Fibre Optic Network Reliability & Security

Levels of Protection

Presented by Brian Savory
Business Development Manager, Optelian

UbuntuNet Connect 2012
15-16 November – Dar es Salaam, TZ
Hypothesis

• Can private fibre optic networks provide the same level of reliability and security as carrier provided bandwidth?

Abstract

• Purpose – to provide emerging NRENs information on how to implement a reliable and secure private fibre network
• Design – information collected from personal research and developed from personal professional experience as well as data gathered from being part of the research and education community for over ten years
• Findings - a beginner’s cookbook for developing a reliable and secure private fibre network for research and education
• Value – NRENs “lessons learned” document to refer to when planning and implementing a private fibre network
Fibre Optic Network Reliability & Security

Levels of Protection

Presentation Outline

• Bio
• Background
• Acquiring / owning dark fibre
• Physical layer protection
• Monitoring of optical performance
• Encryption of transmitted data
• Conclusion
Brian Savory’s Bio

• Professional Experience
  ➢ Business Development Manager, Optelian
  ➢ Fibre based transport networks and wireless
  ➢ Built, operated and maintained private fibre optic networks

• Research & Education (R&E) Experience
  – Internet2 Involvement
    • Network Architecture, Operations & Policy Program Advisory Group
    • Program Committee
  – Southern Light Rail (SLR) - R&E Regional Optical Network (RON) in the Southeast, US – Internet2 Connector / commodity Internet provider
    • President & Executive Director
    • University of Alabama System RON connects campuses and NASA Marshall Space Flight Center to Atlanta
  – IEEAF / USAID / RENU Project in Uganda
    • Worked with Ed Fantegrossi / Don Riley
    • Learned many lessons about deploying R&E fibre optic networks in Africa

• Education
  ➢ BSEE, Georgia Institute of Technology
  ➢ MBA, Georgia State University
Background
Causes of fibre Cuts
examples from Level 3 *

1. Most common cause of fibre cuts come from construction companies and excavators that don’t call before they dig.

2. Squirrel chews account for a whopping 17% damages so far this year.

3. Extreme weather conditions - hurricanes, mud slides and ice storms ...

4. Vehicle damage – cars running into telephone poles; truckers underestimating the height of their rigs.

5. Vandalism - 7% of annual outages to people using fibre cable for gun practice

6. Phone cables and electrical cables on the same pole – dust storm blew down a poles; stress on the cable pulled down more poles, until 19 poles were lying on the ground.
Causes of fibre Cuts
examples from Level 3 *

7. Plane crash – small plane overshot the runway and clipped a pole that fibre was attached.

8. Ice storm caused limbs fall onto the electric utility primary power which crossed into the communications space. The cable caught on fire in multiple places while suspended in the air and surrounded by ice covered limbs.

9. During the cleanup efforts after hurricane Katrina, one of our field managers was about 2 miles inland when he spotted a three foot long shark in one of the trenches beside our fibre.

10. Right-of-way dispute – unhappy landowner dug 2 ft. by 10 ft. trench and cut the fibre and ducts; when field techs got on scene, landowner was waiting on them with his 12 gauge shotgun.

* “Beyond Bandwidth” - Level 3 Communications Blog, “The 10 Most Bizarre and Annoying Causes of fibre Cuts”, August 4, 2011 By Fred Lawler
Fibre Optic Network - Data Vulnerability

- In 2000, three main trunk lines of Deutsche Telekom were breached at Frankfurt Airport in Germany.
- In 2003, an illegal eavesdropping device was discovered hooked into Verizon's optical network.
- International incidents include optical taps found on police networks in the Netherlands and Germany and on the networks of pharmaceutical giants in the U.K. and France.
- John Pescatore, Gartner Vice President, distinguished analyst and a former NSA-trained U.S. Secret Service security engineer, said that while fibre optic cable hacking had been taking place for nearly a decade, avoiding detection and processing the stolen data was much more difficult. Things have changed.
- The required equipment has become relatively inexpensive and commonplace and an experienced hacker can easily pull off a successful attack.
- "You can jump on the Internet right now and buy a tap for about $900," says Andy Solterbeck, General Manager of the Data Protection Business Unit at SafeNet, an encryption company.
Network Security - Acquiring / Owning Dark Fibre Assets
Acquiring / owning dark fibre

