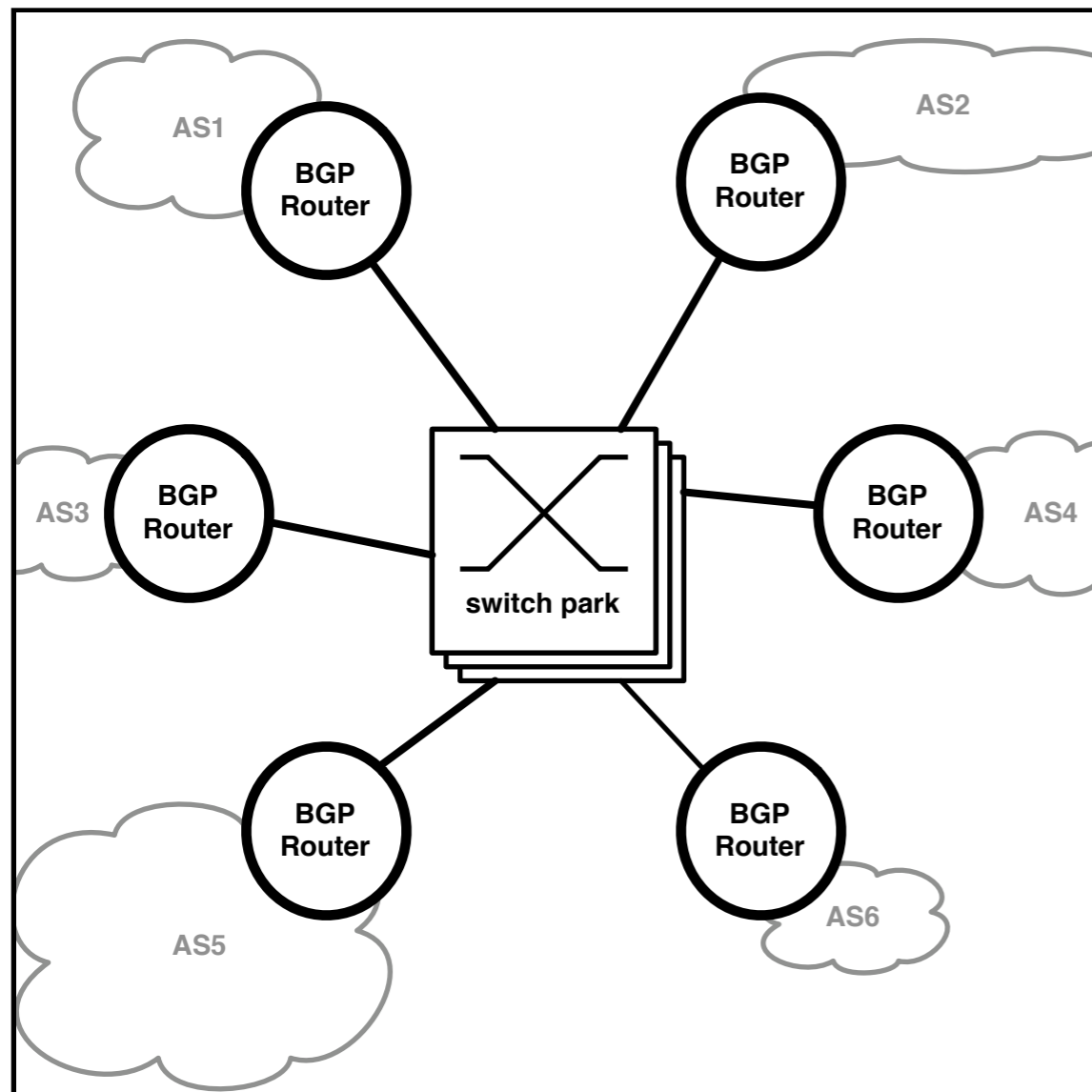


Some IPv6 related issues seen on the AMS-IX peering platform

Ariën Vijn
