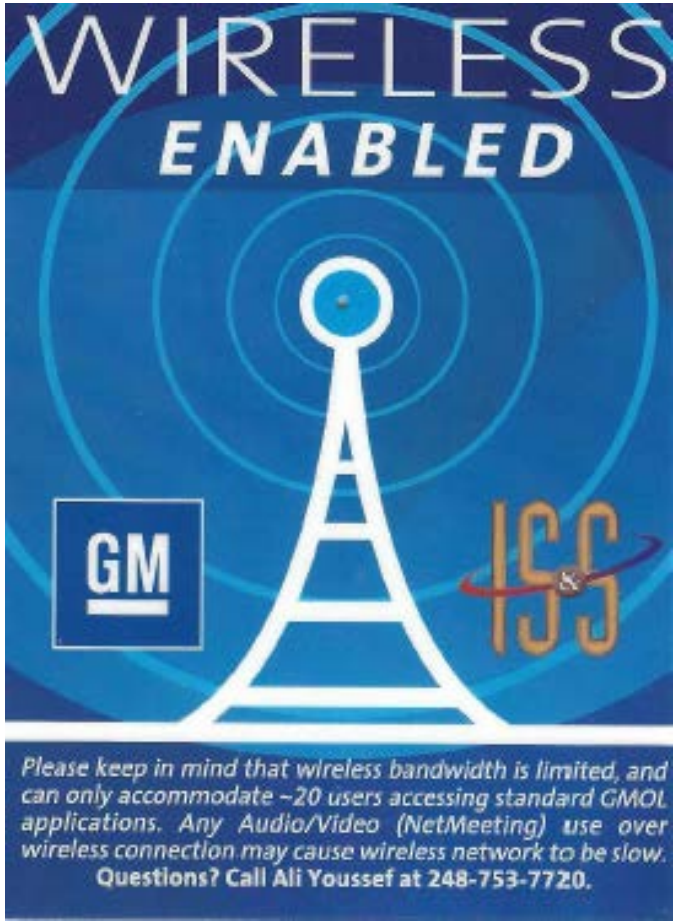
The Evolution Of Guest Access

Ali Youssef *CPHIMS PMP CWNE # 133*
Sr. Mobility Architect @ Henry Ford Health System
Twitter: Aliyoussef_

Guest Access - The Beginning

- Islands of Wi-Fi coverage
- Autonomous access points
- Best Effort Support
- Limited access point capabilities
- Limited bandwidth and visibility

