NETGEAR®

Networking Solutions for IP Surveillance

Table of Contents

BENEFITS OF IP SURVEILLANCE NETWORKS 3

IP NETWORK COMPONENTS AND STANDARDS 4

NETWORK PLANNING – GENERAL CONSIDERATIONS 6

CHOOSING A SWITCH: BANDWIDTH & PORTS 6

CHOOSING A SWITCH: POWER OVER ETHERNET 7

REFERENCE DESIGNS 8

- 20 CAMERAS 8
- 200 CAMERAS 9
- 1000 CAMERAS 12

MANAGED INFRASTRUCTURE 16

Video surveillance based on digital IP technology is revolutionizing the physical security industry. This solution guide will help you understand the basics of IP surveillance, and show you how to plan and specify an IP network.

The network is a crucial element in any surveillance installation because it enables all the other surveillance functions, not only transmitting video streams so they can be viewed and stored, but often carrying power to the cameras themselves via a Power over Ethernet (PoE) feature described in detail later on in this guide.

The key factors required to ensure a successful surveillance network are as follows:

- **Adequate bandwidth**. The network and the switch(es) that control it must be able to move traffic at "line rate" (full speed) to avoid risking delays, poor camera control or even loss of data.
- **Resilience**. The network switch(es) must have access to an alternate power supply should the main source of power fail.
- **Security**. The network must be protected from hacking, including physical hacking.

This guide will provide technical guidance and reference designs for installations with 20, 200 and 1000 cameras. Before covering design issues, however, it's worth reviewing just why IP surveillance is becoming the number one choice for projects of every size.

BENEFITS OF IP SURVEILLANCE NETWORKS

IP surveillance was once affordable only by large enterprises, but several factors have changed that situation. Today, most organizations have already installed IP networks upon which surveillance video transmissions can piggyback. Also, prices for IP video cameras and storage devices have fallen dramatically. As a result, IP surveillance is not only a viable choice for organizations of any size. It's usually the best choice.

IP surveillance offers a number of benefits that analog installations can't match.

- **No new cabling**. Traffic can be carried by an existing physical IP network. PoE (power over Ethernet) allows cameras to be connected to that network, eliminating the need for expensive Ethernet and power cabling to those cameras.
- **Lower labor costs**. Digital network-attached storage (NAS) devices reduce labor costs by eliminating the need for personnel to mount, replace and store tape cartridges and deal with all the other small but time-consuming problems endemic to tape systems.
- **More convenient viewing access**. Security personnel, administrators and other authorized parties can access surveillance video from any location on a 24/7 basis. Video clips can be distributed to law enforcement as e-mail attachments. There is never a need for third parties to visit the scene of an incident to view the video.
- **More reliable storage**. Unlike tape, digital storage doesn't degrade over time or when copied. NAS devices incorporate redundancy features and data integrity checks to ensure that every bit of footage is captured and available on demand within a few seconds.
- **Easier integration with applications**. IP surveillance systems are much easier to integrate with monitoring applications, from simple motion detection to advanced video content analysis such as face or license plate recognition, because no analog-to-digital conversion is necessary.
- **No risk of obsolescence**. As the world becomes increasingly digital, analog surveillance systems will inevitably become obsolete over time, whereas IP surveillance systems are future-proof and will always be easy to upgrade, typically through software alone.

IP NETWORK COMPONENTS AND STANDARDS

No matter what the size of the IP surveillance system, it will always include one or more of the following components:

- IP cameras
- Video servers to record, aggregate, process and broadcast video streams
- Clients. Typically, the clients (monitoring stations) are PCs equipped with dedicated surveillance software to enable real-time viewing and/or review of stored video
- NAS devices to store the video
- Switches to manage network traffic. The switches are crucial, because if they lack the appropriate feature set or bandwidth capacity, the entire surveillance network won't function properly.
- Cabling. For adequate performance, Cat5E or better cabling is recommended.

In operation, the video information from the cameras is transmitted (streamed) to a video server, where it is aggregated, processed, stored and distributed to the monitoring stations and storage devices. Some of the details of how this takes place are described below. This information can be important, as factors like transmission modes and video compression modes can have a significant effect on bandwidth requirements, storage requirements and cost.

Transmission Modes

There are two basic transmission modes, unicast and multicast. Most cameras can be set to transmit in either mode.

Unicast mode is a direct, one-to-one means of transmitting a video stream, e.g. from a camera to a video server, or from a video server to a client. This means that if a video server needs to transmit to four clients, it must send the same transmission four times. In a system with dozens of camera streams and numerous clients, unicasting can easily overwhelm the bandwidth capacity of a network's switch(es).

Multicast mode is a one-to-many mode where servers "publish" a video stream and clients "subscribe." In multicast mode, video streams – identified by an IP address – are broadcast across the network, and any client on that network has the potential to access them. Access to any given stream is controlled by the Internet Group Management Protocol (IGMP). Under this protocol, clients are divided into groups based on which streams they are authorized to access. Two switch components are required to manage the process:

- an IGMP Querier that generates query messages to determine which clients belong to various groups
- an IGMP Snooper which "listens" to the various ports on the client hardware to determine which ports are "interested" – and then sends data only to those ports, eliminating unnecessary network traffic and maximizing efficiency. In networks that have been upgraded to the IPv6 standard, the IGMP Querier will be replaced by a Multicast Listener Discovery (MLD) Querier and an MLD Snooper.
-

Generally speaking, both the unicast and multicast modes have their advantages and disadvantages. A unicast network is easier to set up, and may have a lower initial cost. However, for surveillance applications, multicast capabilities are preferable. Being restricted to the unicast mode can overburden a network, and if transmissions exceed a network's or subnet's bandwidth capacity – a condition known as over-subscription – the switch controlling it will simply block further transmissions. This is obviously unacceptable when 100 percent 24/7 coverage is required.

