Lab 2 - Wireless Networking Fundamentals

CNIT 34600-001

Group 1

Ethan Hammond

Tommy Odle

Submitted to: Justin Anderson

Date Submitted: 10/20/2023

Date Due: 10/21/2023

Table of Contents

PROCEDURES

The following procedures outline the steps taken to complete this project. For reference, *Italicized* words represent options, **bold** words represent buttons, and words in `Courier New` represent inputs that are typed.

Cisco 3502 Flash Reset

To factory reset the 3502 access point (AP), the following procedure was done. This is important for achieving all future configurations in future procedures.

1. Plugged serial cable from serial port on 3502 to laptop
2. Opened PuTTy window on laptop
3. Entered “COM7” into hostname
4. Clicked **Connect**
5. Held onto Mode button
6. Plugged in ethernet cable from 3750 to 3502
7. Released mode button when prompted.
8. Entered dir flash to enter the flash directory.
9. Used delete flash:private-multiple-fs to wipe the config.
10. Typed reset to restart the AP

Cisco 3750G1 Switch Configuration

The following procedure begins on the terminal of the Cisco 3750 switch and goes through the network configurations needed. These configurations provided internet connectivity to the access point.

1. Used `en|conf t` to enter configuration mode

2. Entered `hostname 3750G1`
3. Typed `int Vlan3001` to enter VLAN 3001 interface
4. Entered ip address `44.32.1.5 255.255.255.0|exit`
5. Typed `vlan 3001` to enter vlan 3001
6. Used `name vlan 3001` to give it a name
7. Typed `exit|int g3/0/48` to enter uplink interface
8. Entered `switchport mode access|switchport access vlan 3001|exit`
9. Used `ip default-gateway 44.32.1.1` to give the switch a default route
10. Entered `end|wr` to save the configuration

Cisco 3502 AP SSIDs Configuration

Because each radio interface needs an SSID to function, the following steps were taken to create an SSID for the 2.4 GHz and 5.0 GHz stations. This gave each station a logical identifier for clients to connect to.

1. Used `en|conf t` to enter config mode
2. Entered `ip domain name CNIT346Group1` to set a domain name
3. Typed `dot11 ssid CNIT346Group1a` to set an SSID for 5GHz
4. Used `authentication open` to set no password
5. Entered `guest-mode` to set the SSID to broadcast
6. Used `dot11 ssid CNIT346Group1g` to set an SSID for 2.4GHz
7. Used `authentication open` to set no password

8. Entered `guest-mode` to set the SSID to broadcast

Cisco 3502 AP Radio Configuration

The following steps were taken to configure each radio interface on the 3502 AP. This gave clients the ability to connect to the network.

1. Used `en|conf t` to enter config mode.
2. Used `interface dot11radio0` to enter the 2.4GHz radio.
3. Entered `ip address 44.32.1.4 255.255.255.0` to set an IP.
4. Used `ssid CNIT346Group1g` to set the SSID.
5. Entered the 5G interface with `interface Dot11Radio1`
6. Used `ip address 44.32.1.5 255.255.255.0` to set an IP.
7. Typed `ssid CNIT346Group1a` to set the SSID.

Antenna Propagation Captures

The following procedure begins on the desktop of the Macbook Pro and illustrates how different antennas were compared to observe different propagation patterns. These results can be seen in Appendix A.

1. Opened NetSpot on Macbook Pro
2. Clicked **Create New…**
3. Selected *From file*
4. Clicked **Select**
5. Double-clicked *KNOY Floor 3 Map* on Desktop directory
6. Set proper scaling of floor space by entering proper measurements

7. Clicked **Next | Start scan**
8. Plugged antenna into AP
9. Moved to each marked spot on the floor plan and scanned each spot
10. Saved/recorded final heatmap and data rates (See Appendix A)
11. Switched out the antenna for each scan

Cisco 3502 AP WPA, WEP, and ACLs Configuration

To set up basic security protocols and techniques on the AP, the following procedure was performed. This provided authentication (using WPA and WEP) and basic firewall rules (ACLs) to the AP.

