique for each device and are used to identify where the device is in order to send and receive data with it.

Duplicate IP addresses (such as two cameras having 192.168.1.20) can cause communication issues or complete connectivity loss.



There are two types of IP address formats in today's networks. IPv4 and IPv6. Though they are both used to provide a network address to a device, they are different in how they appear in style and length.

IPv4 (the most common IP address format used today) consists of 4 groups (called octets), each with a numeric value between 0 and 255. An example of an IPv4 address format is **192.168.1.17**.



IPv4 will yield over 4.2 Billion unique addresses in theory, though there are blocks of IPv4 addresses that are reserved for special purposes and are unavailable to the public.

IPv6 is 8 groups of Hexadecimal characters (A-F, 0-9). It is much longer and more complex than IPv4, but yields many more total unique IP addresses than IPv4 (340 undecillion).

An example of an IPv6 address format is **FA80:4322:0012:0000:341A:B3EF:FE1E:F97A**. It is possible that some vertical markets may require IPv6 addresses (such as government), otherwise common use of IPv6 is not likely.

An IP address has two components, the network address and the host address.

Subnet masks are used to determine what part of the IP address is the network and which is the host.

They are formatted in the same way as an IPv4 address, with 4 octets consisting of numbers ranging between 0 and 255.

In simple networks, each octet is typically either a 0 (all bits off) or 255 (all bits on). An example of a subnet mask is 255.255.255.0. Using the IP address example of 192.168.1.17 and a subnet mask of 255.255.255.0, would mean the first three octets of the IP are the 'network' side and must match in order to communicate over the network (i.e. 192.168.1.x). The last octet is the host side and can range anywhere from 0 to 255. If you wanted to set an IP address that can talk to the 192.168.1.17 address, yours must start with 192.168.1.x.

The host side (x) can be anything from 0 to 255 and still communicate.

There are three common types of network classes:

- **Class A** addresses range from 0.0.0.0 to 127.255.255.255 and have a default subnet mask of 255.0.0.0. Class A addresses allow 16 million IP's per network and 128 different subnets.
- **Class B** addresses range from 128.0.0.0 to 191.255.255.255 and have a default subnet mask of 255.255.0.0. Class B addresses allow 65,000+ IP's per network and 16,000+ different subnets.
- **Class C** addresses range from 192.0.0.0 to 223.255.255.255 and have a default subnet mask of 255.255.255.0. Class C addresses allow 256 IP's per network and almost 3 million different subnets.



Class A	Network	Host	Host	Host
Subnet Mask	255	0	0	0

Class B	Network	Network	Host	Host
Subnet Mask	255	255	0	0

Class C	Network	Network	Network	Host
Subnet Mask	255	255	255	0

A MAC (Media Access Control) address is a permanent and unique 12 (hexadecimal) character ID given to a network device (i.e. an IP camera).

It is possible that an IP camera (for example) has more than one MAC address, if a camera has two Network Interface Cards (NICs) like an Ethernet port and wireless. Each NIC will have its own MAC address.

An example of a MAC address is 01:A3:FD:00:7B:52.

The first 6 digits of a MAC address is known as an Organizationally Unique Identifier (OUI).

An OUI is unique to a specific manufacturer, however, manufacturers can have more than one OUI. OUI lookup engines can determine the device origin. [Click here](#) for an example of an OUI lookup tool.

Here are some OUI examples and their respective manufacturers:

00:40:8C	=	
00:18:85	=	
4C:11:BF	=	

Dynamic IP addresses are IP addresses that can (and likely will) change over time.



These addresses are most commonly given out by a Dynamic Host Configuration Protocol (DHCP) server.

Many network devices default to DHCP addressing. A DHCP server has a 'pool' of addresses that it is able to hand out to IP devices on the network that request it.

For example, an IP camera that is configured for DHCP is plugged into a network switch will 'ask' the DHCP server for a valid IP address. The DHCP server will provide an available address from the 'pool' and give it to the camera. However, if the camera reboots or its lease time has expired, the IP address it is given will likely change.

Because of the ever-changing nature of dynamic IP addresses, it can cause issues with connectivity to the device.

Static addresses are the opposite of dynamic, meaning that a static address will not change unless done so intentionally.

This provides much more reliable connectivity to IP devices, as they always remain at the same IP address. Static addresses are assigned manually to a device.

Zero-Configuration Networking (also known as ZeroConf) is a set of technologies that enables devices to communicate over IP in the absence of configuration and administration.

ZeroConf IP addresses are Class B addresses beginning with 169.254.x.x.

An IP device (that supports ZeroConfig) that is configured for DHCP addressing, which is plugged into a network without a DHCP server, will default to a ZeroConf address as a temporary means for IP communication.

ZeroConf addresses should be used on a temporary basis only and should be changed to a valid internal IP address that matches the network it is connected to.

Public IP addresses are provided to a home or business from an ISP (Internet Service Provider), such as Comcast, Verizon FioS, Century Link, etc. and are generally reserved for modems. The Internet is an example of a huge network of devices with public IP addresses.

Public IP addresses are reserved for devices that reside outside of the internal (private) network.

Private IP addresses are given to devices that reside within a private network (such as your home or office LAN).



Most commonly in surveillance this includes cameras, servers, switches, etc. that are not directly connected to the Internet.

Though these devices may have connectivity to the Internet (to send email alerts, for example), they are commonly protected internally by a firewall and have no direct public facing IP address.

There are 'portions' of IP addresses that are reserved for private networks, such as:

- 192.168.0.0 - 192.168.255.255 (65,536 IP addresses)
- 172.16.0.0 - 172.31.255.255 (1,048,576 IP addresses)
- 10.0.0.0 - 10.255.255.255 (16,777,216 IP addresses)

A converged network is where all devices are connected and share the same network and bandwidth resources.

The advantage of using an existing network for IP video surveillance is the reduced cost of implementation. On a converged network there is no need to buy additional equipment. You simply plug in your surveillance devices to the existing equipment and they will be part of the overall network.

The disadvantage of using a converged network is that all traffic (surveillance, email, web surfing, file sharing, etc.) are all fighting for finite bandwidth resources. IP video (especially HD video) is bandwidth intensive and can chew up much of the available bandwidth that is shared with everyone, thus causing issues for the entire network.

A dedicated network is where each system (i.e. surveillance, email, file sharing, etc.) has its own physical network with its own dedicated bandwidth resources available.

The advantages of a dedicated network include bandwidth usage not impacting other systems or networks. It also reduces finger pointing and scapegoating when issues arise on other networks/systems.

The cons of dedicated networks include the higher cost associated with purchasing dedicated physical equipment (i.e. switches) and the additional management required for each individual network.

So how do you know which type of network is most appropriate for your IP video surveillance system? It comes down to evaluating a few key points.

These points include:



- Available bandwidth:
 - Does the existing network have enough bandwidth available to handle the additional load of the surveillance system?
- The relationship between IT and security administrators:
 - Whose budget will the additional cost of dedicated hardware come from? ○ Who will control the network?
 - Will a dedicated network help avoid blame if something goes wrong?
- Ongoing maintenance costs:
 - Who will be maintaining the network?
- Security concerns:
 - Does using an existing network increase the risk of unauthorized access to the entire network?



Class 3 - Network Hardware

There are many types of network cabling available. The most common types used for IP video surveillance are Cat5e and Cat6.

These cables feature 4 pairs of copper wires that are twisted together inside of the jacket. For each of these cable types there are different levels of shielding available.

The most common rating used in IP surveillance is Unshielded Twisted Pair (UTP). UTP cable has no shielding around the wire pairs or pair bundle.

Shielded Twisted Pair (STP) commonly uses a foil wrap to help reduce Electro Magnetic Interference (EMI).

Network equipment (such as switches for example) are rated to handle certain speeds. Most surveillance network gear today is rated at 100 Mb/s (Fast Ethernet) or 1000 Mb/s (GbE). These speed ratings describe how much data each port can handle (this is also called 'throughput').

Fast Ethernet (100 Mb/s) is commonly used for connection to field devices (such as cameras, encoders, I/O modules, etc.). Even with multi-megapixel and 4K resolutions, cameras rarely use more than 15 Mb/s and do not warrant the use of GbE for the bulk of the network.

Gigabit Ethernet (GbE) devices can handle 10X more data per second than Fast Ethernet. GbE is typically used for backbone switch interconnections as these connections can require data rates well over what Fast Ethernet can handle.

10 Gigabit Ethernet (10 GbE), though uncommon in surveillance, is generally used in data center applications where large quantities of switches and servers (each capable of delivering GbE) are connected together.

