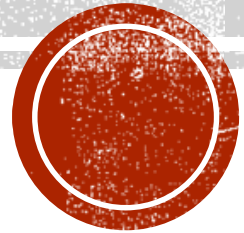
WIRELESS SECURITY, NETWORKS AND FACTS ABOUT THE IoT

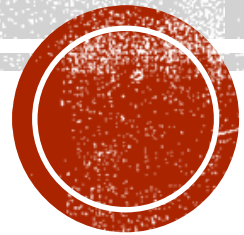
Dan Durkee, Executive VP\Partner\Network Engineer
Connecting Point Computer Center
303 S Third St, Bismarck, ND 58504
ddurkee@connectingpoint.biz



AGENDA

- Security Policies – Who has them? Do we need them?
- Wireless Encryption – Where have we been and were are we going?
  - The Wireless Spectrum – where does wireless fit?
  - A Quick Look – Meraki, Ruckus
  - Encryption Method
  - Authentication Method
  - Encryption Algorithm
- Network Infrastructure – Better Security
- Fun Facts about the Internet of Things – (Time Permitting)

SECURITY POLICIES

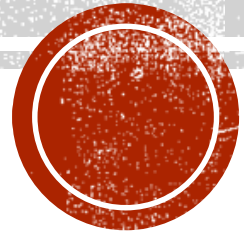


WHO HAS A FORMAL WIRELESS SECURITY POLICY?

SO WHERE DO WE START WITH POLICIES?

- Encryption Method
- Authentication Method
- Encryption Algorithm
- Network Infrastructure

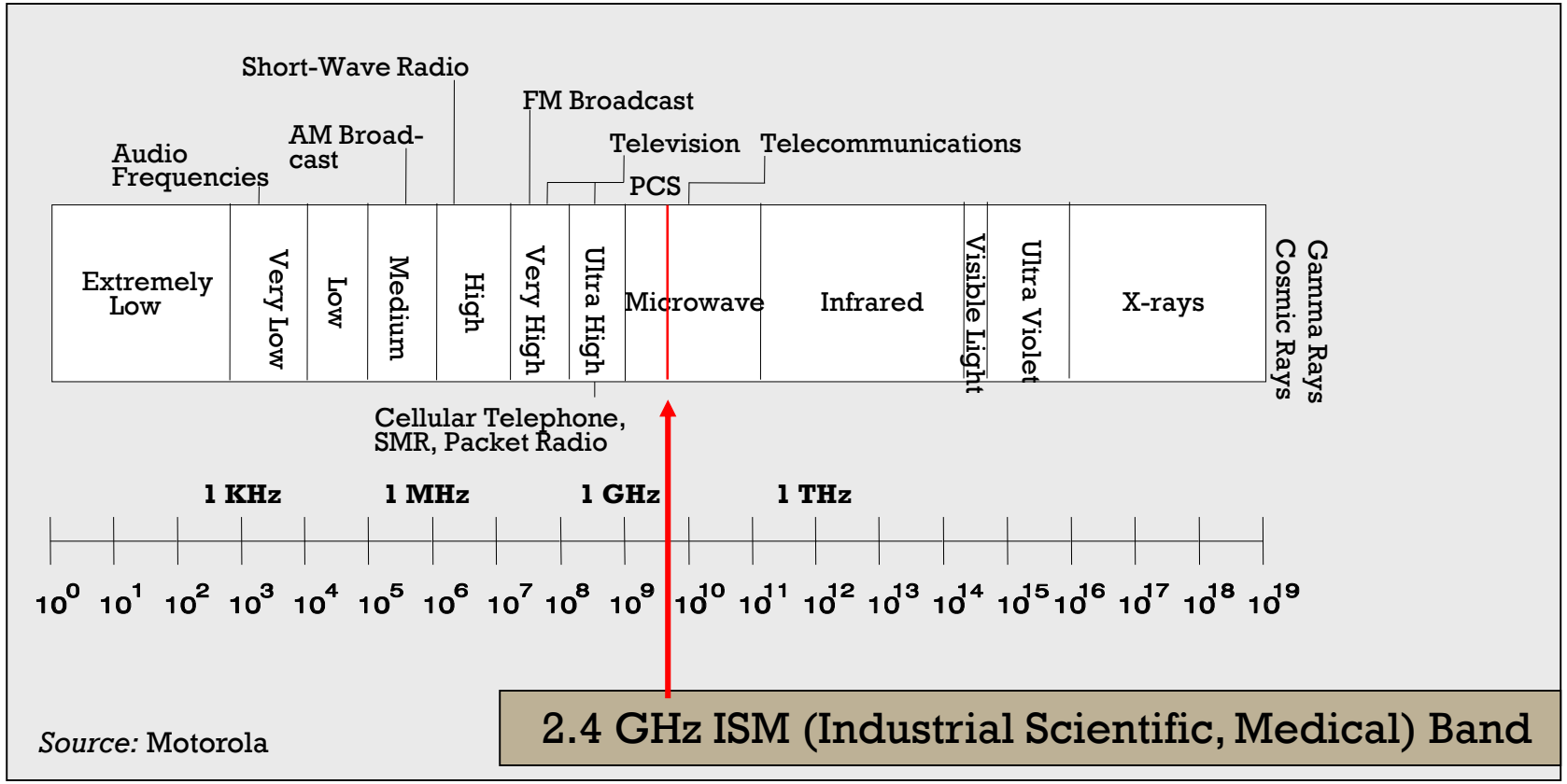
WIRELESS SECURITY



WIRELESS ENCRYPTION – A BRIEF HISTORY

- The Wireless Spectrum – where does wireless fit?
- A Quick Look – Meraki, Ruckus
- Encryption Method
  - WEP – Short for Wired Equivalent Privacy (or Wireless Encryption Protocol)
  - WPA - Wi-Fi Protected Access
  - WPA2 - Wi-Fi Protected Access 2
- Authentication Method
  - PSK
  - Radius Server
- Encryption Algorithm
  - TKIP
  - AES

THE WIRELESS SPECTRUM - WHERE WIRELESS FITS?



