

Campus Wireless Standards May 24, 2006 (DRAFT)

The University of Utah has a need to provide ubiquitous wireless access across campus without impacting or hindering local organizations. ITC has approved ubiquitous wireless to mean authenticated access to encrypted networks, with authenticated unencrypted as optional

This wireless network must be accessible to all faculty, staff, students and visitors. These standards provide direction to university organizations in making wireless networks secure and available to the university community

I. Centrally Switched Campus Wireless Standards. Ubiquitous Campus Wireless

Access Points and their configuration must comply with these standards.

A. Security Requirements

- Access Points may support WPA2 with CCMP, TKIP, and WEP, along with 802.1X with dynamic WEP. 802.1X with dynamic WEP must be supported until the end of summer 2006. WPA1 and WPA2 will be turned on at this time and WEP will be disabled.

B. SSID's usage and conventions

- Uconnect.utah.edu (originally Uconnect.utah.edu) is mandatory for all AP's and area served by these AP's. Not just common area or specific locations. hotspot.utah.edu (originally inUconnect.utah.edu) will be installed on an opt-out basis and will be unauthenticated and unencrypted internet access from outside of the campus firewall.
- The Uconnect.utah.edu SSID can be serviced by subnets outside of your internal department networks to provide commodity network access without lowering your internal department security policies.
- hotspot.utah.edu will be unauthenticated, unencrypted access to the commodity internet. It will place users outside the campus firewall and treat them like any other external ISP. Bandwidth and port restrictions will be implemented on this network as directed by ISO. hotspot.utah.edu will dhcp ipv4 address space outside the common 155.x.x.x and 128.x.x.x address space.
- Secondary encrypted/secured local department SSID's configured on the same infrastructure may provide direct access to department internal services if needed. You may not use Uconnect.utah.edu or hotspot.utah.edu in your department SSID's to avoid confusion.

C. Authentication

- Uconnect.utah.edu and hotspot.utah.edu will be deployed with the following centrally provided services. Uconnect.utah.edu will use WPA2 enterprise mode

University of Utah Wireless Standards - 6/6/2006
DRAFT

authentication to campus radius mesh. hotspot.utah.edu will be deployed with centrally provided Cisco Clean access manager also accessing the campus radius mesh.

- Local department authentication could be handled at the local organizational level via RADIUS realms based on the domain part of the username. All campus wireless users will have access via the base uNID (u00000000) through the centrally maintained radius mesh maintained by OIT.

D. Hardware to be used.

- All AP's and hardware purchased will comply with the published hardware standards and connect to campus provided centrally switched wireless hardware, Trapeze and Aruba
- Only AP's that have been certified to co-exist by the wireless committee can be installed in the same geographic location to avoid interference with ubiquity and ease of use.

E. Roaming and Scalability

- All devices will be configured with roaming and seamless connectivity in mind.
- Roaming on Uconnect.utah.edu will be allowed and enabled in all locations to allow campus-wide coverage. Roaming configuration will be defined by the Campus Wireless Committee.
- Scalability is inherent in 802.11a and 802.11b/g networks with load balancing, radio hand-off, zoning, and multicast rates.

II. Local wireless installations (private and local SSID's)

- All implementations of internal use only specific wireless must not interfere with the ability to provide general campus access to those users who want it. It is also recommended that unique named SSID's must be used to avoid confusion anywhere possible.
- All implementations of nonstandard 802.11 a/b/g wireless will not interfere with the campus centrally managed wireless or any other campus wireless implementations where roaming and campus wide access are implemented.
- Login VLAN switching is supported subject to the following two requirements ...
 - The user must log in with a "Departmental userid" as defined above. In addition, the departmental Radius server must provide additional account attributes;

University of Utah Wireless Standards - 6/6/2006
DRAFT

- This feature is only supported on OIT-provided wireless networking equipment. Note that as of 01/2006, Trapeze is the only authorized vendor that supports this feature.