Invented for life

BOSCH

BVMS - Network design guide

Author:

Wrobel Maciej (BT-VS/XSW-SEC)

Date:

21 August 2023

Table of Contents

1 Document information 3

2 Introduction 4

2.1 The infrastructure 4

2.2 The application 4

2.3 This guide 4

2.4 Configuration details 4

3 Requirements 5

3.1 Definitions 5

3.2 Requirements 5

4 Understanding a network 8

4.1 The OSI reference model 8

5 Hardware 14

5.1 Manufacturers 14

5.2 Managed and unmanaged equipment 14

5.3 Security 14

5.4 Quality (Class) of Service 17

6 System design 18

6.1 Used ports 18

6.2 Network blueprints 18

7 System monitoring 22

7.1 BVMS internal monitoring 22

7.2 Simple Network Monitoring Protocol (SNMP) 22

8 Troubleshooting 24

8.1 OSI reference model 24

8.2 Tools 24

1 Document information

Project	BVMS
Reference	
Version	41
Last modified	2023, Aug 21 13:22

2 Introduction

2.1 The infrastructure

The network infrastructure for the video surveillance system is similar to a road for a car: you can have a 500.000 EUR Ferarri, but that will not allow you to drive through the desert. The network infrastructure needs to fit the application, in this case a video surveillance system, and can make or break the entire system. This guide should help system architects, designers and installers to prevent network-related issues and troubleshoot network-related issues.

2.2 The application

A video surveillance system is nothing more than an IT application, running on top of an IT infrastructure. This means that the system is depending on IT components, but system functionality can also be expanded using standard IT tools. An example, mentioned in this guide as well, relates to system monitoring. There are hundreds of IT applications build to monitor the state of an IT system, which can also be used to monitor the state of a, BVMS based, video surveillance system.

2.3 This guide

The purpose of this guide is to cover only those IP technologies that are relevant for Bosch video surveillance systems. It is not the goal to serve as training or textbook for IP network technology in general.

“Simplicity is the ultimate sophistication.” (Clare Boothe Luce)

Keeping things simple is key in keeping them understandable. It will make things easier in the installation, configuration, maintenance and troubleshooting.

Assumed knowledge level

Bosch offers a basic network training on its online Bosch Security Academy (part of the 01 BVMS Professional Level "Online" Training Plan: Technical focus, IP networking basics). However, Bosch recommends using industry standard training as well, to get familiar with networking technologies and concepts, for example Cisco CCNA or Juniper JNCIA. This guide does not replace training, but puts the content of such training in a video surveillance context.

Network resilience

This guide does not describe any technologies related to network resilience (such as (rapid) spanning tree, routing protocols, or virtual router redundancy protocol). Bosch recommends attending industry standard trainings which cover these topics, for example Cisco CCNA or Juniper JNCIA.

Wikipedia

This document contains links to specific articles on Wikipedia. Although these articles can provide additional insights into a specific topic, Bosch is not responsible for the content of these articles.

2.4 Configuration details

It is not in the scope of this guide to offer configuration examples; it should answer the "what" and "why" questions. For Bosch products, the configuration details can be found in the product configuration manuals. For non-Bosch products it is recommended to contact the vendor of the specific product.

3 Requirements

Most of the content of this document serves as a network design "guide". This means the content should be interpreted and the exact implementation would depend on the exact system requirements. This section is different: it lists the exact requirements a Bosch video surveillance system would imply on the network.

3.1 Definitions

The issues mentioned in the table below will effect the stability of the network.

Issue	Description
Latency	Latency represents the time it takes the network to carry data from one part of a network to another part. The latency between two devices connected to the same switch is typically between 0 and 5ms. The (internet) latency between Europe and North America is typically between 25ms and 50ms. The end-to-end latency is depending on the media (for example copper has typically a higher latency compared to fiber), the physical distance, the number of (network)devices and the performance of those devices.
Packet loss	Multiple databits travelling on a network form a "packet". When the network is interrupted, or experiences instabilities, it will drop databits and as a result, only parts of the packet will be received by the destination. This phenomenon is called packet loss. Depending on the application a certain amount of packet loss is tolerated by error correction mechanisms.
Out of order	In order for applications to use packets, they should be received in the correct order. When there are multiple routes between two network devices, packets could be routed using both paths. This could result in packets arriving at the destination at a different order compared to how they are send. The order needs to be restored at the destination, but this takes time and processing power.

3.2 Requirements

A video surveillance system uses two different types of communication:

- Control traffic is used for sending controls and events between two components of the system. This includes, for example, system events ("storage state failure") and security events ("IVA alarm 1 triggered"), but also pan-tilt-zoom controls.
- Media traffic contains the actual video and optional metadata. This is mainly used for live viewing and recording.

3.2.1 Control traffic

Requirements

The bandwidth below should not be used for an exact bandwidth calculation as the exact bandwidth is depending on the exact use-cases of the system. For example, each additional event that is configured will consume additional bandwidth when this event is triggered.

The control traffic is measured when no video streams (recording or live) are being used.

Source	Destination	Average Bandwidth	Latency / Packet loss / Out of order	Description
Management Server	Video Recording Manager	1 mbit/s	50ms / 1% / 1%	Used for device monitoring, events and the activation of the configuration. The speed of the activation of the configuration depends on the available bandwidth.
Management Server	Camera	10 kbit/s	50ms / 1% / 1%	Used for device monitoring and events.
Management Server	Operator Client	1 mbit/s	50ms / 1% / 1%	When the operator client first connects to the management server, or the configuration is updated, the configuration needs to be transferred from the management server to the operator client. The bandwidth between the management server and operator client will effect the start-up time of the operator client. Additionally this communication channel is used for status information, events and alarms.
Management Server	DVR	128 kbit/s	50ms / 1% / 1%	Used for device monitoring and events.
Video Recording Manager	iSCSI target	1 gbit/s	50ms / 1% / 1%	The iSCSI target should be on the same local network as the Video Recording Manager. Not meeting this requirement can effect the ability to format the iSCSI target or increase the regular initialization, and can lead to recording gaps.
Video Recording Manager	Camera	10 kbit/s	50ms / 1% / 1%	Used for recording management.
Management Server	Enterprise Management Server	n/a	n/a	There is no communication between the Management Server and the Enterprise Management Server.

