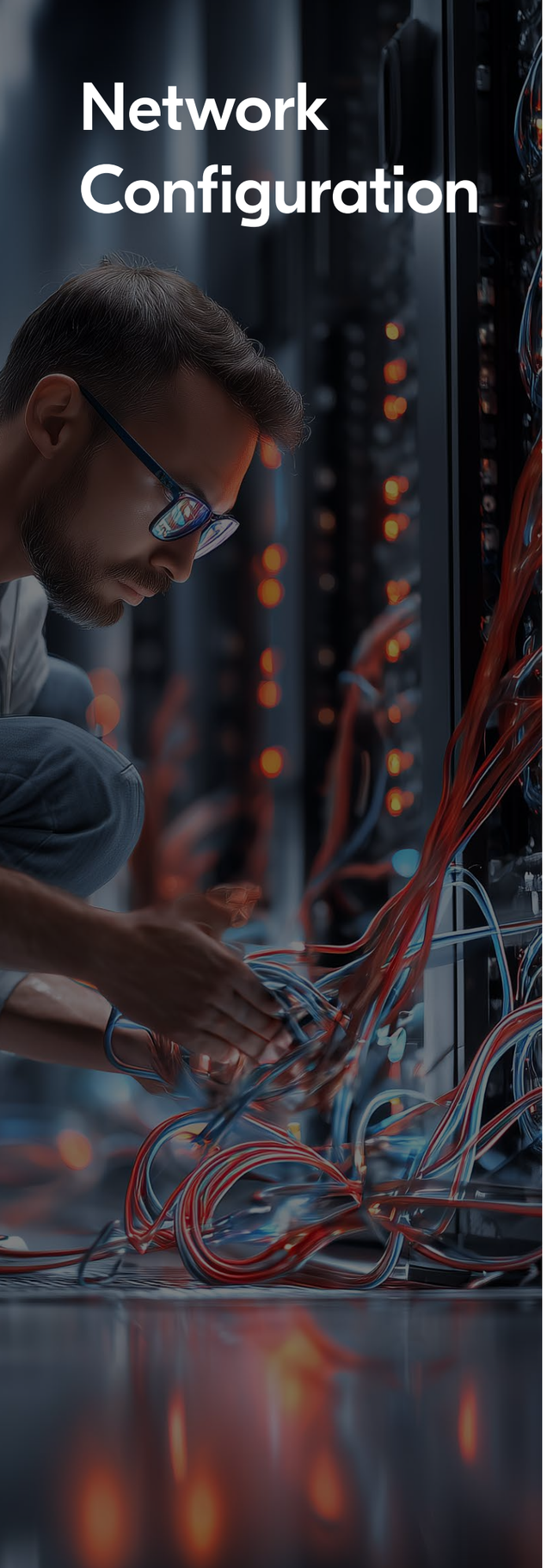
kramer

AVoIP Deployment Guide

Optimizing Networks for Kramer KDS Devices

Introduction

Audio-Visual over Internet Protocol (AVoIP) represents a fundamental shift in how audio and video signals are distributed and managed. By leveraging standard network infrastructure, AVoIP offers unparalleled flexibility, scalability, and cost-effectiveness compared to traditional analog or proprietary digital AV distribution methods. This guide is designed to provide a comprehensive understanding of the network principles essential for a successful AVoIP deployment, with a specific focus on integrating Kramer KDS series devices. We will explore key network concepts, including topology, power over Ethernet (PoE), multicast, and switch considerations, ensuring a robust and efficient AVoIP system.



Network Configuration

Basics: Topology and Principles

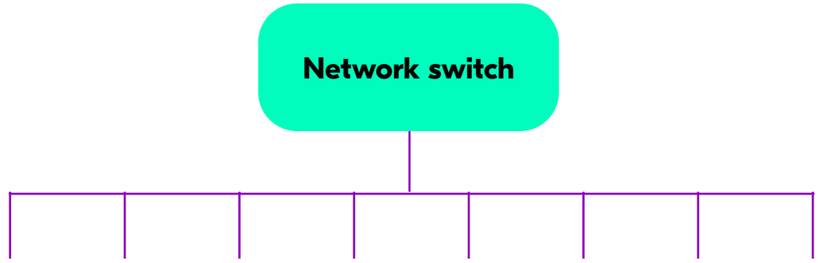
A robust network foundation is paramount for reliable AVoIP performance. Unlike traditional point-to-point AV systems, AVoIP relies on a shared network infrastructure, making network design critical.

Key Principles:

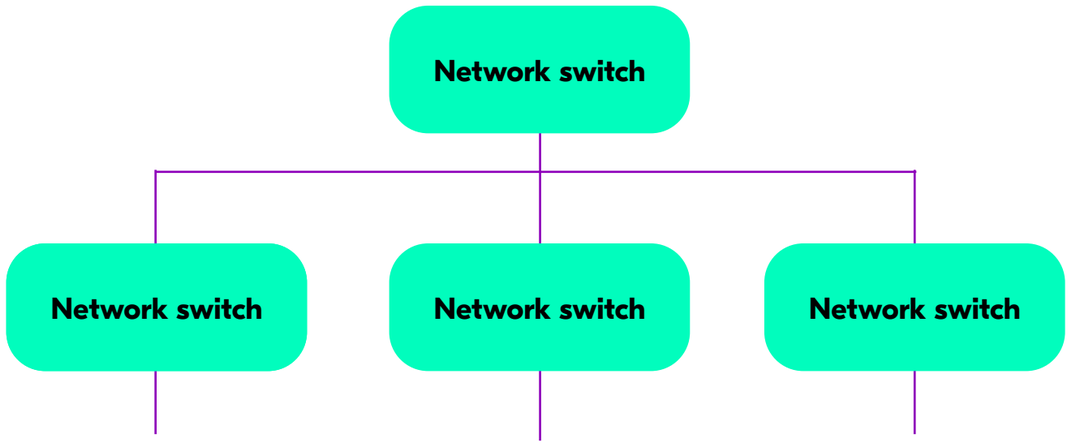
- Dedicated AV Network (Recommended): For optimal performance and to prevent congestion from other network traffic, it is highly recommended to deploy AVoIP devices on a dedicated network segment or VLAN.
- Bandwidth Planning: Accurately calculate the total bandwidth required by all AVoIP streams. This dictates the necessary capacity of your switches and uplinks. Consider future expansion.
- Quality of Service (QoS): Implement QoS policies on your switches to prioritize AV traffic. This ensures that video and audio streams receive preferential treatment over less critical data, preventing latency, jitter, and dropped frames.
- IP Addressing: Use a structured IP addressing scheme (e.g., separate VLANs for AV and control) to manage devices efficiently. Ensure ample IP addresses are available.

