Security at IXPs

Frank Habicht

Af-IX

Maputo, August 24, 2015

Security at IXPs

Agenda

- General
- One big special thing
- Verifying routes in Route Servers
- Value-add

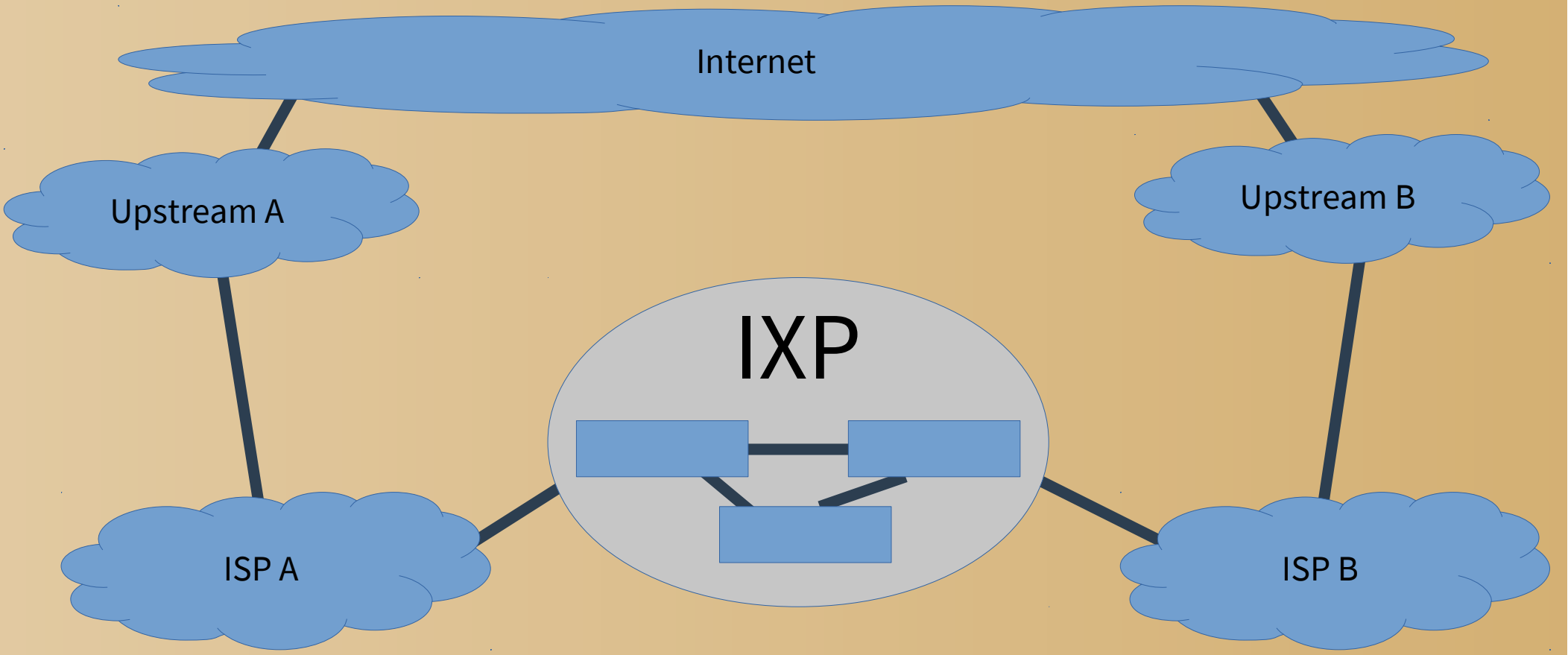
Security at IXPs

secure Switches, routers, servers

An IXP doesn't implement “security” (for others).
It makes everything faster, also bad things.
ISPs and End Users should take care of security.

