

# San Jose State University

---



College of Engineering

*CMPE-209*  
Project Report

## **Securing voice over WLAN (VoWLAN)**

Under the guidance of:  
Dr. Xiao Su

# Securing Voice over Wireless Local Area Network (VoWLAN)

Maulik Thaker  
004676309  
maulikthaker@gmail.com

Jahanzeb Baqai  
003977572  
jbaqai@usa.net

Gopal Lokesh  
004657836  
gopallokesh@yahoo.com

Venkatesh Babu  
003749214  
mpvbabu@yahoo.com

## ABSTRACT

Many enterprises are adopting VoWLAN (Voice over Wireless LAN) systems to enjoy lower costs. There are number of vendors who are providing VoWLAN solution. All have their own way of providing security solutions to their customers. In this paper we discuss how VoWLAN works, various VoWLAN security challenges and how these security challenges are handled by solutions provided by major vendors like Aruba Wireless Networks, Cisco, Meru Networks and Juniper Networks. Finally, comparisons of solutions are discussed, and concluding remarks are drawn

**Keywords :** VoWLAN, Access Points, WAP,

## 1. INTRODUCTION

Wireless LANs (WLANs) are becoming a fixture in the enterprise and quickly proving their worth. At the same time, many enterprises are adopting VoWLAN (Voice over Wireless LAN or Wireless VoIP). VoWLAN market will initially be driven by specific corporate needs, such as warehouse and retail sales tracking and control, ubiquitous mobile telephony in medical campuses and hospitals, and mobile security applications.

The convergence of voice and data networks enables new applications and cost reductions. VoWLAN provides mobility, productivity and ROI. VoWLAN becomes an increasingly viable option with the influx of new

VoWLAN enabled phones, including dual mode cellular/VoWLAN phones. More details about how VoWLAN works is discussed in following **VoWLAN deployment** section.

Compared to VoIP on wired LAN, VoWLAN provides ability to roam between Access Points and maintain a voice connection during the process. VoWLAN requires additional security for the voice transmission, its associated control signaling and configuration.

Some of the challenges for adoption of VoWLAN are: Excessive latency and jitter (degraded voice quality), Poor coverage, Roaming latency between Access Points (interrupted voice service), Security issues, Retransmissions and dropped packets, Low capacity (reduced number of calls), Quality of service (required for voice), Power consumption requirements. Major VoWLAN security issues are: Eaves dropping, User authentication, Man in the middle attack, Session hijacking, and Denial of service. More details of above mentioned security issues are discussed in following section.

There are number of vendors who are providing VoWLAN solutions to handle most of VoWLAN challenges. All have their own way of providing security solutions to their customers. More details about VoWLAN solutions from major companies like Aruba Wireless Networks, Cisco, Meru Networks and Juniper Networks are discussed in following section. Comparison of different

solutions from different vendors with respect to Technology, Wireless security, Wireless QoS, Network Features, Performance and Cost are provided in following section. Finally, we make concluding remarks and summarize this paper along with Reference Section.

## 2. VOWLAN DEPLOYMENT

Figure 1 below shows possible way of VoWLAN deployment in enterprise. VoWLAN can be used in one of the two possible ways. One way is to route calls from the phone to a WLAN access point and then to a VoIP gateway. The gateway may already be in use to deliver This set-up allows all regular PBX functions that are available on a wired desk phone to be available on the VoWLAN phones. Calls that are made to phones outside the company will go through the PBX to the PSTN (Public Switched Telephone Network).VoIP over wired

networks. The calls are then translated between the IP network and the private branch exchange (PBX). Another way for VoWLAN to work is for software-based phone, also known as softphones, to route calls over the Internet. In this scenario, users can use the softphone on their PDA, cellular phone or laptop to place calls from a location or hotspot that offers a WLAN. The call could be routed anywhere over the Internet thereby making it virtually free.

