Large surveillance systems
An Allied Telesis, Axis, Genetec and NetApp joint solution guide.

In cooperation with:
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>1.</td>
<td>HP DL 360p Gen8 E5-2650 servers</td>
<td>5</td>
</tr>
<tr>
<td>2.</td>
<td>Genetec Security Centre 5.2</td>
<td>5</td>
</tr>
<tr>
<td>2.1</td>
<td>Configuration</td>
<td>5</td>
</tr>
<tr>
<td>2.1.1</td>
<td>Servers and archivers</td>
<td>5</td>
</tr>
<tr>
<td>2.2</td>
<td>Best practices and recommendations</td>
<td>6</td>
</tr>
<tr>
<td>2.2.1</td>
<td>Directory role</td>
<td>6</td>
</tr>
<tr>
<td>2.2.1.1</td>
<td>Design considerations</td>
<td>6</td>
</tr>
<tr>
<td>2.2.2</td>
<td>Failover directory</td>
<td>6</td>
</tr>
<tr>
<td>2.2.2.1</td>
<td>Directory failover design considerations</td>
<td>7</td>
</tr>
<tr>
<td>2.2.3</td>
<td>Media router role</td>
<td>7</td>
</tr>
<tr>
<td>2.2.3.1</td>
<td>Design considerations</td>
<td>7</td>
</tr>
<tr>
<td>2.2.4</td>
<td>Multicast requirements</td>
<td>7</td>
</tr>
<tr>
<td>2.2.5</td>
<td>Archiver Role</td>
<td>8</td>
</tr>
<tr>
<td>2.2.5.1</td>
<td>Design considerations</td>
<td>8</td>
</tr>
<tr>
<td>2.2.6</td>
<td>Storage</td>
<td>8</td>
</tr>
<tr>
<td>2.2.6.1</td>
<td>Recommended archiver hard drive configuration</td>
<td>9</td>
</tr>
<tr>
<td>2.2.7</td>
<td>Failover archiver role</td>
<td>9</td>
</tr>
<tr>
<td>2.2.8</td>
<td>Optimizing Windows</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.1</td>
<td>Antivirus configuration</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.2</td>
<td>Windows firewall</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.3</td>
<td>Windows update</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.4</td>
<td>Uninstalling unwanted programs</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.5</td>
<td>Disabling the screen saver</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.6</td>
<td>Disabling Power management</td>
<td>10</td>
</tr>
<tr>
<td>2.2.8.7</td>
<td>Display resolution</td>
<td>10</td>
</tr>
<tr>
<td>2.2.9</td>
<td>Optimizing Security Centre</td>
<td>10</td>
</tr>
<tr>
<td>2.2.9.1</td>
<td>Windows</td>
<td>11</td>
</tr>
<tr>
<td>2.2.9.2</td>
<td>Disk imaging</td>
<td>11</td>
</tr>
<tr>
<td>2.2.9.3</td>
<td>Network</td>
<td>11</td>
</tr>
<tr>
<td>2.2.9.4</td>
<td>Security Center servers</td>
<td>11</td>
</tr>
<tr>
<td>2.2.9.5</td>
<td>Update drivers</td>
<td>11</td>
</tr>
<tr>
<td>2.2.9.6</td>
<td>Configuring scheduled backups</td>
<td>11</td>
</tr>
</tbody>
</table>
3. Netapp Storage
   3.1 Configuration of SAN 12

4. Allied Telesis Network
   4.1 Network configuration 14
   4.2 Basic concepts and best practices 15
      4.2.1 Power Over Ethernet (PoE) 15
      4.2.2 Multicast 15
      4.2.3 Quality of Service (QoS), 17
      4.2.4 Virtual LAN (VLAN) 18
      4.2.5 Network Consolidation 19
      4.2.6 Network Resiliency 21
Overview

Today, large IP Video Surveillance Systems (VSS) consisting of over 1000 cameras are becoming more common. Such a network, supporting a significant number of end-users, needs to be very reliable, manageable, and scalable. Such applications are often found in several facilities:

- City or municipal street and public surveillance networks
- City or municipal traffic monitoring networks
- Transportation and transit line networks
- Large education campuses (college, university)
- Large business parks
- Large retail malls
- airports
- Other high security installations

Recognizing the interest and importance of experience with large VSS, Axis hosted a global technical conference in corporation with global partners\(^1\) to setup two large VSS’s, using different state-of-art technologies, with the aim to test and identify critical components, establish a set of best practices for network design, configuration, reliability, scalability, and troubleshooting. Together with the partners the findings are presented in a set of white papers as solution guidelines for system integrator and engineers.

The two VSS setups vary in both hardware and software. Each network consists of 1000 cameras. Due to logistics limitations we have decided to separate the two VSS as indoor and outdoor setups. It is important to know that the naming of the 2 systems depends only on the cameras. In the outdoor system both indoor and outdoor Axis cameras are used, whereas in the indoor system only indoor cameras were used. The other components in the VSS works well with both indoor and outdoor installations.

This paper describes the indoor surveillance system that was setup during the conference. The indoor surveillance system is a joint solution deploying hardware from multiple partners consists of HP VMware server configuration, with Genetec VMS on top, NetApp SAN storage solution and Allied Telesis network solution. In this paper we will present the actual configuration implemented by each partner. We will also bring up basic concepts and best practices provided by the partners within networking, storage and VMS.

\(^1\) Including HP, NetApp, Allied Telesis, Genetec, Milestone, ABB, Weidmuller, Microsemi, Moodifier, Veracity, Firetide and Raytec
1. **HP DL 360p Gen8 E5-2650 servers**

One server ran Windows Server 2008 with Axis Virtual Camera, AVC and NetApp SANtricity 10.84 on top. The SANtricity management client configured and administrated the NetApp E-5460 storage system installed in the core of the indoor network.

