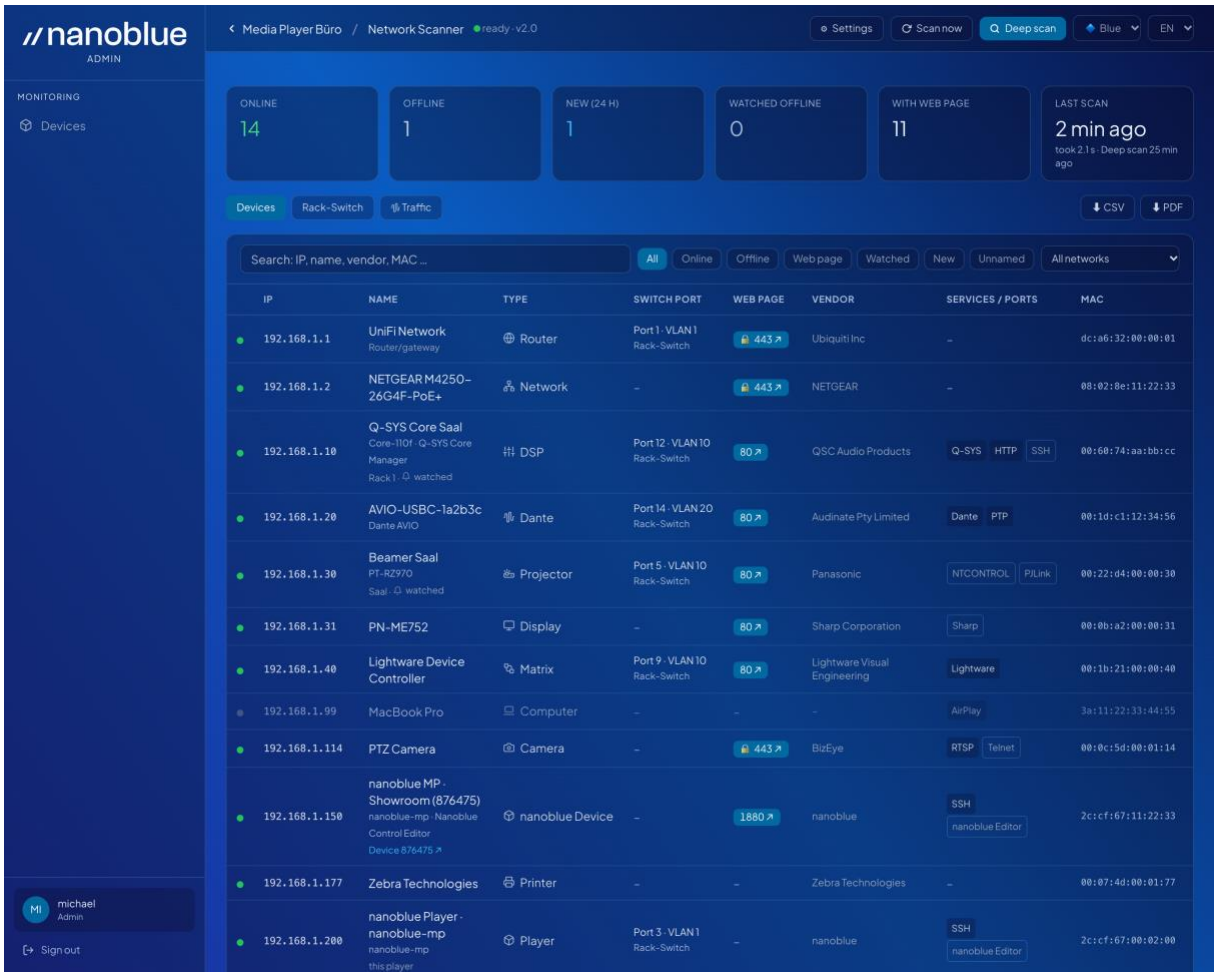
nanoblue® Network Scanner

See, monitor and configure every device on the network remotely – with switch view and PoE control, securely via the nanoblue cloud



Network Scanner in the nanoblue portal: key figures, filters and the device list with type, web page, vendor, services and time last seen.