Most IP surveillance networks combine these two modes, using unicast to transmit from the cameras to the video server, and multicast to transmit to the clients.

Video Compression

All video data captured by the camera is compressed prior to transmission, and the mathematical algorithm used for this has important effects on both the end user and the network itself. These effects include:

- image quality
- latency
- bandwidth requirements
- storage requirements

There are three popular standards right now. In order of their "age" (year introduced), they are:

- MJPEG (mid-1990s)
- MPEG4 (1998)
- H.264 (2003)

In addition, some of the major IP camera vendors use their own proprietary standards.

The details of video compression are extremely complicated and beyond the scope of this guide. In practical terms, MJPEG offers the best image quality, but also requires the most storage capacity. MJPEG once had the lowest latency of the three, which means better live viewing and more responsive control of pan, tilt and zoom (PZT) cameras. NETGEAR switches have eliminated this problem.

MPEG4 reduces storage requirements relative to MJPEG, but with some reduction in image quality as well. (For most surveillance purposes, MPEG4 image quality is certainly acceptable.) H.264 uses the same mathematical approach as MPEG4, but improves on its performance in terms of storage requirements. H.264 is rapidly gaining acceptance as the standard of choice.

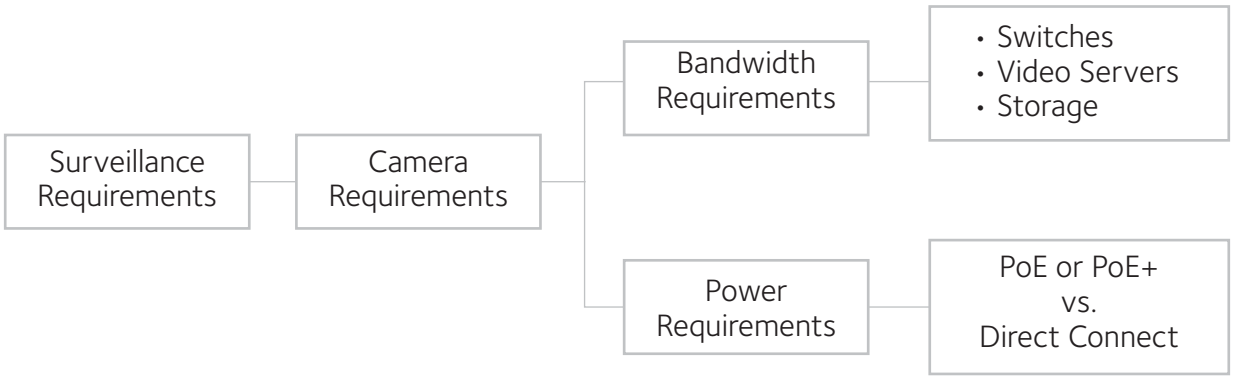
Security

A separate, but extremely important consideration that requires some explanation is network security in an IP network. Obviously, any network will be protected through access control, e.g. support for role-based access with authentication and passwords. In addition, IP networks have a physical vulnerability. The very fact that cameras are often located in the remote corners of warehouses, etc. means that an attacker could easily disconnect a camera and put a PC in its place, thus obtaining unauthorized access to the network.

To prevent this, NETGEAR switches make use of the fact that every physical device on a network has a unique Media Access Control or MAC address. NETGEAR switches can sense this address, and be programmed to block any unauthorized device. The ultimate in protection can be achieved through the use of the Radius (Remote Authentication Dial-In User Service) protocol associated with an authentication server that can block access to ports even if hackers succeed in spoofing and emulating MAC addresses during an attack.

NETWORK PLANNING – GENERAL CONSIDERATIONS

The planning of an IP surveillance network has five steps, as show below:



The surveillance requirements – area to be surveilled, level of detail to be captured, need (or lack thereof) for PTZ cameras and so on – will determine the number and type of cameras, which will in turn determine bandwidth and power requirements for the switches. Bandwidth requirements will also affect the choice of server and the storage capacity required. The following section will focus on choosing the appropriate switch(es). The key factors for choosing the IP switch(es) for a surveillance network are:

- bandwidth requirements
- number of ports
- power requirements

CHOOSING A SWITCH: BANDWIDTH & PORTS

NETGEAR recommends two lines of Managed switches for IP surveillance networks:

- The NETGEAR Intelligent Edge M4100 series. These are Fast Ethernet (10/100) and Gigabit Ethernet (GigE) access layer switches with several Gigabit ports for uplink functions.

- The NETGEAR Next-Gen Edge M5300 series. These are Gigabit Ethernet (GigE) switches with embedded 10 Gigabit ports (10GbE) for uplink functions and virtual chassis stacking

Determining which switch within these two families requires answering four questions.

1. *Will the network use Fast Ethernet cameras or Gigabit Ethernet cameras?* For the vast majority of surveillance applications, Fast Ethernet cameras are the norm. In this case, cost-effective NETGEAR Fast Ethernet switches may be adequate, based on the total bandwidth requirement. (See question 4.) Note that these Fast Ethernet switches, in spite of their name, do include a Gigabit port for uplink purposes in a two-tier network. Sometimes, however, even a deployment with only Fast Ethernet cameras may require 10 Gigabit uplink capabilities. If Gigabit Ethernet cameras are used, a Gigabit switch is required.

2. *What is the average bandwidth required per camera?* This figure depends on a number of factors, primarily the resolution, the frame rate and the compression algorithm used by the camera. In general, the higher the resolution and the higher the frame rate, the more bandwidth and the more memory capacity required. The best way to determine this figure is to consult with the camera vendor.

3 *How many cameras will be in the network?* This determines how many ports the switch(es) will need – one port per camera. Note that all of the NETGEAR Fast Ethernet switches are equipped with several Gigabit ports for uplink purposes.

