Dallmeier

REV. 2.0.1 | 2020-11-24

WHITEPAPER

## BASIC INFORMATION

# SWITCH BASICS & VIDEO NETWORKS

EXPLANATIONS, FUNDAMENTAL SPECIFICATIONS AND APPLICATION EXAMPLES
FOR SWITCHES IN DIGITAL VIDEO NETWORKS

MADE IN GERMANY

See more.

The manufacturer accepts no liability for damage to property or pecuniary damages arising due to minor defects of the product or documentation, e.g. print or spelling errors, and for those not caused by intention or gross negligence of the manufacturer.

Figures in this document may differ from the actual product.
Specifications subject to change without notice. Errors and misprints excepted.

# INHALT

**CHAPTER 1:** **ABSTRACT** .......... **4**

**CHAPTER 2:** **EXPLANATION** .......... **5**
2.1 General .......... 5
2.2 Internal Bandwidth .......... 5
2.3 Power over Ethernet .......... 6
2.4 Layer 2 and 3 Switches .......... 7
2.4.1 OSI Reference Model .......... 7
2.4.2 Layer-2-Switch .......... 7
2.4.3 Layer-3-Switch .......... 8
2.5 Managed and Unmanaged Switch .......... 8
2.6 Access, Distribution and Core Switch .......... 8
2.7 Broadcast Domain and Broadcasting .......... 9
2.8 SFP Port .......... 10
2.8.1 SFP Twisted Pair Cable Types .......... 10
2.8.2 SFP Fibre Cable Types .......... 10
2.8.3 Dual-Purpose SFP Port .......... 11
2.9 Quality of Service .......... 11
2.9.1 Integrated Services .......... 11
2.9.2 Differentiated Services .......... 11
2.10 Spanning Tree Protocol .......... 12
2.11 Encoder and Decoder .......... 13
2.12 Unicast and Multicast .......... 13
2.12.1 Unicast .......... 13
2.12.2 Multicast .......... 14
2.13 Internet Group Management Protocol .......... 15
2.13.1 IGMP Querier .......... 16
2.13.2 IGMP Snooping .......... 17
2.14 Protocol Independent Multicast .......... 18

**CHAPTER 3:** **EXAMPLES** .......... **19**
3.1 Unicast and Multicast .......... 19
3.2 Simple Video Network .......... 22
3.3 Middle-Size Video Network .......... 23
3.4 Large Video Network .......... 25

**CHAPTER 4:** **IMPORTANT NOTES** .......... **26**

# ABSTRACT

A switch is a network device with core function for every digital video surveillance system. It is responsible for controlling and distributing data packets, and enables the connections between network components and terminal devices.

The IT market offers a wide range of switches which significantly differ in terms of quality and integrated functions. Particularly with respect to the proper functioning of further components and devices, selecting an appropriate switch should also include qualitative and economical arguments.

In order to ensure that the functions of Dallmeier systems can be fully used, this document contains several definitions as well as basic information and examples concerning the areas and ranges of application and usage of the various switches. In addition, tables with performance classes, standard values and basic specifications are included to offer guidance and assistance in choosing and using the suitable switch.

Since not all components and combinations are testable or manageable, Dallmeier accepts no warranty or liability whatsoever for the descriptions, data and examples given in this document. Furthermore, the respective notes and standard values are to be regarded as recommendations only. They exclusively serve informational purposes and are not legally binding.

A list of the switches that have been extensively checked and tested can be found in the white paper “Whitelist Switch”.

# EXPLANATION

## 2.1 GENERAL

An up-to-date switch is not - as many might describe it - a multiple power outlet (hub) for network cables, but rather an intelligent control center that forms the backbone of a digital video surveillance. Therefore, the switch should be chosen carefully. A low-quality switch can have major effect on a video network, which then often results in undefinable phenomena:

- Delays in establishing a connection
- Increased delay during live transmissions
- Recording gaps
- Connection losses
- Encoder/decoder failures
- Jitter and/or image artifacts during the transmission
- etc.

## 2.2 INTERNAL BANDWIDTH

A hub imperceptibly distributes the incoming signal to all of the connected devices. The available bandwidth must thereby be divided among all devices within the network. With switching, on the contrary, a direct connection is established between two terminal devices. Consequently, multiple connection lines can be used simultaneously and with full network bandwidth, provided that, the switch is capable of meeting the required switching capacity.

A bottleneck only emerges if several devices try to communicate with one specific station at the same time. Switches typically have 8, 16, 24 or 48 ports (connections). These access ports are usually available in a 10/100 MBit/s and a 10/100/1000 MBit/s version.

A switch should be capable of simultaneously managing the full network bandwidth on all connections. This means that, for example, a 24 port switch with 100 MBit/s each must at least have an “internal” bandwidth (wirespeed) of 2400 MBit/s (2,4 GBit/s). Low-budget switches often do not achieve this performance. Sometimes, corresponding specifications can also be found under “backplane speed” or “forwarding rate” in the respective product data sheets. Unfortunately however, the wirespeed is not indicated by all manufacturers.

Apart from the regular ports, several devices feature up to 4 additional so-called “uplink ports”. These ports are used for the connection to further switches. In most cases, the uplinks therefore support a higher speed or are designed as a module slot for so-called “STP modules” (also known as “mini GBIC”; for details, see below).

*Whether a switch port can be used as an uplink or access port, depends on the respective configuration of the port.*

## 2.3 POWER OVER ETHERNET

Power over Ethernet (PoE) denotes the procedure by which various network components (e.g. a network camera) can be provided with data and simultaneously powered with electricity over an Ethernet cable.

If a terminal devices is connected to a PoE capable switch, the function, first of all, determines, whether the terminal device (PD = powered device) requires power, by performing a resistance test. In the next step, the maximum amount of electricity the device is capable of consuming is determined based on the PoE class.

With PoE, the maximum output power of a PSE (Power Supply Equipment) is limited to approx. 15 Watt. As a result of power losses, which have to be taken into account, the end consumer (the network component), however, may only draw a maximum of 12.95 W. With the newer PoE+ standard, an output power of up to 30 W is possible.

Since there are only very few cases in which a switch can provide all ports with maximum PoE power, the behavior of the switch must be defined. However, the configuration options are predetermined by the respective device. Some devices only offer a restricted number of PoE outlets, others limit the performance by a PoE budget, and again others allow for a detailed power configuration via the switch management culminating in a shutdown priority. If the PoE budget is depleted, further ports are no longer supplied with electricity. For some switches, this already applies as soon as the budget of the maximum theoretical power is reached.

*Test the emergency case as well and simulate a power outage. Not every switch is capable of sequentially switching on the PoE ports (inrush current/starting current).*

The standards IEEE 802.3af or IEEE 802.3at describe a consumer (Powered Device, PD) and the power provider (Power Source Equipment, PSE).

| Class | Performance Powered Device (PD) | **Max. Performance Power Source Equipment (PSE)** |
|---|---|---|
| 0 (IEEE 802.3af) | 0.44 W – 12.95 W | 15.4 W |
| 1 (IEEE 802.3af) | 0.44 W – 3.84 W | 4.0 W |
| 2 (IEEE 802.3af) | 3.84 W – 6.49 W | 7.0 W |
| 3 (IEEE 802.3af) | 6.49 W – 12.95 W | 15.4 W |
| PoE+ (IEEE 802.3at) | 12.95 W – 25.5 W | 30.0 W |

Table 2-1: Performance classes according to IEEE 802.3af (PoE) and IEEE 802.3at (PoE+ / PoE plus)

# 2.4 LAYER 2 AND 3 SWITCHES

## 2.4.1 OSI Reference Model

The OSI reference model is a reference model for network protocols as layer architecture. It describes the communication across different technical systems. For this purpose, the model defines seven successive layers, each with a narrowly defined task. The network protocols of a layer are defined with clear interfaces and are easily interchangeable, even if, like the Internet Protocol, they have a central function.

| OSI Reference Model | | | | | |
|---|---|---|---|---|---|
| OSI Layer | | Example Protocols | Unit | Connection Elements | Description |
| 7 | Applications | HTTP<br>FTP<br>HTTPS<br>SMTP<br>LDAP<br>RTSP | Data | Gateway (Firewall), Content-Switch, Layer-4-7-Switch | Enables applications to access the network |
| 6 | Presentation | | | | Translation of application formats into a network format and vice versa (formats, en-/decodes) |
| 5 | Session | | | | Establishes logical connections, controls, synchronizes and terminates them |
| 4 | Transport | TCP<br>UDP<br>SCTP<br>SPX | Segments | | Transforms data packets according to protocol, controls them and provides them to the above layers |
| 3 | Network | ICMP<br>IGMP<br>IP<br>IPsec<br>IPX | Packets | Router<br>Layer-3-Switch | Regulates the exchange of data packets, takes on the routing, established and terminates connection channels |
| 2 | Data Link | Ethernet<br>Token Ring<br>FDDI | Blocks (Frames) | Bridge<br>Switch | Ensures reliable data exchange, connects bits to blocks, adds a checksum and forwards it to the network layer |
| 1 | Physical | | Bits | Repeater<br>Hub | Mechanically and electrically establishes a physical connection in order the transmit bits |

Table 2-2: OSI reference model

## 2.4.2 Layer-2-Switch

Layer 2 is also called the "data link layer" in die OSI model and is mainly responsible for an error-free data transmission. A so-called "layer-2-switch" works with MAC addresses (Media Access Control address) documented in the SAT (Source Address Table) together with the corresponding physical port.

