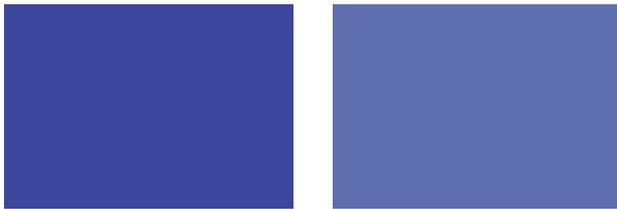
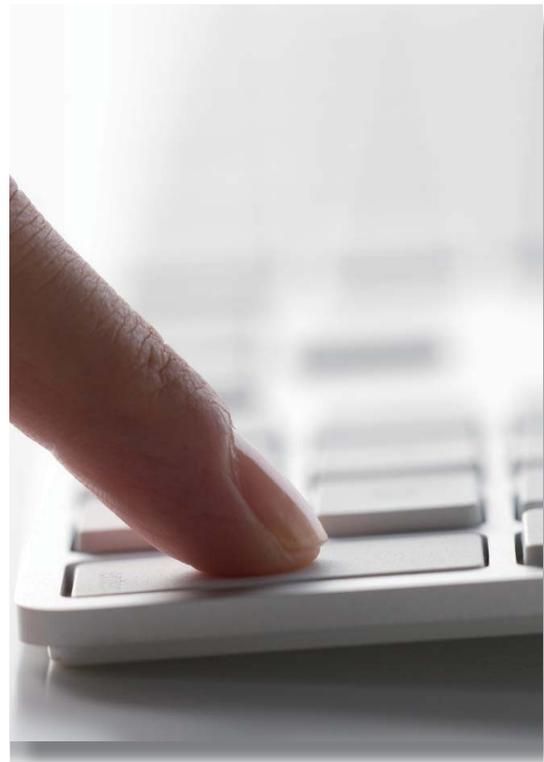


How do Ethernet Switches Affect the Overall Network?

Do not underestimate networking peripherals!



When building a digitalized surveillance system, not only do the selection and setup of cameras, network video recorders (NVR), digital video recorders (DVR), switches and/or hubs play an important role of the entire system, even routers would also be taken into consideration as well. There are a diverse range of different network peripherals out there to choose from, but how do you use them efficiently? Read on to find out how Alex (a virtual user) is beneficial from EtherWAN's offers to build his IP security solutions.



Technology

Contemporary control and management systems, such as building automation or access control and surveillances, are changing the way they connect. Devices such as remote controllers, badge readers and CCTV cameras are now connecting via Ethernet and IP network connections rather than analog or slower serial connections. This migration of technologies requires different networking knowledge in order to boost the IP surveillance solution value. As long as users are able to wisely build the network topology, efficiently plan the bandwidth control and well utilize the redundancy management offered by layer 2 managed switches, the total cost of ownership should be control in an affordable range. Ultimately migration to IP security is a reachable goal.

Challenge

Ever since Alex's first hands-on experience with a project on digital network system integration, Alex has been enthusiastically studying all types of networking, digitalized IT products and peripherals, including digital surveillance, access control and burglar alarm system et cetera. Through detailed observation and understanding, Alex discovered a few interesting facts that were worth looking at.

First, no matter in which types of digital security systems' diagram layout, devices such as Managed Switches, Ethernet Switches, Ethernet Media Converters or SFP Switches, Combo Switches and SNMP Switches can be seen. Although they look similar, they were labeled with different names that can be seen around the LAN/WAN networks and internet clouds in the network diagram. Next, a similar network interface device was also spotted, but labeled with Access Router or Load Balance Router, each specified for different uses.

What made Alex more curious was the fact that he thought these devices were merely networking hubs, but why are there so many different technical terms and usages of them?

Alex discovered that in the world of IT network management, factors such as different information, data stream, data path, network subnets and transmission methods will ultimately influence the types of network transmission devices required to use. In accordance with the devices required for security systems, the network topology/environment, data flow, bandwidth requirement, transmission layout and network security are the major factors for determining which network device to use.

In the mean time, Alex's supervisor handed over several boxes to him and said, "We are planning to introduce some networking products into our digital surveillance

Quick Questions

- How to digitalize existing analog cameras and access control into network format?
- How to convert video and data signal?
- How do we define if the network is an expansion of the existing, or a stand-alone network?
- How to plan network bandwidth?
- How to implement networking devices?

and access control systems. There are some different types of networking products here, using our company's product, setup a show room with a network that can connect to the existing analog cameras, DVRs, NVRs, workstation system, as well as providing one computer each for all the six departments in which the PCs will also be part of this network. In addition, video surveillance monitoring and control functions must be provided to our south branch office, but this connection must not interfere our company's existing network bandwidth and information security, do not forget to interconnect the access control reader to the network as well."

The items in the boxes contain: 24-port 10/100/1000 Base SFP Switch-1, 8-port Industrial 10/100 Base TX PoE Switch-3, H.264 video server-10 (free management software included), 10/100 Base Media Converter-8, RS-232/422 TCP/IP converter.

