***CNIT 45600: Wireless Security***

CNIT45600

Team Trash  
Ethan Hammond  
Tommy Odle  
Elliot Tuchscherer  
Submitted To: Justin Anderson  
Date Submitted: 02/09/24  
Date Due: 02/09/24

# 

# TABLE OF CONTENTS

[**TABLE OF CONTENTS 2**](#_rub24lr8wt5j)

[**EXECUTIVE SUMMARY 3**](#_duvv6dpzej6x)

[**BUSINESS CASE 4**](#_ttlx7fmth08y)

[**PROCEDURES 5**](#_rlftsb6cs2ls)

[Topology Setup 5](#_5fs4ncv7qfiz)

[Cisco 3750 Switch Factory Reset, Port Configuration, and DHCP Configuration 5](#_d2g62qlvjyys)

[ADCS and NPS Install 9](#_6n9psz8yxogb)

[WPA-PSK Cracking 10](#_93kmwzjc65ys)

[MAC Address Spoofing 11](#_9ft6ikurto3u)

[**RESULTS 12**](#_dh6umdpyymac)

[**CONCLUSIONS AND RECOMMENDATIONS 15**](#_7q1vo6jpvdfi)

[**BIBLIOGRAPHY 16**](#_l5f7xcbqj7io)

[**APPENDIX A: PROBLEM SOLVING 18**](#_g63dv5v27weq)

[Problem 1: MAC Filters Not Applying Properly 18](#_wql6eyax9r54)

[Problem 2: Flashing APs 18](#_ctjl4xe72ow0)

[Problem 3: RADIUS Not Working 19](#_672ruongt007)

[**APPENDIX B: KNOWLEDGE-BASED QUESTIONS 20**](#_kon1tg4t29fo)

[**APPENDIX C: Switch and AP Configs 23**](#_z5z3n9pu0hjw)

[Switch Config: 23](#_ljvy76v6z1pt)

[AP1 Config: 32](#_356ji2z89cp6)

[AP2 Config: 37](#_d23hh5bbmt0m)

# EXECUTIVE SUMMARY

A secure wireless network environment can be constructed for a company using many different protocols, topologies, and equipment. For this scenario, two Cisco Access Points (APs), a Cisco 3750 switch, and an ESXI 7.0 server were used in conjunction with the 802.11 security protocols WPA PSK and WPA 2 Enterprise. The Cisco 3750 switch was configured to supply network to the APs and ESXI server using L2 access protocols and did not serve any security or L3 functions. One AP was configured with WPA PSK personnel with a hidden SSID and the other with WPA 2 Enterprise. A Windows Server 2019 VM was deployed on the ESXI 7.0 server and Active Directory was activated. The RADIUS server was then configured (via AD) on this VM to supply the 802.1X/EAP authentication for users on the WPA 2 Enterprise network. The WPA 2 Enterprise AP was then pointed at the RADIUS server via the VM’s IP address. Steps were also taken to show vulnerabilities of WPA PSK such as MAC spoofing and packet sniffing using Wireshark. This lab report includes the business case, procedures, results, conclusions, recommendations, references, troubleshooting, and device configurations for this network.

# BUSINESS CASE

Small to medium enterprise environments may not require new and expensive equipment to build a fast and secure network. Older Cisco equipment, such as 3702 APs and a 3750 switch, can offer 802.11ac speeds (up to 1300Mbps) on 5Ghz along with WPA 2 802.1X/EAP authentication. A Windows Server could then run AD and RADIUS to provide enterprise-level security to clients. New users, groups, and computers could also be easily created and managed from the Windows Server, making administration fast and easy. Windows Server is relatively light to run (especially with only AD and RADIUS being used) and doesn’t require a big and powerful computer to run on. Furthermore, ACLs can also be configured on the APs to provide an extra layer of security, potentially blocking unwanted networks and hosts. A Cisco 3750 could act as a central device for the APs and Windows Server to connect to and reach the internet. This switch also offers POE capabilities, meaning the APs would not need to be plugged into a power socket to operate.

# 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. Pipes | are used to represent chained selections, clicks or commands.