1. Used `en | conf t` to enter config mode.
2. Used `interface dot11radio0` to enter the 2.4GHz radio.
3. Entered `encryption key 2 size 128bit AAAAAAAAAAAAAAAAAAAAAAAAA transmit-key`
4. Used `encryption mode ciphers wep128` to set it to WEP.
5. Entered the 5GHz interface with `interface dot11radio1`.
6. Used `encryption mode ciphers aes-ccm tkip.`
7. Entered `dot11 ssid CNIT346Group1a` to enter the SSID.
8. Used `authentication key-management wpa version 2` to set it to use WPA2.
9. Typed `wpa-psk ascii 7 CNIT346Group1aPassword|exit` to set the password.
10. Entered `access-list 700 permit 6883.cb9e.3fbc 0000.0000.0000`

11. Entered `access-list 700 permit a0e7.0b68.c0d6 0000.0000.0000`
12. Entered `access-list 700 permit a4cf.9910.c5b4 0000.0000.0000|end`
13. Used `wr` to save the configuration

Roaming and Handoffs

These steps go through how roaming was observed using Wireshark. The packets that were observed were reassociation packets and proved that roaming and handoffs were being done (see Objective 6 for results).

1. Turned on two laptops in lab
2. Connected each to CNIT346RoamingTest
3. Opened Wireshark on one laptop
4. Moved laptop with Wireshark opened to AP in KONY 203
5. Moved laptop without Wireshark opened to AP in KNOY 236
6. Started capture on laptop with Wireshark opened
7. Moved laptop without Wireshark opened from KNOY 203 to KNOY 236
8. Stopped capture on Wireshark
9. Typed `wlan.fc.type_subtype=3` in filter bar
10. Recorded results (see Objective 6)

Objective 3: Antenna Propagation

Antennas were used to generate heat maps, coverage area, and data rates. The antennas that were used can be seen in Appendix A below with their data rates, throughputs, and signal strengths. The table also provides the proof of why the highly directional antenna provides the most effective coverage.

Table 1: Performance of Signal Propagations with Different Antennas

	Max Signal (dBm)	Max Data Rate (Mbps)	Max Though-put (Mbps)
2.4 GHz Rubber Ducky Horizontal	-49	27.87	37.69
2.4 GHz Rubber Ducky Vertical	-48	20.17	31.41
5.0 GHz Rubber Ducky Horizontal	-60	72.17	59.85
5.0 GHz Rubber Ducky Vertical	-60	70.03	53.51
5.0 GHz Omnidirectional Horizontal	-63	78.79	53.87
5.0 GHz Omnidirectional Vertical	-60	77.01	51.43
2.4 GHz Yagi	-49	23.20	34.82
5.0 GHz Highly Directional	-58	82.89	55.14
5.0 GHz Patch	-61	74.88	54.98

Objective 4: Mobility Performance

Performance and monitoring software was used to take baseline measurements of wireless signals from various areas around the third floor of KNOY. The readings were taken at 2.4 GHz and 5 GHz to represent antenna propagation. They were also taken using the regular vertical rubber ducky antennas. The following measurements are averages of the results of these readings:

2.4 GHz:
Signal Strength: -48.67 dBm
Data Rates: 23.75Mbps
Throughput: 34.64 Mbps

5GHz:
Signal Strength: -60.2 dBm
Data Rates: 75.96 Mbps
Throughput: 54.80 Mbps

Objective 5: Wireless Security

Part 1

Part 1 was accomplished by disabling the broadcasting of the SSID via the AP. SSID broadcasting is disabled by turning off guest mode in the dot11 ssid fields. A protocol analyzer like Wireshark is able to find the SSID of an access point even though it is not being broadcasted because APs still send out beacon frames and beacon requests that can be picked up by the analyzer. Management frames, if not encrypted, can still be sniffed out as well. These, along with MAC address association with requests, can be seen by all packet analyzers and the SSID be revealed.