Total throughput capacity is typically 70%-80% of the total rated speed. Meaning a GbE switch (rated for 1000 Mb/s) will provide actual throughput speed of 700-800 Mb/s.

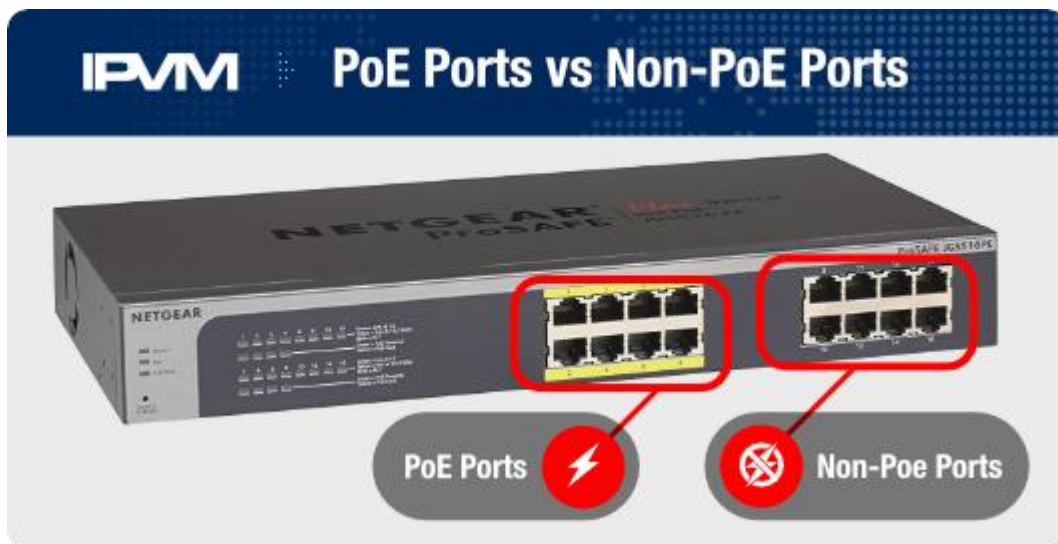
In IP surveillance networks an Ethernet switch is a central connection device. Switches distribute data within a network, and in the case of IP surveillance this commonly includes connecting cameras to recorders and recorders to viewing clients.

Ethernet switches can come in many sizes ranging from 4 ports, up to 96 ports or more in a single unit. In enterprise applications, multiple switches can be connected together.



Fast Ethernet switches can have 2 or 4 GbE ports, which are useful for switch interconnections. Some may come with SFP/+ ports for use with fiber optic or other high bandwidth cabling formats.

Ethernet switches can also be Power over Ethernet (PoE) capable. PoE capable switches will run power along with data down a single cable, thus powering the cameras connected to it.



These switches can have all or only some ports PoE capable (with the others being data only ports).

A key consideration with PoE switches is their total power budget vs. how many PoE ports are available.

Switches can also be managed or unmanaged.





Managed switches allow for users to connect and change settings in them. Unmanaged switches are simply plug and play and have not configuration capabilities.

Unmanaged switches are typically a lower cost option than managed switches and are found in systems where advanced configurations are not required.

Managed switches have different levels of management, such as 'smart switches' or 'fully managed' switches.

The actual feature sets available on these switches vary by manufacturer.

Some of these features may include the ability to remotely reboot a connected device by cycling PoE power, set up network monitoring via. SNMP, segment traffic into VLANs, or configure multicast. None of these functions are found on an unmanaged switch.

Hubs are not common into today's surveillance system, for good reason. Hubs will broadcast traffic to all ports simultaneously. Switches, by contrast, transmit traffic only to the port(s) for which the traffic is intended. Hubs can quickly flood the network with unnecessary traffic due to its broadcast method.

Routers are used to connect multiple networks together. Traffic is inspected by the router and if it is destined for a location outside of the local network it sends it to the modem and out into the Internet.



A router commonly includes a firewall feature, which helps protect the network against unwanted outside intrusion. In surveillance, routers are often used to connect the surveillance network to another network, while protecting the surveillance network with a firewall.



A router is also sometimes called a 'default gateway'.

A default gateway is an IP address (most often the private IP address of the router) that tells a device (such as a camera or recorder) where to go to send data destined for a network outside of its private network.

Remote connectivity to a surveillance network is typically not possible without a default gateway set on the network devices. As an example, if your computer doesn't have a valid default gateway configured, it will not be able to reach the Internet.

Some routers have switch ports built into them. This allows a single device to act as a switch and a router, eliminating the need for multiple devices in a small network. These converged routers are common in the consumer market.

The switch ports on these routers typically do not have PoE capabilities and the router itself may not support important switch functions such as VLANs.

Media converters help overcome the 100m distance limitation of Ethernet cables by adapting to fiber optic or coax cabling mediums.

Fiber optic converters support higher bandwidth, longer distances, and are immune to common interference that can affect Ethernet cables.

Coax converters will allow the use of existing coax cable to connect IP cameras (for example).

The maximum distance of most Ethernet cabling (Cat5e/Cat6) cannot exceed 100m (330'). Distances over this can create video quality issues and communication issues between devices.

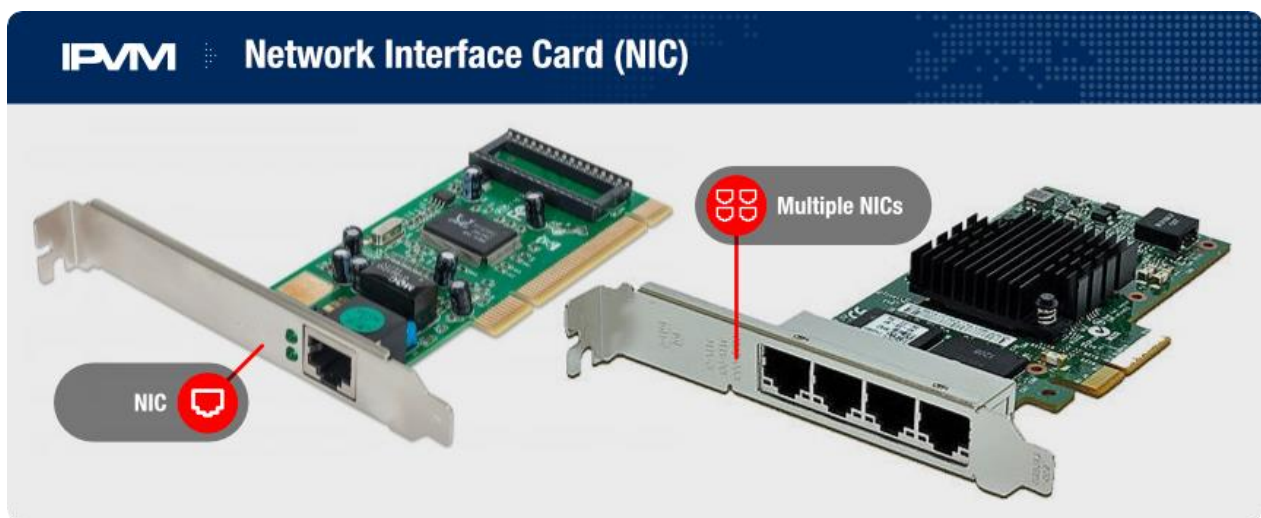
With Ethernet extenders it is possible to exceed the 100m limitation of Ethernet cabling. Powered UTP extenders are connected to both ends of a long run and can greatly increase the maximum distance by 8 or 9 times.



A Network Interface Card (NIC) is what allows a device to connect to a network. A NIC could be embedded in a device (such as an IP camera) or connected as a dedicated device (such as high end servers).

IP Cameras typically only have one NIC, but a server may have two or more NIC's, each connected to their own physical network.

For example, in the case of a video server, one NIC may be connected to the camera network, while the second NIC is connected to client viewing workstations on a different network.



This image shows what a multi-NIC dedicated card looks like. It is possible for a computer to have multiple NIC's in a mixed wired and wireless network, where the wired port is one NIC and the wireless function is separate NIC.

Customer Premise Equipment (CPE) is existing equipment that typically connects a home/office/building to a telecommunications network. Most commonly today an example of CPE is a modem.



Class 4 - PoE, VLANs and QoS

Power over Ethernet (PoE) uses a single cable to transmit data and power. With PoE capable devices, there is no need to run a dedicated power cable.

PoE is supported by almost all professional IP cameras today.

