Sun City Computer Club

Securing a Home Network

September 15, 2020

To view or download a MP4 file of this seminar
With audio

https://vimeo.com/747789422

- Use the above link for access

View and/or listen to the audio recording

Dixie Normous Credit Card Security ™

Is your credit card number in a hacker's database?

You can easily find out now! All you need to do is enter its information here and we will scan thousands of hacker databases to see if any they have match yours.

Credit Card Number:

Expiration Date:

Your Zip Code:

SCAN DATABASE

Vocabulary

- Safer not Safe
- E-postcard not e-mail
- ADMINISTRATOR
- Passphrases not passwords
- Radio not wireless

- First job computing 1962
- 9 years semi-conductor manufacturer
- 30 years Cyber engineer Major Oil Co.
- Very early WEB experience
- 3 years Alyeska Pipeline DHS
- Major Cyber Security Certifications
- Network of cyber professionals
- Computer Club presentations
- Cyber Security SIG
- Windows SIG
- Senior University

What does/did John know

you

Biggest cyber security threat

you

Best cyber security defense

The chase

- Use cellular
  Wi-Fi & Bluetooth off unless required
- Use Linux
  bootable CD/DVD write protected USB
  Virtual machine
  tethered to Cellular hotspot
- Old devices
  smart phone for IoT command & control
  old laptop/desktop for Linux
- Hard wire ethernet connection
  Unplugged when not in use
- If you can *see them, they* can see you
- *They* are not after you, *they* are after any/everyone

Multiple

- IDentity
- Machines
- Browsers
- Security suites
- HOME NETWORKS
  segmentation
  VLANs Guest wireless
- email addresses
- Phone numbers

How Internet gets into your home

- Dial-up modem
- Digital Subscriber Line DSL
- Satellite down link
- Wi-Fi metro mesh
- Fixed Wireless
- Cellular
- Cable modem

- The Internet is vital
- The Internet is vulnerable
  DNS, BGP, DDOS, radio, EMP
- Attacks are stealthy
- Cloud

Cable modem

- Uses portion of bandwidth to home
  TCP/IP
- Shared with neighbors
- NAT
  Network Address Translation
- DHCP
  Dynamic Host Configuration Protocol
  DNS, host name, subnet, etc.

Router, Wireless Access Point

- Default route to Internet
- Firewall
- Security Appliance
- QOS
  Quality of Service
- VPN
- Speed bottleneck

Router WAP settings

- Wi-Fi protected setup OFF
- Remote Access OFF enable only when needed
- STRONG Admin passphrase
- Firewall ON
- UPnP Universal Plug and Play OFF
- MAC filtering
- Parental Controls
- Band control 2.4GHz 5GHz
- WPA2 Personal Shared Secret
- Broadcast SSID
- DHCP on and configured
- Firmware update

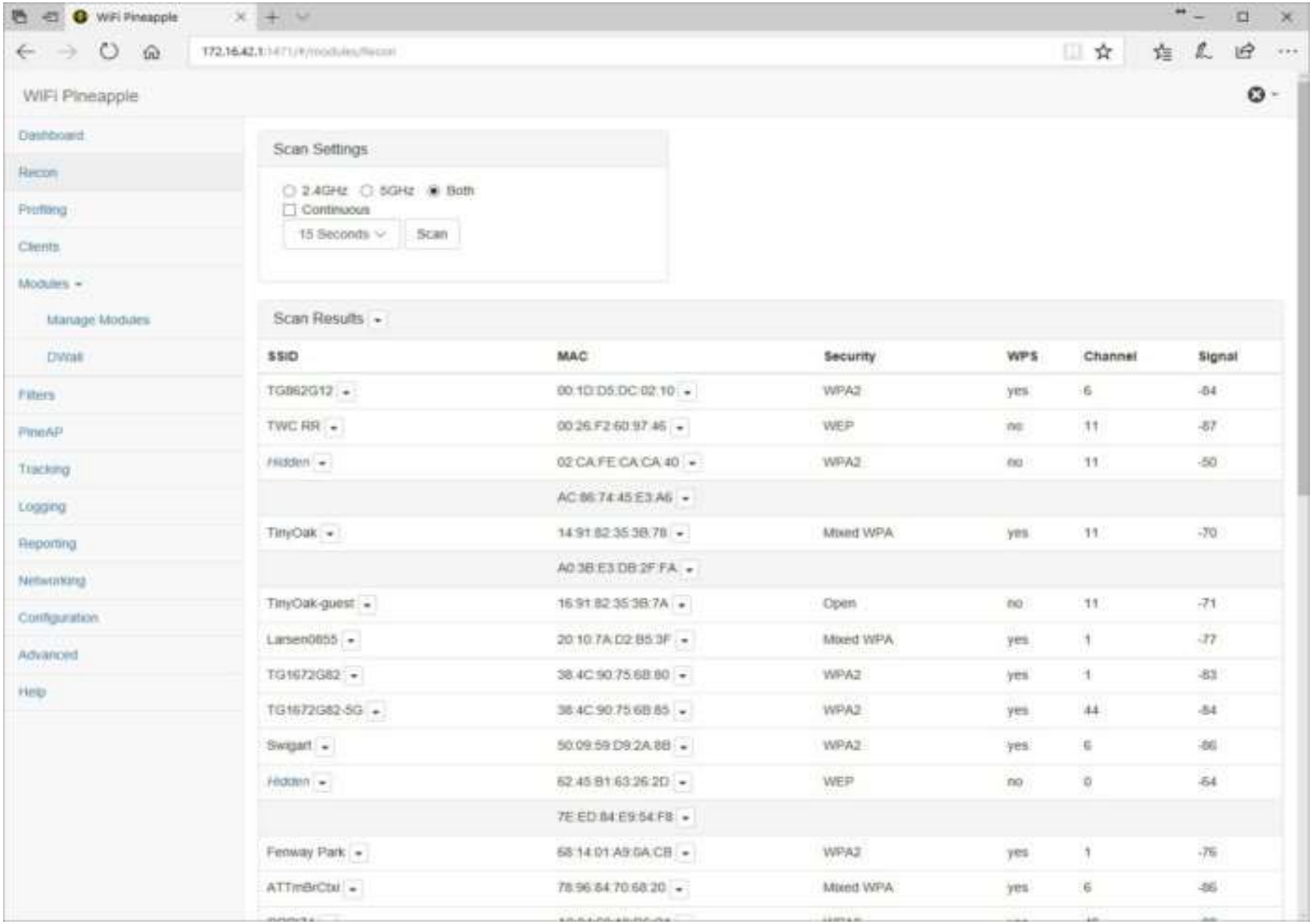
DNS & Name Lookup

- Hierarchical Distributed
- Each device – closest device
- Quad 9 Quad 1
- Local hosts file
- Keep trusted record of IP addresses

Wireless Access Point(s)

- SSID - Network name
- ADMINISTRATOR passphrase
- Disable Remote Access
- Use Guest Access
- Use VLans
- MAC filtering
- Network Map

