Wireless Networking at Fermilab

Andy Rader; Anna Olivarez; Phil DeMar
rader@fnal.gov
aolivarez@fnal.gov
demar@fnal.gov
NLIT 2013
May 14, 2013

U.S. DEPARTMENT OF ENERGY

Fermilab

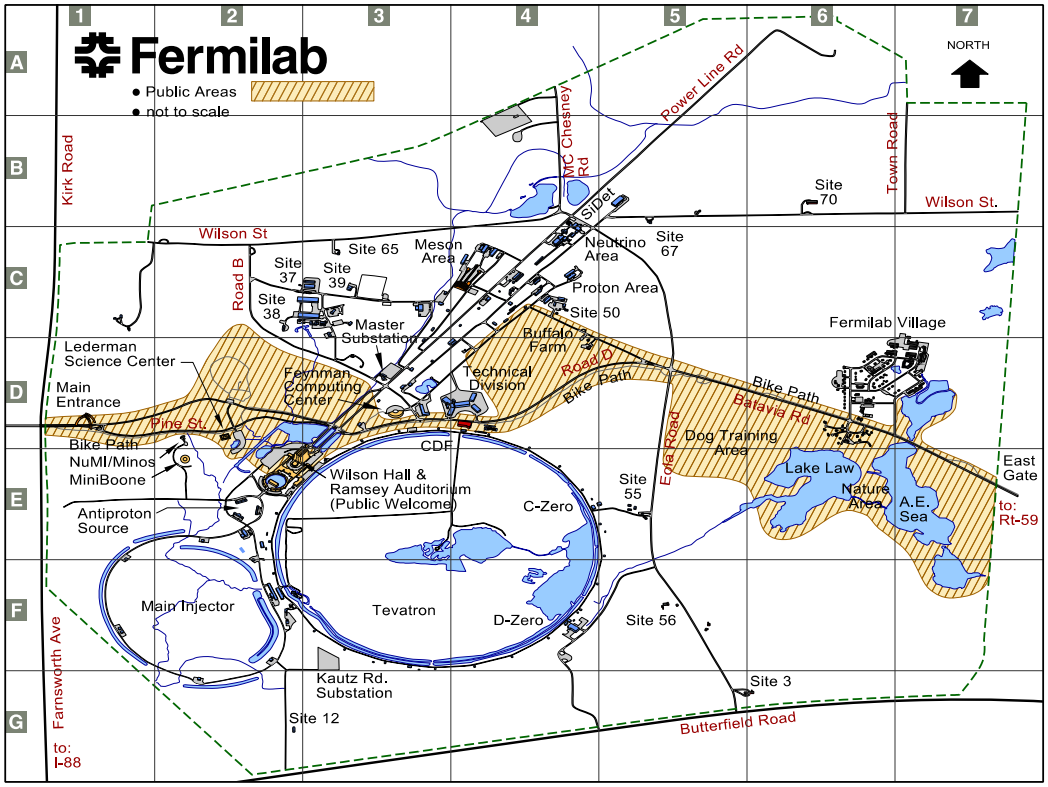
Outline

- Current wireless network at Fermilab
- Wireless pilot
- Guest network
- Looking forward

Wireless Service Philosophy

- Wireless network treated like wired network from a security policy standpoint
- Wireless users provided with a valid routable IP address:
  - Not a NAT (private) address
- Systems w/ registered mac address granted access:
  - Guests granted access after visitor registration
- BYOD allowed on the network after registration
- Goal is wireless coverage in all wired areas
- Vision is wireless becomes default user connection type
  - Possible solution for aging copper infrastructure across campus

Campus Overview



- > 10 sq. miles
- ~ 3,500 users
- Many remote areas

Wilson Hall

- 16 floors
- ~80 access points
- Highest concentration of users
- Building design and construction cause unique challenges for wireless

- Open atrium makes it difficult to contain signal
- Concrete construction blocks vertical floor bleed