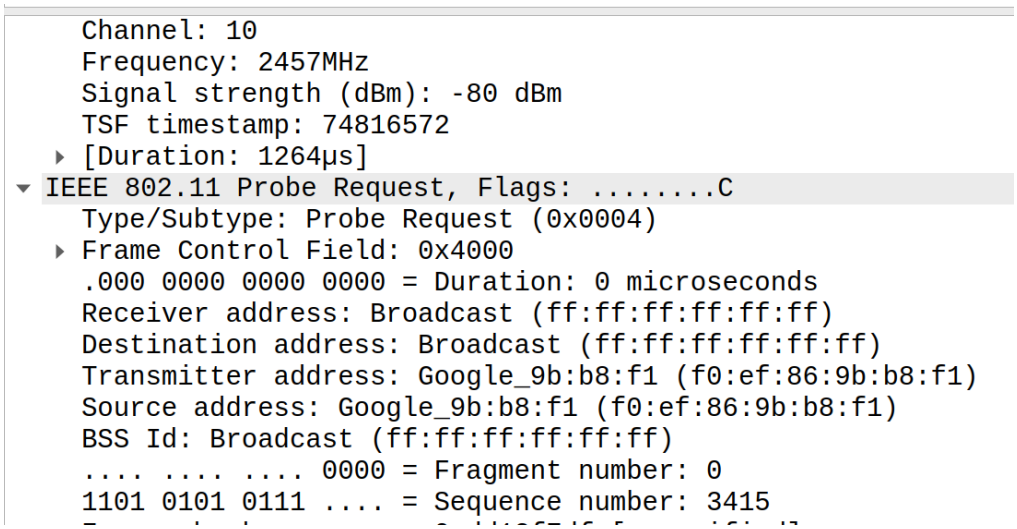

Figure 5: 802.11 Frame with Hidden SSID

The screenshot above shows a beacon frame from a hidden SSID. Although an SSID can be hidden and broadcasting can be disabled, it will still have to send out beacon frames to be picked up by clients for timing windows of connecting and transmitting data.

Part 2

Part 2 was accomplished by adding a MAC address filter to block a personal laptop from connecting to the AP. This was tested by kicking everybody off of the AP, adding a MAC address filter for 1 specific host, and having both try to reconnect. The client with the filtered MAC address was proven to be unable to connect. No matter the encryption, there is no ability to associate with the AP by layer 2, thus there are no steps of authentication that are passed.

Part 3

Part 3 was partially accomplished with issues that are outlined in the problem solving appendix below. With WEP being established, all authentication steps should be completed with

a correct WEP key. Also, unlike WPA2, with an incorrect WEP key there would be also no steps of authentication completed as WEP uses one shared key to authenticate.

Part 4

Part 4 was accomplished by adding WPA2-PSK to the 5 GHz radio on the AP. With a correct PSK, the client is able to pass all steps of authentication. However, with an incorrect PSK, the client will still be able to pass the first 2 steps of authentication as they will have to become associated with the AP first. Once they are associated, they can then complete the 4 way handshake to exchange the PSK and authenticate fully.

Analysis Questions:

- Are these individual steps sufficient to secure an enterprise network?
- To secure a home office/small office network? What if you combine these methods?
- What additional steps could be taken to further secure the enterprise wireless network?

These individual steps are not sufficient to secure an enterprise network. In a business environment, there needs to be further authentication and authorization because one PSK should not be shared throughout an entire company for the network. A home office, however, would not require further steps for authorization. These methods can be combined if a small office is on a separate network than the rest of the company. Steps that should be taken to improve this include adding a RADIUS box to authenticate off of. This could also be combined with LDAP to have users authenticate with their own Active Directory credentials. AD credentials can also be used to determine the level of authorization within a network that a client gets access to.

Objective 6: Roaming and Handoffs

Part 1

After connecting to our group's access point and starting a large file download, the client walked down the hall and into the stairwell before it was disconnected from the network. When this happened, the download was paused on the web browser with a network error message. This is because when the client disconnects from the network, it does not rejoin a different network or AP with the same BSSID in time for the download to continue. However, when the client walked back close enough to KNOY 376, the client rejoined the network and the download continued on from where it left off at. If you could re-enter the BSS quickly enough, before the client completed a reassociation request and received a reassociation response from another AP and BSSID, the download would never be truly interrupted because a reassociation would never occur. The process seemed to be faster to disconnect with the 5 GHz band. This was presumably because 5 GHz does not propagate as well through walls, with KNOY having many walls in the way of rooms, this was to be expected.