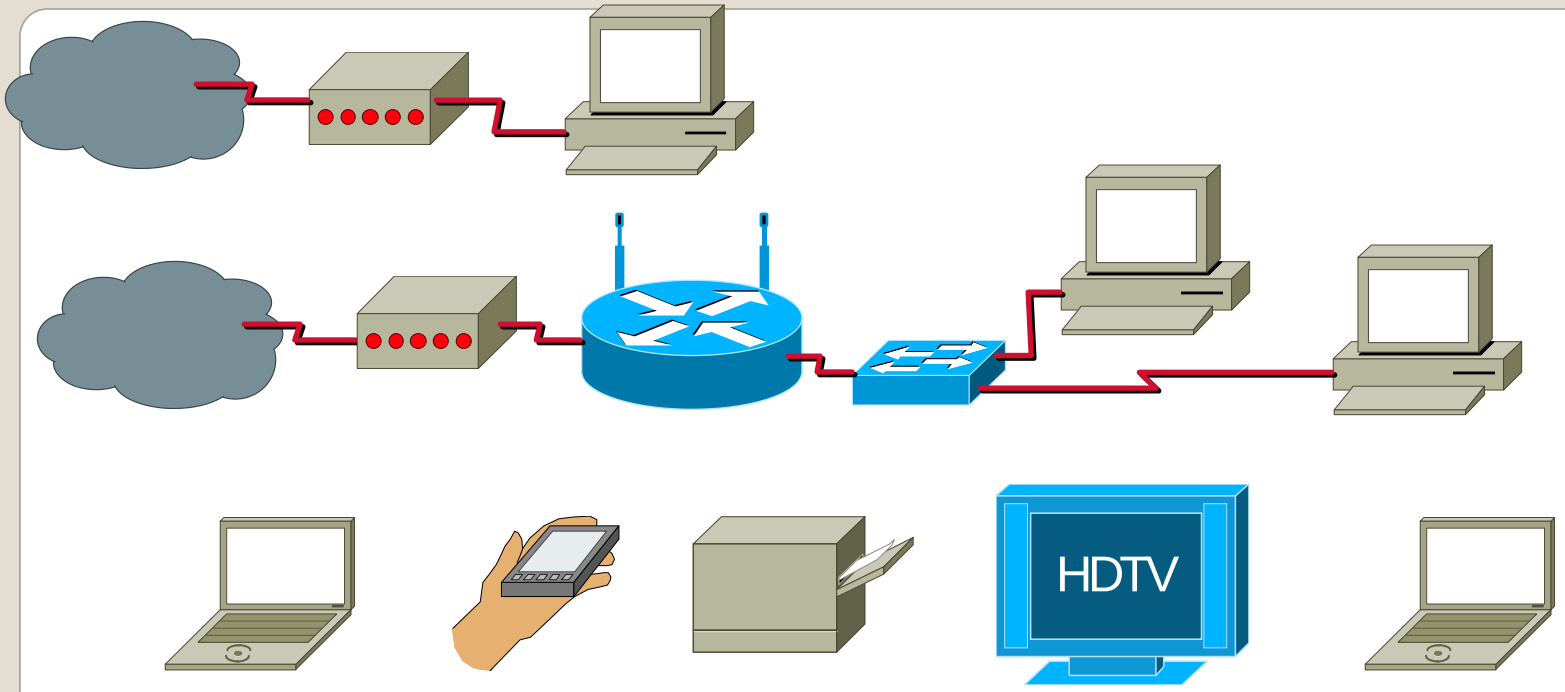
- Radio
- Disassociate

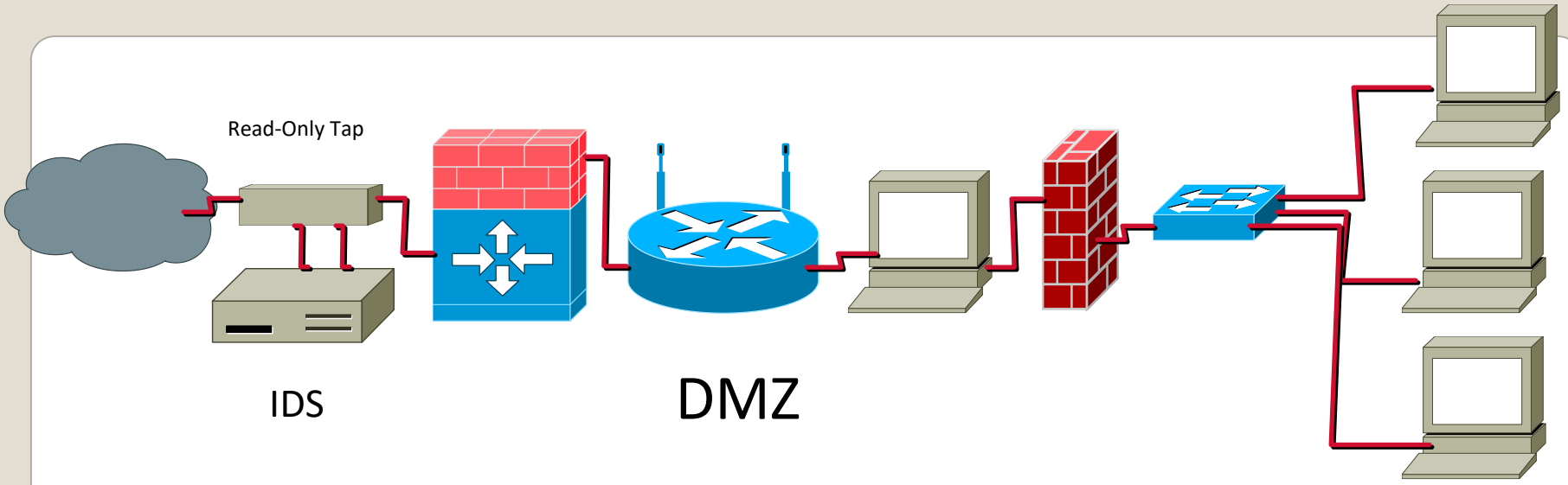

WiFi Pineapple
WIFI Pineapple
Dashboard
Recon
Profiling
Clients
Modules
Manage Modules
DWall
Filters
PineAP
Tracking
Logging
Reporting
Networking
Configuration
Advanced
Help
Scan Settings
2.4GHz
5GHz
Both
Continuous
15 Seconds
Scan
Scan Results
SSID
MAC
Security
WPS
Channel
Signal
TG862G12
00:1D:D5:DC:02:10
WPA2
yes
6
-64
TWC RR
00:26:F2:60:97:46
WEP
no
11
-67
Hidden
02:CA:FE:CA:CA:40
WPA2
no
11
-50
AC:86:74:45:E3:A6
TinyOak
14:91:82:35:3B:78
Mixed WPA
yes
11
-70
A0:3B:E3:DB:2F:FA
TinyOak-guest
16:91:82:35:3B:7A
Open
no
11
-71
Larsen0855
20:10:7A:D2:B5:3F
Mixed WPA
yes
1
-77
TG1672G82
38:4C:90:75:6B:80
WPA2
yes
1
-83
TG1672G82-5G
38:4C:90:75:6B:85
WPA2
yes
44
-84
Swigart
50:09:59:D9:2A:8B
WPA2
yes
6
-86
Hidden
62:45:B1:63:26:2D
WEP
no
0
-64
7E:ED:84:E9:54:F8
Fenway Park
68:14:01:A9:0A:CB
WPA2
yes
1
-76
ATTmBrCbl
78:96:84:70:68:20
Mixed WPA
yes
6
-86