Topology:

Star Topology: Most AVoIP deployments utilize a star topology, where all devices (encoders, decoders, control systems) connect directly to a central network switch. This simplifies cabling and fault isolation.



Spine-and-Leaf Topology: For larger, more complex deployments, a spine-and-leaf architecture offers superior scalability and lower latency. Leaf switches connect to endpoints, and spine switches interconnect the leaf switches, providing high-bandwidth paths between network segments.



Power over Ethernet (PoE)

Power over Ethernet (PoE) is a technology that allows network cables to carry electrical power along with data. This simplifies AVoIP deployments by reducing the need for separate power outlets for each AV device.

Why PoE?

- Reduced Cabling: Eliminates the need for separate power cables, simplifying installation and reducing clutter.
- Flexibility: Allows devices to be placed wherever network cabling exists, even in locations without easy access to power outlets.
- Cost Savings: Lower installation costs due to less wiring and fewer electricians required.
- Centralized Power Management: Easier to manage power from a central location, facilitating remote power cycling and UPS integration for continuous operation.
- Safety: PoE operates at low voltages, making it inherently safer than AC power.

Existing PoE Standards:

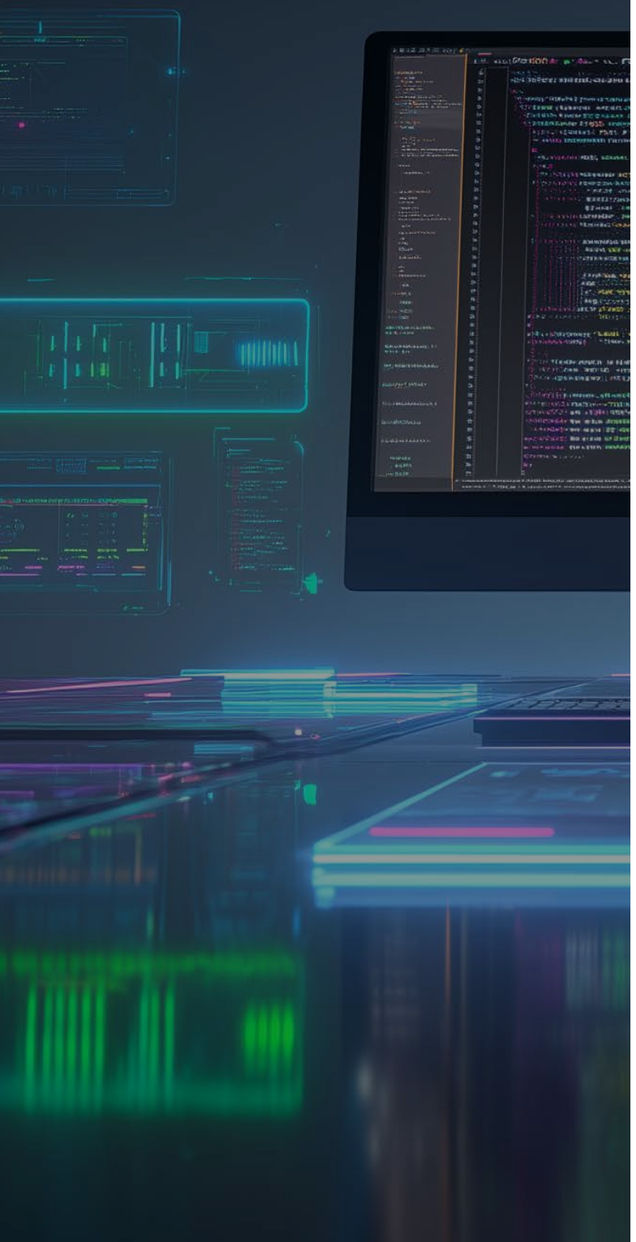
- IEEE 802.3af (PoE): Provides up to 15.4W of DC power to each device (12.95W available at the device). Suitable for many low-power devices.
- IEEE 802.3at (PoE+): Delivers up to 30W of DC power (25.5W available at the device). Commonly used for devices requiring more power, such as pan-tilt-zoom (PTZ) cameras or tablets. Many Kramer KDS encoders/decoders can be powered by PoE+.
- IEEE 802.3bt (PoE++ / 4PPoE):
  - Type 3: Delivers up to 60W of DC power (51W available at the device).
  - Type 4: Delivers up to 100W of DC power (71W available at the device).

These higher power standards are designed for power-hungry devices like LED lighting, thin clients, and high-performance wireless access points.

Benefits for AVoIP:

PoE simplifies powering Kramer KDS devices, especially when placing them near displays or sources where power outlets might be scarce. Ensure your network switches provide sufficient PoE budget for all connected devices.

Multicast and AV Streaming



Multicast is a method of sending network traffic from one source to multiple specific destinations simultaneously, efficiently distributing data to only those devices that need to receive it.

How Multicast Works

- A source (e.g., an AVoIP encoder) sends data to a special multicast IP address.
- Devices that wish to receive this data (e.g., AVoIP decoders) “join” the multicast group associated with that address using the Internet Group Management Protocol (IGMP).
- Network switches, if configured for IGMP snooping, learn which devices are interested in specific multicast streams and forward the data only to the ports where those devices are connected. This prevents unnecessary traffic flooding across the network.