ariën.vijn@ams-ix.net

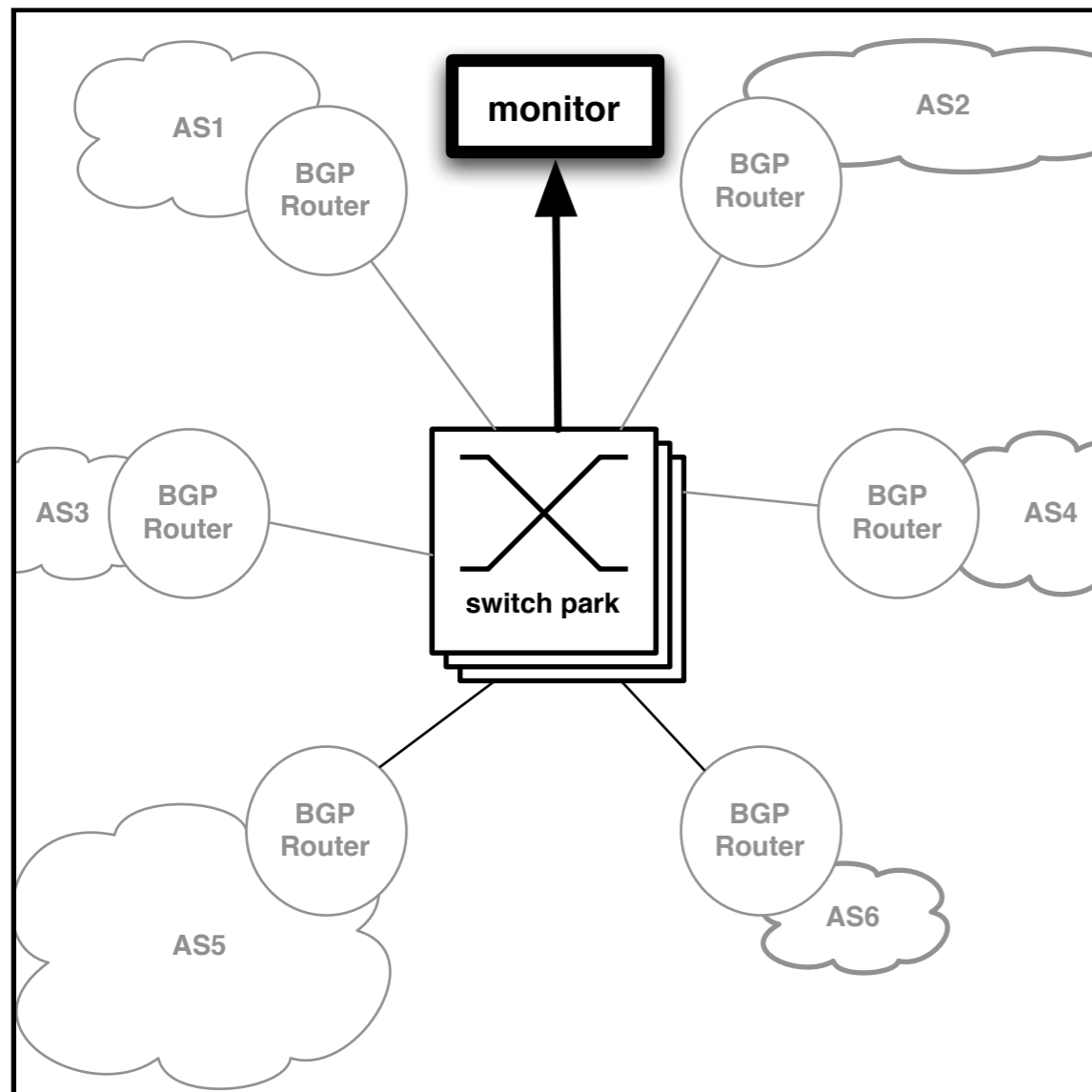


Introduction



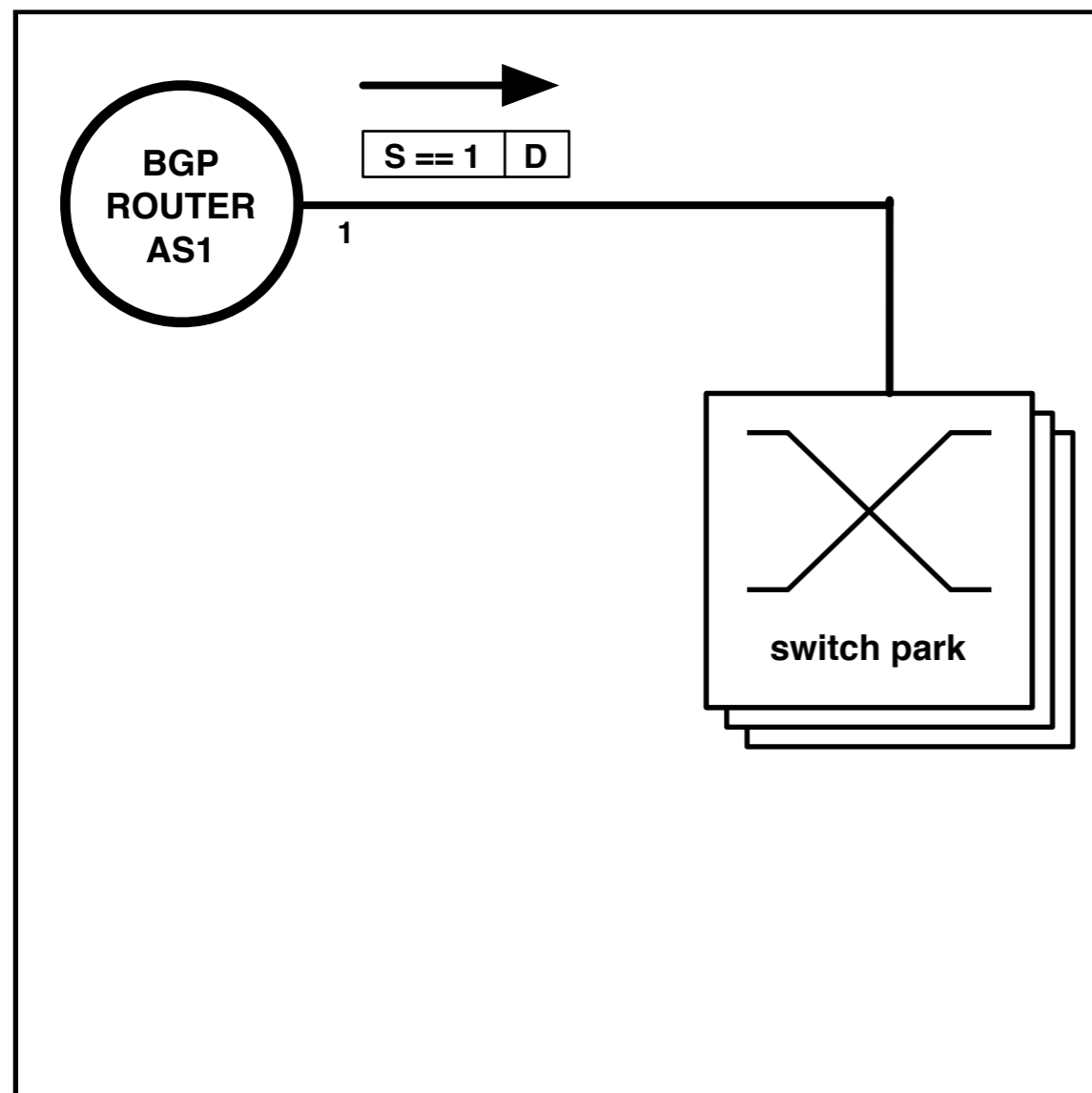
- Obviously we do not control the routers connected to AMS-IX.
- We only do layer-2, so what is this presentation about?