Meraki

Network: Dan Durkee - Wireless

- Monitor
- Configure
  - SSIDs
  - Access control
  - Firewall & traffic shaping
  - Users
  - Splash page
  - SSID availability
  - Network-wide settings
  - Group policies
  - Radio settings
  - Add devices
- Organization
- Help

Access control

SSID: Hockey

Network access

Association requirements

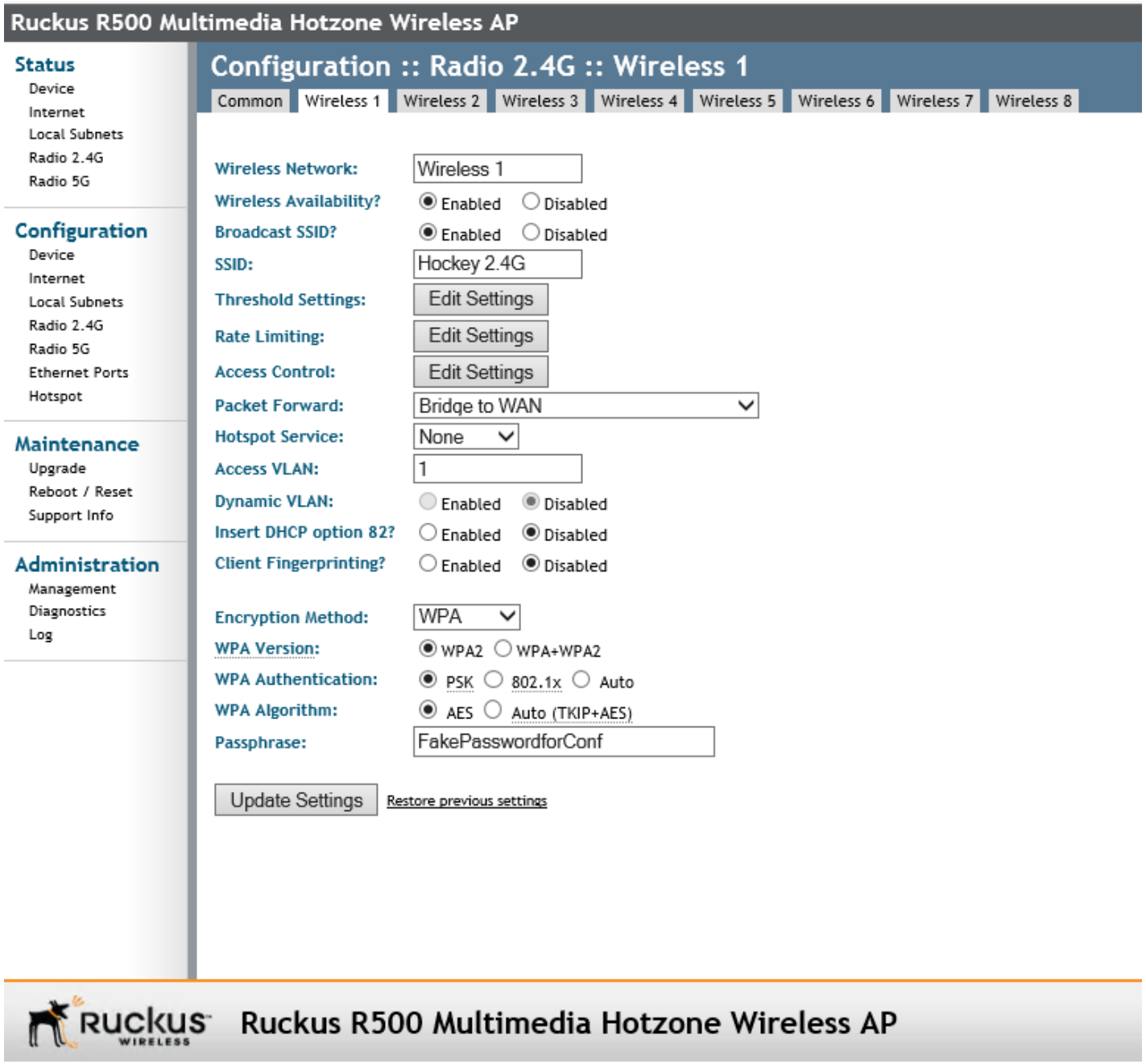
- ○ Open (no encryption)
  Any user can associate
- ◉ Pre-shared key with WPA2
  Users must enter this key to associate: •••••••••• Show key
- ○ MAC-based access control (no encryption)
  RADIUS server is queried at association time
- ○ WPA2-Enterprise with Meraki authentication
  User credentials are validated with 802.1X at association time

WPA encryption mode: WPA1 and WPA2

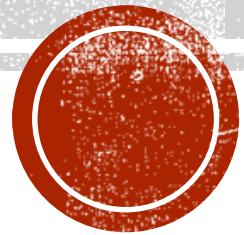
802.11r: Disabled

Splash page

- ◉ None (direct access)
  Users can access the network as soon as they associate
- ○ Click-through
  Users must view and acknowledge your splash page before being allowed on the network
- ○ Sign-on with Meraki authentication
  Users must enter a username and password before being allowed on the network
- ○ Sign-on with SMS Authentication BETA
  Users enter a mobile phone number and receive an authorization code via SMS.
  After a trial period of 25 texts, you will need to connect with your Twilio account on the Network-wide settings page.
- ○ Billing (paid access)
  Users choose from various pay-for-access options, or an optional free tier
- ○ Systems Manager Sentry
  Only devices with Systems Manager can access this network


Ruckus R500 Multimedia Hotzone Wireless AP
Status
Device
Internet
Local Subnets
Radio 2.4G
Radio 5G
Configuration
Device
Internet
Local Subnets
Radio 2.4G
Radio 5G
Ethernet Ports
Hotspot
Maintenance
Upgrade
Reboot / Reset
Support Info
Administration
Management
Diagnostics
Log
Configuration :: Radio 2.4G :: Wireless 1
Common
Wireless 1
Wireless 2
Wireless 3
Wireless 4
Wireless 5
Wireless 6
Wireless 7
Wireless 8
Wireless Network:
Wireless 1
Wireless Availability?
Enabled
Disabled
Broadcast SSID?
Enabled
Disabled
SSID:
Hockey 2.4G
Threshold Settings:
Edit Settings
Rate Limiting:
Edit Settings
Access Control:
Edit Settings
Packet Forward:
Bridge to WAN
Hotspot Service:
None
Access VLAN:
1
Dynamic VLAN:
Enabled
Disabled
Insert DHCP option 82?
Enabled
Disabled
Client Fingerprinting?
Enabled
Disabled
Encryption Method:
WPA
WPA Version:
WPA2
WPA+WPA2
WPA Authentication:
PSK
802.1x
Auto
WPA Algorithm:
AES
Auto (TKIP+AES)
Passphrase:
FakePasswordforConf
Update Settings
Restore previous settings
Ruckus R500 Multimedia Hotzone Wireless AP

ENCRYPTION METHOD



WEP – WIRED EQUIVALENT PRIVACY OR WIRELESS ENCRYPTION PROTOCOL

- WEP is part of the IEEE 802.11 wireless networking standard and was designed to provide the same level of security as that of a wired LAN. Because wireless networks broadcast messages using radio, they are susceptible to eavesdropping. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.
- WEP was the encryption scheme considered to be the initial standard for first generation wireless networking devices. WEP is used at the two lowest layers of the OSI model - the data link and physical layers; it therefore does not offer end-to-end security. WEP - Wired Equivalent Privacy (WEP) was once the most widely used Wi-Fi security algorithm.
- WEP recycles the same key for encrypting all the packets flowing across the network.
- WEP was ratified as a Wi-Fi security standard in September of 1999
- The Wi-Fi Alliance officially retired WEP in 2004

WPA - WI-FI PROTECTED ACCESS

- Short for Wi-Fi Protected Access, a Wi-Fi standard that was designed to improve upon the security features of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP (i.e., as a software upgrade to existing hardware), but the technology includes two improvements over WEP:
- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

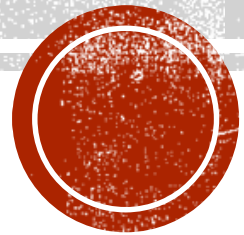
WPA - WI-FI PROTECTED ACCESS

- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.
- It should be noted that WPA is an interim standard that will be replaced with the IEEE's 802.11i standard upon its completion.