3.2.2 Media traffic

Source	Destination	Bandwidth	Latency / Packet loss / Out of order	Description
Camera	iSCSI target	variable	50ms / 1% / 1%	The iSCSI target should be on the same local network as the camera. The bandwith depends on the profile of the camera. Used for recording (direct or ANR).

Source	Destination	Bandwidth	Latency / Packet loss / Out of order	Description
Camera	Operator Client	variable	50ms / 1% / 1%	The network latency will impact the pan-tilt-zoom behaviour of moving cameras. the bandwidth depends on the profile of the camera. Used for live traffic or local replay.
DVR	Operator Client	variable	50ms / 1% / 1%	
Video Recording Manager	Operator Client	variable	50ms / 1% / 1%	Transcoding can be used to reduce the required bandwidth. Only applicable when VRM replay is used.
iSCSI target	Operator Client	variable	50ms / 1% / 1%	The iSCSI target should be on the same local network as the operator client. Only applicable when direct-iSCSI replay is used.

4 Understanding a network

This section describes general concepts and technologies which are important to understand what a network is and how it behaves.

4.1 The OSI reference model

The OSI reference model is a conceptual model that is used to structure network communication, and is used in wired connections (for example ethernet and xDSL) and wireless connections (for example WiFi and cellular). Understanding the OSI reference model is essential in order to understand how networks operate, and design, commission, maintain and troubleshoot them.

Layer	Name	Description
1	Physical	Sending bits (1/0) over a physical media, for example a copper cable or a wireless link.
2	Data link	Provides error checking on top of the first layer.
3	Network	Introduces routing of data, including addressing schemes.
4	Transport	Provides a reliable way of communication between two specific nodes on the network.
5	Session	Manages a session, a two-way continuous "conversation" between nodes on the network.
6	Presentation	Presents the data received on the network to the higher level application layer.
7	Application	Well-known protocols operate on this layer, for example the HTTP protocol.

More information can be found on Wikipedia - OSI model.

Morse-code

Morse-code is an example of a network that can be considered having two layers: the physical layer represents the "beeps". The application layer would translate these beeps directly into useful information (. . . - - - . . . for SOS, being short, short, short, long, long, long, short, short, short).

4.1.1 OSI Layer 1: physical layer

The physical layer is responsible for sending bits (1/0) from one device to the next device. This is done using electrical (copper), light (fiber) or radio (WiFi) signals.

Cabling

The first level of the OSI reference model includes the cabling. Depending on the electrical environment shielded (STP or FTP) or unshielded cabling (UTP) can be used. On top of that, category 5 or category 6 cabling can be used, depending on the required speed and electrical environment. Due to the difference in cost and specifications a general recommendation on the type of cabling, which is cost-effective, cannot be made. However, unshielded category 5E cabling can be considered the minimum recommended cable.

Network equipment

A network can consists of multiple types of devices, for example as (legacy) hubs, switches, wireless access points, and routers. Together with the cabling these devices form the heart of the network, and allow, for example, workstations, mobile devices, servers, and video surveillance cameras to communicate.

Power of Ethernet

Low-powered devices which need to be connected to the network can be powered from the network as well, which avoids the additional costs of a separate power installation. Voice-over-IP phones, wireless access points and surveillance cameras are popular devices to be powered by power over ethernet. There are different variants of power over ethernet. The version(s) supported by the power delivering device and consumption device should be listed in their respective datasheets.

> Ensure that the power over ethernet variant of the consuming devices matches with the delivering devices. Non-standard variants exist as well. These might not be compatible with equipment based on standards.

Specification	Name	Maximum power
802.3at Type 1 (802.3af)	PoE	15.40W
802.3at Type 2	PoE+	30.0W
802.3bt Type 3	4PPoE	60W
802.3bt Type 4	n/a	100W

Source: Wikipedia - Power over Ethernet

4.1.2 OSI Layer 2: data link layer

On top of the physical layer the data link layer is, among other tasks, responsible for addressing multiple devices on the network. It combines bits from the physical layer into a frame.

MAC addresses

Each physical device on the network (video surveillance cameras, storage devices, workstations, but also WiFi devices such as smart phones) has a unique MAC address, which is tied to that specific hardware (with some exceptions). When a device is connected to the network, the network device relates the MAC address of the device to the physical port number (it essentially builds a table with MAC addresses and the physical location of that address). When frames needs to be send to a specific MAC address, the device knows to which physical port the device is connected and "forwards" the frames to this physical port.

Virtual LANs (VLAN)

Virtual LANs are able to, virtually, separate a network into multiple sub-networks. These separated networks are virtually disconnected, and can only be connected on the third layer of the OSI reference model. There are several reasons for using VLANS in a network design:

- Limit overhead: in a network all devices communicate with each other (broadcasting the question: "*who are you?*") to ensure that, if necessary, they can start communicating very fast. Introducing a VLAN in a network splits that huge network into multiple, disconnected, networks (which can be connected on the third layer of the OSI reference model). This reduces the overhead in the network.
- Increase security: when an attacker gets access to a huge network, he immediately has access to all the network resources and devices. Splitting the network into multiple virtual networks reduces the exposure of network resources and devices when an attacker is able to get into a specific part of the network.

4.1.3 OSI layer 3: network layer

On top of the data link layer the network layer is, among other tasks, responsible for connecting devices which are spread out over multiple (layer 2) networks. It combines frames from the data link layer into packets.

IP addresses

Next to a (physical) MAC address, each device also has a (logical) IP address. Compared to MAC addresses, an IP address is configurable and can move from one device to another device. There is a difference between private addresses (which can be used for internal networks) and public addresses (which are used on the internet).

Private IP addresses will never be assigned to Internet networks and are sometimes referred to as non-routable IP addresses. The Internet Assigned Numbers Authority (IANA) has reserved the following IP addresses for private networks:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

Subnet masks

Subnets (sub-networks) are used for IP communication and for minimizing the size of a network (or broadcast domain). According to Classless Inter-Domain Routing (CIDR) there is no longer a fixed assignment of an IP address to a network class. There is only a subnet mask that divides the IP address in a network part and a host part. “1” in the subnet mask defines the network, “0” defines the host. As an example we examine the IP address 192.168.128.121. The example for a subnet mask is 255.255.255.252.

