Dallmeier

REV. 2.0.1 | 2020-11-24

WHITEPAPER

BASIS-INFORMATION

SWITCH BASICS & VIDEO NETZWERKE

ERLÄUTERUNGEN, GRUNDLEGENDE DATEN UND ANWENDUNGSBEISPIELE
ZU SWITCHES IN DIGITALEN VIDEONETZWERKEN

MADE IN GERMANY

See more.

INHALT

ZUSAMMENFASSUNG

Ein Switch ist ein Netzwerkgerät mit zentraler Funktion für jedes digitales Videoüberwachungssystem. Er ist für die Steuerung und Verteilung von Datenpaketen verantwortlich und ermöglicht die Verbindung von Netzwerkkomponenten und Endgeräten.

Der IT-Markt bietet eine große Auswahl an Switches, die sich in Bezug auf Qualität und integrierte Funktionen wesentlich unterscheiden. Vor allem hinsichtlich der Funktionsfähigkeit weiterer Komponenten und Geräte, sollte daher die Wahl eines geeigneten Switches qualitative und ökonomische Argumente mit einbeziehen.

Um sicherzustellen, dass der komplette Funktionsumfang von Dallmeier-Systemen genutzt werden kann, enthält dieses Dokument verschiedene Begriffserklärungen sowie Grundlageninformationen und Anwendungsbeispiele zu spezifischen Einsatzgebieten und Verwendungszwecken der unterschiedlichen Switches. Darüber hinaus sind Tabellen mit Leistungsklassen und Richtwerten inklusive grundlegender Daten enthalten, die dem jeweiligen Nutzer beim Einsatz und der Auswahl des geeigneten Switches Orientierung bieten und Hilfestellung leisten.

Da nicht alle Komponenten und Kombinationen testbar bzw. überschaubar sind, übernimmt Dallmeier für die in diesem Dokument ausgeführten Beschreibungen, Daten und Beispiele keinerlei Haftung oder Gewährleistung. Zudem handelt es sich bei den jeweiligen Hinweisen und Richtwerten ausschließlich um Empfehlungen, welche lediglich zu Informationszwecken dienen und rechtlich unverbindlich sind.

Eine Liste von Switches, die von uns umfassend getestet und geprüft wurden, finden Sie im Whitepaper „Whitelist Switch“.

ERLÄUTERUNG

2.1 ALLGEMEIN

Ein moderner Switch ist nicht - wie viele ihn beschreiben - eine Mehrfachsteckdose (Hub) für Netzwerkkabel, sondern vielmehr eine intelligente Schaltzentrale, die das Rückgrat einer digitalen Videoüberwachung bildet. Daher sollte die Wahl des Switches sorgfältig getroffen werden. Ein minderwertiger Switch kann ein Videonetz erheblich beeinträchtigen, was sich dann oft in unerklärbaren Phänomenen äußert:

- Verzögerungen beim Verbindungsaufbau
- Erhöhtes Delay bei Live-Übertragungen
- Aufzeichnungslücken
- Verbindungsabrisse
- Encoder-/Decoder-Ausfälle
- Ruckeln und/oder Bildartefakte bei der Übertragung
- etc.

2.2 INTERNE BANDBREITE

Ein Hub verteilt das anliegende Signal ungesehen auf alle angeschlossen Geräte. Dadurch muss die verfügbare Bandbreite zwischen allen Geräten im Netzwerk aufgeteilt werden. Beim Switching hingegen wird eine direkte Verbindung zwischen zwei Endgeräten geschaltet. Somit können mehrere Leitungen nebeneinander mit der vollen Netzwerkbandbreite genutzt werden, sofern der Switch die erforderliche Schaltleistung erfüllen kann.

Ein Flaschenhals entsteht nur dann, wenn mehrere Geräte gleichzeitig versuchen mit einer bestimmten Station zu kommunizieren. Switches haben typischerweise 8, 16, 24 oder 48 Ports (Anschlüsse). Diese Access Ports sind üblicherweise in den Ausführungen 10/100 MBit/s und 10/100/1000 MBit/s erhältlich.

Ein Switch sollte in der Lage sein, auf allen Anschlüssen gleichzeitig die volle Netzwerkbandbreite zu verwalten. Dies bedeutet, dass z. B. ein 24-Port-Switch mit je 100 MBit/s mindestens über eine „interne“ Bandbreite (Wirespeed) von 2400 MBit/s (2,4 GBit/s) verfügen muss. Switches aus den unteren Preisklassen erreichen diese Leistung oftmals nicht. Entsprechende Angaben sind manchmal auch unter den Begriffen „Backplane Speed“ oder „Forwarding Rate“ in den jeweiligen Produktdatenblättern zu finden. Leider wird der Wirespeed jedoch nicht von allen Herstellern angegeben.

Verschiedene Geräte besitzen neben den regulären Ports bis zu 4 weitere sog. „Uplink Ports“. Diese Ports werden für die Verbindung zu weiteren Switches verwendet. Die Uplinks unterstützen deshalb in den meisten Fällen eine höhere Geschwindigkeit oder sind als Modulslot für sog. „SFP-Module“ ausgeführt (auch Mini-GBIC genannt; Näheres hierzu nachstehend).

> *Ob ein Switch-Port als Uplink oder als Access Port verwendet werden kann, hängt von der jeweiligen Konfiguration des Ports ab.*

2.3 POWER OVER ETHERNET

Mit Power over Ethernet (PoE) wird das Verfahren bezeichnet, mit welchem über ein Ethernet-Kabel diverse Netzwerkkomponenten (z. B. eine Netzwerkkamera) gleichzeitig mit Daten und Strom versorgt werden können.

Beim Anschluss eines Endgeräts an einen PoE-fähigen Switch ermittelt die Funktion zunächst über eine Widerstandsprüfung, ob das Endgerät (PD = Powered Device) Strom benötigt. Im nächsten Schritt wird über die PoE-Klasse bestimmt, wie viel Strom das Gerät maximal verbrauchen kann.

Die maximale Abgabeleistung eines PSE (Power Supply Equipment) ist bei PoE auf ca. 15 Watt begrenzt. Aufgrund von zu berücksichtigenden Leitungsverlusten darf der Endverbraucher (die Netzwerkkomponente) jedoch maximal nur 12,95 W beziehen. Beim neueren Standard PoE+ ist eine Abgabeleistung von bis zu 30 W möglich.

Da ein Switch in den wenigsten Fällen alle Ports mit maximaler PoE-Leistung versorgen kann, muss das Verhalten des Switches festgelegt werden. Die Konfigurationsmöglichkeiten sind jedoch vom jeweiligen Gerät abhängig. Einige Geräte weisen nur eine begrenzte Anzahl von PoE-Ausgängen auf, andere limitieren die Leistung über ein PoE-Budget und wieder andere erlauben eine detaillierte Leistungskonfiguration über das Switch-Management, bis hin zu einer Abschaltpriorität. Ist das PoE-Budget erschöpft, werden weitere Ports nicht mehr mit Strom versorgt. Dies gilt bei einigen Switches bereits dann, wenn das Budget der theoretisch maximalen Leistung erreicht wird.

> *Testen Sie auch den Ernstfall und simulieren Sie einen Stromausfall. Nicht jeder Switch beherrscht sequenzielles Einschalten der PoE-Ports (Einschaltstrom/Anlaufstrom).*

Die Standards IEEE 802.3af oder IEEE 802.3at beschreiben einen Verbraucher (Powered Device, PD) und den Stromversorger (Power Source Equipment, PSE).

Klasse	Leistung Verbraucher (PD)	Max. Leistung Stromversorger (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

Tabelle 2-1: Leistungsklassen nach IEEE 802.3af (PoE) und IEEE 802.3at (PoE+ / PoE plus)

2.4 LAYER 2 UND 3 SWITCHES

2.4.1 OSI-Referenzmodell

Das OSI-Referenzmodell ist ein Referenzmodell für Netzwerkprotokolle als Schichtenarchitektur. Es beschreibt die Kommunikation über unterschiedlichste technische Systeme hinweg. Dazu definiert dieses Modell sieben aufeinanderfolgende Schichten (engl. layers) mit jeweils eng begrenzten Aufgaben. Die Netzwerkprotokolle einer Schicht sind mit klaren Schnittstellen definierte und einfach untereinander austauschbar, selbst wenn sie, wie das Internet Protocol, eine zentrale Funktion haben.

OSI-Referenzmodell					
OSI-Schicht / Layer		Protokoll-beispiele	Einheit	Kopplungsele-mente	Beschreibung
7	Anwendungen (Application)	HTTP FTP HTTPS SMTP LDAP RTSP	Data	Gateway (Firewall), Content-Switch, Layer-4-7-Switch	Ermöglicht Anwendungen den Zugriff auf das Netzwerk
6	Darstellung (Presentation)				Übersetzung von Applikationsformaten ins Netzwerkformat und umgekehrt (formatiert, ver-/entschlüsselt)
5	Sitzung (Session)				Baut logische Verbindungen auf, kontrolliert, synchronisiert und beendet diese
4	Transport (Transport)	TCP UDP SCTP SPX	Segmente		Wandelt Datenpakete laut Protokoll um, kontrolliert diese und stellt sie den darüberliegenden Schichten zur Verfügung
3	Vermittlung (Network)	ICMP IGMP IP IPsec IPX	Pakete	Router Layer-3-Switch	Steuert den Austausch von Datenpaketen, übernimmt die Wegfindung (Routing), baut Verbindungskanäle auf und ab
2	Sicherung (Data Link)	Ethernet Token Ring FDDI	Blöcke (Frames)	Bridge Switch	Sorgt für zuverlässigen Datenaustausch, verbindet Bits zu Blöcken, fügt eine Prüfsumme hinzu und gibt diese an die Vermittlungsschicht weiter
1	Bit Übertragung (Physical)		Bits	Repeater Hub	Stellt mechanisch sowie elektrisch eine physikalische Verbindung her, um Bits zu übertragen

Tabelle 2-2: OSI Referenze Modell

2.4.2 Layer-2-Switch

Der Layer 2 wird im OSI-Modell als „Sicherungsschicht“ bezeichnet und ist hauptsächlich für eine fehlerfreie Datenübertragung zuständig. Ein sog. „Layer-2-Switch“ arbeitet mit MAC-Adressen (Media-Access-Control-Adresse), welche mit dem dazugehörigen physikalischen Port in der SAT (Source-Address-Table) festgehalten werden.

