IXP Operations
MENOG6 - Riyad, SA

Kurt Erik Lindqvist
kurtis@netnod.se

Setting up

- There is a lot to be said about forming an IX
  - Governance
  - Founding members
  - Starting capital
  - Legal / Regulation
- But I won't go into to that….

Setting up

- Establishing IXP operations
  - Many IXPs where started by the operators that needed it
  - And it was staffed from NREN / or volunteers
- As an IX grows
  - You will need dedicated staff
  - Either your own, or contracted by the association

Setting Up

- As part of the operation you will want to have resources available to your members
  - Traffic stats for the aggregated IX, public
  - (Traffic stats per port on the IX)
  - A connected members list that is public
  - Ticket system
  - CACTI like monitoring of the equipment, environment etc

Location, Location, Location

- Critical for the operation of an IX is easy access by all operators
  - Important that the datacenter operator / location of the IX is seen to be neutral to the market (I.e not a market actor or competitor to the ISPs at the IX)
  - At minimum access should not be dependent on dominant actor or incumbent

Location, Location, Location

- The datacenter used for the IX should allow for co-location of routers/ equipment by members
  - But also "Distant" connections, i.e dark fiber or transport connections
- The datacenter should
  - If providing co-location for ISPs be accessible 24x7 by everyone

Location, Location, Location

- Have some form of backup power (UPS, diesel or both)
- Have routines for testing power facilities regularly
- (Fire fighting)
- Adequate cooling, hot/cold isle or equivalent

Equipment

- The IX consist of one or more Layer 2 switches. Layer 2 only
- The IX might (should) have free services connected - these are then behind the IX ASN and router
  - But that is not used for the bi-lateral peering

Equipment

- The Equipment should
  - Support mgmt access filtering and monitoring over IPv4 / IPv6
  - Authenticated login
  - 3d party optics if applicable
  - Support (and have enabled) port security, i.e only one MAC address behind each port

Equipment

- Make sure you block spanning-tree
  - You don’t want your IX to be part of your members infrastructure
- Monitor the equipment (with for example Nagios) and have the ops team receive emails and SMSes

Addressing

- Use public IPv4 and IPv6 addresses as allocated from RIPE
  - These blocks should be 'PI' (or IX in the case of IPv6)
- Each participant get one IPv4 one IPv6 address
  - Addressing schemes varies
    - Do not do EUI64 addresses for IPv6

Services

- Co-location of services that are for the common good at the IX is desirable. For example
  - (Your) ccTLD servers
  - Anycasted root-server copies (and perhaps other (cc)TLDs
  - NTP servers
- These services should be behind the IX ASN and that should peer freely with anyone connected

General

- Peering agreements are bi-lateral
  - There have been many attempts at forced multilateral peering, i.e everyone peers with everyone - but no successful one (E.g FICIX - moved from multi to bi-lateral)
- Define a geographical scope for your IX, if it is larger than city/metro it will start competing with your members

General

- A well connected IX, with many local operators as well as access to (peering with) the local ccTLDs and a root-server copy is an important component in a reliable national Critical Infrastructure
  - Examples Estonia vs. Georgia
- Having operators
- This is not the same as regulated or forced interconnects though

Useful links

- EIX-WG in RIPE
  - http://www.ripe.net/ripe/wg/eix/index.html
- Switch wishlist 3.0
  - http://www.ripe.net/ripe/wg/eix/wishlist-v3.0.html
- And once you are up - Join Euro-IX!!
  - A good way to share operational experiences from all around the world with other IXes
  - http://www.euro-ix.net

?