WPA2 - WI-FI PROTECTED ACCESS 2

- Short for Wi-Fi Protected Access 2, the follow on security method to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication. [Adapted from Wi-Fi.org]
- There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

AUTHENTICATION



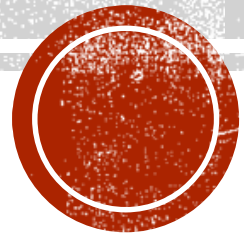
WPA2- PRE-SHARED KEY (PSK)

- Short for Wi-Fi Protected Access 2 - Pre-Shared Key, and also called WPA or WPA2 Personal, it is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users and/or networks without dedicated IT staff who can manage an enterprise authentication server.
- To encrypt a network with WPA-PSK you provide your router/AP not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. Using a technology called TKIP (for Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed.

WPA2-ENTERPRISE (RADIUS SERVERO

- A router (or Wi-Fi router) feature that is designed to authenticate individual users to an external server via username and password. WPA Enterprise also gives each PC a unique encryption key, which the user never sees, so they can't share it. To use WPA/WPA2 Enterprise you need a RADIUS server.
- Also applies to wireless access points and wireless controllers supporting WPA2

ALGORITHM



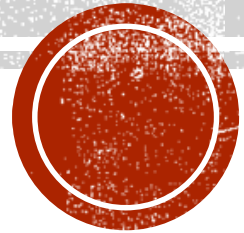
TEMPORAL KEY INTEGRITY PROTOCOL

- Temporal Key Integrity Protocol or TKIP was a stopgap security protocol used in the IEEE 802.11 wireless networking standard.
- TKIP was designed by the IEEE 802.11i task group and the Wi-Fi Alliance as an interim solution to replace WEP without requiring the replacement of legacy hardware.
- This was necessary because the breaking of WEP had left Wi-Fi networks without viable link-layer security, and a solution was required for already deployed hardware. TKIP is no longer considered secure and was deprecated in the 2012 revision of the 802.11 standard

ADVANCED ENCRYPTION STANDARD

- The Advanced Encryption Standard (AES), also referenced as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
- AES is based on the Rijndael cipher developed by two Belgian cryptographers, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.
- For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

NETWORK INFRASTRUCTURE



ROGUE APS

- Rogue AP is unmanaged AP plugged into wired enterprise network by unwilling or malicious employees or visitors
- Rogue AP can expose wired enterprise network to outsiders over its RF signal spillage
- Rogue AP threat is not mitigated by firewalls, WPA2, 802.1x, NAC, anti-virus or wire side scanners
- Sensor based wireless intrusion prevention system (WIPS) detects, blocks and locates Rogue APs
- Testing of AP's connectivity to monitored enterprise network is key technology enabler for reliable protection from Rogue APs

RADIUS SERVERS

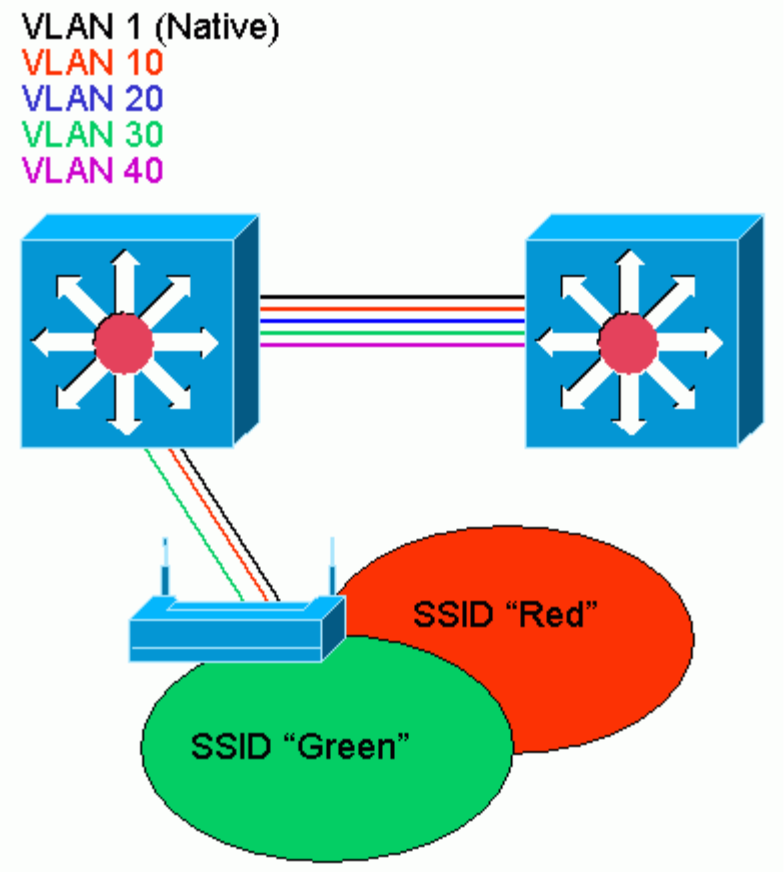
- The use of a Radius server for authentication can provide additional security but it will add server and administrator costs and may be the most appropriate for only the larger schools.
  - RADIUS Centralized User Authentication
    - Authentication is provided between the wireless client and the RADIUS server, in conjunction with the IEEE 802.1x standard-based network log-in
  - Any RADIUS supporting EAP-MD5, EAP-TLS, EAP-TTLS
    - Implemented in conjunction with 802.1x to provide a secure authentication solution for Wireless clients
  - RADIUS Accounting
    - Username, start time, stop time, packet input/output