Der Switch verwendet die Source-Address-Tabelle, um Entscheidungen für die Datenweiterleitung zu treffen (dieses Verhalten wird auch als „Switching“ bezeichnet). Der Vorteil von Layer-2-Switches liegt darin, dass sie ohne große Vorkenntnisse in Betrieb genommen werden können (Plug and Play).

2.4.3 Layer-3-Switch

Der Layer 3 ist im OSI-Modell die „Vermittlungsschicht“. Sie sorgt für das Schalten von Verbindungen und das Weiterleiten von Datenpaketen. Verbindungsaufbau sowie die Weiterleitung zu anderen Ports (Netzwerken) werden über das Internet Protocol (IP) und diverse Routingfunktionen realisiert.

Der Layer-3-Switch lässt sich als Kombination aus Router und Switch darstellen. Voraussetzung für das optimale Einbinden von Layer-3-Switches ist aufgrund der Vielzahl ihrer Funktionen eine detaillierte und individuell an das Netzwerk angepasste Konfiguration.

2.5 MANAGED UND UNMANAGED SWITCH

Managebare Switches verfügen, neben der grundlegenden Switching-Funktion (Layer 2), in der Regel über eine Bedienerschnittstelle. Dies bietet zusätzliche Steuer- und Überwachungsfunktionen, wie z. B. Virtual Local Area Network (VLAN), Quality of Service (QoS), Spanning Tree Protocol (STP/RSTP), IP-Filterung, Routing usw., die für ein Netzwerk ab einer/m bestimmten Größe/Funktionsumfang hilfreich bzw. notwendig sind.

Das Management wird je nach Hersteller über eine Steuersoftware, Weboberfläche, Konsole oder einer Kombination dieser Möglichkeiten vorgenommen. Da der Benutzer diese Art von Switches aktiv in ihrer Arbeitsweise beeinflussen kann, bezeichnet man sie als „Managed Switch“. Folglich bezeichnet man einen Switch, der das Eingreifen eines Benutzers nicht vorsieht, als „Unmanaged Switch“.

2.6 ACCESS, DISTRIBUTION UND CORE SWITCH

Ein Access Switch ist ein Switch, welcher als Schnittstelle zu Endgeräten verwendet wird. Er erlaubt die Verbindung verschiedenster Geräte (Kameras, Aufzeichnungsserver, Workstations) mit dem Netzwerk.

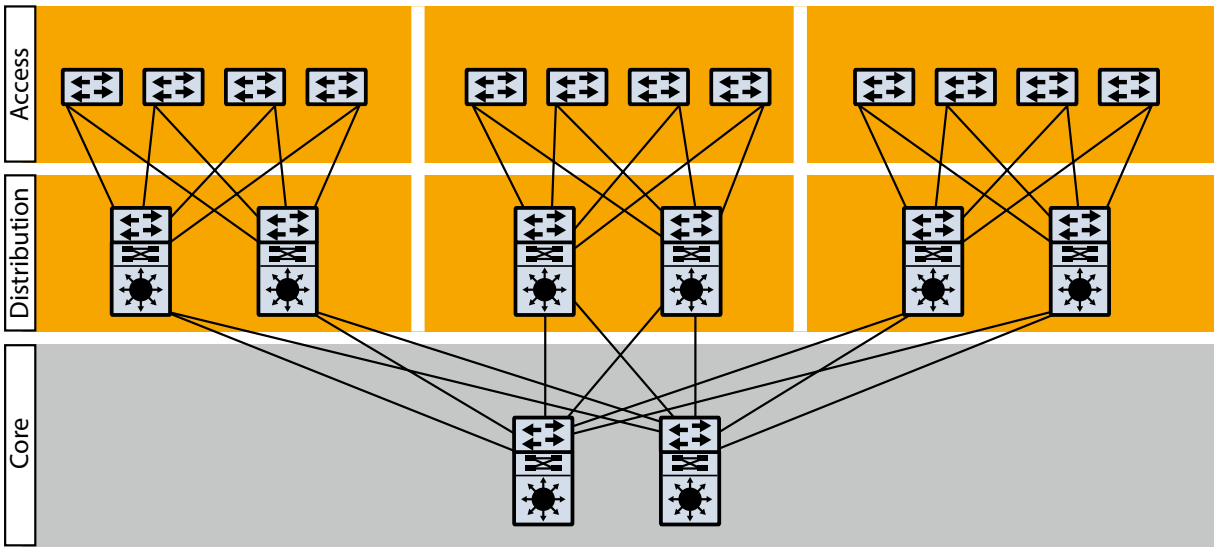

Abb. 2-1: Core, Distribution und Access Switches

In großen Netzwerken werden oftmals Distribution Switches als Verteiler zwischen Access und Core Switch eingesetzt.

Der Core Switch ist ein sehr leistungsfähiger Switch, der das Rückgrat (backbone) eines Netzwerks bildet. Dabei dient er zur Verbindung der verschiedenen Netzwerkkomponenten (Access/Distribution Switches) untereinander. Core Switches sind meist mit Gigabit-Schnittstellen ausgestattet, um den angeschlossenen Netzwerkkomponenten eine hohe Bandbreite zur Verfügung zu stellen..

Ein Core Switch kann auch Access Ports besitzen.

2.7 BROADCAST-DOMÄNE UND BROADCASTING

Eine Broadcast-Domäne besteht aus einem lokalen Netzwerk auf Layer 2 Basis. In diesem Verbund kann jeder Host (Netzwerkgerät) jeden über einen sog. „Broadcast“ (Anfrage an alle im Netz) erreichen.

Broadcasts können auch auf Layer 3 (Internetprotokoll) des OSI-Modells abgesetzt werden, vorausgesetzt die darunterliegende Ebene unterstützt dies. Broadcast-Domänen werden mit Layer 3 Netzwerkkomponenten (Router, Layer-3-Switch) getrennt. Somit kann ein Broadcast der z. B. von PService (Konfigurations- und Verwaltungsprogramm für IP-Systeme von Dallmeier) ausgelöst wird, nicht von einem Subnetz in ein weiteres Subnetz übertragen werden.

Ein Subnetz ist ein Teilnetz, das mittels einer Subnetzmaske (Layer 3) getrennt wurde. Subnetze werden über Router oder Layer-3-Switches und deren Gateway verbunden. Daraus lässt sich schließen, dass jedes Subnetz seine eigene Broadcast Domäne besitzt.

Möchte man mit PService Dallmeier IP-Geräte scannen, muss man sich in der gleichen Broadcast-Domäne befinden.

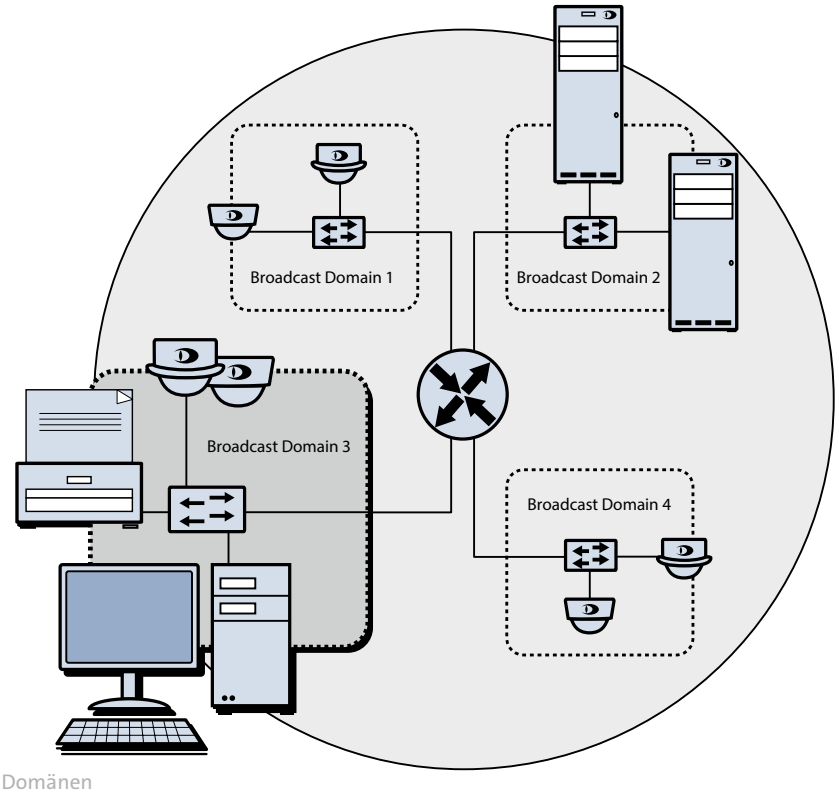

Abb. 2-2: Broadcast Domänen

2.8 SFP PORT

Der SFP (Small Form-factor Pluggable) ist ein Port, der den Anschluss eines SFP-Moduls (auch „miniaturisierter Gigabit Interface Converter“ oder „Mini-GBIC“ genannt) zur Verbindung von Ethernet-Übertragungsmedien, wie Fibre Channels (Glasfaser) oder Twisted Pairs (verdrillte Adernpaare aus Kupfer), im Netzwerk erlaubt.

Abb. 2-3: Beispiel für eine SFP-Schnittstelle mit einem passenden Modul

2.8.1 SFP Twisted Pair Kabeltypen

Shielded Twisted Pair (STP) bzw. Foiled Twisted Pair (FTP) Kabel besitzen vier Kupfer Adernpaare. Ein Paar besteht aus zwei Adern, was sich auf insgesamt acht Adern pro Kabel beläuft. Diese Adernpaare sind mit je einem Paarschirm (S = Drahtgeflecht- oder F = Folienschirm) umgeben.

Unshielded Twisted Pair (UTP) Kabel bestehen ebenfalls aus Kupfer und haben grundsätzlich denselben Aufbau wie STP/FTP Kabel, jedoch keinen Paarschirm. Dies hat zur Folge, dass UTP-Kabel anfälliger gegen äußere elektromagnetische Einflüsse sind. Es gibt mehrere Varianten des STP/FTP/UTP Kabels, die sich durch ihr Material und das Vorhandensein eines Gesamtschirms unterscheiden.

2.8.2 SFP Glasfaser Kabeltypen

Bei Monomodefasern (Single-Mode Fibre, SMF) wird ein einzelner Lichtstrahl eines Lasers durch die Mitte der Faser übertragen. Diese Art der Glasfaserübertragung eignet sich besonders für weite Übertragungswege.

