

**UC DAVIS WIRELESS NETWORKING**  
**DISCUSSION FRAMEWORK**  
(FEB. 21, 2007 DRAFT)

**ABOUT THIS DOCUMENT**

---

This document provides a framework for campus discussion of wireless networking. Here, we summarize several key recent developments in support of wireless improvements, and we outline plans for future growth, such as the implementation of the 802.1x standard as the means for authenticating wireless users and providing robust over-the-air encryption.

Specifically, in this document, we have included the following:

- Centrally-managed wireless networking at UC Davis: Plans and status (p.2)
- UC Davis Wireless At A Glance: Current and future (p.5)
- Implementation of 802.1x on MoobileNet (p.7)
- Accessing departmental VLANs: Preferred VLAN attribute in LDAP (p.8)
- Implementation of endpoint network admission controls (p.9)

**DISCUSSION POINTS**

---

- Preparing for implementation of 802.1x on MoobileNet (MoobileNet-x)
- Preparing for extension of 802.1x to departmental VLANs
- Preparing for implementation of endpoint network admission controls

# CENTRALLY-MANAGED WIRELESS NETWORKING PLANS & STATUS

## BACKGROUND

---

In June 2006, the CCFIT Wireless Task Group recommended that the campus move toward increased and improved wireless services by centralizing the deployment and management of the wireless infrastructure. A centrally-managed solution would provide a number of benefits, including:

- Standardized services
- Seamless roaming
- Secure access
- Radio frequency (RF) management, and
- Improved coverage.

Improved wireless services support the mission of the University by providing reliable anytime/anywhere services that enhance staff, student and faculty collaboration and productivity.

## IMPROVING WIRELESS SERVICES: RECENT DEVELOPMENTS

---

The technological components required to support a next generation centrally-managed wireless solution are nearly in place. These components are either undergoing final integration testing or have been deployed on a small, proof-of-concept scale. A brief description and status update of each of those technological components are provided below.

### *Testing and development*

In anticipation of the demand for improved wireless services, Communications Resources (CR), in conjunction with the IET Middleware group has engaged in several testing and development efforts. Goals:

- Enhance the versatility and performance of the existing centrally-managed wireless infrastructure;
- Facilitate the long-term expansion of wireless networking at UC Davis by upgrading the current wireless network to a next generation controller-based solution.

Once these development efforts are completed, all the principal technological components will be in place to support a major expansion of wireless services. Anticipated completion: March 2007.

### *Evaluation of Next Generation Wireless Systems*

- What we've done: Configured and tested next generation wireless networking systems from vendors such as Cisco, Foundry/Meru and Aruba.
- Testing criteria: Performance, features, service enhancements, management capabilities, and ease of integration into the university network.
- Timeframe: CR is completing the final testing and will produce a summary report with functional requirements and a recommended wireless solution.
- Key functional requirements under test:
  - *Radio Frequency (RF) Management* – RF management features inherent within the access-points and the wireless management software provide the means to dynamically adjust channel and power settings on access-points, detect rogue transmitters, and mitigate interference sources.

- *High Density Wireless Support* – Classroom spaces with a high concentration of end-users demand substantial throughput. The centrally managed solution must support high-density configurations as well as “standard” density deployments.
- *Security Features* – Encrypted wireless access will be deployed on wireless services, and enhancements to network admission such as the 802.1x protocol must be supported and manageable.
- *Management of Department Wireless LANs* – The wireless architecture will provide the means for university departments to extend secure and authentication wireless connectivity into departmental Virtual LANs (VLANs). The wireless solution must integrate with Radius and LDAP services to extend wireless services directly to campus department networks.
- *Managed Guest Access* – The wireless solution must support the integration of restricted services for guests and visitors to the university.

#### ***Enhanced Authentication Services***

- Two key projects are underway:
  - Incorporating a 802.1x component to the existing MoobileNet wireless network
    - *See p. 5 for an overview and status update*
  - Developing processes and tools to enable department network administrators to populate the campus LDAP servers with lists of users authorized to access departmental VLANs via wireless connections (longer term). This will also be extended to the “wired” network
    - *See p. 5 for an overview and status update*

#### ***Wireless System Deployments***

- In partnership with the Veterinary School, CR has tested and deployed a controller-based wireless solution that scales to support incidental as well as intensive use.
  - *See p. 5 for a summary.*

#### ***Deployment Modeling Tools***

- CR has developed modeling tools that characterize costs associated with deploying a centrally-managed, controller-based solution.
  - Can characterize the capital costs associated with wireless deployments by geographic area, by building, or by functional areas such as classrooms spaces, research spaces, administrative areas, etc.
- CR has acquired modeling tools that optimize the placement of wireless access-points within buildings to provide the most efficient coverage.
- Working on characterizing the operational and life cycle costs associated with centrally-managed wireless support.

