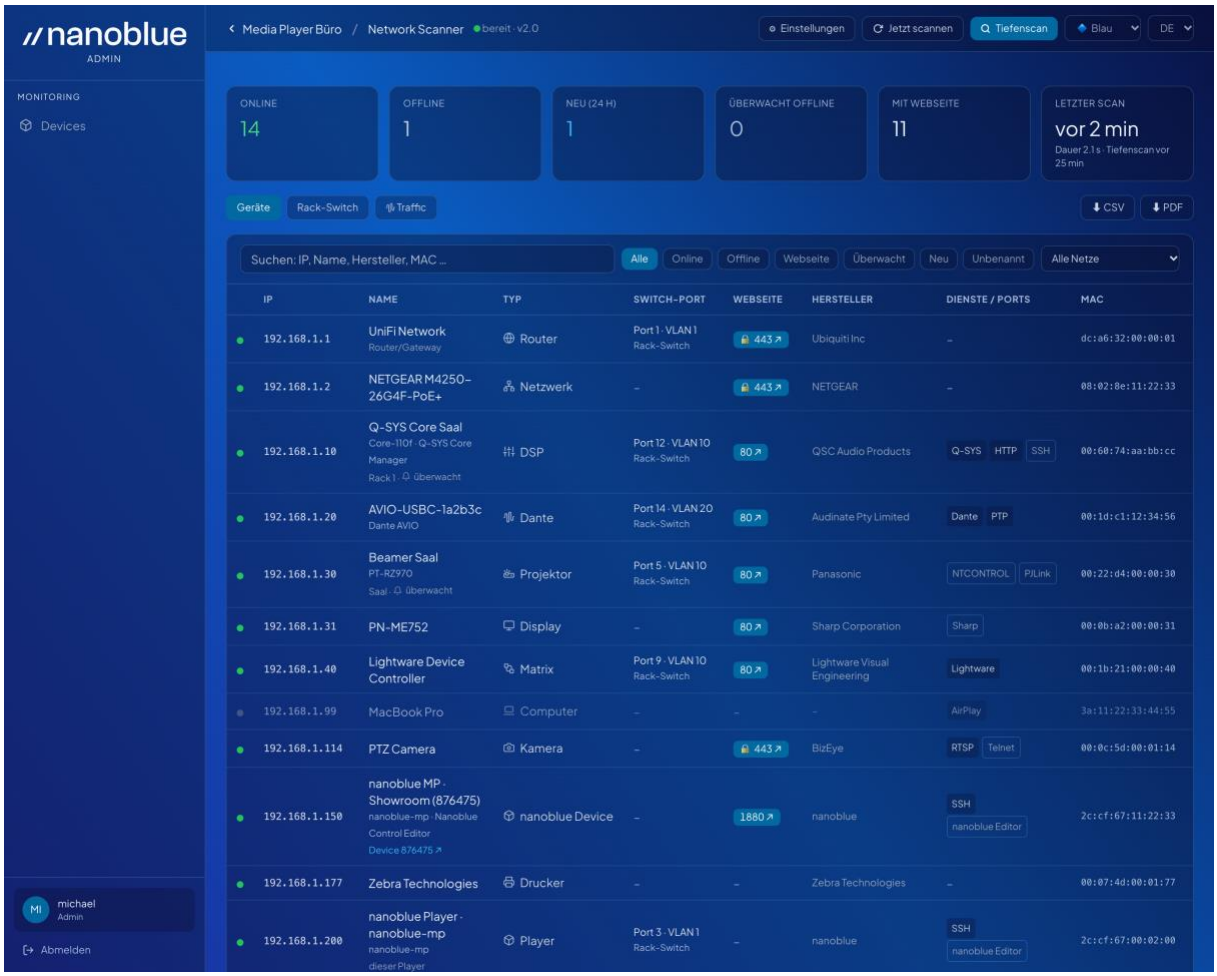
nanoblue® Network Scanner

Alle Geräte im Netzwerk sehen, überwachen und aus der Ferne konfigurieren – mit Switch-Ansicht und PoE-Steuerung, sicher über die nanoblue Cloud



Network Scanner im nanoblue Portal: Kennzahlen, Filter und die Geräteliste mit Typ, Webseite, Hersteller, Diensten und Zeitpunkt der letzten Sichtung.

Worum es geht

Jeder nanoblue-Mediaplayer kennt das Netzwerk, in dem er steht. Der Network Scanner nutzt das: Er findet alle Geräte in den lokalen Netzen des Players – Mediensteuerungen, DSPs, Dante-Geräte, Displays, Projektoren, Kameras, Switches, Router – und zeigt sie übersichtlich im nanoblue Portal an. Ohne Zusatzhardware, ohne Software beim Kunden und ohne Änderungen an der Firewall.