Description	Binary form	Decimal form
Subnet mask	11111111.11111111.11111111.11111100	255.255.255.252
Network address	11000000.10101000.10000000.01111000	192.168.128.120
Address range	11000000.10101000.10000000.01111000 11000000.10101000.10000000.01111001 11000000.10101000.10000000.01111010 11000000.10101000.10000000.01111011	192.168.128.120 192.168.128.121 192.168.128.122 192.168.128.123

The first address (192.168.128.120) is the network address, the last address is the broadcast address (192.168.128.123). Both cannot be assigned to a host.

Subnetting

The network, combining the subnet-mask 255.255.255.252 and network address 192.168.128.120 is sometimes also referred to as 192.168.128.120/30 (due the subnet-mask containing 30 "1" bits). 192.168.0.0/24 would represent the network 192.168.0.0 with the subnetmask 255.255.255.0

Subnetting

A larger subnet mark relates to a smaller network. The subnet mask used in the example above (255.255.255.252) is the largest subnet mask that can be used, creating the smallest usable network (two devices).

Ports

A port allows multiple software programs to offer services on the same device. For example, one device might offer a web-service on port 443 (HTTPS) while also offering a command-line service on port 23 (SSH).

Routing

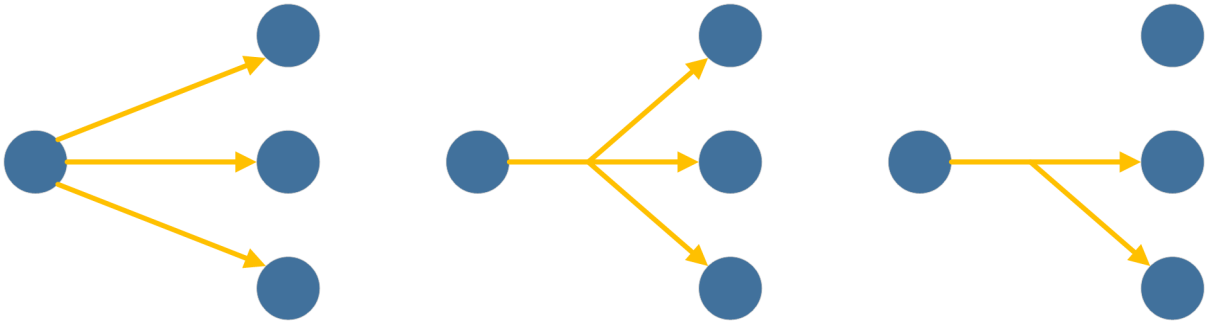
When two (layer 2) networks are disconnected, they cannot communicate. A router can connect multiple networks together. For example, if video surveillance cameras and their related storage are located in a network which is configured with 192.168.1.0/24, and the video surveillance workstations are located in a network which is configured with 192.168.2.0/24, the workstations will not have access to the live or recorded streams. A router can act as a bridge between these two networks.

Packet distribution

Unicast is a 1:1 communication. In a unicast communication the stream is, for each target, duplicated in the encoder and all streams are sent to their respective targets.

Multicast is a 1:n communication where n is a part of all. In a multicast communication the stream is duplicated in the switch that is directly connected to the targets.

Broadcast is a 1:all communication and cannot be routed.



Unicast Broadcast Multicast

IP multicast is a method of forwarding IP datagrams to a group of interested receivers. It scales to a larger receiver population by not requiring prior knowledge of how many receivers there are. Multicast uses network infrastructure efficiently by requiring the source to send a packet only once, even if it needs to be delivered to a large number of receivers.

Switches

Layer 2 switches that cannot understand multicast addresses flood traffic that is sent to a multicast group to all the members of a segment; in this case the system's network card (and operating system) has to filter the packets sent to multicast groups they are not subscribed to.

IGMP snooping

There are switches that listen to multicast traffic and maintain a state table of which network devices are subscribed to a given multicast group. This table is then used to forward traffic destined to a given group only to a limited set of hosts (ports). This is done through the use of IGMP snooping.

Some Layer 2 switches support IGMP snooping as well. They examine (snoop) all Layer 3 information in the IGMP packets sent between the host and (normally) routers. When the switch receives the IGMP Host Report from a host for a particular multicast group, the switch adds the host's port number to the associated multicast table entry. When the switch receives the IGMP Leave Group message from a host, it removes the host's port from the table entry.

Performance

There are some switch manufacturers that perform queries via software, not hardware. The examination of each Layer 3 packet for IGMP information leads to high CPU rates and therefore to major performance problems. The software-based query tables tend to corrupt after short periods of time with such large workloads. This can lead to incorrect video connections and network flooding. Avoid switches that are software driven.

Multicast addresses

IP addresses in the range of 224.0.0.0 through 239.255.255.255 are reserved for multi-casting. For devices, 225.x.x.x - 232.x.x.x and 234.x.x.x - 238.x.x.x. can be used. More details can be found at: http://www.iana.org/assignments/multicast-addresses/

An IP multicast group address is used by sources and destinations to send and receive content. Sources use the group address as the IP destination address in their data packets. Receivers use this group address to inform the network that they are interested in receiving packets sent to that group. For example, if some content is associated with group 239.1.1.1, the source sends data packets destined to 239.1.1.1. Receivers for that content will inform the network that they are interested in receiving data packets sent to the group 239.1.1.1. The receiver "joins" 239.1.1.1. The protocol used by receivers to join a group (or leave a group) is called the Internet Group Management Protocol (IGMP).

Routing protocol

In Bosch video surveillance networks the PIM Sparse Mode protocol is used for dynamic routing of multicast packets. The PIM-SM protocol causes the definition of a Rendezvous Point (RP, Level 3 switch) per multicast group. This RP switch receives multicast packets. Other switches with multicast receivers can request multicast packets from this RP switch. The RP then forwards the multicast packets to these switches or connects the source and the receiver along the shortest path from source to receiver.

Limits apply

Although multicast video uses UDP, the amount of multicast connections is limited by a maximum number of client registrations (via TCP) that accompany the UDP video streams. Due to this side-effect it is possible to create a connection between a Bosch encoder and maximum 100 decoders simultaneously (1 client registration), or a connection between a Bosch encoder and maximum 50 web pages simultaneously (2x client registration), or a combination of these two types of connections.

