



Information Technology Standards

UNM Wireless Standard

IT Standard Issued: June 05, 2007

Supersedes: None, New Standard

Responsible

Executive: Chief Information Officer (CIO)

CIO's Signature for approval

Responsible Office: Office of the CIO

<http://cio.unm.edu/>

Contact:

For questions about this standard, contact Director of Information Technology Services--Communications Network Services

For questions and information regarding the UNM Wireless Network please refer to <http://its.unm.edu/wireless/>

If you require a consultation for installing or removing wireless network access in your area, please contact the ITS Support Center at 277-4848 or refer to <http://fastinfo.unm.edu>

If you wish to report a non-compliant wireless deployment, or have any questions about compliancy, please contact the ITS Support Center at 277-4848 or refer to <http://its.unm.edu/wireless/>

Summary of Standard:

This document describes the University of New Mexico's (UNM) standard for the use of wireless technologies on campus. It applies to all uses of Wireless Local Area Network (WLAN) technologies at all physical locations, including buildings and outdoor areas, of UNM, and to all IEEE 802.11(a/b/g) compliant wireless devices connected to the University of New Mexico Wireless Network (UNMWN) managed by Information Technology Services (ITS) herein referred to as the Central Wireless Authority (CWA).

Who is Affected by this Standard:

Wireless network technologies increasingly play a significant role in complementing the Campus Data Communications Network (CDCN), bringing important benefits in convenience, flexibility,

and ubiquitous access. This standard applies to and affects any units or individuals connecting to the UNM Wireless Network (UNMWN) and to the CDCN.

Why We Have this Standard:

UNM encourages use of its CDCN and UNMWN in support of education, research, and public service. However, this resource is limited and vulnerable to attack. UNM therefore reserves the right to deny access to its CDCN and UNMWN by devices that do not meet its standards for security. Standards compliance is necessary to help protect all devices connected to the CDCN and UNMWN and to assure accountability and traceability to comply with federal laws.

UNM envisions a consistent experience for wireless users throughout campus via a single standard wireless deployment, central management, and reduction of interference. All or parts of this standard may need to be updated as the technology matures and/or changes.

All Wireless Local Area Networks connected to the CDCN are subject to the Enforcement section of this standard and are subject to periodic review as new technologies emerge and are adopted by the CWA.

The goals of the standard are:

- To reduce the potential security risks that may be associated with wireless network technologies.
- To reduce potential interference and performance issues on the UNMWN.
- To assure that all users with proper equipment can access the UNMWN and are presented with a uniform interface.

Responsibilities:

- CIO (Chief Information Officer)
 - approve the standard.
 - review and approval of exceptions and enforcement of the standard.
- CWA (Central Wireless Authority)
 - manage the UNMWN, including user support.
 - review requests for and make recommendations to the CIO regarding exceptions.
 - reconvene the wireless sub domain as necessary for review and updates of the standard.
 - proactively monitor and analyze the wireless environment.
 - reserves the right to disconnect devices that pose security risks, performance issues and interference, or do not have an approved registration.
 - provide updated information at <http://its.unm.edu/wireless> on Service Set Identifiers (SSIDs), Guest or Public Access and Secure Access guidelines.
- Wireless sub-domain
 - review and provide recommendations to update the standard.

- University units
 - comply with the standard.
 - submit all exceptions requests to the CWA by completing the exceptions form at the end of this document and must include justification with some design data indicating the unit's knowledge of WiFi and efforts to minimize interference. Exceptions must be submitted in writing to the CWA through fastinfo at <http://fastinfo.unm.edu>.
 - submit all wireless service requests for installations, changes or exceptions, including cost estimates and site survey and analysis requests. Requests must be submitted in writing to the CWA through fastinfo at <http://fastinfo.unm.edu>.
 - take steps to address the security and promote the reliability of the UNMWN and the CDCN.

Mandatory Procedures:

In order to provide access to the largest possible population and at the same time provide secure access to the UNMWN, both unencrypted and encrypted (secure) access will be supported.

The CWA will provide two levels of access. The first Service Set Identifier (SSID) will be labeled UNM_Secure and will provide WPA encryption with authentication requiring a UNM NetID. The second SSID will be labeled UNM_Guest and will have no encryption and no authentication. Access on this SSID will be limited to web services via HTTP (port 80), HTTPS (port 443) and VPN (associated ports).