Besonders praktisch: Die Konfigurationsseiten der gefundenen Geräte lassen sich mit einem Klick direkt aus dem Portal öffnen – sicher über die verschlüsselte Verbindung des Players, als stünde man vor Ort im Netzwerk. Und für Techniker vor Ort gibt es dieselbe Liste auch direkt im lokalen Netz.

Mit einem Netgear-Switch kommen Port-Belegung, VLANs, PoE-Steuerung, Kabeltest und Port-Überwachung dazu – und die Traffic-Analyse findet heraus, wer das Netz flutet, wenn Bild oder Bedienung ruckeln.

Die wichtigsten Funktionen

Geräte automatisch finden und erkennen

- **Alle Netze des Players**: kabelgebunden und WLAN, jedes Netz einzeln ein- oder ausschaltbar.
- **Hersteller** aus der Netzwerkadresse (MAC) des Geräts.
- **Dienste** über Bonjour/mDNS: z. B. Dante, AES67, Q-SYS, NDI, NMOS, Lightware, AirPlay, Shelly.
- **Steuerschnittstellen** über offene Ports: z. B. PJLink, Q-SYS QRC, Yamaha RCP, Crestron, Extron, Telnet, RTSP.
- **Webseiten** der Geräte samt Seitentitel – oft steht dort schon das Modell, z. B. „NETGEAR M4250“ oder „Q-SYS Core Manager“.
- **Switch-Port und VLAN** je Gerät von Netgear-Switches (z. B. AV Line M4250) über LLDP – man sieht, an welchem Port ein Gerät hängt.
- **Eigene nanoblue-Geräte** werden automatisch erkannt (über die registrierte Netzwerkadresse) und mit Typ, Name und Device-ID angezeigt – statt als namenloses Gerät – mit Link direkt zur Geräteseite im Portal.
- **Gerätetyp** wird daraus automatisch abgeleitet (Router, Netzwerk, Audio/DSP, Dante, Display, Projektor, Kamera, Steuerung …) und lässt sich korrigieren.



Geräteliste: Status, IP, Name, Typ, Switch-Port und VLAN, Buttons zur Webseite (= verschlüsselt), Hersteller, Dienste, MAC und letzte Sichtung.

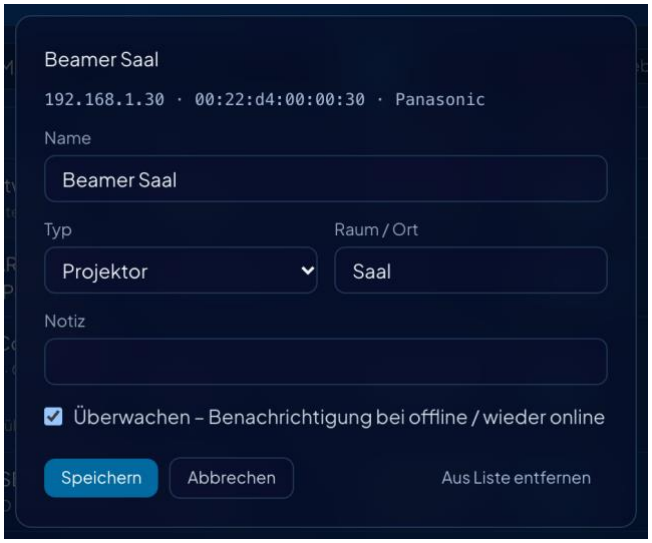
Sparsam im Betrieb

Scan	Wann	Was
Schnell-Scan	alle 5 Minuten (einstellbar)	Welche Geräte sind da? Dauer ca. 1–5 Sekunden.
Tiefenscan	stündlich, für neue Geräte sofort und per Button	Dienste, Steuerschnittstellen, Webseiten.

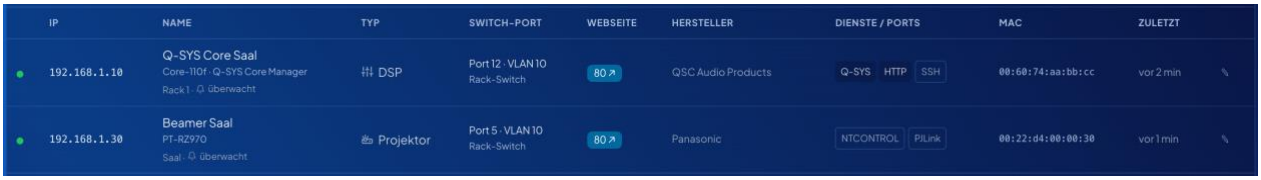
Der Scanner läuft als eigener, schlanker Dienst neben den übrigen Funktionen des Players und ist in Rechenzeit und Speicher fest begrenzt. Wiedergabe, Interactive UI und Steuerung bleiben davon unberührt.