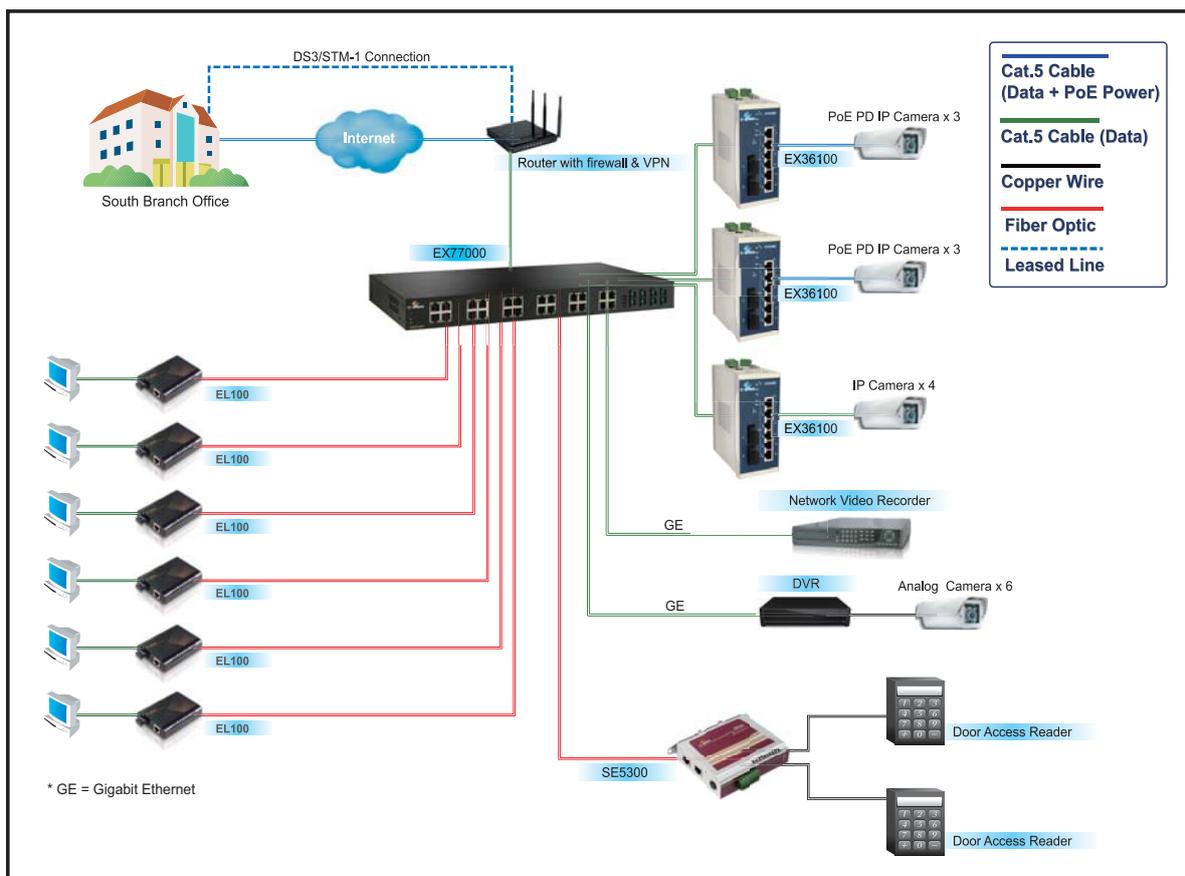
Solution

Assuming that the H.264 network camera used by Alex is 1.3 Megapixels (1280x1024), we will use the following calculation and arrangement to determine the bandwidth required for the video surveillance system. If users at the head office are viewing the cameras at 15 frames per second (FPS) with the video quality set to highest, the bandwidth required is approximately 2.09Mbps (value for reference only, IP Cameras from different vendors may differ); while south branch users are viewing the cameras at 10FPS with the video quality set to normal, the bandwidth required is approximately 0.98Mbps (value for reference only, IP Cameras from different vendors may differ). If users at south branch connect to this network via a 10Mbps ADSL connection, approximately 10 video streams can be viewed, if more than 10 streams are opened, bandwidth would be insufficient and the video cannot be viewed in a swiftly manner. Hence, it is recommended that the maximum number of simultaneous connections that the IP Camera can provide should be limited. Another option is to install leased lines (DS3/STM-1) between the head and branch office to overcome the problem of insufficient bandwidth.

Currently, Alex will need the 24-port 10/100/1000 Base SFP network switch to interconnect the computers from the six departments, network cameras and access control system together. This switch will be the core switch of the entire network, it will also be the entry point to the outside network (Internet and south branch office). At this point, we will assume that this switch is EtherWAN's EX77000 series of Hardened Ethernet Switches, and the three 8-port industrial grade 10/100 Base-TX switches are based on EtherWAN's EX36100 series of switches.