On each of the remaining five servers, VMware ESXi 5.1.0 U1 in an HP branded release was installed as the hypervisor. Four of the servers were virtualized into four virtual machines running Windows Server 2008 with Genetec Security Center 5.2 VMS on top. The fifth server had the same set up, but was virtualized into five virtual machines for a total of 21 VM’s. Each virtual machine had a file archivers with 240 Mb/s throughput per archiver handling 50 cameras per archiver.

2. **Genetec Security Centre 5.2**

2.1 **Configuration**

Genetec Security Center 5.2 GA software was used for the conference. In order to recreate the processing and bandwidth demands of a 1000 cameras system, more than 75 physical cameras was installed and distributed at Axis Communications HQ in Lund, Sweden. In order to simulate the load of a 1000 camera system, the Axis Virtual Cameras software was used to simulate the remaining cameras by replicating the physical ones.

2.1.1 **Servers and archivers**

As stated, each virtual machine hosted one archiver and each archiver was configured to record on the Netapp storage. 5.5 TB was dedicated per archiver.

Furthermore, SQL Express was used for the directory and for each archiver database. The database was stored locally on each archiver in order to improve performance.

Due to the limited time scope of the conference, no Failover directory and archiver were deployed for this set up. However, we strongly recommend for a project with 1000 cameras or more to have redundancy in place.

As an archiver can handle 240 mbps of total throughput in a virtualized environment, 21 archivers are necessary to handle 1000 cameras, assuming an average bit stream of max 5 mbps per camera.

Genetec recommends the following minimum system requirements for the archivers:

- Quad core intel Xeon E5640 2.66 Ghz or better
- 8 GB of RAM or better
- 80 GB SATA II hard drive or better for the OS and Security Center applications
- Standard SVGA video card
- 1024x768 or higher screen resolution
- 100/1000 Ethernet network interface card
- DVD ROM drive
- Windows Server 2008 SP2/R2 (64-bit)
2.2 Best practices and recommendations

2.2.1 Directory role

The Directory role identifies the Security Center system. Only a single instance of this role is permitted on a system. The server hosting the Directory role is called the main server, and it must be set up first. All other servers added to the system afterwards are called expansion servers and must connect to the main server to be part of the same system.

The Directory role takes care of the following system functions:
> Client application connection authentication
> Software license enforcement
> Central configuration management
> Event management and routing
> Audit trail and activity trail management
> Alarm management and routing
> Incident management
> Scheduled task execution
> Macro execution

2.2.1.1 Design considerations

Security Center Directory 5.x was designed to support up to 2 million entities. In practice it has been tested with 300 000 entities. If there are more than 300 cameras in the solution, installation on a stand-alone machine is mandatory.

2.2.2 Failover directory

The failover directory solution built in the Security center can provide hot standby and load balancing simultaneously. It can thereby protect up to 5 failover directories at once. Therefore, the end user no longer has to worry about which Directory to connect to as the system will automatically connect to the least busy Directory.

To simplify the user experience, Security Center also offers two mechanisms for database synchronization: backup and restore mode and SQL mirroring. The backup and restore mode consists of transferring the primary database to the Failover Directory servers at a pre-defined interval and the SQL mirroring mode offers continuous synchronization.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Backup and Restore</th>
<th>SQL Mirroring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic Failover</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Loss / Failover</td>
<td>Up to the last backup</td>
<td>No</td>
</tr>
<tr>
<td>Data Loss / Failback</td>
<td>Yes, if no manual backup</td>
<td>No</td>
</tr>
<tr>
<td># Entities / System</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td># Clients / Dir</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>SQL Requirements</td>
<td>SQL Express</td>
<td>SQL Standard</td>
</tr>
<tr>
<td>DB Servers</td>
<td>Hosted on Genetec servers</td>
<td>Any server</td>
</tr>
<tr>
<td>Management</td>
<td>Directory Manager Role</td>
<td>SQL Mirroring (witness)</td>
</tr>
<tr>
<td>Client Disconnection</td>
<td>Dir connection + 1 min</td>
<td>No</td>
</tr>
</tbody>
</table>

For small budget (no need for SQL standard) where customers have some tolerance for data losses, the built-in Failover Directory is a good choice.
2.2.1 Directory failover design considerations

<table>
<thead>
<tr>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of failover directories</td>
<td>5</td>
</tr>
<tr>
<td>Number of entities on FOD systems</td>
<td>Same as Directory</td>
</tr>
</tbody>
</table>

Note: There is no limitation to the number of cameras in a system utilizing failover directory for either failover option; Backup and Restore and SQL mirroring. There is no real-time synchronization while using the backup and restore option in Security Center. Scalability is not a problem either for SQL Mirroring.

2.2.3 Media router role

The Media Router is an Omnicast specific role that ensures that all video streams use the most optimal route to get from their source to their destinations, while performing any necessary transformation (for example, from unicast to multicast, or from IPv4 to IPv6).

