Bosch IP Video Networks

en Bosch IP Video Manual

Table of Contents

1 Introduction

This manual collects important information for different target groups on the requirements that Bosch IP Video products have on networks.
The target groups are:

– Pre-sales persons
– Persons who manage Bosch IP Video projects
– Persons who perform installations and configurations

The purpose of this manual is to cover only those IP technologies that are relevant for Bosch IP Video networks. It is not the goal to serve as compendium or textbook for IP network technology in general. Readers who are not familiar with IP network technologies should first improve their knowledge in this field before starting to read this manual.
Product documentation and data sheets are deciding when you find information in this manual which seems doubtful.

Outline of this manual

Chapter *2* gives examples for different Bosch IP Video network scenarios.
Chapter *3* explains basic terms and network concepts.
Chapter *4* lists the Bosch IP Video networks key features and provides detailed descriptions on network concepts like multicast used to achieve these key features.
Chapter *5* provides important information to start planning Bosch IP Video networks like formulas for bandwidth and storage calculations.
Chapter *6* gives hints on planning Bosch IP Video networks and shows some example scenarios.
The following illustration shows this outline:

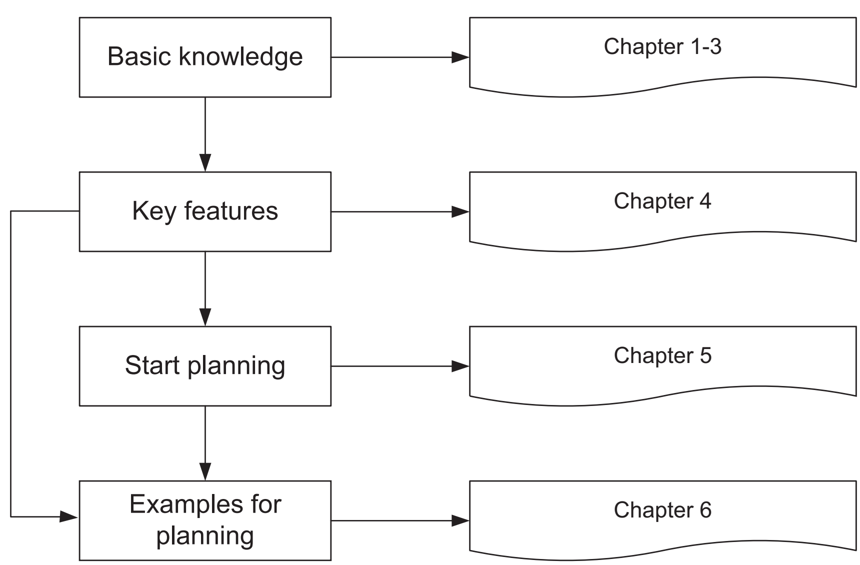

Figure 1.1 Outline of this manual

Who should read what?

Pre-sales persons should adjust their knowledge on basic network concepts and they should know the key features of Bosch IP Video networks (chapter 1-4).
Project managers should also adjust their knowledge and read chapters 1-4. They can continue in chapter 6 to pick up examples for planning that are of interest for them.
Supporters who must install and maintain Bosch IP Video networks can complete their knowledge on key features in chapter 4 and can concentrate on chapter 5 and 6.

VRM vs. NVR recording solution

This manual describes some examples with an NVR recording solution, others with the VRM recording solution. Our strategy is to remove the NVR recording solution completely and exchange it with the VRM recording solution in the next couple of years.

Enhancements planned for the future

The following topics are planned to be covered in the next release of this manual:

- Network redundancy
- Verifying networks
- Storage technologies

For detailed troubleshooting information on specific issues see the Bosch ST Product Knowledge Base (`http://knowledge.boschsecurity.com`).

Used network icons

The following illustration provides a legend for the used network icons:

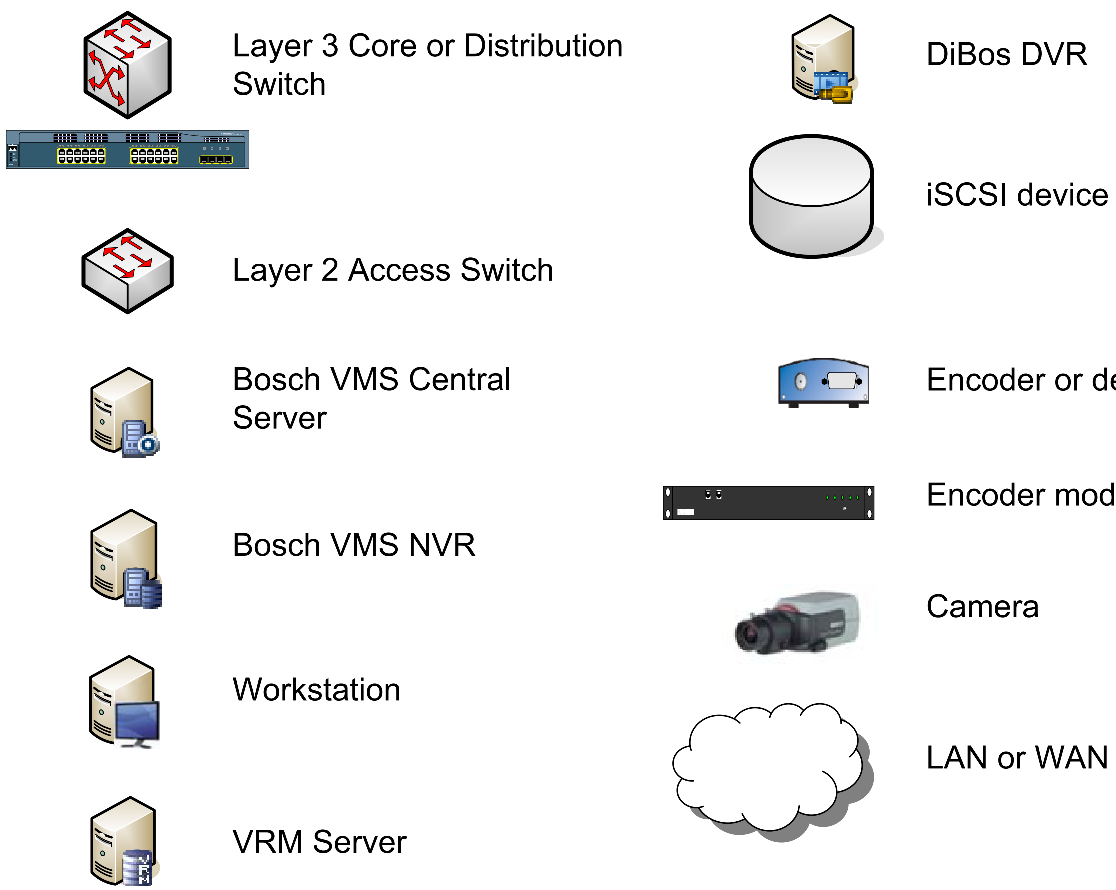

Figure 1.2 Used network icons

2 Examples for Bosch IP Video network solutions

The following sections give some examples on how to use a Bosch IP Video network solution for different CCTV scenarios. These examples do not cover the whole range of Bosch IP Video network solutions but only give a first impression.

Remote view on a PC

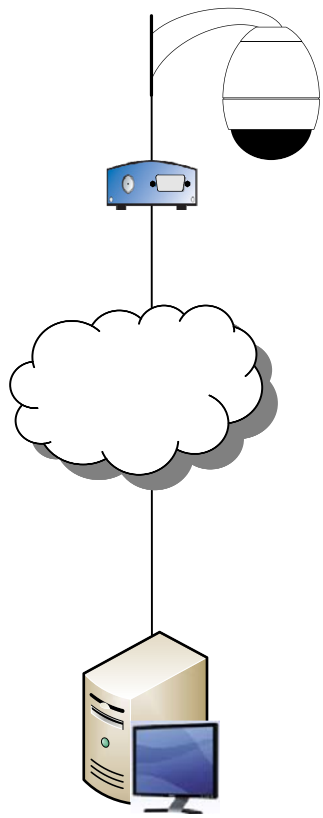

Figure 2.1 Remote view on a computer

This example shows a PTZ camera with an encoder connected to a workstation via a small network.

This offers the following features:

– View, control and record video on PC
– Intercom audio to talk to remote end
– Remote telemetry
  PTZ in-window controls, control matrix, DVR

Remote view on a monitor

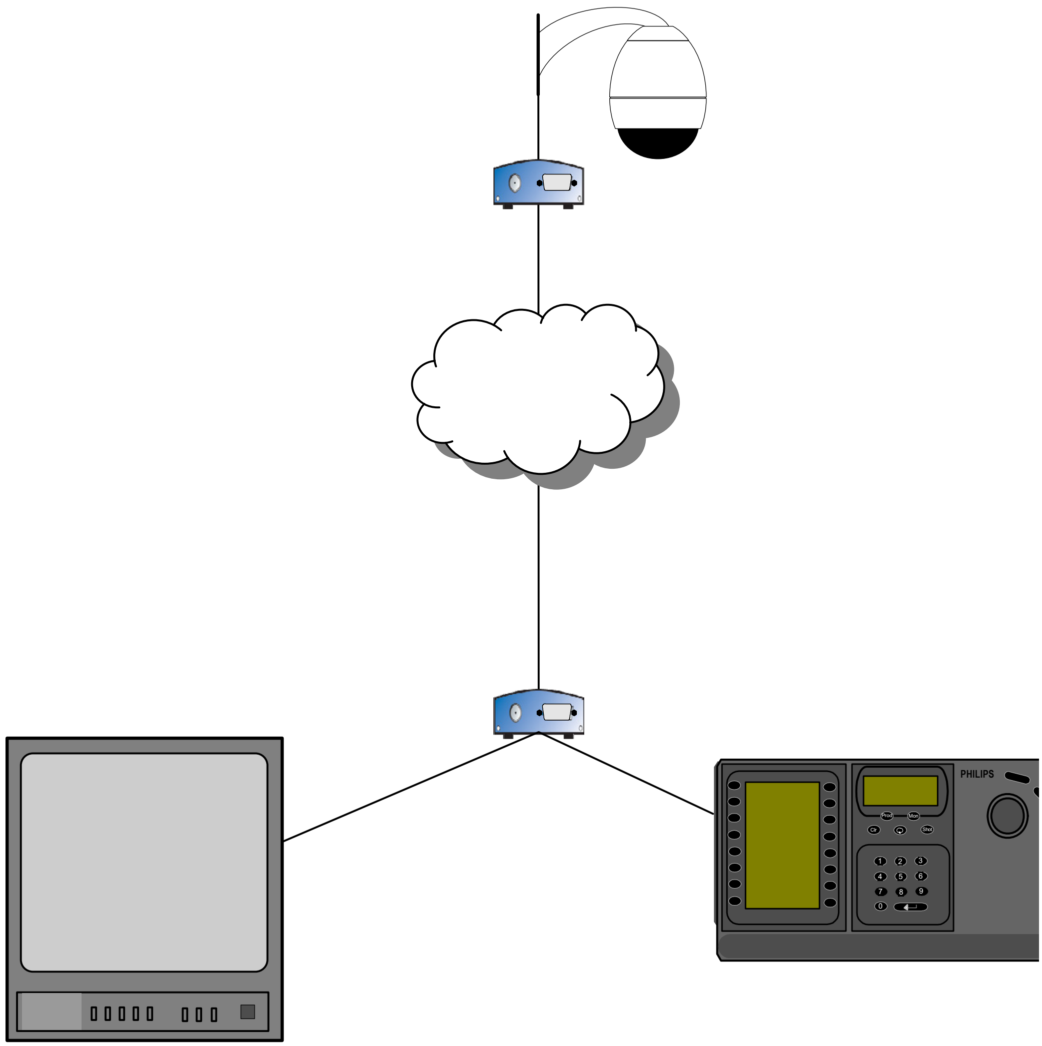

Figure 2.2 Remote view on a monitor

This example shows a PTZ camera with an encoder connected to a decoder via a small network. The decoder is connected to an analog monitor and an IntuiKey keyboard.
This offers the following features:

– View on a standard CCTV monitor
– Intercom audio to talk to remote end
– Supports RS232 keyboards and control pads, PTZ control, control matrix, DVR

CCTV observation system

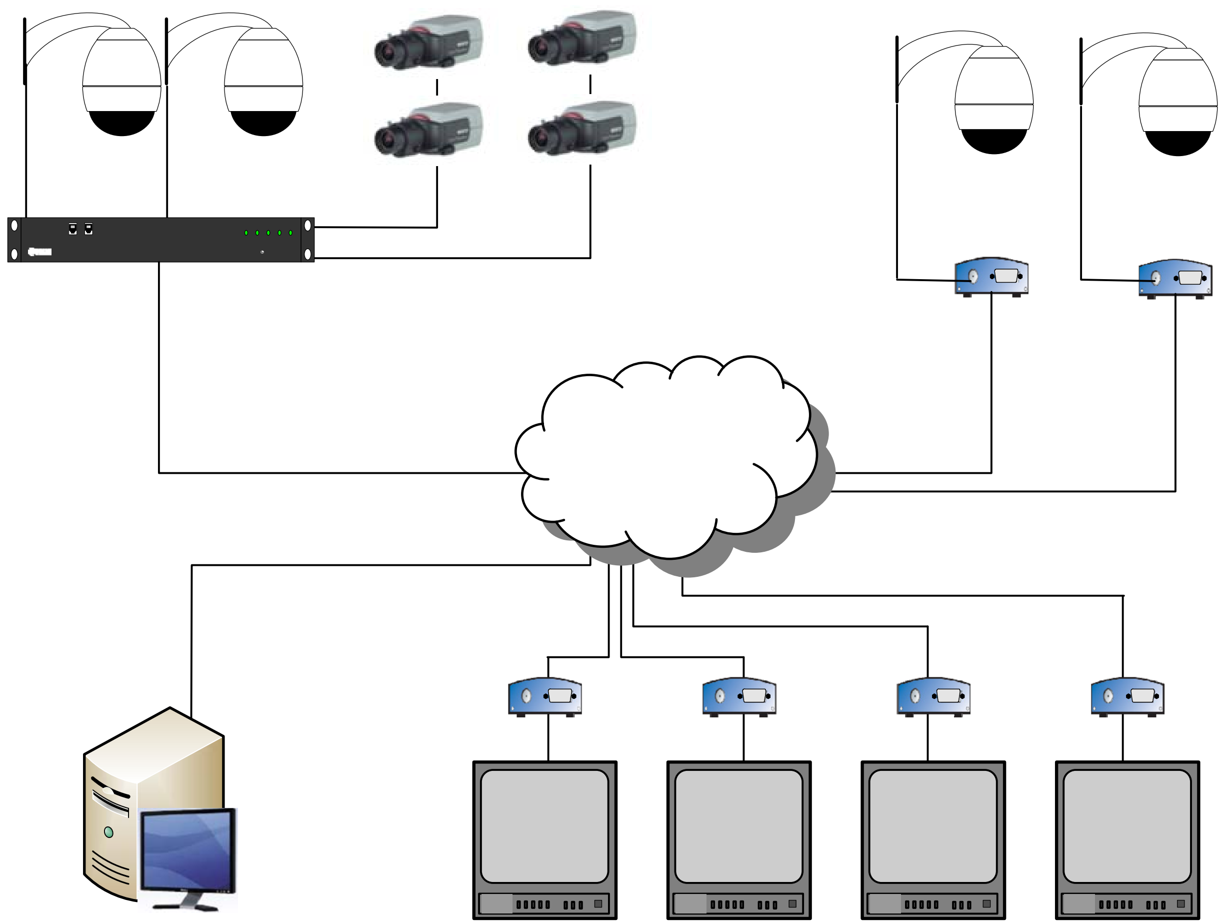

Figure 2.3 CCTV observation system

This example shows a number of various cameras with encoders connected to a workstation and to decoders via network. The decoders are connected to analog monitors.

This offers the following features:

– Flexible, expandable, remote CCTV
– VIDOS or Bosch VMS management application
– Comprehensive user interface supports in operation tasks
  Push-buttons and/or site map interface
  PC and CCTV views, switch view on alarms
  Snapshots, in-window PTZ control

Digital recording at the edge

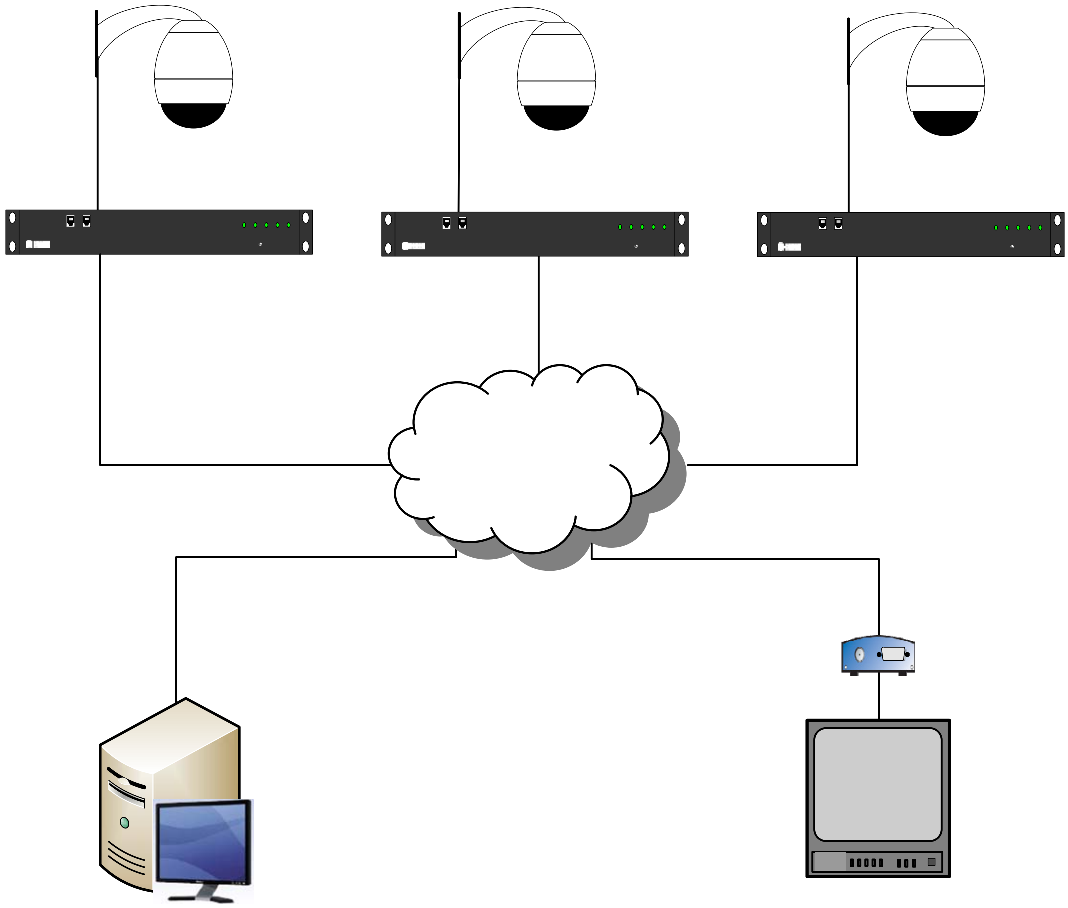

Figure 2.4 Digital recording at the edge

This example shows some PTZ cameras with encoders connected to a workstation and a decoder via network. The encoders have their own storage built in.

This offers the following features:

- Simple, reliable, high-quality
- From 18 hours to 1 week recording
- View at one quality, record at another, recording uses no network bandwidth
- Autonomous, set-up and playback with Web and/or VIDOS / Bosch VMS

Multi-site CCTV

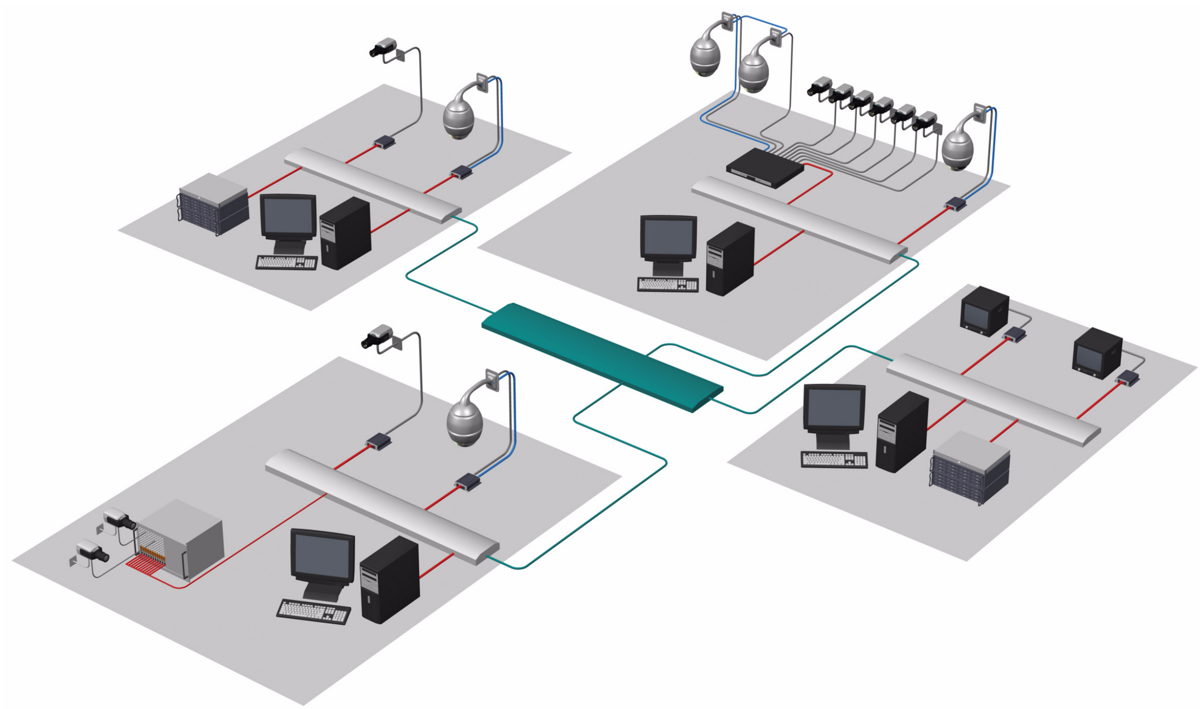

Figure 2.5 Multi-site CCTV

This example shows a number of various cameras with encoders located in different places connected to a workstation via network. The various locations are also connected via network. Each location has its own storage using various technologies for recording.

