NSLS-II Control System Cybersecurity

Robert Petkus
NSLS-II Controls

Control System Cybersecurity Workshop, ICALEPCS
11 October 2009

2009 ICALEPCS

BROOKHAVEN
NATIONAL LABORATORY
BROOKHAVEN SCIENCE ASSOCIATES

Outline

- Scope and Overview
- BNL Lab Policy
- Controls Network Architecture
- External Access
- Beam-lines
- Wireless
- Security Tools
- Conclusion

Scope Overview

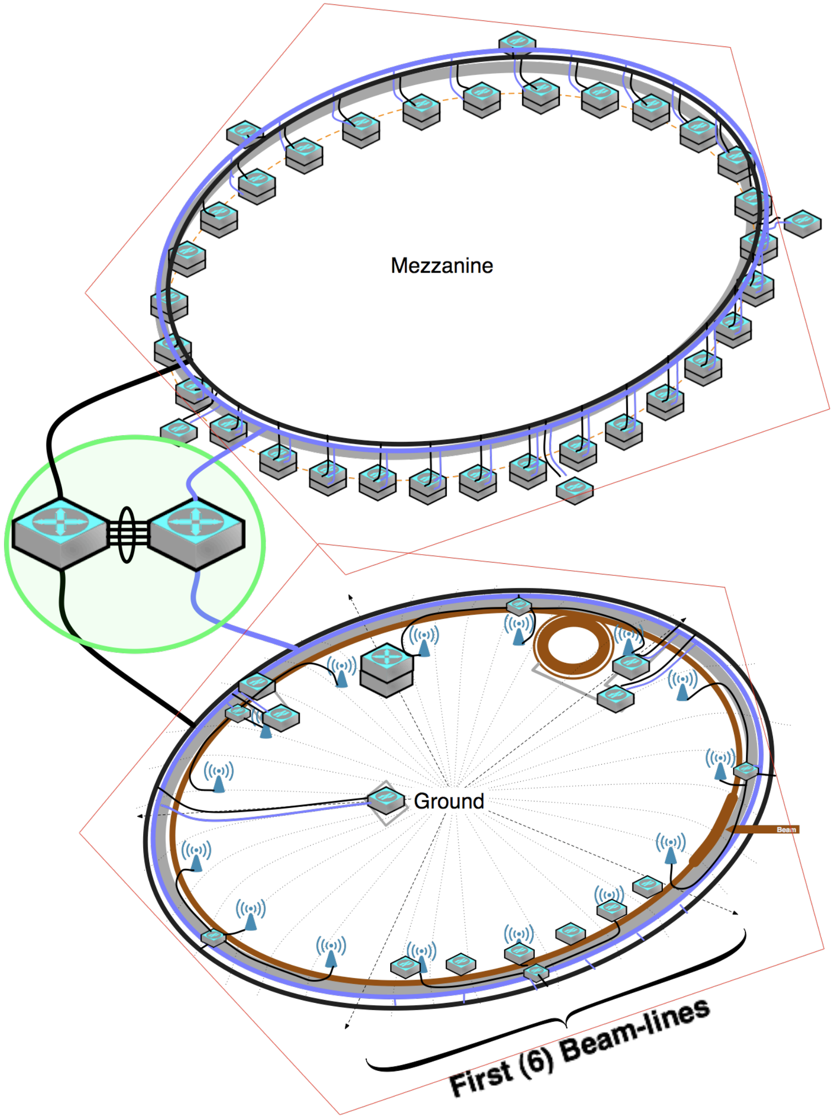
- Design a robust, scalable, and secure network
- Offer excess multi-path bandwidth
- Compliance with NIST cyber recommendations
- Security and flexibility at the beam-lines
- Provide transparency to IT management and retain operational autonomy (abide lab doctrine)
- Deploy comprehensive real-time monitoring