2.2.3.1 Design considerations

<table>
<thead>
<tr>
<th>Limit</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of media router per system</td>
<td>1</td>
</tr>
<tr>
<td>Number of redirectors per server</td>
<td>1</td>
</tr>
<tr>
<td>Number of streams</td>
<td>300</td>
</tr>
<tr>
<td>Maximum throughput</td>
<td>300 mbps</td>
</tr>
<tr>
<td>Maximum timespan for export</td>
<td>1 day</td>
</tr>
</tbody>
</table>

2.2.4 Multicast requirements

- IGMP v2 or IGMP v3 Snooping shall be enabled on all VMS network switches. The IGMP version enabled in the switches must match the IGMP version on the cameras, servers, and clients.
- An IGMP Querier must be present on a single switch on the VMS network. If there are multiple subnets, each one must have their own IGMP Querier.
- If multicast routing is required, then recommended protocol is PIM-SM (Sparse Mode), RFC 4601. This may also be referred to as Data-Driven.
- The switches must support and have allocated enough IGMP groups for the Genetec system. These groups are used for the following:
  - Camera streams
  - Sequences
  - Analog Monitors
  - Video Walls
  - Multicast test address
  - When multicast groups are routed, the total number of groups in the same switch will be multiplied by the number of VLAN routes.

Example: If a single multicast group is routed between 3 VLAN’s in the same switch, it counts as 3 multicast groups to the total amount supported by that switch.
2.2.5 **Archiver Role**

The Archiver role is responsible for the discovery, command & control, and status polling of video units. All communications between the system and video units are established through this role.

All events generated by the units (motion, video analytics) are forwarded by the Archiver to the concerned parties on the system. The Archiver also manages the video archive and performs motion detection on video units that do not support this feature.

2.2.5.1 **Design considerations**

The following table lists the upper limit capacities of the Archiver based on bit rate and network capabilities:

<table>
<thead>
<tr>
<th>Server</th>
<th>Server Spec</th>
<th>Directory and Archiver (Video only)</th>
<th>Archiver (Video only)</th>
</tr>
</thead>
</table>
| Low    | >Intel Core 2 X6800 @ 2.93 GHz  
>2 GB of RAM  
>80 GB hard drive for OS and Security Center applications  
>256 MB PCI-Express x16 dual-head video adapter  
>1280 x 1024 or higher screen resolution  
>100/1000 Ethernet Network Interface Card  
>16x DVD ± RW Drive | Up to 50 cameras or 50 Mbps of throughput | Up to 75 cameras or 75 Mbps of throughput |
| Medium | >Intel Core i7 870 @ 2.93 GHz  
>8 GB of RAM DDR3  
>80 GB SATA II hard drive for OS and Security Center applications  
>512 MB PCI-Express x16 dual-head video adapter  
>1600 x 1200 or higher screen resolution  
>100/1000 Ethernet Network Interface Card  
>16x DVD ± RW Drive | Up to 100 cameras or 150 Mbps of throughput | Up to 150 cameras or 200 Mbps of throughput |
| High   | >Intel Core i7 2600 @ 3.4 GHz  
>8 GB of RAM DDR3  
>80 GB SATA II hard drive for OS and Security Center applications  
>1 GB PCI-Express x16 dual-head video adapter  
>1600 x 1200 or higher screen resolution  
>100/1000 Ethernet Network Interface Card  
>16x DVD ± RW Drive | Up to 100 cameras or 200 Mbps of throughput | Up to 300 cameras or 300 Mbps of throughput |

Please note additional considerations for server specifications that can affect maximum capacities listed:

- When video streaming is not in multicast from the camera, the maximum throughput calculation must include camera streams being redirected by the Archiver.
- Unit based motion detection must be used to achieve maximum capacity.
- Software based motion detection could reduce the maximum capacity by as much as 50%.
- Watermarking could reduce the maximum capacity by as much as 20%.
- Systems above 300 cameras or doors must isolate the Directory on a dedicated server.
- A more powerful server than the high end specification will not necessarily increase the maximum capacity.
- Maximum capacity of a virtual machine with the exact same specifications as the proposed physical machine is reduced by 20%.
- 2 dedicated Network Interface Card (NIC) should be assigned per instance of the Archiver Role when using virtualization, one will be used for the camera network and another one for the storage.
- Virtual machine must run on Windows Server 2008 R2.
- In case of video redirection (Multicast by archiver) Maximum concurrent redirection throughput is 150Mbs.

2.2.6 **Storage**

The Security Center system writes to the volumes until they are full. Once all designated storage space is consumed, the archiver will start deleting and re-writing.
Over time, fragmentation will occur on the drives which will affect the speed of the writing and reading, and since defragmenting the drive is NOT an option, the smaller the drive is, the less fragmentation will occur and the better the performance will be.

Another good reason why we don’t recommend a volume greater than 8TB is related to performance of the NTFS file system itself. The default configuration of Omnicast is to create a video file every 20 minutes with a folder by day for each camera.

Example:
> Recording for 90 days of retention across 200 cameras
> 90x200 = 18,000 folders
> 3 x 24 x 90 x 200 = 1,296,000 files

When browsing a volume in this example, the speed will be sluggish and the performance degraded. For this project we deployed 5.5 TB per logical drive.

2.2.6.1 Recommended archiver hard drive configuration

> New Technology File System (NTFS) is preferred file system for archiving
> The preferred New Technology File System (NTFS) cluster size is “largest available”
> Storage –level disk compression is not recommended
> A minimum of 2 logical drives per Omnicast Archiver
> A maximum of 4 TB to 8TB per logical drive
  – As a general rule, we should have at least 0.2% of the Total Disk Size set as the Min. free space; in other words, about 1 GB for every 500 GB). Try to increase it if it is small

**Note:** These recommendations reduce the impact of fragmentation on system performance as one logical drive can be defragmented while the other is in use.