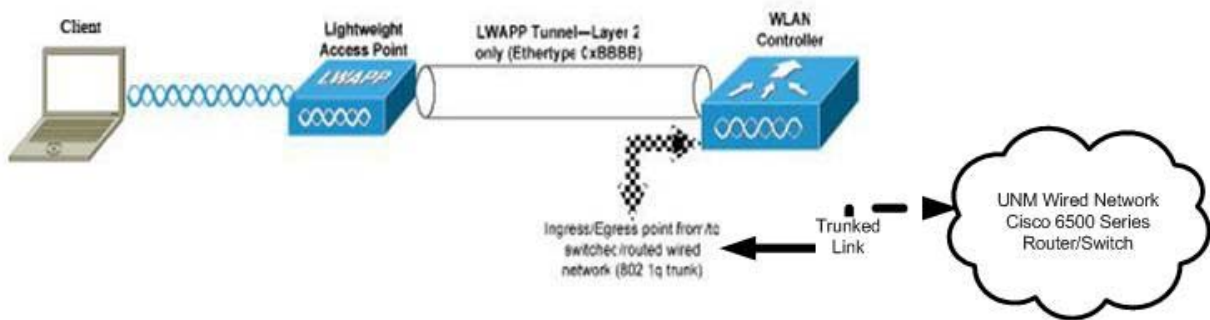
The University recognizes that some units have needs that may justify installation of a private or restricted wireless deployment. These entities may implement additional wireless technologies as long as they do not interfere with the operation of the UNMWN. They must also comply with the responsibilities listed for UNM organizations or departments under the "Responsibilities" section in this standard and provide a .5 FTE to manage the unit's wireless deployment. In addition they must comply with the Design Guidelines and Specifications for installation located at <http://its.unm.edu/communications/designguidelines> by hiring an approved contractor for installation and placement of WAPs.

Entrepreneurial wireless deployments (non CWA managed) shall provide encryption and authentication at a minimum that offers the same level of encryption employed by the CWA and offer authentication for accountability. These units will be responsible for account creations and client configurations for accessing their wireless infrastructure. Guest access for these units (non-encrypted and non-authenticated) will also be restricted to mimic guest services provided by the CWA in an effort to minimize security risks.

All wireless network access points connected to the CDCN must be registered with the CWA and use the SSID format UNM_Dept_Guest and UNM_Dept_Secure (e.g. UNM_CS_Guest and UNM_CS_Secure for the Computer Science Department). The registration process requires information including the responsible university unit as well as technical and operational information about the access point(s). To register an access point, complete the online Registration Form at <http://its.unm.edu/wireless/registration>.

Encrypted wireless access will be evaluated on a regular basis by the CWA as technologies and standards evolve. Data is encrypted between the Client and the WLAN controller for the wireless portion. Data passing beyond the controller onto the wired network is not encrypted. If required, units must provide encryption at the application level using VPN, SSL, Certificates or some other encryption method or solution. Please refer to the figure below for a graphical representation of where encryption takes place on the central wireless infrastructure.

Cisco AireSpace Encryption Diagram



NOTE:

Encryption only takes place between the Client and the WLAN Controller for the wireless portion. Once the data goes beyond the controller onto the wired network it is no longer Encrypted unless VPN, SSL, Certificates or some other encryption between the client and server or service is utilized.

Access Control: Access methods to the UNMWN may change periodically as the CWA continues to adopt secure methodologies for accessing the UNMWN. Please refer to the campus wireless information page for up to date access methods at <http://its.unm.edu/wireless>

Enforcement: The CWA must foster campus-wide network standards (wired and wireless) to meet the networking requirements of all campus constituencies and limit access to network connections which do not conform to generally accepted standard network protocols and security measures.

The CWA or ITS Security staff will notify a university unit operating a wireless access point (WAP) that does not appear to be compliant with this standard. Wireless access points not brought into compliance may be denied CDCN access. The CWA or ITS Security staff may report noncompliant wireless network WAPs connected to CDCN to the operating unit's higher management via the CIO with recommendations for corrective measures.

In addition, the CWA or ITS Security staff may report otherwise legitimate non-data unlicensed wireless devices operated in a manner not compatible with the UNMWN to the CIO and the operating unit's higher management with recommendations for corrective measures. Examples of

such devices include but are not limited to non-shielded microwave ovens, telephone handsets or frequency jammers.

In a perceived emergency situation, the CWA or ITS Security staff may take immediate steps, including denial of CDCN access, to ensure the integrity of the university data network and systems, safeguard the health and safety of university community members and property, or protect the university from liability.

All decisions, notifications, or measures taken under this standard may be appealed to the CIO through the CIO's Office.

Considerations for Wireless Deployments:

University units deploying wireless access points should be aware that while the Federal Communications Commission (FCC) establishes regulations for use of the unlicensed radio frequency spectrum, it does not license or control the use of these frequencies. Therefore other devices that legitimately use these frequencies may disrupt wireless data network communications. Similarly, wireless data network use may disrupt other legitimate uses of these frequencies. For example, the frequencies used in the 802.11b wireless data standard are in the unlicensed 2.4 GHz Industrial, Scientific and Medical (ISM) band. Devices legitimately using this and other unlicensed bands include cordless telephones, microwave ovens, sprinkler systems, traffic signals, and others.

When deploying wireless services for a unit, interference in these frequency bands must be anticipated and dealt with through careful engineering to ensure service quality and reliability.