The switch uses the source address table to make decisions concerning the transmission of data (this behavior is also called "switching"). The advantage of layer-2-switches is that they can be operated without requiring a high level of background knowledge (plug and play).

### 2.4.3 Layer-3-Switch

The 3rd layer in the OSI model is called the "network layer". It ensures that connections are set up and data packets are forwarded. The establishment of a connection as well as the transmission of data packets to other ports (networks) are realized by using the internet protocol (IP) and various routing functions.

The layer-3-switch can be described as a combination of router and switch. In order to achieve ideal integration and due to the multitude of their functions, layer-3-switches require a detailed configuration which is individually adjusted to the network.

## 2.5 MANAGED AND UNMANAGED SWITCH

Apart from the fundamental function of switching (layer 2), manageable switches generally have a user interface. This offers additional management and monitoring functions, such as e.g., Virtual Local Area Network (VLAN), Quality of Service (QoS), Spanning Tree Protocol (STP/RSTP), IP-Filtering, Routing, etc., which are helpful or necessary for a network in excess of a certain size/functional range.

Depending on the manufacturer, the management is performed by using a control software, web interface, console or a combination of all of these possibilities. Since the user can actively influence the way these kinds of switches work, they are called "managed switches". Consequently, a switch that does not allow for the intervention of a user is known as "unmanaged switch".

## 2.6 ACCESS, DISTRIBUTION AND CORE SWITCH

An access switch is a switch that is used as an interface to terminal devices. It allows for the connection of various devices (cameras, recording servers, workstations) to the network.

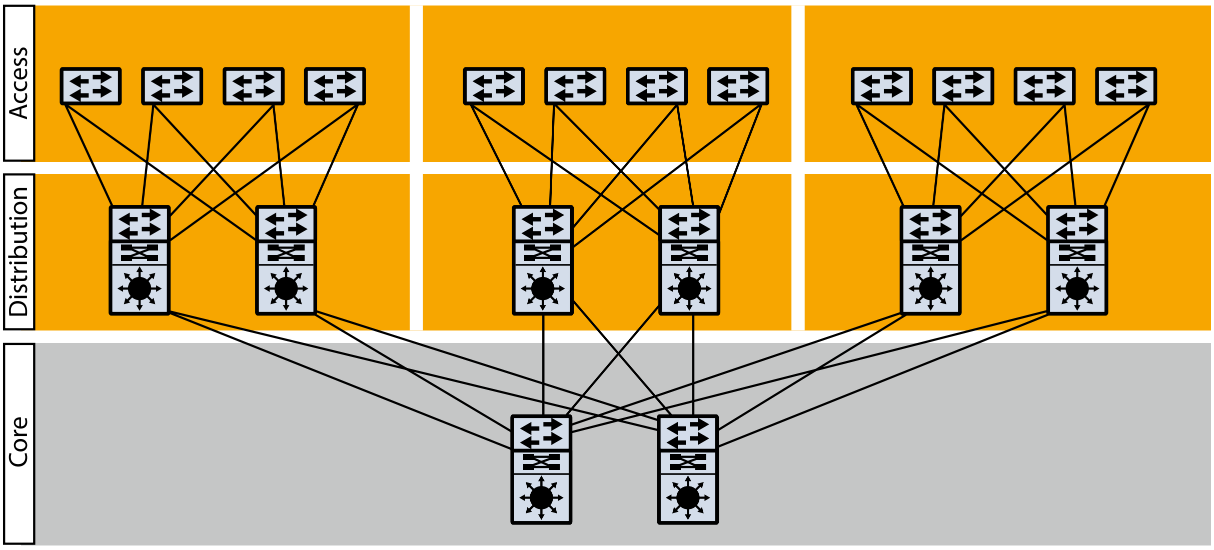

Fig. 2-1: Core, Distribution and Access switches

In large networks, distribution switches are often applied as distributors between access and core switch.

The core switch is a high-capacity switch that forms the backbone of a network. It thereby serves as an interconnection among the different network components (access/distribution switches). Core switches are usually equipped with Gigabit interfaces in order to provide the connected network components with a high bandwidth.

*A core switch can also have access ports.*

## 2.7 BROADCAST DOMAIN AND BROADCASTING

A broadcast domain consist of a layer-2-based local network. Within this network each host (network device) is available to all the other hosts by a so-called “broadcast” (request to all participants within the net).

Broadcasts can also be send to layer 3 (internet protocol) of the OSI model, given that, however, this is supported by the layer below. Broadcast domains are separated by layer 3 network components (routers, layer-3-switches). Thus, a broadcast initiated by, e.g., PService (configuration and management software for IP systems by Dallmeier) cannot be transmitted from one subnet to another.

A subnet is part of a network which was separated by means of a subnet mask (layer 3). Subnets are connected via routers or layer-3-switches and their gateways. This suggests, that each subnet has its own broadcast domain.

*In order to scan Dallmeier IP devices with PService, you have to be located within the same broadcast domain.*

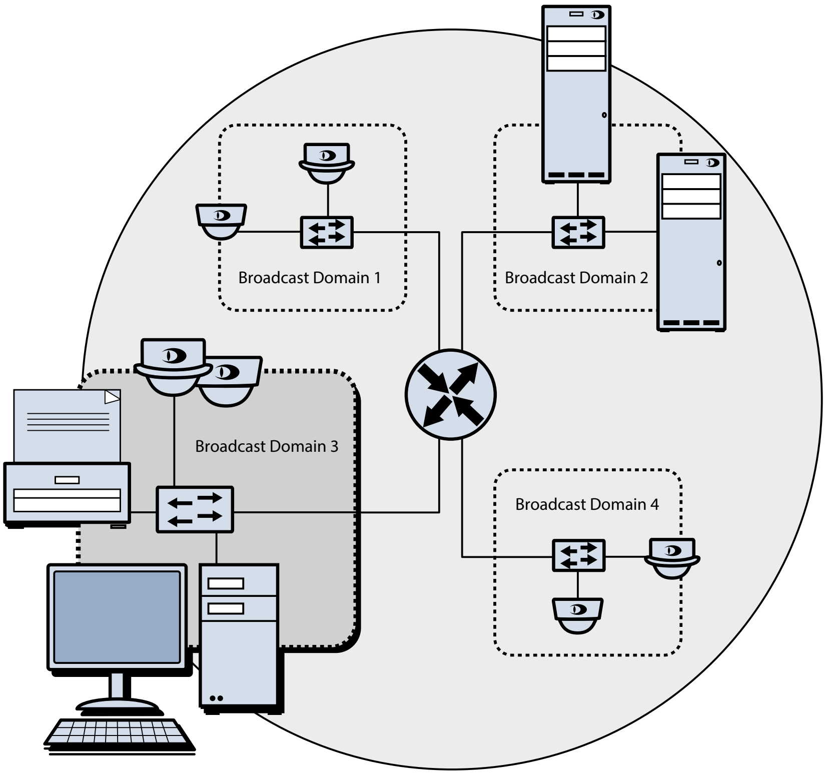

Fig. 2-2: Broadcast Domains

## 2.8 SFP PORT

The SFP (Small Form-factor Pluggable) is a port that allows for the connection of a SFP module (also known as “miniaturized Gigabit Interface Converter” or “mini GBIC”) in order to link Ethernet transmission media, such as fibre channels (optical fibre) or twisted pairs (twisted wire pairs made out of copper), in the network.

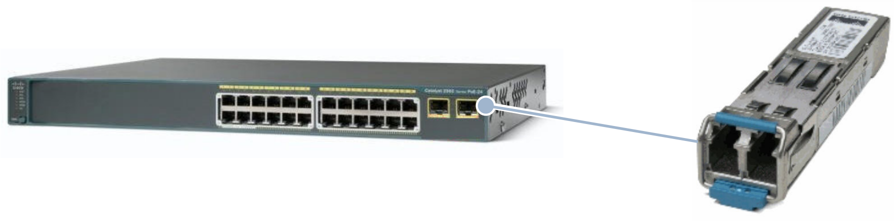

Fig. 2-3: Example of a SFP Interface with a matching module

### 2.8.1 SFP Twisted Pair Cable Types

Shielded twisted pair (STP) respectively foiled twisted pair (FTP) cables have four copper wire pairs. One pair consists of two strands, totaling eight strands per cable. Each of these wire pairs is surrounded by a pair shield (S = wire mesh shield or F = foil shield).

Unshielded twisted pair (UTP) cables are made out of copper as well, and generally have the same structure as STP/FTP cables, but without a pair shield. Consequently, UTP cables are more susceptible to external electromagnetic interferences. STP/FTP/UTP cables come in several variants which differ in material and in the presence of an overall shield.

