



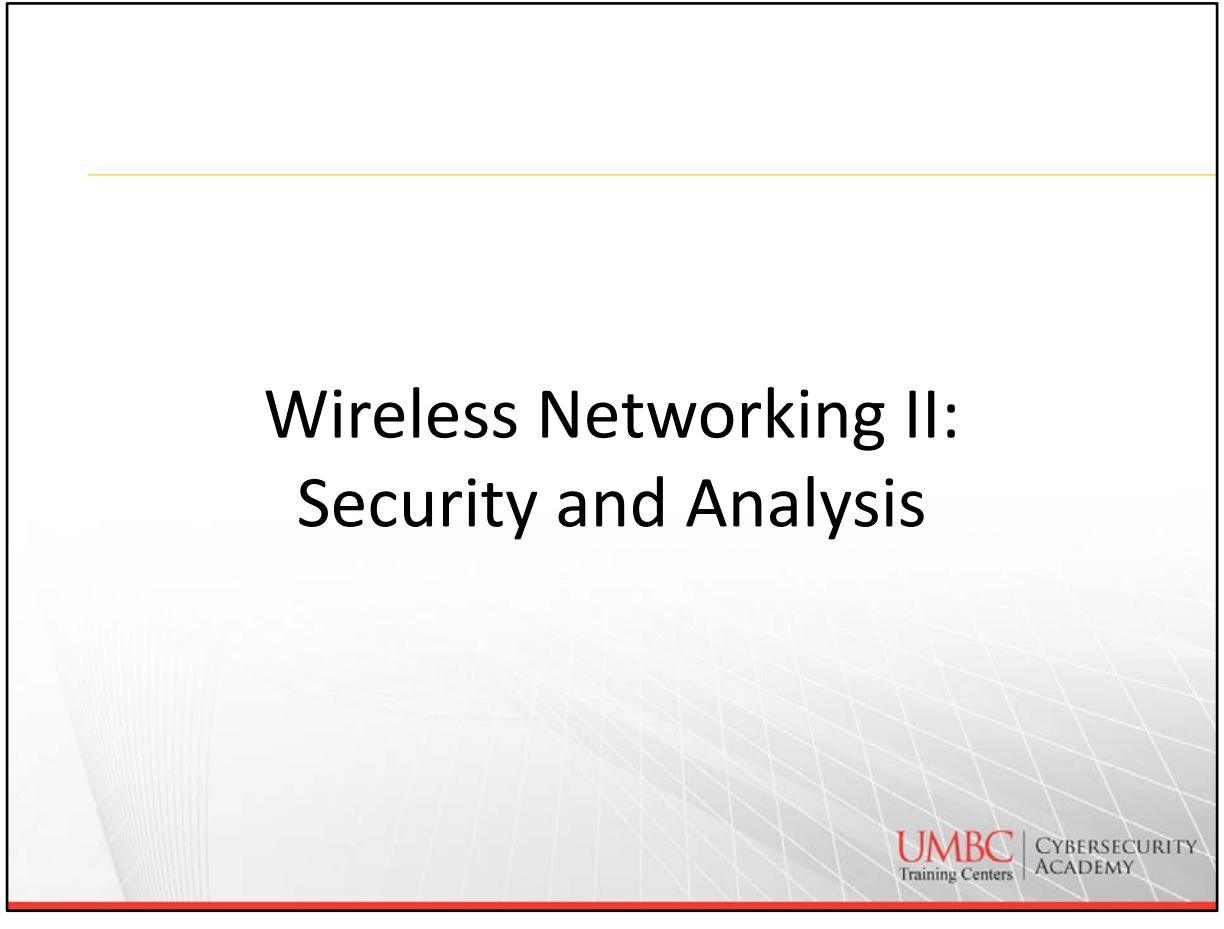
UMBC
TRAINING CENTERS

Wireless Networking II: Security & Analysis

TABLE OF CONTENTS

<u>SECTION 1</u>	<u>1</u>
<u>SECTION 2</u>	<u>54</u>
<u>SECTION 3</u>	<u>98</u>
<u>SECTION 4</u>	<u>156</u>
<u>SECTION 5</u>	<u>205</u>
<u>SECTION 6</u>	<u>235</u>
<u>SECTION 7</u>	<u>257</u>
<u>SECTION 8</u>	<u>278</u>
<u>SECTION 9</u>	<u>306</u>
<u>SECTION 10</u>	<u>323</u>
<u>SECTION 11</u>	<u>362</u>
<u>SECTION 12</u>	<u>379</u>
<u>SECTION 13</u>	<u>406</u>
<u>SECTION 14</u>	<u>436</u>
<u>SECTION 15</u>	<u>462</u>
<u>SECTION 16</u>	<u>496</u>
<u>SECTION 17</u>	<u>526</u>
<u>SECTION 18</u>	<u>546</u>

Wireless Networking II: Security and Analysis



UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Staff & Facilities
- Reference
- Topics of Instruction

Staff and Facilities

- Introductions
 - Background, strengths, experience, what you want to accomplish with this course, how will you use this course?
- Facilities Overview
- Network Setup and Configuration
- Class Hours

Topics of Instruction

- Security and Standards Overview
- Client Devices and Access Points
- Security Infrastructure
- Legacy (In)Security
- Encryption
- Dynamic Keys and RSN
- PSK Authentication
- 802.1X and EAP
- Radius and LDAP

Topics of Instruction

- Security Risks and Threats
- BYOD and Guest Access
- WLAN Auditing
- Wireless Security Monitoring
- Roaming
- WLAN Troubleshooting
- Policies...Yes, Policies

Standards and Security Overview

- Standards Organizations
- Lineage of Wireless
- Networking and Security Basics
- History of Security

Security Infrastructure

- Planes
- WLAN Architectures
- VPN Wireless Security
- Infrastructure Management

Legacy Security

- Authentication
- WEP
- TKIP
- VPNs
- SSID Segmentation

Encryption

- More on WEP
- TKIP
- CCMP
- Wi-Fi Alliance Certifications

Dynamic Key Encryption

- Dynamic Key Generation
- RSN and RSN Information Element
- Key Hierarchy
- Handshakes

Preshared Keys

- WPA and WPA2 Personal
- Passphrases and PSK

802.1X and EAP

- AAA
- 802.1X
- Certificates
- Legacy Authentication
- EAP Types

LDAP and RADIUS

- LDAP
- RADIUS
- Attribute Value Pairs

Security Risk

- Rogue Devices
- Eavesdropping
- Attacks
- Hijacking
- P2P
- Management Interfaces
- Guest Access

BYOD

- Mobile Device Management (MDM)
- On-boarding
- Guest Access
- Network Access Control (NAC)

WLAN Auditing

- Layer 1 and 2 Audits
- Pentesting
- Audit Recommendations
- Tools

Monitoring

- WIDS/WIPS
- Device Classification
- Analysis
- 802.11n/ac nuances
- Management Frame Protections

Roaming

- Roaming in General
- Roaming in a RSN
- OKC
- Fast BSS Transitions

WLAN Troubleshooting

- Best Practices
- OSI Model
- Client Issues
- Is It a Design Problem?

Policies

- General Policies
- Functional Policies
- Industry Regulations
- WLAN Policy Recommendations

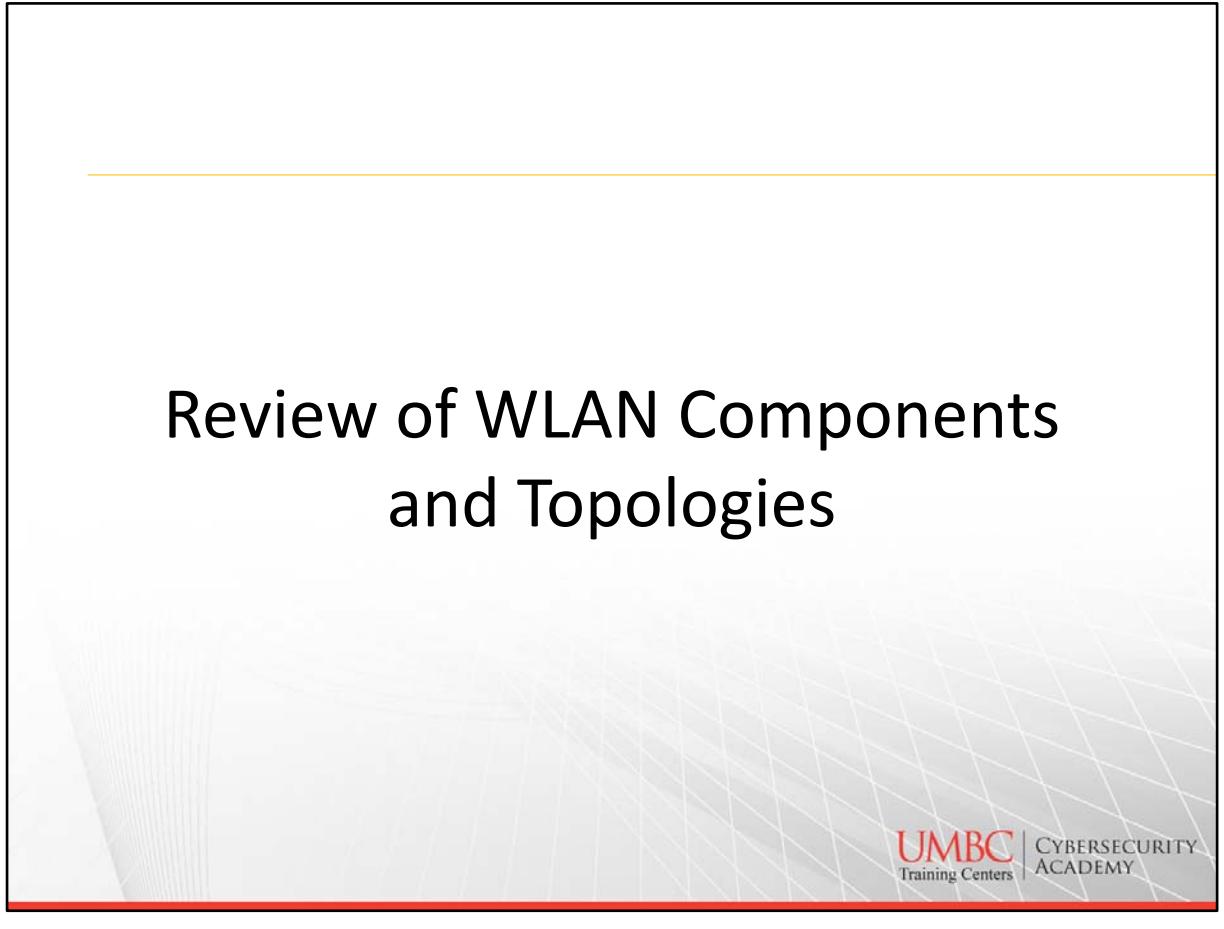
Administrivia

- Using Linux
- Open wireless network—use at your own risk

Let's Read On, Shall We?



Review of WLAN Components and Topologies



UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- WLAN Topologies
- Major Components
- 802.11 Topologies
- 802.11 Configuration Modes

Wireless Networking Topologies

- WWAN: broad geographical area
 - Cellular providers
 - GPRS, CDMA, TDMA, GSM, LTE
- WMAN: cities and suburbs
 - 802.16 and WiMax
 - Last mile solutions
 - Many thousand access points
 - Vertical markets



WWAN using cell networks used in bus services with access points

Some vertical markets for WMAN: Train service along established routes

Wireless Networking Topologies

- WPAN: close proximity access
 - Laptops, tablets, smartphones
 - 802.15 Bluetooth and FHSS
 - Peer-to-peer connections (IBSS)
 - Few feet, typically
- WLAN: building or campus networks
 - 100s of feet
 - Global enterprise networks



UMBC | CYBERSECURITY
Training Centers ACADEMY

Enterprise networks are typically managed by Network Management Servers

VPNs are also used in large enterprise networks

WPANs: there are 3 classes of Bluetooth devices, 1, 2, 3.

Class 1 runs at 100mW with a max range of about 100 meters

Class 2 at 2.5mW and about 10 meters

Class 3 at 1mW or less than 10 meters

Image from Bluetooth.com

802.11 Topologies

- Main component is the station (STA)
 - Access point and clients devices
- 802.11-2012 defined topologies
 - Basic Service Set (BSS)
 - Extended Service Set (ESS)
 - Independent Basic Service Set (IBSS)
 - Mesh Basic Service Set (MBSS)
- Half-duplex communications



Simplex is one way like a traditional radio station

Full Duplex is when two stations can talk back and forth simultaneously; telephone or cell phone

Half duplex: two-way but only one station can talk at a time

Access Point

- Half-duplex device
- Switch-like intelligence (CAM tables)
- Address and direct wireless traffic at Layer 2
- Forward upper layer (3-7) data
- MAC Service Data Unit (MSDU) is the payload in a wireless data frame
- Support for VLANs
- Up to 4 MAC address may be used



Often called wireless routers

VLANs are used to create separate broadcast domains to segregate different data e.g. user and management.

More on access points in an upcoming section.

Access Points



UMBC | CYBERSECURITY
Training Centers ACADEMY

Pictures from:
Linksys.com
D-link.com

802.11 Components

- Clients: radios not in an AP
 - Associated: layer 2 connection with an AP
- Integration service: delivery of MSDU between Distribution System (DS) and 802.11 WLAN
- Portal: way into a non 802.11 LAN
 - AP or WLAN controller
- Distribution System: interconnects one or more BSSs via a LAN

Distribution System (DS)

- Wireless traffic can be sent back to wireless medium or into the Integration Service
- Distribution System Medium (DSM): logical physical medium connecting APs
- Distribution System Service (DSS): switch-like intelligence using Layer 2 addressing
 - **Translational bridge** between two mediums

Wireless DS (WDS)

- Uses 4 MAC address formatted frame
- Bridges, repeaters, mesh networks
- Can provide coverage and backhaul
- Repeaters extend the WLAN coverage
 - Not connected to the wired backbone
 - Same frequency channel
 - Extra contention for medium
 - 50% overlap is necessary



Example of coverage and backhaul would be N access points using two radios

Service Set Identifier

- SSID is *logical* name of the wireless network
- Up to *32 characters and case sensitive*
- Cloak the SSID, but it's not security

“FBI Surveillance Van”

“hidden”

“0701322819”

“linksys00037”

“B2E47”

“/000/000/000”



Verizon FIOS

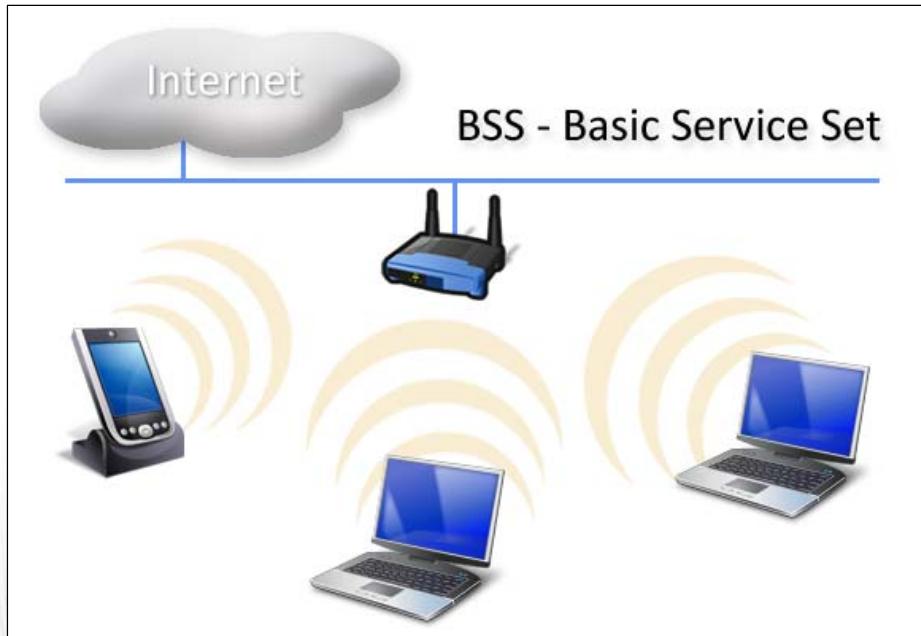
AWCC mobile number in Afghanistan

It's important to understand the environment from which you will be working or collecting....Research, target, customer.

Basic Service Set (BSS)

- One AP and one or more clients
- Member stations with a Layer 2 connection are *associated*
- Normally connected to a DS
- Clients talk to each other through an AP
 - Exception is Wi-Fi Direct

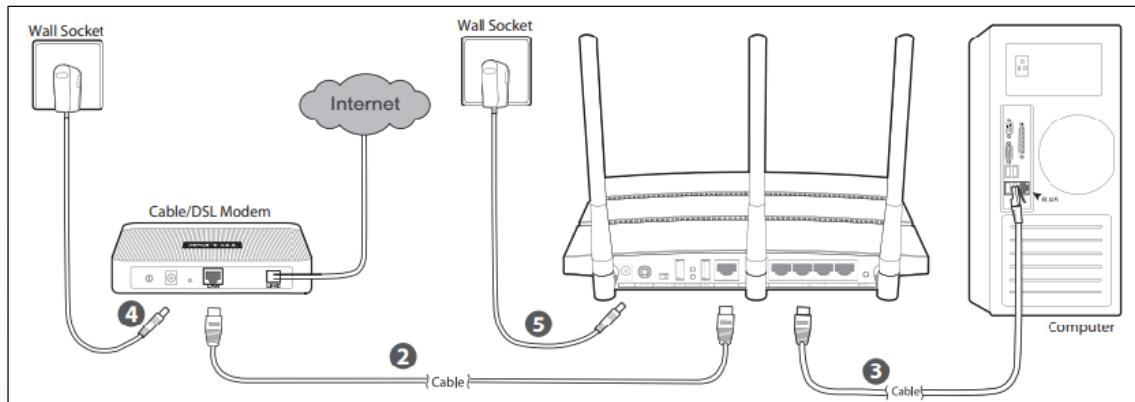
Basic Service Set



UMBC | CYBERSECURITY
Training Centers ACADEMY

Identify the DS, the BVI, and portal.

Basic Service Set



UMBC | CYBERSECURITY
Training Centers ACADEMY

BSS Identifier (BSSID)

- 48-bit MAC address of the AP radio
- Unique layer 2 identifier of each BSS
- First 3 octets are the OUI
 - 00:12:17:BA:14:04
- Lookup OUI on IEEE site:
 - <http://standards-oui.ieee.org/oui.txt>
- Why would I care about the OUI?

To look up default admin and password of a particular vendor.

Basic Service Area (BSA)

- Physical area of coverage by an AP in a BSS
- RSSI value threshold will determine data rates through Dynamic Rate Switching (DRS)
- Not a perfect circle
- Depends on power, gain, RF environment, surroundings, and much more.
- Heat Mapping Tools
 - Ekahau HeatMapper
 - iBWave

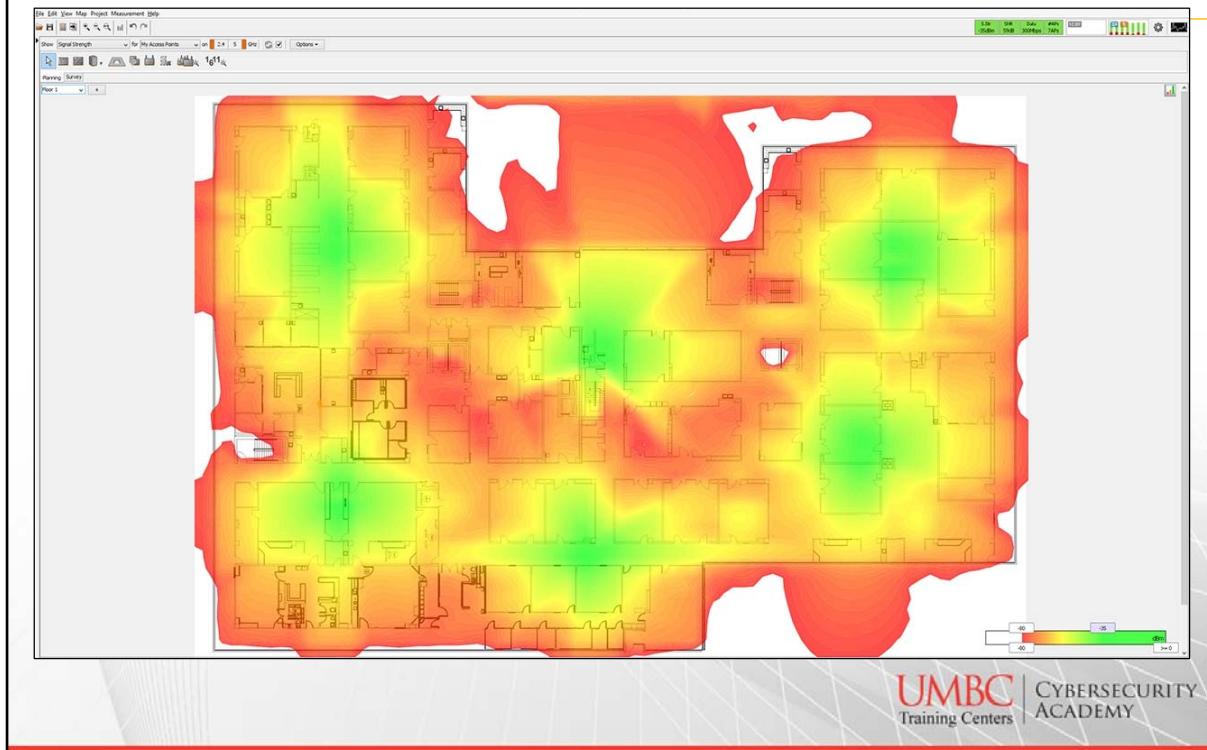


Why do you think a BSA is not a perfect circle?

iBWave mobile wi-fi tool

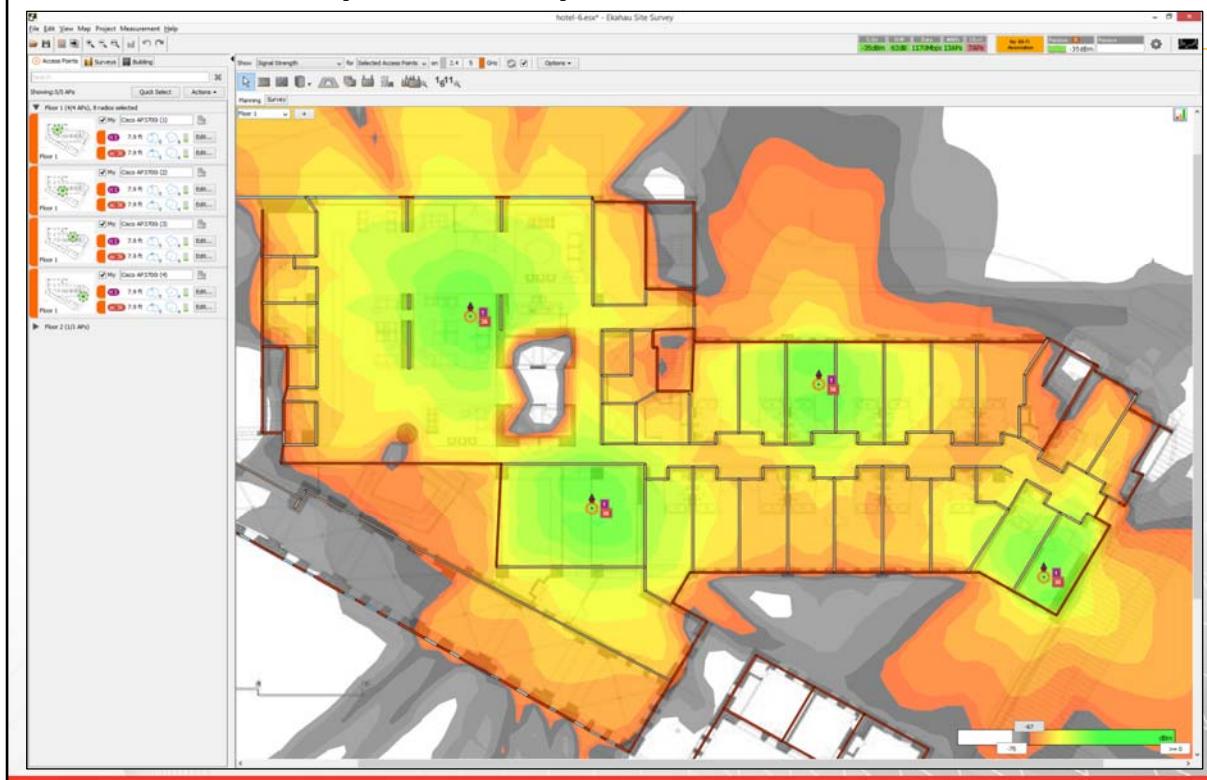
Ekahau software to do heat maps

Heat Map Example



From ekahau.com

Heat Map Example

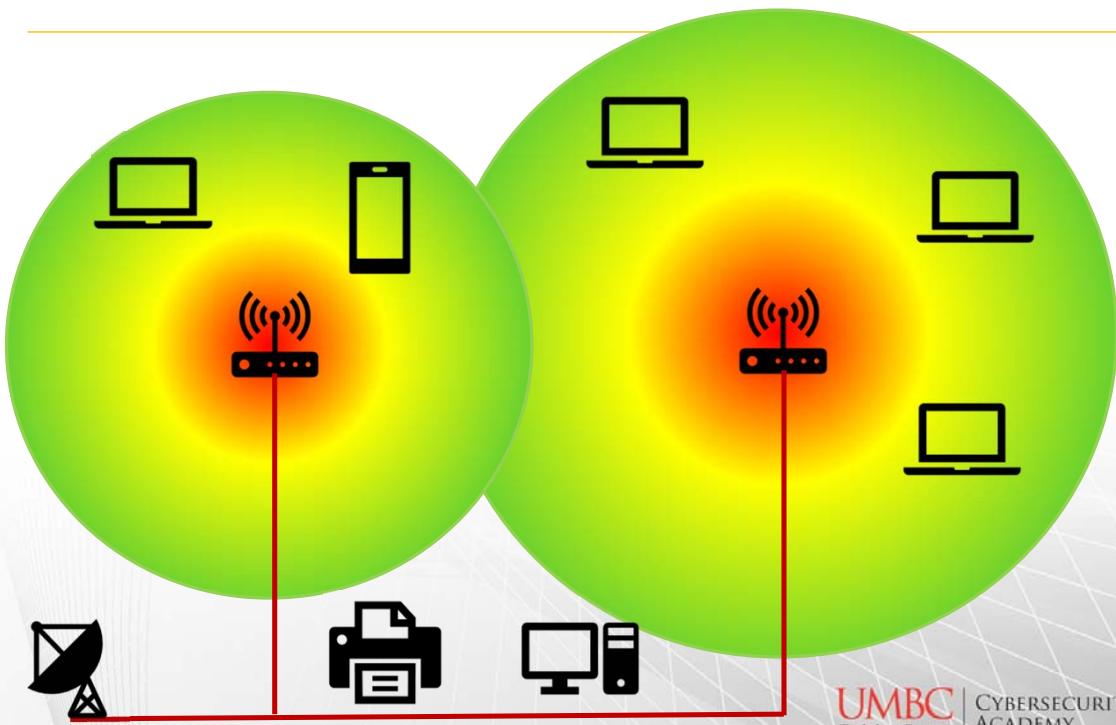


From ekahau.com

Extended Service Set (ESS)

- Two or more BSS connected by DSM
- Partially overlapping coverage cells
 - Seamless roaming of clients
- Non overlapping cells
 - Nomadic roaming after losing connectivity
- Colocation of cells
 - High density client environments
- AP have the *same SSID (ESSID)* but different BSSIDs

ESS

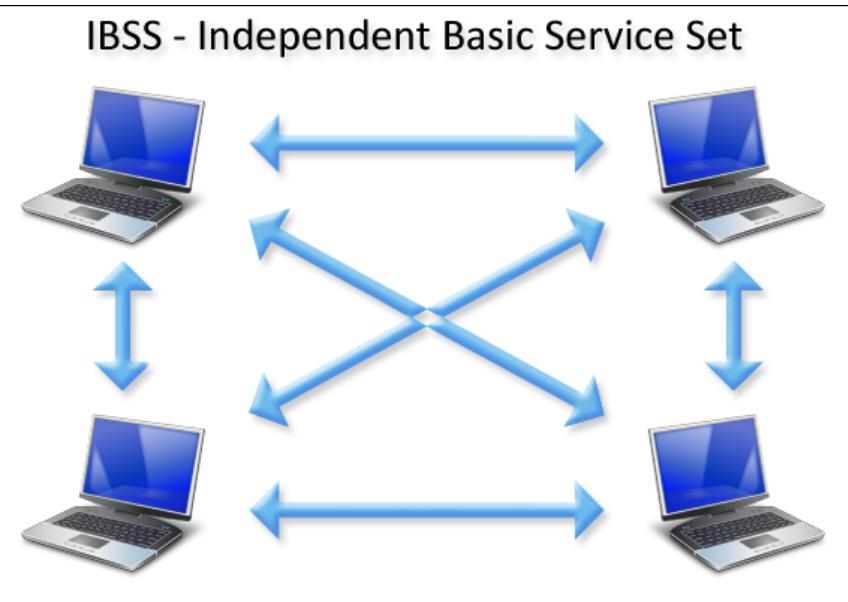


UMBC | CYBERSECURITY
Training Centers ACADEMY

Independent Basic Service Set (IBSS)

- No access point, only clients
- Peer-to-peer, ad-hoc networks
- Traffic is transmitted directly to each other
- Same frequency channel
- Same SSID
- **Auto-generated BSSID by first client**
 - Virtual MAC for Layer 2 identification

IBSS



UMBC | CYBERSECURITY
Training Centers ACADEMY

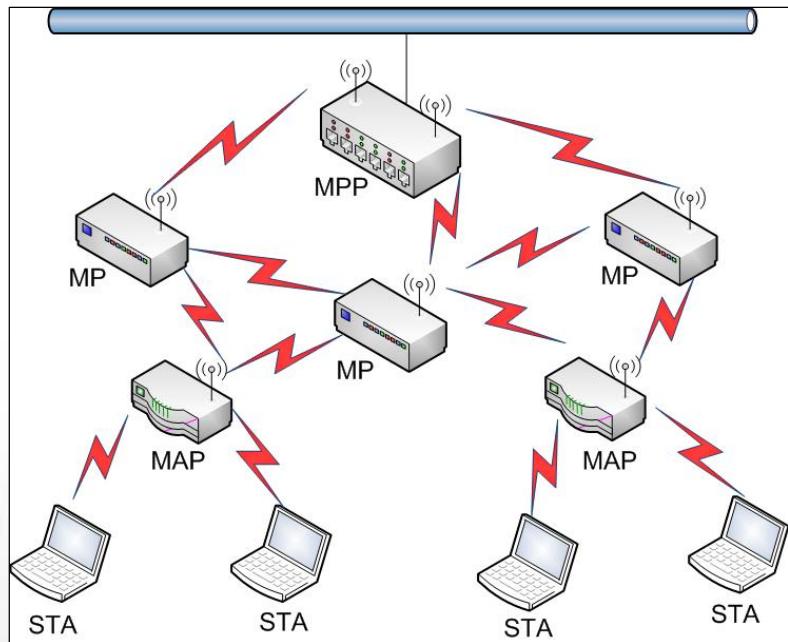
Mesh Basic Service Set (MBSS)

- Deployed where wired access is not feasible
- Wireless distribution of traffic
- At least one AP is connected to wired network
 - Mesh Point Portal (**MPP**), mesh root, gateway
- Other APs connect back to the MPP and provide wireless backhaul—Mesh Points (**MP**)
- AP that service device clients or stations—
Mesh AP (**MAP**)

MBSS

- Hybrid Wireless Mesh Protocol (HWMP) does layer 2 “routing”
- Metrics used can be proprietary
 - RSSI
 - SNR
 - Client Loading
 - Hop Counts

MBSS



UMBC | CYBERSECURITY
Training Centers ACADEMY

AP Modes or Configurations

- **Root** mode: access to the DS
 - AP mode or access mode
- **Workgroup bridge** mode: wireless backhaul for wired clients
- **Repeater** mode: extends coverage but adds overhead and contention
- **Mesh** mode: wireless backhauls in a mesh
- **Scanner** mode: sensor radio in a WIDS
 - Monitor mode

AP Operation Modes

The screenshot shows a sidebar menu on the left with options: Quick Setup, Operation Mode (highlighted with a red border), WPS, Network, Wireless, DHCP, and System Tools. To the right is a main content area with a green header bar labeled "Operation Mode". Below it, a message says: "Please select the proper operation mode according to your needs:". A list of seven options follows, each with a radio button and a description. The first option, "Access Point", is selected and highlighted with a red border. The other options are: "AP Client Router", "AP Router", "Multi-SSID", "Repeater(Range Extender)", "Bridge with AP", and "Client". At the bottom right of the content area is a red-bordered "Save" button.

Please select the proper operation mode according to your needs:

- AP Client Router - Wirelessly connect to WISP station/hotspot to share Internet network.
- AP Router - Wired connect to ADSL/Cable Modem via WAN port and share network.
- Access Point - Transform your existing wired network to a wireless network.
- Multi-SSID - Create multiple wireless networks to provide different security areas.
- Repeater(Range Extender) - Extend your existing wireless coverage by repeating signal.
- Bridge with AP - Combine two local networks via wireless connection.
- Client - Acting as a "Wireless Adapter" to connect your wired devices (e.g. laptop).

Save

AP Operation Modes

The screenshot shows the Cisco WAP321 Wireless-N Selectable Access Point configuration interface. The main title is "WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup". On the left, there's a navigation menu with sections like Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN, Wireless (selected), Networks, Scheduler, Scheduler Association, Bandwidth Utilization, MAC Filtering, WDS Bridge, WorkGroup Bridge, QoS, WPS Setup, WPS Process, System Security, Client QoS, SNMP, Captive Portal, and Single Point Setup. The Networks section is currently selected. The main content area is titled "Virtual Access Points (SSIDs)" and contains a table with 8 rows, each representing a VAP. The columns are: VAP No., Enable, VLAN ID, SSID Name, SSID Broadcast, Security, MAC Filter, and Channel Isolation. Row 0 has "AllYourBase" as its SSID name and "WPA Personal" as its security. Rows 1 through 7 are currently empty. Buttons for Add, Edit, Delete, and Save are at the bottom of the table.

In this AP, you can set up to 8 Virtual SSIDs.

This AP can also be set up as a WDS Bridge or Workgroup Bridge.

Client Station Modes

- Infrastructure
 - Default associated to an AP in a BSS or ESS
- Ad-hoc
 - IBSS networks for peer-to-peer communications

Summary

- WLAN Topologies
- 802.11 Topologies
- 802.11 Configuration Modes

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

Security Review

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Standards Organization
- Lineage of Wireless
- Networking and Security Basics
- History of Security

Standards Organizations

- Institute of Electrical and Electronics Engineers (IEEE)
- Internet Engineering Task Force (IETF)
- Wi-Fi Alliance
- International Organization for Standardizations (ISO)

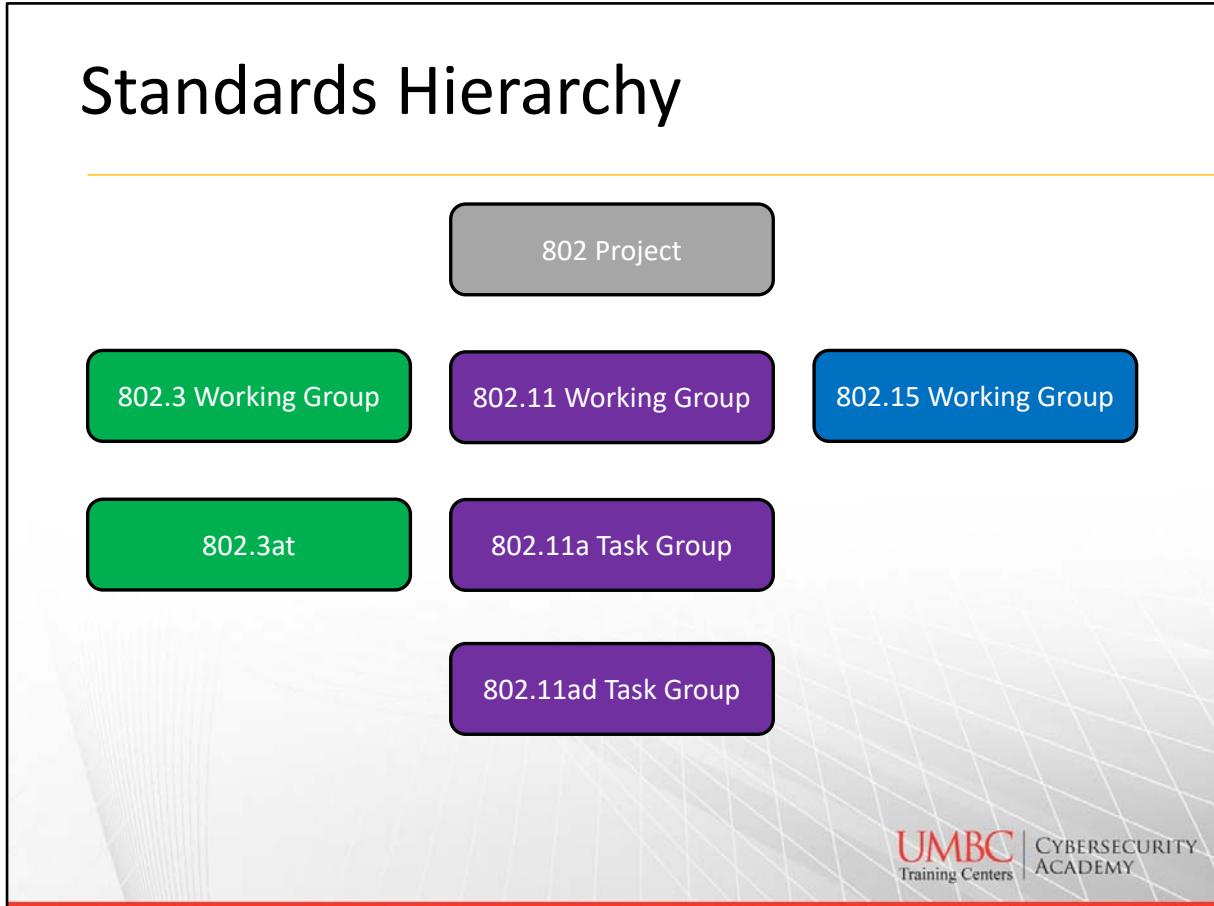


We'll touch on these organizations in the next few slides and see how they fit into the overall picture of wireless technologies.