4.1.4 OSI layer 4: Transport layer

User Datagram Protocol (UDP)

UDP is a connectionless protocol and designed with minimal overhead, which makes it very suitable for time-sensitive communication. Due to the lack of control and overhead, it does not guarantee the delivery of data. Using the user datagram protocol on top of the network layer, packets are combined into datagrams.

Live

UDP is very suitable to transport live media, for which delay should be minimized. This includes, for example, video generated by video surveillance cameras, but also other streaming audio and video services, such as Netflix and Spotify.

Transmission Control Protocol (TCP)

In contrary to UDP, the TCP protocol introduces overhead to ensure a reliably and error-checked stream of data. The transmission control protocol guarantees the delivery of the information by means of error-detection and resending data when necessary. Using the transmission control protocol on top of the network layer, packets are combined into segments.

Recording

Due to its reliability the TCP protocol is very suitable for recording video.

Retransmits

When a network experiences congestion or stability issues, TCP will try to retransmit the data packages, which will introduce an additional load on the network. If 5% of the data packages needs to be retransmitted, the network is generating 5% more data than needed. In networks which are fully loaded this can result in (additional) data loss.

Overview

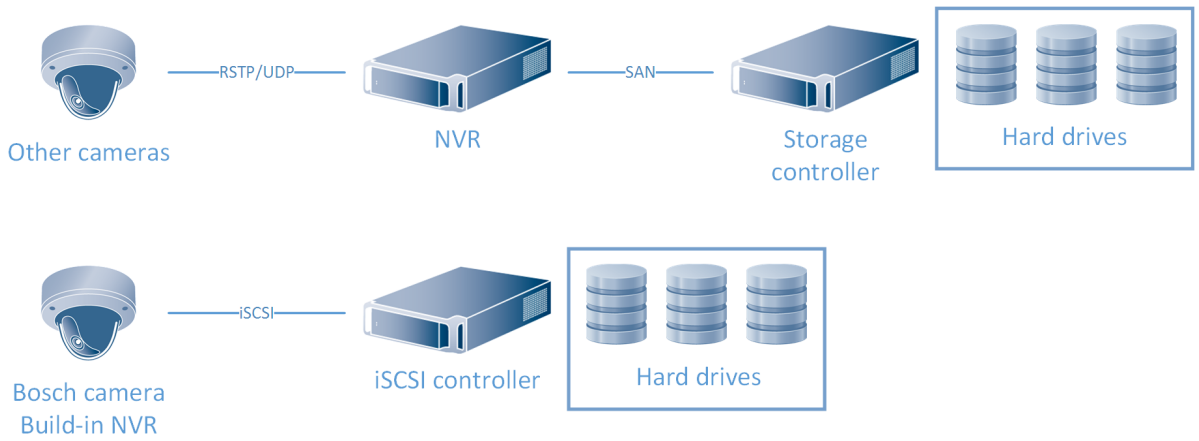
	TCP	UDP
Connection type	Connection oriented	Connectionless
Protocol	Reliable	Best-effort
Sequencing	Yes	No
Examples	E-mail, file-sharing, web-browsing	Video, audio

4.1.5 OSI layer 5 (and higher): Session, application and presentation layers

Layers on top of the transport layer combine datagrams or segments into data which can be used by higher-level protocols, for example HTTP and iSCSI.

iSCSI

The iSCSI protocol, which is used by Bosch cameras to record cameras onto an iSCSI target, is running on top of the transmission control protocol. Using the iSCSI protocol inside the camera allows the camera to record video directly onto a storage environment, removing the need of a network video recorder (NVR).



Compared to the "traditional" way of recording, which is UDP based, iSCSI is less resilient to network interruptions as it relies on the transmission control protocol to send huge amounts of data. However, there is a huge benefit of using a TCP based protocol for video recording: when the network drops a video-frame, the camera retransmits the video-frame automatically, which results in gap-less recording.

5 Hardware

5.1 Manufacturers

There are several hardware manufacturers which produce network equipment, for example: Cisco; HPE; Juniper; Allied Telesis and Netgear.

Manufacturer selection

Bosch is neutral towards network equipment vendors. Vendor selection is not in the scope of this guide. Bosch does recommend selecting a network equipment vendor which has a reliable reputation in the IT industry and offers a training and/or certification program.

5.1.1 Training programs

The training programs mentioned below and serve as an example. Local IT training centres might offer customized network training for video surveillance professionals.

Vendor	Program
Cisco	CCNA routing and switching
Juniper	JNCIA-Junos
HPE	Deploying the Mobile-First Campus using ArubaOS-Switches

5.2 Managed and unmanaged equipment

Unmanaged network equipment does not have a user-interface: it's plug and play. Most unmanaged equipment does therefore not support multicast or other advanced networking technologies. Another disadvantage of unmanaged network equipment is that it makes it more difficult to get to the bottom of network-related problems.

Managed network equipment has a user interface which allows the equipment to be configured and fine-tuned for its specific purpose. This is, mostly, done using either a command-line interface or a web-interface.

5.3 Security

Security should be build up in layers. Network security is crucial: it's main goal is to prevent unauthorized persons to access the environment. Only when unauthorized persons have breached through the network security layers, the security of the video surveillance system itself (including hardening of the operating system, system authentication, and encryption of live and recorded video) becomes important. This section describes several methods to harden the network, and provide logical intrusion detection.

5.3.1 Assigning IP addresses

One of the first steps in limiting the risk of an internal attack on a network, executed by unauthorized locally attached network devices, is to limit available unused IP addresses. This is done by using IPAM, or IP Address Management, in conjunction with subnetting the IP address range that will be used.

5.3.2 Disable unused switch ports

Disabling unused network ports ensures that unauthorized devices do not get access to the network. This mitigates the risk of someone trying to access a security subnet by plugging his device into a switch or unused network socket. The option to disable specific ports is a common option in managed switches, both low cost and enterprise.