## Topology Setup

To begin setting things up, all of the equipment was collected from KNOY 371, put in KNOY 374D, and hooked up to power and network. This was mainly done to ensure all equipment was powering on and working properly. The steps below show how this was done.

1. Grabbed two Cisco 3702 APs, Cisco 3750 switch, Dell Precision, and network/power cables from KNOY 371
2. Dropped off all equipment to KNOY 374D
3. Plugged Cisco 3750 into power
4. Plugged Dell Precision into power
5. Plugged uplink cable into port g1/0/1 on Cisco 3750
6. Plugged CAT5e/6 cable from port g1/0/48 to Dell Precision
7. Plugged one Cisco 3702 into port g1/0/13 on Cisco 3750
8. Plugged other Cisco 3702 into port g1/0/15 on Cisco 3750

## Cisco 3750 Switch Factory Reset, Port Configuration, and DHCP Configuration

The Cisco 3750’s function was to provide internet connectivity to all devices and to act as a DHCP server for the APs. The following steps show how this was configured.

1. Rebooted Cisco 3750
2. Held **MODE** button upon start up to boot into ROMMON mode
3. Opened Cisco 3750 terminal
4. Entered flash\_init | delete flash:vlan.dat | y | delete flash:config.txt | y | boot
5. Entered enable | conf t
6. Typed hostname CNIT456TeamTrashSW
7. Used int g1/0/1 to enter g1/0/1 port configuration
8. Entered switchport mode access | exit
9. Repeated steps 7-8 on g1/0/13, g1/0/15, and g1/0/48
10. Used ip dhcp pool POOL1 to create DHCP pool
11. Entered network 44.33.16.0 255.255.255.192 | default-router 44.33.16.1 | dns-server 44.2.1.44 44.2.1.45 | exit
12. Typed ip dhcp excluded-address 44.33.16.0 44.33.16.19 | ip dhcp excluded-address 44.33.16.41 44.33.16.63

**Factory Reset on Cisco 3702 APs**

In order to set up the access points, they need to be in autonomous mode instead of CAPWAP mode for controllers. This is done by physically holding the *mode* button and entering commands.

1. Unplugged AP from switch
2. Held reset button on AP
3. Plugged cable from AP to switch
4. Held reset button for 30 sec
5. Access AP terminal
6. Entered dir flash: | delete flash:private-multiple-fs | reset | y
7. Typed enable | conf t | enable secret <password> to set enable password
8. Typed hostname CNIT456TeamTrashAP1
9. Used int BVI 1 to enter bridge interface
10. Entered ip add 44.33.16.5 255.255.255.192 | exit
11. Used int dot11radio1 to enter 5.0 GHz interface
12. Typed no shut | end | wr
13. Repeated steps 1-12 on AP 2 with the following changes
    1. For step 8, entered “CNIT456TeamTrashAP2” instead of “CNIT456TeamTrashAP1”
    2. For step 10, entered “44.33.16.19” instead of “44.33.16.5”

**CNIT456TeamTrashAP1 Configuration**

The first access point was configured for WPA-PSK to provide a proof of concept for weaknesses in authentication methods.

1. Typed enable | conf t
2. Entered ip domain name CNIT456TeamTrashAP1.lcl
3. Used dot11 ssid CNIT456TeamTrashAP1 to create wireless SSID
4. Typed authentication open | authentication key-management wpa | guest-mode | wpa-psk ascii 7 <password> | exit
5. Used interface Dot11Radio1 to enter 5.0 GHz
6. Typed encryption mode ciphers aes-ccm tkip | ssid CNIT456TeamTrashAP1
7. Entered access-list 701 deny aabb.ccdd.eeff 0000.0000.0000
8. Entered access-list 701 permit 0000.0000.0000 ffff.ffff.ffff

**CNIT456TeamTrashAP2 Network Configuration**

The second access point was configured with strong authentication methods with a RADIUS server on WPA2. This was designed to be a strong network that was not to be broken.