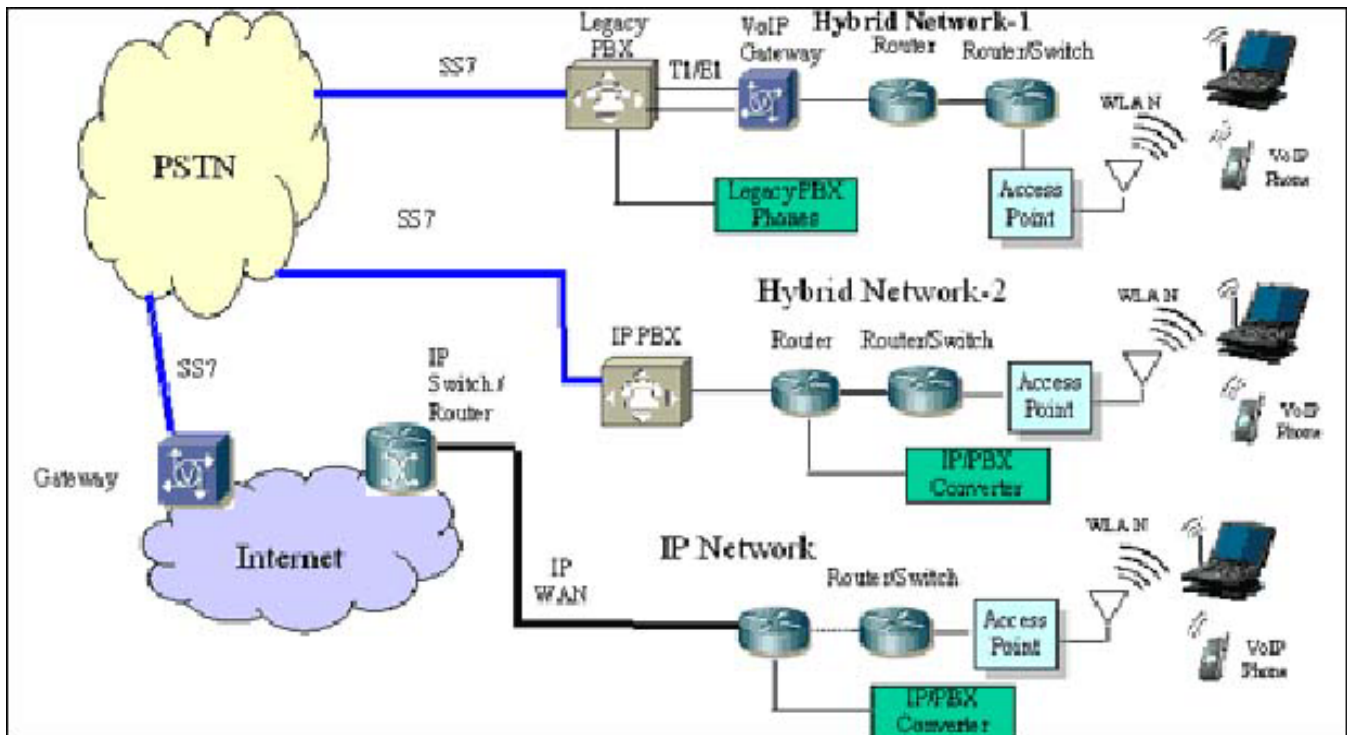


Figure 1. (Source: Internet Engineering Consortium)

### 3. SECURITY THREATS IN WIRELESS LOCAL AREA NETWORK (WLAN)

WLAN works in open radio frequencies which exposes to more attack than wired LAN, the intruder can use an antenna and receiver to detect and tune to radio frequency of the target wireless network.

Despite the advantages of wireless networking, WLANs are vulnerable to security threats. Common threats include eavesdropping, unauthorized access, and interference and jamming, and physical damage.

#### 3.1 EAVESDROPPING

This is a passive attack where the intruder, will listen/observe the network messages between wireless Access Point (AP) and also between Wireless AP and Wireless Client without altering message. This will compromise the confidentiality of sensitive and proprietary information exchanged on the wireless network.

##### **Countermeasures:**

Using spread spectrum technology that is not easy to decode, and also encryption of messages over the air.

Using encryptions such as WPA/WPA2, EAP (Extensible Authentication Protocol) with RADIUS Authentication server.

WPA (WiFi Protected Access): The WPA security model has four components for better securing connectivity:

- Wireless Transport Layer Security Protocol (WTLSP) provides confidentiality, integrity, and authenticity.
- WPA Identity Module (WIM) provides credential portability and client authentication.

- WMLScript CryptoLibrary facilitates cryptographic applications to transmit, store, forward or receive signed data from clients.
- WPA Public Key Infrastructure (WPKI) is a wireless implementation of PKI techniques.

#### 3.2 UNAUTHORIZED USER ACCESS

This is an active attack; the intruder will enter a WLAN disguised as an authorized user of wireless network. Once inside network the intruder can violate the confidentiality and integrity of network traffic by sending, receiving and altering the data traffic.

One of the approach used by intruder to gain network access could be place fake AP with higher signal strength in the wireless network, use this AP to trick clients initiating connection with AP to intruder network. The user will be denied to logon to network, during which the intruder will capture user id and password information. The attack is difficult detect since unsuccessful logon are relative common in WLAN due to error rate in radio transmissions.

