

NETZWERKANFORDERUNGEN KVM-OVER-IP™

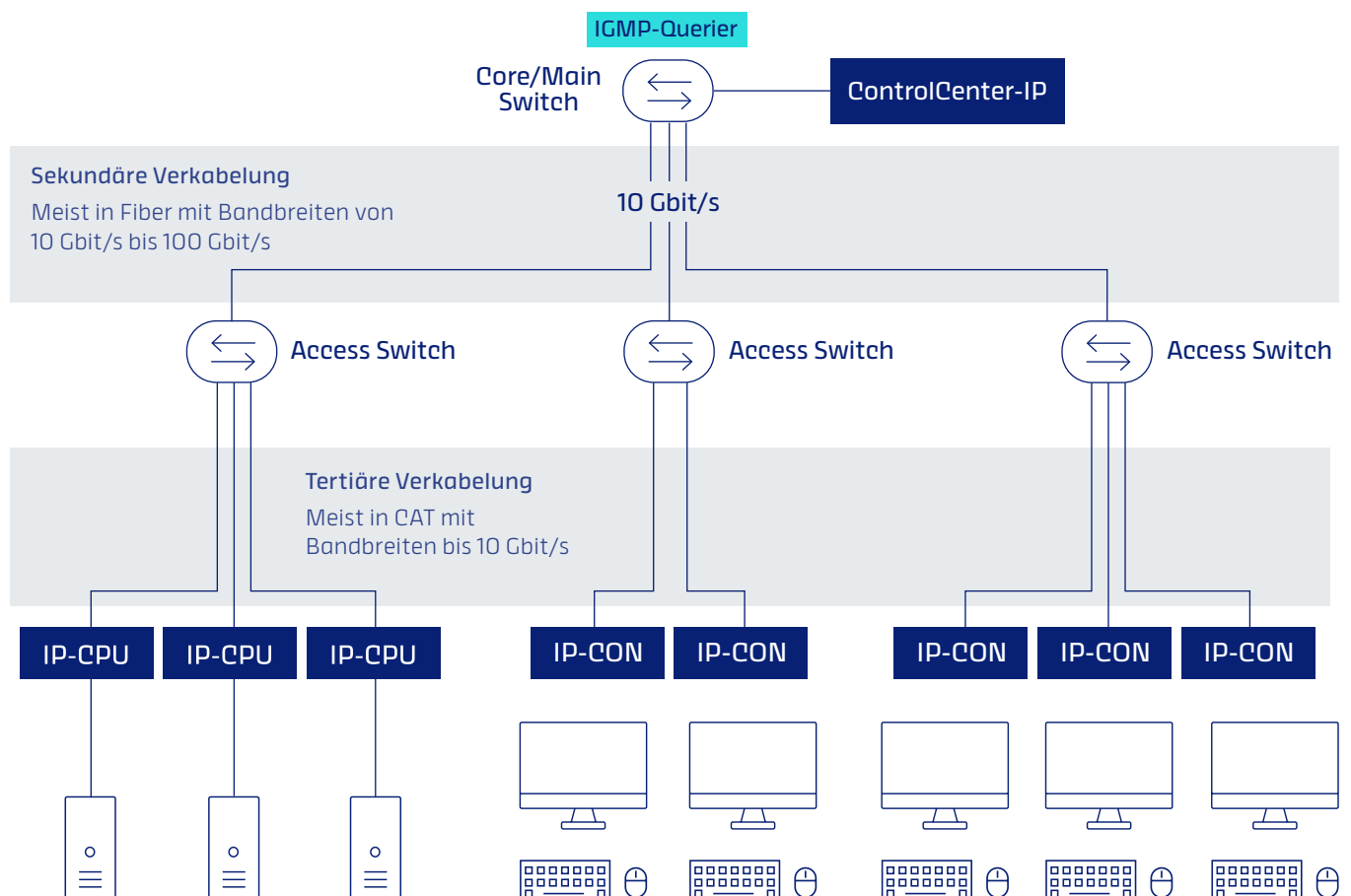
Mit KVM-over-IP™-Lösungen überwinden Sie die Grenzen dedizierter Signalübertragung. Die Systeme werden dadurch flexibler, skalierbarer und ermöglichen den parallelen Zugriff mehrerer Nutzer – über dieselbe IP-Infrastruktur. G&D setzt auf Multi-Gbit-Technologie und nutzt Standard-IP-Netzwerke als Basis. Systemerweiterungen lassen sich einfach durch handelsübliche Komponenten realisieren. Die Konfiguration ist intuitiv, viele Geräte sind nahezu plug-and-play-fähig. Für eine optimale Performance sollten jedoch bestimmte Aspekte der Netzwerktopologie berücksichtigt werden: Besonders wichtig ist die ausreichende Dimensionierung des Uplinks zwischen Access- und Core-/Main-Switch – abgestimmt auf Anzahl und Betriebsmodus der angeschlossenen Endgeräte.

