IXpect

Continuously monitor (your) IX peering LANs.

Marcel

Tassilo

Thomas

ixpect.net 2025-10-28

DD-IX Keep Local Traffic Local

Agenda

DD-IX & Our Challenges

Design & Deployment

Probes & Notifiers

Discussion & Outlook

DD-IX’s Challenges

- Community IX
- Dresden, Germany
- 2023–10 – founding
- 2024–11 – in operations
- 9 active + 3 future peers

DD-IX’s Challenges

- Community IX
- Dresden, Germany
- 2023–10 – founding
- 2024–11 – in operations
- 9 active + 3 future peers

✓ declarative operated IXP with two PoPs

✓ hardened switch port config engaged

IXpect

DD-IX's Challenges

- Community IX
- Dresden, Germany
- 2023-10 – founding
- 2024-11 – in operations
- 9 active + 3 future peers

✓ declarative operated IXP with two PoPs

✓ hardened switch port config engaged

– supervise IXP LAN hygiene

IXpect

Design

IXpect

Inspirations

arpwatch & ndmon

IXP-Watch*

arpsponge*

proxy ARP detection**

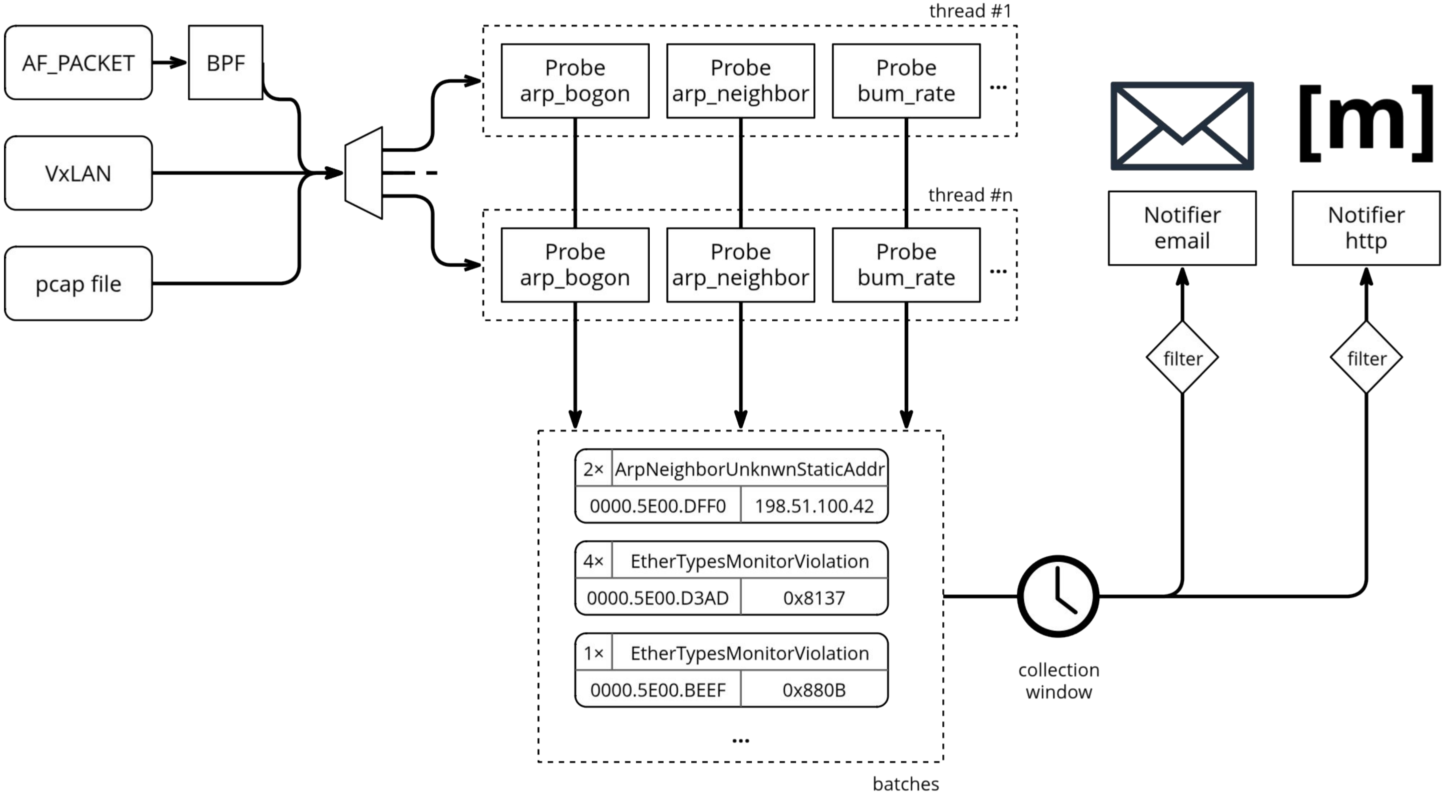
*) no feature parity
**) requires additional probe script

Principals

- safety & security comes first
  - inspected packets are not trustworthy
  - work passive, only – IXpect cannot send packages into the peering LAN

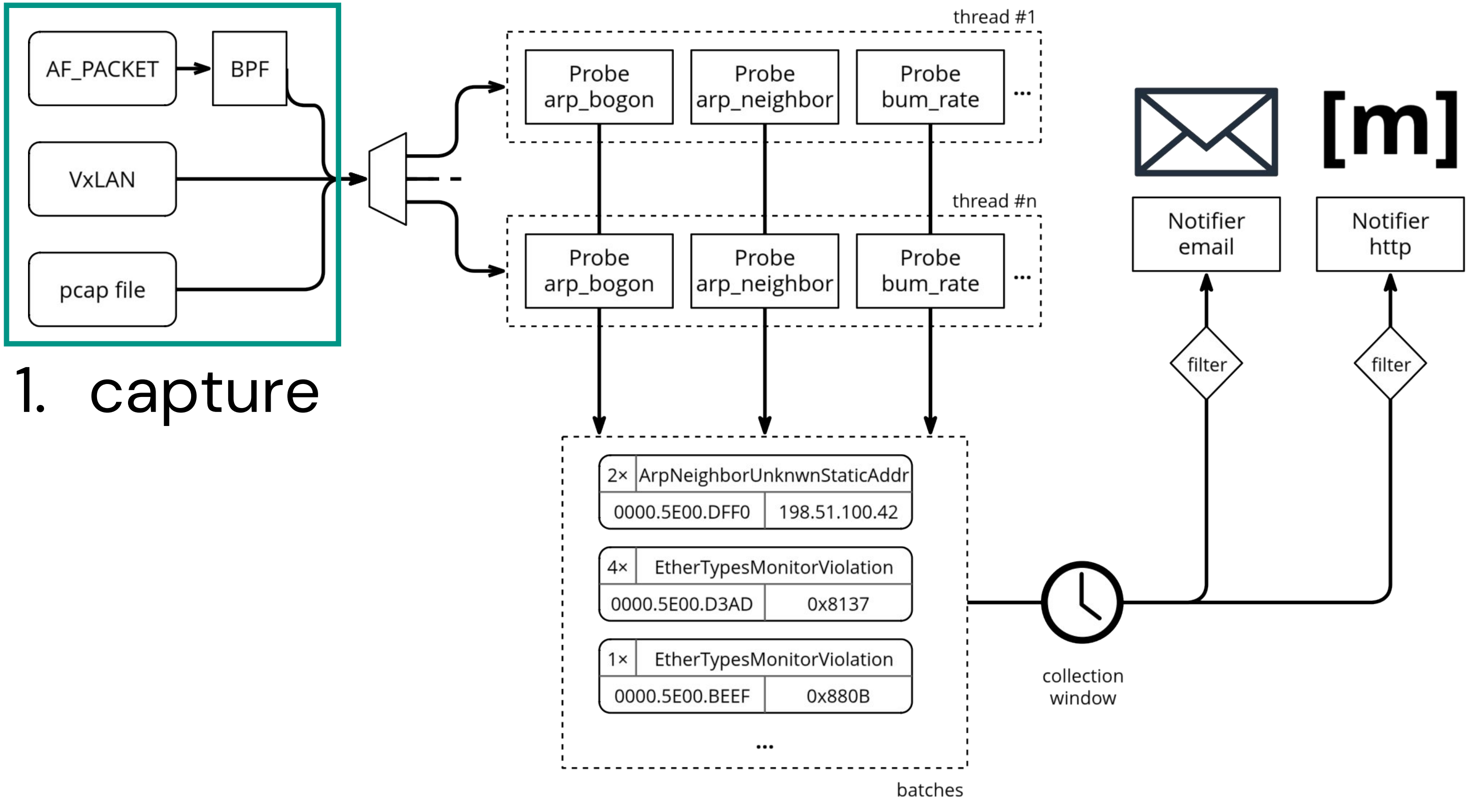
- safety & security is hard
  - never leak any traffic into/from the management network
  - hard isolation makes security more easy