1. Entered 44.33.16.19 into browser
2. Clicked **SECURITY** | **Encryption Manager | RADIO1-802.11AC5GHz** | **Cipher**
3. Selected *AES CCMP* from Cipher dropdown menu
4. Clicked **Apply-Radio1** | **SSID Manager**
5. Selected *New* | *Radio1-802.11AC5GHz* | *Open Authentication* | *Network EAP*
6. Selected *with EAP* under Open Authentication dropdown
7. Selected *Customize*
8. Selected *Radius* from EAP Authentication Servers Priority 1 dropdown
9. Selected Enable WPA
10. Selected *WPAv2* from Enable WPA Dropdown
11. Clicked **Apply** | **Server Manager**

**CNIT456TeamTrashAP2 RADIUS Configuration**

RADIUS was configured to authenticate users from Active Directory onto the SSID from the Windows Server.

1. Selected *New*
2. Entered Radius for Server Name
3. Entered 44.33.16.11 for Server
4. Entered <secret> for Shared Secret
5. Typed 1812 for Authentication Port
6. Typed 1813 for Accounting Port
7. Selected *Radius* under EAP Authentication Priority 1 dropdown
8. Clicked **Apply**
9. Opened CNIT456TeamTrashAP2 terminal
10. Entered en | conf t
11. Entered dot11 ssid CNIT456TeamTrashAP1
12. Entered guest mode | end | wr

## ADCS and NPS Install

For RADIUS authentication to work properly, the Windows Server needed to possess Active Directory Certificate Services and Network Policy Server capabilities.

1. Opened Server Manager on the Windows Server and clicked “Add Roles and Features”.
2. Selected *Network Policy Server* and clicked yes to all boxes in the wizard.
3. Restarted the server to install NPS.
4. Repeated step 1 and selected *Active Directory Certificate Services* and selected the machine to be a root CA.

**RADIUS Configuration on Windows Server 2019**

RADIUS was configured on Windows Server 2019 to authenticate users to a specific SSID via an AD security group through the server.

1. Opened Network Policy Server in Start menu
2. Selected *NPS (Local)*
3. Selected *RADIUS Server for 802.1X Wireless or Wired Connections*
4. Clicked **Configure 802.1X**
5. Selected *Secure Wireless Network*
6. Clicked **Next** | **Add…**
7. Entered AP2 for Friendly name
8. Entered 44.33.16.19 for Address (IP or DNS)
9. Entered <secret> for Shared secret and Confirm shared secret
10. Clicked **OK** | **Next**
11. Selected *Microsoft: Protected EAP (PEAP)* under Type
12. Clicked **Next** | **Add…**
13. Entered adm
14. Clicked **OK** | **Next** | **Next** | **Finish**

## WPA-PSK Cracking

To prove the practicality of WPA2, the WPA-PSK SSID was cracked with the airmon-ng utility hosted on an Ubuntu laptop. The process of it includes finding MAC addresses and a word list to attempt to find the password.

1. Opened an Ubuntu laptop and opened a terminal prompt.
2. Used sudo apt install airmon-ng to install the cracking utility.
3. Used sudo airmon-ng start wlp0s20f3 to put the NIC in promiscuous mode.
4. Entered sudo airodump-ng -d 04:62:73:AE:A4:50 -w ./wpa-psk-crack.txt -c 52 wlp0s20f3mon
5. Utilized sudo aircrack-ng -w ./wordlist ./wpa-psk-crack.txt-01.cap to iterate through a wordlist to crack the password.
6. Used the password to log into the network via SSID.

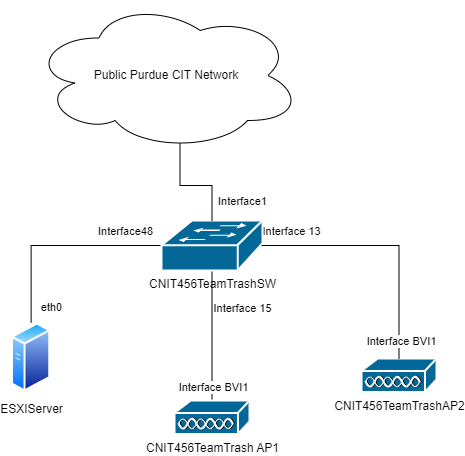
## MAC Address Spoofing

MAC Address spoofing is a way to get around MAC filters on networking devices. A MAC can be spoofed on a NIC to appear as a different or trusted user.

