T-NETWORK

Network Requirements and Recommendations for TiGHT AV T-NETWORK Series

T-NETWORK 4K60 Video (Low Latency) | Dante Audio & Dante AV Options

Document Type: Technical White Paper (Official Release)
Applies To: TiGHT AV T-Network Series
Video: Up to 4K60
Options: Dante Audio and Dante AV (Dante Video) where supported
Version: 1.0
Release Date: [Insert Date]
Author: TiGHT AV Technical Team
Confidentiality: Public

Revision History

Version	Date
1.0	2026-01-16

---

1. Executive Summary

This white paper defines the **minimum network requirements** to deploy **TiGHT AV T-Network Series** AVoIP **4K60 low-latency video distribution**, with optional **Dante Audio** and **Dante AV (Dante Video)** workflows where supported.

AV-over-IP performance is primarily determined by correct handling of:

- **High-bitrate real-time video**
- **Multicast traffic control (IGMP)**
- **QoS for Dante timing/audio/video traffic**
- **Uplink capacity planning**
- **MTU/Jumbo frame support when required by selected security mode**

---

2. Audience and Scope

2.1 Intended Audience

- Network administrators and IT operations teams
- AV systems engineers and integrators
- Consultants designing enterprise AV network architectures

2.2 In Scope

- Layer-2 switching requirements (IGMP, VLAN, QoS)
- Layer-3 considerations (when routing is unavoidable)
- Uplink capacity planning guidance
- MTU/Jumbo frame requirements by security mode
- Baseline deployment topologies

2.3 Out of Scope

- Vendor-specific switch configuration for every manufacturer
- Comprehensive cybersecurity policy design
- Wireless transport guidance (not recommended for primary AVoIP transport)

---

3. System Traffic Overview (What the Network Must Carry)

3.1 Video Bandwidth Characteristics

T-Network Series endpoints deliver high-quality, low-latency video over **1GbE**. When using Dante AV video modes, bandwidth depends on content and mode, and can exhibit bursts.

Typical Dante AV video bandwidth figures (sizing reference):

- **4K peak:** ~850 Mbps (±20 Mbps)
- **4K average:** ~442 Mbps
- **1080p average:** ~187 Mbps

Key implication: A single 4K stream can approach the practical capacity of a 1GbE port during peaks. This requires:

- Dedicated **1GbE full-duplex** access ports for endpoints
- Correct multicast control to avoid unintended flooding
- Careful uplink planning

3.2 Multicast and Unicast Behavior

T-Network Series supports **RTSP Unicast** and **RTSP Multicast** stream delivery. Multicast is commonly used for **one-to-many** distribution.

Key implication: Multicast must be controlled using **IGMP snooping** and an **IGMP querier**, otherwise streams may flood ports and degrade performance.

3.3 Control, Discovery, and Management

In addition to video/audio streams, the network carries:

- Device discovery traffic

- Control and management traffic (web UI/API, monitoring services as enabled)
- Dante discovery/clock/control traffic (when Dante is enabled)

Key implication: Avoid blocking discovery/control services within AV VLAN(s) unless a controlled alternative design is implemented.

3.4 Security and Encryption Considerations

T-Network Series supports two AES-256 encryption modes **Standard Security Mode** and **High Security Mode**. **High Security Mode** requires **Jumbo frames** (see Section 8).

---

4. Minimum Switch Hardware Requirements (Layer-2)

4.1 Managed Switching (Required)

A managed switch is required for stable AVoIP operation.

Minimum features:

- 1GbE ports for endpoints
- VLAN support (802.1Q)
- IGMP snooping (per VLAN)
- IGMP querier capability (per VLAN)
- QoS (DSCP-based preferred; multiple queues)
- Operational visibility (interface counters, multicast tables, IGMP status)
- Ability to disable EEE (Energy Efficient Ethernet) on relevant ports (recommended for real-time AV/Dante)

4.2 Edge Ports (Endpoints)

Minimum requirements for each encoder/decoder port:

- 1GbE full duplex
- Stable cabling and link integrity (Cat6 or better recommended)

Recommendation: Do not connect endpoints through unmanaged switches.

4.3 Uplinks and Backplane Capacity

The uplink is typically the first bottleneck in scaled deployments.

Minimum guidance:

- For multi-switch designs, use **10GbE (or higher) uplinks** between access and distribution switches.
- Design for headroom; avoid sustained uplink utilization near saturation.
- Ensure the switch backplane and buffers are appropriate for high-rate multicast/unicast streaming.