4. *What is the total bandwidth required per switch?* This is a simple calculation:

   Average bandwidth per camera x total number of cameras = total bandwidth required (Gbps)

   The total Gbps that the switch can transfer – the "switching fabric" of that switch – must exceed the answer to this equation. And if the switch must be connected to an upper layer (such as a Core or Distribution Layer), then the uplink connection must support the total bandwidth required for that uplink without creating a bottleneck.

CHOOSING A SWITCH: POWER OVER ETHERNET

Most IP cameras are designed to accept Power over Ethernet (PoE), which is a relatively new technology (introduced in 2000) than enables power to be delivered over the same Ethernet cable as data, with no danger of cross-talk, interference or corruption of the data streams. There are two versions available:

- PoE provides up to 15.4W per port, with up to 12.9W available to the IP camera
- PoE+ provides up to 30W, with up to 25W available to the IP camera

To determine which switch in the M4100 or M5300 family is required for a particular installation, ask the following questions:

1. *Do the cameras require PoE or PoE+?* Generally speaking, PoE will be adequate for Fast Ethernet cameras, while PoE+ will be required for PTZ cameras, dome cameras and Gigabit Ethernet cameras.

2. *How many watts are required per camera?* This information can easily obtained from the vendor.

3. *How many cameras will be on the network?*

4. *What is the total wattage requirement?* It can be calculated as follows:

   Average watts per camera x total number of cameras = total PoE budget required

   Obviously, the power capacity of the switch – its "PoE budget" – must exceed the total power requirements of the switches on the network.

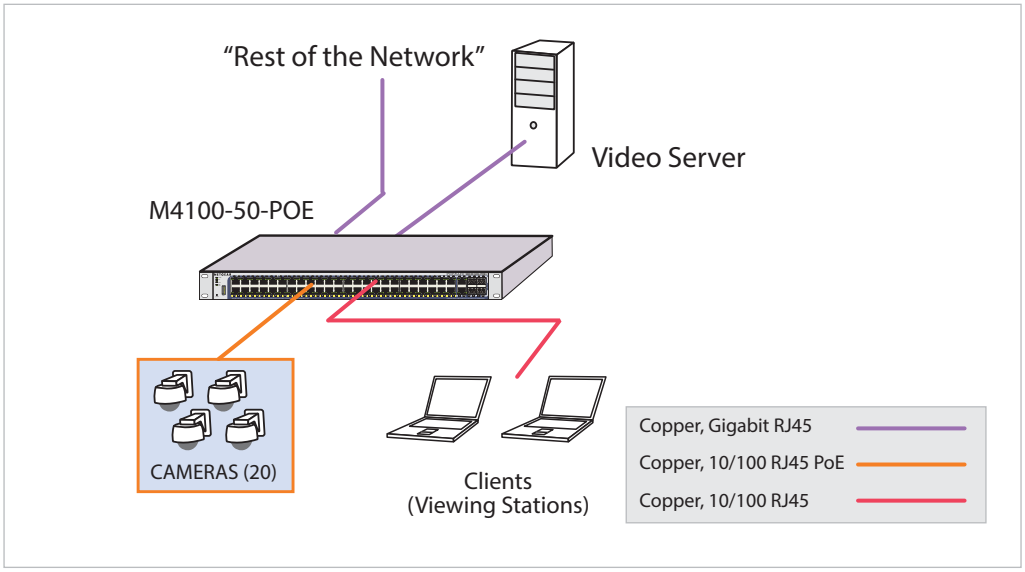
REFERENCE DESIGNS

The following reference designs will provide general guidance on how to plan a highly reliable and cost-effective surveillance network. Each network was designed with four criteria in mind:

- simplicity, to enable easy installation and management
- minimum impact on available network bandwidth
- resilience to ensure the 24/7 coverage that's critical for a surveillance network
- security

Reference Design: 20 Cameras

The diagram below shows a typical installation with 20 cameras and one server, where the traffic is all managed by a single switch. It is a complete solution that is ideal for a small facility with typical interior lighting conditions. The cameras are all fixed, Fast Ethernet cameras. It's assumed there's no need for PTZ capabilities. The video server has a 1 Gigabit bandwidth capacity.



The benefits of this design include the following:

Simplicity

- The switch can be configured with a unique, easy-to-use web-based interface as well as the industry-standard command line interface (CLI).
- The switch delivers PoE power to all the cameras (with a maximum PoE budget of 380w), so no power cabling is required.

Minimum Bandwidth Impact

- The cameras transmit a unicast stream to the server. The server in turn transmits multicast streams to the rest of the network, which minimizes the video stream bandwidth burden on the network.
- An IGMP Querier that determines which clients belong to various groups is combined with an IGMP Snooper that determines which ports within those groups are "interested." The result is that data is sent only to the appropriate ports, eliminating unnecessary network traffic and maximizing efficiency.

Resilience

- Redundant Power Supply (RPS) protection. The switch can be connected to a back-up power supply to provide redundancy and ensure 24/7 reliability.
- External Power Supply (ESP) option: If the power demands of the network should exceed the PoE budget, additional power can be supplied via an EPS module, ensuring that the network is scalable over time.

