

Design of a Wireless Voice and Data  
Ethernet Network

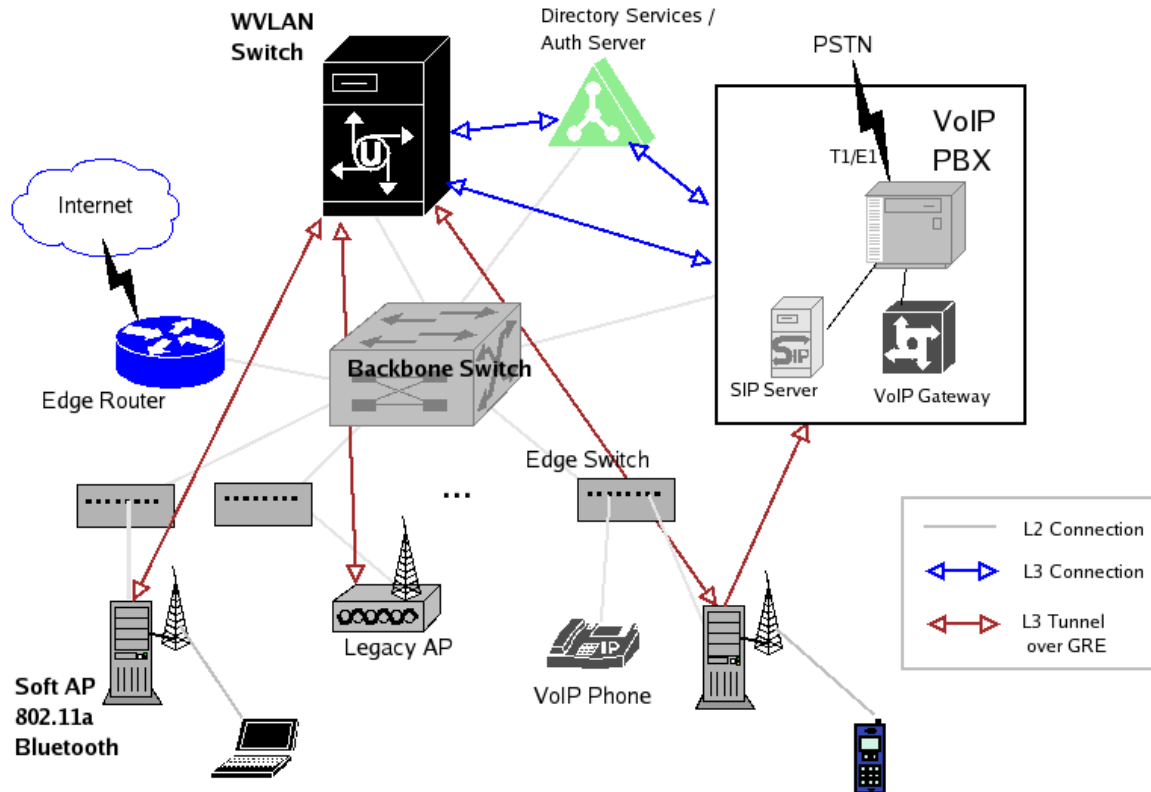
Max Baker  
EE6968 – Wireless LANs  
Prof. Inder Gopal, Fall 2004  
Columbia University  
Department of Electrical Engineering