> Do not create multiple partitions on the same disk (logical drives) and use them for archiving
> Do not archive on the same disk used to run Windows. Using the same disk could crash Windows due to Windows running out of disk space
> Archiving disk must be dedicated to the Archiver and must not be used by other software
> Do not allocate the same disk to multiple Archivers
> If archiver backups are enabled, they must not be done on the same physical disk as the one recording the original video
> It is recommended to deactivate the indexing service on the video archiver drive(s)

2.2.7 Failover archiver role

When using Failover Archivers in Security center, the failover scheme is 1:N where N should not exceed 3 (it should be noted that this is good practice to get 99.9% of availability, not a software limitation).

Like the Omnicast Primary Archiver Failover Archivers can handle a maximum capacity of 300 cameras or 300Mbps this includes the number of cameras protected by a failover archiver.

With a Failover Camera license you can install as many Archiver as you need. There is no limitation on the number of Failover Archivers in Security Center.

It is not possible to failover onto the base package machine.

In Security Center the failover servers per Archiver role is 2.
2.2.8 Optimizing Windows

2.2.8.1 Antivirus configuration
If the Security Centre servers and workstations require an antivirus application installed, it is necessary to configure exclusions. We also recommend to disable features such as "automated scans" & "Scan upon definition update", as well as any network monitoring or firewall services bundled with the antivirus software. We also recommend to configure exclusions on the antivirus for:

> The video files location
> The SQL database and where the logs are being stored
> The location where the Omnicast server and client software is installed

2.2.8.2 Windows firewall
A firewall is a software or hardware that checks information that comes from the internet or from a network, depending on the settings, will either block the information or let it through. A firewall can help prevent malicious software (such as worms) from gaining access to your computer.

If the Security Centre servers and workstations require a windows firewall enabled, we recommend to create exceptions for Security Centre server and client exe files.

2.2.8.3 Windows update
Normally, Windows has the updates set on automatic, so it will immediately download and install them, pushing changes to your PC, especially in its major components.

If Security Center server or workstation is connected to the Internet, these updates will automatically download and install. This will initiate a restart of the Windows system without proper planning. In this case, it is recommended to use the "notify me but don’t automatically download or install them" feature. It is also recommended to have a maintenance plan in place that covers upgrading the machine periodically.

If Security Centre server or workstation is not connected to the Internet, it is recommended to have updates pushed through the local network. It is also recommended to have a maintenance plan in place that covers updating the machine periodically.

2.2.8.4 Uninstalling unwanted programs
Many PC manufacturers pack their computers with programs you might not want. Keeping the software on your computer might slow it down by using precious memory, disk space, and processing power.

We recommend to uninstall all the unused programs on the server. This should include both manufacturer – installed software and software you installed yourself but don’t want anymore, especially utility programs designed to help manage and tune the computer’s hardware and software. Utility programs such as virus scanners, disk cleaners and backup tools often run automatically at start-up, quietly taking up precious resources in the background where you can’t see them. Often the end user has no idea they are even running.

2.2.8.5 Disabling the screen saver
Turning off the screen saver is recommended on client workstations to improve performance and CPU usage. The default screen saver should be kept on Security Centre servers.

2.2.8.6 Disabling Power management
The “Always on” power scheme should be set on servers/workstations used for video walls.

2.2.8.7 Display resolution
Using the monitor’s native resolution is recommended. This can be achieve by selecting the highest available resolution in the computer display settings.

2.2.9 Optimizing Security Centre
In every video management system ensuring all configurations are set to their optimal settings is a vital step.
2.2.9.1 Windows
   > A 64 bit operating system is recommended to run all Security center applications and services
   > Security Center must not be installed on a domain controller
   > If client applications are used for testing purposes on the servers, they must be exited upon finishing to save resources

2.2.9.2 Disk imaging
   > Disk imaging is not supported

2.2.9.3 Network
   > Static IP addresses are recommended for Security center servers and video units. Avoid using DHCP
   > If VLANs are being used, all VLANs must be managed by the network equipment, not the servers or clients. VLAN tagging in Windows is not supported
   > Windows may be used as an IGMP querier on a 3rd party server not running Security center. IGMP querying must be done on the network level if otherwise

2.2.9.4 Security Center servers
   > No other hosting applications should be running in parallel with Security Center (example: web servers, FTP servers, domain)

2.2.9.5 Update drivers
Update all hardware drivers to the latest version supported by the manufacturer on all Security center servers and workstations. These drivers should be downloaded from the manufacturer’s website (e.g. HP, Dell etc) opposed to the hardware component’s website (e.g. NVIDIA, Intel etc.)

The most important drivers are:
   > Video (video cards and Direct X)
   > Network (NICs)
   > Chipset

2.2.9.6 Configuring scheduled backups
Setting up scheduled backups is an important set in any Security Centre environment. These backups hold key system information such as database and registry information. In case of system failure you will always be able to return your system to a previous backed up state.
3. Netapp Storage

3.1 Configuration of SAN

The NetApp storage system hardware used at the Axis Global Technical Conference was based on the E5400 controller model and came equipped with the following:

- A 4U 60 disk chassis
- Dual redundant storage controllers
- Four 10Gbit iSCSI ports
- 58 3TB NL-SAS disks
- Two 800GB SSD disks

The 58 NL-SAS disks were setup as 11x RAID5 Volume Groups with five disks per group. Each group had two volumes of approx. 5.6TB of capacity. Three disks were saved for hot swappable spares.

The two 800GB SSD disks were setup as a RAID1 Volume Group with two disks. One 700GB volume was created from that group.

The 22 volumes made from the NL-SAS disks were used as Archive volumes for the camera feeds. The one volume made from SSD disks were used by the VMware ESX hosts to store and boot virtual machines from.

