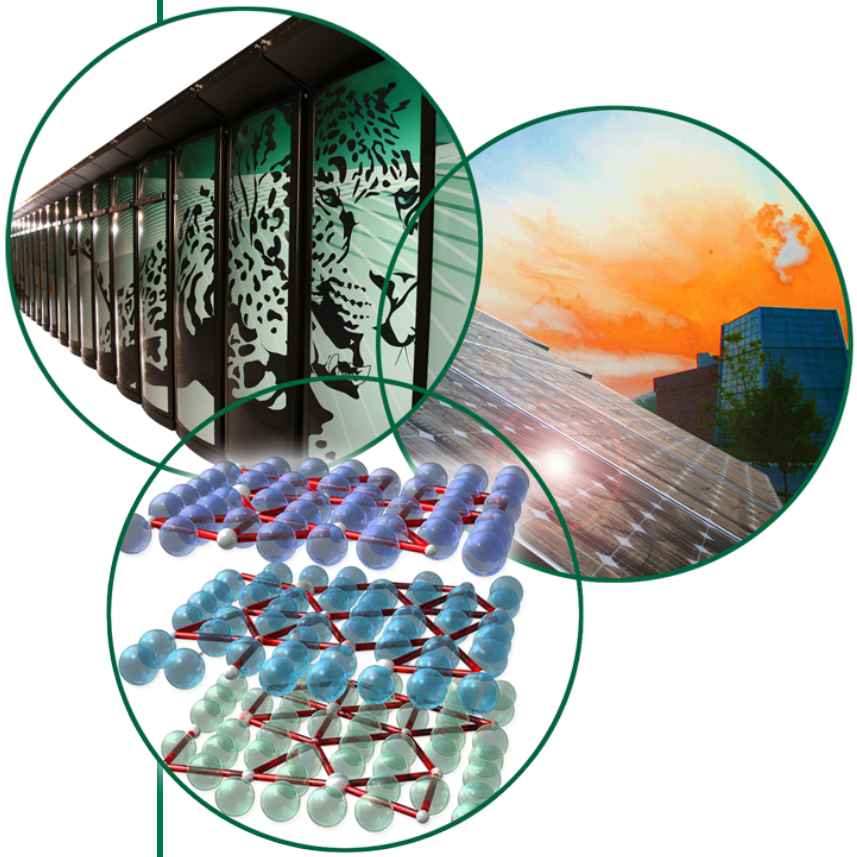
ORNL Minimal Internet Experience



ESCC

Jan 2012

Susan Hicks

U.S. DEPARTMENT OF ENERGY

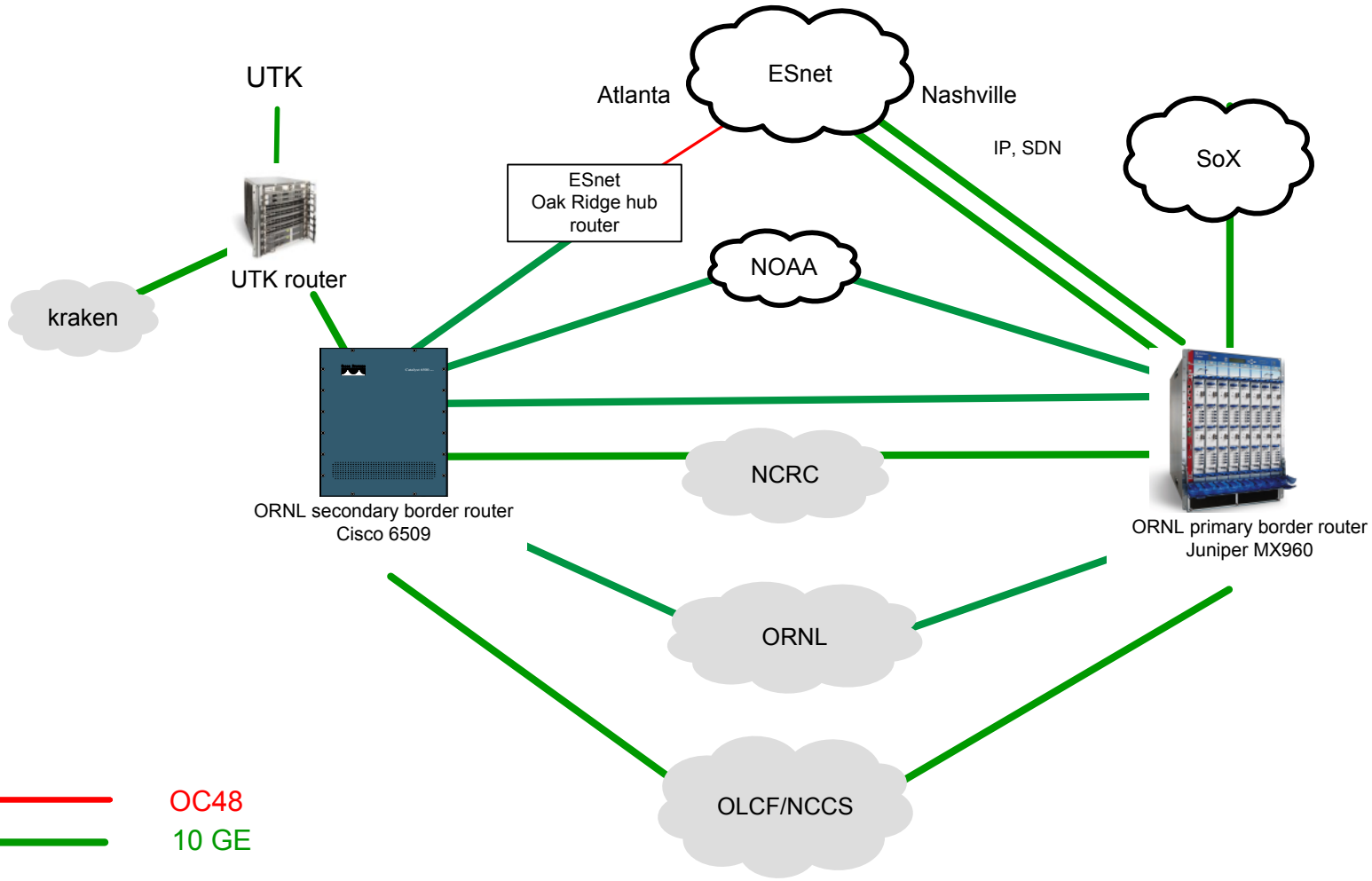
OAK RIDGE NATIONAL LABORATORY

MANAGED BY UT-BATTELLE FOR THE DEPARTMENT OF ENERGY

Minimal Presence Implementation

- Implemented minimal presence due to incident last April
- Did not disconnect from the Internet
- OLCF, NCRC not affected
- Some projects remained accessible
- User access suspended (email, web, etc.)

ORNL External Overview



OAK RIDGE National Laboratory

Need Predetermined Plans

- Administrative
  - Who is driving what
  - Channels of communication/approval
  - Identify key personnel
- Technical
  - How to segregate/isolate
  - Rebuilding systems

Predetermined Plans Continued …

- Identify Critical Functions Requiring External Access
  - Financial Systems
  - Emergency Management Systems
  - DOE Sponsored Projects
  - WFO Projects
- Identify Systems
  - Groups of Systems
  - Services

Lessons

- Insufficient Segregation (network, services, roles)
  - Business and Research
  - Within Research
  - Infrastructure
  - Privileged Credentials
- Early Detection and Containment is Crucial
  - More Comprehensive Monitoring Needed

Questions?

OAK RIDGE
National Laboratory