Why it is Used in AV Streaming

- Efficiency: Multicast significantly reduces network traffic compared to unicast (one-to-one) or broadcast (one-to-all). Instead of sending duplicate streams to multiple decoders, a single stream is sent onto the network segment, and the switch intelligently replicates it only to necessary ports.
- Scalability: Allows a single source to feed dozens or hundreds of destinations without overwhelming the source device or the network bandwidth. This is crucial for large-scale AV distribution systems.
- Lower Bandwidth Consumption: By avoiding duplicate streams, multicast conserves network bandwidth, leaving more capacity for other network services.

Multicast IP Addresses and Limitations

- **IP Range:** Multicast IP addresses fall within the **Class D** range, which is 224.0.0.0 to 239.255.255.255.
  - **Local Network Control Block** (224.0.0.0/24): Reserved for local network control messages (e.g., IGMP, OSPF, EIGRP). Traffic in this range is not forwarded by routers.
  - **Globally Scoped Addresses** (224.0.1.0 to 238.255.255.255): Used for general-purpose multicast applications.
  - **Limited Scope Addresses** (239.0.0.0/8): Often used for “private” or administratively scoped multicast within an organization, preventing them from being routed globally. AVoIP systems commonly use addresses in this range.
- **Limitations:**
  - **No Acknowledgement:** Multicast is typically a connectionless protocol (UDP-based), meaning there is no inherent mechanism for receivers to acknowledge receipt of packets. This makes it efficient but sensitive to packet loss.
  - **Requires Network Intelligence:** Without proper switch configuration (IGMP snooping), multicast can flood the network, behaving like a broadcast and causing severe performance degradation.
  - **Routing Complexity:** Routing multicast traffic across different subnets requires specific multicast routing protocols (e.g., PIM - Protocol Independent Multicast), which add complexity to network design.

IGMP Snooping: Importance and Versions

What is IGMP Snooping?

IGMP Snooping is a network switch feature that “listens in” on IGMP (Internet Group Management Protocol) messages exchanged between hosts (AVoIP decoders) and multicast routers. By snooping on these messages, the switch builds a table that maps multicast groups to specific switch ports. This allows the switch to intelligently forward multicast traffic only to the ports where interested receivers are connected, rather than flooding it to all ports in a VLAN.

Why is it Important?

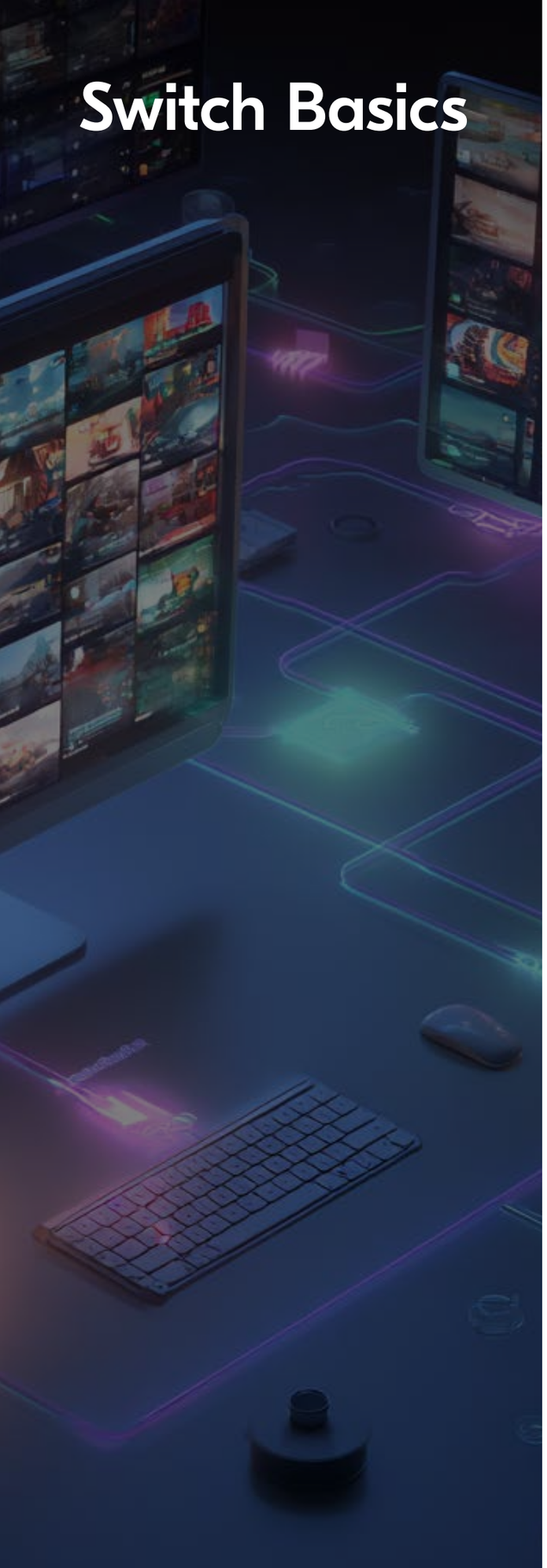
- **Prevents Flooding:** Without IGMP snooping, the switch would treat all multicast traffic as broadcast, sending it out of every port in the VLAN. This can quickly overwhelm network devices and consume valuable bandwidth, leading to performance issues like dropped frames, high latency, and network instability.
- **Optimizes Bandwidth:** Ensures efficient use of network resources by directing high-bandwidth AVoIP streams only where they are needed.
- **Enhances Scalability:** Allows for larger AVoIP deployments by preventing network congestion.

IGMP Versions

- **IGMPv1 (RFC 1112):** The original version, providing basic group membership queries and reports.
- **IGMPv2 (RFC 2236):** Introduced group-specific queries and a leave-group message, allowing hosts to explicitly tell the router when they are leaving a multicast group, leading to faster pruning of unnecessary traffic. Most commonly used version in AVoIP deployments.
- **IGMPv3 (RFC 3376):** Offers Source-Specific Multicast (SSM) capabilities, allowing hosts to specify not only which multicast group they want to join but also which specific source they want to receive traffic from. This can provide greater control and efficiency in complex multicast environments. While AVoIP systems generally rely on IGMPv2 for basic functionality, some advanced features or larger scale deployments might benefit from IGMPv3.