PoE is defined by IEEE standards, which include:

- **802.3af**: This is 'standard' PoE and supports up to 15.4W. It is used by 90%+ of all IP cameras.
- **802.3at**: This is known as 'high' PoE or PoE+. It provides up to 30W of power and is commonly used with PTZ cameras or outdoor units with heaters/blowers.
- **802.3bt**: This is currently in draft stages only, but is stated to have the potential for up to 100W. This is beyond the need for almost all IP cameras.

PoE classes more precisely segment how much power a device requires. The chart below breaks down these classes.

802.3af/at PoE Classes		
PoE Type/Class	Max Watts at Source (PSE)	Max Watts at Camera (PD) @100m
802.3af (Class 0)	15.4 W	0.44 - 12.95 W
802.3af (Class 1)	4.0 W	0.44 - 3.84 W
802.3af (Class 2)	7.0 W	3.84 - 6.49 W
802.3af (Class 3)	15.4 W	6.49 - 12.95 W
802.3at (Class 4)	30 W	12.95 - 25.5 W

PoE devices (such as cameras), when connected to a PoE switch, will negotiate which class it belongs to therefore determining how much PoE power it requires for operation.

For example, if a camera negotiates as a Class 2 device, the switch knows it will not require above 6.49W of power at the device.

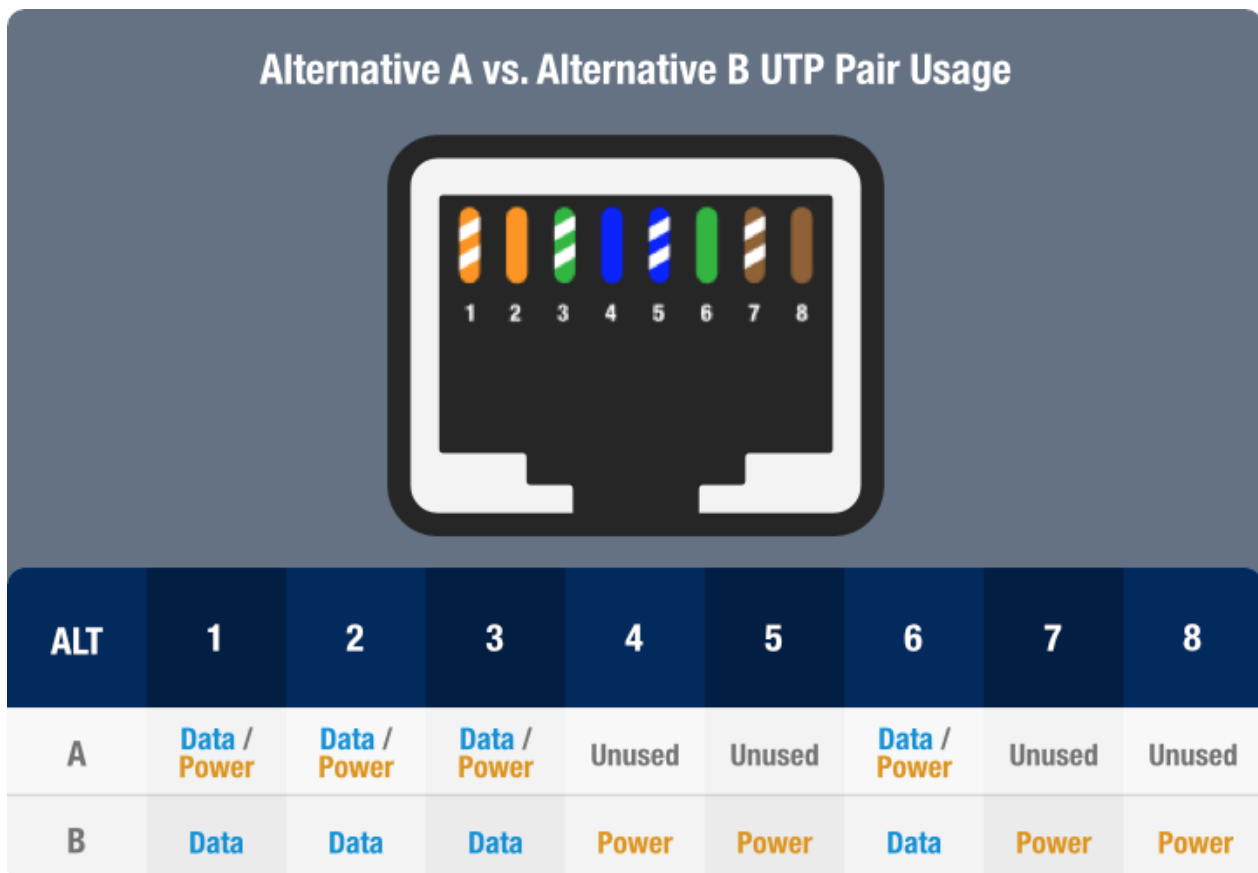


A PoE device that does not negotiate a specific PoE class will default to Class 0, allowing the full range of 802.3af power (0.44—12.95W) to the device. Most PoE devices negotiate as class 0 devices.

Most PoE capable devices in surveillance adhere to the 802.3af/at standard. However there are some non-standard PoE implementations. For example, some Ubiquiti products use a 24VDC base for PoE instead of the standards compliant 48VDC base. While power is still sent along with the data on a single cable, this is a non-standard implementation.

If you want to use standardized PoE, make sure the device states IEEE 802.3af/at compliance.

There are two common ways that PoE is sent down a Category cable. Alternate 'A' injects power down the SAME pairs as data. This means that two of the four available pairs are unused. Alternate 'B' injects powers down the unused pairs. All 4 pairs are used, either for data or power.



Most surveillance devices today will auto sense which pairs are used for data and power, meaning that most devices are Alternate A or B agnostic.



The actual order of pins may vary according to EIA/TIA 568A or B standards. This only affects the data pairs and not the power pairs. Regardless of which wiring standard is used, if the device is 802.3af/at compliant, power is applied to the device in the same way.

PoE is limited to the same maximum distance as the cabling, most commonly 100 meters for Ethernet cable. Data being carried over this distance can experience degraded video or total drop outs before the power drops below what the standard guarantees.

PoE extenders are available to push power and data past the 100m distance limitation. These extenders can provide 300m or even 600m total distance.

When calculating total PoE power budget of a switch it is important to know the maximum power draw of the cameras that are connected to it.

The power specification of the camera is typically higher than what the actual consumption will be.

This example shows 7 total cameras across 3 different models:

Quantity	Camera Model	PoE Power Spec	Total Power Needed
2	Axis Q1604	7.0 W	2 * 7 W = 14 W
2	Bosch Starlight 7000 HD PTZ	24.0 W	2 * 24 W = 48 W
3	Dahua HF3101N	6.0 W	3 * 6 W = 18 W
Total Wattage Needed: 80 Watts, 802.3at rated			

The total wattage needed is 80 W but they are not all the same PoE type. The Axis and Dahua cameras use less than what is available by 802.3af (up to 15.4 W). The Bosch PTZ's, however, require 24 W each. This means the Bosch cameras require 802.3at (PoE+), so it is important to verify the switch has a total power budget of 80 W and at least two PoE+ capable ports.

Commonly a PoE switch provides power to a camera. However, there are some cases where PoE capable Midspan injectors are put in series with the cable run to provide PoE power while connected to a non-PoE capable switch. It is possible for an NVR to have embedded PoE switch ports.

Many PoE switches will provide less total power than what is required for full 802.3af support on all ports.