### **PREPARING FOR 802.1X WIRELESS**

---

Once 802.1x services enter into production mode, new wireless services can be rolled out to campus customers who access the centrally-managed wireless system. The following wireless services are in testing and development:

#### ***Enhanced Security***

The use of the 802.1x with Dynamic WEP session keys will provide encryption and security for the campus wireless network and its users. Because 802.1x is a newer protocol, older and less popular operating systems do not always have built-in software clients. To

mitigate this issue, the new wireless solutions are being tested to ensure backward compatibility with current Web-based authentication systems in use on campus.

### ***Department VLAN Support***

With 802.1x and Radius services, department VLANs can be extended into the wireless network and access control can be delegated to department network administrators.

- o Controller-based solution incorporates department VLAN support as a standard service feature.
- o Existing MoobileNet can accommodate limited department VLAN support.
- o *See p. 5 for an overview and status update.*

### ***Network Admission Control (NAC) System***

IET is examining ways of enforcing end-point (personal computer) security measures. Such measures might include requiring end-points to have up-to-date software patches, current anti-virus software, and an installed personal firewall before being allowed to connect to the campus network. During the 802.1x authentication process, NAC systems interrogate end-points to ensure that they meet minimum-security requirements before access is granted. We are evaluating several NAC products.

- o *See p.9 for an overview and status update*

## **PREPARING FOR BROADER CAMPUS DEPLOYMENT**

---

The pace of wireless deployment in the short-term will depend upon demand from campus departments and the availability of core funds to support deployments across campus. Several issues need to be addressed to prepare for any significant expansion/upgrade of centralized wireless infrastructure and to deliver enhanced wireless services on a larger scale. IET is working with a campus working group established by CCFIT to identify options and address these issues.

### ***Funding***

A next generation wireless solution will require a significant funding commitment by the campus. The cost to “paint” the campus will be on the order of \$8 million. However, the solutions being tested and developed can be built out and supported over a number of years. Deployment can be as large or small as practical within the bounds of available funding.

### ***Prioritization***

Deploying a centrally-managed wireless solution over a number of years will require the campus to prioritize the buildings or functional spaces that will receive enhanced services first. CR can cost any suggested prioritization list, and several examples and recommendations have been developed to this effect. However, the final decision on priority should have widespread consensus on campus.

### ***Rates and Cost Recovery***

Currently, IET recovers one-time costs (consulting fee, equipment costs) from departments requesting wireless services. Replacement costs for equipment and funding for operations and maintenance is covered by core funds and from wired network fees. An additional revenue source will need to be identified to cover expenses as these costs grow in relation to the demand for centrally-managed wireless services.

## WIRELESS SERVICE CHARACTERISTICS

---

- Open access points (no encryption)
- Cisco "Fat" AP's w/ BlueSocket gateways
- Captive portal, Web page re-directs – Kerberos login
- Lookup tools for help desk support
- Nessus scan
- Guest access via sponsor registration
- Approx. 270 APs currently managed from the NOC

## DEPLOYMENT MODEL AND COVERAGE

---

- APs are deployed in campus "common areas"
- Departments fund MoobileNet AP deployment in their spaces
- Wireless gateways are centrally funded
- Wireless VLANs are geographically deployed; roaming within VLAN

## FUNDING

---

- Current investment in wireless services is very limited.
- No revenue stream directly related to wireless services.