## Table of Contents

1.	Architectural Overview .....	3
2.	Wired Voice Network.....	4
2.1.	PBX.....	4
2.2.	VoIP Gateway and SIP Server .....	4
2.3.	E911 Support.....	4
2.4.	Wired Telephony Devices.....	4
3.	Wireless Data and Voice Network .....	4
3.1.	Existing Data Network Integration .....	4
3.1.1.	Requirements and Impact .....	4
3.1.2.	Overlay vs. Unified.....	5
3.2.	Authentication Services .....	5
3.2.1.	EAP-TTLS .....	5
3.2.2.	EAP-SIM.....	6
3.2.3.	Webtrap Authentication .....	6
3.2.4.	Directory Service Integration.....	6
3.3.	Wireless Voice/LAN Switch.....	6
3.3.1.	Hardware Requirements & Considerations .....	6
3.3.2.	Network Management.....	6
3.3.3.	RF Management.....	7
3.3.4.	AP Management.....	9
3.3.5.	Firewall and DMZ.....	9
3.3.6.	Localization Services .....	9
3.3.7.	VoIP .....	10
3.4.	Soft Access Points (APs) .....	11
3.4.1.	L1 Support .....	11
3.4.2.	L2 Support .....	12
3.4.3.	L3 Support .....	13
3.4.4.	Bluetooth (802.15.1).....	13
3.5.	3 <sup>rd</sup> Party APs .....	13
3.5.1.	GRE and IPSec Support.....	13
3.5.2.	IAPP .....	13
4.	Conclusion.....	14

# 1. Architectural Overview

This document describes the architectural design of a wireless voice and data network. The wireless network is overlaid onto an existing Ethernet network and consists of Wireless Access Points (APs), a Wireless Voice/Data LAN (WVLAN) Switch, and PBX. This design focuses on two components: the Access Points and WVLAN Switch.



**Figure 1 - Wireless Voice and Data Network Overview**

The wireless network is logically separated from the existing Ethernet network. Layer-Three (L3) data traffic from wireless clients is encapsulated in encrypted L3 tunnels between the Switch and APs as shown in Figure 1. Voice traffic is tunneled directly to the VoIP Gateway to reduce the network latency of voice traffic.

Voice over IP (VoIP) services are provided to three types of phones: Type 1 is an 802.11a phone with SIP stack, Type 2 is a cell phone with SIM card that also has a Bluetooth interface, and Type 3 is a wired IP Phone.

This system is targeted at the corporate environment where data and voice security are main design requirements. Another requirement of the wireless network is self-configuration; no site survey is required and the switch provides all channel and power settings.

## **2. Wired Voice Network**

### **2.1. PBX**

The Public Exchange (PBX) is a hardware device that controls the interface between the telephone exchange and the enterprise telephony system. The Public Switched Telephone Network (PSTN) is connected to the PBX with E1 or T1 lines that carry 30 or 24 voice channels respectively.

### **2.2. VoIP Gateway and SIP Server**

Most Voice over IP (VoIP) devices use the Session Initiation Protocol (SIP) for the call-setup phase of a phone call. The SIP server allows for phone calls to be “dialed” over an IP network without involving the PSTN. The WVLAN Switch integrates into the SIP Server by informing it when phones attach to the network and at which IP address they can be reached. The Switch allows for extension following by having the SIP server route incoming calls from a wired extension to the users’ wireless handset.

The VoIP Gateway is an integral part of the PBX that converts voice data from the PSTN to IP packets and vice-versa. The Switch integrates with the Gateway by providing it with the IP address of the current Wireless Access Point or wired IP Phone where a user is receiving calls. The VoIP Gateway must support GRE and IPSec as detailed below in section 3.4.3.

### **2.3. E911 Support**

E911 support is required of telephony systems in some states. Each phone must be associated to an exact physical location. This information is made available to emergency services and law enforcement agencies for use during 911 calls. The WVLAN Switch has physical localization capabilities of wireless clients as detailed in section 3.3.6. This information is passed back to the PBX to be used for E911 compliance.

### **2.4. Wired Telephony Devices**

Wired phone extensions are provided using VoIP Phones connected to the existing Ethernet network. Analog extensions needed for faxes and modems are provided using FXS to Ethernet gateways.

## **3. Wireless Data and Voice Network**

### **3.1. Existing Data Network Integration**

#### ***3.1.1. Requirements and Impact***

As the wireless network is made to overlay on the existing Ethernet network, the existing network must be able to support the additional load. The VoIP gateway server and WVLAN Switch will be bottlenecks of traffic and must be connected to the L2 backbone with at least a 1Gbps connection. The WVLAN switch and connecting core-switch should be able to support multiple Gigabit Ethernet ports and channel bonding.

