Global Information Assurance Certification Paper

802.11x Vulnerabilities, Attacks and Solutions
David C. Weiler
Version 1.3

ABSTRACT

802.11x is a wireless standard introduced 12 years ago that promised to revolutionize the LAN as we know it. Yet, with this charge to create a mobile workforce, several limiting factors have arisen stunting the growth of the WLAN. The total number of remote and mobile workers is currently 78 million with that number expecting to grow to 106 million by 2006. Over 1.5 Billion dollars of WLAN devices have been deployed.

Speed and security continue to be the most prominent concerns to the 802.11x standard. Throughout this paper I will look at the history of 802.11x, some configurations for 802.11x, and how the standard itself attains a higher level of maturity. Regarding the standards security issues, I will describe its current level of security, concerns with this current security level and finally some security recommendations.

CONCLUSION

From the research it would appear that 802.11x will be a technology player for years to come. The ability to be mobile at the workplace or at home has become more than a luxury, it has become necessity. Based on my research I then conclude:

1. WLAN security can only be addressed through a combination of security techniques.
2. 802.11x needs to continue improving the standard in order to deal with its ongoing security issues.
3. The WEP protocol should undergo drastic changes or should be abandoned altogether.
4. Hardware manufacturers need to ship devices pre-hardened and provide more educational information about the security issues with their product.

HISTORY OF 802.11

In today's fast-paced world, Ethernet continues its dominance on the LAN. Defined by the Institute of Electrical and Electronic Engineers (IEEE) with the 802.3 standard, Ethernet has provided an evolving, cooperative, scalable and interoperable networking standard. With line speeds ranging from 10mbps to 1000mbps, Ethernet has attempted with fairly good success to keep pace with the public demand for higher bandwidth.

Twelve years ago the IEEE established the 802.11 Working Group to create a wireless local area network (WLAN) standard. The standard specified an operating frequency in the 2.4GHz band, which lay the groundwork for this technology. In 1997 the group approved IEEE 802.11 as the first WLAN standard. Data rates for 802.11 at that time were a mere 1 and 2 Mbps. Due to the disparity between the 1 to 2 mbps WLAN and the current wired LAN with speeds of 10-100mbps, the committee quickly agreed that more work needed to be done in this area, that is, a technology that was more scalable and faster. The group began work on another 802.11 extension that would satisfy these future needs. In 1999, the group approved two new extensions to 802.11 which were designed to work with the existing 802.11 MAC layer, one being the IEEE 802.11a - 5GHz, and the other IEEE 802.11b - 2.4GHz.

802.11 CONFIGURATIONS

> There are two different ways to configure a network: ad-hoc and infrastructure. In the ad-hoc network, computers are brought together to form a network "on the fly." There is no structure to the network; there are no fixed points; and usually every node is able to communicate with every other node. A good example of this is when employees bring laptop computers together to communicate and share design or financial information. Although it seems that order would be difficult to maintain in this type of network, algorithms such as the spokesman election algorithm (SEA) [4] have been designed to "elect" one machine as the base station (master) of the network with the others being slaves. Another algorithm in ad-hoc network architectures uses a broadcast and flooding method to all other nodes to establish who's who.
>
> The second type of network structure used in wireless LANs is the infrastructure. This architecture uses fixed network access points with which mobile nodes can communicate. These network access points are sometime connected to landlines to widen the LAN's capability by bridging wireless nodes to other wired nodes. If service areas overlap, handoffs can occur. This structure is very similar to the present day cellular networks around the world. (Lough, Blankenship, Krizman page 3)

Today, 802.11b is mainstream and certainly is the most common wireless protocol for both business and home use. 802.11b theoretically can move up to 11mbps of data over

the 2.4 GHz range. The standard uses DSSS, (Direct Sequence Spread Spectrum Signaling) "where data at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference" (webopedia.com) instead of FHSS (Frequency Hopping Spread Spectrum) technologies, where "the data signal is modulated with a narrowband carrier signal that "hops" in a random but predictable sequence from frequency to frequency as a function of time over a wide band of frequencies" (webopedia.com). Interestingly enough, FHSS was the spectrum first approved for 802.11, but with the advent 802.11b was replaced by DSSS because of its capacity for greater throughput.