IEEE

- Better known for the LAN standard
- Creates the standards for communications
 - 802 Project
- Standards working groups tackle problems or needs in the community
 - 802.3 (Ethernet) 802.11 (WLAN)
- Written documentation of the technical processes and equipment functions

Standards Hierarchy



UMBC | CYBERSECURITY
Training Centers ACADEMY

802 project is the LAN/MAN standards committee
802.11 was the 11th group under 802 project.

Standards are created by the working group and updated by task groups through amendments.

IETF

- Under the Internet Society (ISOC)
- Making the Internet work better!
- Protocol standards
- Best practices
- Informational documents
- Request for Comments
 - Statements or definitions
 - Obsoletes and updates



RFC describe network protocols, services, or policy. Some RFC end up becoming Internet standards.

Wi-Fi Alliance



- Originally the WECA
- Global industry association that promotes the growth of Wireless LANs
- Certification testing and programs
 - **Interoperability and compatibility** of WLAN products (30,000 certified products)
- Independent testing of products in 8 countries

Some Wi-Fi Alliance Certifications

- Wi-Fi Protected Access (WPA, WPA2, WPA3)
- Wi-Fi Multimedia (WMM)
- WMM-Power Save
- Wi-Fi Protected Setup (WPS)
- Wi-Fi Direct
- Voice Programs
- Tunneled Direct Link Setup
- Hotspot 2.0 and Passpoint
- Miracast



Are any of these familiar?

WPA – after realizing the original 802.11 security standard was weak; meant as an interim solution until IEEE standard could catch up. The IEEE standard that addressed the weaknesses and vulnerabilities was 802.11i; Therefore, **WPA was a pre-802.11i certification**. With WPA certification, TKIP, passphrase, and Extensible Authentication Protocols were seen.

Two modes, personal and enterprise.

WPA2 – after 802.11i amendment. This certification also has personal and enterprise. WPA2 uses CCMP which is Counter Mode with Cipher-block Chaining Message Authentication Code Protocol.

WMM certification is tied to 802.11e amendment which addresses QoS in WLANs. **What is QoS?** Categorize time-sensitive applications such as video and voice. 802.11e conformity is mandatory for 802.11n devices seeking WMM certification.

WMM-PS is a certification tied to mobile devices and battery life.

WPS targets SOHO users to simplify establishing authentication and association of devices. Pin-based and push button configuration. NFC is also an option with some devices. **What are some security vulnerabilities with WPS?**

Wi-Fi Direct is a certification for direct connection of devices to one another for printing, sharing, and display purposes. **Have you seen Printers setup for Direct connect?**

Hotspot 2.0 is oriented toward access to public WiFi and connecting to those access points securely. In larger metropolitan deployments it is designed to provide cellular type roaming.

Miracast integrates the display of streaming video content between devices. Devices identify and connect to each other and optimize the streaming of video. Provides 802.11n performance, ad-hoc connections via Wi-Fi Direct and WPA2 security. Wi-Fi display technical specification.

Wi-Fi Generations

Generation	Technology	Frequency Band	Max Advertised Data Rate
Wi-Fi 1	802.11a	5.0 GHz	54 Mbps
Wi-Fi 2	802.11b	2.4 GHz	11 Mbps
Wi-Fi 3	802.11g	2.4 GHz	54 Mbps
Wi-Fi 4	802.11n	2.4, 5.0 GHz (single, selectable, or concurrent)	600 Mbps
Wi-Fi 5	802.11ac	5.0 GHz*	6.9 Gbps
Wi-Fi 6	802.11ax	5.0 GHz*	9.6 Gbps

* Backwards compatibility with legacy devices

ISO and the OSI Model

- 7-layer logical representation
- Application FTP, HTTP
- Presentation ASCII, JPEG
- Session PPTP
- Transport TCP, UDP
- Network IP, IPX address
- **Data Link** **MAC address**
- **Physical** **Cabling, media, NIC, RF**



This model is the core of data communications and understanding networking.

Open Systems Interconnection.

Presentation: delivery and formatting of information

Session: opens, closes, and manages sessions between end user processes

Data link layer: organizing bit-level data between devices and detecting and correcting physical layer errors.

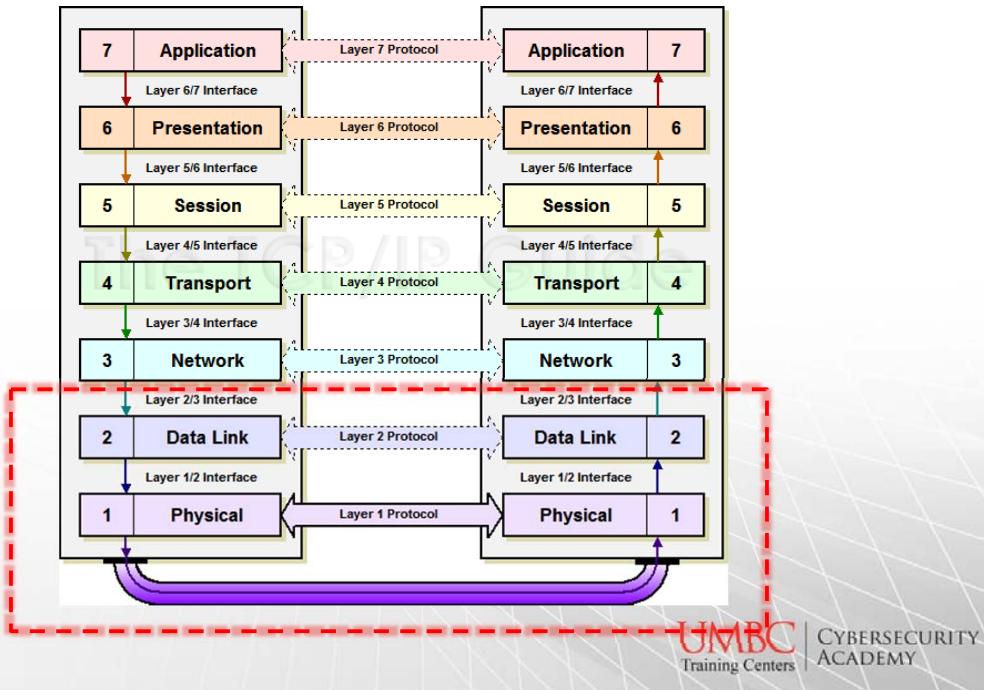
Physical layer: bit-level data streams

Both Data and Physical layers have two sublayers

OSI Model

- Open Systems Interconnection
- Peer-to-peer communications
- One-to-one mapping across networks
- Encapsulation
- De-encapsulation
- Top-down and bottom-up approach

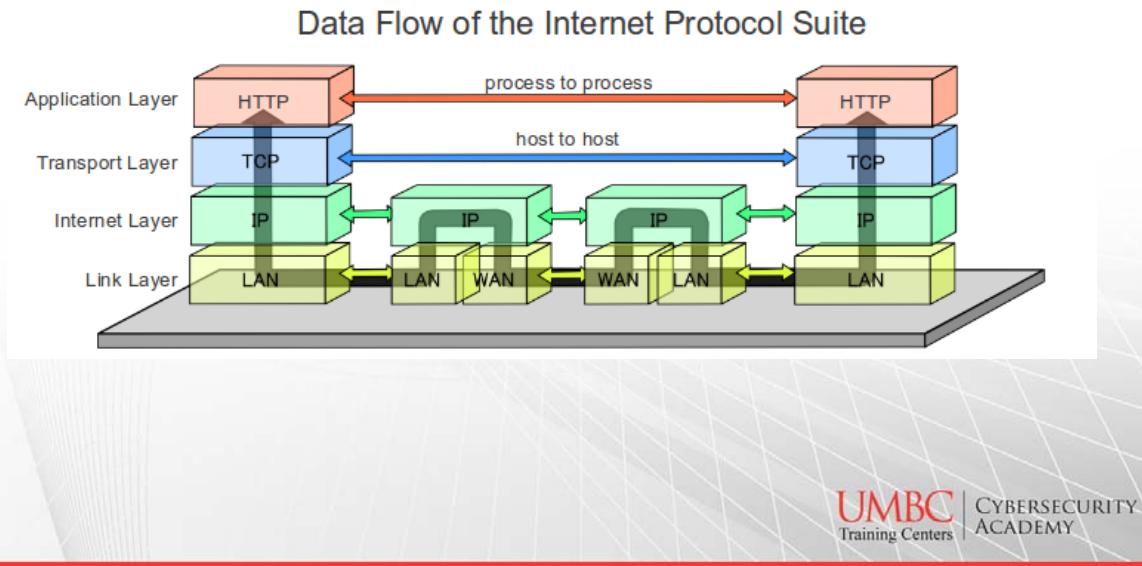
OSI



The red dashed box is where WLANs live

DOD Network Model

- Application, Transport, Internet, & Link Layer

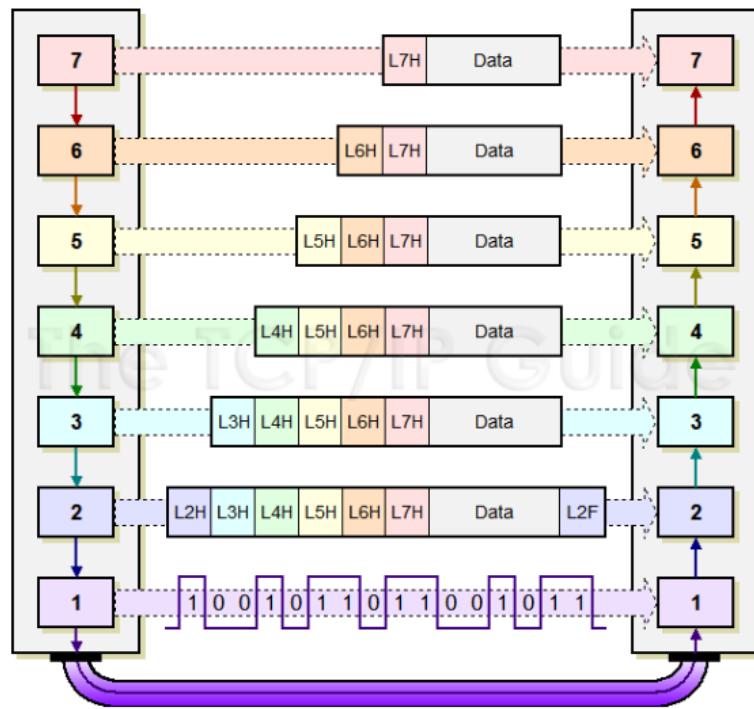


DOD model see the peer-to-peer communications in a 4 layer model.

The OSI DL and Physical layers are merged into the Link Layer. Everything above the OSI Transport layer (UDP/TCP) is lumped into the Application layer.

What is the mapping to OSI and DOD?

Encapsulation



CYBERSECURITY
ACADEMY

OSI Model Layers 2 and 1

- Where 802.11 lives
- Layer 2 – Data link layer sublayers
 - Logical Link Layer (upper)
 - **Media Access Control (lower)**
- Layer 1 – Physical medium, RF
 - Physical Layer Convergence Protocol (PLCP)
 - Physical Medium Dependent (PMD)



Explain the logical link (network layer); convergence (between layer 2 and 1) and PMD (media dependent)

PLCP is the interface between PMD and MAC

PMD is responsible for transmitting the data onto the wireless medium

Local Regulatory Domain Authority

- Licensed and unlicensed communications are regulated in these areas:
 - Frequency
 - Bandwidth
 - Max IR
 - Max EIRP
 - Indoor/outdoor use
 - Spectrum sharing (e.g. 802.11h)



UMBC | CYBERSECURITY
Training Centers ACADEMY

These are important to know. LRDA varies from country to country but these are similar areas that are regulated.

Local Authorities

- International Telecom Union-Radiocommunication (ITU-R): United Nations
 - Administrative and Radio Regulatory Regions
- Region A (Americas), Region 2 (Americas)
- US: Federal Communications Commission
- Key take-away is how communications are regulated

IEEE Standard and Amendments

- Original 802.11 Standard
- Periodic Roll-ups
- 2007 amendments
- 2012 amendments
- 2016 amendments
- Post-2016 amendments



In 2007 and 2012 the previous amendments to the standards were rolled up into these larger year amendments.

Original 802.11 Standard

- Defines technologies at the Physical and MAC sublayer of the Data Link Layer
- Infrared and obsolete
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- 2.4 GHz ISM band
- Speed versus throughput
 - Overhead and medium access methods



Original standard came out in 1997....So long ago.

With FHSS and DSSS in the original standard at a rate of 1 and 2 Mbps

802.11 b/g/a technologies equate to about 50% or less than advertises
802.11 n/ac 60-70% advertised throughput

Early 802.11

- 802.11b - 1999
- 2.4 GHz ISM bands
- DSSS backwards compatible
 - 1 & 2 Mbps
- High Rate DSSS (HR-DSSS)
 - 5.5 & 11 Mbps
- 22 MHz wide channels

Early 802.11

- 802.11a - 1999
- 5 GHz UNII bands
 - Unlicensed National Information Infrastructure
- Orthogonal Freq Division Multiplexing (OFDM)
- Mandatory 6, 12, 24 Mbps
- 6, 9, 12, 18, 24, 36, 48, 54 Mbps supported
- Not compatible with 802.11b/g
- 20 MHz wide channels

Early 802.11

- **802.11g** – 2003
- **2.4 GHz ISM band**
- Extended Rate Physical (ERP)
 - ERP-DSSS (backwards with b)
 - 1, 2, 5.5, 11 Mbps
 - ERP-OFDM
 - Mando 6, 12, 24 Mbps
 - 6, 9, 12, 18, 24, 36 ,48, 54 Mbps supported
 - Protection mechanisms to **support 802.11b**

Protection Mechanisms

- Coexistence of 802.11b and 802.11g
 - Three modes
 - B only: everything drops to b speeds
 - G only: only g clients are associated (pure G)
 - B/G mixed: protection used by G radios to support DSSS and HR-DSSS clients



Mixed mode doesn't necessarily mean everything drops to B speeds. There is a little more overhead than in a pure G.

G needs to inform B clients that there's traffic. So they communicate in a B language, then transmit G data in G language.

Early Ratified Amendments

- 802.11d – 2001
- Added **country codes** to beacon and probe responses
- Maintain compliance with country specific regulations

Early Ratified Amendments

- 802.11h – 2003
- Dynamic Frequency Selection (DFS)
 - AP tests for the presence of radar; chooses channel
- Transmit Power Control (TPC)
 - Maximum TX power per channel; AP decides
- Avoid interference with radar and SATCOM
- Added **11 more channels to 5 GHz UNII bands**
 - UNII-2 Extended

Early Ratified Amendments

- 802.11i – 2004
- **Robust Security Network (RSN)**
- Stronger encryption and better authentication
- Data privacy
- Data Integrity
- Authentication



Not to be confused as 802.1i

802.11i – 2004

- Data Privacy
 - CCMP with AES (block cipher)
 - Optional TKIP with RC4 (streaming cipher)
 - WiFi Alliance Certification (WPA2, WPA)
- Data Integrity
 - Message Integrity Checks (MICs, Michael)
 - Trailer includes 32-bit CRC (FCS)

802.11i – 2004

- Authentication
 - 802.1X / Extensible Authentication Protocol
 - Enterprise solutions
 - Passphrase or Preshared Keys (PSK)
 - WPA Personal
 - WPA2 Personal
 - *WPA2 is fully compliant certification with 802.11i*

More Ratified Amendments

- 802.11e – 2005
- Quality of Service (QoS) for time sensitive
 - Voice over WiFi (VoWiFi)
 - Video
- Hybrid Coordinated Function
 - Enhanced Distributed Channel Access
 - Prioritization of frames based on upper layer protocols
 - *WiFi Multimedia (WMM) is a WiFi Alliance certification that defines 4 priority categories*

UMBC | CYBERSECURITY
Training Centers ACADEMY

We'll see more on the priority categories later...

802.11r – 2008

- R is for roaming
- Fast BSS transition (FT) or fast secure roaming
- Handoffs between APs using RSN
- Allows bypassing 802.1X authentication for higher QoS data that is latency sensitive
- VoWiFi handsets in an enterprise network

802.11k – 2008

- Radio Resource Management (RRM)
- TPC under the 802.11h
- Client Statistics
- Channel Statistics for channel management
- Neighbor reports for handoffs
- Fast BSS Transitions



SNR, signal strength, and data rates from the client; transmission retries and error information back to the AP

Channel management decision by the AP

802.11w – 2009

- Robust management frames
 - Disassociation, Deauthentication
- Prevent some layer 2 Denial of Service
- Unicast frames use CCMP mechanisms
- Broadcast and Multicast use Broadcast Integrity Protocol (BIP)
- MFP comes in to play with WPA3

802.11n – 2009

- 2.4 and 5 GHz bands
- Increase throughput
 - High Throughput (HT)
 - Up to 600 Mbps
- MIMO with OFDM
- Backwards compatible with 802.11a/b/g
- Frame Aggregation and Block ACKs
- Reduced Inter-Frame Spacing (RIFS)

802.11s – 2011

- Wireless Distribution System (WDS)
- AP can be a portal to non-wired DS
 - Mesh access point (MAP)
- Mesh routing protocols and metrics
 - Mesh points (MP)
- Mesh portal point (MPP) is the gateway to an external network like 802.3

More Recent Amendments

- 802.11aa – QoS enhancements at MAC
 - Link reliability, improved application performance
- 802.11ae – QoS management frames (QMF)
 - Frames transmitted at QoS categories
- 802.11ad – VHT at 60 GHz bands
 - Up to 7 Gbps speeds
 - Short distance LOS
 - Wired equivalent transfers, video streaming

More Recent Amendments

- 802.11ac – 2013
 - Very High Throughput (VHT) at Gigabit speeds
 - Only in 5 GHz bands
 - Wider channels 80 and 160 MHz wide
 - 256 Quadrature Amplitude Modulation (QAM)
 - More Spatial Streams (up to 8)
 - Multi-user MIMO (MU-MIMO)

802.11 – 2016 Standard

- Rolled up all the previous ratified amendments under one standard
- Approved in December 2016
- Last major roll up previous was in 2016
- Since December 2016, there have been 5 recent amendments

Most Current Wi-Fi Generation



- **802.11ax – 2018**
- Sometimes referred to as AX Wi-Fi
- Up to 9.6 Gbps
- Using 1024 QAM
 - 10 bits per symbol
- **160 MHz wide channels**
- Stream all those 4K and 8K things

802.11ax

- 980 subcarrier channels
- Up to 8 spatial streams
- More neighbor network aware
- Upload and download MU-MIMO
- Orthogonal Frequency Division Multiple Access (OFDMA)
- Great white paper published by Wi-Fi Alliance



UMBC | CYBERSECURITY
Training Centers ACADEMY

Image from tp-link.com

MU-MIMO in 802.11ac works only in download.

https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_6_White_Paper_20181003.pdf

Core, Distribution, Access Layers

- Used to describe the networking architecture
- Core: High speed switching
 - Aggregation of data
 - Fastest and redundancy built-in
 - **WLAN Controllers**
- Distribution: Routes to smaller node clusters or networks
 - VLANs and Subnets
 - **Wireless Bridges and WLAN Controllers**
- Access: Slower delivery to end users and nodes
 - **Access Points**



The core does not route or manipulate traffic but rather switches.

802.11 Security Components

- 5 components to wireless security
 - Policy (Regulation, Standards, Compliance)
 - Privacy (Encryption)
 - Authentication, Authorization, and Accounting
 - Segmentation (VPN, GRE, VLAN, FW, Routers)
 - Monitoring (overlay or integrated)



Policy- should cover authority, audience, auditing, and violation. General and Function Policies

Privacy through encryption.

AAA

Segmentation by separating user traffic in the network, physically or logically

Security History

- In the beginning...
 - Wired Equivalent Privacy (WEP)
- Shared Key authentication
- Open System authentication
- Then in 2004...
 - 802.11i ratification
 - Enhanced Data Privacy (CCMP/AES)
 - Enhanced Authentication
 - Robust Secure Network (RSN)



802.11i defined stronger encryption and authentication

Enhanced Data privacy with stronger encryption methods CCMP or Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CCMP AES became mandatory with option TKIP/RC4

CCMP/AES is mandatory for 802.11n and 802.11ac in those devices seeking certification and data rates

Enhanced Authentication through PSK and EAP methods which also generate seeding material for the generation of dynamic encryption keys

RSN is the establishment between two stations the procedures to authenticate and associate with each other and create dynamic encryption keys between the two radios through a 4-way handshake process.

Summary

- Standards Organization
- Lineage of Wireless
- Networking and Security Basics
- History of Security

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

WLAN Devices and Architecture

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- WLAN Client Devices
- WLAN Architecture
- Special WLAN Infrastructure

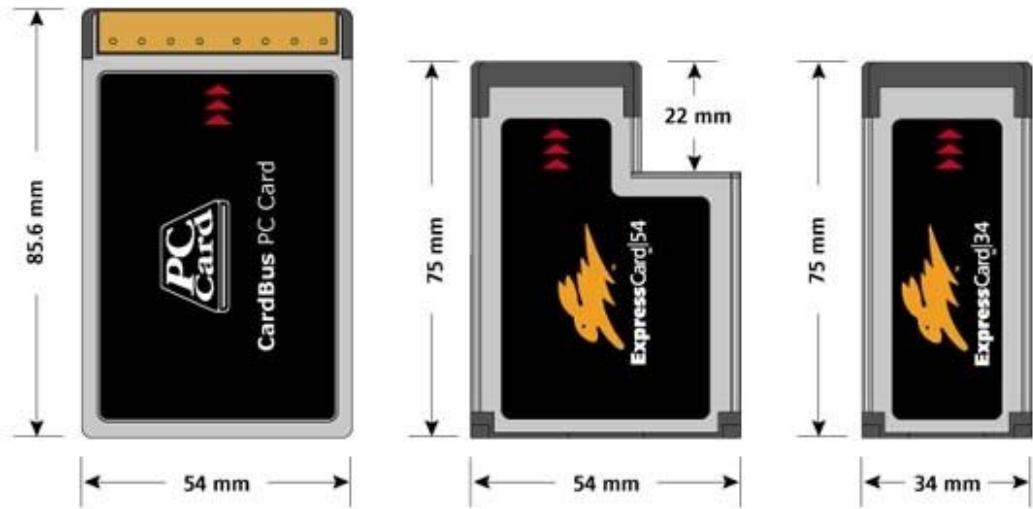
Client Devices

- Wireless NIC are half-duplex transceivers
- Variety of form factors
 - External
 - Internal
- Many chipsets
 - Components in an integrated circuit that manage data flow; support frequency bands
 - Chipset manufacturers sell product to radio card vendors
 - wikidevi.com/wiki/List_of_Wi-Fi_Chipset_Vendors
 - Tech Info Depot : Network



The WikiDevi page will be going to the archive in at the end of October. Tech Info Depot is picking up the slack.

PCMCIA Form Factors



PCMCIA Cards



Internal and external antenna were available to support many legitimate and not so legitimate purposes

ExpressCard



Secure Digital and Compact Flash



USB



Internal Radios

Mini PCI

Mini PCI
Express

Half Mini
PCI Express



UMBC CYBERSECURITY
Training Centers ACADEMY

You can find these in laptops, access points, and tablets.

In laptops they are installed in the bottom of the laptop or under the keyboard, antenna leads go up the sides of the monitor.

Devices and OS Relationship

- Device is the physical hardware
- Hardware contains the radio chipsets
- Applications access the hardware via the operating system kernel
- Layers of abstraction in between
- Application → Kernel → Hardware

Estimated 30 billion IOT devices in the next few years. Everyone with a smartphone, no child left behind.

Device and OS Relationship

- Between the application and kernel are libraries: Shared Objects (.so) & DLLs (.dll)
- Between the kernel and the hardware are drivers: Kernel Modules & SYS files (.sys)
- Some modules are built into the kernel others are loaded as needed, LKM
- lsmod, insmod, rmmod, modprobe



Shared objects in Linux are typically under path/to/lib/ directories
In Windows under Windows/System32/ directories

lsmod will show currently loaded modules

insmod will load a module

rmmod will remove a module

modprobe will load any dependencies

At the User Level

- Configure the device through a software interface to the user—client utility
- Not the driver itself
- Categories of client utilities
 - Operating System: Windows Zero Config
 - Vendor specific: Alfa Networks
 - Third-party utilities: Aircrack-ng

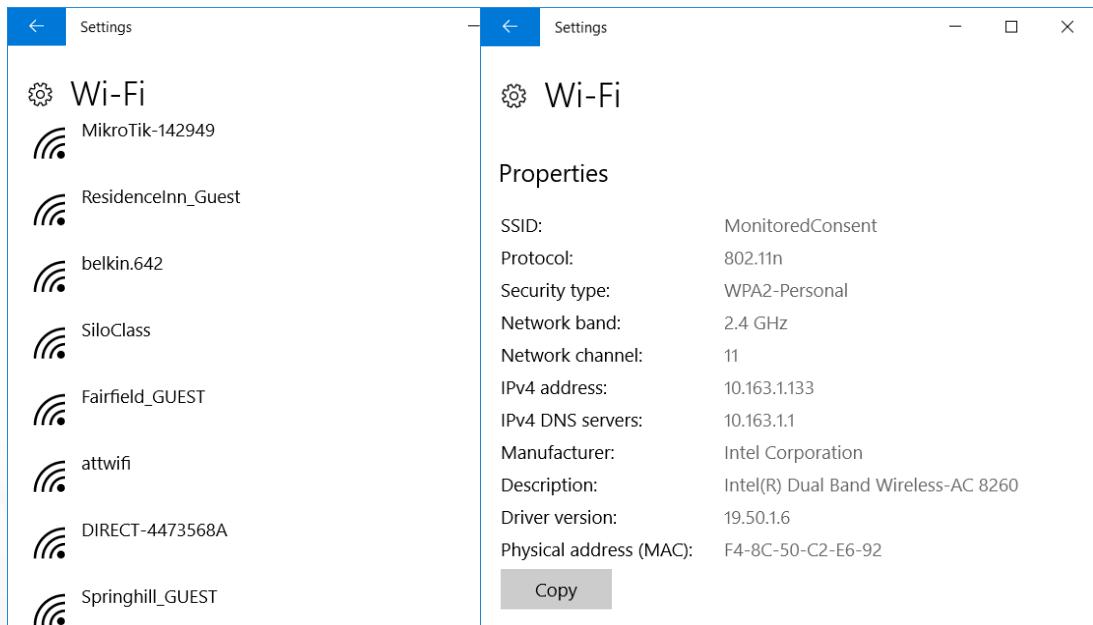


Driver is the interface between the physical hardware and the operating system

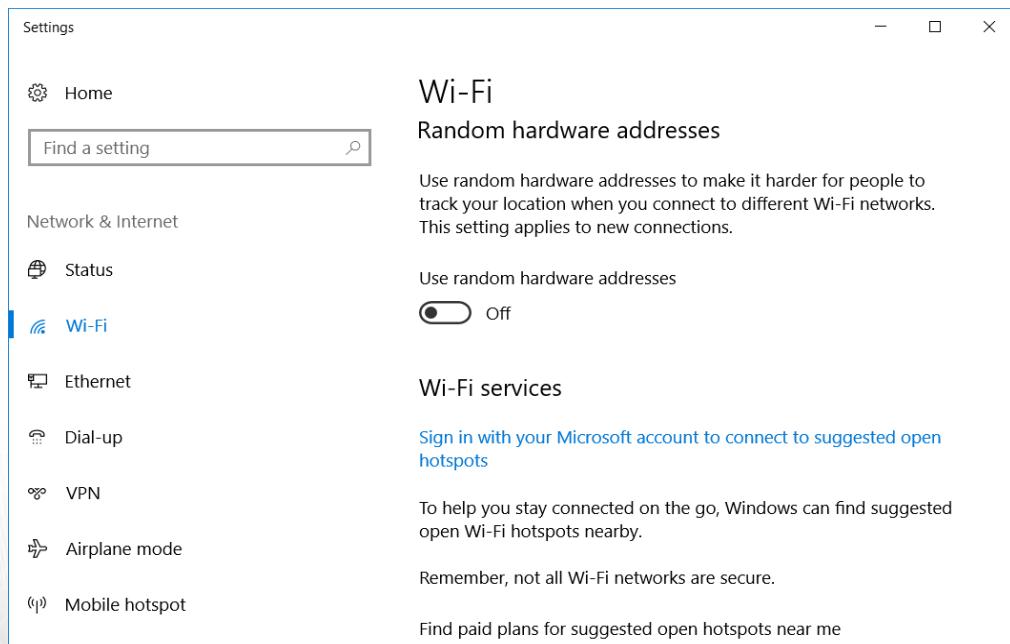
Vendor specific for peripheral devices; more configuration setting and statistical tools (Intel PROset Wireless)

Third-party utilities better support different EAP types and easier administration (Aironet and Cisco)

Windows 10

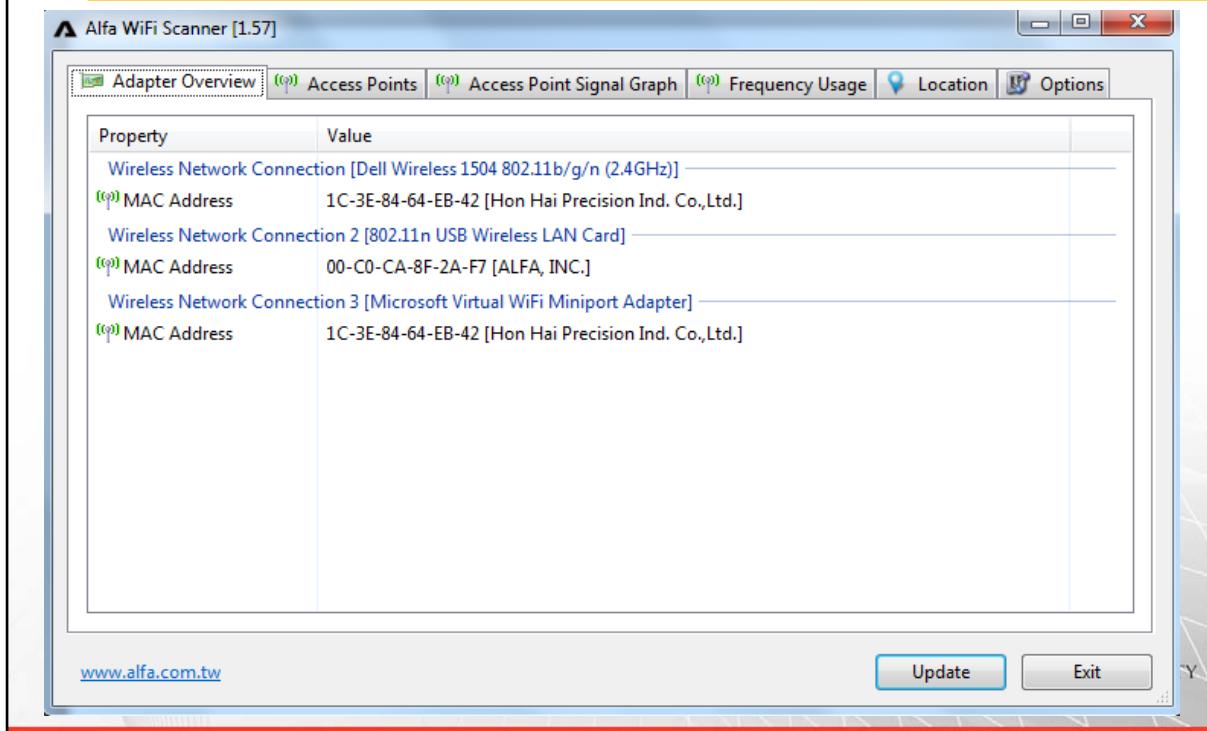


Windows 10

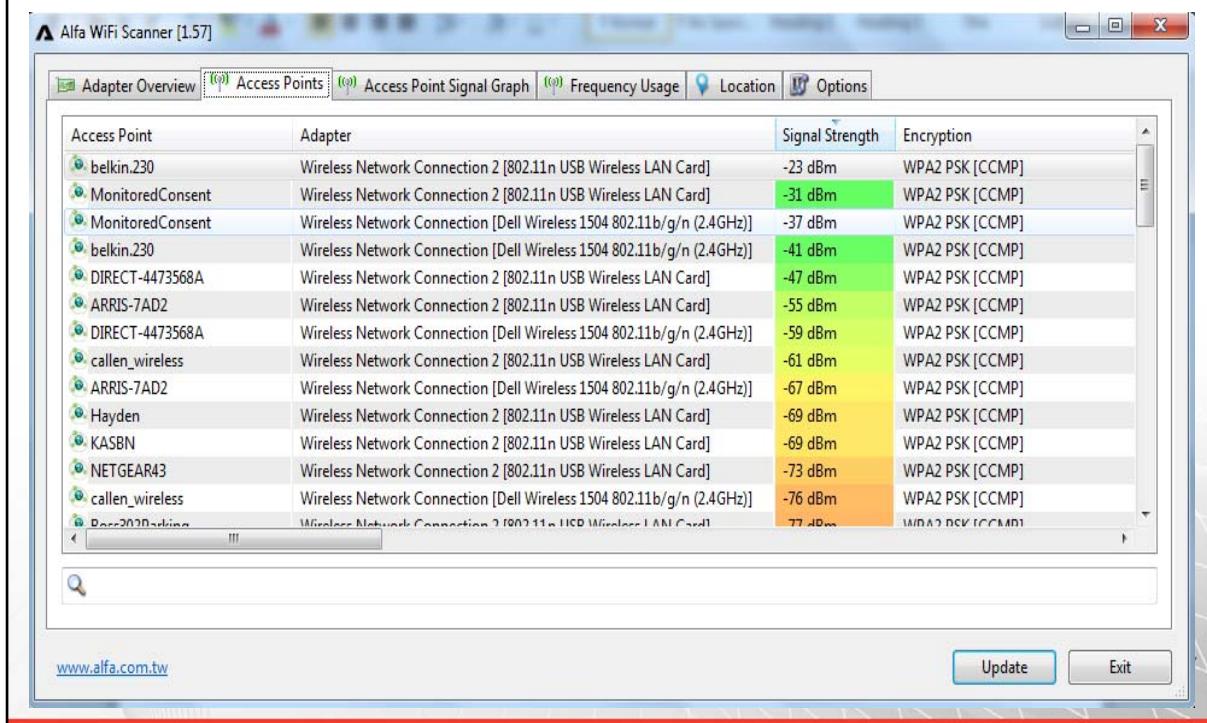


UMBC | CYBERSECURITY
Training Centers ACADEMY

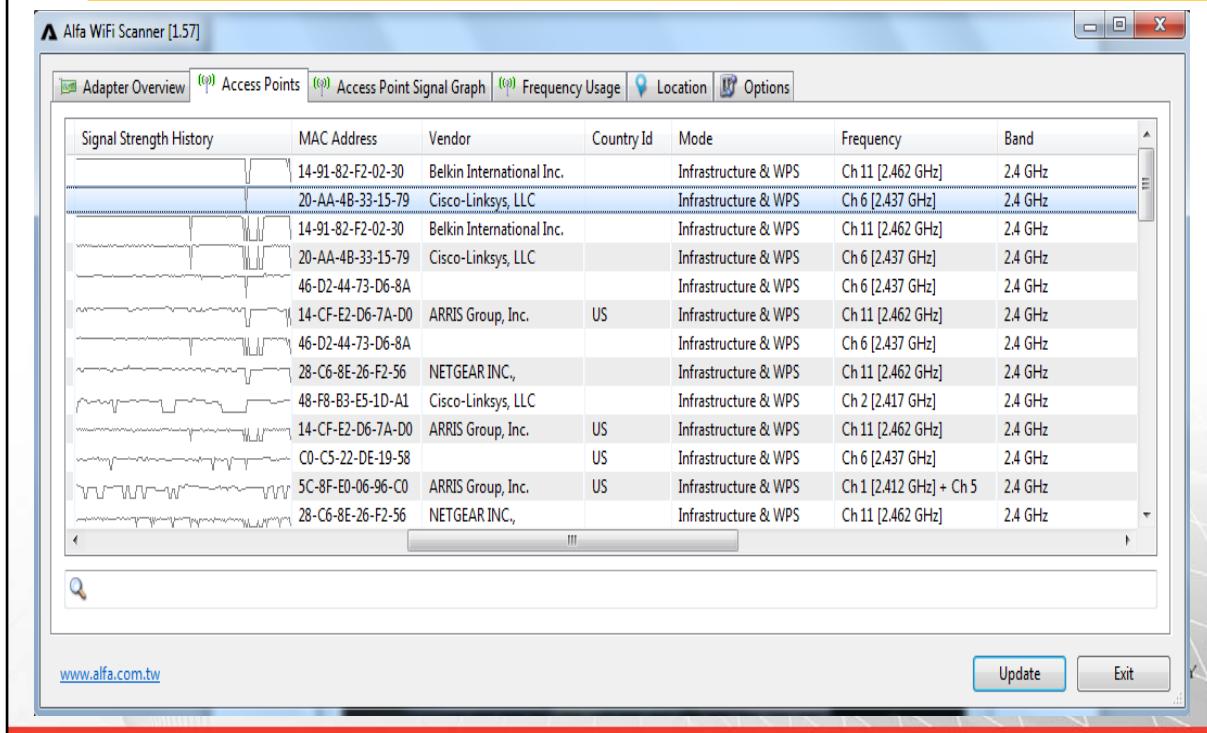
Alfa WiFi Scanner



Alfa WiFi Scanner



Alfa WiFi Scanner



Logical Planes of Operation

- **Management**: administrative network management and monitoring
- **Control**: control or signaling as in network intelligence and not the device (routing, switching)
- **Data**: where the network traffic is actually forwarded; this is the device
- In WLANs, each plane varies by architecture and vendor



Management: Centralized Network Management Server

Control: Layer 3 and Layer 2 decision making

Data: the physical switch or router

WLAN Management Plane

- WLAN Configuration or Settings
 - SSID, power, PSK
- Monitoring and Reporting
 - Statistics and session data
- Firmware Management
 - Upgrade APs and clients

Management Interface - Radio

The screenshot shows the Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup management interface. The left sidebar navigation menu includes: Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN, Wireless (selected), Radio, Rogue AP Detection, Networks, Scheduler, Scheduler Association, Bandwidth Utilization, MAC Filtering, WDS Bridge, WorkGroup Bridge, QoS, WPS Setup, WPS Process, System Security, Client QoS, SNMP, Captive Portal, and Single Point Setup.