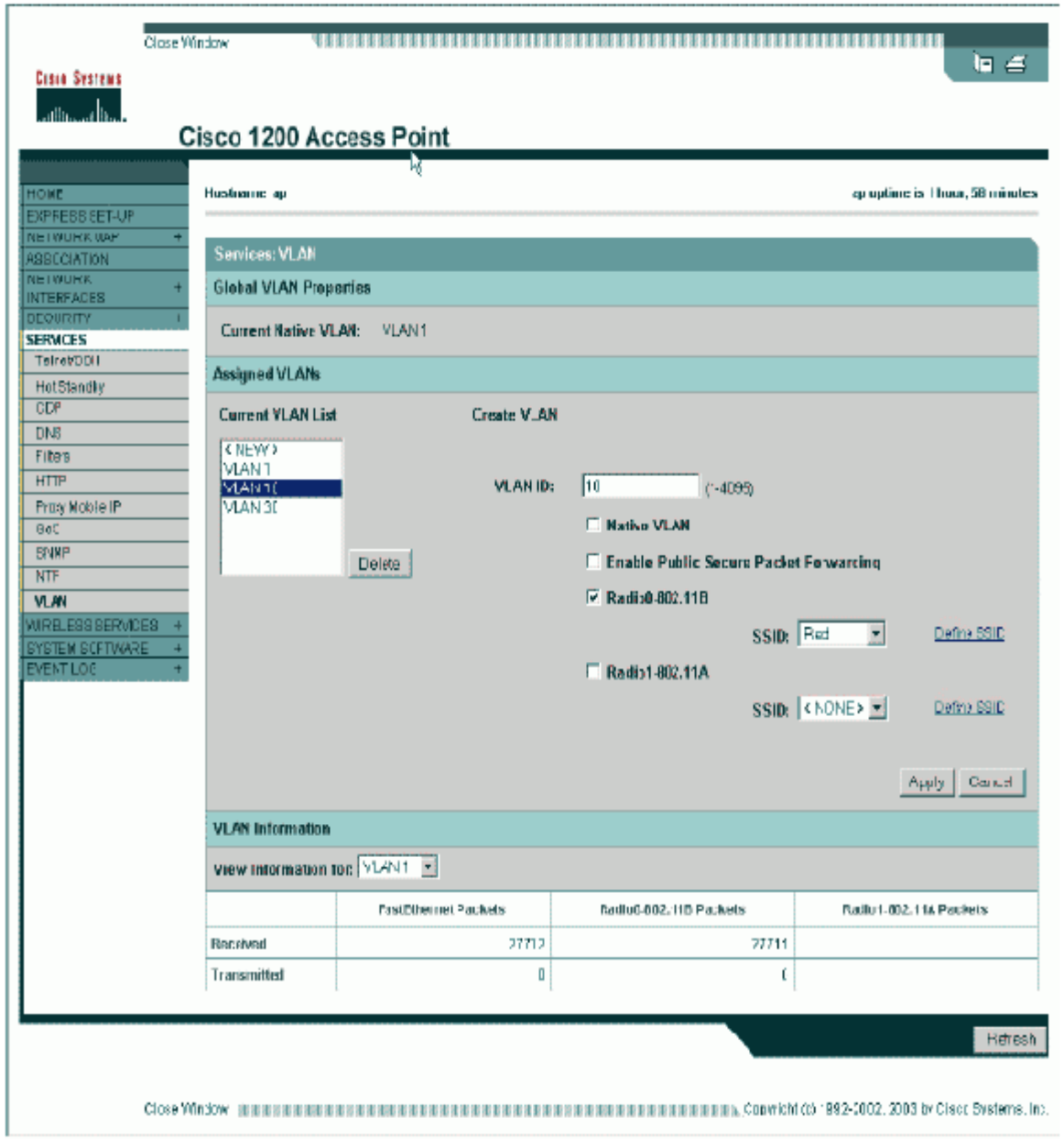
SEGMENTING NETWORK TRAFFIC

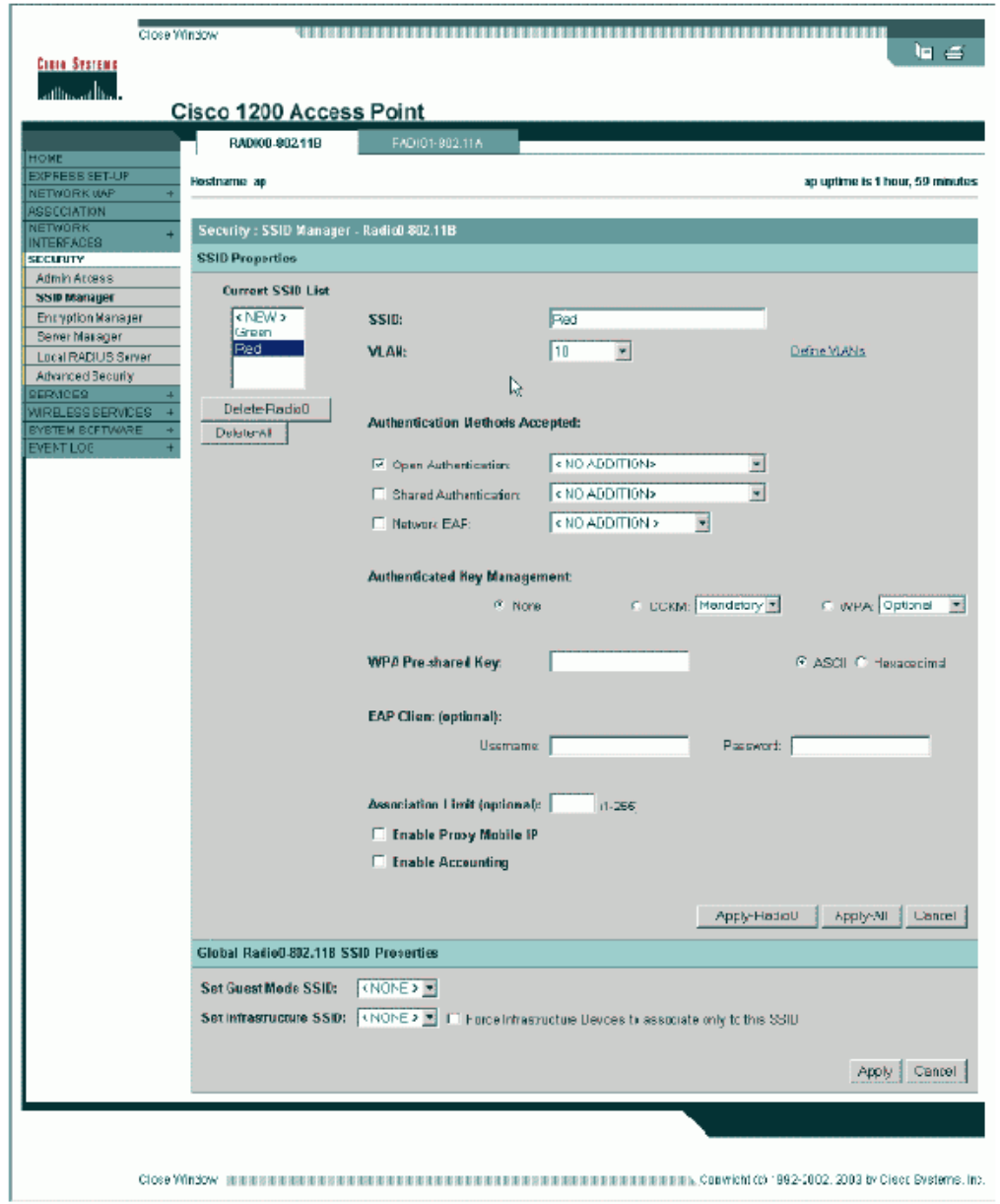
- Segmenting with a Switch – Tagging with VLANS
- Segmenting with a Router – Additional LAN Ports or DMZ
- Segmenting with Additional Switches and Internet Connection
- Identity Management