What it is about

Every nanoblue media player knows the network it is in. The Network Scanner makes use of this: it finds all devices on the player's local networks – control systems, DSPs, Dante devices, displays, projectors, cameras, switches, routers – and shows them clearly in the nanoblue portal. No additional hardware, no software at the customer site and no firewall changes.

Particularly practical: the configuration pages of the devices found can be opened directly from the portal with one click – securely via the player's encrypted connection, as if you were on site in the network. And for technicians on site, the same list is also available directly on the local network.

With a Netgear switch, port assignment, VLANs, PoE control, cable test and port monitoring are added – and the traffic analysis finds out who is flooding the network when picture or controls stutter.

Key features

Find and identify devices automatically

- **All networks of the player**: wired and Wi-Fi, each network can be switched on or off individually.
- **Vendor** from the device's network address (MAC).
- **Services** via Bonjour/mDNS: e.g. Dante, AES67, Q-SYS, NDI, NMOS, Lightware, AirPlay, Shelly.
- **Control interfaces** via open ports: e.g. PJLink, Q-SYS QRC, Yamaha RCP, Crestron, Extron, Telnet, RTSP.
- **Web pages** of the devices including page title – often this already shows the model, e.g. "NETGEAR M4250" or "Q-SYS Core Manager".
- **Switch port and VLAN** per device from Netgear switches (e.g. AV Line M4250) via LLDP – shows which port a device is connected to.
- **Own nanoblue devices** are recognised automatically (via the registered network address) and shown with type, name and device ID – instead of as an anonymous device – with a link straight to the device page in the portal.
- **Device type** is derived automatically (router, network, audio/DSP, Dante, display, projector, camera, control …) and can be corrected.



Device list: status, IP, name, type, switch port and VLAN, buttons to the web page (🔒 = encrypted), vendor, services, MAC and time last seen.

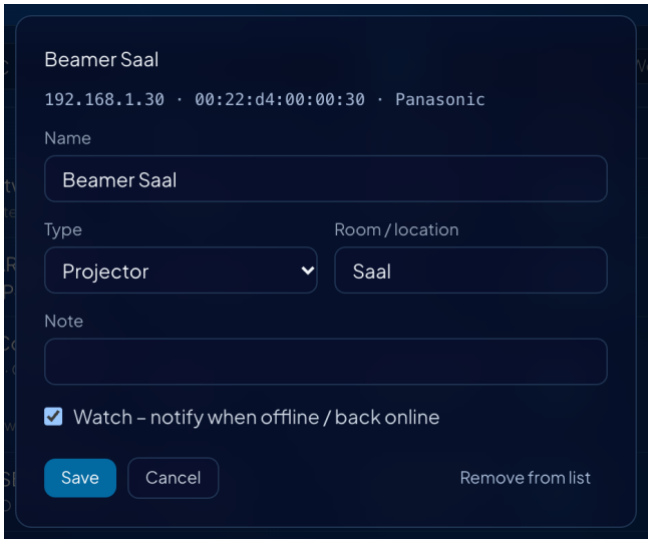
Light on resources

Scan	When	What
Quick scan	every 5 minutes (adjustable)	Which devices are there? Takes about 1–5 seconds.
Deep scan	hourly, immediately for new devices and at the push of a button	Services, control interfaces, web pages.

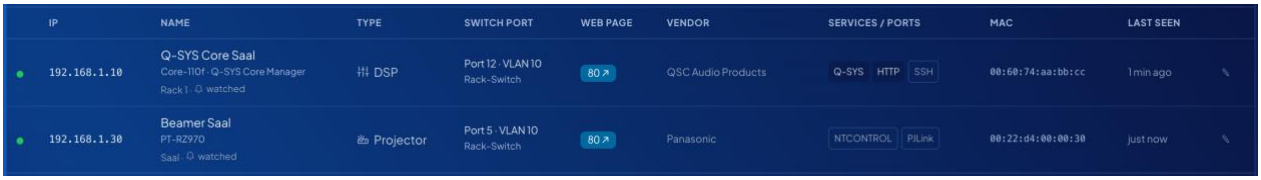
The scanner runs as a separate, lightweight service alongside the player's other functions and is strictly limited in CPU time and memory. Playback, Interactive UI and control are not affected.