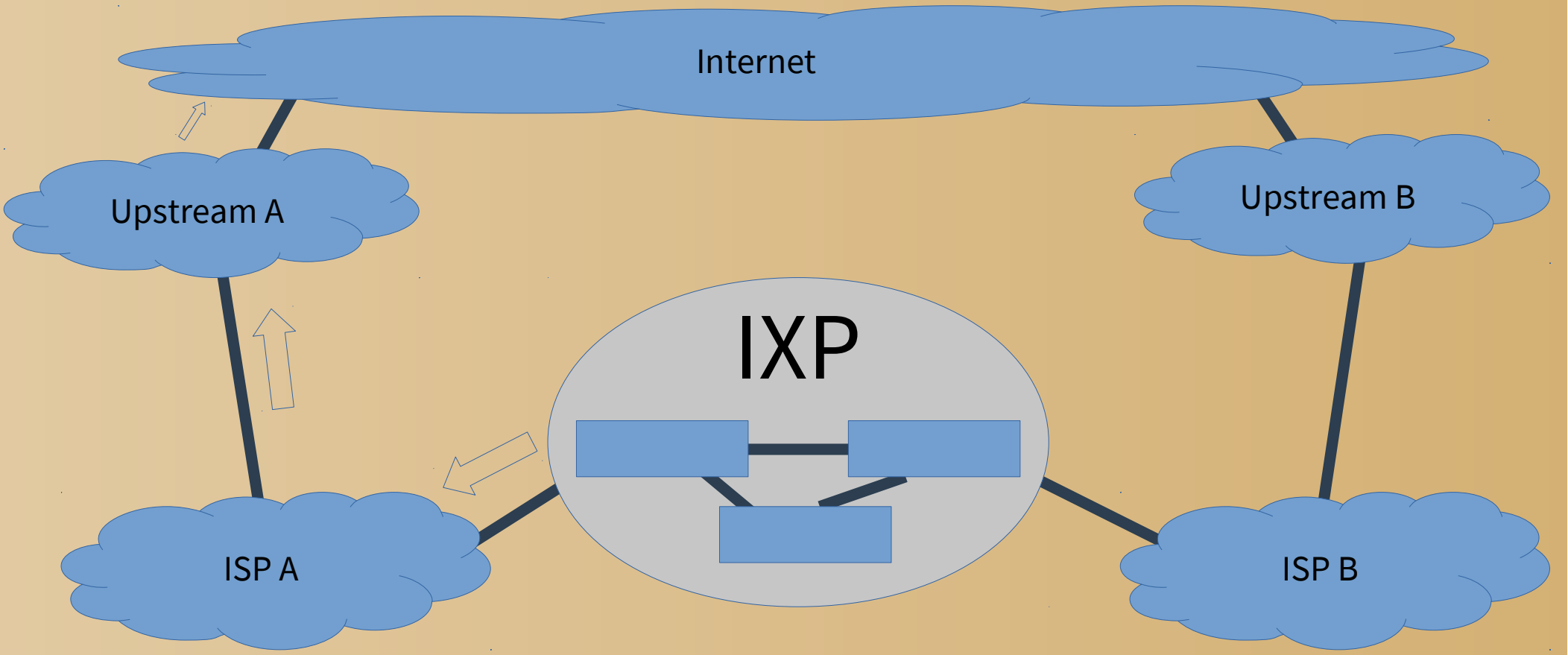
IXP connections should be treated as untrusted outside connections.