5.3.3 Access Control Lists (ACL)

An access control list acts as a simplified firewall, and allows system administrators to set rules for limiting the communication between network endpoints. Access control lists can be configured on most managed network equipment. It is recommended to check the product datasheet for the exact specifications. An example: 192.168.0.3 can communicate to 192.168.0.254 using port 3260. The communication on all other ports is prohibited. This is translated in: camera3 can communicate to storage server 254 using the iSCSI protocol. All other communication between these device is prohibited.

As most access lists end with a "deny all other traffic" statement, they provide a very good first layer of defence against unauthorized network access by restricting the communication in the network.

Metaphor

Configuring an access control list on a network of high ways, it is possible to deny all vehicles from entering the highway, except when they travel between Amsterdam and Paris and the vehicle length is less then 10 meters.

Compared to a firewall access list to not check the content of the the traffic. In the example above camera3 can also communicate with storage server 254 using HTTP traffic over port 3260. In order to check if the network endpoints are also using the correct protocol, a firewall is needed.

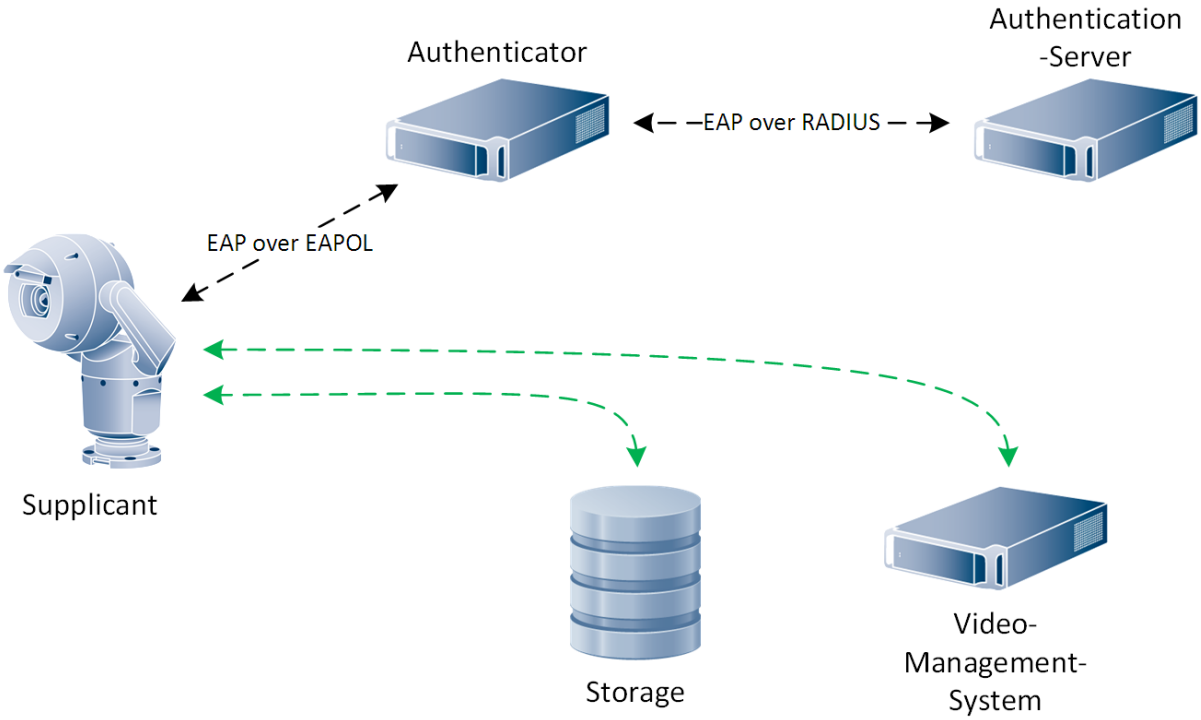
5.3.4 802.1X

Security devices are mostly located at the physical edge of the network. Especially detection devices, such as cameras, are installed in places that are accessible by the public. As these devices are connected to the network, this also increases the risk of unwanted access to the network: people could try to disconnect the security device and connect their own equipment to try to gain access to the network.

IEEE 802.1x is a standard published by the Institute of Electrical and Electronics Engineers Standards Association. This standard is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism to prevent unauthorized devices to access network resources.

This protocol involves three kinds of main elements:

- The element that wants to be able to access the network resources is called the supplicant, for example a video surveillance camera.
- The element that verifies if the supplicant may access the network resources is called the authenticator. Mostly this is a manageable switch, router or wireless access point.
- The element that actually steers the authentication process is called the authentication server. The authentication server contains the information which is used to decide if a supplicant may or may not access the network resources. Typically this is a server which supports the RADIUS protocol, which is a networking protocol that provides centralized authentication, authorization and accounting. The RADIUS protocol is part of the Internet Engineering Task Force (IETF) standards.



802.1X can be configured on most managed network equipment. Sometimes the network device offers a combined authenticator and authentication server. It is recommended to check the product datasheet for the exact specifications. All Bosch cameras are able to authenticate themselves on the network using 802.1x.

Metaphor

Configuring 802.1x list on a network of high ways, it is possible to deny all cars to enter the highway, except when their license plate is known to the monitoring system.

5.3.5 Firewalls

A firewall has a similar function then an access control list: it restricts network traffic between network endpoints. On top of what an access control list can do (described above), a firewall typically also performs "packet inspection". This allows a firewall to look at the content of the network traffic, verify if the right protocol is used, and if the traffic is matching the protocol specifications. As a result, it is not only able to check if traffic on port 3260 between the camera and storage server is allowed, it is also able to check if the traffic matches the specification of the iSCSI protocol.

Firewalls can be deployed as software only packages or combined hardware and software appliances. Well-known vendors include Cisco, Juniper Networks and Checkpoint.

Metaphor

Configuring a firewall on a network of high ways, it is possible to deny all vehicles from travelling, except when they travel between Amsterdam and Paris and the vehicle length is less then 10 meters, the vehicle colour is red, it at least carries two people, and the weight is less then 1500KG.

5.3.6 Intrusion Detection and Prevention Systems (IDS/IPS)

Intrusion Detection and Prevention systems go one step further compared to firewalls. These systems acts as a "virusscanner" on the network. They are able to detect and block known and unknown attack methods based on the signature and behaviour of an specific attack. Well known vendors include McAfee, Cisco, Trend Micro and Fire Eye.