Key configuration settings visible on the page:

- RTS Threshold: 2347 (Range: 0-2347, Default: 2347)
- Maximum Associated Clients: 200 (Range: 0-200, Default: 200)
- Transmit Power: Full - 100%
- Fixed Multicast Rate: Auto Mbps
- Legacy Rate Sets:

Rate (Mbps)	54	48	36	24	18	12	11	9	6	5.5	2	1
Supported	<input checked="" type="checkbox"/>											
Basic	<input type="checkbox"/>											
- MCS (Data Rate) Settings:

Index	0	1	2	3	4	5	6	7
Enable	<input checked="" type="checkbox"/>							
Index	8	9	10	11	12	13	14	15
Enable	<input checked="" type="checkbox"/>							
- Broadcast/Multicast Rate Limiting: Rate Limit (50 Packets Per Second, Range: 1-50, Default: 50), Rate Limit Burst (75 Packets Per Second, Range: 1-75, Default: 75)
- TSPEC Mode: Off
- TSPEC Voice ACM Mode: Off
- TSPEC Voice ACM Limit: 20 Percent (Range: 0-70, Default: 20)
- TSPEC Video ACM Mode: Off

© 2012 Cisco Systems, Inc. All rights reserved.

Management Interface - Stats

The screenshot shows a web browser window for the Cisco WAP321 Wireless-N Selectable-Band Access Point. The URL is 192.168.2.2/admin.cgi?action=main. The page title is "Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup". The left sidebar has a "Status and Statistics" section with "Radio Statistics" selected. The main content area displays various radio statistics:

Radio Statistics	
Refresh	
Packets Received:	727
Bytes Received:	122,964
Packets Receive Dropped:	0
Bytes Receive Dropped:	0
Fragments Received:	4
Multicast Frames Received:	725
Duplicate Frame Count:	7
FCS Error Count:	5,243,471
ACK Failure Count:	3
WEP Undecryptable Count:	0
Packets Transmitted:	149,300
Bytes Transmitted:	38,847,974
Packets Transmit Dropped:	0
Bytes Transmit Dropped:	0
Fragments Transmitted:	0
Multicast Frames Transmitted:	149,326
Failed Transmit Count:	0
Transmit Retry Count:	2
RTS Failure Count:	4,294,967,294
RTS Success Count:	2
Multiple Retry Count:	1
Frames Transmitted Count:	149,335

At the bottom of the page, it says "© 2012 Cisco Systems, Inc. All rights reserved."

Management Interface

The screenshot shows the Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup management interface. The left sidebar menu includes:

- Run Setup Wizard
- Status and Statistics
- Administration** (selected)
- System Settings
- User Accounts
- Time Settings
- Log Settings
- Email Alert
- HTTP/HTTPS Service** (selected)
- Management Access Control
- Upgrade Firmware
- Download/Backup Configuration File
- Configuration Files Properties
- Copy/Save Configuration
- Reboot
- Discovery - Bonjour
- Packet Capture
- Support Information
- ▶ LAN
- ▶ Wireless
- ▶ System Security
- ▶ Client QoS
- ▶ SNMP
- ▶ Captive Portal
- ▶ Single Point Setup

The main content area displays the following configuration settings:

- HTTP Service**:
 - HTTP Server: Enable
 - HTTP Port: 80 (Range: 1025-65535, Default: 80)
 - Redirect HTTP to HTTPS:
- HTTPS Service**:
 - HTTPS Server: Enable
 - HTTPS Port: 443 (Range: 1025-65535, Default: 443)
- Generate SSL Certificate**:
 -
- SSL Certificate File Status**:
 - Certificate File Present: Yes
 - Certificate Expiration Date: Dec 26 20:00:03 2019 GMT

At the bottom left, it says "© 2012 Cisco Systems, Inc. All rights reserved."

WLAN Control Plane

- Protocols that provide *intelligence*
- Decisions about MAC addresses
- VLANs
- Dynamic RF (Radio Resource Management)
- Roaming and hand-offs
- Load Balancing
- Mesh and WDS Protocols

Control – VLANs

The screenshot shows the configuration interface for a Cisco WAP321 Wireless-N Selectable-Band Access Point. The left sidebar menu is expanded, showing options like Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN (selected), Port Settings, VLAN and IPv4 Address (selected), IPv6 Addresses, Wireless, System Security, Client QoS, SNMP, Captive Portal, and Single Point Setup. The main content area is titled "VLAN and IPv4 Address". It contains two sections: "Global Settings" and "IPv4 Settings". In "Global Settings", the MAC Address is listed as 18:E7:28:50:3E:A8, Untagged VLAN is set to Enable with ID 1, and Management VLAN ID is also set to 1. In "IPv4 Settings", the Connection Type is set to DHCP (radio button selected). The Static IP Address is set to 192.168.1.245, Subnet Mask is 255.255.255.0, and Default Gateway is 192.168.1.1. Domain Name Servers are set to Dynamic. The footer of the interface includes the copyright notice "© 2012 Cisco Systems, Inc. All rights reserved."

Control – Wireless Distribution

The screenshot shows the Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup interface. The left sidebar menu is visible, showing various configuration options under the Wireless category. The main content area is titled "WDS Bridge". It contains three sections for different WDS interfaces, each with fields for Spanning Tree Mode, Local MAC Address, WDS Interface, Remote MAC Address, and Encryption.

WDS Interface	Spanning Tree Mode	Local MAC Address	Remote MAC Address	Encryption
WDS Interface 1	<input checked="" type="checkbox"/> Enable	18:E7:28:50:3E:A8	(XXXXXXXXXXXXXX)	None
WDS Interface 2	<input type="checkbox"/> Enable		(XXXXXXXXXXXXXX)	None
WDS Interface 3	<input type="checkbox"/> Enable		(XXXXXXXXXXXXXX)	None

Control – QoS

The screenshot shows the Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup interface. The left sidebar menu is visible, showing various configuration options like Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN, Wireless (selected), Radio, Rogue AP Detection, Networks, Scheduler, Scheduler Association, Bandwidth Utilization, MAC Filtering, WDS Bridge, WorkGroup Bridge, QoS (selected), WPS Setup, WPS Process, System Security, Client QoS, SNMP, Captive Portal, and Single Point Setup. The main content area is titled 'QoS' and displays two tables for configuring Quality of Service.

EDCA(Enhanced Distributed Channel Access)Template: Optimized for Voice ▾

Queue	Arbitration Inter-Frame Space	Minimum Contention Window	Maximum Contention Window	Maximum Burst
Data 0 (Voice)	1	3 ▾	15 ▾	0
Data 1 (Video)	3	7 ▾	31 ▾	0
Data 2 (Best Effort)	3	15 ▾	63 ▾	0
Data 3 (Background)	10	63 ▾	1023 ▾	0

Wi-Fi Multimedia (WMM): Enable

Queue	Arbitration Inter-Frame Space	Minimum Contention Window	Maximum Contention Window	TXOP Limit
Data 0 (Voice)	2	3 ▾	15 ▾	0
Data 1 (Video)	5	15 ▾	63 ▾	0

© 2012 Cisco Systems, Inc. All rights reserved.

WLAN Data Plane

- *Physical location* where user data is forwarded
 - Can be the AP or a WLAN Controller
 - If it's at the AP, then it is at the “*edge*”

WLAN Architectures

- Three main WLAN Architectures
- Autonomous: traditional APs
- Centralized: WLAN Controller APs
- Distributed: cooperative APs

Autonomous Architecture

- Autonomous APs known as fat or standalone access points
- All three logical planes at the AP
- At least two physical interfaces
 - Radio for 802.11
 - Ethernet RJ45
 - Bridged Virtual Interface (BVI)
 - Translational bridge (802.11 and 802.3)



Autonomous access points can be of SOHO or Enterprise type. Enterprise APs offer more robust features.

Autonomous Architecture

- No centralized management
- *Network Management Service* (NMS)
 - Manage and monitor many devices
 - RF spectrum management
 - Management plane
 - SNMP to monitor and manage
 - Hardware or virtual appliance



What are the differences in SNMP versions?

Centralized Architecture

- Autonomous APs replaced by controller based
 - Thin or lightweight access points
- All 3 planes moved to the **WLAN controller**
 - “Wireless switches”
 - Multilayer switch (Layer 2 and 3)
 - Numerous capabilities

WLAN Controllers

- AP management through Control and Provisioning of Wireless APs (CAPWAP)
- Traffic Tunneling of user traffic from AP to WLAN controller using *Generic Routing Encapsulation (GRE)*
- Access Point and WLAN Profiles
- VLANs with 802.1Q tagging
- VPN concentrators
- Captive Portals



GRE is used because the AP don't do anything in this architecture. GRE encapsulates 802.11 frames in IP packets and sent to the WLAN controller.

AP profiles are configurations for single or groups of APs

WLAN Profiles based on SSID and what clients connect to them; Role based access controls to the user

WLAN Controllers

- Failover and load balancing
- WIDS and WIPS integration
- RF spectrum management
- Firewalls and access controls
- Power over Ethernet (PoE)
- *Split MAC*: some of the 802.11 management and control are left up the controller based AP and not sent to the WLAN controller

WLAN Controller Data Forwarding

- 2 types of controller data forwarding models
- *Centralized*: All data is handled by WLAN controller
- *Distributed*: Some forwarding is handled at edge when centralized resource aren't needed
 - AP decides how and where to forward
 - Avoid high latency links (VoWiFi)
 - Vendors moving to Distributed



Why would the push be to distributed over centralized? Think about 802.11n and 802.11ac

Distributed Architecture

- *Cooperative* access points where access points can communicate with each other
- WLAN controller is absent
- Each AP is responsible for data forwarding decisions of user traffic
- Network Management Server handles configuration and monitoring
 - On-site or cloud-based
- Scalability is done by adding APs



Distributed architecture lends itself to easy scalability. Only APs have to be deployed as the company grows. In a centralized architecture, WLAN controller might have to be deployed and they are expensive.

Distributed – Single Point Setup

The screenshot shows the configuration interface for a Cisco WAP321 access point. The left sidebar menu includes options like Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN, Wireless, System Security, Client QoS, SNMP, Captive Portal, and Single Point Setup. The Single Point Setup option is currently selected and expanded, showing sub-options for Access Points, Sessions, Channel Management, and Wireless Neighborhood. The main content area displays the 'Access Points' section, which states that Single Point Setup allows WAP321-A-K9 access points to propagate settings. It shows that Single Point Setup is Enabled and lists one access point detected in the cluster: 'ciscosb-cluster'. A table provides details for this access point:

Location	MAC Address	IP Address
No Default	18:E7:28:50:3E:A8	192.168.2.2

Below the table, there are fields to enter the location of the AP ('Location: No Default') and the name of the cluster ('Cluster Name: ciscosb-cluster'). A radio button indicates the clustering IP version ('Clustering IP Version: IPv6 (radio button) IPv4'). A 'Disable Single Point Setup' button is also present. On the right side of the interface, there is a sidebar titled 'Clustered' showing a network icon and the text '1 Access Points'.

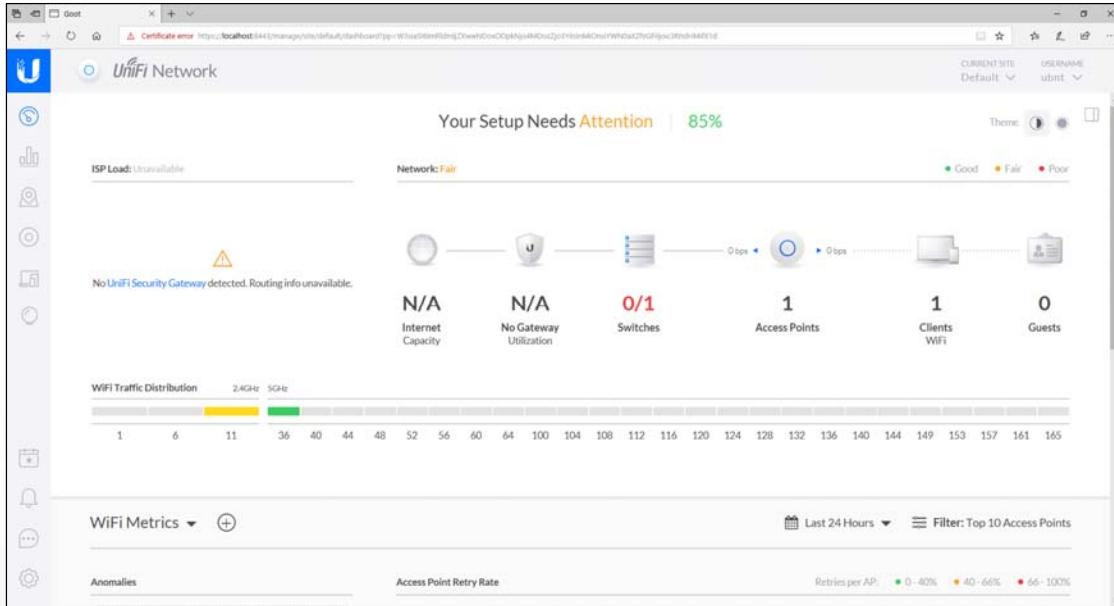
This is Cisco's version of Distributed/Cooperative Access Points. A single access point can propagate settings to other Single Point Setup access points.

Distributed Architecture

The screenshot shows the Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup interface. The main title is "cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup". On the left, there's a navigation menu with items like Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN, Wireless, System Security, Client QoS, SNMP, Captive Portal, and Single Point Setup (which is currently selected). Below the menu is a "Wireless Neighborhood" section with a "Neighbors (21)" table. The table lists various access points with their signal strength bars. A "Single Point Setup" section at the top right shows the IP address 192.168.2.2 and MAC address 18:E7:28:50:3E:A8. A sidebar on the right indicates "1 Access Points" and "Clustered". The bottom of the screen shows a copyright notice: "© 2012 Cisco Systems, Inc. All rights reserved."

Single Point Setup with Neighbor Listing.

Distributed – Ubiquiti UniFi

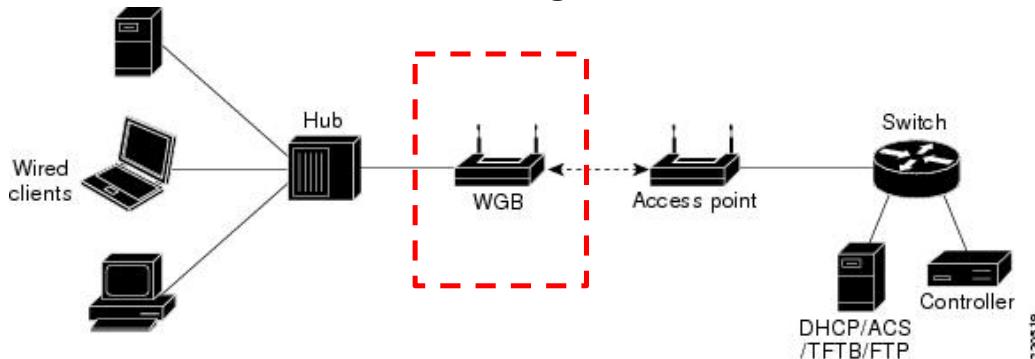


Special WLANs

- Wireless Workgroup Bridge
- Wireless Bridge
- Enterprise WLAN Routers
- WLAN Mesh Access Points
- WLAN Arrays
- Virtual Access Points

Wireless Workgroup Bridge

- Wireless connectivity for wired devices
- The WGB joins a BSS as a client
- Vendor specified number of wired clients
 - Universal client for a single wired device



230519

Workgroup Bridge

The screenshot shows the Cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup interface. The main title bar reads "cisco WAP321 Wireless-N Selectable-Band Access Point with Single Point Setup". The left sidebar menu includes options like Getting Started, Run Setup Wizard, Status and Statistics, Administration, LAN, Wireless (selected), Radio, Rogue AP Detection, Networks, Scheduler, Scheduler Association, Bandwidth Utilization, MAC Filtering, WDS Bridge, WorkGroup Bridge (selected), QoS, WPS Setup, WPS Process, System Security, Client QoS, SNMP, Captive Portal, and Single Point Setup. The main content area is titled "WorkGroup Bridge" and contains two sections: "Infrastructure Client Interface" and "Access Point Interface". In the Infrastructure Client Interface, "WorkGroup Bridge Mode" is set to "Enable". The SSID is "TC-Visitors", Security is "WPA Personal", and VLAN ID is "1". Connection Status is "Disconnected". In the Access Point Interface, Status is "Enable", SSID is "Access Point SSID", Security is "None", and MAC Filtering is "Disabled". The bottom of the page includes a copyright notice: "© 2012 Cisco Systems, Inc. All rights reserved."

Wireless LAN Bridge

- Connectivity between two or more wired networks; no connectivity for wireless clients
- Indoor and outdoors
- Can be used for link redundancy
- *Root and nonroot* (parent/child)
- Point to point (PtP)
- Point to Multipoint (PtMP)
- Not a repeater



PtP only two wired networks (one has to be the root, the other nonroot)

PtMP connects several wired networks; root bridge is centralized and non root bridges connect to the root bridge

There can only be one root

Repeaters add additional contention

Outdoor Bridge Considerations

- Fresnel zone (3 Dimensional)
- Earth bulge, FSPL, link budget, fade margin
- Local Regulatory Domain restrictions
 - Max IR and EIRP
- ACK timeouts for long distance
 - Can be adjusted to compensate for long hauls
- Omnidirectional antennas (squashed donut)



Curvature of the earth beyond 7 miles.

Fresnel Zone and FSPL based on frequency and distance.

IR: Intentional Radiator is up to but not including the antenna.

EIRP: Power measured at the antenna.

Point to Point (PtP)



UMBC | CYBERSECURITY
Training Centers ACADEMY

Point to Multipoint (PtMP)



UMBC | CYBERSECURITY
Training Centers ACADEMY

SOHO Access Point

- Also known as “Wireless Routers”
- Support standards-based security
- DHCP, DNS, and basic services
- Comply with IEEE standards
- Often “Wi-Fi Certified”
- Static TX power
- Bridge and repeater functions as options
- Some are physically configurable and modified



Removeable antennas and Wireless cards. USB ports and so on.

SOHO Wireless Router



UMBC | CYBERSECURITY
Training Centers ACADEMY

Photo from linksys.com

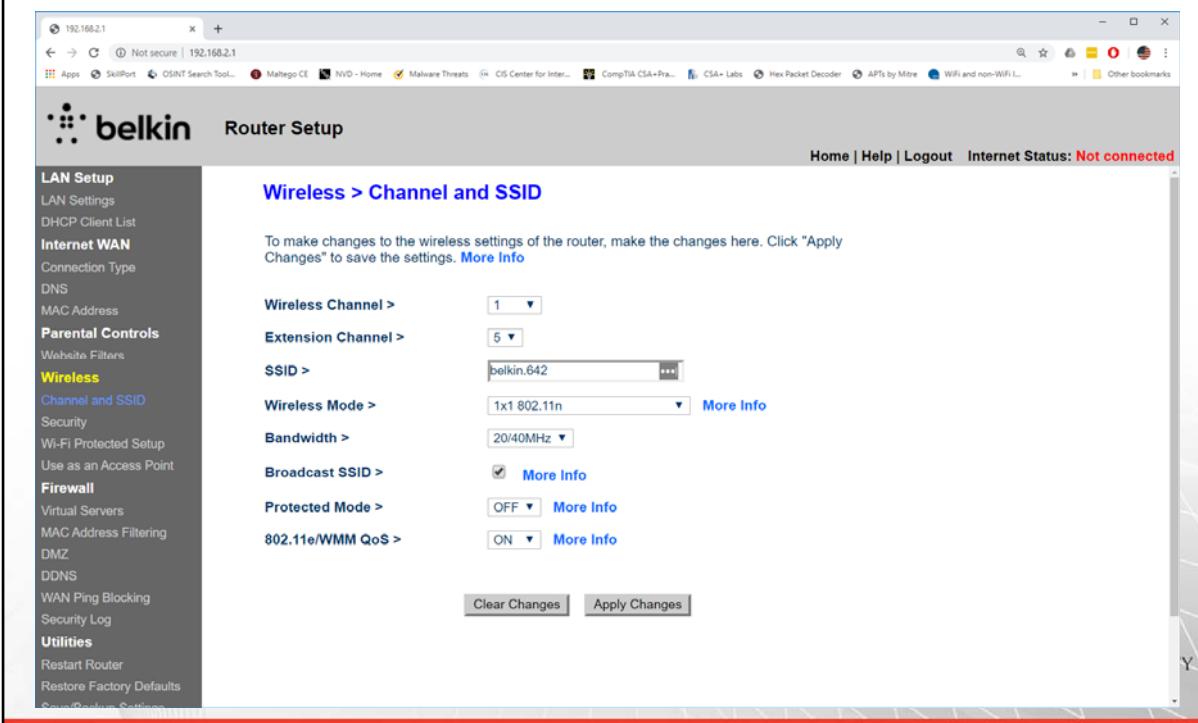
SOHO Wireless Router

The screenshot shows a web-based interface for a Belkin SOHO Wireless Router. The title bar reads "belkin Router Setup". The main content area is titled "Status". On the left, a sidebar lists various configuration categories: LAN Setup, Internet WAN, Parental Controls, WebSite Filters, Wireless, Firewall, Utilities, and a "Restore Factory Defaults" link. The "Wireless" section is currently selected. The main status area contains several tables with router information:

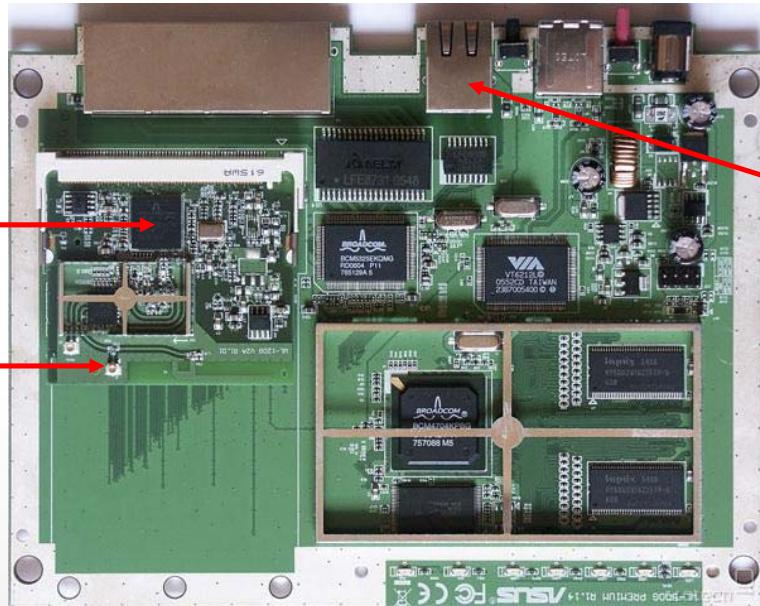
- Language**: Current Language: English; Available Languages: English, Français, Deutsch, Español, Nederlands, Italiano, 简体中文, 繁體中文, 한국어.
- Version Info**: Firmware Version: 4.00.07 (Dec 19 2012 13:48:00); Boot Version: 0.07; Hardware: F9K1001v4 (01); Serial No.: 121312GB404178.
- LAN Settings**: LAN/WLAN MAC: EC:1A:59:8E:26:42; IP Address: 192.168.2.1; Subnet Mask: 255.255.255.0; DHCP Server: Enabled (2 LAN, 1 WLAN Clients).
- Internet Settings**: WAN MAC Address: EC:1A:59:8E:26:43; Connection Type: Dynamic; WAN IP: 0.0.0.0; Subnet Mask: 0.0.0.0; Default Gateway: 0.0.0.0; DNS Address: 0.0.0.0.
- Features**: Firewall Settings: Enabled; SSID: belkin.642; Security: WPA/WPA2-Personal (PSK); UPnP: Enabled; Remote Management: Disabled; WPS: Enabled.

At the top right of the status area, it says "Internet Status: Not connected". The browser's address bar shows "192.168.2.1" and indicates "Not secure". The title bar also shows "192.168.2.1".

SOHO Wireless Router



SOHO Access Point



UMBC | CYBERSECURITY
Training Centers ACADEMY

ASUS WL-500g Premium

Removable Wireless Card

MMCx Antenna connector

USB port

Enterprise WLAN Router

- Remote office wired and wireless solution
- WLAN routers have routed interfaces
- Using VPN tunnels
- Same SSIDs, VLANs, and security
- What's the difference between SOHO?
 - Better and more reliable features \$\$\$
 - VPN client, PoE, PAT and NAT, Cellular backhaul



IEEE standards compliant

Wi-Fi Certifications

Antennas are removable

Adjustable Tx power

Support for advanced security such as RADIUS

Enterprise WLAN Router



Business class AP with VPN

TPLink Wireless N router with VPN

Multiple SSIS and guest WLAN

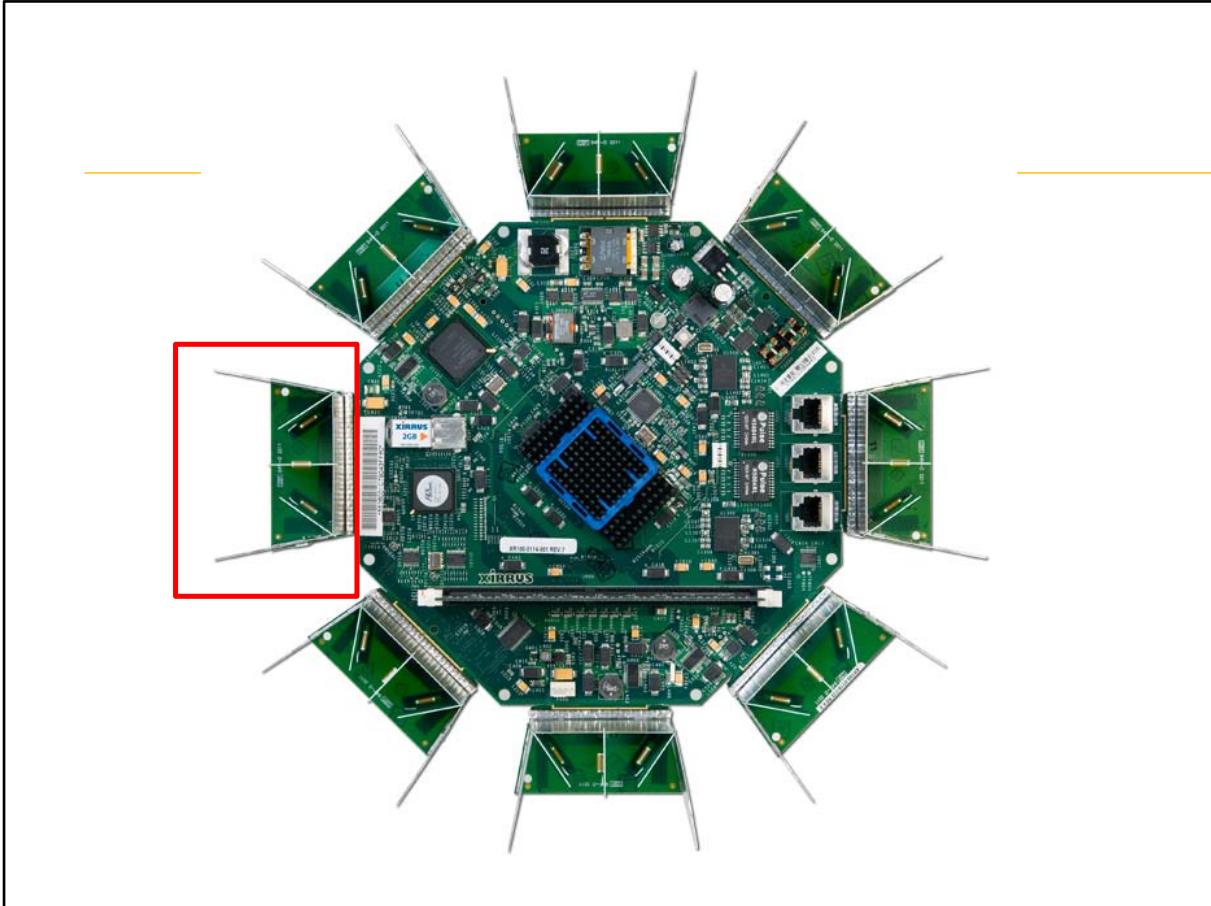
Picture from tp-link.com

WLAN Mesh Access Point

- APs communicate with each other wirelessly using Layer 2 “routing” protocols
- Updates routes based on proprietary protocols: RSSI, data rates, hop counts, etc
- Originally repeater based
- Dual band most common
 - 2.4 GHz for clients
 - 5 GHz for backhaul

WLAN Array

- Multiple access points and a single WLAN controller in a single device
- 4-16 access points; one as a WIDS sensor
- Sectorized antennas are used for each AP
- High density environments
- 360 degree coverage



Red Box depicts the antenna

Picture from Xirrus.com

Virtual Access Point

- Multiple access points using a single BSSID
- Clients may be roaming across physical APs
 - Zero handoff latency
- All APs on same channel and contention is handled by a WLAN Controller
 - *Single Channel Architecture*

Summary

- WLAN Client Devices and Form Factors
- Logical Planes of Operation
- WLAN Architecture
 - Autonomous, Centralized, Distributed
- Special WLAN Infrastructure
 - Bridges, Enterprise WLAN Routers, Mesh APs, Cool Arrays, and Virtual APs

QUESTIONS??



802.11 MAC Architecture

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Packets, Frames, and Bits
- Data Link Layer
- Physical Layer
- Interoperability
- Frame Types and Information
- Protection Mechanisms
- Power Management

Packets, Frames, and Bits

- Layer 4-7 data is packaged into *packets* at Layer 3, network layer
- Layer 3-7 data is wrapped up into a *frame* at Layer 2, data link layer
- At the physical layer data is transmitted as *bits*
- How does the upper layer data move down to the data link and physical layers in 802.11

Data Link Layer MSDU

- Split into the Logical Link and MAC sublayers
- MAC sublayer is where we focus
- MAC Service Data Unit (**MSDU**) is the Logical Link data pushed down to the MAC sublayer
 - Data payload (IP packet + LLC data)
 - Only 802.11 data frames have MSDU
 - Max size of **2,304 bytes**
 - With 802.11n, **Aggregate-MSDU is 3,839 bytes**

MPDU

- MAC Protocol Data Unit
- MSDU + MAC header information
- 802.11 frame with 3 components
 - MAC header
 - Frame control info, duration, MAC addressing, etc
 - Frame body
 - Variable in size; different types; encrypted MSDU
 - Frame check sequence (FCS)
 - 32-bit cyclic redundancy check (CRC)

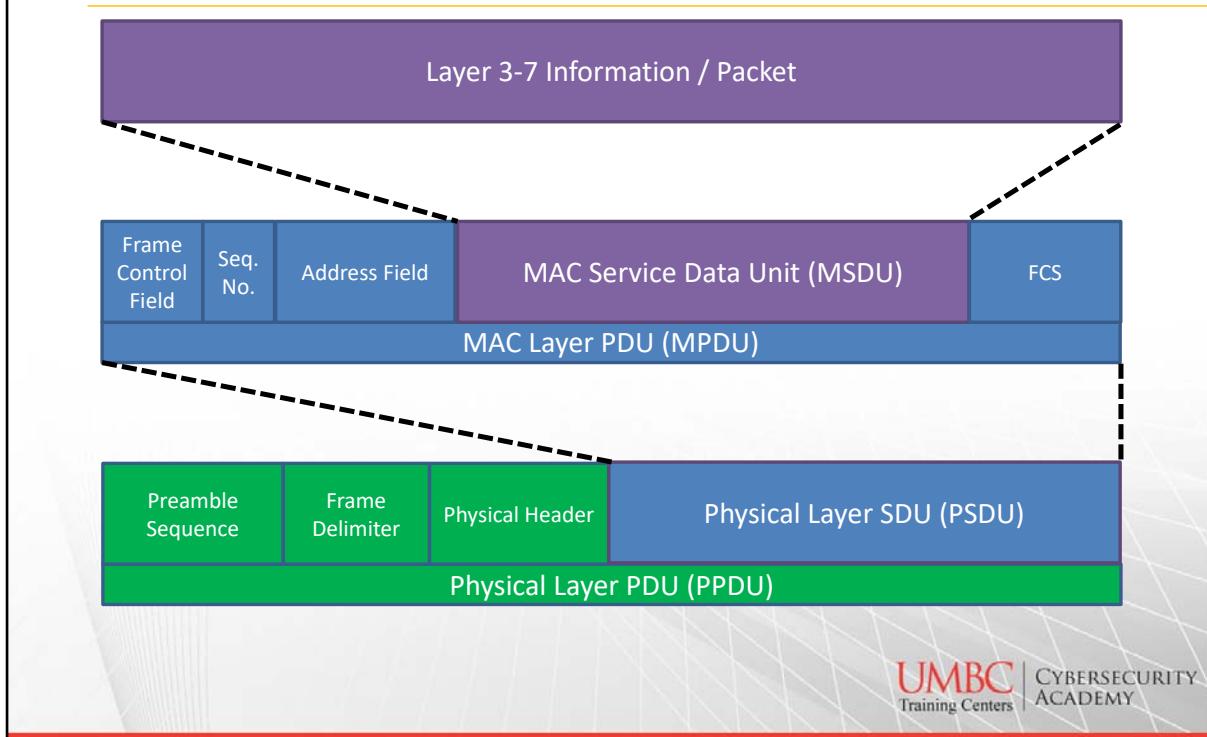
Physical Layer

- Divided into two sublayers
- Physical Layer Convergence Protocol (PLCP)
 - Prepares the frame for transmission
 - Creates the PLCP Protocol Data Unit (PPDU)
- Physical Medium Dependent (PMD)
 - Modulates and transmits the data as bits

PLCP

- PLCP Service Data Unit (PSDU)
 - PSDU is the MAC's MPDU and is the payload for the PPDU
- PLCP Protocol Data Unit (PPDU) wraps PSDU
 - Preamble for synchronization
 - Frame delimiter
 - Physical header
 - Hands off to PMD

Putting It All Together



UMBC | CYBERSECURITY
Training Centers ACADEMY

Interoperability

- Integration service (IS) delivers the MSDU payloads between 802.11 LAN and non-802.11 LANs through a *portal*
- Frame size is the difference
 - 802.3 payloads can be 1,500 or 1,504 bytes
 - 802.11 MSDU payloads of 2,304 bytes
 - IP limits of 1,500 bytes
 - TCP/UDP limits of 576 and 512 bytes



1500 or 1504 depending on VLAN tagging information
RFC 791

Interoperability

- MAC addresses
 - Individual address (unicast)
 - Group addresses (multicast & broadcast)
- Up to 4 MAC addresses in a 802.11 frame
 - **Distribution Status (DS)**
 - Source (SA): original sending station
 - Destination (DA): final destination, server, station
 - Transmitter (TA): station that is transmitting
 - Receiver (RA): station intended to receive frame

MAC Addresses and DS Status

- Two bits in the Flags section identify how the addresses will be used
- **Fourth MAC is used in a WDS configuration**
- Ad-hoc networks do not DS addresses

To DS	From DS	Address1	Address2	Address3	Address4
0	0	DA	SA	BSSID	X
0	1	DA	BSSID	SA	X
1	0	BSSID	SA	DA	X
1	1	RA	TA	DA	SA (WDS)

MAC Addresses and DS Status

```
▼ IEEE 802.11 Data, Flags: .p....F.
  Type/Subtype: Data (0x0020)
  ▼ Frame Control Field: 0x0842
    .... .00 = Version: 0
    .... 10.. = Type: Data frame (2)
    0000 .... = Subtype: 0
  ▼ Flags: 0x42
    .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
    .... .0.. = More Fragments: This is the last fragment
    .... 0.... = Retry: Frame is not being retransmitted
    ..0. .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .1.. .... = Protected flag: Data is protected
    0.... .... = Order flag: Not strictly ordered
    .000 0000 0000 0000 = Duration: 0 microseconds
  Receiver address: IPv4mcast_12 (01:00:5e:00:00:12)
  Transmitter address: CiscoMer_79:a9:a2 (00:18:0a:79:a9:a2)
  Destination address: IPv4mcast_12 (01:00:5e:00:00:12)
  Source address: CiscoMer_8e:70:48 (cc:03:d9:8e:70:48)
  BSS Id: CiscoMer_79:a9:a2 (00:18:0a:79:a9:a2)
  STA address: IPv4mcast_12 (01:00:5e:00:00:12)
```

802.11 Frame Types

- Management
 - Join and leave the BSS
 - No upper layer information
- Control
 - Assist with the delivery of data
 - Clear/acquire the channel, ACKs
- Data
 - Actual data from upper layers
 - May have no data, but MAC control purpose
 - MSDU is encrypted



No data in a data frame serves some MAC control purpose but since it is empty, nothing to encrypt

There are some Wireshark filters to sort through frame types and subtypes in the Wireless supplemental.

Beacons

- Management frame sub-type
- APs send out beacons
- Clients in an IBSS transmit beacons
- Timestamps for clock synchronization
- Used for all information about the parameters of the BSS before joining
- ~10 times per second



Beacons contain: time stamps, SS parameters, Channel information, data rates, Service set capabilities, SSID, Traffic indication maps, QoS capabilities, RSN capabilities, and vendor specific information.

Beacon Frame – BSS

- Wireshark filter `wlan.fc.subtype == 8`

```
> Frame 7178: 225 bytes on wire (1800 bits), 225 bytes captured (1800 bits)
> IEEE 802.11 Beacon frame, Flags: .....
└ IEEE 802.11 wireless LAN
  └ Fixed parameters (12 bytes)
    └ Timestamp: 3035878707584
      └ Beacon Interval: 0.102400 [Seconds]
    └ Capabilities Information: 0x0431
  └ Tagged parameters (189 bytes)
    └ Tag: SSID parameter set: HoneyBaked
    └ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    └ Tag: DS Parameter set: Current Channel: 11
    └ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    └ Tag: ERP Information
    └ Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    └ Tag: QBSS Load Element 802.11e CCA Version
    └ Tag: HT Capabilities (802.11n D1.10)
    └ Tag: HT Information (802.11n D1.10)
    └ Tag: Extended Capabilities (8 octets)
    └ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
    └ Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
    └ Tag: Vendor Specific: Ubiquiti Networks Inc.
    └ Tag: RSN Information
```

Advertised: SSID, supported rates, Channel, TIM, vendor specific information

Beacon Frame – Not a BSS

```
> Frame 7104: 144 bytes on wire (1152 bits), 144 bytes captured (1152 bits)
> IEEE 802.11 Beacon frame, Flags: .....
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
    Timestamp: 412056068716
    Beacon Interval: 0.102400 [Seconds]
    > Capabilities Information: 0x0402
  ▼ Tagged parameters (108 bytes)
    > Tag: SSID parameter set: SETUP
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 11
    > Tag: IBSS Parameter set: ATIM window 0x0
    > Tag: ERP Information
    > Tag: ERP Information
    > Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Vendor Specific: Broadcom
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
```



What is this?

