

BGP over an IX: risky business!

BGP over an IX: risky business!

- * Not a question of trust:

peer router may be compromised

BGP over an IX: risky business!

- * Not a question of trust:

peer router may be compromised

- * BGP TCP MD5 hack:

always good to have, but doesn't protect against IP/ethernet layer attacks

Risk #1: taking over IP address

```
conf t
in gi3/0
ip address 193.148.15.1
^Z
```

Risk #1: taking over IP address

```
conf t
in gi3/0
ip address 193.148.15.1
^Z
```

- * Rogue router answers ARP requests for this IP #
- * Alternating correct/incorrect ARP entries for address
- * Feel it right away, harder to find out what the exact problem is

Risk #2: taking over MAC address

```
conf t
in gi3/0
mac 0005.dc66.1008
^Z
```

Risk #2: taking over MAC address

```
conf t
in gi3/0
mac 0005.dc66.1008
^Z
```

- * Switches keep learning different addresses
- * Feel it right away, but invisible on routers, so AMS-IX NOC must diagnose

The solution

The solution

- * Static ARP tables on member routers solve taking over IP address

The solution

- * Static ARP tables on member routers solve taking over IP address
- * Only allowing predefined MAC addresses for each member port solves taking over MAC address

The solution

- * Static ARP tables on member routers solve taking over IP address
- * Only allowing predefined MAC addresses for each member port solves taking over MAC address
- * Only allowing predefined MAC addresses for each member port may solve other stuff as well

The solution

- * Static ARP tables on member routers solve taking over IP address
- * Only allowing predefined MAC addresses for each member port solves taking over MAC address
- * Only allowing predefined MAC addresses for each member port may solve other stuff as well
- * No ARP needed any more, maybe even filter ALL broadcasts?

But deployable?

But deployable?

- * Foundry MAC filters: documentation suggests bad performance, but inconclusive

But deployable?

- * Foundry MAC filters: documentation suggests bad performance, but inconclusive
- * Are there any benefits if not all ports are filtered?

But deployable?

- * Foundry MAC filters: documentation suggests bad performance, but inconclusive
- * Are there any benefits if not all ports are filtered?
- * Management:
 - Yes, more work
 - Should be doable if MAC addresses are assigned by AMS-IX (any equipment that doesn't support configurable MAC address?)

Questions?

Thanks for listening!

comments:

iljitsch@gamepoint.net

(or any of my other email addresses)

