

5. IP Network technologies

The Internet Protocol (IP) is the most widely used computer communication protocol today. It is the base protocol used for Internet, communication such as e-mail, web and multimedia. One of the reasons for its popularity is its scalability. In other words, it works as well in very small installations as it does in very large ones and is supported by an increasingly wide range of high-performance, low-cost and industry-proven equipment and technologies.

This chapter provides an overview of the different technologies in use, based on IP, to take full advantage of a network video system.

5.1. Ethernet

In today's offices, computers are most likely to be using TCP/IP connected via an Ethernet network. Ethernet gives a fast network at a reasonable cost. Most modern computers are supplied with an integrated Ethernet interface or can easily accommodate an Ethernet network interface card (NIC).

Common Ethernet types:

10 Mbit/s (10 Mbps) Ethernet

This standard is rarely used in production networks today due to its low capacity, and has been replaced by 100 Mbit/s Ethernet since the late 90's. The most common topology used for 10 Mbit/s Ethernet was called 10BASE-T; it uses 4 wires (two twisted pairs) on a cat-3 or cat-5 cable. A hub or switch sits in the center and has a port for each node. The same configuration is used for Fast Ethernet and Gigabit Ethernet.

Fast Ethernet (100 Mbit/s)

Supporting data transfer rates of up to 100 Mbit/s, Fast Ethernet is the most common Ethernet type used in computer networks today. The main standard is called 100BASE-T. Although newer and faster than 10 Mbit Ethernet, in all other respects it is the same. The 100BASE-T standard can be subdivided into:

- 100BASE-TX: Uses twisted pair copper cabling (cat-5).
- 100BASE-FX: 100 Mbit/s Ethernet over optical fiber.

Note: most 100 Mbit network switches support both 10 and 100 Mbit to ensure backward compatibility (commonly called 10/100 network switch).

Gigabit Ethernet (1000 Mbit/s)

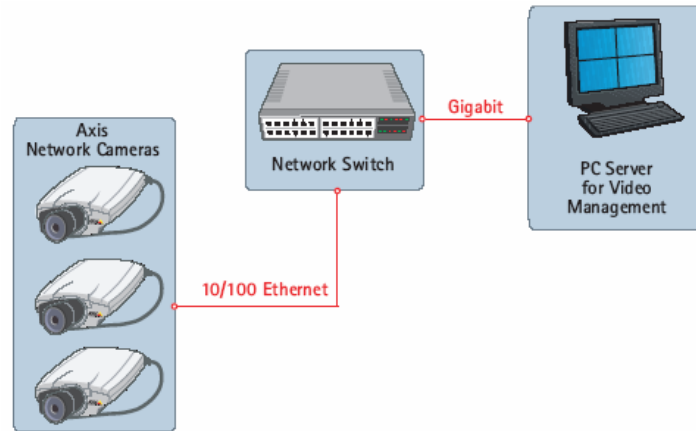
This is the current standard that is being endorsed for desktop computers by networking equipment vendors. The most common use today is however for backbones in between network servers and network switches. 1000 Mbit/s is widely used and it can be subdivided into:

- 1000BASE-T: 1 Gbit/s over cat-5e or cat-6 copper cabling.
- 1000BASE-SX: 1 Gbit/s over multi-mode fiber (up to 550m).
- 1000BASE-LX: 1 Gbit/s over multi-mode fiber (up to 550m). Optimized for longer distances (up to 10km) over single-mode fiber.
- 1000BASE-LH: 1 Gbit/s over single-mode fiber (up to 100km). A long-distance solution.

10 Gigabit Ethernet (10 000 Mbit/s)

This is viewed as the new choice for backbone in enterprise networks. The 10 Gigabit Ethernet standard uses seven different media types for LAN, WAN and MAN (Metropolitan Area Network). It

is currently specified by a supplementary standard, IEEE 802.3ae, and will be incorporated into a future revision of the IEEE 802.3 standard.



5.2. Power over Ethernet

Power over Ethernet (PoE) is a technology that integrates power into a standard LAN infrastructure. It enables power to be provided to the network device, such as an IP phone or a network camera, using the same cable as that used for network connection. It eliminates the need for power outlets at the camera locations and enables easier application of uninterruptible power supplies (UPS) to ensure 24 hours a day, 7 days a week operation.