How Do Clients Find a BSS?

- Passive Scanning
 - Listening for beacons from AP
 - Same SSID, then RSSI is compared
 - In an IBSS, clients take turns beaconing
- Active Scanning (probing the wire)
 - **Probe requests** (directed or null)
 - AP responds with a **probe response**
 - Associated clients still probe off-channel



Passive scanning listening to beacons (beacons are only sent on the support channel from the AP)

Active scanning sends out on all channels from the client

Directed probe request has the SSID set, the AP with that SSID responds with the capabilities just like what's found in a beacon frame

Null probe request: hearing APs should reply

Off channel probing is used if a client needs to roam

Probe Request – Null

- Broadcast with SSID length of zero (0)

```
> Frame 813: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
> IEEE 802.11 Probe Request, Flags: .....
└ IEEE 802.11 wireless LAN
    └ Tagged parameters (98 bytes)
        └ Tag: SSID parameter set: Wildcard SSID
            └ Tag Number: SSID parameter set (0)
            └ Tag length: 0
            └ SSID:
                └ Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
                └ Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
                └ Tag: DS Parameter set: Current Channel: 1
                └ Tag: HT Capabilities (802.11n D1.10)
                └ Tag: Extended Capabilities (4 octets)
                └ Tag: Interworking
                └ Tag: Vendor Specific: Apple, Inc.
                └ Tag: Vendor Specific: Microsoft Corp.: Unknown 8
                └ Tag: Vendor Specific: Broadcom
```

Probe Request – Directed

- Wireshark filter `wlan.fc.subtype == 4`

```
▼ Frame 1008: 65 bytes on wire (520 bits), 65 bytes captured (520 bits)
  Encapsulation type: IEEE 802.11 Wireless LAN (20)
  Arrival Time: Apr  3, 2018 06:05:01.330746000 Eastern Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1522749901.330746000 seconds
  [Time delta from previous captured frame: 0.522298000 seconds]
  [Time delta from previous displayed frame: 7.873544000 seconds]
  [Time since reference or first frame: 51.813116000 seconds]
  Frame Number: 1008
  Frame Length: 65 bytes (520 bits)
  Capture Length: 65 bytes (520 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: wlan]
  > IEEE 802.11 Probe Request, Flags: .....
  ▼ IEEE 802.11 wireless LAN
    ▼ Tagged parameters (41 bytes)
      > Tag: SSID parameter set: gogoinflight
      > Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
      > Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
      > Tag: Vendor Specific: Broadcom
```

SECURITY
EMY

Probe Response

wlan.fc.subtype == 4

```
> IEEE 802.11 Probe Response, Flags: ....R...
> IEEE 802.11 wireless LAN
> Fixed parameters (12 bytes)
> Tagged parameters (302 bytes)
> Tag: SSID parameter set: Classic Nails
> Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
> Tag: DS Parameter set: Current Channel: 1
> Tag: Country Information: Country Code US, Environment Any
> Tag: ERP Information
> Tag: ERP Information
> Tag: RSN Information
> Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
> Tag: QBSS Load Element 802.11e CCA Version
> Tag: HT Capabilities (802.11n D1.10)
> Tag: HT Information (802.11n D1.10)
> Tag: Extended Capabilities (3 octets)
> Tag: Vendor Specific: Microsoft Corp.: WPS
> Tag: Vendor Specific: Broadcom
```

0040	07 06 55 55 20 01 0b 1e	2a 01 00 2f 01 00 30 14	3 dc 14 ed bb ff 09 92	P : -v?... C
0050	01 00 00 0f ac 04 01 00	00 0f ac 04 01 00 00 0f	c 0b a5 ec 00 00 00 00@i <.....
0060	ac 02 0c 00 32 04 0c 12	18 60 0b 05 05 00 3a 00	1 73 73 69 63 20 4e 61	d.....Cl assic Na
0070	00 2d 1a 3c 18 1f ff ff	00 00 00 00 00 00 00 00	6 24 30 48 6c 03 01 01	ils..... \$OHL...
0080	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	3d 16 01	..US ... *.../...0.
0090	00 15 00 00 00 00 00 00	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
00a0	00 00 00 00 00 7f 03 00	00 08 dd 81 00 50 f2 04	00a0P..
00b0	10 4a 00 01 10 10 44 00	01 02 10 3b 00 01 03 10	00b0	-J....D.;
00c0	47 00 10 00 00 00 00 00	00 00 00 00 00 00 00 00	00c0	G..... .
00d0	00 00 00 10 21 00 04 50	61 63 65 10 23 00 06 35	00d0I..P ace.#..5
00e0	32 36 38 41 43 10 24 00	06 31 32 33 34 35 36 10	00e0	268AC-\$.. -123456-
00f0	42 00 04 31 32 33 34 10	54 00 08 00 06 00 50 f2	00f0	B..1234. T.....P.
0100	04 00 01 10 11 00 11 50	61 63 65 20 41 63 63 65	0100P ace Acce
0110	73 73 20 50 6f 69 6e 74	10 08 00 02 20 0c 10 3c	0110	ss Point<
0120	00 01 01 10 49 00 06 00	37 2a 00 01 20 dd 09 00	0120I... 7*... .
0130	10 18 02 05 00 0c 00 00	dd 18 00 50 f2 02 01 01	0130P....

Probe Responses can give up more information than should be advertised.

Authentication

- First of two steps to connect to BSS
- Devices must authenticate to communicate
- Validation to the AP or peer client in a IBSS
- Two methods
 - Open System Authentication (OSA)
 - Shared Key

Open System Authentication

- Authentication without any real validation
- Exchange of niceties
- Never fails, but that may be as far as you get
- Used with more advanced network security implementations (WPA, WPA2, 802.1X/EAP)

Shared Key Authentication

- Deprecated with WEP
- 4-way authentication exchange
 - Client sends a request
 - AP responds with cleartext challenge
 - Client encrypts challenge with WEP key
 - AP decrypts the response with WEP key
- Same WEP key is used to later “encrypt” data frames



Just know that it is an authentication method that isn't used but is here for your edification.

Association

- Second step in connecting to a BSS
- Client that associates is a member of the BSS
- Client requests association
- AP responds by granting or denying
 - If granted, the client also gets an *Association ID (AID)* which will be used later
 - AID is a unique ID given to every associated client
- Associate clients can communicate layers 3-7

Association Request

- Wireshark filter `wlan.fc.type_subtype == 0`

```
> Frame 6305: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
> IEEE 802.11 Association Request, Flags: .....
< IEEE 802.11 wireless LAN
  < Fixed parameters (4 bytes)
    > Capabilities Information: 0x0431
      Listen Interval: 0x0001
  < Tagged parameters (88 bytes)
    > Tag: SSID parameter set: TC-Visitors
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6(B), 9, 12(B), 18, [Mbit/sec]
    > Tag: Extended Supported Rates 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: RSN Information
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Information Element
```

Association Response

- Wireshark filter `wlan.fc.type_subtype == 1`

```
> Frame 6307: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits)
> IEEE 802.11 Association Response, Flags: .....
< IEEE 802.11 wireless LAN
  < Fixed parameters (6 bytes)
    > Capabilities Information: 0x0431
      Status code: Successful (0x0000)
      ..00 0000 0000 1001 = Association ID: 0x0009
  < Tagged parameters (104 bytes)
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 6, 9, 11(B), 12, 18, [Mbit/sec]
    > Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Authentication and Association States

- Authentication state: authenticated or not
- Association state: associated or not
- 3 possible combined states*
 - 1 unauthenticated and unassociated
 - 2 authenticated and unassociated
 - 3 authenticated and associated
 - *4 authenticated and associated with security mechanisms complete (PSK or 802.1X/EAP)

Rates

- *Basic* rates, basically what's mandatory
 - May be called required (6,12,24 Mbps with some)
 - Clients must be capable of these AP rates
- *Supported* rates
 - What's advertised by the AP
 - Clients don't have to support them

Roaming

- Transition to one AP from another
- *Decision to roam is on the client*
 - RSSI, noise levels, error-rates
- Clients are also probing for other APs
 - Clients can be authenticated to many APs, but only associated with one
- Handoffs to APs done directly or through a WLAN Controller



Decision to roam is on the client. Knowing this is great for MITM and Evil Twin attacks

Reassociation

- When a client roams to another AP
- Re-associating to the same SSID but different Basic Service Set as in an ESS
- Buffered data is sent from the previous AP to the new AP if necessary

Disassociation & Deauthentication

- Not a request `wlan.fc.type_subtype == 10`
- Can be from either AP or client station
- Cannot be refused, except in 802.11w when the MIC fails
- Deauthentication causes disassociation

```
> Frame 6608: 26 bytes on wire (208 bits), 26 bytes captured (208 bits)
> IEEE 802.11 Deauthentication, Flags: .....
`- IEEE 802.11 wireless LAN
   `- Fixed parameters (2 bytes)
      Reason code: IEEE 802.1X authentication failed (0x0017)
```

Acknowledgements

- Every unicast frame is followed by an ACK
- Delivery verification
- Control frame
- Only way to know if transmission and receipt was successful
- Transmitter address is copied into the Receiver address field and sent back in the ACK frame

Unicast Acknowledgment

```
▼ IEEE 802.11 Acknowledgement, Flags: .....
    Type/Subtype: Acknowledgement (0x001d)
    ▼ Frame Control Field: 0xd400
        .... .00 = Version: 0
        .... 01.. = Type: Control frame (1)
        1101 .... = Subtype: 13
    ▼ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is op
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0... .... = Protected flag: Data is not protected
        0.... .... = Order flag: Not strictly ordered
        .000 0000 0000 0000 = Duration: 0 microseconds
Receiver address: Apple_92:71:5d (98:b8:e3:92:71:5d)
```

Fragmentation

- Typically used in legacy 802.11 a/b/g
- Breaks the 802.11 frame into smaller pieces
 - Adds overhead
 - Followed by a SIFS and an ACK
- Large frames would need to be retransmitted, whereas only the fragment would be
- Frame aggregation in 802.11 n/ac



Frame aggregation is used in n and ac networks so fragmentation is less likely to be used

Protection Mechanisms

- Can be used when 802.11b and g are present
- G is accommodating B
 - G uses ERP and B uses DSSS (different language)
- 802.11b only: DSSS and HR-DSSS is only used
- 802.11g only: ERP-OFDM is only used (pure G)
- 802.11b/g: default of most g APs (mixed mode)
 - Support for DSSS, HR-DSSS, and ERP-OFDM
 - Radio communicate at their native transmission



In b only: data rates are 1, 2, 5.5, and 11 Mbps; b and g radios can communicate

In g only: only g radios can talk; n can but only at ERP-OFDM rates

Protected Mode (Mixed Mode)

- ERP stations can use higher rates
- G radios send out NAV distribution
 - RTS/CTS or CTS-to-self in B language
 - RTS/CTS or CTS-to-self sets duration ID
 - B radios can understand and set their NAV timers
- *NonERP present* bit is set by G access point
 - When AP gets an 802.11b client association
 - If AP hears another AP supported data rates
 - If AP hears a management frame with supported data rates of 802.11 or 802.11b data rates

Non ERP Present

```
□ IEEE 802.11 wireless LAN management frame
  □ Fixed parameters (12 bytes)
    Timestamp: 0x000001019df2a024
    Beacon Interval: 0.104448 [Seconds]
    □ Capabilities Information: 0x1431
  □ Tagged parameters (263 bytes)
    □ Tag: SSID parameter set: RAGNAR
    □ Tag: Supported Rates 12(B), 18, 24, 36, 48, 54, [Mbit/sec]
    □ Tag: DS Parameter set: Current Channel: 1
    □ Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    □ Tag: Country Information: Country Code US, Environment Any
    □ Tag: QBSS Load Element 802.11e CCA Version
    □ Tag: ERP Information
      Tag Number: ERP Information (42)
      Tag length: 1
    □ ERP Information: 0x00
      .... .0 = Non ERP Present: Not set
      .... ..0. = Use Protection: Not set
      .... .0.. = Barker Preamble Mode: Not set
      0000 0... = Reserved: 0x00
```

802.11n HT Protection Modes

- Mode 0: Greenfield with only HT radios
- Mode 1: HT Nonmember (nearby)
- Mode 2: HT 20 MHz Protection
- Mode 3: Non-HT mixed mode
 - Most common mode for legacy devices



Mode 1 with only HT stations but hears a non-HT client or AP on one of the channels in the 40 MHz channel space

Mode 2: when a 20 MHz only HT client associates; 40 MHz clients use protection to prevent 20 MHz-only clients from transmitting at same time

Mode 3: one or more non-HT clients associate to the BSS

RTS/CTS

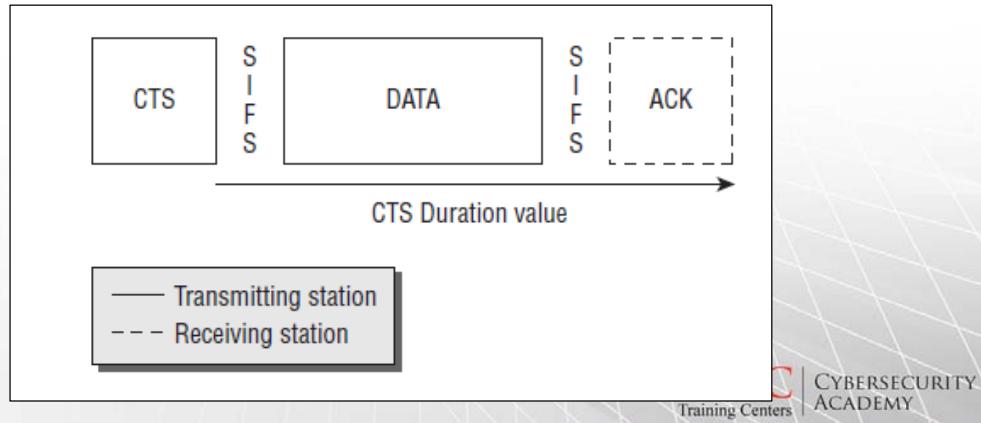
- Stations use virtual and physical carrier sense
 - NAV timers and Clear Channel Assessment
- What if you can't hear a station, is it safe?
- Hidden nodes and Protection mechanism
- RTS/CTS performs NAV distribution
 - RTS reset NAV timers to wait for CTS, Data, ACK
 - CTS reset the NAV timers again to Data and ACK



CTS is implemented after a number of consecutive non-ACKs from a station. For example a client in a hotel using the free Wifi that sends data but doesn't get the ACK back not just once but several in a row. The device will then go to RTS.

CTS-to-Self

- Protection mechanism in mixed mode
- Preferred over RTS/CTS due to overhead
- CTS-to-Self in the 802.11b DSSS language



Data Frame

- Simple data frame has MSDU data
- Should be encrypted
- *Null function frames* are sent to the AP to inform it of Power Save status changes
 - Power Management bit is set or not