Part 2

The theoretical effect of roaming aggressiveness is the amount of signal strength increase that a different AP must have for a client to jump from the current AP onto the new one. The more aggressive this setting is set to, the lower the signal strength increase needs to be before the client will roam to a different better AP. It is fairly simple to tell if a client is obtaining a clean handoff because there will be reassociation requests from the client to the first AP, and a reassociation response from the new AP. If there is a disassociation, there will be no reassociation response from the second access point. The roaming handoffs from APs can be

seen in Figures 6a and 6b below. The frames show reassociation requesets from the client and reassociation responses from the access point.

It is possible to perform a seamless handoff between different brands of APs. However, it can be difficult because of different 802.11 roaming protocols or wireless standards and configuration inconsistencies between methods of configuration between brands. It is not impossible to fail a handoff when there are two different wireless standards due to compatibility issues. But, as roaming is initiated by the client, it can most of the time be done seamlessly. Different clients make a difference on roaming performance because of roaming aggressiveness settings, wireless standards, wireless compatibilities, and other client to AP wireless connection considerations.

Part 3

When roaming from an AP in KNOY 204 to KNOY 238 on the same channel, there was a reassociation request picked up but no reassociation response. As there is no reassociation response from the AP, there is no proof that can be given that the client roamed from AP to AP on the same channel. This is likely to happen because if the client and the AP are on the same channel, they are sharing and competing for the same frequency band space, and need to wait for each other and share the medium. This is specifically important within the 2.4 GHz band because it only has 3 non-overlapping channels. The rest of the channels are overlapping, meaning more interference in the medium when multiple devices are trying to communicate at the same time.