Steps

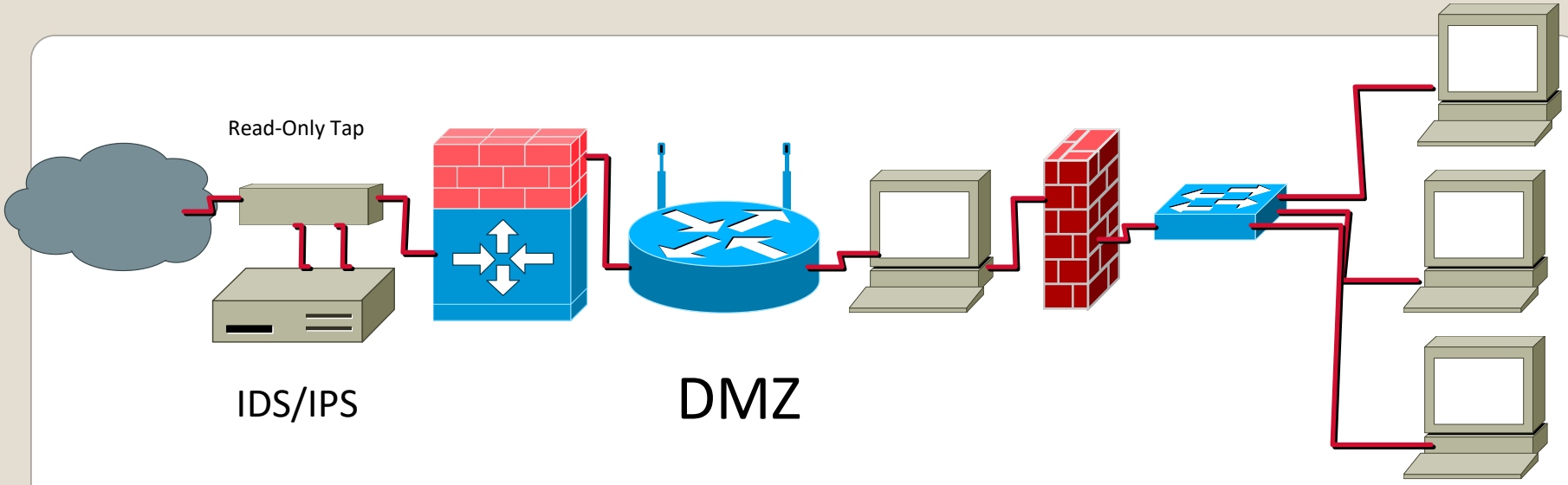
- Design
- Configure
- Instrument
- Monitor

  Maintain and Enhance


HDTV



Wireless



Wireless

- 1-2-3-4
- Steganography
- Hash
- Symmetric
- Asymmetric

cryptography

- 1-2-3-4
- Algorithm
- Key
- Plain text
- Cypher text

cryptography

Steganography

hash

- One way
- Fixed length output
- Any length input
- Message digests
- E.g. MD2,MD4,MD5,SHA-1,SHA-2
- Used for integrity, digital signing & passphrases

symmetric

- Plain text, algorithm, key, cypher text
- Algorithm usually public
- Key space is important
- Reversible with the one key
- Does not scale
- E.g. RC4,SEAL DES,3DES,RC5,Rijndael
- One-time pad
- Cryptanalysis
- Control

CIA

- Confidentiality
- Integrity
- Authentication
- Non-Repudiation

Asymmetric

- Public & private key
- Intractable problem
- Symmetric key exchange in presence of advisory
- Thousands of times slower
- E.g. RSA, El Gamal, ECC
- Public key distributed and verified via Digital Certificate
- Signing via digital signature

Uses of cryptography

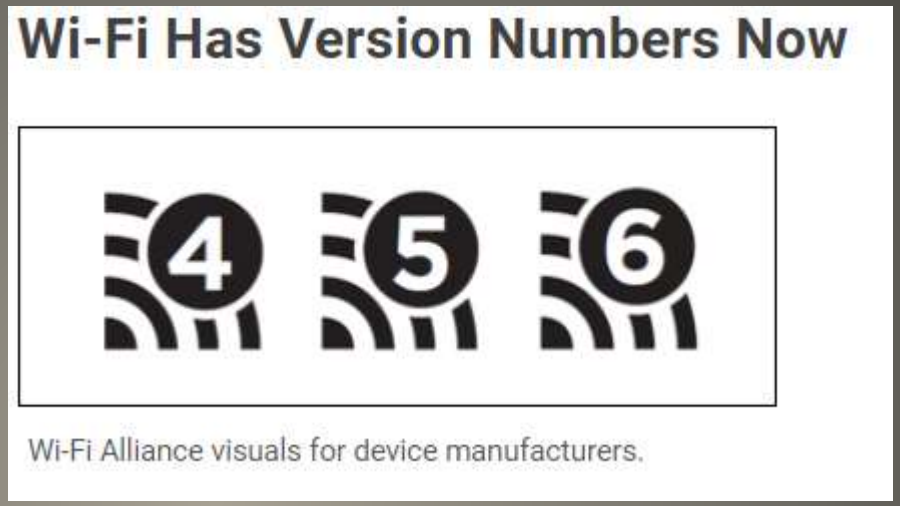
- Code signing
- VPN
- Confidentiality
- Integrity
- Authentication
- Non-Repudiation
- Disk and file encryption
- IPSec
- PKI
- blockchain

Digital Certificates

- Part of PKI
- Binding of public key to entity
- Verified and signed by certificate authority
- Chain of trust Built in
- Self signed abuse
- CA abuse
- WEB proxies

Wi-Fi

- Radio
- Alliance
- ad-hoc
- 2.4GHz
- 5GHz
- RF power
- Channels
- Interference yours theirs
- a/b/g/n/ac



Wi-Fi

- Security
  - WEP
  - WPA
  - WPA2
  - WPA3
- Shared key PSK Enterprise
- Wi-Fi Protected Setup (WPS)
- Data capture only data is encrypted
- Disassociate attacks
- Spoofing
- Replay

- Network Tap
  Privacy, IDS, IPS, network flow
- DMZ server
  Filtering WEB proxy, split DNS, honeypot
- Evidence

Prevention - good
Detection - vital

Configure

- Hardware and software firewalls
  - Filter BOTH ways Default Deny
- Operating system options
  - Linux, BSD, Tails
- Segmentation is key

Instrument

- Logging to maximum
- Central logging server in protected zone
- Host based IDS tripwire, regmon
- Defense in depth
- SNMP off or secured

Monitor

- Filter logs discard benign
- Check Configurations often
- Inventory and Update

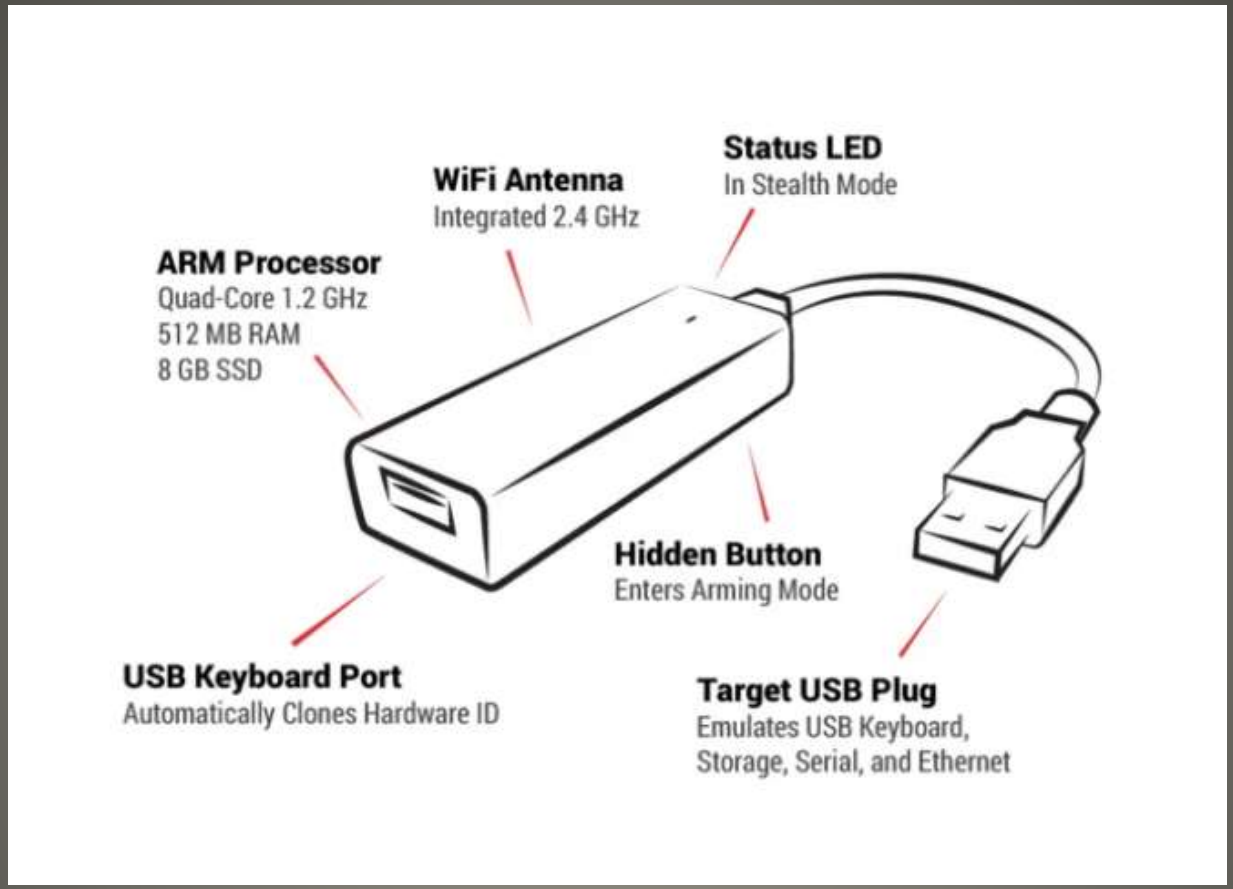
- ShieldsUp!
  www.grc.com
  GRC's UPnP Exposure Test
- Shodan