Lab Policy

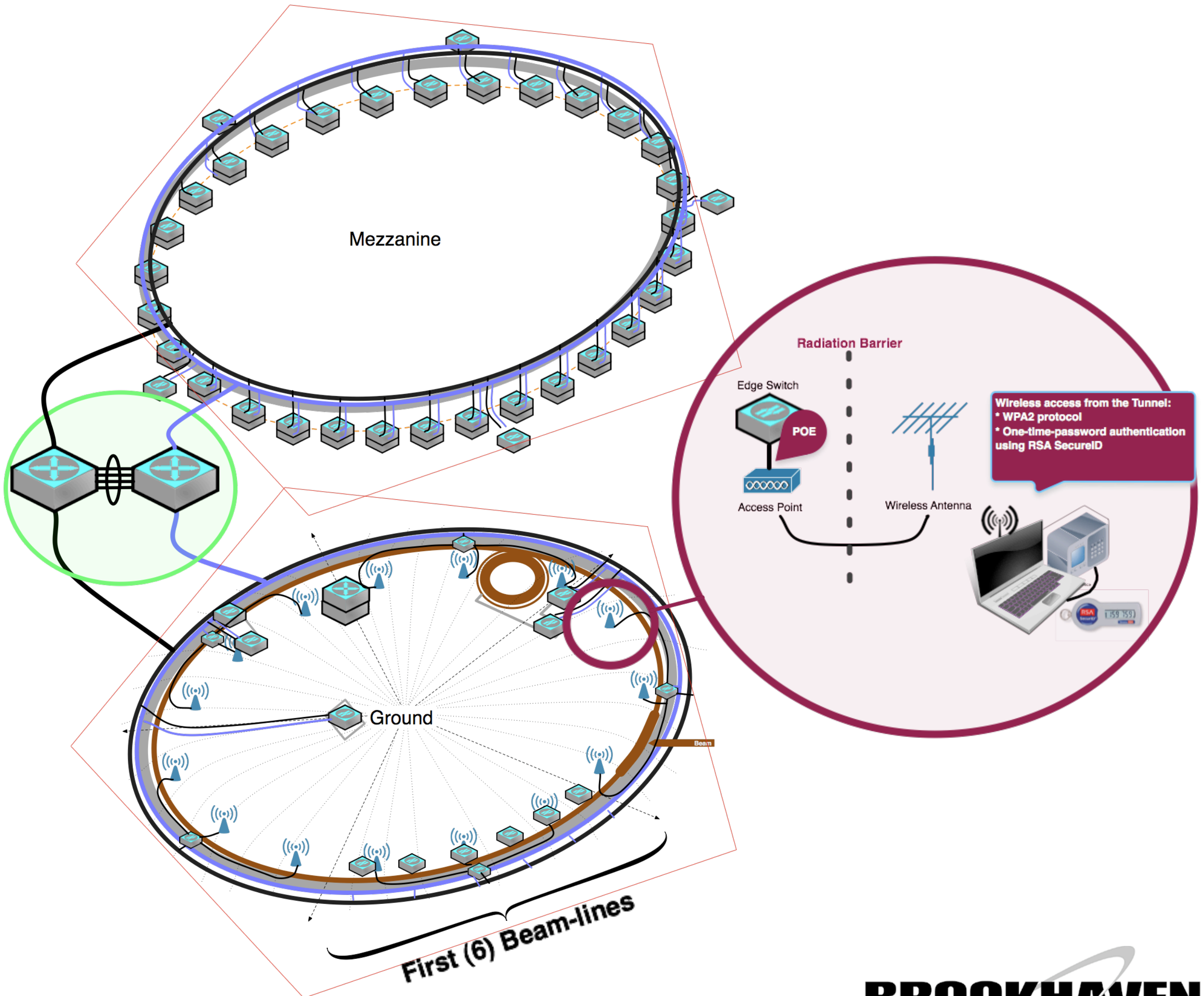
- Minimum security as specified in several NIST publications
  - Information systems (800-53)
  - Remote access (800-46)
  - Wireless (800-97)
  - Industrial control systems (800-82)
- Encrypted central log facilities
- Periodic vulnerability scanning (Nessus)
  - Goodbye crate
- Strong authentication - CryptoCard or RSA SecureID
- Authorization against lab-wide Active Directory
- Incorporation of lab configuration standards using a configuration manager (Cfengine)

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Control Network Architecture