##### **Countermeasures:**

Deploying efficient authentication and intrusion detection mechanism that enables to detect fake AP's, raise an alert to the administrator about the intrusion.

AP's to maintain ACL's with valid MAC address of client that can be connected to network and to avoid sending user and password information, before wireless AP's is authenticated with the client.

#### 3.3 DENIAL OF SERVICE

The intruder will transmit strong interfering/overlapping radio frequency of the target network which seriously affect the network bandwidth in turn the network performance. The intruder could perform this action remotely (few 100 feet's away) from the target network

### Counter measures:

To have the network that can switch over to channels or frequencies that have more available bandwidth. The reactive measure is to use direction finding equipment can detect the source of jamming signal, but not necessarily in time to prevent jamming signals.

The WLAN is also prone to other common network attacks such as,

- Man in the Middle
- Session Hijacking

The IEEE as come up with new supplement specification to fill the shortcomings in existing 802.11 specifications security, with 802.11i. 802.11i provides an alternative to Wired Equivalent Privacy (WEP) and introduces 802.1x access control, dynamic re-keying, per session, key distribution mechanisms and strong cryptographic algorithms. Centralized security management forms a key part of 802.11i.

## 4. VOIP WLAN NETWORK VULNERABILITIES, THREATS AND CHALLENGES:

The VoWLAN carries the same security vulnerabilities and threats of WLAN that carry data. In addition, VoWiFi phones bring new security challenges to WLANs for two primary reasons.

- The current VoWiFi phones have limited security standards/protocol support, computing resource and battery life. Which leads to the network to handle and manage security issues to support VoWiFi phones
- They require secure, fast handoffs between WiFi phone and Access Point while WiFi phone move from one Access Point to another, two often-opposing goals.

Thus WLAN supporting voice services offers more opportunity for hackers than data WLAN. VoFi phones are more susceptible to earlier mentioned attacks such as Man in the Middle, Eavesdropping, and Unauthorized access to network.

The Voice enabled WLAN are more likely to extend the coverage of RF transmission across the building surroundings, attacker could jam/interference RF transmission of WLAN resulting denial of Service or steal authentication credentials and gain access to WLAN.

The VoWiFi phones are inherently used for mobile use, and can be easily lost or stolen. If they are not password-protected, the finder can make calls whenever in range of WLAN.

Often the only method available to identify these WiFi phones on the WLAN is to use the MAC address, but this form of authentication is imperfect, as MAC addresses are easily detected and spoofed.

SoftPhone are based on PC, Laptop or PDA, these clients can access WLAN for both data services and Voice. PDA clients differ from single-purpose mobile VoFi phones because of support of both voice and data streams simultaneously, rather than only voice.

This compromises networks that are designed to separate voice and data onto different VLANs; either PDA joins the voice VLAN, in which case the voice streams must be allowed through firewall onto the enterprise LAN, compromising data security. Or the PDA works on the data VLAN in which case the QoS and handoff mechanisms associated with the special voice VLAN will not be available to PDA.

## 5. QUALITY OF SERVICE (QOS) ISSUES IN VOWLAN

The voice traffic is sensitive to latency reaching the destination, the encryption used to transmit voice stream securely should not be computationally intensive for limited capabilities of VoWiFi phones. The WLAN network has to address latency by prioritizing VOIP packets, which leads to reduce delay.

IEEE as introduced supplemental specification to 802.11 to address the QoS support for both WLAN and wired LAN with 802.11e specification. The QoS feature includes the prioritization of data, voice, and video transmissions.

The secure fast handoff requirement; VoFi phones are hand held devices that are carried around the building while in operation. User expectations are for continuous, unbroken conversation; the voice stream cannot be interrupted for more than few tens of milliseconds without causing annoyance to user.

This leads technical challenge due to range limitation of WiFi signals. A VoFi phone moving in a building will have to roam between APs frequently, as an AP may only have range of 30-50 feet. This requires network AP's to re-authenticate VoFi phone while switching from one AP to another AP without compromising network security and voice quality.

This requires network architecture that performs efficiently re-authentication, encryption re-keying, connection redirection and QoS context switching. This must be performed every time VoFi phone roams from one AP to another.