This offers the following features:

- Central monitoring of remote sites
- Retail stores, banks, train stations, local government schools, libraries, etc.
- Record locally, view remotely or ...central recording...or a combination
- Manage with Bosch VMS or VIDOS

NOTICE!

Note the limits for example in the number of recorded cameras that Bosch VMS cannot exceed!

Large-scale CCTV

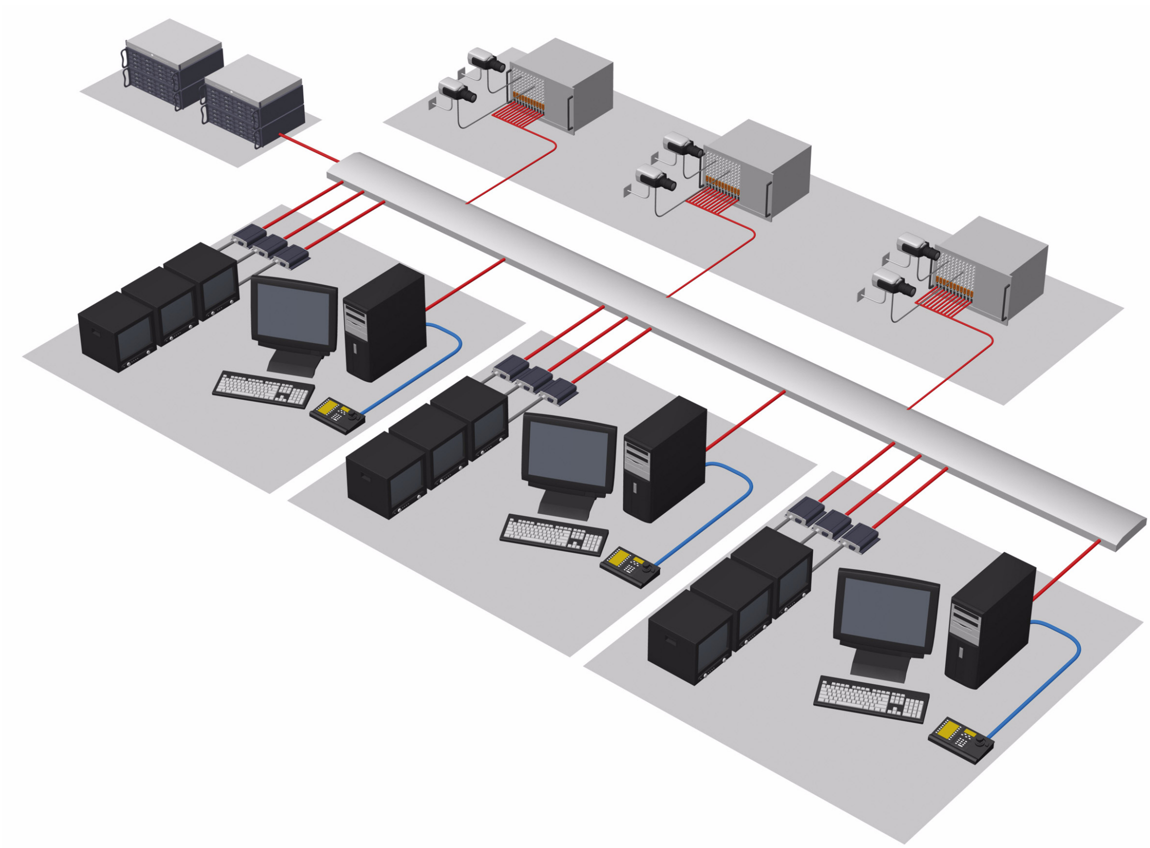

Figure 2.6 Large-scale CCTV

This example shows some IP cameras connected to its own storage and connected to a central storage and to workstations and decoders via network.The decoders are connected to analog monitors. The workstations are connected to IntuiKey keyboards.

This offers the following features:

- Only IP has the scalability and flexibility
- Any camera on any monitor, record any camera, playback to any monitor
- Multiple viewers, dispersed locations, recording remote from cameras
- Lowest cost adds and changes

NOTICE!
Note the limits for example in the number of recorded cameras that Bosch VMS cannot exceed!

3 General network concepts

This section provides the general network concepts that we use to realize Bosch IP Video networks.
This chapter covers the following:

- *Section 3.1 OSI 7 Layer Model*
- *Section 3.2 Hubs and switches*
- *Section 3.3 Routers and Layer 3 switches*
- *Section 3.4 Unicast – broadcast – multicast*
- *Section 3.5 IP addresses*
- *Section 3.6 Ports*
- *Section 3.7 VLAN*
- *Section 3.8 Network models*
- *Section 3.9 Centralized or decentralized recording*

3.1 OSI 7 Layer Model

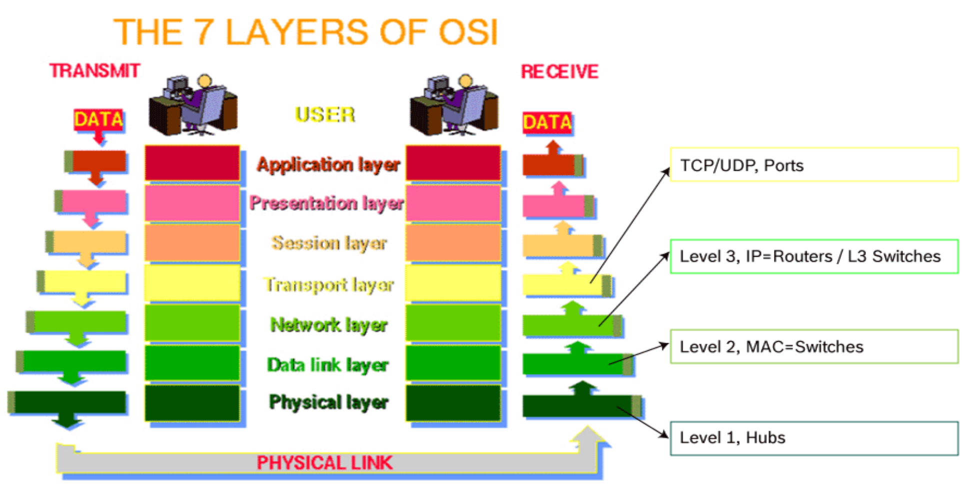

Figure 3.1 OSI 7 Layer Model

Switches can either be Layer 2 switches or Layer 3 switches. Layer 2 switches are switching based on MAC addresses. A MAC addresses is a 48-bit hexadecimal address burned into a chip on a network interface card (NIC), for example: 00-17-A3-CE-C6-5F. This MAC address is unique for each network device.
Layer 3 switches offer a wider variety of features, for example they can filter for IP addresses or can perform cross-network routing.
Hardware driven and software driven Layer 3 switches are available. Hardware driven switches are faster but more expensive. In Bosch IP Video networks hardware driven switches should be preferred.

3.2 Hubs and switches

This section provides basic knowledge on switch selection as it pertains to Bosch IP Video networks.
Hubs/repeaters and switches allow the physical media of network interfaces to connect.
Hubs/repeaters send the IP packets to all hosts in the segment. In Bosch IP Video networks hubs and repeaters are not used.

A **switch** is a networking device that connects network segments. Layer 2 switches forward data at the Data Link Layer of the OSI model, Layer 3 switches forward data at the Network Layer of the OSI model.
Forwarding packets in Layer 2 is based on MAC addresses. The switch builds a MAC address table where it learns which device is connected to which port. This gives the switch the ability to create unicast sessions between clients with full duplex communication.
Section 3.3 Routers and Layer 3 switches describes Layer 3 switches.

Key features in a switch used for Bosch IP Video networks:
- VLAN support
- Manageable
- Cut-through or fragment-free switching
- Rapid Spanning Tree Protocol
- SNMP
- Port mirroring (for error analysis)
- IGMP snooping (IGMPv.2 or greater)
- Multicast routing (for Core switches only)

And if you have decided to implement multicast now or in the future:
- Your switch should be hardware driven.
- The chip must be able to perform multicast queries.
- The number of possible multicast groups must be considered.
  See *Section 3.4 Unicast – broadcast – multicast* for details.

Notes:
A 1 Gbit switch should handle maximum approximately 250 cameras with 2 Mbps. This reserves an overhead of approximately 50%. If you have more than 250 cameras attached to a 1 Gbit switch, redesign your network.
Avoid stacking switches: A “master” switch manages all other switches. This master switch’s traffic gets priority. With video this can cause connection losses.

3.3 Routers and Layer 3 switches

Routers forward data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs or a LAN and its ISP’s network.
Today routers are mostly replaced by Layer 3 switches. The difference is that a Level 3 switch only routes the first bit of a stream to a specific target and switches the other bits. A router routes all packets.

NOTICE!
Do not use WLAN in Bosch IP Video networks managed with Bosch Video Management System. The reason is that especially Bosch VMS needs a reliable and persistent network connection. If for example an Operator Client is disconnected by network interruptions the user must again log on to the computer.
In networks without Bosch Video Management System, WLAN can cause recording gaps and frame losses in Live video.

3.4 Unicast – broadcast – multicast

Unicast is a 1:1 communication.
Broadcast is a 1:all communication.
Multicast is a 1:n communication where n is a part of all.
The following illustration shows the difference between unicast and multicast.

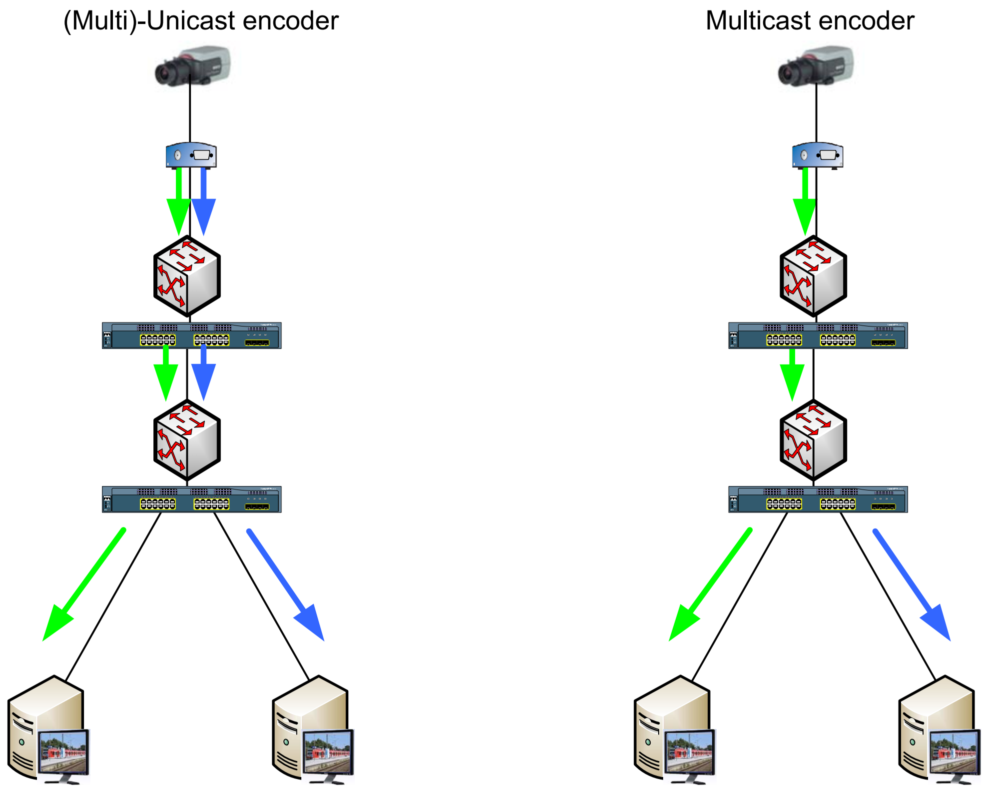

Figure 3.2 Unicast - Multicast

In a multi-unicast communication the stream is duplicated in the encoder and both streams are sent to their respective targets.

In a multicast communication the stream is duplicated in the switch that is directly connected to the targets.

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.

Unicast stresses the network more than multicast does, but maybe more important it stresses the performance of the encoder significantly more.

When do you use multicast?

You must use multicast when a video stream is to be viewed by more than 5 clients simultaneously.

Which features must a switch have for multicast?

– Multicast Layer 2 features and Multicast Querier
– IGMP snooping, PIM Sparse Mode
– Multicast routing (for L3 switches only)
– Switch must be hardware driven

Section 4.3 Multicast, page 22 provides details.

3.5 IP addresses

Each IP address is a 32-bit binary number, for example:

10101100 00010000 10000000 00010001

Each Octet (byte) can be represented in decimal: 172 16 128 17

The address can be written in dotted decimal: 172.16.128.17

Private IP addresses

Private IP addresses will never be assigned to Internet networks. Furthermore, these addresses will not route through the Internet. Private IP addresses 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

Multicast addresses

IP addresses in the range of 224.0.0.0 through 239.255.255.255 are reserved for multicasting.
For devices, you can use 225.x.x.x - 232.x.x.x and 234.x.x.x - 238.x.x.x.
For details see `http://www.iana.org/assignments/multicast-addresses/`

Subnet masks

Subnets are used for IP communication and for minimizing broadcast domains. 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.
Be careful with assigning a subnet mask. If an encoder gets a different subnet mask as the other encoders in its group, the encoder is not detected although having the correct IP address.

Description	Binary form of the addresses
IP address	11000000.10101000.10000000.01111011
Subnet mask	11111111.11111111.11111111.11111100
Calculation	AND operation of IP address and subnet mask
Network address	11000000.10101000.10000000.01111000
Address range	11000000.10101000.10000000.01111000 11000000.10101000.10000000.01111001 11000000.10101000.10000000.01111010 11000000.10101000.10000000.01111011

Description	Decimal form of the addresses
Address range	192.168.128.120 192.168.128.121 192.168.128.122 192.168.128.123
	The first address is the network address, the last one is the broadcast address. Both cannot be assigned to a host.

3.6 Ports

A **port** is a "logical connection place" and specifically, using the Internet protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network. Higher-level applications that use TCP/IP such as the Web protocol, Hypertext Transfer Protocol, have ports with pre-assigned numbers (usually port 80). These are known as "well-known ports" that have been assigned by the Internet Assigned Numbers Authority (IANA).

Other application processes are given port numbers dynamically for each connection. When a service (server program) initially is started, it is said to bind to its designated port number. As any client program wants to use that server, it also must request to bind to the designated port number. Port numbers are from 0 to 65535. Ports 0 to 1023 are reserved for use by certain privileged services.
Well known ports are assigned by the IANA (Internet Assigned Numbers Authority), and range from 1023 and below.
Registered ports are listed by the IANA and have a range from 1024 to 49151. These are used for different proprietary applications.
Dynamically Assigned Ports are ports ranging from 49152 to 65535, and these are assigned dynamically for the duration of a session.
Multicast port numbers can range between 1 and 65535.
In each Bosch encoder or IP camera you configure the transport protocol for video data: **TCP** or **UDP**. The following table contrasts TCP with UDP:

TCP vs. UDP	**TCP**	**UDP**
Connection Type	Connection-oriented	Connectionless
Protocol	Reliable	Best Effort
Sequencing	Yes	No
Examples	E-mail File sharing Downloading	Voice streaming Video streaming TFTP

See *Section 6.1 Used ports* for planning port settings in Bosch IP Video networks.

3.7 VLAN

There are several reasons for using VLANS in a network design:
- Limit broadcast domains
- Increase security

As each VLAN represents its own subnet, a router or Layer 3 switch must be used to route between the subnets.
Using a VLAN helps you to build an own video LAN.
See *Section 6.4 VLAN* for planning VLAN in Bosch IP Video networks.

3.8 Network models

For Bosch IP Video networks we recommend using the hierarchical network model as basis.
This 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 QoS.
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 in our Video IP environment, one switch takes over both the tasks of the Core and the Distribution Layer.

In Bosch IP Video networks, we use the term **Centralized Recording** when recording happens in the Core Layer.
The following illustration shows an example for centralized recording:

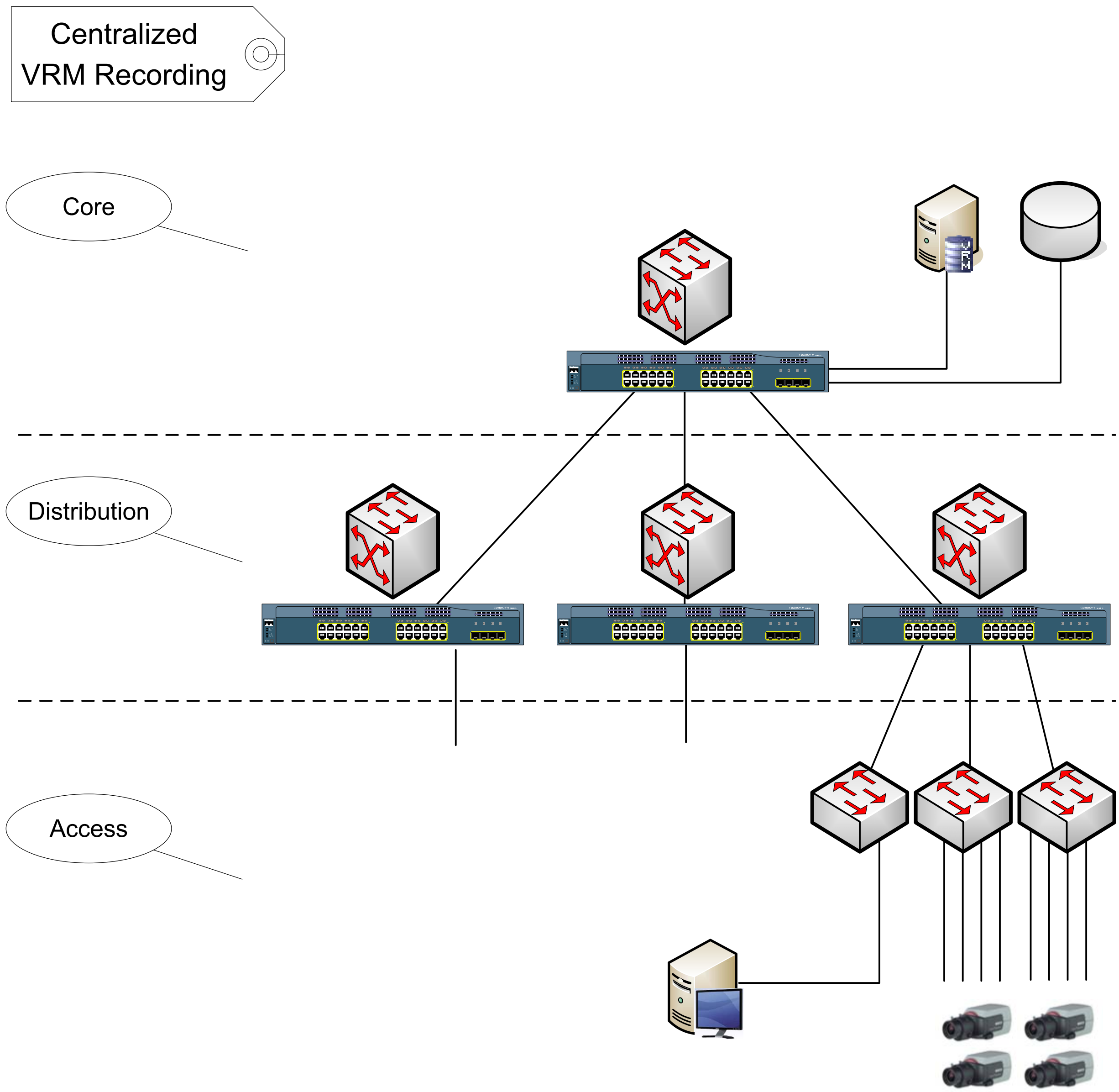

Figure 3.3 Centralized VRM recording

For video networks we must take an additional factor into account. Recording video data generates a huge amount of network traffic. In some scenarios this traffic can remain in the Access Layer to avoid network overload in the Core Layer. For example, you can configure VRM recording or Direct-To-iSCSI recording in the Access Layer.
The following illustration shows an hypothetical example for decetralized recording on 2 locations with VRM:

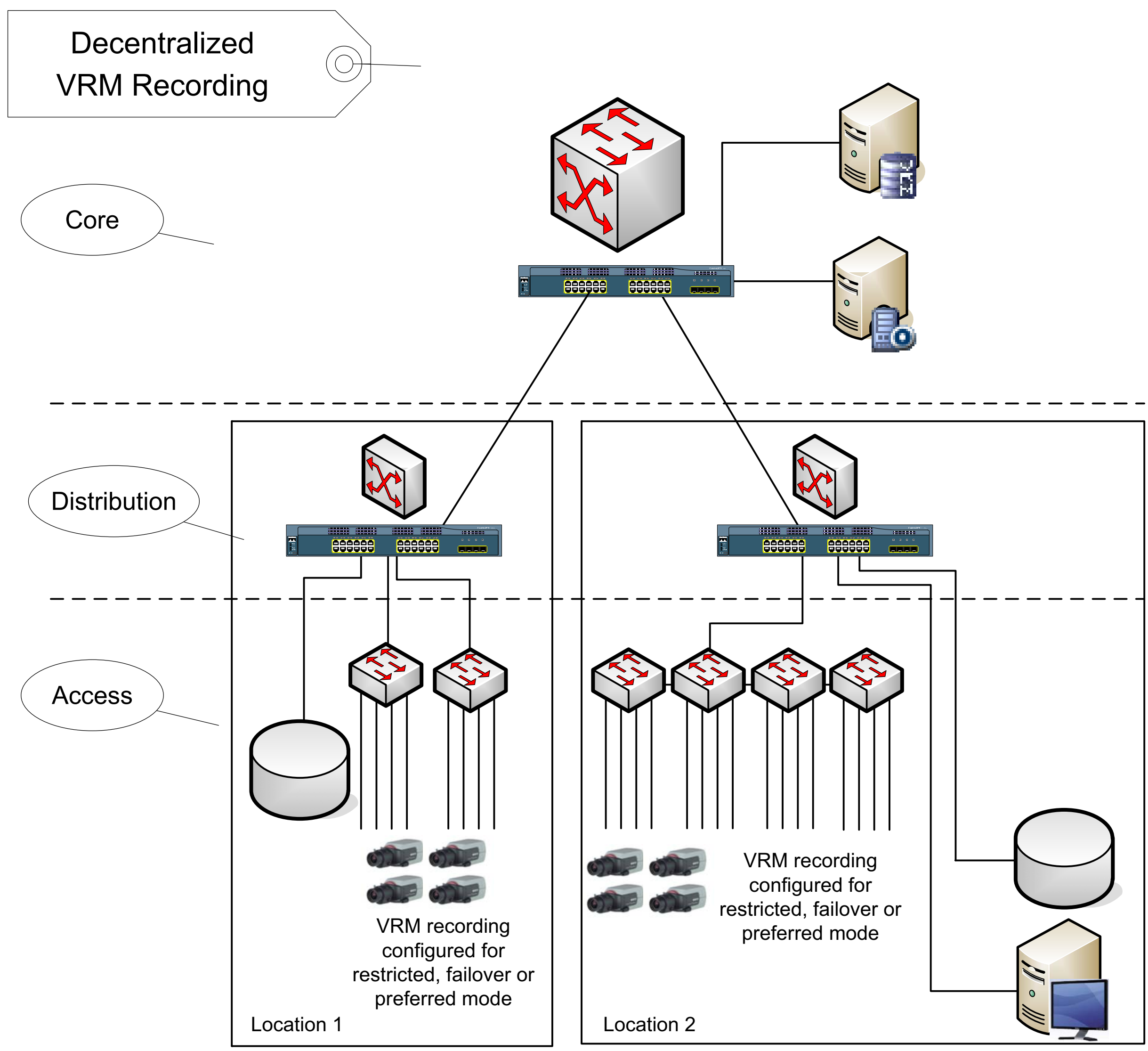

Figure 3.4 Decentralized VRM recording

The VRM recording for each encoder must be configured for restricted mode, failover mode or preferred mode. Otherwise it is not ensured that the recording traffic stays in location 1 or 2.

NOTICE!
When disk space is low, restricted mode or preferred mode fall back to all mode.

3.9 Centralized or decentralized recording

Bosch IP Video networks provide all possible variants of centralized recording or decentralized recording at the camera location.

There are many factors that influence the decision for centralized or decentralized recording. For example if your network covers several buildings, recording should be located in each building. But central viewing and evaluating the recorded video data is easier in a centrally recording environment. Centralized recording is realized when the storage devices are connected to the Core switch. The entire network must be able to transport the recorded video data.

Decentralized recording is realized when the storage devices are connected to the Access Layer switch. The network is segmented into “traffic zones”. The recorded video data stays within the subnets and does not flood the network. If you go for decentralized recording, your Access switches must be designed for the expected traffic.

If you use VRM for recording in a decentralized environment, do not configure the **All** mode. In the **All** mode the VRM decides where to store the video data and hence it can happen that the video data is stored in another traffic zone as where the recorded camera is located. The **Failover**, **Preferred** and the **Restricted** mode fall back to the **All** mode, when disk capacity is reached.

Direct-to-iSCSI recording with VIP X1600 modules is a typical example for decentralized recording. All recording traffic is forwarded directly to the iSCSI target, and never touches the network.

Storage devices can be:

- NVR computers
- iSCSI devices with or without VRM server
- Local recording devices like internal hard disks, SD cards

See *Section 6.5 Examples for recording solutions* for planning the recording in Bosch IP Video networks.

4 Bosch IP Video key features

This chapter gives an overview on the key features that Bosch IP video solutions provide:

– *Section 4.1 Video quality and resolution*
– *Section 4.2 Dual streaming*
– *Section 4.3 Multicast*
– *Section 4.4 Bandwidth*
– *Section 4.5 Video Content Analysis*
– *Section 4.6 Recording at the edge*

4.1 Video quality and resolution

MPEG compression versus bit-rate

Ask your local support for a table listing the bit rates for different resolutions and frame rates for MPEG4 or for H.264.

Comparison Wavelet, MPEG-4, MJPEG and MPEG-2, H.264

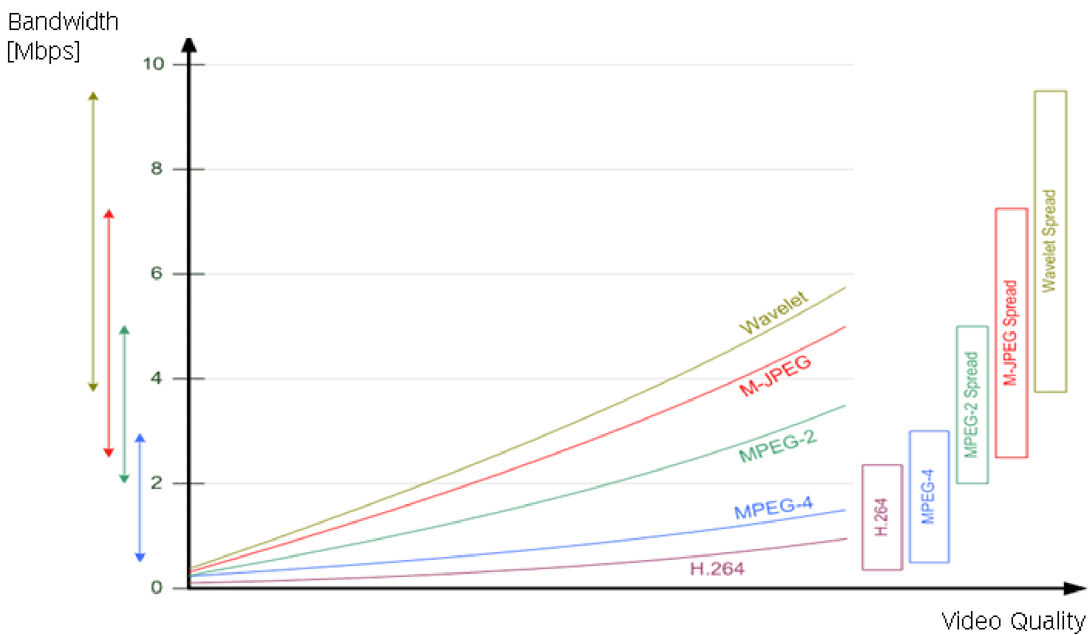

Figure 4.1 Comparison of different compression methods

The following diagramm shows that H.264 is the compression technology with the most efficient way to use the available bandwidth.

4.2 Dual streaming

With dual streaming you can view at one quality, record at another. For old platforms keep in mind that dual streaming creates high load on an encoder and not all possible frame rate / resolution combinations are possible for both streams. On new platforms like VIP X1600 XFM4 both streams can be configured simultaneously and independently.

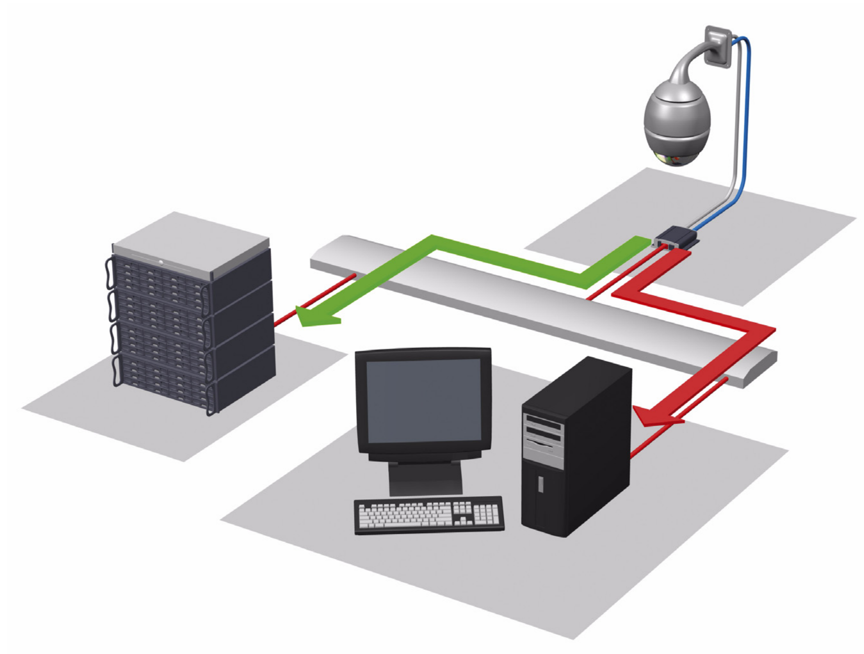

Figure 4.2 Dual streaming example 1

Or one stream is used for viewing locally and the other one for viewing remotely:

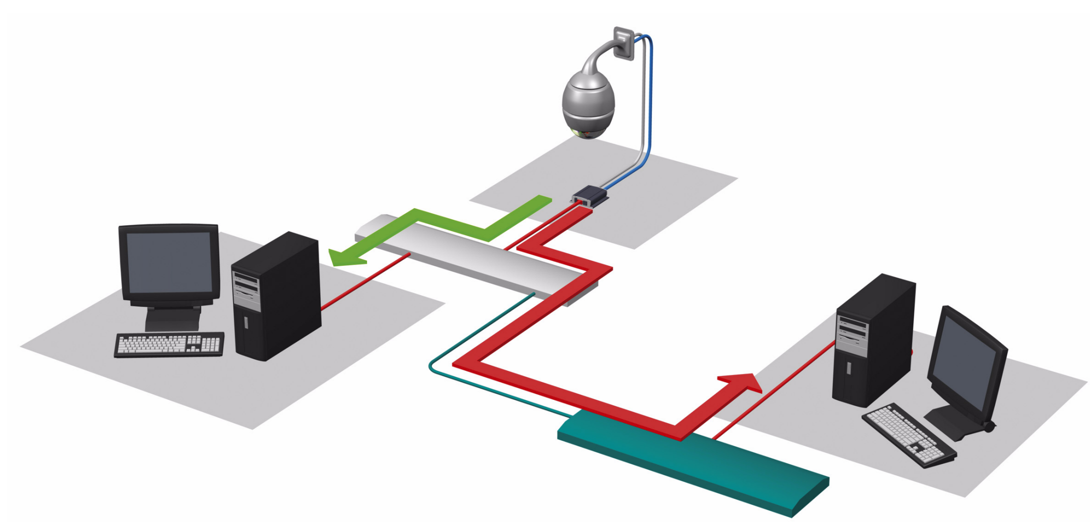

Figure 4.3 Dual streaming example 2

4.3 Multicast

This section provides detailed information on configuring multicast on an encoder and on a switch.

The decision for multicast or unicast depends on the system architecture. For example if you want an encoder send its video data to 10 workstations and / or recording devices simultaneously, use multicast.

See the data sheet of your application for the maximum number of unicast and multicast connections.

CAUTION!

Do no use 1 multicast address for 2 streams.

L2 and L3 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.
There are switches that listen to multicast traffic and maintain a state table of which network systems 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.
If there is no Layer 3 switch/router available, some Layer 2 switches can act as IGMP snooping querier. 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.
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

A key concept in IP multicast is the IP multicast group address (224.0.0.0 - 239.255.255.255). 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).

Multicast routing protocol (PIM Sparse Mode)

In Bosch IP Video 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.
In Bosch IP Video applications before the multicast stream is sent the receiver must send an RCP+ request to the encoder; see *Section Example, page 23* for details.

Example

In the following illustration the multicast data flow is shown after establishing the connection between a Source (encoder) and a Receiver (decoder) is shown.

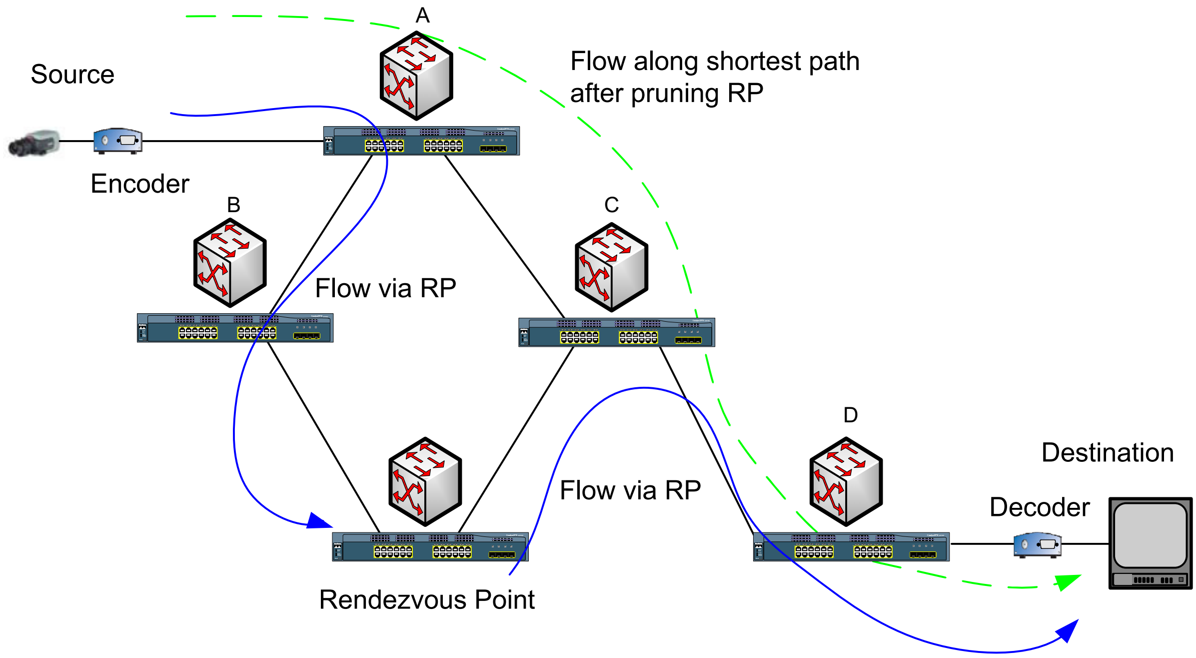

Figure 4.4 Multicasting with Rendezvous Point

If a decoder makes a video request to an encoder, first an RCP+ connection is established between the encoder and the decoder.

1. RCP+ request from decoder to encoder.
2. Encoder sends RCP+ reply with multicast address to decoder.
3. Encoder starts sending.
4. Decoder sends an IGMP Report stating that he wants to receive a multicast stream.
5. Neighboring router D sends a PIM Join message towards the Rendezvous Point (RP).
6. Neighboring router A forwards multicast stream towards the RP.
7. RP sends multicast stream to decoder.
8. RP connects Source and Receiver along the shortest path. If required the RP is pruned and does not continue forwarding the multicast stream.

Note:
Although multicast video uses UDP, the amount of multicast connections is limited by a maximum number of RCP+ registrations (via TCP) that accompanies the UDP video streams. Due to that effect it is possible to make a connection between an encoder and maximum 50 decoders simultaneously (1 RCP+ registration), or a connection between an encoder and maximum 25 web pages simultaneously (2x RCP+ registration). Or a combination of these two types of connections.

Encoder settings
On the configuration pages of an encoder click the **Multicasting** page, rename **0.0.0.0** to **1.0.0.0**. The encoder automatically inserts a unique multicast address based on the device's MAC address.

Note:
If you insert a valid multicast address (in the range 224.0.0.0 - 239.255.255.255) on the **Multicasting** page, the device does not insert a multicast address based on the device's MAC address.

When a firewall is used, enter a port value that is configured as non-blocked port in the firewall.

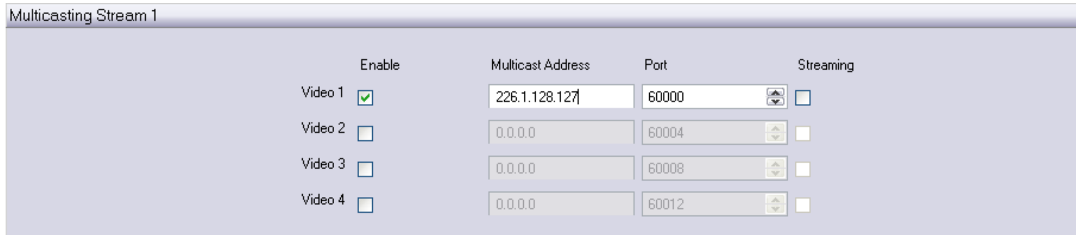

Figure 4.5 Port number for multicast

In the user interface of the encoder there is an option called **Streaming**. If you check this option, the encoder continuously sends the multicast stream to the switch. This means that the multicast connection is not preceded by a RCP+ registration. The encoder streams always all data to the switch. The switch in return (if no IGMP multicast filtering is supported or configured) sends this data to all ports, with the result that the switch will flood.
When you use a non-Bosch device for receiving a multicast stream, enable **Streaming**.
Streaming is used if a device does not use the RCP+ protocol. Non-Bosch devices (for example a VLC player) usually do not support RCP+.

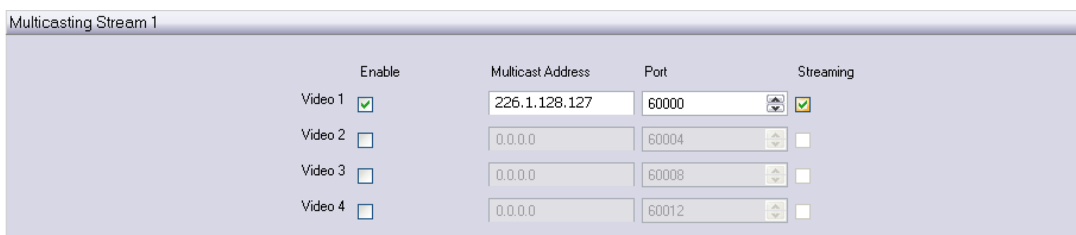

Figure 4.6 Multicast streaming

Another scenario for using streaming is when the video of one encoder has to be viewed by more than 50 decoders. This can happen in a TV broadcast application. For example a university campus with 1 encoder transmitting video towards different decoders spread over the campus, the same encoder can be loaded with more than 100 decoders when setting the encoder to “streaming mode”.
To prevent the “flooding” of the switch when the streaming option is selected, an intelligent switch, which uses IGMP snooping, has to be used. Now all the ports where the multicast stream does not need to be streamed to are blocked for multicast streams.

4.4 Bandwidth

Compression efficiency depends on the complexity (detail level) of the scene and varies with motion. Hence, an efficient use of bandwidth and disk space is required.
IT managers want to manage network usage to avoid overload and bottlenecks.
Bandwidth limits keep encoders within bandwidth budget.
The following illustration shows an example of a configuration page used for bandwidth limits in Bosch VMS.