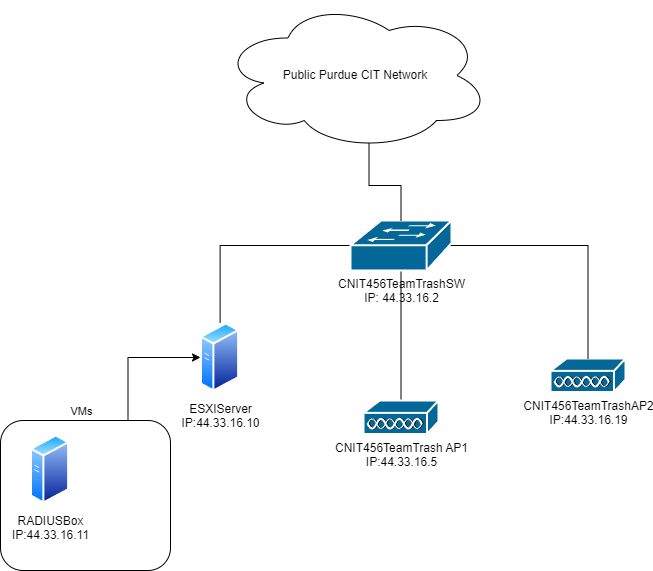
1. Opened a terminal on Ubuntu.
2. Added an ACL on the MAC address filter to block the current address on the NIC.
3. Attempted to connect to the network and got blocked.
4. Typed ip link set dev wlp0s20f3 address aa:bb:cc:dd:ee:ff to change the MAC address.
5. Connected to the network.

# RESULTS

In order to accomplish the necessary objectives required for this network four physical machines were configured from scratch. A Cisco switch and two Cisco access points (APs) were factory reset and are used to accomplish the necessary network requirements. Additionally, a server has been set up with ESXi that currently hosts a Windows Server VM with Active Directory enabled. AP1 was configured with SSID cloaking to make it harder to detect for an outside observer to detect and a MAC access list was put in place so that only computers with a specific MAC address could connect. Additionally, AP1 was configured with WPA-PSK as its encryption standard unlike AP2 which was configured with WPA 2 Enterprise. WPA 2 Enterprise requires some sort of RADIUS system which is what the Windows Server VM with Active Directory is there for. For a more overall understanding of the network, the logical and physical diagrams of the network are included in the figures below. All objectives were accomplished and machine configurations can be seen in Appendix C.



*Figure 1: Physical Diagram of the Network*



*Figure 2: Logical Diagram of the Network*

# CONCLUSIONS AND RECOMMENDATIONS

It was concluded that for a small-to-mid wireless enterprise environment, the constructed network has effective security and speeds for the given equipment and resources. A switch can effectively supply each device with network, supply power to APs over POE, and serve as a central DHCP server from which clients can receive an IP address from. An AP configured with WPA PSK may not give enough security for an enterprise-level wireless network as demonstrated with MAC spoofing and password cracking. An AP configured with WPAv2 802.1X/EAP however, does supply a strong and secure network for enterprise environments. A Windows server serves as an effective option for 802.1X/EAP authentication via RADIUS.

The largest recommendation for improving and strengthening this wireless network would be to convert the AP using WPA PSK to using WPAv2 802.1X/EAP. This would provide all wireless networks in the environment with enterprise-level security. Another recommendation would be to create connection request policies to require users to be on the correct SSID to authenticate.