802.11 uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) rather than the ever-popular Carrier Sense Multiple Access with Collision Detection (CSMA/CD) used in Wired Ethernet LANs. CSMA/CA basically utilizes a four-way handshake to authenticate. For example, node 1 decides it would like to communicate, so it sends out a Request to Send or RTS packet to node 2. If node 2 receives the packet from node 1 and believes it is ready to receive more packets, node 2 replies to node 1 with a Clear to Send (CTS) packet. Node 1, after receiving the Clear to Send packet from node 2 then starts to transmit its data to node 2. At last, node 2 then sends an Acknowledgement (ACK) packet back to node 1 for each packet it receives from node 2. CSMA/CA is a good method of avoiding collisions on a network. However, CSMA/CA has additional overheads that CSMA/CD does not. CSMA/CA actually increases network traffic because it has to broadcast before any real data is put onto the cable. CSMA/CA prevents multiple nodes from seizing the medium immediately after completion of the preceding transmission. Technically 802.11 cannot even detect a collision while a transmission is in progress because 802.11 devices are half duplex (refers to the transmission of data in just one direction at a time. i.e. a walkie-talkie is a half-duplex device because only one end can send or receive data/voice at a time. Whereas, a telephone is a full-duplex device because both ends can send and receive data/voice simultaneously) and cannot receive while transmitting. (Lough, Blankenship, Krizman page 6)

> The major motivation and benefit from wireless LANs is increased mobility. Untethered from conventional network connections, network users can move about almost without restriction and access LANs from nearly anywhere. Examples of the practical uses for wireless network access are limited only by the imagination of the application designer. Medical professionals can obtain not only patient records, but also real-time vital signs and other reference data at the patient bedside without relying on reams of paper charts and physical paper handling. Factory floor workers can access part and process specifications without impractical or impossible wired network connections. A wireless connection with real-time sensing allows a remote engineer to diagnose and maintain the health and welfare of manufacturing equipment, even on an environmentally hostile factory floor. Warehouse inventories can be carried out and verified quickly and effectively with wireless scanners connected to the main inventory database. Even

> wireless "smart" price tags, complete with liquid crystal display (LCD) readouts, allow merchants to virtually eliminate discrepancies between stock-point pricing and scanned prices at the checkout lane. The list of possibilities is almost endless. (Lough, Blankenship, Krizman page 2)

802.11 PRESENT LEVELS OF SECURITY

Let me start by saying that all networks are vulnerable, whether they are wired or wireless. Each network has its own security issues that need to be dealt with in an effective manner. The following examples illustrate both wired and wireless networks share many of the same risks.

1. Physical threats to the network itself, which include external threats and sabotage.
2. Unauthorized access and eavesdropping.
3. The attack from the inner sanctums of ones network, the authenticated user attack, otherwise known as the ex-employee hit or the disgruntled employee attack.

This is not to say that the wireless world's woes stop with these elementary security examples. That is not the case. 802.11 has more than its share of out-of-the-box issues that need to be addressed in addition to those already mentioned.

Extended Service Set ID (ESSID) is an alphanumeric code that is entered into all access points and wireless clients on that same network. (Schenk, Garcia, Iwanchuk page 11) ESSID is used as an entry-level security solution whereby it matches the wireless client's number with the access point number, thus granting access to the WLAN. Without a match the client does not obtain access to the network.

Access Lists are configured as another layer of security that enables the network administrator to manually select which MAC addresses he or she would like to have access to the WLAN. If a client's MAC is not present in the access points Access List, that client will not have access to the WLAN.

> 802.11 supports two methods for authentication. They are WEP (Wired Equivalent privacy) or Shared Key and Open Systems. In an Open System, any requesting device may be granted authentication. However, success is not guaranteed. The device receiving the request may still deny authentication. In a Shared Key system, devices that possess a secret key can only be authenticated. Obviously, transmission of the Shared Key could lead to its interception of unauthorized users. It is therefore encrypted. (Zyren and Petrick page 6)

The Open Systems authentication is usually implemented on a network where security is not or will not be a concern. Open Systems allows any device to authenticate to any access point in clear text, therefore this type authentication is implemented when the priority is that the WLAN be up and running in a short amount of time.