## 6. SECURITY ISSUES FOR VOWLAN HANDLED BY MAJOR PLAYERS

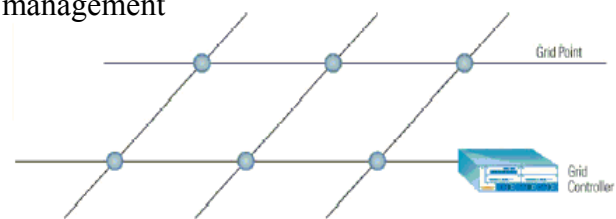
### 6.1 ARUBA NETWORKS WLAN

#### 6.1.1 ARCHITECTURE:

Aruba VoWLAN architecture has densely deployed thin wireless access point also known as grid points (GP), the GP's connect to existing LAN infrastructure using grid controller

In addition to wireless connectivity functionality, GP's are capable of RF monitoring, security, trouble shooting and location service.

The grid controller is a high-performance WLAN switch with hardware encryption engine, also with software that manages grid of GP's to deliver the desired mix of wireless services as the load on the grid changes. The grid controller provides policy engine to store and enforce security profiles and policies, stateful per-user firewall and an interface to allow provisioning of services such as virus detection and remediation. It also acts as authentication proxy for the enterprise user authentication server and performs automated RF management



Wireless grid: densely deployed Access point and Grid controller

Source: Aruba Networks

#### 6.1.2 AUTHENTICATION AND ACCESS CONTROL

GPs connect to the grid controller by encrypted tunnels, to deter eavesdrop on the wired LAN. And the grid controller itself is a certified-secure

appliance. This enables it to act as a proxy for the enterprise authentication server.

A client wishing to join a wireless grid signals to the nearest GP. The messages are forwarded on the secure tunnel to the grid controller, which communicates with the enterprise authentication server. Once the client is authenticated, the grid controller maintains its authentication information.

When the client roams to new GP, its signals an association request using new PairWise master keys to that GP, and the information is tunneled securely to the grid controller. The grid controller acts as a proxy and authenticates the client, enabling continuing service which short cuts re-authentication of client with authentication server and reducing load on authentication server.

Hence the grid controllers act as anchor point for secure handoffs as VoWiFi phones move between GP's.

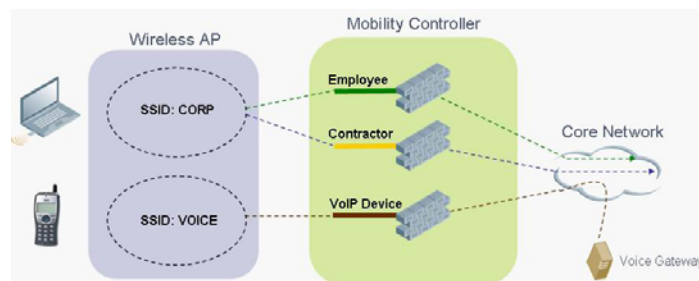
Following authentication, the grid controller proceeds with authorization. It retrieves the user's profile and applies it to all traffic streams, including voice streams. This is possible because the grid controller includes a full, user-aware stateful firewall and all traffic from wireless clients must pass through firewall to reach the wired LAN.

The grid controller provides administrator with tools to define policies and apply them to classes or individual devices, users.

Policy can be set based on:

- a. User identity
- b. Device identity
- c. Device state
- d. Resource requested
- e. Application used
- f. User location
- g. Time-of-day
- h. Authentication method

The policy based user authentication enables to support older VoWiFi phone that are less secure than other WLAN client with special treatment using role-based access control. The older voice phones use MAC address for authentication and static-key WEP encryption



Role Based Access Control (Source: Aruba Networks)

Role based access control places each user or device into a “role” – or a collection of access rights and policies – typically learned through an authentication system. Example roles include employee, contractor, voice handset or IT staff. Each role has an associated set of policies which can include bandwidth limits, time of day restrictions, location based restrictions and firewall policies that permit or deny network traffic based on source, destination and service. Aruba enforces access rights using ICSA certified policy enforcement firewall.

The firewall is user-aware and stateful, it can allow a certain user or device to send only a certain protocol traffic. This enables to enforce a rule that the phone can send only voice-protocol traffic, and only to the IP PBX as a destination.

The firewall also manages opening and closing of sockets dynamically required for maintaining the call session to prevent security vulnerabilities by opening range of sockets that can be supported for voice calls.

Aruba's universal authentication for wireless access allows MAC address, 802.1x, VPN and captive portal browser based authentication to be active simultaneously. Universal authentication allows laptops and modern PDAs to authenticate using 802.1x with dynamic encryption, guests to authenticate using browser based authentication and voice handsets to authenticate using MAC addresses. Aruba mobility controllers support enterprise grade scalability by permitting MAC addresses used for authentication to be stored in a RADIUS or LDAP database.