# BIBLIOGRAPHY

Canonical. (n.d.). Ubuntu Manpage: Aircrack-ng - A 802.11 wep / WPA-psk key cracker. https://manpages.ubuntu.com/manpages/xenial/man1/aircrack-ng.1.html

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. (2021, July 12). Wi-Fi Protected Access 2 (WPA 2) configuration example. Cisco. https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/67134-wpa2-config.html

Configuring autonomous AP for local radius authentication. Cisco Community. (2023, January 4). https://community.cisco.com/t5/wireless-mobility-knowledge-base/configuring-autonomous-ap-for-local-radius-authentication/ta-p/3118775

Configuring DHCP. (n.d.). https://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/consolidated\_guide/b\_consolidated\_3850\_3se\_cg\_chapter\_0111011.pdf

Configuring radius authentication with WPA2-Enterprise. Cisco Meraki Documentation. (2024, February 1). https://documentation.meraki.com/MR/Encryption\_and\_Authentication/Configuring\_RADIUS\_Authentication\_with\_WPA2-Enterprise

How to update access point firmware using TFTP when it is not possible to perform update through the HTTP interface. Cisco Community. (2020, November 18). https://community.cisco.com/t5/wireless-mobility-knowledge-base/how-to-update-access-point-firmware-using-tftp-when-it-is-not/ta-p/3131109

wikiHow. (2021, October 21). How to change mac address on ubuntu: 7 steps (with pictures). https://www.wikihow.com/Change-MAC-Address-on-Ubuntu

# APPENDIX A: PROBLEM SOLVING

Found within this section are several issues experienced during the development of this project. Each problem below can be divided by a *Problem Description* detailing the issue, a list of *Possible Solutions* brainstormed and further explained, any *Solutions Attempted*, and finally a detailed description of the *Final Solution*.

## Problem 1: MAC Filters Not Applying Properly

**Problem Description:** After configuring MAC filters on AP 1, it would either not work or block everyone off the network. Additionally, there were troubles changing MAC addresses on Windows.

**Possible Solutions:** (1) Turn off SSID cloaking (2) Reconfigure the MAC filters (3) Factory Reset the AP

**Solutions Attempted:** Solutions 1 and 2 were attempted. Though solution 1 did not fix the problem it helped narrow down the problem and fix any additional problems with computers trying to join the network

**Final Solution:** While reconfiguring the MAC filters it was noticed that there were no filters set to permit with a full mask.

## Problem 2: Flashing APs

**Problem Description:** The APs needed to be factory reset however upon trying to reset them it was noticed they were stuck on CAPWAP and it was necessary to change them to ROMMON.

**Possible Solutions:** (1) Standard factory reset procedures (2) Exchange to a different APs (3) Flash the AP wirelessly

**Solutions Attempted:** All solutions were attempted. Standard factory reset did not yield any results as while it was factory reset the AP was unusable for our needs. Exchanging APs only worked for one as all other APs were configured to be in CAPWAP mode.

**Final Solution:** The final solution to get the APs configured correctly involved downloading the correct tar file form the Purdue TFTP server and flashing the AP. Then the AP was configured to boot from the installed OS and not the previously configured one.

## Problem 3: RADIUS Not Working

**Problem Description:** As a requirement for WPA2 Enterprise, a RADIUS box has to be properly configured in order to properly authenticate. While it was working fine after one day it suddenly stopped working. The authentication worked and devices were able to enter the network but DHCP would not work.

**Possible Solutions:** (1) Reconfigure AP 2 (2) Reconfigure the Active Directory(3) Factory Reset the AP (4) Restart the ESXI and Windows Server

**Solutions Attempted:** All solutions were attempted. Trying to reconfigure both the AP and Active Directory did not yield any results even when reconfiguring everything from scratch. As part of reconfiguring from scratch the AP was factory reset but that too proved unsuccessful.

**Final Solution:** Rebooting the ESXI and Windows server fixed the issue as network connectivity was restored for all users on AP 1.

# APPENDIX B: KNOWLEDGE-BASED QUESTIONS

**How can a packet analyzer find the SSID of an AP if it does not broadcast the SSID?**

A packet analyzer like Wireshark can be used to find the SSID of an AP even if it is not broadcasting the SSID. Even with SSID broadcasting disabled, an access point sends beacon responses through the RF medium. Since the RF medium is shared, a sniffer can see the SSID response of the AP allowing the user onto the network.