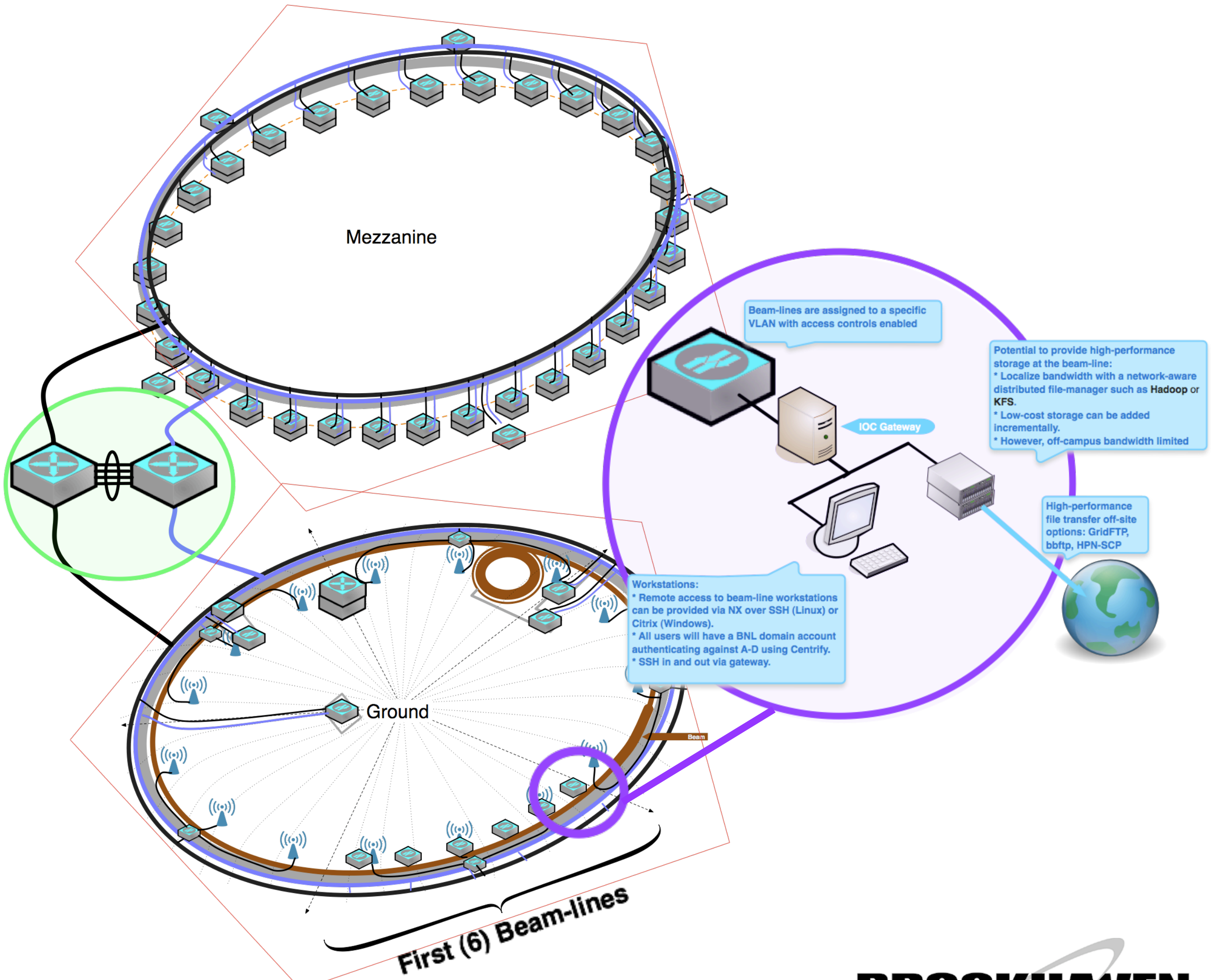


Control Network Architecture



Wireless access from the Tunnel:
* WPA2 protocol
* One-time-password authentication using RSA SecureID

Control Network Architecture



Beam-lines are assigned to a specific VLAN with access controls enabled

Potential to provide high-performance storage at the beam-line:

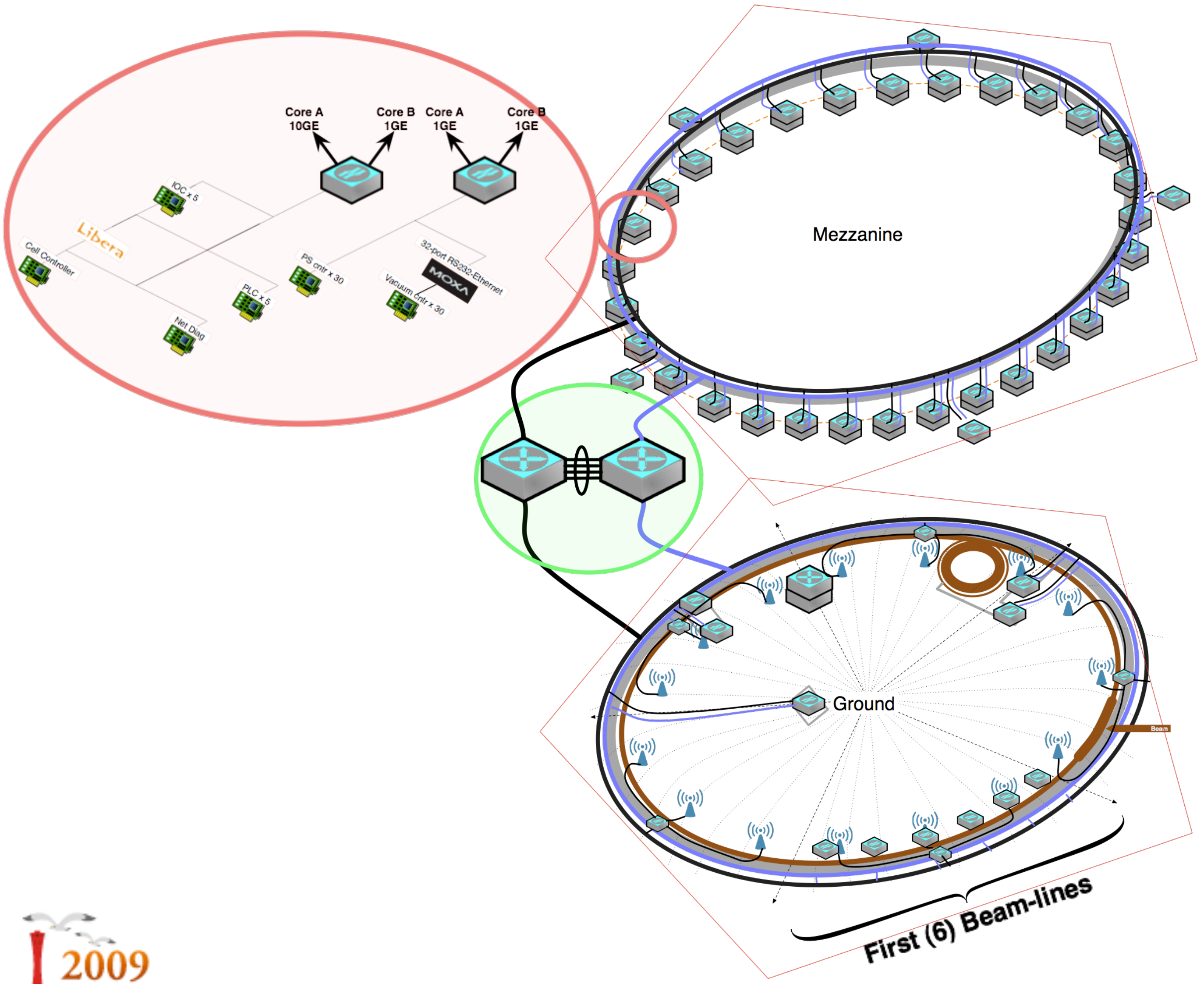
- Localize bandwidth with a network-aware distributed file-manager such as **Hadoop** or **KFS**.
- Low-cost storage can be added incrementally.
- However, off-campus bandwidth limited