Geräte benennen und überwachen

- Jedem Gerät einen Namen, Typ, Raum und eine Notiz geben – das Gerät wird über seine MAC-Adresse wiedererkannt, auch wenn sich die IP ändert.
- **Überwachen**: Fällt ein überwachtes Gerät aus, kommt eine Benachrichtigung über nanoblue Notify (Telegram, Browser-Push) – und eine Entwarnung, sobald es wieder da ist.
- Optional: Hinweis, sobald ein neues, unbekanntes Gerät im Netz auftaucht.
- Filter für Online, Offline, mit Webseite, überwacht, neu und unbenannt; Suche über alle Felder.



Gerät benennen und überwachen.



Filter „Überwacht“: die wichtigen Geräte einer Anlage auf einen Blick.

Ereignisse

Neue Geräte, Ausfälle, Wiederkehr und IP-Wechsel werden mit Zeitpunkt protokolliert. So lässt sich nachvollziehen, wann ein Gerät zuletzt im Netz war oder seit wann ein neues Gerät angeschlossen ist.

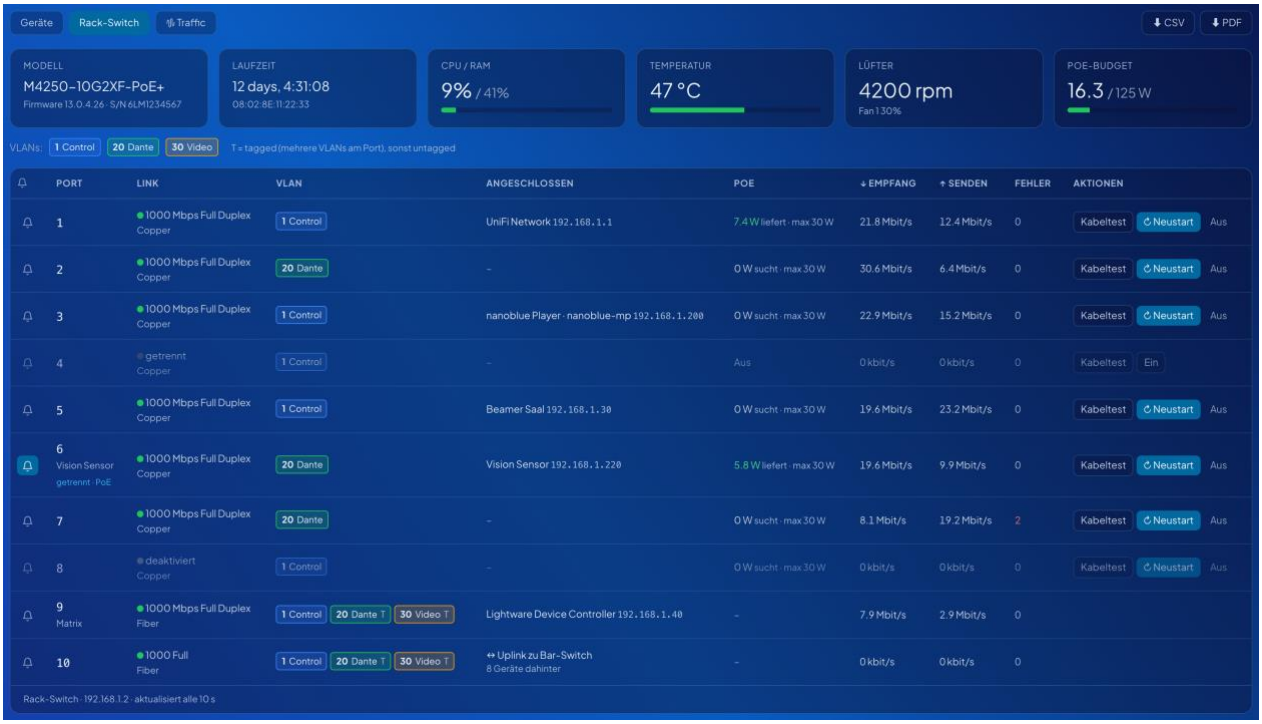
Switch-Ansicht mit PoE-Steuerung

Für hinterlegte Netgear-Switches (z. B. AV Line M4250) gibt es neben der Geräteliste einen eigenen Reiter. Er zeigt den Zustand des Switches und jedes Ports live – alle 10 Sekunden aktualisiert, solange die Ansicht offen ist. Im Hintergrund wird der Switch dafür nicht belastet.