Architecture



IXpect

Architecture



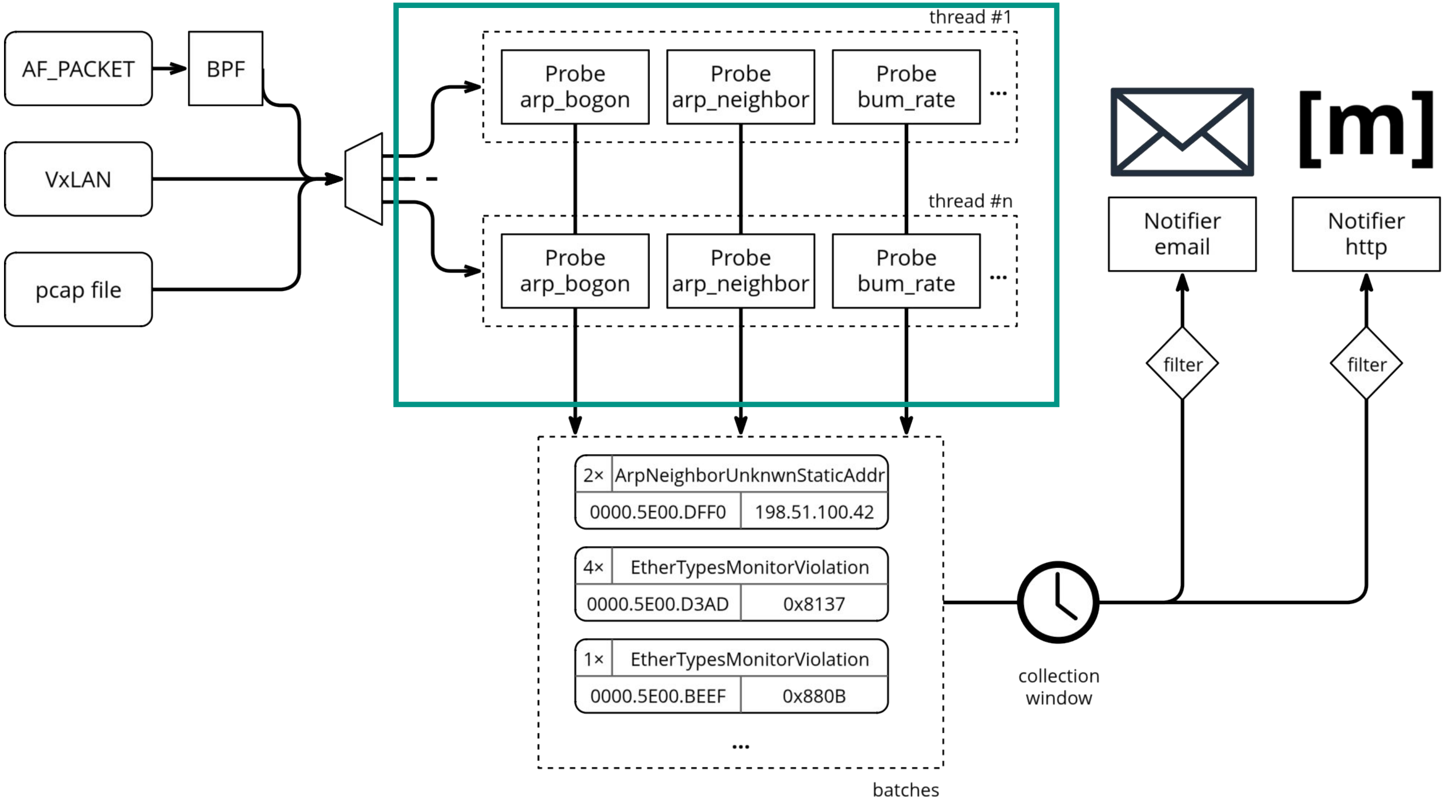
2×	ArpNeighborUnknwnStaticAddr	
0000.5E00.DFF0	198.51.100.42	
4×	EtherTypesMonitorViolation	
0000.5E00.D3AD	0x8137	
1×	EtherTypesMonitorViolation	
0000.5E00.BEEF	0x880B	

...