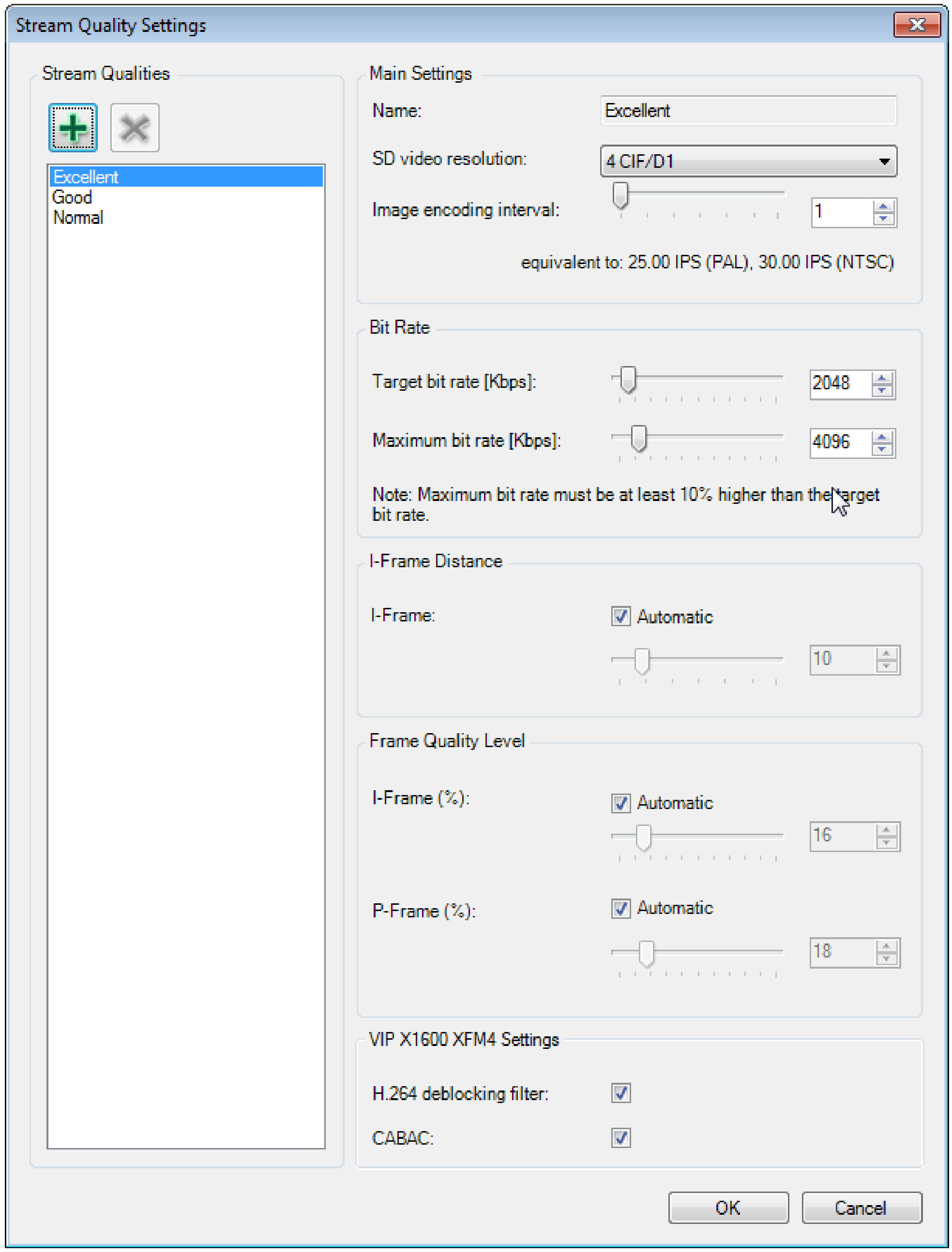

Figure 4.7 Stream quality settings in Bosch VMS

In addition to the image activity level (movement in image), the overall bit rate is mainly influenced by the following encoder's technical parameters:

– Encoding interval (frame rate)
– Video resolution
– I-frame distance
– I/P-frame quality

The encoder's setting allows for configuring a target and maximum bit rate. The target data rate is the value the encoder aims for, whereas the maximum data rate shall never be exceeded. Based on the settings above, the encoder tries to vary either the quality or the encoding interval to keep the maximum data rate depending on the image activity level.

4.5 Video Content Analysis

The default algorithm for Video Content Analysis (VCA) is called Motion+. Another more powerful algorithm that Bosch offers is IVA. Both are working in the encoders. This improves the scalability because no PC must be updated with new software. Video Content Analysis adds bandwidth to the network. But other vendors must stream the entire video over the network to detect motion on a PC. With built-in VCA only a small additional overhead containing the result of VCA is added to the video stream.
Motion detection saves disk space because it triggers recording on motion, with pre-alarm recording.
Features:

- Selectable areas can trigger on direction of motion.
- Tamper detection

4.6 Recording at the edge

Pre-alarm recording can be performed locally on the encoders / IP cameras without loading the network. Recording in encoders avoids 24/7 loading of network
You can record the streams independently on different media. Thus, video can be recorded centrally on iSCSI drives and redundantly on the local media. If necessary, for example in case of a network failure, VRM can fill up the gap in the central recording (ANR, Automatic Network Replenishment).

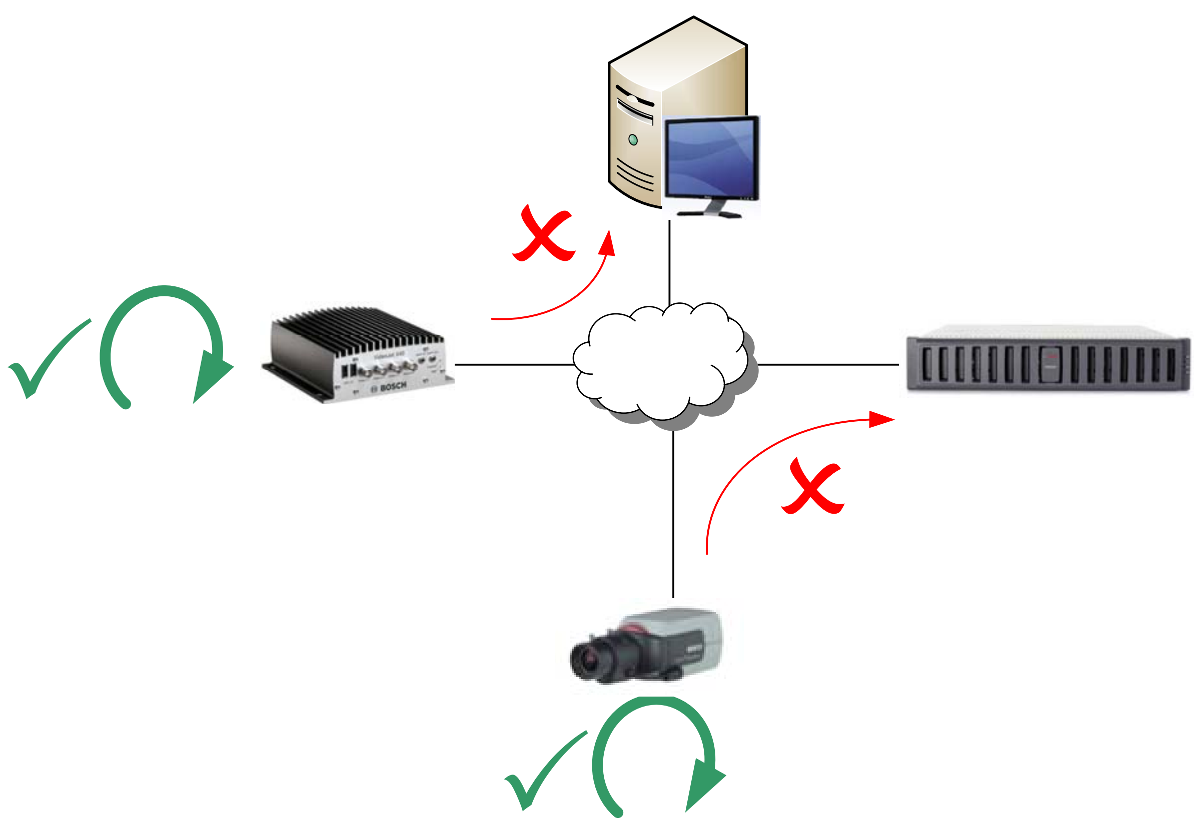

Figure 4.8 Recording at the edge

5 Calculating network bandwidth and storage capacity

The following is covered:

– *Section 5.1 Network bandwidth calculation*
– *Section 5.2 Storage calculation for VRM recording*

The formulas that are described in this chapter are designed for general use in Bosch IP Video networks. But in specific projects it can be necessary to deviate from these formulas if sensible.

When a stream from an encoder is sent through a network to an iSCSI device for storage, a network overhead is added to each data packet.

When the stream is stored on an iSCSI device, the network overhead is removed. On the storage the recording block-header is added as overhead for storage. The storage calculation must only consider the overhead for storage. Recording block headers are maintained by VRM and encoder. The additional overhead on the network traffic can be neglected.

The following illustration shows the relation:

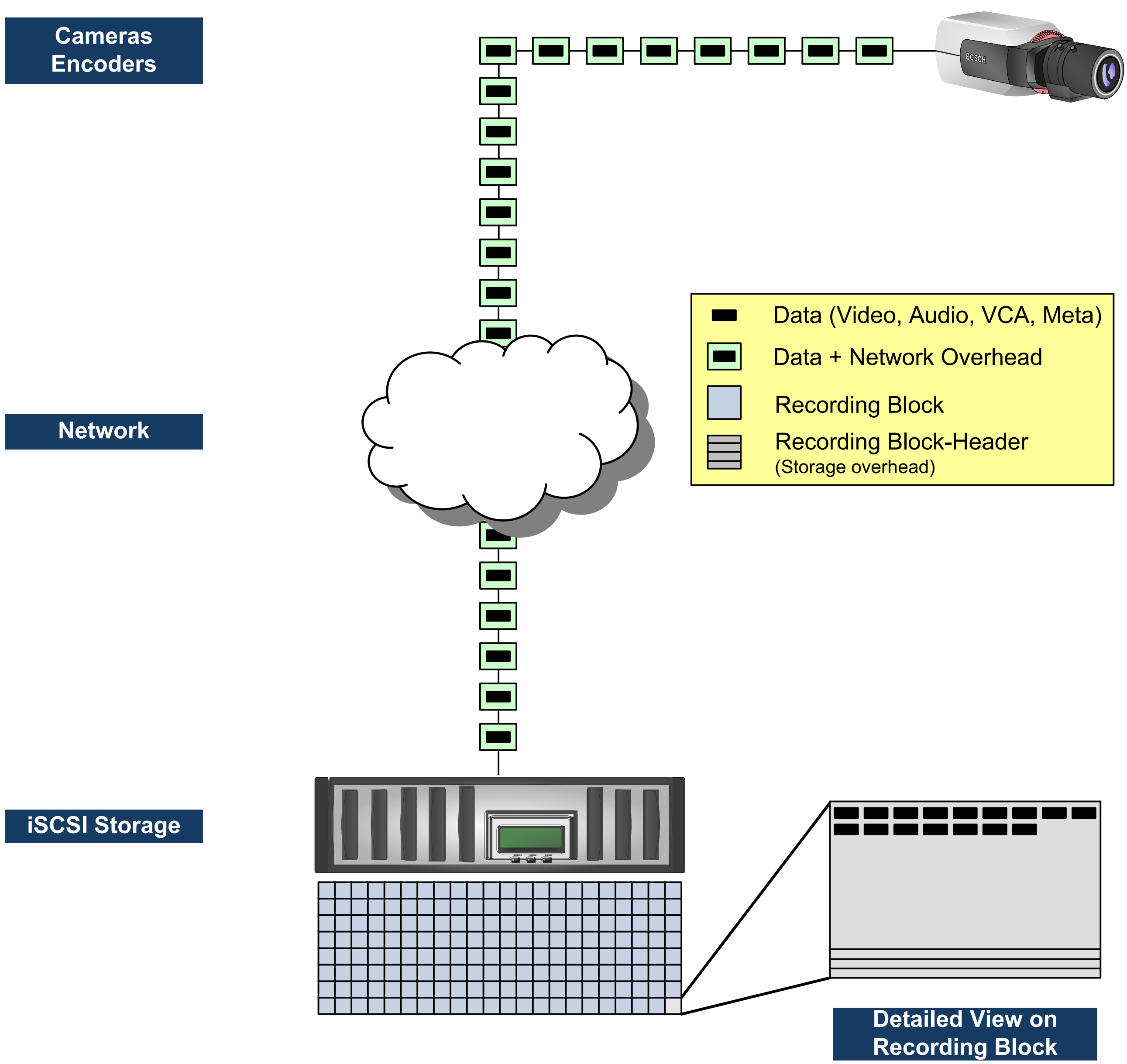

Figure 5.1 Relation between network bandwith and storage calculation

5.1 Network bandwidth calculation

A camera or encoder can provide up to two MPEG4/H.264 streams and an additional M-JPEG stream (which is not considered here).
Before making bandwidth calculations the following questions should be answered:

– How many streams are used for recording? For example: VRM recording uses single streaming, Direct-to-iSCSI uses dual streaming.
– For unicast: How many streams are used for live view, for example the number of connected clients?
– Which mode is used? Unicast or Multicast? (See *Section 3.4 Unicast – broadcast – multicast*)

The cnfigured values define a bit rate for this encoder. This bit rate can be limited by a maximum bit rate that you can also configure for an encoder. Usually an average bit rate is reached and rarely the maximum bit rate. Traffic shapes usually are not smooth but can show traffic bursts.
In general, statements of bandwidth are made at designated connections within the entire network (for example between 2 switches or at a VRM). Therefore all used connections at this spot have to be considered in a worst case scenario.

Formula for CIF-4CIF resolution

The general formula for the overall network bandwidth calculation of one stream is:
Used abbreviations:
<bw_net> = Network bandwidth in Mbps
<bw_enc> = Maximum or average bandwidth in Mbps (as from the encoder’s settings)
<ov_vca> = Overhead for audio and VCA metadata = 1.20
<ov_net> = Overhead for network transmission = 1.40
<ov_netiscsi> = Additional overhead for network transmission for iSCSI recording= 1.05
<bw_net> = <bw_enc> * <ov_vca> * <ov_netiscsi> * <ov_net>

When you do not use VCA, audio, or iSCSI transmission, remove the corresponding factors in the formula for your bandwidth calculation.

Example

20 IP cameras record with 3 Mbps maximum bandwidth on an iSCSI device. VCA and audio are not used.
The recommended provided bandwidth at the network video recorder is:
<bw_net> = 20 * 3 Mbps * 1.4 * 1.05 = 85 Mbps
Section 6.2 Bandwidth calculation provides bandwidth calculation for planning Bosch IP Video networks.

5.2 Storage calculation for VRM recording

For VRM recording we assume a maximum overhead of 10%. The overhead comprises of indexing information which is filed on the storage (assumption: continuous recording 24 hours).

Used abbreviations
<bcc> = Basic capacity consumption in GB per day
<bw_enc> = Maximum bandwidth in Mbps (as from the encoder’s settings) without network overhead
<ov_vca> = Overhead for audio and VCA metadata = 1.20
<ov_vrmrec> = Recording overhead = 1.10
<occ> = Overall capacity consumption in GB
<minrt> = Minimum retention time in days

Basic capacity estimation
<bcc> = <bw_enc> * <ov_vca> * <ov_vrmrec> * 3600 * 24 / 8 / 1024

Overall capacity estimation
The overall capacity consumption includes the minimum retention time:

<occ> = <bcc> * <minrt> * camera-count + 150 * camera-count

The minimum overall capacity is calculated with the minimum retention time. As safety buffer we recommend 150 GB per camera. This safety buffer comprises of free storage and the blocks that are reserved for recording for one camera.

NOTICE!
When the disk capacity is smaller than the minimum overall capacity, recording stops.

Section 6.3 Storage calculation provides storage calculations for VRM recording.

6 Planning Bosch IP Video networks

This section provides information on planning Bosch IP Video networks and gives some examples of network scenarios:

– *Section 6.1 Used ports, page 31*
– *Section 6.2 Bandwidth calculation, page 39*
– *Section 6.3 Storage calculation, page 44*
– *Section 6.4 VLAN, page 46*
– *Section 6.5 Examples for recording solutions, page 48*

6.1 Used ports

This section provides information on ports used in Bosch IP Video networks. Some examples with Bosch VMS, VIDOS or Web browser illustrate where the open ports are required.
The following illustrations show the used ports for a wide variety of Bosch IP Video network scenarios:

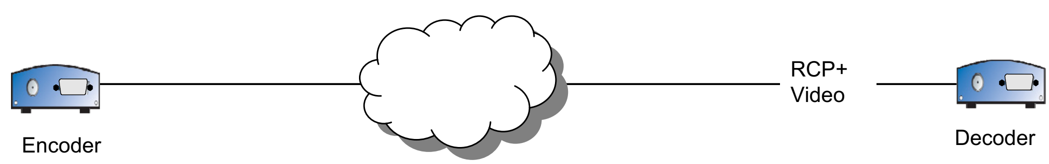

Figure 6.1 Open ports for an encoder-decoder connection

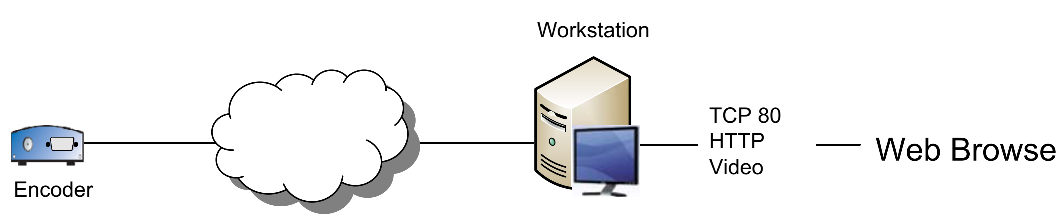

Figure 6.2 Open ports for Web browser connected to an encoder

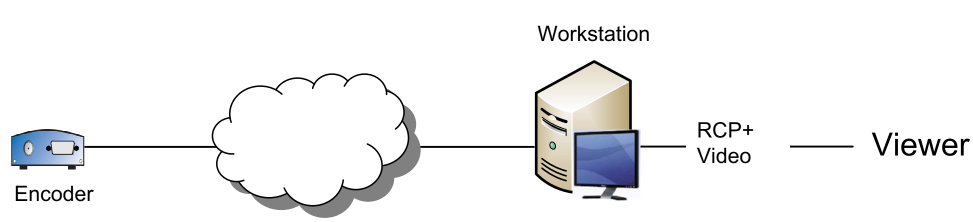

Figure 6.3 Open ports for Viewer connected to an encoder

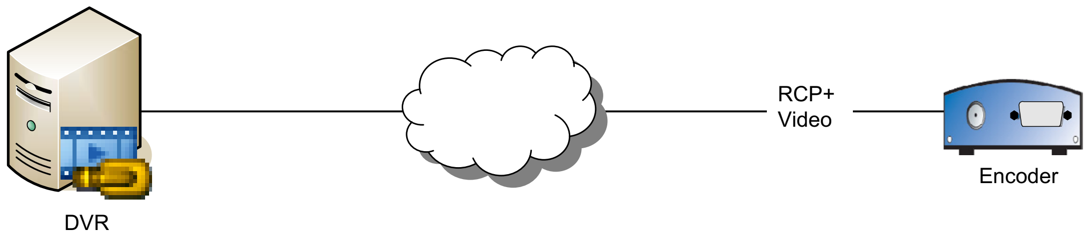

Figure 6.4 Open ports for an encoder connected to a DVR

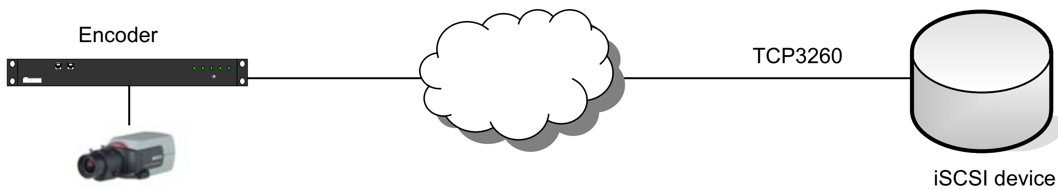

Figure 6.5 Open ports for Direct-to-iSCSI recording

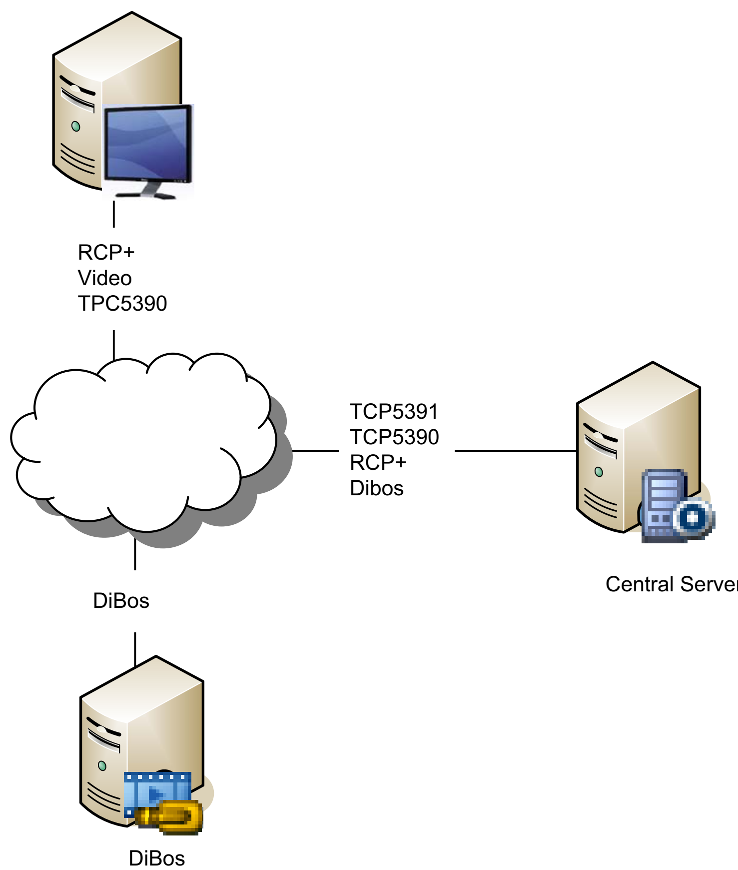

Figure 6.6 Open ports for a DiBos recorder connected to Bosch VMS

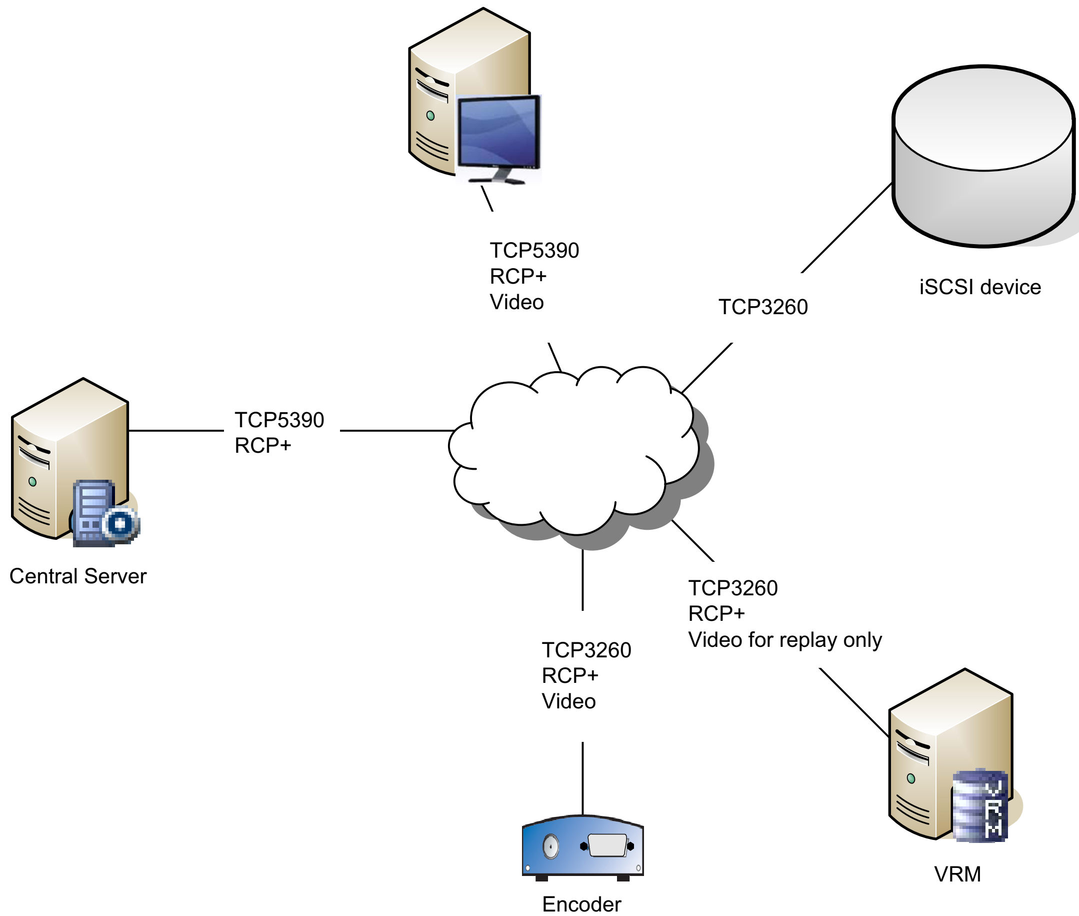

Figure 6.7 Open ports for Bosch VMS recording with VRM

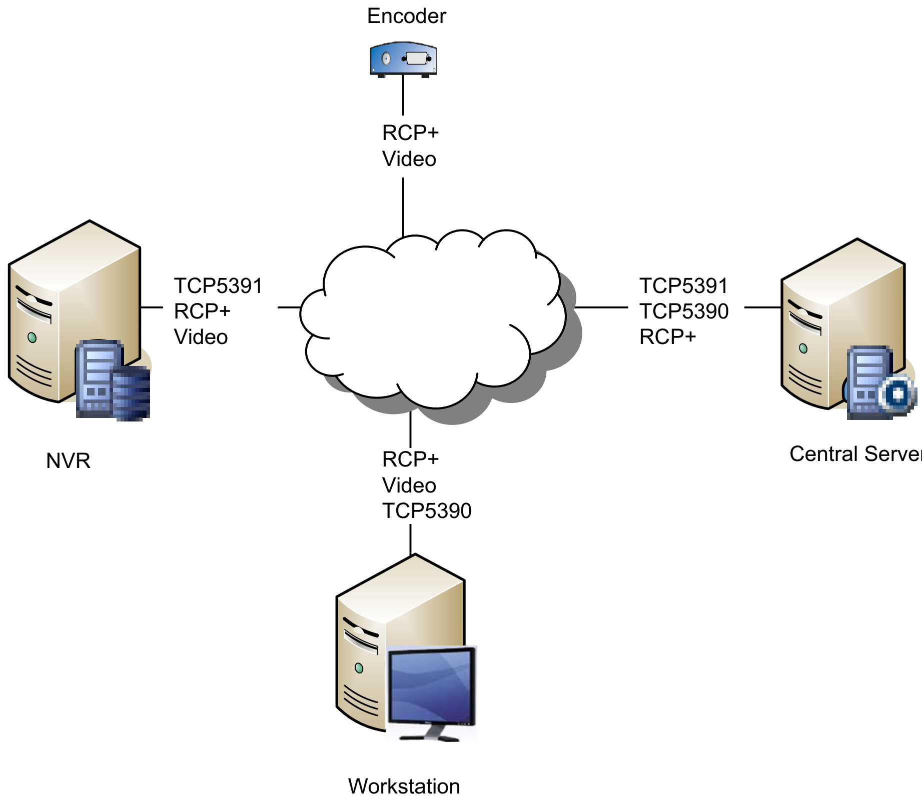

Figure 6.8 Open ports for a Bosch VMS recording with NVR

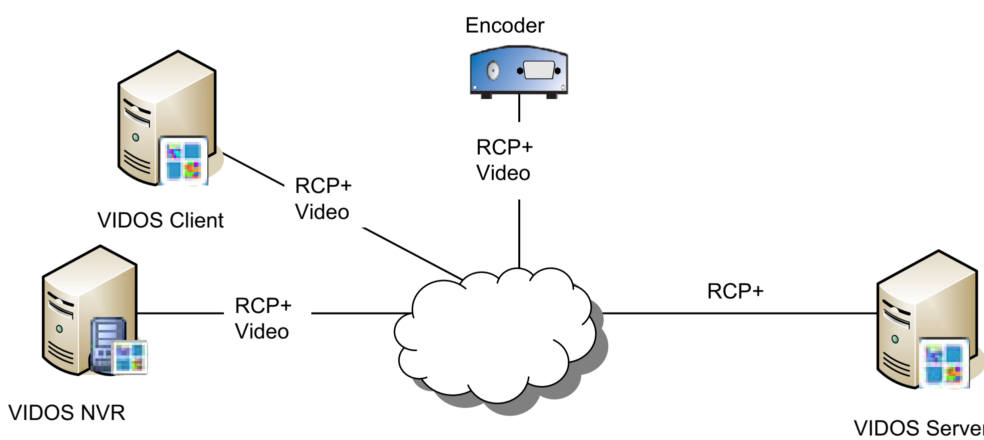

Figure 6.9 Open ports for an encoder connected to a VIDOS system

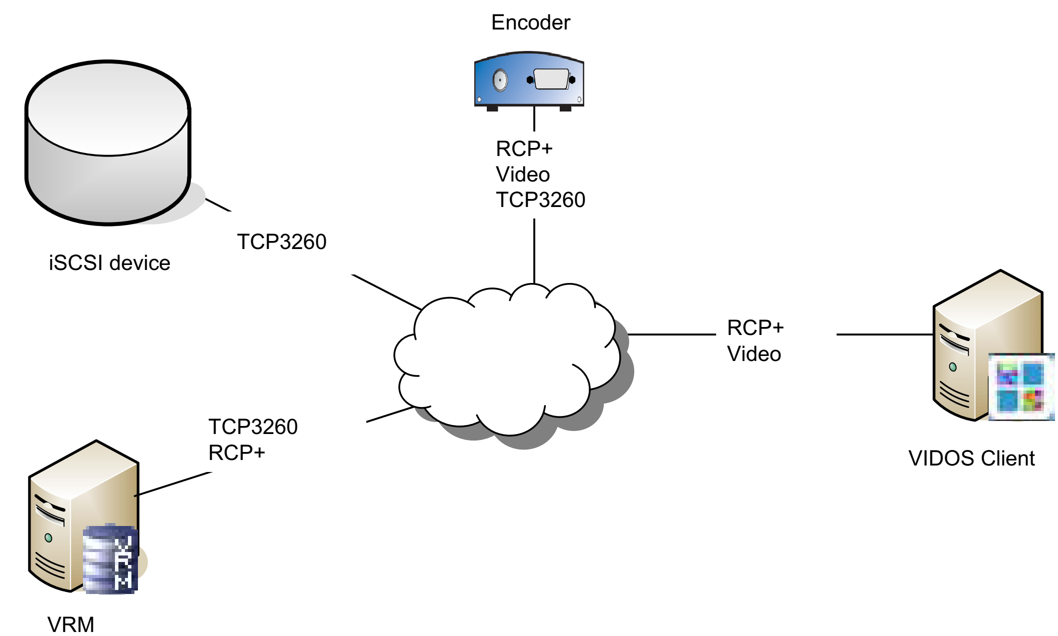

Figure 6.10 Open ports for an encoder recorded via VRM and a VIDOS client

Legend

Abbreviation	Used ports
RCP+	UDP1756 (RCP+), UDP1757 (Scan Target), UDP1758 (Scan Response) UDP1800 (Multicast Network Scan Target), TCP80 or 10000-101000 (HTTP Tunneling), TCP443 or 10443-10543 (SSL)
Video	UDP1024-65635 (randomly assigned)
DiBos	TCP135, UDP135, TCP/UDP1024-65535 (randomly assigned)
iSCSI	TCP3260

Bosch VMS uses the following ports:
- Central Server: TCP5391, TCP5390, RCP+
- Client Workstation: RCP+, Video
- Bosch VMS NVR: TCP5391

Alarm messages back from the encoder to the Client Workstation can only be detected if TCP port 1756 is opened back to the Client Workstation.
When using a Proxy Server and Microsoft Internet Explorer, configure exceptions for the Bosch IP devices.

6.1.1 Centralized VRM recording

The following illustration shows the open ports in a centralized VRM recording scenario:

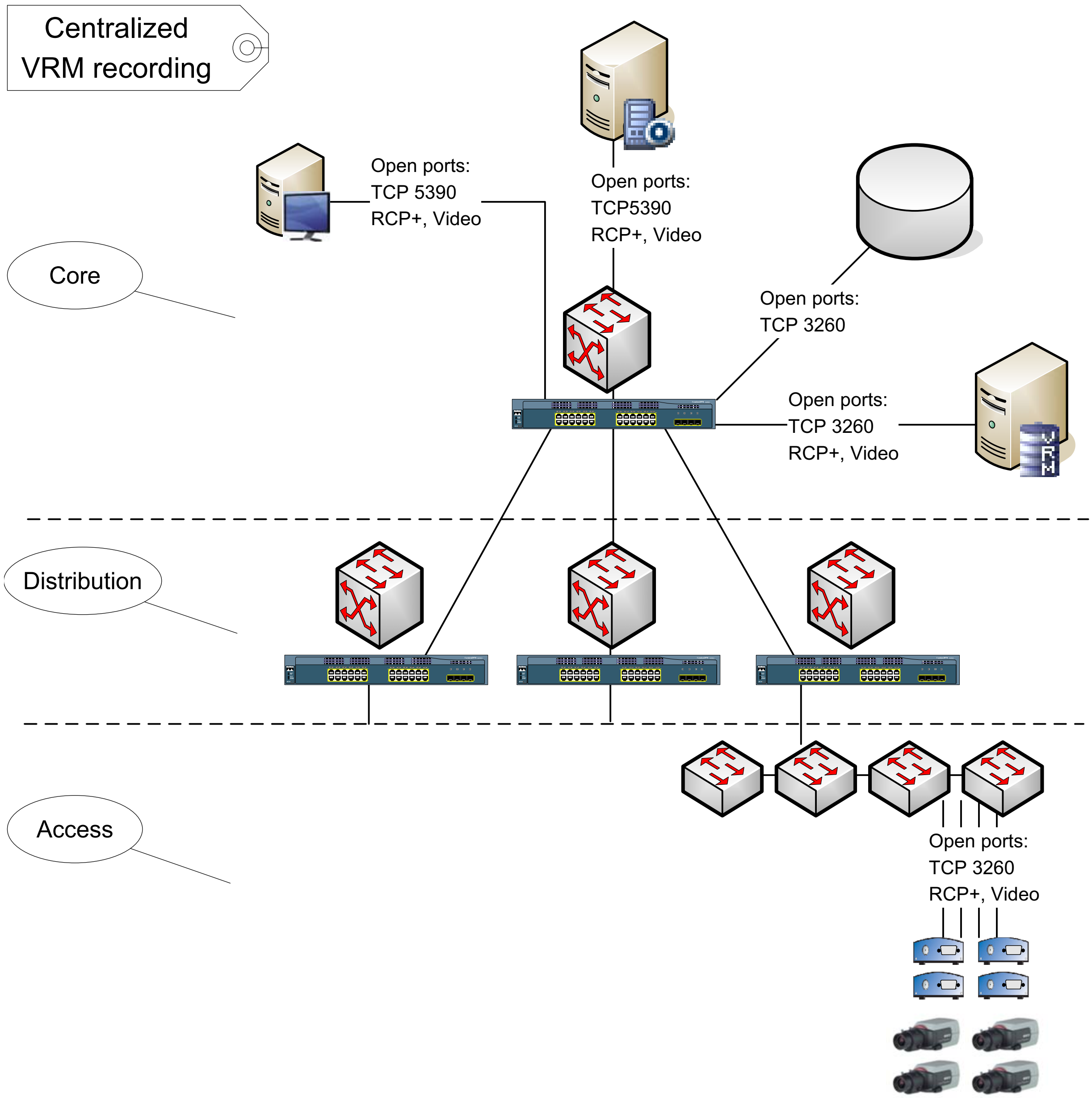

Figure 6.11 Centralized Bosch VMS VRM recording

6.1.2 Decentralized VRM recording

The following illustration shows the open ports in a decentralized VRM recording system:

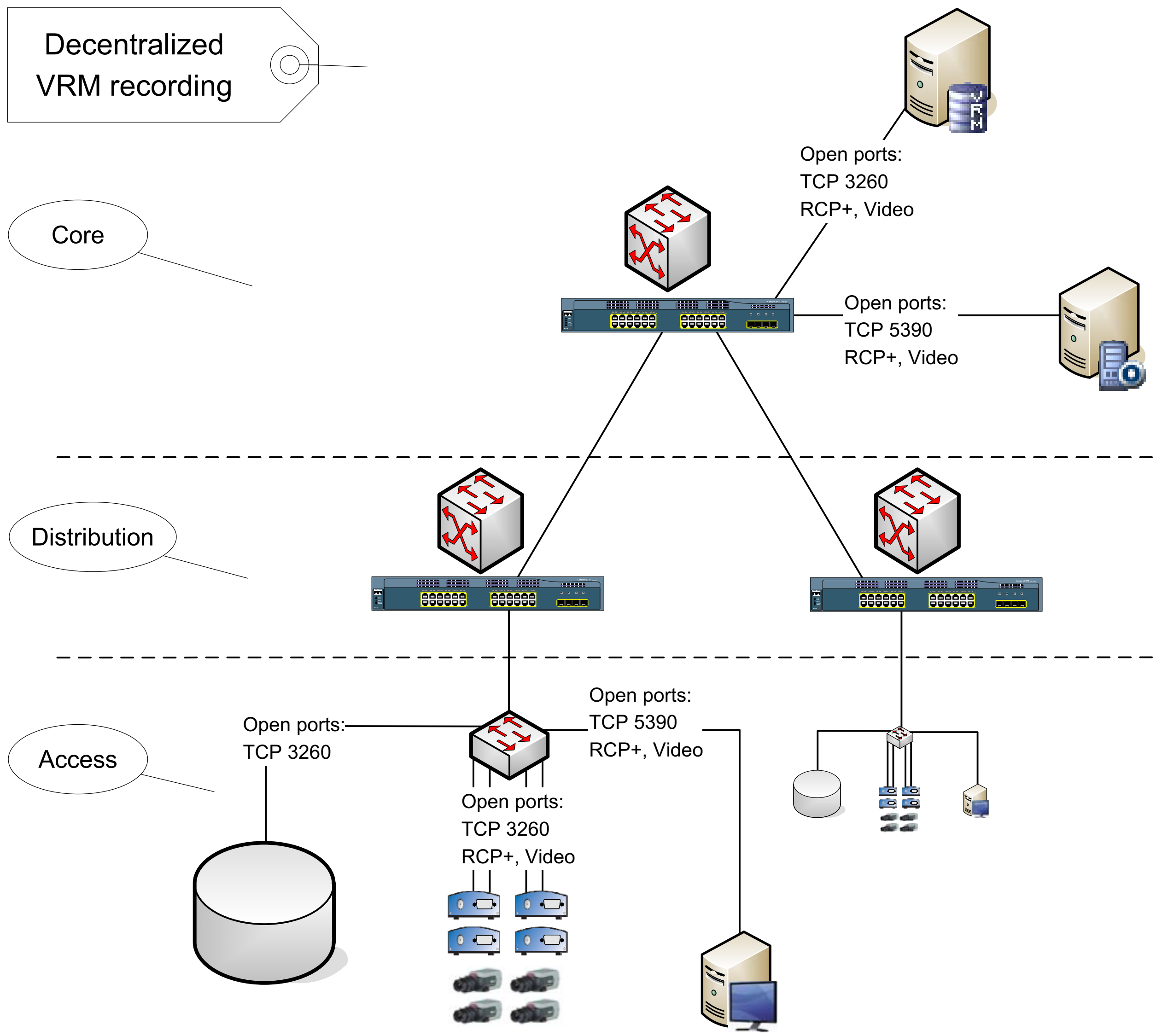

Figure 6.12 Decentralized Bosch VMS VRM recording

6.1.3 Centralized NVR recording

The following illustration shows a hierarchical network with centralized NVR recording. The open ports to be configured between Distribution and Core are noted.

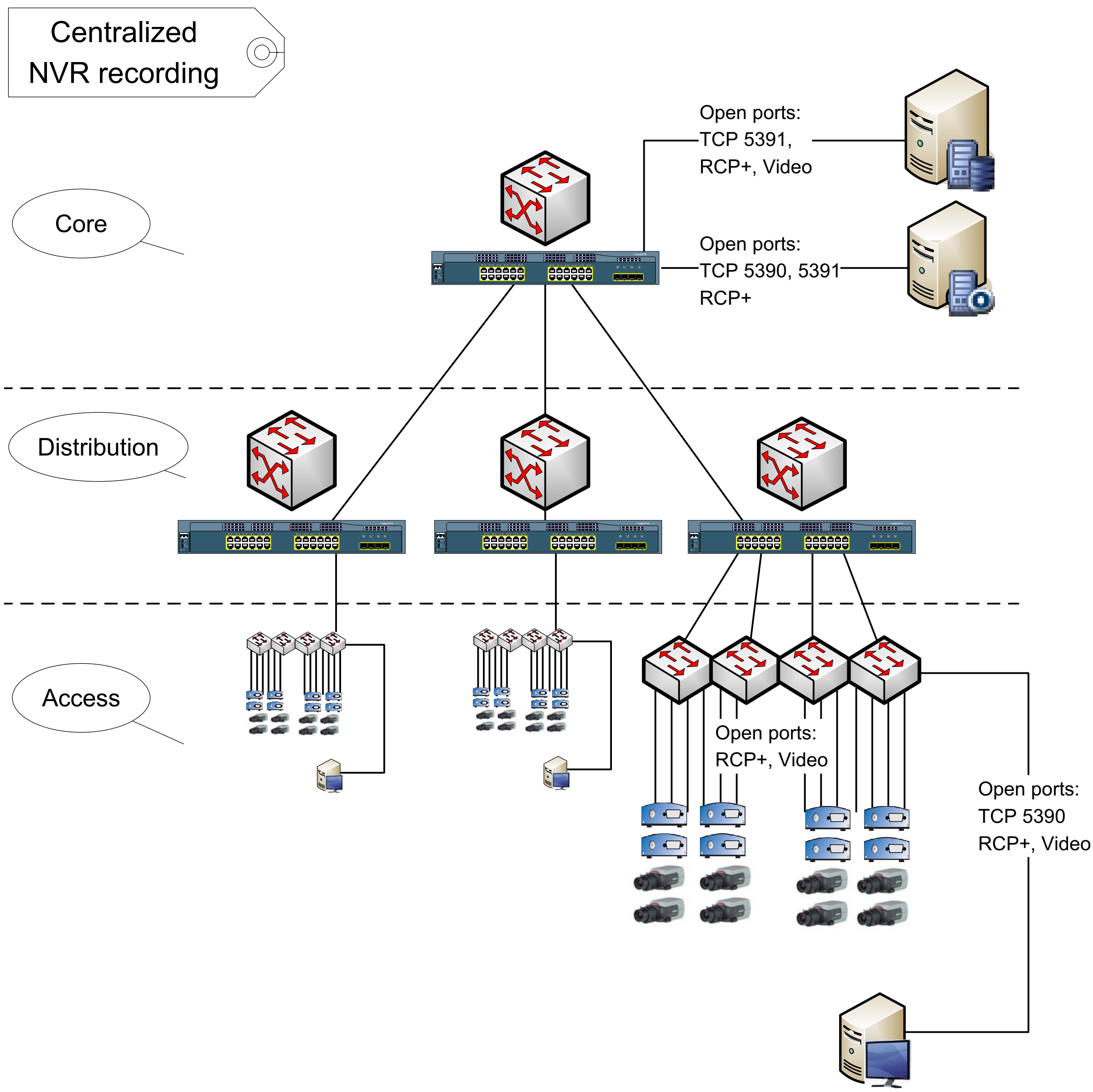

Figure 6.13 Centralized Bosch VMS NVR recording

6.1.4 Decentralized NVR recording

The following illustration shows a hierarchical network with centralized NVR recording and the open ports.

