

Campus Wireless Standards v. 2.8

December 7, 2006

The University of Utah has a need to provide ubiquitous wireless access across campus without impacting or hindering local organizations. The Information Technology Council (ITC) has approved ubiquitous wireless to mean authenticated access to an encrypted wireless network, with unencrypted network access 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. Definitions

- A. Ubiquitous: defined by the ITC as an encrypted, authenticated, and persistent wireless network provided campus-wide
- B. Roaming: being allowed to maintain a persistent IP/Wireless connection while moving
- C. uconnect.utah.edu: encrypted campus access wireless standard
- D. hotspot.utah.edu: open un-encrypted open wireless access, off campus address space
- E. secure.utah.edu: deprecated encrypted campus standard wireless
- F. insecure.utah.edu: deprecated un-encrypted campus standard wireless
- G. SSID: service set identifier; the broadcast wireless network name visible to the end user
- H. WPA: Wi-Fi Protected Access; depreciated version 1 of the WPA encryption
- I. WPA2: current version 2 of the WPA encryption
- J. CCMP: Counter Mode with Cipher Block Chaining Message Authentication Code Protocol; encryption technologies
- K. TKIP: Temporal Key Integrity Protocol; encryption technologies
- L. Dynamic WEP: (Wired Equivalent Privacy) standard or rotating wep keys dynamically
- M. 802.1x: encryption technologies
- N. AP: access point; hardware wireless access point that provides wireless services
- O. VLAN: virtual local area network; a local network that can be virtualized anywhere vlans are supported
- P. Encryption: a computer-based algorithm to encrypt data
- Q. Authentication: a means of identifying that the user has knowledge of the necessary credentials to access your service
- R. EAP: Extensible Authentication Protocol; a universal authentication framework.
- S. TTLS-PAP: Tunneled Transport Layer Security - Password Authentication Protocol, a form of authentication

II. Centrally Switched Campus Wireless Standards: Ubiquitous Campus Wireless

Access Points and their configuration must comply with these standards.

A. Security Requirements

University of Utah Wireless Standards

- Access Points broadcasting the uconnect.utah.edu SSID will support WPA and WPA2 with CCMP and TKIP. 802.1X with dynamic WEP must be supported until October 13, 2006. WPA1 and WPA2 will be turned on prior to this time and dynamic WEP will be disabled by December 31, 2006.

B. SSIDs: usage and conventions

- uconnect.utah.edu (originally secure.utah.edu) is mandatory for all APs and areas served by campus accessible APs, not just common areas or specific locations. hotspot.utah.edu (originally insecure.utah.edu) will be installed on an opt-in 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 internal department networks to provide commodity network access without diminishing 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 an external ISP. Bandwidth and port restrictions will be implemented on this network as directed by the Information Security Office (ISO). hotspot.utah.edu will use DHCP IPv4 address space outside the common 155.x.x.x and 128.x.x.x address space.
- Secondary encrypted/secured local department SSIDs configured on the same infrastructure may provide direct access to department internal services if needed. The uconnect.utah.edu and hotspot.utah.edu SSIDs may not be used in department SSIDs 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 WPA1/WPA2 enterprise mode authentication to the campus radius mesh. hotspot.utah.edu will be deployed centrally via the Cisco Clean Access Manager.
- Local department authentication can 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 (u0000000) through the centrally maintained radius mesh maintained by OIT.

D. Hardware to be used.

- All APs and hardware purchased with approval by the appropriate governing bodies and with approved central campus funding* should comply with campus hardware and authentication standards and connect to campus-provided centrally switched wireless hardware: Trapeze (lower campus) and Aruba (Health Sciences).

University of Utah Wireless Standards

- The campus standard Extensible Authentication Protocol (EAP) type for uNID access is TTLS-PAP. Other EAP types may be used to support local department requirements.
- APs should be installed to avoid interference with the campus goal of ubiquity in a given geographic location avoiding channel overlap and interference wherever possible.
- Central funding for department-maintained hardware that meets the campus hardware and authentication standards may be requested through the Student Computing Advisory Committee (SCAC), to purchase APs to improve density and coverage within the department. SCAC requests of this nature will compete with all other SCAC requests. For departments using Office of Information Technology (OIT) as the owner/manager of the APs, OIT will upgrade/replace hardware as needed, depending on funds availability.
- If, a campus department wants to depart from the approved campus wireless standards, they may do so with their own funding, provided that such deployment of non-standard systems will not interfere with the operation of the standards-based campus wireless network.

E. Roaming and Scalability

All devices will be configured with roaming and seamless connectivity, where possible, per the ITC definition of ubiquitous campus wireless coverage: campus-wide encrypted and authenticated wireless coverage providing persistent connections in transit.

(www.it.utah.edu/leadership/committees/ITC/minutes/itc_minutes_2006_04.pdf, section IV). Notwithstanding the ITC definition, persistent connections across the entire campus may not be feasible at this time, because of differences in the characteristics of currently installed wireless hardware.

- Roaming on uconnect.utah.edu will be allowed and enabled, where possible, 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 SSIDs)

- All implementations of internal use-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 SSIDs 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.

University of Utah Wireless Standards

- 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;
 - This feature is only supported on OIT-provided wireless networking equipment.