Introduction



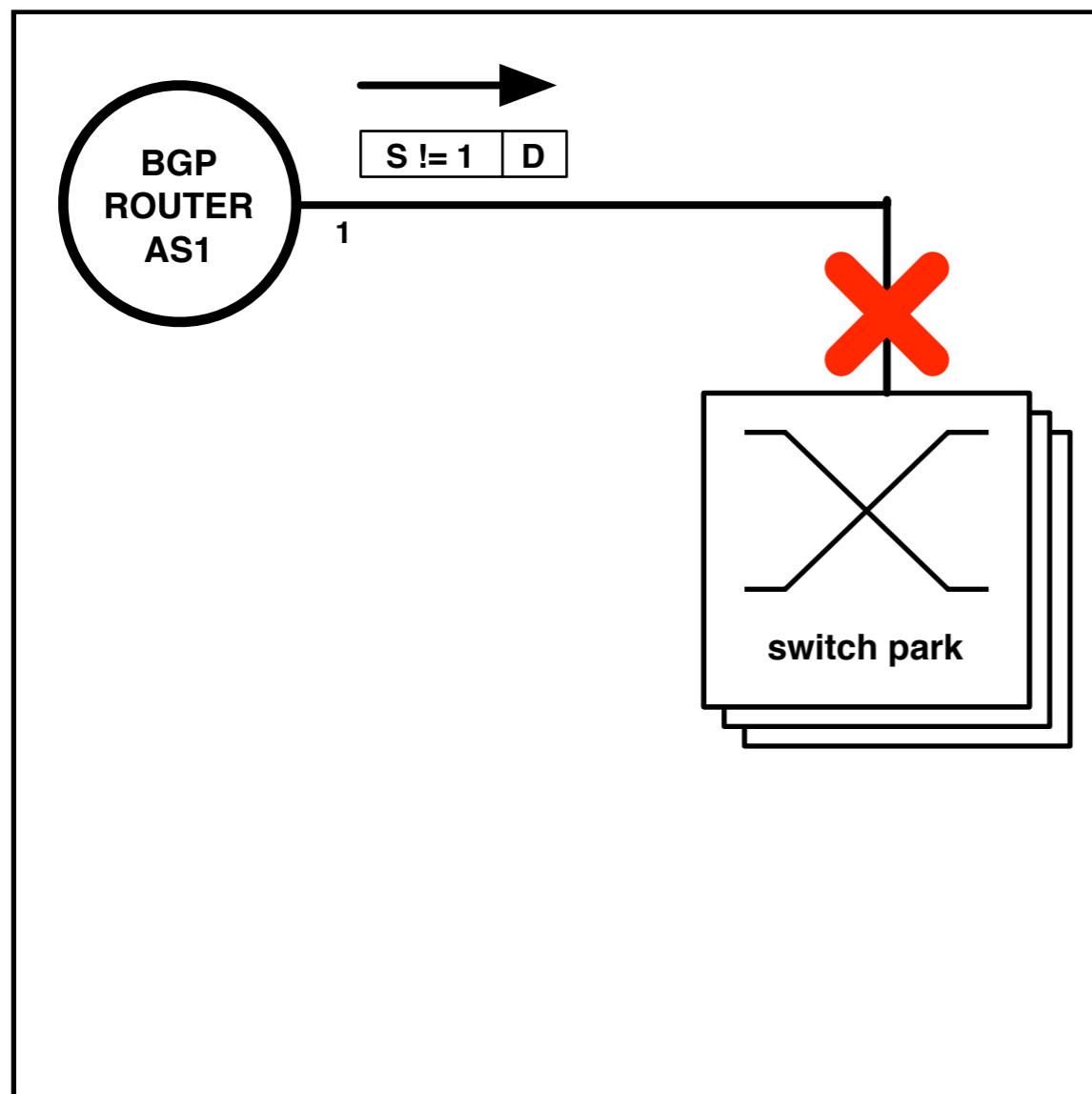
- Obviously we do not control the routers connected to AMS-IX.
- We only do layer-2, so what is this presentation about?
- It is about the multicast and flooded traffic.