### 2.8.2 SFP Fibre Cable Types

With single-mode fibres (SMF), a single laser light beam is transmitted through the middle of the fibre. This kind of fibre optic transmission is particularly suited for long transmission paths.

With multi-mode fibres (MMF), a LED is used for transmission. The LED does not send a bundled light beam through the cable, but rather emits multiple light beams with different angles of incidence.

| Name | Cable Type | Maximum Length |
|---|---|---|
| 10BASE-T | UTP / STP | 100 m (approx. 109.36 yd) |
| 100BASE-TX | UTP / STP | 100 m (approx. 109.36 yd) |
| 1000BASE-T | UTP / STP | 100 m (approx. 109.36 yd) |
| 1000BASE-CX | STP | 25 m (approx. 27.34 yd) |
| 100BASE-FX | MMF | 2 km (approx. 1.24 mi) |
| 1000BASE-SX | MMF | 500 m (approx. 546.81 yd) |

| Name | Cable Type | Maximum Length |
|---|---|---|
| 1000BASE-LX | MMF / SMF | 550 m (approx. 601.49 yd) /<br>10 km (approx. 6.21 mi) |
| 1000BASE-ZX | SMF | 70 km (approx. 43.5 mi) |
| 10GBASE-ZR | SMF | 80 km (approx. 49.71 mi) |

Table 2-3: SFP cable types

### 2.8.3 Dual-Purpose SFP Port

The dual-purpose is a port that allows for the connection of a SFP module or a RJ45 connector in order to link to the network.

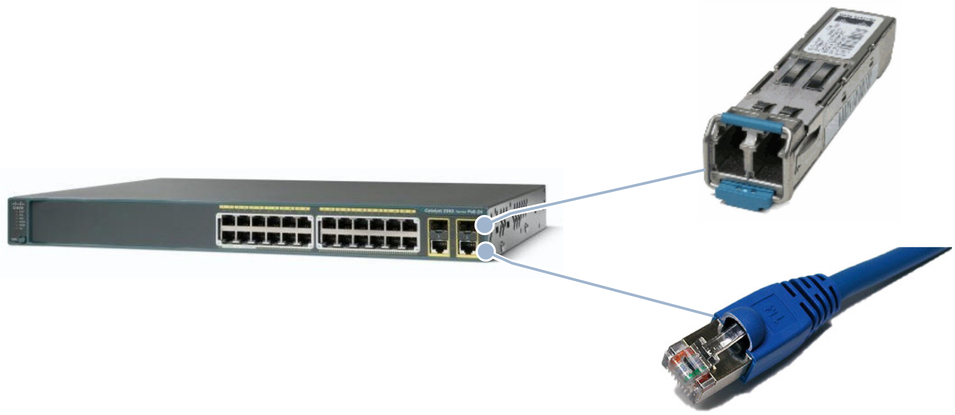

Fig. 2-4: Example of a Dual-Purpose interface

## 2.9 QUALITY OF SERVICE

Quality of Service (QOS) is a packet prioritisation which ensures that time-critical or essential applications are treated preferentially in terms of receiving their data over the network. There are two mechanisms for QoS:

### 2.9.1 Integrated Services

With Integrated Services (IntServ) required bandwidths are already pre-reserved on the individual network devices. In order to implement this mechanism correctly and completely, it must be supported by all network components.

### 2.9.2 Differentiated Services

With Differentiated Services (DiffServ) data packets are marked and processed by the network according to the configuration.
In practice, DiffServ has meanwhile won out over IntServ due to a better scalability and a higher compatibility.

## 2.10 SPANNING TREE PROTOCOL

The spanning tree procedure, which's task it is to prevent loops (parallel connections) in switched Ethernet networks and disable redundant paths, operates on the MAC layer (layer 2).

A loop can cause significant malfunctions within a network (particularly with regard to "broadcast storms"). In order to prevent such functional disorders, Spanning Tree Protocol (STP) covers the existent physical network with a "spanning tree" in which each destination is available by a single path only. Redundant connections are eliminated by deactivation of the respective ports. Which connection is terminated, depends on its quality.

The logical spanning tree is established with the bridge protocol (following communication among the switches (if STP capable)) by defining a root bridge (root of the spanning tree). The data packets used here are called "Bridge Protocol Data Units" (BPDU). They are distributed throughout the network from switch to switch by means of broadcasts. After the tree structure is established, a status report (Keepalive) is cyclically output by the root bridge from one switch to the, in each case, subsequent switch every 2 seconds.

If one of these status reports fails, there has been a change within the network (e.g. a network connection or switch failure) and the network must reorganized itself. This reorganization process includes the deletion and reestablishment of the logical spanning tree. With STP, this can last up to 30 seconds. During that period of time, all communication within the network other than the spanning tree protocol is blocked.

Since in the past such downtimes were not acceptable in certain situation, the rapid spanning tree protocol (RSTP) was introduced as a further development of the spanning tree protocol. With this upgrade, the net is no longer blocked immediately after the failure of a status report, but an alternative route is identified parallel to the regular network operation. As soon as the calculation of the alternative is successful, the current structure (faulty) is replaced by the new calculation. Consequently, the duration of network outages can be limited to less than one second.

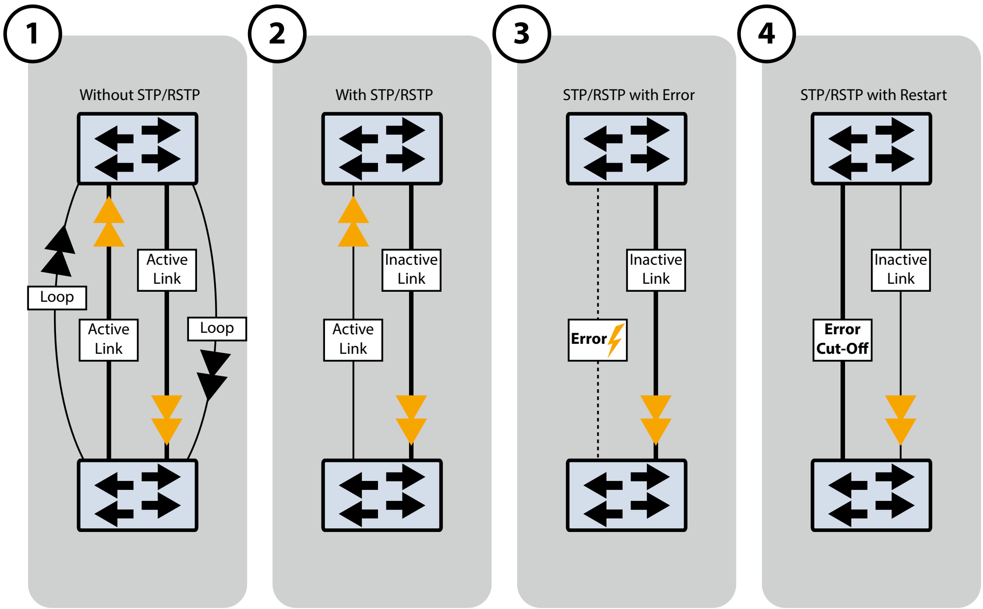

Fig. 2-5: STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol)

## 2.11 ENCODER AND DECODER

In the following descriptions a network capable device is called an encoder if its main task is to capture, encode and distribute video data, such as e.g. a network camera.

A network capable device is called a decoder in the following descriptions if its main task is to receive, decode and display video data, such as e.g. a workstation with client software for evaluation of the video footage.

## 2.12 UNICAST AND MULTICAST

### 2.12.1 Unicast

Unicast is a connection established between a sender (encoder) and a receiver (decoder). Consequently, a separate transmission channel is initialized for each connection established between a client and a recording device or camera. The more viewers there are, the more connections are needed which can lead to an overload of the network as well as of the sender (e.g. camera overload).