In addition, unmanaged and unauthenticated wireless data network access poses significant campus network security, integrity, and reliability risks. Such access poses risks to mission-critical university services data and potential university liabilities. University owned or operated wireless devices and devices connected to university infrastructure services must be carefully managed to ensure the integrity of the UNMWN and the CDCN.

To help ensure equitable and optimal university wireless data network service and to help best serve the university mission, the Central Wireless Authority (CWA) will be responsible for authorizing and coordinating the connection of wireless data devices to the Campus Data Communications Network (CDCN). The CWA will also exercise authority over the deployment and use of university owned or operated wireless devices.

Website Address for this Standard:

<http://cio.unm.edu/standards>

Related Documents:

The following documents may be located at <http://www.unm.edu/~ubppm/ubppmanual/toc.htm>

- Policy 2500 "Acceptable Computer Use,
- Policy 2510 "Computer Use Guidelines

- Policy 2520 “Computer Security Controls and Guidelines,”
- Policy 2560 “IT Governance” NOT POSTED OR OFFICIAL YET
- Policy 2590 “Access to Administrative Computer Systems.”

The following document may be located at

- Design Guidelines and Guide Specifications
<http://its.unm.edu/communications/designguidelines>

Glossary: [Alphabetical list defining terms in the standard that have a specialized meaning.]

802.11a - An IEEE wireless network standard that increases the bandwidth throughput to 54 Mbps and operates on the 5 GHz UNII band. At the same power and gain, signals at 5 GHz appear to travel only half as far as signals at 2.4 GHz. Furthermore, because the 802.11a standard operates in a different frequency range from the 802.11b and 802.11g standards, 802.11a is not hardware compatible with the other two standards. Some devices include both 802.11a and 802.11b/g units in the same enclosure.

802.11b - An IEEE standard for wireless data networking that uses the 2.4 GHz ISM band and is rated at up to 11 Megabits per second (Mbps) throughput. Both indoor and outdoor signal range and strength can vary greatly depending on use of external antennae and whether or not obstructions exist. Line of sight (LOS) is typically required between 802.11b devices in order to communicate effectively with each other. Since 802.11b allows for only three non-overlapping channels (1, 6, & 11), interference issues can occur by having too many access points in one location. Bluetooth devices, microwave ovens, cordless phones, and other electronic devices, operating in the 2.4 GHz band, may cause other interference issues.

802.11g - An IEEE wireless network standard that increases the bandwidth throughput to 54 Mbps. Like 802.11b, 802.11g devices also operate on the 2.4 GHz band, and likewise, are susceptible to channel interference and interference from other common electronic devices. Most 802.11g devices are backwards compatible with the 802.11b standard, although providing this compatibility may impact 802.11g bandwidth.

CDCN - Campus Data Communication Network is UNM's campus-wide network

CWA - Central Wireless Authority. Organization tasked with managing University of New Mexico Wireless Network (UNMWN). Currently ITS-CNS, contact person is the Director of ITS-CNS.

UNMWN - University of New Mexico Wireless Network - A wireless deployment that allows access by all UNM constituents. This type of deployment is considered Enterprise class and is implementing and managed by the University’s Central Wireless Authority (CWA).

LAN - Local Area Network. The wired network, or the Campus Data Communication Network (CDCN), is UNM's campus-wide LAN, that WAPs are connected to.

NON-ITS Supported Access Point - An access point that is connected to the CDCN without the approval or knowledge of the CWA. Most commonly contractors, employees, connect these access points to the CDCN or students that want to improve their own productivity by being able to work wirelessly. There are several problems with NON-ITS supported access points, which stem from the fact that they are not actively managed and they are not likely to be configured securely and in compliance with the UNM Wireless Standard. These devices not only pose a

security threat, they are adversely affect throughput and performance due to radio frequency interference.

SSID - Service Set Identifier. The SSID may be used as a relatively insecure security key for a Wireless LAN (WLAN), somewhat like a password. If the SSID is set in the Access Point, then only client wireless cards configured with the same SSID may connect to that Access Point.

VPN - Virtual Private Network. A VPN utilizes encryption to provide a secure means of connection over an otherwise insecure network.

WAP - Wireless Access Point. A WAP is a hardware device that serves as a common connection point for devices in a wireless network. It acts as a network switch that is used to connect segments of a LAN, providing access by multiple users of the wireless network.

Wi-Fi - Is a brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks (WLAN) based on the IEEE 802.11 specifications. It was developed to be used for mobile computing devices, such as laptops, in LANs, but is now increasingly used for more services, including Internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras..

WLAN - Wireless Local Area Network. The term often used for a wireless network consisting of one or more WAPs that provide network connectivity to computing devices equipped with wireless capability. A WLAN uses radio frequency (RF) spectrum and provides the functionality of a wired LAN without the physical constraints of the wire.

Keyword Index:

Wireless, 802.11b, 802.11g, Wireless Network. Wireless Standard, Campus Wireless.