High-performance file transfer off-site options: GridFTP, bbftp, HPN-SCP

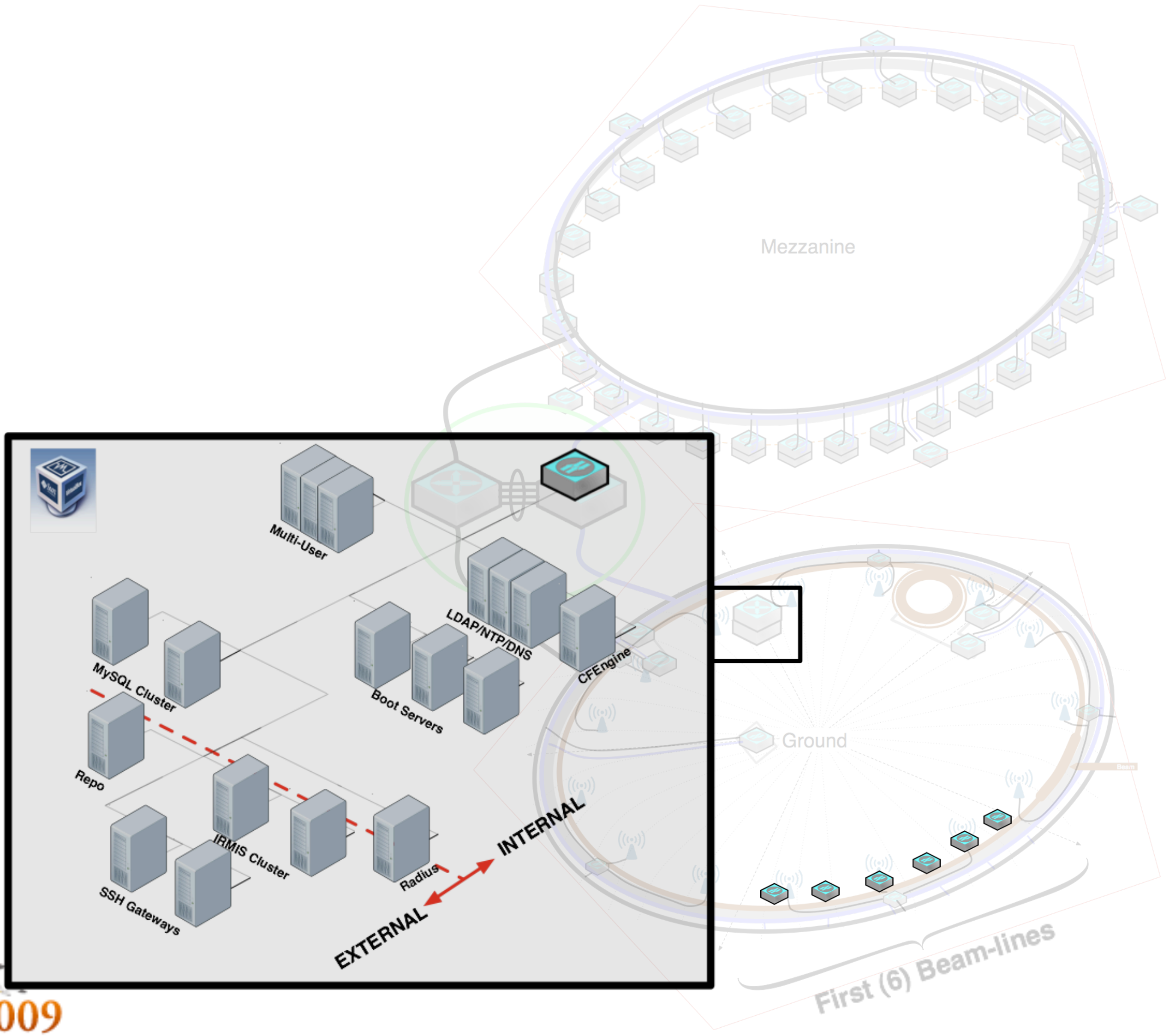
Workstations:

- Remote access to beam-line workstations can be provided via NX over SSH (Linux) or Citrix (Windows).
- All users will have a BNL domain account authenticating against A-D using Centrify.
- SSH in and out via gateway.

Control Network Architecture



Control Network Architecture



Control Network Overview

- Private network discreet from the BNL campus network
  - No email, web-surfing, cross-pollination of any sort
- Benefits - Security
  - 100% resource dedication, no hefty port channels burdened with office or VoIP VLAN chatter
  - Insulation from destructive vulnerability scanning
  - Operational control
- Cons
  - Points of ingress/egress are required though...
  - Can all user expectations be provided for?

Control Network Overview

- The network will utilize VLANs and ACLs to segment traffic into logical broadcast domains for improved performance
  - IOCs, BPMs, PLCs, power supplies, etc., occupy different VLANs
  - ACLs define exceptions and granular access
  - Addresses will be allocated to ensure that each block can be referenced by a single ACL
- Adoption of QoS and Storm Control functionality to control unknown or "hazardous" unicast / broadcast traffic
- Centralized configuration management of network
- All switch ports disabled by default - devices can't be attached to network ad-hoc
  - Registration of all MAC addresses
- SSH/TACACS+ access to switches for accreditation/encryption
- SNMPv3 using SHA authentication and AES encryption

External Access Production

- Interactive access to the controls network offsite via multi-homed SSH gateways
  - OpenSSH-LPK (code.google.com): public keys stored in LDAP
  - One-time-password (OTP) hard/soft token a la CryptoCard or RSA SecurID
  - SecurID continuously generates a new synchronized password every 60 seconds
  - CryptoCard utilizes a challenge-response based on portions of the prior session string - often requiring resynchronization
  - SecurID likely to be the only sanctioned mechanism when NSLS-II enters production
- VPN solution under consideration