Fermilab

Many Mixed Use Areas

- Small, dense pockets of cubicles/offices
- Labs & large high-bay areas
- Sparsely placed buildings

Fermilab

Our Own Village

- 40+ houses, 7 dorm buildings (91 rooms), & 20 apartments
- Outdoor mesh challenging due to dense foliage
- Copper infrastructure nearing 50 years old

Fermilab

User Base

- Heterogeneous mixture of device types:
  - Many owned by other institutions and individuals
- No restrictions on device type or number
- Individually managed devices are welcome after registration
- Large transient user base (conferences, students)
- Multiple wireless devices per user an emerging trend

WLAN Devices By the Numbers

- ~400+ Cisco wireless access points
- 2 Cisco 5508 controllers
- 22 Cisco 1522 outdoor mesh
- 16 Cisco bridges (8 point to point links)

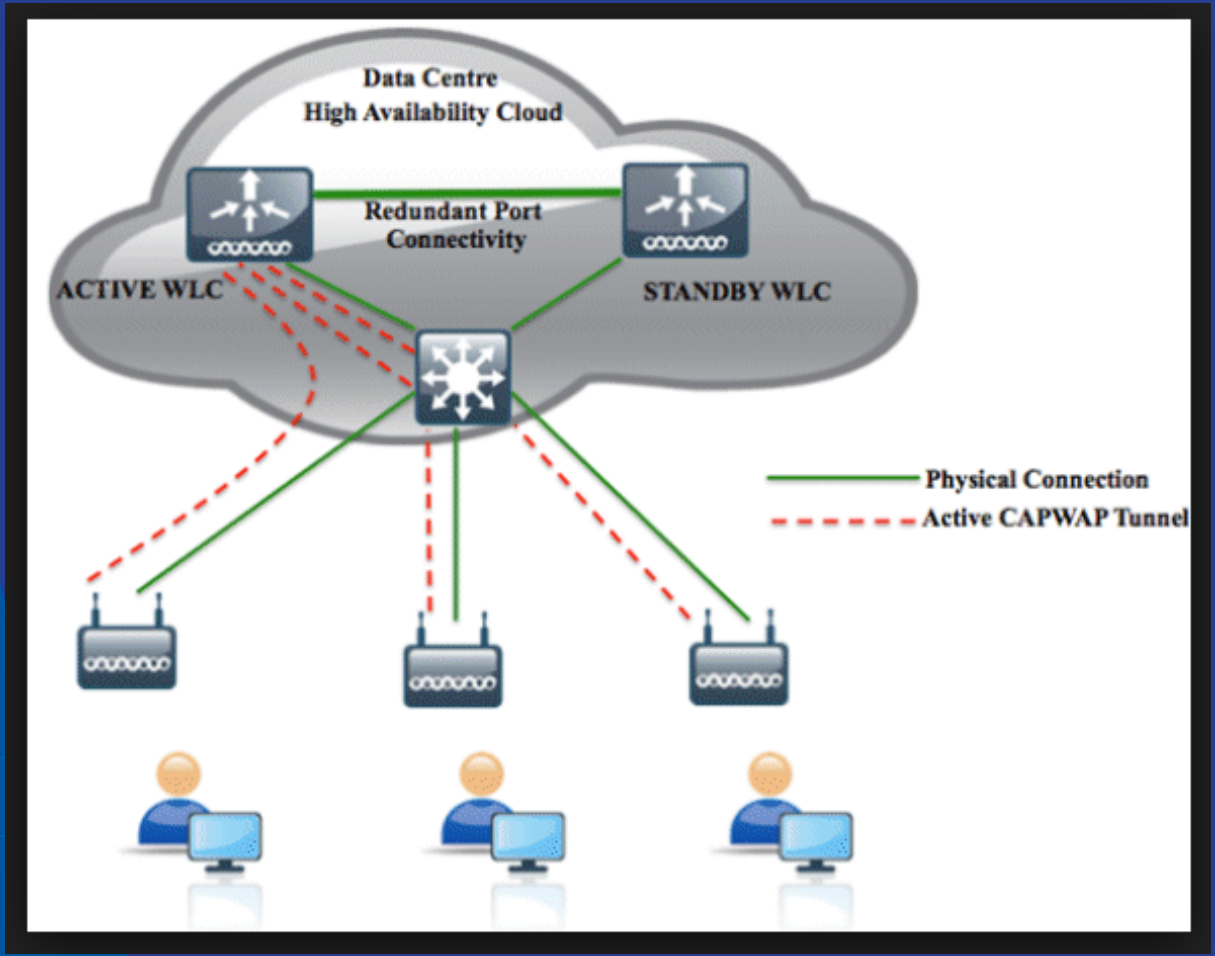
Wireless Equipment

- Single vendor wireless equipment implementation
  - Centrally managed as well
- Redundant controllers:
  - Active/active configuration, balanced by building to avoid roaming
- Many devices based on older technology; system refresh needed
- Sprawling nature of the campus results in dedicated point to point wireless bridge links as well

Current Design

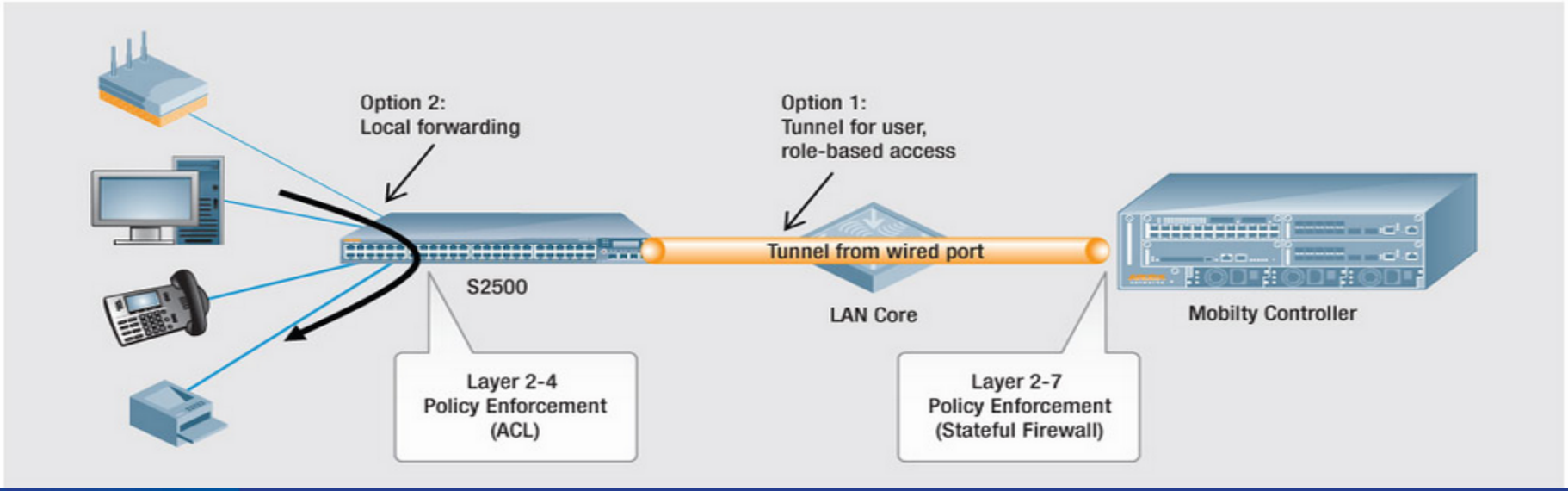
- Single SSID for guests and employees
  - Common security policy
- Two large IP pools for entire campus
- Rogue detection
- Limited location ability