Typische Bandbreitenanforderungen bei KVM-over-IP™

VisionXS-IP-Modelle gibt es in mehreren Varianten: DVI-I, DP-HR und DP-HR-DH mit 1 Gbit; DP-UHR und TypeC-UHR mit Multi-Gbit (1–10 Gbit). Die Bandbreite ist standardmäßig unbegrenzt, kann aber optional begrenzt werden.

- **1920 × 1080: 300–400 Mbit/s**
(Office-Anwendung bei ca. 40 % Änderung; z. B. VisionXS-IP-DVI-I)
- **2560 × 1440: 500–600 Mbit/s**
(Office-Anwendung bei ca. 40 % Änderung; z. B. VisionXS-IP-DP-HR)
- **2x 2560 × 1440: 800–900 Mbit/s**
(Office-Anwendung bei ca. 40 % Änderung; z. B. VisionXS-IP-DP-HR-DH)
- **3840 × 2160: 2000–2500 Mbit/s**
(Office-Anwendung bei ca. 40 % Änderung, z. B. VisionXS-IP-DP-UHR) – die maximale Videobandbreitennutzung beträgt 5 Gbit/s
- **Standbild: 25 Mbit/s bei 3840 × 2160**

Grundlagen



Stellen Sie sicher, dass der Uplink vom Access- zum Core-/Main-Switch der Anzahl und dem Betriebsmodus der verbundenen Endgeräte gerecht wird.

Beispiel: 30 × VisionXS-IP-DP-HR-CPU bei 10 Gbit Uplink
⇒ Uplink mit 10 Gbit/s ist ein Nadelöhr, da 30 × 1 Gbit/s bei den CPUs sichergestellt werden müssten.