```
▼ Flags: 0x11
..... .01 = DS status: Frame from STA to DS via an AP (To DS: 1 F
..... .0.. = More Fragments: This is the last fragment
..... 0... = Retry: Frame is not being retransmitted
...1 .... = PWR MGT: STA will go to sleep
..0. .... = More Data: No data buffered
.0... .... = Protected flag: Data is not protected
0.... .... = Order flag: Not strictly ordered
```

Power Management

- Legacy power management modes
 - Active and Power Save mode
- Active mode (continuous aware mode)
 - No battery conservation
 - Station is ready to receive and transmit
- Power Save mode
 - Radio takes a nap
 - Power management bit is set to 1

Entering PS Mode

- Initiated by the client station when enabled or typically on battery power, otherwise AM
- Client sends a null data frame to AP
 - Power management bit set to 1
- Dozes and wakes periodically for beacon
- AP buffers client station data

Power Management (TIM)

- Traffic Indication Map (TIM)
 - Remember the AID?
- Data is buffered at AP for napping clients
- TIM is in the beacon
 - Which clients have buffered data at the AP
- When the nap is over, client checks for its AID in the beacon TIM
- PS-Poll is sent to the AP if AID is present
- More Data bit is set if more buffered data is there

Power Management (DTIM & ATIM)

- If TIM wasn't enough
- Delivery Traffic Indication Map for broadcast and multicast traffic in BSS
- DTIMs are also sent in beacons
- Announcement TIM (ATIM) is used in an IBSS
 - Ad-hoc clients only
 - Notify each other of buffered data

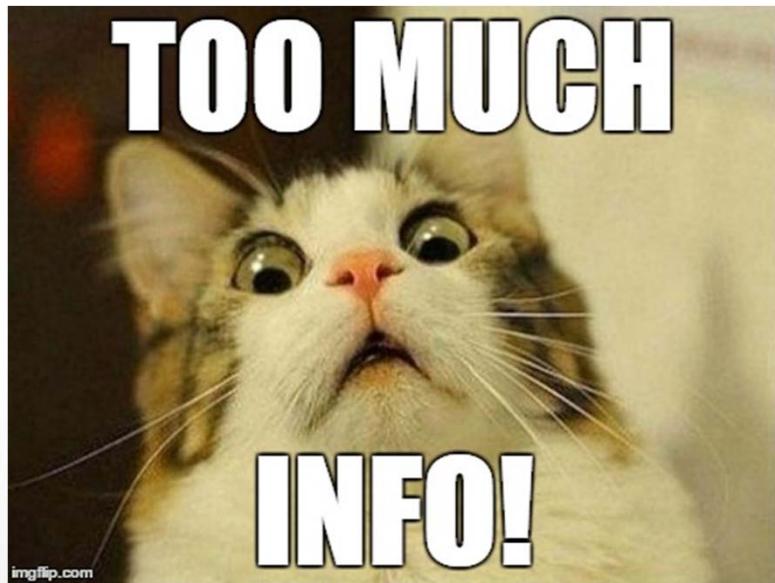
Automatic PS Delivery

- Result of 802.11e amendment
- The AP sends a frame to the device to wake
- “Hey, you have data!”
- QoS amendment targets voice and video latency sensitive devices

802.11n Power Management

- Spatial Multiplexing Power Save
 - MIMO device can shut down all but one radio
- Power Save Multi-Poll (PSMP)
 - Extension of APSD under 802.11e

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

Summary

- Packets, Frames, and Bits
- Data Link Layer
- Physical Layer
- Interoperability
- Frame Types and Their Information
- Protection Mechanisms
- Power Management

Security Infrastructure

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Planes
- WLAN Architectures
- VPN Wireless Security
- Infrastructure Management

Integration Service

- Frame format transfer from 802.11 to 802.3 and vice versa
- Removes the 802.11 MSDU encapsulation and repackage into an Ethernet frame
- The portal is the AP or WLAN controller that does the Integration Service

Distribution System

- We've already heard about the DS
- The connection between APs in an ESS
- **Medium** is the physical, e.g. Ethernet cabling
- **Service** is the intelligence that makes the decision where to push the frames

Planes of Operation

- What happens where in the 802.11 network
- Logically separated into
 - Management Plane
 - Control Plane
 - Data Plane
- Varies from BSS to ESS and SOHO to Enterprise
- All three can be spread across multiple devices or all integrated into one **depending on WLAN Architecture**

Management Plane

- Network administration and monitoring
- Configuration of the WLAN
- Updates and firmware upgrades
- Statistics reporting
- Site and individual AP settings through software user interface



Configs include SSID, channel, security settings, power.

Management Plane – Site

The screenshot shows the UniFi Network Management Plane interface, specifically the 'Site' configuration page. The left sidebar lists various settings categories: Site, Wireless Networks, Networks, Routing & Firewall, Threat Management (BETA), DPI, Guest Control, Profiles, Services, Admins, User Groups, Controller, User Interface (BETA), Notifications, and Cloud Access. The main content area is titled 'Site' and contains three sections: 'SITE CONFIGURATION', 'LED AND SCREEN SETTINGS', and 'SERVICES'. In 'SITE CONFIGURATION', the 'Site Name' is set to 'Default', 'Country or Territory' is 'United States', and 'Timezone' is '(UTC-04:00) New York'. In 'LED AND SCREEN SETTINGS', 'Enable status LED / Screen' is checked and set to 80% brightness. 'Enable Rack Multi-Screen Synchronization' is also checked. In 'SERVICES', 'Advanced Features' and 'Automatic Upgrades' are unchecked, while 'Enable alert emails' is checked. A 'Speed Test' section shows a speed of 20 minutes with 'LAST RESUME' highlighted. The bottom right corner features the UMBC Cybersecurity Academy logo.

Management Plane – Site

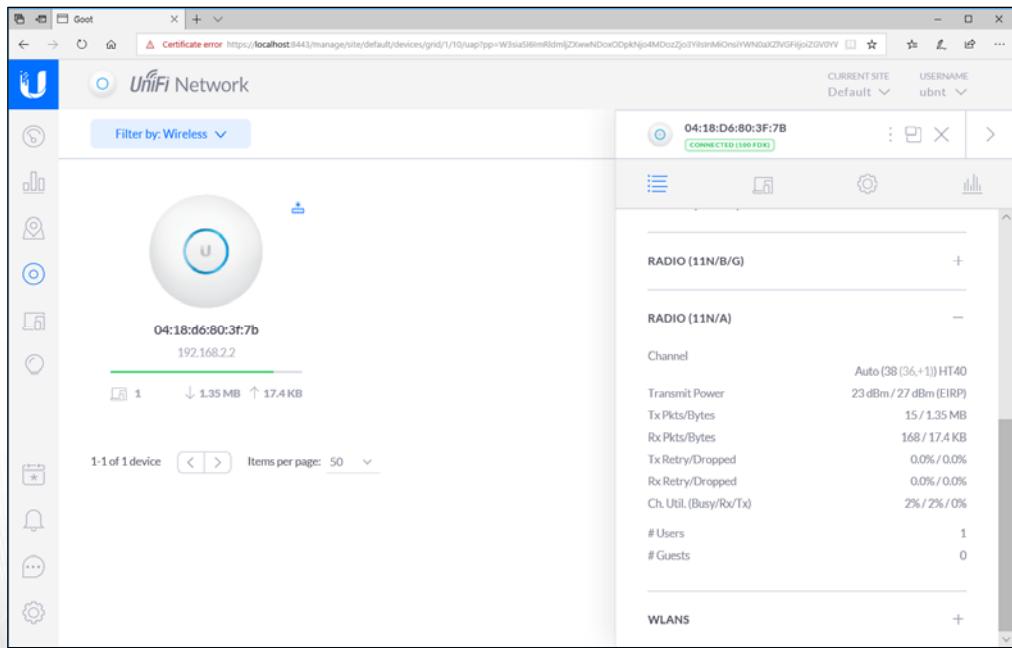
The screenshot shows the Unifi Network Management Plane - Site interface. The top navigation bar includes 'CURRENT SITE' set to 'Default' and 'USERNAME' set to 'ubnt'. The main dashboard displays several key metrics:

- Wireless Clients (per ESSID):** Shows 1 client connected to the 'Tali-bar' access point.
- Current Usage: Top Access Points:** Shows 1 client connected to access point 04:18:d6:80:3f:7b, which is handling 1.44 MB of traffic.
- Wireless Clients (per Radio Type):** Shows 1 client connected to both 2.4 GHz and 5 GHz radios.
- Quick Look:** Provides detailed information about network activity:
 - Most active AP: 04:18:d6:80:3f:7b (down 1.42 MB, up 18.6 KB)
 - Most active client: d0:77:14:3c:10:78 (down 638 B, up 23.5 KB)
 - Longest connected client: d0:77:14:3c:10:78 (down 638 B, up 23.5 KB)

On the left, a sidebar menu lists various management options: System Stats, Wireless Clients, Current Usage, Top Access Points, Wireless Clients (per Radio Type), Quick Look, Most active AP, Most active client, Longest connected client, and Logout.

UMBC CYBERSECURITY
Training Centers ACADEMY

Management Plane – AP



UMBC CYBERSECURITY
Training Centers ACADEMY

Control Plane

- Decision making based on protocols
- Switching and routing intelligence
- Content addressable memory tables
- How the network devices interact with one another



Radio resource management, Fast transitions, load balancing, mesh network protocols

Data Plane

- Where the data is actually forward or manipulated
- AP or WLAN controller

WLAN Architecture Types

- Autonomous
- Centralized
- Distributed

Autonomous Architecture

- APs are known as fat or standalone APs
- Traditional APs deployed early on and SOHO
- Independent of each other in an enterprise
- All planes of operation reside within
- Have a Bridge Virtual Interface that physically interfaces between the 802.11 and 802.3
 - Single IP address is the management interface
- Large deployments can be cumbersome



As a BVI it has both 802.11 and 802.3 protocol stack. The IP is shared between the radio and ethernet connection.

Centralized Architecture

- Instead of a bunch of individuals, a **WLAN controller** is integrated
- Lightweight or thin controller-based APs
- All planes moved from AP to the controller
- Encryption/decryption and time sensitive operations might still reside with AP, or not.
- If not, everything is tunneled back to controller (GRE, proprietary, or CAPWAP)



Controller make all or most of the operations.

Split MAC architecture where the AP can make decision such as decryption/encryption, WIDS, RF spectrum

Generic Routing Encapsulation or Control and Provisioning of Wireless Access Points

Centralized and the Controller

- WLAN Controller often referred to as wireless switches
- Built in security might include
 - Virtual LANs
 - RBAC controls
 - Captive portals
 - VPN concentrators
 - WIDS/WIPS and Firewalls
 - GUI or CLI management interfaces



A remote office WLAN controller can exist in larger deployments dispersed geographically. A remote WLAN controller would be deployed to support local controlled AP in a remote site. The remote WLAN controller would be thought of as a subordinate to the main office WLAN controller. The remote controller would support a limited number of AP and feature. The remote WLAN controller would get configs from the main office controller. The two would communicate over the internet though some secure mechanisms such as VPNs

Controller Data Forwarding

- 802.3 destined traffic ends up in the WLAN controller for integration
- Centralized Data Forwarding
 - Everything is encapsulated and sent back to the AP for handling
 - Including encryption and decryption
- Distributed Data Forwarding
 - Some of the data can be handled by the AP
 - Advantageous in newer 802.11ac speed networks

Distributed WLAN Architecture

- Now we have cooperating (**cooperative**) access points without a WLAN controller
- Cooperative communication protocols are often proprietary, e.g Cisco SPS
- Control and data planes reside in the APs
- Scalable and works well with 802.11n/ac
- Management plane remains centralized
 - Network Management Service



Cisco's Single Point Setup

Centralized Network Management

- As the number of autonomous APs increase, management became unwieldy > 20-25 APs
- The need for consolidated management and pull the management plane to a server
- Network Management Server (NMS)
 - Manage more than WLAN APs
 - Switches, firewalls, routers, oh my
 - RF spectrum monitoring
 - Talks management protocols (SNMPv3, CAPWAP)



Control and data plane are still in the APs.

The move towards a consolidated NMS more efficient than a stand alone dedicated Wireless Network Management server in a data center or closet.

Even more recent has been a push to virtual machines to run the NMS.

Cloud Networking and Mgmt

- Wireless Architecture can be managed from cloud server solutions
- Eliminates the need for local servers or application software
- Data and control planes remain local, though
- Vendors offer cloud management as a service through subscriptions
- Cloud-enabled networking (CEN)

Enterprise WLAN Routers

- Different from Enterprise APs
- Each interface is routable rather than bridged
- VPN client reach back to main office
- Top notch hardware = \$\$
- Granular security features
- Cell service backhaul

Mesh Access Points

- Why go wireless when you can go WIRELESS!
- Create dynamic infrastructure that responds to network changes
- Proprietary L2 routing protocols and metrics
 - Traffic loads, strength, effective data rates, hops
- Discovery of peers by listening to the air
 - Mesh specific beacons looking for suitable peers
- **Simultaneous Authentication of Equals (SAE)**



Dynamically self-create and heal. Similar to how the real internet works with routing protocols.

PMKSA can be a result of an 802.1X/EAP or PSK authentication or SAE

Mesh Access Points

- Wi-Fi Certified EasyMesh
- Geared toward SOHO network coverage
- Standards based to multiple AP networks
- Forming adaptable networks with minimal user intervention
- Self organizing, load balancing, scalability

This Thing Called Bridging

- Wireless bridges operate at the **distribution layer** often as a back up or a back haul link
- Point-to-point or point-to-multipoint
- One bridge AP is the root, all other non-root
- Root role would be of supplicant
- VPN adds additional L3 security to the link

Virtual Private Networks

- Back in the day, VPNs provided the WLAN security before strong L2 encryption
- Today, they're *paramount* for **remote access** to corporate network resources
- VPN + Host-based Firewalls = Happy Admins
- Traditional VPN models or architectures:
 - Site to Site (router to router)
 - Client / Server



VPNs do what or rather afford us what?

CVPN client can be a laptop, router, WLAN controller or an AP.

VPN

- Get us data integrity, privacy through encryption, authentication, and encapsulation
- Two basic VPN implementations
 - Layer 3 VPN (IPSec)
 - SSL/TLS VPN
- Client software for Layer 3 VPN
- Web browser for SSL/TLS



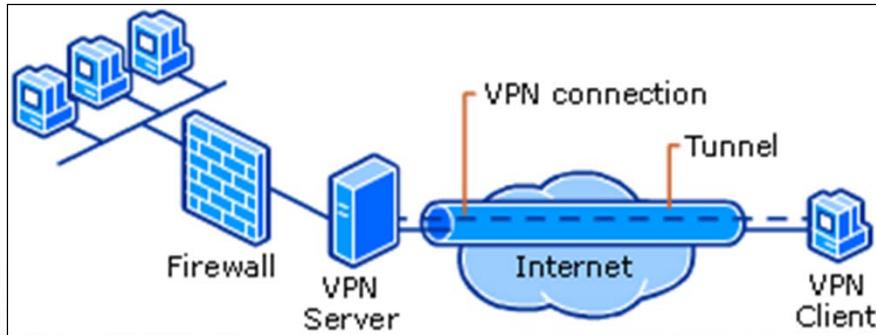
IPSEC supports DES, 3DES, AES encryption to name a few.

SSL 3.0 = TLS 1.0

Minimum of TLS 1.1 should be used

TLS is preferred over Layer 3 VPN clients because of software and NAT traversal or firewall issues with UDP Ports 4500 and 500

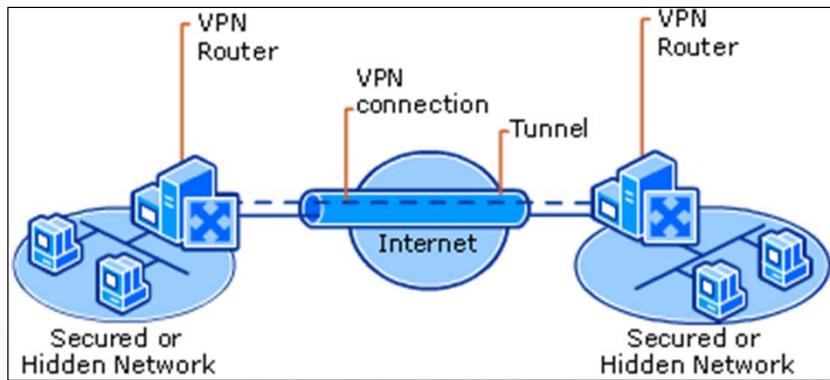
VPN at Open Network



UMBC | CYBERSECURITY
Training Centers ACADEMY

Pictures from technet.Microsoft.com

VPN Site-to-Site



UMBC | CYBERSECURITY
Training Centers ACADEMY

Pictures from technet.Microsoft.com

How Does It All Get Managed?

- Infrastructure Management
- Firmware upgrades, configuration updates, monitoring alerts and alarms, overall performance metrics
- NMS is key to success
- Managed through GUI or command line
 - HTTPS instead of HTTP
 - SNMPv3 but needs tweaking
 - Secure Shell version 2
 - Telnet, anyone?



SNMPv3 uses SHA or MD5 authentication, privacy through encryption, access control for users and groups

Username and passwords replaces community strings that were previously susceptible to sniffing because it was cleartext. Although many of these configs are optional, it should be changed from default regardless of device or protocol.

Summary

- Planes of Operation
- WLAN Architectures
 - Autonomous, Distributed, Centralized
- VPN Wireless Security
- Infrastructure and WLAN Management

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

Legacy Wireless Security

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Authentication
- WEP
- TKIP
- VPNs
- SSID Segmentation
- Security Speed Bumps



Security speed bumps that are not effective are SSID hiding or cloaking and MAC filtering.

Legacy Mechanisms

- Three legacy security mechanism
 - Open system authentication
 - Shared key authentication
 - WEP encryption
- Pre-RSNA security mechanism that are still defined in 802.11 standard
- Why? Backwards compatibility, of course!
- RSNA: dynamic encryption between 2 radios



Notice that the difference between the shared key AUTHENTICATION and WEP ENCRYPTION, not to be confuse both as an encryption.

Legacy Authentication Types

- Authentication is nothing more than two radios verifying they are 802.11 devices
- Two types: *Shared Key* and *Open System*
- Shared key: uses a matching WEP key
 - Cleartext challenge from AP to client
 - Encrypted challenge from client to AP
 - Same WEP key is used for data encryption later
 - Deprecated and should not be used



802.11 authentication is not the same as what you probably understand as what comprises authentication or the verification of credentials.

If the encrypted challenge matches what the AP computes with the shared key and the clear text challenge, then the station can proceed to association

Legacy – Shared Key Authentication

WEP Key: abab123456



WEP Key: abab123456



Legacy Authentication – OSA

- Open system: **only non-deprecated pre-RSNA**
 - Null authentication that does not fail
 - Exchange of niceties
- Authentication is followed by association
- Layer 2 connection to the AP is formed
- Client STA is now part of the BSS
- More advanced authentication occurs next
 - Extensible Authentication Protocols



In an IBSS, Open System Authentication is used.

Wired Equivalent Privacy “Encryption”

- Defined in original 1997 standard
- Layer 2 encryption with RC4 stream cipher
- Layer 3-7 data of MSDU is encrypted
- 64 or 128 bit WEP keys
 - 40 and 104 bit keys + 24 bit Initialization Vector
 - IV is created by the device driver and sent in **cleartext prepended** to each frame
 - IV is also combined with static 40/104 bit key
 - Seeds the encryption algorithm

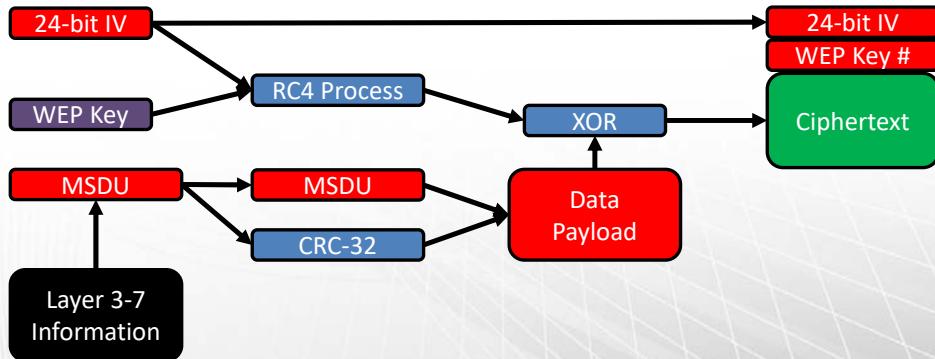


Anyone see a problem with prepending cleartext part of the seeding material that used as input into the encryption algorithm?

IV reuse mathematically occurs every 16.7 million frames

WEP “Encryption”

- The same shared key is used to encrypt data
- Could have up to 4 WEP keys



More on WEP Encryption

- WEP static keys
 - 10 hexadecimal or 5 ASCII characters
 - 26 hexadecimal or 13 ASCII characters
 - Up to 4 static keys can be used but both stations need to know which keys are used
- WEP shortfalls
 - IV collisions
 - Weak Key from weak IVs
 - Reinjection through tools like aireplay-ng
 - Bitflipping for the ICV



Reinjection attacks help generate the collection of weak IVs, usually with an ARP packet
Bitflipping to find a match to the Integrity Checksum Value ICV

Temporal Key Integrity Protocol

- Replacement for WEP as part of the pre-802.11i standard
- Theoretically, no new hardware just firmware
- Temporary fix for later CCMP/AES
- Uses RC4 stream cipher
- Part of the requirement for **WPA** certification
- Optional for legacy devices in RSN

TKIP

- *Time based keys dynamically generated through a 4-way handshake process*
- Sequencing counter to prevent replay attacks
- Stronger seeding material for RC4 cipher
- Message integrity check (MIC or Michael)
- Generation of PTK and GTK
 - PTK for unicast
 - GTK for multicast and broadcast



More on the 4-way later

MICs defeat the bitflipping weaknesses of WEP

Virtual Private Networks

- If WEP is so insecure then we should all use VPNs, right?
- In the context of legacy wireless security
- Not so much because faster L2 encryption
- Added overhead and configuration
- VPNs work at Layer 3 or Layer 4/5



Keep in mind that VPNs in the context of legacy security

VPNs are still recommended when using insecure BSS and hotspots.

Layer 4/5 VPNs exist such as SSL/TLS VPNs in a web browser

VPNs

- Used for **remote access**
- Hotspots and insecure networks
- Bridge links
- Provide encryption, encapsulation, authentication, and data integrity
- Major protocols used in L3 VPNs
 - Point-to-point tunneling protocol (PPTP)
 - Layer 2 Tunneling Protocol & IP Security (IPSec)



PPTP are outdated and have been replaced with IPSEC and SSL VPNs

The problem with PPTP is that it uses MS Point to point encryption which isn't considered strong, furthermore, it uses MS-CHAPv2 which passes username in cleartext and is susceptible to offline dictionary attacks

L2TP and IPSEC are used together to provide confidentiality, integrity, and authentication

IP Security

- Suite of protocols
- Transport or tunnel modes
- Transport mode only encrypts the payload and used for host-to-host communications
- Tunneled mode everything is encrypted inside another packet
 - Header, payload, IP addresses
 - Gateway-to-gateway communications

IPSec and VPNs

- Use public and private key cryptography
- Internet Security Association and Key Management Protocol (ISAKMP)
- Internet Key Exchange (IKE)
- Diffie-Hellman key exchange to establish a shared secret across an unsecure medium

SSL VPNs

- No certificates or complex client software required = less admin intervention
- **Web browser** is all that is needed
- Secure Sockets Layer was replaced by Transport Layer Security
- TLS 1.1 or higher for secure communications
- SSL is still part of the vernacular
- Less Firewall and NAT issues

SSID Segmentation

- Autonomous enterprise APs would broadcast out several SSIDs, capable of up to 16
- Each SSID was tied to a VLAN assignment
- Each VLAN had a separate subnet and needed routing through a L3 device
- Additional overhead in beacons and performance degradation
- Limit to 3-4 SSIDs per radio



Employee, guest, or voice SSIDs might be commonplace and more practical

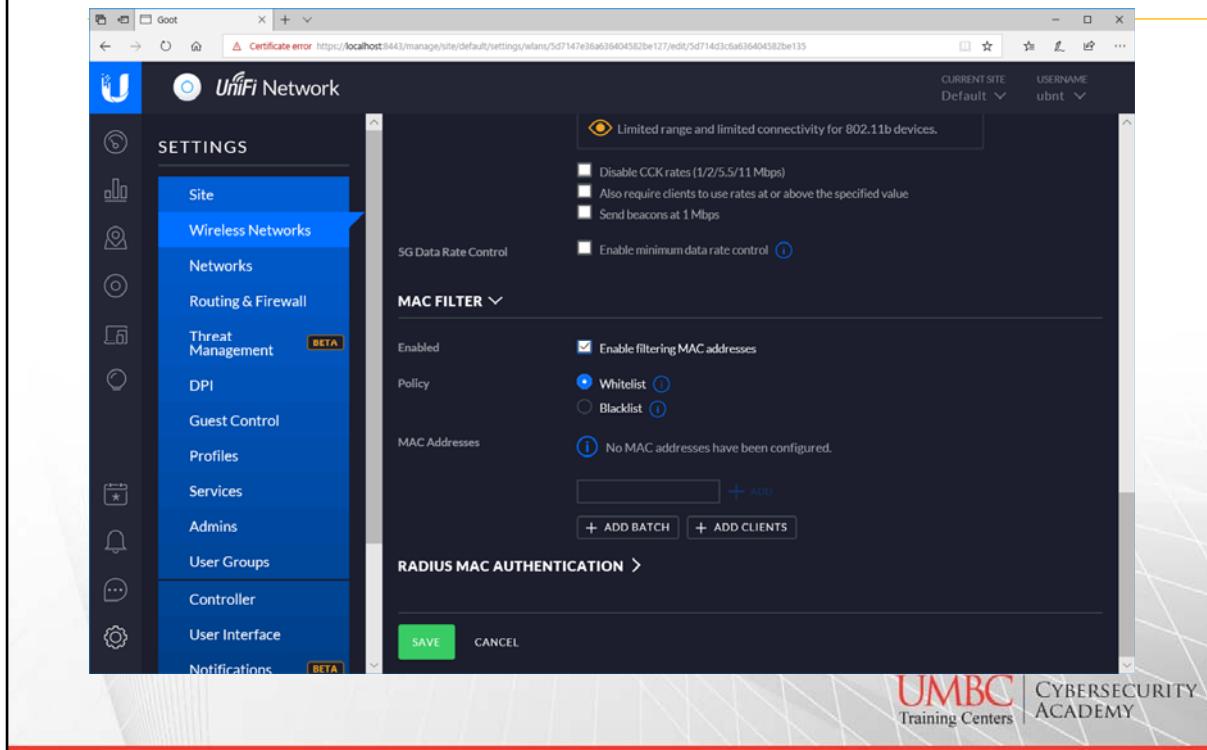
Legacy Security through Obscurity

- MAC Filters
 - Only allow whitelist of devices
 - Circumvented by spoofing
- SSID Hiding or cloaking
 - Also presented as “hidden” network
 - Hides the SSID in the beacon frame
 - Clients have to know the SSID to authenticate and associate with the AP
 - Just use a protocol analyzer



All we have to do is look at the network traffic going to and from the BSSID and find the SSID in the frame, or kick off a client which will reconnect using the true SSID in the probe request.

MAC Filtering Still Used?



Do You Even Cloak?

The screenshot shows the Unifi Network management interface. The left sidebar has a 'SETTINGS' menu with various options like Site, Wireless Networks, Networks, Routing & Firewall, Threat Management, DPI, Guest Control, Profiles, Services, Admins, User Groups, Controller, User Interface, and Notifications. The 'Wireless Networks' option is selected. On the right, under the 'ADVANCED OPTIONS' tab, there are several configuration sections:

- Multicast and Broadcast Filtering**: Includes options like 'Block LAN to WLAN Multicast and Broadcast Data' (unchecked), 'Use VLAN' (set to VLAN ID 2-4009), and 'Enable fast roaming' (unchecked).
- VLAN**: Shows 'Hide SSID' (unchecked) and 'WPA2 Encryption' (set to AES/CCMP Only).
- Fast Roaming**: Shows 'Group Rekey Interval' (set to 3600 seconds) and 'User Group' (set to Default). A note below says: "Note that the configuration and rate limits of this user group will be ignored by any client that has a user group already selected."
- UAPSD**: Shows 'Scheduled' (unchecked) and 'Multicast Enhancement' (unchecked).
- Scheduled**: Shows 'Enable Unscheduled Automatic Power Save Delivery' (unchecked) and 'Enable WLAN schedule' (unchecked).
- Multicast Enhancement**: Shows 'Enable multicast enhancement (IGMPv3)' (unchecked).

A red arrow points to the 'Prevent this SSID from being broadcast' checkbox in the 'Fast Roaming' section.

In the bottom right corner, there is a watermark for 'UMBC Training Centers CYBERSECURITY ACADEMY'.

Summary

- Authentication
- WEP
- TKIP
- VPNs
- SSID Segmentation
- Security Speed Bumps



Pre-RSNA security mechanisms:

WEP encryption
Shared Key Authentication
Open system authentication with two frame exchange.

Open system authentication is the only pre-RSNA security mechanism NOT deprecated

Before a Layer 2 connection occurs, authentication followed by association with an AP

QUESTIONS??



Encryption

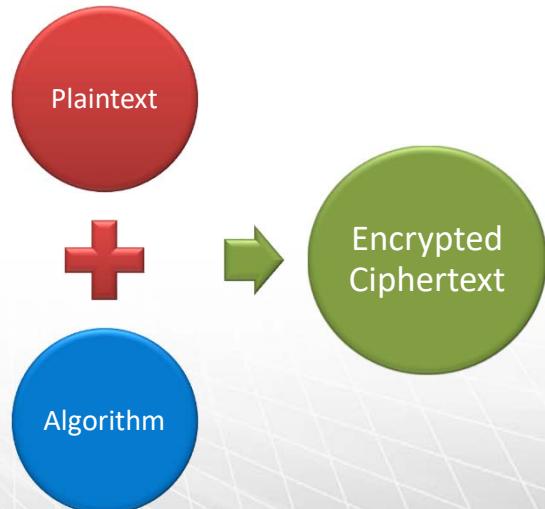
UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Encryption
- WEP
- TKIP
- CCMP
- Wi-Fi Alliance Certifications
- WPA3
- OWE

Encryption

- Why is it important?
- Unbounded medium
- CIA Triad
- Plaintext
- Cipher or Algorithm
- Encrypted Ciphertext



UMBC | CYBERSECURITY
Training Centers ACADEMY

Here we only touch on Encryption as it will apply to WLANs and not the larger concepts of cryptography

Encryption Algorithms

- Symmetric
 - Both ends have the same key or shared secret
 - WEP, TKIP, CCMP use symmetric
- Asymmetric
 - Paired keys: public and private
 - Mathematically related
 - Public key cryptography and signatures
 - Certificates for PKI



Symmetric encryption is typically faster

Public key cryptography builds upon the asymmetric algorithms.

How do you get the same secret to both ends?

Stream and Block Ciphers

- Streaming ciphers work on bit-by-bit
 - Better on inconsistently sized plaintext
 - Ron Rivest's Code 4 (RC4/ARC4)
- Block ciphers work on fixed chunks
 - Block sizes of 64-256 bits
 - *Rounds* of iterative processes that apply the algorithms simpler functions repeatedly on blocks
 - DES, 3DES, AES



DES is a sym block cipher that has its history in the '70s. It uses blocks of 64 bits and a 64 bit key. 8 bits of the key were used for parity which meant the key was more like 56 bits.

3DES uses 3 DES keys for an effective key size of 168 bits

AES is another sym block cipher that has 3 different key lengths 128, 196, 256 bits. As such each are referred to by their key lengths, e.g. AES-256.

AES is the algorithm used in CCMP and WPA2 certified devices.

WLAN Encryption Methods

- As defined by 802.11-2012 standard:
 - WEP, TKIP, and CCMP only
 - Symmetric algorithm
- Layer 2 encryption that protects MSDU
- MSDU can be 0-2,304 bytes
 - Variances in MSDU length due to encryption used
- *WEP* is legacy encryption for *pre-RSNA*
- TKIP and CCMP are used for RSNA



MSDU is the Layer 3-7 data. Encryption only occurs on the data frame types. **What are the other frame types?**

We'll look at WEP, TKIP, and CCMP a little more next

WEP, again

- Part of the original 1997 standard
- Streaming cipher
- Uses RC4 and 64 or 128 bit keys
- Up to 4 different static keys
- 8 additional bytes of overhead
 - 4 for the cleartext IV + padding + Key ID
 - 4 for the Integrity Checksum Value (ICV)
 - Result up to 2,312 byte frame size ($2,304 + 4 + 4$)



ICV is the cyclic redundancy check (CRC) and used for the verification of data integrity

Now the 802.11 frame be up to 2,312 bytes in size

The key ID is sent as part of the IV. Padding in the IV section is 6 bits plus 2 bits for Key ID.

TKIP, again

- Replacement for WEP and interim solution before the 802.11i release
- Streaming cipher with RC4
- 128-bit time based key
- Message Integrity Code (MIC)
- 20 additional bytes of overhead
 - 8 for IV and Extended IV (4 + 4)
 - 8 for MIC and ICV (8 + 4)
 - Result is up to 2,324 byte frame size



From what I can tell, the MIC is the integrity check on the ciphertext and the address portions of the header.

The ICV is the CRC on the entire MPDU which is the MSDU plus header

Ah, CCMP

- Counter mode with cipher block chaining message authentication code protocol
- Replacement for TKIP and WEP
- Block cipher with AES 128-bit key
- WPA2 certification mandates CCMP
- Only method Wi-Fi Alliance will certify in 802.11n and 802.11ac devices
- Components of CCMP provide CIA



Counter mode affords confidentiality

CBC-MAC provides integrity and authentication

CCMP

- Inputs into the CCMP process
 - 128-bit time based key
 - Packet number aka sequence number
 - Number used once aka **nonce**
 - Data frame itself needing protection
 - Additional authentication data that includes addresses
- 16 bytes of additional overhead
 - 8 for the CCMP header
 - 8 for the MIC
 - Result is up to 2,320 byte frame size

Wi-Fi Alliance Certifications

- WPA and WPA2
 - Personal with a Passphrase
 - Enterprise with a form or 802.1X/EAP
- WPA is pre 802.11i
- WPA2 is fully compliant with 802.11i
- High Throughput (HT) and Very High Throughput (VHT) data rates not allowed with WEP or TKIP



TKIP and WEP can only support up to a 54 Mbps data rate.

WPA3 from 802.11s

- 802.11s initially defined Hybrid Wireless Mesh Protocol to help with path selection
- Path determination meant to be less proprietary and more open and “easy”
- In the 802.11s amendment was defined peer-to-peer authentication method—**SAE**
- The simultaneous authentication of equals is a more secure replacement for PSK



Later you'll learn that the Wi-Fi Alliance has a certification called EasyMesh where multiple access points work together to form a unified network that provides efficient coverage indoors and out.

WPA3, Anyone?

- Another **Wi-Fi Alliance certification** introduced in mid-2018
- Supports both Personal and Enterprise modes
- Requires Protected Management Frames
- Two primary modes
 - Personal (SAE) is still based on a passphrase
 - Enterprise uses 192-bit strength keys
- Transition mode (mixed)
 - PMF enable in WPA2-PSK devices



Recall that Management Frame Protections are in line with 802.11w amendment.

Simultaneous Authentication of Equals (SAE)

WPA3-Personal

- Using password (passphrase/PSK) based authentication in **SAE**
- Can be effective with weak passwords*
- Forward secrecy of transmitted data ensured with compromised passwords
- Dragonfly key exchange
- Resistant to offline dictionary attacks
- Attacker would have resort to online attack



The SAE exchange only allows for one guess of the passphrase.

The AP should recognize repeated authentication failures and take an action, e.g. throttling, flagging, logging.

Forward secrecy is ensured despite a compromise of the static PSK because the actual traffic encryption keys remain unknown.

WPA3-Enterprise 192-bit

- Specific about higher security requirements in sensitive enterprise environments
 - DoD, USG, and Industrial
 - CCI, PCI, PHI, PII
- Requires Protected Management Frames
- EAP types using TLS

WPA3-Transition Mode

- Since SAE is not backwards compatible there just has to be some way
- Transition mode supports SAE and WPA2-PSK on the same BSS **using the same pre-shared key** with both protocols
- An attacker with this transition mode knowledge could offline attack the WPA2-PSK
- Problem? Then do two separate BSSs

Opportunistic Wireless Encryption

- Based on RFC 8110
- User in open wireless network where authentication is not possible
- Provide data privacy with ease-of-use
 - **Protections against passive eavesdropping**
- Each device uses established cryptography mechanism to generate encryption keys called a *pairwise secret used in a 4-way handshake*
- Unauthenticated data encryption for users

OWE

- No additional configuration or user interaction
- Key generation is based on Elliptic-curve Diffie-Hellman (ECDH)
- Protected management frames
- Does not provide authentication either way
- Man-in-the-middle is still possible with an evil twin access point
- **Wi-Fi Alliance Enhanced Open** certification

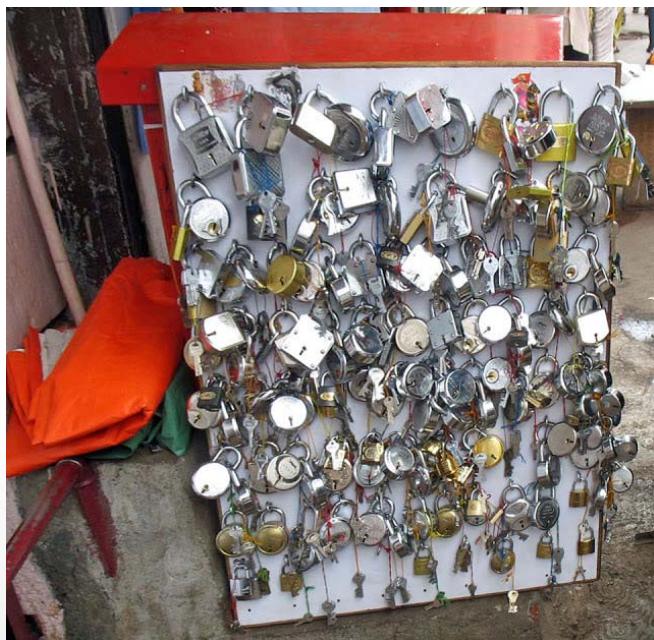
OWE Discovery

- It's in the beacons and probe responses
- AP advertise support for OWE in their Authentication and Key Management suite
- Specifically advertised in the RSN element
- Open system authentication followed by OWE association in which DH public keys are exchanged and a Pairwise Master Key created
- Both stations need to support OWE

Summary

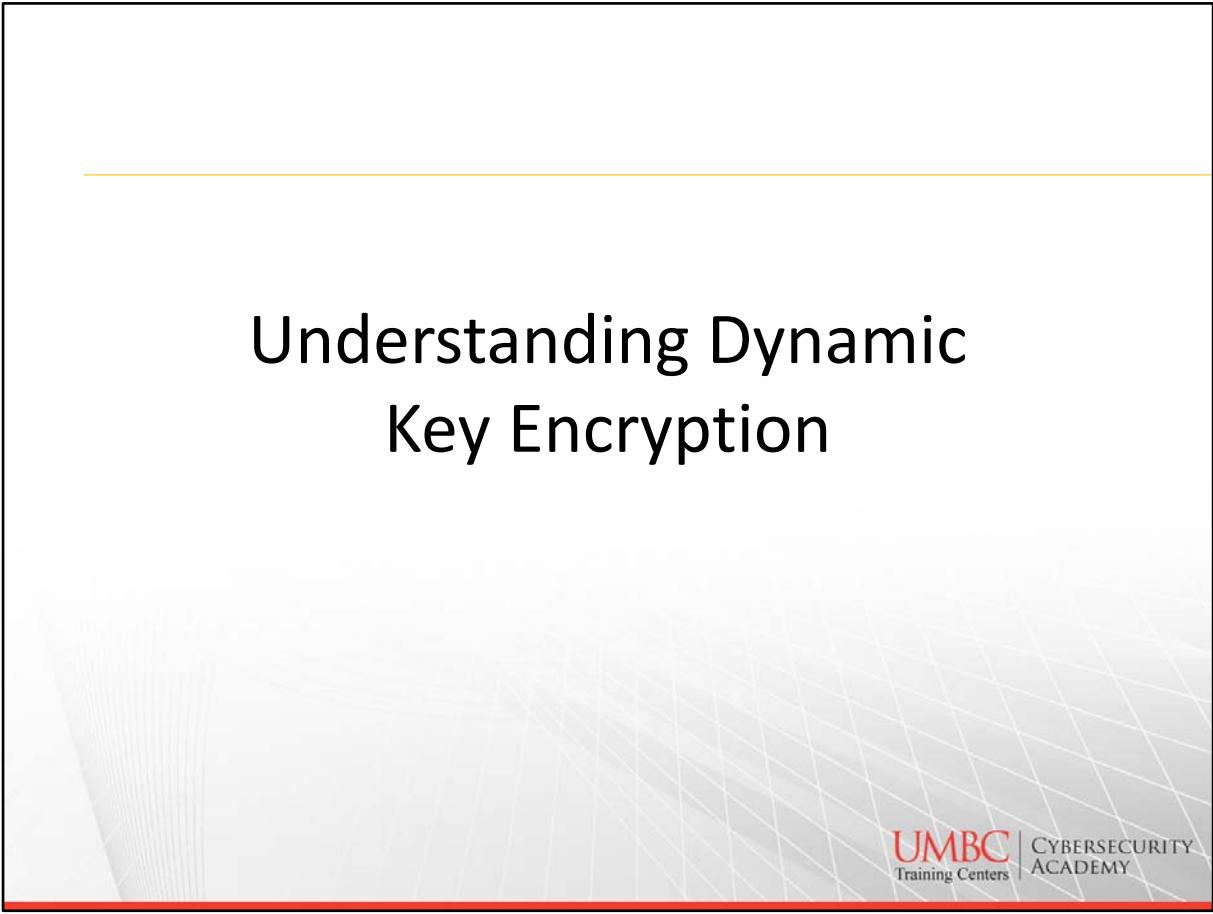
- WEP is pre-RSNA
- Only TKIP and CCMP are considered RSN
- 802.11-2012 defines 3 encryption methods
 - WEP, TKIP, CCMP
- Encryption is for Layer 3-7 data (MSDU) only
- CCMP only for 802.11n and 802.11ac devices
- CCMP is mandatory and TKIP optional in WPA2
- WPA3 supports 2 modes*

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

Understanding Dynamic Key Encryption



UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Dynamic Key Generation
- RSN and RSN Information Element
- Key Hierarchy
- Handshakes

Dynamic Encryption

- Pre-RSNA and RSNA algorithms
- Need for data privacy and confidentiality
- Successful EAP process provides the seed
- Passphrase and PSK also provide the seed
- Seeding material goes into the dynamic key generation process
- **Key is not susceptible to Social Engineering**
- **Keys are per user per session**



WEP is pre-RSNA and **TKIP/RC4 and CCMP/AES** are RSNA algorithms.

The users have no knowledge of the keys, thus they can't compromise them through SE attempts. Also since keys are per user per session, a compromised key only exposes one user's session data and not everyone else's as with pre-RSNA WEP algorithms.

Each time a supplicant associates to an AP, a new key is generated even if the supplicant was just connected a few minutes earlier to the same AP.

Robust Security Network

- As defined in the 802.11i amendment and rolled into the 2016 standard
- RSN and their security associations
- Two STAs authenticate and associate with each other and go through 4-way handshake
 - Dynamic keys are generated
- CCMP/AES mandatory with TKIP/RC4 optional
- 802.11n/ac data rate only possible with CCMP



Encryption keys between the two radios has to be unique as part of the robust security network associations.

RSN

- Robust Security Network can only allow for RSN Associations (RSNA)
- Only CCMP/AES and/or TKIP/RC4
- Unicast keys can be either
- Multicast/Broadcast key drops to lowest
- No pre-RSNA, e.g. WEP



The unicast PTK created can be of either CCMP/AES or TKIP/RC4 methods. However, if both CCMP and TKIP STAs are part of the same RSN, the GTK uses the lowest common method.

RSNA in Basic Service Set

- Each STA pairing has a unique unicast key
- The BSS has a single multicast/broadcast key
- For example, an AP using CCMP/AES and a single SSID with 5 associated clients
 - 1 GTK and 5 PTKs



Keep in mind that an AP can broadcast out two or more SSIDs. Each then becomes a single Basic Service Set.

In an IBSS, each peer station paring has a unique PTK. The GTK is defined by each peer STA.
In an IBSS with 5 peer stations, 5 PTK and 5 GTK are used.

Transition Security Network (TSN)

- One or more pre-RSNA in same BSS as RSNA
- The GTK would then drop to pre-RSNA
 - Multicast and broadcast traffic

Virtual BSSIDs

- Normally an AP has a single BSSID (MAC)
- AP can broadcast out multiple SSIDs
- To avoid client confusion, AP might use virtual BSSIDs tied to each SSID
- One up number of MAC
- Common in larger WLAN deployments

RSN Information Element

- RSNIE declares RSN capabilities
- Found in 4 management frames
 - Beacon, probe response, association request, and the reassociation request
- **Identifies encryption capabilities and whether 802.1X/EAP or Passphrase (PSK) in use**
- STAs will know each other security capabilities before association occurs

RSN Information Element

- Pairwise Cipher Suite information
- Group Cipher Suite information
- Client STAs must support the declared method
- Authentication Key Management (AKM) suite
 - Which authentication methods
 - 802.1X/EAP
 - Passphrase (PSK)



PCS contains the suite information about the encryption used by unicast stations

GCS contains cipher suite information about the broadcast/multicast traffic

AKM

- Not to be confused with AKM suite in RSNIE
- Authentication and Key Management
 - How is authentication occurring?
 - Passphrase (PSK) or 802.1X/EAP?
 - OWE?
 - How are keys being managed?
 - Dynamic encryption key generation?
 - **Seed material is a result of either auth method**
- AKM begins with Discovery ends with 802.11 frames being encrypted

AKM Soup to Nuts

- Discovery
- Open System Authentication
- Master key creation
- Temporal keys made
- Authorization
- Encryption



Discovery is the beacons, probe request and probe response. Here the RSN information is exchanged to include encryption in use and authentication methods in effect.

Master key creation is when the AS and supplicant generate the PMK. The PMK is securely sent from the AS to the authenticator to be used in the temporal key generation process.

The 4-way handshake creates the temporal keys. The controlled port is then opened on the authenticator.

Keys, Lots of Keys

- Hierarchy of keys
- 5 keys in a RSNA
- It all begins with the *Master Session Key*
 - At least 64 bytes in size
 - Generated as a result of 802.1X or PSK process
 - The seeding material after those processes
- Two Master Keys are created from the MSK
 - Unique Pairwise Master Key (PMK)
 - Groupwise Master Key (GMK)



In EAP process, the MSK is exported to the supplicant and AS.

PMK is the first 256 bits of the MSK which was 64 bytes long. The PMK is generated at the AS and securely sent to the authenticator.

GMK is randomly generated on the authenticator.

Keys, More Keys

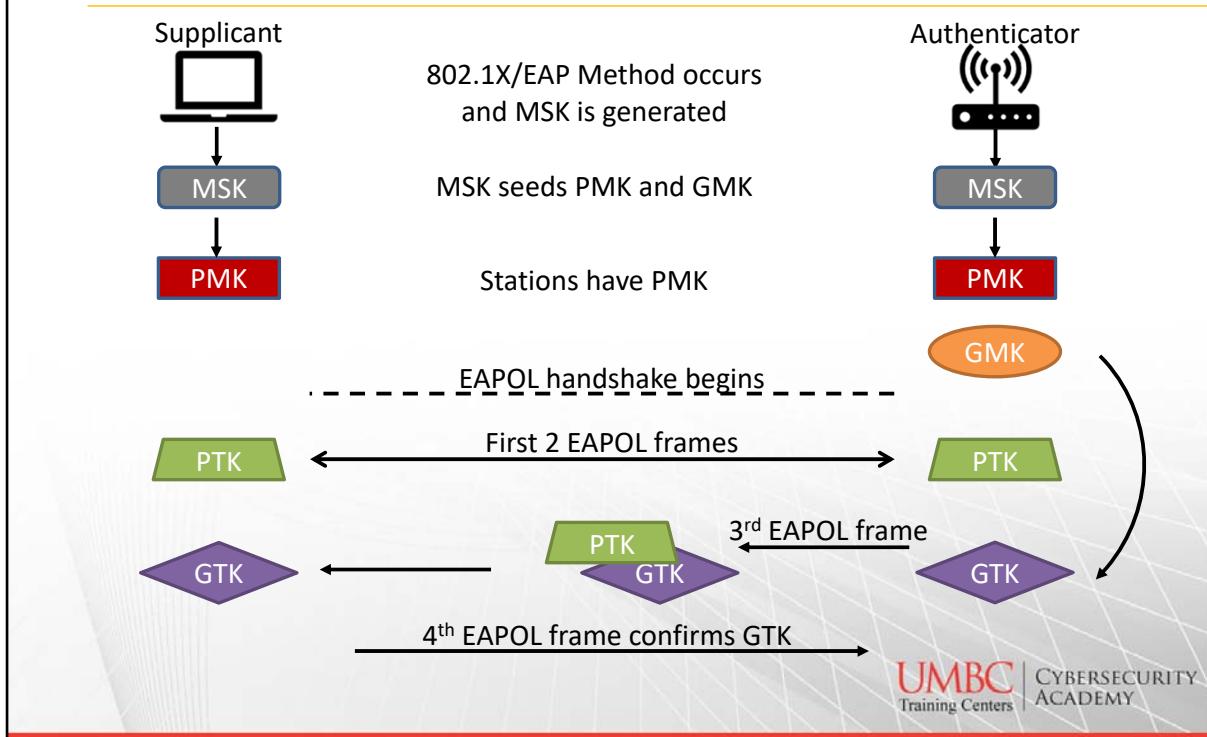
- The PMK and GMK each seed the creation of temporal keys via the **4-way handshake**
 - Pairwise Transient Key (PTK)
 - Group Temporal Key (GTK)*
- PTK has three sub keys!
 - Key Confirmation Key (integrity of handshake)
 - Key Encryption Key (privacy of handshake)
 - Temporal Key (actual MSDU payload encryption key)



We should already know at this point what is the purpose of each key, PTK and GTK.

It should be noted the GTK is created by the authenticator and shared with each client supplicant in the BSS

Key Generation in 802.1X/EAP RSN



The generation of the PTK requires 5 pieces of data, the Pairwise Master Key (PMK), the Authenticator Nonce (*Anonce*), the Suplicant Nonce (*Snonce*), the STA MAC address, and the AP MAC address. Each nonce is a random number generated by the supplicant and authenticator, respectively. Using these 5 pieces of data leads to a unique STA-AP key pairing.

The PMK is the 256-bit key created from an 8-63 ASCII case-sensitive characters or 64 hexadecimal character WPA/WPA2 Personal pre-shared key.

4-Way Handshake, Finally!

- Final process to generate new PTK and transfer the GTK
- EAPOL frames between supplicant and authenticator
- There's a pseudorandom function to generate the PTK =
PRF (PMK + Anonce + Snonce + AMAC + SMAC)
- Controlled port becomes unblocked



The GTK is transferred to the supplicant through the 3rd message of the handshake. The GTK is encrypted with the PTK.

If a new GTK needs to be sent to all associated STAs for whatever reason, it is encrypted with each station's individual PTK.

Peer-to-Peer Comms in a BSS

- Wait, what? I thought peer comms were disallowed or prohibited!
- Unless they have permissions and yet more keys, yes more keys
- Normally peer-to-peer has to go through AP
 - Helps mitigate peer-to-peer attacks
- Station-to-station link (STSL) 802.11i-2004
- Tunneled Direct Link Setup (TDLS) 802.11z-2010



STSL involve two client STAs in a RSNA BSS to communicate with each other after a PeerKey handshake occurs and facilitated by the AP. The PeerKey handshake creates a STSL Master Key which seed the creation of STSL Transient Key (STK).

STSL is defined by the 802.11i-2004 amendment but really never took off.

TDLS

- Defined in the 802.11z-2010 amendment
- Between two peer stations in a RSN BSS
- Multimedia streaming between video clients and smart TVs
- TDLS Peer Key (TPK) handshake
- TPK security associations (TPKSA)
- Go off channel but periodically check back with AP to remain associated



This can occur only after the two peer stations are authenticated, associated, and authorized to a traditional BSS.

What type of 802.11 networks do you think this occurs? 802.11n and 802.11ac

All the RSNA types

- Pairwise Master Key SA
- Pairwise Transient Key SA
- Group Temporal Key SA
- STSL Master Key SA
- STSL Transient Key SA
- TDLS Peer Key SA



Up to this point we've seen a number of RSNA association in specific environments. Here's the nomenclature for each.

Passphrases and Pre-shared Keys

- The passphrase in a WPA/WPA2 personal network is between 8-63 ASCII characters
- The passphrase is mapped to the PSK through another function: **PBKDF**
- The resulting PSK is 256 bits or 64 hex chars
- Need **SSID, SSID length, and the Passphrase**
- **The PSK becomes the PMK**

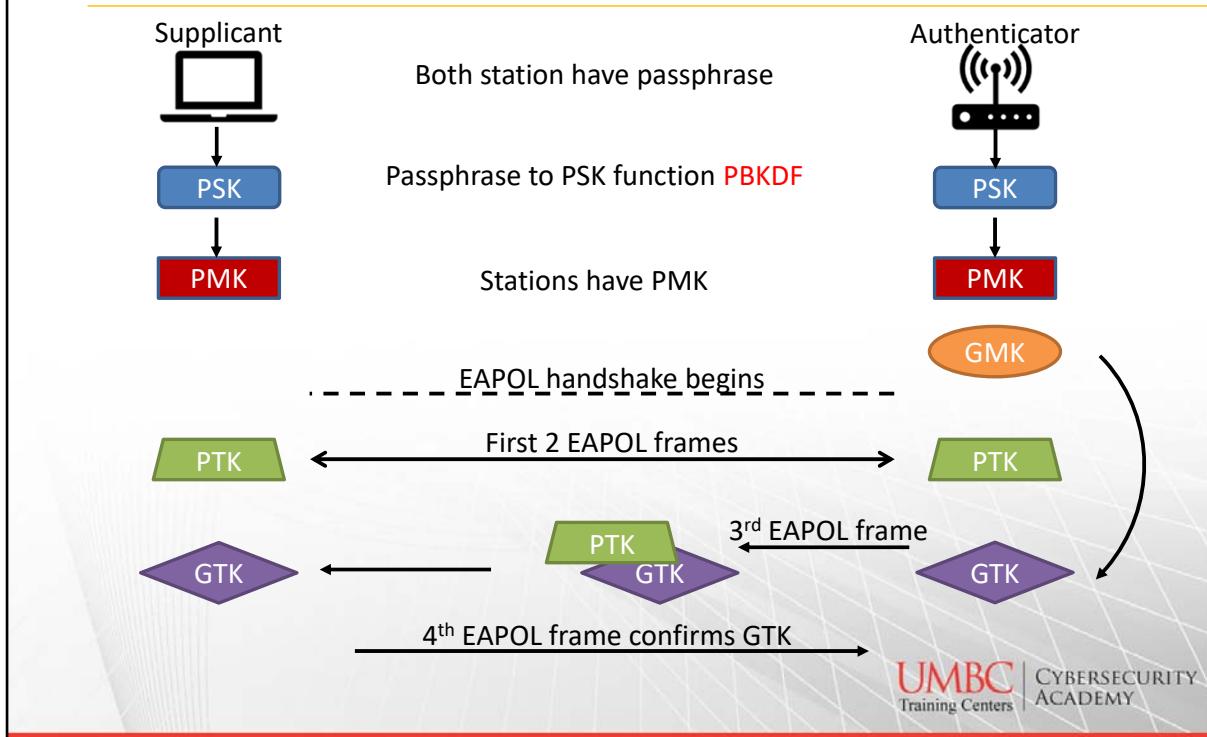


The Password Based Key Generation Function need three pieces of information to generate the PSK:

Passphrase-to-PSK

- PSK = PBKDF (Passphrase, SSID, SSID len, 4096, 256)
- SSID Len is the number of octets of the SSID
- 4096 is the # times the passphrase is hashed
- 256 is the # of output bits in the PSK
- PSK becomes the PMK

Key Generation in PSK RSN



The generation of the PTK requires 5 pieces of data, the Pairwise Master Key (PMK), the Authenticator Nonce (*Anonce*), the Supplicant Nonce (*Snonce*), the STA MAC address, and the AP MAC address. Each nonce is a random number generated by the supplicant and authenticator, respectively. Using these 5 pieces of data leads to a unique STA-AP key pairing.

The PMK is the 256-bit key created from an 8-63 ASCII case-sensitive characters or 64 hexadecimal character WPA/WPA2 Personal pre-shared key.

Key Generation in SAE

- Ties back to 802.11s WDS and Mesh
- Variant of *Dragonfly* which is password-authenticated key exchange
- Goal is to share a key between devices without compromising the key
- Commit and Confirm phase
- Client initiates the commit in infrastructure



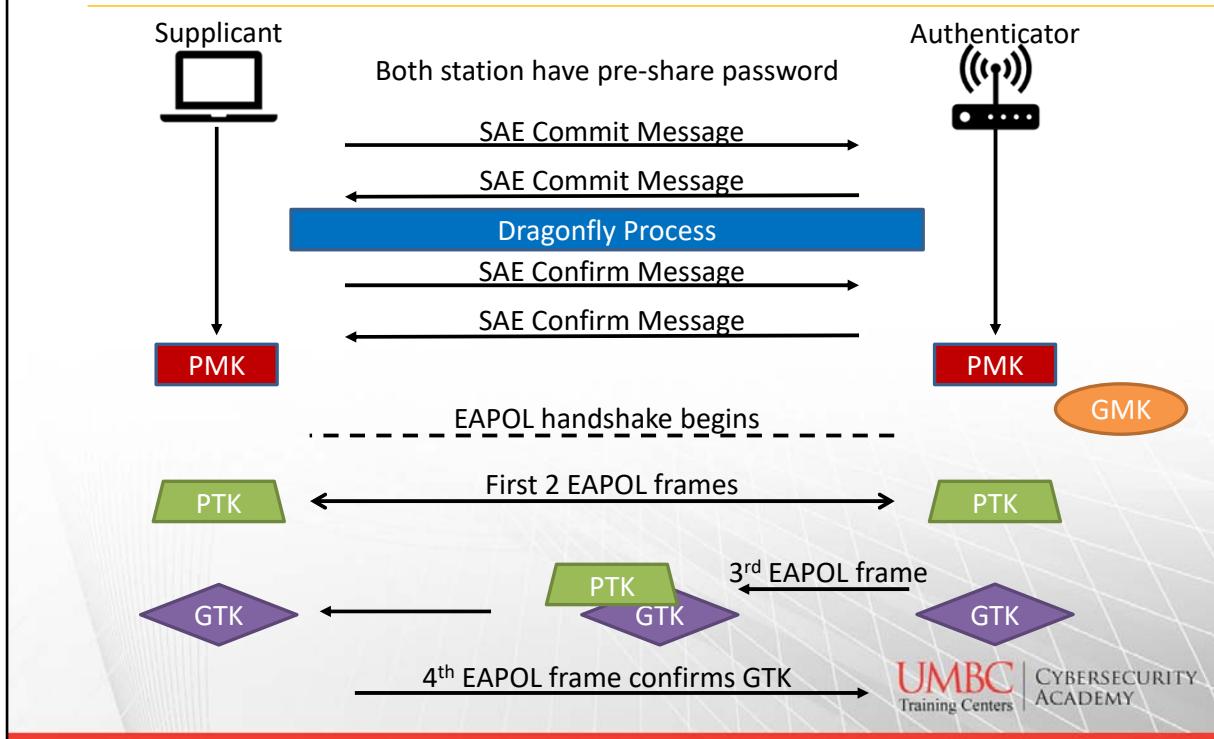
The dragonfly handshake prevents offline dictionary attacks and provides the forward secrecy.

As it is a password authenticated key exchange, the password is turned into a high-entropy key.

Key Generation in SAE

- A pre-shared password is converted to a group element using a hash-to-element method
- Each peer picks two random numbers and calculate elliptic curve information which is then sent to each other in **commit** frames
- A confirm phase occurs where the peers calculate a secret point (x,y coordinates)
- **Confirm** frames verify the same *secret guess*

Key Generation in SAE



Final Thoughts on Keys

- PMK is result of 802.1X/EAP or PSK processes
- The PMK is the seed for any 4-way
- Dynamic keys are generated every time a STA associates or roams to another AP
- 802.1X/EAP process takes time to complete usually 700ms
- Dynamic key prevent SE attempts
- PTK are per session per device

Summary

- Dynamic Key Generation
- RSN and RSN Information Element
- Key Hierarchy
- Handshakes

QUESTIONS??



Preshared Keys

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- WPA and WPA2 Personal
- Passphrase and PSK

Review of AKMP

- Authentication and Key Mgmt Protocol can be either one of: 802.1X/EAP or PSK
- AKM services are seen in the RSNIE in four 802.11 management frame subtypes:
 - From AP: Beacon, Probe Response
 - From client STA: Association Request and Re-association Request
- AKMP supports authentication and encryption key generation

Pre-shared Key Authentication

- It is an AKMP
- WPA Personal and WPA2 Personal
 - TKIP/RC4
 - CCMP/AES
- Recommended for SOHO deployments
- Less adept setups
- Vulnerable to SE attempts
- How do you get a PSK from a Passphrase?



By this point we should know that WPA and WPA2 are WiFi Alliance certifications. Furthermore, WPA was prior to the 802.11i amendment in 2004. WPA2 is fully compliant with 802.11i amendment.

PSK = PBKDF (SSID, SSID Len, 4096, 256, Passphrase)

Passphrase to PSK

- Passphrase can be 8-63 ASCII characters
- Can be custom or manufacturer default
 - abc123!!!
 - myvoiceismypassport
 - 44f49464 (Belkin)
- Passphrase plus magic is converted to 64 character hex or 256-bit length key PSK



The passphrase, SSID, and SSID length are hashed together 4096 times to get an output that is 256 bits long.

PSK to PMK

- The 256-bit PSK is the Pairwise Master Key
- PMK becomes the seed material for the 4-way
- Since each client uses the same passphrase, the PMK is the same for each client
- **Nonces and MAC address add the differences**
- If you get the passphrase you can get the PSK
- If you have the PSK, you have the PMK

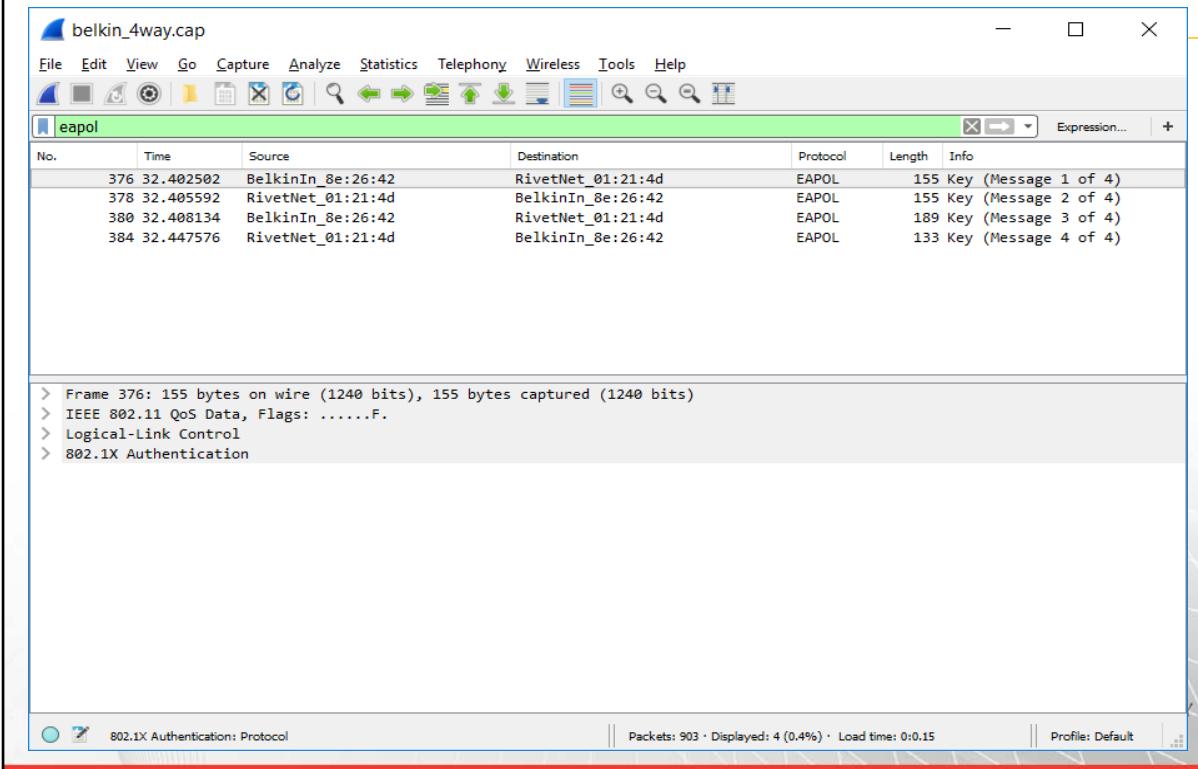


The PMK is the same for each client in that BSS, the difference or uniqueness for the PTK is a result of the 4-way handshake

PMK to PTK

- The Pairwise Transient Key generation uses the PMK as seed for the 4-way handshake
- 4-way handshake uses:
 - Client MAC address
 - AP MAC address
 - ANonce
 - SNonce
- 4-way can be seen in cleartext as EAPOL

Clean 4-way Handshake Capture



PMK to PTK Vulnerabilities

- The 4-way can be obtained passively with a monitor mode wireless card
- The PSK PBKDF is public domain
- Someone could capture the 4-way compute the PTK and decrypt unicast traffic
- Vulnerable to offline dictionary attacks
- Stupid human tricks...Social Engineering
- WPA and its TKIP/RC4 is considered weak



Well it can be trivial if passphrases are weak or left to manufacturer default.

If you can capture the 4-way handshake, we have everything except the PMK. The PMK is the PSK. We can reverse the PSK and get the passphrase, sort of....

If you can SE someone to give you the passphrase, it will lead you to the PSK which is the same as the PMK

Offline Passphrase/PSK Cracking

- Not necessarily an easy feat
- Passphrase can be between 8-63 ASCII chars
- PBKDF function also hashes 4096 times
- Need the 4-way handshake or at least 2 of the frames in a capture file
- Aircrack-ng with a password file
`aircrack-ng -w [wordlist] [capture file]`
- How many variations of 63 ASCII chars?



If it was so easy, what would be the point?

You can speed up the process by having a capture file with only the 4-way hand shake.

Keep in mind that the password wordlist will probably contain the most common passphrases. In the event that the passphrase is hella complex, multiple CPUs or GPUs and lots of time will be needed.

Offload the cracking to EC2 servers

Aircracking the Passphrase

