CCTV Surveillance System Network Design Guide

First Edition, March 2012

www.moxa.com/product

CCTV Surveillance System Network Design Guide

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Moxa Americas

Toll-free:	1-888-669-2872
Tel:	+1-714-528-6777
Fax:	+1-714-528-6778

Moxa Europe

Tel:	+49-89-3 70 03 99-0
Fax:	+49-89-3 70 03 99-99

Moxa China (Shanghai office)

Toll-free:	800-820-5036
Tel:	+86-21-5258-9955
Fax:	+86-21-5258-5505

Moxa Asia-Pacific

Tel:	+886-2-8919-1230
Fax:	+886-2-8919-1231

Table of Contents

Preface and Introduction

Purpose

This document will focus on the network design of CCTV video surveillance systems, specifically by highlighting the key considerations and recommended network design of a CCTV video surveillance system. This information is intended for system integrators and network solution providers.

Approach

In this paper, we will first describe a typical customer scenario for an IP-based video surveillance system in an airport facility. We will complete a network design for this hypothetical system, and use this case study to illustrate the key network considerations and design concepts involved in creating this network.

Additional Notes

- An IP video surveillance system includes several components, including cameras, encoders/decoders, data storage, video management software, and network equipment. This document focuses on the network itself, so component descriptions, video or storage product selection, storage design, video management software planning, video related technology, etc. are beyond the scope of this document.
- The reader should possess a basic understanding of networking basics, e.g. Ethernet, LAN, switching and routing technology, etc.
- The specific case study in this document is fictional; however, it does include many requirements and details inspired by actual customers. Design practices adopted in this document are the product of Moxa's experience acquired from supporting similar projects.

A Typical CCTV Network Project

There really are no fixed rules or "one size fits all" solutions when it comes to network design. However when faced with complex network design, understanding the key network design considerations will help you identify the most important components which you will need to focus on, in order to tackle the complexity of the network and design a solution that will meet those key design considerations.

In this chapter we'll first describe a sample customer case, which will be used as an example of how to approach IP network design. Then, a proposed network design is presented. Different network considerations are raised and explained in detail.

Customer background information

- Acme International Airport (AIA) is an international airport operated by a Acme, Inc.
- A video surveillance system consisting of 810 analog cameras was built 3 years ago to provide security monitoring and assist with passenger services. The cameras are installed at 6 airline terminals and one administration building.
- One Operations Control Center (OCC) is located in the administration building, which manages the video surveillance system centrally.
- To improve management efficiency and reduce the high maintenance cost of the existing system, Acme plans to build an IP network.

Project requirements

- The project focuses on designing a new IP network for the video surveillance system.
- The IP network must be very reliable, providing sufficient bandwidth and redundancy. Network recovery time must be below 50ms should there be any network device failures or broken links.
- The video feed captured by the analog cameras must be digitized and compressed before being transmitted on the network.
- The digitized videos shall be archived in a central storage server, located at the OCC. Videos are archived 24 hours a day, 365 days a year.
- Acme anticipates that network bandwidth utilization will grow by 30% in the next 3 years. The network design should take into considerations and accommodate this growth rate.

Terminal sites

- Two workstations (with required software) are installed at each site. Every workstation can simultaneously monitor monitor up to 16 live video streams captured from any local cameras. The video format is 4CIF (D1), H.264, 30 fps (frames per second).
- At each site, one workstation is installed to simultaneously play backup to 16 archived videos
- One management server is installed at each site to manage the site network
- All captured videos shall be sent to OCC for storage; the video format is 4CIF (D1), H.264, 30 fps

OCC

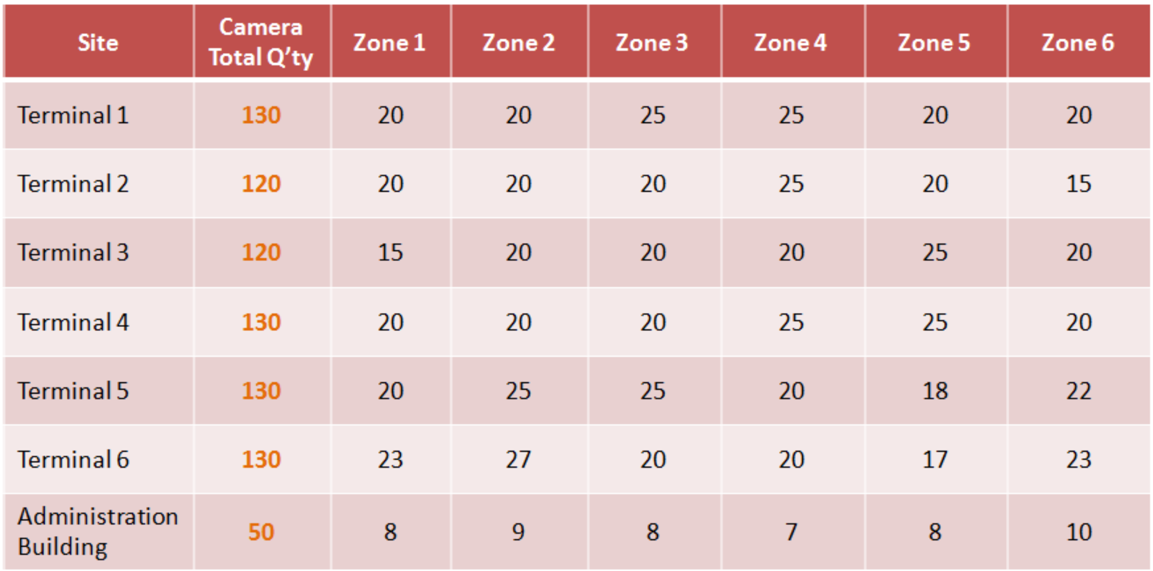
- One video archive server is set up to store video streams received from the administration building and all terminals
- One management server is installed to manage the entire network
- Two workstations (with required software) are deployed. Each workstation can simultaneously monitor up to 16 live video streams captured from any camera in the administration building. The video format is 4CIF (D1), H.264, 30 fps.
- Five workstations (with required software) are set up; each can simultaneously play back up to 16 archived videos or monitor up to 16 real-time feeds from cameras

Video cameras

- The company has decided to use a video server which supports one video input and one video stream (H.264). Every analog camera shall be directly connected to one video server for video digitization and compression.
- The consumed bandwidth for this video feed (D1 format, H.264 compression, 30 fps) is around 4 Mbps
- To meet monitoring requirements and optimize operational efficiency, analog cameras at each site are grouped into “zones”. The cameras in each “zone” can be connected as “clusters” based on their physical location. There are 4 to 5 cameras in an average cluster. For each “zone” with 20 cameras, there are approximately 4 to 5 clusters.

The following table shows the number of analog cameras in total and in each “zone” at each site.