Bei Multimodefasern (Multi-Mode fibre, MMF) wird eine LED für die Übertragung verwendet. Diese sendet nicht einen gebündelten Lichtstrahl durch das Kabel, sondern gibt mehrere Lichtstrahlen mit verschiedenen Einfallswinkeln ab.

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) / 10 km (approx. 6.21 mi)
1000BASE-ZX	SMF	70 km (approx. 43.5 mi)
10GBASE-ZR	SMF	80 km (approx. 49.71 mi)

Tabelle 2-3: SFP Kabeltypen

2.8.3 Dual-Purpose SFP Port

Der Dual-Purpose ist ein Port, der den Anschluss eines SFP-Moduls oder eines RJ45-Steckers zur Verbindung mit dem Netzwerk erlaubt.

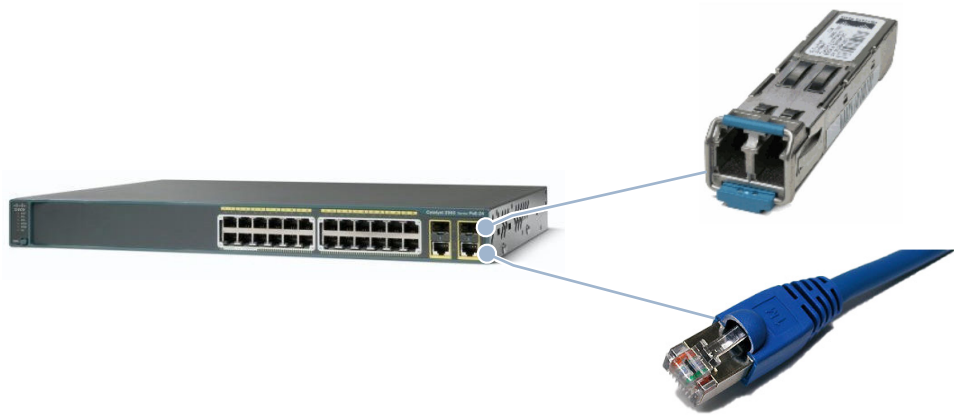

Abb. 2-4: Beispiel für eine Dual-Purpose Schnittstelle

2.9 QUALITY OF SERVICE

Quality of Service (QOS) ist eine Paket Priorisierung die sicherstellt, dass zeitlich kritische oder wichtige Anwendungen ihre Daten bevorzugt über das Netzwerk erhalten. Für QoS existieren zwei Mechanismen:

2.9.1 Integrated Services

Bei Integrated Services (IntServ) werden benötigte Bandbreiten schon im Vorhinein auf den einzelnen Netzwerkgeräten reserviert. Um diesen Mechanismus ordnungsgemäß und vollumfänglich zu implementieren, muss dies von allen Netzwerkkomponenten unterstützt werden.

2.9.2 Differentiated Services

Mit Differentiated Services (DiffServ) werden Datenpakete markiert und entsprechend der Konfiguration vom Netzwerk verarbeitet.
DiffServ hat sich mittlerweile in der Praxis wegen einer besseren Skalierbarkeit und einer höheren Kompatibilität gegenüber IntServ durchgesetzt.

2.10 SPANNING TREE PROTOCOL

Das Spanning Tree Verfahren, dessen Aufgabe es ist Schleifen (parallele Verbindungen bzw. „Loops“) in geswitchten Ethernet-Netzwerk zu unterbinden und redundante Pfade vorzuhalten, arbeitet auf der MAC-Ebene (Layer 2).

Eine Schleife kann in einem Netzwerk erhebliche Fehlfunktionen (insbesondere in Hinblick auf „Broadcast Storms“) verursachen. Um dies zu vermeiden, legt das Spanning Tree Protocol (STP) über das vorhandene physikalische Netzwerk einen „Spannbaum“ in dem jedes Ziel nur über einen Pfad erreichbar ist. Redundante Verbindungen werden durch Deaktivieren der jeweiligen Ports beseitigt. Welche Verbindung getrennt wird, hängt von seiner Qualität ab.

Der logische Spannbaum wird durch die Definition einer Root Bridge (Wurzel des Spannbaums) über das Bridge Protokoll (darauffolgende Kommunikation der Switches (falls STP-fähig) untereinander) aufgebaut. Die hier verwendeten Datenpakete nennt man „Bridge Protocol Data Units“ (BPDU). Sie werden mittels Broadcasts im Netzwerk von Switch zu Switch verteilt. Nach dem Aufbau der Baumstruktur wird von der Root Bridge zyklisch alle 2 Sekunden ein Statusbericht (Keepalive) von einem Switch zum jeweils nachfolgenden Switch ausgegeben.

Bleibt einer dieser Statusberichte aus, ist eine Veränderung im Netzwerk aufgetreten (z. B. Ausfall einer Netzwerkverbindung oder eines Switches) und das Netzwerk muss sich reorganisieren. Diese Reorganisierung beinhaltet das Löschen und den Neuaufbau des logischen Spannbaums. Das kann bei STP bis zu 30 Sekunden dauern. Während dieser Zeit wird außer dem Spanning Tree Protokoll jede Kommunikation im Netzwerk unterbunden.

Da solche Ausfallzeiten in der Vergangenheit in bestimmten Situationen nicht akzeptabel waren, wurde als Weiterentwicklung des Spanning Tree Protocol das Rapid Spanning Tree Protocol (RSTP) eingeführt. Mit dieser Weiterentwicklung wird das Netz nicht mehr unmittelbar nach dem Ausfall eines Statusberichts blockiert, sondern es wird parallel zum regulären Netzbetrieb eine alternative Route ermittelt. Sobald die Berechnung der Alternative erfolgreich ist, wird die aktuelle Struktur (fehlerhaft) durch die neue Berechnung ersetzt. Somit kann die Dauer von Netzausfällen auf weniger als eine Sekunde begrenzt werden.

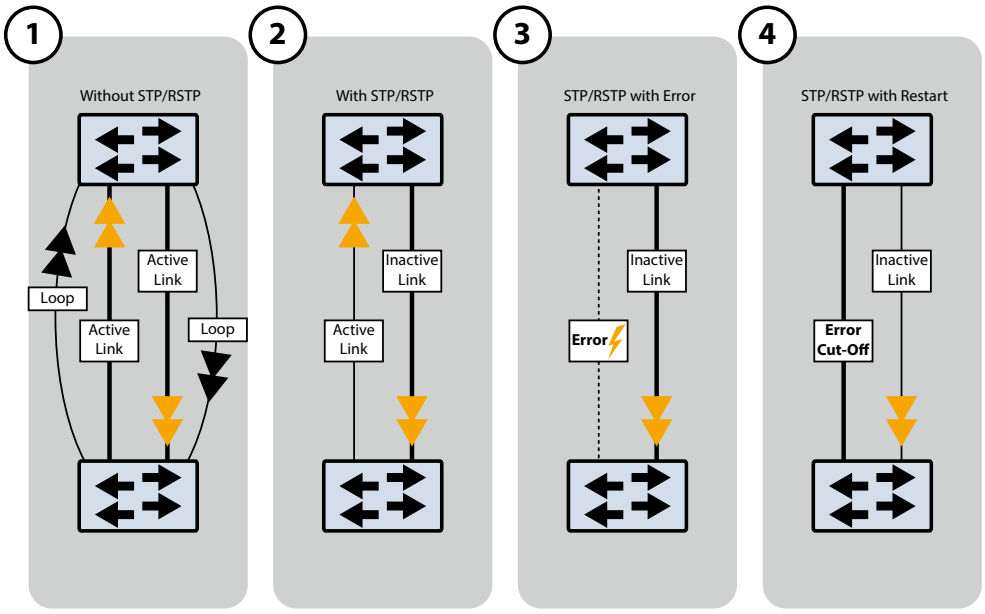

Abb. 2-5: STP (Spanning Tree Protocol) und RSTP (Rapid Spanning Tree Protocol)

2.11 ENCODER UND DECODER

Als Encoder wird in den folgenden Ausführungen jedes netzwerkfähige Gerät bezeichnet, dessen Hauptaufgabe in der Erfassung, Codierung und Versendung von Videodaten besteht, wie z. B. eine Netzwerkkamera.

Als Decoder wird in den folgenden Ausführungen jedes netzwerkfähige Gerät bezeichnet, dessen Hauptaufgabe im Empfang, der Dekodierung und der Anzeige von Videodaten besteht, wie z. B. eine Workstation mit Client Software zur Auswertung des Videomaterials.

2.12 UNICAST UND MULTICAST

2.12.1 Unicast

Unicast ist eine Verbindung, die von einem Sender (Encoder) zu einem Empfänger (Decoder) aufgebaut wird. Folglich wird für jeden Verbindungsaufbau von einem Client zu einem Aufzeichnungsgerät oder einer Kamera ein separater Übertragungskanal initialisiert. Je mehr Betrachter es gibt, desto mehr Verbindungen werden benötigt, was zu einer Überlastung des Netzwerks und auch des Senders (z. B. Kamera Overload) führen kann.