The existing Ethernet network must be robust enough to handle the additional traffic generated by the wireless voice and data clients. This document assumes that the new system is being integrated into a modern switched Ethernet environment. Each PC that is to become a soft Access Point must be on at least a 100Mb switch port. Also assumed is proper uplink connectivity between the edge switches and the core switches, using Gigabit-Ethernet or multiple bonded 100Mb ports.

### ***3.1.2. Overlay vs. Unified***

The first design decision in a wireless network is whether to use an overlay model or unified model. In a unified model the wireless network is logically truncated at the edge switch and is treated as an extension of the existing network. This usually involves VLAN routing and upgrades of the edge switches. Placing extra requirements on the edge switches, possibly replacing them, is a costly proposition in terms of hardware and management resources.

This wireless network deployment is targeting the lowest total cost of ownership (TCO) possible and attempts to use as much of the existing network as possible. An overlay model where by the wireless network is treated separately from the existing wired network is more secure and easier to deploy. The overlay model also allows for easier central management: changes to the wireless network will not require trips to wiring closets. All L3 traffic truncates at the WVLAN Switch or the VoIP Gateway allowing for the ability to firewall wireless traffic, enforce bandwidth and usage restrictions, and perform security checks such as an IDS system.

## **3.2. Authentication Services**

A single server or cluster of servers provides authentication services. Two types of authentication are required, one for the wireless voice clients and one for the wireless data clients. In order to prevent security tokens from being passed out to the Access Points, which exist on possibly insecure host PCs, all authentications will be securely tunneled to the authentication server through the WVLAN Switch from the APs. By funneling the authentication requests through the WVLAN Switch, the authentication server never has to be directly exposed to the rest of the network. The network connection between the Switch and Authentication Server can be optimized. The Authentication Server does not have to be burdened with the connection overhead incurred by having every AP connect directly to it.

The main consideration in having the WVLAN Switch front-end the Authentication Server from wireless clients is to allow for fast roaming of wireless clients. The WVLAN Switch caches both voice and data clients' authentication tokens. When a client roams between APs it is not required to reauthenticate, which can take on the order of seconds. For a voice client this delay would cause an unacceptable reduction in the quality of service.

### ***3.2.1. EAP-TTLS***

Wireless Data clients and wired voice clients on the network will be required to authenticate using an EAP-TTLS version of 802.11i. Authentication services may be provided by a 3<sup>rd</sup> party server but must provide EAP-TTLS over Radius.

### **3.2.2. EAP-SIM**

Wireless voice clients will use EAP-SIM to authenticate to the network. Each SIM card will need to be registered in the authentication system and assigned to a user. This will normally be done when the phones are deployed to users.

### **3.2.3. Webtrap Authentication**

Wireless data users that do not have the ability to connect to the network via EAP-TTLS due to security or hardware reasons will be able to connect to the network through an open (no L2 authentication) method. The client will be placed in a “sandbox” in the DMZ where the client is assigned an IP address but not allowed to send and receive traffic. A web proxy will trap any outgoing HTTP/HTTPS requests and the client will be forwarded to a secure web page where they can authenticate. Clients that connect this way are assumed to be guests to the enterprise and will be granted DMZ access, but will not be allowed through the Firewall. The WVLAN switch will provide webtrap authentication, serving as a proxy client to the existing authentication server.

### **3.2.4. Directory Service Integration**

The authentication services as well as the WVLAN Switch should be able to become an object in the directory services used in the network, and tie into the authentication framework available. This should include at least Microsoft Windows Domain Services, NIS, NIS+, LDAP, and Novell NDS. Integration into existing administrative structures allows for easier maintainability and password synchronization.