1. capture

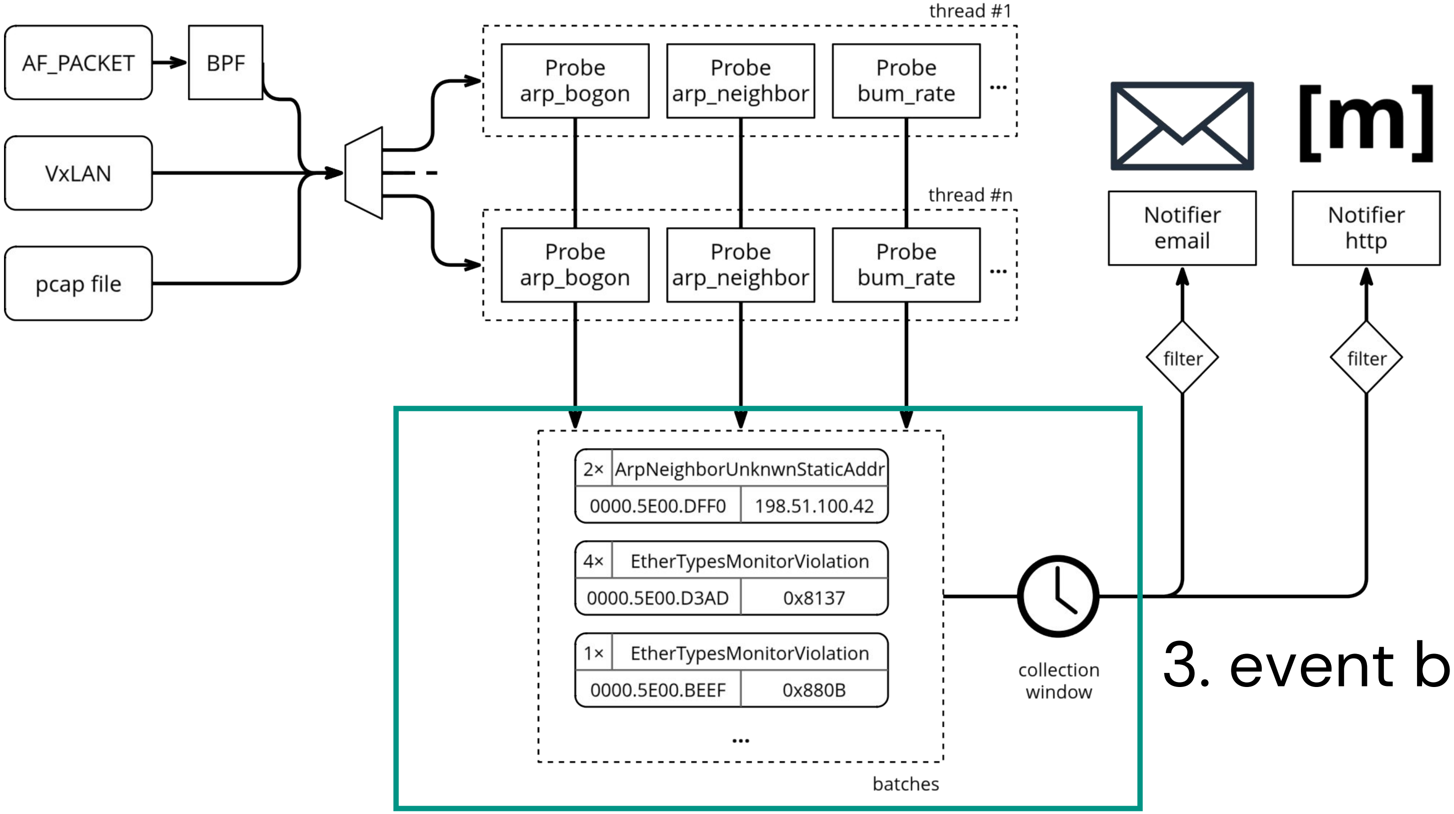
Architecture

2. event creation



IXpect

Architecture



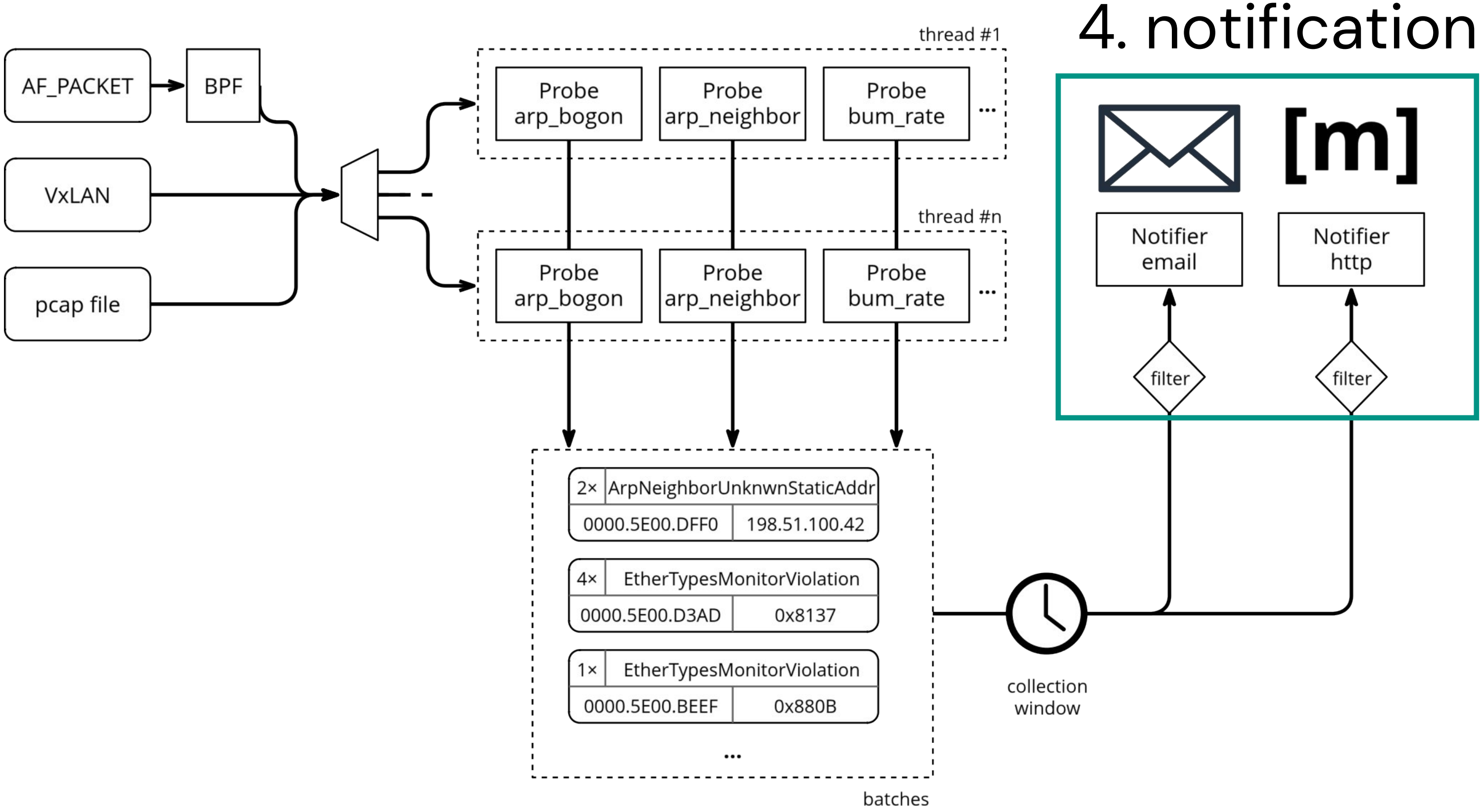
2×	ArpNeighborUnknwnStaticAddr
0000.5E00.DFF0	198.51.100.42
4×	EtherTypesMonitorViolation
0000.5E00.D3AD	0x8137
1×	EtherTypesMonitorViolation
0000.5E00.BEEF	0x880B

3. event batching

IXpect

Architecture

4. notification



2×	ArpNeighborUnknwnStaticAddr
0000.5E00.DFF0	198.51.100.42
4×	EtherTypesMonitorViolation
0000.5E00.D3AD	0x8137
1×	EtherTypesMonitorViolation
0000.5E00.BEEF	0x880B