**Which steps of authentication and association are you able to complete if your MAC is not in the ACL?**

If your MAC is not in the ACL, you are able to pass the initial authentication in WPA2. You could also possibly associate with the network by sending association requests. However, when the user is associated and pressed for authentication, the MAC filter will block it out.

**Which steps of authentication and association are you able to complete if your PC is not using WPA-PSK? Are these individual steps sufficient to secure an enterprise network? A home office network? What if you combine these methods? What additional steps could be taken to further secure the enterprise wireless network?**

If a PC is not using WPA-PSK, it would fail after state 1. Once the AP tries to authenticate the user, they will be denied. The user will never get associated with the network as they will not pass the authentication step. WPA-PSK is not sufficient to secure an enterprise network, but it is sufficient for a home network that does not have sensitive information. Using a MAC filter and WPA-PSK is still not sufficient for an enterprise network. Enterprise networks must be more secure containing authentication servers and individualized credentials to users. It also required internal auditing to ensure no insider threats are present.

**What are the weaknesses of AES-CCMP and are they easily exploited? How?**

AES-CCMP have limited weaknesses, but it is not a perfect encryption method. The biggest weakness is key length as the users are responsible for making long enough passwords. Another weakness lies in vulnerabilities in key creation processes as the protocols are external and AES-CCMP uses it. This is a weakness as it is not directly associated with AES-CCMP.

**How many different ways can you find the SSID of an AP without the SSID being broadcast?**

An SSID can be found off of an AP without it being broadcasted in multiple different ways including using a packet analyzer or de-authing a user so that they have to reconnect to the network.

**Can the AP distinguish between the original authenticated client and the attacker? What happens when both the original client PC and the attacker’s PC are using the same MAC address while connected to the same AP simultaneously?**

The AP can distinguish between a client and an attacker based on which MAC addresses are associated. This occurs because 802.11 works on layer 2, containing MAC addresses. When

a client with the same MAC address tries to connect, it will not allow the user on unless they are spoofing a different MAC address. If two are on at the same time, there are traffic sending issues and connection interruptions until the AP can kick the attacker off.

**What are the exact vulnerabilities in WPA-PSK and how can they be mitigated?**

The vulnerabilities in WPA-PSK are mostly dictionary susceptible attacks including offline dictionary attacks. The biggest flaw is the ability to sniff packets without being on the network of people associating to the network, and then using a utility to dictionary attack the passphrase.

# APPENDIX C: Switch and AP Configs

## Switch Config:

Current configuration : 4768 bytes

!

! No configuration change since last restart

! NVRAM config last updated at 01:29:21 UTC Wed Mar 30 2011

!

version 15.0

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname CNIT456TeamTrashSW

!

boot-start-marker

boot-end-marker

!

enable secret 5 $1$twn4$YIE77iHXOhPNJwk8y2bzJ/

!

username user password 7 06320E2D4747071E2E1606185A5D6B

no aaa new-model

switch 1 provision ws-c3750e-48pd

system mtu routing 1500

ip dhcp excluded-address 44.33.16.0 44.33.16.19

ip dhcp excluded-address 44.33.16.41 44.33.16.63

!

ip dhcp pool POOL1

network 44.33.16.0 255.255.255.192

default-router 44.33.16.1

dns-server 44.2.1.44 44.2.1.45

!

!

ip domain-name CNIT456TeamTrashSW

vtp mode transparent

!

!

crypto pki trustpoint TP-self-signed-223086592

enrollment selfsigned

subject-name cn=IOS-Self-Signed-Certificate-223086592

revocation-check none

rsakeypair TP-self-signed-223086592

!