VLANS

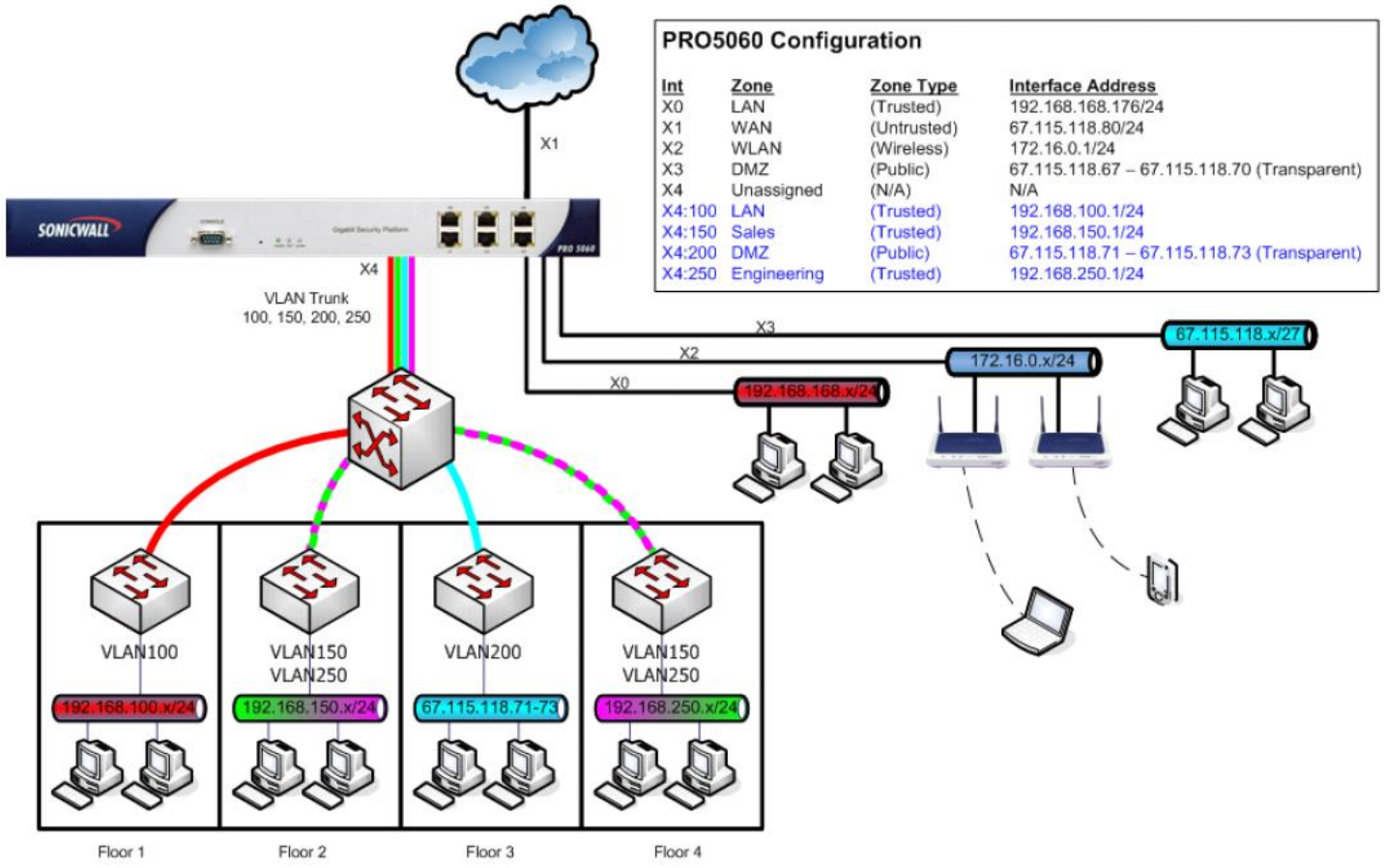
- In this sample network, VLAN 1 is the Native VLAN, and VLANs 10, 20, 30 and 40 exist, and are trunked to another switch chassis. Only VLANs 10 and 30 are extended into the wireless domain. The Native VLAN is required to provide management capability and client authentications.



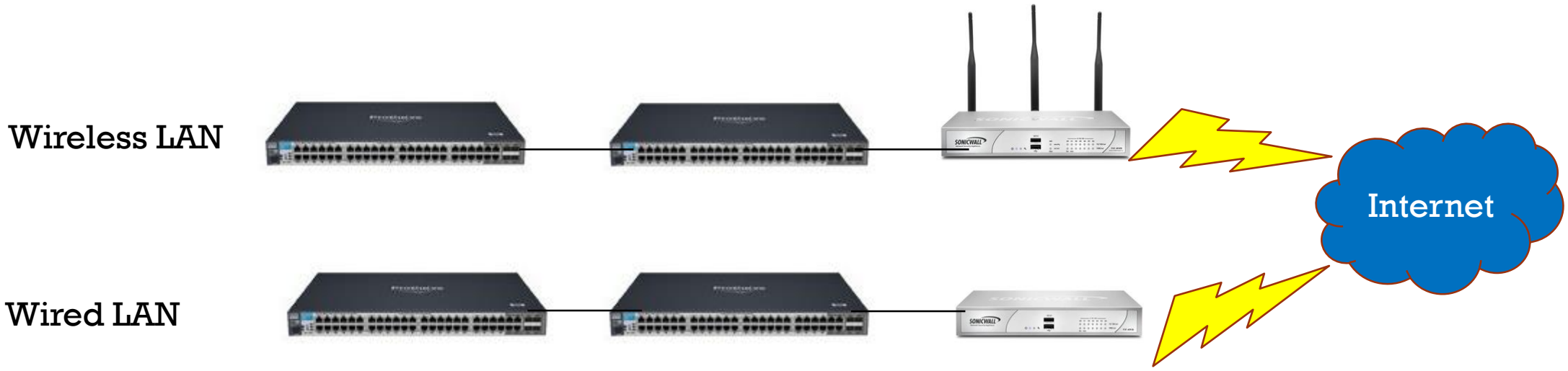

Close Window
Cisco Systems
Cisco 1200 Access Point
HOME
EXPRESS SET-UP
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
SERVICES
Telnet/SSH
Hot Standby
CDP
DNS
Filters
HTTP
Proxy Mobile IP
QoS
SNMP
NTP
VLAN
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname: ap
ap uptime is 1 hour, 58 minutes
Services: VLAN
Global VLAN Properties
Current Native VLAN: VLAN1
Assigned VLANs
Current VLAN List
Create VLAN
< NEW >
VLAN 1
VLAN 10
VLAN 30
Delete
VLAN ID: 10 (1-4095)
Native VLAN
Enable Public Secure Packet Forwarding
Radio0-802.11B
SSID: Red
Define SSID
Radio1-802.11A
SSID: < NONE >
Define SSID
Apply
Cancel
VLAN Information
View information for: VLAN1
FastEthernet Packets
Radio0-802.11B Packets
Radio1-802.11A Packets
Received 27713 27711
Transmitted 0 0
Refresh
Close Window
Copyright (c) 1992-2002, 2003 by Cisco Systems, Inc.