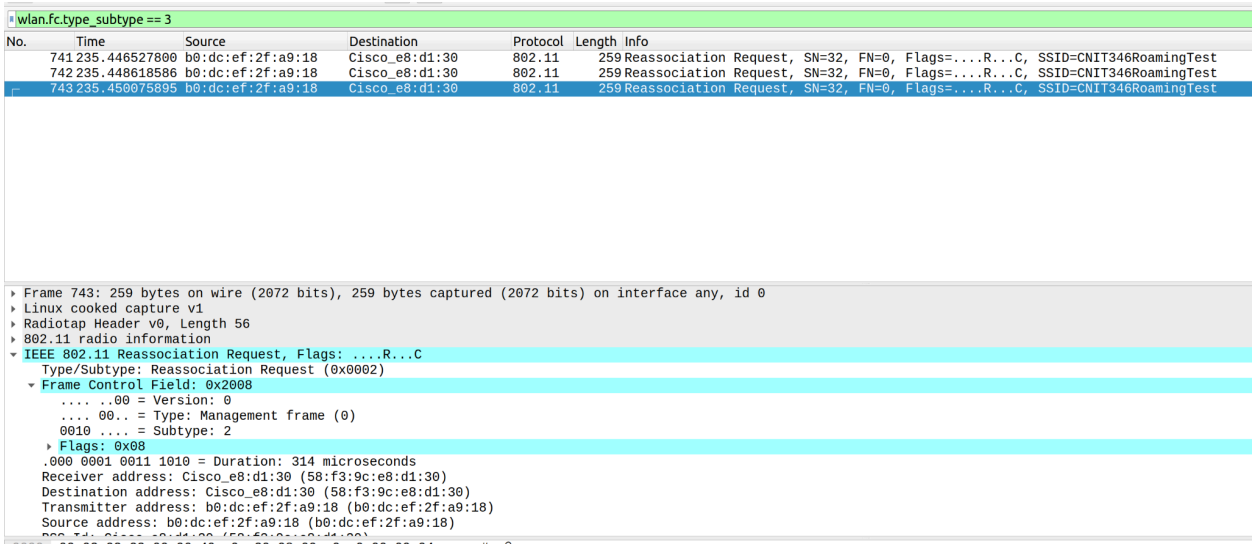

Figure 1a: Roaming reassociation request

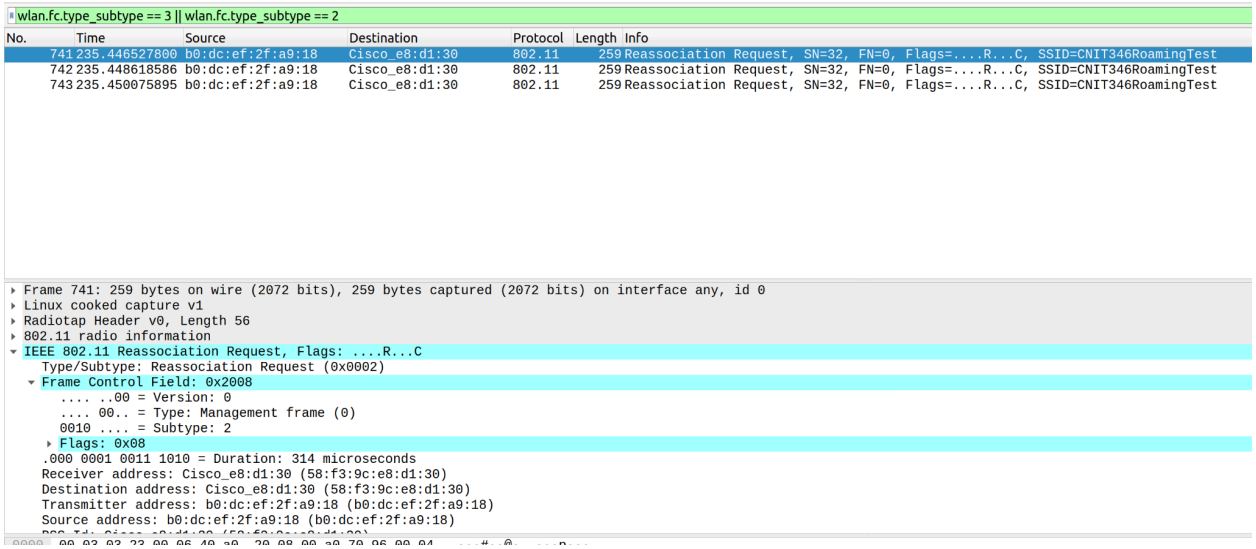

Figure 1b: Roaming reassociation request and responses

BIBLIOGRAPHY

(A. Smith, personal communication, October 10, 2023).

Cisco. (2018, February 2). *Configuration of WPA/WPA2 with pre-shared key: IOS 15.2JB and later*. Cisco. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/116599-config-wpa-psk-00.html

Cisco. (2019, March 28). *Disable SSID broadcast on a wireless access point*. Cisco. https://www.cisco.com/c/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/smb5177-disable-ssid-broadcast-on-a-wireless-access-point.html

Cisco. (2021, September 21). *Configure WEP on Aironet access points and Bridges*. Cisco. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/10953-confwep.html

Cisco. (2023, April 2). *Cisco IOS Configuration Guide for Autonomous Aironet Access Points Cisco IOS release 15.3(3)jab - configuring the access point for the first time [Cisco Aironet 1600 series]*. Cisco. https://www.cisco.com/c/en/us/td/docs/wireless/access_point/15-3-3/configuration/guide/cg15-3-3/cg15-3-3-chap4-first.html

Fall2023_lab2_writeup. (n.d.). https://purdue.brightspace.com/d2l/le/content/831279/viewContent/14176875/View

(J. Anderson, personal communication, October 10, 2023).

Seamless roaming between different APS brands?. Reddit. (n.d.). https://www.reddit.com/r/HomeNetworking/comments/o1qayj/seamless_roaming_between_different_aps_brands/

