



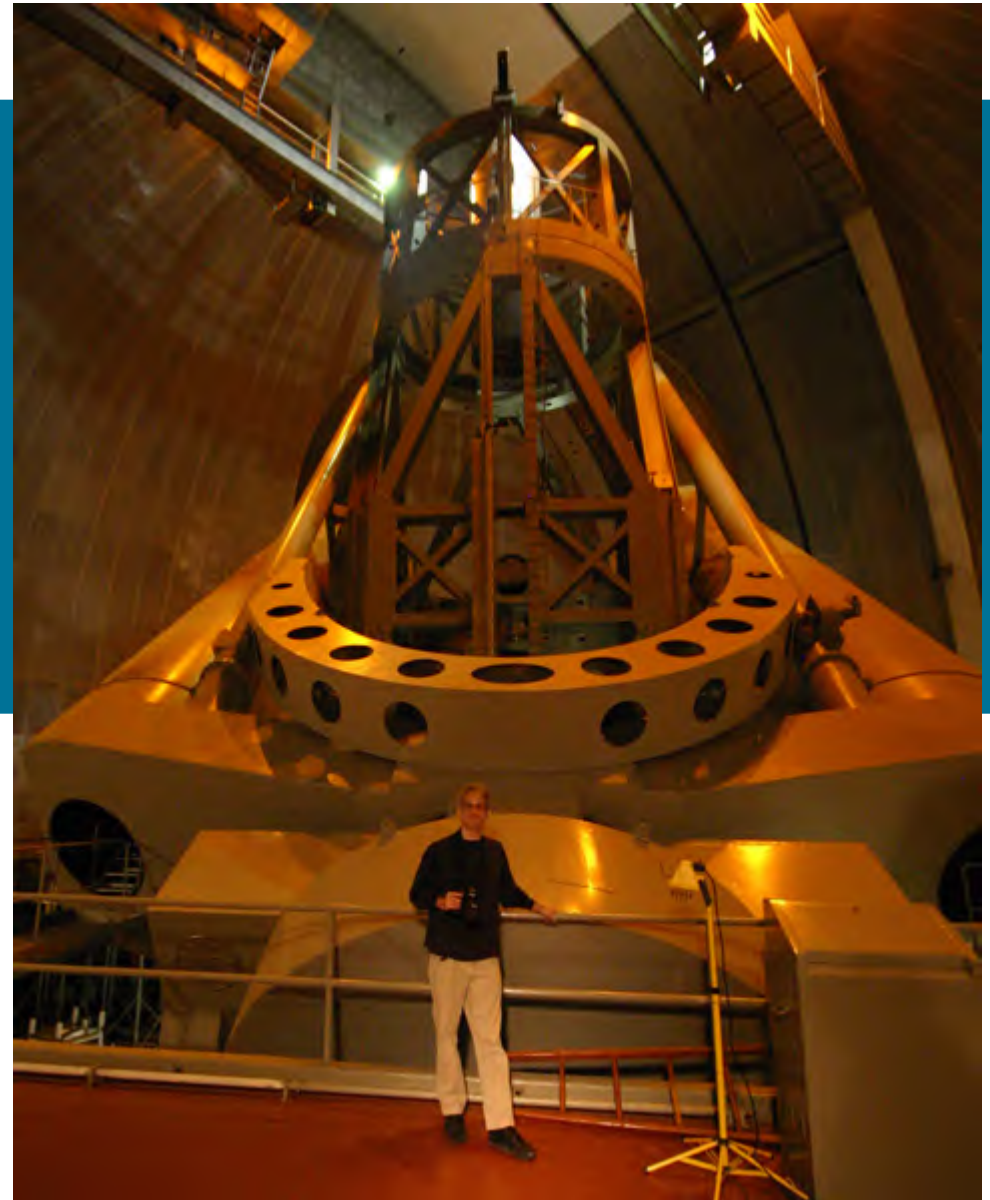
# Protecting FPP / FCF connections

Protecting links of the Control Plane

Landon Curt Noll  
chongo@cisco.com