Figure 2-1



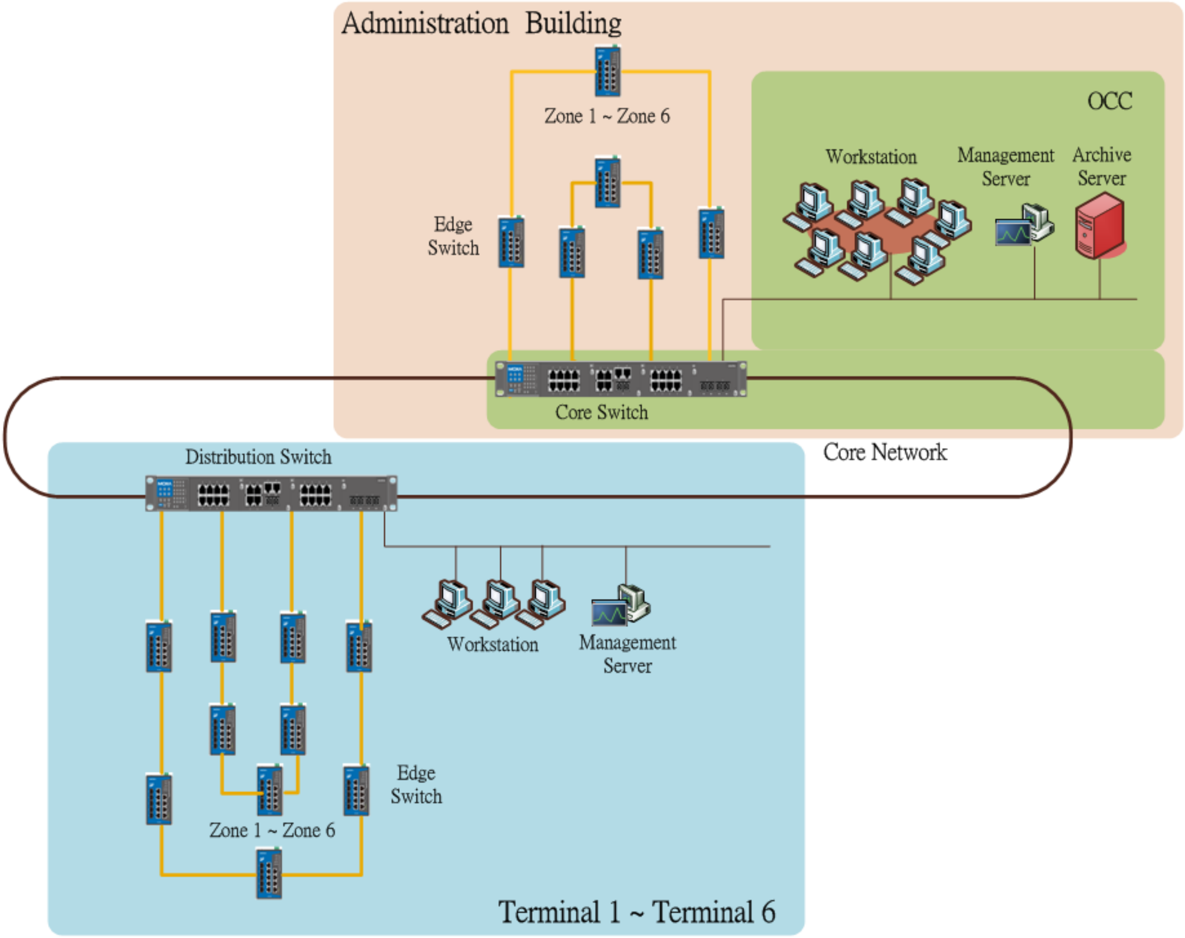
Site	Camera Total Q’ty	Zone 1	Zone 2	Zone 3	Zone 4	Zone 5	Zone 6
Terminal 1	130	20	20	25	25	20	20
Terminal 2	120	20	20	20	25	20	15
Terminal 3	120	15	20	20	20	25	20
Terminal 4	130	20	20	20	25	25	20
Terminal 5	130	20	25	25	20	18	22
Terminal 6	130	23	27	20	20	17	23
Administration Building	50	8	9	8	7	8	10

Proposed Network Design

The proposed network design is illustrated in Figure 2-2.

Key design considerations are described in the following section.

Figure 2-2



Design Considerations

Network Requirements

A good network is a network that fulfills user's requirements and functions reliably. Good networks do not appear by chance; the first and most important step to a good network design is collecting and analyzing customer's network requirements.

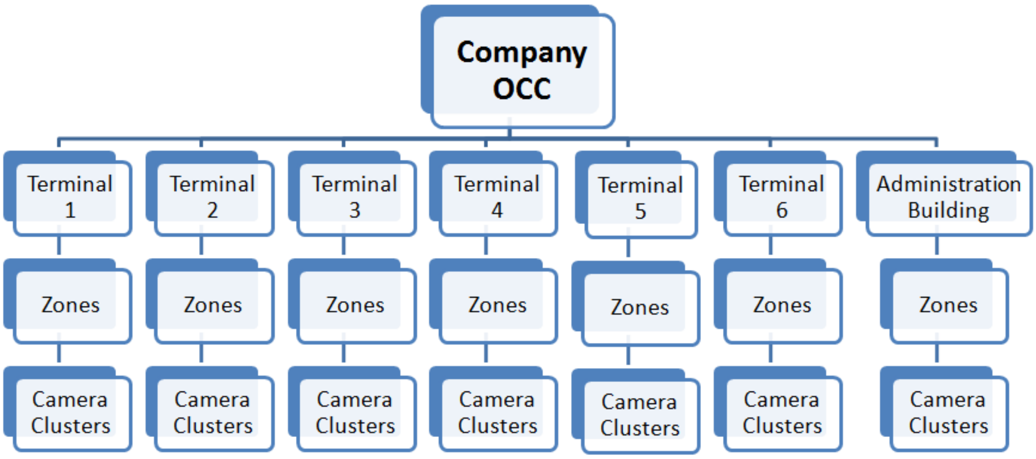
Users generally do not consider "requirements" from an underlying technical, systems, or network design perspective. Instead, users' "requirements" are primarily oriented around business goals, application functionality, accessing applications efficiently, and experiencing minimal interruptions when there is a system failure. It is the network designer's responsibility to understand and convert these broad, business-level requirements to specific network requirements.

Network requirements should be clearly communicated and well defined before a network design starts, though in some cases a network designer needs to clarify additional details along network design process.

Network requirements are also the benchmark to measure the success of the network design against.

In our sample case, we can summarize the key network technical requirements as follows:

- An IP network which connects OCC (inside Administration Building), all 7 sites (6 Terminals and 1 Administration Building) and CCTV cameras spreading over the 7 sites. With a clear understanding of the relationship among cameras, video zones, terminal and administration building, a structural view can be drawn as shown in Figure 2-3.
  Figure 2-3



- Video live viewing, archiving, archive playback functions are supported at sites (Terminals and Administration Building). The network must have sufficient network bandwidth, and plan for future network growth (30%).
- Network recovery time <= 50ms

Network Hierarchy

Business requirements are evolving, and so is the supporting network. To cope with changes effectively, the network must be scalable. A flat or collapsed network may appear simple, but it is difficult to scale and manage.

Depending on their roles and physical locations, network devices can be divided into "groups" which share similar networking characteristics. The "groups" are the building blocks of a network. Within the group, networking services like switching, routing, redundancy, security, traffic prioritization, etc. can be planned and deployed accordingly.

This hierarchical or modular approach provides several benefits:

- **Availability**
  - Reduces failure domains
  - Enhances redundancy
- **Manageability**
  - The network can be configured by group
  - Easier troubleshooting
  - Minimum impact to entire network from individual changes
  - Effective policy implementation, e.g. security, traffic prioritization
- **Scalability**
  - Easier to replicate, change and expand

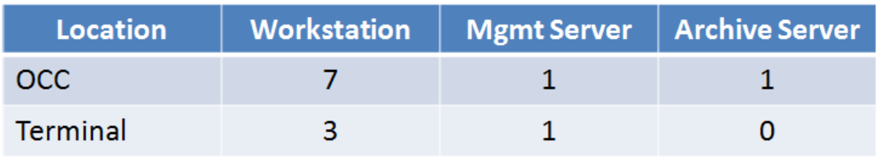
A three-layered network architecture is commonly used and has proven to be effective. The three layers are:

- **Core Layer**
  This layer provides very high speed transport to distribution layers and ensures reliable delivery of data packets. It is the backbone of the network.
- **Distribution Layer**
  This layer provides transport between access and core layers. More network transmission control is implemented at this layer, like VLAN, filtering. Redundancy and routing are implemented too.
- **Access (Edge) Layer**
  End nodes such as network devices and workstations are connected to this layer. Switching functions are implemented along with administrative policy, such as security, traffic prioritization.

In the case of AIA, the entire network should be able to transport data traffic among cameras, workstations and servers. (CCTV camera quantities and locations are listed in Figure 2-1.) These cameras capture video and send video data over the network for viewing and archiving.

The location and quantity of workstations and servers are listed below.