Introduction



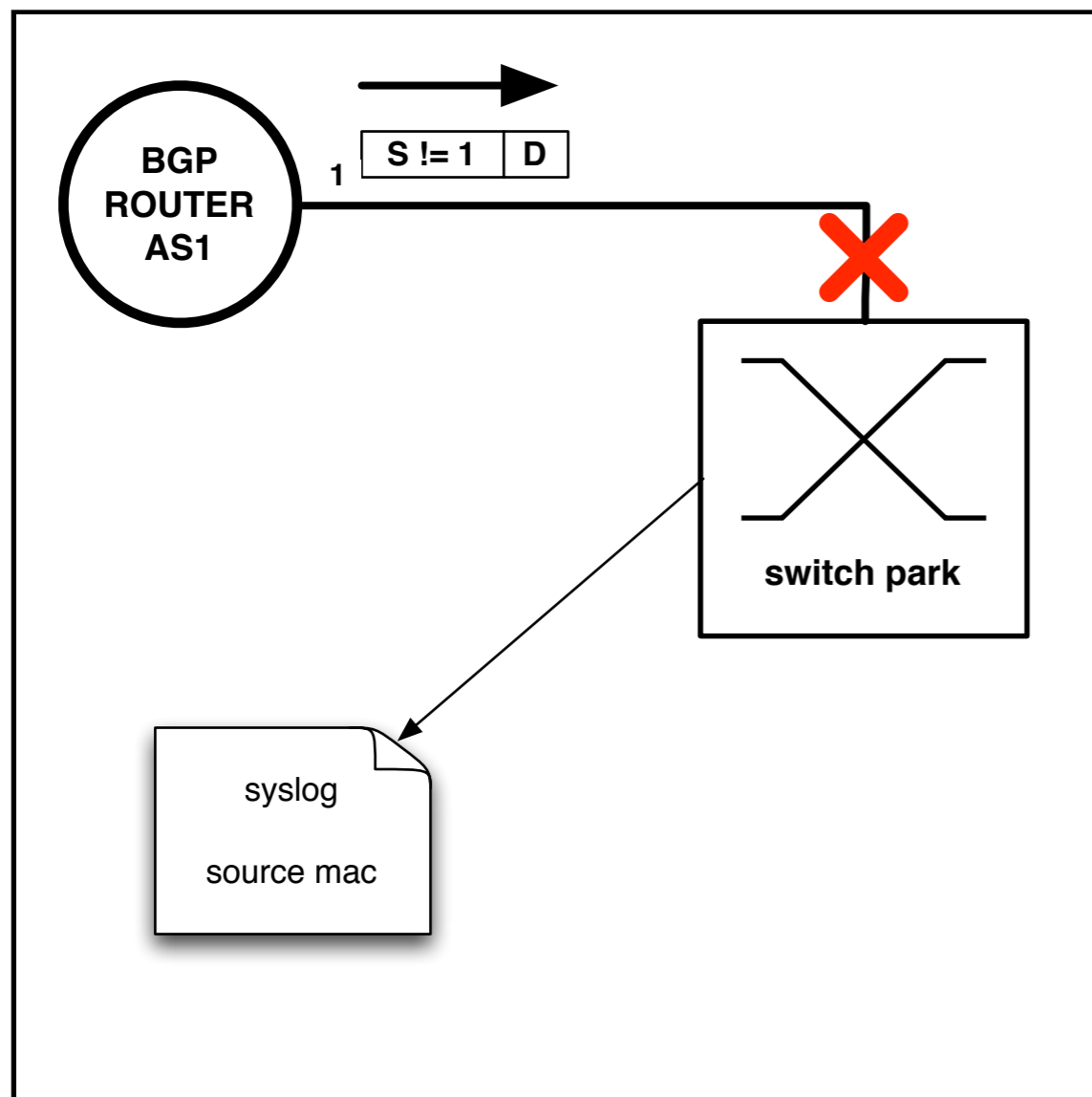
- Obviously we do not control the routers connected to AMS-IX.
- We only do layer-2, so what is this presentation about?
- It is about the multicast and flooded traffic.
- And it is about the things we see via port security feature.