- Dark fibre network - privately owned and operated optical fibre network over dark fibre leased or purchased from another supplier, rather than by purchasing bandwidth or leased line capacity from a carrier, thereby avoiding outages caused by carrier circuit grooming.
- Dark fibre networks may be used for private wide-area networking infrastructure or as Internet access infrastructure.
- Dark fibre networks may be point-to-point, point-to-multipoint, or use self-healing ring or mesh topologies.
- Dark fibre networks can operate using wavelength division multiplexing (WDM) to add capacity where needed and to provide an upgrade path between technologies without removing the network from service.
- Dark fibre metropolitan area or regional networks can use relatively inexpensive Gigabit Ethernet equipment over WDM, rather than more expensive SONET ring systems.
- Dark fibre networks offer high bandwidth for research collaboration, video and wireless.
Physical Layer Protection
Physical Layer Protection

• Fibre network design
  – The ideal network design features multiple fibre-optic providers connected via dual-entry with self-healing optical network architecture. This redundant connectivity ensures network resiliency.

• Aerial fibre vs. underground fibre
• Diverse fibre routes
• Dual fibre entry
Aerial vs. Underground

- It is a common misconception when considering fibre backbone security that underground fibre is more secure than aerial.
- However, both aerial and underground installations are subject to fibre outages.
- Yet aerial installations are lower cost and easily allow for alternate cable routes; aerial construction is as much as 40 to 50 percent less expensive than underground.
- The security strategy to minimize the disruption is to reroute data from damaged or destroyed fibre optic cables to other fibre optic cables so that networks that remain intact.
- The optimal strategy for building a fibre network is to have a hybrid strategy that employs both aerial and underground fibre in order to provide a cost effective reliable fibre plant.
Diverse Routes - Protection Switching

- A major factor in network reliability is to make sure the fibre backbone has redundant fibre routing available.
Diverse Entry

- In order to ensure optimal network reliability all buildings, data centers, wireless sites and telecom hubs should have dual entries into the telecom equipment facility.
Network Security - Monitoring Optical Performance
Monitoring Optical Performance

- Optical link monitor (OLM)
- Path protection module (PPM)
- Optical Time Domain Reflectometer (OTDR)
Optical Link Monitor

- Detects fibre intrusion, fibre degradation or fibre cut
- Measures and reports round-trip link loss on the link as well as transmit and receive power levels
- Generates alarms when any of these measured values cross preset thresholds, pinpointing the location of a fault without manual intervention
- Loopback module at the remote site is fully passive and temperature hardened
Path Protection Module (PPM)

- Provides automatic switching between primary and secondary optical paths based on provisionable power thresholds.
- Optical protection is provided by redundant primary and secondary transmit paths. In the receive direction, the optical power levels of the primary and secondary inputs are continuously monitored. The switch back mode, from secondary to primary path, is configurable and can be set to automatic or manual.
Optical Time Domain Reflectometer (OTDR)

- Single Mode Optical Time Domain Reflectometer
  - Used to estimate a fibre's length and overall attenuation
  - Used to locate faults, breaks and to measure optical return loss
  - Light weight, compact, hand-held unit that can save and transfer the measurement data to a PC
- Embedded OTDR solution as part of WDM system
- OTDR module as part of a optical node shelf

Sample OTDR Trace

[Graph showing OTDR trace with Time, Power, and Distance axes, highlighting a fault location]
Network Security - Encryption
Encryption Primer

- IP-based data method for protection - MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices
- The Advanced Encryption Standards (AES) defined by the U.S. National Institute for Standards and Technology (NIST) are the current de facto standards for encryption in enterprise networks.
- AES-256 - 256 bit key is most secure

Encryption of Transmitted Data

- Layer -1, -2 or -3
- WDM
Transport Security - Encryption

Principles of Encryption

L3 encryption

Router  
Site A  
DWDM-transport  
Site B  
Router

L2 encryption

Router  
Switch  
Layer-2 Encryptor  
Site A  
DWDM-transport  
Layer-2 Encryptor  
Site B  
Switch

L1 encryption

Router  
Switch  
Site A  
DWDM-transport  
Site B  
Router

Optelien
DWDM Transmission with Encryption

Transmission over fibre

Client Interfaces

Optelian
Conclusion

• With proper physical layer, optical network design and encryption, if required, a private fibre optic network can provide the same or a better level of reliability and security as carrier provided bandwidth.