Figure 2-4



Location	Workstation	Mgmt Server	Archive Server
OCC	7	1	1
Terminal	3	1	0

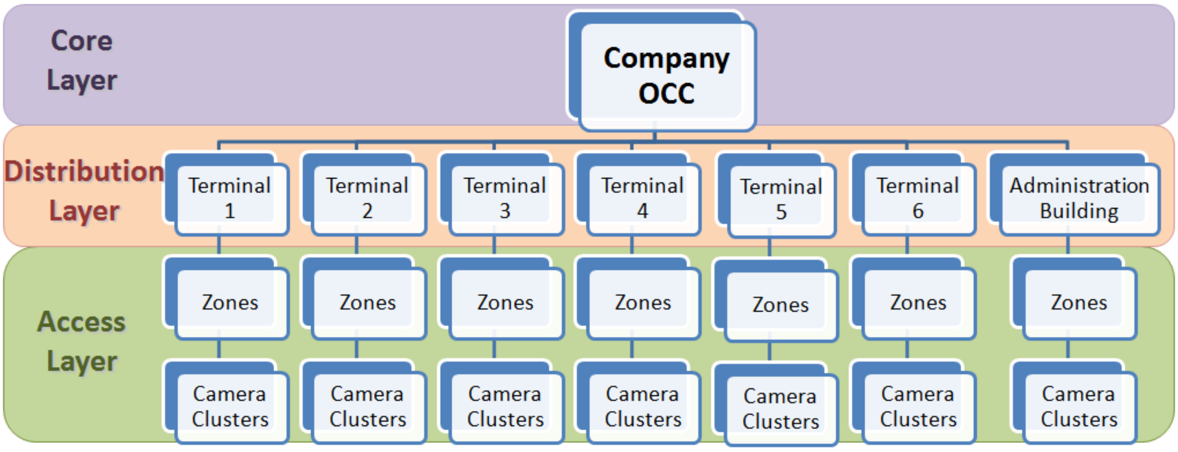
Consistent with network hierarchy best practices, we will divide AIA’s network into 3 layers: Access, Distribution and Core Layer. The location of each AIA network element in this three-layer structure is illustrated in Figure 2-5

Access Layer: The layer provides network access to all cameras and transports video streams to Distribution Layer.

Distribution Layer: This layer connects the Access Layer and Core Layer and provides network access to workstations/servers at Terminals.

Core Layer: This layer provides network access to workstations/servers installed at OCC, transporting data traffic coming from or going to the Distribution Layer.

Figure 2-5



Network Topology

There are different topologies to choose from when connecting devices together to form a network. No matter what topology you opt for, the most important consideration is how to achieve high network availability. A highly available network minimizes the impact to business applications from a single point of failure in the network, regardless of whether the failure is caused by a link, component in a network device or network device itself.

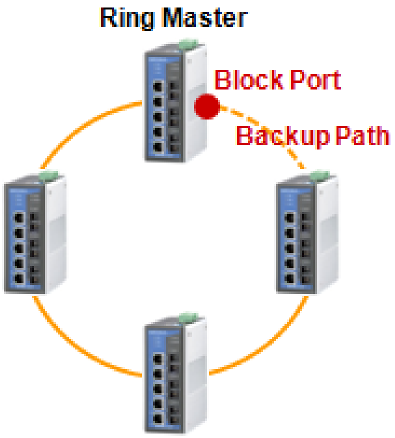
To improve network availability, normally additional links or network devices are introduced to create redundancy. In an Ethernet layer 2 network, redundant links sometimes cause loops which results in a serious downgrade to network performance, or even a halt to network operations in the worst cases.

There are IEEE standard Ethernet protocols that deal specifically with redundancy. IEEE 802.1D STP (Spanning Tree Protocol) is defined to create a loop-free network and use redundant links as backup data path whenever a primary path is not available. It can be implemented on many different topologies and is widely deployed in many systems. STP’s network recovery time ranges between 30 to 60 seconds, however, which is a limitation in many industrial applications. IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) is an updated version of STP. Though the protocol greatly improves network recovery time, it still may take up to several seconds to converge when there is a network link status change.

To provide network redundancy solution to many industrial applications which require sub-second network recovery time, some industrial Ethernet switch manufacturers have developed proprietary protocols, mostly using ring topology. These proprietary protocols can deliver far faster network convergence than STP or even RSTP

For example, Moxa’s proprietary ring topology is Moxa Turbo Ring, a proprietary self-healing technology that enables fast fault recovery of under 20 ms (at a full load of 250 switches). It is built on a physically looped topology, ring. In Turbo Ring (see Figure 2-5), a Master switch is either manually assigned or automatically detected. The master switch disables a port on the ring, making the ring logically a bus topology. The redundant link connecting to the blocked port serves as backup path; it does not transport data. When there is a link or device failure in the ring, the backup path becomes available again. The network recovery process takes less than 20ms for a network with 250 devices; excellent performance that meets industrial requirements.

Figure 2-6



To further enhance network availability, Moxa Turbo Ring technology supports multi-ring topology. There are three topology options: Ring Coupling, Dual-Ring, and Dual Homing (Figure 2-7 to 2-9). A customer can choose the best fit option based on specific network redundancy requirements and deployment or cabling costs.

Figure 2-7

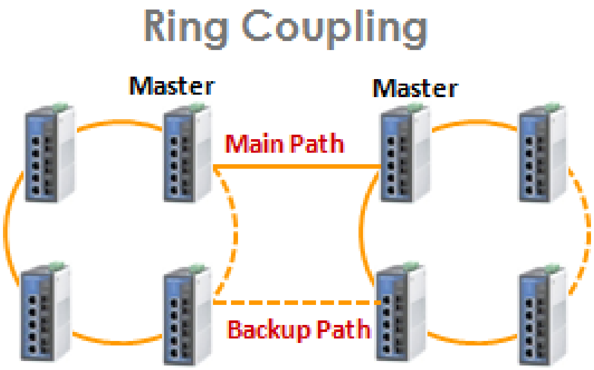


Figure 2-8

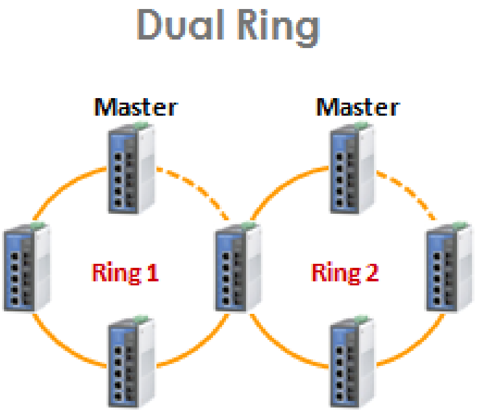
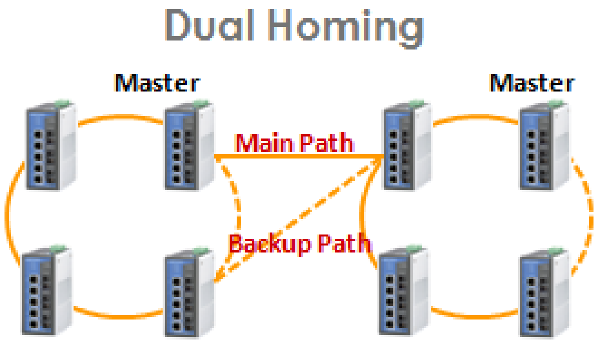
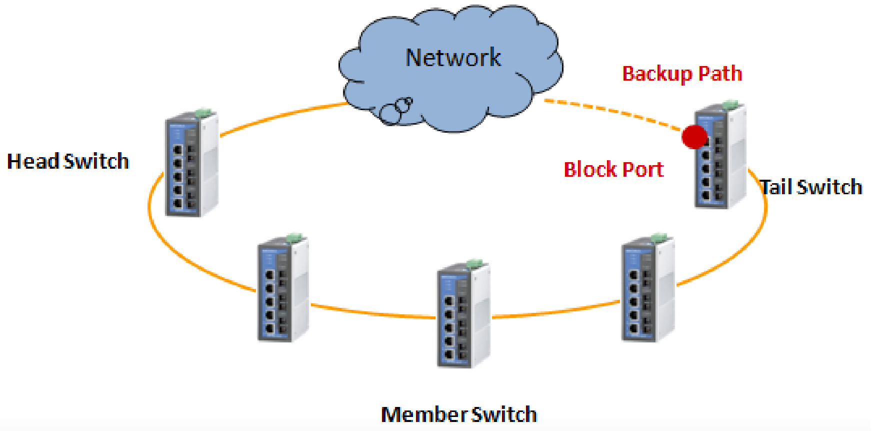


Figure 2-9



Moxa's Turbo Chain is another innovative breakthrough that allows the creation of multiple redundant networks beyond the current limitations of redundant ring technology. Turbo Chain is easy to configure by linking two user-configured end ports within the same network segment. Turbo Chain easily connects and extends existing redundant networks by enabling high network availability with its self-healing capability (recovery time < 20 ms). In addition, Turbo Chain supports standard IEEE 802.1w/D RSTP and STP protocols.

