NETWORK REQUIREMENTS KVM-OVER-IP™

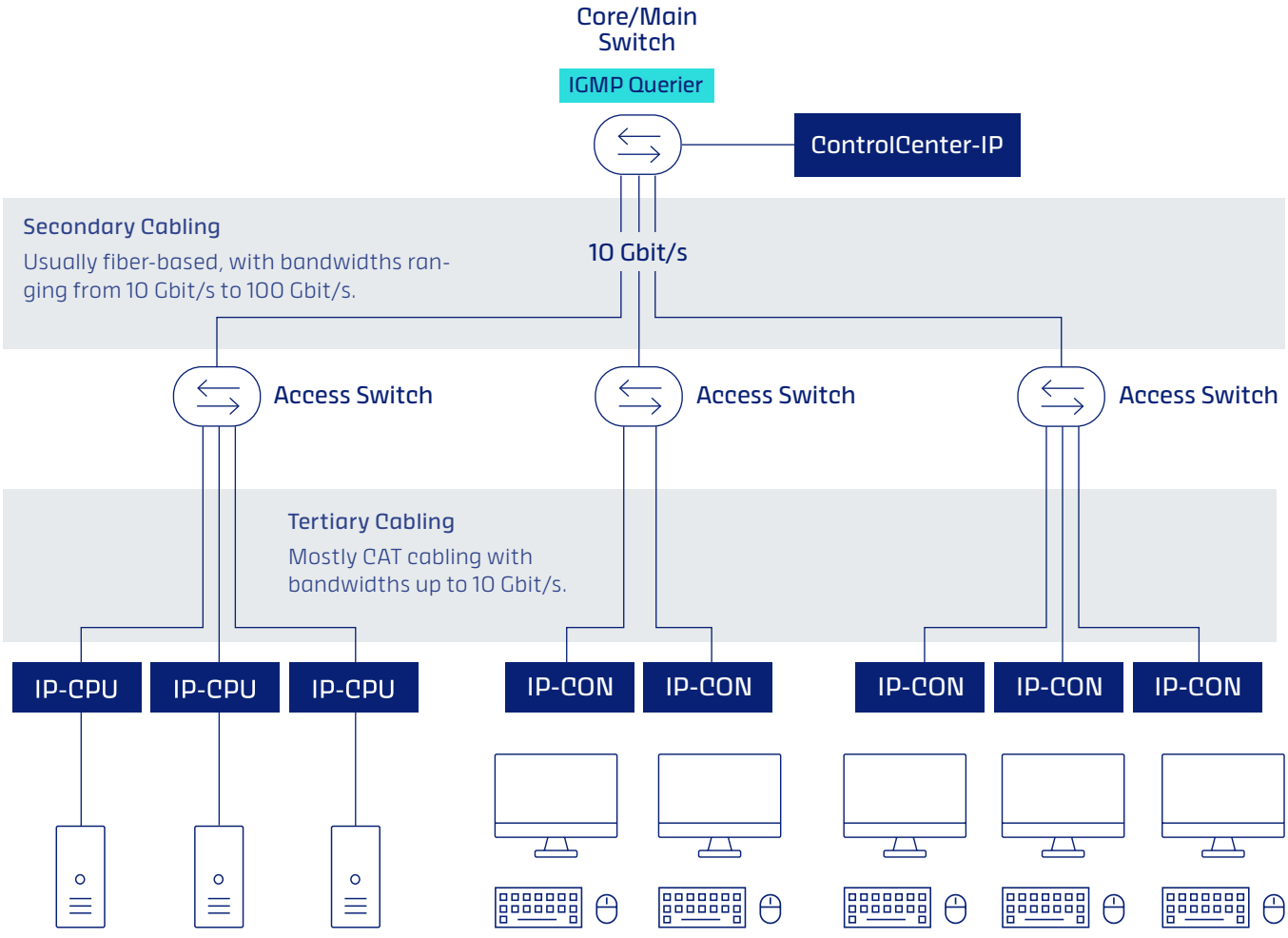
With KVM-over-IP™ solutions, you overcome the limitations of dedicated signal transmission. The systems thus become more flexible and scalable and enable parallel access for multiple users - via the same IP infrastructure. G&D uses multi-Gbit technology and standard IP networks as a basis. System extensions can be easily implemented using commercially available components. The configuration is intuitive, many devices are virtually plug-and-play capable. However, for optimal performance, certain aspects of the network topology should be taken into account: Particularly important is the adequate sizing of the uplink between the access and core/main switch - tailored to the number and operating mode of the connected end devices.