Metaphor

Configuring an IDS on a network of high ways, it is possible to detect accidents as they happen by combining information on the vehicles speed, trajectory, and matching it to the movement of other vehicles. Configuring an IPS on a network of high ways, it is possible to stop accidents as they happen (limiting the damage) by combining information on the vehicles speed, trajectory, and matching it to the movement of other vehicles.

5.4 Quality (Class) of Service

Live video will be send between the cameras and the operator workstation. This traffic needs to be as “live” as possible (lowest delay) and there should be no artifacts within this video. When a network experiences congestion and delay, some packets may be dropped. Class of Service (CoS, sometimes also referred to as Quality of Service) enables the network administrator to divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs. This allows packet loss to happen according to rules that are pre-configured. This mechanism is only used in situations where there is not enough bandwidth on the network. This can be due to a disruption but also due to a temporary increase in demand from an external application.

6 System design

6.1 Used ports

The network ports that are used in a Bosch video surveillance system are listed in the BVMS configuration manual.

6.2 Network blueprints

For Bosch video surveillance systems it is recommended to use a hierarchical network model. Such a model divides a network into three Layers: Core, Distribution, and Access Layer.

The Access Layer is responsible for connecting devices to the network. Its defining characteristics generally revolve around either high port density. Modern Access Layer switches also contain access list and quality of service.

The Distribution Layer is where policies are applied. Distribution Layer designs usually focus on aggregating access devices usually located in different subnets into boxes with significant processing resources so that policies can be applied.

Finally, the Core Layer is the "backbone". Its job is simply to move packets from point A to point B as fast as possible and with the least possible manipulation. Core and Distribution are only separated into different switches in large networks. Very often, one switch can take both the tasks of the Core and the Distribution Layer.

Reference design

The reference designs mentioned in this chapter are generalized and need to be adjusted to the specific system set-up. The equipment list only considers the components connected to the video surveillance system. Additional connections (for example, to other parts of an IT environments) are not considered and need to be added manually.

Cable length limitations

The reference designs do not take cable length limitations into consideration.

6.2.1 32 cameras

This first reference design is based on a system with 32 cameras and 5 workstations located within one building.

Depending on the used cameras, the network needs to process a total bandwidth of 160 Mbit/s (based on an average of 5Mbit/s per camera) to the storage device. This means that a single 100Mbit/s interface is not sufficient, and at least 1 gigabit interface should be used. If the storage device has multiple gigabit interfaces, it is recommended to connect two gigabit interfaces.

It is recommended to connect the entire system to a single PoE access switch with at least 2 gigabit ports. The storage device can, depending on the model, be connected using multiple network interfaces (teamed) to the gigabit ports on this switch.

Due to the simplicity of the environment an unmanaged access switch is recommended. As a result multicast cannot be enabled, but this is also unnecessary with 5 workstations.

Equipment	Number	Ports (100Mbit/s)	Ports (1Gbit/s)	Managed
Access switch	1	32+5	2	NO

Equipment	Number	Ports (100Mbit/s)	Ports (1Gbit/s)	Managed
Distribution switch	0	n/a	n/a	NO
Core switch/router	0	n/a	n/a	NO

6.2.2 64 cameras (campus)

The second reference design is based on a system with 64 cameras and 5 workstations within one building.

As access switches with more than 48 ports do not exist, multiple switches need to be used. It is recommended to split the system in two parts, connecting up to 32 cameras to a access switch with at least 1 gigabit port. This port will be used as an uplink to the core switch, which will be used to send 160Mbit/s (based on an average of 5Mbit/s per camera) + live feeds to the core switch.

The core switch connects the 2 access switches, the 5 workstations, and the storage device. This adds up to at least 9 gigabit ports.

Due to the simplicity of the environment an unmanaged access switch and a managed core switch is recommended. This way the network traffic travelling through the core switch can be analysed and optimizations can be done, when this is necessary. As a result multicast cannot be enabled, but this is also unnecessary with 5 workstations.

Equipment	Number	Ports (100Mbit/s)	Ports (1Gbit/s)	Managed
Access switch	2	32	1	NO
Distribution switch	0	n/a	n/a	NO
Core switch/router	1	n/a	9	YES

6.2.3 128 cameras (campus)

Redundancy

If the organisation is heavily depending on the availability of the system, it is highly recommended to deploy mechanisms which mitigate network failure. Due to the complexity this is outside of the scope of these reference designs. The section "Training programs" can provide guidance in finding a relevant training.

As access switches with more than 48 ports do not exist, multiple switches need to be used. It is recommended to split the system in four parts, connecting up to 32 cameras to a access switch with at least 1 gigabit port. This port will be used as an uplink to the core switch, which will be used to send 160Mbit/s (based on an average of 5Mbit/s per camera) + live feeds to the core switch.

The core switch connects the 4 access switches, the 10 workstations, and the storage device. This adds up to at least 16 gigabit ports. For each additional storage device two additional gigabit ports are recommended.

Due to the amount of workstations it is recommended to deploy multicast, which means the access and core switches should both be managed. This way the network traffic travelling through the core switch can be analysed and optimizations can be done, when this is necessary.

Equipment	Number	Ports (100Mbit/s)	Ports (1Gbit/s)	Managed
Access switch	4	32	1	YES

Equipment	Number	Ports (100Mbit/s)	Ports (1Gbit/s)	Managed
Distribution switch	0	n/a	n/a	NO
Core switch/router	1	n/a	9	YES

6.2.4 256 cameras or more (campus)

Due to the potential complexity no specific recommendation can be made, and a tailored design is required. In general it is strongly recommended to deploy an environment with managed switches to enable the deployment of multicast.

6.2.5 Multi-site

There are three ways to deploy a BVMS system with subsystems, spread across different geographical locations. A short description of the differences is included below, for more details it is recommended to have a look at the BVMS system design guide or join an on-line or classroom BVMS training.

Enterprise: multiple BVMS management servers which provide a combined experience to the operator. The operator sees multiple subsystems, but has full alarm management functionality.

VRM-based: one BVMS management server connecting to multiple recording managers. From the operator's perspective this is experienced as one big system.

Unmanaged sites: one BVMS management server which connects, on request, to subsystems. The operator is able to access the live and recorded footage, but does not have alarm management capabilities.

