

# ESnet RADIUS Authentication Fabric

---

- **Title:** The ESnet RADIUS Authentication Fabric (*New Proposal*)
- **Investigators:** Michael Helm, Abdelilah Essiari; Olivier Chevassut, Dhivakaran Muruganantham, Mary Thompson, TBD.
- **Funds Requested** (FY2006): \$416,444
- **Long-Term Funding:** (amount, source, likelihood): \$475,000; DOE MICS office will make deployment and funding decision in FY06
- **Goal:**
  - Federate One-time password (OTP) deployments at DOE labs to enable researchers to use the same token to authenticate across sites.
  - Benefit all of DOE's collaborative science and distributed computing programs by providing easy to use, best practice cross-site authentication.

# ESnet RAF: Business Case

---

- One Time Passwords
  - Robust, simple protection from identity theft (most important hacking vector)
  - Comparatively simple to deploy and use
  - Users and applications cannot cope with multiple tokens and deployments
- RADIUS – IETF / industry standard authentication protocol
  - All OTP vendors support RADIUS
  - RADIUS will route OTP token codes to site OTP verification databases
- DOE Labs and collaborators will federate OTP authentication at the RADIUS servers that constitute the RAF
- Results:
  - Applications support a single authentication protocol: RADIUS
  - Users need only a single OTP token: issued by home site
  - Distributed computing and large scale science
    - Secure, defensible environment
    - “Best case” outcome for scientists and support staff

# ESnet RAF: Approach

---

- Issue: Reliable service – 24x7 geographically dispersed service
  - We need to complete development of the RAF architecture:
  - Tested integration of multiple OTP deployments
    - Error conditions must be signaled to users and administrators
    - Challenge-response must be fully supported
  - IPSEC support between RADIUS servers and clients, and OTP back end authentication servers
- Issue: Protocol development – Kerberos and secure authentication support
  - Kerberos and RADIUS *must* work together
    - Support FNAL and other similar OTP+Kerberos deployments
  - We need to provide more complete end-to-end security beyond RADIUS
- LBNL and ESnet have a unique combination of capabilities
  - Advanced cryptographic research experience AND deployment capability for security solutions
  - Access to remote facilities
- RAF is a unique opportunity to provide benefit for all of DOE's collaborative science and distributed computing programs