Virtual

- VLan
  Virtual Local Area Network
- VPN
  Virtual Private Network
- Virtual Machine
- SDN
  Software Defined Network

- Got old?
  Inventory Network Map
- Got old?
  Use device (NonCellular)as IoT controller
- Hard wired
- Segmentation
- Tape on appropriate cameras
- Turn down gain on microphones
  use sound muffling material on mic covers
- Home assistants, computer audio, ultra frequency communications

USB


Status LED
In Stealth Mode
WiFi Antenna
Integrated 2.4 GHz
ARM Processor
Quad-Core 1.2 GHz
512 MB RAM
8 GB SSD
Hidden Button
Enters Arming Mode
USB Keyboard Port
Automatically Clones Hardware ID
Target USB Plug
Emulates USB Keyboard,
Storage, Serial, and Ethernet

Screen Grab

Rubber Ducky and friends

USB

- Use charging HUB for guest, not a computer
- USB condom
- Rubber Duckie
- Flame thrower
- Disable autorun
- SCAN with security suites on virtual machine - sandbox Linux Live CD

Cutting the cord

- Cable delivers all channels
- Streaming services, require selection at service and credit card or financial info
- Opt-in may include ad delivery to nearby devices
- Cutting the cord Blog post

Smart getting smarter

- Smart TV
- Smart utility meters
- Smart homes
- Smart abuse

ALL the protections will NOT prevent the ONE lure

Chicken little

Tower Search Results!

Alert! 17 Towers (7 Registered,10 Not Registered) found within 3.00 miles of **105 Liatris Ln, Georgetown, TX 78628**.

Info! The NEAREST Tower is .81 miles away and is owned by **American Towers Llc**.

Ok! No Applications for Future Towers detected as of 09/06/20.

Tower Type	ID Num	Site Owner	Height	Dist
Registered	(1)	American Towers Llc	199 feet	.81 miles
	(2)	Chisholm Trail Special Utility District	35 feet	1.08 miles
	(3)	T-mobile West Tower Llc	104 feet	1.41 miles
	(4)	City Of Georgetown Texas	110 feet	1.53 miles
	(5)	Sba 2012 Tc Assets, Llc	109 feet	2.23 miles
	(6)	Cellco Partnership	145 feet	2.51 miles
	(7)	Cellco Partnership	99 feet	2.54 miles
Not Registered	(1)	Crown Communication Llc	200 feet	1.34 miles
	(2)	Gte Mobilnet Of Austin Lp	198 feet	1.55 miles
	(3)	City Of Georgetown	120 feet	1.56 miles
	(4)	Voicestream Wireless	150 feet	1.77 miles
	(5)	Chisholm Trail Special Utility District	35 feet	2.02 miles
	(6)	Acc Mc Caw Cellular Of Fresno	160 feet	2.04 miles
	(7)	Williamson County, Texas	400 feet	2.16 miles
	(8)	T-mobile	126 feet	2.65 miles
	(9)	Grace Bible Fellowship	27 feet	2.75 miles
	(10)	T-mobile	106 feet	2.82 miles
Future		(No Towers Detected)		

- Check your account usage

Overview / **My Services** / **Data Usage**

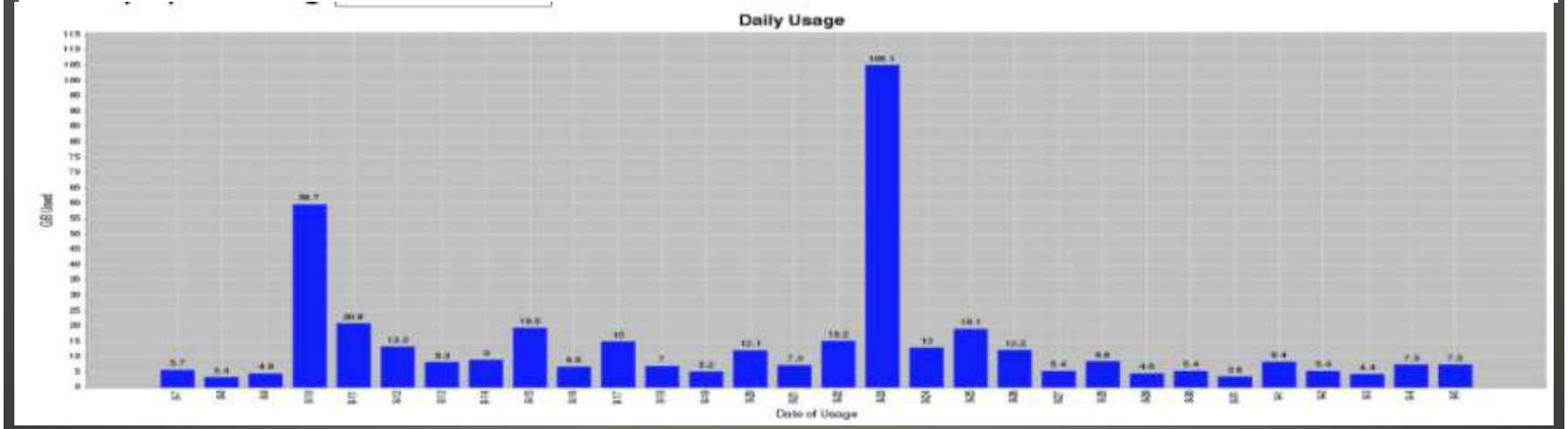
Monthly Usage Graph

As of 11:59 PM local time,

Our data measuring and reporting system is designed to update the information reported on this page every 24 hours. Typically, those updates will be processed and posted to this page each day by or before 9:00 a.m. *Central Time*, reflecting data usage through approximately 11:59 p.m. *local time* of the prior day. In those cases where a new update to this page shows no incremental data usage in the 24 hours since the last update, one of two conditions apply: either (a) there was no incremental data usage in that time period; or (b) the transmission of daily data usage (from our counter to this page) was delivered too late to be deemed useful to the customer and was thus not counted and not applied to the customer's data usage total.