- **Switch**: Modell, Firmware, Seriennummer, Laufzeit, CPU- und RAM-Auslastung, Temperatur, Lüfter.
- **PoE-Budget**: Verbrauch aller PoE-Geräte im Verhältnis zur verfügbaren Leistung – man sieht, ob noch Reserve für ein weiteres Gerät da ist.
- **Je Port**: Link und Geschwindigkeit, das angeschlossene Gerät aus der Geräteliste, PoE-Leistung in Watt mit Status und Grenze, aktuelle Bandbreite empfangen/senden sowie Übertragungsfehler.
- **VLANs**: je Port die VLANs in den Farben der Netgear-Oberfläche, gekennzeichnet als untagged oder tagged (T), dazu eine VLAN-Übersicht. So sieht man sofort, welche Geräte im Dante-, Video- oder Steuer-Netz hängen.
- **PoE schalten**: Port aus, ein oder Neustart (über die eingebaute Neustart-Funktion des Switches). So lassen sich hängende Kameras, Access Points, Touchpanels oder Player aus der Ferne neu starten, ohne dass

jemand vor Ort den Stecker ziehen muss. Nur für Admins, mit Rückfrage, die das angeschlossene Gerät nennt, und mit Eintrag im Protokoll.

- **Kabeltest**: der Switch misst das Kabel an einem Port und meldet „in Ordnung“, Unterbrechung, Kurzschluss oder Übersprechen – mit Entfernung zur Fehlerstelle in Metern. Ideal, wenn ein Port langsamer läuft oder Fehler meldet. Nur für Admins, mit Rückfrage (der Port ist dabei einige Sekunden getrennt).



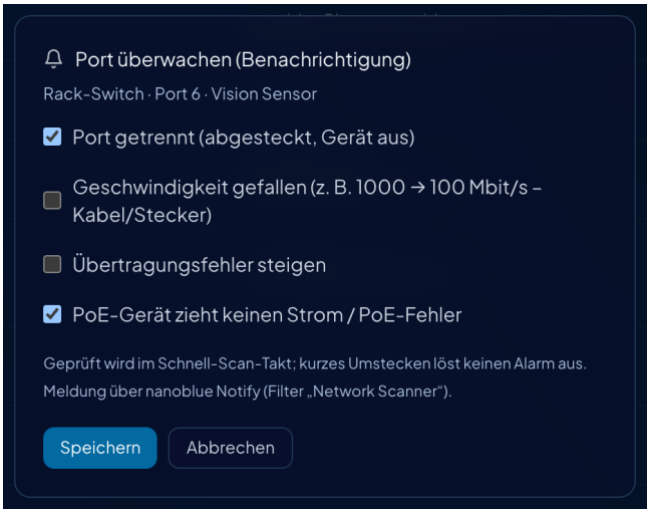
Switch-Ansicht: Zustand des Switches, PoE-Budget, VLANs und je Port Link, VLAN, angeschlossenes Gerät, PoE-Leistung, Bandbreite, Überwachung und PoE-Buttons.

Switch und Ports überwachen

Wichtige Ports lassen sich einzeln überwachen (Glocken-Button in der Switch-Ansicht). Gemeldet wird über nanoblue Notify – mit Switch, Port und angeschlossenem Gerät, jeweils mit Entwarnung:

Überwachung	Meldung, wenn …
Switch erreichbar	der Switch nicht mehr antwortet oder die Anmeldung scheitert (Haken je Switch in den Einstellungen)
Port getrennt	ein Kabel abgesteckt oder das Gerät ausgeschaltet wurde
Geschwindigkeit	der Port langsamer läuft als sonst, z. B. 100 statt 1000 Mbit/s – typisch für ein beschädigtes Kabel oder einen schlechten Stecker
Übertragungsfehler	die Fehler an einem Port steigen – ein Hinweis auf Kabelprobleme, bevor es zum Ausfall kommt
PoE	ein PoE-Gerät keinen Strom mehr zieht oder der Port einen PoE-Fehler meldet

Geprüft wird im Takt des Schnell-Scans. Kurzes Umstecken löst keinen Alarm aus – erst wenn der Zustand bei zwei Prüfungen hintereinander besteht.



Port überwachen: was gemeldet werden soll, wählt man je Port.

Dokumentation exportieren

Mit den Buttons ⬇ CSV und ⬇ PDF über der Liste lässt sich der aktuelle Stand jederzeit festhalten – die Geräteliste (mit den gesetzten Filtern) oder die Ports eines Switches:

- **CSV**: öffnet sich direkt in Excel – IP, Name, Typ, Raum, Hersteller, MAC, Dienste, Webseiten, Switch-Port, VLAN, Überwachung, zuletzt gesehen bzw. je Port Link, VLAN, Gerät, PoE und Bandbreite.
- **PDF**: übersichtliche Tabelle im Querformat mit Datum und Player – ideal als Anlagendokumentation bei Übergabe oder Wartung.