Importance for Kramer KDS Devices:

Kramer KDS devices leverage multicast for efficient video distribution. Proper IGMP snooping configuration on your network switches is critical to ensure that multicast streams are directed only to the intended decoders, preventing network congestion and performance issues. Without IGMP snooping, switches may flood multicast traffic to all ports, leading to network instability.



Switch Basics

Trunk (Uplink, Downlink) and Network Design Considerations

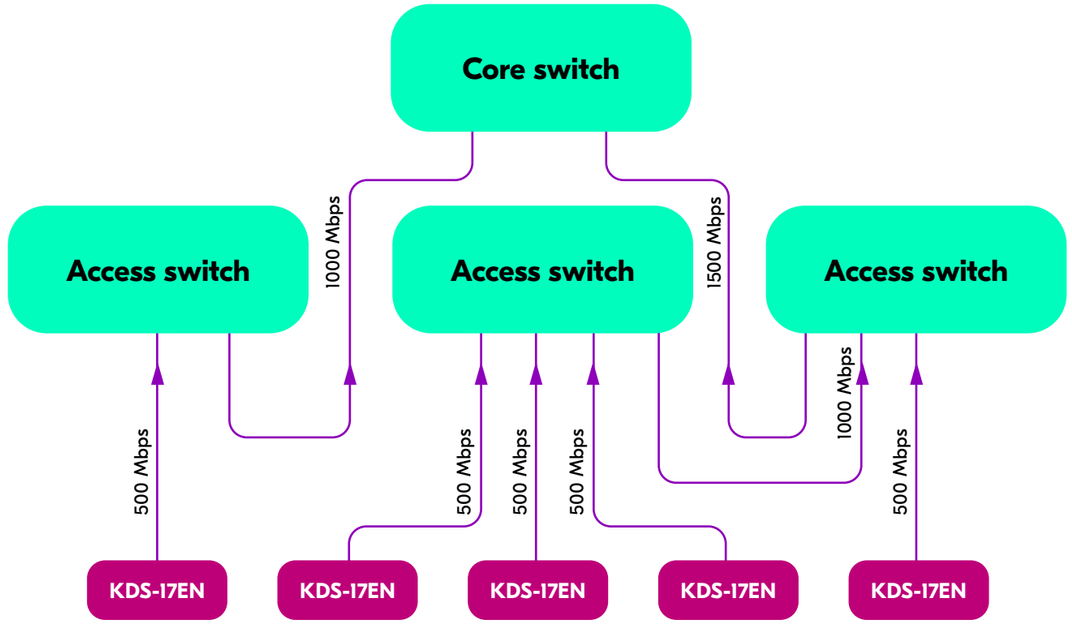
Network switches are the backbone of any AVoIP system, connecting all devices and facilitating data flow. Understanding their configuration and design is vital.

Trunk Ports:

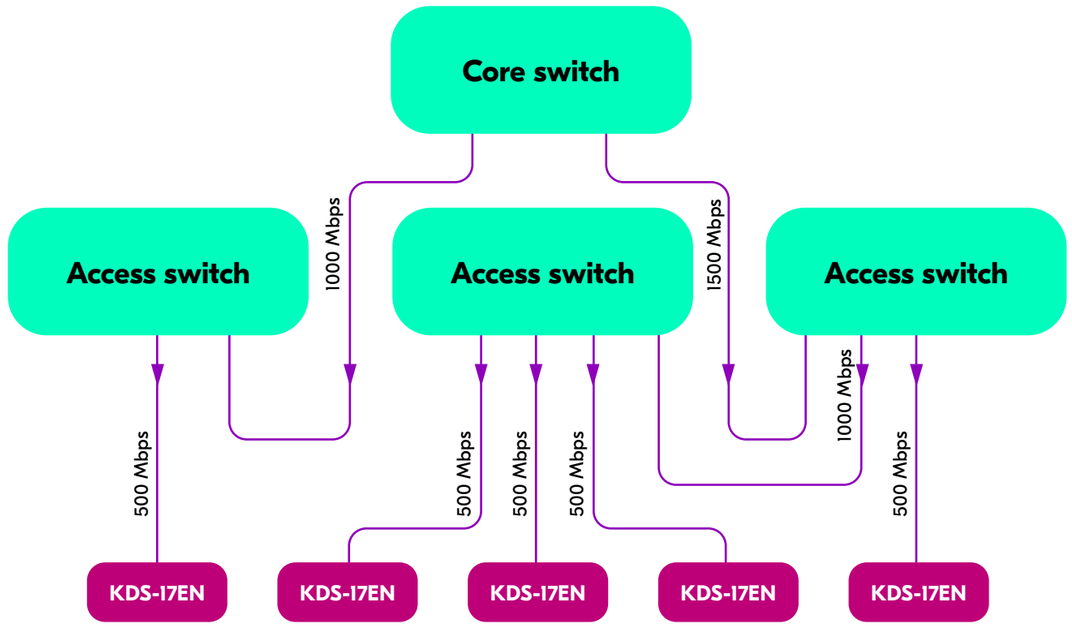
- A trunk port is configured to carry traffic for multiple VLANs (Virtual Local Area Networks) over a single physical link.
- In AVoIP, trunk ports are often used for inter-switch connections (uplinks/downlinks) or for connecting to routers/firewalls when different VLANs need to communicate.
- They use tagging (e.g., IEEE 802.1Q) to identify which VLAN each packet belongs to

Uplink and Downlink:

Uplink: A port on a switch that connects to a higher-level switch (e.g., a core switch or another aggregation switch), or to a router. Uplinks typically require higher bandwidth to handle aggregated traffic from multiple downstream devices.



Downlink: A port on a switch that connects to an end device (e.g., an AVoIP encoder/decoder, PC, IP camera) or to a lower-level switch (e.g., an access layer switch).