5. Minimum Multicast Requirements (IGMP)

5.1 IGMP Snooping (Required When Using Multicast)

Enable **IGMP snooping** on every switch and VLAN that carries multicast video/audio.

5.2 IGMP Querier (Required)

At least one device in each VLAN carrying multicast must act as the **IGMP querier**.

Baseline timer guidance (starting point):

- Query Interval: 30 seconds
- Query Response Interval: 10 seconds
- Last Member Query Interval: 100 ms

5.3 IGMP Querier Source IP Requirement (Important)

For stable multicast operation, the **IGMP Querier Source IP address must be a valid Layer-3 (L3) IP address** associated with the VLAN/subnet carrying multicast traffic (typically the IP address of the SVI/gateway interface or routed interface for that VLAN). The querier source IP **must not be 0.0.0.0**.

Why 0.0.0.0 Querier Source IP Can Cause Multicast Instability

Some platforms implement an IGMP "querier" as a **Layer-2 bridging function** rather than a full Layer-3 querier. In these cases, IGMP General Queries may be generated with IPv4 **Source IP (SIP) = 0.0.0.0**. While some networks may appear to function, this behavior can cause interoperability issues with certain switch platforms like the one used in T-NETWORK units and IGMP snooping implementations.

When the querier uses **SIP 0.0.0.0**, T-NETWORK switch ASICs chipset may not reliably:

- Identify the correct **router/querier port** used to control multicast forwarding state
- Maintain multicast membership state correctly in the **IGMP snooping table**
- Refresh multicast forwarding entries consistently as timers age out

This can result in **intermittent multicast failures**, such as streams not building consistently or streams stopping after a period of time when snooping state expires.

TiGHT AV Recommendation

Deploy a **proper L3 IGMP querier** per VLAN carrying multicast AV traffic, using a **real VLAN interface IP address** This provides consistent behavior across enterprise switch platforms and helps prevent multicast membership and forwarding instability over time.

5.4 Fast Leave / Immediate Leave (Recommended)

Enable the vendor equivalent of:

- **Immediate Leave** (preferred), or
- **Fast Leave** on receiver access ports

This improves responsiveness when decoders change sources.

5.5 Block Unknown / Unregistered Multicast (Recommended)

Enable the vendor feature that prevents forwarding multicast traffic to ports that have not explicitly joined a multicast group.

---

6. VLAN Segmentation (Minimum and Recommended)

6.1 Minimum VLAN Recommendation

At minimum, deploy a dedicated **AV VLAN** for:

- Video streams
- Endpoint discovery and control
- Optional Dante services (small systems)

6.2 Recommended VLAN Model (Scaled Systems)

For larger deployments or mixed traffic environments, segment services into:

- **AV-Video VLAN** (TNET Video/Audio streams)
- **Dante VLAN** (Dante audio and/or Dante AV video (if enabled), clocking, discovery)
- **Management/Control VLAN** (web UI, monitoring, management stations)

---

7. QoS Requirements (Especially for Dante)

7.1 Video-Only Networks

If the AV network is isolated and engineered with sufficient headroom, QoS may be optional.
If links are shared or congestion is possible, QoS is strongly recommended.

7.2 Minimum QoS When Dante Is Enabled

When Dante Audio and/or Dante AV is in use, QoS is required to protect time-sensitive clocking and real-time media flows.

Minimum QoS capabilities:

- DSCP-based QoS (DiffServ)
- Multiple hardware queues (4 queues or more recommended)
- Strict priority for highest priority traffic classes
- Consistent trust boundary and policy across all switch hops

Common DSCP values used in Dante environments (reference):

- **CS7 (DSCP 56):** Highest priority timing/clock events
- **EF (DSCP 46):** Real-time audio (and related media flows depending on mode)

Additional Dante-related recommendations:

- Disable **EEE (Energy Efficient Ethernet / Green Ethernet)** on Dante-connected ports and uplinks carrying Dante traffic.
- Ensure QoS is applied consistently end-to-end (every switch hop).

---

8. MTU and Jumbo Frames (Security-Mode Dependent)

8.1 High Security Mode (Jumbo Frames Required)

Jumbo Frames are required only when using High Security Mode.
If High Security Mode is enabled, configure **Jumbo frames end-to-end** across the full path:

- Endpoint ports
- Access switches
- Trunks/uplinks
- Any routed interfaces in-path

Minimum (High Security Mode): MTU **≥ 9000** consistently across all devices in the stream path.