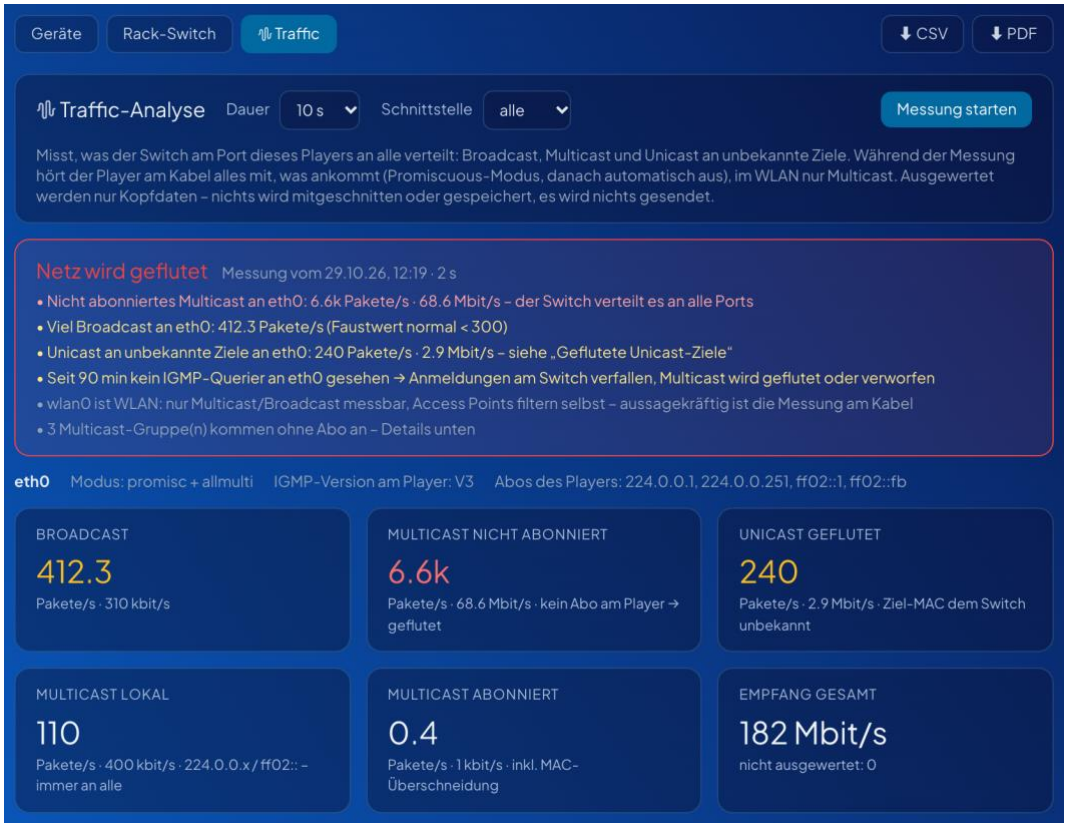
Traffic-Analyse: Wer flutet das Netz?

Bildprozessoren, Matrizen und Displays reagieren empfindlich, wenn der Switch zu viel Verkehr an alle Ports verteilt – das Bild ruckelt, Bedienungen hängen, Geräte sind kurz nicht erreichbar. Die Traffic-Analyse misst genau diesen Verkehr am Port des Players und zeigt, wer ihn verursacht und warum. Mit dem Button „Messung starten" im Reiter „Traffic" läuft eine Messung über 10, 30, 60 oder 120 Sekunden – am besten, während das Problem auftritt.

