

CWU Wireless Networking Strategy

As wireless networking technology has evolved rapidly in recent years and prices have plummeted, its popularity has risen. There is great interest across campus in making this technology widely available. ITS recognizes the value of wireless networking but believes the technology is still immature, suffering from deficiencies in bandwidth, security and interoperability with the wired infrastructure. For this reason wireless in the immediate future will hold a subordinate position to the wired network, functioning as a complement to it, not as a replacement for it. In order to meet the needs and desires of the CWU community while simultaneously addressing the concerns of ITS networking staff, *wireless infrastructure on campus will be the sole responsibility of ITS*. As with the wired network, only ITS is authorized to extend the wireless network and will do so in accordance with standards and an established plan.

Security Model

Wireless networking is inherently insecure due to its transport medium. Unlike the wired network where physical access to a data jack is required, an unauthorized wireless host can easily join an unprotected WLAN from the privacy of the owner's vehicle or other location beyond the reaches of any physical security providing the first line of defense for the wired network. Moreover, whereas in the switched CWU network environment a particular host sees only broadcasts and packets destined for its Ethernet address, a WLAN host can see and capture all traffic. Thus there are two levels of security concerns – the ability to connect to the WLAN, and once connected, the ability to eavesdrop on network traffic. The CWU WLAN infrastructure will address both of these issues by enforcing authentication and encryption.

Authentication

SSID

A client adapter associates with an access point based on a common Service Set ID (SSID). Access points can be configured to broadcast their SSID in beacon packets, in which case the client does not need to know the SSID of the access point to associate. This feature will be disabled on CWU access points with the result that the client must have its SSID configured. Since the SSID will be well-known, this provides little security, but it does provide a first line of defense against outsiders who are attempting to map the WLAN. It also prevents accidental association with the CWU WLAN.

MAC Authentication

In the wired environment a host must be registered before it can access the CWU network. If the host is unknown the switch automatically places it on an isolated VLAN where it can do minimal harm. Only when a host is registered and associated with a responsible party can it communicate on the greater network. Likewise, WLAN hosts must be registered before they can connect to the network. The registration interface will

remain the one currently in place for the wired network. A wireless option has been added to the Category drop-down list in support of WLAN hosts.

Each access point will be configured to require MAC authentication. With this setting in place the access point will look up the MAC address of a host attempting to associate. If it does not find the address the attempt will be rejected and the host will not be able to communicate on the WLAN. Host registrations will be maintained in the NetDB tables just as they are for wired hosts. Access points will be configured to query redundant freeRADIUS servers for MAC authentication. The RADIUS daemon has an Oracle interface which permits it to look up the address in the database and return the results to the access point. MAC authentication attempts will be logged by the RADIUS servers and a process can be configured to send alerts for failed attempts. MAC authentication will form the second line of defense against unauthorized access to the WLAN.

User Authentication

The best method to ensure only authorized hosts can access the WLAN is to require username/password authentication. Port-based authentication is addressed in the IEEE 802.1x standard. The implementation of this standard that will be utilized by CWU is EAP-TTLS/PAP. This method operates in a manner similar to SSL-enabled web communications. A certificate is required for the authentication server but not for the supplicant (the client component). Traffic is encrypted and login credentials pass within the encrypted tunnel. These credentials are then verified via LDAP against eDirectory by the RADIUS server. At present EAP-TTLS is the only widely available EAP method that permits authentication against eDirectory, as the other methods require access to the clear-text or NT-hashed password for verification. Closely related to EAP-TTLS, PEAP had the potential to provide this functionality as well, but Microsoft took a proprietary approach with its implementation of the protocol and required it to use MS-CHAPv2 authentication in the tunnel.

Since the PEAP implementation integrated into Windows will not meet our needs, in most cases a third-party supplicant is required. Experiments with the Meetinghouse AEGIS client, the Funk Odyssey client and the Alfa & Ariss SecureW2 client on the Windows platform have all been successful. The AEGIS client is full-featured and integrates well with the workstation login process (including the NetWare client) as does the Odyssey client, permitting single signon to the workstation, but these two are commercially licensed products. The SecureW2 supplicant is more basic and functions as an add-on to the wireless networking component of Windows. It is free. CWU has elected to purchase a 1000-user license for the Odyssey client. It is available as a free download for Windows XP and 2000 users during the host registration process.

There are also supplicants available for other platforms. The Open Source Open1x supplicant runs on Linux and some Unix variants. Both Meetinghouse and Alfa & Ariss sell supplicants for the PocketPC, and Meetinghouse supports Linux as well. Apple's OS X v10.3 and higher include 802.1x support for the internal AirPort Extreme wireless interface. Many modern Intel laptops are also being shipped with built-in driver support for the protocol.

With these security measures in place, when a device and/or user on the WLAN disrupts the network, several steps can be taken to mitigate the problem. The host's entry in the database can be disabled, preventing MAC authentication from completing and preventing the DHCP server from returning an address. The user can also be prevented from authenticating. If the infraction is severe, the user object in eDirectory can be disabled, but this will prevent the user from logging in to eDirectory altogether. If it is desirable only to deny access to the WLAN, then there is WLAN access control flag associated with the user object which can be set to false. Once any of these measures is taken, the access point can be forced to de-authenticate the device, removing it from the network.