8.2 Standard Security Mode (Default — Jumbo Frames Not Required)

Standard Security Mode does not require Jumbo frames.
In Standard Security Mode, T-Network Series can operate with standard Ethernet MTU settings (typically 1500), assuming all other minimum network requirements are met.

8.3 Operational Notes

- A single non-jumbo hop in an otherwise jumbo-enabled path can cause fragmentation, packet loss, or stream failure.
- If your enterprise network enforces MTU 1500, deploy using **Standard Security Mode** unless your security requirements mandate High Security Mode and you can validate jumbo support end-to-end.

---

9. Network Ports and Firewall Requirements (Inter-Subnet Deployments)

This section lists the **communications ports and protocols** used by TiGHT AV T-Network Series devices for discovery, control, management, firmware operations, and optional enterprise integrations. If endpoints and control systems are separated by **firewalls or routed subnets**, the relevant ports must be permitted between:

- Control system / management stations ↔ Encoders / decoders
- Monitoring/IT services ↔ Encoders / decoders (as enabled)

- Enterprise integrations (MQTT/LDAP) ↔ Encoders / decoders (as enabled)

Important design note (Discovery across subnets):
Some discovery mechanisms are **broadcast or link-local multicast** and typically do **not** traverse routers by default. If your deployment spans subnets, discovery may require one of the following:

- Direct IP management/control, or
- An mDNS gateway/reflector (for mDNS), and/or controlled multicast forwarding where intentionally configured.

9.1 Required Ports (Firewall Allow List)

TYPE	DESCRIPTION	PROTOCOL	NETWORK PORT/RANGE
WEBSOCKET	Web front-end and back-end communication (WS/WSS over TCP)	TCP	4446
STREAM PREVIEW	Display the unit's current stream image (MJPEG over HTTP)	HTTP (TCP)	8080
IR ENCODE	Translate/sending IR signal to IR format or Global Cache IR format	TCP	59401
IR DECODE	Translate/receiving IR signal from Pronto to HEX format	TCP	59402
AUTO STATUS	Default port to send "getstatus" response information	UDP	54327
LLDP	Link Layer Discovery Protocol (Layer 2)	Ethernet (L2)	None (EtherType 0x88CC)
DISCOVERY	Broadcast discovery service	UDP	6797
MDNS	Multicast DNS discovery	UDP	5353
UNIT CONTROL AND INFORMATION QUERY	Unit control and information query commands	UDP	6798
API COMMANDS	Functional API port (TCP mode; not used for SW connection communication control)	TCP	4001
SSH API COMMANDS	API/control port in SSH mode	SSH (TCP)	4005
TCP TO RS232 TUNNELING PORT	Direct access to the unit's RS232 port via TCP tunnelling	TCP	4002
TCP TO RS232 TUNNELING PORT IN SSH MODE	Direct access to the unit's RS232 port via TCP tunnelling in SSH mode	SSH (TCP)	4003
FW UPGRADE VIA SW	Firmware upload via HTTP/HTTPS (URL-based)	HTTP/HTTPS (TCP)	80 / 443

FW UPGRADE STATUS QUERY	Firmware upgrade status query via HTTP/HTTPS	HTTP/HTTPS (TCP)	80 / 443
UPLOADING 5 SERIAL USER COMMAND	Upload RS232 user commands via HTTP/HTTPS	HTTP/HTTPS (TCP)	80 / 443
UPLOADING 40 IR USER COMMANDS	Upload IR user commands via HTTP/HTTPS	HTTP/HTTPS (TCP)	80 / 443
UPLOADING VIDEO WALL CONFIG FILE	Upload video wall configuration file via HTTP/HTTPS	HTTP/HTTPS (TCP)	80 / 443
UPLOADING UNIT CONFIG FILE	Upload unit configuration file via HTTP/HTTPS	HTTP/HTTPS (TCP)	80 / 443
UPLOADING TRIGGER COMMANDS FILE	Upload trigger commands file via HTTP/HTTPS	HTTP/HTTPS (TCP)	80 / 443
GETTING DEBUG INFORMATION FROM DECODER	Retrieve debug information from decoder via HTTP/HTTPS	HTTP/HTTPS (TCP)	80 / 443
SNMP	SNMP management (queries and traps)	UDP	161 (queries), 162 (traps)
MQTT	Message broker connectivity (unencrypted / TLS)	TCP	1883 (unencrypted), 8883 (TLS)
LDAP	Directory service (LDAP / LDAPS)	TCP	389 (LDAP), 636 (LDAPS)

Notes and recommendations

- Prefer **HTTPS (443)** where possible for management operations.
- **Discovery across subnets:** UDP 6797 (broadcast) and mDNS (UDP 5353) typically do not traverse routers without explicit gateway/reflector services.
- **LLDP** is normally Layer-2 (non-routed). Firewall rules typically do not apply to LLDP across subnets.