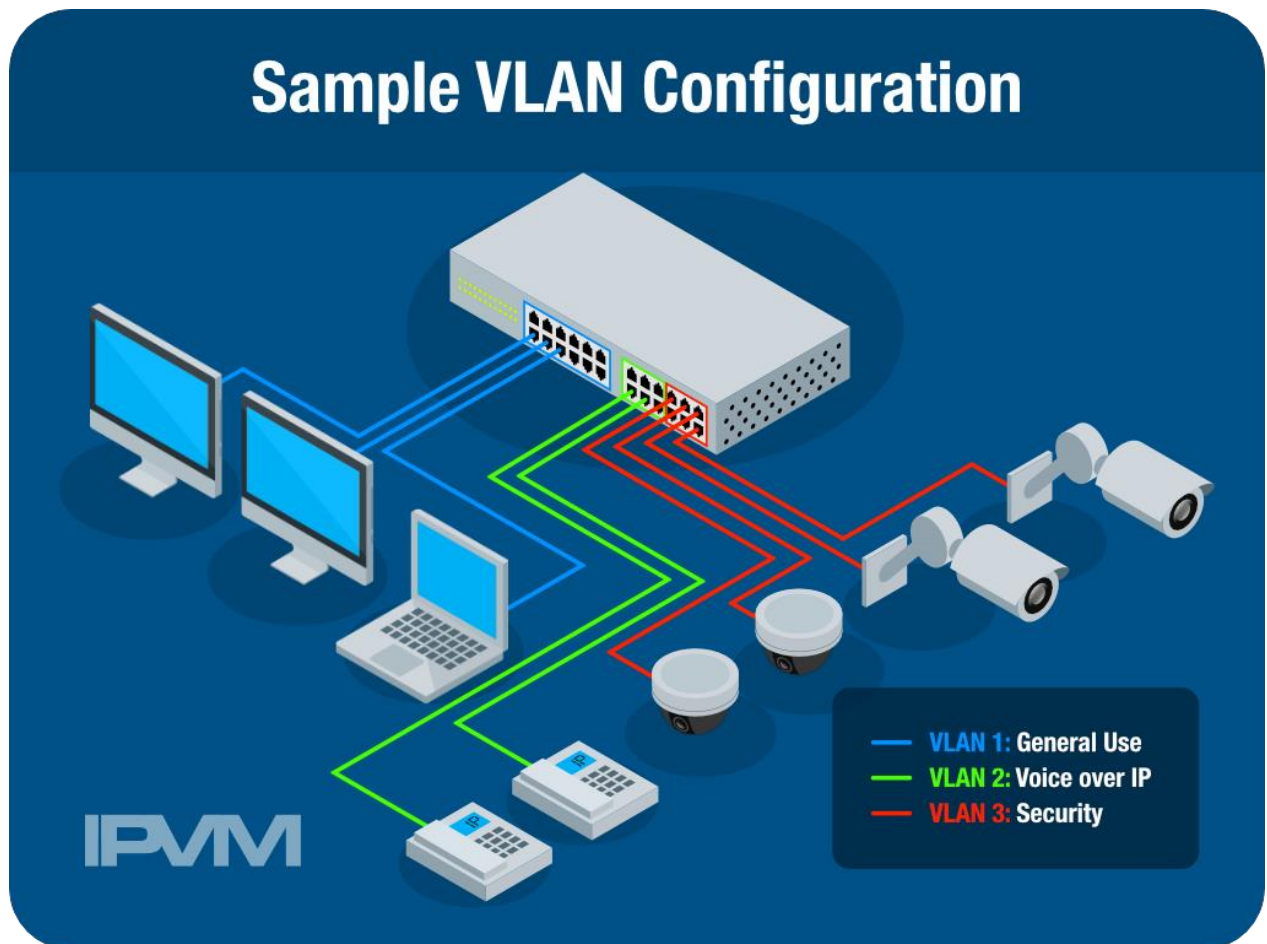
For example, 12 port switches may support 90 total watts of power, which equals 7.5 watts available per port. In order for this switch to provide full 802.3af (15.4 watts) power for each port the total power budget would need to be 184.8 watts.



PoE capable Midspan injectors can also be used to bolster additional power needed. If the switch does not have enough total power for all cameras, a Midspan could be put in series with the cable runs to the PoE+ cameras (for example). This will reduce the overall power load on the switch and offload it to the Midspan.

Virtual Local Area Networks logically divide a switch or switches into multiple separate virtual networks which by nature are isolated from each other unless specifically routed together.

Most VLANs are implemented using 802.1Q tagging. The diagram below shows how VLANs on a single switch can segregate traffic from different applications on a shared network



VLANs can be static or dynamic. In a static VLAN, the switch port that the device is connected to determines the VLAN ID.

Dynamic VLANs are created by policy, either in the switch, or a separate server. When a device is connected to the switch it is assigned a VLAN ID based on MAC address or login credentials. Dynamic VLANs are a bit more flexible as it allows devices to connect to any port on the switch,



but still get the correct VLAN ID. However initial setup of a Dynamic VLAN can be more time consuming than Static.

A main benefit of VLANs is increased security. By segmenting networks that cannot talk to each other unless specifically routed together, it is possible for a surveillance network to coexist with a general data or voice network on the same switch without interfering with each other.

VLANs are NOT used to save bandwidth, though it is a popular myth.

VLANs can also be used with Quality of Service (QoS) to help prioritize bandwidth. A surveillance VLAN, for example, may have higher priority than a VLAN for general data traffic.

Managed switches are required to implement VLANs, as unmanaged switches have no configuration capabilities. The majority of managed switches today support VLANs.

In small systems, VLANs are generally not used because low cost unmanaged switches are commonly deployed. Setting up a VLAN requires additional setup, therefore additional cost making it less attractive in small systems.

Shared networks more often employ VLANs to separate surveillance, voice and general data traffic, for example. These VLANs may be routed together to allow certain individuals on other VLANs access to the surveillance network.

Dedicated networks commonly do not use VLANs, as the networks are physically segregated by hardware devices.

However, in large scale dedicated networks VLANs could be used in circumstances where camera traffic needs to be isolated from client viewing stations to prevent the viewing stations from accessing the cameras web interface directly. Large scale networks may also include access control hardware which is recommended by the manufacturers to have its own VLAN.

Quality of Service (QoS) refers to strategies used to manage available bandwidth for specific applications, such as prioritizing one type of traffic over another. For example, QoS may be used to prioritize voice and video traffic over general data traffic (such as file sharing, Internet browsing, etc).

QoS is generally applied by application, VLAN or user. Setting QoS by application is common and will determine which application should have higher priority. For example, FTP traffic may be assigned a lower priority than streaming video to help maintain proper frame rate and quality of the video. However, voice traffic may be prioritized above video, as degradation in



voice is more noticeable to users, while video may handle light latency better, making voice the higher priority.

Setting QoS by application requires that all components (cameras, switches, servers, etc.) support QoS, normally via DiffServ, which is the most common means of tagging traffic by application.

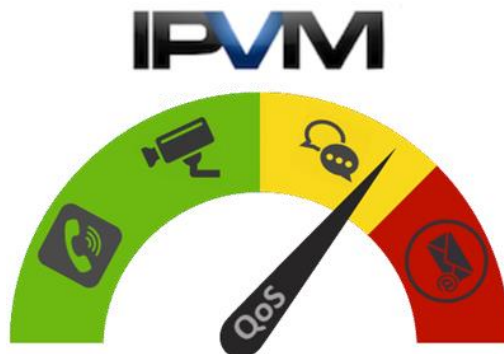
Setting QoS by VLAN will assign different QoS values to each VLAN. For example, a security VLAN may have higher priority than an office VLAN. Setting QoS by VLAN requires that all devices support VLAN tagging, but QoS itself is setup at the switch, requiring nothing additional at the end device(s).

Setting QoS by user, though uncommon in security, may be preferred by network administrators or database workers who require certain bandwidth to complete their tasks.

Regardless of which method is used, managed switches are required.

QoS does not guarantee bandwidth, it prioritizes it by arranging the order in which packets/data are queued for sending.

Setting up QoS on an IP camera, typically a DiffServ code point (DSCP) must be configured in the camera itself, which correlates to priority level, assigned in the switch. Some cameras have the ability to set different DSCP's for audio, video, alarm, and management so these are prioritized differently. Not all IP cameras support DiffServ.

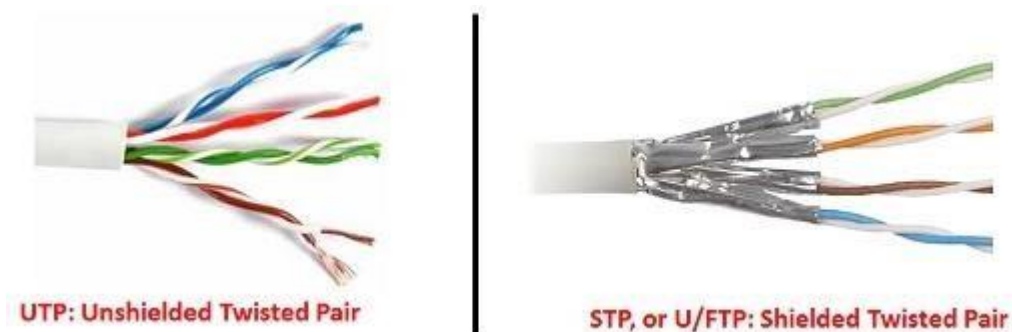


Class 5 - Network Cabling

The two common types of twisted pair cabling used in surveillance are Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP). STP can also be called Unscreened/Foil shielded Twisted Pair (U/FTP).

Shielding, where each pair is wrapped in a foil shield should not be confused with cable screening, where the entire wire bundle is wrapped by metallic foil or mesh.