Close Window
Cisco Systems
Cisco 1200 Access Point
RADIO0-802.11B
RADIO1-802.11A
HOME
EXPRESS SET-UP
NETWORK MAP
ASSOCIATION
NETWORK INTERFACES
SECURITY
Admin Access
SSID Manager
Encryption Manager
Server Manager
Local RADIUS Server
Advanced Security
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap
ap uptime is 1 hour, 59 minutes
Security: SSID Manager - Radio0-802.11B
SSID Properties
Current SSID List
< NEW >
Green
Red
Delete Radio0
Delete All
SSID: Red
VLAN: 10
Define VLANs
Authentication Methods Accepted:
Open Authentication: < NO ADDITION >
Shared Authentication: < NO ADDITION >
Network EAP: < NO ADDITION >
Authenticated Key Management:
None
CCKM: Mandatory
WPA: Optional
WPA Pre-shared Key:
ASCII
Hexadecimal
EAP Client (optional):
Username:
Password:
Association Limit (optional): (1-256)
Enable Proxy Mobile IP
Enable Accounting
Apply-Radio0
Apply-All
Cancel
Global Radio0-802.11B SSID Properties
Set Guest Mode SSID: < NONE >
Set Infrastructure SSID: < NONE >
Force Infrastructure Devices to associate only to this SSID
Apply
Cancel
Close Window
Copyright (c) 1992-2002, 2003 by Cisco Systems, Inc.

ROUTERS – PORTS AND DMZ



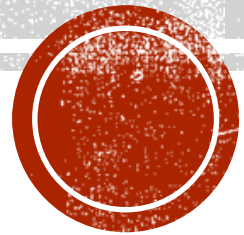
SWITCHES AND ADDITIONAL INTERNET CONNECTION



IDENTITY MANAGEMENT – CISCO IDENTITY SERVICES

- ***Centralize and unify network access policy management*** to provide consistent, secure access to end users
- ***Gain greater visibility*** and more accurate device identification
- ***Implement logical network segmentation based on business rules*** by taking full advantage of Cisco TrustSec technology
- ***Simplify guest experiences*** for easier guest onboarding and administration
- ***Streamline BYOD and enterprise mobility*** with easy, out-of-the-box setup for self-service device onboarding and management
- ***Share deep contextual data with third-party ecosystem partner solutions*** through Cisco Platform Exchange Grid (pxGrid), included within ISE. Contextual data improve the efficacy of partner solutions and accelerate their abilities to identify, mitigate, and remediate network threats.

BASIC RECOMMENDATIONS



PHYSICAL CONTROL

- Physically hide or secure access points to prevent tampering. In many buildings, access points can be installed in the plenum space above the ceiling, providing optimal coverage in a secure location.
- Use video surveillance cameras to monitor your office building and site for suspicious activity.

(POST 2006) SECURITY MODES - BASIC

- WPA2 + AES
- WPA + AES
- WPA + TKIP/AES (TKIP is there as a fallback method)
- WPA + TKIP
- WEP
- Open Network (no security at all)

- Mac Filtering? - MAC filters can be used but they can also be easily spoofed. This can be extra administration for the network admin.

CHANGE THE DEFAULT PASSWORD OF THE AP AND THE CONTROLLER

- Change any default passwords on the AP and carefully restrict remote administration of the AP. If possible, do not allow administration of the Access Point from the wireless network.

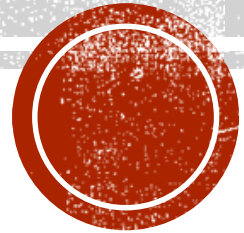
CHANGE DEFAULT SSID – HIDE SSID

- Change the default SSID (the wireless access point identifier) and disable the broadcasting option. In order for a user to find such a network, they must know the SSID name and will need to manually enter it into their client system. This is inconvenient for the user but provides a higher level of security. There is software out on the internet that can discover these WAPs even if then changes are implemented.

ENABLE LOGGING

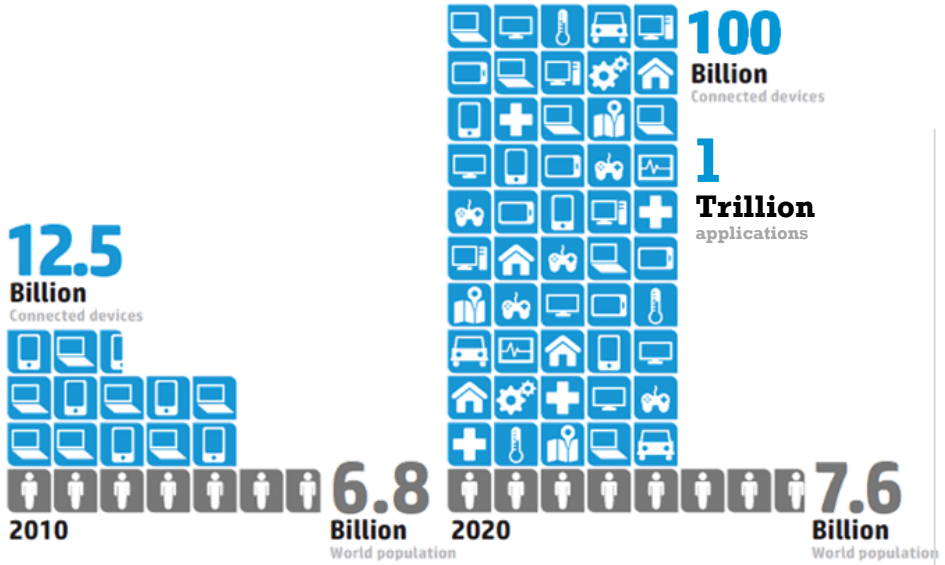
- Enable logging on your access point. This will be helpful if you must track user activity in the event of a security incident such as a network intrusion or a stolen laptop.