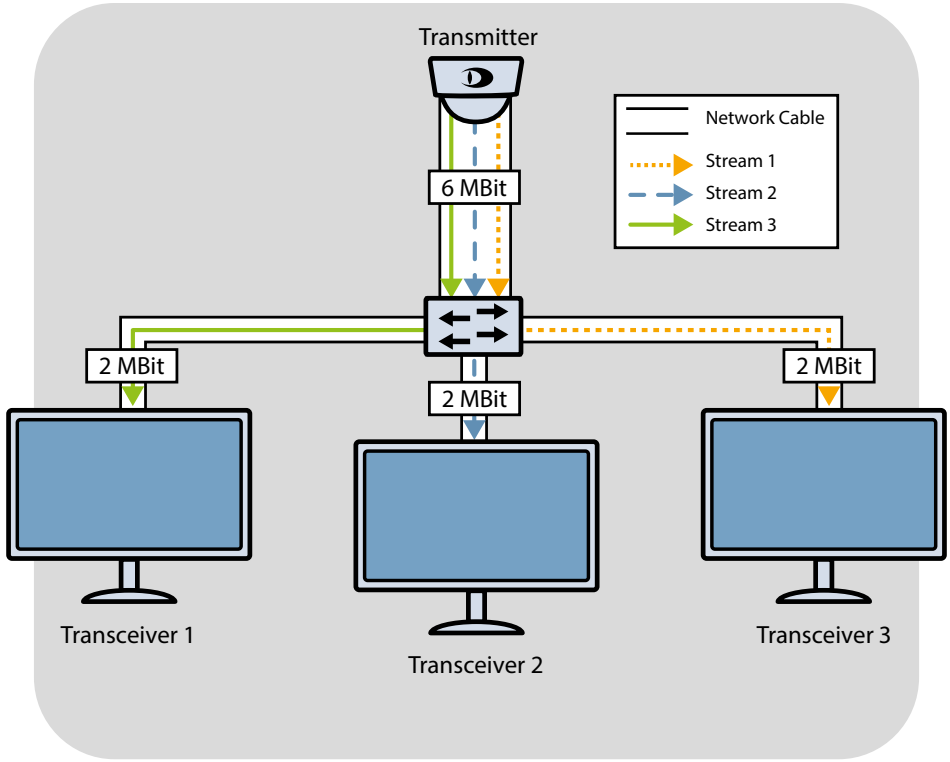

Abb. 2-6: Beispiel für Unicast

2.12.2 Multicast

Als Multicast bezeichnet man eine Verbindung, die von einem Sender (Encoder) zu mehreren Empfängern (Decoder) aufgebaut wird. Es ermöglicht die Übertragung eines Datenstromes von einem Sender (über einen einzigen Kanal) an beliebig viele Teilnehmer. Multicast kann somit die Menge des Netzwerkverkehrs den das mehrfache Anzeigen von Kameras erzeugt erheblich reduzieren. Der Sender erhält dazu eine spezielle zusätzliche IP-Adresse (Gruppenadresse) aus dem Multicast-Bereich zwischen 224.0.0.0 bis 239.255.255.255.

Die Teilnehmer melden sich mit Hilfe des Internet Group Messaging Protocols (IGMP) an. Die beteiligten Netzwerkkomponenten, wie Router oder Switches, müssen dafür Sorge tragen, dass möglichst nur die erwünschten und benötigten Multicast-Ströme übermittelt werden. Für Multicast sind die Adressen im Bereich 225.x.x.x bis 232.x.x.x und 234.x.x.x bis 238.x.x.x frei verfügbar. Für den lokalen Einsatz empfiehlt sich der Bereich 239.x.x.x bis 239.255.255.255, da dieser als nicht öffentlich gekennzeichnet ist und nicht ins Internet geroutet wird.

Die Adressangaben sind unverbindlich. Beachten Sie daher die aktuellen Spezifikationen und Richtlinien zu den einzelnen Adressbereichen!

Damit Multicast (IGMP) eingesetzt werden kann, muss es von allen beteiligten Komponenten (Switch, Kamera, Aufzeichnungsserver) unterstützt werden. Eine einzige nicht Multicast-fähige Netzwerkkomponente kann die gesamte Funktion beeinträchtigen. Multicast stellt relativ hohe Ansprüche an Switches.

Dallmeier nutzt Multicast-Verbindungen hauptsächlich für die Live-Übertragung vom Encoder zum Decoder.

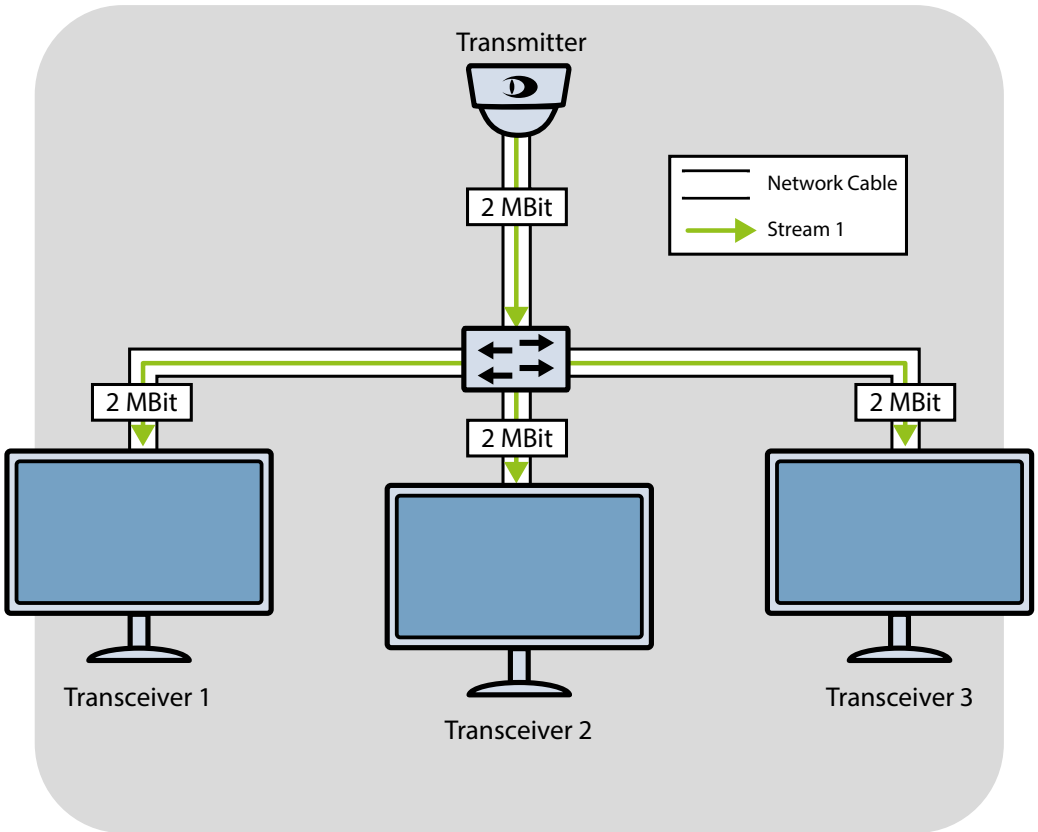

Abb. 2-7: Beispiel für Multicast

2.13 INTERNET GROUP MANAGEMENT PROTOCOL

Grundsätzlich fluten Switches das zugrundeliegende Netzwerk innerhalb einer Broadcast-Domäne mit Multicast-Verkehr, um sicherzustellen, dass alle Multicast-Streams in alle Bereiche des Netzwerkes übertragen werden. Der Multicast-Stream wird auch an Teilnehmer übertragen, die diesen eigentlich nicht empfangen wollen (sog. „flooding“). Dies hat zu Folge, dass sehr viel Bandbreite beansprucht wird und führt somit besonders beim Einsatz mehrerer Sender, wie z. B. Kameras, Panomera® usw., dazu, dass sowohl das Netzwerk als auch alle Geräte innerhalb des Netzes überlastet werden und eine geregelte Übertragung nicht mehr zustande kommen kann.

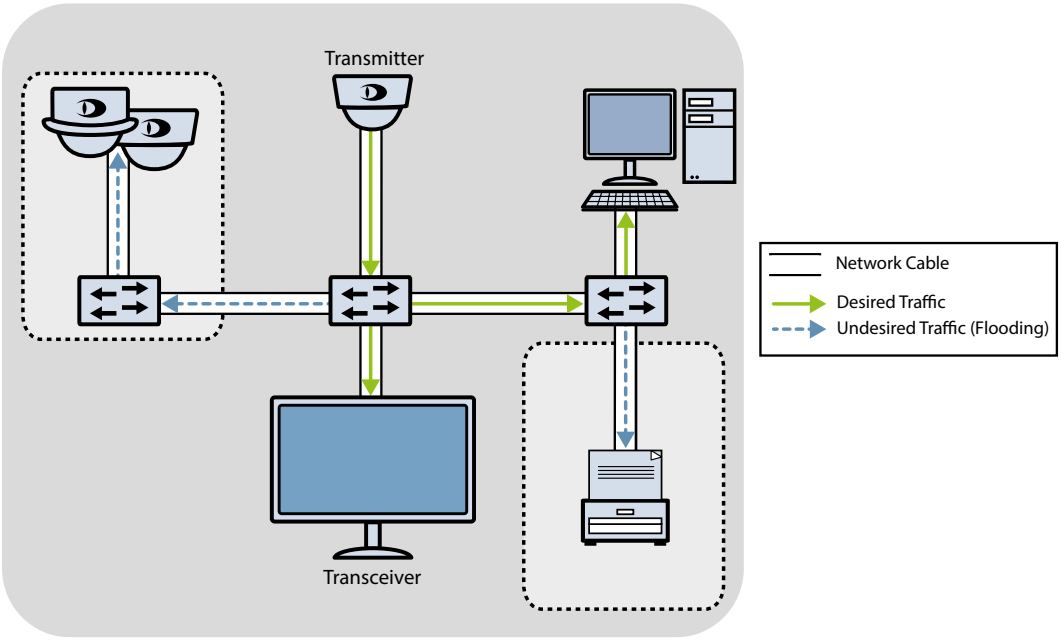

Abb. 2-8: Multicast-Verkehr mit IGMP

Mit dem Internet Group Management Protocol (IGMP) lässt sich der Multicast-Verkehr in einem Netzwerk beschränken, da es die Möglichkeit bietet, dynamisch Gruppen zu verwalten. Diese Verwaltung findet nicht beim sendenden Host (Kamera, Encoder) sondern im Switch an den der Empfänger eines Multicast-Streams angeschlossen ist statt. Die Empfänger betreten eine Multicast-Gruppe indem sie einen sog. „IGMP Join“-Befehl senden oder auf eine allgemeine Anfrage des IGMP-Queriers antworten.

2.13.1 IGMP Querier

Der IGMP-Querier ist ein administrativ festgelegter „Hauptswitch“ zu dem alle Multicast-Streams gesendet werden. Er ist der Empfänger aller IGMP Befehle und verwaltet somit die Multicast-Gruppen. Es kann immer nur ein Querier pro Netz (Broadcast-Domäne) definiert werden. Des Weiteren ist zu beachten, dass alle Multicast-Streams, auch nicht aufgeschaltete, immer zu diesem Querier gesendet werden.

Es ist nicht möglich den Multicast-Verkehr zum Querier zu limitieren. Aus diesem Grund sollte der IGMP-Querier möglichst zentral und in der Nähe der Multicast-Quellen (Panomera®, Kameras, Encoder) positioniert werden. Zudem ist zu beachten, dass genügend Bandbreite auf dem Weg zum Querier zur Verfügung steht.