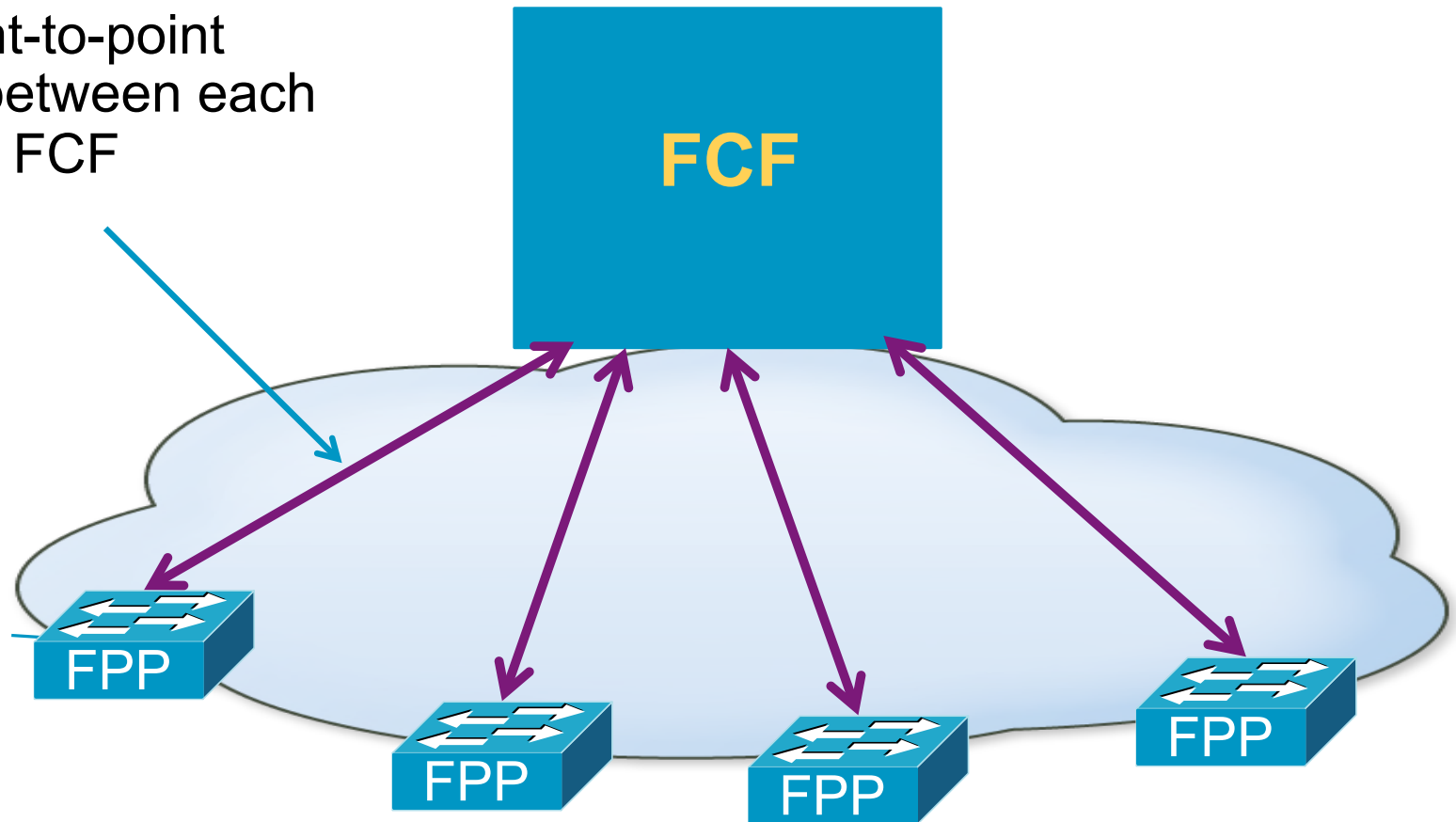
T11/10-033v1

Landon Curt Noll and the Palomar 200-inch telescope  
"Who is watching your fabric?"