Each volume was then mapped to a specific host, both physical and virtualized. In this particular case the ‘VMLUN’, made from the SSD disks, was mapped to the ‘GTC_Genetec’ Host Group. By mapping to the Group level both physical VMware servers could access and use the volume.
The 'Archive' volumes were mapped to each active Archiver/virtualized Windows host. Once the volumes were mapped, each Archiver detected the new volume and it was configured for use via Security Centre.

After verifying functionality a number of physical and simulated cameras were configured and activated. Below is a screen shot showing the load generated by the setup, where according to Genetec, around 300 cameras were active at the time. Each active volume group showed between 1.7MB/s and 18MB/s and the combined utilization of the storage was around 43MB/s (360Mbit/s out of a possible 24Gbit/s).
4. **Allied Telesis Network**

In this chapter we will describe the reference network solution that was deployed using Allied Telesis network equipment and network concepts highlighted by Allied Telesis.

4.1 **Network configuration**

To support the IP video network and enable remote camera control and operation, a high-speed IP/Ethernet network is required with its design and functionality tailored to IP video applications.

The requirements for this kind of network infrastructure are best met by a network design in which different services are split into different VLANs, and transported over resilient links or rings protected by an extremely fast failover mechanism.

The Allied Telesis fast failover network protection solutions are the Ethernet Protected Switched Ring (EPSR) and Virtual Chassis Stack (VCStack). These are extremely reliable, high-performance protection mechanism that can restore connectivity within 50ms of a link failure being detected. Services such as IP video surveillance can each be provisioned with one or more VLANs running over the EPSR rings or Aggregated Links (LAGs) with data on Layer 2 or Layer 3 switched between the rings, the links and the central site facility.

A reliable, scalable design is achieved by subtending multiple rings of various SwitchBlade x908s or SwitchBlade x8112s with VCStack providing the gateway between the rings and central site.

This network design is very scalable, potentially providing extremely reliable network services to thousands of cameras, and hundreds of network devices, such as monitors encoders or digital video recorders. When multiple services share the same network infrastructure, it is necessary to guarantee the Quality of Service expected, ensuring timely delivery of traffic and access to applications when required.

Bandwidth usage must be controlled, so no individual service can starve the others of bandwidth. Moreover, for loss and jitter-sensitive applications like video, it is extremely important to be able to deliver the data streams in a smooth, lossless fashion.

The Allied Telesis SwitchBlade x908, SwitchBlade x8112, and x900 Series switches are extremely feature-rich Quality of Service offerings that can manage the characteristics of over 1,000 separate data streams simultaneously, thereby making them ideal for the provisioning of shared service networks involving real-time applications.

Robust access switches as GS95016/PS WebSmart network switches features PoE+ for connectivity with security cameras integrating simplicity with the performance and reliability of managed switch; thus providing an inexpensive yet secure and reliable solution for users to integrate management at the edge networks.
4.2 Basic concepts and best practices

4.2.1 Power Over Ethernet (PoE)

PoE technology is composed by two elements, a Power-sourcing-Equipment (PSE) providing the power and a Powered Devices (PD).

<table>
<thead>
<tr>
<th>Class</th>
<th>Power usage</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.44 W to 12.95 W</td>
<td>default – IEEE802.4af</td>
</tr>
<tr>
<td>1</td>
<td>0.44 W to 3.84 W</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3.84 W to 6.49 W</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6.49 W to 12.95 W</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>12.95 W to 25.50 W</td>
<td>IEEE802.3at</td>
</tr>
</tbody>
</table>

PoE is referred to devices supporting class from 1 to 3 while PoE+ to devices supporting Class 4 and below.

The main PoE related parameters in a network design are the **total power budget** available on the switch – and the **guarantee power per each port**.

During planning, it is required to verify the PSE and PD classes so that a PSE equipment is always able to provide the power required by the connected PD device.

To create a future-proof network it is preferable to rely on switches IEEE802.3at capable.

4.2.2 Multicast

There are three types of communication between IP Cameras and other Video devices in a network:

- **Unicast** - the IP Camera address directly the streaming to another Video device
- **Broadcast** - the IP Camera address the streaming to all Video devices
- **Multicast** - the IP Camera the streaming to a select group of Video devices

**Unicast** is great for communicating directly between one source and one destination e.g. IP camera to VMS - however when the destination are more than one, unicasting becomes inefficient, the same information need to be transmitted multiple times consuming bandwidth.

**Broadcast** communication is used once you need to communicate with all the devices in a network, using a special broadcast address the same information is sent to all the network member. Useful in specific situation may overload the receiving device.

**Multicast**, transmit the information only to client interested in receiving it without consuming more bandwidth. Client requiring a specific information from a specific source ask to be registered to the multicast group and receive the information.
Figur 6. Unicast vs. Multicast – Unicast transmission sends a separate stream of data to each receiver, while multicast transmission sends one stream of data that is separated as it passes through the routers and sent on to the receivers.

To ensure that the information is not duplicated within a link it is necessary to coordinate the action of all the actors: the transmitter, the receiver and the switch. This is performed through multicast host router signaling protocol called Internet Group Management Protocol (IGMP). Internet Group Management Protocol (IGMP) in IPv4 networks control and limit multicast traffic through a network through the use of query and report messages between destinations and sources.

Three IGMP version has been defined: IGMPv1, IGMPv2 and IGMPv3.

IGMPv1 was the first version to become an Internet Standard.
IGMPv2 adds support for "low leave latency" to improve the performances in a multicast network, easily discovering when no more members are present on a network segment.
IGMPv3 adds support for "source filtering", permitting to minimize the information exchange to a subset of the available sources.

IGMP is a communication between destination and source. To optimize the network performances a switch must be able to check the IGMP packets and take actions to forward or not a specific stream to a specific port or network segment. This feature called IGMP snooping is mandatory in the efficient network.