Typical bandwidth requirements for KVM-over-IP™

VisionXS-IP models are available in several variants: DVI-I, DP-HR and DP-HR-DH with 1 Gbit; DP-UHR and TypeC-UHR with multi-Gbit (1-10 Gbit). The bandwidth is unlimited by default but can optionally be restricted.

- **1920 × 1080: 300–400 Mbit/s**
  (Office application with approx. 40% change; e.g., VisionXS-IP-DVI-I)
- **2560 × 1440: 500–600 Mbit/s**
  (Office application with approx. 40% change; e.g., VisionXS-IP-DP-HR)
- **2x 2560 × 1440: 800–900 Mbit/s**
  (Office application with approx. 40% change; e.g., VisionXS-IP-DP-HR-DH)
- **3840 × 2160: 2000–2500 Mbit/s**
  (Office application with approx. 40% change; e.g., VisionXS-IP-DP-UHR) – the maximum video bandwidth usage is 5 Gbit/s
- **Static image: 25 Mbit/s at 3840 × 2160**

Basics



Ensure that the uplink from the access switch to the core/main switch meets the number and operating mode of the connected end devices.

Example: 30 × VisionXS-IP-DP-HR-CPU with a 10 Gbit uplink ⇨ the 10 Gbit/s uplink becomes a bottleneck, as 30 × 1 Gbit/s from the CPUs would need to be supported.

Requirements for network switches

- At least Layer 2 managed switch
- VLAN support to separate KVM-over-IP™ traffic from other network operations.
- QoS with DiffServ/DSCP support for performance enhancement and prioritization:
  Quality of Service (QoS) is a packet prioritization mechanism that ensures time-critical or important applications receive their data preferentially over the network.
  With DiffServ / DSCP support, data packets are marked and processed by the network according to the configuration. DSCP specifies how exactly a packet is handled.
- IGMP and multicast support for matrix applications. The console modules use IGMP to communicate to the network switch which multicast group they want to join or leave.
- IGMP snooping support to reduce the network load.
  IGMP snooping prevents multicast traffic from being flooded to all network switch ports, restricting it only to where it is needed.
- Option to set up an IGMP snooping querier: Administratively defined "main switch" to which all multicast streams are sent. It is the recipient of all IGMP commands and therefore manages all multicast groups.
- Ensure adequate performance of the network switch: check forwarding bandwidth, switching capacity, and forwarding performance.
- Avoid bottlenecks when using multiple network switches: If end devices are distributed across several switches, the connections between them can become a bottleneck. Plan the network topology accordingly.

Recommended settings for the network switches

- Activate IGMP Fast Leave to ensure optimized bandwidth management when switching between multicast groups (switching processes) and to avoid image interference.
- Deactivate Spanning Tree TCN Flooding on the network ports to which the matrix is connected in order to ensure optimized bandwidth management and avoid image interference.

IGMP Snooping	IGMP snooping can prevent multicast traffic from being flooded to all switch ports, thereby reducing network load.
→ IGMP Querier	Administratively defined "main switch" to which all multicast streams are sent. It is the recipient of all IGMP commands and therefore manages the multicast groups. The querier should be set up as close as possible to the IP CPUs to maximize traffic aggregation via multicast.
→ IGMP Fast Leave	Optimized bandwidth management for all devices in a switched IP network, even if several multicast groups are used simultaneously.
Quality of Service (QoS)	Quality of Service is packet prioritization that ensures that time-critical or important applications receive their data preferentially via the network.
→ Differentiated Services (DiffServ)	With this QoS application method, data packets are marked and processed by the network according to the configuration.
→ DSCP	Functionality of the "Differentiated Services" (DiffServ). Used to classify data packets. DSCP specifies how exactly a packet is handled.