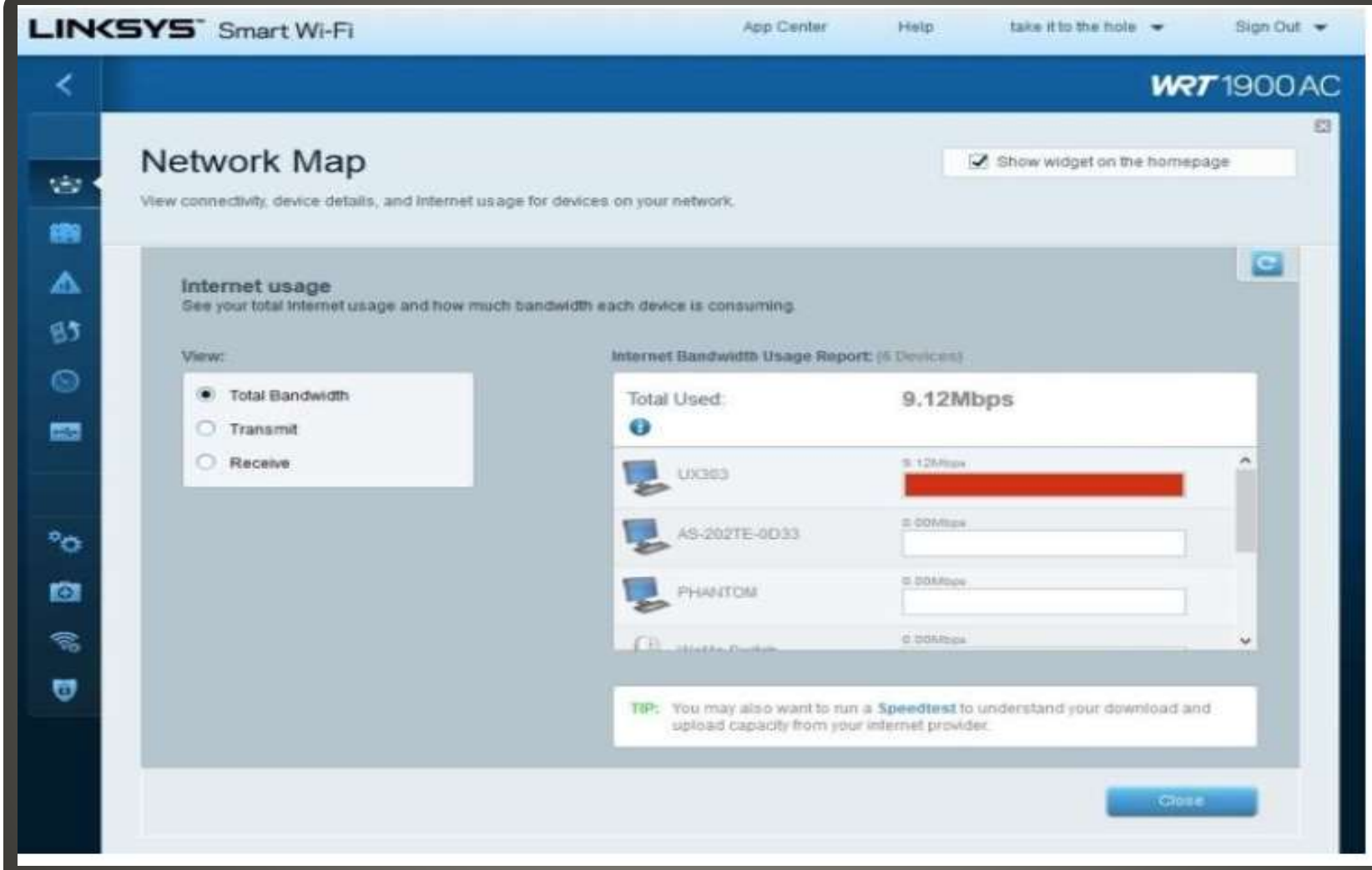
More Information

- Frequently Asked Questions
- Data Plan Summary
- Daily Usage Graph
- Monthly Usage Graph
- Update Notification Preference