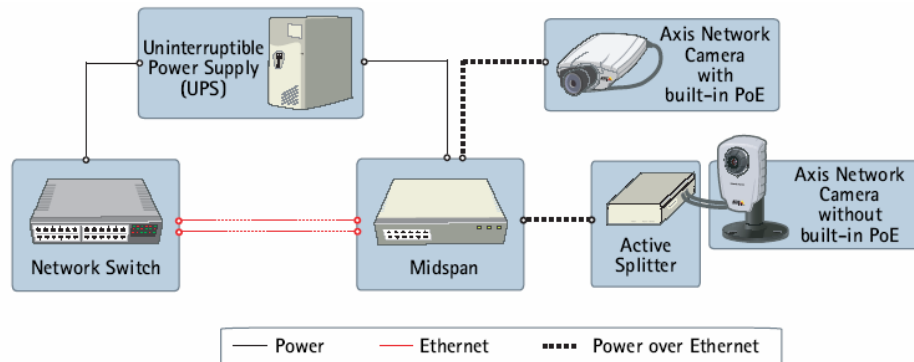
PoE technology is regulated in a standard called IEEE 802.3af and is designed in a way that does not degrade the network data communication performance or decrease the network reach. The power delivered over the LAN infrastructure is automatically activated when a compatible terminal is identified, and blocked to legacy devices that are not compatible. This feature allows users to freely and safely mix legacy and PoE-compatible devices, on their network.

The standard provides power up to 15.4W on the switch or midspan side, which translates to a maximum power consumption of 12.9W on the device/camera side – making it suitable for indoor cameras. Outdoor cameras as well as PTZ and dome cameras have a power consumption that normally exceeds this, making PoE functionality less suitable. Some manufacturers also offer non-standard proprietary products providing suitable power for these applications as well, but it should be noted that since these are non-standard products, no interoperability between different brands is possible. The 802.3af standard also provides support for so-called power classification, which allows for a negotiation of power consumption between the PoE unit and the devices. This means an intelligent switch can reserve sufficient, and not superfluous, power for the device (camera) - with the possible result that the switch could enable more PoE outputs.

Using Power over Ethernet

PoE works across standard network cabling (i.e. cat-5) to supply power directly from the data ports to which networked devices are connected. Today, most manufacturers offer network switches with built-in PoE support. If an existing network /switch structure is in place, customers can benefit from the same functionality by adding a so-called Midspan to the switch, which will add power to the network cable. All network cameras without built-in PoE can be integrated in a PoE system using an Active Splitter.

The following diagram shows how a network camera can receive power over a network cable and can continue to function even when there is a power failure.



5.3. Wireless networks

Even if wired networks are present in most buildings today, sometimes a non-wired solution holds substantial value to the user, financially as well as functionally. For example it could be useful in a classified building, where the installation of cables would not be possible without damaging the interior, or within a facility where there is a need to move the camera to new locations on a regular basis without having to pull new cables every time, like in retail. Another common use of wireless technology is to bridge two buildings or sites together without the need for expensive and complex ground works.

Wireless technology exists both for analog and network video systems – therefore going beyond the networking perimeter. There are two major categories for wireless communications:

■ Wireless LAN (also known as WLAN):

A LAN is by definition a Local Area Network, i.e. over short distances and normally indoors. Nowadays, the wireless LAN standards are well defined and devices from different vendors work well together.

■ Wireless bridges

When it is necessary to connect buildings or sites with high speed links, a point-to-point data link capable of long distances and high speeds is required. Two commonly used technologies are microwave and laser.

Wireless LAN standards

■ 802.11a

Standard using the 5GHz band providing up to ~24 Mbps actual throughput at up to 30m/100feet in outdoor environments. Limited range of products supporting it. Theoretical bandwidth is 54Mbps.

■ 802.11b

Standard providing up to ~5 Mbps actual throughput at up to 100m/300feet in outdoor environments. It uses the 2.4GHz band. Theoretical bandwidth is 11Mbps.

■ 802.11g

The most commonly used standard providing improved performance compared to 802.11b. Up to ~24Mbps actual throughput at up to 100m/300feet in outdoor environments. It uses the 2.4GHz band. Theoretical bandwidth is 54Mbps.