Network Design Considerations for AVoIP:

- Managed Switches: Always use managed switches. They provide critical features like VLANs, QoS, IGMP snooping, and port mirroring, which are essential for AVoIP.
- Non-Blocking Architecture: Choose switches with a non-blocking architecture, meaning they can handle full wire-speed traffic on all ports simultaneously without bottlenecks.
- Port Density: Select switches with enough ports to accommodate all current and future AVoIP devices, plus other network components.
- PoE Budget: If using PoE, ensure the switch has adequate PoE budget to power all connected Kramer KDS devices and any other PoE-powered equipment.
- VLANs: Create separate VLANs for AVoIP traffic, control traffic, and other network services to isolate traffic, enhance security, and improve performance.
- Spanning Tree Protocol (STP): Implement STP or Rapid STP (RSTP) to prevent network loops, which can cause broadcast storms and bring down the network.
- Loop Prevention: In addition to STP, consider enabling loop guard or similar features on switch ports connected to end devices.
- Storm Control: Configure storm control to prevent broadcast, multicast, or unicast storms from overwhelming the network.

1G, 2.5G, and 10G Switches: Differences and Use Cases

The choice of network switch speed is critical for AVoIP, directly impacting performance and the types of video resolutions and compression ratios that can be supported.

1 Gigabit Ethernet (1G) Switches:

- Bandwidth: Provides 1000 Mbps (or 1 Gbps) per port.
- Use Cases:
  - Compressed AVoIP (H.264/H.265): Ideal for highly compressed video streams like H.264 or H.265, which have lower bandwidth requirements.
  - Kramer KDS-7, KDS-17, KDS-100 Series: These devices, including the KDS-7, KDS-17, and KDS-100 series, are designed to operate efficiently over 1G networks, often utilizing light compression or H.264/H.265 compression for high-quality video delivery.
  - Control Networks: Suitable for control and management traffic that requires less bandwidth.
  - Advantages: Most cost-effective and widely available.
  - Limitations: Not suitable for uncompressed or lightly compressed 4K video.

2.5 Gigabit Ethernet (2.5G) Switches:

- Bandwidth: Provides 2500 Mbps (or 2.5 Gbps) per port.
- Use Cases:
  - Intermediate Compression: Can support slightly higher quality compressed video or lower latency for 4K content compared to 1G.
  - Upgraded PoE: Often supports higher PoE standards (e.g., PoE++) on more ports than 1G switches.
  - Niche Applications: Less common in dedicated AVoIP deployments but can bridge the gap between 1G and 10G if specific bandwidth needs arise that exceed 1G but don't warrant full 10G.
  - Advantages: Better performance than 1G without the full cost of 10G.
  - Limitations: Still insufficient for uncompressed 4K and limited availability of native 2.5G AVoIP endpoints.

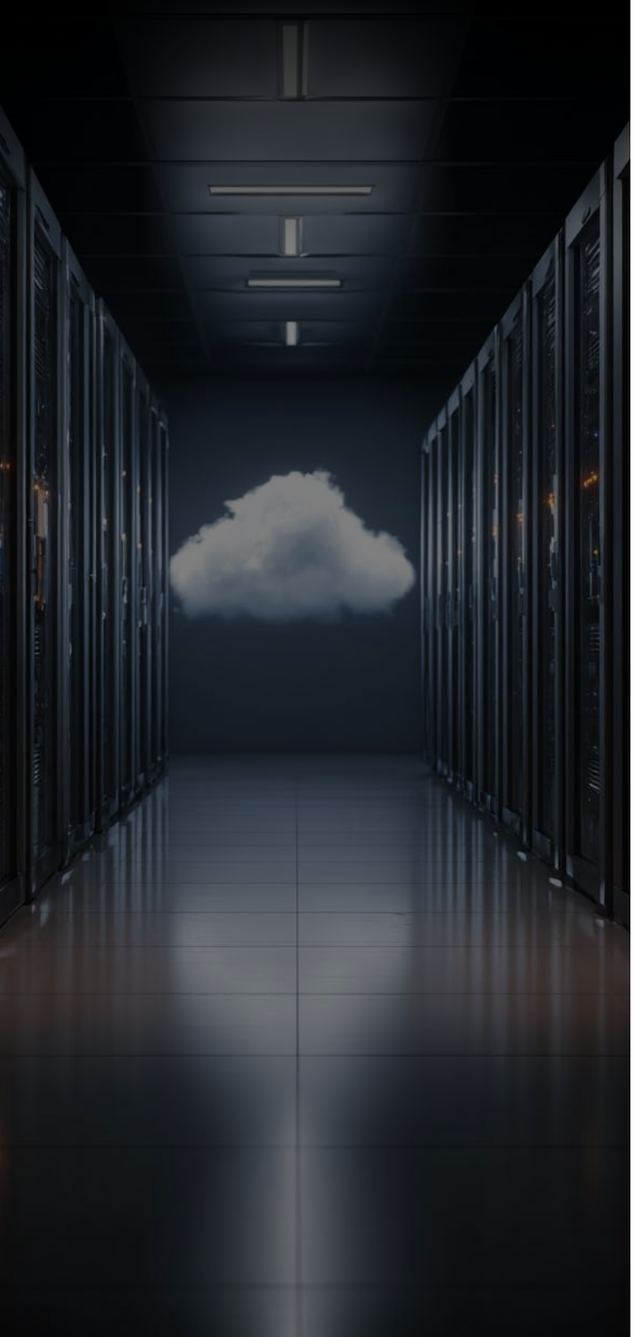
10 Gigabit Ethernet (10G) Switches:

- Bandwidth: Provides 10,000 Mbps (or 10 Gbps) per port.
- Use Cases:
  - SDVoE Deployment: Essential for Software Defined Video over Ethernet (SDVoE) systems, which aim to distribute uncompressed or lightly compressed 4K/60 4:4:4 video with near-zero latency. Kramer's Zyper4K series devices are prime examples of AVoIP products designed for SDVoE, requiring 10 Gbps per stream.
  - High-Bandwidth Uncompressed Video: Any application requiring very high-resolution, high-frame-rate, and color-accurate video without significant compression artifacts.
  - Aggregation/Spine Layers: Crucial for uplink and spine connections in large networks where multiple 1G or 2.5G access switches aggregate traffic.
  - Advantages: Supports the highest quality and lowest latency video. Future-proofs the network for evolving AV demands.
  - Limitations: Higher cost per port and higher power consumption compared to 1G/2.5G.