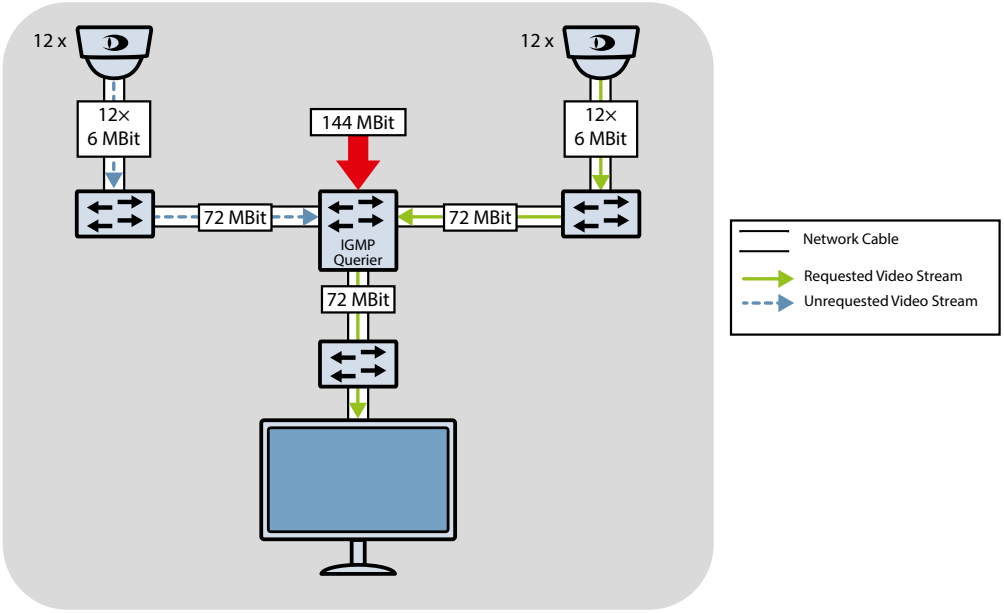

Abb. 2-9: Beispiel für IGMP-Querier

2.13.2 IGMP Snooping

IGMP-Snooping ermöglicht es einem Switch, der IGMP-Konversation zwischen dem Multicast-Sender und dem IGMP-Querier bzw. zwischen Multicast-Empfänger und dem IGMP-Querier zu „lauschen“. Anhand dieser Konversation legt jeder Switch auf dem IGMP-Snooping aktiviert ist eine Liste (Membership-List) für die Multicast-Gruppen an und leitet die Multicasts nur zu den Mitgliedern dieser Liste weiter.

Wenn nun ein Gerät abgesteckt oder auf einen anderen Port umgesteckt wird, würde der Switch Multicast-Daten an den falschen Port schicken. Um das zu vermeiden fordert der IGMP-Querier zyklisch alle Endgeräte auf, ihre Multicast-Gruppenzugehörigkeit bekanntzugeben. Die zurückkommenden Antworten auf solche Querier-Anfragen (IGMP Reports) veranlassen die Switches, ihre Membership-Listen entsprechend zu aktualisieren.

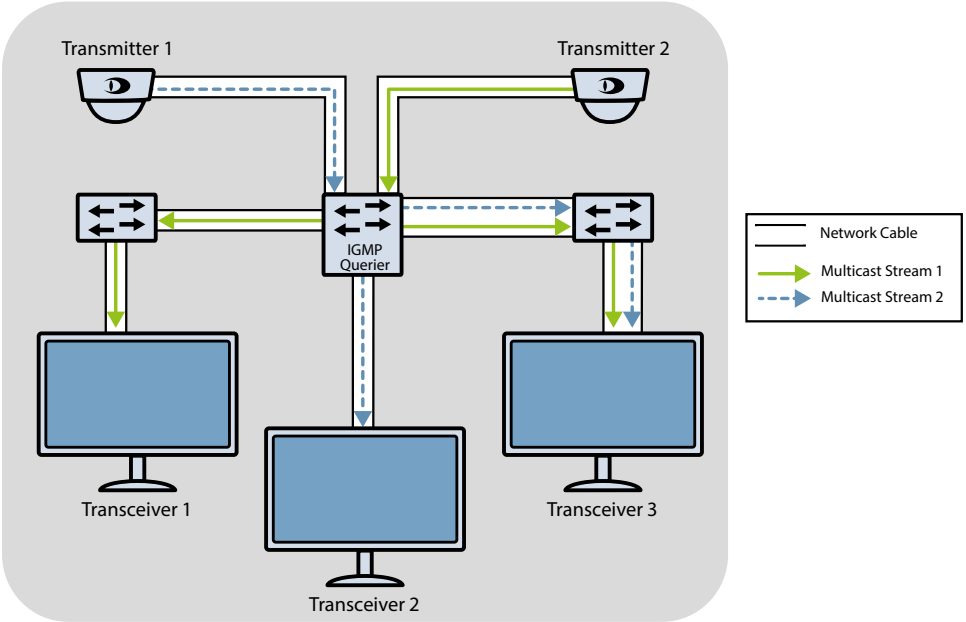

Abb. 2-10: Beispiel für IGMP-Snooping

2.14 PROTOCOL INDEPENDENT MULTICAST

Protocol Independent Multicast (PIM) ist eine Sammlung von Multicast-Routing-Protokollen, die unabhängig von den primären Routing-Protokollen wie RIP, OSPF usw. funktioniert. Es erstellt eine Multicast-Routing-Tabelle für die vorhandenen Multicast-Gruppen. PIM legt innerhalb der konfigurierten Domäne eine Baumstruktur mit Verzweigungen zu allen verbundenen Netzwerken an. An sich gab es zwei Varianten von PIM, von denen sich aber nur PIM-SM durchsetzen konnte.
Bei PIM-SM (Sparse Mode) wird ein zentraler Punkt angelegt, der als „Rendezvous Point“ (RP) bekannt ist, ähnlich dem IGMP-Querier in Layer 2. Andere Router senden einen „PIM Join“-Befehl an den RP, um am Multicast teilzunehmen.

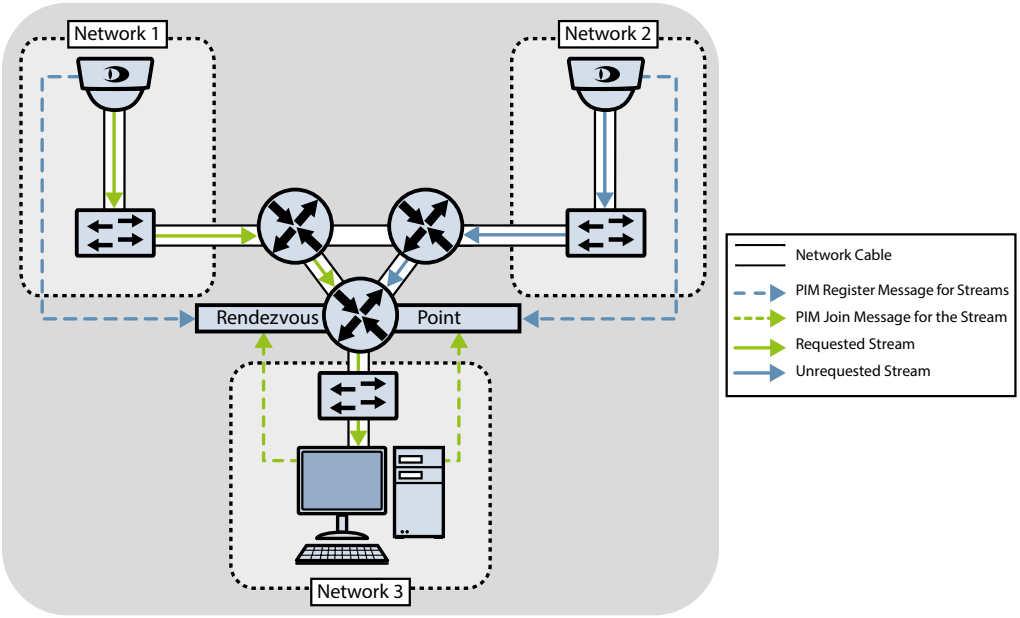

Abb. 2-11: Rendevous Point (RP) mit PIM-SM (Sparse Mode)

PIM(-SM) wird vor allem in großen Netzwerken mit vielen Multicast-Sendern empfohlen.

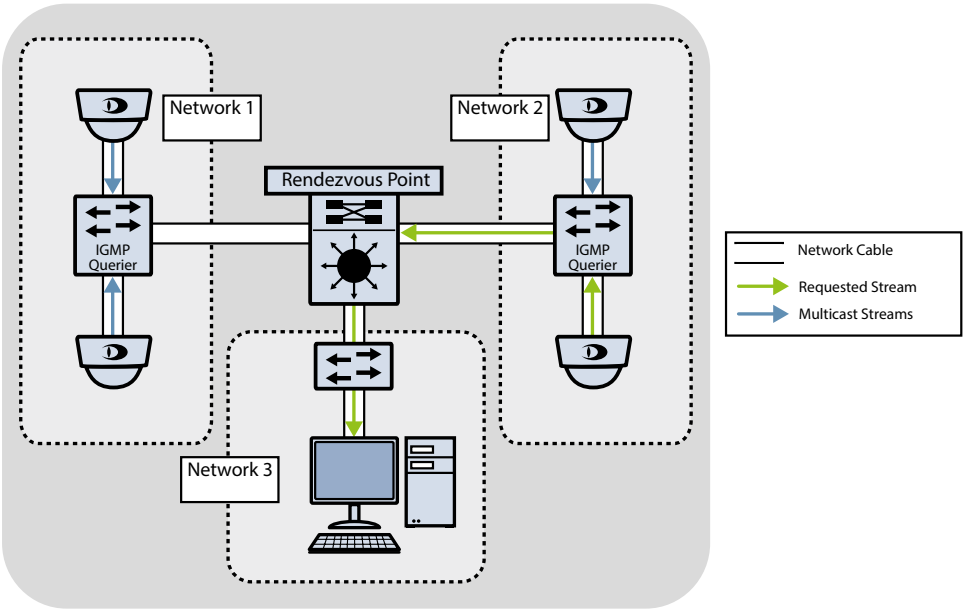

Abb. 2-12: Beispiel für PIM(-SM) in einem großen Netzwerk (viele Multicast-Sender)

BEISPIELE

3.1 UNICAST UND MULTICAST

Wenn gleichzeitig mehrere Decoder das Live-Bild eines Encoders anzeigen sollen, muss der Encoder in einem Unicast-Netzwerk den Video-Stream für jeden einzelnen Decoder über das Netzwerk senden. Die Auslastung des Netzwerkes und der Encoder steigt demzufolge erheblich an und kann zu Störungen wie Ruckeln oder Bildartefakten führen.