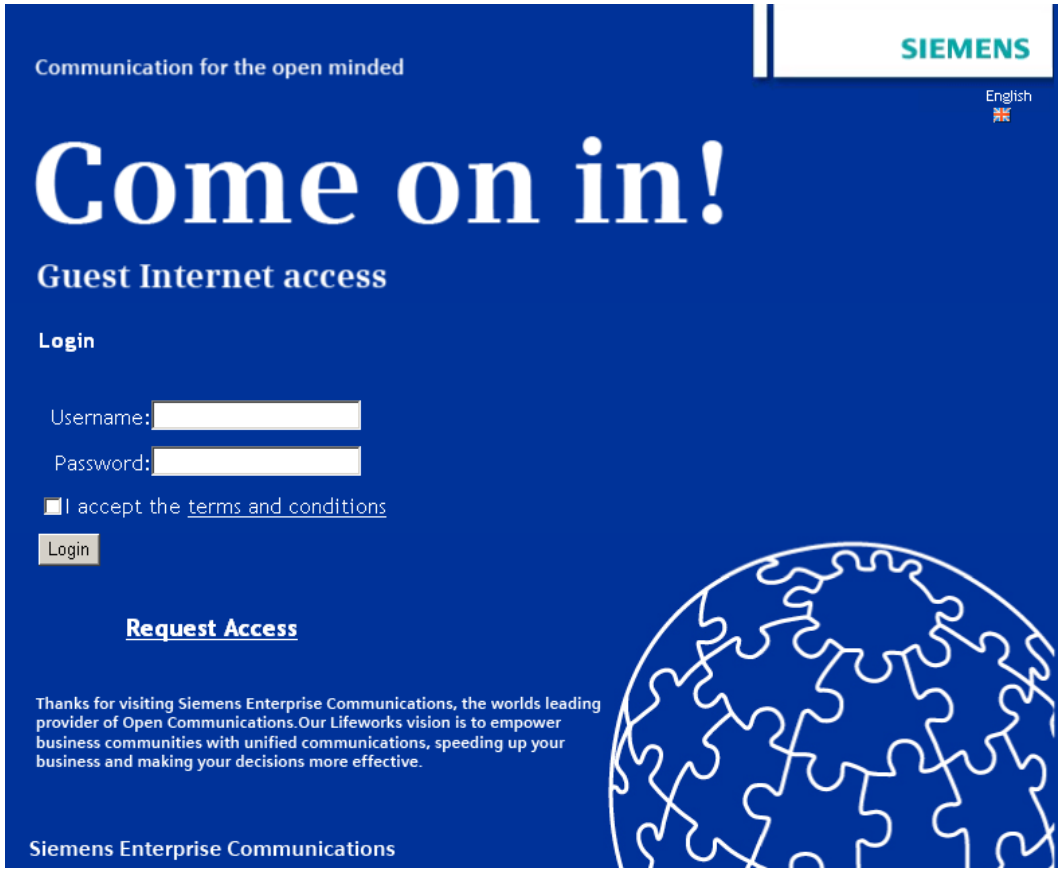


Guest Access Today

- Ubiquitous reliable connectivity is expected
- QoE and patient satisfaction can cost you real dollars.
- Mission critical in some settings
- The name of the game is guest/patient engagement and collecting useful analytics
- High priority response
- IT, Marketing, and Security collaboration.

Guest Onboarding Experience

- Guest Access Design heavily dependent on customer requirements, and desired end user experience.
- Captive portal with terms and conditions
  - Internal, or external
  - Sponsored or self registration
  - Open Access
  - Unique Key/scratch ticket.
  - Guest Brochures



Guest Onboarding Example

Captive Portal

- Branding – Identifying your business
- Key Communications. Driving traffic to specific sites
- Terms and Conditions – Liability
  - Music and Video downloads.
- Multi-lingual Support
- Auto Browser Pop-up

