Policies, Security & Reliability in NSI Systems

Henrik Thostrup Jensen htj@nordu.net

OGF43 @ GEC22

March 2015, Washington D.C.

Disclaimer

I am not a network engineer

For more details consult someone who actually knows something about network engineering

Policies

"This isn't Nam… there are rules"

- Walter Sobchak (The Big Lebowski)

- Transit Policies 101
  - Can connect customers with customers
  - Can connect customers with peers
  - Can <u>not</u> connect peers with peers
  - Can connect customers with transit providers
  - Can <u>not</u> connect peers with transit providers
  - Can <u>not</u> connect transit provider with another transit provider
- One network can carry many hats

Policies

- There are lots of exceptions
- Only connect some customers to a certain transit provider
  - NORDUnet does not connect all its customers to GEANT
  - NORDUnet only announces some customers to Telia
- Not all customers are announced to all peers
- It is all about business agreements
  - No one will move your data for free…

Policies

- Transit Policies at its worst…
  - GEANT-NetherLight-NORDUnet-RUNnet
    - And KIAE.ru
  - Sometimes things are not economically rational
    - And cannot be described sensible with AUPs
  - Sometime you cannot connect networks even though it looks like it
  - NML model does not work very well here

Policies

- Policy is not necessarily the same on a link
  - E.g.: NORDUnet might sell RUNnet a 10g link into NetherLight on its 100G link
  - This example fits quite well with GNA

Policies

- Sometimes policy isn’t about transit and AUPs
- The ANA infrastructure
  - A fabric, not really an infrastructure
  - In retrospect: I think this is one of the big sources of disagreement
    - Layer 1&2 engineers will see things as fabric.
    - IP engineers as an infrastructure

Policies

- Fabrics don’t come with rules
  - It comes with a price ☺
- Most NRENs suck at business models and pricing
  - So it is more of a service swap (we are better at those)
  - So there is a limit to how much fabric one can use
- ANA is technologically heterogeneous
  - And multi-domain
  - Hours and hours of super-fun meetings
- Spending some to think about ANA/GNA would be good for NSI

Security

“Distrust and caution are the parents of security”
- Benjamin Franklin

- Case: Transit provider and customer
  - Knowing where to send the bill – and verifying it
  - Do not bypass provider-customer and peering relations
  - Customers pay for the infrastructure of transit providers
  - External parties cannot just allocate resources - only customers
  - Customers can do endpoint verification
    - Extremely difficult for transit networks
  - An obvious attack vector for DOS

Security

- Cancelling connections
  - How does a customer terminate a circuit if the requester is malicious or unavailable
  - forcedEnd should NOT rely on third parties
  - Not involving 3rd parties is good for security and system reliability
  - Also an obvious attack vector

Security

- Case: Network and Open Exchange
  - If a third party allocates resources, terminate/ forcedEnd relies on that third party
  - Control over resources should not rely on third parties
  - Yet another attack vector

Security

- NSA Access Revocation
  - Message proxying / relaying is nightmare
  - Putting the NSA id helps
    - Still relies on third parties behavior
    - Access revocation should not rely on third parties
    - Relies on third parties to correctly identify requester
  - Explicitly allowing an NSA is pretty much the same as setting up a control peering
  - Control peering = Explicit control

Security

- Complete trust in the control place
  - Everyone would have to be okay letting in a new network
  - Pretty much networks don’t work
  - It should be easy to get networks on
    - Full trust in control plane makes this difficult
  - Makes attacks very straightforward

- Everyone trusting everyone is not the way to design a multi-domain system controlling critical infrastructures

Security

- How to increase security
  - Verification over trust whenever possible
  - Avoid 3rd party involvement whenever possible
  - No Relaying – A can of worms for security and reliability
  - Avoid tree as it causes indirect control flow of resources
    - Transit is a resource paid by the customer
    - Transit networks should get explicit notification from customer

Security

- Someone is going to screw up
- There are bugs in software
- Attacks will happen

Reliability

Anything that can possibly go wrong, does
- Murphys Law

- Last week we had a site failure and two link failures
  - AC/DC converter failure at optical pop
  - “Unscheduled maintenance” by link operator
  - Most weeks are better
  - But failures surprinsingly common

Reliability

- Ethernet+VLANs sucks at handling failures
  - A transport technology, not a "real" service
- Ethernet+VLANs across multiple networks = Unreliable service
- If we don't find a way to handle this…
  - The service provided by NSI will be unreliable
  - Guarantying bandwidth, but not protecting against failure
  - Probably a worse service than best effort that can handle link failures

Reliability

- Static circuits is a step back in network engineering
  - Most networks have a way to handle this, but only inside the network
  - But there are several approaches to this between networks (that isn't IP)
  - A very real issue, that we have spend to little time on
  - Doing protected/double paths in NSI is probably the worst approach to this
    - We do not have to re-invent solutions for everything

Reliability

- Technologies that can do this
  - IP (typically only best effort)
  - MPLS (For multi-domain: Labels can be leaked over BGP, e.g. MD-VPN)
  - Carrier Ethernet (IEEE 802.1aq)
  - THRILL (mainly data-center, not backbone)
  - OTN (but only inside a network AFAIK)

Reliability

- Some networks can already provide protected multi-domain circuits
- NORDUnet, GEANT and many of their customers can do MD-VPN (but not all)
  - Not all GEANT customers are multi-homed
  - Have already been used for traffic engineering
- Doing this between domains with different technology is difficult
  - Common denominator is Ethernet and IP
- MD-VPN is low hanging fruit
  - But not enough in itself

Reliability

- Does not have be perfect from day 1
  - Two networks can do protected circuits internally
  - Reduces single point of failure to the demarcation point
  - Some networks already have the capability to provide protected circuits between them
- On message relaying (again)
  - No network will allow third party agents to carry MPLS label configuration, alien waves, etc. for configuration

Summary

- Policies - Networks are full of them
  - Don't ignore them – NOC will nuke the circuits
- Security - Not optional
  - We need to be a lot more conservative
  - Stop doing "the everything model"
- Reliability
  - Things break, especially networks, deal with it
- A lot of the policy and security thinking went into the service table design
  - I might not have communicated this very well
- IMHO these issues are more important than topology distribution…