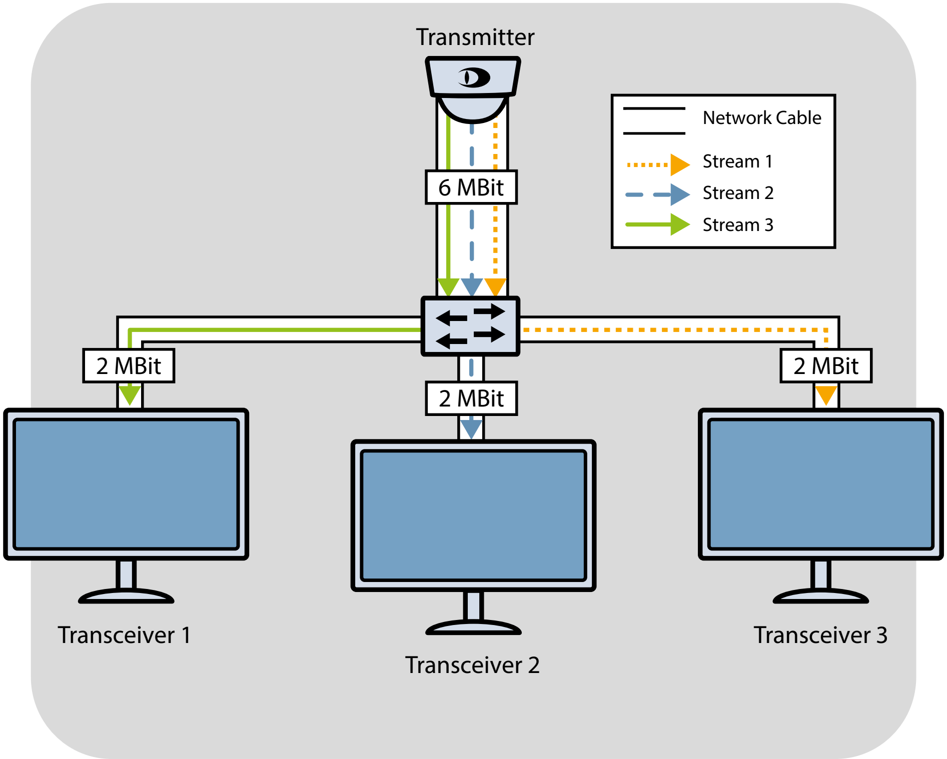

Fig. 2-6: Example for Unicast

### 2.12.2 Multicast

Multicast is a connection established between a sender (encoder) and several receivers (decoders). It allows for the transmission of a data stream from a sender (via a single channel) to as many participants as desired. Consequently, multicast can significantly reduce the amount of network traffic caused by the multiple display of cameras. For this purpose, the sender receives a particular additional IP address (group address) from within the multicast range 224.0.0.0 through 239.255.255.255.

The participants log in using the Internet Group Messaging Protocol (IGMP). The involved network components, such as routers or switches, have to ensure that, if possible, only the desired and required multicast streams are transmitted. For multicast, the addresses in the range 225.x.x.x through 232.x.x.x and 234.x.x.x through 238.x.x.x are available without restriction. For the local application, the range between 239.x.x.x and 239.255.255.255 is recommended, since it is not marked as public and not routed into the internet.

*The address details are nonbinding. Therefore, adhere to the current specifications and guidelines concerning the individual address ranges!*

In order to use multicast (IGMP) it must be supported by all participating components (switch, camera, recording server). A single multicast incapable network component can affect the entire function. Multicast makes relatively high demands on switches.

*Dallmeier mainly uses multicast connections for the live transmission from encoder to decoder.*

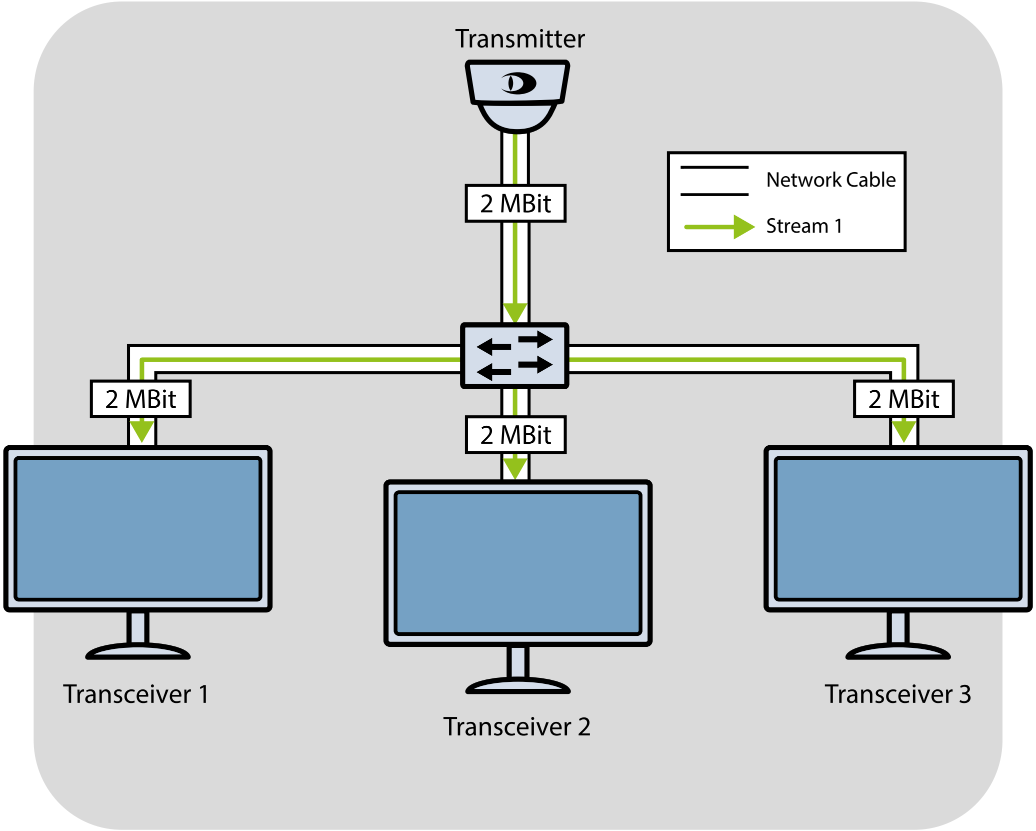

Fig. 2-7: Example for Multicast

## 2.13 INTERNET GROUP MANAGEMENT PROTOCOL

In general, switches flood the underlying network within a broadcast domain with multicast traffic in order to ensure that all multicast streams are transmitted to all areas of the network. The multicast stream is also transmitted to participants that actually do not want to receive it (so-called “flooding”). The consequence is, that a lot of bandwidth is demanded. Especially, if several senders, such as e.g., cameras, Panomera®, etc., are used, this thus leads to an overload of the network as well as of all the devices within the net, and prevents a controlled transmission from being able to come about.

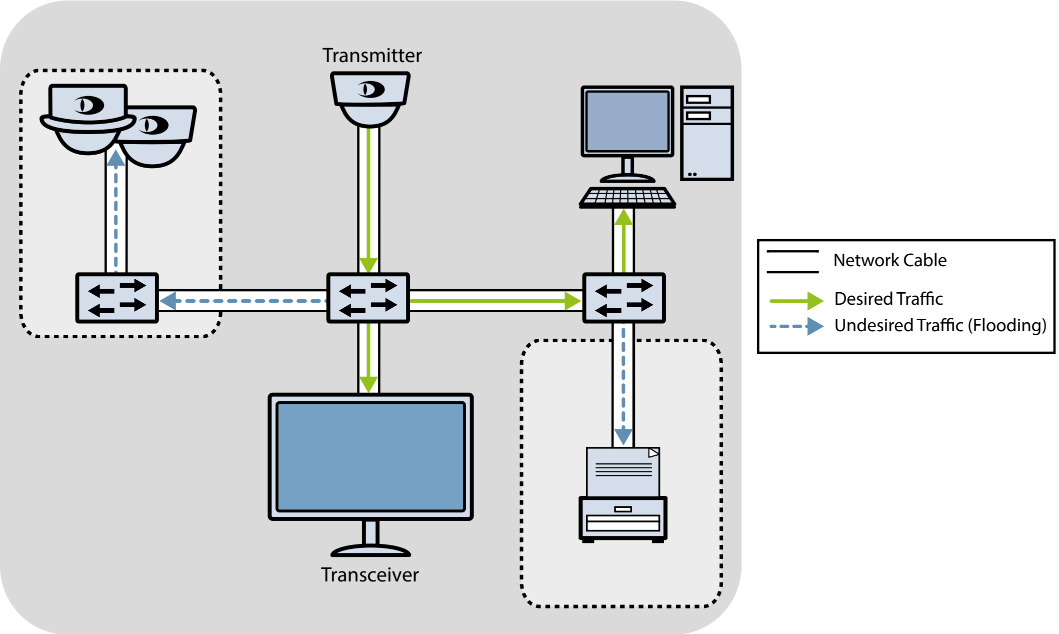

Fig. 2-8: Multicast traffic with IGMP

With the Internet Group Management Protocol (IGMP), the multicast traffic within a network can be limited, for it offers the possibility of managing groups dynamically. This management does not take place on the host device (camera, encoder), but rather within the switch to which the receiver of a multicast stream is connected. The receivers join a multicast group by sending a so-called “IGMP Join” command or by replying to a general request sent by the IGMP querier.

### 2.13.1 IGMP Querier

The IGMP querier is an administratively set “core switch” to which all multicast streams are sent. It is the receiver of all IGMP commands and, hence, manages the multicast groups. Only one querier at a time can be defined per net (broadcast domain). Furthermore, it is important to note that all multicast streams, including those that are not requested, are always sent to this querier.