Summary of Use Cases for Kramer KDS

- For Kramer KDS-7, KDS-17, and KDS-100 series devices, which are designed for H.264/H.265 compressed video or up to 1G light compression codecs, 1 Gigabit (1G) switches are generally sufficient and cost-effective.
- For high-bandwidth, low-latency applications requiring uncompressed 4K video, such as SDVoE deployments (like Kramer's Zyper4K series), 10 Gigabit (10G) switches are mandatory.

VLANs: Importance and Configuration



Virtual Local Area Networks (VLANs) are a fundamental networking technology that allows you to logically segment a single physical network into multiple broadcast domains. This is critically important for AVoIP deployments.

Importance of VLANs:

- Traffic Isolation: Separates different types of traffic (e.g., AVoIP, control, data, voice) onto their own logical networks. This prevents broadcast storms from one segment affecting another and ensures that high-bandwidth AVoIP streams do not contend with general data traffic.
- Improved Performance: By reducing the size of broadcast domains and isolating high-bandwidth traffic, VLANs minimize unnecessary packet forwarding, leading to better overall network performance for AVoIP.
- Enhanced Security: Limits the visibility of network devices and traffic to only those within the same VLAN, improving security by containing potential breaches.
- Simplified Management: Organizes devices logically, making network management, troubleshooting, and policy enforcement much simpler.
- Flexibility: Allows for easier relocation of devices within the network without re-cabling, as devices can remain in their assigned VLAN regardless of physical port.

Key Parameters and Considerations:

- VLAN ID Assignment: Each VLAN is assigned a unique numerical ID (e.g., VLAN 10 for AV, VLAN 20 for control). This ID is used to tag traffic belonging to that VLAN.
- Tagging (IEEE 802.1Q): When traffic traverses a trunk port (which carries multiple VLANs), packets are “tagged” with their respective VLAN ID. End devices (like Kramer KDS encoders/decoders) typically reside on “access ports” which are untagged for a single VLAN.
- Port Assignment (Access vs. Trunk):
  - Access Ports: Connect to end devices (e.g., AVoIP encoders/decoders). An access port belongs to a single VLAN, and traffic leaving the port is untagged.
  - Trunk Ports: Connect switches to other switches or to routers. They carry traffic for multiple VLANs, and traffic is tagged with the appropriate VLAN ID.
- Inter-VLAN Routing: If devices in different VLANs need to communicate (e.g., a control system in the control VLAN needs to manage AVoIP devices in the AV VLAN), a Layer 3 switch or router must be configured to route traffic between these VLANs. This should be done carefully to avoid unnecessary traffic crossing VLAN boundaries.
- Management VLAN: It is best practice to create a dedicated VLAN for managing network devices (switches, routers, etc.) to enhance security.
- AVoIP VLAN vs. Control VLAN: For Kramer KDS deployments, it is highly recommended to separate AVoIP streams (multicast video/audio) onto one VLAN and control traffic (e.g., Kramer K-Net, TCP/IP commands) onto another. This ensures that even if control traffic is heavy, it does not impede the real-time performance of AV streams.

Audio Streaming: Dante and AES67 Network Requirements

Professional audio over IP has become a cornerstone of modern AV systems, with Dante (Audinate) and AES67 being leading standards. Both leverage standard IP networks for audio transport, offering flexibility and scalability. While Kramer KDS devices primarily focus on video, understanding these audio standards is vital for integrated AV deployments.

Dante

Dante is a proprietary audio networking technology that provides uncompressed, multi-channel digital audio over standard Ethernet networks with extremely low latency.

Network Requirements for Dante:

- Dedicated Gigabit Ethernet: While Dante can operate on 100 Mbps networks for smaller systems, Gigabit Ethernet (1G) is strongly recommended and often required for most professional applications, especially with a high channel count. A dedicated network or VLAN for Dante traffic is crucial.
- Managed Switches: Absolutely essential. Switches must support QoS, IGMP snooping, and ideally, Precision Time Protocol (PTP) for optimal synchronization.
- Quality of Service (QoS): Critical for prioritizing Dante traffic. Dante uses DiffServ Code Point (DSCP) values. Voice (EF) for PTP clock synchronization and control, and Class A (CS7) for audio data. Switches must be configured to honor and prioritize these markings.
- IGMP Snooping: Necessary to prevent audio multicast traffic from flooding the entire network. The Dante primary clock master typically acts as the IGMP querier.
- Multicast and Unicast: Dante uses a combination of multicast (for most audio streams) and unicast (for control and discovery).
- Jumbo Frames (Optional): While some sources suggest jumbo frames, Dante typically operates efficiently without them and they can introduce complexity. Avoid unless specifically required.

Best Practices for Dante:

- Disable Energy Efficient Ethernet (EEE/Green Ethernet): EEE can cause clocking issues and dropouts. Always disable it on switch ports connected to Dante devices.
- Disable Spanning Tree Protocol (STP) on Edge Ports: For Dante devices directly connected to switch access ports, disable STP or enable PortFast (Cisco) or equivalent rapid spanning tree settings to ensure immediate port availability.
- Dedicated Clock Master: Ensure a stable and reliable Dante clock master.
- Flat Network Design: Dante prefers a flat Layer 2 network for audio data, minimizing routing hops between devices to maintain low latency.
- Separate Control/Management: If using Dante Controller, it can be on a different VLAN, but the audio traffic itself should ideally be on its own dedicated audio VLAN.

AES67

AES67 is an open standard for high-performance audio over IP interoperability. It defines a set of network requirements to ensure different audio-over-IP technologies (including Dante, when configured for AES67 compatibility) can communicate.