Shared Key Authentication approach provides a better degree of authentication than the Open Systems approach. The 802.11 standard does not specify how to distribute keys, however, the process is as follows:

1. A requesting station sends an Authentication frame to access point.
2. When the access point receives an initial Authentication frame, the access point will reply with an Authentication frame containing 128 bytes of random challenge text generated by the Wired Equivalent Privacy (WEP) engine in standard form.
3. The requesting station will then copy the challenge text into an Authentication frame, encrypt it with a shared key, and then send the frame to the responding station.
4. The receiving access point will decrypt the value of the challenge text using the same-shared key and compare it to the challenge text sent earlier. If a match occurs, the responding station will reply with an authentication indicating a successful authentication. If not, the responding access point will send a negative authentication. (Weatherspoon page 3)

The WEP Protocol was chosen to meet the following criteria:

1. Reasonably Strong – the protocol must be able to meet the needs of the end user and the network administrator.
2. Self-synchronizing – devices often physically leave and return to coverage areas.
3. Computationally efficient - the WEP algorithm can be used as a software or hardware solution.
4. Exportable – it can be exported outside of the United States and imported to other countries. This is not the case for some higher level of encryption.
5. Optional – It is an option not required in an 802.11 compliant system. (Weatherspoon page 2)

   Within WEP encryption two distinct processes are applied to the plaintext data. One encrypts the plaintext and the other protects it against authorized data modification. The secret key (40 bits) is concatenated with an initialization vector ("IV, 24-bits) resulting in a 64-bit total key size. The resulting key is input into the Pseudo-random Number Generator (PRNG). The PRNG (RC4) outputs a pseudorandom key sequence based on the input key. The resulting sequence is used to encrypt the data by doing a bitwise XOR. The result is encrypted bytes equal in length to the number of data bytes that are to be transmitted in the expanded data plus 4 bytes. This is because the key sequence is used to protect the Integrity Check Value (ICV, 32-bits) as well as the data. (Weatherspoon page 2)

To protect against unauthorized data modification, an integrity algorithm (CRC-32) operates on the plaintext to produce the ICV. The ciphertext is accomplished by the following sequence of events:

1. Compute the ICV using CRC-32 over the message plaintext
2. Concatenate the ICV to the plaintext

3. Choose a random initialization vector (IV) and concatenate this to the secret key
4. Input the secret key+IV into the RC4 algorithm to produce a pseudorandom key sequence
5. Encrypt the plaintext+ICV by doing a bitwise XOR with the pseudorandom key sequence under RC4 to produce the ciphertext
6. Communicate the IV to the peer by placing it in front of the ciphertext

The IV, plaintext, and ICV triplet forms the actual data sent in the data frame.
In decryption, the IV of the incoming message is used to generate the key sequence necessary to decrypt the incoming message. Combining the ciphertext with the proper key sequence yields the original plaintext and ICV. The decryption is verified by performing the integrity check algorithm on the recovered plaintext and comparing the output ICV' to the ICV transmitted with the message. If ICV' is not equal to ICV, the received message is in error, and an error indication is sent to the MAC management and back to the sending station. (Weatherspoon page 2)

802.11 SECURITY CONCERNS

Anytime one plans to launch an 802.11 network the foremost issue should be, how am I going to secure my WLAN? The following are various examples of some of the more pronounced security issues with 802.11.

1. Extended Service Set ID (ESSID) –Many access points will broadcast the network name, allowing some client software to provide remote wireless clients with a list of all available wireless networks. Also many vendors have assigned a default ESSID number to their wireless products, so if a person knew a WLAN was using Cisco products the first ESSID they would try would be Cisco's out-of-the-box ESSID setting which is 101. Broadcasting the ESSID can be disabled. (Schenk, Garcia and Iwanchuk page 11)
2. MAC Spoofing – MAC addresses can be spoofed through a simple process of sniffing wireless traffic. After sniffing the clear text wireless packets, one can easily extrapolate one of the MAC addresses listed as "approved" from the access points Access List. A NIC can then be configured to utilize the sniffed MAC, thus the client will have access to the WLAN.
3. WEP – uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plain text to produce ciphertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext. This mode of operation makes stream ciphers vulnerable to several attacks. If an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts two ciphertext encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical as more ciphertexts that use the same key stream are

known. Once one of the plaintexts becomes known, it is trivial to recover all of the others. (Borisov, Goldberg and Wagner page 1)