*It is not possible to limit the multicast traffic towards the querier. That is why, the IGMP querier should be positioned as centrally and as close to the multicast sources (Panomera®, cameras, encoders) as possible. In addition, it is important to ensure that enough bandwidth is available on the way to the querier.*

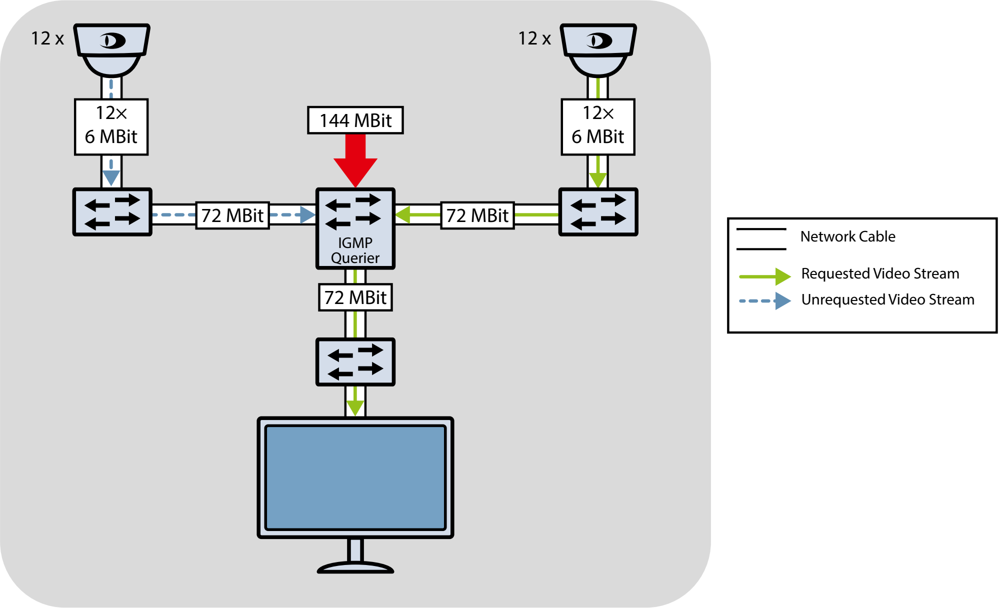

Fig. 2-9: Example for IGMP Querier

## 2.13.2 IGMP Snooping

IGMP snooping enables a switch to “eavesdrop” on the IGMP conversation between the multicast sender and the IGMP querier or between the multicast receiver and the IGMP querier, respectively. Based on this conversation each switch creates a list (membership list) for the multicast groups activated on the IGMP snooping and exclusively forwards the multicasts to the members of this group.

Now, if a device is unplugged or plugged into a different port, the switch would send multicast data to the wrong port. In order to prevent such a case, the IGMP querier cyclically requests all terminal devices to reveal their multicast group membership. The replies returned to such querier requests (IGMP reports) induce the switches to update their membership lists accordingly.

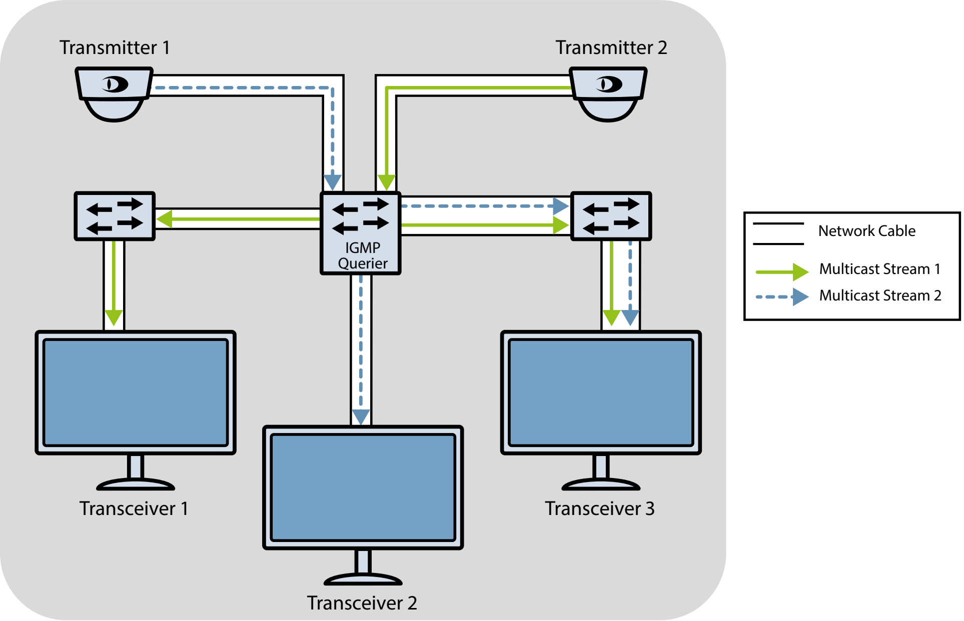

Fig. 2-10: Example for IGMP Snooping

## 2.14 PROTOCOL INDEPENDENT MULTICAST

Protokol Independent Multicast (PIM) is a collection of multicast routing protocols that works without reference to the primary routing protocols, such as RIP, OSPF, etc.. It creates a multicast routing table for the  existent multicast groups. PIM establishes a tree structure within the configured domain with branches to all of the connected networks. Actually, there had been two types of PIM of which, however, only PIM-SM was able to prevail.

With PIM-SM (Sparse Mode), a central point known as “Rendezvous Point” (RP) is created, similar to the IGMP querier in layer 2. Other routers send a “PIM Join” command to the RP in order to participate in the multicast.

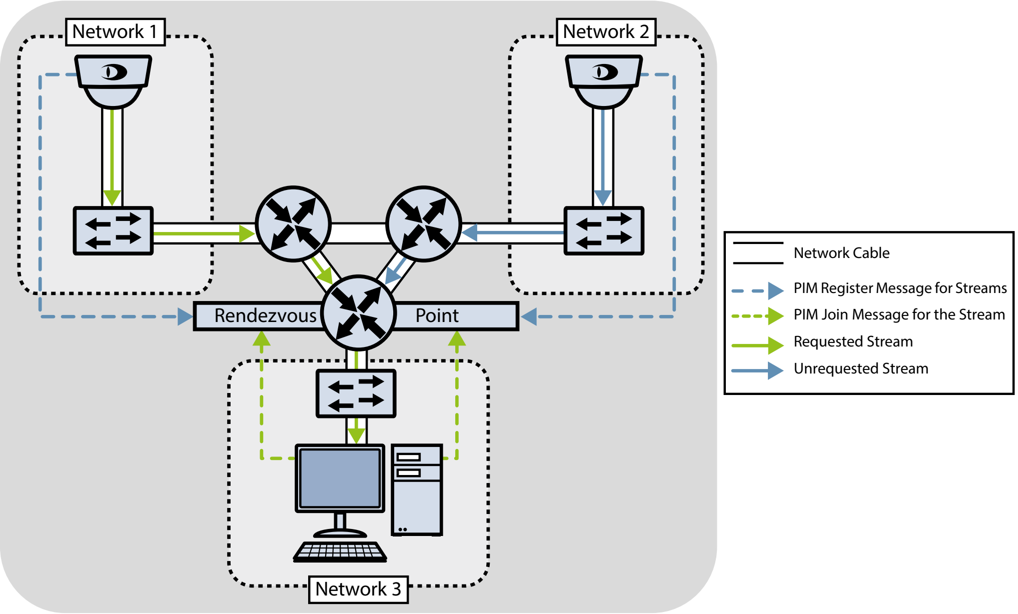

Fig. 2-11: Rendevous Point (RP) with PIM-SM (Sparse Mode)

*PIM(-SM) is primarily recommend in large networks with many multicast senders.*

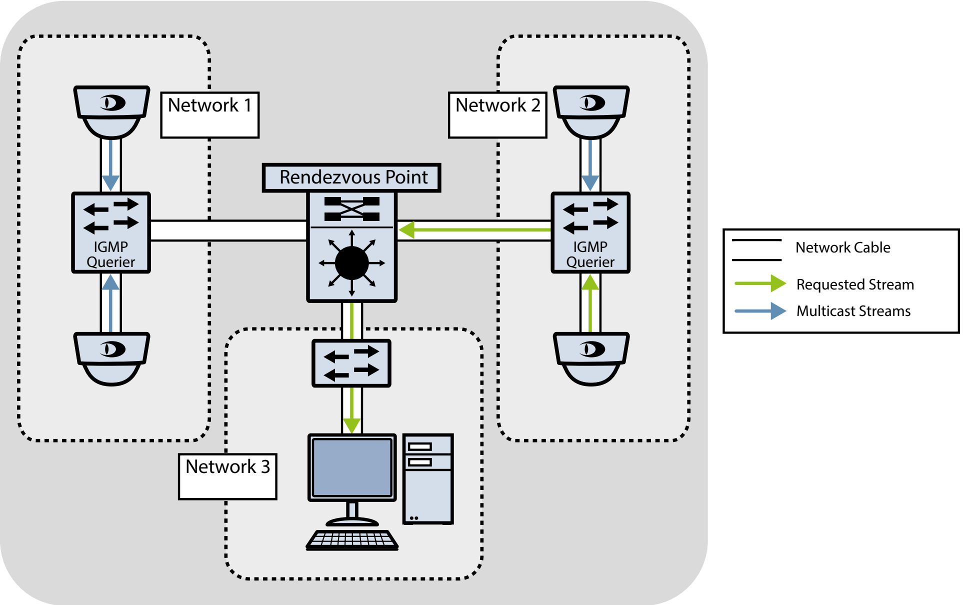

Fig. 2-12: Example for PIM(-SM) in a Large Network (Many Multicast Senders)

# EXAMPLES

## 3.1 UNICAST AND MULTICAST

If more than one decoder is to simultaneously display the live image of an encoder, the encoder within a unicast network must send the video stream over the network for every single decoder. Consequently, both network and encoder load increase significantly and can lead to errors such as jitter or image artifacts.