```
root@kali: /usr/share/wordlists
File Edit View Search Terminal Help

[00:02:11] 187800/9822768 keys tested (1395.58 k/s)
Time left: 1 hour, 55 minutes, 6 seconds          1.91%
Current passphrase: andriany

Master Key      : D5 07 18 E3 E6 57 AD 56 DE 1D 8D F1 BD A5 5F 10
                  F0 B2 CE A0 CD D7 9B FD 48 03 77 93 43 D9 58 A9
Transient Key   : 66 42 AB 1E 08 E6 E0 B4 DF 86 C6 5D 6E A2 20 F6
                  BF C3 9C 1D ED D1 74 9D 04 83 82 C6 99 C0 B3 A4
                  D5 5E 36 67 D6 25 D0 D0 6F EF 83 B3 F5 2C 35 CC
                  44 EC 3E 34 F4 8F 95 1A 96 00 53 E0 6D 09 67 0D
EAPOL HMAC     : 6C D0 BD 07 CE A1 E8 3C 25 B9 4D C0 F4 88 8C 81
```

UMBC | CYBERSECURITY
Training Centers ACADEMY

Precomputed Hash Tables

- **Without:** take a plaintext value, encrypt it with the appropriate algorithm, then compare
 - Wordlist available in flat plaintext files
 - Self generate or go grab some
 - CPU intensive alone or offload to cloud
 - Time consuming

Precomputed Hash Tables

- Sets of hashed guesses using what you know
 - SSID, SSID length, and passphrase guesses
- Eliminates the guessed passphrase and PBKDF
- You precompute the PSKs
- Very large!
- Gig or Terabytes in size
- WPA/WPA2 catch is the PMK



Recall that the PMK takes into account the pre-shared key and the SSID.

Two networks with the exact same pre-shared key will have different PMKs

Mitigating PSK Vulnerabilities

- Use CCMP/AES and WPA2 certified devices
 - CCMP/AES solely supported for 802.11n/ac speeds
- Up the entropy or “randomness” in passphrase used in SOHO deployments
- *Minimum of 20* characters passphrases
 - Mixed case letters, numbers, symbols
 - #TCumbc_11235813213455!
- Use a proprietary PSK solution

SAE

- Simultaneous Authentication of Equals
- Part of the 802.11s amendment for mesh
- Peer-to-peer authentication
- Prove you know the passphrase without revealing the passphrase
- STAs get **one guess** at the passphrase
- Generate a PMK from and SAE exchange
- Aims to prevent dictionary attacks



SAE is based on a Dragonfly key exchange. It is a zero-proof key exchange. Meaning that a user or device must prove knowledge of a password without actually having to reveal that password.

The goal of SAE is to address the previous weaknesses with PSK authentication

Summary

- Getting to a PTK from a passphrase
- Passphrase vulnerabilities
- Passphrase security recommendations

QUESTIONS??



802.1X and EAP

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- AAA
- 802.1X
- Certificates
- Legacy Authentication
- Lots on EAP types

Authentication

- Verification of **identity** or credentials
- Three categories
 - Something you know, e.g. password
 - Something you have, e.g. Token or certificate
 - Something you are, e.g. biometrics
- Single or multi-factor authentication
 - Combining categories

Triple A or AAA



- Authentication, Authorization, and Accounting
- AAA can be extended to WLAN
- Roots in the dial-up era
- Accounting may be a regulatory requirement for some vertical markets or industries
- Many ways to do AAA
- Who is doing what, where, and how long.

UMBC | CYBERSECURITY
Training Centers ACADEMY

There are a number of ways to accomplish AAA, such as a RADIUS server or another open source RADIUS spin-off

Authentication

- You want access, great. Who are you?
- Show me your credentials:
 - Username/password
 - Certificates
 - OTP
 - CACs or USB dongles
 - Preshared keys (PSK)
- Verification of identity



Generally speaking, this is authentication. Show me your creds and I will verify your identity.

Later with EAP, there are more specific ways to verify identity and the requirements for credentials

Authorization

- Now that you are verified, where can you go?
- Authorization gives access to specific or any network resources
- Remote Authentication and Dial-in User Service (RADIUS) can do the authorization
 - Has AAA capabilities
 - Based on RFC 2865 and RFC 2866
 - Standalone or built-in
 - Can verify and authorize on behalf of others



In an enterprise class WLAN deployment, the use of authentication and port-based access control is dictated for enterprise RSNs

Authentication and authorization is defined in RFC 2865 and accounting in RFC 2866

RADIUS servers might be a standalone server in a larger data center or built-in to some enterprise class access points and WLAN controllers

Verification and authorization interface with other protocols such as LDAP, AD or some other proprietary protocol

Accounting

- RFC 2866 defines the last A in AAA
- Records for forensic purposes, e.g. logs
- Who did what where, for how long and how much data was sent or received
- Vendor Attribute Value Pairs (AVP)



UMBC | CYBERSECURITY
Training Centers ACADEMY

AVPs are used by certain vendors or implementations of RADIUS which we will see later can be used for further refinement of things like RBAC, permissions, and more.

Port-based Access Control

- Also known as 802.1X
- Client-server access control through ports
- Not isolated to WLAN, origins in Ethernet
- Authorization framework that controls traffic passing through a port and accessing network resources
- 3 specific roles or components
- 802.1X is used with L2 authentication



The IEEE 802.1X standard defines a client and server-based access control and authentication protocol that restricts unauthorized clients from connecting to a LAN through publicly accessible ports. The authentication server authenticates each client connected to a switch port and assigns the port to a VLAN before making available any services offered by the switch or the LAN. Until the client is authenticated, 802.1X access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the client is connected. After authentication is successful, normal traffic can pass through the port.

Layer 2 authentication protocol is EAP to validate users at the Layer 2.

802.1X Supplicant

- Station's software asking for access
- Supplying credentials
- Client laptop or mobile device



UMBC | CYBERSECURITY
Training Centers ACADEMY

The Supplicant

- Needs to be validated before access to network resources
- Supplicant client software can be:
 - OS integrated, e.g. Windows 10 client utility
 - Vendor-specific, e.g. external NIC utility
 - Third party and less common
- EAP supplicant must support the same EAP protocols on the AS
- Is not the driver



OS integrated software may be the NIC configuration settings

The Supplicant

- Many EAP protocols use certificates
 - Based on X.509 standards
 - Trusted authorities
 - Root CA would need to be installed on supplicant end
- Some supplicant client software allow to input credentials directly
- Domain users and computers can leverage Active Directory

802.1X Authenticator

- Port traffic controller
- Two virtual ports: controlled and uncontrolled
- Authentication traffic only passes
- Authenticator can be an access point or WLAN controller



UMBC | CYBERSECURITY
Training Centers ACADEMY

The uncontrolled port only allows EAP traffic to pass through it whereas the controlled port blocks all other non-EAP types of traffic

The Authenticator

- The middle man in between the supplicant and authentication server (AS)
- Traffic blocker until successful Layer 2 EAP authentication occurs
- Communicates with the AS
- Authenticator and AS might be the same device in a standalone autonomous AP

Authenticator to AS Comms

- Authenticator has to know how and where to talk to AS
- IP address of the AS
- UDP ports 1812/1813 or UDP 1645/1646
- Shared secret
 - Validate and encrypt communications



IANA assigned UDP 1812 and 1813 for RADIUS; pre-IANA might be configured for UDP 1645 and 1646

802.1X Authentication Server

- Validates supplicant's EAP credentials
- Uses a native database or proxy queries
- Notifies the authenticator if successful



UMBC | CYBERSECURITY
Training Centers ACADEMY

If successful, the port states change. But there's a lot more here.

The Authentication Server (AS)

- Can **proxy** query external databases
 - Active Directory
 - LDAP
 - Proprietary directory services
- RADIUS
- FreeRADIUS
- Cisco TACACS+ and Access Control System

Authentication Server

- RADIUS servers can use attributes in response
- Vendor specific attributes (VSA)
- Attributes shared back with authenticators
- VLAN assignments
- Enhancement of RBAC mechanism
- Integration of Network Access Control (NAC)
- Support Extensible Authentication Protocols



NACs can verify health of clients wanting to get network access. This includes patch levels and AV if necessary

Credentials

- Username/password combinations
- User@Domain for LDAP
- Machine IDs
- X.509 and Protected Access Credentials (PAC)
 - CACs or USB Fobs
- One-time passwords (SecurID and LastPass)
- Administrative overhead with certs and PKI



Machine ID tied to a security identifier (SID) in Active Directory. Domain objects and computers.

PACs are created by the Radius service and issued out to the individual user identities and later presented back to the same RADIUS server

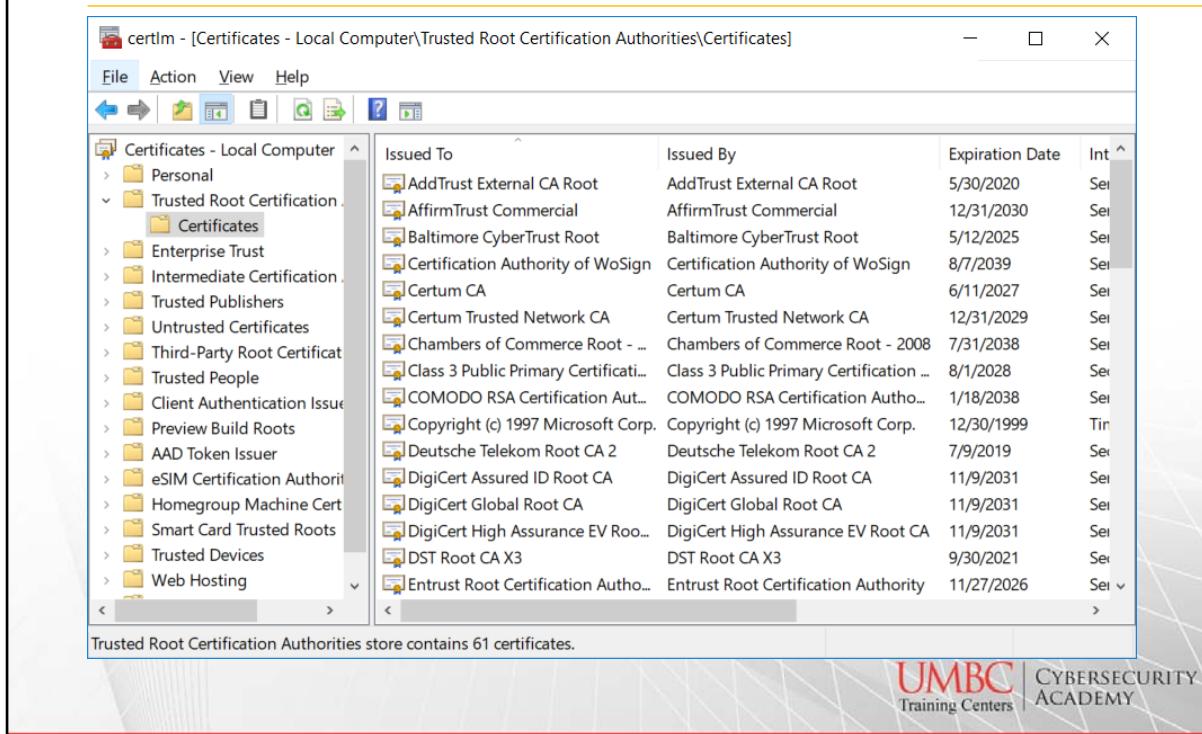
Certificates and EAP

- Best and most secure authentication method is **mutual authentication**
- Certificates from the AS would be presented
- Server certificates can be used to create a TLS tunnel and aid in **tunneled authentication**
- Server certs would be signed by a Root CA
- Root CA cert is stored on the supplicant
- Root CA is most likely already in the OS



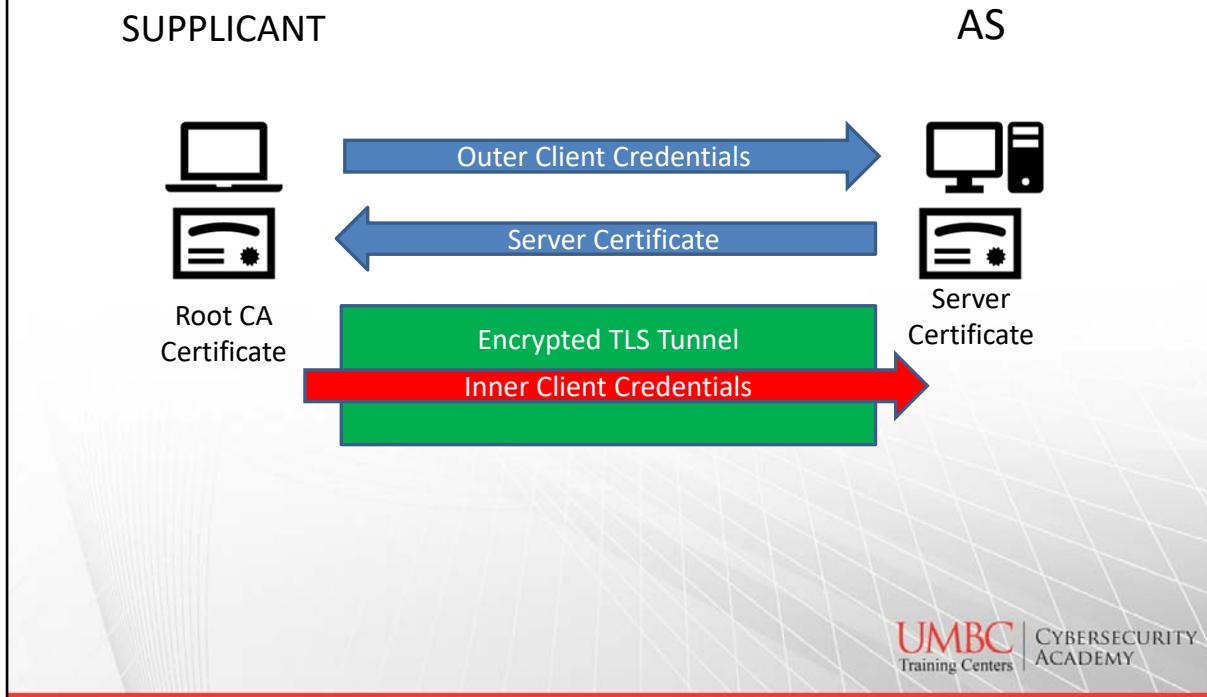
The authentication server validates itself to the supplicant. This requires more administrative overhead because a certificate is needed for the AS credentials.

Win10 Root Certificate Authorities



Updated certificates are pushed out with updates and patches and become part of what is known as certified trust list (CTL)

Mutual and Tunneled Authentication

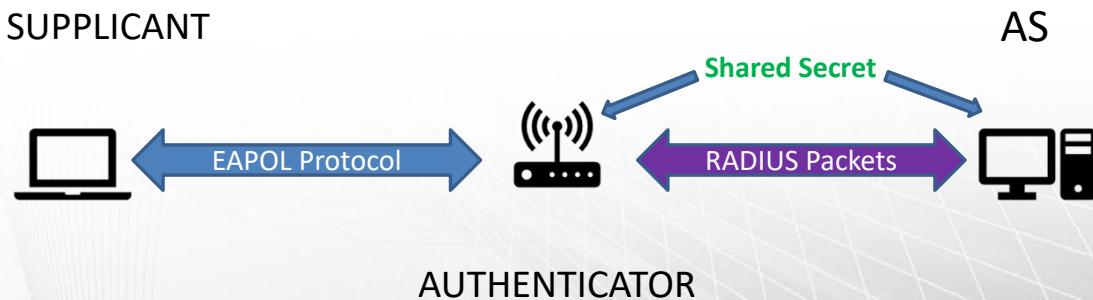


Client Certificates

- Within the context of a larger PKI
- Can be used as credential presented to AS
- Validation credentials of the supplicant
- Internal CA is often the chosen route
- Root CA that signs or authorizes subordinate CA to issue certificates, e.g. Windows PKI

Shared Secret

- Validates authenticator and AS to each other
- EAP data from supplicant is encapsulated in a **RADIUS packet** when passed to AS



UMBC | CYBERSECURITY
Training Centers ACADEMY

Legacy Authentication Protocols

- Before there was EAP
- Password Authentication Protocol (PAP)
- Challenge Handshake Authentication (CHAP)
- Microsoft-CHAP (MS-CHAP)
- MS-CHAPv2
- Legacy = vulnerabilities
- All can be used inside EAP-TTLS tunnels



Password Authentication Protocol originally designed for Point-to-Point Protocol

CHAP used an MD5 hash of the password

MS-CHAP used a weak hashing protocol in early active directory versions

MS-CHAPv2 came out with Windows2K and passes the username in clear text. It does support mutual authentication.

Extensible Authentication

- Extending capabilities for many different authentication methods
 - Layer 2 authentication protocol
 - Can offer uni- or bi-directional authentication
 - In enterprise WLANs, used in conjunction with 802.1X (port-based access control)
 - EAPOL message exchange between AP and client STA



Sometimes you might see EAPOW (EAP over Wireless) in place of EAPOL

EAP Exchange Soup-to-Nuts

1. Probe request and probe response
2. Open authentication request and response
3. 802.11 association request and response
4. EAP identity request from authenticator
5. EAP identity response from supplicant
6. RADIUS access request from Authenticator to RADIUS server
7. RADIUS access challenge / EAP access challenge
8. EAP challenge response / RADIUS access challenge
9. RADIUS access accept / EAP success
10. Four way handshake to generate dynamic keys
11. IP address assignment via DHCP process

Strong EAP Types

- Mutual authentication
- Certificates, X.509 or similar
- Tunneled credentials
 - Two sets of supplicant identities
 - Outer and inner
- Tunnels exist only for the exchange of inner credentials then they go away

Strong EAP Types

- EAP-Protected EAP (PEAP)
- EAP-Tunneled TLS
- EAP-TLS
- EAP-Flexible Authentication via Secure Tunneling (FAST)
- EAP-SIM

EAP-PEAP

- EAP inside of EAP...Inception?
- **Uses outer and inner identities**
- Two distinct phases
- It protects the inner identity
- 3 common inner EAP methods
 - EAP-MS-CHAPv2 EAP-PEAPv0
 - EAP-TLS EAP-PEAPv0
 - EAP-GTC EAP-PEAPv1

EAP-PEAP

- Regardless of version there are **two phases**
- Phase 1 uses outer bogus or anonymous identity and establishes a TLS tunnel
- Phase 2 uses the encrypted TLS tunnel to do the “real” inner EAP method

EAP-PEAP Inner EAP Methods

- EAP-MSCHAPv2
 - No certificates
 - Username and hashed password
 - Popular default version of PEAP
- EAP-TLS
 - Client-side certificates required
- EAP-Generic Token Card (GTC)
 - Cisco's version
 - OTP, tokens, or username/passwords

EAP-TTLS

- Tunneled TLS
- Two phases
- Used with **legacy inner authentication protocols**
- Client-side certificates are optional
- Usually username and password types
- Quite common



Server side certificates are necessary obviously to establish the phase one TLS tunnel

EAP-TLS

- Very secure EAP method
- Need client-side certificates for **mutual authentication**
- Deployed with PKI infrastructure in place
- Tunnel is not normally used



Again, obvious that server side certificates will be needed for the TLS tunnel establishment.

Tunneling is optional because of the certificate presented to each other.

EAP-FAST

- Remember FAST-PAC!
- Designed as a replacement for LEAP
- Provides mutual authentication
- Quasi-certificates called PACs
 - Protected Access Credentials
 - Generate by the RADIUS server and provisioned to clients, either manually or automatically
- At least two, sometimes three phases



This is another Cisco developed protocol

LEAP by Cisco was susceptible to offline dictionary attacks, why? The username is sent cleartext!

So there was a need to replace LEAP, but not need certificates.

The PACs need to get on the clients somehow. This can be done manually by an administrator or automatically in optional Phase 0. Otherwise if manually done, then the two ends go straight to Phase 1 which proceeds just like the other Tunneled Authentication methods in the previous EAP methods.

There are some flaws with EAP-FAST: During automatic provisioning, the supplicant just trusts that the PAC being provisioned comes from a trusted source. Which may leave the whole provisioning susceptible to MITM attacks

EAP-SIM

- Based on RFC 4186
- Uses the SIM card in a GSM device
- Extends authentication by allowing the parties to *mutually authenticate* each other
- EAP-SIM uses dynamic session-based keys
- Allow handsets to transition from GSM network to 802.11 using EAP-SIM authentication
- Seamless switching between mobile and Wi-Fi networks—better speeds and reduce GSM traffic

EAP-SIM

- Requires a special RADIUS (AAA) server
- RADIUS server converts the RADIUS protocol request to MAP protocol
- The EAP request is forwarded to 3G network Home Location Register (HLR)

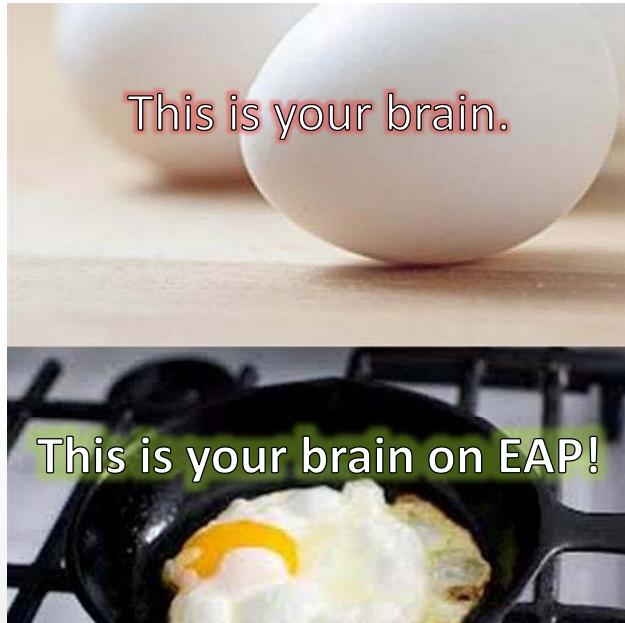
Weak EAP Types

- Pseudo or nonexistent mutual authentication
- Usernames passed in cleartext
- Cryptographically weak hashing of passwords
- Vulnerable to social engineering or offline dictionary attacks
- EAP-MD5 and EAP-LEAP

Summary

- AAA
- 802.1X
- Certificates
- Legacy Authentication
- Lots on EAP types
- Which ones require client-side certs
- Which one support true mutual authentication
- What a generic EAP exchange looks like

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

RADIUS and LDAP

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- LDAP
- RADIUS
- Attribute Value Pairs

It's Lightweight!

- Lightweight Directory Access Protocol
- A way to provide directory services
- Hierarchical databased structure
- Usernames and passwords
- Active Directory
- Novell eDirectory Services
- Solaris NIS+
- OpenLDAP



Directory information such as users, groups, computers, objects, files, folders, username and passwords

LDAP

- LDAP can use either TCP or UDP 389
- LDAP over SSL TCP 636
- Can be queried by RADIUS AS
 - Proxy authentication



UMBC | CYBERSECURITY
Training Centers ACADEMY

RADIUS

- What can it do for an organization?
- Couple it with an enterprise WLAN?
- Framework for 802.1X/EAP authorization
- Melds with RSN authentication and port control requirements for an enterprise
- Two IETF RFCs
 - RFC 2865 and RFC 2866
- Client/Server Model



AAA Authentication and Authorization and Accounting

Is part of the RSN framework for authentication and port control

RADIUS

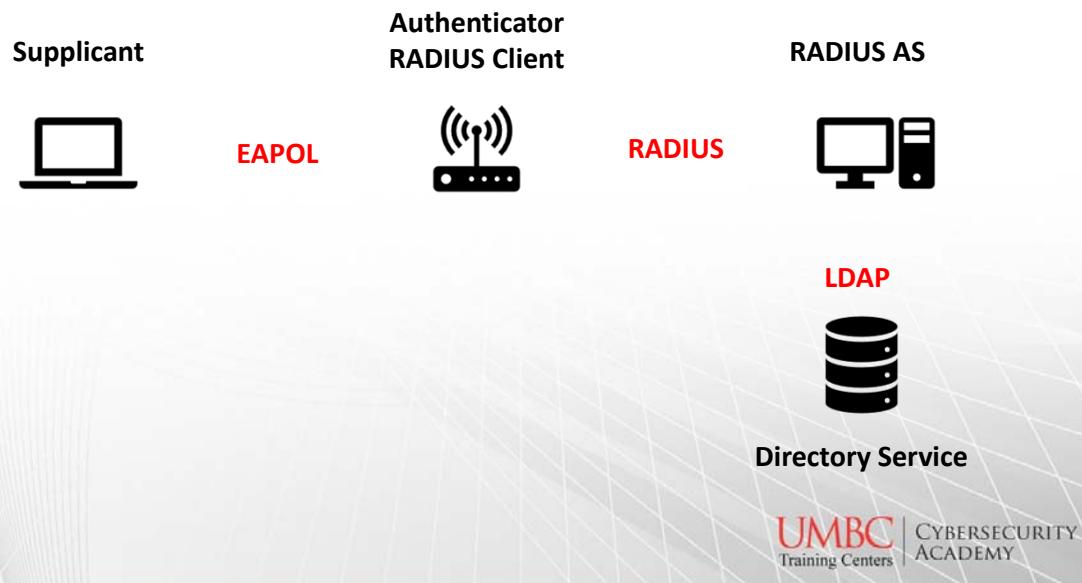
- **Authentication and Authorization** defined under RFC 2865
- RADIUS client communicates with the server using RADIUS protocols and packets
 - Access-Request
 - Access-Challenge
 - Access-Accept or Reject
- The RADIUS client is the authenticator



The client can also be known as the Network Access Server.

The access-challenge request more information from the supplicant based on the implemented EAP type

RADIUS



RADIUS

- Accounting defined in RFC 2866
- Track user and device access to network resources
- Provide forensic information if needed
- Back in the day it was used for actual accounting for billing purposes



Who authenticated, when, how long they were in, what they accessed and who much data was moved.

RADIUS Config

- Shared Secret between RADIUS client and server
- IP address of the RADIUS server
- UDP Ports 1812/1813
- Server certificate for TLS tunnels
- Internal database or backend proxied authentication?



If using a server cert, the corresponding Root CA has to be installed on the clients

RADIUS Proxy Authentication

- RADIUS service may be integrated into AD
 - Network Policy Service
- If not, then RADIUS server joined to a domain
- Or, LDAP account used by RADIUS to query
- IP and ports of directory service configured?

RADIUS Deployments

- Simple, Easy Single Site
 - Everything is local
- Distributed Sites
 - Autonomous RADIUS, Replicated LDAP
 - Autonomous RADIUS, Centralized LDAP
 - Centralized RADIUS and LDAP



Distributed Autonomous Radius and replicated LDAP doesn't require authentication across the WAN. If the WAN link goes down, no worries.

In a Distributed Autonomous RADIUS and Centralized LDAP might be a little more cost effective because you don't have to replicate LDAPs locally. Authentication does happen over the WAN link, and when the WAN link breaks down, we break down. No new clients can authenticate.

Everything centralized: might be more cost effective but consider where the EAP authentications are going...across the WAN and we know what happens when the WAN breaks down. Roaming may be affected for client that don't support fast secure roaming such as OKC or Fast BSS Transition because of the lag time to go over a WAN link to do EAP authentication.

RADIUS Proxies

- Why proxy?
- Vendor licensing or config restrictions
- Each AP authenticator might require a license or static IP address
- Another network device can be the advocate for many more devices—one IP, one license
- Could proxy for domains or realms



The realm presented to the proxy would help the proxy distinguish and choose which realm or domain's RADIUS server to send the authentication

Miscellaneous RADIUS

- Enterprise APs can have built-in RADIUS and LDAP client
- Some RADIUS servers can offer up captive portals and MAC authentication
 - Hotels and other hotspots
- TLS for RADIUS communicating peers
 - More secure than traditional RADIUS comms
 - TCP 2083 instead of UDP 1812/1813



Traditional radius comms used MD5.

RADSec is next gen Radius protocol

Attribute Value Pairs

- Used to store and provide data in database
- AVP can communicate AAA information
 - 255 standard RADIUS attributes
- Carry data in the RADIUS request and response packets
- Vendor Specific Attributes (VSA)
 - Up to 255 additional extended attributes

Attributes

- Specified in Access-Accept messages as a result of 802.1X/EAP authentication process
- Can be used for VLAN assignment IAW policy
- Assignment of users to roles
- Role-based access controls (RBAC)
 - Finer tuned access restrictions for users
 - Users, roles (profiles) and permissions
 - Tied in with AD or LDAP

Summary

- How LDAP and RADIUS tie together
- RADIUS deployment types
- Attribute Value Pairs
 - VLAN assignment
 - Role-based access controls
 - Tie in to AD or LDAP user permissions and assignments

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

Photo from quora.com

Security Risks

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Rogue Devices
- Eavesdropping
- Attacks
- Hijacking
- P2P
- Management Interfaces
- Dirty Guest Access and Hotspots

Rogues

- Any wireless device connected to wired infrastructure not administratively managed
- Provides a wireless portal to the network
- Intentional but most likely not malicious
- Access point
- Adhoc IBSS connection
- Wireless printer
- IoT devices such as cameras



More often than not it was an employee just wanting better more convenient access to network in some way.

Rogue Risks

- Data theft
- Data destruction
- Service interruptions
- Malware
- Warez
- Third-party attacks

Rogue Prevention

- Effectively communicated policies and training
- Disallowing IBSS communications
- Ethernet port controls, 802.1X
 - SNMP port suppression
- WIDS/WIPS
 - WIPS can Layer 2 DoS device
 - Effective against 2.4/5GHz



Rogue devices operating outside the normal ISM or UNII bands may go unnoticed, e.g. 4.9GHz and 900MHz devices.

Eavesdropping

- Recall that devices go off channel and listen/probe for other basic service sets
- Listening for beacons or conducting probe requests for any BSS
- Can be casual or malicious
- Casual is broken down into passive and active

Casual Eavesdropping

- WLAN discovery
- Hardly considered illegal*
- Listening for beacons is **passive scanning**
- Using probe requests and null probes is **active scanning**
- Free tools to make it easy and fun

Malicious Eavesdropping

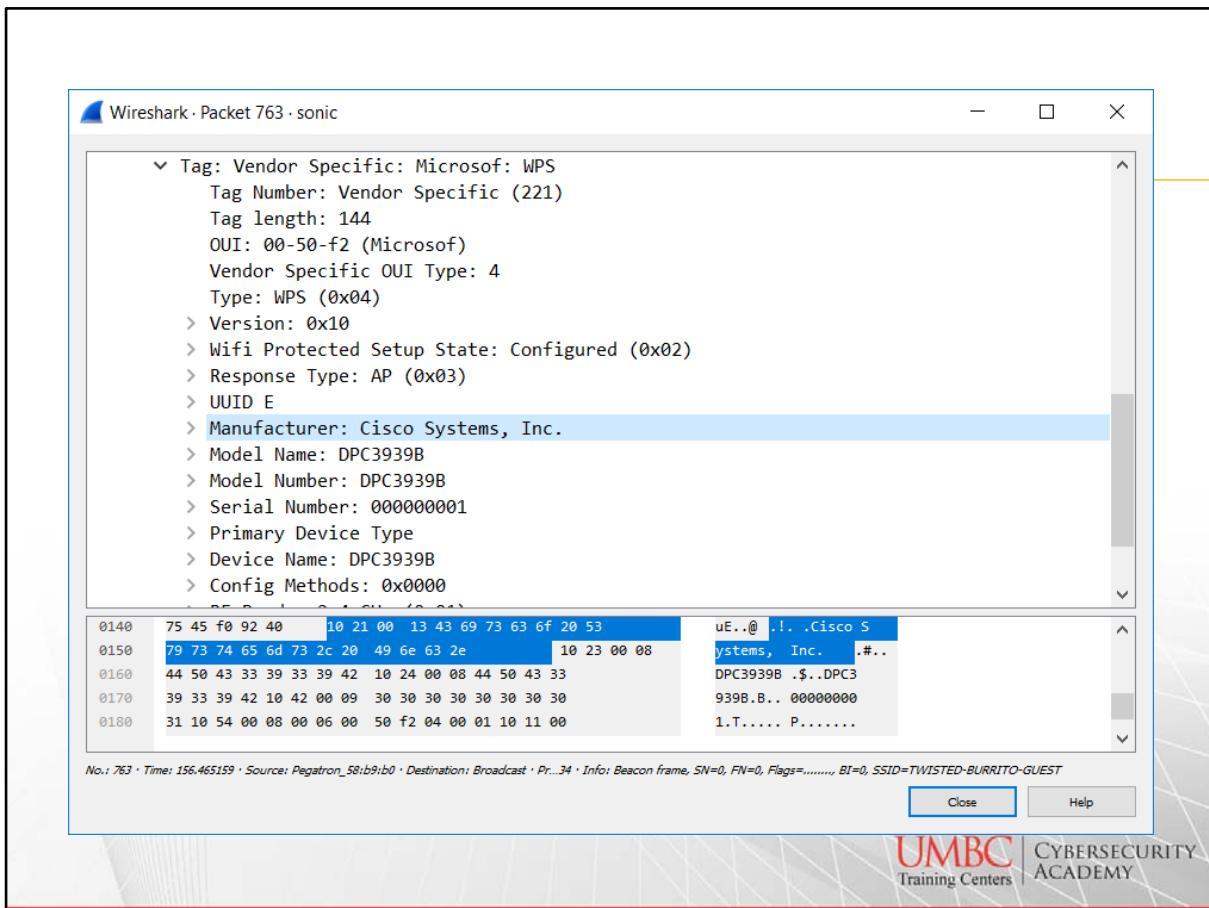
- Enter a protocol analyzer and legal issues
- Setting a wireless interface in **monitor mode**
- Capture 4-way handshakes
 - Try to recover the passphrase and PSK
 - Decrypt session data

Why Does Eavesdropping Matter?

- Layer 2 information can be gathered cleartext
- MAC filtering, if in use, can be analyzed
- Wired leakage from Layer 2 discovery protocols
- WIDS/WIPS cannot hear a listener
- Vendor information about devices
 - Research vulnerabilities



Layer 2 discovery protocols: Link Layer Discovery Protocol and CDP can give up unwanted information



Eavesdropping Mitigation

- Encryption, of course!
- CCMP/AES to protect what?
- Disabling talkative wired protocols
- With PSK and passphrases: > 20 mixed chars
- RF Shielding

Authentication Attacks

- Offline dictionary attacks and weak authentication processes
 - EAP-LEAP
 - Legacy Authentication, MS-CHAPv2
- Passphrases
 - Social engineering
 - Offline dictionary brute forcing



Keep in mind legacy authentication protocols can be used if they are tunneled correctly.

What EAP methods allow for legacy authentication?

Should never use anything less than 20 characters and definitely no PSK in the enterprise!

Denials-of-Service

- Attacker prevents legitimate users from accessing information or services
- Either your device is the target or a service not on your device is the target
- DoS against a WLAN essentially disables the WLAN and any resources via the portal
- Can be either malicious or unintentional
- Target can be entire WLAN, an AP, or a client

Denials-of-Service at Layer 1

- From a WLAN perspective can be Layer 1 or 2
- Layer 1 is the physical medium, RF, channels
- Typically, non 802.11 device in same RF space
- Disruption of services can be continuous or sporadic in nature, e.g. microwave, Bluetooth
- Intentional devices can be narrowband or wideband transmitters
- Intentional DoS can be amplified with antennas



Some layer 1 intentional devices may be legitimate in the fact they are trying to prevent wireless devices in a non-wireless environment.

Narrowband devices can affect a single channel or portions thereof, whereas, a wideband device can affect an entire band such as 2.4 GHz or 5.0 GHz.

Denials-of-Service at Layer 1

- Intentionally putting a 802.11 device in continuous transmit mode owns the channel
- Layer 1 attacks mess with the CSMA-CA and the half-duplex nature of 802.11
- **Physical carrier sense and the Clear Channel Assessment to “avoid a collision”**
- If a device is talking, everyone else waits

Denials-of-Service at Layer 1

- Intermittent RF interference can affect frames and bit errors = less acks = higher retrans rates
- Intermittent interference then affects overall performance and latency
- RF attacks can be a precursor to highjacking, man-in-the-middle, or Wi-Fi phishing
- Check your NMS, WIDS/WIPS, use a SpecA

Denials-of-Service at Layer 2

- MAC sublayer of data-link layer
- Tampering with 802.11 frames
- Spoofing disassociation and deauthentication
 - Both are notifications and not requests
 - Deauth results in disassociation
- Target a single STA or AP
 - Destination address is manipulated

Denials-of-Service at Layer 2

- Nefarious channel beaconing
- Probe response flood
- Conversely, how about an association flood
- Fake AP
- The NAV timer and virtual carrier sense
- But what about 802.11w?
 - Only protects some management frames
 - Not all Layer 2 attacks can be prevented



Beacons out as the legitimate AP with current SSID but advertising a bogus channel. The bogus channel may be interpreted incorrectly causing the device to DoS itself?

Probe response flood sends out spoofed probe response that appear to come from the legitimate AP to the client which then tries to connect and is left hanging.

An association flood hits the AP with numerous association requests which might hit max threshold for client associations thus preventing anymore legit associations.

FakeAP is a tool that can broadcast out a large number of fake SSIDs and BSSIDs, as a result, a client may take significant time to attempt to authenticate to a non-existent WLAN.

What if an attacker could send out data frame with the Duration/ID set to something high in terms of microseconds, something approaching 32,767? By design, other stations would look at the Durations and set their count down timers (plus a random backoff) Virtually, the medium would be busy but in reality, it's not. The attacking devices has won contention.

Management Frame Protection is designed to deliver robust management frames to protect them or help thwart spoofing of deauth and disassociations.

MAC Spoofing

- We should know that MAC filtering is garbage
- It is used sometimes to identify legitimate hotspot or pay-for-access clients