APPENDIX A: Heat Maps

Figure 2: Propagation with Horizontal Rubber Ducky Antenna on 2.4 GHz

Figure 3: Propagation with Vertical Rubber Ducky Antenna on 2.4 GHz

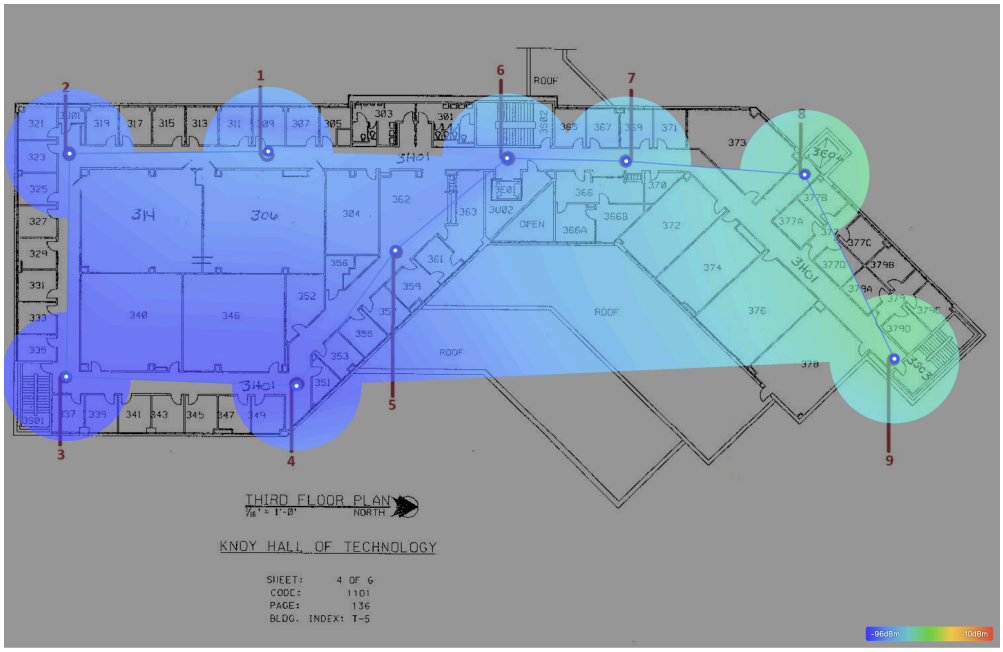

Figure 4: Propagation with Horizontal Rubber Ducky Antenna on 5.0 GHz

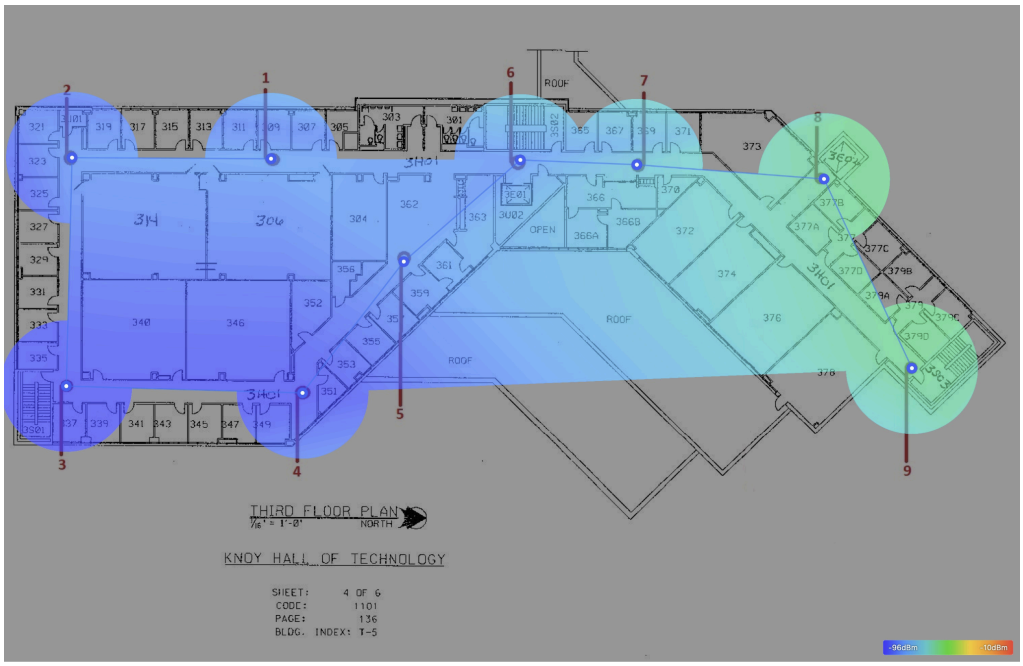

Figure 5: Propagation with Vertical Rubber Ducky Antenna on 5.0 GHz

Figure 6: Propagation with Horizontal Omnidirectional Antenna on 5.0 GHz

Figure 7: Propagation with Vertical Omnidirectional Antenna with 5.0 GHz

Figure 8: Propagation with Yagi Antenna on 2.4 GHz

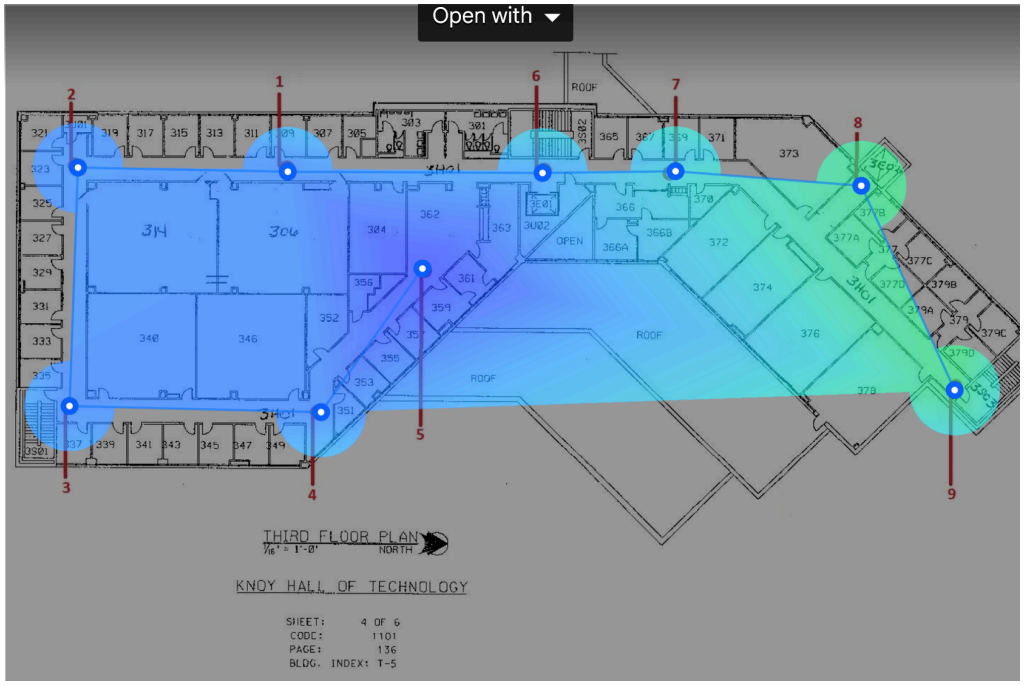

Figure 9: Propagation with Highly Directional Antenna on 5.0 GHz

Figure 10: Propagation with Patch Antenna on 5.0 GHz

APPENDIX B: Problem Solving

Problem 1

Problem Description: In order to establish a rudimentary form of encryption for Wireshark analysis, WEP was chosen. However, with WEP installed, clients could not authenticate into the network.

Problem Solutions: It was attempted to change key encryption and hash algorithms to match the client's key. It was also attempted to use older key algorithms to allow the client to connect to the AP.

Final Solution: The last solution that was attempted was to turn off TKIP and authenticate solely based on the string of the pre-shared WEP key. This unfortunately also did not solve the issue and WEP was not fully set up and working. WPA2 was working efficiently for encryption, but WEP was never fully configured due to this issue.

APPENDIX C: Networking Device Configs

AP Running Config:

```
Current configuration : 2352 bytes
!
! Last configuration change at 02:49:26 UTC Mon Mar 1 1993
version 15.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 3502
!
!
logging rate-limit console 9