## **6.2 CISCO NETWORKS VOWLAN**

### **6.2.1 APPROACH**

Cisco Voice over WLAN solution provides organizations advantage of the proven cost savings and enhanced productivity tools of IP communications for an increasingly mobile workforce. Cisco been a market leader is in a unique position to bring together the key elements of a Voice over WLAN Solution

The Cisco VoWLAN solution accelerates productivity of office workers in all industries, accessing Cisco CallManager call-handling and conferencing tools, as well as rich media applications, from anywhere on campus. And organizations with mobile employees can reduce cell phone bills by deploying 802.11-enabled devices to support voice communications. The Cisco VoWLAN solution also lets enterprises standardize on a laptop or personal digital assistant (PDA) for voice and data communication to reduce the number and type of mobile communications devices they need to support and secure, helping enable broad deployment of mobility-enabled enterprise applications.

### **6.2.2 ARCHITECTURE**

At the heart of the Cisco VoWLAN solution is an intelligent, end-to-end network infrastructure. It is an enterprise solution in which the Cisco Aironet

wireless network infrastructure and the IP Communications system work together to provide reliable, manageable connectivity. The Cisco VoWLAN solution addresses the challenges of implementing a converged solution using several advanced technologies.

Cisco's Wireless LAN Solution delivers one integrated network, both wired and wireless, for data, voice and video. This integration enables common QoS policies, fast secure roaming, simplified deployment and operation of the converged network. through the Cisco Compatible Extensions program, wireless clients are enabled with critical features such as QoS to support upstream voice communications.

### **6.2.3 SECURE INTEROPERABLE PORTFOLIO OF VOICE CLIENTS**

The Cisco Wireless IP Phone is an easy-to-use IEEE 802.11b wireless IP phone that provides comprehensive voice communications in conjunction with Cisco Call Manager and Cisco Aironet® series of Wi-Fi access points. The Cisco Compatible Extensions program gives voice client manufacturers the ability to design current and future voice wireless innovations into a wide variety of devices. The wireless clients are a key elements in Cisco's Self Defending Network which provides a Secure wireless Connectivity, Threat Defense, and Trust and Identity Management.

### **6.2.4 VOICE SECURITY SOLUTION:-**

VPN  
IPSec  
Firewall  
NAT (Stateful l NAT )  
CCKM (Cisco Centralized Key Management )

### **6.2.5 ENCRYPTION AND AUTHENTICATION**

LEAP  
WEP (40/128 bit)  
TKIP/MIC per WPA,

(TKIP= Temp Key integrity protocol, MIC = Mess Integrity check)  
 CCKM  
 EAP-FAST (available with v3.0 in Feb '06)  
 WPA (WPA = 802.1x + EAP + TKIP + MIC).

### 6.2.6 CISCO CASE STUDY

The network diagram shows the topology of a site called “Central Site 1,” which was setup to simulate the customer’s main location in Asia. This site included an access layer, collapsed distribution/core layer, server farm layer, Cisco cluster, unity voice mail servers and several IP Phones.

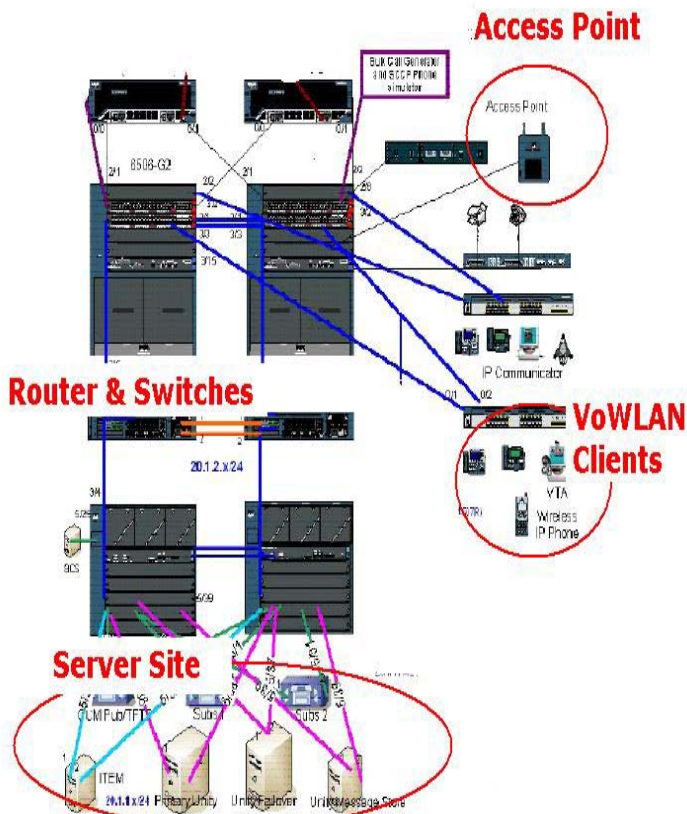


Figure 1: Physical Network Topology – Central Site 1

This site was also connected over a WAN at two different locations which were the Northern America. The Branch Office was an office located

in another Asia Pacific country with only IP Phones.