Introduction



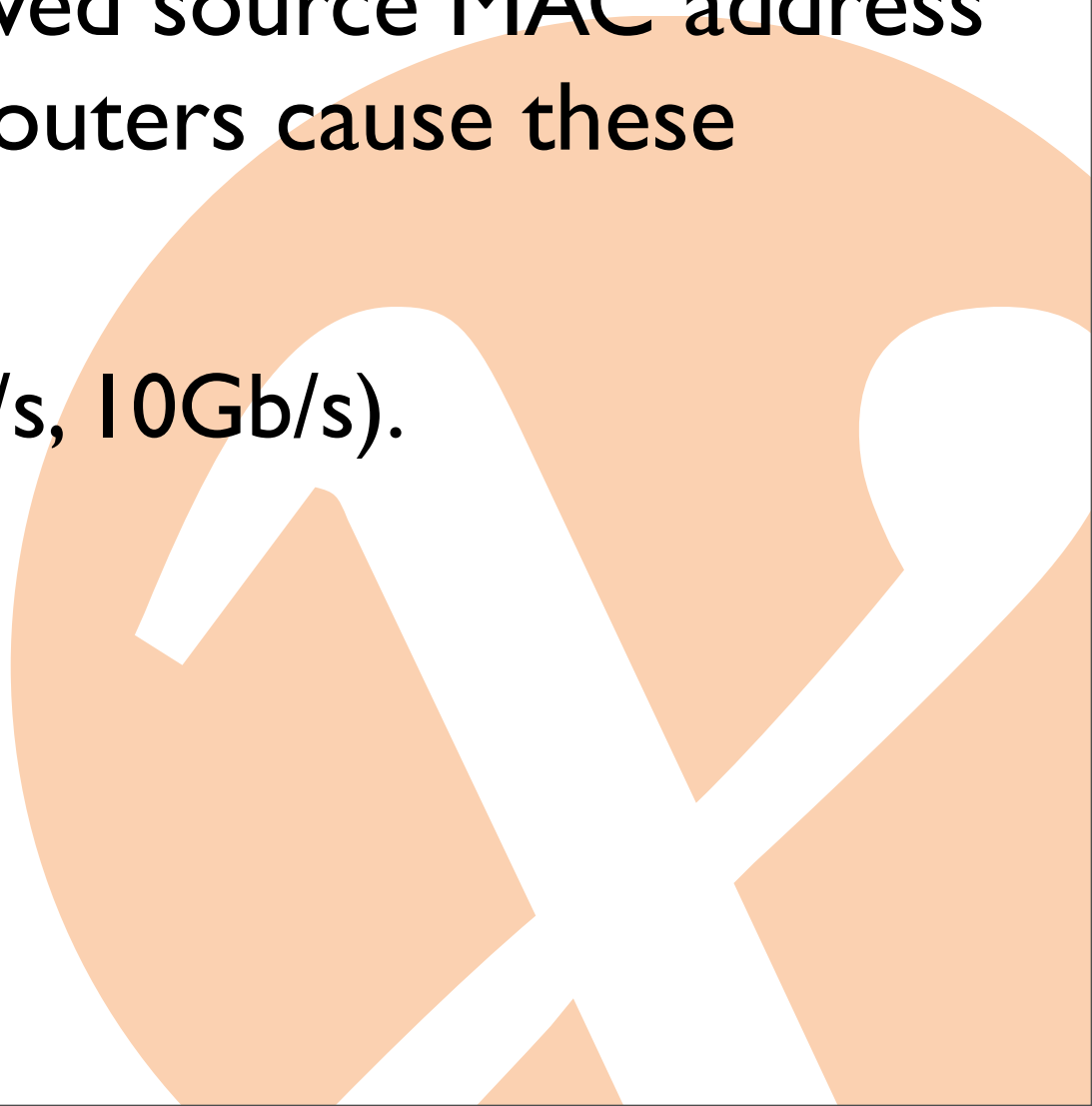
- Obviously we do not control the routers connected to AMS-IX.
- We only do layer-2, so what is this presentation about?
- It is about the multicast and flooded traffic.
- And it is about the things we see via port security feature.
 - We only allow one MAC address per port (loop-mitigation).
 - Port security blocks or shuts the port if any other source MAC address is seen.