In the same way that IGMP manages multicast groups for IPv4, MLD works with IPv6. As for IGMP the IPv6 switch must be able to check and analyze the MLD packet. This capability required for an efficient IPv6 network is called MLD snooping.

Increasing the network complexity can be required to transmit multicast between different IP subnet and to maintain the same efficiency guarantee by the IGMP protocol.

The transmission between different subnets is supported by the multicast routing protocols responsible for constructing distribution trees and forwarding multicast packets. There are a number of different routing protocols, but they generally follow one of two basic approaches – Dense Mode or Sparse Mode.

Dense Mode protocols are based on the assumption that there are a number of multicast group members densely distributed across a network. The Dense Mode is supported by Distance Vector Multicast Routing Protocol (DVMRP) that is the widest used or by the Protocol Independent Multicast Dense Mode (PIM-DM) is both an IPv4 and an IPv6 routing protocol, operates in a similar fashion to DVMRP and is best suited to situations where there are numerous members for each multicast group Sparse Mode protocols are based on the assumption that group members wanting to receive multicast data are sparsely distributed across a network and that bandwidth is not necessarily widely available. The sparse...
mode is supported by **Protocol Independent Sparse Mode (PIM-SM)** is both an IPv4 and an IPv6 routing protocol and implement RFC 2715 "Interoperability Rules for Multicast Routing Protocols". For IPv4, this means that PIM-SM, PIM-DM and DVMRP can operate at the same time on different interfaces, and for IPv6, this means PIM-SM and PIM-DM can operate at the same time on different interfaces.

### 4.2.3 Quality of Service (QoS)

Any switch is equipped with LAN ports connected to the devices and WAN port connected to the network aggregation or core devices of the network. In the considered DVS network the access switches LAN port are connected to the IP cameras while the WAN ports are connected to the core switch.

The access switches are designed to provide a large number of LAN ports and a limited number of WAN ports, creating a blocking architecture. In a switch with 24 Gigabit LAN ports and 4 Gigabit LAN port it may happen that the WAN port are not able to manage all the traffic coming from the LAN ports or to increase the latency of some packets.

In a network transporting video streams latency and packet lost are not allowed so it is necessary to find a way to minimize the latency and avoid packet lost at least for the video streams.

**Quality of Service in a switch** is the capability to understand the traffic type incoming and decide how to manage it.

The QoS functionality classifies the incoming data flow, assign to each packet a priority and manage the packet according to the priority. Applying QoS and giving multicast data packets priority over other packets when processed by the network switch or router avoid packet los and minimize the latency.

**QoS Mechanisms** – Perhaps the simplest and most obvious way of providing a high service level without congestion is by over-provisioning a network without any QoS mechanism. This is very expensive because requires to build a network from the outset that is designed to cope with all traffic, now and in the future.

Moreover any change in the future will impact on the network traffic and the overprovisioning can become no more valid.

**QoS at Layer 2 – 802.1Q**

IEEE-802.1P, involves the addition of a user priority field to the IEEE-802.1Q VLAN (Virtual Local Area Network) header. The three bit field gives 8 levels of priority and offers a simple QoS mechanism for Layer 2 switches.

**QoS at Layer 3 – the Type of Service Field**

An early attempt to introduce QoS into IP (Layer 3) was the TOS (Type of Service) field. It has now been superseded by the DiffServ model.

**Architectures for QoS**

The priority field methods alone are not satisfactory for large and complex networks. To properly support multimedia real-time applications it is necessary to go to an architecture that actively controls traffic. The two methods developed for IP networks are Integrated Services (IntServ) and Differentiated Services (DiffServ).

> **IntServ** – Integrated Services essentially defines an end-to-end pathway through a network for each application’s packets using Resource Reservation Protocol (RSVP). Each switch in the network relay on this info to manage the traffic

> **DiffServ** – In this model traffic is classified into flows and marked, using the DiffServ field (same bits as the TOS) performing an admission control mechanism at the entry point of a network
No further classification or profiling is required or performed inside the network. In this way the most intensive classification and profiling of traffic occurs near the edge of the network, with this function performed on ingress.

Allied Telesis Layer 3+ switches support the RSVP protocol and are eminently suitable for classifying traffic on a per flow basis and therefore able to support the IntServ methodology, but DiffServ is predominantly used and it is extremely well supported by Allied Telesis Layer 3+ switches.

QoS and Queuing

Queue management is fundamental to QoS. It enables bandwidth control, and ensures that traffic is dealt with as its priority requires.

Implementation of QoS in Allied Telesis Products

Allied Telesis’ products support the full QoS suite, from IEEE-802.1P within the IEEE802.1Q tag at Layer 2, to the TOS field, RSVP (RFC 2205), IntServ Controlled Load Service Class (RFC2211), and the DiffServ architecture (RFC 2475). Allied Telesis high-end Layer 3 switches provide full classification and re marking capabilities based on the DiffServ Code Point (DSCP) as well as source and destination Layer 2 (MAC), Layer 3 (IP / IPX), and Layer 4 (TCP / UDP port) addresses. In addition classification can take place on the Ethernet encapsulation type and protocol, as well as VLAN source and destination addresses.

This very advanced classification capability operating in the data plane of Allied Telesis’ switches enables very advanced traffic classification based on the type of traffic, its source, and priority.

This means that network designers can roll out different service levels to their networks based on service charge, as well as implement admission control, consistent with the overall DiffServ philosophy.