Name and monitor devices

- Give each device a name, type, room and a note – the device is recognised by its MAC address even if the IP changes.
- **Watch**: if a watched device fails, a notification is sent via nanoblue Notify (Telegram, browser push) – and an all-clear as soon as it is back.
- Optional: notice as soon as a new, unknown device appears on the network.
- Filters for online, offline, with web page, watched, new and unnamed; search across all fields.



Name and watch a device.



Filter "Watched": the important devices of an installation at a glance.

Events

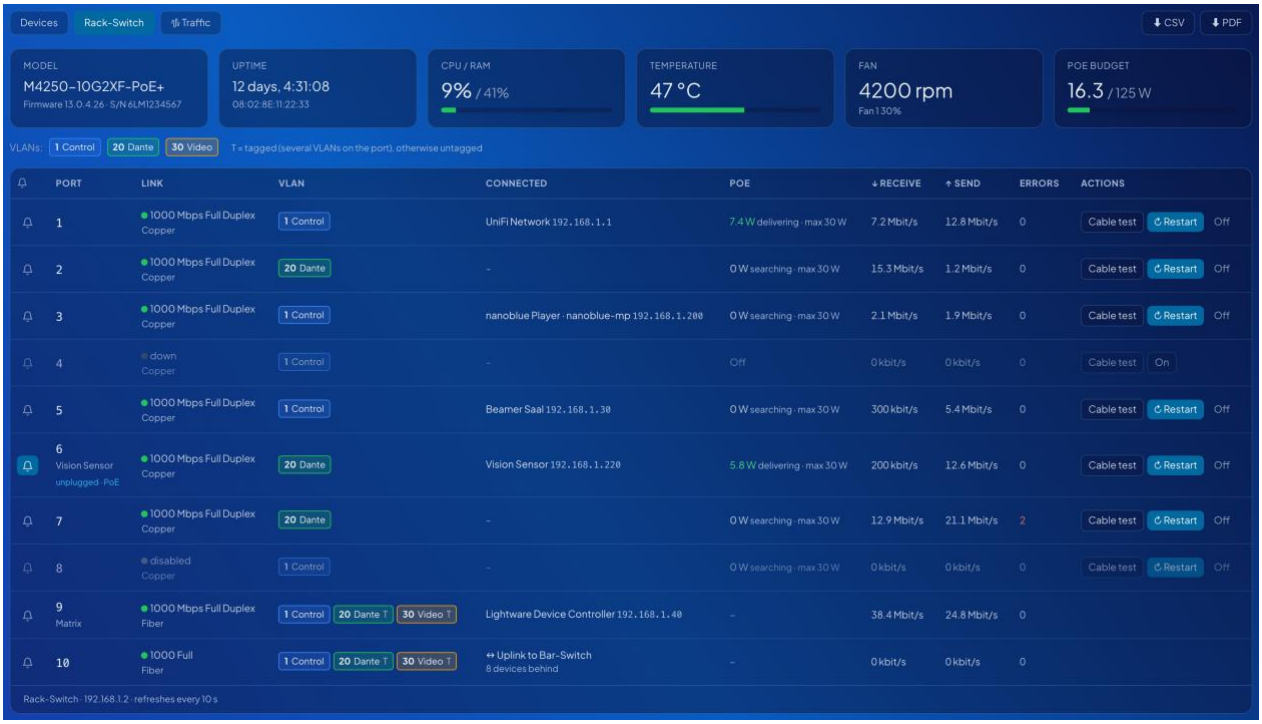
New devices, failures, returns and IP changes are logged with a timestamp. This shows when a device was last on the network or since when a new device has been connected.

