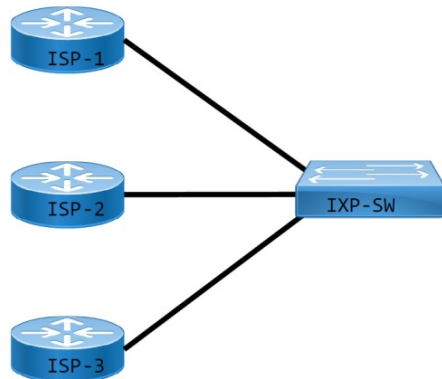


IXP Upgrade Status

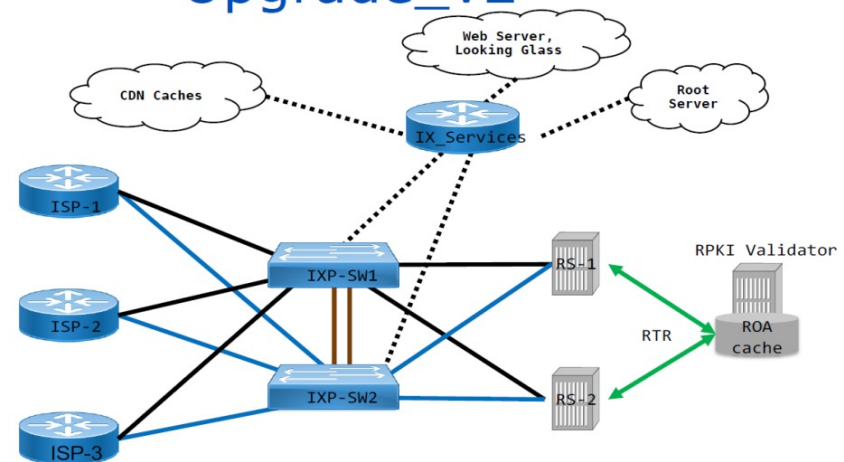
- Discussion with APNIC has commenced in regards to IXP upgrade.
- Works to start within a months time.
- Proposed designs for active and passive setup.

IXP Active Setup

Current Setup - FJIX

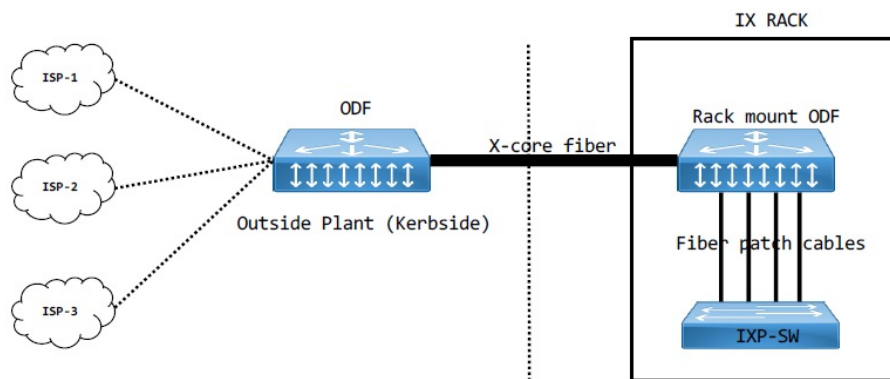


Upgrade_v2

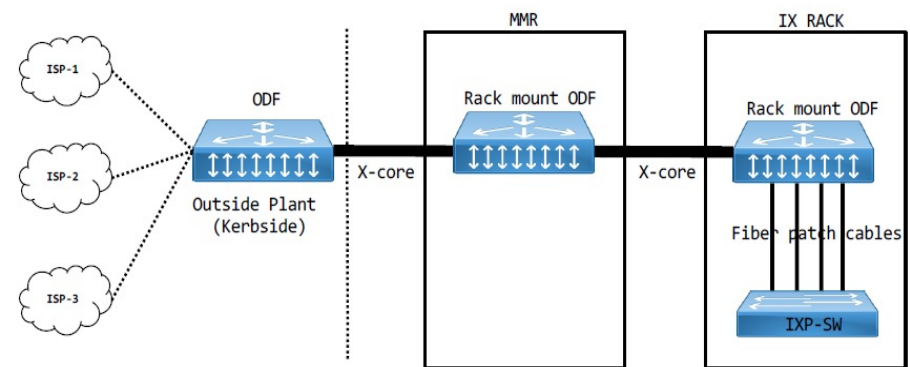


IXP Passive Setup

Passive Network: v1



Passive Network: v2



Security Baselines for IXP

- Enforcement of minimum security baseline for members to join IXP.
- This will include meeting compliance and adhering to standards.
- This practice will provide greater security assurance to other members who are following security best practices.

Incorporating security with IXP design

- Not allowed Ethernet frame formats
- Not allowed Ethertypes
- Link-local protocols, such as IRDP, ICMP redirects, Discovery protocols (CDP, EDP), VLAN/trunking protocols (VTP, DTP), BOOTP/DHCP, etc.
- Restricted by the MAC port security configuration

Vulnerability assessments

- With the help of Trustwave we can get greater visibility of cyber threats.
- Focus on enterprise network security and internet security.
- TAF also analyses this data and share will respective authorities as advisory for known vulnerabilities and threats in Fiji.
- This enables our never ending fight against cyber threats while assuring a much cleaner and safer browsing to our own people.