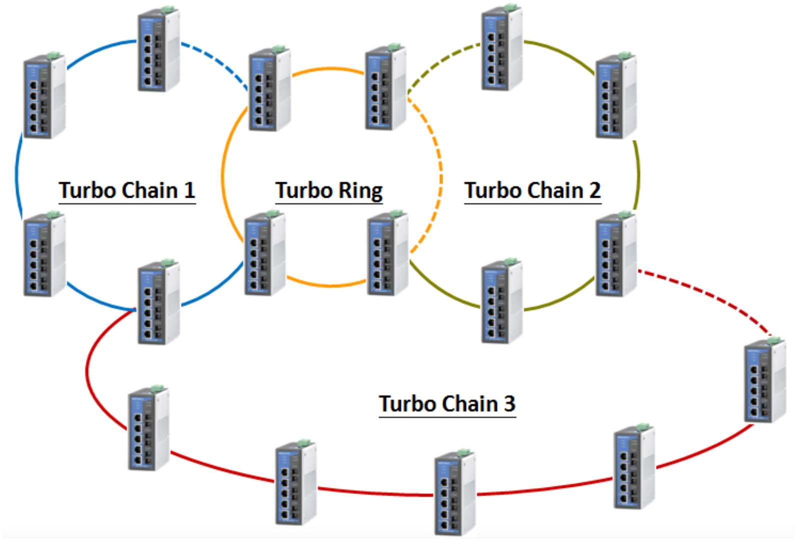
Figure 2-10



Though Turbo Chain's network recovery time is <20ms, the overall network recovery time could possibly be much higher once the recovery time of the "attached-to" network (the "Network" in Figure 2-10) is factored in. For example, if the "network" uses STP redundancy protocol, the overall network recovery time may take up to 60 seconds in some cases. In this case the limitation and bottleneck is occurring in the STP portion of the network, not Turbo Chain.

The best results are achieved by hooking up Turbo Chains to networks that also possess fast recover time, such as Turbo Rings. When combining Turbo Ring and Turbo Chain together, say Turbo Ring in the core network and Turbo Chain in the distribution or access network, the network recovery time will be less than 20ms. The combined technology provides the greatest flexibility in designing a highly redundant network and best network performance.

Figure 2-11



Because AIA requires very strict network recovery time of less than 50ms, we propose Moxa Turbo Ring and Turbo Chain technology to fulfill the requirement.

For the core layer, one core switch is planned to provide network access to network resources at the OCC, the archive server, the network management server, and workstations (Figure 2-4).

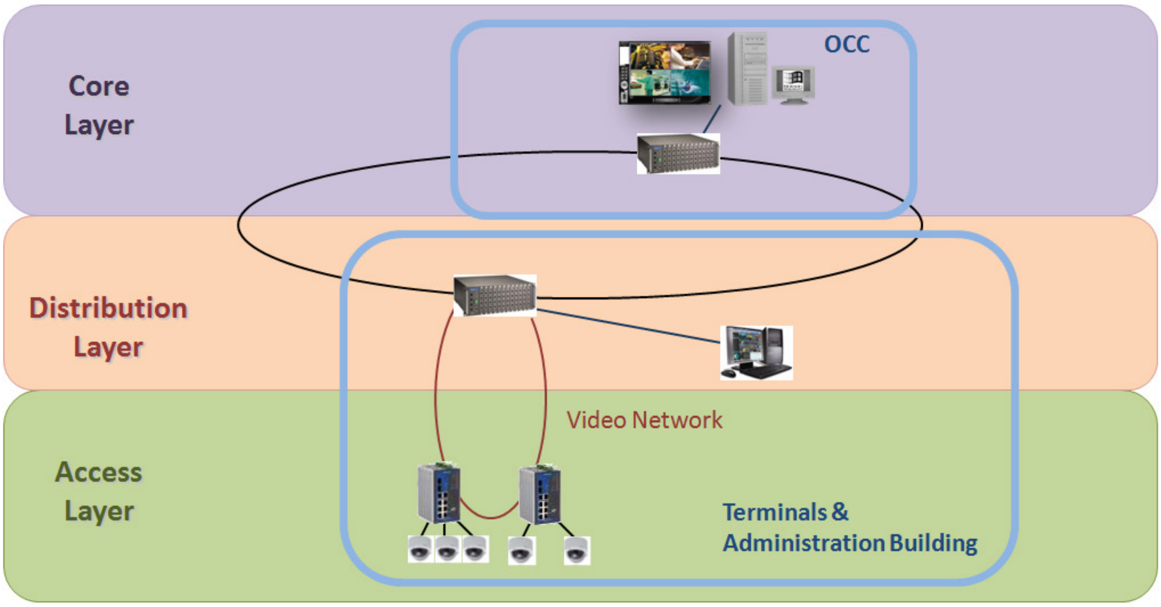
In the distribution layer, one distribution switch is planned to provide access to network resources stationed at each terminal. Network resources include the network management server and workstations (Figure 2-4). Twelve distribution switches are used in total.

The core switch at OCC and the distribution switch at each terminal are connected together in such a way as to form a Turbo Ring.

For the access layer, at each terminal, the cameras are connected to edge switches. All switches belonging to the same zone create a Turbo Chain, whose Head attaches to the first distribution switch and Tail attaches to the second distribution switch in the Terminal. For cameras whose vantage points are overlapping, it is ideal to connect them to separate access-layer switches. This creates system redundancy

Figure 2-12 is the simplified view of the network chart according to the layered hierarchy and Figure 2-2 is the detailed view.

Figure 2-12



Overall, the proposed network topology addresses the three most important requirements: network availability, flexibility and cost.

Bandwidth

The demand for video quality is a key driver of the network bandwidth consumed by a video surveillance system. The higher the video quality, the more bandwidth and data storage required.

A video is basically a stream of still images or frames. The quality of each image is closely related to its resolution. The frame rate is the number of frames taken in a specific time span. Higher resolution and frame rate increase required network bandwidth and storage space.

To save space and increase transmission efficiency, a video normally is compressed before being transported on a network. Compression efficiency varies greatly depending on the selected compression technology. Some of the most used digital video formats in IP video surveillance systems are:

- Motion JPEG
- MP-4
- H.264

Video streams using MPEG-4/H.264 compression are sensitive to packet loss and latency. Adequate network bandwidth should be prepared to prevent packet loss and latency in the first place. When planning to provide network bandwidth, we need to consider not just the normal traffic flow, but also any additional data traffic triggered by a network failures (when the redundant path is activated), and estimated growth rate.