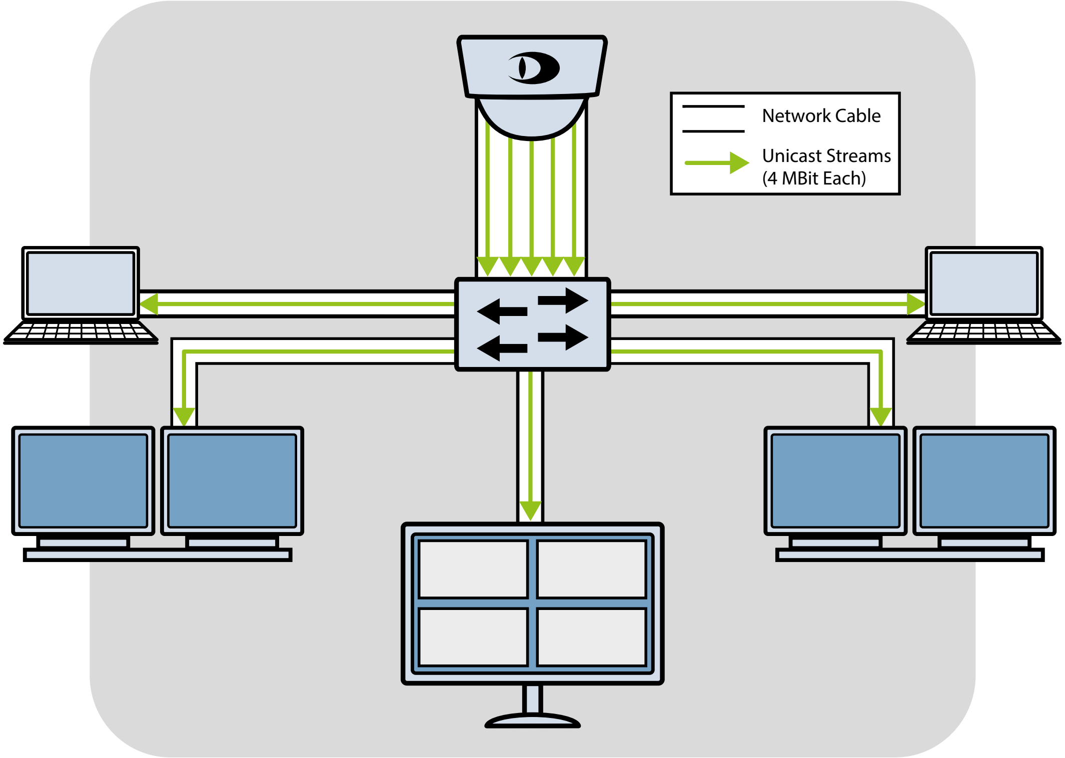

Fig. 3-1: Example for a unicast network

In this case, it is reasonable to set the encoders to multicast operation. Moreover, it is necessary to use switches that support multicast.

With multicast operation, the network load and particularly the encoder performance decreases considerably. The video stream is no longer individually sent to every single decoder, but only once to a multicast group. The task of forwarding to the individual decoders of the group is undertaken by the multicast capable switch.

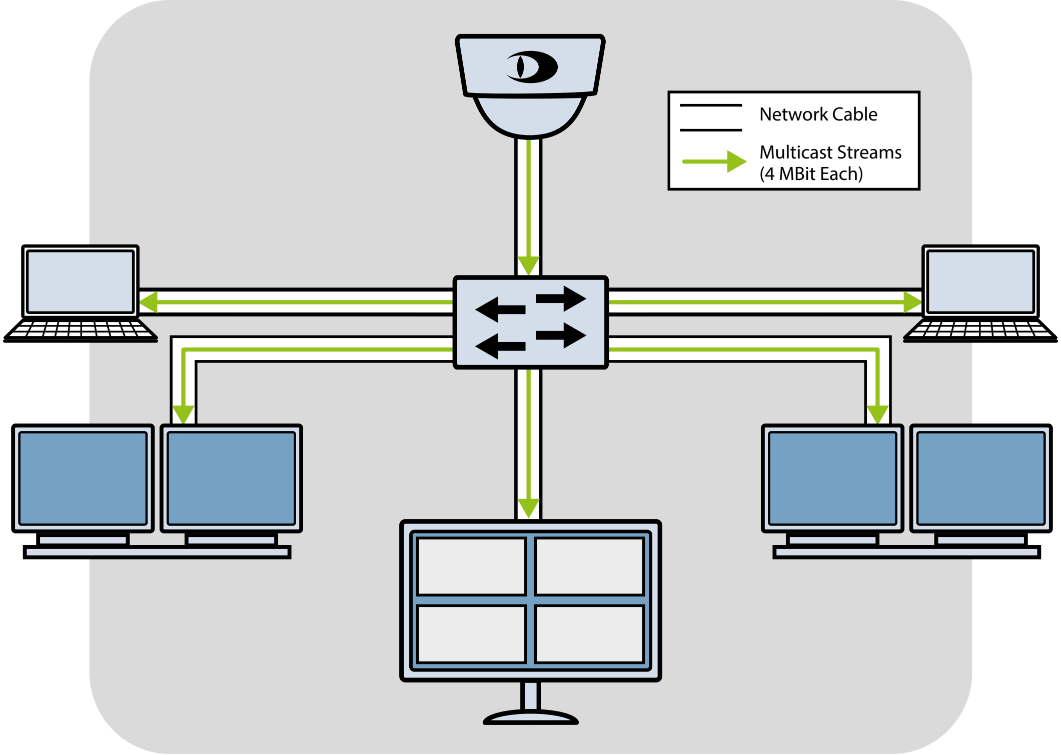

Fig. 3-2: Example for video streaming to a multicast group (IGMP V1)

)However, even in this case the network load is not ideal. Since the switch always sends the video stream to all of the decoders of the multicast group, whether the decoder is active and in need of or wants to display the live image, or not.

In order to optimize the network load and thereby ensure an error-free functioning of the system, it is recommended to always use a multicast switch that supports the IGMP V2 snooping function. This function monitors the communication between the switch and the decoder of a multicast group. Hence, a statement can be made which decoder is currently active and actually requires the video stream.

*There is no way for IGMP V1 to log off a multicast stream, whereas IGMP V2 does have this ability.*

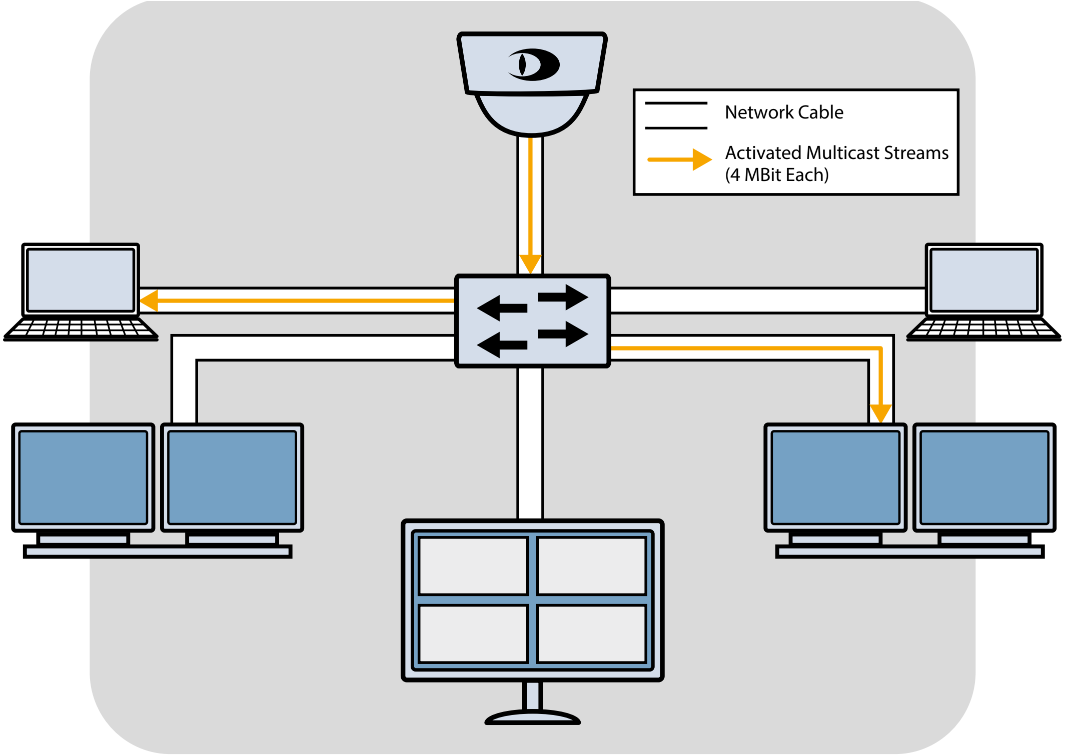

Fig. 3-3: Example for video streaming with a multicast switch (IGMP V2)

In conclusion, the switch no longer forwards the video stream to all of the decoders, but only to those that are relevant. Again the network load decreases considerably and can be regarded as optimized.