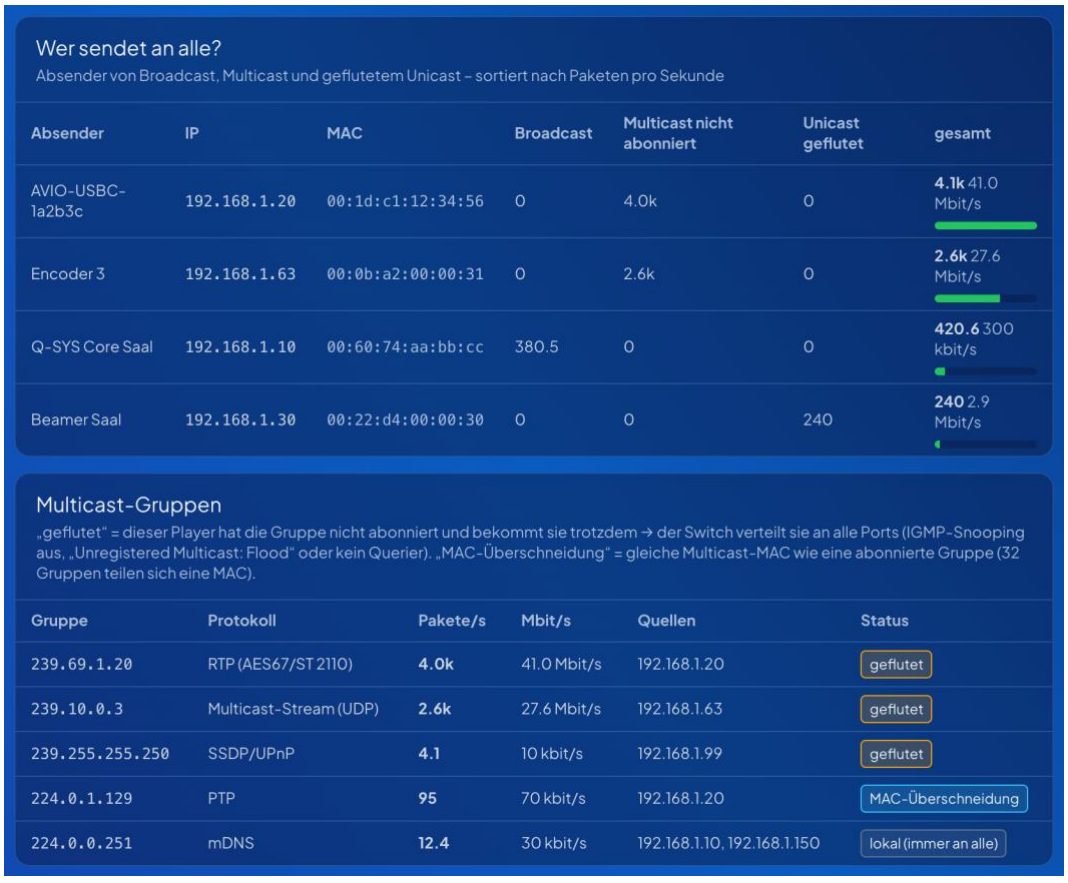
Messwert	Bedeutung
Broadcast	Pakete an alle (ARP, DHCP, Geräte-Suche). Faustwert: unter 300 Pakete/s unauffällig.
Multicast nicht abonniert	Streams (Video, Audio, Dante/AES67 …), für die sich der Player nicht angemeldet hat. Kommen sie trotzdem an, verteilt der Switch sie an alle Ports – die häufigste Ursache für ein „geflutetes" AV-Netz.
Unicast geflutet	Pakete an ein bestimmtes Gerät, dessen Adresse der Switch nicht kennt – er schickt sie deshalb überallhin. Typisch bei Geräten, die nur empfangen (z. B. Stream-Ziele).
Multicast lokal	Steuerverkehr, den jeder Switch an alle schickt (mDNS, IGMP, Geräte-Ankündigungen). Nur auffällig, wenn er stark ansteigt.
IGMP-Querier	Der Switch oder Router, der regelmäßig nachfragt, wer welchen Stream will. Fehlt er, verfallen die Anmeldungen nach einigen Minuten und Multicast wird an alle geflutet. Der Player beobachtet das dauerhaft.

- Ampel mit Befunden im Klartext, z. B. „Nicht abonniertes Multicast: 6.600 Pakete/s · 69 Mbit/s – der Switch verteilt es an alle Ports" oder „Seit 90 min kein IGMP-Querier gesehen".
- „Wer sendet an alle?": die lautesten Absender mit Gerätenamen aus der Scan-Liste – so ist der Verursacher sofort gefunden.
- Multicast-Gruppen mit Quelle, Paketen und Bandbreite und dem Status „geflutet", „abonniert", „lokal" oder „MAC-Überschneidung"; dazu die gefluteten Unicast-Ziele und alle Protokolle.
- Export als CSV oder PDF – als Nachweis für den Kunden oder den Netzwerk-Verantwortlichen.

- Datenschutz: Der Player hört nur zu und sendet nichts. Ausgewertet werden nur die Kopfdaten (Absender, Ziel, Protokoll), keine Inhalte; nichts wird mitgeschnitten oder gespeichert. Jede Messung wird mit Benutzer und Zeitpunkt protokolliert.



Traffic-Analyse: Ampel mit Befunden und die Messwerte je Netzwerk-Anschluss.



Wer sendet an alle, und welche Multicast-Gruppen werden geflutet?

Geräte-Webseiten über die Cloud öffnen

Ein Klick auf „80 ↗“ oder „🔒 443 ↗“ öffnet die Konfigurationsseite des Geräts in einem neuen Browser-Tab – vom Büro, von unterwegs oder vom Smartphone aus. Die Verbindung läuft verschlüsselt über den Player; im Netz des Kunden muss dafür nichts freigegeben werden.

- Bis zu 12 Web-Sitzungen gleichzeitig; Übersicht der offenen Sitzungen mit „Beenden“ und „Alle beenden“.
- Sitzungen enden automatisch nach 15 Minuten ohne Nutzung, spätestens nach 8 Stunden.
- Wird dasselbe Gerät erneut geöffnet, bleiben Anmeldung und Zwischenspeicher am Gerät erhalten – die Seite öffnet sich in wenigen Sekunden.