Due to the potential complexity no specific recommendation can be made, and a tailored design is required.

Port-forwarding risks

It is not recommended to deploy port-forwarding to enable systems to communicate across multiple locations. It is strongly recommended to deploy a professional virtual private network (VPN) or use dedicated leased lines. Port-forwarding enables a device or service to be reached directly from the internet. This causes a huge risk by allowing potential attackers to connect to such a device or service, and start figuring out how they can use this device or service to connect to other components of the system.

6.2.6 Wireless

Wireless networks can be used in video surveillance systems, but it is essential the values in the section requirements are met. Please note that, in the specific case of wireless networks, these values are not constant. A growing tree between two wireless antenna's, or even a thunderstorm, can increase the packet loss to unacceptable values and potentially result recording gaps. When a wireless network is deployed, Bosch strongly recommends to put the storage device as close as possible, and preferably on a full wired connection, to the camera. The connection from the camera and storage device to the operator is less crucial, but should still meet the values mentioned in the Requirements section.

Troubleshooting

The reliability of wireless networks is not only depending on the quality of equipment, but on the environment as well. This poses an additional risk to the stability of the system, and can even allow external changes to disrupt the communication between the components of the security system. It is strongly recommended to evaluate the risks related to deploying a wireless network for the purpose of physical security.

Troubleshooting

The Bosch technical support teams will only offer limited support when wireless networks are deployed. If the technical support team suspects issues with the wireless network, an indication will be given to which network endpoints are involved (for example, camera1 and workstation5), but no further recommendation on the network set-up and configuration can be given. It is expected the system integrator and/or end-user is trained to operate and troubleshoot the wireless equipment.

7 System monitoring

It order to keep the system in good health, deploying a system monitoring solution is crucial. BVMS has built-in system events, which are perfectly suitable for monitoring systems up to 256 channels. For systems over 256 channels, which require a dedicated network infrastructure, Bosch recommends to deploy an external monitoring tools based on the Simple Network Monitoring Protocol (SNMP). This allows system integrators and end-users to keep a careful eye on the technical state of the entire system (including the network infrastructure) and prevent problems before they appear.

7.1 BVMS internal monitoring

The BVMS internal monitoring monitors the state of the video surveillance system itself. It triggers alarms when the connection between system components is lost, and when the system is struggling with recording. When the system is actively managed by a system administrator, Bosch recommends to send these alarms to administrative accounts only. If administrators do not use the system on a daily basis, e-mail alarms can be configured to notify the administrators of system failures. This way the operators themselves are not flooded with technical information they probably cannot understand.

Alternatively operators can be notified of system events. In this case Bosch suggests to create a specific priority and mark these alarms with a specific colour and workflow. In the workflow the operator is forced to notify the system administrator (which could be external) of the specific event, which can then be further investigated.

> Some events, for example the "storage state failure" do not seem to impact the system's capability to record, but it does indicate that the specific camera is struggling to continuously record.

> To ensure a stable and reliable system, it is highly recommended to investigate all events that are enabled by default. A sign-off on the system's delivery should only be done without any active system events.

7.2 Simple Network Monitoring Protocol (SNMP)

The Simple Network Monitoring Protocol (SNMP) is a protocol that is used for equipment monitoring by all major IT vendors. SNMP is available in most managed IT network equipment.

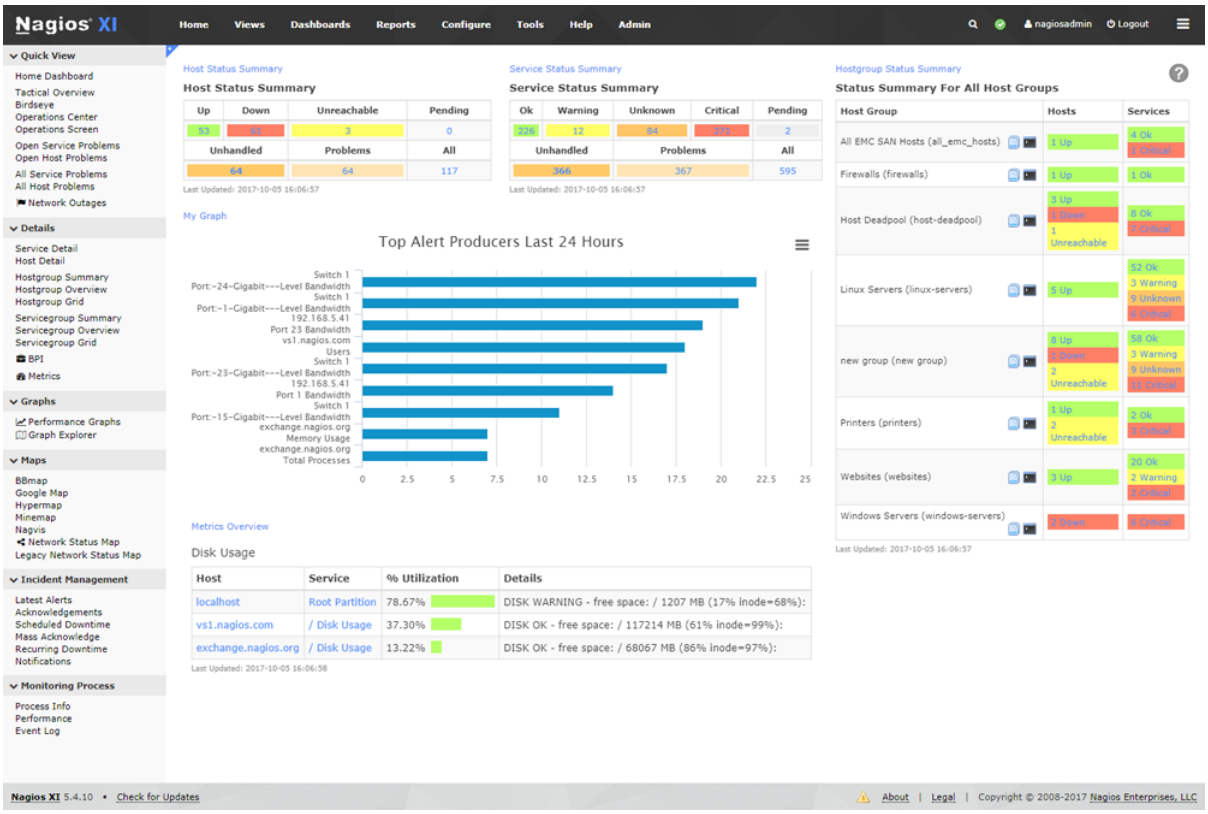
7.2.1 BVMS as a SNMP client

BVMS can function as a SNMP "receiver", receiving SNMP messages from IT equipment. The SNMP client is integrated into the BVMS internal monitoring mechanism, as described above. This means the system can generate events and alarms based on SNMP messages received from IT network equipment, for example, when a switch port goes down (a cable is disconnected?).