External Access Today

- To-date, the controls group uses the general campus SSH gateways or a SSL / IPsec Cisco VPN
- OpenVPN server software on the controls private lab network enable other groups *within* the lab to gain access.
  - OpenVPN is simplistic to deploy and relies on SSL and DHCP
- LDAP-TLS is utilized for AA
  - Migration to lab-wide Centrify (AD integration for UNIX platforms via PAM) by year’s end
  - Centrify for authorization within the controls private network remains an open question. Options include
    - Authorization through a multi-homed relay
    - OpenLDAP proxy to AD
    - Stand-alone LDAP deployment (double work)

Beam Lines

- Beamlines are assigned to their own VLANs
- Channel Access Gateways stand between their hardware and ours
- External access to workstations can be achieved using NX over SSH (Linux or Solaris Server, All clients) or Citrix (Citrix XenServer on Linux, all clients)
  - Key, certificate, or two-factor authentication
- *However* all users with access to the controls network must have a valid BNL account
- Ingress filtering to protect against MAC spoofing - drop packets whose source address is unqualified

Beam Lines + Secure Storage

- Network is designed to provide for a secure distributed storage solution
  - 131 Gbps bandwidth local to switch, 20 Gbps uplink
  - Inexpensive, high-performance storage management solutions with either robust or nascent security potential
    - Hadoop (Map/Reduce reverse eng. of Google FS)
      - Implementation under development for client-side encrypt/decrypt and kerberos integration
    - KFS (another recode of Google FS)
    - NFSv4: gss / krb5p
    - GlusterFS (parallel FS with storage aggregated via IB RDMA or 1/10GE)
      - Implementation available utilizing Stunnel for encrypted transfer
      - Investigations into Cisco's General Routing Encapsulation
  - File transfer using BBFTP (no encryption of data, usernames only), GridFTP (certificate based authentication and encryption)

More on NX

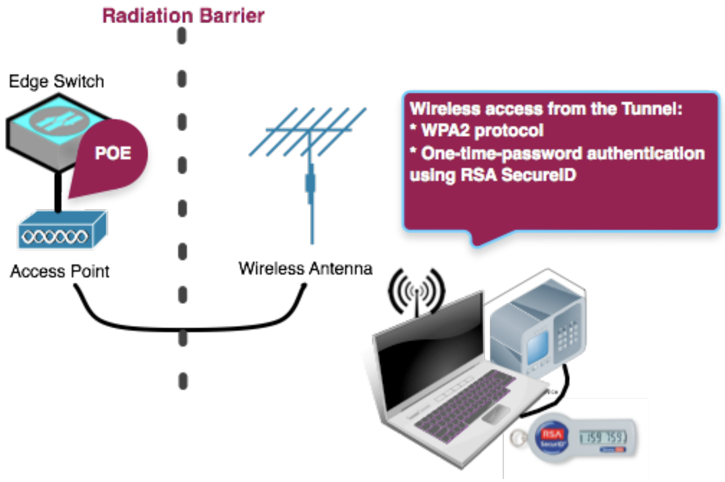
- NX and Citrix are (2) attractive implementations of secure remote desktop software for potential consumption by staff and researchers
- NX currently in use in the controls group, consists of:
  - NXServer: allows UNIX system to act as terminal server, balances requests among NXNodes
  - NXNode: support 1000s of connections, redistribute sessions among servers, chooses shortest network path to user
  - NXAgent: multiplex X client connections into single connection
- NX uses highly-efficient X protocol compression using differential encoding and image streaming
  - Maintains memory cache (messagestore) achieving 60-80% hit rate (100% for images)
  - Encodes and calculates checksums, decodes on the fly
  - Uses a fixed TCP window accepting only enough bytes to make a full packet at that size
  - Final stream of data ZLIB compressed for a reduction of 30%
- Can encapsulate RDP (MS) and RFB (VNC)
- Tunneled via SSH
- Cryptographic host key exchange
- On the other hand, VNC:
  - Draws remote screen by sending huge amounts of data over wire
  - Screen differences sent on client pull, no client caching

NX and Citrix

- Citrix Metaframe, based on an adaptively pushed server buffer with client-side caching has been replaced
- Citrix XenServer constitutes a wholly new architecture
  - Combines Xen Hypervisor on Linux, a Virtual Desktop Infrastructure (VDI) where an entire user environment is accessed remotely
  - Like other VMs, network traffic is bridged to ensure packets are isolated from one another
  - Each user has their own dedicated desktop image including the OS and applications, OS is streamed to desktop on demand
  - Essentially, the same cryptographic host key exchange as in NX
  - Encrypted connection is handled via SSH or (preferably) the XenAPI SSL network service
  - “Xenstore” process determines client ACLs and ensures the client can only touch his domain
  - Optimal configuration urges expensive storage backend (NetApp)
- Conclusion
  - For an unrestrained (free) experience with NX, I recommend FreeNX
    - Although this version does not offer load balancing or other advanced features
  - Citrix is a powerful enterprise suite but is expensive and potential overkill