Security at IXPs



Maputo, August 24, 2015

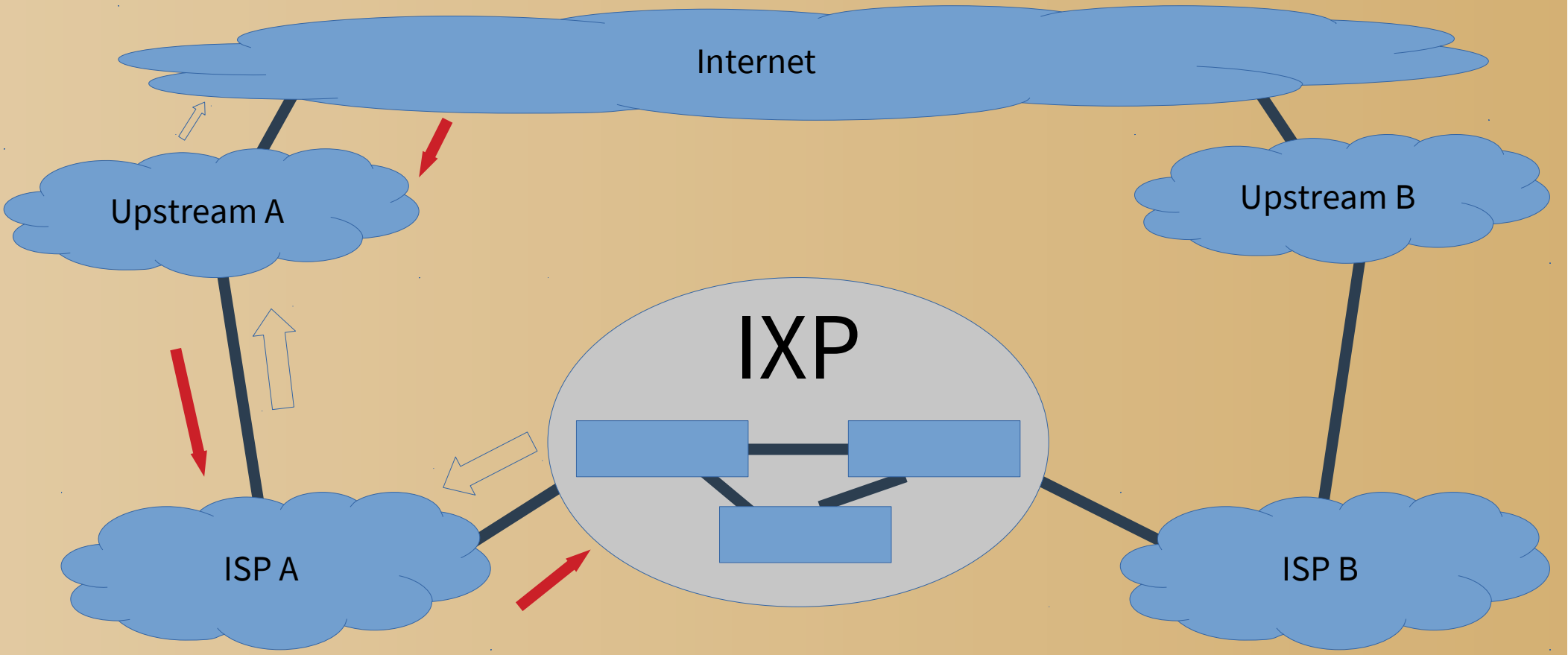
Security at IXPs



196.223.5.0/24

Maputo, August 24, 2015

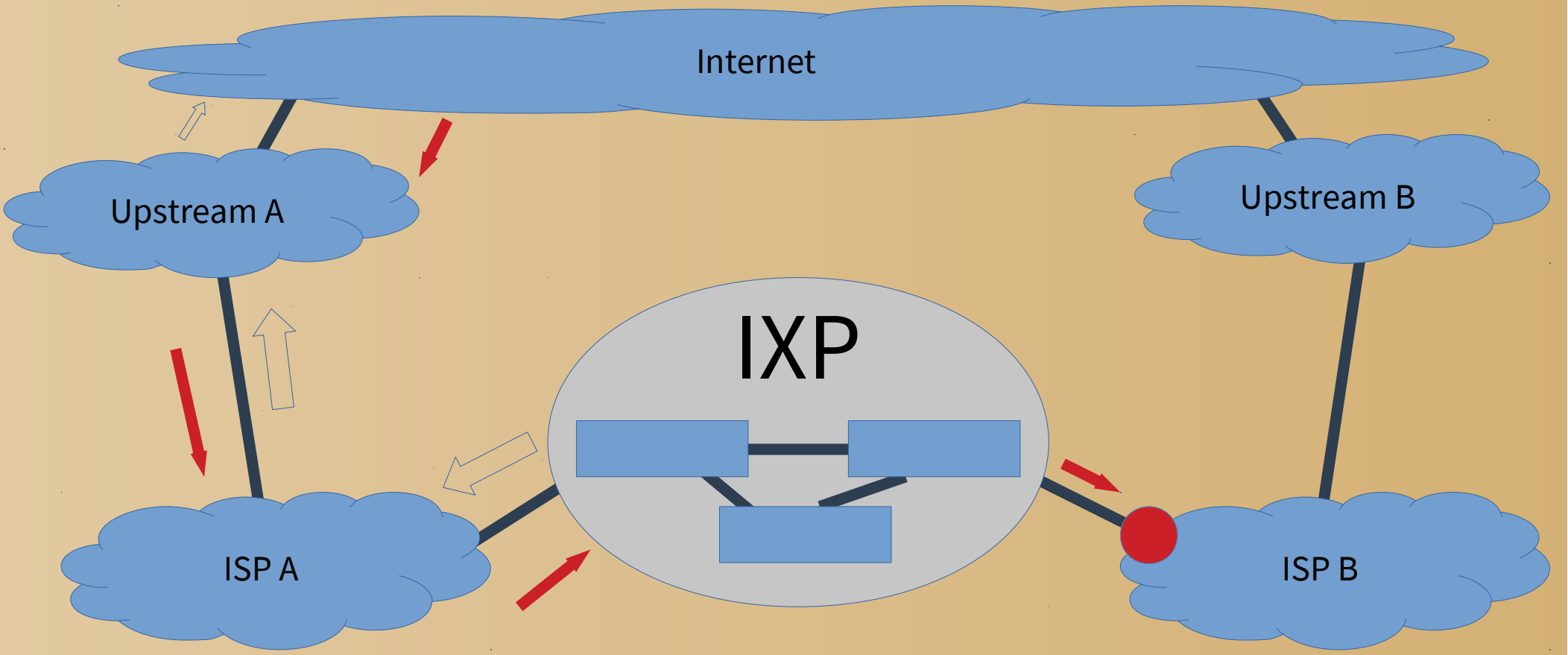
Security at IXPs



196.223.5.0/24

Maputo, August 24, 2015

Security at IXPs



196.223.5.0/24

Maputo, August 24, 2015

Security at IXPs

Do not advertise your IXP peering LAN subnet to anywhere.
The only devices that need to know it are the directly connected ones.
Peers should use next-hop self in iBGP.

Security at IXPs

For all needs that are not Public Peering:

- get a separate address block,
- announce it to every peer,
- get many peers to donate IP Transit for this block
- put your statistics collector, website, monitoring, rancid, cacti, IXPManager, sflow collector, etc there

Security at IXPs

Verifying routes in Route Servers

- I recently asked an IXP to check what they accept from peers into their Route Servers
- I do keep Cisco prefix lists manually maintained
- I am in the process of changing to BIRD
- want to also automatically update filters based on IRR data

Security at IXPs

Security as Value-add in IXPs

- It's not in the core of the functions of an IXP
- But IXPs are places with a lot of diverse networks connected
- Co-operation to find or investigate security issues

Security at IXPs

Thanks.

Questions ?

Maputo, August 24, 2015