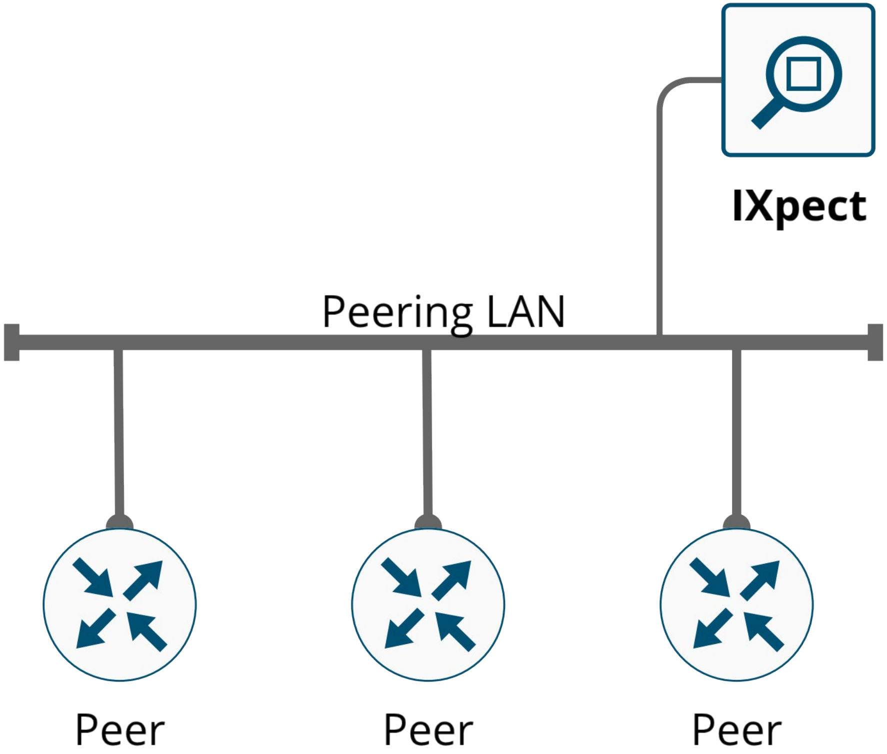
Deployment

https://ixpect.net/0.1/setup/

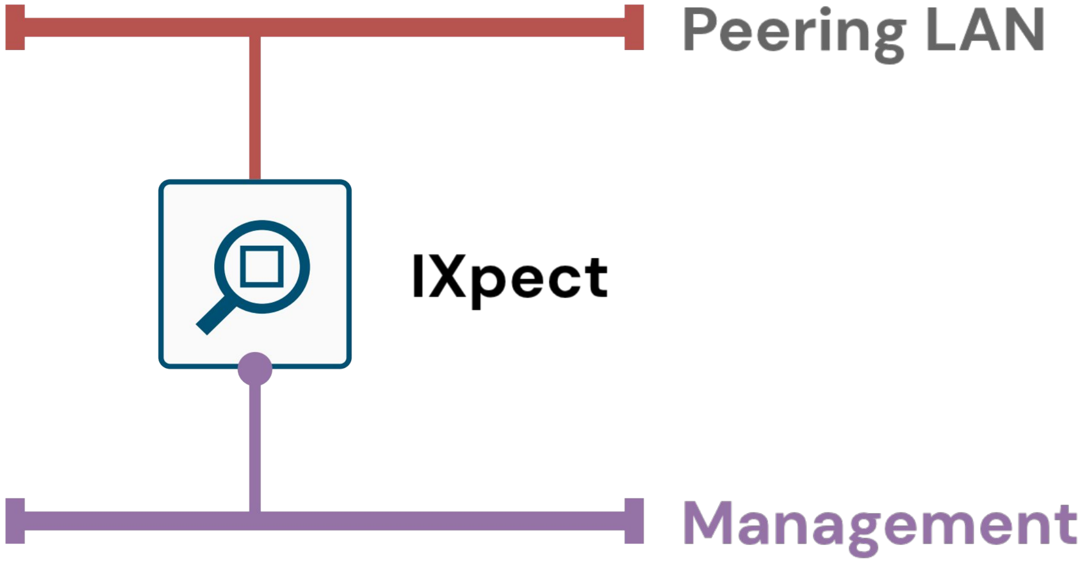
Deployment

IXpect **passivly** monitors on a generic peering port

alternative sources like VxLAN or pcap files are also supported

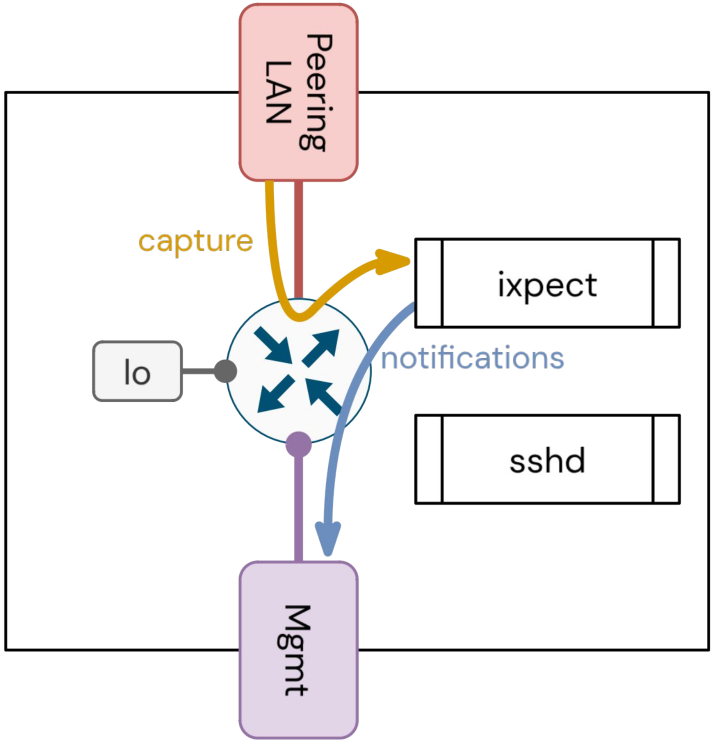


Deployment AF_PACKET



Deployment AF_PACKET

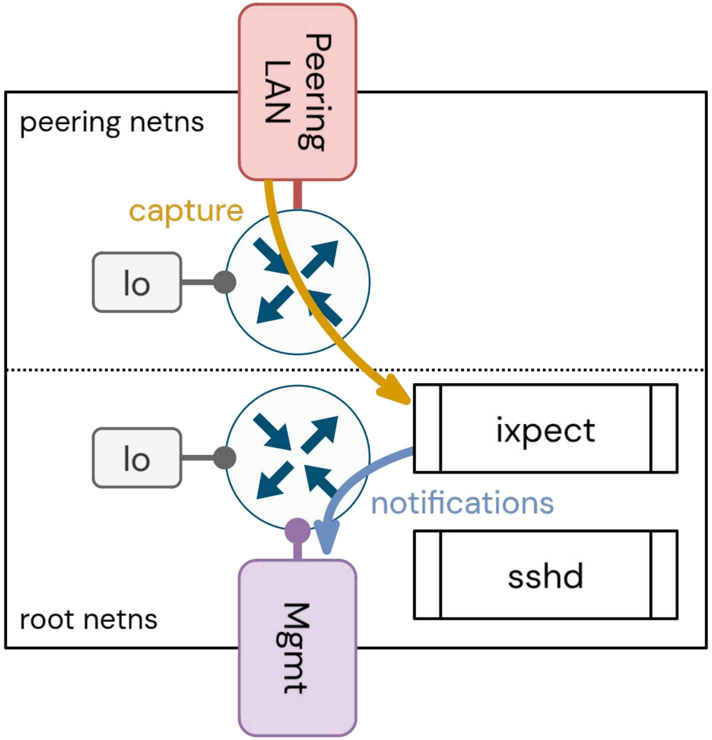
- No traffic nor ARP leaks?



IXpect

Deployment AF_PACKET

- No traffic nor ARP leaks!
- Isolation through network namespaces (netns).



IXpect

Deployment VxLAN

- IXpect can decap and inspect packets from VxLAN natively
- can be used with IMET routes in EVPN to inspect BUM traffic

Probes

https://ixpect.net/0.1/probes/

arp_bogon

Monitors ARP requests for IP addresses in non-whitelisted networks.

```
probes:
  arp_bogon:
    enable: true
    prefixes:
    - 192.0.2.0/24
```

Events

ARP_BOGON_SOURCE

ARP_BOGON_TARGET

arp_neighbor

Monitors the resolutions of IP addresses to MAC addresses.

```
probes:
  arp_neighbor:
    enable: true
    dynamic_enable: true
    static_resolutions:
    - ip: 192.0.2.1
      mac: 00:00:5e:00:53:01
    - ip: 192.0.2.42
      mac: 00:00:5e:00:53:2a
```

Events

ARP_NEIGHBOR_NEW_DYNAMIC

ARP_NEIGHBOR_SPOOFED_DYNAMIC

ARP_NEIGHBOR_SPOOFED_STATIC

ARP_NEIGHBOR_UNKNOWN

bum_rate

Monitors for BUM packet rates of individual source mac addresses.

Events

BUM_RATE_BROADCAST_EXCEEDED

BUM_RATE_MULTICAST_EXCEEDED

BUM_RATE_UNICAST_EXCEEDED

```
probes:
  bum_rate:
    enable: true
    window: 15s
    # absolute packet thresholds
    # by type within `window`
    thresholds:
      broadcast: 500
      multicast: 500
      unicast: 500
```

IXpect

ether_type

Monitors ethernet frames for packets with not allowed EtherTypes.

```
probes:
  ether_type:
    enable: true
    allowed_ether_types:
     - 0x0800 # IPv4
     - 0x0806 # ARP
     - 0x86dd # IPv6
```

Events

```
ETHER_TYPE_VIOLATION
```

IXpect

ipv6_bogon

Monitors for IPv6 packets from sources outsite the connected-networks and ICMPv6 packets with target address to unconnected-networks.

```
probes:
  ipv6_bogon:
    enable: true
    prefixes:
      - 2001:db8::/32
```

Events

IPV6_BOGON_SOURCE

IPV6_BOGON_TARGET

IXpect

ipv6_neighbor

Monitors the mapping of static and dynamic IPv6 addresses to mac addresses.

Events

IPV6_NEIGHBOR_NEW_DYNAMIC

IPV6_NEIGHBOR_SPOOFED_DYNAMIC

IPV6_NEIGHBOR_SPOOFED_STATIC

IPV6_NEIGHBOR_UNKNOWN

```
probes:
  ipv6_neighbor:
    enable: true
    dynamic_enable: true
    static_resolutions:
    - ip: 2a02::1
      mac: 00:00:5e:00:53:01
    - ip: fe80::200:5eff:fe00:5301
      mac: 00:00:5e:00:53:01
```

IXpect

ipv6_router

Monitors for IPv6 ICMPv6 router advertisement and router solicitation packets.

```
probes:
  ipv6_router:
    enable: true
```

Events

`IPV6_ROUTER_ADVERTISEMENT`

`IPV6_ROUTER_SOLICITATION`

stp

Monitors for spanning tree protocol BPDU frames.

```yaml
probes:
  stp:
    enable: true
```