Switch view with PoE control

For stored Netgear switches (e.g. AV Line M4250) there is a separate tab next to the device list. It shows the state of the switch and every port live – refreshed every 10 seconds while the view is open. The switch is not loaded in the background.

- **Switch**: model, firmware, serial number, uptime, CPU and RAM load, temperature, fans.
- **PoE budget**: consumption of all PoE devices relative to the available power – shows whether there is reserve for another device.
- **Per port**: link and speed, the connected device from the device list, PoE power in watts with status and limit, current bandwidth received/sent and transmission errors.
- **VLANs**: the VLANs per port in the colours of the Netgear interface, marked as untagged or tagged (T), plus a VLAN overview. You see at once which devices are in the Dante, video or control network.
- **Switch PoE**: port off, on or restart (via the switch's built-in restart function). Hung cameras, access points, touch panels or players can be restarted remotely without anyone on site pulling the plug. Admins only, with a confirmation naming the connected device, and logged.

- **Cable test**: the switch measures the cable on a port and reports OK, break, short circuit or crosstalk – with the distance to the fault in metres. Ideal when a port runs slower or reports errors. Admins only, with confirmation (the port is disconnected for a few seconds).



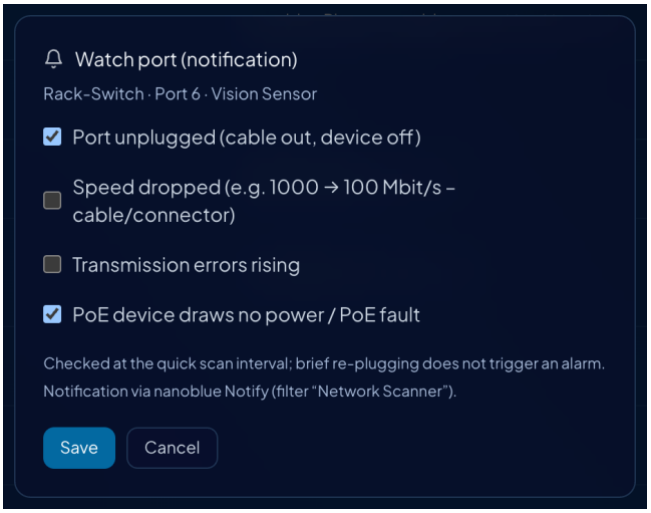
Switch view: switch state, PoE budget, VLANs and per port link, VLAN, connected device, PoE power, bandwidth, monitoring and PoE buttons.

Monitor switch and ports

Important ports can be monitored individually (bell button in the switch view). Notifications are sent via nanoblue Notify – with switch, port and connected device, each with an all-clear:

Monitoring	Notification when …
Switch reachable	the switch no longer responds or the login fails (checkbox per switch in the settings)
Port unplugged	a cable has been unplugged or the device switched off
Speed	the port runs slower than usual, e.g. 100 instead of 1000 Mbit/s – typical of a damaged cable or a bad connector
Transmission errors	errors on a port increase – a sign of cable problems before a failure occurs
PoE	a PoE device no longer draws power or the port reports a PoE fault

Checks run at the quick scan interval. Briefly re-plugging does not trigger an alarm – only if the condition persists for two checks in a row.



Watch port: what should be reported is chosen per port.

Export documentation

With the buttons ⬇ CSV and ⬇ PDF above the list, the current state can be recorded at any time – the device list (with the filters set) or the ports of a switch:

- **CSV**: opens directly in Excel – IP, name, type, room, vendor, MAC, services, web pages, switch port, VLAN, monitoring, last seen, or per port link, VLAN, device, PoE and bandwidth.
- **PDF**: clear table in landscape format with date and player – ideal as installation documentation at handover or maintenance.