This image shows how UTP and STP differ when looking under the jacket.



There are some key physical differences between UTP and STP, such as:

- *Metallic Foil Shield:* A thin layer of foil surround wire pairs on STP cable.
- *Thicker Jacket:* The added foil layer in STP makes the jacket itself thicker, adding weight and diameter.
- *Cores, Pull Strips, and Groundwires:* Depending on the manufacturer, STP could have a plastic 'core' divider, strings to help strip the jacket and additional grounding wires.

The physical difference of STP cabling can provide added benefits that UTP does not possess, including:

- *EMI Resistance:* The primary advantage shielding is protection from Electromagnetic Interference (EMI). Because each pair is individually wrapped, it reduces or eliminates ambient interference to permeate the cable.
- *Isolated line noise:* Unshielded cable can be a source of interference within itself. Shielding reduces or eliminates this problem.

STP cabling should be used anywhere that there could be a problem with interference, including adjacent to high voltage lines, near inductive sources (such as electrical motors, power transformers, etc.), near GSM/Walkie Talkie devices (such as high powered repeaters or



transmitters), and near fluorescent light fixtures. These are all common sources of interference that can negatively affect network video.

UTP cabling is the most common cable type deployed today. Despite some manufacturer's claims, it is our experience that STP cabling is NOT required for outdoor runs. STP should be used where Ethernet is run in 'high risk' environments (described above), or where earth grounding switches and endpoint devices is not possible.

Cabling best practices should be considered in order to maintain a neat and organized cabling infrastructure. Some of these best practices include:

- *Label all cables:* Properly labeling all cables can help reduce troubleshooting time and can eliminate lengthy 'hunt and peck' diagnosing efforts.
- *Use Cable Trays/Hooks/Tubing:* These help eliminate displacement if cables are laying on ceiling tile (for example) and will keep the cabling up and away from potential harm.
- *Jacket color is important:* Using different colored cables for different applications can drastically help identify which cables belong to which system. Red should be avoided as that is commonly used to identify fire cabling.
- *Draw a map:* Identifying each cable run and drop on a floor plan can save a lot of troubleshooting time. This makes cable runs easily identifiable and can be shared with others who may be doing work that could disturb cabling.
- *Don't use excessive service loops:* BICSI recommends 3m at the rack and 1m at the outlet or device. Lengthy service loops can exceed the recommended cable bend radii and cause line interference. It also adds unnecessary weight to the cable infrastructure.

There is no universal code or specs for running cable. BICSI has published a number of best practices guides for design and installation. A bid may reference a BICSI publication number to define how the installation is to be executed.

Commonly cited publications include:

- NECA/BICSI 607-2011, Standard for Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings
- BICSI 002-2011, Data Center Design and Implementation Best Practices
- ANSI/BICSI 001-2009, Information Transport Systems Design Standard for K-12 Educational Institutions
- ANSI/NECA/BICSI 568-2006, Standard for Installing Commercial Building Telecommunications Cabling



- Electronic Safety and Security Design Reference Manual (ESSDRM)
- Telecommunications Distribution Methods Manual (TDMM)

The three main types of cable test tools are Certifiers, Qualifiers and Verifiers.

Certifiers are the only one to test to EIA/TIA568B standards. It is the most expensive test tool.

Qualifiers deliver a detailed technical test but are not standards compliant. They are cheaper than Certifiers, but more expensive than Verifiers.

Verifiers provide basic cable testing and commonly do not store or save results:

- Wiremap: Determines whether UTP is terminated correctly typically to EIA/TIA568A/B. A graphical display is easier to identify exactly which pins are the issue and how they are crossed.
- Length/distance to fault: Can tell the length of the cable run and how far to a short or fault.
- Cable Identification: Has a remote unit that is a unique identifier. This can be used to more easily identify a single cable within a large bundle.
- Service Detection: Can identify use of Ethernet, PoE, or Plain Old Telephone Service (POTS) service. It will not verify proper operation, however.

Cable verifiers range from \$125-\$450 USD, depending on graphical display vs. LED, display size, etc.

Qualifiers add additional functions and are the middle ground between verifiers and certifiers. Qualifiers additional features include:

- Service testing: Also detects speed (i.e. 10/100, GbE, etc.) in addition to service detection.
- PoE testing: Also displays voltage and max wattage of PoE to help troubleshoot power budget issues.
- Saved test results: Most can save test results to onboard storage so they can be used for documentation.
- More detailed display: Displays detailed fault information showing whether there is a short or crosstalk issue.

Qualifiers are more expensive than verifiers and can range between about \$1,100 to \$1,800



Certifiers test to ANSI/EIA/TIA standards. They include all of the features of verifiers and qualifiers, adding more in depth tests, including:

- Crosstalk: Measures the amount of signal leakage between pairs.
- Propagation delay: Measures the amount of time it takes for the signal to reach the end of the cable.
- Insertion/return loss: Measures signal loss caused by connections in the cable (insertion loss) or reflects signal back at the test point (return loss), commonly caused by poor terminations or cable faults.

Certifiers can range from \$5,000 to \$10,000+ and must be factory calibrated every 2 - 3 years.

Integrators should keep at least a verifier on hand, though for larger installations, the additional cost of a qualifier may be justified. Only in rare cases is a certifier needed.





Class 6 – Protocols

The two major protocols used for video transmission are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

TCP is connection-oriented, which requires a connection between both devices to perform a handshake prior to communicating. It also has error correction, where each set of packets is confirmed as received via an acknowledgement by the recipient before the next set is sent. This ensures that all data was received and in the correct order. Packets not properly received will be retransmitted until properly sent.

UDP is connectionless and packets are sent out without a handshake or confirmation of receipt. No error correction is done with UDP. Packet loss and errors are common with packets arriving out of order, or not at all.

TCP tends to drop frames, causing a stuttering affect when bandwidth is insufficient, while UDP tends to smear the image in addition to some stuttering.

There is minimal impact on latency between TCP and UDP, with both averaging 250-300ms.

UDP tends to be preferred for live viewing as there is lower overhead and network glitches can generally tolerated better.

TCP tends to be preferred for recording, as TCP helps to ensure all frame are received and are in the correct order.

IP cameras commonly support TCP and UDP, but may not have it as a user selectable option. Often the VMS it is connected to determines which protocol to use.

Not all VMS's allow control of the protocol:

- Avigilon: No manual control. UDP is used by default video
- ExacqVision: No direct control, but is generally determined by the driver being used. In ONVIF and RTSP cameras the protocol may be selected by appending “#transport=x” where ‘x’ is TCP or UDP.
- Genetec: Allows manual control. By default cameras are set to ‘auto’, which attempts multicast UDP, then unicast UDP, then TCP to connect.



- Milestone XProtect: Some manual control, if it's supported by the camera and driver. TCP is used by default and connections from the recorder to the client is TCP only.

Unicast and Multicast are transmission methods for video. Unicast is the most commonly used method, where each connection to a camera (for example) gets its own copy of the video feed. For example, if a camera streams at 2 Mb/s and four clients request video, a total of 8 Mb/s is needed.

Multicast will send the video to a single multicast group, which may contain many clients. Now the 2 Mb/s stream will only require 2 Mb/s instead of 8 Mb/s.

Multicast is not a must-have capability, but in large installation can be useful. For example, when a large number of clients are viewing a large number of cameras.

Multicast networks require all components support Internet Group Management Protocol (IGMP). IGMP manages multicast groups and is supported by almost all managed switches. Multicast networks add complexity to setup and installation. Many (but not all) camera manufacturers support multicast. VMS support is limited:

- Avigilon: Supported by Avigilon cameras, but not Avigilon Control Center.
- DVTel: Supported in all versions of Latitude.
- Exacq: Currently no multicast support.
- Genetec: Multicast is supported in all versions.
- Milestone: Multicast is supported only in Milestone Corporate.
- OnSSI: Multicast is supported only in Ocularis ES.

Correctly synchronized network time is critical in surveillance systems. Simple Network Time Protocol (SNTP) is the most commonly used time protocol. It is a less complex and less accurate form of Network Time Protocol (NTP). SNTP is generally accurate within a few milliseconds, which is sufficient for surveillance.

Windows time protocol should not be used in surveillance, as it is inaccurate and can cause a drift of several seconds.

Most cameras support time synchronization to a time server. However, because time is synchronized to Universal Coordinated Time (UTC), which applies no time zone or daylight saving time, these must be set correctly within the camera or other network device.



It is not recommended to set the time on a camera (for example) manually, as it can be difficult to get all cameras to the same second, or even minute. Drifting will occur over time which can cause obscure time differences (6 minutes, 18 minutes off, etc.) between devices.