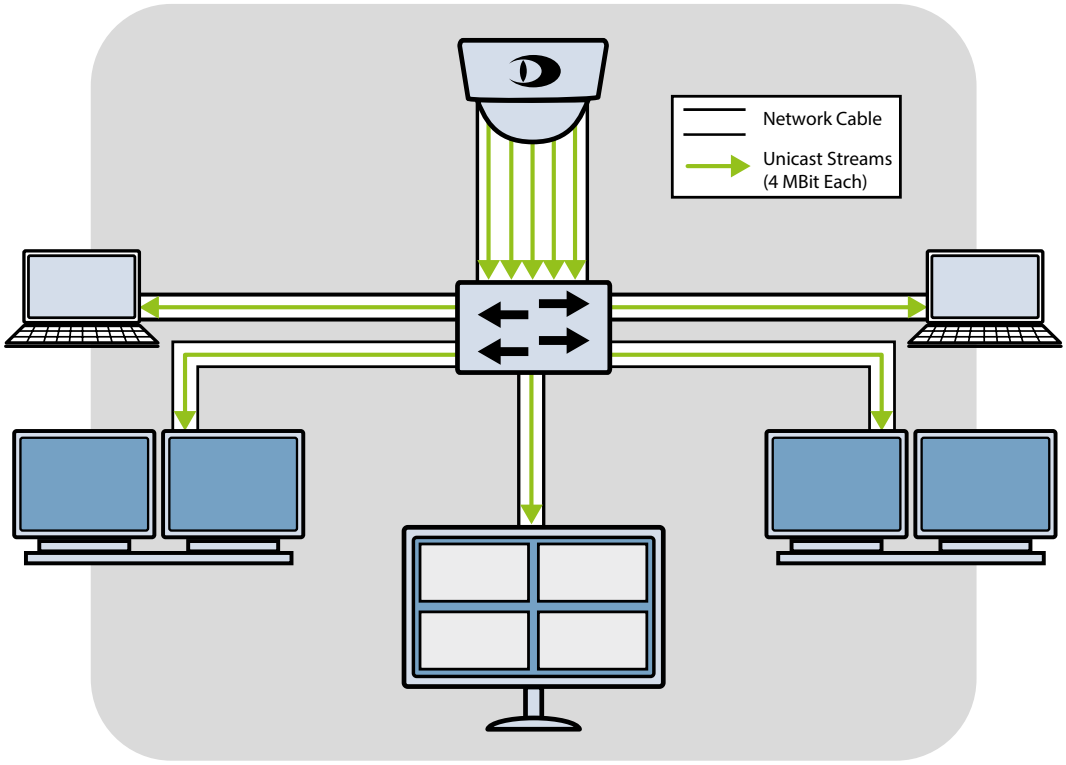

Abb. 3-1: Beispiel für ein Unicast-Netzwerk

In diesem Fall ist es sinnvoll, die Encoder auf Multicast-Betrieb einzustellen. Zudem müssen Switches verwendet werden, die Multicast unterstützen.

Bei Multicast-Betrieb wird die Auslastung des Netzwerkes und insbesondere der Encoder-Performance beachtlich gesenkt. Der Video-Stream wird nicht mehr einzeln an jeden Decoder gesendet, sondern nur noch einmal an eine Multicast-Gruppe. Die Weiterleitung an die einzelnen Decoder der Gruppe übernimmt der Multicast-fähige Switch.

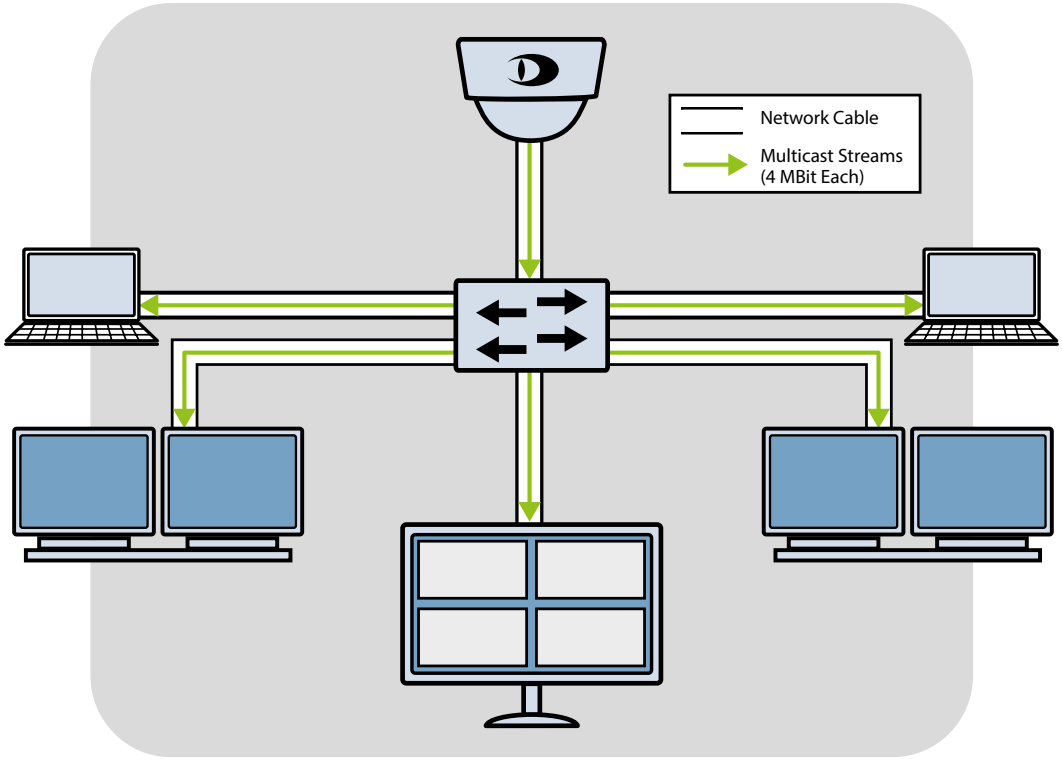

Abb. 3-2: Beispiel für das Video-Streaming an eine Multicast-Gruppe (IGMP V1)

Die Netzwerkauslastung ist aber auch in diesem Fall nicht optimal. Denn der Switch sendet den Video-Stream immer an alle Decoder der Multicast-Gruppe, ob der Decoder aktiv ist und das Live-Bild benötigt bzw. anzeigen will oder nicht.

Um die Netzwerkauslastung zu optimieren und damit eine störungsfreie Funktion des Systems sicherzustellen, wird empfohlen, immer einen Multicast-Switch zu verwenden der die Funktion IGMP V2 Snooping unterstützt. Diese Funktion beobachtet die Kommunikation zwischen dem Switch und dem Decoder einer Multicast-Gruppe. Damit kann eine Aussage darüber getroffen werden, welcher Decoder gerade aktiv ist und den Video-Stream tatsächlich benötigt.

IGMP V1 hat keine Möglichkeit der Abmeldung eines Multicast-Streams, IGMP V2 hingegen besitzt diese Fähigkeit.

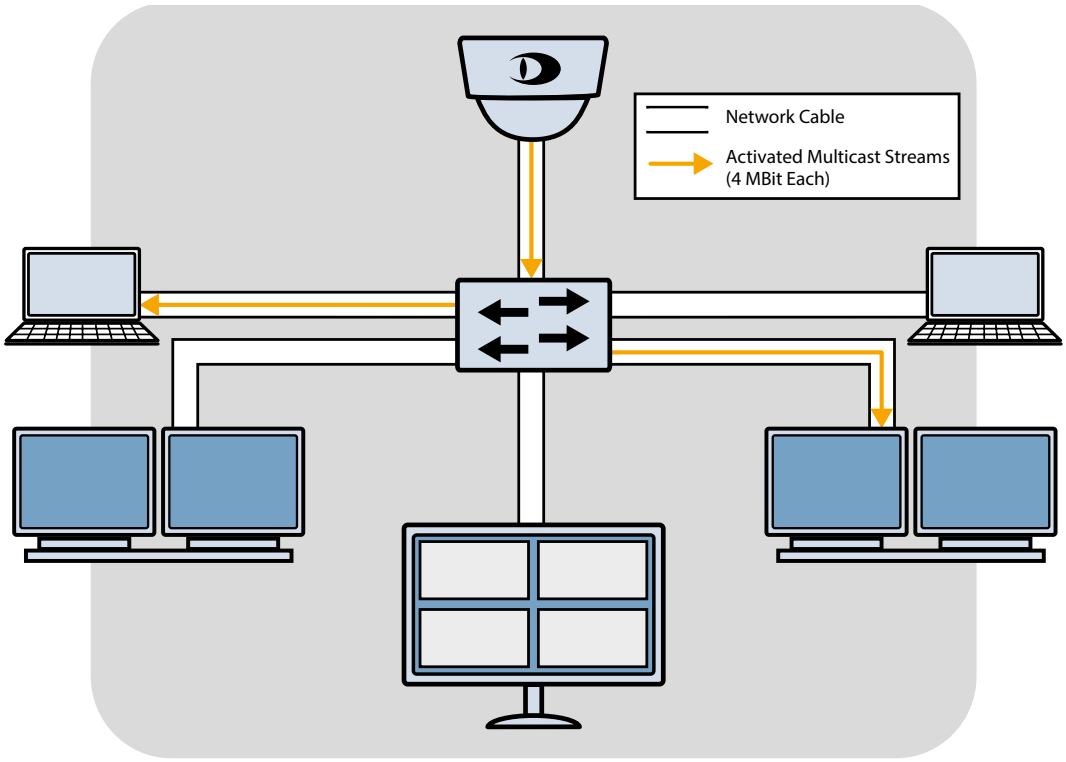

Abb. 3-3: Beispiel für das Video-Streaming mit einem Multicast-Switch (IGMP V2)

Im Ergebnis leitet der Switch den Video-Stream nicht mehr an alle, sondern nur noch an die relevanten Decoder weiter. Die Netzwerkauslastung sinkt noch einmal beachtlich und kann als optimiert betrachtet werden.