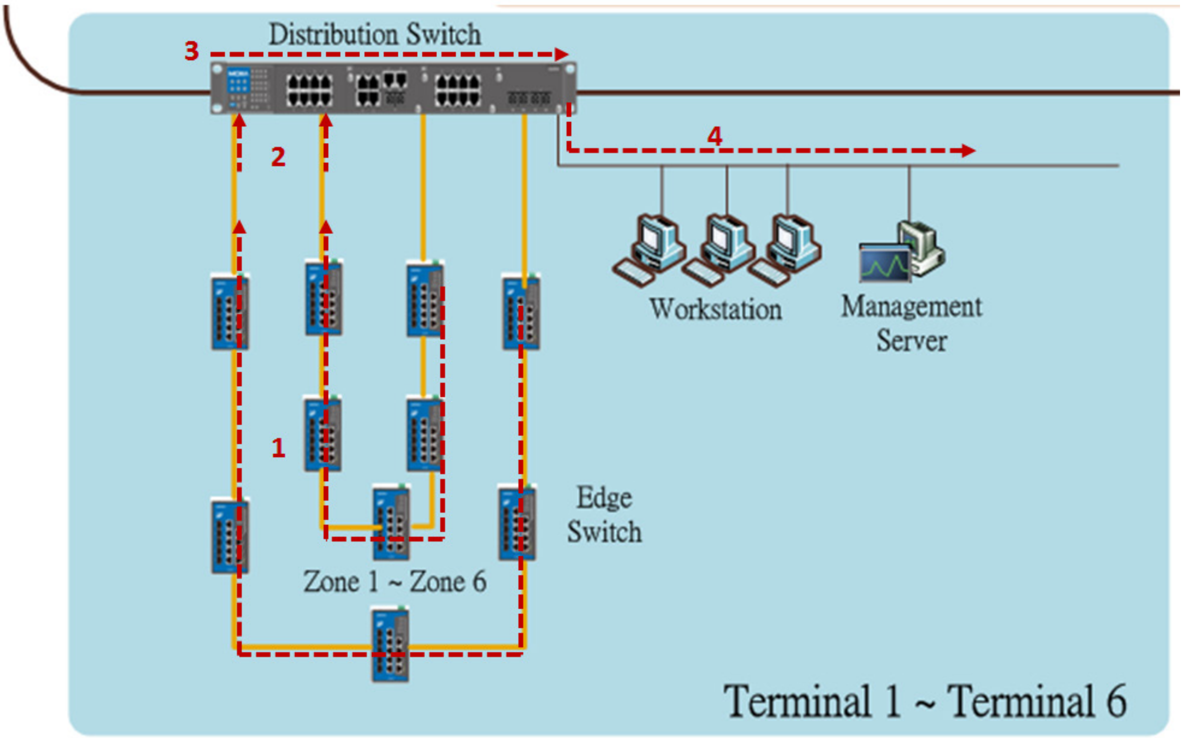
In most cases, the significant bandwidth of interest is created by the video streams going between two endpoints: the source and destination. In terms of network bandwidth consumption, command and control data, though critical, consumes trivial bandwidth compared to video data. For live viewing, the source is a camera or video server and the destination is a monitor. For playback, the data traffic goes from an archive server to a monitoring workstation.

For AIA, an additional 30% growth rate for the following three years must be included when calculating network bandwidth.

Access Network at Terminal

As in Figure 2-13, the access network consists of several edge switches connected in a Moxa Turbo Chain topology with one end (Turbo Chain Head) connecting to one distribution switch and the other end (Turbo Chain Tail) to the other distribution switch. The number of Turbo Chains corresponds to the number of zones in each terminal. For example, there are 6 zones in Terminal 1, so this Terminal has 6 independent Turbo Chains.

Figure 2-13



To estimate the bandwidth requirement for a network, we need to analyze traffic flow, then calculate the bandwidth consumption from all possible traffic sources, and also add bandwidth reserved for future growth.

In figure 2-13, the traffic (numbered 1) running on a Turbo Chain is the aggregation of video streams captured from all cameras of the chain. A zone consists of 15 to 25 cameras. The table below shows the bandwidth requirement for a 20-camera zone. Typically the access network bandwidth is 1 Gbps.

Figure 2-14

Traffic Flow #	Data Type	Source	Destination	Video Bitrate (Mbps)	# of Video Streams	Data Rate (Mbps)	Network Bandwidth (Mbps)
1	video capture for view/archive	camera/video server	OCC archive server	4	20	80	104

Access Switch at Terminal

According to the bandwidth calculation, the minimum port requirement for an access switch is as follows.

Figure 2-15

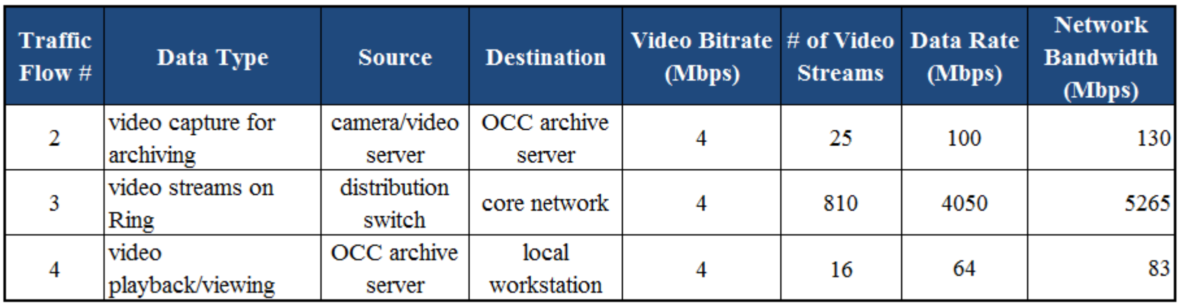
Purpose	100 Mbps port q'ty	1 Gbps port q'ty
Access port for local CCTV cameras	5	0
Turbo Chain connectivity	0	2

Distribution Network at Terminal

As in Figure 2-13, the distribution network comprises a pair of switches at the Terminal. Each distribution switch transports the data traffic going to the OCC from local cameras, data traffic running on the Turbo Ring, and that coming from OCC to local workstations.

The following table summarizes the bandwidth calculation for the distribution network in Figure 2-13.

Figure 2-16

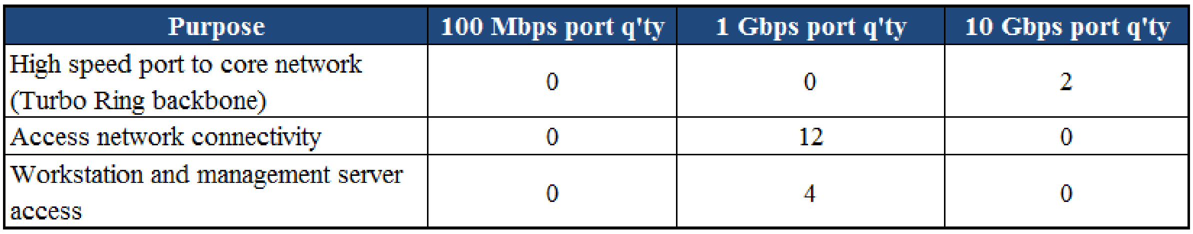


Traffic Flow #	Data Type	Source	Destination	Video Bitrate (Mbps)	# of Video Streams	Data Rate (Mbps)	Network Bandwidth (Mbps)
2	video capture for archiving	camera/video server	OCC archive server	4	25	100	130
3	video streams on Ring	distribution switch	core network	4	810	4050	5265
4	video playback/viewing	OCC archive server	local workstation	4	16	64	83

Distribution Switch at Terminal 1

As mentioned earlier in the chapter, the backbone network topology is Moxa Turbo Ring. The minimum port requirement for the distribution switch, derived from required bandwidth, is as follows:

Figure 2-17

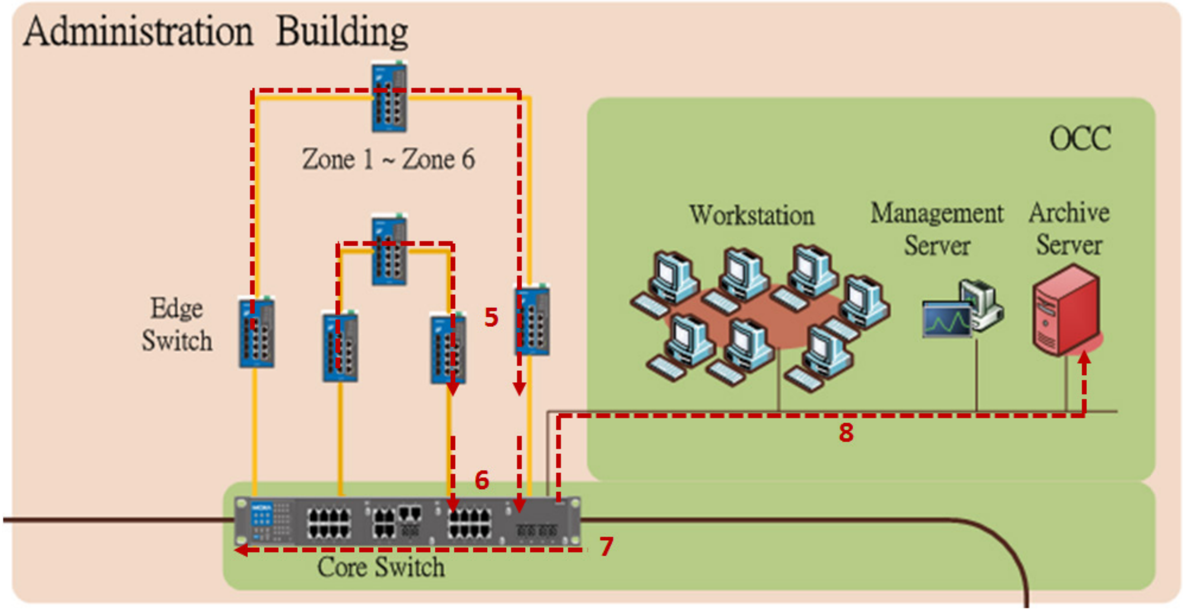


Purpose	100 Mbps port q'ty	1 Gbps port q'ty	10 Gbps port q'ty
High speed port to core network (Turbo Ring backbone)	0	0	2
Access network connectivity	0	12	0
Workstation and management server access	0	4	0

Access Network at Administration Building

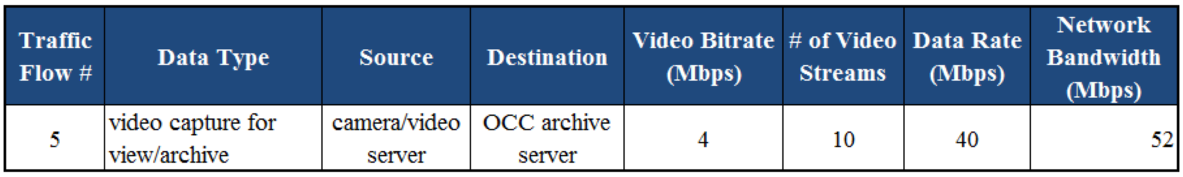
As in Figure 2-19, the access network consists of several edge switches connected in a Moxa Turbo Chain topology with one end (Turbo Chain Head) connecting to one core switch and the other end (Turbo Chain Tail) to the other core switch.

Figure 2-19



The bandwidth requirement for the access network is as follows.

Figure 2-20

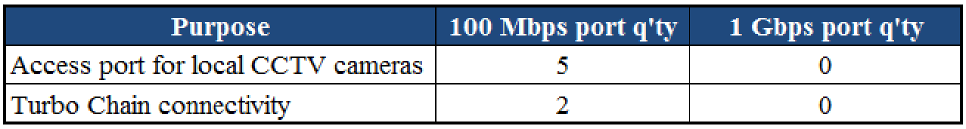


Traffic Flow #	Data Type	Source	Destination	Video Bitrate (Mbps)	# of Video Streams	Data Rate (Mbps)	Network Bandwidth (Mbps)
5	video capture for view/archive	camera/video server	OCC archive server	4	10	40	52

Access Switch at Administration Building

The minimum port requirement for the access switch according to the bandwidth calculation is as follows:

Figure 2-21

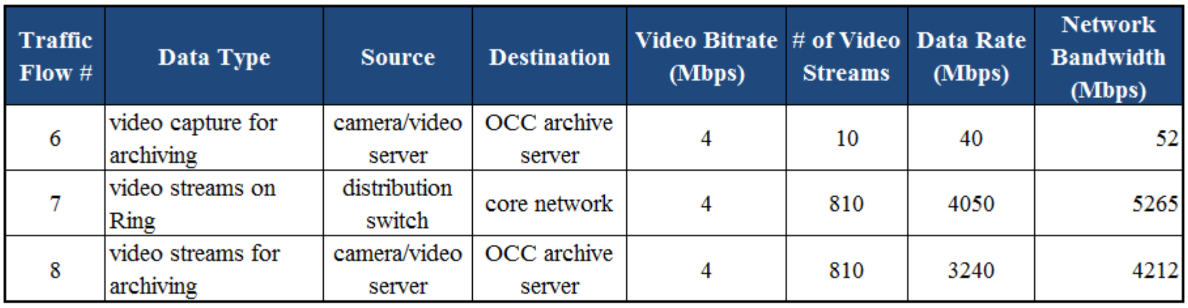


Purpose	100 Mbps port q'ty	1 Gbps port q'ty
Access port for local CCTV cameras	5	0
Turbo Chain connectivity	2	0

Core Network at Administration Building

The bandwidth requirement for the core network is as follows:

Figure 2-22

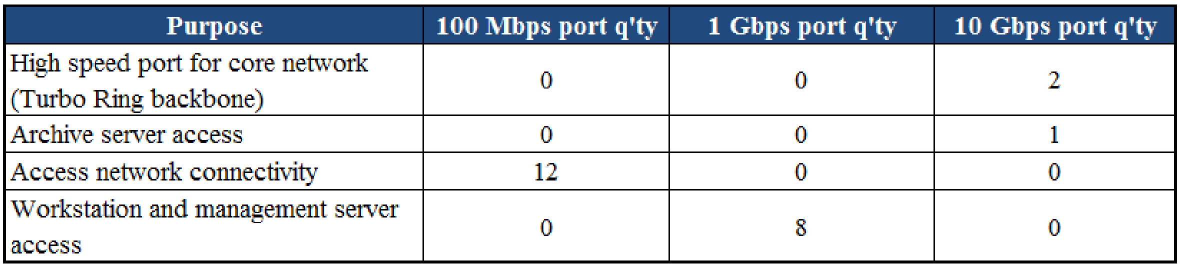


Traffic Flow #	Data Type	Source	Destination	Video Bitrate (Mbps)	# of Video Streams	Data Rate (Mbps)	Network Bandwidth (Mbps)
6	video capture for archiving	camera/video server	OCC archive server	4	10	40	52
7	video streams on Ring	distribution switch	core network	4	810	4050	5265
8	video streams for archiving	camera/video server	OCC archive server	4	810	3240	4212

Core Switch at Administration Building

The minimum port requirement for the core switch according to the bandwidth calculation is as follows:

Figure 2-23



Purpose	100 Mbps port q'ty	1 Gbps port q'ty	10 Gbps port q'ty
High speed port for core network (Turbo Ring backbone)	0	0	2
Archive server access	0	0	1
Access network connectivity	12	0	0
Workstation and management server access	0	8	0

LAN Segmentation and Routing

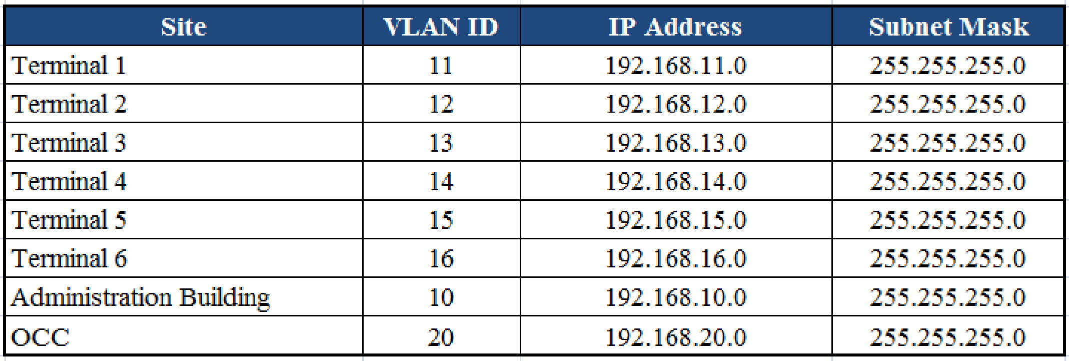
In order to manage traffic isolation and improve network security, the big Ethernet layer 2 network is segmented into VLANs. All cameras, workstations and server in one terminal are deployed in one VLAN. There are 6 different VLANs assigned to 6 Terminals respectively and one VLAN to Administration Building video servers. OCC itself is another VLAN for network resources like archive server, workstations and management servers.