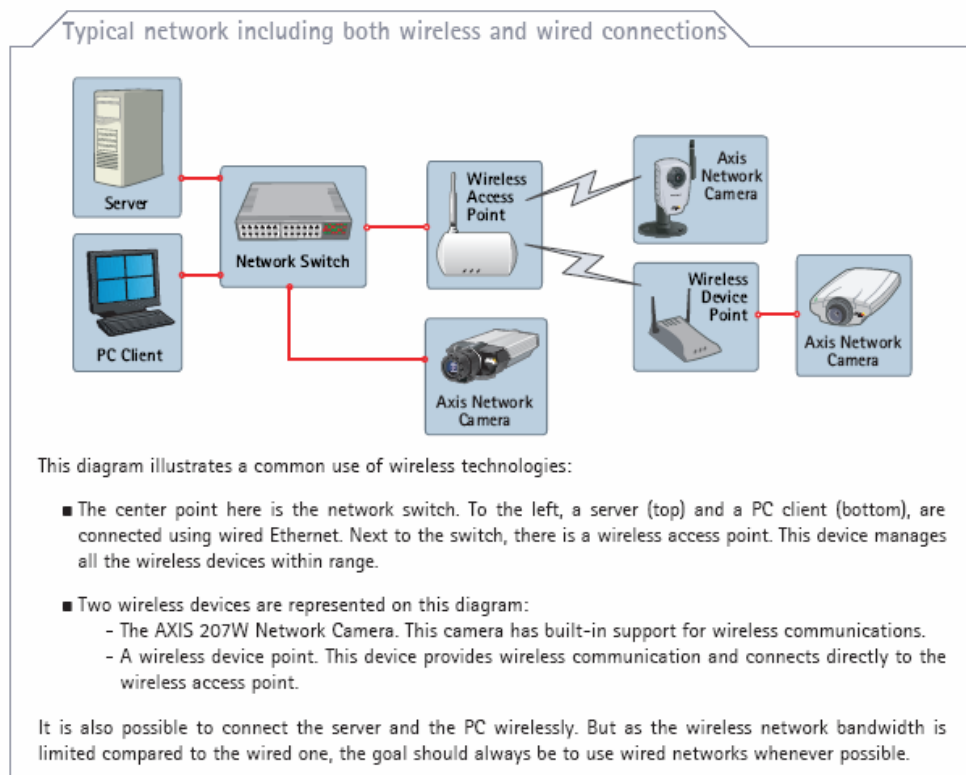
■ 802.11n

Next generation of the 802.11 Wireless LAN standard. The actual throughput will be in excess of 100Mbps.

Broadband wireless access

■ 802.16 - WiMAX

IEEE 802.16, also known as WiMAX, is a specification for fixed broadband wireless metropolitan access networks (MANs) that use a point-to-multipoint architecture. The standard defines the use of bandwidth between the licensed 10GHz and 66GHz and sub 11GHz frequency ranges. 802.16 supports very high bit rates in both uploading to and downloading from a base station up to a distance of 50km/30 miles to handle such services as VoIP (Voice over IP).



About security in wireless networks

Due to the nature of wireless communications, everyone with a wireless device present within the area covered by the network is able to participate in the network and use shared services, hence the need for security.

Please refer to section 5.5.2, page xx, for further information about security in wireless networks.

Wireless bridges

Some solutions may also use other standards than the dominating 802.11 standard, providing increased performance and much longer distances in combination with very high security. This also includes the use of other means of Radio Frequency, such as microwave links. Another common technology is optical systems such as laser links. A microwave link can provide up to 1000Mbps for distances up to 80km/130miles. For locations outside the range of all these systems, there is also the option of satellite communication. Due to the way this system operates, transmitting up to a satellite and back down to earth, the latency can be very long (up to several seconds). This makes it less suitable for functions like manual dome control and video conferencing where low latency is preferred. If larger bandwidth is required, the use of satellite systems also becomes very costly.

5.4. Data transport methods



5.4.1. IP addresses

An IP address (Internet Protocol address) is a unique number that devices use in order to identify and communicate with each other on a network utilizing the Internet Protocol standard. An IP address consists of four numbers separated by a dot ".", each number is in the range 0-255. For example, the address could be "192.36.253.80".

The IP address is further split up into a network part and a host part. The boundary between the two parts is decided by a netmask or a prefix length. A netmask of 255.255.255.0 means that the first 3 bytes will be the network address and the last byte the host address. A prefix length is a different way of providing the boundary, for example the same address as the previous example has a prefix length of 24 bits (i.e, 192.36.253.80/24).