VMSs handle time stamps in two ways:

Stamping on arrival: Each frame of video is marked with the time it was received. This can eliminate inaccurate camera time issues.

Using camera time stamps: The time provided by the camera is used, which unless properly synchronized can cause issues. For example, if a camera time is off by two hours, the video on the VMS system will be marked two hours off. This can cause major problems with playback, as the video is stored two hours off from where it should be. This can make synchronized playback unusable or worse, render the video inadmissible in court.

Public time servers can be used to synchronize time on network devices that have Internet access. A private time server can be configured on the LAN using an existing server (for example). All devices can synchronize with this server and would not require them to have Internet access. Dedicated GPS servers can also be used in environments that require very precise time (to the nanosecond), but they're often expensive (\$125+) and unnecessary for surveillance.

It is recommended to synchronize all surveillance network devices to a time source, preferably the same one.

Simple Network Management Protocol (SNMP) can be used to monitor health and performance of network devices. Device information can be requested by a SNMP manager application, or sent from the device to the manager application via traps. Requests could include CPU usage, bandwidth, disk write speed, etc. Traps can notify the manager for events including temperature alerts, power supply failures, camera tampering, etc.

Devices (such as cameras, switches, servers, etc.) are added to a monitoring manager application which interprets SNMP requests and traps. Sensors are associated with a device and can include anything that is able to be monitored (such as bandwidth, uptime, ping, throughput, etc.).

SNMP support varies by device. Servers and switches commonly provide more detail than IP cameras. Most cameras are limited to simple ping and HTTP requests. Some cameras support traps upon critical failures which include, temperature alarms, hardware failures, power supply problems, etc.



Servers deliver more detailed information such CPU load, throughput, memory usage, disk I/O, etc.

Managed switches also deliver detailed information usually on a port by port basis, such as throughput, errors, VLAN traffic, etc.

Management Information Base (MIB) files are created by a manufacturer that contains details about available requests and traps. The file is imported into the monitoring program.



Class 7 – Installation

BICSI is a standards making body prevalent in the IT world. They're best known for publishing two manuals for cabling standards:

- **Telecommunications Distribution Methods Manual (TDMM):** This covers design and planning of network systems, covering cabling, bonding/grounding systems, cable supports, equipment room planning, space calculations, and more. It also forms the basis of the Registered Communications Distribution Designer (RCDD) credential.
- **Information Technology Systems Installation Methods Manual (ITSIMM):** This focuses on actual installation issues, such as cable terminations and support, fire stopping methods, planning cable paths and spaces, etc. It is used as study material for BICSI's certified installer program.

RCDD is generally used by engineers of network infrastructure design, however, it is not commonly used in surveillance.

BICSI publishes standards, not codes. The material is viewed as best practice, but is not required for inspection or code compliance, unless specifically referenced by a code.

Some key takeaways from the TDMM and ITSIMM include:

- **Modular plugs are OK:** Originally connecting to an edge device (such as a camera) with a modular plug (direct attached) vs. a jack and patch connection was against the standard. However, in recent years BICSI has approved the use of modular 'direct attached' connections.
- **Patch panel terminations:** Cables at the 'head end' must be terminated to a patch panel and cannot be terminated with a plug and attached directly to a switch.
- **Testing:** BICSI requires that each cable is certified and documented.
- **Labeling:** Typically label identifiers include which room, rack, patch panel and port a cable terminates to.
- **Cable Support:** Cables should be supported every 48-60 inches or installed in cable trays or conduit.
- **Maintain fire stopping:** Careful repair of fire stop pathways must be done if penetrating a fire wall.
- **Telecommunications Rooms:** Guidelines for how telecommunications room should be located, sized and laid out.



- **Grounding/Bonding:** Specifies use of dedicated telecommunications grounding/bonding infrastructure, consisting of a dedicated grounding backbone run to each telecommunications room, terminated to a grounding busbar. Equipment/racks are connected to the busbar for proper grounding.
- **Power Distribution:** Provides guidelines for power conditioning, protection and UPS systems.



Class 8 - Remote Network Access

Remotely accessing video can be difficult for 3 reasons:

- **Private Networks:** Most video surveillance devices use private IP's, which are not accessible by nature over the public Internet.
- **Firewalls:** Most surveillance networks are firewalled, which blocks direct access to the public Internet.
- **Dynamic Addressing:** Many home / small systems and remote locations use dynamic public IP addresses. These IP's may (and likely will) change leaving a previously accessible remote location now inaccessible.

Port forwarding is one of the oldest ways to provide remote access. It requires manual configuration of the firewall to map a private IP address to a public IP address. Port 80 and port 554 are most often used and opened. Some systems require multiple ports to be opened for configuration, control and/or authentication. This will require multiple internal ports to be mapped to external ports. For example, like this Dahua DVR.

✓ 192.168.1.169:8080	HTTP TCP Any -> 8080
✓ 192.168.1.169:37777	TCP TCP Any -> 37777
✓ 192.168.1.169:37778	UDP UDP Any -> 37778
✓ 192.168.1.169:554	RTSP UDP Any -> 554
✓ 192.168.1.169:554	RTSP TCP Any -> 554
✓ 192.168.1.169:161	SNMP UDP Any -> 161
✓ 192.168.1.169:443	HTTPS TCP Any -> 443

If two NVR's are to be viewed remotely and they both use port 80, the port mapping could look like:

- NVR1: 145.10.234.12:8080 ---> 192.168.3.8:80
- NVR2: 145.10.234.12:8081 ---> 192.168.3.9:80

Universal Plug n Play (UPnP) is a set of protocols that automate device discovery and configuration on the LAN. It aims to eliminate manual port configuration (such as port



forwarding) by doing the port mapping automatically without user interaction. UPnP is unreliable, however, and its functionality is often turned off on network devices. Because of this port forwarding is often used instead of UPnP in professional networks.

Dynamic Domain Name Service (Dynamic DNS) is used to map a dynamic public IP (provided by the ISP) to a common name that does not change. This means that a remote device is accessible via a host name like NVR3.dyndns.org instead of the public IP (such as, 84.32.34.11). The DDNS service updates the IP address corresponding to each hostname periodically, or automatically detects changes and updates immediately in some cases.

In surveillance, DDNS is commonly used with DVR's and consumer cameras. Some manufacturers may host their own DDNS service for free to users who purchase their equipment.

Dedicated Virtual Private Networks (VPNs) are typically hardware appliances located at each site. They are used to create a secure tunnel to each other through the Internet. In surveillance these are commonly used in larger multi-site installations.

VPNs have the benefits of 'high security' due to the protected encrypted tunneling they implement from end-to-end.

VPN benefits include high reliability/ high uptime due to the hardware based portal and appliance or thick client architecture of the connections.

VPNs typically permit granular management, reporting, and monitoring of the connections using them.

However, VPN disadvantages include:

- High Cost – often thousands of dollars to purchase a management appliance plus ongoing contract security and maintenance fees.
- High Complexity – VPNs are seldom easy to properly setup without specific training or skills

'Site-to-site' VPNs are typically used to connect multiple entire offices, while 'Remote Access' VPNs are typically used to connect single clients to a network due to their less expensive prices.

Cloud / Phone Home products and services are usually closed to outside integrations and use proprietary equipment/ cameras.

Cloud / Phone Home services aim to eliminate the complexity and potential errors of port forwarding, UPnP and Dynamic DNS.



These cloud connections bypass firewalls and form a VPN automatically without user interaction. Nestcam, Arlo, and AVHS are two prominent examples of this.

These connections use Transport Layer Security (TLS) and include these basic steps:

1. Initiating device sends a HELLO message to request a connection.
2. Server sends HELLO along with a security certificate.
3. A handshake is performed and a secure tunnel is set up.
4. Once the TLS tunnel is in place, data sent through it is encrypted, with protocol and data specifics obscured (shown only as "application data" in the example below.)