Operating on top of these, in the control plane is Allied Telesis’ full suite of routing protocols (OSFP, BGP4, RIPv1, RIPv2, and IS-IS). These protocols complement the extensive QoS capabilities of the switches and make them ideal for a wide variety of networks, from large to small.

Traffic classification is complemented by extensive queuing capability, with eight priority queues at the output ports, supporting the full 8 802.1P TOS levels. The Random Early Discard (RED) curve features that are built into the queues enhance congestion control further and work extremely well in conjunction with the TCP suite, which ‘backs off’ sending packets when it detects that packets have been discarded, and so automatically manages network congestion.

To ease congestion, large packet buffering memory within the switches assists in ‘smoothing’ out peaks in traffic through the switch.

In the Allied Telesis QoS model, traffic is classified into flow groups and traffic classes, and policies are applied to these. Each policy has a weighted fair bandwidth distributor queuing mechanism that operates to guarantee minimum bandwidths, and enforce maximum bandwidths. The ability of Allied Telesis switches to provide min/max bandwidth guarantees means that a network provider can guarantee service levels to users. The queuing also acts to distribute bandwidth between the traffic classes, so as manage bandwidth across the switch. Hence, admission control can be effectively applied to users.

4.2.4 Virtual LAN (VLAN)

In simple terms, a VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN. It means that:

- Broadcast packets sent by one of the workstations will reach all the others in the VLAN
- Broadcasts sent in the VLAN will not reach any workstations that are not in the VLAN
- Broadcasts sent not in the VLAN will never reach workstations that are in the VLAN
- The workstations can all communicate with each other without needing to go through a gateway
- The workstations can communicate with each other using non-routable protocols
The basic reason for splitting a network into VLANs is to reduce congestion on a large LAN. The early solution to this problem was to segment the network using routers. This would split the network into a number of smaller LANs. There would be less workstations on each LAN, and so less congestion.

As switches became more available, there was a move from chained hubs to a set of hubs connected to a switch. A switch only sends traffic to a given port if the traffic has to go to that port. Therefore, switches have the effect of reducing congestion at workstations by stopping the workstations from seeing all the traffic from the other ports of the switch.

A simple switched network, though, still needs routers to set the boundaries of where broadcasts are sent (referred to as “broadcast containment”).

The above figure introduces the concept of a LAN segment. This is also referred to as a collision domain. Each LAN segment consists of all the devices attached to a single switch port - the switch stops packets from different ports from colliding with each other.

**Advantages of using VLANs**

- **Performance.** Routers that forward data in software become a bottleneck as LAN data rates increase. Doing away with the routers removes this bottleneck.
- **Formation of virtual workgroups.** It is relatively easy to put all the IP Cameras working together on a particular project all into a single VLAN. They can then more easily share resources with each other.
- **Greater flexibility.** When IP Cameras move around the place if the VLANs are set up the right way, they can plug their Cameras in at the new location, and still be within the same VLAN. This is much harder when a network is physically divided up by routers.
- **Ease of partitioning off resources.** If there are servers or other equipment to which the network administrator wishes to limit access, then they can be put off into their own VLAN. Then users in other VLANs can be given access selectively.

**4.2.5 Network Consolidation**

In the past the paradigm was one service—one network for different reason. The media used by the services was different, e.g coaxial cable for CCTV and Ethernet cable for the IP network.
With the technology evolution a lot of services are now migrating in the IP Ethernet direction, so that the Ethernet can be now considered as the universal transport for large part of the available services.

Despite the use of a single technology there are still concerns in use a unique network to transport the services because are usually managed by different teams and requires different security levels.

On the other side the use a single network minimize the cost and is becoming mandatory for the ICT.

The capability to serve different services within a single physical network without impacting performances and security is called **Network Consolidation**.

To consolidate services within a single network it is required to virtually insulate the different networks using VLAN at layer 2 or also using Virtual Routing Protocol (VRP) at layer 3.

Moreover it is required that the network is protected and that any user connected to a switch port can access only the permitted resources. This capability go under the name of Network protection.

**Network protection**

It’s not simply security or firewalling. A mission critical network, like a consolidated one, must be properly protected along its perimeter not only at the internet connection point – it is well known that most threats come from inside rather than outside the company. Therefore it is becoming more and more mandatory to perform access control at every LAN port rather than only at wireless access points.

Software and security companies like Microsoft and Symantec already provide access control and protection architectures and systems aimed at integrating into a single framework the server and application access control as well as the physical access control performed by the access LAN Switches.

**Tri-Authentication and centrally controlled VLAN assignment**

Allied Telesis Tri-Authentication technology, (Microsoft and Symantec certified and available on every AlliedWare+ powered switch), implements the enforcement point challenging every device that tries to access the network with an authentication procedure that can be IEEE 802.1x, web based or just MAC address based for the basic devices like old printers.

Once the device has been authenticated and identified with either method, the LAN port to which it is connected will be automatically assigned the VLAN that the network manager decided to associate to that specific device.
In a consolidated network environment, Tri-authentication usefulness goes far beyond the protection against unauthorized access. If we consider it as a mechanism for centrally managing the automatic association of every device to its own VLAN, the process of device installation and connection to the network becomes much simpler and error proof because there will be no more a specific port to which the device shall be connected but every LAN port will be the right one. This way a surveillance camera will always be associated to the surveillance virtual network while every other device won’t, regardless of which port is used.

Another positive by-product is the reduction of installation costs because of fewer mistakes and because the installation task can be handled by less experienced staff.