Certain blocks of addresses have been reserved for private use:

10.0.0.0/8 (netmask 255.0.0.0)
172.16.0.0/12 (netmask 255.240.0.0)
192.168.0.0/16 (netmask 255.255.0.0)

These addresses are intended for private internets. They may not be routed out on the public Internet.

5.4.2. IPv6

IPv6, or Internet Protocol version 6, is designed as an evolutionary upgrade to the Internet Protocol and will, in fact, coexist with the older IPv4 for some time. IPv6 is designed to allow the Internet to grow steadily, both in terms of the number of hosts connected and the total amount of data traffic transmitted.

The most obvious improvement in IPv6 over the IPv4 is that IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet, providing for an unlimited (for all intents and purposes) number of networks and systems. For instance, IPv6 is intended to provide each cell phone and mobile electronic device its own address.

5.4.3. Data transport protocols for network video

The most common protocol for transmitting data on computer networks today is the TCP/IP Protocol suite. TCP/IP acts as a "carrier" for many other protocols – A good example is HTTP (Hyper Text Transfer Protocol) used to browse web pages on servers around the world using the Internet.

TCP/IP protocols and ports used for network video

Common protocols and their port numbers used for the transfer of network video include:

Protocol	Transport Protocol	Port	Common usage	Network video usage
FTP File Transfer Protocol	TCP	21	Transfer of files over the Internet/intranets	Transfer of images or video from network camera/video server to a FTP server or to an application
SMTP Send Mail Transfer Protocol	TCP	25	Protocol for sending e-mail messages	A network camera/video server can send images or alarm notifications using its built-in e-mail client
HTTP Hyper Text Transfer Protocol	TCP	80	Used to browse the web, i.e to retrieve web pages from web servers	The most common way to transfer video from a network camera/video server where the network video device essentially works as a web server making the video available for the requesting user or application server
HTTPS Hypertext Transfer Protocol over Secure Socket Layer	TCP	443	Used to access web pages securely using encryption technology	Secure transmission of video from network cameras/video servers can also be used to authenticate the sending camera using X.509 digital certificates
RTP Real Time Protocol	UDP/TCP	Not defined	RTP standardized packet format for delivering audio and video over the Internet. Often used in streaming media systems or videoconferencing	A common way of transmitting MPEG based network video Transmission can be either unicast (one to one) or multicast (one to many)
RTSP Real Time Streaming Protocol	TCP	554	Used to setup and control multimedia sessions over RTP	

The TCP/IP protocol suite's most used transport protocols are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP provides a reliable, connection-based transmission channel; it handles the process of breaking large chunks of data into smaller packets, suitable for the physical network being used, and ensures that data sent from one end is received on the other. UDP, on the other hand, is a connectionless protocol and does not guarantee the delivery of data sent, thus leaving the whole control mechanism and error-checking to the application itself.

In general TCP is used when reliable communication is preferred over transport latency. TCP's reliability through retransmission may introduce significant delays. UDP on the other hand provides no retransmissions of lost data and therefore does not introduce further delays.

5.4.4. Transmission methods for network video: Unicasting, Multicasting, and Broadcasting

There are different methods for transmitting data on a computer network:

- Unicast - the sender and the recipient communicate on a point-to-point basis. Data packets are sent addressed solely to one recipient and no other computers on the network will need to process this information.
- Multicast - communication between a single sender and multiple receivers on a network. Multicast technologies are used to reduce network traffic when many receivers want to view the same source simultaneously, by delivering a single stream of information to hundreds of recipients. The biggest difference compared with unicasting is that the video stream only needs to be sent once. Multicasting (i.e IP-Multicasting) is commonly used in conjunction with RTP transmissions.
- Broadcast - a one-to-everybody transmission. On a LAN, broadcasts are normally restricted to a specific network segment and are not in practical use for network video transmissions.

5.5. Network security



There are several ways to provide security within a wired or wireless network and between different networks and clients. Everything, from the data sent over the network to the actual use and accessibility of the network, can be controlled and secured.

5.5.1. Secure transmission

Providing secure transmission of data is like using a courier to bring a valuable and sensitive document from one person to another. When the courier arrives to the sender, he would normally be asked to prove his identity. Once this is done, the sender would decide if he is the one he claims to be, and if he can be trusted. If everything seems to be correct, the locked and sealed briefcase would be handed over to him, and he would deliver it to the receiver. At the receiver, the same identification procedure would take place, and the seal would be verified as “unbroken”. Once the courier had left, the receiver would unlock the briefcase and take out the document to read it.