The IP Phones were connected to the access switches and the PC connected to the switch port of the IP Phones The Cisco Wireless IP Phone delivers up to six extensions, wireline voice quality, small form factor, standard and extended Li-ion battery options, menu driven graphical user interface, inter-campus secure-seamless roaming, Cisco Wireless Security Suite IEEE 802.1X Cisco LEAP and 40/128 bit static Wired Equivalent Privacy (WEP).

### 6.3 JUNIPER / MERU NETWORKS APPROACH TO VoWLAN.

#### 6.3.1 APPROACH

Juniper Networks and Meru Networks have entered into an agreement to co-market secure, pervasive wireless VoIP. The partnership will combine Meru's Air Traffic Control technology with Juniper's IP routing and security offerings. Policy enforcement of network security with the combined solution will remain the same whether users are wired or wireless. Security and consistency have been the major customer barriers to adoption of wVoIP, issues that the combined solution will aim to address.

The key issues around VoIP in general (including wireless VoIP) are security of the network and the ability to deliver consistent, high quality VoIP communications. Juniper offer a range of security, quality, and reliability features on both routing and security portfolio that keep the network secure and help improve the reliability and quality of all VoIP services.

Meru also sees the Juniper partnership adding value to Meru's wVoIP solution, particularly in the area of network security.

Enterprises deploying VoIP must ensure their existing IP network is capable of handling additional voice requirements. VoIP traffic

demands a high level of performance, reliability and security to obtain the same level of quality as traditional voice services. The Juniper Networks secure and assured VoIP networking solution is designed to meet these VoIP requirements and enable high quality, secure VoIP communications.

The Juniper Networks VoIP solution is secured by a robust, voice-aware security platform that defends the entire business network against security threats. VoIP introduces new security challenges that must be defended to prevent Denial of Service (DoS) attacks, toll fraud, PBX hacking or unauthorized access, eavesdropping and many others. The Juniper Networks VoIP solution is designed to protect against these threats to ensure corporate assets remain secure. Junipers range of security products includes high performing Firewall/VPN devices, IDP for application level threat protection and SSL VPNs for extending the reach of a business VoIP network.

### 6.3.2 PREDICTABLE AND ASSURED QUALITY IS ACHIEVED BY:

- Comprehensive QoS techniques to classify, prioritize and schedule VoIP traffic
- Hardware acceleration for fast processing of VoIP media traffic

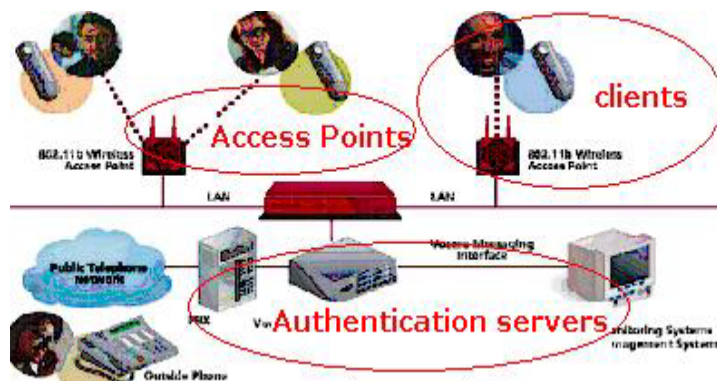
### 6.3.3 VOWLAN IS SECURED BY:

- H.323 and SIP Application Layer Gateways to dynamically open and close Firewall pinholes
- Zone architecture to separate voice network from data network with policy control
- Dynamic route-based VPNs with failover capabilities
- Site-to-site VPN with encryption (DES, 3DES, AES) to prevent eavesdropping or man-in-the-middle attacks
- H.323 and SIP policy based access controls
- IDP for application layer security
- SSL VPNs that extend VoIP network to remote users

In addition to routing and Firewall/IPSEC VPN technology, additional security protection is available through the Juniper Networks Intrusion Detection and Prevention (IDP) products. IDP provides protection against worms, Trojans, spyware and many others as well as SIP protocol anomaly detection. Enterprises frequently deploy IDP products to protect the PBX and other voice assets.