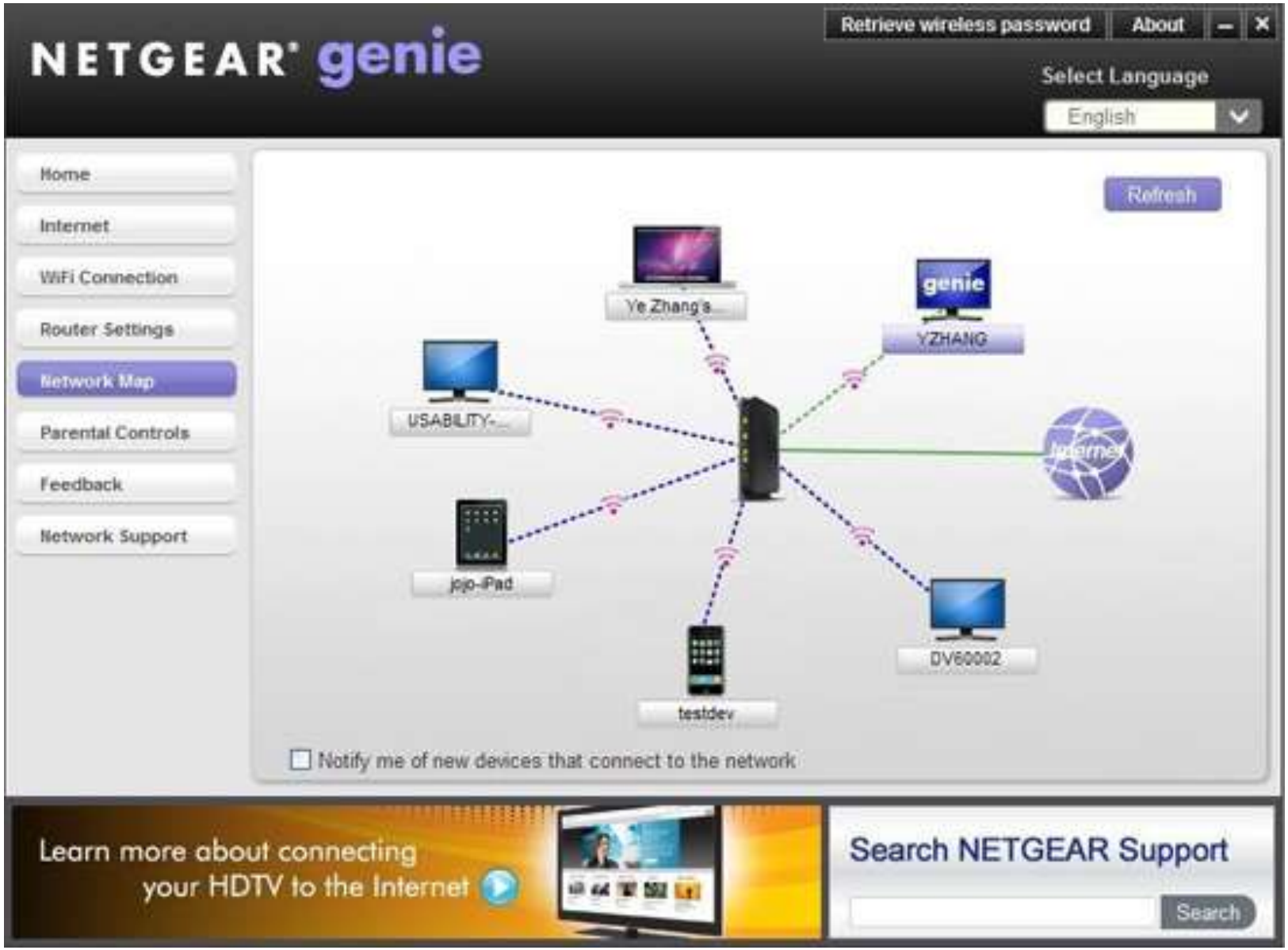


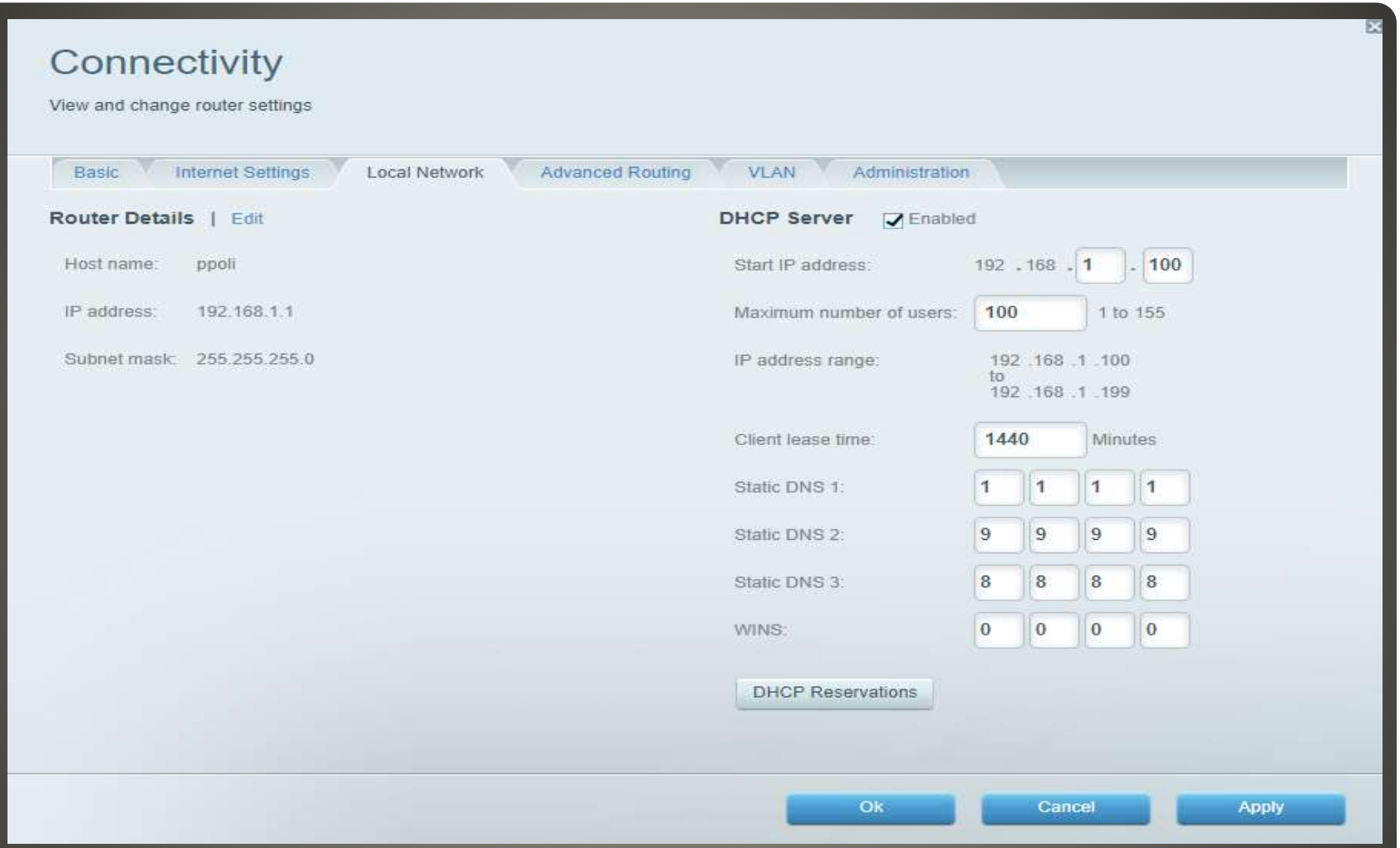
Suddenlink

Linksys Network Map

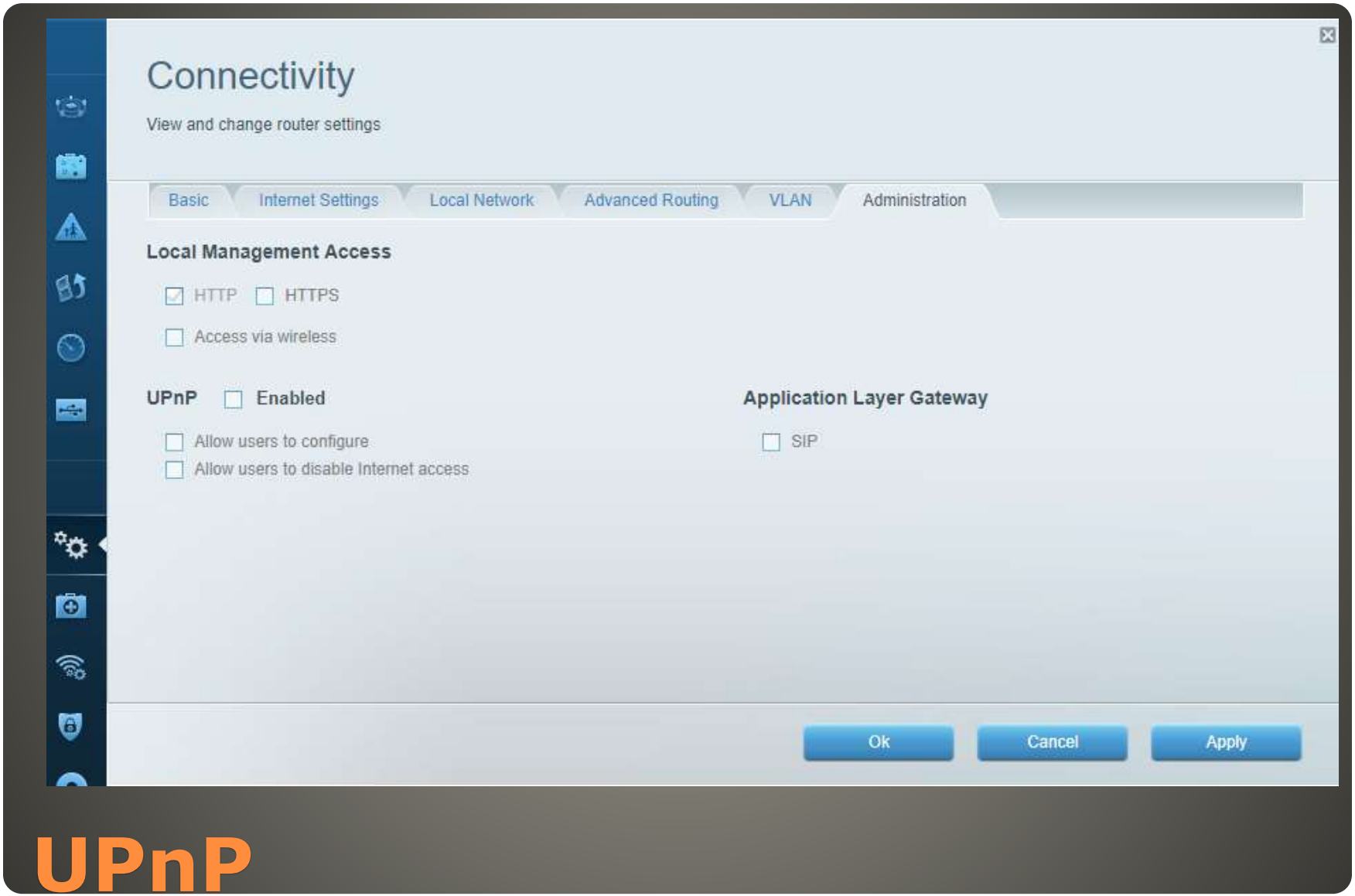


Linksys Network Usage

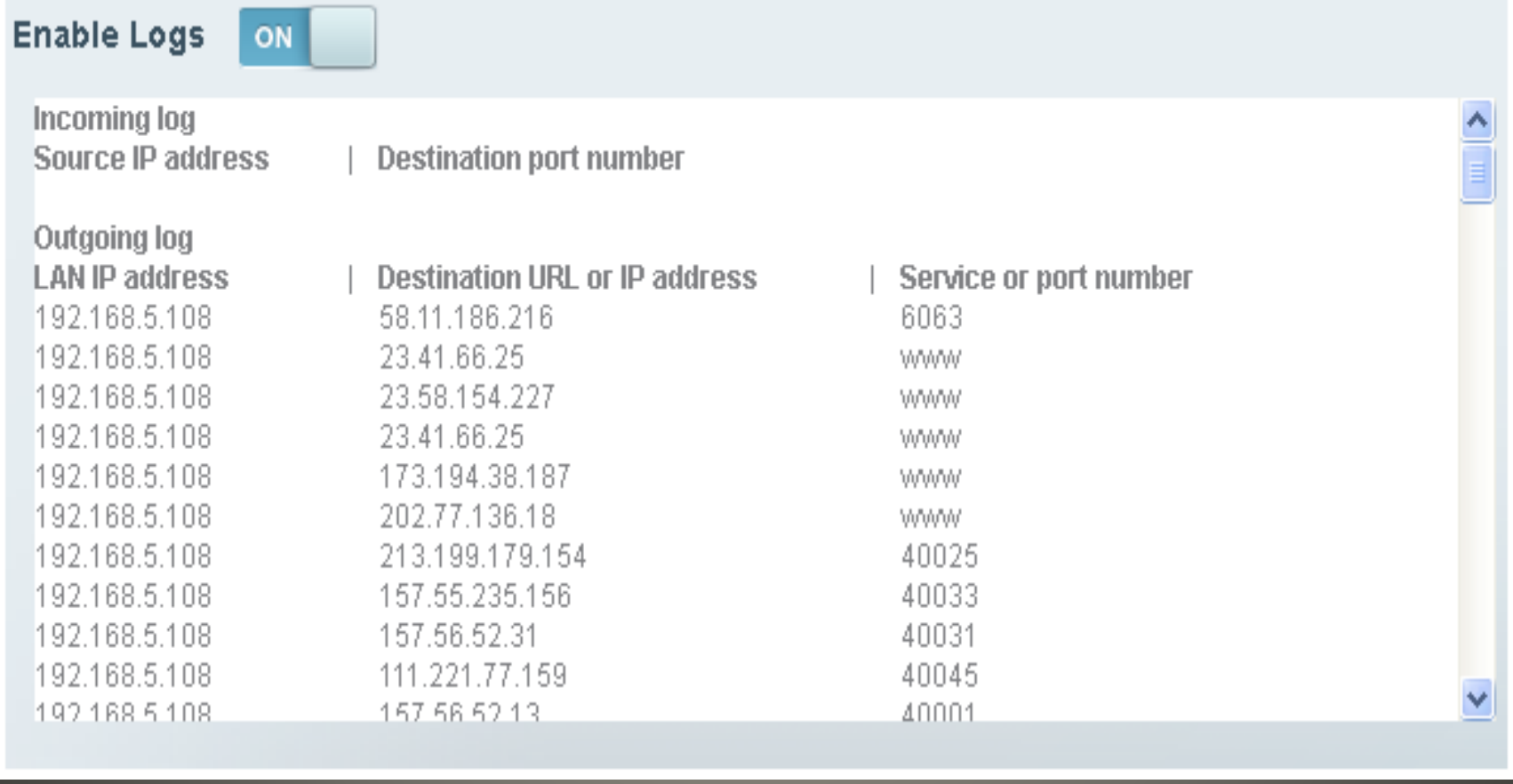

NETGEAR genie
Retrieve wireless password
About
Select Language
English
Home
Internet
WiFi Connection
Router Settings
Network Map
Parental Controls
Feedback
Network Support
Refresh
Ye Zhang's...
genie
YZHANG
USABILITY-...
Internet
jojo-iPad
DV60002
testdev
Notify me of new devices that connect to the network
Learn more about connecting your HDTV to the Internet
Search NETGEAR Support
Search