!

crypto pki certificate chain TP-self-signed-223086592

certificate self-signed 01

30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030

30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274

69666963 6174652D 32323330 38363539 32301E17 0D313130 33333030 31323932

315A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F

532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3232 33303836

35393230 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100

F1649473 D7B38AB5 E0BB9D52 AA9BF3F7 B63E8FEC 90F0A389 9F08C9D8 FA94C05D

0AE1F278 B35709B5 A1A3A60E 55493AAF D5ED691F 801B79F4 33403E39 145D6BA2

8F4AB033 7C1F8DFD FCD1F63E A1AB9FF2 065AEE05 83CDD080 585EAA11 B518707E

20FE8EBC 78C34777 98AB910B 24201ED9 E4378936 4F821003 84D7411A 59DA5FA3

02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D

23041830 16801401 2DAC886B C72A9EDD 99DBA7E7 7629910B BD7D1230 1D060355

1D0E0416 0414012D AC886BC7 2A9EDD99 DBA7E776 29910BBD 7D12300D 06092A86

4886F70D 01010505 00038181 00C1ABDC 4BBFA7CF 1E0FD481 13E3AFBD 2EFA7344

7A487B4C FC6F6425 3EF915B8 431B07D8 DDB05F4A B2826AA3 CC5985D0 B8194967

8E1B7FC5 06718E98 E4C4A6F9 794EC1E1 5DB3B315 FDC54581 CC59880C D0421ADB

976118CE 2D4AD9B8 E7D18AC4 B81A8E72 B9E7554C D7A8EA73 CD92BD07 EBD0DBE9

A75C208B 0AE715B9 426E3C33 3C

quit

spanning-tree mode pvst

spanning-tree extend system-id

!

!

!

!

!

!

!

!

!

vlan internal allocation policy ascending

!

vlan 3003

!

ip ssh version 2

!

!

!

!

!

!

!

!

!

!

interface FastEthernet0

no ip address

!

interface GigabitEthernet1/0/1

description "Uplink"

switchport mode access

!

interface GigabitEthernet1/0/2

!

interface GigabitEthernet1/0/3

!

interface GigabitEthernet1/0/4

!

interface GigabitEthernet1/0/5

!

interface GigabitEthernet1/0/6

!

interface GigabitEthernet1/0/7

!

interface GigabitEthernet1/0/8

!

interface GigabitEthernet1/0/9

!

interface GigabitEthernet1/0/10

!

interface GigabitEthernet1/0/11

!

interface GigabitEthernet1/0/12

!

interface GigabitEthernet1/0/13

description "AP 1"

switchport mode access

!

interface GigabitEthernet1/0/14

!

interface GigabitEthernet1/0/15

description "AP 2"

switchport mode access

!

interface GigabitEthernet1/0/16

!

interface GigabitEthernet1/0/17

!

interface GigabitEthernet1/0/18

!

interface GigabitEthernet1/0/19

!

interface GigabitEthernet1/0/20

!

interface GigabitEthernet1/0/21

!

interface GigabitEthernet1/0/22

!

interface GigabitEthernet1/0/23

!

interface GigabitEthernet1/0/24

!

interface GigabitEthernet1/0/25

!

interface GigabitEthernet1/0/26

!

interface GigabitEthernet1/0/27

!

interface GigabitEthernet1/0/28

!

interface GigabitEthernet1/0/29

!

interface GigabitEthernet1/0/30

!

interface GigabitEthernet1/0/31

!

interface GigabitEthernet1/0/32

!

interface GigabitEthernet1/0/33

!

interface GigabitEthernet1/0/34

!

interface GigabitEthernet1/0/35

!

interface GigabitEthernet1/0/36

!

interface GigabitEthernet1/0/37

!

interface GigabitEthernet1/0/38

!

interface GigabitEthernet1/0/39

!

interface GigabitEthernet1/0/40

!

interface GigabitEthernet1/0/41

!

interface GigabitEthernet1/0/42

!

interface GigabitEthernet1/0/43

!

interface GigabitEthernet1/0/44

!

interface GigabitEthernet1/0/45

!

interface GigabitEthernet1/0/46

!

interface GigabitEthernet1/0/47

!

interface GigabitEthernet1/0/48

switchport mode access

!

interface GigabitEthernet1/0/49

!

interface GigabitEthernet1/0/50

!

interface GigabitEthernet1/0/51

!

interface GigabitEthernet1/0/52

!

interface TenGigabitEthernet1/0/1

!

interface TenGigabitEthernet1/0/2

!

interface Vlan1

ip address 44.33.16.2 255.255.255.192

!

ip http server

ip http secure-server

!

