

ix.watch Privacy

Version 1.0, in effect from 13 October 2026. The current version is at <https://ix.watch/privacy>.

ix.watch publishes what networks send onto IXP peering LANs. That's mostly about routers, not people, but some of it can be personal data, and so can what we keep about visitors and alert subscribers. This page says what, why and for how long.

Who we are

ix.watch is run by Bouwhuis IT, Piet Heinstraat 12, 7511 JE Enschede, the Netherlands (KvK 64554643). We decide what is collected and why, which makes us the controller under the GDPR. For anything on this page, mail privacy@ix.watch.

What we publish about networks

Our captures, and the sensors other networks run for us, see the broadcast and multicast frames that reach every port on a peering LAN. When a frame is something that shouldn't be there, we record its sender as a source: one MAC address on one IXP. For each source we publish:

- the IXP, the MAC address and the device vendor that MAC belongs to;
- the network it belongs to: its AS number, its name, and its peering IP addresses on that LAN;
- what it sent and how often, with first and last times;
- the decoded headers of its last few frames, such as addresses, ports and advertised IPv6 prefixes;
- the raw frames themselves, as a pcap: up to five per source, each up to 1,600 bytes, payload included. Depending on the protocol, a frame can carry a device's name, model, software version or management address, a DHCP client's hostname, or a Synching device ID.

We tie a MAC to a network using the IXP's member list (its IX-F export), PeeringDB, the routers' own neighbour tables and bgp.tools. Names come from PeeringDB and bgp.tools. Sources we can't tie to a network aren't listed: the public pages only count them. Someone who searches for a source's exact MAC address sees its IXP, vendor, what it sent, how often and when, on a page search engines are asked not to index, but not its IP addresses or frames. The operators of that IXP can see all of it once they log in, so they can track them down.

Most of this is about companies' equipment. But some AS numbers belong to individuals, whose network name is often their own name, and a workstation bridged onto the LAN can give away its user's hostname. That makes some of it personal data.

Why

Stray traffic on a peering LAN costs every member's router work, can leak details an attacker would like, and now and then breaks the LAN. Publishing who sends it, live and with the frames to prove it, lets networks see and fix their own, and lets IXPs and their members hold each other to the rules. That is our legitimate interest (GDPR article 6(1)(f)). We keep it to what that needs: only

what a network sends onto a shared LAN, where every other member receives it anyway, and only for as long as it is current.

How long

A source drops off the site and the API 7 days after its last frame, with its frames and pcap. Hourly counts of frames per source stay in our metrics store for 6 months. What others copied from the public API while it was up is out of our hands.

Mailing a network

We sometimes mail a network about what it sends. We find its contact in the RIPE database (its abuse or e-mail contact) and write from an address that forwards replies to us. We keep that correspondence for 2 years.

Visiting ix.watch

- **No cookies** on ix.watch, and nothing kept in your browser's storage.
- **Statistics.** We count visits with [Umami](#), which we host ourselves. It records the page, where you came from, your browser, operating system, device type and country, and a few clicks (on the tip buttons and the alerts link). It sets no cookies and doesn't store your IP address. Our interest: knowing which pages are used.
- **Server logs.** Our web servers and the API log each request: your IP address, the time, the page asked for, the referrer and your browser. We use them to keep the service running and to deal with abuse, and keep them for 30 days.
- **PeeringDB, straight from your browser.** The search box, the network pages and the IXP pages ask [PeeringDB](#) directly, so PeeringDB sees your IP address and what you search for. Its [policies](#) apply to that.
- **Fonts and scripts** come from our own servers.

Alerts

To set up alerts for your network or IXP you log in at alerts.ix.watch with your PeeringDB account. From PeeringDB we receive your PeeringDB ID, name, e-mail address, whether it's verified, and the networks, organisations and IXPs you may act for. We use that to let you in and to check which networks you may set up alerts for. A cookie keeps you logged in for 8 hours; a second one lasts 10 minutes while you log in.

For each network or IXP with alerts we keep:

- who set it up (your PeeringDB ID) and its settings;
- up to five addresses that get the mail, and whether each has confirmed;
- which of its sources we've mailed about, and when we sent what.

We need these to send the alerts you asked for (article 6(1)(b), a contract with you). We send them from our own mail server. Every mail has an unsubscribe link that works in one click. Replies to

alerts reach us through our own mail forwarding. Unsubscribing deletes the address at once. An address nobody confirms within 30 days is deleted. When alerts end, because you turned them off or a subscription ran out unpaid, we delete the subscription, its addresses and the record of what we sent 12 months later, and the log of what we sent keeps 12 months in any case. Stripe keeps its own payment records, as the law requires of it.

Paying

Alerts for networks that aren't personal are paid; tips are optional. Both go through [Stripe](#). We give Stripe your e-mail address and the AS number; Stripe collects your payment details, address and, in the EU, VAT number. We never see your card. We keep a link to your Stripe customer and how long you've paid for, and we keep invoices for 7 years because Dutch tax law requires it. Outside the EU, Stripe sells the subscription to you as the merchant of record, under [its own privacy policy](#).

Running a sensor

If you run a sensor for us, we keep its account, the IXPs it may report on, the name we credit it to on the site, and the IP addresses it connects from. Its frames are handled as above. Stop the sensor and mail us, and we take its IXP off the site and delete its account.

Who else gets it

What's on the site and the API is public by design: anyone can read and copy it. Beyond that we share personal data only with Stripe, for payments, and with authorities when the law makes us. We don't sell it and don't use it for advertising. We run the site, the API, the alerts, the database and mail on our own servers in the Netherlands. Stripe and PeeringDB are based in the United States. Stripe transfers data under the EU's standard contractual clauses and the EU-US Data Privacy Framework.

Your rights

You can ask us what we hold about you, and have it corrected or deleted. You can also have its use restricted, get a copy, or object to how we use it. Mail privacy@ix.watch. We answer within a month.

If something we publish names you, or wrongly ties a source to your network, tell us and we'll correct or remove it. Because the listing exists to show what networks send, we may keep listing a network's equipment while it keeps sending. If you think we've got it wrong, you can complain to the Dutch data protection authority, the [Autoriteit Persoonsgegevens](#), or to the one where you live.

Changes

When we change how we use personal data, we change this page and its date first. We mail alert subscribers about any change that affects them.