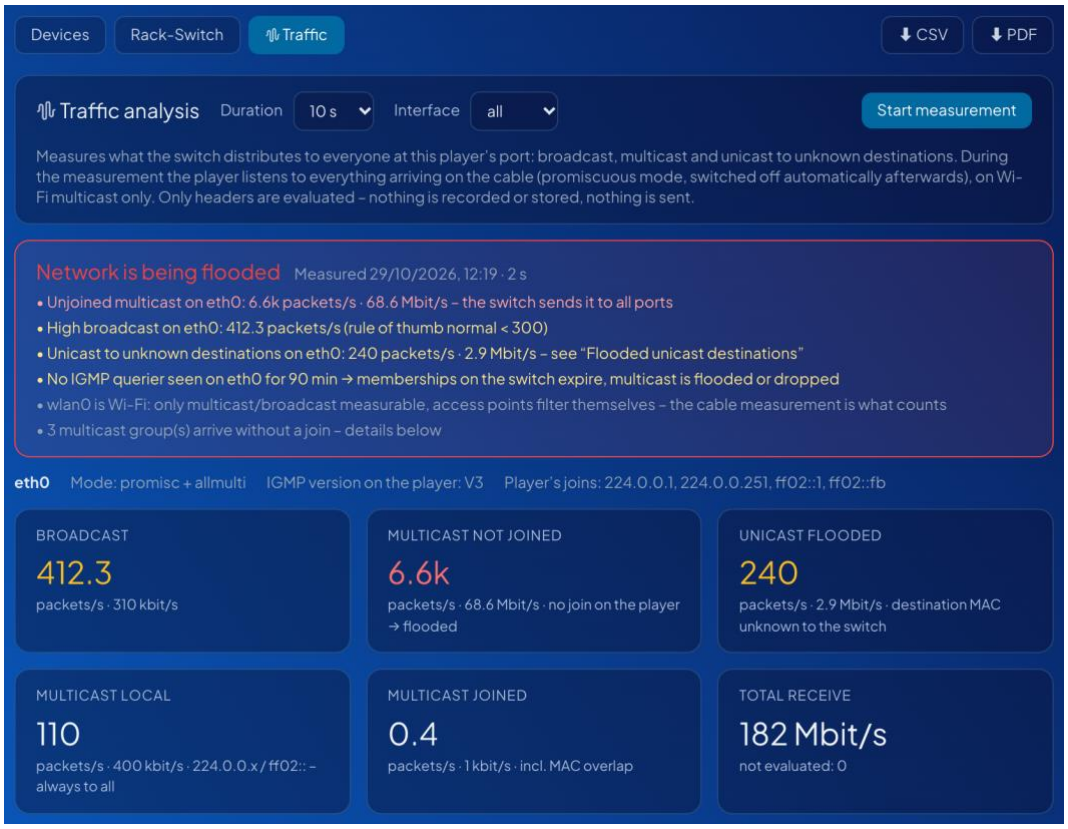
Traffic analysis: who is flooding the network?

Image processors, matrices and displays are sensitive when the switch distributes too much traffic to all ports – the picture stutters, controls hang, devices are briefly unreachable. The traffic analysis measures exactly this traffic at the player's port and shows who causes it and why. The button "Start measurement" in the "Traffic" tab runs a measurement of 10, 30, 60 or 120 seconds – ideally while the problem occurs.