Encryption

The 802.11 standard requires products to support 40-bit Wired-Equivalent Privacy (WEP) encryption with static keys, operating at the datalink layer. Most vendors support 128-bit WEP. Unfortunately 40-bit WEP provides only minimal security and even static 128-bit WEP keys can be broken fairly easily with tools available on the Internet. For these reasons extensions to WEP have been devised by Cisco including dynamic key rotation, message integrity check (MIC) and the temporal key integrity protocol (TKIP). Features such as these are being incorporated into the future 802.11i wireless security standard and into products supporting the interim Wi-Fi Protected Access (WPA) specification. While awaiting a truly secure wireless architecture based on these new specifications many organizations are opting for IPSec encryption at the network layer as an alternative or complement to WEP.

CWU will initially encrypt the data stream via 128-bit rotating dynamic WEP keys. A unicast key is negotiated during the EAP authentication phase and then is renegotiated periodically based on the authentication timeout set by the RADIUS server. Access points will also be configured to rotate broadcast keys. While WEP can be broken, the amount of data required to do so is significant, making compromise unlikely if keys are rotated frequently. For additional protection, users always have the option to further secure traffic at layer 3 by establishing an IPSec tunnel to CWU's VPN concentrator. *Static WEP will not be supported*, as it is insecure and unmanageable.

As enhanced security features become available, they will be tested and implemented by ITS Networks.

Integration with the Dynamic Network Environment

The CWU network is divided into sectors, each containing a standardized set of VLANs. Though the network segments assigned to these VLANs vary from sector to sector, the VLAN name and number remain the same. This consistency ensures mobility for dynamic hosts. See <http://netdb.cts.cwu.edu/dynanet-info.html> for details (on-campus browsing only). This existing model will support the addition of VLANs for the wireless

network. The VLANs wlan1, wlan2 and wlan3 will be defined for each sector, and network segments will be assigned to them. Initially these VLANs will be globally trunked with their routing handled at the core. This approach is necessary in order to support roaming of devices without loss of IP connectivity. In the future it is likely that a solution to the mobility problem such as proxy mobile IP will be implemented. In that case traffic will be segregated by defining the segments for the WLAN VLANs at each sector router and making the VLANs local to each sector.

Each sector has a native management VLAN where switches reside. For security reasons, the management interfaces of access points will not reside on this VLAN. A new wlan-mgmt VLAN dedicated to this purpose will be created for each sector and access points will be homed there. This VLAN will be configured as the native VLAN for the connecting switch port. For security reasons wlan-mgmt will not be mapped to an SSID. This configuration inhibits a host from gaining Layer 2 connectivity to an access point via malicious configuration of its SSID. The access points support 802.1q VLAN trunking on their LAN interface, with the benefit that associated clients can reside on different network segments. Only the registration, wlan-mgmt and wlan[1-3] VLANs will be trunked.

In order to permit registration of a wireless device from the device itself, the SSID 'hostreg' will be defined and linked to the registration VLAN. The hostreg WLAN will be open and unencrypted, will not require MAC authentication, and will have its SSID broadcast. This will permit an unregistered device to associate with it and complete the registration process. As on the wired network, the registration interface will automatically detect the host's MAC address, eliminating transcription errors. Once registered the user must install the supplicant (if required) and wait until the next quarter hour before attempting connection to the production network.

On the wired network, a host is homed on a staff or lab segment based on its Ethernet address. On the wireless network the determination is made based on username. The RADIUS server examines the username and returns attributes to the access point instructing it to place the host on a specific VLAN. Faculty/staff will be placed on wlan1, while students will be placed on wlan2. wlan3 will be reserved for future use. With different classes of users homed on different network segments, access list can be configured on the router to restrict access to services.

Implementation

Implementation of the wireless network will be a multi-year cooperative effort among various groups within ITS and Facilities. Prioritization of buildings is being completed by the University Information Technology Advisory Committee (UITAC). The ultimate goal is to extend wireless coverage to as much of the campus as is technically and financially feasible, including exterior spaces. The project will be implemented in phases as funding is secured. Initial plans are to complete coverage in the Library, Science, Shaw-Smyser, Black, Music, Hebler, Psychology and portions of the SUB and Bouillon by the end of 2004. Initial outside coverage will include the campus green and the Barge courtyard.

Project Standards

- MAC:* 802.11g, 802.11a (limited deployment)
- authentication:* 802.1x (EAP-TTLS/PAP implementation)
- RADIUS:* freeRADIUS running on redundant Linux servers (Open Source)
- database:* Oracle 8i running on Linux with Java interfaces
- access point:* Cisco 1220 APs with b/g radio modules

These devices also have a spare slot where we can install a radios (or a different technology when it becomes available) should the need arise for greater bandwidth in specific cases such as Geology or Computer Science. High-gain external antennae for the b/g radios will be utilized where appropriate to provide wider coverage.

The 1220 access points use Power Over Ethernet (POE). We will be installing POE capable switches where funding permits and AP density warrants their use. Otherwise power injectors will be utilized. POE will save us the expense of running power to the devices and will permit us to cold start them remotely.

Since access points are typically installed in locations which are difficult to access, it is desirable to have serial port connectivity to the devices should network connectivity be lost and unrecoverable via a cold restart. Such access has the potential to save many hours in staff time by eliminating the necessity for site visits except in the case of hardware failure. An additional network cable will be run to each access point permitting serial access from the comm room. Depending on budget and AP density, terminal servers may be installed for remote access.

- NIC:* WiFi compatible with 128-bit WEP support

Known to work well are Cisco, Linksys, Intel Centrino, Broadcom and Apple AirPort Extreme. For future security capabilities consider a WPA or 802.11i compatible NIC.

- supplicant:* Funk Odyssey, integrated Apple OS X supplicant

Known to work but currently unsupported are SecureW2, Meetinghouse AEGIS, and the Dell TrueMobile integrated client.