Security

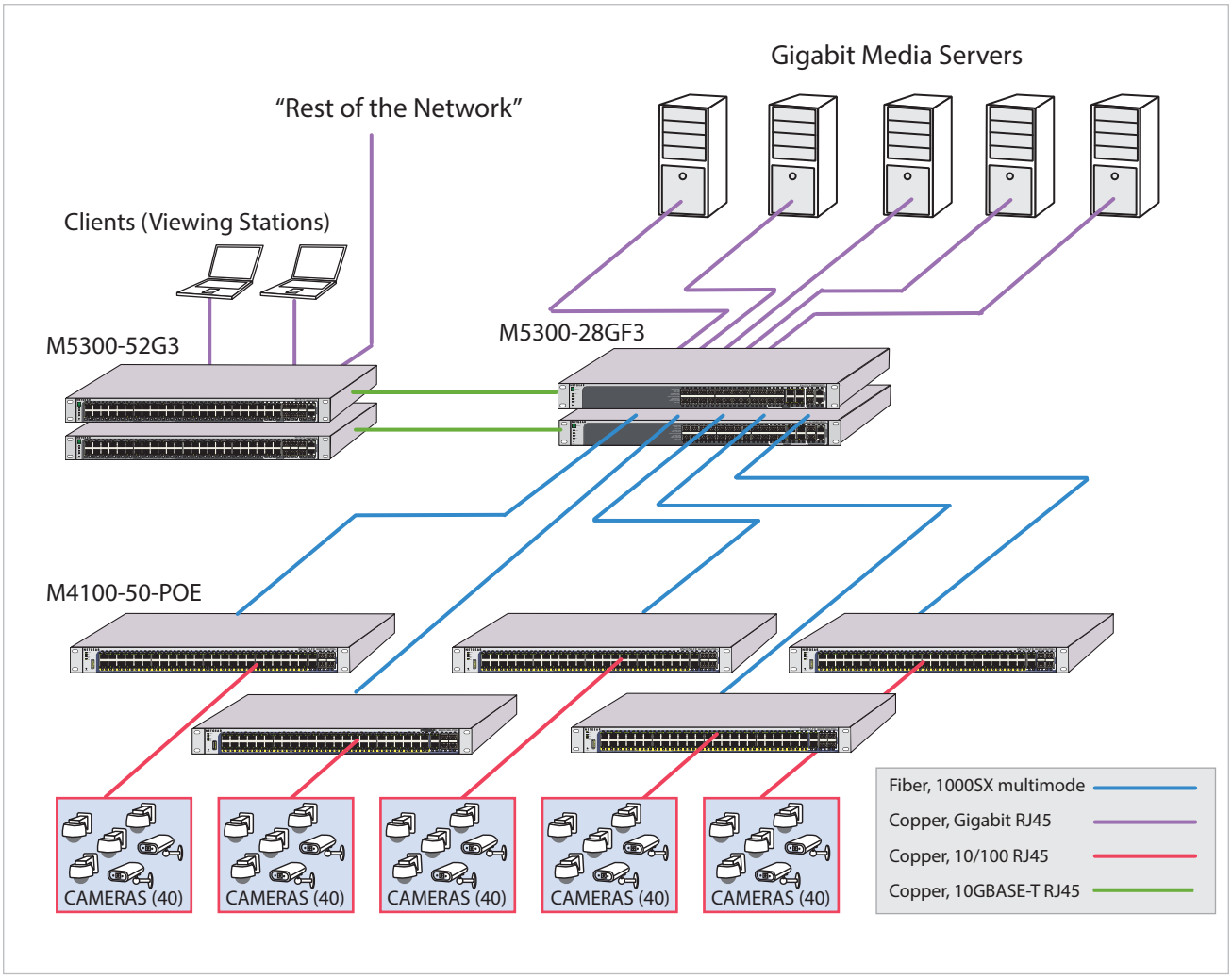
- The switch provides for MAC-based security to prevent physical hacking, e.g. unscrewing a camera and replacing it with a PC.
- Assuming the cameras support the IEEE 802.1x authentication standard for port-based Network Access Control, a higher level of security can be implemented using a RADIUS server or Windows Server 2008 Network Policy Server (NPS). With this approach, access to ports can be blocked even if hackers succeed in spoofing and emulating MAC addresses during an attack.

Bandwidth and Power Calculations: 20 Cameras	
Average bandwidth per camera	9.48 Mbit/s based on specific set of image resolution, compression type and ratio, frame rates and scene complexity
Total bandwidth for twenty cameras	9.48 x 20 = 190 Mbit/s
PoE Class	1 (maximum 2.7W)
Total PoE budget	2.7 x 20 = 54W
Key NETGEAR Components	
Switch	M4100-50-POE (48 ports Fast Ethernet PoE 802.3af, Layer 2+)
Redundant Power Supply	RPS5412 (Optimal Power one-to-one RPS unit) or RPS4000 (RPS unit up to four switches)
External Power Supply	RPS4000 (supplemental PoE power up to four switches)

Reference Design: 200 Cameras

This 200-camera installation would be typical for a facility where cameras must be located in multiple locations, e.g. a warehouse, a parking lot, administrative offices and so on. It consists of several IP subnets and associated VLANs but without Layer 3 routing complexities. All the cameras are on the same subnet. The servers that manage them are on another subnet, while the clients/viewing stations may be on other subnets. Each access-layer switch connects forty cameras, and also powers them via PoE. All the cameras are fixed, Fast Ethernet cameras (without PTZ capabilities) and have PoE capability.

This design delivers a highly available network that provides uninterrupted connectivity. It incorporates a level of redundancy such that there are no points of hardware failure. Further, critical components can be swapped without interruption of service.



The benefits of this design include the following:

Simplicity

- The "private VLAN" capability of the NETGEAR switches in this design means that camera deployment is inherently less complicated when the cameras are all in the same Layer 2 network. The network is also easier to manage without Layer 3 routing to the servers.
- With a Dynamic Host Configuration Protocol (DHCP) server, already up and running in most IT departments, and also available in NETGEAR switches, the need for configuring the cameras is entirely eliminated.
- This network design avoids the use of the Spanning Tree Protocol, which is complex and difficult to configure. The network's highly resilient Distribution layer allows for the best of both worlds with redundant links to the servers and access layer switches, as well as advanced load balancing and seamless failover capabilities – made as simple as "trunking"
- A Multicast VLAN Registration (MVR) feature replicates the multicast video streams from the access subnet across as many other subnets as desired, preserving all of the bandwidth-conserving features of the access subnet (IGMP Querier and Snooper) and the publish/subscribe model. This eliminates all the complexities of multicast routing to clients/viewing stations.