*In the following examples "live" or "live multicast" indicates, whether the switch fully and correctly supports the IGMP V2 snooping function. This function is required for all of the used switches in order to ensure full compatibility with Dallmeier network systems.*

## 3.2 SIMPLE VIDEO NETWORK

- Up to 24 cameras with 4 MBit/s each
- One recording server
- Two viewing clients with a 2×2 split each
  (4× 4 MBit/s = 16 MBit/s ×2, live direct off the camera, unicast)
- One switch
  (24× 100 MBit/s + 4× 1 GBit/s)

A video system with up to 24 cameras can easily be realized with only one switch. The cameras are operated at a bandwidth of 100 MBit/s and with PoE using the access ports of the switch. This constellation requires the recording server to be connected to a 1 GBit/s switch interface, since the bandwidth of the cameras, which are to be recorded, alone have a bandwidth of 96 MBit/s (24× 4 MBit/s). It must be considered that further bandwidth is needed in order to view the recording and for possibly required backup runs. Depending on how the viewing clients display their live image of the cameras (VIProxy, direct, multicast, PRemote, etc.), the bandwidth needed for this purpose must be accounted for as well when planning the network. In the current example, the live image is taken directly off the camera. Although this requires an additional connection to the camera, it preserves the server interface (contrary to proxy operation).

As a result, the viewing client can be operated on a 100 MBit/s interface (16 MBit/s (4×4 MBit/s) per client), yet it should be considered that not only live viewing, but possibly also backups and other functions are executed on the client. This is why, it is recommended to connect clients with a 1 GBit/s line to the switch as well. If needed, further accesses to the network can be realized with the remaining 1 GBit/s port.

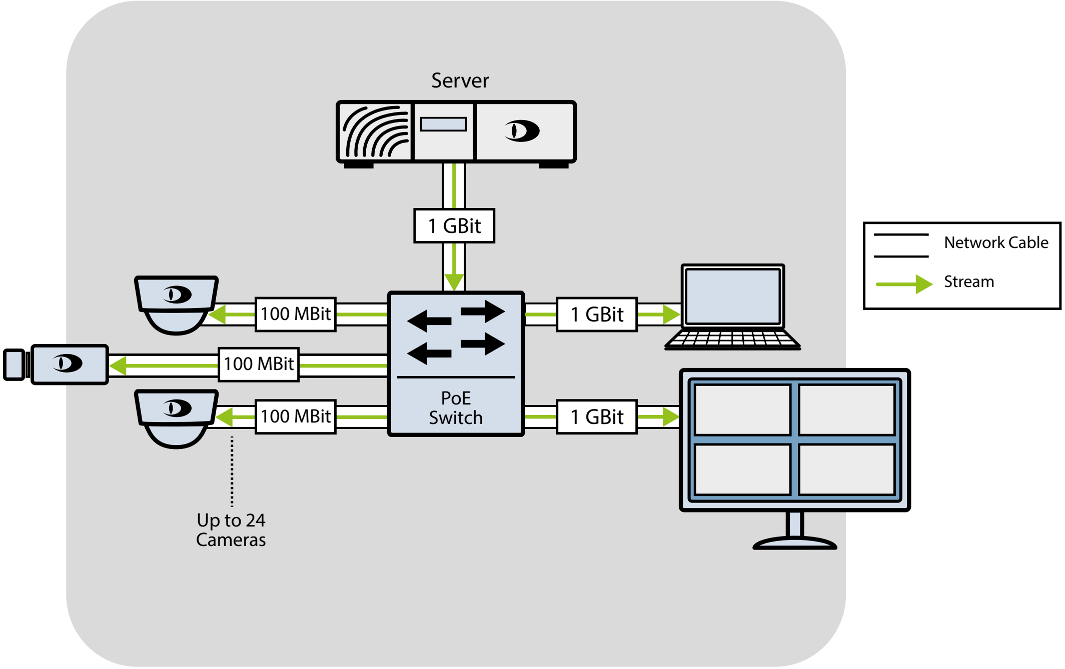

Fig. 3-4: Simple network

*Cameras, recording server and switch form a unit. Together with the clients they form a video network.*

## 3.3 MIDDLE-SIZE VIDEO NETWORK

- Up to 48 cameras
- Two recording servers
- Four viewing clients with one 2×2 split each
  (4× 4 MBit/s = 16 MBit/s ×4, live directly from the camera, unicast)
- Up to three switches
  (2× access switch with 24× 100 MBit/s + 4× 1 GBit/s and a core switch with 8× 1 GBit/s)
- Optionally, one further redundant core switch

A middle-size video network is realized in a similar way as described in the example before. The cameras belonging together and the recording servers are united on one switch as not to permanently strain the connection among the switches and to facilitate a required error search, wherever necessary (cameras, recording server and switch form a unit). Depending on the requirements and local conditions, two network structures are available to choose from.

The cheaper version is the "series connection" of the switches whereby the switches are interconnected in series over the uplink (preferably with 1 GBit/s). However, it must be considered that such a structure is not endlessly expandable. The limit is constituted by the uplink of the switch which is stressed most. Likewise, a series connection of the switches is more prone to failures. The connection to a external network is established either at the beginning or at the end of a series connection.

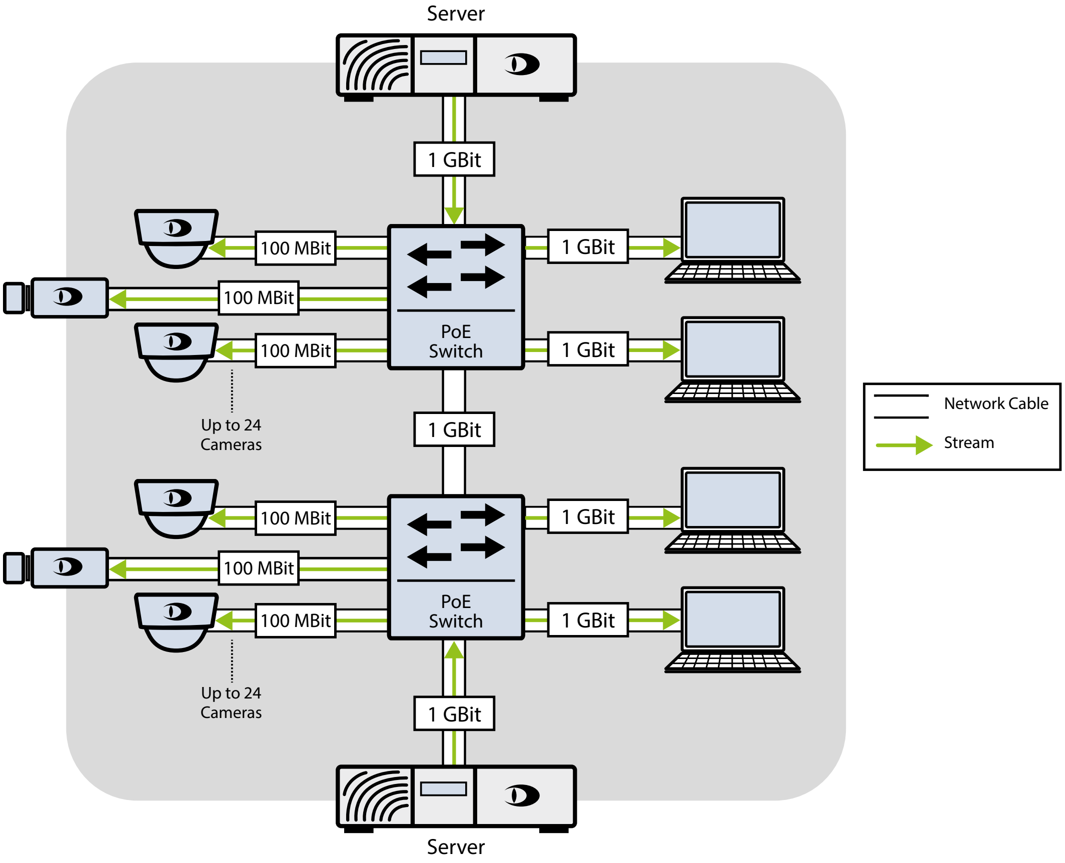

Fig. 3-5:: Series connection of switches (only reasonable up to a certain size)

The other option consists in shaping a star with the switches that are to be connected. The core of this network structure is represented by a core switch, which, depending on the requirements, can be set up for redundancy. The core switch is a particularly high-performance switch which establishes the connection between the access switches as well as other nets (with 1 GBit/s). This holds several advantages: short communication channels (maximum bandwidth), expandability, easy troubleshooting and low susceptibility to switch failures.