Different VLANs do not exchange data traffic unless layer 3 routing function is implemented. In the design, distribution switches and core switch are L3 switches providing routing function to VLANs. Routing protocol such as RIP, OSPF is enabled on these switches.

Currently the maximum number of cameras at any one site (Terminal or Administration Building) is 130. A 24 bit subnet mask allows up to 254 IP addresses in one network, which is sufficient for current use as well as for future expansions.

Customer may have its VLAN and IP addressing policy, the following table is a reference should the customer not possess predefined rules.

Figure 2-24



Site	VLAN ID	IP Address	Subnet Mask
Terminal 1	11	192.168.11.0	255.255.255.0
Terminal 2	12	192.168.12.0	255.255.255.0
Terminal 3	13	192.168.13.0	255.255.255.0
Terminal 4	14	192.168.14.0	255.255.255.0
Terminal 5	15	192.168.15.0	255.255.255.0
Terminal 6	16	192.168.16.0	255.255.255.0
Administration Building	10	192.168.10.0	255.255.255.0
OCC	20	192.168.20.0	255.255.255.0

Multicast

A single video camera (encoder) produces a single video stream. If there is only one viewer on the network or the video stream is destined to just one archive server, it is "unicast" data traffic. Sending a video stream to multiple viewers or network recorders simultaneously requires multiple "unicast" data streams, which is inefficient. Moreover, the viewers may dynamically subscribe or unsubscribe to a video stream, making the situation more difficult to manage. This is when IP multicast technology comes in play for video surveillance system.

By implementing multicast, a camera (source) produces only one single video stream regardless of the number of viewers or recorders (destination), the network infrastructure handles duplication of the video stream according to where the users are. The benefits of this approach are reducing the load on the source, minimizing network device processing time, and maximizing network efficiency. All interested receivers will join a multicast group to receive the video stream of that multicast group. A multicast group is identified by a multicast group address.

The multicast group membership has to be established first before IP multicast functions as expected. IGMP (Internet Group Management Protocol) is the communications protocol for hosts and adjacent routers on an IP network to establish multicast group membership.

A switch will by default flood multicast traffic to all ports in a broadcast domain, which results in broadcasting unnecessary data traffic to the ports there are not users on. IGMP snooping can be implemented to further improve network bandwidth efficiency.

IGMP snooping is a feature that allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them.

In the AIA network, a video stream coming from a camera must be sent across network to OCC for storage and may be viewed by a workstation at local Terminal or/and by a workstation at OCC. Because any single video stream may have multiple dynamic viewers on the network, it makes perfect sense that we implement multicast technology so that every video encoder sends just one video stream and let the network do the duplication and intelligent filtering/forwarding.

Every single camera (recorder) is assigned a single multicast group with a unique multicast group IP address. A user (viewer or recorder) then subscribes to that multicast address whenever it wishes to receive the video stream.

In Figure 2-24, each VLAN is a broadcast domain. For multicast traffic to travel from domain to domain, it requires routers and multicast routing protocol. The distribution switches at Terminals and core switch at OCC are performing both switching and routing functions. Multicast routing protocol should be enabled at these routers so that field video streams can be sent to viewers and recorder at OCC.

The key design concepts related to IP multicasting are as follows:

- Defining IP multicast group addresses to cameras/recorders
  - The network operator should set its IP multicast addressing policy to follow. If not, one should use the IP multicast address range that is not reserved by IANA, say 230.x.x.x.
- Enable IGMP function in distribution and core switches, and recorders
- Enable IGMP snooping function in access switches
- Enable multicast routing protocol in distribution and core switches

There are several multicast routing protocols to choose from, e.g. DVMRP, PIM-DM, PIM-SM

QoS (Quality of Service)

Video traffic is sensitive to latency, packet loss, and jitter. A video stream with H.264 or MPEG4 compression, is more sensitive to packet loss because an I-frame loss will make a section of the video difficult to decipher. Network bandwidth and QoS are two critical factors to reducing packet loss, delay and jitter.

Network bandwidth must be carefully planned so that network congestion can be avoided. However network congestion may occur even with careful planning, especially in a network infrastructure that converges data, voice and video. QoS is the solution that manages network congestion when bandwidth is constrained. QoS does not create bandwidth, nor does it resolve network performance issues. Data traffic is dynamic and continuously competes for network bandwidth; QoS gives priority to the traffic that is marked high or preferred priority, so that the most important data is less likely to be discarded or delayed when network congestion occurs.

Basically the network supports QoS based on the label marked on data packets. Traffic priority can be marked in layer 2 COS (Class of Service) and Layer 3 DSCP (Differentiated Services Code Point) data fields. The layer 2 COS marking uses the 802.1p User Priority bits (3 bits) within the 802.1Q header. The layer 3 DSCP uses the first six bits of the Type of Service (TOS) byte of the IP packet header to identify priority.

The traffic classification and marking is suggested to be enabled at endpoints so that the network can prioritize incoming traffic according to the QoS marking. Alternatively, in case that an endpoint does not support traffic classification, the connected access switch needs to be able to do it based on pre-determined rules or policies. Once the data traffic is marked, the network that is properly configured for QoS support will perform queuing and congestion management.

The following are key concepts when implementing QoS:

- Consistent QoS policy is essential
- QoS should be implemented end-to-end, all the way from endpoints to access layer switches, distribution and core layer switches.
- Implementing traffic classification at endpoints or access layer switches
- Distribution layer and core layer switches should preserve the marking and perform congestion management according to the marking.

Security

The key concepts in enforcing network security are two-fold:

- Implementing access control to protect the network from intrusion
- Protecting network when access control fails to fend off malicious intrusion or there is unexpected data traffic on the network which presents security risk

The most direct and convenient way to access the network is through access switches at terminals and the administration building, from either the port connecting to the encoder or the port that is reserved for future use. Implementing port based security is the starting point to prevent network access from unauthorized users.

IEEE 802.1X is an IEEE Standard for port-based network access control. There are three roles in the 802.1X authentication process: the supplicant, authenticator and authentication server. Video encoder is the supplicant that provides credentials (userid/password) to authenticator for verification. An authentication server, e.g. RADIUS server, has to be installed and configured properly on the network for authentication verification. An access switch is the authenticator that receives credentials from encoder and submits the information to authentication server for verification. A camera/encoder is not allowed to access the network until credentials verification is passed.

After authentication check is passed, a client is granted network access. The network is still vulnerable to the data traffic the client sends across. In some cases, an internal user can jeopardize the network by sending illegal data traffic, no matter it's done purposely or unintentionally.

ACL (Access Control List) can be deployed at switches to further filter the data traffic going into (inbound) and moving out (outbound), giving granular control over data traffic. It defines what types of data or services can be accepted and what to reject.

As mentioned earlier in the document, LAN segmentation (VLAN) can divide a network into multiple sub-networks and limit data traffic on VLAN base, hence enhance network security.