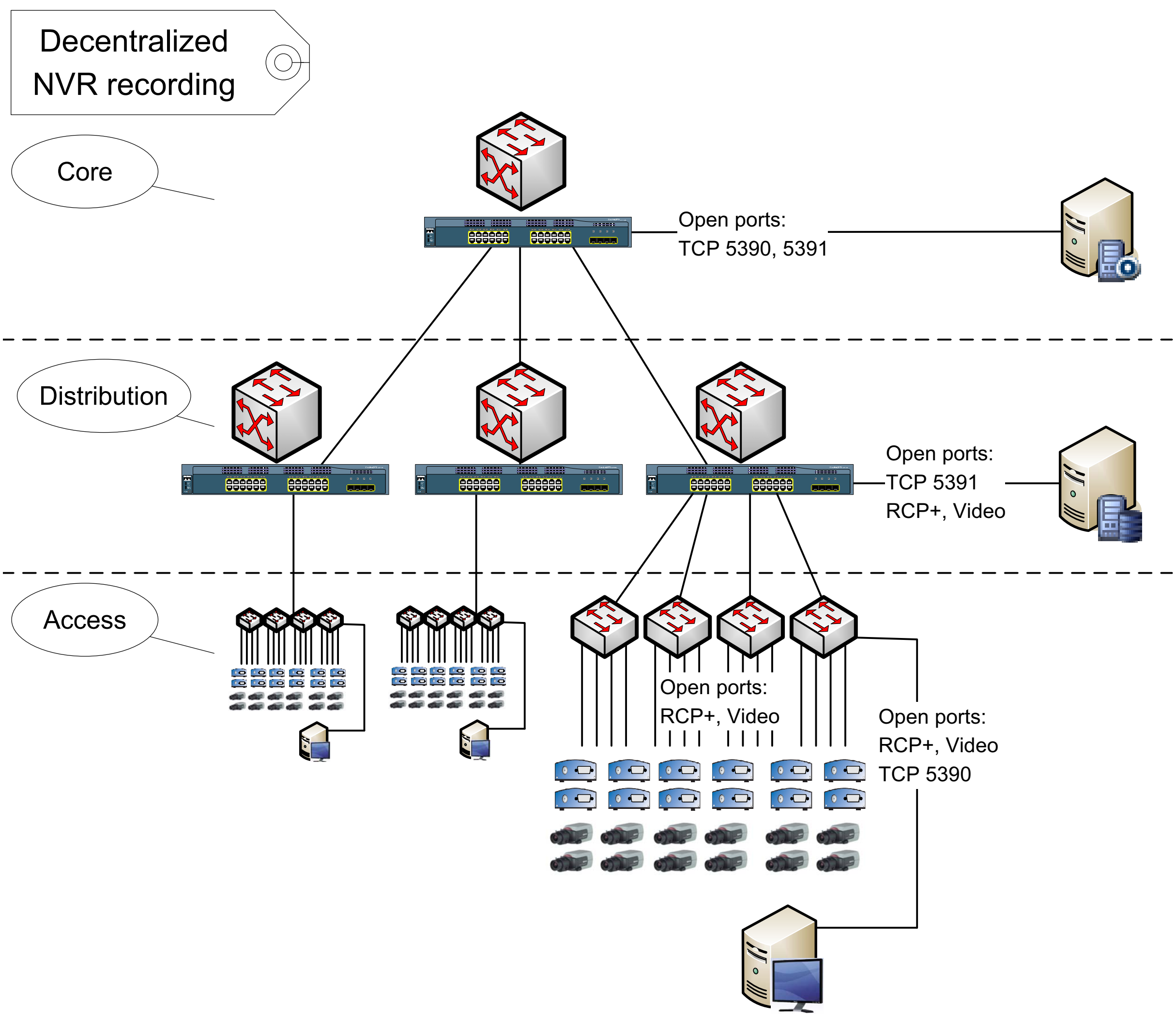

Figure 6.14 Decentralized Bosch VMS NVR recording

6.2 Bandwidth calculation

There are a lot of reasons to do some bandwidth calculations in a network:

- All network devices have a limited bandwidth
- Find out bottlenecks
- Equalize and distribute video traffic
- Optimize response time and load

Video traffic is usually transmitted by UDP packets.

UDP is a kind of “lightweight”, connectionless protocol which has a small protocol overhead and does not support handshake and re-transmit. Thus the video packets are very susceptible to any kind of network disturbances. Video packets can be disordered or get completely lost in the network.

The video stream receiver (e.g. a workstation or NVR) processes the video in real time without any buffer. So any kind of disturbance is directly visible as jerking video or results in gaps.

UDP has a smaller protocol overhead compared to TCP: UDP 8 Byte, TCP 20 Byte

To overcome packet losses due to network congestions and peaks we recommend considering a security margin on top of your calculations.
The following calculations disregard the traffic between Central Server and Clients, NVRs or VRMs.

6.2.1 Decentralized VRM recording

The following example scenario is calculated:

- Bosch Video Management System with decentralized continuous VRM recording
- 1 Distribution/Core switch, 9 Access switches, 3 Access blocks
- 270 IP cameras, 30 per switch
- 9 workstations, 3 per Access block
- Playback: 4 streams per workstation playback speed 1x
- Parallel live view of 25 cameras
- Live bandwidth: 1 Mbps
- Recording bandwidth: 2 Mbps
- Each block is configured as an own VLAN. The routing is performed in the Core switch.
- No audio and no VCA is used.

The following illustration shows the example scenario with the required maximum bit rates. The Core and Distribution Layer are merged. Only one of the three Access switch blocks is displayed.

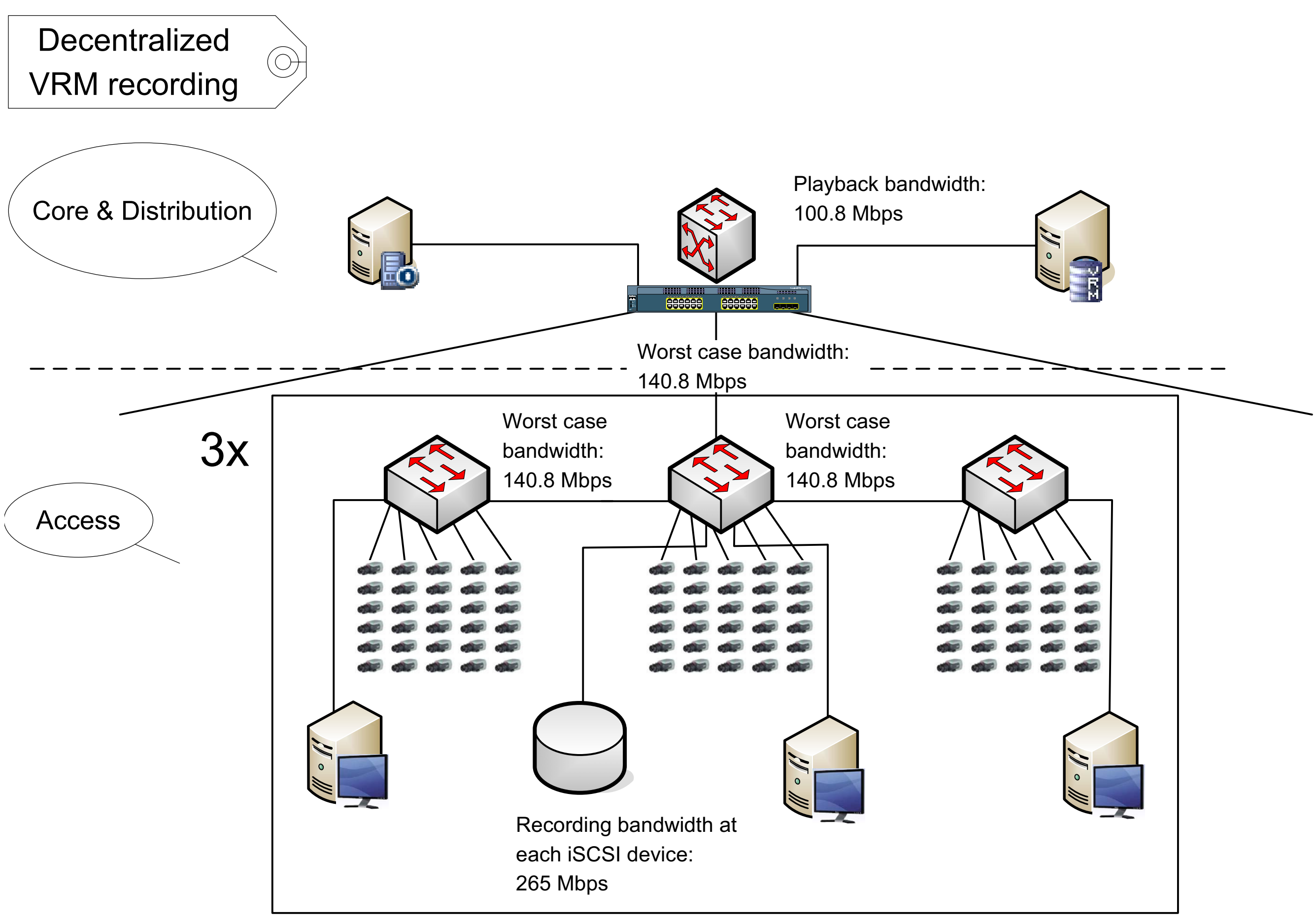

Figure 6.15 Decentralized VRM recording

Note:
This example assumes that the encoders perform their iSCSI recording in **Restricted** mode with only one iSCSI device configured. That means there is a fixed relationship between encoders and iSCSI disk arrays. The other recording modes can produce additional traffic between the Access Layer switches because the VRM server can decide where encoder data is recorded. If two of the three switches fail in one segment, recording stops.
If you configure **Failover** or **Preferred** mode, ensure that you configure primary and secondary iSCSI disk arrays that are in the same network segment as the encoder.

Bandwidth calculations
Consider the following restrictions:
- The iSCSI disk array in this example supports up to 128 concurrent sessions (one session is an IP connection to an encoder)
- The iSCSI disk array in this example has a limited bandwidth of 300 Mbps.
- Multicast network with PIM Sparse Mode for multicast routing must be configured.

The bandwidth calculation is performed for the uplink from an Access switch to the Core switch.
- Overall recording bandwidth:
  <bw_net> = 270 * 2 Mbps * 1.4 * 1.05 = 794 Mbps

  To keep the restrictions of iSCSI disk arrays it is required to have at least 3 iSCSI disk arrays:
  794 Mbps / 300 Mbps = 2.65.
- Live viewing bandwidth:
  <bw_net> = 25 * 1 Mbps * 1.4 = 35 Mbps
- Playback bandwidth:
  <bw_net> = 9 * 4 streams * 2 Mbps * 1.4 * 1.05 = 105.8 Mbps

  Note:

  Playback is forwarded from the iSCSI device to the VRM Server and from there to the client who has requested it.
- Worst case live and playback between Access and Core Layer:
  <bw_net> = 35 Mbps + 105.8 Mbps = 140.8 Mbps

6.2.2 Decentralized VRM recording with export

The example scenario in *Section 6.2.1 Decentralized VRM recording* is calculated. When an Operator Client VRM user exports video data of a camera, this data is sent from the storage device to the client computer.

The requirement is that the export is as fast as possible. But the live, playback and recording traffic must not be affected.

The following illustration shows the example scenario.

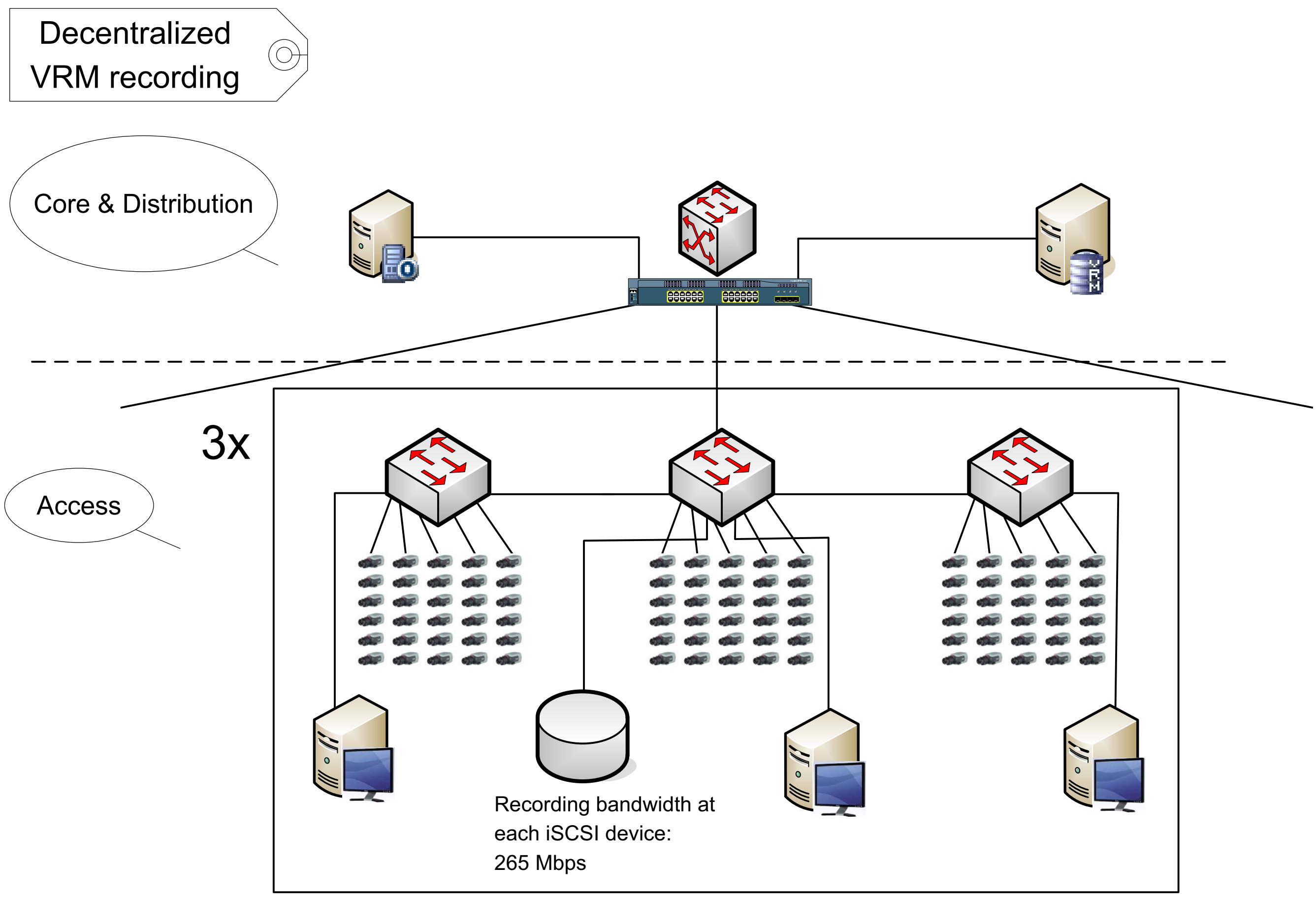

Figure 6.16 Decentralized VRM recording with export

The bottleneck in this scenario is the iSCSI device. The maximum bit rate is 300 Mbps. For an additional export 48 Mbps are theoretically available. Each export reads with 40 Mbps. All three clients can cause an export bandwidth of 3 * 40 Mbps = 120 Mbps.

In this example, a second iSCSI device is required to have enough free bandwidth for export.

6.2.3 Centralized NVR recording

The following example scenario is calculated:

– Bosch Video Management System with centralized continuous NVR recording.
– No multicast
– 20 VideoJet X40 encoders with 2 cameras each.
– 3 workstations
– Parallel live viewing of 20 cameras on a workstation
– Parallel playback of 9 cameras on a workstation
– Live bandwidth: 1 Mbps
– Recording bandwidth: 2 Mbps
– No audio and no VCA is used.

The following illustration shows the example with the required maximum bit rates. The Core and Distribution Layer are merged.

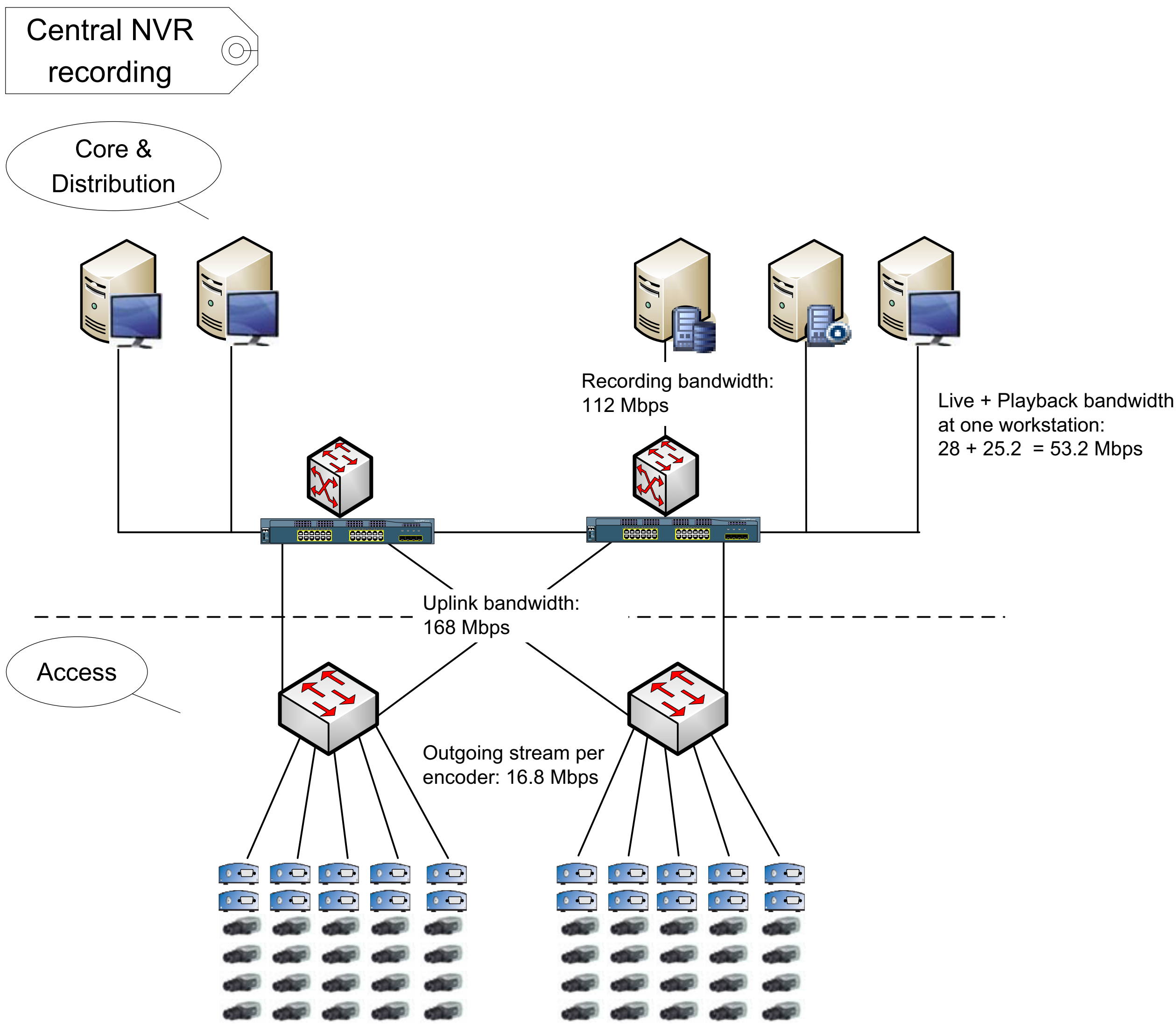

Figure 6.17 Central NVR recording

The Rapid Spanning Tree Protocol ensures that the data is transferred only via one path through the network. The other possible paths are only used in case of failure (redundant network). The bandwidth calculation must consider all possible links, i.e. all uplinks in this example must be designed to transport the full load.

Bandwidth calculations

– Recording data stream at NVR:
  <bw_net> = 40 * 2 Mbps * 1.4 = 112 Mbps
– Live Viewing at workstation:
  <bw_net> = 20 * 1 Mbps * 1.4 = 28 Mbps
– Playback at workstation:
  <bw_net> = 9 * 2 Mbps * 1.4 = 25.2 Mbps
– Outgoing stream from 1 encoder (no multicast):
  <bw_net> = 4 * (1 Mbps + 2 Mbps) * 1.4 = 16.8 Mbps
– Uplink from Access switches to Core switches (all encoders, no multicast):
  <bw_net> = 10 * 16.8 Mbps= 168 Mbps

6.2.4 Centralized NVR recording with export

The example scenario in *Section 6.2.3 Centralized NVR recording* is calculated.