SSL VPNs extend an enterprise VoIP network to remote workers as well as partners and customers. SSL VPN technology allows remote workers to use their existing phone number and feature set through a softphone. This provides flexibility and convenience and enables enterprises to fully utilize their VoIP network.

The Juniper Networks Firewall / IPSec VPN security devices are purpose-built to perform essential security functions. These integrated devices combine a Stateful Inspection firewall with Deep Inspection technology for application-level protection, IPSec virtual private networking (VPN) capabilities, and denial of service (DoS) mitigation functions. Plus they are all manageable by a policy-based central management system, NetScreen-Security Manager.



Source : [www.merunetworks.net](http://www.merunetworks.net)

They are available in a range of devices built to meet the throughput requirements of enterprises of all sizes.

Generalizing the facts, from the figure above, Aruba/Meru takes control of security issues in the following respects.

#### Access Controls

- Unique User Identification
- Encryption and Decryption: TKIP. Dynamic re-keying via WPA-capable RADIUS server.

#### Audit Controls

- Via SNMP thro' WPA-compliant RADIUS server.

#### Integrity

- TKIP – MIC – Data compromised.

#### Person or Entity Authentication

- Using WPA with 802.1x authentication.

#### Security Management

- Risk Analysis: Continuous Monitoring of air waves - rogue access points, ad hoc stations, improper configurations ,accidental associations.

## 7. ANALYSIS :-

Per our analysis, Aruba is the best choice for the customer who already have network infrastructure and wants to add on the VOIP service. The following are the pros and cons

### 7.1 ARUBA

- Pros
  - Cost = 9k
  - Outstanding voice quality
  - Best QoS in compare to other vendor solution.
- Cons
  - Not scaleable
  - Performance degradation in stressful condition

On the other hand , Cisco provides the best security solution for the VoWLAN and support rich set of features including routing and switching function.

### 7.2 CISCO

- Pros
  - Support rich set of features includes routing and scalability
  - Best security solution as compare to other vendors in the market
- Cons
  - Cost = 52k
  - Poor QoS implementation, drop Voice traffic in heavy stress load
  - Poor (as compare to other vendors) voice quality in both normal and stress mode

### 7.3 JUNIPER / MERU

These companies are different in their ways of keeping security features depending upon the cost. They have products with increased security, but then you have to compromise with the cost. Though, their average cost of their product can turn out to be around 35k.

The comparison chart in the next page shows all the relevant security and additional technical details that these companies provide publicly. Though some of the core technical details were not obtained due to trade policy issues.

## 8. COMPARISON CHART

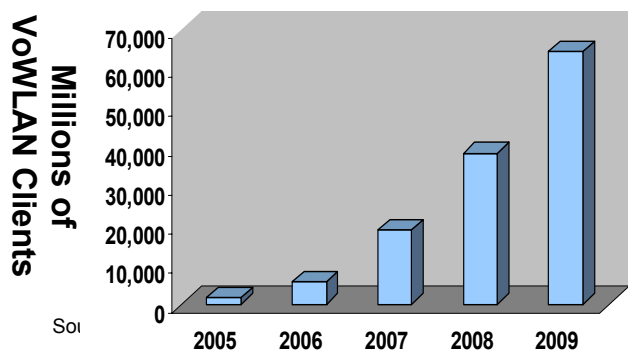
	<b>Cisco</b>	<b>Aruba</b>	<b>Juniper/Meru</b>
<b>LAN Security / VPN</b>	Yes	Yes	Yes secure by (DES, 3DES, AES)
<b>Firewall</b>	Statefull Firewall	Statefull Firewall	Statefull Firewall
<b>NAT</b>	Statefull NAT	Yes	Yes
<b>Zone :- Separate Voice with Data</b>	Yes	Yes	Yes
<b>IDT (Intrusion Detection and Prevention)</b>	No	Yes	Yes
<b>Wireless Security</b>			
<b>Encryption and Authentication</b>	1) LEAPWEP (40/128 bit), TKIP/MIC per WPA, (TKIP= Temp Key integrity protocol, MIC = Mess Integrity check) ,CCKM, EAP-FAST (available with v3.0 in Feb '06), WPA, (WPA = 802.1x + EAP + TKIP + MIC)/	WEP(128bit) ,PMK/PTK (PMK=Pairwise Master Key, PTK=Pairwise Transient Key), WPA2	<b>WEP(128bit) ,WPA</b>
	802.11i	802.1x/802.11i	802.1x/802.11i
<b>Encryption Method</b>	Centralized + client side	Centralized	Centralized
<b>Roaming</b>	Fast Secure L2/L3 Roaming		
<b>Wireless QoS</b>			
<b>Wireless QoS</b>	QBSS	QOS	QOS
<b>Network Features</b>			
<b>Discovery Protocol</b>	Cisco Discovery Protocol		
<b>Alternate TFTP Support</b>	Yes		
<b>Provisioning and Configuration</b>	DHCP/static IP Addressing	DHCP/Static	DHCP/Static
<b>Site Survey, Trace Route</b>	Yes	Yes	Yes
<b>Seamless-Secure Roaming, and VLAN support</b>	Yes	Yes	Yes
<b>Performance</b>			
<b>Delay &amp; Jitter</b>	Max = 260msec Ave = 40msec	Max = 40msec Ave = 10msec	Max = 250msec Ave = 40msec
<b>R-Value</b>	With QoS= 80 Without Qos = 50	With QoS= 75 Without Qos =75	With QoS= 65 Without Qos =45
<b>Voice Quality b/w two AP</b>	75	76	70
<b>Cost</b>	\$51,978	\$8,780	\$35,875
R-value ratings - An ITU specification that determines call quality, R-value measures packet loss, jitter and delay			