A secure communication is created in the same way, and is divided into three different steps:

Authentication

This initial step is for the user or device to identify itself to the network and the remote end. This is done by providing some kind of identity to the network/system, like a username and password, an X509 (SSL) certificate, and using the 802.1x standard.

Authorization

The next step is to have this authentication authorized and accepted, that is verifying whether the device is the one it claims to be. This is done by verifying the provided identity within a database or list of correct and approved identities. Once the authorization is completed, the device is fully connected and operational in the system.

A closer look at IEEE 802.1x authentication

Pushed by the wireless community looking for stronger security methods, the 802.1x standard is among the most popular authentication methods in use today: IEEE 802.1X provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.

How it works

Clients and servers in an 802.1x network authenticate each other with the help of digital certificates provided by a Certification Authority. These are then validated by a third-party entity, such as an authentication server called a RADIUS server, one example of which is Microsoft Internet Authentication Service.

The Axis network video device presents its certificate to the network switch, which in turn forwards it to the RADIUS server. The RADIUS server validates or rejects the certificate and responds to the switch, which then allows or denies network access accordingly, on a preconfigured port.

This makes it possible to leave network sockets open and available: the access point will not connect you into the network until proper identity is provided.

Privacy

The final step is to apply the level of privacy required. This is done by encrypting the communication, which prevents others from using/reading the data. The use of encryption could provide a substantial decrease in performance, depending on the kind of implementation and encryption used.

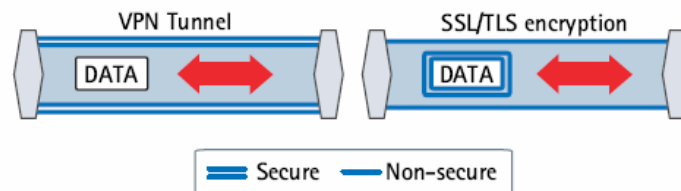
Privacy can be achieved in several ways. Two of the more commonly used methods are VPN and SSL/TLS (also known as HTTPS):

■ VPN (Virtual Private Network)

A VPN creates a secure tunnel between the points within the VPN. Only devices with the correct "key" will be able to work within the VPN. Network devices between the client and the server will not be able to access or view the data. With a VPN, different sites can be connected together over the Internet in a safe and secure way.

■ SSL/TLS

Another way to accomplish security is to apply encryption to the data itself. In this case there is no secure tunnel like with the VPN solution, but the actual data sent is secured. There are several different encryption techniques available, like SSL, WEP and WPA, the later two being used in wireless networks. When using SSL, also known as HTTPS, the device or computer will install a certificate into the unit, which can be issued locally by the user or by a third-party body such as Verisign.



5.5.2. Security in wireless networks

Due to the nature of wireless communications, everyone with a wireless device present within the area covered by the network is able to participate in the network and use shared services, hence the need for security.

WEP

WEP (Wireless Equivalent Privacy) adds RSA RC4-based encryption to the communication, and prevents people without the correct key to access the network.

The problem with WEP is that it has several flaws that make it vulnerable to attacks, therefore it is not able to provide basic levels of security. The main flaws in WEP are the static encryption key and the short initialization vector. Since it is easy to attack WEP with inexpensive off-the-shelf equipment, wireless networks should not rely on WEP for security.

WPA

WPA (WiFi Protected Access) resolves the main flaws with WEP. With WPA, the key is changed for every frame transmitted using Temporal Key Integrity Protocol (TKIP). The Initialization vector length is increased from 24 to 48 bits. WPA is considered as the base level of security for wireless networks.

For even higher security WPA2 should be used. WPA2 uses Advanced Encryption Standard (AES) instead of TKIP. AES is the best encryption available for wireless networks today. WPA2 also includes 802.1x authentication (see section about 802.1x).

5.5.3. Protecting single devices

Security also means protecting single devices against intrusions, such as unauthorized users trying to gain access to the unit, or viruses and similar unwanted items.

Access to PCs or other servers can be secured with user names and passwords, which should be at least 6 characters long (the longer the better), combining numbers and figures (mixing lower and upper cases). In the case of a PC, tools like finger scanners and smart cards can also be used to increase security and speed up the login process.

To secure a device against viruses, worms and other unwanted items, a virus scanner of good quality with up-to-date filters is recommended. This should be installed on all computers. Operating systems should be regularly updated with service packs and fixes from the manufacturer.