Events

`STP_PACKET_FOUND`

Event Processing

IXpect

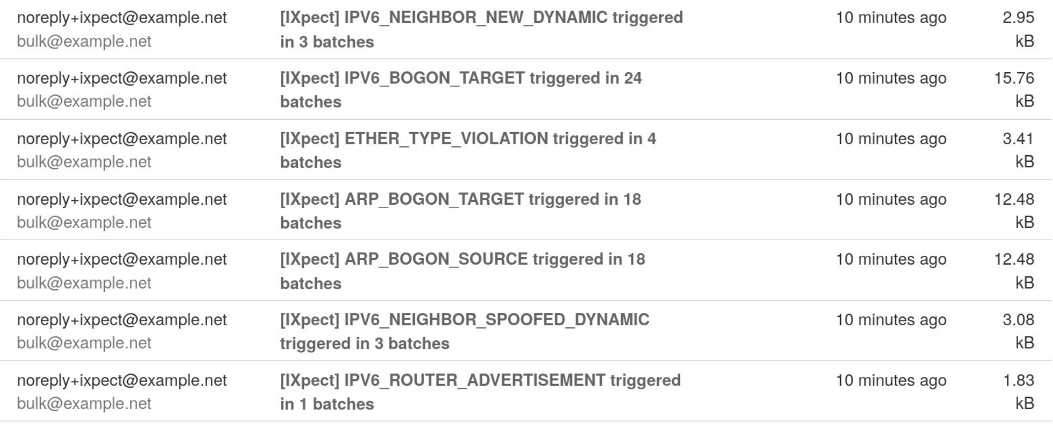
Batching

- merge events with same „data“
- one notification per „event type“

IXpect

Batching

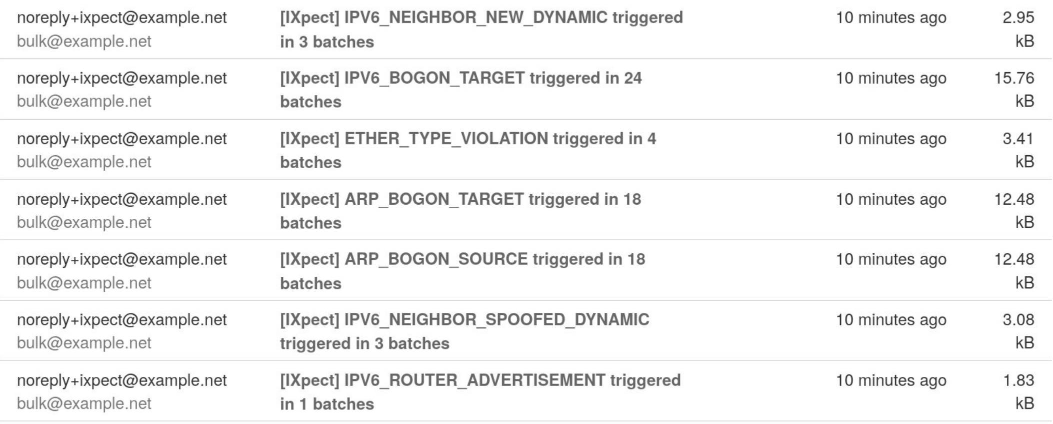
- merge events with same „data“
- one notification per „event type“



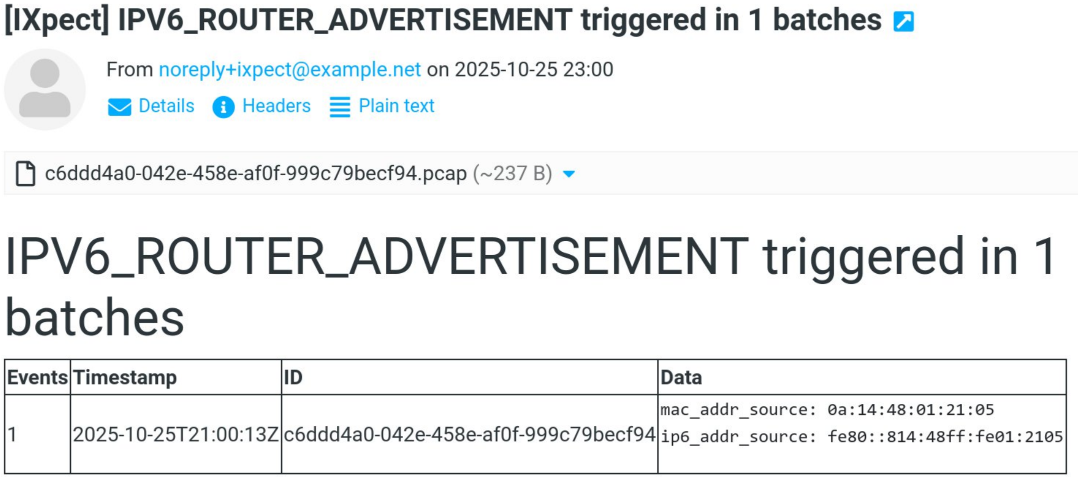
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_NEIGHBOR_NEW_DYNAMIC triggered in 3 batches**	10 minutes ago	2.95 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_BOGON_TARGET triggered in 24 batches**	10 minutes ago	15.76 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ETHER_TYPE_VIOLATION triggered in 4 batches**	10 minutes ago	3.41 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ARP_BOGON_TARGET triggered in 18 batches**	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ARP_BOGON_SOURCE triggered in 18 batches**	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_NEIGHBOR_SPOOFED_DYNAMIC triggered in 3 batches**	10 minutes ago	3.08 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches**	10 minutes ago	1.83 kB

Batching

- merge events with same „data“
- one notification per „event type“



noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_NEIGHBOR_NEW_DYNAMIC triggered in 3 batches**	10 minutes ago	2.95 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_BOGON_TARGET triggered in 24 batches**	10 minutes ago	15.76 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ETHER_TYPE_VIOLATION triggered in 4 batches**	10 minutes ago	3.41 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ARP_BOGON_TARGET triggered in 18 batches**	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ARP_BOGON_SOURCE triggered in 18 batches**	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_NEIGHBOR_SPOOFED_DYNAMIC triggered in 3 batches**	10 minutes ago	3.08 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches**	10 minutes ago	1.83 kB



[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

From noreply+ixpect@example.net on 2025-10-25 23:00

c6ddd4a0-042e-458e-af0f-999c79becf94.pcap (~237 B)

IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

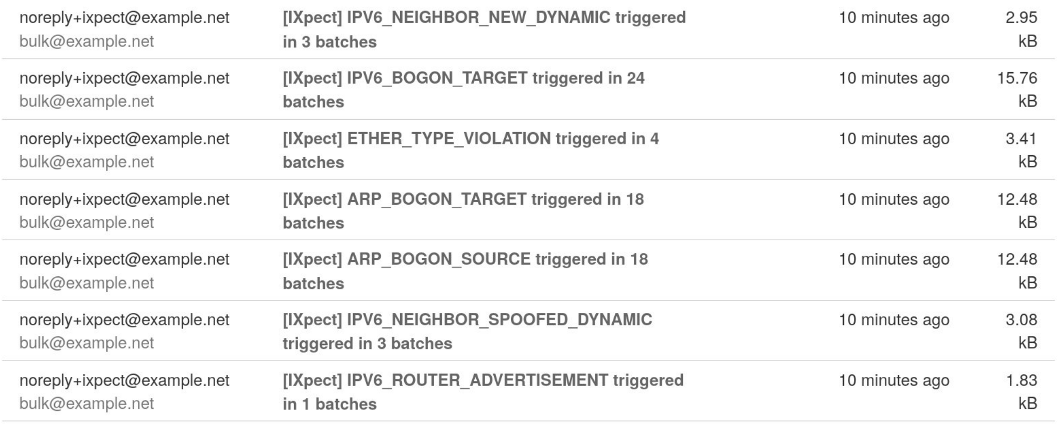
Events	Timestamp	ID	Data

1	2025-10-25T21:00:13Z	c6ddd4a0-042e-458e-af0f-999c79becf94	`mac_addr_source: 0a:14:48:01:21:05`
			`ip6_addr_source: fe80::814:48ff:fe01:2105`

IXpect

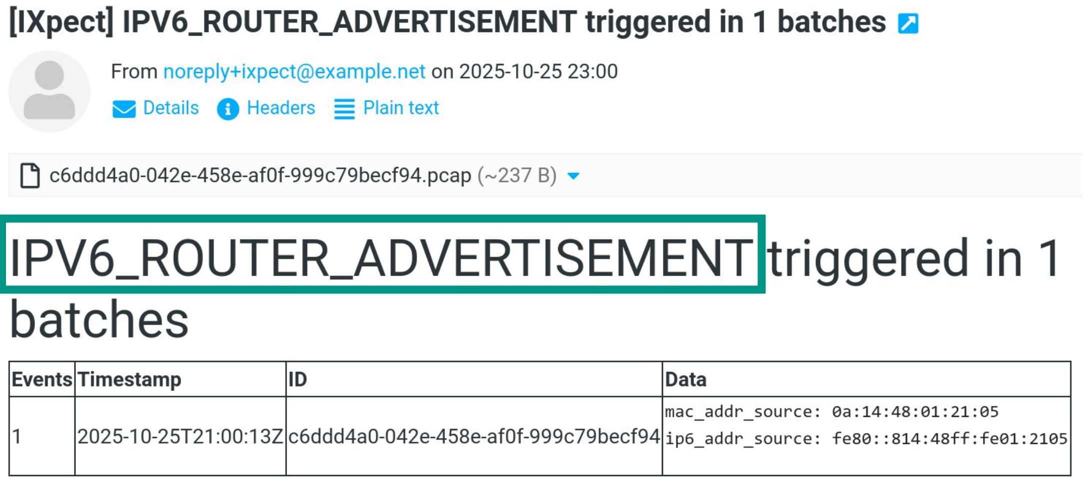
Batching

- merge events with same „data“
- one notification per „event type“



noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_NEIGHBOR_NEW_DYNAMIC triggered in 3 batches	10 minutes ago	2.95 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_BOGON_TARGET triggered in 24 batches	10 minutes ago	15.76 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ETHER_TYPE_VIOLATION triggered in 4 batches	10 minutes ago	3.41 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ARP_BOGON_TARGET triggered in 18 batches	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ARP_BOGON_SOURCE triggered in 18 batches	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_NEIGHBOR_SPOOFED_DYNAMIC triggered in 3 batches	10 minutes ago	3.08 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches	10 minutes ago	1.83 kB

event type



[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

From noreply+ixpect@example.net on 2025-10-25 23:00

c6ddd4a0-042e-458e-af0f-999c79becf94.pcap (~237 B)