4. Hidden WEP Key – With the knowledge of a few of the elements that compose the cipher text of an encrypted transmission, the attack can calculate the hidden WEP key. The Initialization Vector is known, as it is transmitted unencrypted, and the first byte of the plaintext can also be guessed. An 802.2 header is appended to each IP and ARP packet by the protocol before encryption and is identical for every packet. Armed with knowledge of the unencrypted IV and how the first bytes will decrypt, it becomes fairly simple to determine the hidden WEP key. Unlike the previous attacks described, this attack is completely passive and therefore impossible to detect. (Schenk, Garcia, Iwanchuk page 14)

ATTACKS

1. Session Hijacking – By monitoring transmissions between a wireless client and an access point, an attack can be launched by the attacker sending a fake packet to the wireless client. This packet, which as far as the authenticated client believes is coming from the access point, tells the wireless client that the session to the access point is now closed. At that moment the attacker then begins to use the session that the client machine believes was severed. As far as the client is concerned, it does not experience lack of connectivity it simply sends an authorization request immediately after the sever, then continues with it's new session. The attack is further clarified with the following:
    a. The client authenticates itself to the access point.
    b. The attacker sends an 802.11 MAC disassociate management frame using the MAC of the access point. This forces the clients connection to be disassociated. This procedure allows the attacker to actually swap sessions with the authenticated client, unbeknownst to the access point.
    c. The attacker, using the MAC of the original client, is able to access network resources, because the access point is still in the authenticated state. (Mishra and Arbaugh page 8)

2. Man-in-the-Middle – In this attack the man-in-the-middle (attacker) pretends to be a legitimate access point. During this launch, the attacker has the benefit of viewing all the traffic that passes between the wireless client and legitimate access point. "The primary flaw in the design is the asymmetrical treatment of supplicants and access points in the state machines. According to the standard, the authenticator port is in the *Controlled* state only when the session is authenticated. This is untrue for the supplicant, whose port is essentially always in the authenticated state. The one-way authentication of the supplicant to the access point can expose the supplicant to potential Man-In-Middle attacks with an adversary acting as an access point to the supplicant and as a client to the network access point." (Mishra and Arbaugh page 7)

3. Passive Attack to Decrypt Traffic - a passive eavesdropper can intercept all wireless traffic, until an IV collision occurs. By XORing two packets that use the

same IV, the attacker obtains the XOR of the two-plaintext messages. The resulting XOR can be used to infer data about the contents of the two messages. IP traffic is often very predictable and includes a lot of redundancy. This redundancy can be used to eliminate many possibilities for the contents of messages. Further educated guesses about the contents of one or both of the messages can be used to statistically reduce the space of possible messages, and in some cases it is possible to determine the exact contents. When such statistical analysis is inconclusive based on only two messages, the attacker can look for more collisions of the same IV. With only a small factor in the amount of time necessary, it is possible to recover a modest number of messages encrypted with the same key stream, and the success rate of statistical analysis grows quickly. Once it is possible to recover the entire plaintext for one of the messages, the plaintext for all other messages with the same IV follows directly, since all the pairwise XORs are known. (Borisov, Goldberg, Wagner page 2)

4. Active Attack to Inject Traffic- Suppose an attacker knows the exact plaintext for one encrypted message. He can use this knowledge to construct correct encrypted packets. The procedure involves constructing a new message, calculating the CRC-32, and performing bit flips on the original encrypted message to change the plaintext to the new message. The basic property is that RC4(X) xor X xor Y = RC4(Y). This packet can now be sent to the access point or mobile station, and it will be accepted as a valid packet. (Borisov, Goldberg, Wagner page 3)