Minimum Bandwidth Impact

- The "private VLAN" capability of the NETGEAR switches in this design means that all the cameras are isolated and cannot talk to one another, even though they are on the same subnet. Eliminating camera-to-camera "chatter" reduces bandwidth utilization.
- To minimize bandwidth consumption, an IGMP Querier that determines which clients belong to various groups combines with an IGMP Snooper that determines which ports within those groups are "interested." The result is that data is sent only to the appropriate ports, eliminating unnecessary network traffic and maximizing efficiency.
- The avoidance of the Spanning Tree Protocol also enables more efficient use of bandwidth, since all links are active and load balancing is enabled.

Resilience

- Redundant Power Supplies (RPSs). In this design the switches are all equipped with an RSP in the unlikely event that a switch power supply should fail. This approach can be implemented on a one-to-one basis with NETGEAR RPS5412 redundant power supplies if all the switches are in different buildings. If the switches are on the same rack, a NETGEAR RPS4000 can be used to provide redundant power to as many as four switches. The internal power supply of the switches at the Distribution layer is modular and can be "hot swapped" with no interruption to service.
- External Power Supplies (ESPs). If additional power is required beyond the 380w provided by the M4100-50-POE switches, it can be supplied via NETGEAR EPS modules, which can provide the access layer switches with 740w each.
- Redundant Switches. This design features redundant, stacked distribution switches (two M5300-28GF3 switches and two M5300-52G3 switches) with sub-second network failover protection.

Security

- MAC-based port security (MAC address table locking) provides a minimum level of security by preventing an attacker from disconnecting a camera and connecting a PC in its place for hacking purposes.
- Assuming the cameras support the IEEE 802.1x authentication standard for port-based Network Access Control, a higher level of security can be implemented using a RADIUS server or Windows Server 2008 Network Policy Server (NPS) with or without MAC authentication bypass (MAB). With this approach, access to ports can be blocked even if hackers succeed in spoofing and emulating MAC addresses during an attack.
- Because all the cameras on the access subnet are isolated from one another, a successful hack of one camera will yield minimal results to the hacker.

Bandwidth and Power Calculations: 200 Cameras	
Average bandwidth per camera	21.7 Mbit/s based on specific set of image resolution, compression type and ratio, frame rates and scene complexity
Total bandwidth for forty cameras	21.7 x 40 = 868 Mbit/s per Access Layer switch
PoE Class	1 (maximum 2.7W)
Total PoE budget	2.7 x 40 = 108W per Access Layer switch
Key NETGEAR Components	
Distribution Layer Switch	M5300-28GF3 (24 ports Gigabit Ethernet Fiber with 10 Gigabit uplinks, Layer 3)
Access Layer Switch	M4100-50-POE (48 ports Fast Ethernet PoE 802.3af, Layer 2+)
Rest of the network Switch	M5300-52G3 (48 ports Gigabit Ethernet with 10 Gigabit uplinks, Layer 3)
Redundant Power Supply	RPS5412 (Optimal Power one-to-one RPS unit) or RPS4000 (RPS unit up to four switches)
External Power Supply	RPS4000 (supplemental PoE power up to four switches)

Reference Design: 1000 Cameras

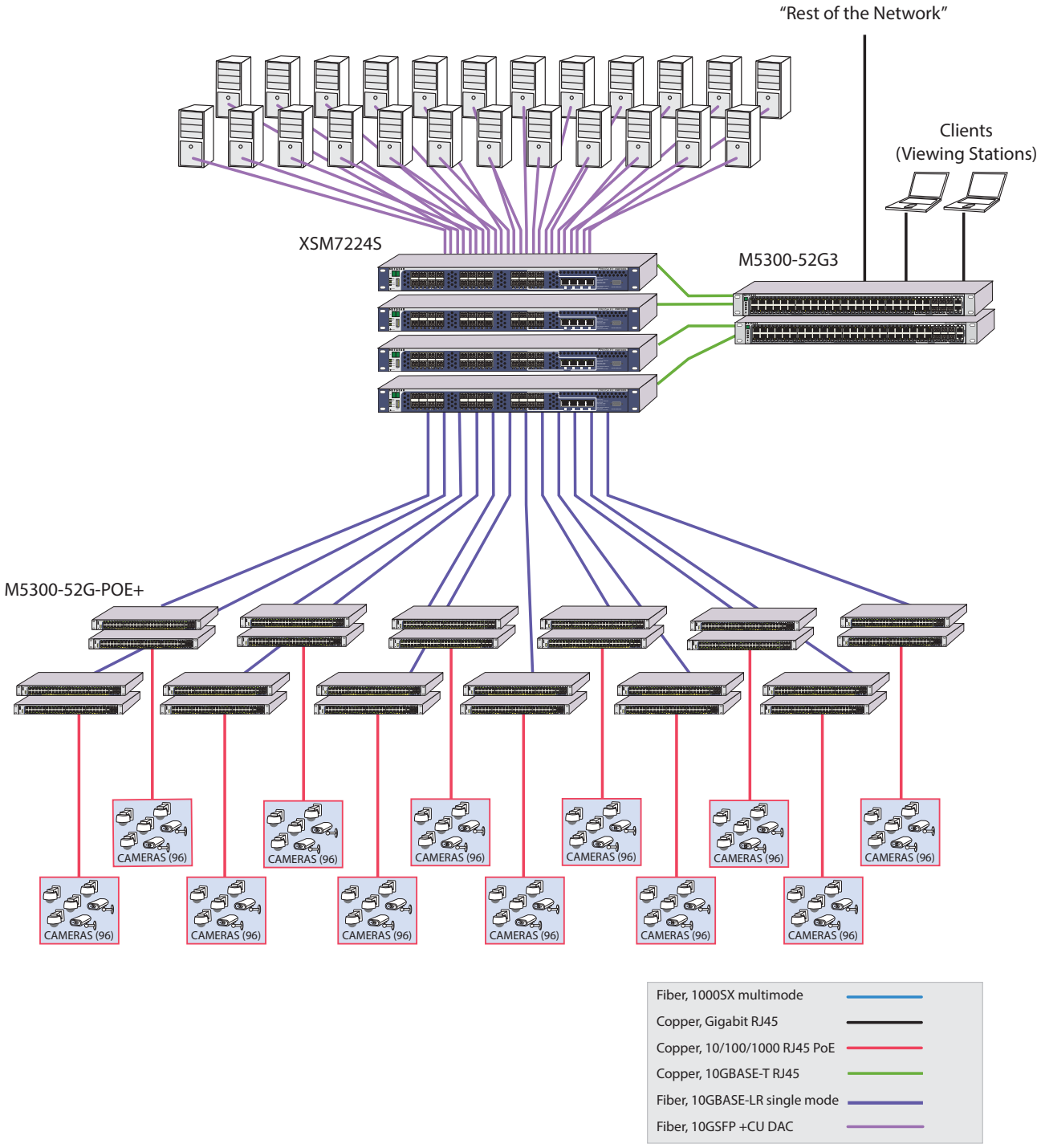
This 1,000-plus camera installation is based on a facility where 12 different sites require surveillance, such as a small college campus. It uses fiber optic cabling due to the distance between the various sites under surveillance. It consists of one unique IP subnet for all the cameras and the servers, with different VLANs but no Layer 3 routing complexities at the access layer. The clients/viewing stations may be on other subnets throughout the rest of the network.