Ereignisse und offene Web-Sitzungen.

Sicherheit

Der Zugriff auf Geräte im Kundennetz ist sensibel. Deshalb gilt: ohne Anmeldung kein Zugang – auf keiner Ebene. Der Network Scanner ist so gebaut, dass im Netz des Kunden kein Port geöffnet und keine Firewall-Regel geändert werden muss.

So läuft eine Verbindung

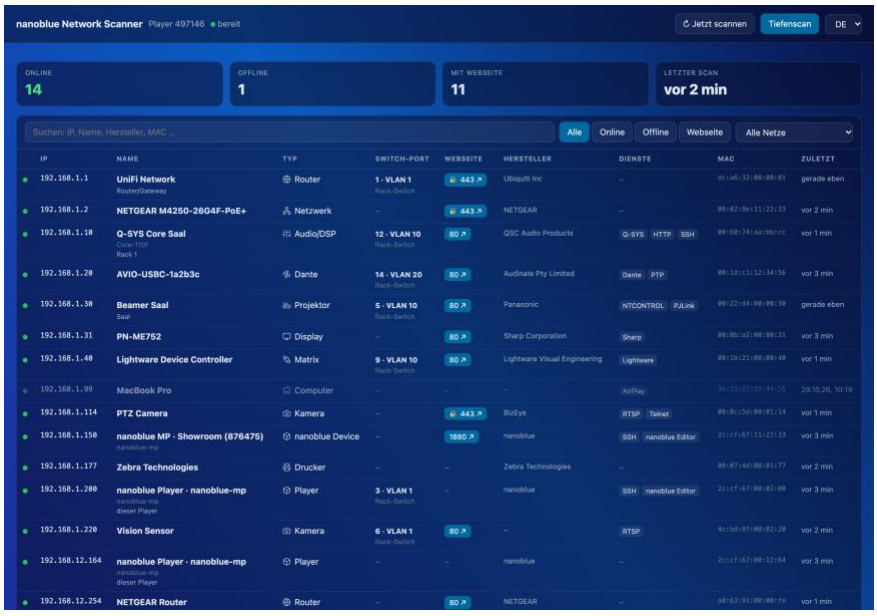
Strecke	Schutz
Browser → nanoblue Cloud	HTTPS mit gültigem Zertifikat (Let’s Encrypt), eigene Adresse je Sitzung (w01–w12.lan.nanoblue.cloud).
Cloud → Player	WireGuard-Tunnel (verschlüsselt, vom Player aus aufgebaut – daher keine offenen Ports beim Kunden) plus geheimer Schlüssel je Player.
Player → Gerät	Nur innerhalb des lokalen Netzes, nur zu Geräten aus der Scan-Liste; verschlüsselte Geräteseiten (HTTPS) werden auch verschlüsselt angesprochen.

Schutzebenen

Ebene	Schutz
Anmeldung	nanoblue Portal mit Passwort und Zwei-Faktor-Authentifizierung (TOTP); nur Geräte, für die der Benutzer freigeschaltet ist.
Rechte	„Network Scanner“ (ansehen, scannen) und „Network Scanner – Web-Zugriff“ (Geräteseiten öffnen) werden je Benutzer ausdrücklich vergeben. Benennen, Überwachen und Einstellungen: nur Admins.
Web-Sitzung	Einmal-Link, nur 2 Minuten gültig; die Sitzung gilt nur für den Browser, der sie angefordert hat (an seine IP-Adresse gebunden), und läuft automatisch ab.
Player	Der Scanner ist im Kundennetz nicht erreichbar – nur über die verschlüsselte Verbindung zur nanoblue Cloud und nur mit einem geheimen Schlüssel je Gerät.
Ziele	Geöffnet werden können nur Geräte aus dem eigenen Netz des Players, die der Scan gefunden hat – kein Internet, keine anderen Netze.
Angriffe	Unbekannte Adressen werden wortlos abgewiesen, wiederholte Versuche gebremst; Einmal-Links (192 Bit) und Sitzungsschlüssel (256 Bit) sind nicht zu erraten. Eine Geräteseite kann keine Aktionen im Portal auslösen. Suchmaschinen und Bots, die die Adressen abrufen, bekommen nur eine Hinweisseite.
Zugangsdaten	Switch-Passwörter bleiben auf dem Player (nur für den Dienst lesbar) und werden nie wieder angezeigt oder an die Cloud übertragen.
Sitzungsende	Automatisch nach 15 Minuten ohne Nutzung bzw. 8 Stunden; einzeln oder alle auf einmal beendbar.
Traffic-Analyse	Nur Zuhören, nur Kopfdaten, nichts gespeichert; der Mitschnitt-Modus des Anschlusses wird nach der Messung automatisch beendet.
Protokoll	Jede geöffnete und beendete Web-Sitzung, jede PoE-Schaltung, jede Traffic-Messung und jedes Leeren der Ereignisse wird mit Benutzer, Gerät und Zeitpunkt protokolliert.