Linksys LAN settings


Connectivity
View and change router settings
Basic
Internet Settings
Local Network
Advanced Routing
VLAN
Administration
Local Management Access
HTTP
HTTPS
Access via wireless
UPnP
Enabled
Allow users to configure
Allow users to disable Internet access
Application Layer Gateway
SIP
Ok
Cancel
Apply

UPnP

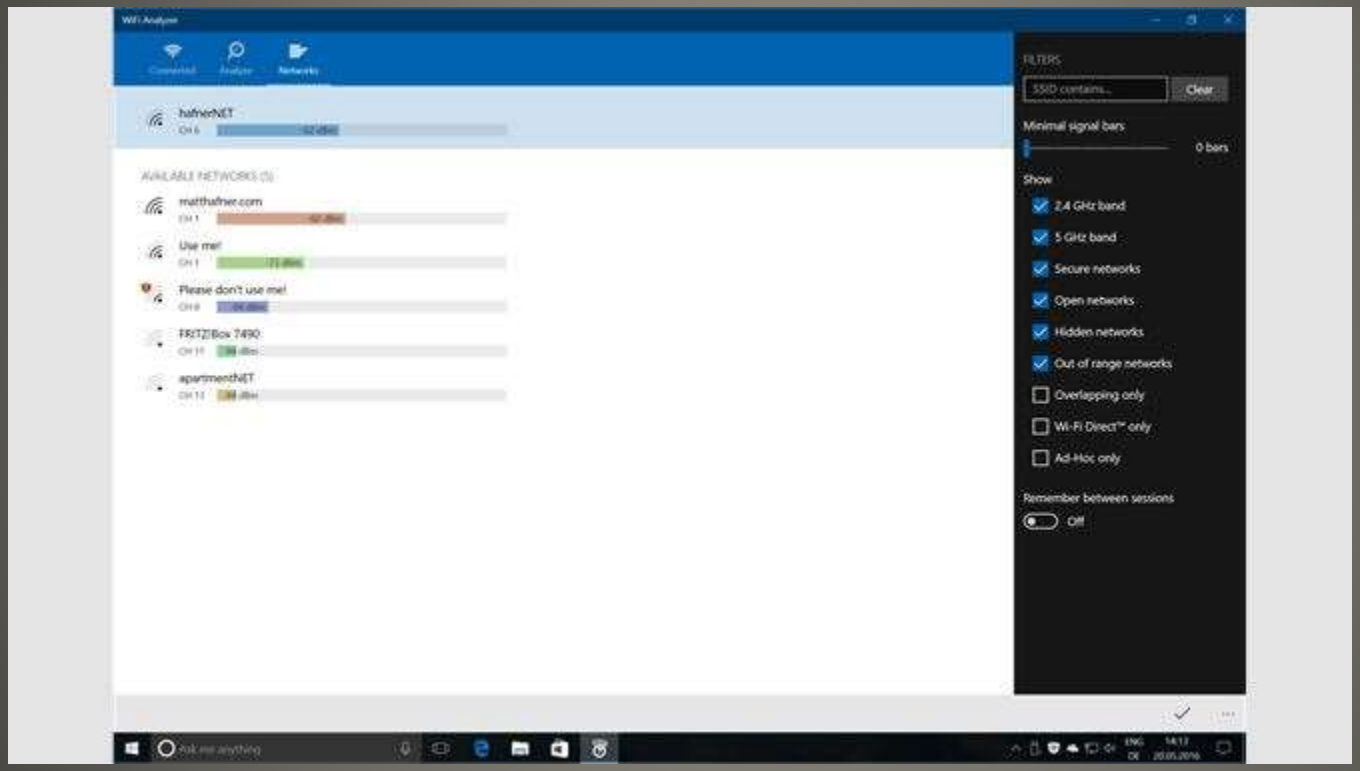


Linksys Troubleshooting Logs

Wireless Access Point Security

- Wi-Fi Protected Setup OFF
- MAC filtering Allow list
- UPnP OFF
- Firewall ON
- Firmware update
- Firewall on LAN side of WAP
- Computer Club classes
- Cyber Security SIG NEWS Archive
- Internet