5. Active Attack from Both Ends - The previous attack can be extended further to decrypt arbitrary traffic. In this case, the attacker makes a guess about not the contents, but rather the headers of a packet. This information is usually quite easy to obtain or guess; in particular, all that is necessary to guess is the destination IP address. Armed with this knowledge, the attacker can flip appropriate bits to transform the destination IP address to send the packet to a machine he controls, somewhere in the Internet, and transmit it using a rogue mobile station. Most wireless installations have Internet connectivity; the packet will be successfully decrypted by the access point and forwarded *unencrypted* through appropriate gateways and routers to the attacker's machine, revealing the plaintext. If a guess can be made about the TCP headers of the packet, it may even be possible to change the destination port on the packet to be port 80, which will allow it to be forwarded through most firewalls. (Borisov, Goldberg, Wagner page 3)

6. Table-based Attack - The small space of possible initialization vectors allows an attacker to build a decryption table. Once he learns the plaintext for some packet, he can compute the RC4 key stream generated by the IV used. This key stream can be used to decrypt all other packets that use the same IV. Over time the attacker can build up a table of IVs and corresponding key streams. Once the table is built, the attacker can decrypt every packet that is sent over the wireless link. (Borisov, Goldberg, Wagner page 3)

SECURITY SOLUTIONS

Throughout this paper I have discussed the true vulnerabilities of the 802.11 standard, including the security issues with WEP, authentication and ESSID. The IEEE organization is well aware of most of the vulnerabilities and has begun the process of dealing with these security concerns.

ROBUST SECURITY NETWORK (RSN)

IEEE is currently improving what they call their Robust Security Network (RSN). RSN makes use of current 802.11 standards as a basis for the much-needed improvements in authentication, key management and access control. With regard to access control, the RSN believes that their 802.1X standard for Port Based Network Access Control is going to be useful. This will be accomplished by abstracting three entities, the supplicant (wireless client), the authenticator (access point) and an authentication server i.e. Remote Authentication Dial-In User Service (RADIUS.) The wireless client then authenticates via the access point to a central server that in turn informs the access point that it is okay for the wireless client to access network resources. To improve its authentication methods RSN uses Extensive Authentication Protocol (EAP). EAP is a challenge response protocol, which means any authentication method can be encapsulated within the challenge response messages. Another plus for EAP is the fact that it is a layer three protocol and therefore routable. Communication between the authentication server and the wireless client is done over the RADIUS protocol and the EAP message is actually an attribute in RADIUS. (Mishra and Arbaugh page 3)

As RSN continues to evolve there are three changes that need to be made to the standard. The first is ensuring per-packet authenticity and integrity. Lack of per-packet authenticity and integrity in IEEE 802.11 frames has been a key contributor in many of the protocols problems. Authenticity and integrity of data frames must also be assured to prevent simple packet forgery attacks. The second change is authenticity and integrity of Extensive Authentication Protocol Over LAN (EAPOL) messages. EAPOL protocol carrier the EAP packets between the access point and the wireless client. EAP-Authenticator needs to be added to the decision message. The key for this attribute can come from the higher-layer authentication protocol. Another approach could be to eliminate an explicit EAP message and use the EAPOL-key as an indication of success at the EAP layer. And last, developing a peer-to-peer based authentication model. Two essential properties of the peer-to-peer model are symmetric authentication and Scalable authentication. In symmetric authentication it is assumed that all entities are untrusted entities and in the scalable authentication concept RADIUS servers need to be able to manage the access point more efficiently and in a scalable manner. (Mishra and Arbaugh page 9)

WEP2

Some of the improvements WEP2 has made available are its increased size of IV space to 128 bits. Keys may be changed periodically via IEEE 802.1X re-authentication to avoid

staleness; no authentication for reassociate/disassociate, no IV replay protection and the use of Kerberos for authentication within IEEE 802.1X is now present. WEP2 is not significantly more secure than WEP itself. Overall WEP2 should not be considered as a security solution. (Schenk, Garcia and Iwanchuk page 16)

AES

> Advanced Encryption Standard is a block cipher. With chunks of data encrypted at once, data is diffused within the block after encryption, rather than being allocated in a linear fashion, as in RC4, it becomes much more difficult to predict the location of specific data within the encrypted stream. This type of cipher should therefore be able to avoid the Integrity Check vulnerabilities. (Schenk, Garcia and Iwanchuk page 16)