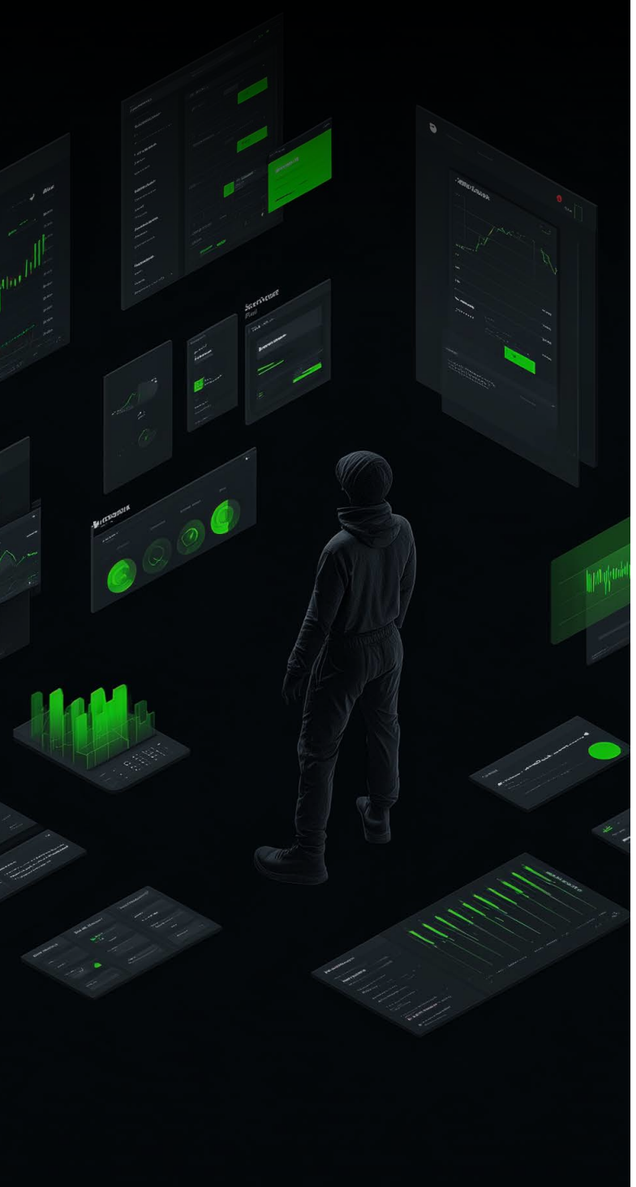
Network Requirements for AES67:

- Gigabit Ethernet (1G): Similar to Dante, 1G Ethernet is the standard requirement.
- Managed Switches: Essential for QoS and IGMP snooping.
- Quality of Service (QoS): Critical for real-time audio. AES67 uses specific DSCP values for PTP timing (EF) and audio streams (AF4).
- Precision Time Protocol (PTP) - IEEE 1588-2008 (PTPv2): AES67 heavily relies on PTP for precise synchronization between devices. Network switches must support PTP transparent clock or boundary clock modes for accurate time distribution.
- Multicast: AES67 primarily uses multicast for audio streams. IGMP snooping is mandatory.
- Dedicated Network/VLAN: Highly recommended to isolate AES67 traffic from other network traffic.

Best Practices for AES67:

- PTP-Aware Switches: Utilize switches that explicitly support PTP (IEEE 1588-2008) to ensure accurate clock synchronization across all devices.
- Consistent QoS Policies: Implement QoS consistently across all network devices involved in the AES67 domain.
- Disable EEE: As with Dante, EEE can negatively impact PTP timing and audio performance.
- Network Segmentation: Use VLANs to separate AES67 audio traffic.
- Redundancy (Optional but Recommended): For critical applications, consider redundant network paths (e.g., using RSTP or dedicated redundant network ports on devices).

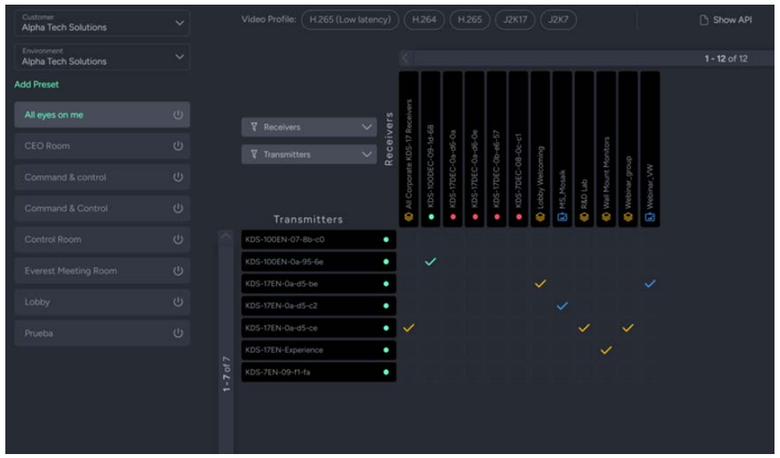
Centralized AVoIP Management Platform



For any substantial AVoIP deployment, especially those involving numerous devices and various content sources and destinations, a centralized management platform becomes indispensable for successful and efficient operation.