# FCoE Control Plane

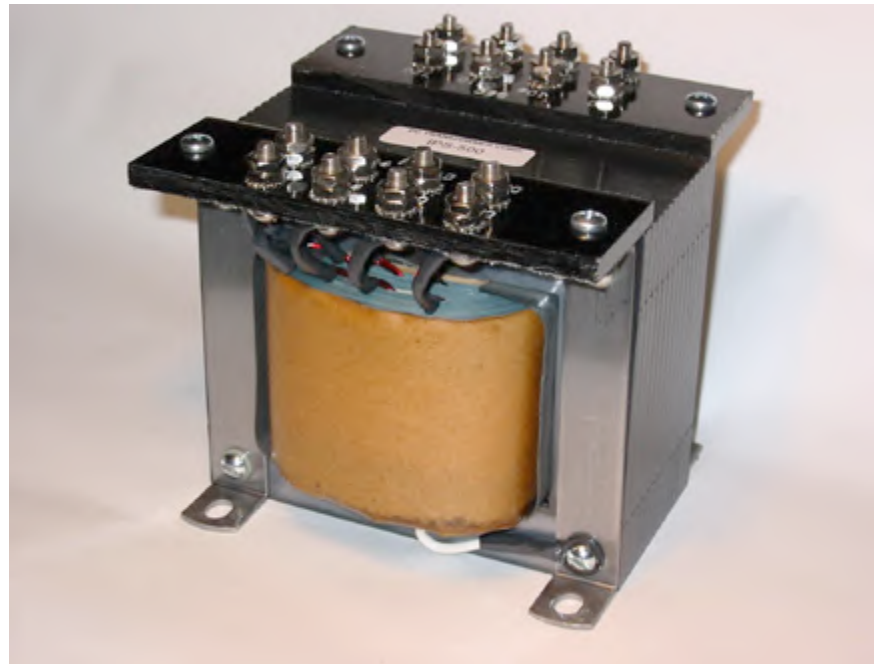
A virtual point-to-point connection between each FPP and the FCF



# FPP / FCF connections

---

- Support a delegation protocol used by the FCF to delegate to the FPP
- Support a protocol to collect statistics and monitor traffic
- The FPP to FCF connection must be secured!



“Isolated yet still connected”

Isolation transformer  
image credit:  
pctransformer.com

# How do we protect FPP / FCF links?

- We must protect control plane traffic from modification!
  - Add Cryptographic Integrity to FIP
  - Co-exists with Encrypting control plane traffic
- Encrypting control plane traffic as a defense in depth
  - Example: MACsec (IEEE 802.1AE)
  - Optional but recommended
- Need a non-IP based solution for FC
  - Don't complicate FC by requiring IP stacks and addressing
  - Don't compound the threat model by introducing IP protocols
  - Eliminates: IPsec, SSL/TLS, and other IP related solutions



Highly Lossy Ethernet  
Image credit: wikipedia  
Creative Commons License

# Protecting links requires keys

---

- Securing the FPP / FCF connection will require the use of cryptographic keys
- Those keys need to be distributed and managed
  - Manage keys throughout their lifecycle
  - Key use and state change audit logs



# Key Management Methodology #1

- Manual Key Management

- For simple environments
- Use pre-shared keys
  - Distribute by “*sneakernet*” or equivalent method

- Pro:

- Simplistic

- Con:

- Naive
- Simple environments have a habit of growing into complex environments
- Manual key management may be neglected
- Manual method will almost certainly fail a security audit



Image Credit:  
Wikipedia  
Creative Commons License

# Key Management Methodology #2

- Key Management Service using OASIS KMIP binary messaging with IEEE P1619.3 architecture
  - For both simple and complex environments



**“That is a BIG prime!”**

Image by [Matthew Harvey](#) © 2003

- Pro:
  - Conforms with best practices
  - OASIS KMIP 1.0 (public review started Dec 2009)
    - On track for Federal Information Processing (FIP) consideration
  - Avoids most neglect problems
- Con:
  - Requires FC aware Key Managers in your data center
  - Requires adding KMIP clients into devices

# Thank You!

---



Button © takomablbelot  
Permission to use with attribution