In den folgenden Beispielen gibt „Live“ oder „Live Multicast“ an, ob der Switch die Funktion IGMP V2 Snooping vollständig und korrekt unterstützt. Diese Funktion ist für alle eingesetzten Switches erforderlich, um vollständige Kompatibilität mit Dallmeier Netzwerksystemen zu gewährleisten.

3.2 EINFACHES VIDEONETZWERK

- Bis zu 24 Kameras mit je 4 MBit/s
- Ein Aufzeichnungsserver
- Zwei Viewing Clients mit je einem 2×2 Split
  (4× 4 MBit/s = 16 MBit/s ×2, Live direkt von der Kamera, Unicast)
- Ein Switch
  (24× 100 MBit/s + 4× 1 GBit/s)

Eine Videoanlage mit bis zu 24 Kameras kann mit nur einem Switch leicht realisiert werden. Die Kameras werden an den Access Ports des Switches mit einer Bandbreite von 100 MBit/s und mit PoE betrieben. Der Aufzeichnungsserver muss bei dieser Konstellation an einer 1 GBit/s Schnittstelle des Switches angeschlossen werden, da allein die Bandbreite der aufzuzeichnenden Kameras 96 MBit/s (24× 4 MBit/s) aufweist. Für die Betrachtung der Aufzeichnung und ggf. erforderliche Sicherungsläufe ist weiterer Bandbreitenbedarf zu berücksichtigen. Je nachdem wie die Viewing Clients ihr Live-Bild der Kameras anzeigen (VIProxy, direkt, Multicast, PRemote usw.) muss die hierfür benötigte Bandbreite bei der Planung des Netzwerks berücksichtigt werden. In diesem Beispiel, wird das Live-Bild direkt von der Kamera abgegriffen. Dies erfordert zwar eine zusätzliche Verbindung zur Kamera, schont aber die Schnittstelle des Servers (im Gegensatz zum Proxy-Betrieb).

Die Viewing Clients könnten demzufolge an einer 100 MBit/s Schnittstelle betrieben werden (16 MBit/s (4×4 MBit/s) je Client), allerdings sollte berücksichtigt werden, dass nicht nur Live betrachtet wird, sondern ggf. auch Backups und andere Funktionen am Client durchgeführt werden. Deshalb wird empfohlen, auch die Clients mit einer 1 GBit/s Leitung am Switch anzubinden. Falls weitere Zugriffe auf dieses Netzwerk erforderlich sind, kann dies mit dem verbleibenden 1 GBit/s Port umgesetzt werden.

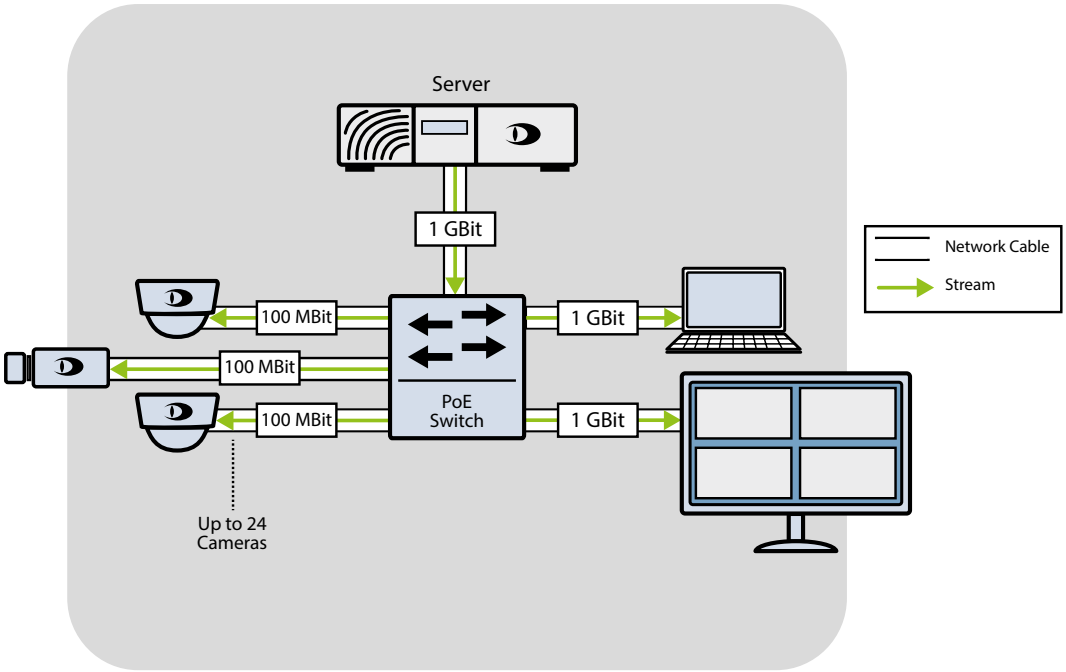

Abb. 3-4: Einfaches Netzwerk

Kameras, Aufzeichnungsserver und Switch bilden eine Einheit. Zusammen mit den Clients bilden sie ein Videonetzwerk.

3.3 MITTLERES VIDEONETZWERK

- Bis zu 48 Kameras
- Zwei Aufzeichnungsserver
- Vier Viewing Clients mit je einem 2×2 Split
  (4× 4 MBit/s = 16 MBit/s ×4, Live direkt von der Kamera, Unicast)
- Bis zu drei Switches
  (2× Access Switch mit 24× 100 MBit/s + 4× 1 GBit/s und ein Core Switch mit 8× 1 GBit/s)
- Optional ein weiterer redundanter Core Switch

Ein Videonetzwerk der mittleren Größe kann ähnlich wie im vorangegangen Beispiel umgesetzt werden. Die zusammengehörenden Kameras und Aufzeichnungsserver werden an einem Switch zusammengefasst, um nicht permanent die Verbindung unter den Switches zu belasten und eine ggf. notwendige Fehlersuche zu erleichtern (Kameras, Aufzeichnungsserver und Switch bilden eine Einheit). Je nach Anforderungen und örtlichen Gegebenheiten kann man sich zwischen zwei Netzwerkaufbauten entscheiden:

Die günstigere Variante ist die “Reihenschaltung“ der Switches, wobei die Switches über den Uplink (möglichst mit 1 GBit/s) in Reihe miteinander verbunden werden. Allerdings muss beachtet werden, dass so eine Struktur nicht unendlich ausbaufähig ist. Das Limit bildet der Uplink des Switches, der am stärksten belastet wird. Ebenfalls ist eine Reihenschaltung von Switches anfälliger für Ausfälle. Die Anbindung an ein externes Netzwerk erfolgt am Anfang oder am Ende der Reihenschaltung.

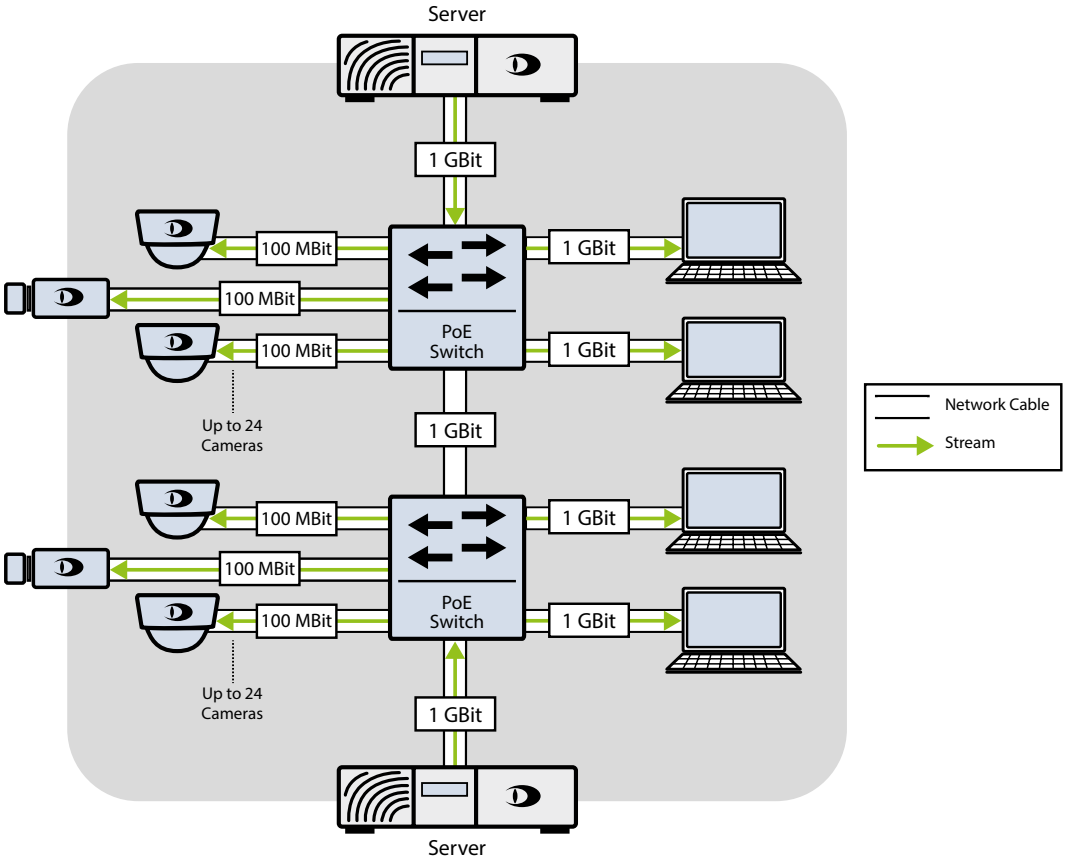

Abb. 3-5: Reihenschaltung von Switches (nur bis zu einer gewissen Größe sinnvoll)

Die andere Variante besteht darin, einen Stern mit den zu verbindenden Switches aufzubauen. Der Kern dieser Netzwerkstruktur wird durch einen Core Switch gebildet, der je nach Anforderung redundant ausgelegt werden kann. Der Core Switch ist ein besonders leistungsstarker Switch, der die Verbindung zwischen den Access Switches sowie anderen Netzen herstellt (mit 1GBit/s). Dies hat mehrere Vorteile: kurze Kommunikationswege (maximale Bandbreite), Ausbaufähigkeit, einfache Fehlersuche und geringe Anfälligkeit bei Switch Ausfällen.