FUN FACTS ABOUT THE INTERNET OF THINGS



DEVICES AND PEOPLE

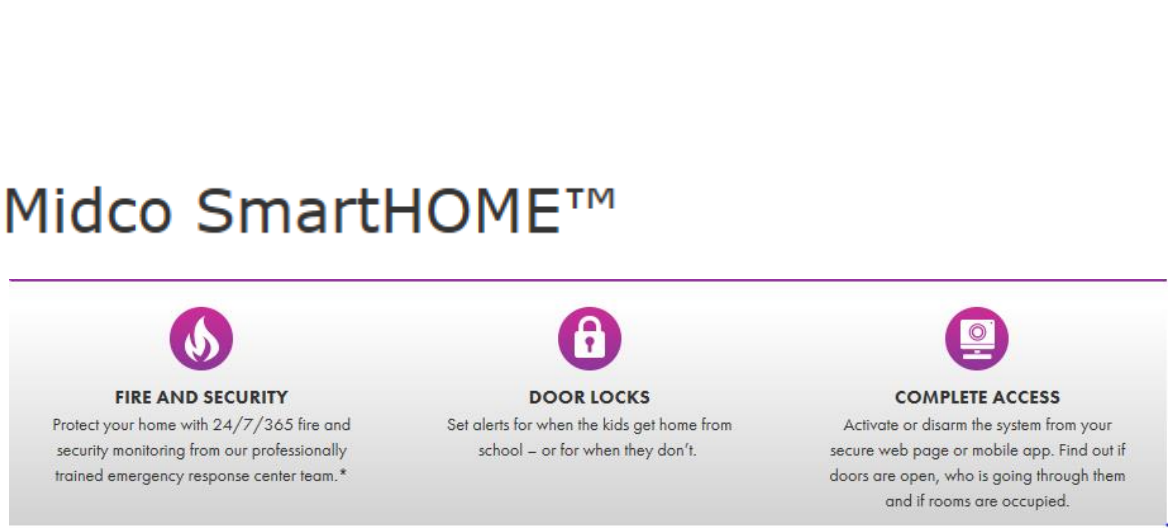
- **In 2010, there were already more "things" connected to the Internet than people.**
- By 2020, the amount of Internet-connected things will reach 50 billion (100 billion according to HP), with $19 *trillion* in profits and cost savings coming from IoT over the next decade, according to **Cisco Systems** (NASDAQ: CSCO) .



More applications, more connected devices

KNOWLEDGE OF THE INTERNET OF THINGS IS GROWING SLOWLY.

- Right now, about half of Americans don't know that smart thermostats and smart refrigerators are already on the market.



CONNECTED HOMES WILL BE A HUGE PART OF THE INTERNET OF THINGS

- By 2019, companies will ship 1.9 billion connected home devices, bringing in about $490 billion in revenue. **Google** (NASDAQ: GOOG) (NASDAQ: GOOGL) and **Samsung** are already ahead of the pack.
- Google bought smart thermostat maker, Nest Labs, last year for $3.2 billion, and Samsung purchased connected home company SmartThings for $200 million.

SMART STUFF

- Five years from now, more than 20% of U.S. consumers will own smart refrigerators and smart watches.

LG Internet Refridgerator

IVP6

- **IPV6 gives us 3.4×10^{38} - 340 undecillian numbers**
- Meaning that companies can build a lot of small devices that connect to the Internet without running out of IP addresses.
- How big is this number?
  - The bakery-cafe chain Au Bon Pain (with a few other organizations) is being sued. This is how much money the person suing them is demanding:

    $2,000,000,000,000,000,000,000,000,000,000,000,000

  - If you extracted all the elements from the Earth's crust, purified them, you somehow sold them at their current market price, they would be worth ...

    ← CLOSER →$1,600,000,000,000,000,000,000,000

    $2,000,000,000,000,000,000,000,000,000,000,000,000

    - Note: One of many reasons that this idea wouldn't make sense in practice is because many elements (like U-235) are valuable but they are valuable because it's hard to manufacture or purify them, not just because they're rare. Plus if you sold them, the market would crash. Both in the sense that the supply would cause a drop in prices, and the sense that the market is like 20 miles above the mantle and you just removed the crust supporting it.

WEARABLE TECH

- **U.S. consumers are warming to wearable tech.** Right now, just 7% of consumers own a wearable tech device, but by the end of next year, that number will have jumped to 28%.

INTERNET CLOTHING

- **Internet-connected clothing is coming.** By 2020, 14% of consumers expect to purchase some form of it.

IOT SECURITY

- **People are already concerned about IoT security.** That's why 69% of U.S. consumers think they should own the personal data on all Internet-connected devices they own.

DO NOT GO COW TIPPING IN DENMARK

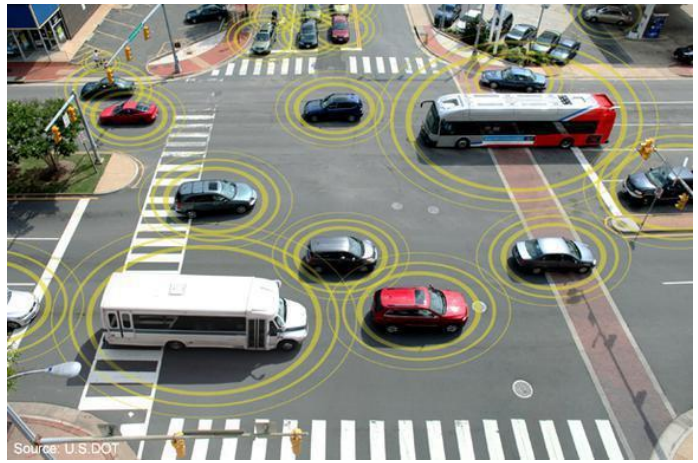
- **The Internet of Things isn't just about devices.** A Dutch company uses Internet-connected sensors on cattle to tell farmers when the animals are sick or pregnant. Each cow sends about 200 MB of data per year.

CAR DATA

- **60% of Americans are willing to share data from their car with the vehicle's manufacturer** -- if it includes one free maintenance session. But carmakers aren't the only ones interested in your car's data; advertisers are already begging for it.

CAR WIRELESS

- **Gartner predicts that one in five vehicles on the road will have some form of wireless connection by 2020.** That's not so far fetched, considering Mercedes-Benz already has a partnership with Nest that allows the car to tell the thermostats to adjust the temperature when a driver arrives or leaves home. And it's really good news for **Sierra Wireless**, which already has **Ford**, **BMW**, **Tesla**, **Volvo**, and **Toyota** as customers.



CAR AND NO DRIVER

- **Autonomous vehicles are a big part of the Internet of Things.** Last month, an **Audi** A7 drove more than 550 miles (from San Francisco to Las Vegas) almost entirely on its own. The car uses some of **NVIDIA**'s processors as part of the brains behind the system.

SMALL CHANGES, BIG SAVINGS

- **Small IoT efficiencies could bring big savings. General Electric** believes that using Industrial Internet (the company's term for the Internet of Things) to make oil and gas exploration and development just 1% more efficient would result in a savings of $90 billion.