## **3.3. Wireless Voice/LAN Switch**

The Wireless Voice/LAN (WVLAN) Switch is a hardware appliance that connects to the existing Ethernet network. The WVLAN Switch performs the following functions:

- a. Manage deployment of soft and legacy 802.11/Bluetooth Access Points
- b. Layer-3 endpoint for all wireless data traffic. This includes layer-3 routing and firewall duties.
- c. RF management and security for wireless network
- d. Coordinate wireless voice traffic sent between VoIP gateway and Access Points

### **3.3.1. Hardware Requirements & Considerations**

The WVLAN Switch must be robust enough to prevent it from becoming a bottleneck for the wireless LAN's traffic. In addition it must be able to handle multiple encrypted layer-three (GRE) tunnels from each access point. To address these requirements, hardware encryption boards will be installed in a PC platform. The motherboard should be able to handle Gigabit Ethernet natively, or through PCI-Express in order to provide enough bandwidth for the incoming L3 tunnels and outgoing routed traffic.

### **3.3.2. Network Management**

The WVLAN Switch can be managed through three interfaces: Command Line Interface (CLI) through SSH or Console Cable, Secure Web Interface, and Simple Network Management Protocol (SNMP).

The WVLAN switch will provide an SNMP interface to be used by network management software. The switch will use as many existing SNMP Management Information Base modules (MIBs) from existing IETF and IEEE standards as possible before resorting to vendor-specific extensions. These include, but are not limited to, SNMPv2-MIB, IF-MIB, LLDP-MIB, ENTITY-MIB, EtherLike-MIB, IANA-ADDRESS\*-MIB, IP-MIB, IP-FORWARD-MIB, MAU-MIB, RADIUS-AUTH-CLIENT-MIB, RADIUS-AUTH-SERVER-MIB. The vendor-specific MIBs for the WVLAN Switch will provide all the same functionality as the CLI (Console or SSH) and web interfaces.

### 3.3.3. RF Management

#### 3.3.3.1. Site Survey

Due to the automated software control of channel selection and power level, the wireless deployment does not require a site survey. Instead, the WVLAN Switch will use the dense grid of Soft APs as access points and RF monitors to perform a *virtual site survey*.

During this survey only a single AP will transmit at a time while the other APs are in monitoring mode. The survey period must be long enough to account for multipath and fading channel effects, on the order of seconds. Samples of the signal-to-noise ratio (SNR) are averaged over the time period. For each AP its neighbor list is scanned for entries that are above a given threshold of SNR :  $S_1$ . Each AP listed with an SNR  $> S_1$  is placed into monitoring mode to control the radio congestion and to support the RF monitoring requirements of the WVLAN Switch. The site survey is repeated for each remaining APs that have not been set to monitor mode.

Each AP in monitoring mode will use a second minimum SNR threshold  $S_2$  as a quality of service metric. If the monitoring AP cannot hear any other APs in bridging mode with SNR  $> S_2$  then it is switched to bridging mode.

The virtual site survey sets the initial state of the wireless network and establishes the **radio proximity table** that records the relative radio strength of neighboring APs. The initial selection of APs in bridging mode and monitoring mode is used in the following channel selection algorithm.

#### 3.3.3.2. Channel Selection

Once the virtual site survey is complete, the access points will be assigned to one of the eight non-overlapping 20MHz-wide channels of the lower bands of 802.11a. Going through the list, each access point will be assigned a channel and then will send out a training sequence. All the neighboring access points will listen and record at what SNR they heard the training sequence. Subsequent APs will continue the process, choosing the channel with the least or no heard SNR as their main channel as shown in the pseudo code of Figure 2. Note that each access point checks each channel, not only the channels in use by our wireless network, because the interference could be coming from an outside source.

```

For each Bridging AP n
  // Find least occupied channel
  For each Channel i
    If (SNR[i] < S)
      channel <= i
      S <= SNR[i]

  broadcast_training_sequence()

  // Record loudest training sequence heard on channel
  For all AP m
    S <= SNR(channel)
    SNR[channel] <= max( S, SNR[channel])