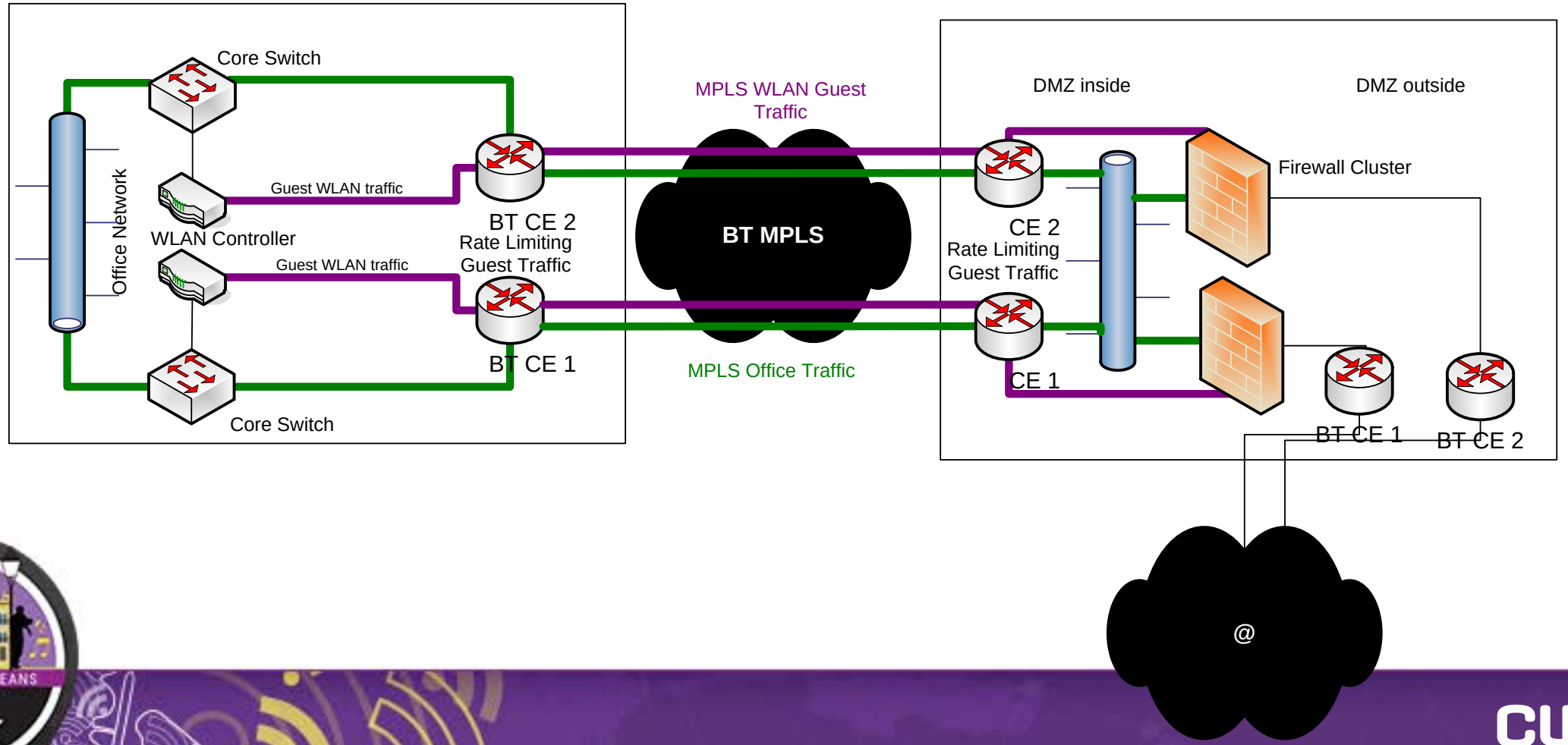
Security Consideration

- Physical and or logical separation from the enterprise network.
- Protecting guests devices from each other.
- Traffic filtering.
  - DNS traffic filtering.
  - Stateful packet inspection.
  - Port level controls (53, 80, 8080, 443, 21, 22, 23,etc.).
  - Layer 7 visibility and control
- Preventing employees from using the guest network with corporate devices.

Evolution of Design

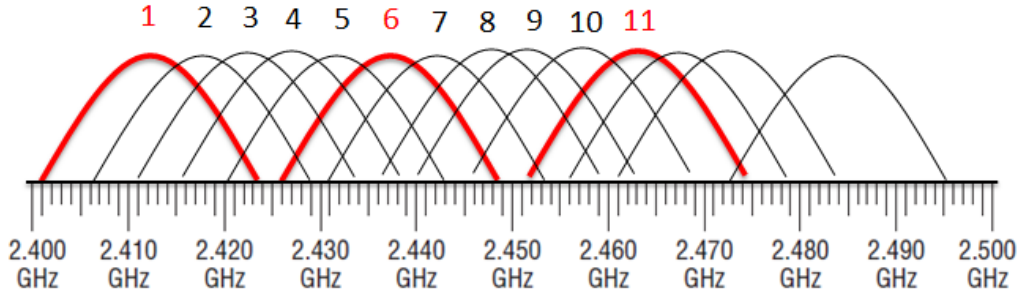
- In the past the key physical design components were wireless access points, controllers, and DMZ / firewall with a robust internet connection.
- Today guest access design can include
  - NAC and automated role provisioning
  - Customized splash pages
  - End Point Security
  - Self Registration
  - Scalable DHCP requirement as well as sophisticated content filtering.