Introduction

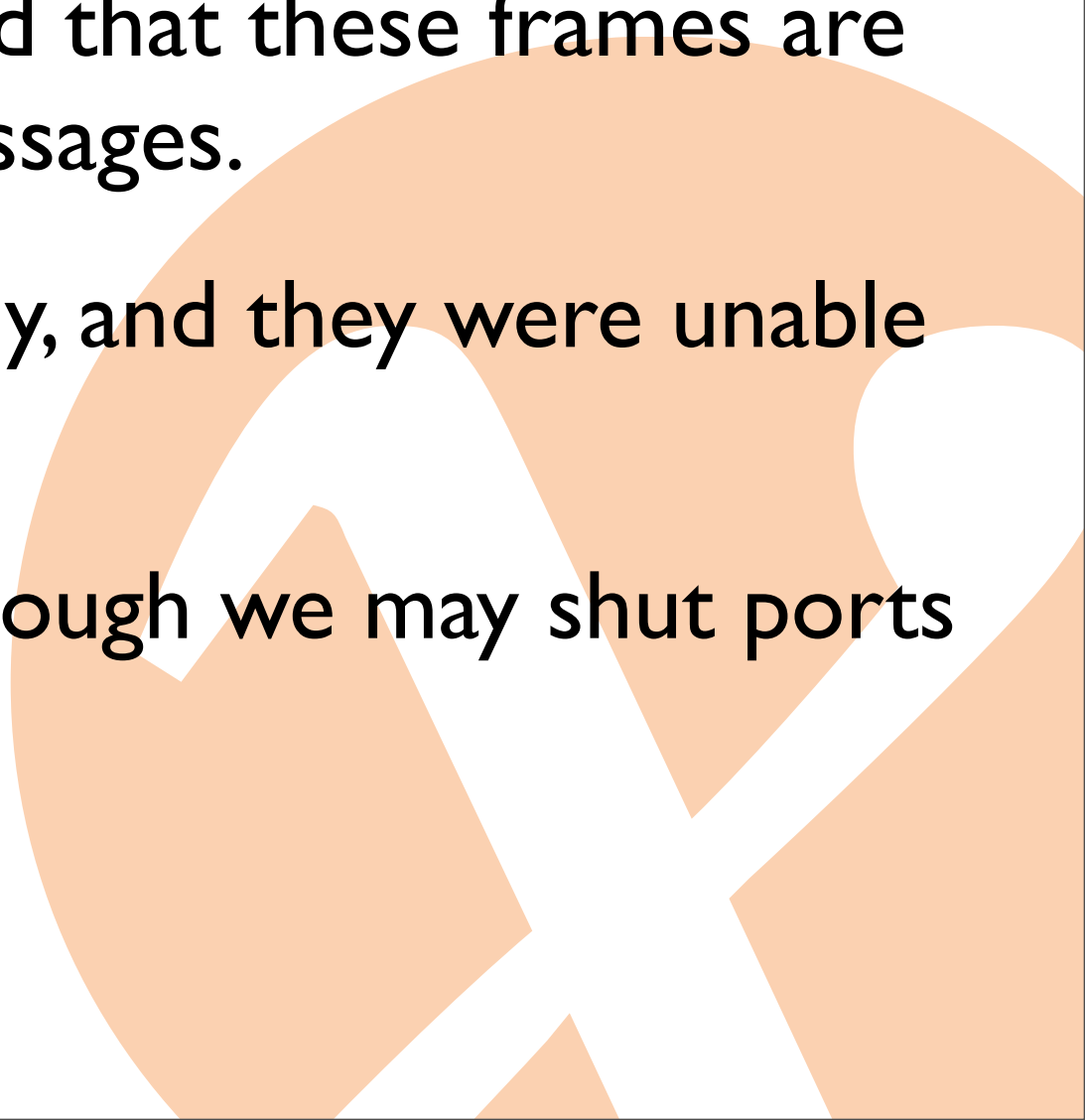


- We only do layer-2, so what is this presentation about?
- It is about the multicast and flooded traffic.
- And it is about the things we see via port security feature.
- We only allow one MAC address per port (loop-mitigation).
- Port security blocks or shuts the port if any other source MAC address is seen.
- Syslog message is generated.