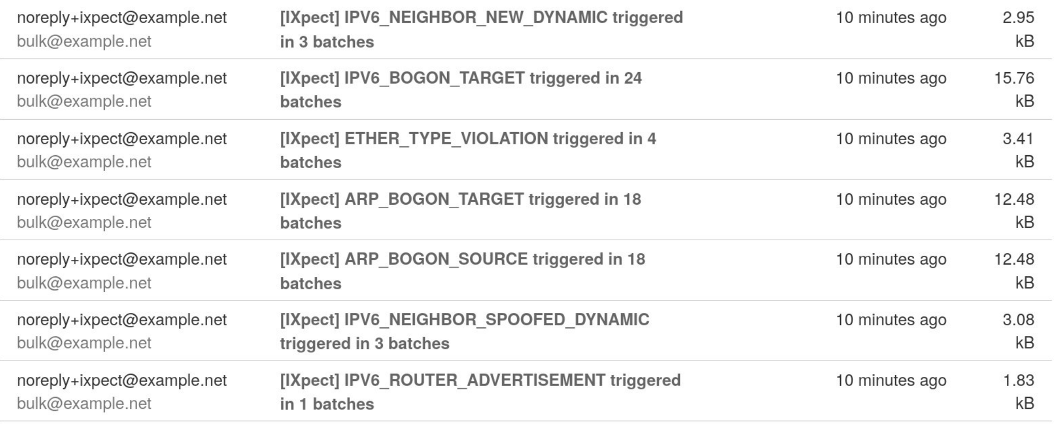
IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

Events	Timestamp	ID	Data

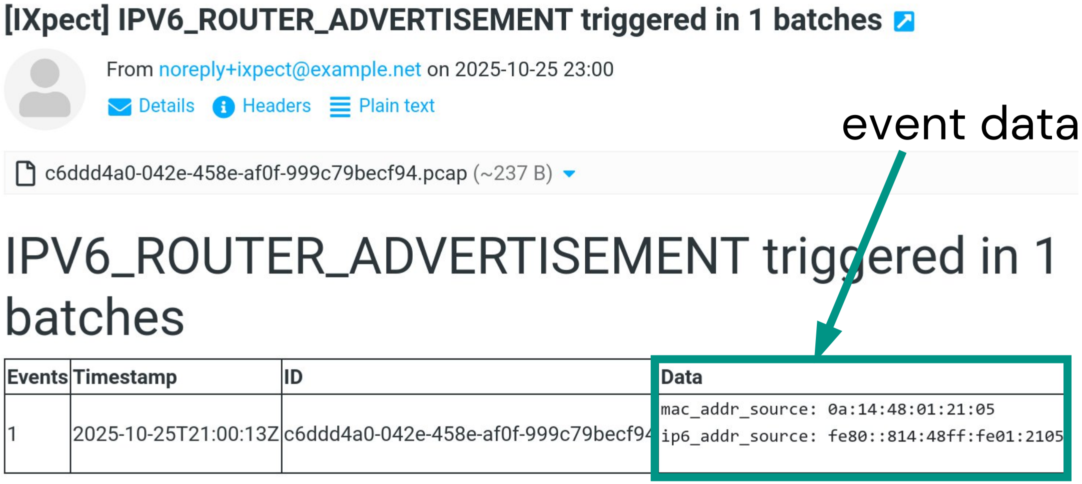
1	2025-10-25T21:00:13Z	c6ddd4a0-042e-458e-af0f-999c79becf94	`mac_addr_source: 0a:14:48:01:21:05`
			`ip6_addr_source: fe80::814:48ff:fe01:2105`

Batching

- merge events with same „data“
- one notification per „event type“



noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_NEIGHBOR_NEW_DYNAMIC triggered in 3 batches	10 minutes ago	2.95 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_BOGON_TARGET triggered in 24 batches	10 minutes ago	15.76 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ETHER_TYPE_VIOLATION triggered in 4 batches	10 minutes ago	3.41 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ARP_BOGON_TARGET triggered in 18 batches	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ARP_BOGON_SOURCE triggered in 18 batches	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_NEIGHBOR_SPOOFED_DYNAMIC triggered in 3 batches	10 minutes ago	3.08 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches	10 minutes ago	1.83 kB



[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

From noreply+ixpect@example.net on 2025-10-25 23:00

c6ddd4a0-042e-458e-af0f-999c79becf94.pcap (~237 B)

event data

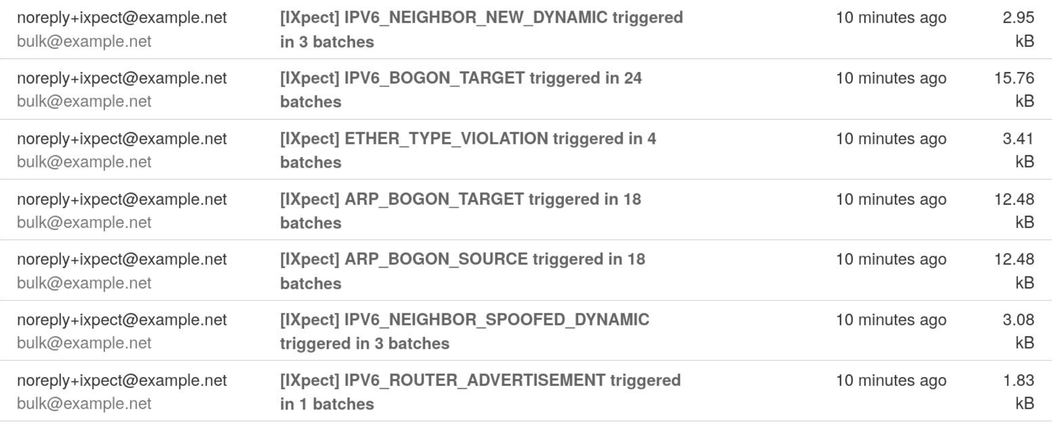
IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

Events	Timestamp	ID	Data
1	2025-10-25T21:00:13Z	c6ddd4a0-042e-458e-af0f-999c79becf94	mac_addr_source: 0a:14:48:01:21:05 ip6_addr_source: fe80::814:48ff:fe01:2105

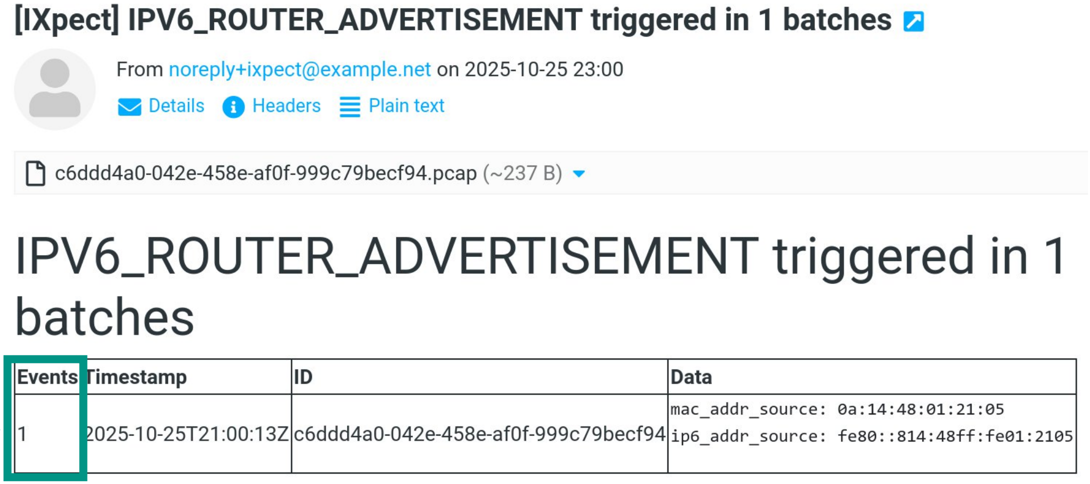
IXpect

Batching

- merge events with same „data“
- one notification per „event type“



noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_NEIGHBOR_NEW_DYNAMIC triggered in 3 batches	10 minutes ago	2.95 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_BOGON_TARGET triggered in 24 batches	10 minutes ago	15.76 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ETHER_TYPE_VIOLATION triggered in 4 batches	10 minutes ago	3.41 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ARP_BOGON_TARGET triggered in 18 batches	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] ARP_BOGON_SOURCE triggered in 18 batches	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_NEIGHBOR_SPOOFED_DYNAMIC triggered in 3 batches	10 minutes ago	3.08 kB
noreply+ixpect@example.net bulk@example.net	[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches	10 minutes ago	1.83 kB