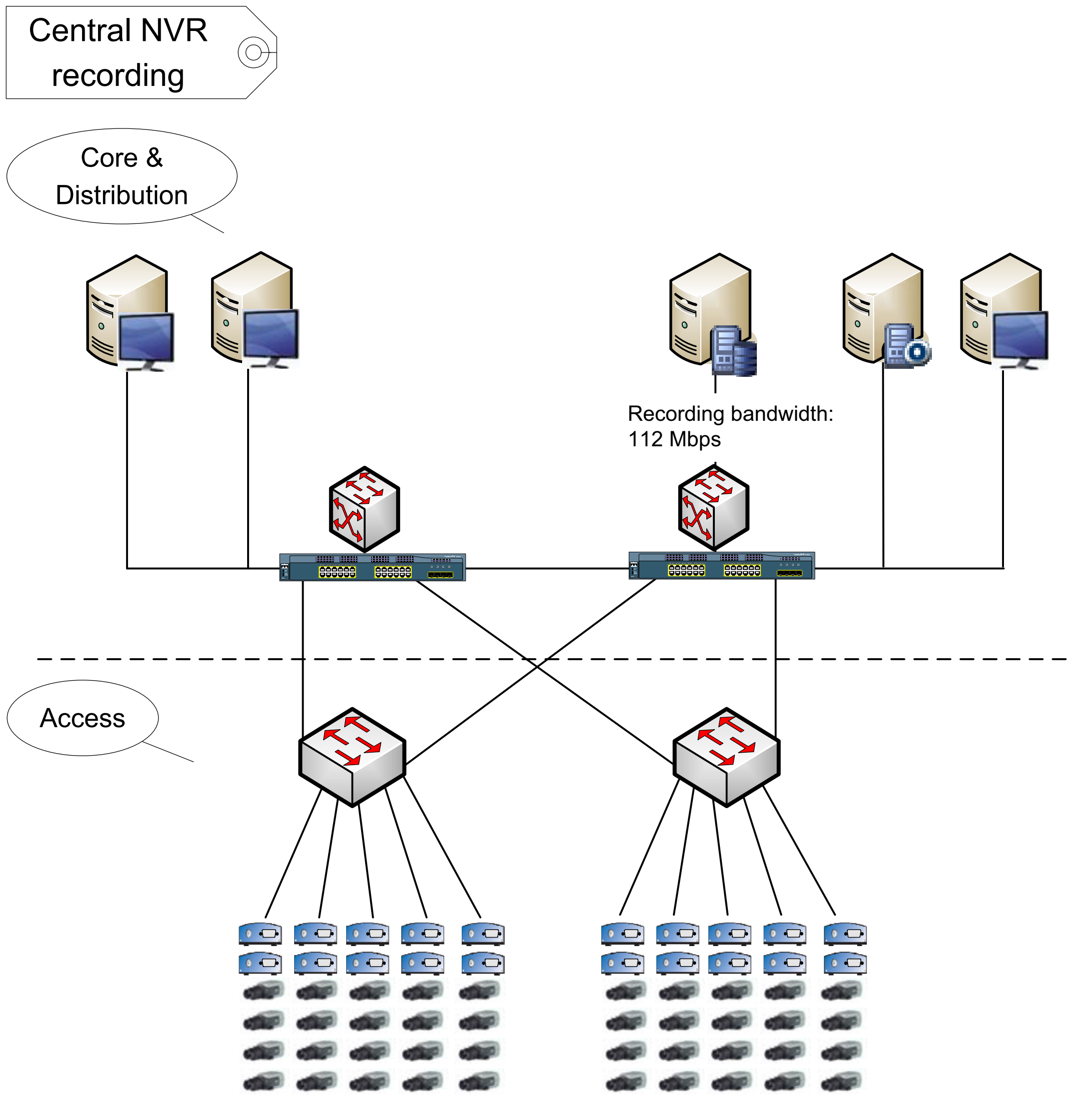

Figure 6.18 Central NVR recording with export

The bottleneck in this scenario is the NVR. The maximum bandwidth is 128 Mbps. For an additional export 16 Mbps are theoretically available. The export reads with 34 Mbps. All three clients can cause an export bandwidth of 3 * 40 Mbps = 120 Mbps.
In this case the export becomes very slow.

6.3 Storage calculation

Used abbreviations

<bcc> = Basic capacity consumption in GB per day
<bw_enc> = Maximum bandwidth in Mbps (as from the encoder’s settings) without network overhead
<ov_vca> = Overhead for audio and VCA metadata = 1.20
<ov_vrmrec> = Recording overhead = 1.10
<occ> = Overall capacity consumption in GB
<minrt> = Minimum retention time in days

6.3.1 VRM recording and iSCSI sessions

This section provides information on VRM recording and iSCSI sessions.

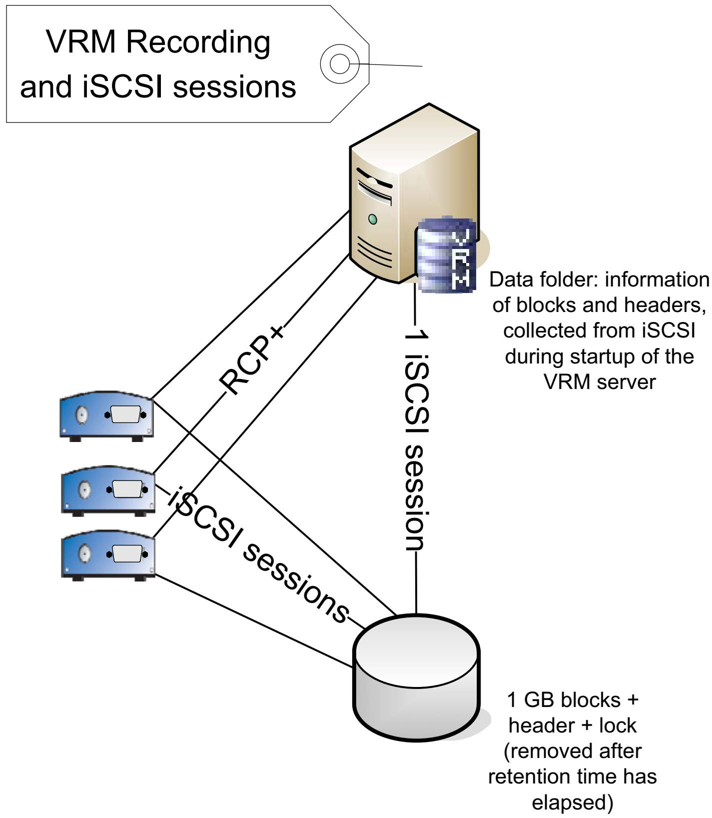

Figure 6.19 VRM recording and iSCSI sessions

Each encoder keeps one iSCSI session open with each iSCSI target. This is also valid for a multichannel encoder. The sessions for each camera are bundled into one session.
The VRM server keeps one iSCSI session open with each iSCSI target. This iSCSI session is also used for playback.
Recording data is directly forwarded to the iSCSI device. The task of the VRM is to “inform” each encoder where on the iSCSI device to stream its data.
If all sessions are used, there is no session left for iSCSI management software or for another device, load balancing does not work.
Load balancing in the VRM server adjusts bandwidth, capacity, and iSCSI sessions.
The recording mode of VRM is automatically changed from **Failover** or **Preferred** mode to **All** mode when the configured targets of **Failover** or **Preferred** mode of fail.

6.3.2 VRM playback

The playback data is streamed from the iSCSI target via encoder and VRM to the client. Each IP encoder uses (per IP address) one iSCSI session for communication with the iSCSI device. VRM supports maximum 32 playback sessions to clients (as per Sep. 2009). VRM 2.0 supports direct replay as per default, i.e. the video data is directly transmitted from the iSCSI device to the playback client. The VRM Server only sends metadata. In this case, the maximum number of playbacks per client is again 32 but the number of clients is only limited by the number of iSCSI sessions on the iSCSI target and the bandwidth of the iSCSI target.

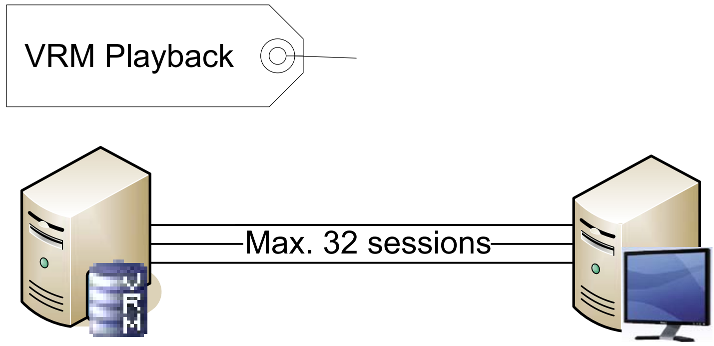

Figure 6.20 VRM playback

6.3.3 VRM storage calculation

To calculate the basic capacity consumption (bcc) in Gigabyte for one day, use the formula described in *Section 5.2 Storage calculation for VRM recording*.

6.3.4 Calculation example 1

- 1 x Dinion IP (= 1 iSCSI host)
- Active recording channels: 1
- Bandwidth: 2 Mbps
- Minimum Retention Time: 14 days

<bcc> = 2 Mbps * 1.10 * 3600 * 24 / 8 / 1024 = 23.20 GB/day
<occ> = (14 days * 23.20 GB/day * 1) + 150 GB = 475 GB

6.3.5 Calculation example 2

- 150 x VIP X1600 Encoder Module (1 Module = 1 iSCSI host)
- Channels per module: 4
- Active recording channels per module: 2
- Bandwidth per channel: 2.8 Mbps
- Number of Modules: 150
- Minimum Retention Time: 10 days

<bcc> = 2.8 Mbps * 1.10 * 3600 * 24 / 8 / 1024 = 34.5 GB/day
<occ> = 34.5 GB/day * 10 days * 150 GB + 150 *150 = 74250 GB

6.4 VLAN

This section describes the use case that cameras are grouped with VLAN.
Some cameras are located near different entrances of the building; other cameras are located in different locations outside of the building.
Depending on their locations the cameras are connected to the nearest switches. But for viewing, the entrance cameras must be grouped and the outside cameras must be grouped. This is realized via VLAN. The Core switch performs the VLAN routing.
The following illustration displays a network using VLAN. There is no recording.

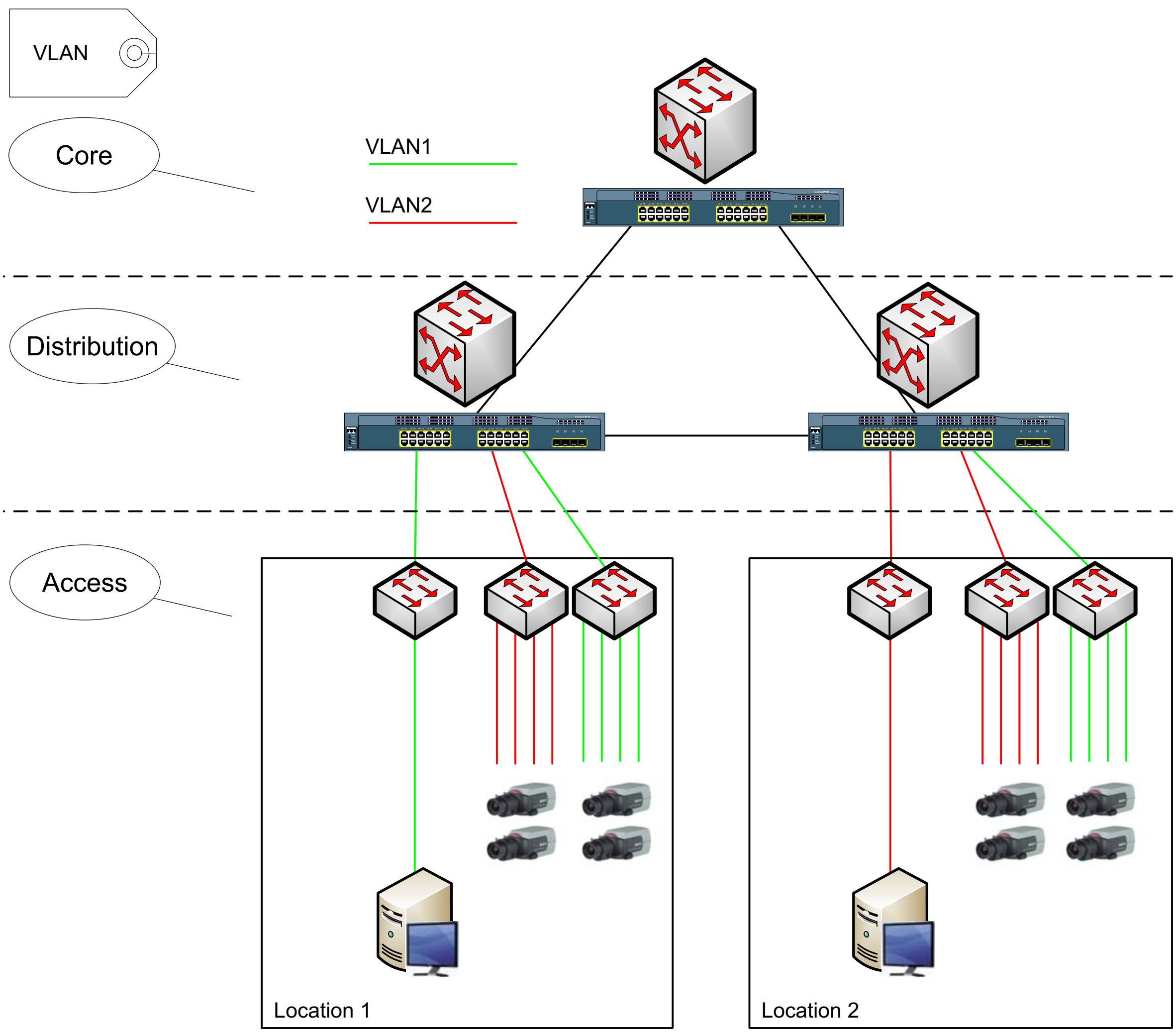

Figure 6.21 VLAN example

The entrance cameras in location 1 and 2 are assigned to the same VLAN (green line) and the outside cameras of both locations are assigned to the same VLAN (red line). The workstation in location 1 only displays the entrance cameras of VLAN1 (“green” cameras), the workstation in location 2 only displays the outside cameras in VLAN2 (“red” cameras).
The advantage is that 2 different physical locations reside on the same subnet which makes the administration easier. The broadcast domain in both locations is smaller and the workstations cannot access the cameras of the other VLAN. This can increase the operational security. The problem arising in this example is that the live video traffic is not kept in each location but sent through the network. Hence if there is additional recording traffic, this traffic should be recorded on each location separately, for example with VRM recording.

Note

When you assign an encoder to another VLAN, it is not reachable in the initial LAN although the IP address of the encoder has not changed.

6.5 Examples for recording solutions

This section shows for various recording solutions which equipment is required.

6.5.1 Direct-to-iSCSI recording

The following example shows a Direct-to-iSCSI recording scenario.
Specifications:

- 500 cameras attached to 34 VIP X1600 base systems (1 base system contains 4 modules, 15 cameras per base system)
- 20 disk arrays
- Live bandwidth: 2 Mbps
- Recording bandwidth: 1 Mbps
- 5 switches
- No audio and no VCA is used.

Each switch is connected to the following devices:

- 7 VIP X1600 modules with 105 cameras per switch (one port per module is reserved for a disk array)
- 8 workstations

The following illustration shows the example scenario with the required maximum bit rates. Core and Distribution Layer are merged. Only one of the five Access Layer segments is displayed.

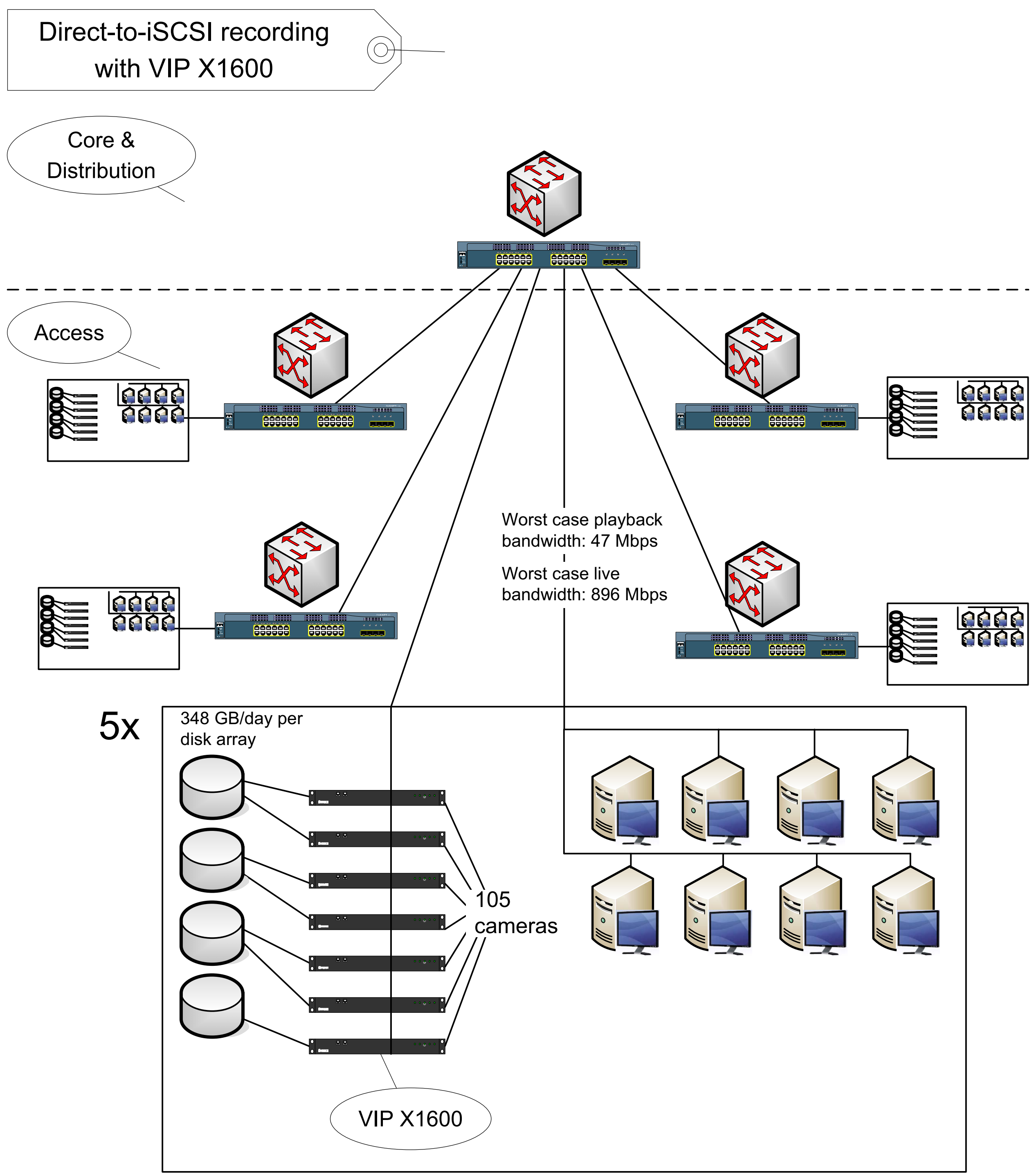

Figure 6.22 Direct-to-iSCSI recording with VIP X1600

Storage calculation

4 disk arrays are connected directly to the encoders. Each disk array records up to 30 cameras with a recording bandwidth of 30 Mbps. As per the storage calculation (see *Section 6.3 Storage calculation*) formula this means:

<bcc> = 30 Mbps * 1.10 * 3600 * 24 / 8 / 1024 = 348 GB/day

Bandwidth calculation

Live requests from within the same segment are uncritical because switching is not required.

Worst case live bandwidth per switch (32 workstations from the other switches request 100 live streams each):
<bw_net> = 320 * 2 Mbps * 1.4 = 896 Mbps
Worst case playback bandwidth per switch (32 workstations from the other switches request one playback stream each):
<bw_net> = 32 * 1 Mbps * 1.4 * 1.05 = 47 Mbps

Requirements for the switches
Layer 3 switch with 1 Gbit uplink port. PIM Sparse mode activated. The Core switch acts as Rendezvous Point for multicast.

6.5.2 Centralized VRM recording

The following example shows a centralized VRM recording scenario.
Specifications:
- 500 IP cameras, 5 disk arrays, and 10 workstations.
- Bosch VMS is used for managing.
- 1 Core/Distribution switch and 12 Access switches are used. Each switch is connected to 44 cameras, (one of the switches is connected to 16 cameras).
- Live bandwidth: 2 Mbps
- Recording bandwidth: 1 Mbps
- No multicast.
- Each Access switch has its own network via VLAN.
- No audio and no VCA is used.

The following illustration shows the example. Only one of the 12 Access switch segments is displayed.