Network Bandwidth and Setup the Stand-alone Network

Before planning, we are going to calculate the largest bandwidth requirement that the head office needs. The largest bandwidth utilization for NVR is around 125.4Mbps (10 units * 2.09Mbps * 6 departments), while the largest bandwidth utilization for DVR is around 75.24Mbps (6 units * 2.09Mbps * 6 departments). According to the bandwidth estimate, we can use the following distribution to ensure that the network bandwidth is utilized efficiently; connect three network cameras each on the first and second EX36100s, while the remaining four cameras can be connected to the third EX36100 (refer to figure 1), the NVR and DVR can be connected to EX77000's two gigabit ports with the DVR connected to the existing 6 analog cameras, so that their signal can be digitalized into network format. This setup will ensure that both the digital and analog systems will have sufficient bandwidth for smooth video operation and data transmission.



▲ The network layout of the recommended solution for Alex

However, let's look at another type of setup where bandwidth utilization is not maximized efficiently. If the first and second EX36100 are connected with four cameras each, and the remaining two is connected to the third EX36100, this time, instead of connecting the NVR and DVR to the Gigabit ports of EX77000, they are connected to the second and third EX36100 respectively with the DVR connected to the 6 analog cameras. NVR's bandwidth consumption will exceed the switch's maximum 100Mbps port speed; total bandwidth will be 100.32Mbps (2 cameras * 2.09Mbps * 6 departments + 75.24Mbps from DVR). Therefore, it is best to distribute the 10 network cameras evenly on three EX36100s as advised earlier.

Product Selections

1 EX77000

Managed Hardened 24-port 10/100BASE and 4 Gigabit ports Ethernet Switch with SFP



2 EX36100

Web-Smart Industrial 8-port 10/100BASE-TX High Power PoE Ethernet Switch



3 EL100

10/100BASE-TX to 100BASE-FX Media Converter



4 SE5300

Industrial 2/4 ports Serial Device Server



Access Control System Ethernet Signal Conversion

If the access control system uses a RS-232/422 serial interface, Alex can use the 2-port industrial grade serial device server (SE5302 from EtherWAN for example) to convert the serial signal to Ethernet format that can be transferred onto the network. If the location of the access control system is over 100 meters, a fiber port can be substituted on SE5302's interface, which can then be connected to the fiber port on EX77000.

Result

The simulated scenario was to study what problems most security installers and system integrators face when designing and creating a network that requires integration of the existing CCTV surveillance and door security system, as well as finding a solution for them.

Efficient Bandwidth Control

First, with regards to bandwidth and video signal quality, EtherWAN had an unbiased view of which one is more important than the other, whereas it is more important for the security installers and system integrators to identify the actual bandwidth that the IP and CCTV cameras will consume, the amount of available bandwidth that the network can offer, so that a reasonable balance between video quality and network performance can be achieved.

With regards to selecting the type of connection to use, EtherWAN's suggestion on implementing fiber connection or Asynchronous Transfer Mode (ATM) based connection such as DS-3/STM-1 are also good alternatives for increasing the amount of available bandwidth in the network. However, due to the high cost, these types of transmission infrastructure are mostly used in public construction.

In general, surveillance systems are more commonly adopted in enterprise networks, therefore, there are some minor differences in the use of network devices as compared with ATM based networks. Although both types of networks employ managed switches, access routers and hubs, they are still differences in the actual application performance. For example, the configurations for management functions such as Quality of Server (QoS) and Virtual Local Area Network (VLAN) will be different.

Network Management & Access Control

Implementation of surveillance system in enterprise networks usually consists of management switches with SNMP function, hubs and routers, as well as VPN function running on the Internet Service Provider (ISP) link for local and remote surveillance control. This is usually operated in 2 to 10Mbps link speeds, which is enough for satisfying the basic requirements of video surveillance.

In addition, with regards to the distance between network devices, data flow, and the different methods of connecting the network devices, EtherWAN has made a good explanation of how these factors that seems unimportant will affect the overall bandwidth utilization of the network. As well as pointing out the advantages and disadvantages of each different setup.

Extended Ethernet Distance

The problems that system installers and system integrators face for camera control and network data conversion, EtherWAN has provided a fulfilling solution by using a series of their Media Converters, Serial Device Converters and Ethernet Extenders to overcome the data conversion problems. On top of that, they have also covered the use of firewalls, which is another important area for protecting video in security systems.

EtherWAN has responded to most of the problems encountered by security installers and system integrators, and come up with a targeting solution. But an important reminder; network management does not deal with data flow and bandwidth control only, security installers and system integrators must also manage the quality of network bandwidth in order to truly attain a smooth transmission of video. Network bandwidth “quality” management is extremely crucial, but is often neglected by security installers and system integrators. When setting up network devices in a security surveillance system, designers often do not apply or follow the general guidelines of enterprise networks’ design.

As a result, the data for video, door security and alarm system are all transmitted on the same network link. When all the systems and services are activated, or any one of the system activates, bandwidth would be insufficient if the network is operating at the highest peak-time of the day. Hence, it is important for switches and routers to support the Quality of Service (QoS) feature, as there is a big difference in video performance compared to using network devices without QoS support. This is why EtherWAN highly recommends using network devices with QoS function.