Each surveillance site is equipped with two stacked 48-port M5300-52G-POE+ Gigabit switches using virtual chassis stacking technology. This stack provides 96 ports that connect the cameras at that site. It also powers them via PoE. All the cameras are fixed, Fast Ethernet cameras (with or without PTZ capabilities) and have PoE capability.

At the distribution layer, virtual stacking technology is also used to stack four XSM7224S 10 Gigabit managed switches that provide distributed link aggregation (one 10 Gigabit link per physical switch) for a 40Gbit/s unidirectional connection to the rest of the network where clients (viewing stations) may be located.

Transmission is in unicast mode between each camera and its access layer server, and multicast mode for the rest of the network. Because clients/viewing stations may be elsewhere throughout the rest of the campus network, the protocols chosen are OSPF for unicast routing, IGMP for multicast group membership and PIM sparse-mode for multicast routing.

This design delivers a highly available network that provides uninterrupted connectivity. It incorporates a level of redundancy such that there are no points of hardware failure and ensures quick fault recovery. Furthermore, critical components can be swapped without interruption of service.


"Rest of the Network"
Clients
(Viewing Stations)
XSM7224S
M5300-52G3
M5300-52G-POE+
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
CAMERAS (96)
Fiber, 1000SX multimode
Copper, Gigabit RJ45
Copper, 10/100/1000 RJ45 PoE
Copper, 10GBASE-T RJ45
Fiber, 10GBASE-LR single mode
Fiber, 10GSFP +CU DAC

The benefits of this design include the following:

Simplicity

- The "private VLAN" capability of the NETGEAR switches in this design means that camera deployment is inherently less complicated when the cameras are all in the same Layer 2 network. The network is also easier to manage without Layer 3 routing to the servers.
- With a Dynamic Host Configuration Protocol (DHCP) server, already up and running in most IT departments, and also available in NETGEAR switches, the need for configuring the cameras is entirely eliminated.
- This network design avoids the use of the Spanning Tree Protocol, which is complex and difficult to configure. The network's highly resilient Distribution layer allows for the best of both worlds with redundant links to the servers and access layer switches, as well as advanced load balancing and seamless failover capabilities – made as simple as "trunking"

Minimum Bandwidth Impact

- The "private VLAN" capability of the NETGEAR switches in this design means that all the cameras are isolated and cannot talk to one another, even though they are on the same subnet. Eliminating camera-to-camera "chatter" reduces bandwidth utilization.
- To minimize bandwidth consumption, an IGMP Querier that determines which clients belong to various groups combines with an IGMP Snooper that determines which ports within those groups are "interested." The result is that data is sent only to the appropriate ports, eliminating unnecessary network traffic and maximizing efficiency.
- The avoidance of the Spanning Tree Protocol also enables more efficient use of bandwidth, since all links are active and load balancing is enabled.

Resilience

- Switch redundancy. The four stacked distribution layer switches provide redundancy with < one second failover. The two switches in each access layer stack at the various surveillance sites are connected to different physical switches at the distribution layer so there is complete redundancy at both layers in the unlikely event that a switch should fail.
- Redundant Power Supplies (RPSs). This design assumes that each two-switch stack in the access subnet is deployed in a different location. Therefore, each stack is provided with a separate RPS – the NETGEAR RPS4000 – in the unlikely event that a switch power supply should fail. Each RPS4000 can provide redundant power to as many as four switches. The internal power supply of the switches at the Distribution layer is augmented with an additional APS300W power module for server-like redundancy. It can be hot swapped if necessary to avoid network downtime.
- External Power Supplies (ESPs). If additional power is required beyond the 380w provided by the M5300-52G-POE+ switches, it can be supplied via RPS4000 in EPS mode, which can provide the access layer switches with up to 1,440w each.
- Redundant links. There are two 10 Gigabit links from each access layer stack to the distribution layer switches, and one of them alone has adequate bandwidth to carry all the aggregated camera streams. Adding a second enables load balancing of the video streams and also provides redundancy should one of the access layer or distribution layer switches fail – an unlikely event.