When connecting a LAN to the Internet, it is important to use a firewall. This serves as a gatekeeper, blocking or restricting traffic to and from the Internet. It can also be used to filter information passing the firewall or to restrict access to certain remote sites.

5.6. QoS (Quality of Service)

Nowadays, fundamentally different networks are merging into one IP network. For example, telephone and video (CCTV) networks are migrating towards IP. In these networks, you will need to control the way to share network resources to fulfill the requirements of each service. One solution is to let the network routers and switches behave differently on different kinds of services (voice, data, video) as the traffic passes through the network. This technique is called Differentiated Services (DiffServ). By using QoS, different network applications can co-exist on the same network, without consuming each other's bandwidth.

Definition

The term Quality of Service refers to a number of technologies to guarantee a certain quality to different services on the network. Quality can be, for instance, a maintained level of bandwidth, low latency, no packet losses, etc. The main benefits of a QoS-aware network can be summarized as:

- The ability to prioritize traffic and thus allow critical flows to be served before flows with lesser priority.
- Greater reliability in the network, thanks to the control of the amount of bandwidth an application may use, and thus control over bandwidth races between applications.

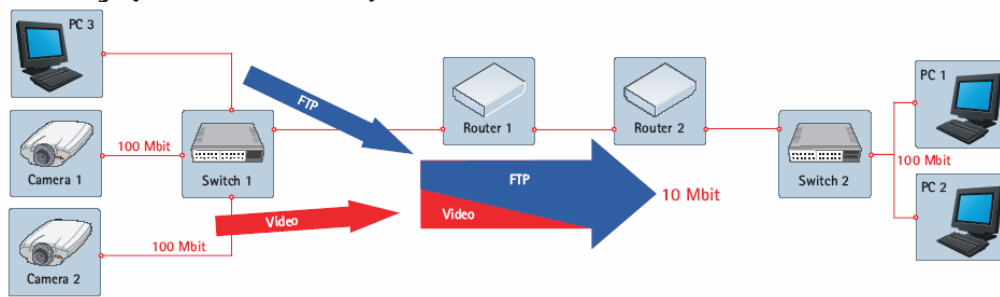
QoS and network video: requirements

To use QoS in a network with network video products, the following requirements must be met:

- All network switches and routers must include support for QoS. This is important to achieve end-to-end QoS functionality.
- The network video products must be QoS-enabled.

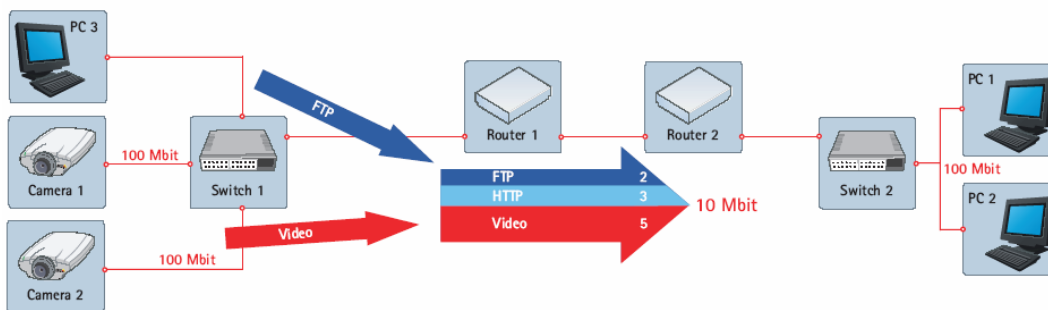
A QoS scenario

Figure 1: ordinary (non-QoS aware) network



In this example, PC1 is watching two video streams from cameras Camera 1 and Camera 2, with each camera streaming at 2.5 Mbps. Suddenly, PC2 starts a file transfer from PC3. In this scenario, the file transfer will try to use the full 10 Mbps capacity between the routers 1 and 2, whilst the video streams will try to maintain their total of 5 Mbps. The amount of bandwidth given to the surveillance system can no longer be guaranteed and the video frame rate will probably be reduced. At worst, the FTP traffic will consume all the available bandwidth.

Figure 2: QoS aware network



The router 1 has been configured to devote up to 5 Mbps of the available 10 Mbps for streaming video. FTP traffic is allowed to use 2 Mbps, and HTTP and all other traffic can use a maximum of 3 Mbps. Using this division, video streams will always have the necessary bandwidth available. File transfers are considered less important and get less bandwidth, but there will still be bandwidth available for web browsing and other traffic. Note that these maximums only apply when there is congestion on the network. If there is unused bandwidth available, this can be used by any type of traffic.