Wireless Controls

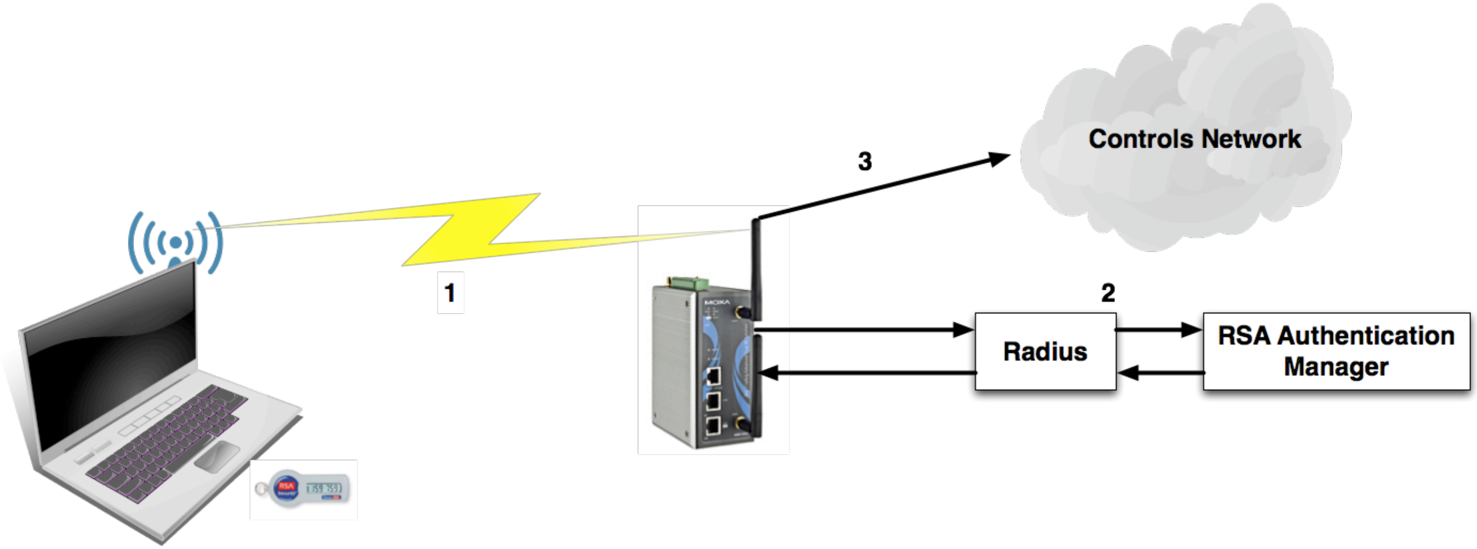
- Reduce infrastructure costs associated with cabling the entire tunnel
- Inexpensive external antennae better suited for a harsh environment
- Simplified power profile using PoE switches
- Ease of access during commissioning (push cart)
- Secure



Wireless access from the Tunnel:
* WPA2 protocol
* One-time-password authentication using RSA SecureID

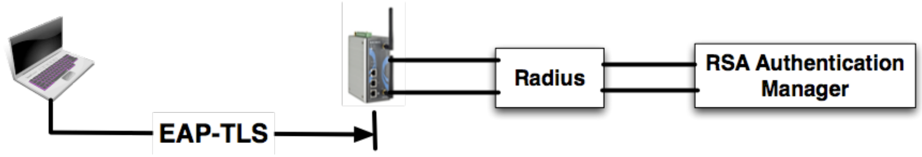
Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID



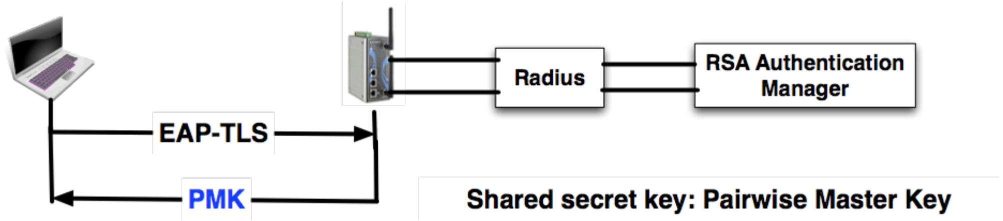
Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID



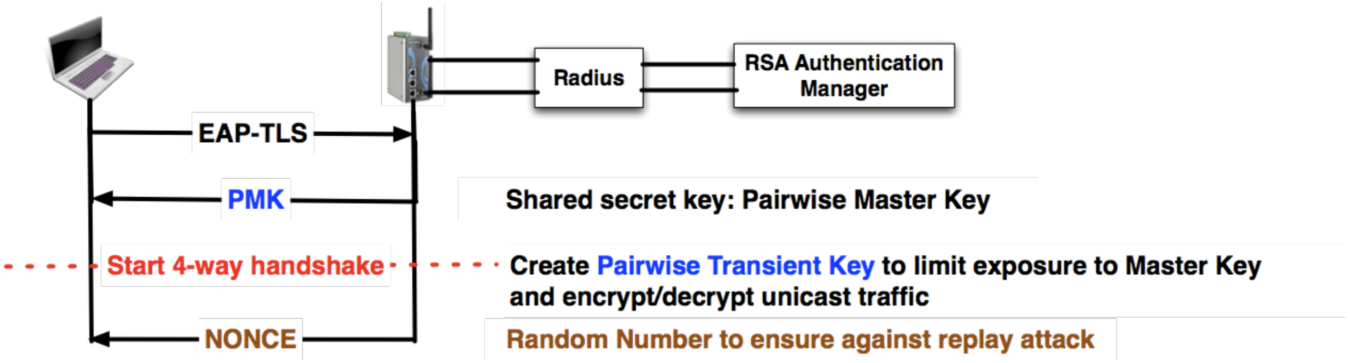
Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID


Radius
RSA Authentication Manager
EAP-TLS
PMK
Shared secret key: Pairwise Master Key

Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID



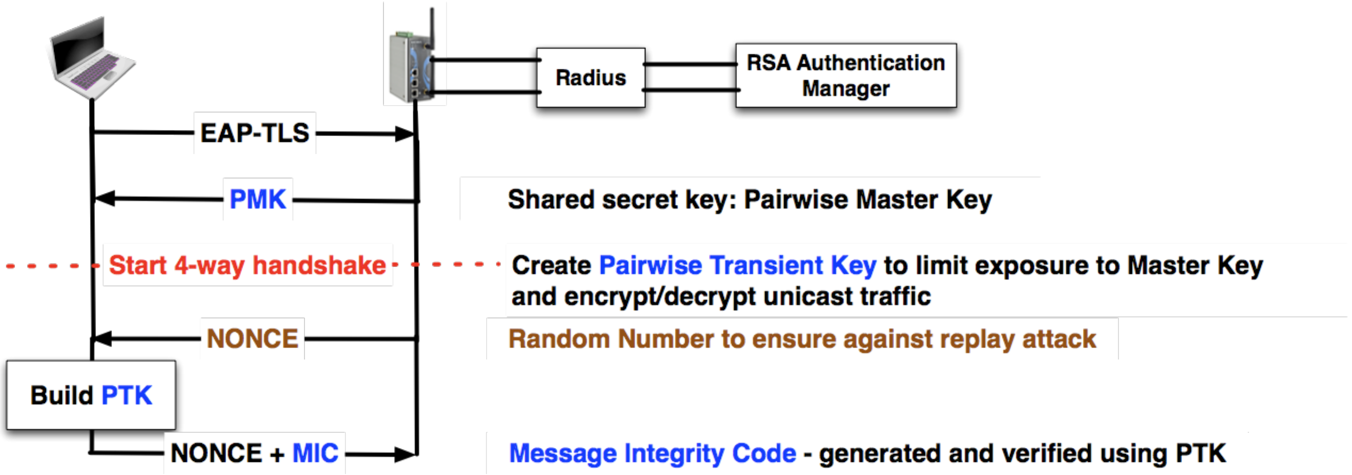
Shared secret key: Pairwise Master Key

Create Pairwise Transient Key to limit exposure to Master Key and encrypt/decrypt unicast traffic

Random Number to ensure against replay attack

Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID



Radius

RSA Authentication Manager

EAP-TLS

PMK

Shared secret key: Pairwise Master Key

Start 4-way handshake

Create Pairwise Transient Key to limit exposure to Master Key and encrypt/decrypt unicast traffic

NONCE

Random Number to ensure against replay attack

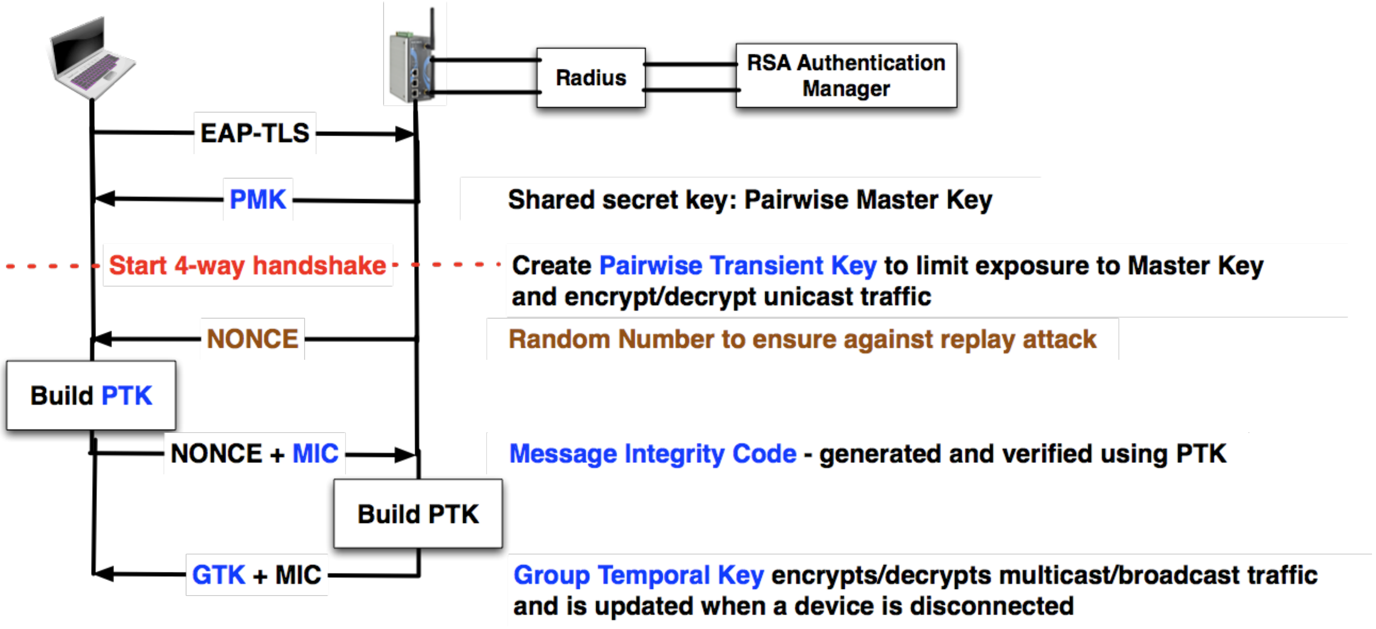
Build PTK

NONCE + MIC

Message Integrity Code - generated and verified using PTK

Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID



Shared secret key: Pairwise Master Key

Create Pairwise Transient Key to limit exposure to Master Key and encrypt/decrypt unicast traffic