IP technology used at G&D

- 1-10 Gbit technology for transmission
- KVM-over-IP™ extender: unicast (1 to 1)
- KVM-over-IP™ matrix system: multicast (m to n), if required, unicast (1 to 1) is also possible with restrictions
- G&D Device Finder: manually initiated broadcast in the subnet of the connected ControlCenter-IP(-XS)
- Maximum Ethernet packet length: 1518 byte (according to IEEE 802.3 standard)
- Jumbo Frames (up to 9,000 bytes) are not required

Security for KVM-over-IP™

- Algorithm: AES256-GCM (K/M and control data) and AES128-CTR (high-speed data; video, audio, GenericUSB and RS232)
- Key exchange for the highly security-relevant keyboard, mouse, and control data occurs fully dynamically every 40 to 80 minutes.
- The key exchange for high-speed data occurs fully dynamically every three to five hours or during switching events.
- Encryption cannot be deactivated!
- Possibility to use additional user certificates for device authentication.
- The use of the optional UID locking reliably restricts the usable end devices, so that after activation no additional devices can be added or exchanged.
- Trusted Platform Module
- Two-factor authentication (2FA): Combines traditional password authentication with a time-based one-time code to provide an additional layer of protection against unauthorized access.

General information on the KVM-over-IP™ matrix system

- The ControlCenter-IP(-XS) takes over the switching logic in the network, optimizes the accessibility of all devices to each other and enables switching to the connected computer modules
- K/M and control data are routed through the matrix switch to enable responsive system control and provide features such as CrossDisplay-Switching.
- High-speed data is routed directly to the end devices
- bluedec™ - G&D's advanced multi-stage lossless compression ensures the best video quality and virtually latency-free, pixel-perfect transmission.
- Users can switch between different sources virtually in real time (less than 500 ms)
- End devices (computer modules, RemoteAccess-IP CPUs, and console modules) do not store any security-relevant information, such as login credentials, that could be accessed in case the devices are lost.
- Processing of all common video signals through a wide range of matrix-compatible KVM-over-IP™ extenders, which can be integrated as "mixed" end devices in matrix operation (Mix & Match).
- Comprehensive rights management and user administration that allow precise control over which user can access which resources.
- Easy commissioning of new end devices through an integrated Device Finder, eliminating the need for manual IP address entry.
- Early detection of security incidents or unusual activities through continuous monitoring via Syslog, Monitoring, and SNMP.

Network ports and protocols used

Port	Service	Type	Description	Comment
–	IGMP	IGMP	IGMP multicast	Not configurable
–	L2 multicast		01:0F:F4.. Device Finder	Not configurable
–	IPsec	ESP	IPSec Encapsulating Security Payload	Not configurable
–	IPsec	AH	IPSec Authentication Header	Not configurable
22	SSH	TCP	Optional communication RemoteAccess-IP-CPU and RemoteTargets	Configurable
49	TACACS+	UDP/TCP	Optional communication authentication service	Not configurable
67	DHCP	UDP	DCHP server	Not configurable
68	DHCP	UDP	DHCP client	Not configurable
80	http	TCP	To open the web application (redirection to HTTPS)	Can be disabled if forwarding is not required or desired
123	NTP	UDP	For time synchronization	Not configurable
161	SNMP	UDP	Optional SNMP agent	Configurable
162	SNMP-Traps	UDP/TCP	Optional SNMP agent	Configurable
389	LDAP	UDP/TCP	Optional communication authentication service	Not configurable
443	https	SSL/TCP	To open the web application	Not configurable
445	CIFS	TCP	For auto backup function	Configurable
514	Syslog	UDP/TCP	Optional Syslog server 1/Syslog server 2	Configurable
636	Active Directory	UDP/TCP	Optional communication authentication service	Not configurable
1812	Radius	UDP/TCP	Optional communication authentication service	Not configurable
2049	NFS	UDP/TCP	For auto backup function	Configurable
3389	RDP	TCP	Optional communication RemoteAccess-IP-CPU and RemoteTargets	Configurable
5900	VNC	TCP	Optional communication RemoteAccess-IP-CPU	Configurable
6137	U2-LAN	UDP	Optional communication U2-LAN	Not configurable
18244	KVM-over-IP	UDP	KVM-over-IP: data port (video, only for end device communication)	Configurable
18245	KVM-over-IP	UDP	KVM-over-IP: Communication Port (K, M, misc)	Configurable
18246	KVM-over-IP	UDP	KVM-over-IP: Control Port and IPSec Internet Key Exchange (IKE)	Configurable
27994	Remote-Port	TCP	Optional remote control access, e.g., IP Control API	Configurable
27996	Database communication	TCP	Internal communication, e.g., MatrixGuard	Configurable
37996	Database communication	TCP	Internal communication	Not configurable