About Pan Tilt Zoom (PTZ) traffic

PTZ traffic is often regarded as critical and requires low latency to guarantee fast responses to movement requests. This is a typical case in which QoS can be used to provide the necessary guarantees. The QoS control of PTZ traffic in Axis network video products is handled by the ActiveX viewer AXIS Media Control (AMC), which is automatically installed the first time the Axis product is accessed from Microsoft Internet Explorer.

5.7. More about network technologies and devices

Hubs, switches and bridges

These devices are essentially used as connection boxes to allow several pieces of equipment to share a single Ethernet connection. Usually 5-24 devices can be connected to one hub. If more devices are used, another hub can be added. To speed up the network, you can use switched hubs that allow several data packets to be transmitted simultaneously.

Gateways and routers

Gateways and Routers are essentially packet forwarders that operate at layer 3 (i.e. the IP layer). Forwarding decisions are made based on IP addresses and IP routing tables. A gateway makes it possible to connect two networks of different technologies into one network. For example, an Ethernet network can be connected with a Token-Ring network.

NAT routers

All devices connecting directly to the Internet must have a unique public IP address. Public IP addresses are sold by Internet Service Providers (ISPs). A device called a Network Address Translator (NAT) makes it possible to connect a LAN with private addresses to the Internet by translating internal private addresses into public addresses.

Gateways

Gateways provide a convenient way to create a local network. A gateway works as a combined router, switch and NAT and is available from many manufacturers.

DHCP servers

It takes time to manage the IP addresses for large numbers of devices on a network. To reduce this administration time and keep the number of IP addresses to a minimum, a DHCP server can be used. This type of server automatically issues network devices with IP addresses when they connect to the network.

Domain Name Servers

In larger networks a Domain Name Server (DNS) is included. This is literally a 'name' server. It associates and remembers given names to corresponding IP addresses. For example, a network camera monitoring a door is more easily remembered and accessed by the word 'door' than it is by its IP address, such as 192.36.253.80.

Firewall

A firewall is designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. For example, using firewalls, one can make sure that video terminals are able to access the cameras while communication from other computers with the cameras will be blocked.

DDNS and dynamic IP addresses

Dynamic DNS is a method of keeping a domain name linked to a changing IP address as not all computers use static IP addresses. Typically, when a user connects to the Internet, the user's ISP assigns an unused IP address from a pool of IP addresses, and this address is used only for the duration of that specific connection. This method of dynamically assigning addresses extends the usable pool of available IP addresses. A dynamic DNS service provider uses a special program that runs on the user's computer, contacting the DNS service each time the IP address provided by the ISP changes and subsequently updating the DNS database to reflect the change in IP address. In this way, even though a domain name's IP address will change often, other users do not have to know the changed IP address in order to connect with the other computer.

In a network video application, a camera watching an entrance door is more easily remembered as "door.camera.axis.com" for instance. But when using DHCP, the camera's IP address may change over time. So a static mapping between "door.camera.axis.com" into the camera's IP address "192.36.253.80" may not be valid after a while. DDNS provides the solution: every time the camera changes IP address, it will contact the DNS server and update the mapping.

"Hi Mr. DNS server, I am door.camera.axis.com and I just got a new IP address 192.168.10.33. Please update my mapping."



SNMP

SNMP (Simple Network Management Protocol) is a set of protocols for managing complex networks – and for remotely controlling and managing network-attached devices.

IPSec

"IP Security" (IPSec) consists of a set of protocols to support secure exchange of packets at the IP layer. IPSec has been deployed widely to implement Virtual Private Networks (VPNs).

UPnP

Universal Plug and Play (UPnP) is a networking architecture that provides compatibility among networking equipment, software and peripherals of the 400+ vendors that are part of the Universal Plug and Play Forum. UPnP works with wired or wireless networks and can be supported on any operating system. Simply, it allow devices to connect seamlessly and to simplify the implementation of networks in the home and corporate environments.

UPnP is a common way for instance to discover network cameras. When you connect a camera for the first time, it may get an address from the DHCP server which you have no idea of what this address is. With UPnP you can search for camera devices and see them pop up.

For further information about network technologies and devices, please visit www.axis.com/products/video/about_networkvideo/