## 9. CONCLUSION

In the document we have tried to cover what are the current security challenges we are facing in implementing VoWLAN, research on solution provided by the industry leader, and finally compare the solution.

Still, some of the ideal solution for securing VoWLAN would be encryption at the End Points / Access Points, Securing Real Time protocol, Key management issues, having better Scheduling schemes at the Access Points and compressing the packet size with proper cryptographic algorithms and resolving some IPsec incompatibilities.

VoWLAN is growing fast , per ABI research by year 2009 the number of VoWLAN client will 70,000 million.



Copyrights® 2004 ABI research

The benefits of the VoWLAN can be enjoyed by everyone, from business user to the normal person in house. It's a technology which benefits all.

The comparison chart reveals all the details regarding the usability of the technology. As time passes these usability requirements will definitely go up exponentially.



Source: 2004 WLAN State of the Market Report., February 2004

## 10. ENDING COMMENTS

The challenges of securing a voice over network may seem insurmountable, but in many cases much of the work may already be done. Voice over Internet

Protocol, as its name implies, is a network service with many of the same security requirements demanded by a secure data infrastructure. An enterprise that has already done its due diligence may only need to address voice specific issues. Indeed, by re-examining the current infrastructure for voice security issues, existing data security is augmented. In any case, a multi-faceted security strategy will help ensure the availability of services, the successful introduction of new services, and the savings benefits of a fully converged infrastructure.

# 11. REFERENCES

## 11.1 UNPUBLISHED ARTICLES

Denning, Dorothy. “**Thinking About Cyberweapons Controls.**” (February 1, 2000, Draft of an Unpublished Paper Presented to the Defense Science Board).

## 11.2 PUBLIC DOCUMENTS

[1] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, “Security Considerations for Voice Over IP Systems”(Recommendations of the National Institute of Standards and Technology)

[2] White Paper on “**Voice over WLAN**” at <http://www.extricom.com/>

[3] Including VoIP over WLAN in a Seamless Next-Generation Wireless Environment White Paper, by Paul Struhsaker. Texas Instruments, 2003

[4] “**Wireless security models, threats and solutions**” by Randall K nichols and Panos C Lekkas. McGraw Hill publication.

[5] Aruba networks white paper “**Wireless grids for voice**” <http://www.arubanetworks.com>

[6] Aruba networks technical brief “ **Beyond the Hype: Voice over Wireless LAN**”

[7] <http://www.networkworld.com/reviews/2005/011005rev.html?page=1>

[8][http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking\\_solutions\\_white\\_paper0900aecd80368807.shtml](http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_white_paper0900aecd80368807.shtml)

[9] <http://www.wi-fiplanet.com/tutorials/article.php/2171721>

[10]Stewart S. Miller - “Wi-fi Security”

[11] “**Wi-Foo**” By Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky, ( Publisher : Addison Wesley, pub date June 28, 2004, ISBN : 0321-20171

[12] 31. Cisco Networkers 2000, <http://www.cisco.com/networkers/nw00/pres/2403.pdf>

[13] Innovators:

<http://www.fortune.com/fortune/fsb/specials/innovators/cook.html>.

[14] F. Robles. “**The VOIP Dilemma**”, SANS Institute, <http://www.sans.org/rr/whitepapers/voip/1452.php>