!
no aaa new-model
no ip source-route
no ip cef
ip domain name CNIT346Group1
ip name-server 44.2.1.44
ip name-server 44.2.1.45
!
!
!
!
dot11 pause-time 100
dot11 association mac-list 700
dot11 syslog
!
dot11 ssid CNIT346Group1a
   authentication open
   authentication key-management wpa version 2
   guest-mode
   wpa-psk ascii 7 1531252530797F720F213A370356173300454A4F5C460A
!
dot11 ssid CNIT346Group1g
   authentication open
```

```
   guest-mode
!
!
!
no ipv6 cef
!
!
username Cisco password 7 00271A150754
!
!
bridge irb
!
!
!
interface Dot11Radio0
 ip address 44.32.1.4 255.255.255.0
 shutdown
 !
 encryption key 2 size 128bit 7 D41F07447BA1D4382450CB68F37A transmit-key
 encryption mode ciphers wep128
 !
 ssid CNIT346Group1g
 !
 antenna gain 0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface Dot11Radio1
 ip address 44.32.1.5 255.255.255.0
 !
 encryption mode ciphers aes-ccm tkip
 !
 ssid CNIT346Group1a
 !
 antenna gain 0
```

```
 peakdetect
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 spanning-disabled
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
!
interface GigabitEthernet0
 no ip address
 duplex auto
 speed auto
 bridge-group 1
 bridge-group 1 spanning-disabled
 no bridge-group 1 source-learning
!
interface BVI1
 mac-address 0007.7d80.7c3c
 ip address dhcp client-id GigabitEthernet0
 ipv6 address dhcp
 ipv6 address autoconfig
 ipv6 enable
!
ip forward-protocol nd
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip ssh pubkey-chain
  username user
!
!
access-list 700 permit 6883.cb9e.3fbc   0000.0000.0000
access-list 700 permit a0e7.0b68.c0d6   0000.0000.0000
access-list 700 permit a4cf.9910.c5b4   0000.0000.0000
bridge 1 route ip
!
!
```

```
!
line con 0
line vty 0 4
 login local
 transport input all
!
end
```