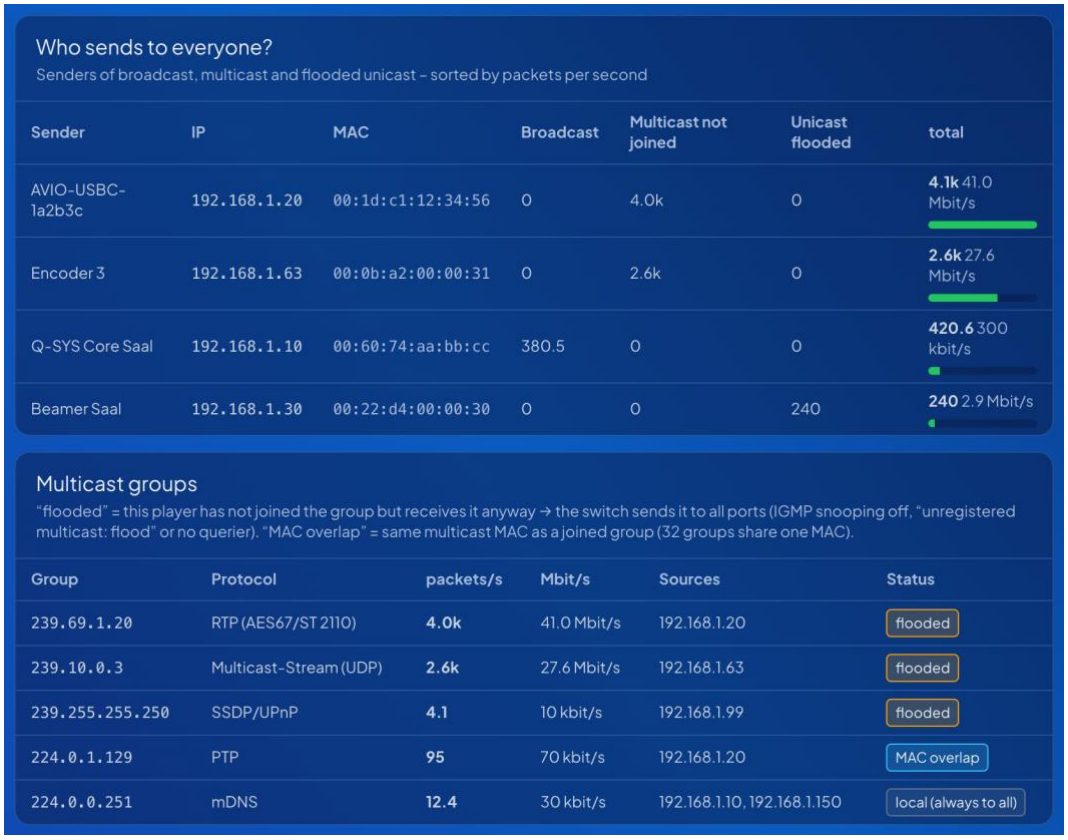
Value	Meaning
Broadcast	Packets to everyone (ARP, DHCP, device discovery). Rule of thumb: below 300 packets/s is normal.
Multicast not joined	Streams (video, audio, Dante/AES67 …) the player has not joined. If they arrive anyway, the switch sends them to all ports – the most common cause of a "flooded" AV network.
Unicast flooded	Packets to a specific device whose address the switch does not know – so it sends them everywhere. Typical for receive-only devices (e.g. stream targets).
Multicast local	Control traffic every switch sends to all (mDNS, IGMP, device announcements). Only conspicuous if it rises sharply.
IGMP querier	The switch or router that regularly asks who wants which stream. If it is missing, memberships expire after a few minutes and multicast is flooded to all. The player watches this permanently.

- Traffic light with findings in plain text, e.g. "Unjoined multicast: 6,600 packets/s · 69 Mbit/s – the switch sends it to all ports" or "No IGMP querier seen for 90 min".
- "Who sends to everyone?": the loudest senders with device names from the scan list – so the cause is found immediately.
- Multicast groups with source, packets and bandwidth and the status "flooded", "joined", "local" or "MAC overlap"; plus the flooded unicast destinations and all protocols.
- Export as CSV or PDF – as evidence for the customer or the network administrator.

- Privacy: the player only listens and sends nothing. Only headers (sender, destination, protocol) are evaluated, no contents; nothing is recorded or stored. Every measurement is logged with user and time.



Traffic analysis: traffic light with findings and the values per network interface.