Current Centrally Tunneled Design



Fermilab

Future Design



- Tunnel “guest” SSID traffic to a central location in order to drop off outside the perimeter
- Locally switch all other SSIDs to decentralize traffic
- Upcoming 802.11ac standard also forces this issue

Outline

- Current wireless network at Fermilab
- **Wireless pilot** ←
- Guest network
- Looking forward

Wireless Pilot Goals

- Template for overall refresh of the wireless network
- Address issues of spotty coverage, drops, and interference
- Reduce support effort
- Begin preparing for large increase in BYOD
  - Higher concentration of wireless devices per AP
- Improve performance to meet rising expectations for user mobility

Overriding Goal

- **Determine if we can improve the reliability & performance to match typical wired end-user connection**

Pilot Philosophy

- Pilot focuses on the real-world end-user experience with the service
- Some specific throughput testing also being performed
- Allow vendors to bid solution based on requirements
- Testing each vendor's solution in full production environment for several weeks
- Great weight given to the number and nature of service desk tickets & reports of problems

Pilot Area

- Feynman Computing Center
- Three floors
- Mixed construction:
  - Offices, cubes
  - Computer rooms
  - Conference rooms

- User/device base is representative of the campus
  - Also very knowledgeable on computing & networking

Pilot Process

- RFP created
  - Based on 802.11n support
  - Backward compatibility with legacy clients (g & b)
- Two vendors responded
- Overriding requirement:
  - “Provide a design that will cover all areas of FCC with >=100 Mbps sustained throughput”
- There were also other requirements
  - Support for voice
  - Rogue detection

Pilot Process for the Vendors

1. Survey building, then provide design of access point placement & number of APs
2. Fermilab provides gigabit POE infrastructure
   - With cable slack to move APs around
3. Fermilab mounts each vendor's APs
4. Vendors given the opportunity to re-survey:
   - APs added or moved as requested
5. Fermilab evaluates the vendor's implementation
   - Design, technical, & cost factors will be considered

Vendor Design Approaches

- One vendor focused on maximum throughput:
  - Small cell sizes & higher density w/ APs
- The other vendor focused on lowest cost solution:
  - Minimizing number of Aps

Fermilab

Switching Between Vendor Implementations

- Both vendor's systems were installed in parallel
- New switches & L3 subnet dedicated to the pilot:
  - Intent - eliminate any possible outside effects
- Switched between services for entire building by enabling/disabling POE power for a vendor's APs
- Over several months, we have been toggling service between vendors

Testing & Evaluation – User Throughput

- Utilized Internet2 Network Diagnostic Tool (NDT)
  - Ran NDT 10 second client-to-server & 10 second server-to-client throughput tests
- Tested at various locations of the building, focusing on:
  - Conference rooms
  - Corners & obstructed areas
  - VIP offices
- Tests repeated several times per day at each location
  - Even rotated days of the week…
- Tests done from both Windows & Mac machines

Sample NDT Test Results

```
TCP/Web100 Network Diagnostic Tool v3.6.5.1
Click START to start the test

** Starting test 1 of 1 **
Connecting to 'psonar2.fnal.gov' [psonar2.fnal.gov/131.225.205.141] to run test
Connected to: psonar2.fnal.gov-- Using IPv4 address
Checking for Middleboxes ..................... Done.
Checking for firewalls ..................... Done.
running 10s outbound test (client-to-server [C2S]) ..... 318.88Mb/s
running 10s inbound test (server-to-client [S2C]) ..... 448.00Mb/s
Sending META information ..................... Done.
The slowest link in the end-to-end path is a  a 622 Mbps OC-12 subnet
Information: Other network traffic is congesting the link

Click START to re-test
```

START | Statistics | More Details... | Report problem | Options...