- Microsoft WiFi Analyzer



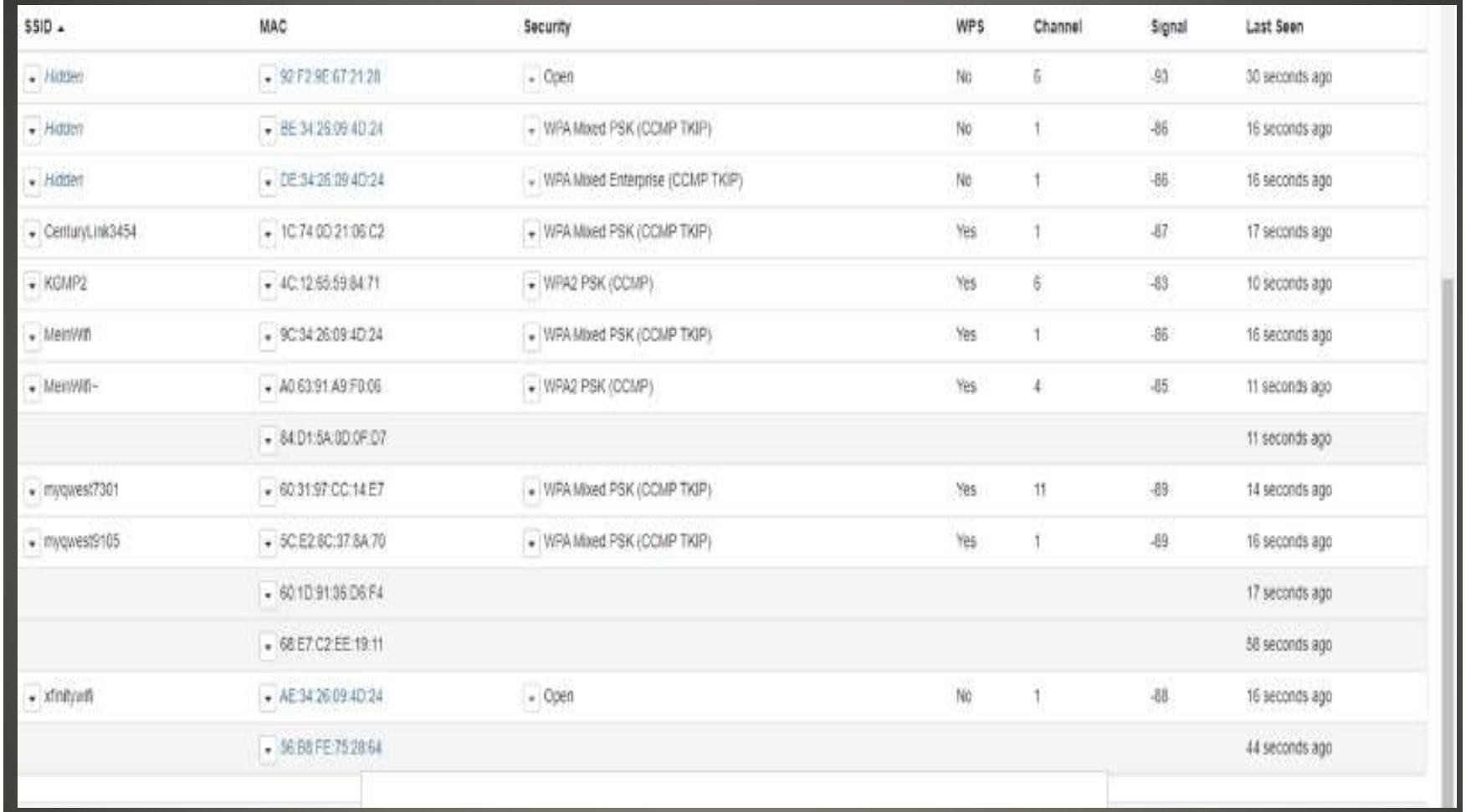
Wireless is radio

MacOS WiFi Scanner

Android Wi-Fi Analyzer


Wifi Analyzer
VIEW
SETTINGS
dlink_RM4*
dlink_Rm7
ITREE450
dlink_Rm3
Verizon-890L-3025
AGECW*
Signal Strength [dBm]
-30
-40
-50
-60
-70
-80
-90
1
2
3
4
5
6
7
8
9
10
11
12
13
14
Wifi Channels

- If you can see them, they can see you
- Segmentation is critical
- Only data is encrypted
  - Clients can be determined
  - Capture THEN decrypt
- Radio attenuation



SSID	MAC	Security	WPS	Channel	Signal	Last Seen
Hidden	92:F2:9E:67:21:28	Open	No	6	-93	30 seconds ago
Hidden	BE:34:26:09:4D:24	WPA Mixed PSK (CCMP TKIP)	No	1	-86	16 seconds ago
Hidden	DE:34:26:09:4D:24	WPA Mixed Enterprise (CCMP TKIP)	No	1	-86	16 seconds ago
CenturyLink3454	1C:74:0D:21:06:C2	WPA Mixed PSK (CCMP TKIP)	Yes	1	-67	17 seconds ago
KGMP2	4C:12:55:59:84:71	WPA2 PSK (CCMP)	Yes	6	-83	10 seconds ago
MeriWifi	9C:34:26:09:4D:24	WPA Mixed PSK (CCMP TKIP)	Yes	1	-86	16 seconds ago
MeriWifi~	A0:63:91:A9:F0:06	WPA2 PSK (CCMP)	Yes	4	-85	11 seconds ago
	84:D1:5A:0D:0F:D7					11 seconds ago
myqwest7301	60:31:97:CC:14:E7	WPA Mixed PSK (CCMP TKIP)	Yes	11	-89	14 seconds ago
myqwest9105	5C:E2:8C:37:8A:70	WPA Mixed PSK (CCMP TKIP)	Yes	1	-89	16 seconds ago
	60:1D:91:35:D6:F4					17 seconds ago
	68:E7:C2:EE:19:11					58 seconds ago
xfinitywifi	AE:34:26:09:4D:24	Open	No	1	-88	16 seconds ago
	96:B8:FE:75:28:64					44 seconds ago

Wireless scan

Dixie Normous Credit Card Security ™

Is your credit card number in a hacker's database?

You can easily find out now! All you need to do is enter its information here and we will scan thousands of hacker databases to see if any they have match yours.

Credit Card Number:

Expiration Date:

Your Zip Code:

SCAN DATABASE

- Chicken Little
- Tortoise and hare
- Each of us safer, all of us safer
- Awareness, Preparedness, Understanding
- Age does NOT diminish cognitive ability
- Life, Liberty, Pursuit of Happiness

  Cyber Security SIG

  Cyber Security Blog

  Internet

- Do nothing no problem
  <most of us>
- Do everything - catastrophic

- Tortoise and Hare
- Chicken Little

Computer Club, Help Center, SIGs, Presentations
Cyber Security SIG meetings, NEWSBLOG
Internet

- Questions, suggestions, comments?

SCCCCyber@gmail.com