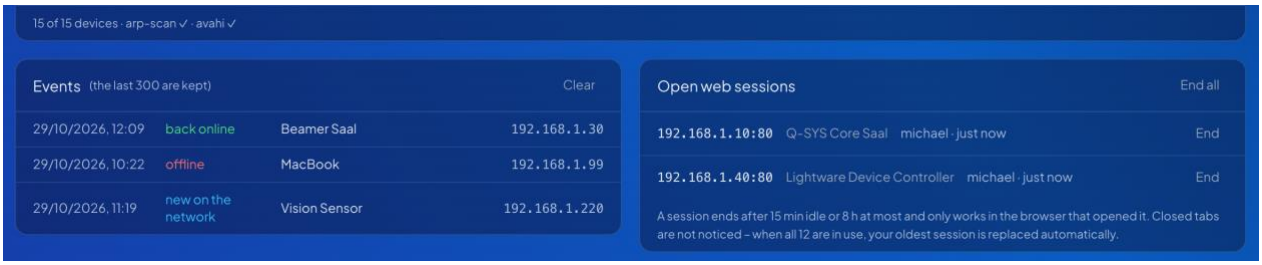


Who sends to everyone, and which multicast groups are flooded?

Open device web pages via the cloud

A click on “80 ↗” or “🔒 443 ↗” opens the device’s configuration page in a new browser tab – from the office, on the road or from a smartphone. The connection runs encrypted via the player; nothing needs to be opened up on the customer’s network.

- Up to 12 web sessions at the same time; overview of open sessions with “End” and “End all”.
- Sessions end automatically after 15 minutes without use, at the latest after 8 hours.
- If the same device is opened again, the login and cache on the device are kept – the page opens within a few seconds.



Events and open web sessions.

Security

Access to devices on the customer’s network is sensitive. That is why: no access without login – at any level. The Network Scanner is built so that no port has to be opened and no firewall rule changed on the customer’s network.

How a connection works

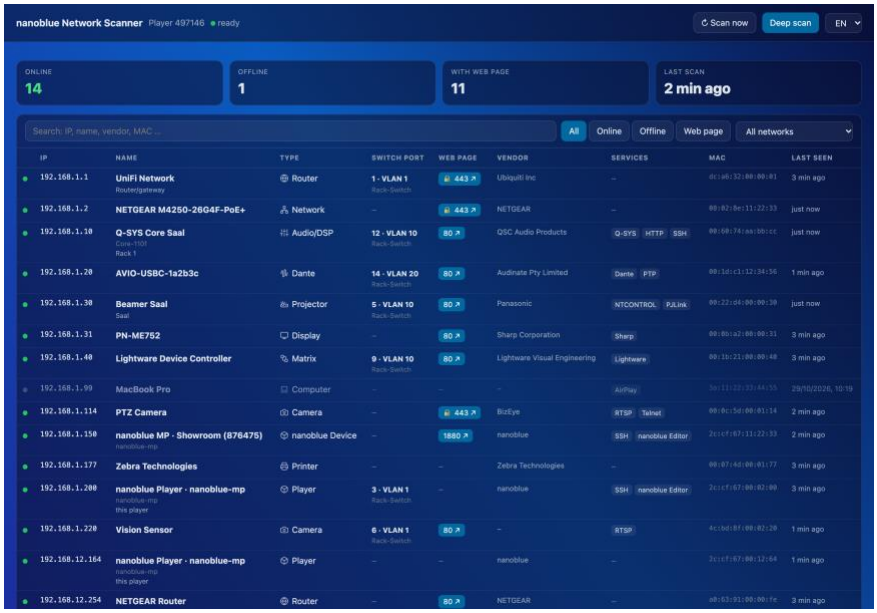
Leg	Protection
Browser → nanoblue cloud	HTTPS with a valid certificate (Let’s Encrypt), separate address per session (w01–w12.lan.nanoblue.cloud).
Cloud → player	WireGuard tunnel (encrypted, established by the player – so no open ports at the customer) plus a secret key per player.
Player → device	Only within the local network, only to devices from the scan list; encrypted device pages (HTTPS) are also accessed encrypted.