Source	Destination	Protocol	Length	Info
195.60.68.121	172.20.128.82	TCP	74	443→46355 [SYN, ACK] Seq=0 Ack=1 win=1460
172.20.128.82	195.60.68.121	TCP	66	46355→443 [ACK] Seq=1 Ack=1 win=1460
172.20.128.82	195.60.68.121	TLSv1	352	Client Hello 1
195.60.68.121	172.20.128.82	TCP	66	443→46355 [ACK] Seq=1 Ack=287 win=1460
195.60.68.121	172.20.128.82	TLSv1	1514	Server Hello 2
195.60.68.121	172.20.128.82	TLSv1	213	Certificate
172.20.128.82	195.60.68.121	TCP	66	46355→443 [ACK] Seq=287 Ack=1449 win=1460
172.20.128.82	195.60.68.121	TCP	66	46355→443 [ACK] Seq=287 Ack=1596 win=1460
172.20.128.82	195.60.68.121	TLSv1	660	Certificate, Client Key Exchange, Change Cipher Spec, New Session Ticket, 3
195.60.68.121	172.20.128.82	TLSv1	300	New Session Ticket, Change Cipher Spec, 4
172.20.128.82	195.60.68.121	TCP	66	46355→443 [ACK] Seq=881 Ack=1830 win=1460
172.20.128.82	195.60.68.121	TLSv1	428	Application Data, Application Data
195.60.68.121	172.20.128.82	TLSv1	151	Application Data
172.20.128.82	195.60.68.121	TCP	66	46355→443 [ACK] Seq=1243 Ack=1915 win=1460
195.60.68.121	172.20.128.82	TLSv1	454	Application Data, Application Data,

Once the tunnel is setup, protocols such as HTTP, RTSP, TCP, UDP, etc. are used for camera control and streaming.

Cloud / Phone home services are the easiest to setup and most reliable for remote connectivity, however, IT administrators may have concerns about allowing devices to get around their firewall.



Class 9 - Network Security

Network security problems with security cameras have become big news, with many leading brands like Hikvision, Axis being exploited multiple times over recent months.

Exploits like IP Camera Trolling, that demonstrate remote control of IP cameras by hackers, are especially alarming.

Do not use manufacturer default passwords, which is becoming a less common feature supported by manufacturers due to security concerns.

Many cameras come with publicly known default password that can be discovered with a simple websearch only and are not controlled or protected.

Default admin logins typically give immediate access to everything, including top settings.

When changing away from defaults, use strong passwords basic as a free method of improving device security.

As easy/ simple as it might be, this step is ignored by many installers.

“Strong” passwords containing:

- 10-15 characters
- Mix of numerical, alphabetic, and special characters
- Nonsequential values and no patterns (ie: qwerty1234)

ONVIF Profile Q will make changing default passwords mandatory.

Use formal methods of managing passwords like keeper apps or protected documents, not handwritten notes or uncontrolled emails/memos.

Many exploits take advantage of open ports like SSH and telnet.

Always turn these off if unused to close off a risky open and unprotected way into cameras.

Search engines like Shodan.io make it easy to find publicly accessible IP devices, make closing off ports and changing default credentials critical.

HTTPS protection is becoming a common option to encrypt data traffic to/from cameras, and is widely supported by camera manufacturers and VMS companies.



However, the video stream may not be encrypted unless the RTSP tunnels are HTTPS too.

Disable camera 'ping' replies to foil hacker attempts to detect cameras on the network.

Always update device firmware for security reasons:

- Often plugs known holes
- Fixes other security vulnerabilities

VLANs also useful to isolate systems, prevent intrusion from other parts of a network. The method of 802.1Q tagging of video data helps ID it to a network VLAN searching for video data. Every packet of data is tagged. This information is interpreted by the switch and forwarded to other devices on the VLAN.

MAC address filtering allows only specific MAC addresses to connect to the switch. Once all devices (cameras, clients, servers) are connected, MAC filtering can be enabled and automatically add connected device MAC information to the 'whitelist'. MAC information can be administered manually to add/remove devices as necessary.

- 'MAC whitelists' only allow specific devices, while:
- 'MAC blacklists' specifically exclude certain devices.

These MAC filters are often available on non-managed, consumer smart switches and routers, not just fully managed gear.

The importance of IP Video/ Network Security has taken central importance due to recent hacking scandals surrounding Hikvision, Foscam, and other mainstream camera brands and network resources.

LDAP/Active Directory can be used to apply existing strong network passwords to a VMS system, where permissions are assigned by a central server (also called single sign-on).

Active directory is not commonly supported by IP cameras, as it is a Microsoft product and most IP cameras run on Linux.

802.1X is a credentials based authentication method, which uses a 'supplicant' (such as a camera) to connect to an authenticator.

The authenticator then checks credentials of the supplicant with an authentication server. The flow is: Supplicant -> Authenticator -> Authentication Server. Setting up 802.1X can be cumbersome and difficult, provides strong network security. All devices which are to use



802.1X, must support it (cameras, servers, switches, etc.). Managed switches must be used with 802.1X.

Disabling ports allows unused ports on a managed switch to be turned off. If a device is connected to a disabled port, it will not connect to the network. However, someone could unplug an active port (such as a camera) and use it to access the network.

Locking plugs mechanically lock a cable into a switch, patch panel or wall jack and a special tool is required to remove them. They can be used to fill unused ports also. With enough time, these devices can be forced or pried out and should not be used as a full proof method of security.

Door locks and physical access control to the server room helps reduce or eliminate unauthorized access to the network equipment. If the door(s) cannot be secured, individual rack cages / switch racks can have locks, etc. to prevent unauthorized access.

None of these security methods are full-proof, but used together can greatly improve the security of your network and network equipment.



Class 10 - Hacking

Recent attacks on cameras and DVRs use commonly open ports to gain access.

Telnet, SSH, and FTP ports are especially vulnerable, as they have been more commonly attacked via malware (such as the Mirai Botnet).

None of the manufacturers now leave SSH nor Telnet open, a basic though important step forward, given the Mirai attacks use of Telnet.

In IPVM audits, Arecont had the worst password security management, with no authentication by default, no enforcing of strong passwords, no auto account lock for failed attempts plus the only manufacturer not to support HTTPS

Hikvision had the strongest password security management, requiring strong passwords, supporting auto lock out for failed attempts and without hardcoded accounts.

Hikvision is the only manufacturer in the audited group of major manufacturers that defaulted phone home access which is a convenience feature but also a potential security risk

Locking accounts upon failed logins is still uncommon with only 3 of the 10 supporting it (Dahua, Hikvision and Samsung) despite this being a common practice and key countermeasure to mitigate dictionary attacks

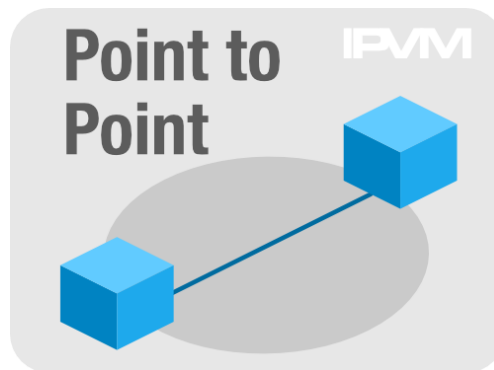


Class 11 – Wireless

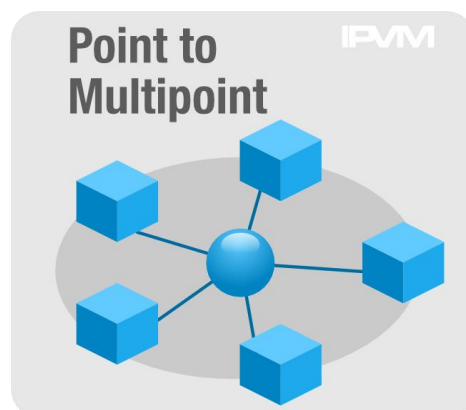
There are 3 basic wireless topologies used in surveillance:

Point to Point (PtP): This is the most common type of link used, which consists of a single radio at the device connected to a single radio on the surveillance network. Most commonly, PtP radios are used to connect cameras from a single location (such as a parking lot pole, for example) to a surveillance system. PtP can also be used as a wireless backhaul, connecting two building together, or multipoint base stations connected to another point in the network.

Directional antennas are often used in PtP applications. These links can span multiple miles and are available in many frequencies (900 MHz, 2.4 GHz, 5.8 GHz and higher). The following image depicts a Point to Point link

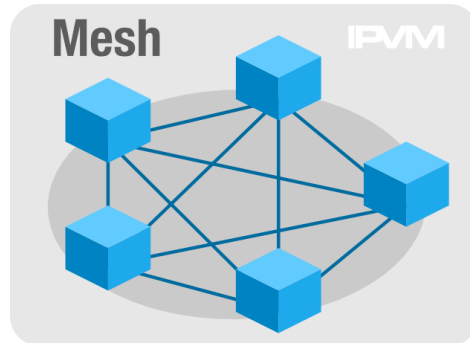


Point to Multipoint (PtMP): A single radio acts as a base station and is connected to the central network, and multiple radios connect to it. These may be the same radio types used in PtP, though some manufacturers have special base stations designed to handle higher data rates. These networks can be small, with a few cameras connected to a base station, or very large city-wide networks. Base stations typically use omnidirectional antennas or very wide angle directional antennas.