Lab Environment Testing - Aggregate Throughput Evaluation

- Utilized Ixia Chariot product (provided by vendors)
  - Ixia Chariot is a suite of traffic simulation and testing tools
- 20 Windows laptops, 20 Macbooks running Ixia client
  - 1 laptop running Ixia server
- No other RF:
  - Building empty, done over the weekend
  - Verified with all access points off
- Laptops placed to simulate “real-world” layout

Ixia Chariot Throughput Testing - Layout

- Laptops placed throughout:
  - cubicle areas
  - break rooms
  - conference rooms

Ixia Throughput Tests (I)

- With each vendor:
  - Locally switched mode:
    - 40 laptops upload
    - 40 laptops download
    - 40 laptops bidirectional (Windows up, Mac down)
    - 40 laptops bidirectional (Mac up, Windows down)
  - Centrally tunneled to controller mode:
    - 40 laptops upload
    - 40 laptops download
    - 40 laptops bidirectional (Windows up, Mac down)
    - 40 laptops bidirectional (Mac up, Windows down)

Vendor Selection – Where We Stand

- Currently gathering test results & user feedback
- Continue to switch between vendors to correlate with service desk tickets / reports of problems
- Expect to select a vendor by end of month

Outline

- Current wireless network at Fermilab
- Wireless pilot
- **Guest network** ←
- Looking forward