7.2.2 BVMS as a SNMP server

BVMS can expose itself as a SNMP "server" as well. This means an external SNMP monitoring system can receive events (SNMP traps) from BVMS, or scan the BVMS system periodically for it's status. Examples of such systems are PRTG, Nagios and Opsview. These systems include dashboards which enable a system administrator to see the system status within one single overview, and dive into details when necessary. For more details on the options, Bosch recommends to reach out to the specific vendor.

The image below shows an example of a Nagios XI dashboard.



8 Troubleshooting

Having the video surveillance system running on top of an IT infrastructure creates some challenges: which component is at fault when the system is not working? Looking at the OSI reference model, described in earlier sections, it is recommended to check layer by layer. This chapter lists the questions that need to be asked related to each layer.

8.1 OSI reference model

Layer	Description	Tools	Questions
1	Physical layer	Managed IT equipment, checking physical installation.	• Is the link status "UP"? • Does the cable length exceed the specification? • What is the quality of the cable? • (PoE) Does the device receive power? • What is the speed of the physical link? • Is the link operating in full-duplex mode?
2	Data link layer	Managed IT equipment.	• Are VLANs being used? If so, is traffic between VLANs routed? • Does the network equipment produce CRC errors? • Does the network equipment drop frames?
3	Network layer	Ping, tracert (Windows), managed IT equipment.	• Can devices reach each other (ping response)? • Is the link stable (ping packet loss)? • How much devices are located in the same subnet (overload in broadcast)? • Is the link responsive (ping latency)? • Is the routing set-up correctly (tracert / traceroute)? • Is multicast operating properly? • Are the correct ports opened in the firewall?
4	Transport layer	Wireshark	• Are UDP packets being send in the right sequence? • Are UDP packets being dropped (missing sequence IDs)? • Are TCP packets being retransmitted? • How many TCP packets are being retransmitted?
5	Session, application and presentation	Wireshark, application log files	• Is the iSCSI session stable? • Is the recording stable (look for recording gaps in the timeline)? • How is the system configured? • Does the application log file show any error messages?

8.2 Tools

8.2.1 Ping

Ping is based on the ICMP (Internet Control Message Protocol), and a very helpful tool to check the connection between two IP connected devices.

Ping

```
ping -n 5 -l 1500 www.google.com
Pinging www.google.com [74.125.224.82] with 1500 bytes of data:
Reply from 74.125.224.82: bytes=1500 time=68ms TTL=52
Reply from 74.125.224.82: bytes=1500 time=68ms TTL=52
Reply from 74.125.224.82: bytes=1500 time=65ms TTL=52
Reply from 74.125.224.82: bytes=1500 time=66ms TTL=52
Reply from 74.125.224.82: bytes=1500 time=70ms TTL=52
Ping statistics for 74.125.224.82:
   Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 65ms, Maximum = 70ms, Average = 67m
```

Ping parameters

Ping has a lot of parameters. In the example above, "*-n 5*" is used to trigger 5 ping commands, and "*-l 1500*" is used to increase the default packet size, which results in an increased network and system load. More details can be found on Microsoft Technet: Ping for beginners.

The output of the ping command gives a comprehensive overview of the stability of the link between the two devices (sent, received and lost) and the delay between the two devices (round trip times).

8.2.2 Logging

Application log files are essential during the troubleshooting process as well. Most people find application log files intimidating, but remember that these log files are written by persons as well. They can show a great deal of useful information on the state of the system, by searching for specific words (for example, "error") or repeating lines. In general, the (open-source) tool Snaketail is very suitable for analysing log files.

8.2.3 Wireshark

Wireshark is the tool used by network professional to analyse the performance and state of the network. There are hundreds of tutorials and videos explaining the Wireshark functionality.

Wireshark can be used to visualize the bytes travelling on the network, and translating them into human readable information. It translates the raw data into packets, and shows an overview of captured packets. Depending on the packets, a direct translation is made to the protocol (for example iSCSI) as well.

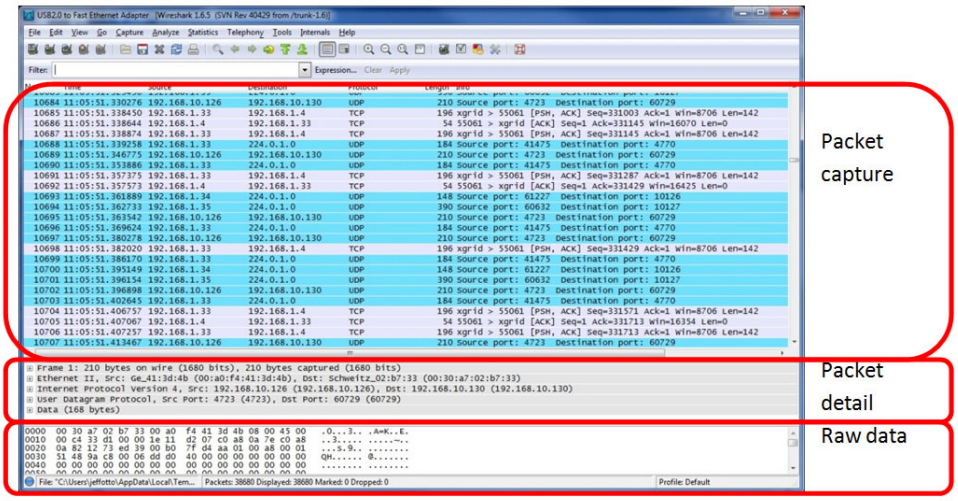


Image source: https://www.deepdotweb.com/2017/11/21/wireshark-tutorial/