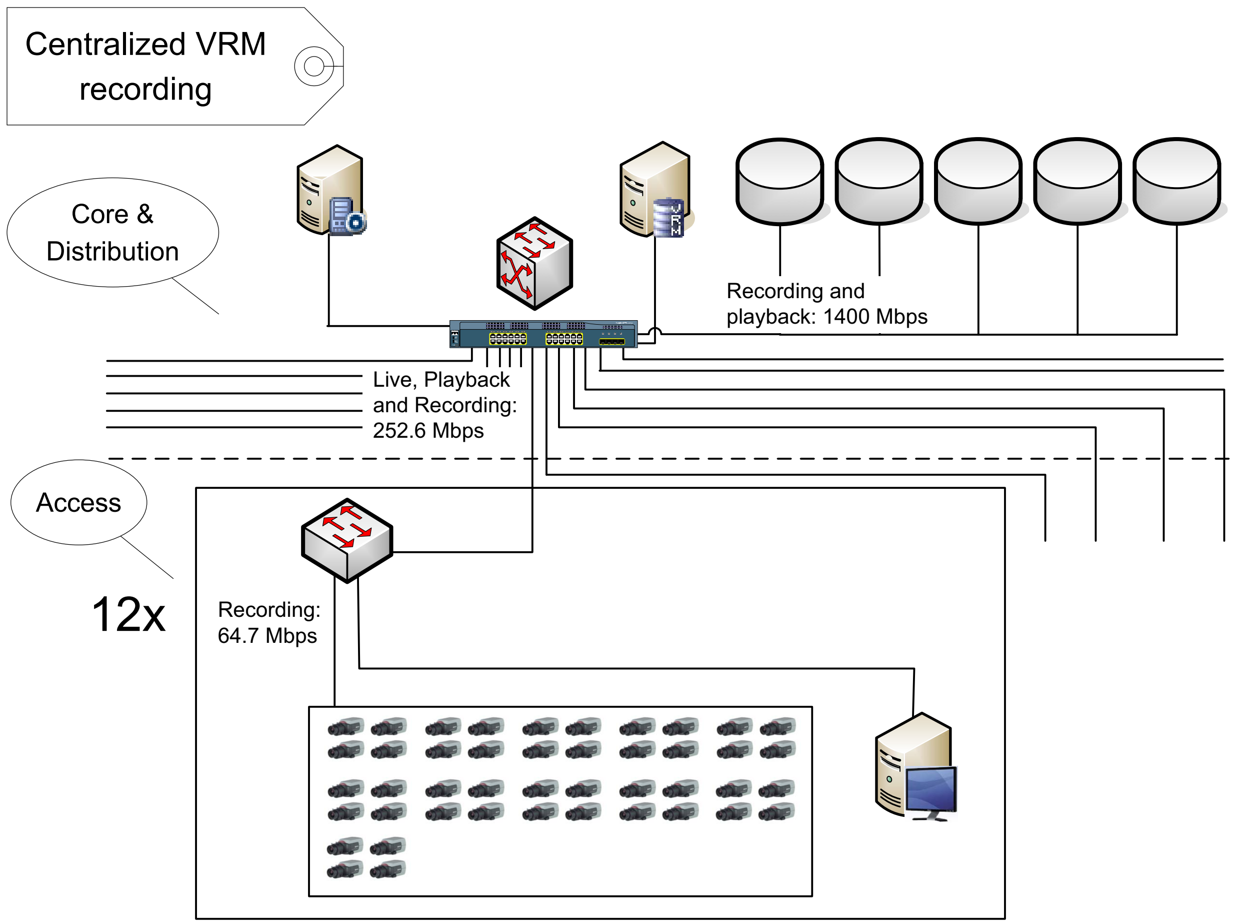

Figure 6.23 Centralized VRM recording

Bandwidth calculation for each Access switch:
Worst case bandwidth for live:
<bw_net> = 44 * 2 Mbps * 1.4 = 123.2 Mbps
Bandwidth for recording:
<bw_net> = 44 * 1 Mbps * 1.4 * 1.05 = 64.7 Mbps
Worst case bandwidth for playback:
<bw_net> = 44 * 1 Mbps * 1.4 * 1.05 = 64.7 Mbps
The overall bandwidth for each Access switch adds up to 252.6 Mbps.

Requirements for the Access switch
Layer 2 switch with 1 Gbit uplink port.

Bandwidth calculation for the Core switch:
Bandwidth for recording:
<bw_net> = 500 * 1 Mbps * 1.4 * 1.05 = 735 Mbps
Worst case bandwidth for playback:
<bw_net> = 500 * 1 Mbps * 1.4 * 1.05 = 735 Mbps

Requirements for the Core switch
Layer 3 switch with 2 Gbit connectivity

Bandwidth calculation for each disk array:
Recording bandwidth / number of disk arrays: 735 Mbps / 5 = 147 Mbps

Requirements for the disk arrays

300 Mbps disk array

6.5.3 Decentralized VRM recording

The following example shows a decentralized VRM recording scenario.

Specifications:

– 500 IP cameras, 12 disk arrays, and 12 workstations.
– Bosch VMS is used for managing.
– 1 Core/Distribution switch and 12 Access switches are used. Each switch is connected to 44 cameras, (one of the switches is connected to 16 cameras).
– Live bandwidth: 2 Mbps
– Recording bandwidth: 1 Mbps
– No multicast.
– Each Access switch has its own network via VLAN.
– No audio and no VCA is used.

The following illustration shows the example. Only one of the twelve Access switch segments is displayed.

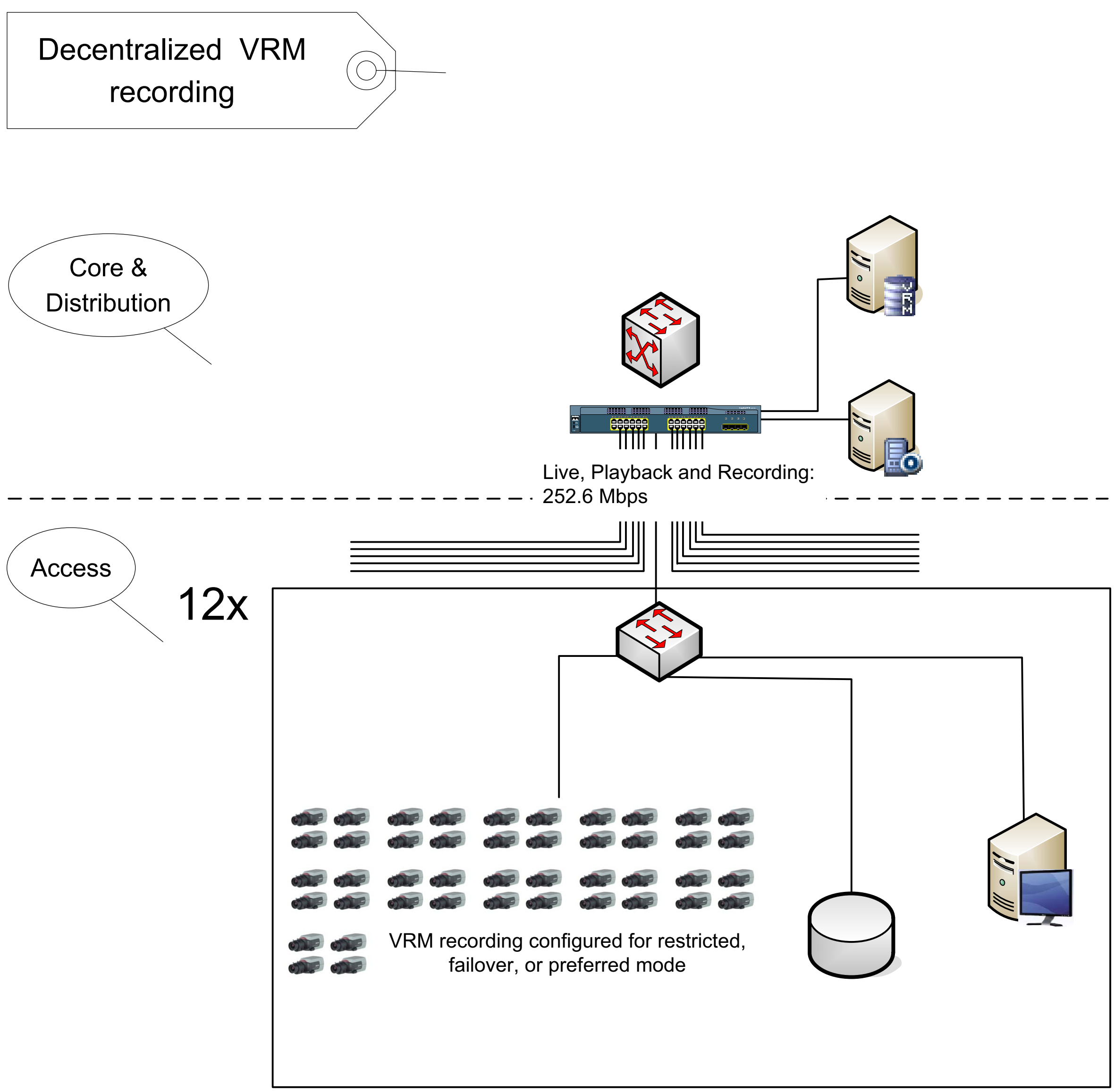

Figure 6.24 Decentralized VRM recording

Note:
The VRM Server in the Core Layer ensures that the video data is recorded on the correct iSCSI devices. Configure **Restricted**, **Failover**, or **Preferred** mode on the encoders to hold the recording traffic in its respective location. If you configure **All** mode, the recording traffic of a network segment can be forwarded to another network segment.
It is very important for decentralized recording that the Access switch segments are spatially separated. Usually they are located in different buildings. But very often the uplink capacities between buildings are not large enough. Keep this in mind when planning.

Bandwidth calculation for each Access switch:
Worst case bandwidth for live:
<bw_net> = 44 * 2 Mbps * 1.4 = 123.2 Mbps
Worst case bandwidth for playback:
<bw_net> = 44 * 1 Mbps * 1.4 * 1.05 = 64.7 Mbps
Bandwidth for recording:
<bw_net> = 44 * 1 Mbps * 1.4 * 1.05 = 64.7 Mbps
The overall bandwidth for each Access switch adds up to 252.6 Mbps.

Requirements for the Access switch
Layer 2 switch with 1 Gbit connectivity.

Requirements for the Core switch
Layer 3 switch with 1 Gbit connectivity

Bandwidth calculation for each disk array:
Recording bandwidth + Playback bandwidth = 129.4 Mbps

Bandwidth calculation for each workstation:
Live bandwidth + Playback bandwidth = 187.9 Mbps

6.5.4 Centralized NVR recording

The following example shows a centralized NVR recording scenario.
Specifications:
– 128 IP cameras, 2 NVRs, and 3 workstations.
– Bosch VMS is used for managing.
– 1 Core/Distribution switch and 4 Access switches are used. Each switch is connected to 32 cameras.
– Live bandwidth: 2 Mbps
– Recording bandwidth: 1 Mbps
– No multicast.
– No audio and no VCA is used.

The following illustration shows the example.

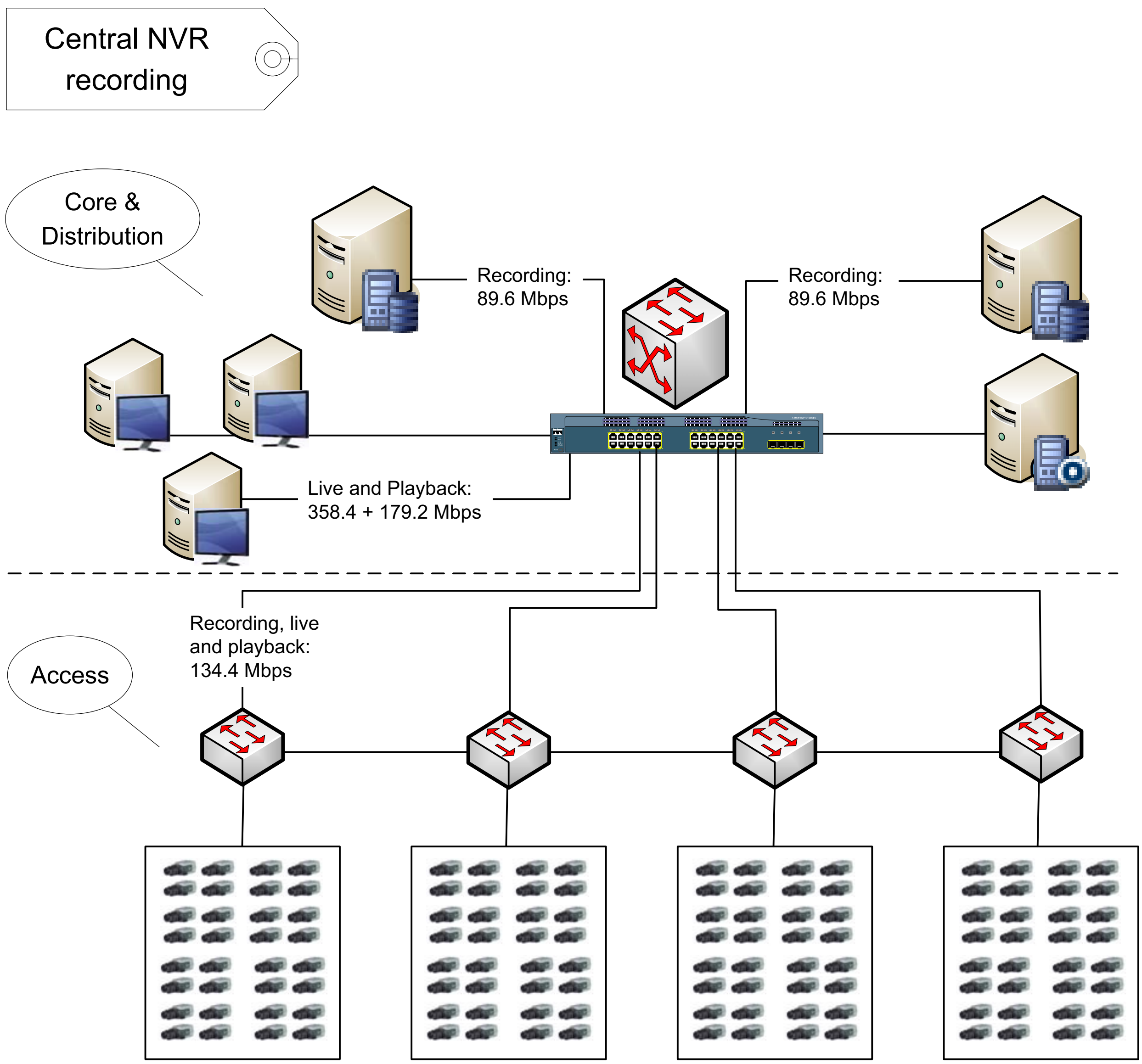

Figure 6.25 Centralized NVR recording

This scenario shows redundant connections between switches. These redundancies must be monitored and a connection loss must trigger an alarm. Otherwise it can happen that one connection after the other breaks without being notified until the last connection loss stops the complete system.

Bandwidth calculation for each Access switch:

Worst case bandwidth for live:

<bw_net> = 32 * 2 Mbps * 1.4 = 89.6 Mbps

Bandwidth for recording:

<bw_net> = 32 * 1 Mbps * 1.4 = 44.8 Mbps

This adds up to 134.4 Mbps for each Access switch.

Requirements for the Access switch

Layer 2 switch with 1 Gbit connectivity and Rapid Spanning Tree Protocol feature activated.

Bandwidth calculation for the Core switch:
Worst case bandwidth for live:
<bw_net> = 128 * 2 Mbps * 1.4 = 358.4 Mbps
Worst case bandwidth for playback:
<bw_net> = 128 * 1 Mbps * 1.4 = 179.2 Mbps
Bandwidth for recording:
<bw_net> = 128 * 1 Mbps * 1.4 = 179.2 Mbps
This adds up to 716.8 Mbps.

Requirements for the Core switch
Layer 3 switch with 1 Gbit connectivity and Rapid Spanning Tree Protocol feature activated.

Bandwidth calculation for each NVR:
Overall recording bandwidth / number of NVRs = 179.2 Mbps / 2 = 89.6 Mbps

6.5.5 Decentralized NVR recording

The following example shows a decentralized NVR recording scenario with a Failover NVR.
Specifications:
- 64 IP cameras, 2 NVRs, and 2 workstations.
- Bosch VMS is used for managing.
- 1 Core/Distribution switch and 2 Access switches are used. Each switch is connected to 32 cameras.
- Live bandwidth: 2 Mbps
- Recording bandwidth: 1 Mbps
- No multicast.
- Each Access switch has its own network via VLAN.
- No audio and no VCA is used.

NVR recording is performed on each network segment independently. Only in case of failure the Failover NVR in the Core Layer takes over the recording task for the failed NVR.
This scenario uses the Rapid Spanning Tree Protocol to avoid that data packets are duplicated and transported via multiple paths.
The following illustration shows the example.

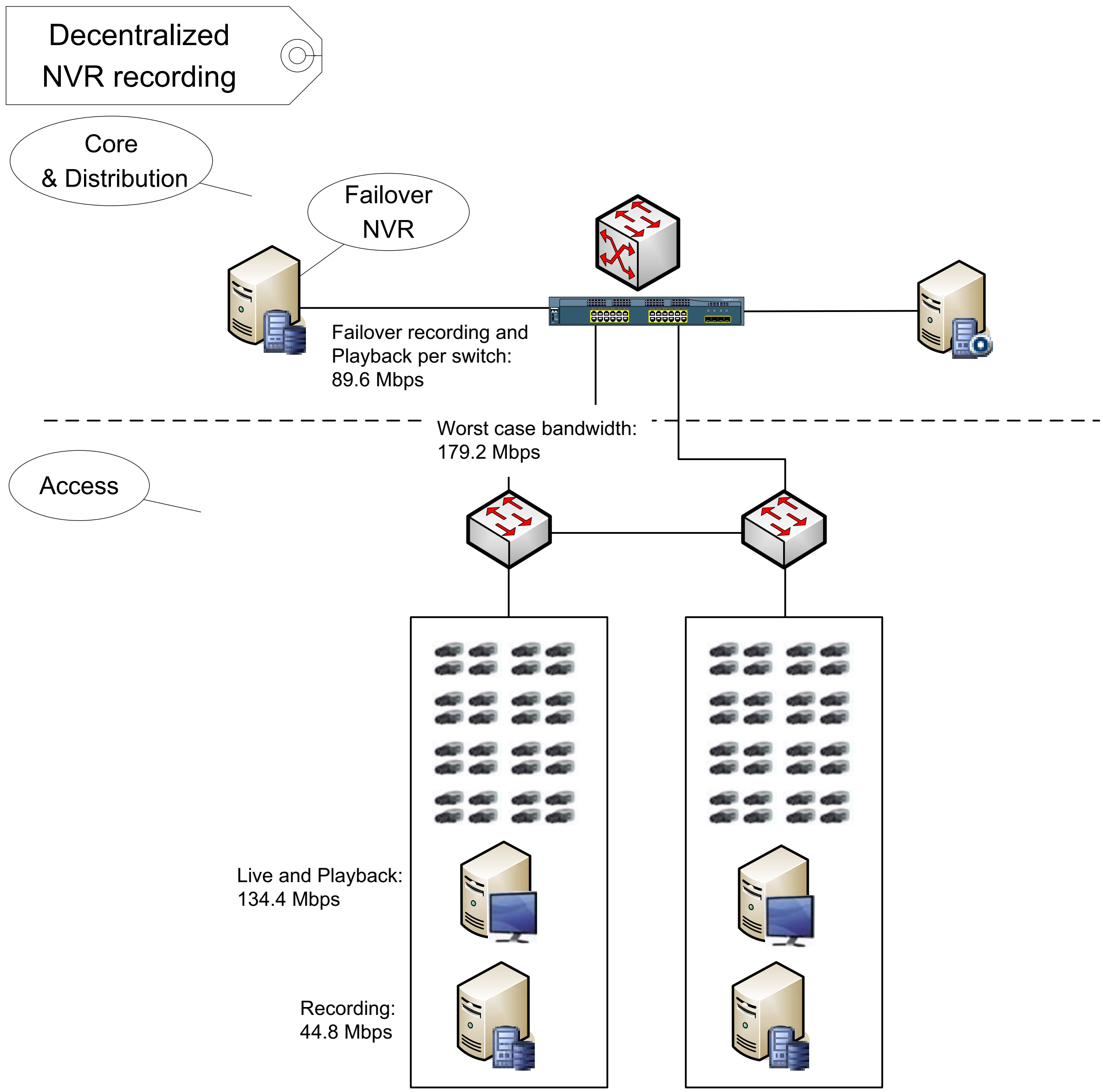

Figure 6.26 Decentralized NVR recording

This scenario shows redundant connections between switches. These redundancies must be monitored and a connection loss must trigger an alarm. Otherwise it can happen that one connection after the other breaks without being notified until the last connection loss stops the complete system.

Bandwidth calculation for each Access switch:

Bandwidth for recording:

<bw_net> = 32 * 1 Mbps * 1.4 = 44.8 Mbps

Worst case bandwidth for playback:

<bw_net> = 32 * 1 Mbps * 1.4 = 44.8 Mbps

Worst case bandwidth for live:

<bw_net> = 32 * 2 Mbps * 1.4 = 89.6 Mbps

Worst case recording bandwidth:

This worst case takes place if one Access switch has lost its connection to the Core switch and the Failover NVR took over the tasks of both NVRs.

<bw_net> = 89.6 Mbps * 2 = 179.2 Mbps

Bandwidth calculation for each NVR:
Recording bandwidth per switch = 44.8 Mbps

Requirements for the Access switch:
Layer 2 switch with 1 Gbit connectivity and Rapid Spanning Tree Protocol feature activated.

Bandwidth calculation for the Failover NVR:
If a Primary NVR fails, the Failover NVR takes over its tasks. In this case the Failover NVR requires 44.8 Mbps for recording and up to 44.8 Mbps for playback.

Requirements for the Core switch
Layer 3 switch with 1 Gbit connectivity and Rapid Spanning Tree Protocol feature activated.

6.5.6 Pros and Cons of the different recording solutions

The following network models are discussed:
- Direct-to-iSCSI recording
- Centralized VRM recording
- Decentralized VRM recording
- Centralized NVR recording
- Decentralized NVR recording

From an IT Engineer point of view the centralized solution is usually preferred. A centralized solution is easier to manage and easier to scale. Additionally all management software and hardware is concentrated in a room or in a part of the building. “At the edge” there are only cameras and encoders.

The disadvantage of centralized recording is that you need very powerful (end expensive) Core switches. Another disadvantage is that you must spend a lot of money and resources for fallback solutions. If the Core switch fails, the entire system stops working when there is no failover.

The decentralized solution offers more stability. When a switch or network segment fails, recording in the other segments is not affected. In a VRM recording environment even the Core switch with the VRM Server connected can fail without an immediate influence on recording. But the scalability of decentralized recording is restricted. When new cameras are added to all network segments, the storages in the segment are possibly too small and must be exchanged. In a centralized solution it is sufficient to exchange or expand the central storage device. And the maintenance of of a large number of distributed devices is much more difficult than the maintenance of the devices in a centralized solution.

Direct-to-iSCSI recording is completely independent from switches. As long as the encoder and the iSCSI device are up and running, recording continues. But you need a number of small storage devices which might be much more expensive than one large storage.

Index

Bosch Sicherheitsssysteme GmbH
Robert-Koch-Straße 100
D-85521 Ottobrunn
Germany
Phone 089 6290-0
Fax 089 6290-1020
www.boschsecurity.com