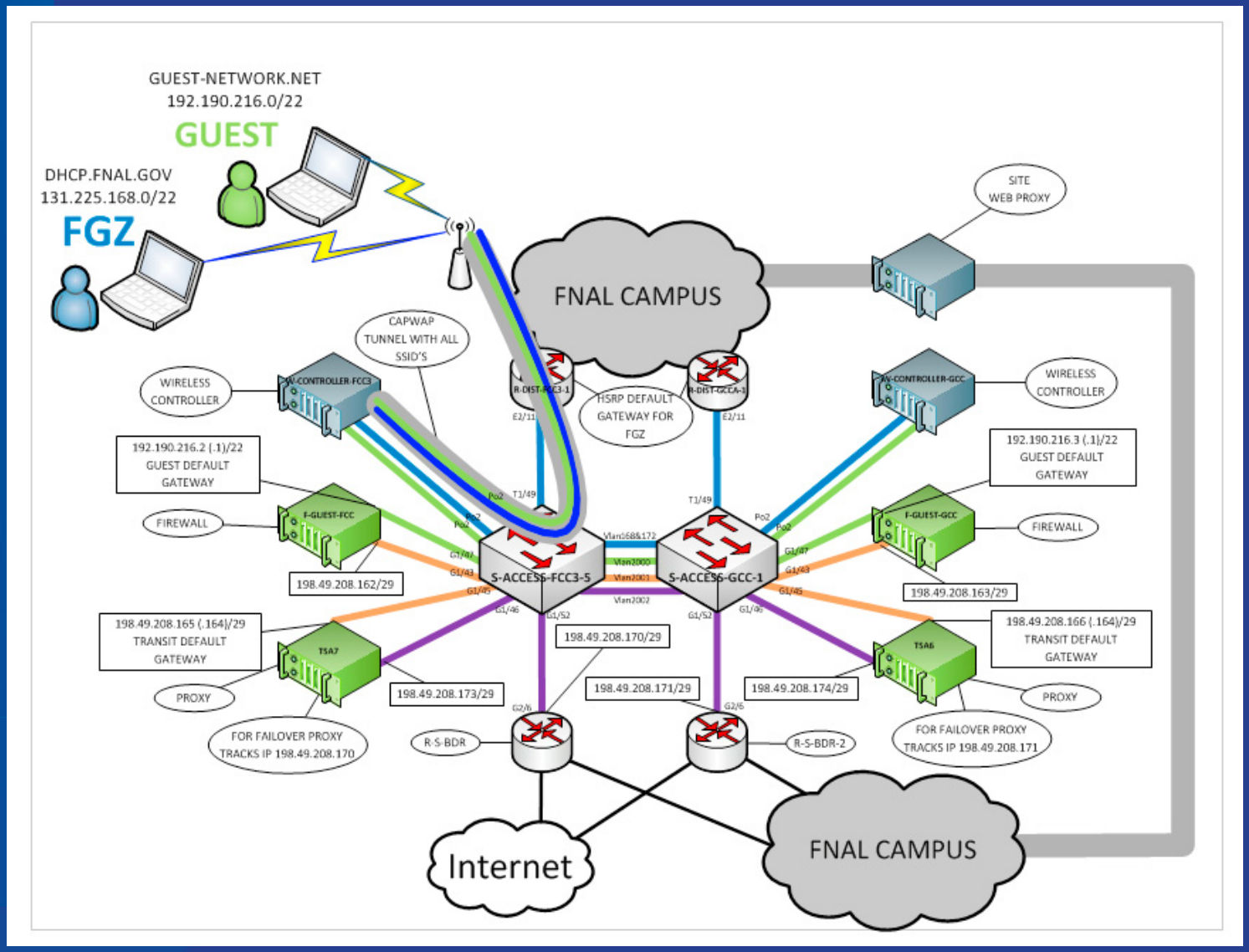
Guest Access to Wireless

- Guests currently granted full access after visitor registration:
  - But subject to all security policies , including scanning
- Need for authentication is minimal:
  - Want to know who is using our network
  - How to contact them in case of a computer security incident
- Services are protected in other ways
- Major concern - public embarrassment to the Laboratory from inappropriate use

New Guest Wireless Service

- Separate SSID for guests to facilitate separate security policy
- Different IP network block from the campus
  - Different domain name as well, outside of dot.gov
- Guest traffic outside site network security perimeter
- Separate firewall and web proxy service
- Eliminates need for aggressive scanning and patch compliance enforcement

Guest Network Design



Fermilab

Outline

- Current wireless network at Fermilab
- Wireless pilot
- Guest network
- **Looking forward** ←

802.11ac

- 5GHz only:
  - Avoids common interference issues with 2.4GHz range
- Wave 1 technology:
  - Targeted at home environment
  - Provides users up to 900 Mbps data throughput
  - Home & enterprise products becoming available now
- Wave 2 technology:
  - Targeted at enterprise environments
  - Provides users >1Gbps data throughput
  - Products expected to emerge in 2014-2015

802.11ac and Fermilab

- Focusing near term investment on 802.11n technology:
  - Anticipating it will remain dominant standard for next 2-3 years
- Will wait until 802.11ac “wave 2” for evaluation & local deployment
- 802.11ac will be initially targeted for high traffic areas
- Procuring APs today with 802.11ac upgrade capability not considered a strategic benefit:
  - Anticipating 2-3 years before wide-scale 802.11ac clients
  - Can replace 802.11n APs with 802.11ac APs where needed
  - Old 802.11n APs could be redeployed to lower traffic areas

Further Down the Road… 802.11ad

- For high bandwidth “last yard” networking
- Runs at 60 GHz
- Possible > 7 Gbps data throughput
- Short distance, 30 feet, does not penetrate walls well
- 802.11ad consumer “WiGig” products out in 2014
  - Currently targeted at personal area networks (PANs)
  - Role in enterprise WLAN, if any, unclear at this point

Impact(s) of 802.11ad?

- Will 802.11ad require an extensive multi-gigabit backhaul infrastructure given the small cell size?
  - Are we just replacing UTP for users with UTP for APs?
- Device turnover increasing as costs drop. The new paradigm a new BYOD device per user per year?
- Will 802.11ad evolve from PANs to enterprise WLANs?
- How might a dramatic increase in WLAN bandwidth change the way we use mobile computing devices?

Summary

- Fermilab initiating hardware refresh of its wireless infrastructure
- Structured pilot program to determine vendor
- Long term vision is to make wireless reliable enough to be default connection type for users
  - Strategy consistent with trends in user mobility needs
- New guest network will migrate guest traffic outside security perimeter

?

Questions