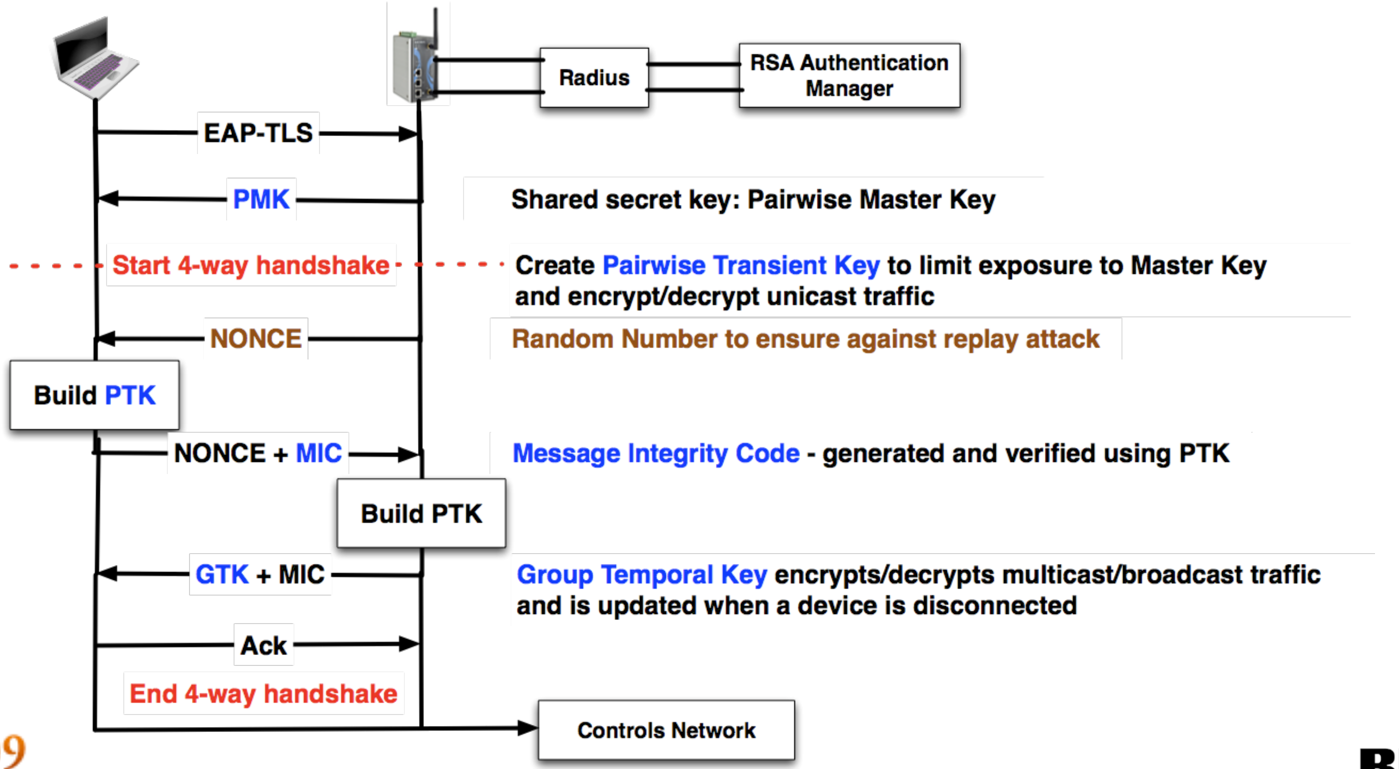
Random Number to ensure against replay attack

Message Integrity Code - generated and verified using PTK

Group Temporal Key encrypts/decrypts multicast/broadcast traffic and is updated when a device is disconnected

Wireless Security

- Wireless available to controls engineering staff
- WPA2 protocol utilizing AES
- Two-factor authentication with RSA SecurID



Radius
RSA Authentication Manager
EAP-TLS
PMK
Shared secret key: Pairwise Master Key
Start 4-way handshake
Create Pairwise Transient Key to limit exposure to Master Key and encrypt/decrypt unicast traffic
NONCE
Random Number to ensure against replay attack
Build PTK
NONCE + MIC
Message Integrity Code - generated and verified using PTK
Build PTK
GTK + MIC
Group Temporal Key encrypts/decrypts multicast/broadcast traffic and is updated when a device is disconnected
Ack
End 4-way handshake
Controls Network

Security/Network Tool Roundup

- Several tools are currently in use or will be deployed in the production controls environment
  - OpenVas (post-Nessus) scanning during pre-production to determine the baseline limitations of control system hardware, routine scanning of server infrastructure
  - Network Enforcer network surveillance software
  - QRadar or IT Sentinel for security compliance management (adherence to NIST)
  - Netem to test protocol behaviors (e.g., CA) via emulation of unfavorable conditions; e.g, variable delay, packet loss, duplication, etc.
  - Snort-MySQL to monitor traffic/packet flows from the sFlow protocol - detailed CA monitoring, detect anomalies
  - Central syslog facilities using syslog-ng tunneled with Stunnel (encrypt TCP within SSL), made browsable with Splunk.
  - Distributed network measurement, latency, data manipulation, and topology discovery tools to discern anomalies, jitter, etc., using tools like perfSonar and NDT
  - Cacti and Nagios

Conclusion - Questions