```

**Figure 2 - 802.11a Channel Selection PsuedoCode**

### 3.3.3.3. Coverage Control of Access Points

The Access Points are considered volatile and dynamic elements since they are hosted inside a PC that is in use. Service can and will be interrupted for APs as computers are halted or rebooted. The WVLAN Switch will have to mitigate the volatile nature of the Wireless Network by being able to detect an AP failure. Upon failure the switch will change a neighboring AP from monitoring to bridging mode rapidly. Crucial to this process is the radio proximity table.

The Switch can either detect an AP failure or it can be by another. An Access Point determines its own capacity as specified in section 3.4.2. When the AP has reached a certain threshold of capacity the Switch will deploy another AP similar to the above failure case. The Switch monitors the status of the original APs and sets the original AP to monitoring mode when it reconnects. The AP that is changed to bridging mode during a period of congestion will be moved back to monitoring mode after the congestion is detected to have passed.

### 3.3.3.4. RF Monitoring

Access Points in monitoring mode will continually scan the Radio Frequency (RF) channels and listen to each band on the physical layer. One primary function of the RF monitoring is to keep the radio proximity table up to date. Other functions of the RF monitoring include:

- Intrusion Detection
- Rogue AP Detection
- Network Congestion and Channel Load Monitoring
- Denial of Service (DoS) and RF Jamming Detection

All processing involved will be done by the Access Point to help distribute the CPU intensive nature of RF spectrum scanning. Once a problem or change in the wireless network is detected the WVLAN Switch is notified. The AP must have the ability to send a complete or partial packet log of the reported problem back to the Switch.

### **3.3.4. AP Management**

The WVLAN Switch is responsible for the software management of the soft and legacy Access Points. The switch will push out software and firmware updates to the Soft APs over the secure L3 Tunnel. Restarts of the Soft APs will be accomplished without disturbing the host PC or requiring a restart. All configuration and security policy changes will be made over an encrypted tunnel as well.

For legacy APs the switch will serve as TFTP server and will initiate configuration and IOS upgrades over SNMP using features of the CISCO-CONFIG-COPY-MIB and CISCO-STACK-MIB. Configuration changes of the legacy APs will be done over SNMP as well.

### **3.3.5. Firewall and DMZ**

The WVLAN Switch is the termination point for all Layer Three (L3) traffic from the wireless network with the exception of voice traffic, which is routed directly to the VoIP Gateway. This makes the Switch a natural place to secure and monitor such traffic. By adding L3 security features to the WVLAN Switch separate policies can be implemented for the wired and wireless networks. Traffic can be divided into priority classes and bandwidth limits can be enforced.

A stateful firewall in the WVLAN switch will limit incoming and outgoing traffic to the wireless network. The Switch will by default have a strong rule set enabled, not opening any incoming TCP or UDP ports to the wireless clients except for those used in establishing VoIP calls. This will require the network administrator to make a conscious decision about what L3 traffic is allowed onto the wireless segment of the network.

All wireless clients will be placed in the DMZ with no outbound or inbound permissions until authorized. Clients authorized by the authentication services will be placed in a traffic class. By default there will be two traffic classes, *guest* and *internal*. *Guest* traffic will be placed in the DMZ and will only be allowed to use the edge router to access the Internet. *Internal* traffic will be allowed through the firewall to the corporate backbone as well. The user can configure additional traffic classes that restrict clients by subnet or list of servers.

### **3.3.6. Localization Services**

The WVLAN Switch will be able to provide an estimate of the physical location of a wireless client. The resolution of that estimate depends on the number of access points the client is in range of. A triangulation method is used to locate the clients. Given the high density of APs in the network, both in monitoring and in bridging mode, the resolution of localization is expected to be high.