Security

- MAC-based port security (MAC address table locking) provides a minimum level of security by preventing an attacker from disconnecting a camera and connecting a PC in its place for hacking purposes.
- Assuming the cameras support the IEEE 802.1x authentication standard for port-based Network Access Control, a higher level of security can be implemented using a RADIUS server or Windows Server 2008 Network Policy Server (NPS) with or without MAC authentication bypass (MAB). With this approach, access to ports can be blocked even if hackers succeed in spoofing and emulating MAC addresses during an attack.
- The dedicated management VLAN for the access layer and distribution layer switches can also utilize a control plane access control list (ACL) to provide additional security.
- Because all the cameras on the access subnet are isolated from one another, a successful hack of one camera will yield minimal results to the hacker.
- If a camera is disconnected or tampering is detected, both the camera and the camera management software on the video server will generate an alarm.

Bandwidth and Power Calculations: Access Subnet	
BANDWIDTH	
Average bandwidth per camera	33.9 Mbit/s based on specific set of image resolution, compression type and ratio, frame rates and scene complexity
Total switch bandwidth requirement for 96 cameras on access subnet per surveillance site (i.e. uplink requirement per site):	96 x 33.9 Mbit/s = 3.19 Gbit/s per Access Layer 2-switch stack
Total server bandwidth requirement (assuming each server manages 48 cameras)	48 x 33.9 Mbit/s = 1.59 Gbit/s
Analysis: Two 48-port Gigabit switches are required per site, each with a 1.63 Gbit/s uplink capability. A 1 Gigabit switch isn't sufficient to provide line rate transmission at 1.63 Gbit/s, so 10 Gigabit switches are required. Two 10 Gigabit switches will provide necessary redundancy. This design also includes 10 Gigabit servers, and assumes each server can handle 48 cameras. At the distribution layer, four 24 port 10 Gigabit Ethernet SFP+ switches provide 480 Gbit/s aggregated bandwidth capacity.	
POWER	
PoE Class	3 (maximum 9w)
Total PoE budget per site	9w x 96 = 864W per Access Layer 2-switch stack
Analysis: With two access layer switches per surveillance site, each switch must provide 432w of PoE. In this design, these switches each have a 380w PoE budget. This budget is expanded by using a dual function external/redundant RS4000 power supply (EPS/RPS) so that each switch would be able to deliver up to 1,440w. Thus, the additional power required for the cameras and the redundancy to ensure continuous operation are both provided. Power to the four distribution layer switches is provided by a supplemental APS300W internal power supply.	

Key NETGEAR Components	
Distribution Layer Switch	XSM7224S (M7300-24XF 24 ports 10 Gigabit SFP+ with 10GBASE-T uplinks, Layer 2+) and its XSM7224L Layer 3 license upgrade
Access Layer Switch	M5300-52G-POE+ (48 ports Gigabit Ethernet PoE+ 802.3at with 10 Gigabit uplinks, Layer 2+)
Rest of the network Switch	M5300-52G3 (48 ports Gigabit Ethernet with 10 Gigabit uplinks, Layer 3)
Redundant Power Supply	RPS4000 (RPS unit up to four switches)
External Power Supply	RPS4000 (supplemental PoE power up to four switches)

MANAGED INFRASTRUCTURE

NETGEAR Managed Switches offer a secure, future-proof networking infrastructure for mid-size organizations and campus networks, with industry-leading lifetime warranty, lifetime technical support and lifetime next business day replacement service. Learn more at www.netgear.com/managed.