Protection layers

Level	Protection
Login	nanoblue portal with password and two-factor authentication (TOTP); only devices the user is enabled for.
Permissions	“Network Scanner” (view, scan) and “Network Scanner – Web access” (open device pages) are granted explicitly per user. Naming, watching and settings: admins only.
Web session	One-time link, valid for 2 minutes only; the session only works for the browser that requested it (bound to its IP address) and expires automatically.
Player	The scanner cannot be reached on the customer’s network – only via the encrypted connection to the nanoblue cloud and only with a secret key per device.
Targets	Only devices from the player’s own network found by the scan can be opened – no internet, no other networks.
Attacks	Unknown addresses are dropped silently, repeated attempts are throttled; one-time links (192 bit) and session keys (256 bit) cannot be guessed. A device page cannot trigger actions in the portal. Search engines and bots calling the addresses only get a notice page.
Credentials	Switch passwords stay on the player (readable only by the service) and are never shown again or sent to the cloud.
Session end	Automatically after 15 minutes without use or 8 hours; can be ended individually or all at once.
Traffic analysis	Listening only, headers only, nothing stored; the capture mode of the interface is ended automatically after the measurement.
Log	Every web session opened and ended, every PoE switching action, every traffic measurement and every clearing of events is logged with user, device and time.

For technicians on site: the LAN page

On the local network, the player shows the same list at http://<player-IP>:1880/netscan – without login, read-only, with a scan button. The links open the devices directly, without going through the cloud. The page also works without an internet connection and can be linked, e.g. in the dashboard or Interactive UI. Naming, watching and settings remain reserved for the portal.

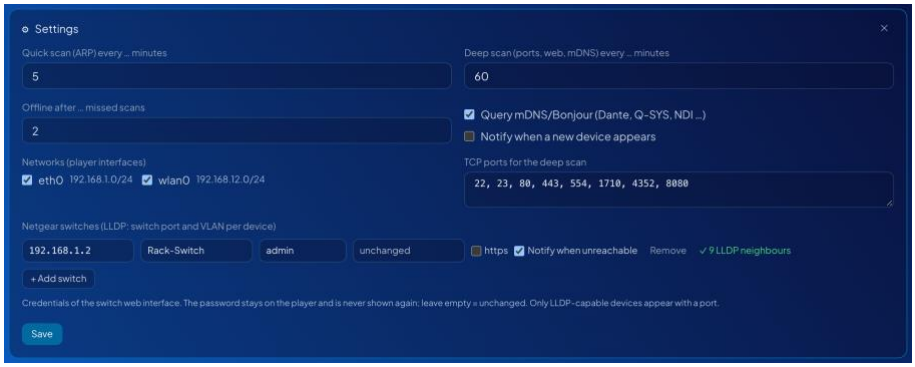


LAN page on the player: device list with direct links for the technician on site.

Settings and integration

- Interval of quick and deep scan, “offline” after how many missed scans, networks, ports queried, mDNS on/off, notice for new devices.

- Settings via the ⚙ button at the top of the page. Store Netgear switches with credentials; the password stays on the player and is never shown again. For each switch it is visible whether the query works and whether a failure is notified.
- Notifications via nanoblue Notify with a separate “Network Scanner” filter – can be switched on or off per recipient; the message contains device, room and a link straight to the scan page.
- Event list: the last 300 events are kept, admins can clear it.
- Own flows on the player (nanoblue Editor) receive all events – e.g. to show a message in the Interactive UI when a display fails.
- User interface in German, English and Spanish; light, dark and blue.



Scanner settings (admins only).

Typical applications

- Remote maintenance: configure a projector, DSP or switch at the customer site without travelling there and without a VPN at the customer.
- Commissioning and documentation: which devices with which IP and which services are on the network?
- Monitoring: notification when an important device fails – often before the customer notices.
- Remote restart: power-cycle a hung camera, access point or touch panel via PoE.
- Network check: PoE reserve, port load and transmission errors at a glance – before failures occur.
- Installation documentation: device list and port assignment including VLANs as PDF or Excel – up to date at any time.
- Stuttering picture, hanging controls: use the traffic analysis to find out within a minute whether the network is being flooded – and by whom.
- Troubleshooting: is the device on the network? Does it have a new IP? Since when has it been gone?

In preparation

Scan devices in further VLANs directly (second network address of the player) · switch port also for devices without LLDP (via SNMP) · history of PoE consumption and bandwidth · warning when the PoE budget is tight · automatic PoE restart of hung devices (self-healing) · maintenance windows without notifications.