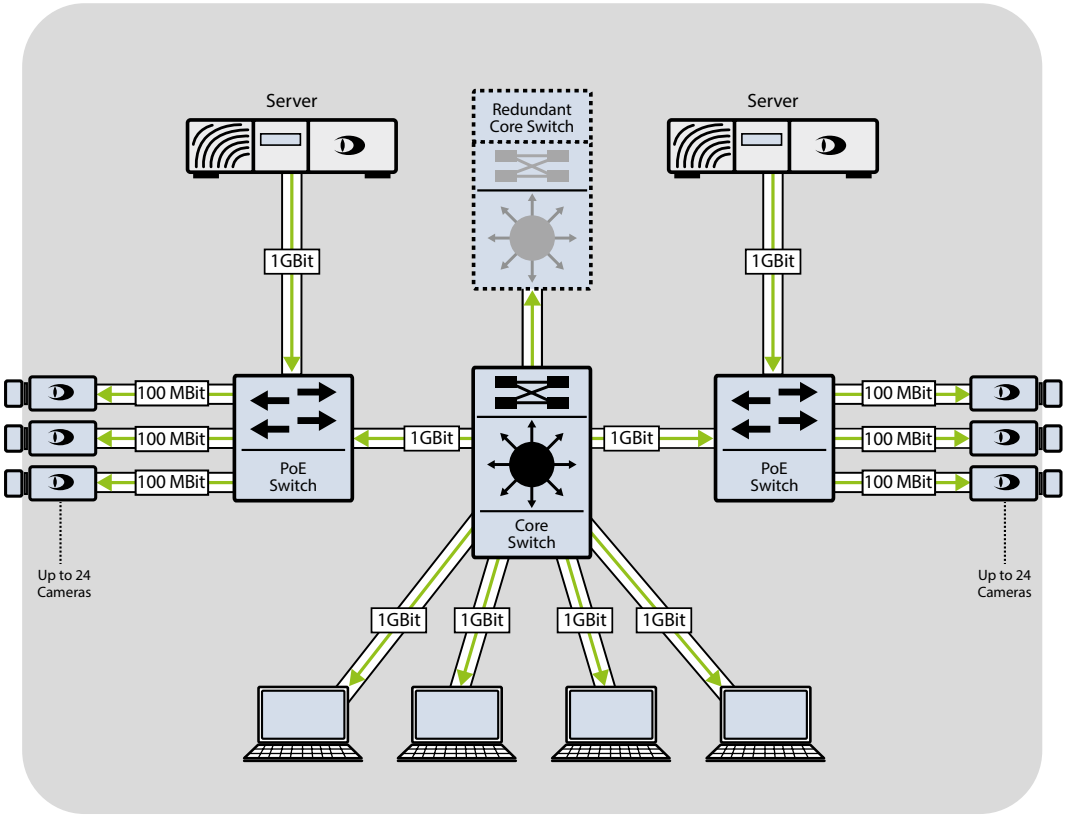

Abb. 3-6: Mittleres Netzwerk mit Core Switch (optional einem weiteren redundanten Core Switch)

3.4 GROSSES VIDEONETZWERK

- Mehr als 120 Kameras
- Mehr als fünf Aufzeichnungsserver
- Mehr als fünf Viewing Clients mit je einem 3×3 Split
  (9× 4 MBit/s = 36 MBit/s ×5, Live Multicast von den Kameras)
- Bis zu sechs Switches
  (5× Access Switch mit 24× 100 MBit/s + 2× 1 GBit/s und ein Core Switch mit 24× 1 GBit/s)
- Optional ein weiterer redundanter Core Switch

In einem Videonetzwerk dieser Größe ist eine sternförmige Infrastruktur unumgänglich. Die Übertragungswege wären ansonsten zu lang und die Bandbreite zu gering. Da in diesem Beispiel viele Viewing Clients arbeiten, ist Multicast nötig, um die Kameras nicht mit Unicast zu überlasten (Overload). Beim Einsatz von Multicast (Liveübertragung) muss darauf geachtet werden, dass alle Netzwerkkomponenten Multicast-tauglich sind (IGMP V2 Snooping).

Wie im vorangegangenen Beispiel werden alle Access Switches, Viewing Clients und externe Netzwerke am Core Switch mit je 1 GBit/s zusammengefasst. Damit beim Ausfall des Core Switches (Single Point of Failure) nicht alle Clients "blind" sind, kann dieser redundant ausgeführt werden und im Notfall einspringen. Dadurch wird die Aufzeichnung nicht durch den Verlust des Core Switches gefährdet, jeder Server ist weiterhin mit seinen Kameras am eigenen Switch verbunden und ist unabhängig vom restlichen Netzwerk.

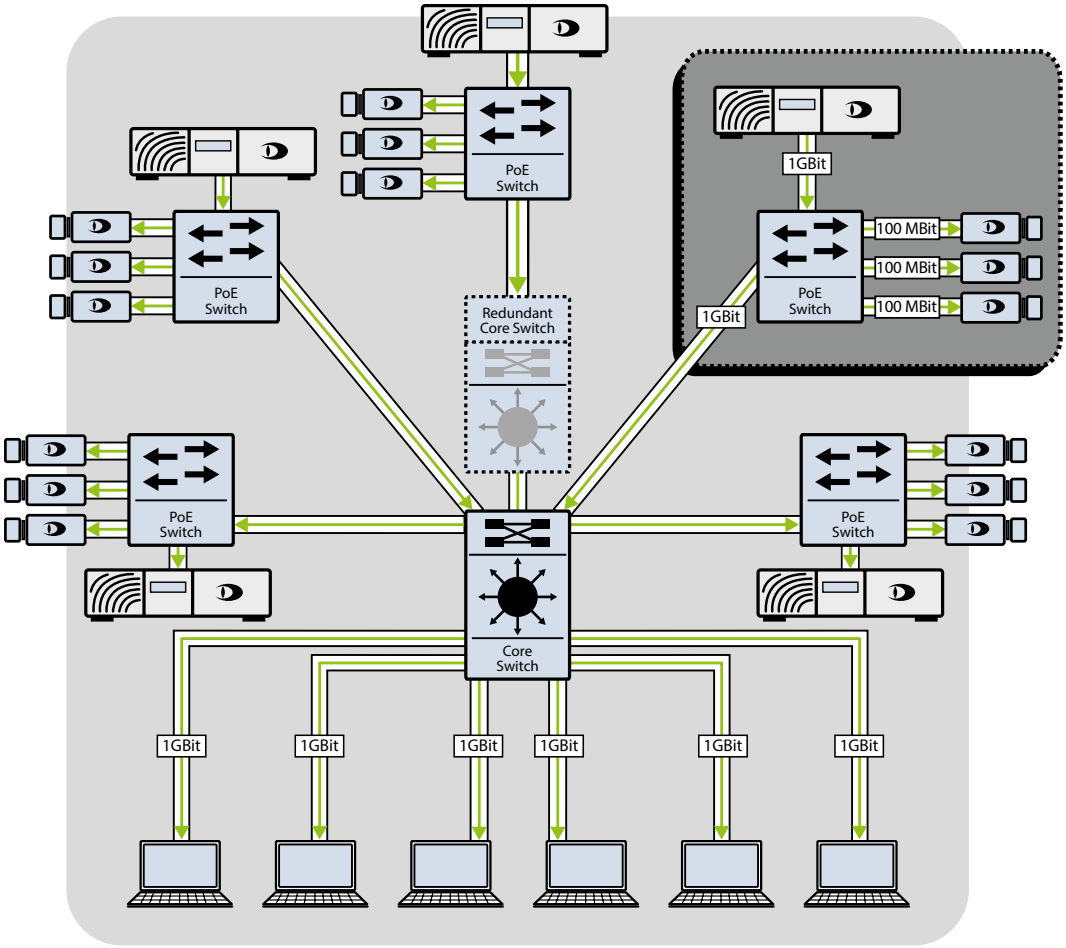

Abb. 3-7: „Großes" Videonetzwerk (mit sternförmigem Aufbau)

WICHTIGE HINWEISE

- Achten Sie darauf, das Videonetzwerk möglichst autark zu betreiben, da die Funktion der restlichen Netzwerkstruktur eventuell durch Lastspitzen oder generell durch Erreichen des Leistungslimits beeinflusst wird (Kommunikation mit Servern, Druckern usw. schlägt fehl).
- Verwenden Sie nach Möglichkeit Produkte nur eines Herstellers, um Inkompatibilität zu vermeiden.
- Ein Potentialausgleich der einzelnen Komponenten sollte durchgehend gewährleistet sein (siehe auch Whitepaper „Strukturierte Verkabelung, Erdung & Potentialausgleich“).
- Bei der Auswahl eines PoE-Switches sind die unterschiedlichen Leistungsklassen (PoE/PoE+) der Dallmeier Kameras zu berücksichtigen (siehe Datenblätter).
- Stellen Sie sicher, dass eine ausreichende PoE-Gesamtleistung vorhanden ist.
- Wählen Sie einen Switch, der sequenzielles Einschalten der PoE-Ports beherrscht.
- Der erhöhte Leistungsbedarf während der Dunkelheit bei Kameras mit integrierten IR-Strahlern ist zu berücksichtigen (siehe Datenblatt).
- Ein Switch ist das Kernstück einer digitalen Videoanlage und der Single Point of Failure (auf Qualität achten und eventuell Redundanzen schaffen).
- Eine korrekte Kupfer-Verkabelung (CAT-5E oder besser) mit maximal 100 m pro Kabelsegment ist Voraussetzung (ebenfalls die Maximallängen für Glasfaser beachten).
- Die Konfiguration eines managebaren Switches erfordert Spezialwissen; ziehen Sie ggf. einen Experten hinzu.
- Nehmen Sie sich Zeit für eine vorausschauende Struktur- und Bandbreitenplanung.
- Für (Standard-) Kameras ist ein 100 MBit/s-Port ausreichend.
- Aufzeichnungsserver sollten an einen 1 GBit/s-Port angeschlossen werden.
- Uplinks sollten eine höhere Bandbreite zur Verfügung stellen (mindestens 1 GBit/s).

[D I E S E S E I T E W U R D E A B S I C H T L I C H L E E R G E L A S S E N]

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