Stackable L2+ L3

MLAG L2+

M7300 10G Aggregation series

M7100 10G Aggregation series

Core/Distribution

MLAG L3

M6100 LAN Access and Aggregation Chassis series

Multi-Role Platform

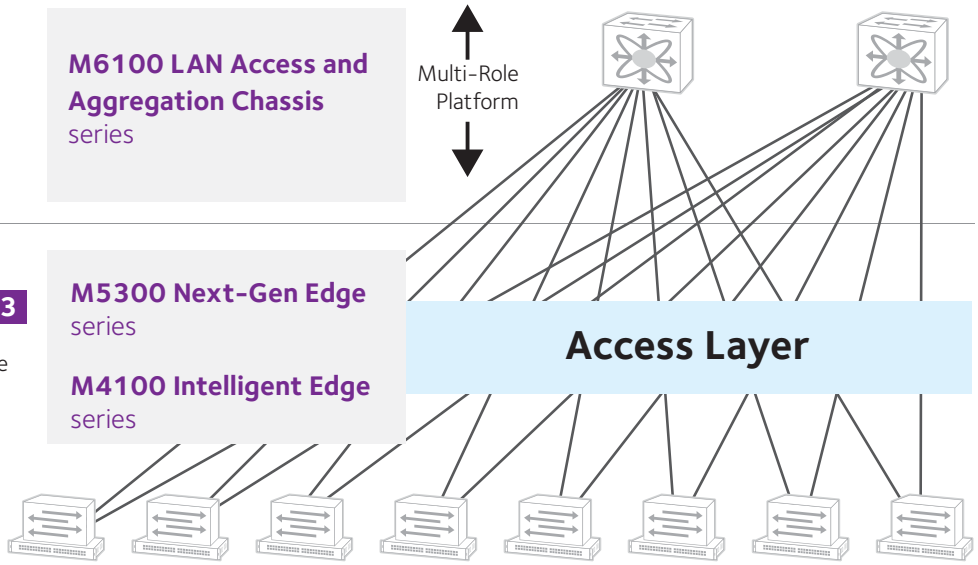
Stackable L2+ L3

Standalone L2+

M5300 Next-Gen Edge series

M4100 Intelligent Edge series

Access Layer



NETGEAR SWITCHING SOLUTIONS					
Product Name	**M7300-24XF**	**M7100-24X**	**M6100 Series**	**M5300-28G**	**M5300-52G**
Order Number	**XSM7224S**	**XSM7224**	**XCM8900**	**GSM7228S**	**GSM7252S**
RJ45 Ports	4 x 10GBASE-T	24 x 10GBASE-T	Up to 144 x 10/100/1000 Up to 72 x 10GBASE-T	24 x 10/100/100 2 x 10GBASE-T (Max: 4)	48 x 10/100/100 2 x 10GBASE-T (Max: 4)
Fiber SFP+ (1000/10G)	24 x SFP+	4 x SFP+	Up to 48 x SFP+	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)
Fiber SFP (100/1000)	-	-	Up to 120 x SFP	4 x SFP	4 x SFP
Power over Ethernet	-	-	Up to 144 x PoE+ / UPOE	-	-
PoE Budget (Watts)	-	-	Up to 6,000W	-	-
Redundant Power Supply	Dual hot swap PSUs	Dual hot swap PSUs	N+1 PSUs	RPS + Modular PSU	RPS + Modular PSU
Feature Set	Layer 2+ (static routing) Optional Full L3 License	Layer 2+ (static routing)	Full L3	Layer 2+ (static routing) Optional Full L3 License	Layer 2+ (static routing) Optional Full L3 License
Form Factor	Rack 1U - Stackable	Rack 1U MLAG	Rack 4U - Chassis	Rack 1U - Stackable	Rack 1U - Stackable
Product Name	**M5300-28G-POE+**	**M5300-52G-POE+**	**M5300-28G3**	**M5300-52G3**	**M5300-28GF3**
Order Number	**GSM7228PS**	**GSM7252PS**	**GSM7328S**	**GSM7352S**	**GSM7328FS**
RJ45 Ports	24 x 10/100/100 2 x 10GBASE-T (Max: 4)	48 x 10/100/100 2 x 10GBASE-T (Max: 4)	24 x 10/100/100 2 x 10GBASE-T (Max: 4)	48 x 10/100/100 2 x 10GBASE-T (Max: 4)	4 x 10/100/100 2 x 10GBASE-T (Max: 4)
Fiber SFP+(1000/10G)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)	2 x SFP+ (Max: 4)
Fiber SFP (100/1000)	4 x SFP	4 x SFP	4 x SFP	4 x SFP	24 x SFP
Power over Ethernet	24 x PoE+ 802.3at	48 x PoE+ 802.3at	-	-	-
PoE Budget (Watts)	380W/720W EPS	380W/1,440W EPS	-	-	-
Redundant Power Supply	RPS + Modular PSU	RPS + Modular PSU	RPS + Modular PSU	RPS + Modular PSU	RPS + Modular PSU
Feature Set	Layer 2+ (static routing) Optional Full L3 License	Layer 2+ (static routing) Optional Full L3 License	Full Layer 3	Full Layer 3	Full Layer 3
Form Factor	Rack 1U - Stackable	Rack 1U - Stackable	Rack 1U - Stackable	Rack 1U - Stackable	Rack 1U - Stackable

Product Name	M4100-50-POE	M4100-D12G	M4100-D12G-POE+	M4100-12GF	M4100-12G-POE+
Order Number	FSM7250P	GSM5212	GSM5212P	GSM7212F	GSM7212P
RJ45 Ports	48 x 10/100 2 x 10/100/1000	12 x10/100/1000	12 x 10/100/1000	12 x 10/100/1000	12 x 10/100/1000
Fiber SFP (100/1000)	2 x SFP	2 x SFP	4 x SFP	12 x SFP	4 x SFP
Power over Ethernet (PoE/PoE+)	48 x PoE 802.3af	Powered by PoE+	10 x PoE+ 802.3at out	4 x PoE+ 802.3at	12 x PoE+ 802.3at
PoE Budget (Watts)	380W/740W EPS	PD Mode	125W	150W	380W
Redundant Power Supply	RPS	1 x PoE+ 30W port in	PD Mode	RPS	RPS
Powered by PoE+ (Passthrough)	-	-	2 x PoE+ 30W ports in Can redistribute 25W	-	-
Feature Set	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)
Form Factor	Rack 1U - Standalone	Desktop	Desktop	Rack 1U - Standalone	Rack 1U - Standalone

Product Name	M4100-26G	M4100-50G	M4100-26G-POE	M4100-24G-POE+	M4100-50G-POE+
Order Number	GSM7224	GSM7248	GSM7226LP	GSM7224P	GSM7248P
RJ45 Ports	26 x 10/100/1000	50 x 10/100/1000	26 x 10/100/1000	24 x 10/100/1000	50 x 10/100/1000
Fiber SFP (100/1000)	4 x SFP	4 x SFP	4 x SFP	4 x SFP	4 x SFP
Power over Ethernet (PoE/PoE+)	-	-	24 x PoE 802.3af	24 x PoE+ 802.3at	48 x PoE+ 802.3at
PoE Budget (Watts)	-	-	192W/380W EPS	380W/720W EPS	380W/1,440W EPS
Redundant Power Supply	RPS	RPS	RPS	RPS	RPS
Powered by PoE+ (Passthrough)	-	-	-	-	-
Feature Set	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)	Layer 2+ (static routing)
Form Factor	Desktop	Rack 1U - Standalone	Rack 1U - Standalone	Rack 1U - Standalone	Rack 1U - Standalone

Product Name	RPS/EPS Unit
Order Number	RPS4000v2
RJ45 Ports	For up to 4 switches
Fiber SFP (100/1000)	
Power over Ethernet (PoE/PoE+)	APS1000W combination
PoE Budget (Watts)	Up to 2,8880W budget
Redundant Power Supply	RPS EPS
Powered by PoE+ (Passthrough)	-
Feature Set	Connects M4100, M5300 and M6100 series
Form Factor	Rack 1U – Four Slots

NETGEAR®

350 E. Plumeria Drive
San Jose, CA 95134
408.907.8000

www.netgear.com