Localization relies on the Switch having physical X,Y,Site coordinate information for each access point. This information is expected to already exist in most corporate campuses as the APs are integrated into existing PCs in the cubicles. The *Management Console* software will allow the entry of a floor plan image that the APs can be mapped to graphically.

The Management Console will use the localization information to visualize a client or access point. The localization information can also be used to visualize security threats and RF utilization and problems in the network.

### 3.3.7. VoIP

The WVLAN Switch provides tight integration with the VoIP infrastructure to allow seamless integration of Wireless VoIP clients.

#### 3.3.7.1. VoIP Gateway Integration and Client Handoff

An L3 tunnel (GRE) is created from each Soft AP to both the WVLAN Switch and the VoIP gateway upon startup. Tunnels to the Gateway server are prespawnd to avoid the penalty of establishing an encrypted connection. When a wireless voice client roams between APs the Switch will direct the VoIP Gateway to forward packets to the new AP over its existing GRE tunnel. Voice packets will then always flow directly between the VoIP PBX and the Access Point to ensure the quickest possible delivery of voice packets.

#### 3.3.7.2. Authentication Caching

The WVLAN switch maintains a list of which clients are authorized to use VoIP services. This authorization list is synchronized with the VoIP gateway. Wireless voice clients will only need to authenticate once per connection; the Switch caches authentication tokens during the lifetime of a client's connection to the wireless network.