3750 switch config:

```
Building configuration...

Current configuration : 2746 bytes
!
! Last configuration change at 00:01:27 UTC Mon Jan 16 2006
!
version 15.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname 3750G1
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
switch 3 provision ws-c3750e-48pd
system mtu routing 1500
!
!
!
!
!
!
vtp mode transparent
!
!
```

```
!
!
!
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
!
vlan internal allocation policy ascending
!
vlan 3001
 name vlan 3001
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0
 no ip address
!
interface GigabitEthernet3/0/1
 switchport access vlan 3001
 switchport mode access
!
interface GigabitEthernet3/0/2
!
interface GigabitEthernet3/0/3
!
interface GigabitEthernet3/0/4
```

```
!
interface GigabitEthernet3/0/5
!
interface GigabitEthernet3/0/6
!
interface GigabitEthernet3/0/7
!
interface GigabitEthernet3/0/8
!
interface GigabitEthernet3/0/9
!
interface GigabitEthernet3/0/10
!
interface GigabitEthernet3/0/11
!
interface GigabitEthernet3/0/12
!
interface GigabitEthernet3/0/13
!
interface GigabitEthernet3/0/14
!
interface GigabitEthernet3/0/15
!
interface GigabitEthernet3/0/16
!
interface GigabitEthernet3/0/17
!
interface GigabitEthernet3/0/18
!
interface GigabitEthernet3/0/19
!
interface GigabitEthernet3/0/20
!
interface GigabitEthernet3/0/21
!
interface GigabitEthernet3/0/22
!
interface GigabitEthernet3/0/23
!
interface GigabitEthernet3/0/24
```

!
interface GigabitEthernet3/0/25
!
interface GigabitEthernet3/0/26
!
interface GigabitEthernet3/0/27
!
interface GigabitEthernet3/0/28
!
interface GigabitEthernet3/0/29
!
interface GigabitEthernet3/0/30
!
interface GigabitEthernet3/0/31
!
interface GigabitEthernet3/0/32
!
interface GigabitEthernet3/0/33
!
interface GigabitEthernet3/0/34
!
interface GigabitEthernet3/0/35
!
interface GigabitEthernet3/0/36
!
interface GigabitEthernet3/0/37
!
interface GigabitEthernet3/0/38
!
interface GigabitEthernet3/0/39
!
interface GigabitEthernet3/0/40
!
interface GigabitEthernet3/0/41
!
interface GigabitEthernet3/0/42
!
interface GigabitEthernet3/0/43
!
interface GigabitEthernet3/0/44

```
!
interface GigabitEthernet3/0/45
!
interface GigabitEthernet3/0/46
!
interface GigabitEthernet3/0/47
!
interface GigabitEthernet3/0/48
 switchport access vlan 3001
 switchport mode access
!
interface GigabitEthernet3/0/49
!
interface GigabitEthernet3/0/50
!
interface GigabitEthernet3/0/51
!
interface GigabitEthernet3/0/52
!
interface TenGigabitEthernet3/0/1
!
interface TenGigabitEthernet3/0/2
!
interface Vlan1
 no ip address
!
interface Vlan3001
 ip address 44.32.1.5 255.255.255.0
!
ip default-gateway 44.32.1.1
ip forward-protocol nd
!
ip http server
ip http secure-server
!
!
!
!
line con 0
line vty 5 15
```

```
!
!
end
```