- Piggybacking to circumvent captive portals
- Applications and built-in utilities can do this
- Can be detected with a WIPS/WIDS looking at sequence numbers and MAC associations

Wireless Hijacking

- The notorious **Evil Twin**
- Soft AP and dual interface cards that are bridged together
- Advertise as the same SSID with more power
- Can RF jam 'em off or deauth them to come to your soft AP
- Enable IP forwarding, DHCP, and captive portal
- SSL striping and **man-in-the-middle** creds grab

Wireless Hijacking

- Wi-Fi Phishing is throwing up a captive portal
- Gather some form of credentials with fake login or similar user data used later
- Hijacking in any of these forms can be prevented with mutual authentication

More Badness

- Encryption cracking
 - WEP and weak IVs
 - ARP flooding to generate IVs
 - Short passphrases and WPA/WPA2-personal
- Prevented with CCMP/AES and strong >20 character length passphrase or 802.1X/EAP

Even More Badness

- Peer-to-peer attacks
 - Ad-hoc IBSS networks
 - APs that allow direct connections between STAs
- Mitigated with **client isolation and personal firewalls**
- Client isolation is a feature that disallows packets arriving at AP from going back out wireless interface

Management Interface Exploits

- Can be chewy-GUI based or command line
- In the probe response, vendor information
- Open source research
 - ExploitDB, US CERT, NIST NVD
- Is SNMP version less than 3?
- Is HTTP the default Layer 7 protocol?
- Is TELNET really enabled? It's 2019!
- What's an admin to do?

Social Engineering

- The human element
- Hi, I'm from...I was wondering if...
- Emails
- Phone calls
- The service person
- Mitigated with training, enforcement of policies, and not using static information

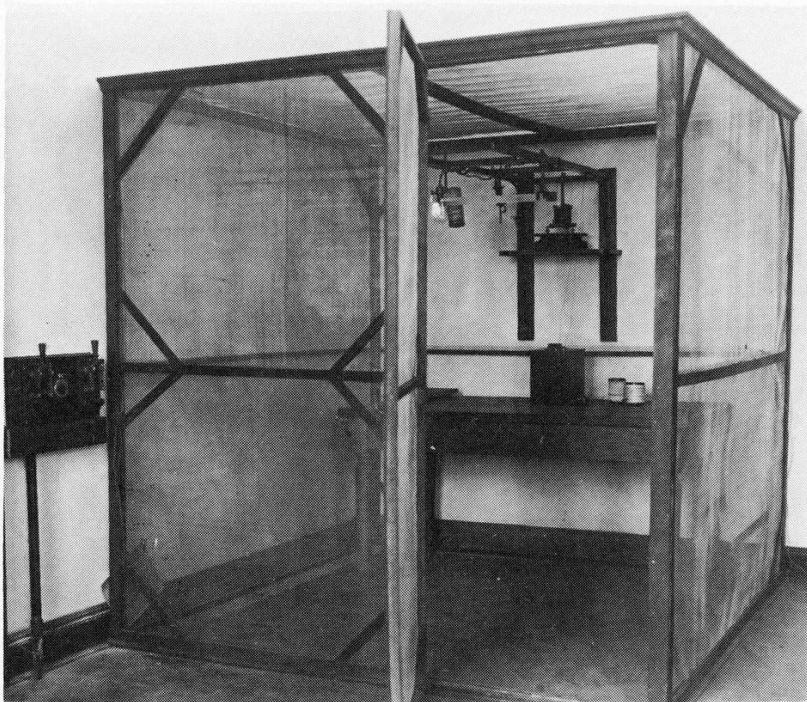


Static information might include passphrases

Hotspot Hygiene

- VPNs when ever possible
- No peer-to-peer what-so-ever
- Personal firewalls that work and updated
- Throw away devices

QUESTIONS??



CYBERSECURITY
ACADEMY



It's a Party, BYOD!



Overview

- Mobile Device Management
- On-boarding
- Guest Access
- Network Access Control

Mobile Device Management

- Company devices on company WLAN
- Employee personal devices on company WLAN
- Guest devices on company guest WLAN
- How do we onboard all of these devices while ensuring safe, secure, and healthy WLAN?
- Manage, secure, and monitor the devices

Is it Company or Personal?

- We can bin devices into company-issued (CID) or bring-your-own-device (BYOD)
- CID would need more in-depth security, why?
- Configs set on CID:
 - VPN clients, corporate email, Wi-Fi profiles, applications, encryption, etc.
 - Remote wipe or lock
 - Standardized software and hardware
- BYOD = mishmash

Is it Company or Personal?

- What's a company to do?
- It depends...
- Onboard the devices with MDM solution
 - Change settings on provisioned devices
- Implement Network Access Controls (NAC)
 - Controls access to network resources



NAC may be an alternative to MDM if the BYOD devices can't be touched, configured, or subject to strict policies.

Mobile Device Management

- Components that make up the architecture
 - Device, obviously
 - MDM server enrolls and provisions devices
 - Quarantine area (walled garden)
 - AP or WLAN Controller
 - Push notifications server
 - Google Cloud Message
 - Apple Push Notifications
 - Interface with Directory Services



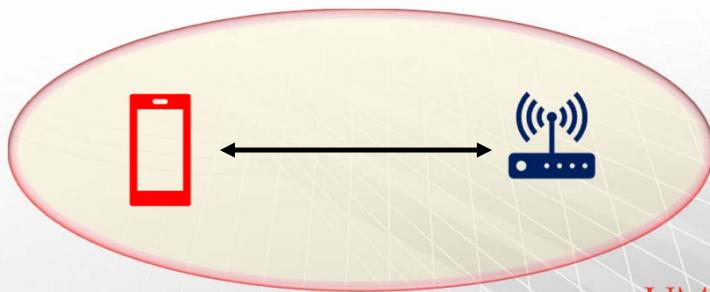
MDM server can lay down profiles, certificates, and configurations. Reference white/black lists of devices. MDM service can be local (physical or virtual) or cloud-based.

Walled garden is a restricted area until onboarding enrollment and provisioning are complete

Over the air management of devices are accomplished through a push notification service.

MDM Enrollment Process

- First hurdle before access to resources
- Used with CID or BYOD
- Device establish association to AP
- Held inside walled garden

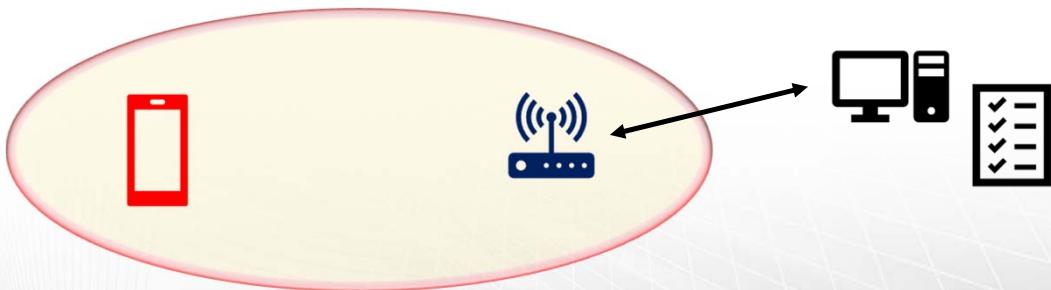


UMBC | CYBERSECURITY
Training Centers ACADEMY

The only thing the device can access is DHCP, DNS, Push notifications, and MDM server

MDM Enrollment

- The AP or Controller contacts MDM server
- Enrollment status checked



UMBC | CYBERSECURITY
Training Centers ACADEMY

If previously enrollment is still valid, the device is released from the walled garden, otherwise the MDM do some more checking

MDM Enrollment

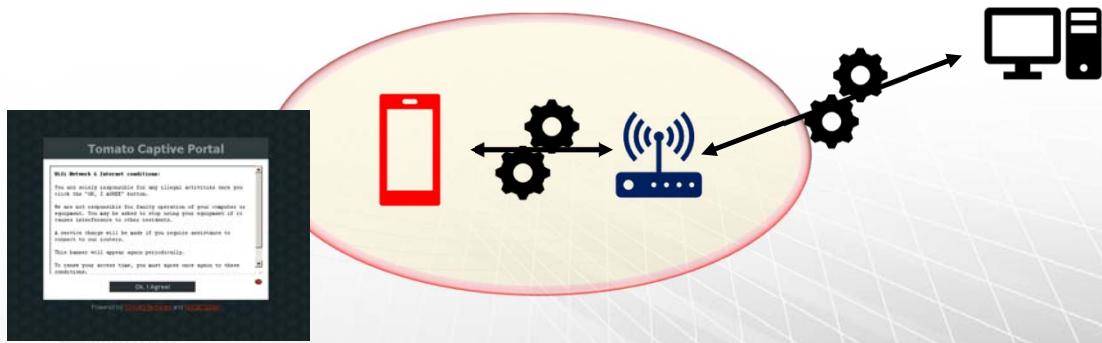
- If device is not enrolled, it may be cross-checked with a Directory Service



UMBC | CYBERSECURITY
Training Centers ACADEMY

MDM Enrollment

- If the directory service checks out, then the device is redirected to MDM server for enrollment process

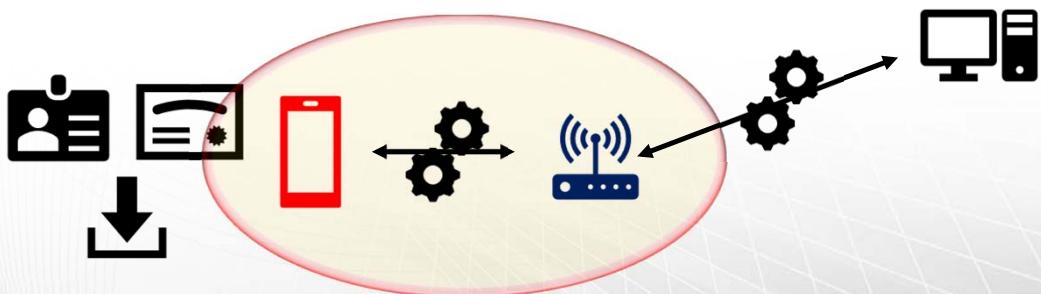


UMBC | CYBERSECURITY
Training Centers ACADEMY

Opening a browser causes a redirect to a captive portal. Should have some legal disclaimer and other goodness related to accepting it otherwise they will not be allowed to proceed.

MDM Enrollment

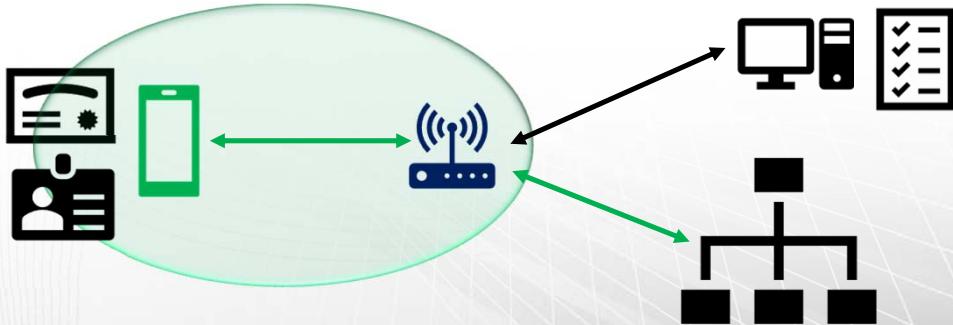
- Once accepted, a profile and certificate may be installed using encrypted channels



UMBC | CYBERSECURITY
Training Centers ACADEMY

MDM Enrollment Success

- If everything goes well, MDM server releases the device
- Device abides by the restrictions and settings



UMBC | CYBERSECURITY
Training Centers ACADEMY

MDM Profiles and Agents

- Profiles create device configs and restrictions
- MDM profiles are created on the MDM server and installed during the enrollment
- Wi-Fi settings and certs can be pushed down
- Agents are application software on the device
 - More so with Android devices
- Agents enforce the pushed restrictions and configurations and respond to new pushes



Wifi settings may designate a specific SSID and security settings. Client certificates can be pushed.

Profiles on personal devices can be removed locally or through the web as needed.

These agents and management of profiles would normally disallow access to personal emails, SMS texts, and the like.

Over the Air Management

- After a device has been enrolled, an admin can make ad-hoc changes to the profile on MDM server
 - Configurations and application changes
 - Device restrictions
 - Message to employee
 - Lock or wipe the device
- MDM server reaches out to Push Service
- Push service gets it to the device



Device can be subjected to application management. All the applications can be seen and monitored. Verification of black/white listed apps. New applications can be pushed or updates to existing one can occur. vE

BYOD and Self-Service Onboarding

- Need to onboard & provision personal devices
- Require a root CA certificate to access secure corporate resources
- Catch-22 scenario
 - Need a certificate to access the network
 - Access the network to get a certificate
- Dual-SSID onboarding
- Single-SSID onboarding



If you have an employee that would like to use his/her personal devices to access the corporate secured network, how do you effect that? How do you get a root CA certificate on the supplicant if the device is not standard issue for the company?

Dual-SSID Onboarding

- Employee connects to an open SSID
- Walled off and presented with captive portal
- Sign-in and download an onboarding app
- Onboarding app pulls down the certificates
- Certificate is used to access secure SSID using 802.1X/EAP process
- Amazing

Single-SSID Onboarding

- Employee connects to secure SSID
- Authentication via 802.1X/EAP-PEAP
 - Two phase: outer, inner identities
 - Server cert is validated through well-known CA
 - Inner identity can be true domain creds
- Once authenticated, an onboarding app is pulled down and installed
- RADIUS change of authorization; reconnect



EAP-PEAP aka protected EAP has three versions v0 MS-CHAPv2, v0 EAP-TLS, v1 EAP-GTC.

Recall that MS-CHAPv2 uses usernames and passwords inside.

After the user/device is initially authenticated, there are no granular restrictions applied yet.

After the onboarding occurs, finer permission, RBAC, VLAN assignment and such can be applied with RADIUS CoA.

RADIUS Change of Authorization

- Allows for dynamic or ad-hoc changes to client profiles without having to wait for reconnect
- Change user/device permission on network
- RFC 3576 defines CoA and may be referenced on device configurations



If there wasn't a CoA mechanism, any changes made would not take effect until the client logged off and logged back onto the network.

What About Those Dirty Guests?



quickmeme.com

UMBC | CYBERSECURITY
Training Centers ACADEMY

Guest WLAN Access

- Access to the Internet and nothing else!
- Protect the corporate network from guests
- Separate SSID, e.g. “UMBC-Guest”
- Guest Virtual LAN and firewall policies
- Absolutely need a captive portal with legal disclaimer
- Consideration of how they get authorized for guest access



How do guest get just Internet access? Self-registration, employee sponsorship, social login

Guest Segmentation

- In the past, SSID was paired with a VLAN (1:1)
 - Multiple SSID broadcasting added WLAN overhead
- Need a separate, easily identifiable, and unhidden SSID for guest access
- VLAN for guests on distinct subnet
- Couple VLAN with firewall policies
 - Eliminates tunneling traffic elsewhere
 - Prevent co-mingling of traffic
 - Point right out to the Internet gateway



RADIUS attributes can be used to assign users to separate VLAN under one SSID.

The guest SSID might need to be displayed especially in multi-tenant buildings

Guest Access and Firewalls

- Permit only necessary ports: DHCP, DNS, HTTP(S), IPSec
- Disallow ports such as SMTP, remote admin
- Stateful firewalls? What are they?
- Application firewalls and DPI?
- **Keep in mind, this is for basic access to Internet and that is all**



Block certain application and perform DPI on unencrypted communications.

Captive Portals

- Web browser becomes an authentication service with legal disclaimer and AUP
- Initial browser traffic is redirected to AP or WLAN controller no matter the destination
- Can be used to register a guest and device
 - MAC authentication enforcement



UMBC | CYBERSECURITY
Training Centers ACADEMY

How Did They Even Get Access?

- Guest accounts can be created ad-hoc through on-site or cloud management services
- Through self-registration on the captive portal
 - Email or text confirmation of credential
- LDAP and employee sponsorship
 - Company gets involved
 - Only legit “authorized” guests get access
 - Email or text confirmation

How Did They Even Get Access?

- Popular social logins using Open Standard for Authorization (**OAuth**) and access tokens
 - Used by retail and service for marketing



The tokens are issued to third-party clients from an OAUTH service. The [OAuth 2.0](#) specification defines a *delegation* protocol that is useful for conveying *authorization decisions* across a network of web-enabled applications and APIs. OAuth is used in a wide variety of applications, including providing mechanisms for user authentication. This has led many developers and API providers to incorrectly conclude that OAuth is itself an *authentication* protocol and to mistakenly use it as such.

Now That You Have Guests

- Enforcement of **client isolation** to prevent peer-to-peer attacks
- Rate limiting and content filtering



UMBC | CYBERSECURITY
Training Centers ACADEMY

Now They Want Encryption

- How can you give them guest access and provide security?
- Configure guest access with PSK
- How about Hotspot 2.0 and Passpoint?
 - Roaming similar to cell networks
 - Device checks for participating networks
 - Credentials, certificates, SIM card
 - Can use PKI and all the accompanying encryption



Xfinity and attwifi

Moving on...Network Access Control

- NAC: Think of it as health and welfare state of your device—accessing your security state
- Access device capabilities and configs
- Can be tied with RADIUS and network access
- Access denied until shortcomings remediated
- Posture assessment
- Fingerprinting
- AAA to track devices and users



Posture assessment could use a persistent agent (company devices) or dissolvable agent (BYOD) to check for security software state, OS updates and patches.

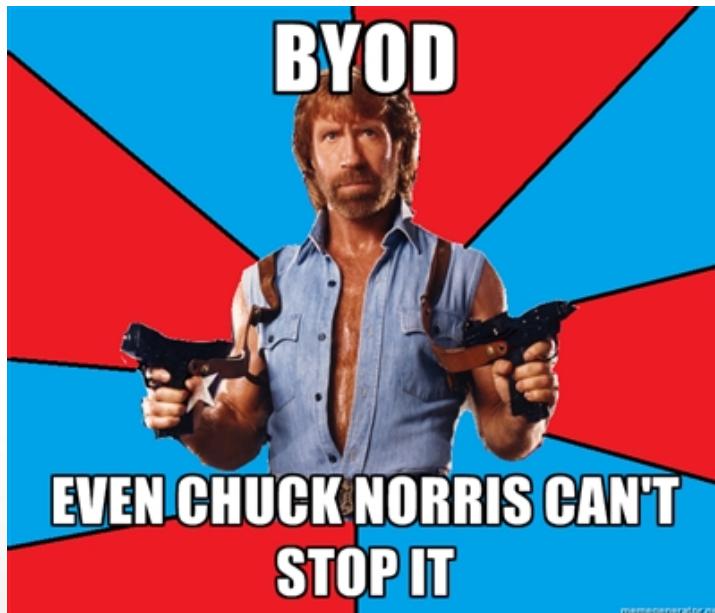
Fingerprinting is used to determine a device's operating system. This determination may lead to further decisions about what sort of agent or application that may need to be installed to get access to the network or whatever.

AAA

Summary

- CID Mobile Device Management
 - Certificates and profiles
- BYOD On-boarding
- Guest Access
 - Segmentation with SSID, VLAN, firewalls
 - Safe and relatively secure access
- Network Access Control

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

WLAN Auditing and Analysis

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Layer 1 and 2 Audits
- Pentesting
- Beyond Layer 1 and 2 Audits
- Audit Recommendations
- Auditing Tools

Auditing in General

- Compliance with company policies, government regulations, industry standards
- Overtime the WLAN changes physically and logically as well as 802.11 standards
- After changes to WLAN
- Provides paper-trail of due diligence and care
- Don't be that company!



Ask about the Target breach in 2014 and how network segmentation was to blame.

Auditing in General

- Audits should occur from different approaches
- View it from Layer 1 and up
- The WLAN may not be the soft point in
- Humans are not perfect
- What are your network devices telling you
- How about some physical security
- **Assess the threats and mitigate the risk**



After an audit is conducted, there should be report that includes mitigation proposals. This can include technical and not technical solution. Examples of each would be a WIPS and a policy.

Layer 1 Auditing

- Looking for sources of interference
- Non-802.11 and 802.11 devices
- Use wireless protocol analyzer
- Really talking about spectrum analyzer
- RF in 2.4 and 5 GHz channels
- Searching out devices that could cause a DoS at Layer 1
- Layer 1 interference can result in Layer 2 problems, e.g. BER and retransmissions

Layer 1 Interference

- Microwaves, security cameras, Bluetooth, baby monitors, cordless phones
- Interference can be narrowband or wideband in nature
- Narrowband is characterized by high amplitude and affecting smaller freq space
- Wideband can disrupt entire 2.4 or 5 GHz space or large sections

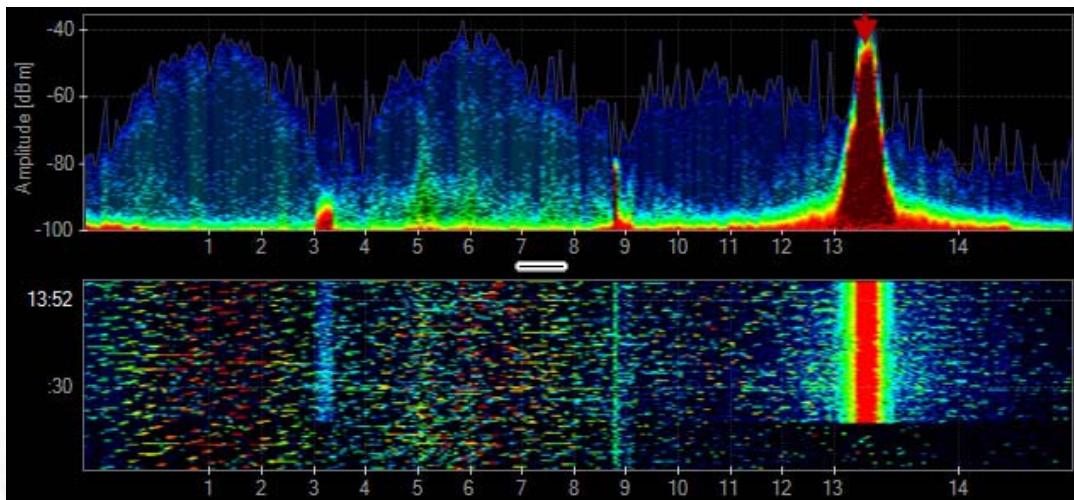


Using a spectrum analyzer is the best tool to locate the narrowband interferer

Layer 1 Interference

- All band interference is another category
- See this with FHSS and Bluetooth
- Not necessarily causes DoS but rather increased in corrupted frames and retrans
- Keep in mind, WLAN operate in unlicensed frequencies and devices state so

Narrowband Interference

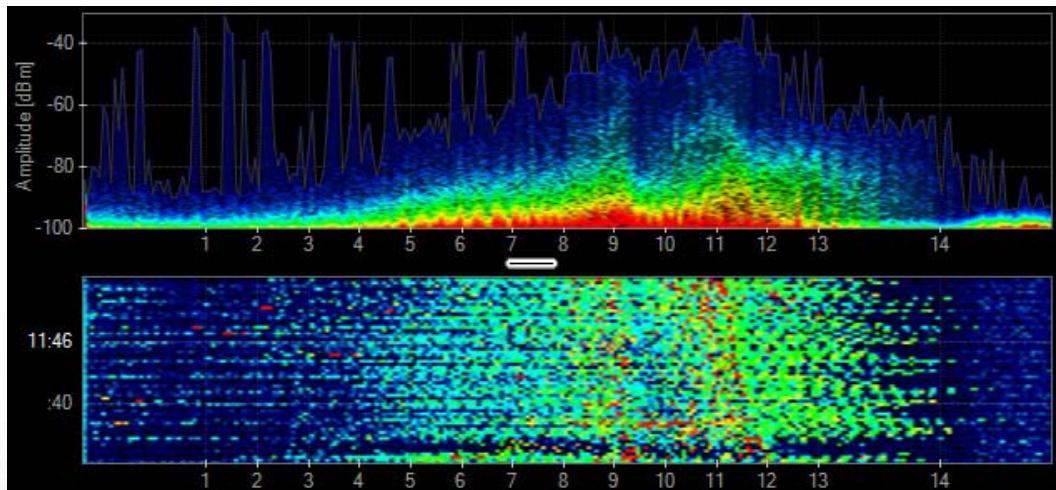


UMBC | CYBERSECURITY
Training Centers ACADEMY

Metageek.com

Cordless phone

Wideband Interference

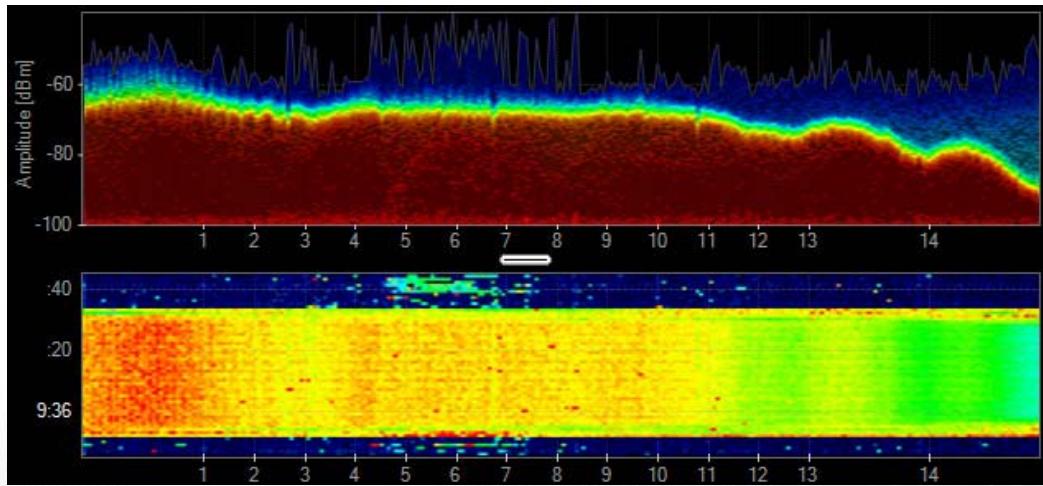


UMBC | CYBERSECURITY
Training Centers ACADEMY

Metageek.com

Microwave oven

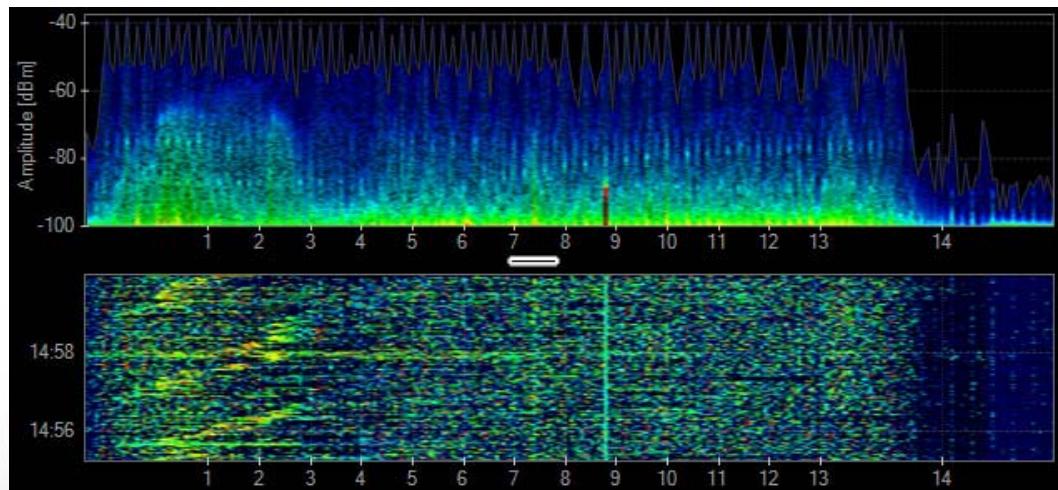
Wideband Jamming



UMBC | CYBERSECURITY
Training Centers ACADEMY

Metageek.com

Bluetooth All-band



UMBC | CYBERSECURITY
Training Centers ACADEMY

Metageek.com

Layer 2 Auditing

- Detection of unauthorized devices
- If you're not using a WIDS/WIPS
- Not necessarily looking coverage or capacity or what neighbors are nearby
- Can be the basis of device inventory
- Compliance with established AKM process
- Sensitive layer 2 information isn't leaked out



Device inventory can be the whitelist used later if you do implement a WIDS/WIPS system.

Authentication and key management. Are all devices using the proper RSNA?

Sensitive information like device name, vendor, firmware versions.

Layer 2 Auditing

- Analyze and build a picture of key information
- MAC addresses of clients and APs
- SSIDs, neighbors, and channels
- Traffic classification and amounts, e.g. QoS
- Any layer 2 attacks
- Ad-hoc connections

Pentesting

- Simulated attack against the WLAN
- Use white, black, or gray knowledge
- Identify vulnerabilities in hardware, software
- Offline dictionary attacks against cleartext protocols, credentials, and weak passphrases
- Open source tools a plenty to help you and the evil-doers of the world
- Plan, document, recommend, mitigate

Auditing the Wired Side

- Are RBAC, firewalls, and ACLS effective if you are hitting the WLAN side
- WLAN front door may be too hard to get thru
- Use the wired side, get to the wireless
- Wired side protocol leakage
- Management interfaces

Social Engineering

- The human factor
- Getting the information using charm or other means...HUMINT
- Why break in when someone invites you in?
- Static information such as passphrases and usernames are susceptible
- Mitigated with enforced policies, training, and management support

WIPS Audits

- Who's watching the watchers?
- Does the WIDS/WIPS alert and log when it is supposed to?
- Simulate the various attacks
- Plug in a rogue devices
- Adjust the thresholds
- The good bad guys are slow and low

Audit Paperwork

- Remember the deliverables
- Statement of work and get out of jail free card
- NDAs
- What knowledge are you given?
 - Black, white, gray
 - Policies and network maps
- Standards, requirements, regulations that dictate specific testing procedures
- Written report can serve as due diligence / care



How we got in, what we found, where did we go, what are our recommendations?

PCI DSS Assessments



Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Procedures

Version 3.2
April 2016

UMBC | CYBERSECURITY
Training Centers ACADEMY

PCI DSS Wireless Requirements



PCI DSS Requirements	Testing Procedures	Guidance
<p>2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.</p>	<p>2.1.1.a Interview responsible personnel and examine supporting documentation to verify that:</p> <ul style="list-style-type: none">• Encryption keys were changed from default at installation• Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions. <p>2.1.1.b Interview personnel and examine policies and procedures to verify:</p> <ul style="list-style-type: none">• Default SNMP community strings are required to be changed upon installation.• Default passwords/passphrases on access points are required to be changed upon installation. <p>2.1.1.c Examine vendor documentation and login to wireless devices, with system administrator help, to verify:</p> <ul style="list-style-type: none">• Default SNMP community strings are not used.• Default passwords/passphrases on access points are not used. <p>2.1.1.d Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for:</p> <ul style="list-style-type: none">• Authentication over wireless networks• Transmission over wireless networks. <p>2.1.1.e Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.</p>	<p>If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network.</p> <p>In addition, the key-exchange protocol for older versions of 802.11x encryption (Wired Equivalent Privacy, or WEP) has been broken and can render the encryption useless. Firmware for devices should be updated to support more secure protocols.</p>

Audit Recommendations

- Identified the vulnerabilities and here are the recommended mitigation steps
- Might end up being:
 - New or revised policies
 - Employee and admin training
 - Better logical and physical security

Auditing Tools

- Hardware
 - Laptops, wireless cards, antennas, amps, spectrum analyzers, cables and connectors, cameras, APs
- Software
 - Broken into use and attack categories
 - Discovery, encryption and authentication cracking, masquerading, insertion, DoS
 - Kali, Aircrack-ng suite, Kismet, Wireshark, Reaver,



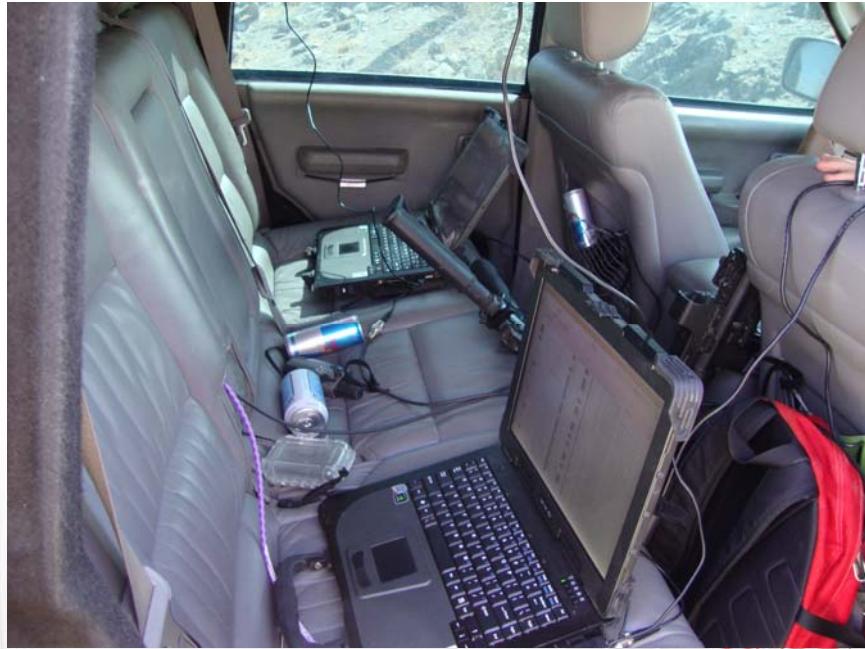
See page 459 for categories

Scanning in Action



UMBC | CYBERSECURITY
Training Centers ACADEMY

Scanning in Action



UMBC
Training Centers

CYBERSECURITY
ACADEMY

Summary

- Layer 1 and 2 Audits
- Pentesting
- Beyond Layer 1 and 2 Audits
- Audit Recommendations
- Auditing Tools

QUESTIONS??



Wireless Security Monitoring



UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- WIDS/WIPS
- Device Classifications
- Analysis and Monitoring
- Specifics About 802.11n/ac
- Management Frame Protections

Need for Monitoring

- Threats abound: Insider threats, evil-doers, APT, and the unwitting employees
- The lines between trusted and untrusted networks and devices become fuzzy
- Centralized capability to provide 24/7 indications and warnings
 - Aggregation of sensors, logs, alerts, forensics
 - Monitoring plus response actions
 - Compliance requirements

WIDS and WIPS

- Threat detection and mitigation
- Adherence to WLAN policies
- Rogue devices, denials-of-service, network recon, active scanning, cracking
- Sensors and management components
- On a bigger scale than a security assessor's
- WIDS detect and notify
- WIPS detect, take action, and notify



Adherence to policy might be enforce clients from trying to connect to unauthorized APs or engage in peer-to-peer connections. Enforcement of only approved authentication and encryption methods.

WIDS/WIPS Server

- Sensors and servers
- Server is the central point for monitoring and data collection
- Can be a standalone device or software application or virtual appliance
- Could be integrated into WLAN controller
- Or tied into a NMS locally or in the cloud

WIDS/WIPS Server

- Analytical engines that detect threats
- Signatures
- Behavior
- Protocols
- RF spectrum
- Performance
- Security personnel can view through a management interface or console



Signatures are patterns

Behaviors are abnormalities or anomalies

Protocol analysis looks at the MAC layer information about frames. Can also look at L3-7 data that is unencrypted. **WHY?**

RF analysis looks at channels, signal strength, SNR.

Performance analysis looks at health statistics like capacity, BER, and coverage? **HOW?**

WIDS/WIPS Sensors

- Emplaced to listen to 802.11 communications
- Look similar to access points
- Employ multiple radios across both bands
- Scan across the 802.11 channels and more
- Can conduct remote captures if needed
- Communicate securely with server using proprietary protocol or CAPWAP
- Centrally managed through secure means



Some sensors may have dedicated radios to listen to more than 2.4 and 5 GHz bands.

Control and provisioning or wireless access points.

Encryption of communications is just as important as encryption of MSDU data.

Central management of sensors can be through SSH, HTTPS, or other secure means

WIDS/WIPS Sensor



UMBC | CYBERSECURITY
Training Centers ACADEMY

Netscout's Airmagnet sensor from enterprise.netscout.com

WIDS/WIPS Models

- **Overlay** and Integrated
- Overlay is deployed on top or or next-to the existing WLAN
- Sensors and server are not part of the WLAN nor do they provide an client STA accesses
- Standalone sensors with more extensive features and capabilities = increase in hardware and costs



There are vertical markets in which a dedicated overlay is called for....DOD, Federal agencies, big box retail, bank. In these markets the cost pale in comparison to the data being protected.

WIDS/WIPS Overlay Solution

- They do add more functionality and are dedicated listeners in 2.4 and 5 GHz
- Can provide better detection and collection
- If the WLAN goes down, the WIDS/WIPS is unaffected and continues to monitor
- Sensors are also known as stand-alone

WIDS/WIPS Integrated Solution

- **Integrated** solutions provide client access and security monitoring in one package
- In a *centralized* WLAN, the WLAN controller is dual-hatted as the WIDS/WIPS server
- In a *distributed* WLAN, a NMS becomes the WIDS/WIPS server
- Either way, the APs are centrally managed



802.11 client access is provided.

WIDS/WIPS Integrated Sensors

- Also known as **part-time sensors**
- Integrated APs will have more than one radio
- Switch between client access and sensing in both bands depending on configuration
- A separate radio may be a full time sensor wrapped up into the AP
- Radios can go off channel periodically (slicing)
- Listen, scan, RF management



Off channel scanning and listening is vendor dependent.

Some solutions with an integrated system is to deploy a few AP as full time sensors and nothing else. There are augmented with the part-time sensors

WIDS/WIPS Integrated Drawbacks

- Time slicing and the time it takes to launch an attack
- Client accesses with higher QoS traffic
- Device containment might also be part-time

Sensor Placement

- One sensor to every 3-5 APs
- Dedicated sensors should be staggered and or placed around the perimeters of building
- Remember the RF environment can change!



Some markets call for a 1:2 or 1:1 ratio

Device Classification

- Device is something with an 802.11 radio or a device operating in 2.4 or 5 GHz bands
- AP, client STAs, Bluetooth, Neighbors, etc.
- Categorization of devices into:
 - Authorized
 - Unauthorized (Unknown)
 - Neighbor
 - Rogue



Authorized: station or access point that is an authorized member of the company network or infrastructure. Manual input may be necessary with an overlay solution. Integrated solutions would be able to label stations as authorized because they would be connected to them through the correct layer 2 methods.

Unauthorized: stations or devices detected but not classified as rogues...further vetting or investigation is required.

Neighbors: identity is known and poses no threat

Rogue: interfering device or potential threat. Not known or managed by the organization but somehow is connected to the network or infrastructure.

Rogue Detection

- Through SNMP polling of MAC addresses
 - Correlation of wired and wireless MACs
- Broadcast addresses and source MACs
 - Rogue AP mistakenly forwards out a broadcast
- Sensor could associate to the rogue AP
 - Sensor would contact server through the AP
- If encryption is enabled on rogue AP, then a MAC comparison between wired and wireless



Sensor and rogue AP might be on separate VLANs in which case, there may be a need to enable 802.1Q trunking to the sensors to see all VLANs.

Most consumer APs have MACs that are one-offs.

Marker packets could be used similarly to the broadcast method in bullet 2.

Rogue Mitigation

- Containment through deauths and L2 DoS
 - Spoofed transmitter addresses
 - Target the AP and the clients
 - Works against infrastructure and ad-hoc
 - Prevent authorized clients from connecting to rogue access points
- Locating the device is the follow-on, next step

Rogue Mitigation

- SNMP can be used for port suppression
- Disable the switch port connected to rogue
- Works well if you have accurate network diagrams and a managed switch
- Locating the device is the follow-on, next step

Device Locating

- Received Signal Strength Indicator
- RF Triangulation: angle of incidence