Für Techniker vor Ort: die LAN-Seite

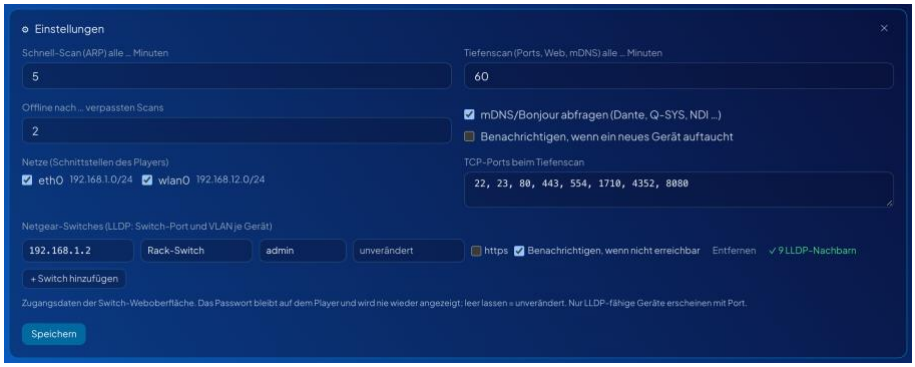
Im lokalen Netz zeigt der Player dieselbe Liste unter http://<Player-IP>:1880/netscan – ohne Anmeldung, nur zum Lesen, mit Scan-Button. Die Links öffnen die Geräte direkt, ohne Umweg über die Cloud. Die Seite funktioniert auch ohne Internetverbindung und lässt sich z. B. im Dashboard oder Interactive UI verlinken. Benennen, Überwachen und Einstellungen bleiben dem Portal vorbehalten.



LAN-Seite am Player: Geräteliste mit Direkt-Links für den Techniker vor Ort.

Einstellungen und Einbindung

- Intervall von Schnell- und Tiefenscan, „offline“ nach wie vielen verpassten Scans, Netze, abgefragte Ports, mDNS an/aus, Hinweis bei neuen Geräten.
- Einstellungen über den Button ⚙ oben auf der Seite. Netgear-Switches mit Zugangsdaten hinterlegen; das Passwort bleibt auf dem Player und wird nie wieder angezeigt. Pro Switch ist sichtbar, ob die Abfrage klappt, und ob bei Ausfall benachrichtigt wird.
- Benachrichtigungen über nanoblue Notify mit eigenem Filter „Network Scanner“ – je Empfänger ein- oder ausschaltbar; die Meldung enthält Gerät, Raum und einen Link direkt zur Scan-Seite.
- Ereignisliste: die letzten 300 Ereignisse werden gespeichert, Admins können sie leeren.
- Eigene Abläufe am Player (nanoblue Editor) erhalten alle Ereignisse – z. B. um bei Ausfall eines Displays eine Meldung im Interactive UI zu zeigen.
- Oberfläche in Deutsch, Englisch und Spanisch; Hell, Dunkel und Blau.



Einstellungen des Scanners (nur Admins).

Typische Einsätze

- Fernwartung: Projektor, DSP oder Switch beim Kunden konfigurieren, ohne hinzufahren und ohne VPN beim Kunden.
- Inbetriebnahme und Dokumentation: welche Geräte mit welcher IP und welchen Diensten sind im Netz?
- Überwachung: Benachrichtigung, wenn ein wichtiges Gerät ausfällt – oft bevor der Kunde es bemerkt.
- Neustart aus der Ferne: hängende Kamera, Access Point oder Touchpanel per PoE aus- und wieder einschalten.
- Netzwerk-Kontrolle: PoE-Reserve, Port-Auslastung und Übertragungsfehler auf einen Blick – bevor es zu Ausfällen kommt.
- Anlagendokumentation: Geräteliste und Port-Belegung samt VLANs als PDF oder Excel – jederzeit aktuell.
- Ruckelndes Bild, hängende Bedienung: mit der Traffic-Analyse in einer Minute klären, ob das Netz geflutet wird – und von wem.
- Fehlersuche: Ist das Gerät im Netz? Hat es eine neue IP? Seit wann ist es weg?

In Vorbereitung

Geräte in weiteren VLANs direkt scannen (zweite Netzwerk-Adresse des Players) · Switch-Port auch für Geräte ohne LLDP (über SNMP) · Verlauf von PoE-Verbrauch und Bandbreite · Warnung bei knappem PoE-Budget · automatischer PoE-Neustart hängender Geräte (Selbstheilung) · Wartungsfenster ohne Meldungen.