Importance of a Centralized Management Platform

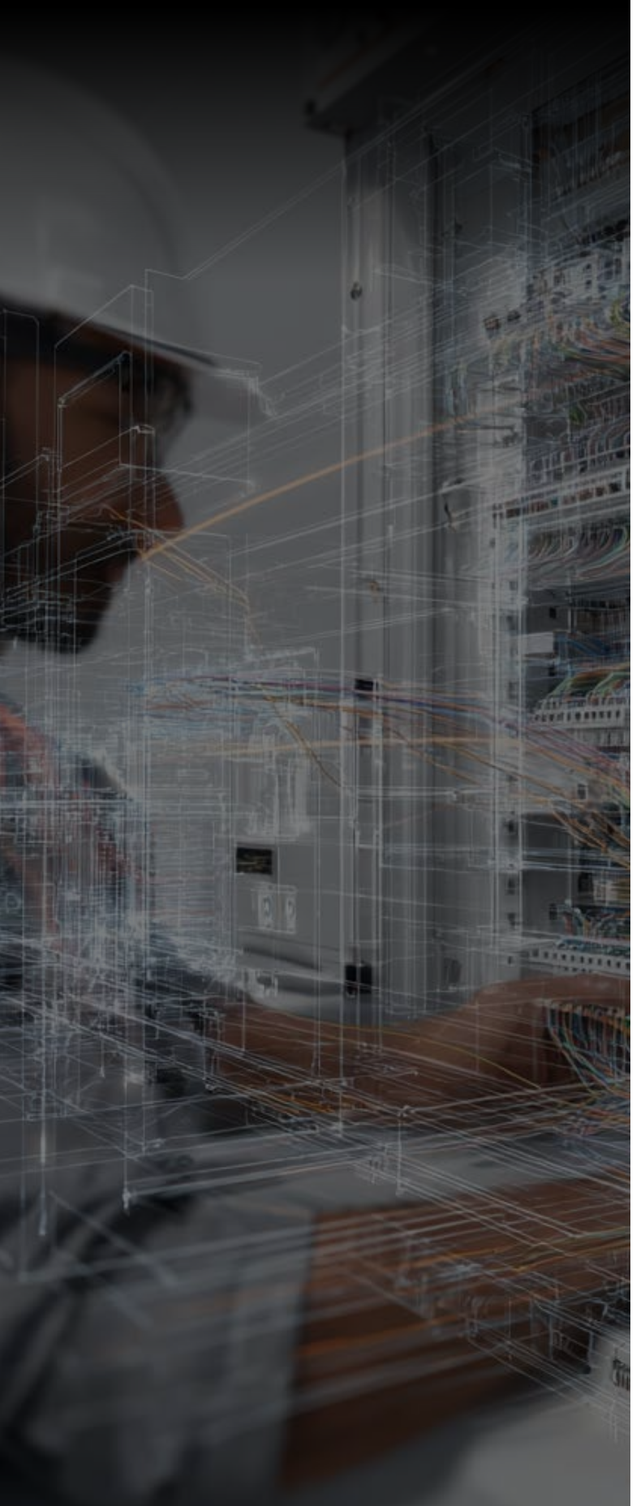
- Simplified Configuration & Deployment: Allows for quick and consistent configuration of multiple AVoIP encoders and decoders from a single interface, significantly reducing deployment time and potential human error. This is particularly beneficial for large-scale Kramer KDS or Zyper4K installations.
- Real-time Monitoring & Status: Provides a dashboard view of all connected AVoIP devices, showing their status, active streams, and any potential issues (e.g., connectivity, bandwidth, temperature). Proactive monitoring helps identify and resolve problems before they impact the user experience.
- Stream Routing & Switching: Offers an intuitive graphical interface for routing video and audio streams between sources and destinations, replacing complex manual IP configurations. This enables dynamic switching and content distribution.
- Troubleshooting & Diagnostics: Centralized logs, error reporting, and diagnostic tools help pinpoint network or device-related issues quickly, minimizing downtime.
- Firmware Management: Simplifies the process of updating firmware across all devices, ensuring they are running the latest versions with bug fixes and new features.
- User Access Control: Enables setting up different user roles and permissions, ensuring that only authorized personnel can make changes to the AV system.
- Scalability & Future-Proofing: A well-designed management platform can easily accommodate system expansion, adding new devices and functionalities without requiring a complete overhaul of the control infrastructure.
- API Integration: Many platforms offer APIs, allowing for integration with broader building management systems, control systems (i.e. Kramer Control), or custom applications.



Benefits for Kramer Deployments

Kramer offers its own management solutions, which are designed to seamlessly integrate with and manage KDS , ZUHD or Zyper4K devices. Leveraging such a platform provides a holistic view and control over the entire AVoIP ecosystem, optimizing operational efficiency and simplifying complex AV routing tasks. It transforms a collection of individual devices into a cohesive, manageable, and highly flexible AV matrix over IP.

Conclusion



For the best performance make sure your network switch is configured correctly

- Choose switches with a non-blocking architecture
- Make sure your switch has sufficient number of ports for your setup
- Enable Multicast
- Enable IGMP Snooping
- Some switcher will require IGMP Querier
- Enable Fast Leave
- Disable green, energy-saving features

Successfully deploying an AVoIP system, particularly with Kramer KDS devices, hinges on a meticulously planned and configured network infrastructure. By understanding the fundamentals of network topology, leveraging Power over Ethernet for simplified installations, mastering multicast for efficient video distribution, and implementing proper VLAN segmentation, integrators can build scalable and reliable AV solutions. The careful selection of network switches based on bandwidth requirements (1G for compressed video like KDS-7/17/100, 10G for uncompressed SDVoE, including Kramer's Zyper4K series) ensures optimal performance. Furthermore, integrating professional audio over IP with standards like Dante and AES67 requires specific network configurations, including QoS, IGMP snooping, and precise PTP timing. Finally, the implementation of a centralized AVoIP management platform is crucial for streamlining configuration, monitoring, and control in complex deployments. Adhering to these principles will not only guarantee a robust AVoIP experience today but also provide a flexible and future-proof foundation for evolving audiovisual technologies.

About Kramer

Kramer audio-visual experiences power creativity, collaboration, and engagement. From AVSM to advanced cloud-based communication, collaboration and control solutions, Kramer creates audio-visual experiences that are more engaging, more inclusive and more connected than ever before. Headquartered in the heart of Startup Nation - Tel Aviv, Israel, with locations around the world, Kramer's audio-visual experts are designing the future of engagement technology. Physical and digital boundaries have blurred. But no matter how hybrid our world becomes, our desire for real, human connection will never cease. Kramer's intuitive, seamless technology breaks down walls, bridges gaps, and makes people feel closer together even when they're far apart.

kramer

www.kramerav.com