[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

From noreply+ixpect@example.net on 2025-10-25 23:00

c6ddd4a0-042e-458e-af0f-999c79becf94.pcap (~237 B)

IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

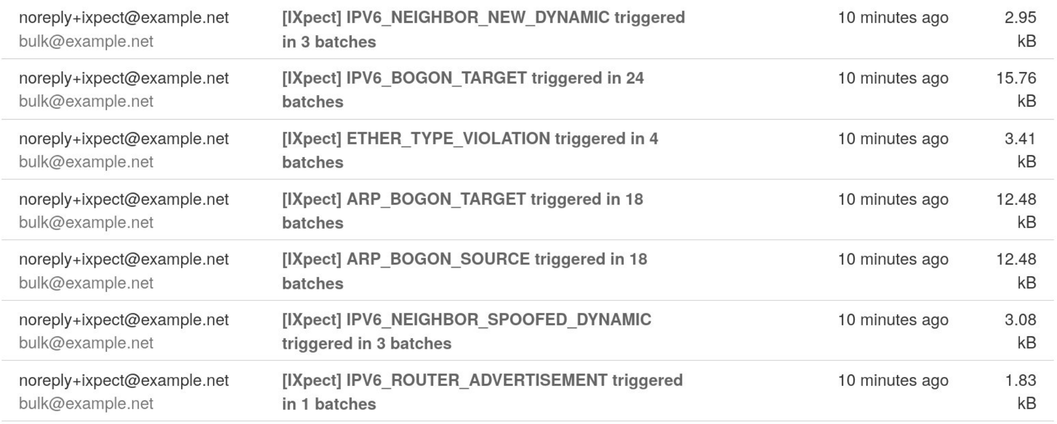
Events	Timestamp	ID	Data
1	2025-10-25T21:00:13Z	c6ddd4a0-042e-458e-af0f-999c79becf94	mac_addr_source: 0a:14:48:01:21:05 ip6_addr_source: fe80::814:48ff:fe01:2105

number of events with same data

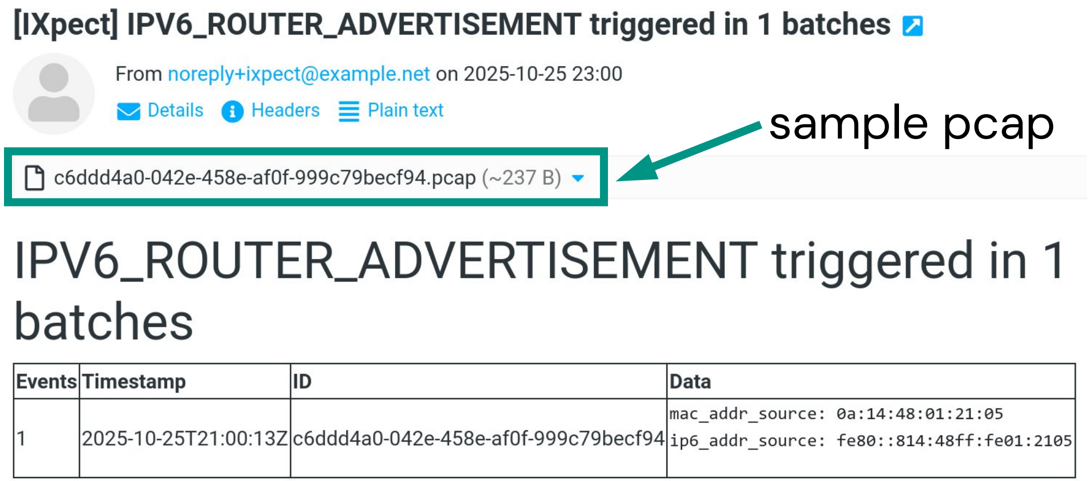
IXpect

Batching

- merge events with same „data“
- one notification per „event type“



noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_NEIGHBOR_NEW_DYNAMIC triggered in 3 batches**	10 minutes ago	2.95 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_BOGON_TARGET triggered in 24 batches**	10 minutes ago	15.76 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ETHER_TYPE_VIOLATION triggered in 4 batches**	10 minutes ago	3.41 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ARP_BOGON_TARGET triggered in 18 batches**	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] ARP_BOGON_SOURCE triggered in 18 batches**	10 minutes ago	12.48 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_NEIGHBOR_SPOOFED_DYNAMIC triggered in 3 batches**	10 minutes ago	3.08 kB
noreply+ixpect@example.net bulk@example.net	**[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches**	10 minutes ago	1.83 kB



[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

From noreply+ixpect@example.net on 2025-10-25 23:00

c6ddd4a0-042e-458e-af0f-999c79becf94.pcap (~237 B)

sample pcap

IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

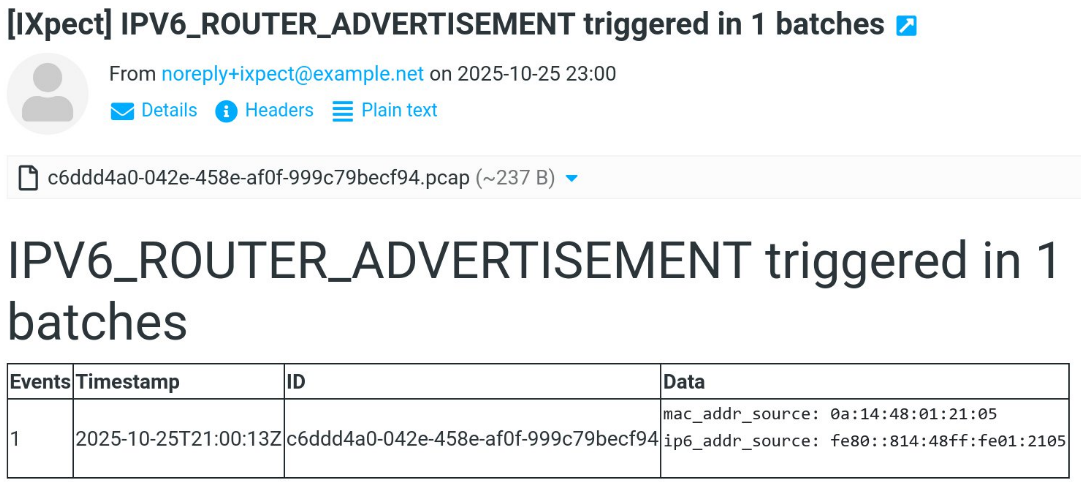
Events	Timestamp	ID	Data

1	2025-10-25T21:00:13Z	c6ddd4a0-042e-458e-af0f-999c79becf94	`mac_addr_source: 0a:14:48:01:21:05`
			`ip6_addr_source: fe80::814:48ff:fe01:2105`

Notifiers

`https://ixpect.net/0.1/notifiers/`

email



[IXpect] IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

From noreply+ixpect@example.net on 2025-10-25 23:00

c6ddd4a0-042e-458e-af0f-999c79becf94.pcap (~237 B)

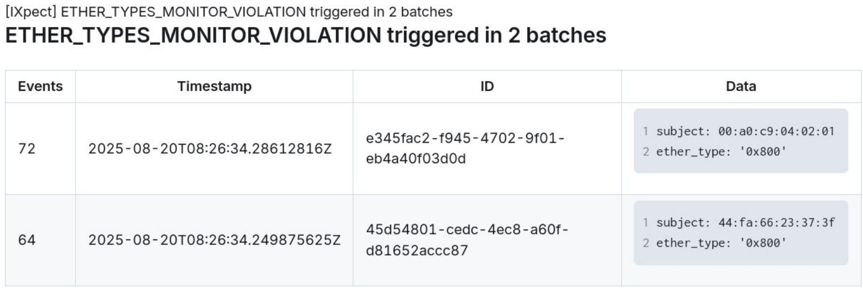
IPV6_ROUTER_ADVERTISEMENT triggered in 1 batches