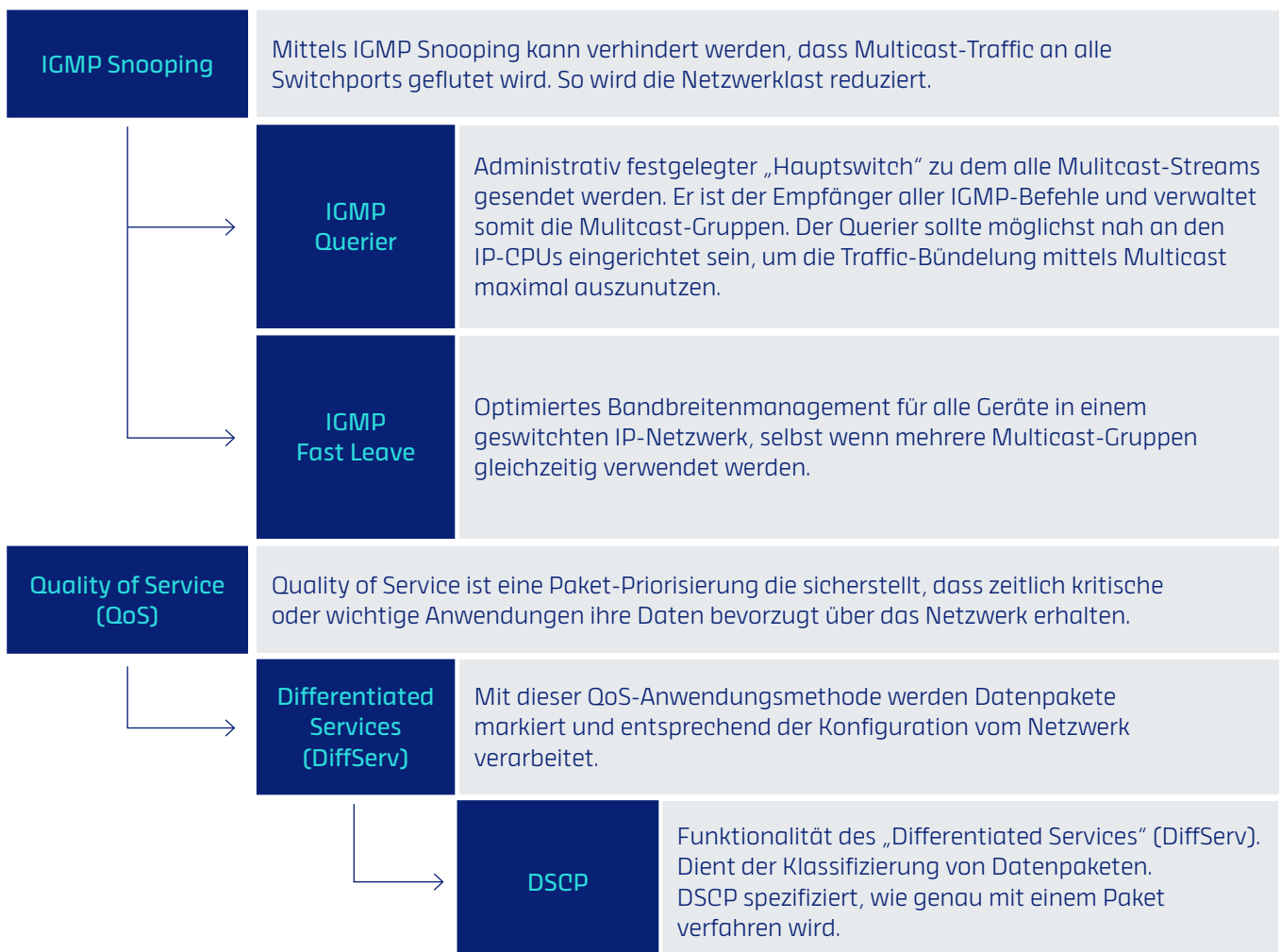
Voraussetzungen der Netzwerk-Switches

- Mindestens Layer-2-Managed-Switch
- VLAN-Unterstützung, um den KVM-over-IP™-Datenverkehr von anderen Netzwerkoperationen zu trennen
- QoS mit DiffServ-/DSCP-Unterstützung zur Performance-Steigerung und Priorisierung:
Quality-of-Service (QoS) ist eine Paketpriorisierung, die sicherstellt, dass zeitlich kritische oder wichtige Anwendungen ihre Daten bevorzugt über das Netzwerk erhalten.
Dank DiffServ-/DSCP-Unterstützung werden Datenpakete markiert und entsprechend der Konfiguration vom Netzwerk verarbeitet. DSCP spezifiziert, wie genau mit einem Paket verfahren wird.
- IGMP- und Multicast-Unterstützung bei Matrix-Anwendungen. Über IGMP teilen die Arbeitsplatzmodule dem Netzwerkswitch mit, welcher Multicast-Gruppe sie beitreten oder welche sie verlassen möchten.
- IGMP-Snooping-Unterstützung zur Reduktion der Netzwerklast. IGMP Snooping verhindert, dass Multicast-Datenverkehr an alle Netzwerk-Switchports geflutet wird, sondern nur dort anfällt, wo er gebraucht wird.