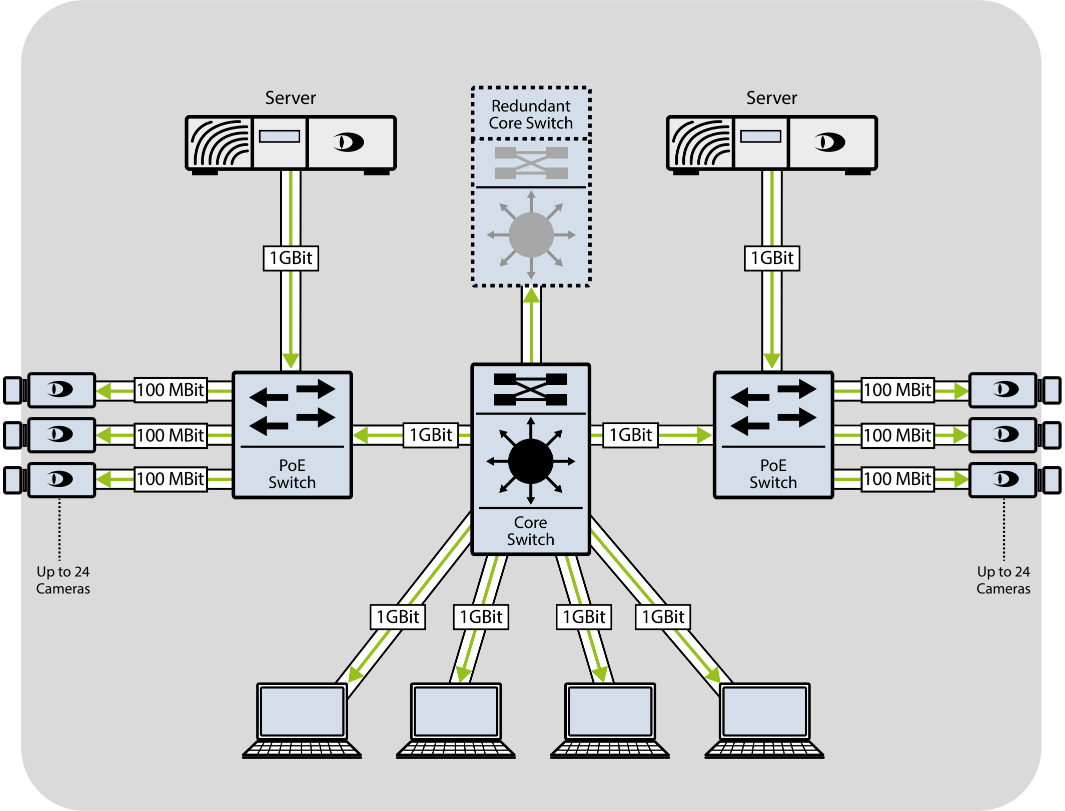

Fig. 3-6: Middle size network with core switch (optionally, a further redundant core switch)

## 3.4 LARGE VIDEO NETWORK

- More than 120 cameras
- More than five recording servers
- More than five viewing clients with one 3×3 split each
  (9× 4 MBit/s = 36 MBit/s ×5, live multicast off the cameras)
- Up to six switches
  (5× access switch with 24× 100 MBit/s + 2× 1 GBit/s, and one Core Switch with 24× 1 GBit/s)
- Optionally, one further redundant core switch

In a video network of this size, a star-shaped topology is inevitable. Otherwise, the transmission paths would be too long and the bandwidth would be to low. Since in this example many viewing clients are in operation, multicast is necessary in order not to overload the cameras with unicast (overload). If multicast (live transmission) is used, it is essential to ensure that all network components are multicast-capable (IGMP V2 Snooping).

As described in the previous example, all access switches, viewing clients and external networks are united on the core switch, with 1 GBit/s each. In order to prevent all of the clients from turning "blind" in cases of switch failures (single point of failure), the core switch can be used redundantly and compensate in an emergency situation. Thus, the recording is not affected by the loss of the core switch, each server stays connected to its cameras on the own switch and is self-sufficient with regard to the rest of the network.

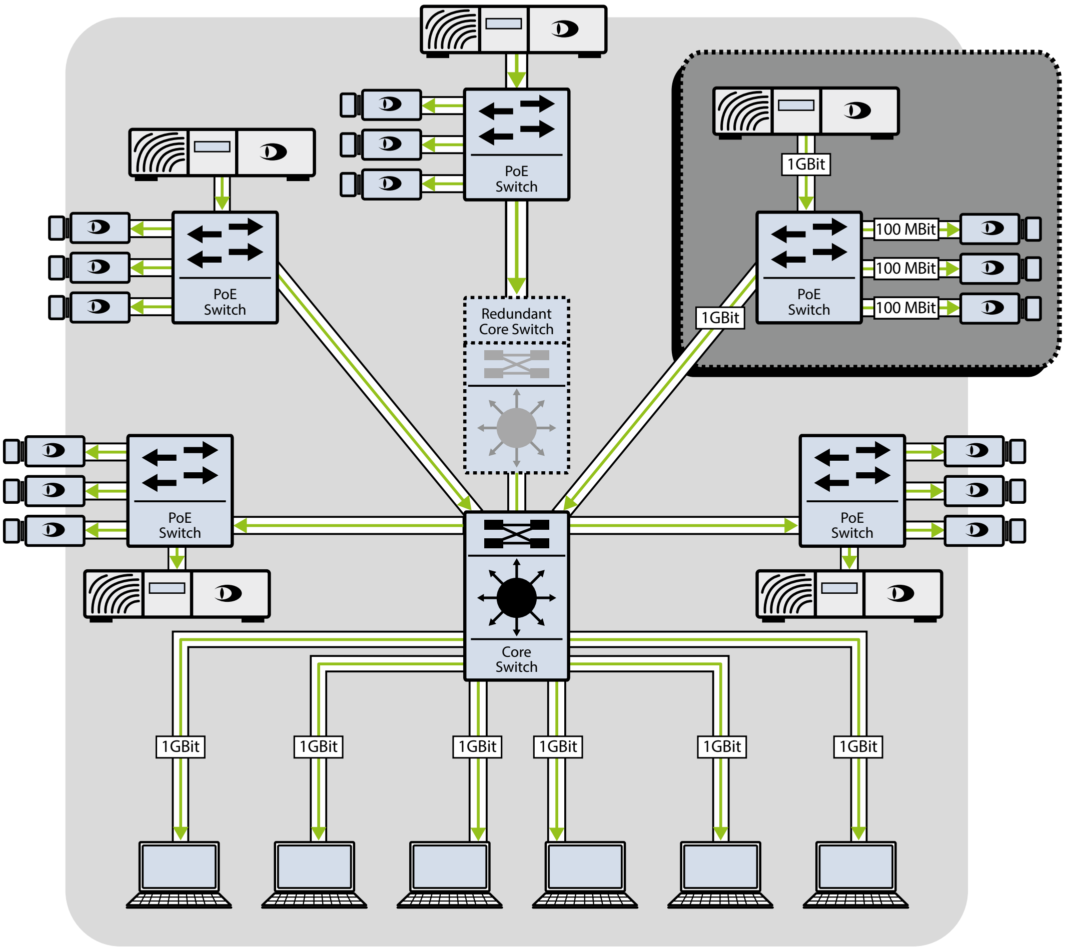

Fig. 3-7: Large network (with a star-shaped structure)

# IMPORTANT NOTES

- Make sure to operate the video network as self reliant as possible, since the functioning of the remaining network structure might be impaired by peak loads or, more generally speaking, by reaching the performance limits (communication with servers, printers, etc. fails).

- If possible, use products of only one manufacturer in order to prevent incompatibility.

- Ensure an equipotential bonding of the individual components at all times (also see white paper "Structured Cabling, Earthing & Equipotential Bonding").

- When selecting a PoE switch, the different performance classes (PoE/PoE+) of the Dallmeier cameras are to be considered (see data sheets).

- Ensure that a sufficient total PoE output power is available.

- Select a switch capable of sequentially switching on the PoE ports.

- The increased power demand for cameras with integrated IR illuminators during low light conditions is to be considered (see data sheet).

- A switch is the centrepiece of a digital video system and the single point of failure (pay attention to quality and perhaps create redundancies).

- A correct copper cabling (CAT-5E or better) with a maximum of 100 m (approx. 109.36 yd) per cable segment is prerequisite (also consider the maximum lengths for optical fibre).

- The configuration of a manageable switch requires special knowledge; consult an expert, if necessary.

- Take your time to foresightedly plan the structure and bandwidth.

- For (standard) cameras, a 100 MBit/s port is sufficient.

- Recording servers should be connected to a 1 GBit/s port.

- Uplinks should provide for a higher bandwidth (at least 1 GBit/s).

[THIS PAGE WAS INTENTIONALLY LEFT BLANK]

HEAD & ACCOUNTS OFFICE

Dallmeier electronic GmbH & Co.KG
Bahnhofstr. 16
93047 Regensburg
Germany

tel +49 941 8700 0
fax +49 941 8700 180
mail info@dallmeier.com

www.dallmeier.com