Events	Timestamp	ID	Data
1	2025-10-25T21:00:13Z	c6ddd4a0-042e-458e-af0f-999c79becf94	mac_addr_source: 0a:14:48:01:21:05 ip6_addr_source: fe80::814:48ff:fe01:2105

```yaml
event:
  notifiers:
    email:
      enable: true
      smtp:
        host: mailin.example.net
      from: noreply+ixpect@example.net
      channels:
        - to:
            - alert@example.net
          events:
            - ARP_NEIGHBOR_UNKNOWN
            - IPV6_NEIGHBOR_UNKNOWN
        - to:
            - bulk@example.net
```

http

Matrix

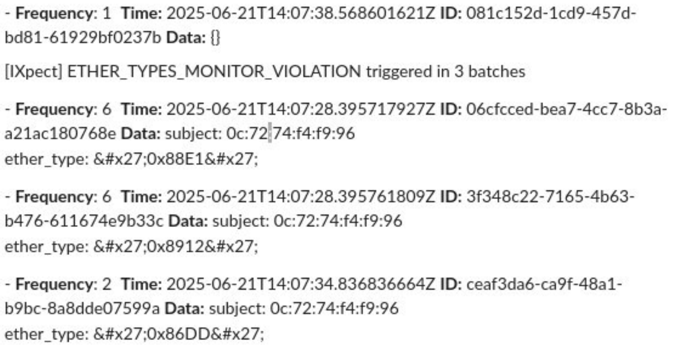


[IXpect] ETHER_TYPES_MONITOR_VIOLATION triggered in 2 batches

ETHER_TYPES_MONITOR_VIOLATION triggered in 2 batches

Events	Timestamp	ID	Data
72	2025-08-20T08:26:34.28612816Z	e345fac2-f945-4702-9f01-eb4a40f03d0d	subject: 00:a0:c9:04:02:01 ether_type: '0x800'
64	2025-08-20T08:26:34.249875625Z	45d54801-cedc-4ec8-a60f-d81652accc87	subject: 44:fa:66:23:37:3f ether_type: '0x800'

Slack (does not support tables)



- **Frequency**: 1 **Time:** 2025-06-21T14:07:38.568601621Z **ID:** 081c152d-1cd9-457d-bd81-61929bf0237b **Data:** {}

[IXpect] ETHER_TYPES_MONITOR_VIOLATION triggered in 3 batches

- **Frequency**: 6 **Time:** 2025-06-21T14:07:28.395717927Z **ID:** 06cfcced-bea7-4cc7-8b3a-a21ac180768e **Data:** subject: 0c:72:74:f4:f9:96
ether_type: &#x27;0x88E1&#x27;

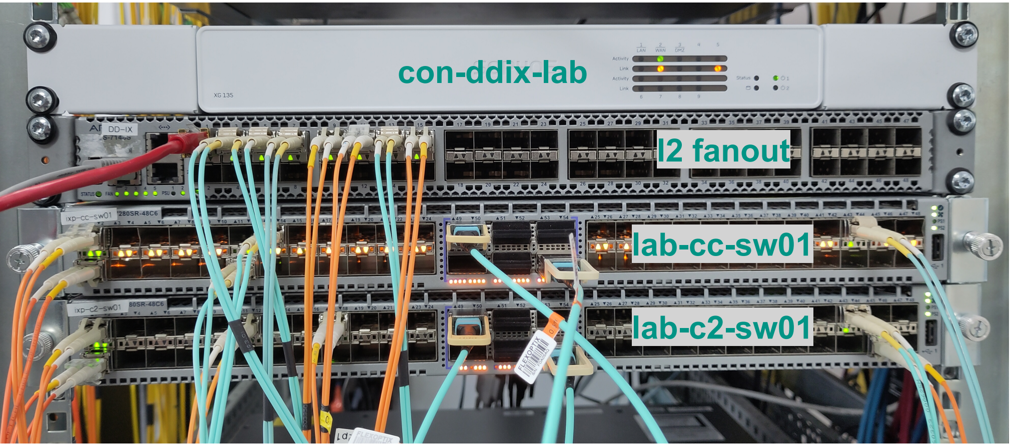
- **Frequency**: 6 **Time:** 2025-06-21T14:07:28.395761809Z **ID:** 3f348c22-7165-4b63-b476-611674e9b33c **Data:** subject: 0c:72:74:f4:f9:96
ether_type: &#x27;0x8912&#x27;

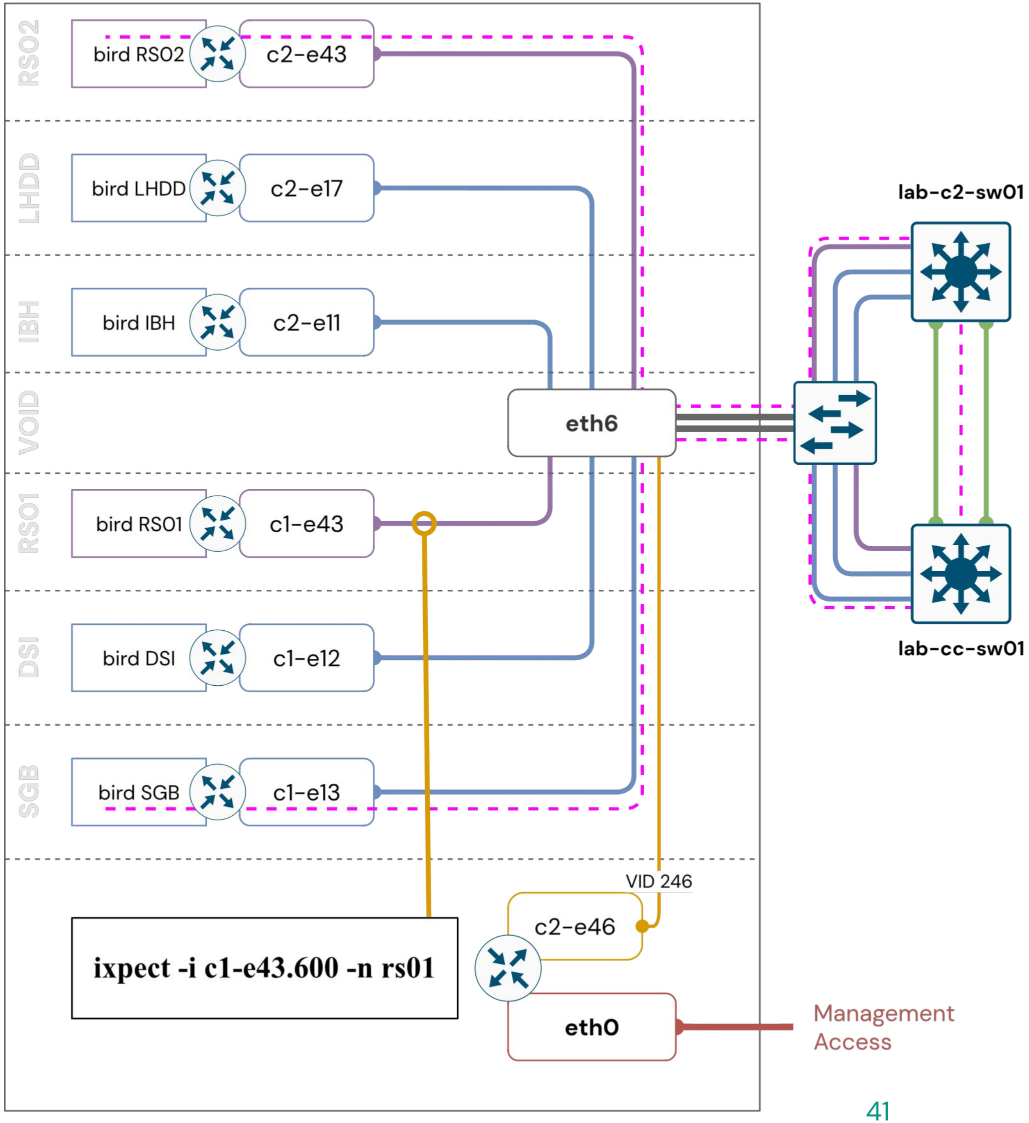
- **Frequency**: 2 **Time:** 2025-06-21T14:07:34.836836664Z **ID:** ceaf3da6-ca9f-48a1-b9bc-8a8dde07599a **Data:** subject: 0c:72:74:f4:f9:96
ether_type: &#x27;0x86DD&#x27;

```
event:
  notifiers:
    http:
      enable: true
      channels:
        - url: https://example.net/api/foo
          method: POST
          content_type: application/json
          template: custom-http.json
          events:
            - ARP_NEIGHBOR_UNKNOWN
            - IPV6_NEIGHBOR_UNKNOWN
```

Demo

DD-IX Lab





```
ixpect -i c1-e43.600 -n rs01
```

con-ddix-lab.ibh.net

IXpect

IXpect – We are not done yet!

Packing provided for:

- Alpine Linux
- Debian GNU/Linux
- NixOS

Future work:

- Probe `l4_protocol`
- IX-F Member Export support
- Additional packet sources?

Documentation: **`https://ixpect.net`**
Code & Issues: **`https://codeberg.org/ixpect/ixpect`**