A PILL WITH A SENSOR

- **In 2008, a company called Proteus Digital Health won a U.S. patent for a pill you can swallow with a tiny sensor inside of it.** The sensor transmits data about when a patient takes his or her medication, and pairs with a wearable device to inform family members if it's not taken at the right time.

MACHINE TO MACHINE CHATTER

- **The U.S. doesn't dominant Internet of Things**. According to a report released by GSMA over the summer, 27% of all global machine-to-machine (M2M) connections are in China, while all of Europe has 29%, and the U.S. has 19%. In the decade leading up to 2020, China's government has committed to spend $603 billion for M2M connections.

Central Daylight Tim

Map Vehicle Fleet Reports Admin Support

VEHICLE LIST

Group: ALL VEHICLES

Attribute: All Attributes

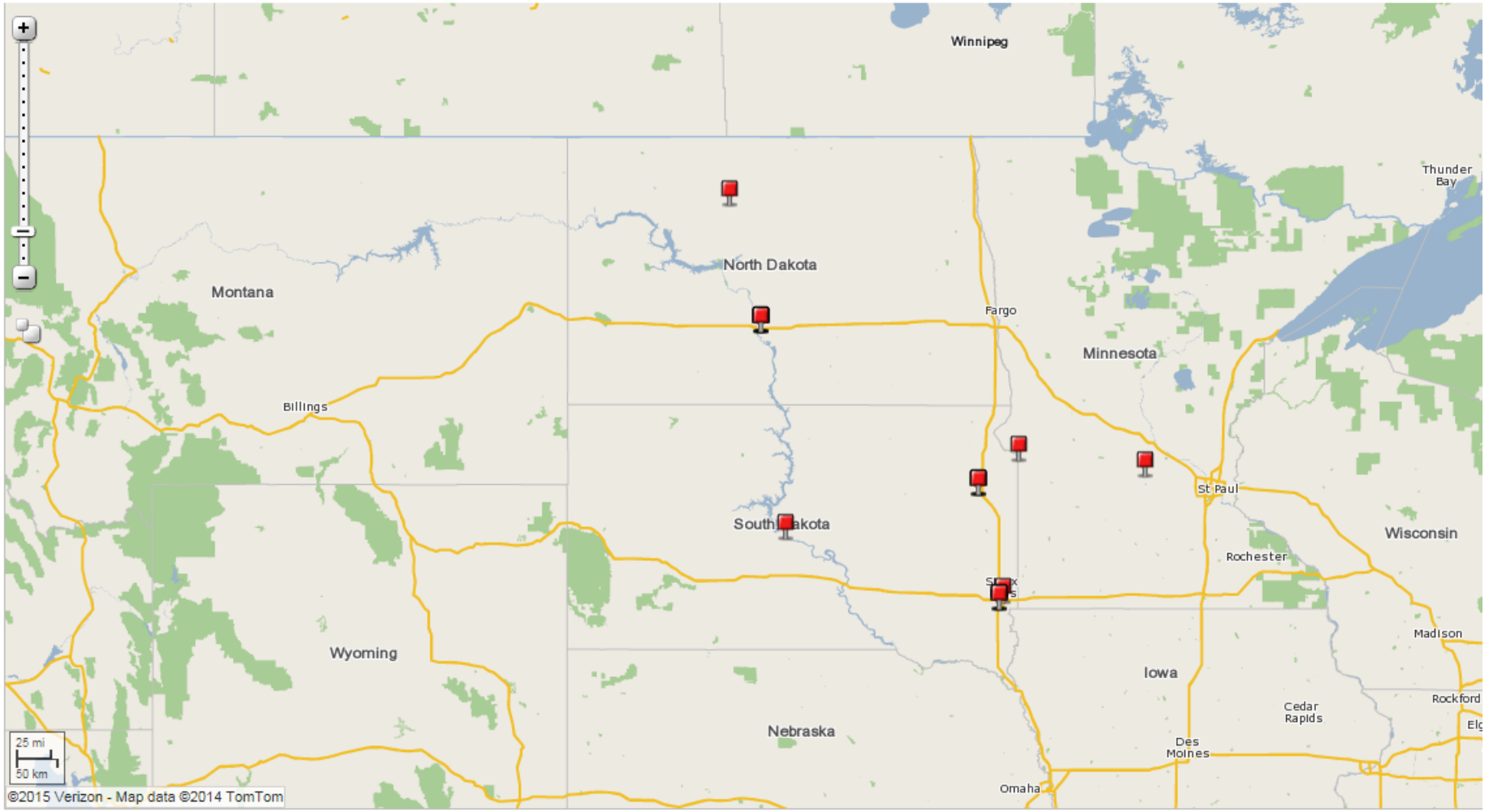
View by: Vehicle Label

Refine:

Select a Vehicle

- BIS - 2007 WHITE CARAVAN
- BIS - 2007 WHITE EQUINOX
- BIS - 2008 GREY IMPALA
- BIS - 2011 SILVER IMPALA
- BIS - 2012 BLACK IMPALA
- BIS - 2013 GOLD EQUINOX
- BIS - 2014 WHITE DODGE CARAVAN
- HUT-2008 WHITE FORD E150 VAN
- PIR-2005 BLUE DODGE CARAVAN SE
- SF - 2007 DODGE CARAVAN
- SF - 2007 WHITE MALIBU
- SF - 2010 BLACK IMPALA
- SF - 2010 WHITE IMPALA
- SF - 2012 SILVER IMPALA
- WTN-2008 BLACK CHEVY TRALBLAZER
- WTN-2008 GOLD EQUINOX
- WTN-2009 BLACK CHEVY IMPALA LT
- WTN-2010 SILVER EQUINOX
- WTN-2015 WHITE DODGE GRAND CARAVAN SE

Overview Map | Location Detail | Track Vehicles



FEDERAL TRADE COMMISSION

- **Consumers aren't the only ones concerned about all of the data the Internet of Things will produce.** In a speech last month, Federal Trade Commission Chairwoman, Edith Ramirez laid out three concerns the U.S. government has with the IoT: ubiquitous data collection, unintended data use, and (of course) security.

ATTACK ON THE INTERNET

- **Malwarebytes Labs predicts that this year, we'll see the first major attack on Internet of Things devices.** "Both mainstream media and the general public will hear about the first major hacker attack against an Internet connected device (that was previously not connected)," the company said in a blog post. How comforting.

RESEARCH

- HP Internal Research 2014
- Accenture 2013 CIO Mobility Survey
- Juniper Research – Jan. 2014
- Cisco Internal Research 2014
- Motorola
- Webopedia and Wikipedia
- 17 Facts and the Internet of Things You Didn't Know, Motley Fool, Chris Neiger, Feb 6, 2015
- XKCD.com