## SERVICE ISSUES

---

- BlueSocket instability
  - BlueSockets periodically stop performing Web redirects
  - Authenticated users continue to function; new users prevented from authenticating
  - Solution: Appears to be a memory leak – working with vendor to diagnose
- Slow login
  - Typical login expected to take 20-30 seconds; includes time for web page redirects and security scan
  - Recent complaints of slower login times; some user reports of logins taking several minutes
  - Troubleshooting revealed 3 security scans being conducted
  - Bluesocket wireless gateway memory leak can cause delays in re-directs
  - Without scans, login period is several seconds (typically)
  - Solution: Ensure only one security scan occurs, fix memory leak (temporary solution – scheduled reboots of wireless gateways)
- DHCP address depletion
  - Users do not need to authenticate to obtain an IP Address
  - Solution: Expanded DHCP address pools & re-balanced wireless VLANs (short-term solution); working with vendor to implement dynamic 1:1 NAT – will allow private address space on the wireless side
- Limited Coverage
  - Working with CCFIT to identify and prioritize coverage areas
- Costs
  - Departments bear the cost of Cisco AP procurement & NAM installation
  - Investigating new cost and funding models
- Security Issues
  - No session encryption unless SSL protocol available
  - Any user can associate with an AP and obtain access to the wireless VLAN
  - Wireless clients may generate malicious traffic onto other wireless users and the campus network
  - Authentication allows access off of the wireless VLAN

- No RF Management
  - Solution: Addressed by controller-based solution.
- No control of non-CR wireless deployments on campus
  - Solution: Policy revisions, required minimum standards.

## **CURRENT DEVELOPMENT EFFORTS**

---

- 802.1x for existing MoobileNet
  - Separate SSID, not beamed
  - Encryption from endpoint to AP
  - Testing underway
  - Applicant support – IT Express ramp up, self-help configuration guides, downloadable configuration tool, communications
  - Populating LDAP with password hashes
- 802.1x for wired network
  - Testing has gone well
  - Feature request into Foundry – multiple authentication hosts required
- RADIUS/LDAP
  - Integration of a preferred VLAN attribute into LDAP
  - Moving RADIUS server into production mode
  - Future integration of various permits, time and location based policy decisions
- Testing controller-based wireless solutions
  - Product testing nearly complete
  - Incorporates 802.1x and captive portal authentication methods
  - Supports LDAP-preferred VLAN attribute – permits secured wireless access to department VLANs (opt-in)
  - Solution addresses security, RF management and roaming issues
  - Integrates with RADIUS authentication development efforts
- Network Admission Control Testing
  - 802.1x integrated into testing regime
  - Testing with wired network access
  - Request for Proposal will be released in March 2007
- Tested and deployed CAT 5e power injectors

## **LONG-TERM PLAN**

---

- Deployment models have been developed – Costs and scope identified on a per building basis
- Wireless Valley Software – modeling tool that optimizes AP placement and coverage within a building
- Wireless infrastructure requirements are now incorporated into new construction projects
- Working with CCFIT & campus to:
  - Identify funding model
  - Prioritize deployment efforts
  - Continue development and enhancements to authentication policies and delegated management tools

## IMPLEMENTATION OF 802.1X ON MOOBILENET (MOOBILENET-X)

### LEADS

---

Tom Arons, Infrastructure Architect: [tgarons@ucdavis.edu](mailto:tgarons@ucdavis.edu); (530) 752-1750

Mark Redican, NOC Manager: [mredican@ucdavis.edu](mailto:mredican@ucdavis.edu); (530) 752-9500

### STATUS

---

- 802.1x authentication for wireless without network admission control is ready to move into production mode. The hardware and associated software infrastructure is tested and in place.
- The customer service issues need to be worked out. We will be working with the School of Veterinary Medicine to learn from their experience as theirs will be the first large population of users. We are investigating a configuration agent from the RADIUS vendor that is expected to lighten the customer service load. The team will be meeting with the vendor in the next couple of weeks. Parameters for beta testing will be set up shortly thereafter.
- A Radius server and software package have been deployed. Testing of 802.1x authentication services with the Radius server is underway.
- 802.1x services are expected to be deployed in a limited production mode in March 2007. MoobileNet-x is expected to be in full production by summer.

### GOALS

---

- Incorporate a 802.1x component to the existing MoobileNet wireless network.
- Provide direct access to the campus wired network (without going through the BlueSocket gateways)

### EXAMPLE OF ENHANCED WIRELESS SECURITY DEPLOYMENT

---

In partnership with the Veterinary School, CR has tested and deployed a controller-based wireless solution that scales to support incidental as well as intensive use.

- This solution provides scalability by supporting high-density spaces such as classrooms, as well as medium and low-density areas.
- Authentication and security mechanisms have been integrated and the solution is in use at the Vet Med Instructional Facility where 802.1x authentication is undergoing integration and testing.