**Consolidation vs. Virtualization**

These two terms are often used as synonyms and at a glance they may look that way, at a deeper analysis they’re not. Virtualization mainly refers to a set of technologies that allow decoupling the physical aspect of an infrastructure from the way it is used and looks like. Virtualization lets you split a physical resource in many virtual resources multiplying the times and ways it can be used. Virtual memory, virtual machines, virtual servers and virtual LANs are examples of ”virtualization” technologies and considered today commodities that every ICT infrastructure can provide.

Consolidation is something more; talking about consolidation is talking about the service and the business that an ICT infrastructure supports. The difference between virtualization and consolidation is someway similar to the difference between moving goods and managing logistics. Moving goods is just one element of logistics in the same way that a virtualization capable network is just the foundation of a consolidated network infrastructure. Therefore ICT managers know very well that without proper network protection mechanisms, a truly resilient architecture, bullet proof per VLAN QoS management and last but not least, VLAN stacking capabilities, there is no consolidation.

**4.2.6 Network Resiliency**

Moving to a Cloud based ICT model is certainly one of the top priorities on most ICT manager’s agenda, and a major challenge too. Flexibility, performance, security, costs and data center are the most frequently occurring and top concerns when evaluating the feasibility of a Cloud approach and defining the migration path.

It almost goes without saying that a consolidated network must be resilient and robust, providing its critical services even in the case of hardware failures. However the resiliency mechanism must be easy to implement, maintain and understand, otherwise troubleshooting a network can be a long and complicated process negatively affecting the Mean Time To Repair (MTTR). In fact the MTTR is made of two values; the time to identify the fault and the actual time to fix it.

While other vendors propose resiliency mechanisms based on an interaction between layer 2 and layer 3 protocols, Allied Telesis Easy Resiliency architecture is pure Layer 2 and relies on two simple to understand technologies: Link Aggregation (or simply LAG) and VCStack.
The cooperation of LAG and VCStack is not only simple and predictable but carries many more benefits that a Layer 3 approach can’t bring.

**Redundancy vs. Resiliency**
Many vendors provide redundant components for increasing reliability. This approach has many drawbacks to be carefully considered.

A redundant part or piece of equipment is usually in hot standby status for most of its lifetime, draining electricity and producing heat but without any contribution to the network. What’s worse is the fact that a resource in standby may well hide a malfunction that will appear and negatively affect network operations, at the critical moment, when the primary parts or devices fail.

This could have been the case of the blackout that has been hitting the Blackberry service recently.

**Failover**
An Allied Telesis network can operate on a large scale at Layer 2 so that you don’t even have to configure complex IP protocols.

The Network reliability is guarantee by the Easy Resiliency solution able to work in either a star or ring architecture.

**Active–Active Architecture**
Allied Telesis Easy Resiliency features an Active–Active architecture in which all physical links and all devices are operational all the time proactively contributing to network performance.

At the same time, since there are no parts in standby, malfunctions or faults are immediately identified and highlighted.

A really green infrastructure - comparing the power consumption of an Active–Active consolidated network to that of a simply redundant network.

If we consider 100% the power drained by a redundant network, an Active–Active resilient network, featuring the same level of performance, will split the traffic between the two branches requiring slightly more than half the power – around 70% at a conservative estimate. Taking into account the savings from air conditioning that can be reduced by 30% as the power consumption. Hence, a simple multiplication of 70% power consumption times 70% of power needed for cooling and the result is 49% consumption meaning a 51% saving. Much more than can be achieved by improving the power efficiency of electronics or, better, that can be added to the savings obtained with green products.

**VCStack™ – Virtual Chassis Stacking**
The VCStackTM in a star topology technology provides a full Active–Active resilient operations. When a fault occurs on any component, the rest of the network will immediately carry packets to destination. The **Active–Active** operations make continuous use of every available piece of electronics: no stand-by
parts, no waste of energy, no added complexity. The Easy Resiliency solution allows use of Link Aggregation (LAG), making possible to increase the available bandwidth simply adding new links to the trunk.

**EPSRing™ – Ethernet Protection Switched Ring**

EPSRing™ is a protection system that prevents loops within Ethernet ring-based topologies. EPSR offers rapid detection and failover recovery rates of less than 50 milliseconds, a rate that is equivalent to that provided by circuit-switched equipment – Carrier Class type protection.

EPSR’s rapid recovery rate enables disruptions in service to go unnoticed in voice, video, or data (Triple-Play). This speedy recovery makes EPSR a more effective alternative to slower spanning tree options when creating resilient Ethernet networks.

EPSR reduces network down time. The key to keeping networks available is extremely fast failover in the event of link or node failure. Many Ethernet networks utilize Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) for preventing loops and assuring backup paths are available. Both protocols are slow to respond to network failures - 30 seconds or more. Today’s networks need a technology that performs better than either STP or RSTP.

EPSR is Allied Telesis’ premier solution for providing extremely fast failover between nodes in a resilient ring. EPSR enables rings to recover within as little as 50ms, preventing a node or link failure from affecting customer experience, even with demanding applications such as IP telephony and streaming video.

EPSR can protect more complex topologies than just a single ring. With the SuperLoop extensions, EPSR can protect a network consisting of any number of rings with multiple points of contact.
About Axis Communications

Axis offers intelligent security solutions that enable a smarter, safer world. As the global market leader in network video, Axis is driving the industry by continually launching innovative network products based on an open platform - delivering high value to customers through a global partner network. Axis has long-term relationships with partners and provides them with knowledge and ground-breaking network products in existing and new markets.

Axis has more than 1,600 dedicated employees in more than 40 countries around the world, supported by a network of over 65,000 partners across 179 countries. Founded in 1984, Axis is a Sweden-based company listed on NASDAQ OMX Stockholm under the ticker AXIS.

For more information about Axis, please visit our website www.axis.com.