PoE

Large and distributed networks such as AIA's are already difficult enough to wire and deploy. Power wiring adds another layer of complexity and cost to any project. In a network with a high number of devices, the sheer amount of cabling and power supplies needed can lead to a messy tangle of electrical cables or even major electrical re-wiring. PoE is now being used to reduce the number of cables required by delivering data and power on one cable to end devices. With PoE, no separate power supply is needed

PoE is defined in the IEEE 802.3af-2003 standard. The IEEE 802.3at-2009 standard, commonly known as PoE+, provides additional power. PoE+ is particularly useful for IP cameras that include pan, tilt, and zoom functionality, as the camera motors in those devices consume additional camera.

However, in the case of AIA, the cameras used are all analog cameras. This means that PoE will be less useful, as many of the devices at the terminals will not be able to take advantage of the technology. However, PoE functionality in the access switches might still be considered as a requirement, if AIA anticipates the need to simplify future upgrades and expansions to IP-based cameras that can draw power entirely through a PoE cable.

When evaluating whether or not to adopt PoE technology for a system, keep in mind the following considerations:

- The number of end and edge devices in the system that can be supported solely through PoE.
- How much power wiring would be necessary to deliver power conventionally.
- Whether power outlets or power sources are readily available at all the edge locations.

Systems that are difficult to wire conventionally and include many remote sites where an conventional power source might be difficult to locate are prime candidates for PoE technology. PoE technology also allows greater flexibility for future changes or upgrades to a network, as network devices can be easily added, removed, or rearranged, so it is useful in networks that expect to expand or adapt frequently.

Support Services

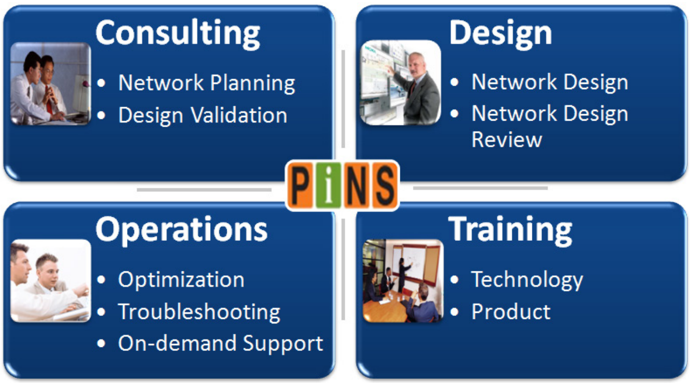
Designing a network is more complicated than it looks. It requires thorough understanding of the network requirements and available networking technology. This document points out some key network design considerations and focus on how to address them, providing the basics in working out a network design.

Designing a network also takes time, resources and skills. In some cases, one may find it necessary to use laboratory testing to verify that the network design is feasible and meets performance metrics. Many different skill sets and a good deal of expensive equipment are needed to conduct laboratory testing.

An organization may or may not have the skills or resources in accomplishing all of these tasks. In many cases the best course it to turn to external providers to supplement an organization with the skills, time, or resources needed to ensure a successful network.

Moxa Professional Industrial Networking Services (PiNS) provides network consulting, design, operations support and training services based on its 25 years of industrial products manufacturing capabilities and accumulated network best practices. To find out more about Moxa PiNS and its support, please contact PiNS@moxa.com.

Fig 2-25 Moxa Professional Services



Selecting Products

Moxa's portfolio includes products tailored for all layers of an industrial CCTV network. The products listed below exemplify the characteristics and feature set that network devices need to excel in a given role.

Core Switches

As the backbone of the network, core switches must support advanced management, high bandwidth, and high port density with flexible media support

Archetypical Device: ICS-G7848/G7850/G7852

The 48-port ICS-G7800 series is an excellent example of core switch qualities. The ICS-G7848/G7850/G7852 series full Gigabit backbone switches include layer 3 switching, extremely high bandwidth capacity with four 10 Gigabit Ethernet ports, and high port density. The switch adapts to many combinations of copper and fiber ports thanks to its modularity. As an industrial-grade core switch, the ICS-G7848/G7850/G7852 increases system reliability and the availability of the network backbone thanks to fanless design, redundant power supply, and Turbo Ring, Turbo Chain, and RSTP/STP redundancy protocols.

Distribution Switch

Distribution layer switches need slightly less bandwidth and port density than core layer switches, but still need more of each than edge switches.

Archetypical Device: IKS-6726/6728

The 24-port IKS-6726/6728 series of industrial rackmount Ethernet switches are designed to meet the rigorous demands of mission critical applications for industry and business, such as traffic control systems and maritime applications. The IKS-6726/6728's Gigabit and fast Ethernet backbone, redundant ring, and 24/48 VDC or 110/220 VAC dual isolated redundant power supplies increase the reliability of your communications and save on cabling and wiring costs. The modular design of the IKS-6726/6728 also makes network planning easy, and allows greater flexibility by letting you install up to 4 Gigabit ports and 24 fast Ethernet ports.

Edge Switches

Edge switches do not need the high port density of distribution or core layer switches, but they do need to operate in the most exposed field and remote conditions. High physical durability is a major factor for Edge switches. In addition, compact size and power-over-Ethernet are very useful in CCTV surveillance systems, as they make the network easier to deploy in cabinets and difficult-to-wire remote locations.

Archetypical Product: EDS-P206A-4PoE Series

The EDS-P206A-4PoE switches are smart, 6-port, unmanaged Ethernet switches supporting PoE (Power-over-Ethernet) on ports 1 to 4. The switches are classified as power source equipment (PSE), and when used in this way, the EDS-P206A-4PoE switches enable centralization of the power supply and provide up to 30 watts of power per port. The switches can be used to power IEEE 802.3at compliant powered devices (PD), eliminating the need for additional wiring, and support IEEE 802.3/802.3u/802.3x with 10/100M, full/half-duplex, MDI/MDI-X auto-sensing to provide an economical solution for your industrial Ethernet network. In addition, the built-in relay warning function alerts network engineers when power failures or port breaks occur.

About Moxa

Moxa delivers network-centric automation solutions that integrate surveillance, automation, and IT systems into a single network platform that simplifies management, reduces costs, and achieves greater network security.

Founded in 1987, Moxa is now one of the leading manufacturers of industrial networking, computing, and automation solutions. Moxa provides thousands of hardware and software products and draws upon 25 years of accumulated expertise. Moxa's products reflect our constant zeal for improvement, keen eye for innovation, and respect for proven solutions and expertise. We harness these properties to create solutions that deliver a competitive edge for our customers and partners in adapting to fast-changing network and market environments.

About Moxa PiNS

Now network designers can harness Moxa's industry-leading expertise through Moxa's professional industrial networking services (PiNS), a new service that ensures your success in designing Edge-to-Core industrial networking solutions tailored to your needs. PiNS offers you detailed and customized networking design and planning, so your network can meet all requirements with optimal performance and industry-proven reliability.

Moxa knows how to tailor network products for the specific needs of each network by using the standards, protocols, and resilient technology built into Moxa's products and solutions. Through PiNS, Moxa shares an accumulated and constantly-growing store of technical know-how and best practices with system integrators and operators to help them achieve network resilience, security and automation integration.

PINS covers every stage of network deployment, from network design and planning, to optimization and configuration review, all the way to technical support service and product training. Along the way, PINS customers receive specific knowledge transfer from Moxa and product training tailored for network managers, operation staff and maintenance engineers.

Further Reading

Moxa White Papers:

“Stay Connected with Turbo Ring” http://www.moxa.com/support/request_catalog_detail.aspx?id=98

“Turbo Chain: Beyond Redundant Ring Technology” http://www.moxa.com/support/request_catalog_detail.aspx?id=128

“PoE Switches for Industrial Networking” http://www.moxa.com/support/request_catalog_detail.aspx?id=58

“PoE Plus: Latest Developments in PoE Technology” http://www.moxa.com/support/request_catalog_detail.aspx?id=156

“IP Video Surveillance in Power Substations” http://www.moxa.com/support/request_catalog_detail.aspx?id=63