### NEXT STEPS

---

- Plan for supplicant support
  - b. IT Express support model
  - c. Self-help configuration guides
  - d. Downloadable configuration tool
  - e. Communications
- Populate LDAP with password hashes

# PREFERRED VLAN ATTRIBUTE IN LDAP (FOR USE BY RADIUS SERVER)

## LEAD

---

Tom Arons, Infrastructure Architect: [tgarons@ucdavis.edu](mailto:tgarons@ucdavis.edu); (530) 752-1750

## STATUS

---

- We have identified several candidate VLANs, both in and out of IET. We will be asking the sysadmins for user lists. Once this is done we can move forward with the static population of LDAP with the preferred VLAN--phase one of the project.

## GOALS

---

- Enable department network administrators to populate the campus LDAP servers with lists of users authorized to access departmental VLANs via wireless connections
  - Implement an attribute that can be used by Identity engines (Radius server) in policy to select a preferred VLAN, rather than the default MobilenetX.
  - Extend department VLANs into wireless infrastructure (limited access to VLAN information/file shares)
  - Incorporate as a standard feature in controller-based wireless upgrade (anywhere access to VLAN information/file shares)
- Establish equivalent or better security than a wired connection
  - Address current security issues with numerous de-centralized deployments of wireless systems.

## TARGET AUDIENCE

---

- All campus wireless users who would like or need access to a departmental VLAN.

## IMPLEMENTATION APPROACH

---

### Proof of Concept:

#### *Phase I (March 2007)*

- Define a preferred VLAN attribute in LDAP for multiple department static deployment (loaded manually based on info provided by departmental SysAdmins)
  - Modifications to existing LDAP (preferred VLAN attribute) and lists of users from network SysAdmins
- Estimated time needed: 1 week

#### *Phase II (Spring 2007)*

- Create multiple valued "eligible" VLAN attribute, statically populated by info provided by departmental SysAdmins
  - Further modifications to LDAP (eligible VLAN attribute) and human readable VLAN lookup table (see above)
- VLAN lookup table translating existing VLAN codes to human readable descriptions
- End User GUI allowing users to select preferred VLAN from eligible VLANs
  - End User GUI – will likely reside on existing hardware
- Estimated time needed: 2-3 weeks

### Production:

#### *Phase III (TBD)*

- Administrative GUI for departmental SysAdmin that allows them to populate a user list of eligible VLANs and an authorization list for VLAN (Network Administrator List)
  - Administrative GUI and Network Contact List on existing hardware
- Estimated time needed: TBD

# IMPLEMENTATION OF NETWORK ADMISSION CONTROL (NAC) SYSTEM

## LEAD

---

Bob Ono, IT Security Coordinator: [raono@ucdavis.edu](mailto:raono@ucdavis.edu); (530) 754-6484

## STATUS

---

- A formal timetable to moving to 802.1x. and hygiene tests via an end-point security solution is being developed.
- The project team completed initial review of two NAC solutions, Safepoint and CyberGatekeeper, offered to UC Davis at substantial pricing discount. Safepoint was precluded from deployment due to Foundry patch prerequisites that could not be installed. CyberGatekeeper did not meet the test criteria.
- Using knowledge gained from the product testing and research, an RFP will be released in March 2007. Anyone interested in participating in the RFP process is invited to contact Bob Ono.
- NAC solutions do not work with fan-out devices.
- An impact analysis is under way. Results will be discussed with the TIF-Security subcommittee.

## GOALS

---

- Implement a system that interrogates end-points to ensure that they meet minimum-security requirements before access is granted. Before being allowed to connect to the campus network, end-points might be interrogated to ensure they have:
  - Up-to-date software patches
  - Current anti-virus software
  - Automatic update function enabled
  - Absence of specific malicious programs, and
  - An installed personal firewall.

## TARGET AUDIENCE

---

- Ultimately all users who access the campus residential computing network, wireless network, virtual private network users and public NAMs.

## IMPLEMENTATION APPROACH

---

End-point security is expected to be deployed in phases, as follows:

- First phase: **Fall 2007** -- ResNet, in partnership with Student Housing.
- Could start with server logging of audit failures, moving to failure messages to end users and finally connectivity denial due to audit failures.
- **Early 2008**: Future phases:
  - Wireless
  - Public NAMS, and
  - VPN users.