

Troubleshooting guide for network connection

Network trouble?

You've come to the right place! This guide helps you troubleshoot issues connected to your network.

The infrastructure

The network is the most unpredictable source of problems in your system. Everything in the network between senders and receivers, for example switches, routers, cables, and proxies, will, at some point, affect the connection.

Network management

Problem

Unpredictable factors can cause issues in the network.

Possible solution

- Make sure the link between the camera and the viewing device has a guaranteed throughput:
 - To achieve this in a LAN (Local Area Network), minimize the number of hops (routers and switches) in the link, and don't share the link with other traffic, such as Voice over IP (VoIP) or other protocols prioritized over video, or demanding services that overload the link.
 - To achieve this in a WAN (Wide area network), guarantee the QoS in each hop, or lease a point-to-point route through your local internet provider.
- We recommend using shielded cables. Depending on the application, EMI/RFI/ESI*, also known as signal interference, can affect the cables negatively. Insulation alone doesn't protect from signal interference, so proper shielding is vital to avoid the effects of signal interference.

* EMI/RFI/ESI - (electromagnetic interference, radio frequency interference, electrostatic interference)

Bandwidth

Problem

Network video products utilize network bandwidth based on their configuration. The bitrate increases if you want a high-quality video with low compression. If the bandwidth is limited, the device must compromise on the quality of the stream (reduce bitrate) to match the available network infrastructure bandwidth, which can cause packet loss.

Possible solution

- In a small surveillance system with 8 to 10 devices, you can use a basic 100-megabit (Mbit) network switch without considering bandwidth limitations.
- For systems with ten or more devices, you can estimate the network load using a few rules of thumb:
 - A device configured to deliver high-quality images at high frame rates uses approximately 2 to 3 Mbit/s of the available network bandwidth.
 - With 12 devices or more, consider using a switch with a gigabit backbone. If you're using a gigabit switch, we recommend installing a gigabit network adapter on the video management software server.

Device overload

Streaming stops if the device crashes due to an overload. Here are some of the factors that can cause a device overload:

- Chipset performance
- Several distributed or edge analytics
- High frequency of HTTP request

Chipset performance

Problem

It's hard to predict how many simultaneous, individually configured streams, with maximum resolution, and full frame rate, a video product (chipset) delivers in all situations. The overall performance depends on the following:

- CPU load or video compression load (depending on the chipset) in the video product
- Total data throughput (bandwidth) from the product and network infrastructure
- Client performance
- Image complexity
- Lighting conditions

Possible solution

- From a user perspective, these are the most common parameters that affect the overall performance negatively:
 - High image resolution
 - Low image compression level
 - Mixing Motion JPEG and H.264/H.265 streams
 - Many clients accessing the server simultaneously
 - Clients accessing different image settings, such as resolution and compression, simultaneously
 - Heavy usage of event settings
 - Motion detection turned on
 - HTTPS
 - Poorly performing client PC which doesn't decode all images
 - Limited or poor network infrastructure causes network congestion, resulting in dropped frames.
- When the image scene, compression level, and compression method are kept constant, an increase in resolution decreases the number of full frame rate streams or causes the frame rate per stream to fall.

Example:

Learning about the chipset helps you understand its limitations. Let's use an ARTPEC-7 as an example. The test results for that chipset show that it can deliver almost six simultaneous H.265 streams in HDTV 1080p at 30 fps, two H.265 streams in 4K at 23 fps, or one H.265 stream in 3712x2784 at 20 fps. Alternatively, it can simultaneously deliver one H.265 stream in 4K at 30 fps and one H.265 stream in 1080p at 30 fps.

Several distributed or edge analytics

Problem

When running many applications on a device, the CPU processing is at the edge and can heavily affect the device's performance and cause unwanted crashes or interruptions. These issues can also occur when an application requires a lot of processing power or when you add several high-quality streams

Possible solution

- Limit the number of running applications.

High frequency of HTTP requests

Problem

Devices and their resources can't handle non-stop requests from an incorrectly configured video management system.

Possible solution

1. Isolate the device from the video management system.
2. In the device's web interface, open a stream using the live view.
3. If you can access the stream this way, try to reduce the number of HTTP requests from the video management system.

Open a support case

Maybe this guide didn't help you solve your issues. If so, you are welcome to open a support case.

Troubleshoot with Wireshark or VAPIX commands

We recommend using Wireshark for attaching a network trace to a support case. If you don't have Wireshark on your computer, you can download it for free *on their website*. Wireshark allows you to filter traffic when recording and reviewing it, and both can be useful in different situations.

Additionally, when troubleshooting connectivity issues with Axis devices (AXIS OS 5.x or later), you can use the following VAPIX commands through a web browser:

- `http://x.x.x.x/axis-cgi/debug/debug.tgz?cmd=pcapdump&duration=30` generates a packet capture file taken from the device for the specified time in seconds. The capture is in standard *.pcap format so that you can review it in Wireshark.
- `http://x.x.x.x/axis-cgi/connection_list.cgi` displays a list of currently open TCP/UDP connections or ports.
- `http://x.x.x.x/axis-cgi/pingtest.cgi?ip=y.y.y.y` pings the specified IP address once and then reports the result.

Support case data and information

Note

- If possible, test your devices on the latest AXIS OS on an LTS track or active track. You can find the latest version at our *Device software* page. Read more about TLS tracks in the *AXIS OS Lifecycle guide*.
- Always attach the device's server report in the support case. *Here's a YouTube video tutorial* on how to download a server report from the device web interface.

Here's a list of the information we'd like you to collect before you contact Axis support:

- Results from any internal investigation of the network and network devices.
- A description of the network and a network topology drawing.
- Detailed information about all the devices on the network.
- A list of firewall and antivirus suites and information about any updates of those programs.
- Results from comparing the failing device with other working devices.
- Wireshark from the failing device and other working devices in the network.
- Results from isolating the device from the network to check if the problem persists.
- Information on how the unit is powered.
- The name of any third-party video or evidence management system in use.
- The age of the installation and information about any recent changes to the network.

Final note

Axis devices operate as intended if they are installed according to their installation guide.

Axis is not responsible for how the device configuration described in this guide affects your system. If the device or system fails due to your changes or you get other unexpected results, we recommend that you restore the device to the default settings.

This guide does not cover all possible issues but the ones that are frequently seen in support cases. As an Axis customer, you're always welcome to contact *Axis helpdesk*.

T10196597

2026-09 (M3.2)

© 2023 – 2026 Axis Communications AB