!

!

!

!

line con 0

line vty 0 4

login local

transport input ssh

line vty 5 15

login local

## AP1 Config:

Current configuration : 2037 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname CNIT456TeamTrashAP1

!

!

logging rate-limit console 9

enable secret 5 $1$SL7B$ykYmqJfxP3OED3QgZxMaT.

!

no aaa new-model

no ip cef

ip domain name CNIT456TeamTrashAP1.lcl

!

!

!

!

dot11 association mac-list 701

dot11 syslog

!

dot11 ssid CNIT456TeamTrashAP1

authentication open

authentication key-management wpa

guest-mode

wpa-psk ascii 7 00141215174C04140B

!

!

dot11 guest

!

!

!

username Cisco password 7 096F471A1A0A

username user password 7 06320E2D4747071E2E1606185A5D6B

!

!

bridge irb

!

!

!

interface Dot11Radio0

no ip address

shutdown

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

no ip address

!

encryption mode ciphers aes-ccm tkip

!

ssid CNIT456TeamTrashAP1

!

antenna gain 0

peakdetect

dfs band 3 block

stbc

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

ip address 44.33.16.5 255.255.255.192

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

!

access-list 701 deny aabb.ccdd.eeff 0000.0000.0000

access-list 701 permit ffff.ffff.ffff 0000.0000.0000

access-list 701 permit 0000.0000.0000 ffff.ffff.ffff

!

bridge 1 route ip

!

!

!

line con 0

line vty 0 4

login local

transport input ssh

line vty 5 15

login

transport input ssh

!

End

## AP2 Config:

Current configuration : 2875 bytes

!

version 15.2

no service pad

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname CNIT456TeamTrashAP2

!

!

logging rate-limit console 9

enable secret 5 $1$Yiwq$XUzPKDB4asIt92EXkC59y/

!

aaa new-model

!

!

aaa group server radius rad\_eap

server name Radius

!

aaa group server radius rad\_mac

!

aaa group server radius rad\_acct

!

aaa group server radius rad\_admin

!

aaa group server tacacs+ tac\_admin

!

aaa group server radius rad\_pmip

!

aaa group server radius dummy

!

aaa group server radius rad\_eap1

server name Radius

!

aaa group server radius rad\_acct1

server name Radius

!

aaa authentication login eap\_methods group rad\_eap

aaa authentication login mac\_methods local

aaa authentication login eap\_methods1 group rad\_eap1

aaa authorization exec default local

aaa accounting network acct\_methods start-stop group rad\_acct

aaa accounting network acct\_methods1 start-stop group rad\_acct1

!

!

!

!

!

aaa session-id common

no ip cef

ip domain name TEAMTRASH.lcl

!

!

!

!

dot11 syslog

!

dot11 ssid CNIT456TeamTrashAP2

authentication open eap eap\_methods1

authentication network-eap eap\_methods1

authentication key-management wpa version 2

accounting acct\_methods1

guest-mode

!

!

dot11 guest

!

!

!

username Cisco password 7 02250D480809

username admin password 7 053F07032A45400E320403015D5545

username user password 7 14231307070D242C0F292726744A46

!

!

bridge irb

!

!

!

interface Dot11Radio0

no ip address

shutdown

antenna gain 2

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

no ip address

!

encryption mode ciphers aes-ccm

!

ssid CNIT456TeamTrashAP2

!

antenna gain 4

peakdetect

dfs band 3 block

stbc

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

ip address 44.33.16.19 255.255.255.192

ipv6 address dhcp

ipv6 address autoconfig

!

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 radius source-interface BVI1

!

!

radius-server attribute 32 include-in-access-req format %h

radius-server vsa send accounting

!

radius server Radius

address ipv4 44.33.16.11 auth-port 1812 acct-port 1813

key 7 053F07032A45400E320403015D5545

!

bridge 1 route ip

!

!

!

line con 0

line vty 0 4

transport input ssh

line vty 5 15

transport input ssh

!

end