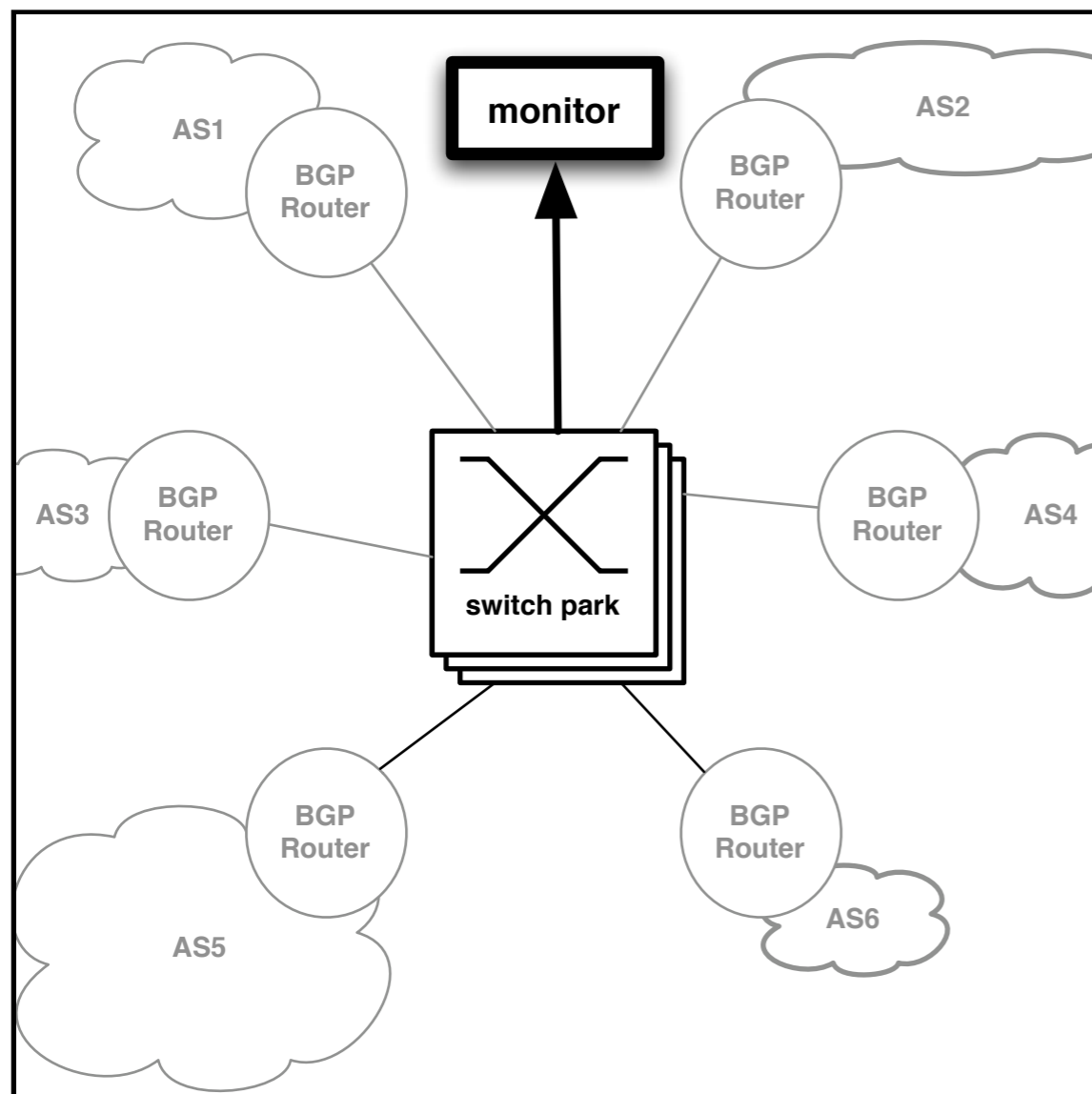
Typical port sec. violations

- Violating addresses look awfully like our v6 peering LAN prefix.
 - Via the ports and OUI of the allowed source MAC address we determined that only Juniper routers cause these violations.
 - All interface types (100Mb/s, 1Gb/s, 10Gb/s).
 - Only v6 enabled routers.
- 

Typical port sec. violations

- Via syslog correlation we determined that these violations occur during the time some V6 peer(s) become unavailable.
 - Capturing violating frames revealed that these frames are basically un-encapsulated BGP messages.
 - We informed the vendor informally, and they were unable to replicate this issue.
 - Does not seem to be harmful, although we may shut ports upon port security violations.
- 

Other issues #1



- Bursts of ICMPv6 ND with wrong source IPv6 addresses, including addresses used by other members.
- Again specific for three out of nine IPv6 enabled routers.
- Does not seem to be harmful.

Other issues #1



- Does not seem to be harmful.
- Why?
- Bogus addresses:
 - ::
 - 2001:7f8:1::
 - Addresses allocated to the members involved.
 - Local link with the last nibble (in network order) wrong.

Other issues #1



- Bogus addresses:
 - ::
 - 2001:7f8:1::
 - Addresses allocated to the members involved.
 - Local link with the last nibble (in network order) wrong.
- Source address of other members:
 - Vast minority of queries.
 - Query from the correct IPv6 source follows quickly (often the next frame).

Other issues #2

```
interface xx/yyy/zzz
  ipv6 address 2001:7F8:1::A5xx:xxxx:n/64
  ipv6 nd ra suppress
  no ipv6 mld router
  no ipv6 mfib forwarding
  no ipv6 pim
```

- Recently, bursts of ICMPv6 multicast listener reports.
- Response on a ICMPv6 multicast listener query.
- Cisco specific for routers doing IPv6 multicast routing in their own AS.
- Solution: **no ipv6 mld router** in interface context.

Conclusion



- Mostly harmless.
- Juniper specific problem might cause a port security violation.
- Foundry issue is under investigation.
 - We will inform the members involved and contact Foundry ourselves.
- Cisco's MLD messages are just another option to add to the router configurations
 - We will update the config guide.

That's all