- Möglichkeit zur Einrichtung eines IGMP-Snooping-Querier: Administrativ festgelegter „Hauptswitch“, zu dem alle Multicast-Streams gesendet werden. Er ist der Empfänger aller IGMP-Befehle und verwaltet somit alle Multicast-Gruppen.
- Ausreichende Performance des Netzwerkswitches sicherstellen: Forwarding-Bandbreite, Switching-Kapazität und Forwarding-Performance überprüfen.
- Engpässe bei der Nutzung mehrerer Netzwerkswitches vermeiden: Werden Endgeräte über mehrere Switches verteilt, kann die Verbindung zwischen diesen zum Flaschenhals werden. Planen Sie die Netzwerk-Topologie entsprechend.

Empfohlene Einstellungen der Netzwerk-Switches

- IGMP Fast Leave aktivieren, um beim Wechsel zwischen Multicast-Gruppen (Switching-Vorgängen) ein optimiertes Bandbreitenmanagement zu gewährleisten und Bildstörungen zu vermeiden.
- Spanning Tree TCN Flooding an den Netzwerkports, an denen die Matrix angeschlossen ist, deaktivieren, um ein optimiertes Bandbreitenmanagement zu gewährleisten und Bildstörungen zu vermeiden.



Genutzte IP-Technik bei G&D

- 1-10 Gbit-Technologie zur Übertragung
- KVM-over-IP™-Extender: Unicast (1 zu 1)
- KVM-over-IP™-Matrixsystem: Multicast (m zu n), im Bedarfsfall ist auch Unicast (1 zu 1) mit Einschränkungen möglich
- G&D Device Finder: Manuell initiiertes Broadcast im Subnetz des angeschlossenen ControlCenter-IP(-XS)
- Maximale Ethernet Paketlänge: 1518 Byte (gemäß Norm IEEE 802.3)
- Jumbo-Frames (bis 9.000 Byte) werden nicht benötigt

Sicherheit bei KVM-over-IP™

- Algorithmus: AES256-GCM (K/M- und Steuerdaten) und AES128-CTR (Hochgeschwindigkeitsdaten; Video, Audio, GenericUSB und RS232)
- Schlüsselaustausch für die sehr sicherheitsrelevanten Tastatur- und Mausdaten sowie die Steuerdaten erfolgt voll dynamisch alle 40 bis 80 Minuten
- Der Schlüsselaustausch für Hochgeschwindigkeitsdaten erfolgt voll dynamisch alle drei bis fünf Stunden oder bei Umschaltereignissen
- Verschlüsselung nicht deaktivierbar!
- Möglichkeit zur Verwendung zusätzlicher Benutzerzertifikate zur Geräteauthentifizierung
- Der Einsatz des optionalen UID-Locking schränkt die nutzbaren Endgeräte zuverlässig ein, sodass nach Aktivierung keine weiteren Endgeräte hinzugefügt oder ausgetauscht werden können
- Trusted Platform Module
- Zwei-Faktor-Authentifizierung (2FA): Kombiniert die klassische Passwortauthentifizierung mit einem zeitbasierten Einmalcode für eine zusätzliche Schutzebene vor unbefugtem Zugriff

