# Security implications of optical bypass

- Lambda appears in middle of campus
  - Passes all but fiber plant
  - Lands on a desk… or in a cluster
- Security implication
  - Dual home, bypass all campus security
  - …and they'll run BGP on it
  - Becomes local net provider (i've got a great connection, want to use some?)
- Diagnosis is suddenly impossible to worse

- Responsibility
  - Who gives the IP addr…
  - Research over network vs. on networks
  - Network arch implications, not so much end host issues
- Policy statements
  - Treat them like outsiders?  Thus certain services on campus respond as if they were off campus elements
- Is it just a big modem?  How is it diffferent?
  - User expectations on usage of lambda is fundamentlaally different

- Blackhole flows if source IP doesn’t match..
  - Whose prob is it?

- Who takes responsibil?

- Replicate the infrastructure
  - But then you have to purchase dwdm gear…
    - And the security stuff is what they wanted to avoid
  - Use optical taps… (w/r/t performance)
    - This is all expensive

- Application routing
- Campuses not knowing what is happening when/where
- Xref ARIN registration process for Ips and having Ren-isac be the clearing house for dynamic lambda route info
- Scaling issues…
- Campuses talk to RONs, not the end user

- Who are the policy folks?
  - This is over their heads…
  - Need the tech folks to take lead
- Work with RONs to not work directly with researchers
  - Try to get campuses back into the line
- BCP and/or Clearinghouse
- We need to get the Dragon/UCLP/BRUW folks in the room
  - Get them to integrate reporting out of path info to clearinghouse