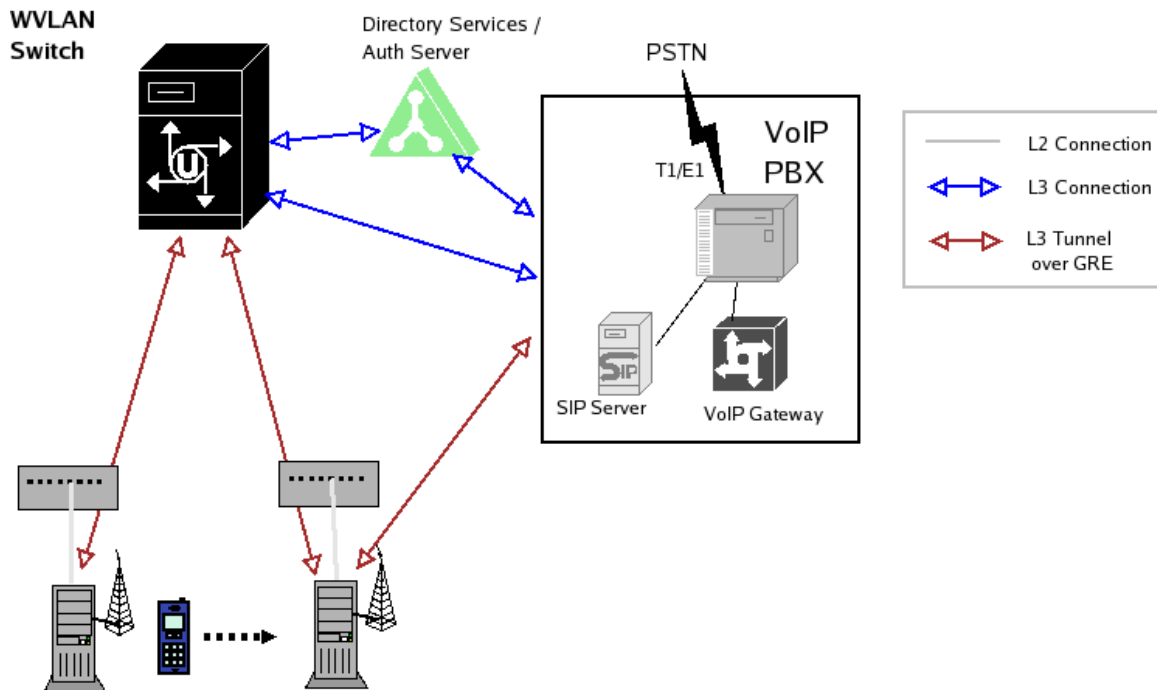


Figure 2 - Wireless Voice Client Roaming

### 3.4. Soft Access Points (APs)

The Access Points (APs) of the wireless network consist of a dual-band 802.11 NIC, a Bluetooth Card and software installed in existing PCs in the enterprise. By using a “soft” access point the installation only requires adding additional cards to the computers – a task that can be accomplished by junior network administrators or in rollout of new PCs. The total deployment cost is kept low by not requiring extra infrastructure deployment such as new wall ports, Ethernet switch ports and power connections for the access points.

The initial software will be deployed using the existing enterprise software management or by hand. The WVLAN switch will then manage further software and firmware updates of the access points.

The Soft AP will be written in C++ with portability in mind. It will have to run on various host platforms including Linux, FreeBSD / OS X, and Microsoft Windows 2k and XP. The software will be separated into portable and system-specific portions. An evaluation of the existing open-source Soft Access points will be used as a baseline. These projects include:

- *HostAP* project
- *Cquire* project
- *Linux bridge, ebtables, and wireless\_tools* projects
- *Lessnetworks Hotspot* project
- *Linksys WRT54G Firmware (Linux Based)*
- *Sveasoft* extensions to WRT54G

The 802.11 card used must provide an interface to raw radio data in order to perform RF monitoring. The card should also be able to be soft-boot so that firmware updates can be accomplished without restarting the host PC. The access point will operate either in a *bridging* or *monitoring* mode.

#### 3.4.1. L1 Support

All data and voice clients will use 802.11a (OFDM Physical Layer) for 802.11 wireless communication. 802.11a was chosen over 802.11b/g for the following reasons:

1. The 5GHz band is much less used and therefore not subject to as much radio interference. The distances that signals travel in this band are reduced compared to the 2.4GHz ISM band, however due to the dense deployment of Soft APs this is not a concern.
2. 802.11a has more non-overlapping channels and can therefore provide higher network capacity.
3. The 2.4GHz band is going to be in use by the Bluetooth NIC. Bluetooth and 802.11b/g traffic may interfere if operating simultaneously from adjacent NICs.

The legacy APs may be 802.11b/g and could be used to provide limited coverage for these physical layers if needed.

### **3.4.2. L2 Support**

The access points can be set to use either the PCF or HCF (802.11e) MAC coordination function to control access to the medium, depending on client support. Contention-free access to the medium supplied by these functions is not critical to guaranteeing bandwidth in this system, but will allow for a higher ratio of clients per access point and better quality of service by giving an upper-bound on packet delay for voice traffic.

Bandwidth is guaranteed by load balancing clients across different APs. Using the eight non-overlapping channels available in 802.11a, neighboring APs will not interfere with each other and can be placed densely. Each AP will monitor its wireless and wired network capacity as well as the CPU load of the host PC. If any of those metrics exceeds given thresholds, the soft AP will notify the WLAN Switch and a neighboring AP in monitor mode will be switched to bridging mode. The AP may be loaded by activities on the host computer in addition to the load placed by the wireless network. The client's request will be deferred to the new AP.

#### **3.4.2.1. Multiple SSID support**

Different SSIDs will be used on each Access Point that will classify the wireless traffic into different security and functional classes. By default three SSIDs will exist: one for voice traffic, one for data traffic, and one for guest traffic. Each of these classes has different encryption and authentication requirements that are best segregated at an early stage.

#### **3.4.2.2. Authentication and Encryption**

Data from wireless clients is authenticated and encrypted using 802.11i standards. Data client authentication is done with 802.1x using EAP TTLS, while voice client authentication uses EAP-SIM. Guest traffic will be authenticated using the *webtrap* method discussed in section 3.2.3.