Mesh: Each wireless node connects to multiple other radios, creating multiple paths for network traffic. If one link fails, data can be rerouted via another path. Mesh radios are typically more expensive than PtP and PtMP radios. The radios can use any type of antenna.



Cameras with built in wireless are uncommon, with some consumer level cameras offering it (mostly cube cameras). These wireless links typically have shorter ranges and are not used in professional systems.

There are two fundamental types of external antennas used in wireless surveillance:

Omnidirectional antennas radiate signal in all directions. These are the same types of antennas used in most wireless consumer routers. The following image depicts what common omnidirectional antennas look like:





Directional antennas come in many styles with varying beamwidths. These could range from 15 degrees to over 100 degrees wide. The following image is an example of a few common directional antenna form factors:



There are some key performance differences between these two antenna styles.

Omnidirectional antennas are easier to setup and require little to no alignment, but offer the shortest range. Directional antennas are aimed often by sight due to their narrow beamwidth. They offer a higher performance range than omnidirectional antennas and are forgiving of small changes due to wind, sway and vibration.

Highly directional antennas are more specialized, providing the strongest signal strength but a high level of complexity to setup due to the extreme narrow beamwidths. These often require lasers, signal strength meters, etc. to aim them correctly, with little, if any forgiveness for wind, sway and vibration.

Antenna gain is important because everything else equal, the higher the gain the further the signal can transmit. Omnidirectional antennas are often as low as 3dB while directional antennas can be 24dB or higher.

Several factors drive how far an antenna can transmit, including:

- The frequency being used: higher the frequency, the shorter one can go (e.g., 5.8Mhz, everything else equal, has shorter range than 2.4Ghz).



- The gain of the antennas being used: the higher the gain (e.g., 24dB instead of 12dB), the farther one can go.
- The sensitivity level the receiver requires. The higher the level, the easier it is to meet but typically less bandwidth is available (e.g., -96dBm vs -74dBm for higher bandwidth levels).
- The transmission power of the radio. Most surveillance wireless systems use licensed frequencies which cap how much power can be put out, constraining how far the signal can go (unlike, e.g., a TV station which is comparatively 'blasting' out transmissions at much lower frequencies).

Ideally, wireless links will have clear line of sight. However different frequencies can handle obstructions better than others. When RF hits an obstruction, some of the signal is absorbed and/or reflected, reducing the level of signal reaching the receiving end. Drywall and wood studs absorb and reflect less of the wireless signal than heavy concrete, brick and steel construction materials. Multipath propagation is a partial reflection of the signal from its intended path, resulting in it being received out of sync with the stronger non-reflected transmission, reducing link quality.

Frequency impacts available throughput and how well it can penetrate an obstruction. Higher frequencies allow for higher throughput. High frequency radios may transmit GbE speeds, while lower frequency radios may be limited to 5 Mb/s or less. Low frequencies are better able to penetrate obstructions better than higher frequencies. For example, 900 MHz, 2.4 GHz, etc. may function without line of sight while 20 or 40 GHz radios may see performance degradation by rain or fog due to the moisture in the air.

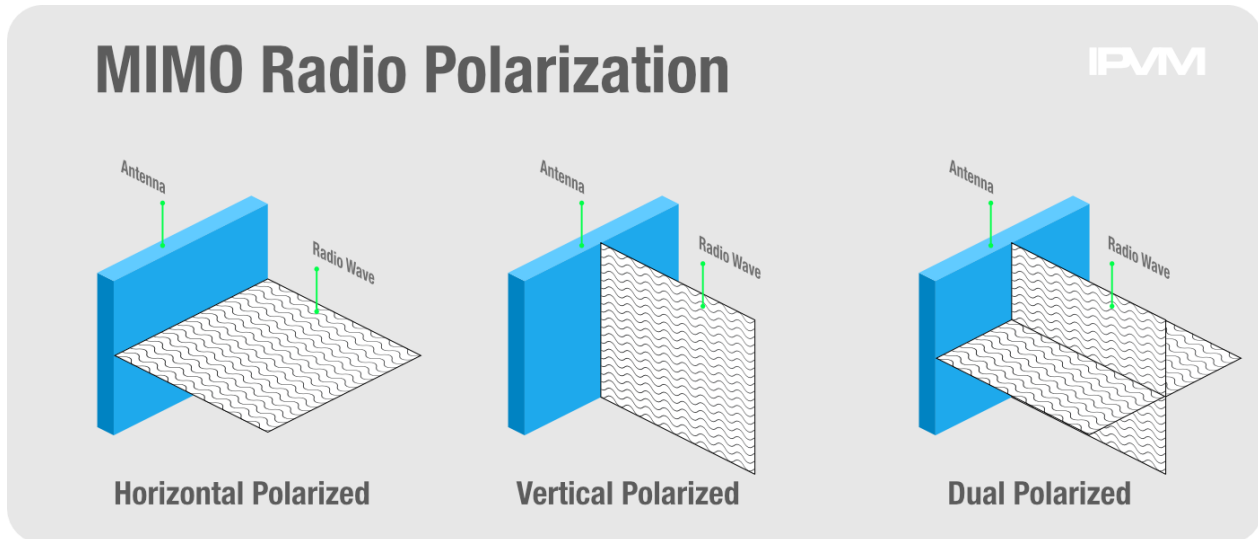
The most common frequencies used in surveillance include 900 MHz, 2.4 GHz and 5.8 GHz.

2.4/5.8 GHz frequencies are non-licensed and free for anyone to use. These are also used commonly in 802.11 (a/b/g/n/ac) home and small office networks, increasing the potential for interference. 2.4 GHz may be used in lower throughput non-line of sight applications, where 5.8 GHz may require full line of sight.

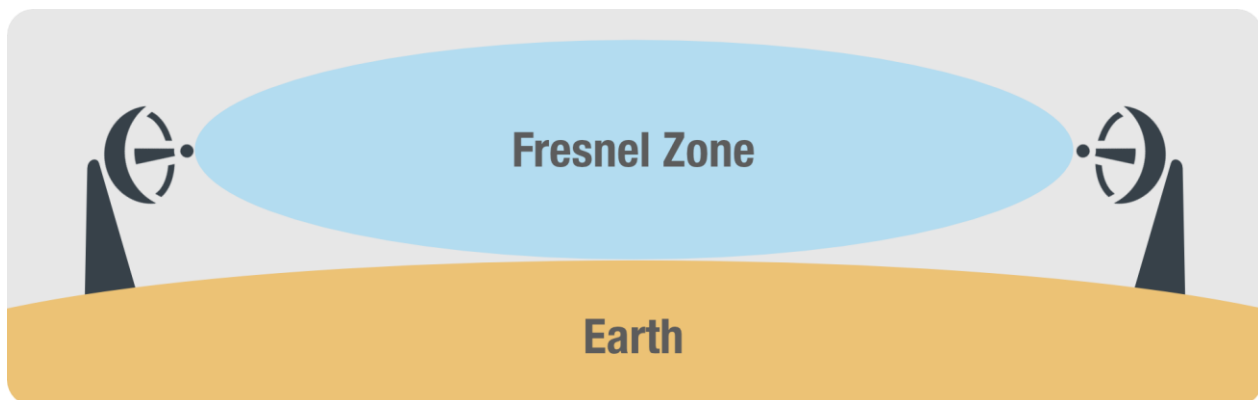
900 MHz, also non-licensed, is most common in non-line of sight applications. The lower frequency band is better able to penetrate objects than 2.4 GHz or 5.8 GHz, however, have a much lower throughput. 900 MHz is also crowded and may experience interference, as many consumer grade products use it.

Multiple Input Multiple Output (MIMO) radios spread the signal across two or more paths. This helps increase bandwidth and resistance to interference. These commonly use a dual-polarized antenna, which transmits both signals at once, rotated 90 degrees. Though less common, they

could use two or more distinct antennas. The following image illustrates single vs. dualpolarized antennas:



There are no hard and fast rules for transmission range in wireless networks. Distances are affected by issues such as obstructions, frequency used, transmission power, and antenna gain. Longer links require more specific and precise antenna alignment and, in very long distances, may even need to take the curvature of the earth into account (illustrated in the following image).



Wireless links are sensitive to environmental factors and fluctuations in site conditions, making maintenance a key consideration when deploying wireless. Things such as antenna alignment, corrosion on the connectors, foliage in line of sight, etc. should be checked periodically.