Allgemeines zum KVM-over-IP™-Matrixsystem

- Der ControlCenter-IP(-XS) übernimmt die Vermittlungslogik im Netzwerk, optimiert die Erreichbarkeit aller Geräte untereinander und ermöglicht die Umschaltung auf die verbundenen Rechnermodule
- K/M- und Steuerdaten werden über den Matrixswitch geroutet, um eine reaktionsschnelle Systemsteuerung zu ermöglichen und Features wie CrossDisplay-Switching bereitzustellen
- Hochgeschwindigkeitsdaten werden direkt zu den Endgeräten geroutet
- bluedec™ – G&Ds hochentwickelte mehrstufige verlustfreie Kompression sorgt für beste Videoqualität und praktisch latenzfreie, pixelperfekte Übertragung
- Anwender können zwischen verschiedenen Quellen nahezu in Echtzeit umschalten (unter 500 ms)
- Endgeräte (Rechnermodule, RemoteAccess-IP-CPUs und Arbeitsplatzmodule) speichern keine sicherheitsrelevanten Informationen wie z.B. Anmeldedaten, die bei einem möglichen Verlust der Geräte ausgelesen werden könnten
- Verarbeitung aller gängigen Videosignale, durch eine vielfältige Auswahl an matrixkompatiblen KVM-over-IP™-Extendern, die im Matrixbetrieb als Endgeräte „gemischt“ eingebunden werden können (Mix & Match)
- Umfassendes Rechtemanagement und eine Benutzerverwaltung, mit denen sich genau steuern lässt, welcher Benutzer auf welche Ressourcen zugreifen kann
- Einfache Inbetriebnahme neuer Endgeräte durch integrierten Device-Finder, wodurch keine manuelle Eingabe der IP-Adressen notwendig ist
- Frühzeitige Erkennung von Sicherheitsvorfällen oder ungewöhnlichen Aktivitäten durch kontinuierliche Überwachung via Syslog, Monitoring und SNMP

Verwendete Netzwerk-Ports und Protokolle

Port	Service	Typ	Beschreibung	Kommentar
–	IGMP	IGMP	IGMP Multicast	nicht veränderbar
–	L2 Multicast		01:0F:F4.. Device Finder	nicht veränderbar
–	IPsec	ESP	IPSec Encapsulating Security Payload	nicht veränderbar
–	IPsec	AH	IPSec Authentication Header	nicht veränderbar
22	SSH	TCP	optional Kommunikation RemoteAccess-IP-CPU und RemoteTargets	veränderbar
49	TACACS+	UDP/TCP	optional Kommunikation Authentifizierungsservice	nicht veränderbar
67	DHCP	UDP	DCHP-Server	nicht veränderbar
68	DHCP	UDP	DHCP-Client	nicht veränderbar
80	http	TCP	zum Öffnen der Webapplikation (Weiterleitung auf https)	deaktivierbar, falls Weiterleitung nicht benötigt bzw. gewünscht wird
123	NTP	UDP	für Zeitsynchronisation	nicht veränderbar
161	SNMP	UDP	optional SNMP agent	veränderbar
162	SNMP-Traps	UDP/TCP	optional SNMP agent	veränderbar
389	LDAP	UDP/TCP	optional Kommunikation Authentifizierungsservice	nicht veränderbar
443	https	SSL/TCP	zum Öffnen der Webapplikation	nicht veränderbar
445	CIFS	TCP	für Auto-Backup-Funktion	veränderbar
514	Syslog	UDP/TCP	optional Syslog server 1/Syslog server 2	veränderbar
636	Active Directory	UDP/TCP	optional Kommunikation Authentifizierungsservice	nicht veränderbar
1812	Radius	UDP/TCP	optional Kommunikation Authentifizierungsservice	nicht veränderbar
2049	NFS	UDP/TCP	für Auto-Backup-Funktion	veränderbar
3389	RDP	TCP	optional Kommunikation RemoteAccess-IP-CPU und RemoteTargets	veränderbar
5900	VNC	TCP	optional Kommunikation RemoteAccess-IP-CPU	veränderbar
6137	U2-LAN	UDP	optional Kommunikation U2-LAN	nicht veränderbar
18244	KVM-over-IP	UDP	KVM-over-IP: Data-Port (Video, nur für Endgeräte-Kommunikation)	veränderbar
18245	KVM-over-IP	UDP	KVM-over-IP: Communication Port (K, M, misc)	veränderbar
18246	KVM-over-IP	UDP	KVM-over-IP: Control Port und IPSec Internet Key Exchange (IKE)	veränderbar
27994	Remote-Port	TCP	optional Remote control access, z. B. IP Control API	veränderbar
27996	Database communication	TCP	interne Kommunikation, z. B. MatrixGuard	veränderbar
37996	Database communication	TCP	interne Kommunikation	nicht veränderbar