9.2 Firewall Rule Guidance by Use Case

A) Same Subnet (Flat AV VLAN)

- Discovery works normally.
- Allow control/management ports from control stations to endpoints.

B) Separate Subnets (Routed / Firewalled)
At minimum, allow:

- **TCP 80/443** (web management and file transfer services)
- **TCP 4001** (API control)
- **UDP 6798** (unit control and information query, if used)

Allow additional ports as required by your use case:

- **TCP 4002/4003** (RS-232 tunneling)
- **TCP 4005** (SSH API control mode)
- **UDP 163 (and 161 if needed)** (SNMP monitoring)
- **TCP 1883/8883** (MQTT)
- **TCP 389/636** (LDAP/LDAPS)

---

10. Capacity Planning (Practical Guidance)

10.1 Key Principle: Avoid Oversubscription on Critical Paths

A 1GbE edge port can be heavily utilized by a 4K stream. Oversubscription becomes critical at:

- Inter-switch uplinks
- Aggregation ports
- Routed interfaces (if used)

10.2 Design Recommendation

- Use **10GbE (or higher)** uplinks for multi-switch deployments.
- Validate based on your stream topology:
    - Unicast fan-out increases uplink usage rapidly
    - Multicast reduces encoder replication but requires proper IGMP design

---

11. Minimum Deployment Checklists

11.1 Access Switch Checklist (Endpoints Connect Here)

- Managed switch with 1GbE full-duplex access ports
- Dedicated AV VLAN (minimum)
- IGMP snooping enabled on AV VLAN(s)
- IGMP querier present for each multicast VLAN
- IGMP querier uses a valid **L3 source IP** (not 0.0.0.0)
- Immediate/Fast Leave enabled on receiver ports (recommended)
- Block unknown/unregistered multicast where supported (recommended)
- QoS enabled and DSCP honored end-to-end (required for Dante)
- EEE disabled on AV/Dante ports (recommended)
- Jumbo frames enabled end-to-end **only if High Security Mode is enabled** (MTU ≥ 9000)

11.2 Distribution/Core Checklist (Multi-Switch Designs)

- 10GbE (or higher) uplinks
- Consistent VLAN trunking and MTU policies
- End-to-end QoS consistency for Dante
- IGMP snooping enabled everywhere multicast exists
- Clear IGMP querier design (per VLAN) with valid L3 source IP
- Routed multicast only when necessary and engineered explicitly

---

12. Recommended Topologies

12.1 Small System (Single Switch)

Minimum: One managed 1GbE switch with IGMP snooping + IGMP querier enabled on the AV VLAN.
If Dante enabled: configure DSCP QoS and disable EEE on relevant ports.

12.2 Medium/Large System (Multiple Switches)

Minimum: Access switches uplinked to distribution with 10GbE (or higher).
Use a dedicated VLAN model and consistent IGMP/QoS policies across all switches.

---

13. Conclusion

TiGHT AV T-Network Series endpoints deliver high-quality, low-latency 4K AV over standard Ethernet when the network is designed to properly support real-time media. The minimum requirements are:

1. **Managed switching** with **IGMP snooping + querier**
2. **IGMP querier uses a valid L3 source IP** (not 0.0.0.0)
3. **1GbE full-duplex** endpoint ports
4. Correct **uplink capacity** planning (10GbE uplinks for multi-switch designs)
5. **QoS + EEE disablement** when **Dante** is enabled
6. **Jumbo frames only for High Security Mode**; **Standard Security Mode does not require Jumbo frames**

Following this baseline ensures stable operation and predictable scaling for professional deployments.

Appendix A — Quick Minimum Requirements Summary

Minimum network requirements (baseline):

- Managed L2 switch

- 1GbE to each endpoint
- IGMP snooping enabled
- IGMP querier enabled (per VLAN carrying multicast) with valid L3 source IP (not 0.0.0.0)
- VLAN support (802.1Q)
- QoS (required when Dante is used)
- Jumbo frames end-to-end **only when High Security Mode is enabled** (MTU ≥ 9000)