- RF Trilateration: distance between radios
- RF fingerprinting and RTLS
- TDoA and AoA
- Signal meter...You're getting warmer!
- Factors affecting measurements:
 - Attenuation, reflection, absorption, multipath



Each of these techniques needs to be overlaid with an accurate map or floor plan that accurately depicts the location of each sensor.

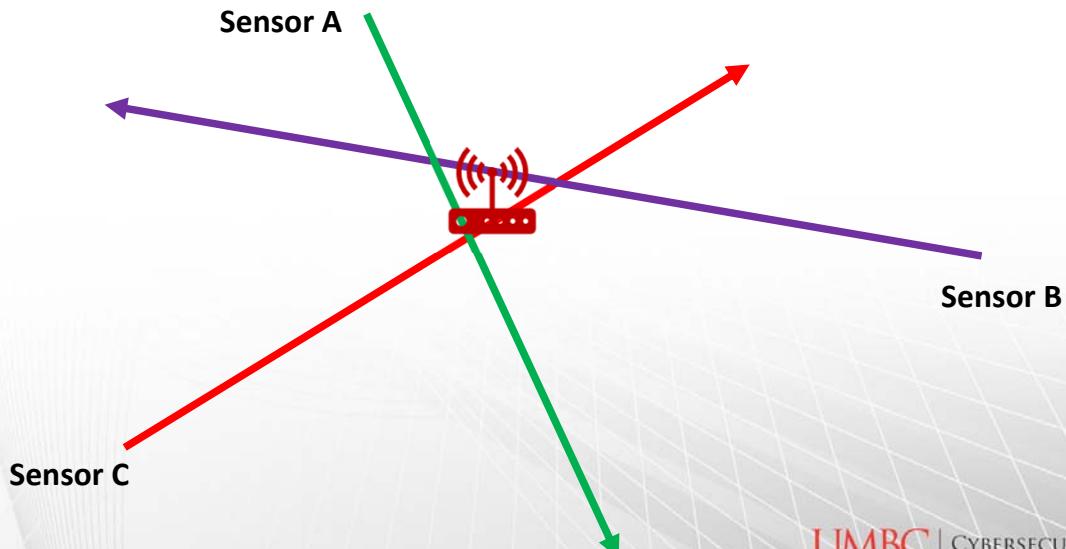
RF fingerprinting uses the RSSI values of transmitting devices as detected by the sensors. Authorized devices and their RSSI values. Their locations have to be well known for this to work. The comparison between authorized and rogue RSSI values are compared.

TDOA works with how long it takes a signal to arrive to a sensor.. Each sensor has to have precise time synchronization and time stamps.

AOA works with smart antenna arrays.

RF Triangulation

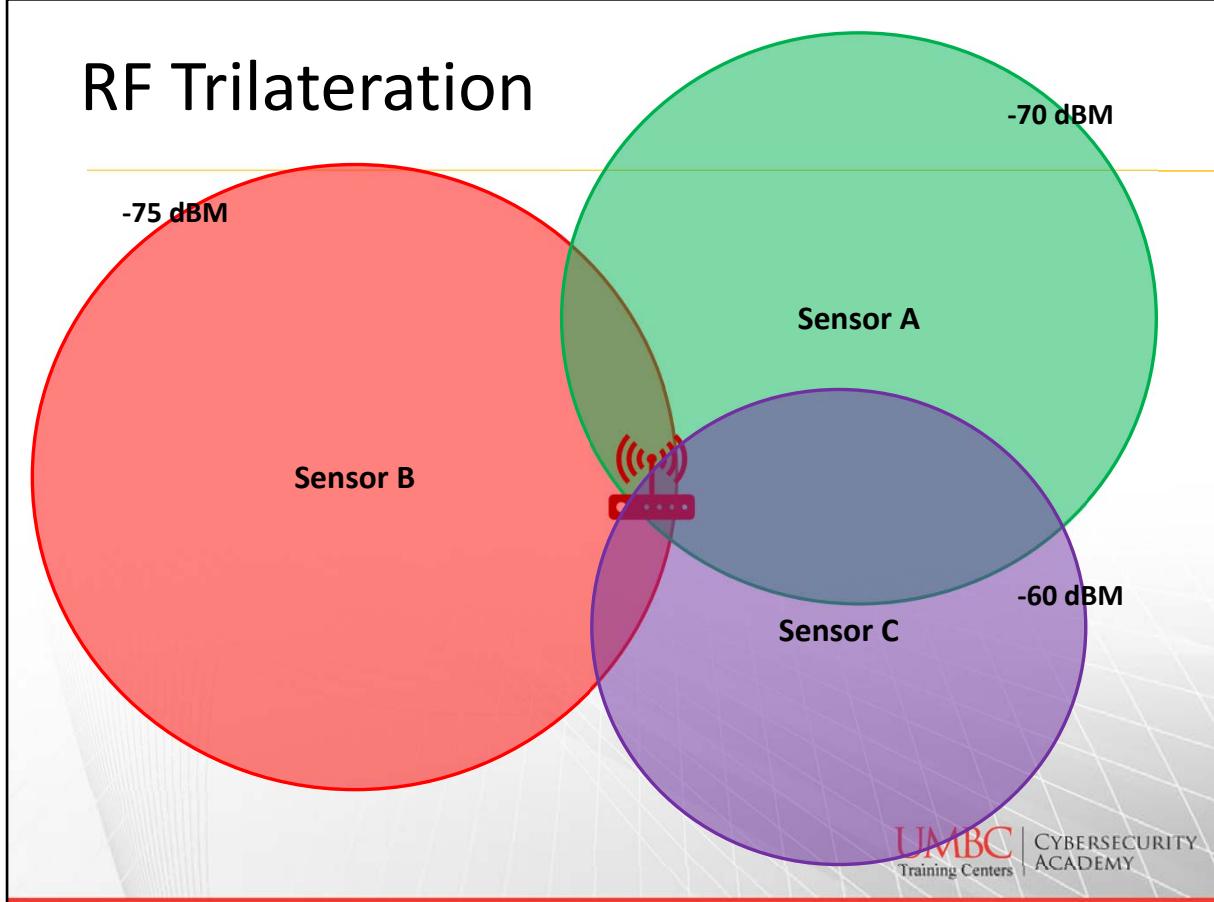
- Might expect ~30 feet accuracy, it depends



UMBC | CYBERSECURITY
Training Centers ACADEMY

Would need smart antenna technologies to get the angle of incidence.

RF Trilateration



Think of timing advance rings for GSM. Each sensor sees the device at a specific RSSI

WIDS/WIPS Analysis

- Data collection can quickly amass and overwhelm manual analytical efforts
- There are plenty of WIDS/WIPS engines to do this work automated
- Analysis can be performed from perspectives
 - Signatures, Behaviors, Protocols, RF, Performance, and Forensics

WIDS/WIPS Analysis

- Signatures: pattern matching to knowns threats or attacks
 - Only as good as your up-to-date signatures
- Behavior: deviations from normal, anomalous or “abnormal”
 - Depends on historical data and baselines
 - Baselines of frame types
 - Protocol fuzzing

WIDS/WIPS Analysis

- Protocol Analysis: pulling apart layer 2 and sometimes layer 3-7 if unencrypted
 - Conduct remote captures and looking at layer 2 frame exchanges
- Spectrum Analysis: listening for interfering devices and attempting to classify a device
 - RF signature analysis
 - Many interferers can go undetected

WIDS/WIPS Analysis

- Performance: how well the WLAN is operating
 - Bit error rates and retransmissions
 - Roaming problems
 - Hidden nodes (CTS/RTS)
 - Set thresholds for historical comparisons
- Forensics: timelining of events
 - What happened when?
 - What lead up to it and did we see?

WIDS/WIPS Monitoring

- Why are we monitoring?
- How are we getting our alerts?
- What else can this expensive piece of equipment do for me?

WIDS/WIPS Policy Enforcement

- Policies regarding security requirements, usage, protections, and WLAN configurations
- Policies are the baselines, WIDS/WIPS verify
- Use the WIDS/WIPS to monitor adherence
- Vigilance with network operations and performance
- Provide interdiction with non-compliant devices or users

WIDS/WIPS Alarms

- Trigger for events
 - Exceeding baselines and thresholds
 - Match on signature
 - Deviation from normal or expected
- Are the triggers warranted? False positive?
- Was a response action employed?
- Some systems can provide remediation steps

WIDS/WIPS Alarms

- What is the criticality level?
 - Informational
 - Minor: could worsen if you ignore me
 - Major: requires immediate attention
 - Critical/Severe: call the President
- Tuning and self learning
- Methods of notification: text, email, phone, log server (remote or local)

WIDS/WIPS Reports

- Generate reports as needed
- Could support legal actions or forensics
- In accordance with industry standards or government regulations
 - PCI-DSS
 - FIPS
 - HIPAA

Complications with 802.11n/ac

- 802.11n and ac devices use physical and MAC layer enhancement to achieve higher rates
- Think of it as a different language
- 802.11n devices can courteously speak to 802.11b/g/a devices if configured
- **HT Greenfield** is no such courtesy thus legacy WIPS 802.11b/g/a sensors can't understand

Management Frame Protection

- Under 802.11w, **both stations** can negotiate MFP with CCMP/AES
- Disassociation, deauthentications, and action frames will be refused if MIC fails
- MFP still **does not** protect against layer 2:
 - EAPOL or association floods
 - PS-Poll floods
 - Virtual carrier sense attacks



A properly configured WIPS/WIDS should catch these layer 2 attacks

Summary

- WIDS/WIPS
- Device Classifications
- Analysis and Monitoring
- Nuances About 802.11n/ac
- Management Frame Protections

QUESTIONS??



I Don't Have a Roaming Problem!



Overview

- General Roaming
- Roaming in RSN
- OKC
- Fast BSS Transitions

Roaming in General

- Who makes the decision to roam?
- How is the decision made?
- Roaming is a BSS transition
- Based on vendor specifics
 - RSSI thresholds
 - SNR
 - Noise floor
 - Bit error rates

Roaming in an ESS

- Client is always off-channel listening and probing looking for something better
- Could just be a RSSI difference
- Initiated by a reassociation request
- Always a client decision
- RSSI is always fluctuating and ping-pong effect
- **A new BSS means new dynamic keys, always**
- New BSS means new PMK and PMKSA



There may be some proprietary metrics used by each vendor to alleviate a ping-pong effect.

PMK is the seed used for the 4-way we keep hearing about. A PMKSA is said to exist after:

Successful 802.1X/EAP authentication
PSK Authentication
SAE authentication
PMK cached by some other means

The PMKSA

- PMK are unique to a radio pairing
- Contains:
 - Pairwise Master Key
 - **PMK Identifier (PMKID)**
 - MAC of the authenticator
 - Lifetime of the PMK
 - The AKMP protocol used
 - Additional parameters
 - Authorized SSIDs

Roaming in an ESS

- *From a high level:*
- Client hears a better AP (TGT)
- Client sends reassociation req to TGT
- TGT tells original AP over backbone about client getting ready to roam (data buffered and forward to TGT)
- Reassociation proceeds with TGT
- Buffered data waiting at TGT sent to client



The buffering of data between two APs is not part of any standard but is one way a vendor might help with roaming in an ESS. This may occur within the WLAN controller or between cooperative APs

More on Roaming

- In PSK environment roaming is fairly quick, way less than 700 milliseconds, ~50ms
- In a basic 802.1X/EAP, the reauthentication process can take about 700 milliseconds
- New dynamic keys are needed in either case
 - 4-way handshake is done regardless of AKMP
- What if you have a time sensitive application?
- Voice over Wi-Fi (VoWiFi) < 150ms

Fast Secure Roaming

- Because 700 ms is forever!
- 802.11-2012 standard defines 3 FSR mechanisms
 - Preauthentication
 - PMK Caching
 - **Fast BSS Transitions (FT)**
- Really focused on enterprise 802.1X/EAP



802.11-2012 standard defines three fast secure roaming mechanism

PMK Caching

- Known as “**fast-secure roam-back**”
- STAs on both ends cache the PMK from the initial 802.1X/EAP authentication
- Clients can then roam-back to a previous AP
- Re-association request from client list **PMKID**
- Skip a new 802.1X/EAP process
- PMK listed is still the 4-way handshake seed
- **Does nothing for a forward roam!**

Preauthentication

- Predict the future...to where a client “might” roam
- PMKSA with all future APs = lots of PMKSAs
- Each PMK is cached on the respective TGT APs
- Alleviates the full 802.1X/EAP process when a target wants to roam
- Just go through the 4-way with the seed PMK
- Client STA learns about future APs



Client STAs or supplicants learn about new AP and BSS through off-channel listening of beacons and probe requests. Once they learn of a potential AP, it does a full 802.1X/EAP but the authenticator is the new potential TGT AP.

Doesn't scale well because all the APs would need to store all the PMKs for every client.
Lots of backend 802.1X/EAP going on behind the scenes

So Preauthentication is Great?

- Not so fast
- 802.1X/EAP preauthentication occurs with every potential target AP
- Every AP would then be caching PMKSA of every potential client STA
- Doesn't scale well

Opportunistic Key Caching (OKC)

- Vendor led caching solution
- A preview of 802.11r “*r is for roaming*”
- Not defined in the 2012 standard
- Suppose to scale better
- As with any method, both the AP and client have to support it
- Downside is that it is proprietary in implementation

OKC

- Starts with an initial 802.1X/EAP process
- Successful EAP yields the PMK, PMK #1
- The PMK is distributed to APs in enterprise
 - *Proprietary* and over the Distribution System
- PMK #1 is forward to new TGT AP
- TGT AP and client **mathematically compute** a new PMK #2
- PMK #2 becomes the seed for the 4-way

Enter Fast BSS Transition!

- 802.11r standard for fast secure roaming
- Concept of **Mobility Domains** in an ESS
- Mobility domains support FT
- Requires an initial 802.1X/EAP when a client joins the mobility domain
- Transition can be over-the-air or DS
- Multi-tiered key hierarchy

The Keys...The Keys

- In FT, there exists more keys
- 3-tiered PMK hierarchy
- Master Session Key (MSK) creates the PMK
- PMK-R0: derived from the MSK
- PMK-R1: second tier key
- PTK: third tier used for encryption

MSK → PMK-R0 → PMK-R1 → PTK

EAP → Level 1 → Level 2 → Level 3



PMK-R0 is held on the original AP or WLAN controller.

PMK-R1 is derived from R0 and sent from the WLAN controller and cached on the APs

R1 is used to generate the PTK used for 802.11 MSDU encryption

Each device that has a key is the key holder of that key

Fast BSS Transition

- *In a Controlled Based infrastructure*
 - WLAN has PMK-R0 and derives all second level PMK-R1 and distributes to appropriate APs
 - The client supplicant also has PMK-R0 and derives PMK-R1 for each AP
 - The appropriate PMK-R1 is the seed for the 4-way when the client STA roams to new AP
 - The distribution of keys is not defined by standard

Fast BSS Transition

- *In a Distributed infrastructure*
 - Original AP has PMK-R0 and derives all second level PMK-R1 and distributes them to the APs
 - The client STA also has PMK-R0 and derives PMK-R1 for each AP
 - The appropriate PMK-R1 is the seed for the 4-way when the STA roams to a new AP
 - The distribution of keys is not defined by standard

Fast BSS Transitions

- Up to this point, we've only really talked about the keys
- So how does the transition actually occur?
 - Over-the-Air
 - Over-the-Distribution System
- The method of transition roaming is indicated in the RSN Information Element in frames

Over-the-Air

- Trims the fat from Open System Authentication, Association, and the 4-way
- The client STA communicates directly with the TGT AP using standard 802.11 authentication and FT authentication algorithm
- The TGT AP and STA use the PMK-R1 to seed the PTK

Over-the-DS

- Uses a set of frames called **FT Action Frames**
- Occurs on the DS medium (Ethernet)
- Client STA sends FT action request to original AP
- FT action is forwarded from original AP to the new TGT AP over the DS
- TGT AP responds with FT response frame
- Reassociation is sent from STA to TGT over-the-air
- PMK-R1 is then used to seed the PTK

Final Note on FT

- The original 4-way handshake in both FT is **abbreviated** in the over-the-air reassociation
- Reassociation in both has the Nonces
- Fast BSS transitions equate ~50 ms
- If no 802.1X/EAP is deployed and only PSK, then the handoffs are always fast

802.11k—Neighbor Reports

- Part of Radio Resource Management (RRM)
- **Input for the STA as part of roaming decision**
- Measurements by AP or STA
- Can be used for pre-handoffs
- In turn, can speed up handoffs
- Neighbor Report is generated by the AP and shared with clients STA
 - AP measure and report neighboring MD APs



Radios in either the AP or client STA can better understand the RF environment in which they operate.

AP can listen to the RF environment and create this neighbor report that it shared with roaming clients to help them understand potential TGT APs in a Mobility Domain that they may roam to.

Neighbor Reports

- Used in connection actions and transition candidate decisions
- AP goes off channel periodically to listen
- BSSIDs and security of neighboring APs
- Mobility Domain
- QoS settings
- Channel and spectrum management
- Client device still makes the roaming decision



Neighbor reports can also be sent from the client station to the AP to aid in the generation of neighbor reports.

RRM mechanism have to be supported by both AP and STA

802.11v—WNM

- Wireless network management
- Its about network conditions
- Information about **network resources** to enhance the overall performance of the WLAN
- Unlike RRM, this is not about the RF
- Lots of information can be exchanged between client STA and AP
- Again, both ends have to support 802.11v



See page 246 for a list of information exchanged.

Why Fast Secure Roaming is #1

- Wi-Fi Alliance **Voice Enterprise** certifications
- Must hit the mark on voice quality while simultaneously existing with data traffic
- Achieved through WMM QoS tagging and prioritization
- Fast Secure Roaming in WPA2-Enterprise
- 802.11k and 802.11v support



Good voice quality, latency, jitter, and low packet loss while at the same time sharing data traffic resources

Layer 3 Roaming and Mobile IP

- What happens when a client device **in use** roams across Layer 3 boundaries? New IP
- How to maintain upper layer (L4-7) comms
- Enter **Mobile IP**
- Not necessarily designed for WLANs
- Originally for the transparent routing of IP datagrams to mobile nodes on the Internet



Defined in RFC 5944.

Mobile IP

- Tunnel and encapsulation method to maintain original IP address
- Home address and home agent
- Home address table
- Care-of-address
- Foreign address



From the RFC: Each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address, which provides information about its current point of attachment to the Internet. The protocol provides for registering the care-of address with a home agent. The home agent sends datagrams destined for the mobile node through a tunnel to the care-of address. After arriving at the end of the tunnel, each datagram is then delivered to the mobile node.

The client receives an IP address from its home agent and the IP address it receives is the home address. The home agent maintains a home agent table which is a MAC/IP mapping. The home agent is the POC for the client when it leaves the home network.

When a client roams to a new IP subnet, the Home Address Table is shared with a foreign agent. The foreign agent is also the care-of-address. The foreign agent uses the HAT to identify the home agent of the mobile client. A mobile IP tunnel is set up between the original home agent and the foreign agent. When an IP datagram arrives at the original home agent for the mobile client, a datagram is encapsulated with a new header and sent through the tunnel to the foreign agent where it then forwards it to the visiting mobile client.

Troubleshooting Roaming

- Roaming and reassociation occurs from one channel to another in a MCA
- How can you see those frames on different channels at the same time?
- Multiple WLAN cards to capture simultaneously on different channels
- Analyze the frame exchanges and determine any root causes



Problems with roaming can occur if the RF environment changes since the last WLAN survey. Coverage is affected by construction, furniture, and objects in the environment. What worked last year, may not be the same this year. Coverage vs capacity consideration and organization's growth can all be factors.

Conducting another thorough WLAN survey may identify culprits and issues.

Summary

- General Roaming
- Roaming in RSN
- OKC
- Fast BSS Transitions
- Mobile IP
- Troubleshooting Roaming

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

WLAN Troubleshooting

UMBC | CYBERSECURITY
Training Centers ACADEMY

Overview

- Best Practices
- Use the OSI Model
- It's Probably the Client
- Proper Prior Planning....
- The Internet is Down

Traditional Problem Solving Steps

- Identify the problem
- Analyze the problem
- Develop solutions
- Select and plan the solution
- Implement the solution
- Evaluate the solution

Technology Problem Solving

- Identify the issue, the exact problem
- Re-create the problem
- Locate and isolate the cause
- Solve the problem
- Test and verify the solution
- Document the problem and solution
- Provide feedback



Identifying if a problem actually exists and what the exact problem is. The internet is down doesn't really narrow down a problem.

- Who, what, when, where should be asked. Were there any new changes. Is it just one client or user. What is the extent. Has this happened before.

Re-create the problem. May need to be mocked up in a virtual lab if it's a real doozy of problem. May need to gather more information to get back to this point.

Locate and isolate. Helps to identify a root cause. This is where we would start using the OSI model to methodically step through the layers.

Solve the problem. What changes do you need to make? Firmware, certificates, updates, patches, firewall rules?

Test and verify the solution. Test in different parts of the network if it affected more than one client/device/user. Also try different times of activity.

Document the problem and solution. Don't recreate the wheel. Change management updates as needed.

Provide some feedback to those affected.

Where to Look

- AP or WLAN controller logs
- Network Management Service
- Log files from AAA, RADIUS, WIDS/WIPS, etc
- Trace files from protocol analyzers
- Spectrum analyzer



As you identify a possible issue, use appropriate resources to help confirm or deny causes.

For example, if a single client is having connectivity issues in a large office setting. You probably are not going to bust out a protocol analyzer as the first tool to use.

Use the OSI Model

- Recall where 802.11 networks operate
- Use a bottoms up approach
- At Layer 1:
 - RF environment, power, physical connectivity, client drivers
- At Layer 2:
 - Suplicant security, mismatched encryption, supported data rates



If you have eliminated the Layer 1 and 2 possible causes, it's most likely not the WLAN.

Client Issues

- Operating system drivers
 - Disable, re-enable the wireless NIC
 - Update the drivers
- Supplicant profiles
 - Delete and recreate the client security profile
- Certificate or passphrase
- Fast secure roaming support



Delete and recreate the client profile on both ends.

Proper Prior Design

- Performance affected by poor design
- Site surveys and revalidation
- Coverage and capacity analysis
- Neighbor problems
- 802.1X/EAP deployment
 - Certificates
 - Backend authentication proxies, etc.
- Redundant services: DHCP, DNS, Gateways

Pre-shared Key Issues

- We know that a passphrase gets us a PSK, and the PSK is the PMK that becomes the seeding material for the 4-way
- The 4-way is an exchange of 4 EAPOL message that, if successful, gets us the PTK
- After the 4-way is successful, the client STA gets an IP address
- Use a protocol analyzer to see if all goes well

PSK Issues

- What the FBI calls a clue
- If the 4-way fails then it might be:
 - Passphrase entered incorrectly
 - Encryption method mismatch

802.1X/EAP Issues

- Remember the three 802.1X roles: supplicant, authenticator, and authentication service
- AS can use an internal or external database
- Layer 2 authentication has to be successful before L3-7 traffic can flow
- Split the problem into zones
 - Zone 1 Backend
 - Zone 2 Supplicant

802.1X/EAP Backend Zone 1

- Backend configurations and settings
- Shared secret between authenticator and AS
- IP address of authenticator and AS
- Ports: UDP 1812/1813 or UDP 1645/1646
- Internal database
- Authentication Proxy
 - If LDAP, is there an account to do the LDAP query?

802.1X/EAP Suplicant Zone 2

- Recall what tunneled authentication entails
- Two phases of tunneled authentication
- Root CA certificate to validate the server's
- Establish TLS tunnel using server certificate
- TLS negotiation failure is probably a cert problem

802.1X/EAP Suplicant Zone 2

- Certificate problems might be tied back to
 - Root CA certificate installed incorrectly in Trusted Root Certificate Authorities
 - Server certificate failing validation
 - Network Time Protocol or system clock settings
 - Client-side certificate installed if needed
- Mismatched EAP types on either supplicant or authentication server



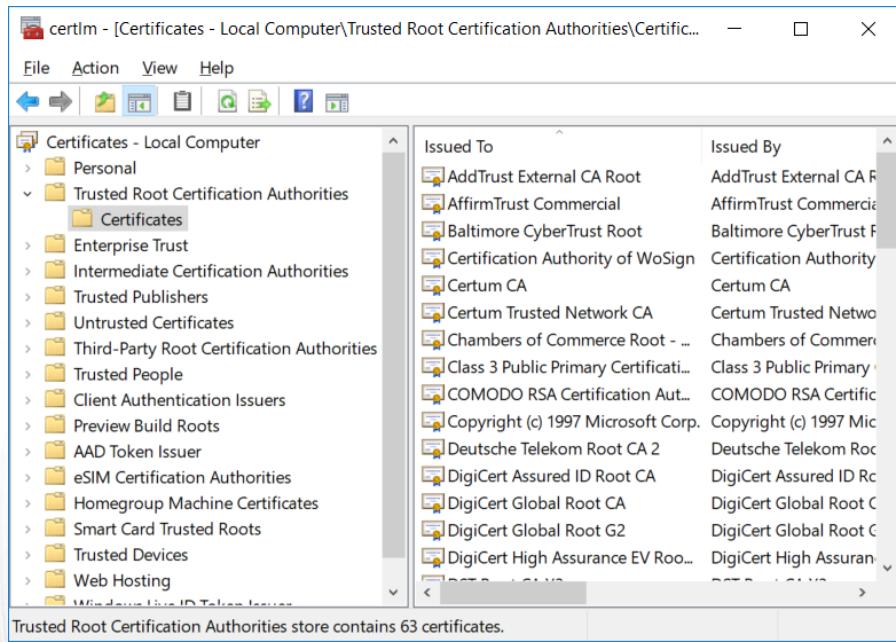
Server certificate could fail validation because it has expired.

Which EAP types needed client side certificates?

EAP-PEAP v0
EAP-TLS
EAP-TLS

Optional for EAP-TTLS and EAP-FAST

Trusted Root Certificate Authorities



UMBC CYBERSECURITY
Training Centers ACADEMY

802.1X/EAP Supplicant Zone 2

- Client supplicant credentials
- After tunnel is established and credentials passed inside the tunnel
- Expired account
- Incorrect password or username
- No account exists
- Machine is not joined to the AD domain

Roaming Problems

- Interruption in the handoff process
- Significant delay in transition
- EAP process can take up to 700ms and VoWiFi doesn't like anything > 150ms
- Both ends need to support FT, preferably WiFi Alliance Voice Enterprise certified
- Ideally, voice client does one 802.1X/EAP authentication; anything else and it's a clue



Devices need to be verified that they support fast secure roaming or fast transitions

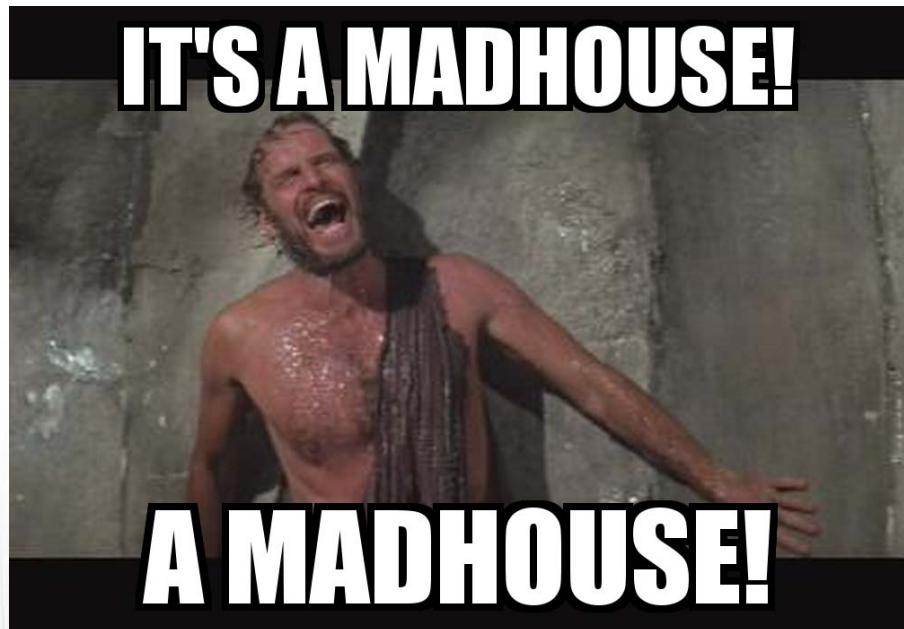
VPN Issues

- Certificates and time
- Network settings
- Firewalls
 - UDP 500 and UDP 4500
- Network address translation (NAT)
- Different vendor types
- Encryption algorithms

Summary

- Basic Technology Troubleshooting
- Use the OSI Model
- It's Probably the Client
 - PSK and EAP Zones
 - Roaming
 - VPN
- WLAN Design and Follow-ups

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY

Wireless Security Policies

Say it isn't so...the last deck?



Overview

- General Policies
- Functional Policies
- Industry Regulations
- WLAN Policy Recommendations

Why Do We Need Policies?

- Network security has many components
- Summation of the right components
- Only as good as the weakest component
- Approach to WLAN security should include:
 - Technical solutions
 - Physical
 - Training (People)
 - Administrative and management (Processes)



If we look at some of the components of a total security approach, we blend in many parts. They all should fit together and reinforce one another.

Policy Influencers

- Internal
 - Organization budget
 - Operational functions and goals
 - Management at all levels, HR
 - Experience
- External
 - Industry standards
 - Government regulations

Goals of WLAN Security Policies

- Have management buy-in and support
- Be flexible, adaptable, and relevant
- Clear and well understood
- Be enforceable
- Meet compliance requirements
- Protect ourselves
- Balance security and usability
- Split between **general** and **functional**

General Policies

- This is the “**why**” do we need a stinkin’ policy
- Should clearly articulate
 - Who in management put the policy in place
 - Applicable audience
 - Risk definition and impact
 - Auditing procedures to verify
 - Reporting procedures
- Don’t reinvent the wheel, use a template!



Executive Management that backs the policy.

To whom the policy applies. Could be one position, many, or all. Employees, admins, visitors, contractors.

Risk definition and impact could be thought of as why do we even need this?

Auditing to ensure compliance to the policy and how it get reported.

SANS and NIST have some good templates.

[Sans.org/resources/policies](https://www.sans.org/resources/policies) and csrc.nist.gov/publications/nistpubs
IF violations do occur what to do about them.

Creating the General Policy

- Start early and tweak often
- Helps ensure security is part of the design
- Have to have **executive buy-in** and support
- Involves more than just the IT folks
- Carefully consider outside influences
- Up front risk assessment
 - Assets at risk and threat analysis
- Effectively communicated to all parties



Policies can be created during the WLAN design phase.

Pull in HR, Legal, Security, Finance, Users, and representatives of groups that might be covered by the policy.

The risk assessment is more of the why do we even need a policy.

Communication and language should be like Goldilocks. It should be readily available online or posted somewhere convenient.

Policy Management

- Adapting to influences
- Maintenance of the policy
- Compliance monitoring, internal and external
- Security audits, e.g. pentests
- Enforcement of violations
 - Documented IAW law, regulations, standards
 - Liability



Policy enforcement and reporting are influenced by how well management supports it, uniformity of enforcement, risk education, compliance with regulations, cost of policy implementation and documented corporate standards.

Functional Policies

- State the technical details
- How to implement solutions and actions
- Define essentials
- Set baselining practices
- Monitoring and reporting procedures



Essentials are procedure like include password policy.

Baselining includes checklists, staging, testing and roll out, minimum configs

Design and implementation might state how segmentation, encryptions, and authentication are applied and used

Minimum Functional Policies

- Password
- Role based access control
- Change control
- Authentication and encryption
- Monitoring
- Client endpoint
- AUP
- Physical security
- Remote office

Functional Policies

- **Password:** complexity, aging, length; supplemental authentication measures; disclosure; *passphrases*
- **RBAC:** based on user identity; what groups get access to what; what to do when roles change
- **Change Control:** consistency and uniformity; upgrades and patches plus documentation; testing and timing of patches



Supplemental such as certs, 2-factor, RTLS

Assignment of users to groups by job function.

Consistency and uniformity of devices in the company environment.

Functional Policies

- **Monitoring:** classifying alerts; alert transmissions; response times and actions
- **Client Endpoints:** client stations; remote access; CID and take home equipment; personal security products
- **AUP:** how the WLAN shall be used; forbidden and permissible

Functional Policies

- **Physical Security:** protection from thievery and rascals; outdoor enclosures
- **Remote Office:** connectivity to main office; nuances to WLAN at remote locations; external influence at site



External influence could be the regulation and standard in a different country all together.

Basic WLAN Specific Policies

- BYOD and MDM
- Guest Access
- Remote Access
- Rogue Device
- Ad-hoc Connectivity
- Proper Use
- WIDS/WIPS

Government and Industry Influences

- DoD Instruction 8420.01, Nov 2017
- FIPS 140-2
- SOX
- GLBA
- HIPAA
- PCI-DSS
- Reporting requirements



DODI 8420.01: Commercial WLAN devices, systems, and technology

QUESTIONS??



UMBC | CYBERSECURITY
Training Centers ACADEMY