Fast Packet Keying

Fast Packet Keying was introduced at the end of 2001 as a technology that will improve WLAN security. Fast Packet Keying allows one to encrypt each packet with a different key. The Fast Packet Keying software saves time by precalculating some of the data needed to generate the keys. The technology has been IEEE approved and is slowly making its way to the manufacturers. (Armstrong page 36)

Virtual Private Network (VPN)

"Client-based IPSec VPN's allow for over-the-air and over-the-wire IPSec encryption of all IP traffic, regardless of the wireless security used. In fact if an IPSec is used, other security measures, such as WEP, should be disabled as they only interfere with the connection of the user's device and require foreknowledge of the security restrictions and keys." (Armstrong page 34) By separating the wireless network from the wired one, and allowing VPN traffic to pass, you are increasing your networks security. In addition to IPSec many are choosing to secure their endpoints with EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security). EAP-TTLS requires no client-side digital certificates. "To date, most wireless LAN security products have been based on EAP-TLS, which uses Transport Layer Security, a successor to SSL (Secure Sockets Layer), and requires customers to set up a certificate authority." (Fisher page 1)

List of References:

1. Schenk, Rob; Garcia,Andrew; Iwanchuk, Russ. "Wireless LAN Deployment and Security Basics" August 29, 2001
http://www.extremetech.com/article/0,3396,s%253D1034%2526a%253D13521,00.asp

2. Zyren, Jim and Petrick, Al. "Brief Tutorial on IEEE 802.11 Wireless LANS" February 1999 http://www.intersil.com/data/an/an9/an9829/an9829.pdf

3. Weatherspoon, Sultan. "Overview of IEEE 802.11 Security." 2nd Quarter 2000
http://developer.intel.com/technology/itj/q22000/pdf/art_5.pdf

4. Borisov, Goldberg and Wagner, David. "Security of WEP Algorithm" 2001
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

5. Armstrong, Illena. "Today's Telecommuting World: Securing WLANS and LANS End-to-End" SC InfoSecurity News Magazine. February 2002. Pages 30-36
http://www.scmagazine.com/scmagazine/2002_02/cover/cover.html

6. Fisher, Dennis. "WLAN Security: Help on the Way" eWEEK Magazine. February 4, 2002 http://www.eweek.com/print_article/0,3668,a=22272,00.asp

7. Mishra, Arunesh and Arbaugh, William A. "An Initial Security Analysis of the IEEE 802.1X Standard" February 6, 2002. http://www.cs.umd.edu/~waa/1x.pdf

8. Ellingson, Jorgen. "Layers One & Two of 802.11 WLAN Security" August 3, 2001
http://rr.sans.org/wireless/WLAN_sec.php

9. Gohring, Nancy. "Hot Spots" eWEEK Magazine. March 11, 2002. Pages 45-46
http://www.eweek.com/print_article/0,3668,a=23730,00.asp

10. Taschek, John. "How Much Wireless Security is Enough." EWEEK Magazine March 25, 2002. Page 62
http://www.eweek.com/print_article/0,3668,a=24538,00.asp

11. Shiver, Jube Jr. "Wireless technology raises security, privacy questions" Los Angeles Times. February 18, 2002.
http://www.nandotimes.com/technology/v-text/story/257467p-2409132c.html?printer

12. Leydon, John. "RSA Supplies Answer to Drive-By Hacking?" December 18, 2001
http://www.theregister.co.uk/content/archive/23447.html

13. Reuters. "RSA Announces Fix for Wireless Security Hole" USA Today. December 17, 2001. http://www.usatoday.com/life/cyber/wireless//2001/12/17/wireless-fix.htm

14. Goodwins, Rupert. "Wireless Security Flaws Exposed" ZDNet. February 19, 2002 http://zdnet.com.com/2102-1105-839948.html

15. Lough, Daniel L; Blankenship, T. Keith; Krizman, Kevin J. "A Short Tutorial on Wireless LANs and IEEE 802.11" http://www.computer.org/students/looking/summer97/ieee802.htm

16. Webopedia – online dictionary and search engine you need for computer and Internet technology. http://www.webopedia.com