Wireless data traffic is encrypted using the Advanced Encryption Standard (AES), which passes FIPS-197 requirements. Currently there are no hardware accelerators for wireless applications that can decrypt and encrypt AES fast enough for voice traffic. The voice clients must instead use the TKIP standard defined in WPA for encryption.

The Soft APs use the host PC to decrypt L2 traffic from wireless clients. This traffic is then passed up to the encrypted L3 tunnels.

#### **3.4.2.3. ARP and DHCP Proxy**

Most Layer-Two (L2) functions are stripped away from the wireless network for efficiency. The two L2 protocols that the clients need are the Address Resolution Protocol (ARP) and the Dynamic Host Configuration Protocol (DHCP).

The WVLAN Switch will perform both ARP Proxy and ARP Caching for the wireless clients. In ARP Caching, if a station ARPs for the IP address of another station, the IP of the Switch is returned and the Switch must perform the routing. For ARP Proxy the Switch will respond to ARP requests destined for the wireless station. Both of these methods are aimed at reducing L2 broadcast traffic on the wireless LAN.

In order for subnet mobility to function the station must be able to use the same IP address at every access point. DHCP Proxy allows the WVLAN Switch to respond to manage traffic between the DHCP server and the wireless client. This ensures that the mobile station will be returned the same IP address when roaming.

### **3.4.3. L3 Support**

The WVLAN Switch controls all Layer-Three (L3) communication on the wireless network. Wireless traffic is tunneled to the switch from the access points using the Generic Routing Encapsulation (GRE) protocol. GRE traffic is then encrypted and sent to the Switch using the IPSec protocol. IPSec allows for a variety of encryption standards. The possible standards would have to be evaluated with the given hardware to determine which would give the lowest delay for the required level of security. A low-delay, lower-security IPSec tunnel would connect the VoIP Gateway and a higher-security, higher-delay IPSec tunnel would funnel data traffic to the Switch.

#### **3.4.3.1. VoIP Routing**

Traffic to wireless VoIP clients will be sent directly from the VoIP Gateway to the Access Point over a low-delay IPSec/GRE tunnel. The Switch notifies the Gateway when mobile clients roam so that voice data can be forwarded to the new AP.

### **3.4.4. Bluetooth (802.15.1)**

A certain number of PCs will also be outfitted with an 802.15.1 adapter using USB or PCI in order to support the Type-2 phones. The Bluetooth networks will be operated in TDM mode for channel access to guarantee delay bounds on the voice traffic. After the Bluetooth pairing procedure the phones will authenticate using EAP-SIM. Traffic will be encrypted using the 4xLFSR (128-bit) key encryption method. If the AP is over capacity (see 3.4.2) it will not allow the Bluetooth device to pair with the AP.

## **3.5. 3<sup>rd</sup> Party APs**

The WVLAN Switch will provide support for 3<sup>rd</sup> party 802.11 Access Points, specifically Cisco 1200's. GRE was chosen as the L3 tunneling protocol specifically because it is available on the Cisco APs.

### **3.5.1. GRE and IPSec Support**

The AP1200 supports GRE to allow subnet mobility. It does not however have IPSec encryption support for GRE tunnels. The AP's wired connection to the L2 network must be physically secured in order to guarantee the integrity of the data from the wireless network.

The AP1200 also does not support multiple GRE tunnels for L2 traffic. Therefore all voice traffic will go route through the WVLAN Switch along with the data traffic.

### **3.5.2. IAPP**

The AP1200 uses the Inter Access Point Protocol (IAPP) to control roaming of mobile clients. The WVLAN Switch will implement IAPP and receive and send roaming information to the 3<sup>rd</sup> party APs.

## **4. Conclusion**

This document introduces the deployment of an overlaid wireless voice and data Ethernet network. The novel approach of providing wireless access using Soft Access Points is explored. A wireless voice/data LAN switch appliance is introduced to manage all aspects of the wireless network including security, RF management and Voice over IP integration. This document serves as the base for a full specification document needed to construct such as wireless network.