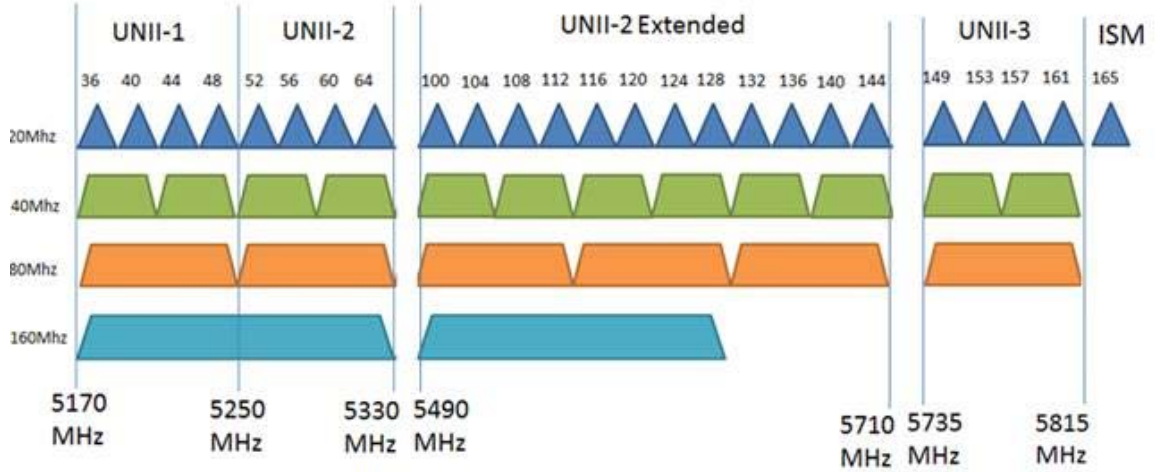
Architecture Overview



RF Considerations

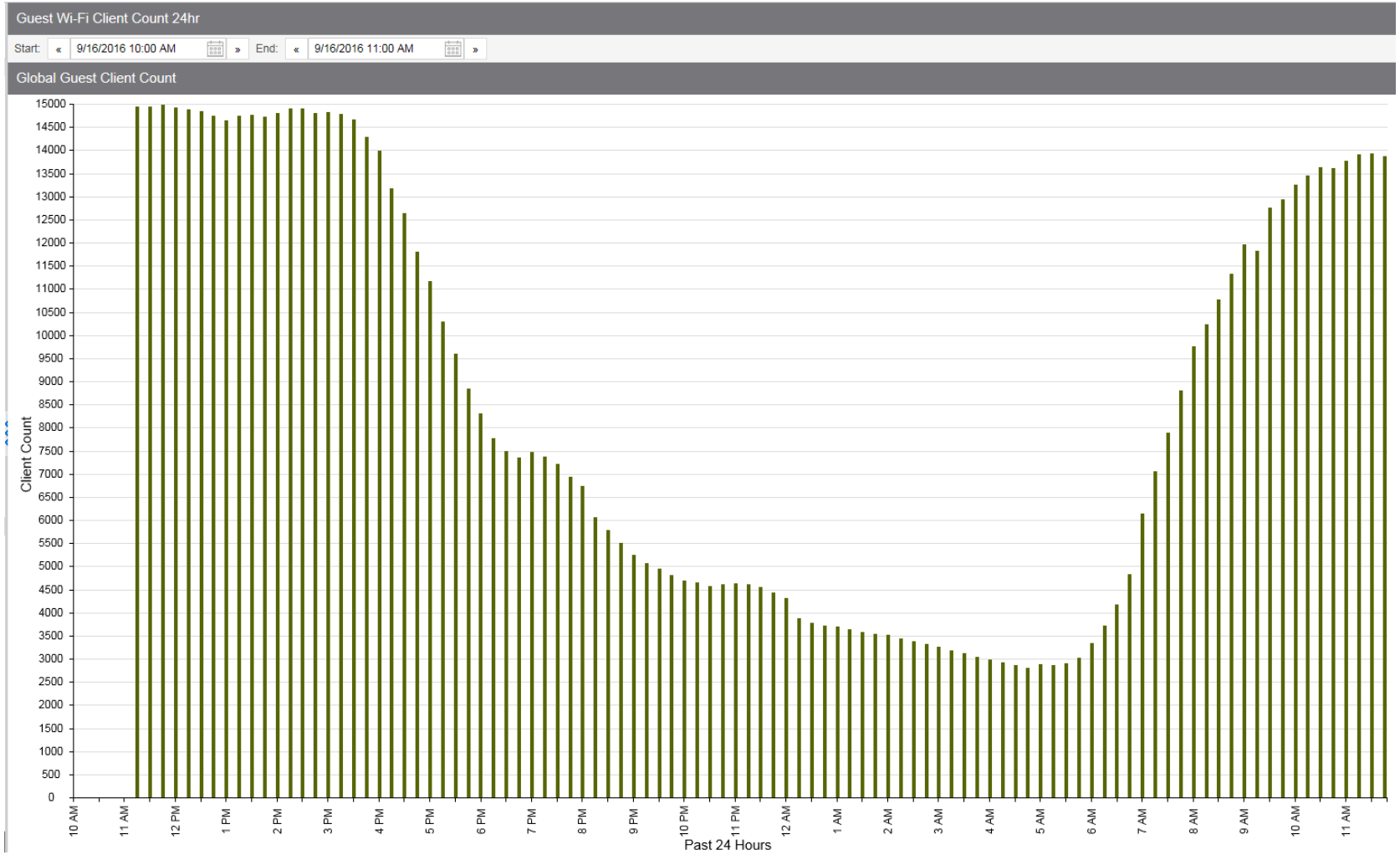
- Drawbacks to physical parallel network.
- Ubiquitous vs localized coverage.
- Leveraging a dedicated SSID in the 2.4 GHz band has its pros and cons.
- Role 5 GHz can play for guest access.
- Guest user density





Wild Fire

- Continuous Growth
- Peak of 15K guests on a given day out of 24K users
- Capacity planning.



DHCP Considerations

- Scalability. Not unusual to pool VLANs or use larger networks to accommodate the user load.
- Limiting the Broadcast domain (drop broadcast/multicast traffic)
- DHCP server on the WLAN Controller vs Dedicated DHCP server
- Clients can inadvertently and unknowingly use up IP addresses and take up a lease.
- Appropriate lease times are critical for success.
- Threshold Alerts.

	Addresses	Hosts	Netmask	Amount of a Class C
/30	4	2	255.255.255.252	1/64
/29	8	6	255.255.255.248	1/32
/28	16	14	255.255.255.240	1/16
/27	32	30	255.255.255.224	1/8
/26	64	62	255.255.255.192	1/4
/25	128	126	255.255.255.128	1/2
/24	256	254	255.255.255.0	1
/23	512	510	255.255.254.0	2
/22	1024	1022	255.255.252.0	4
/21	2048	2046	255.255.248.0	8
/20	4096	4094	255.255.240.0	16
/19	8192	8190	255.255.224.0	32
/18	16384	16382	255.255.192.0	64
/17	32768	32766	255.255.128.0	128
/16	65536	65534	255.255.0.0	256

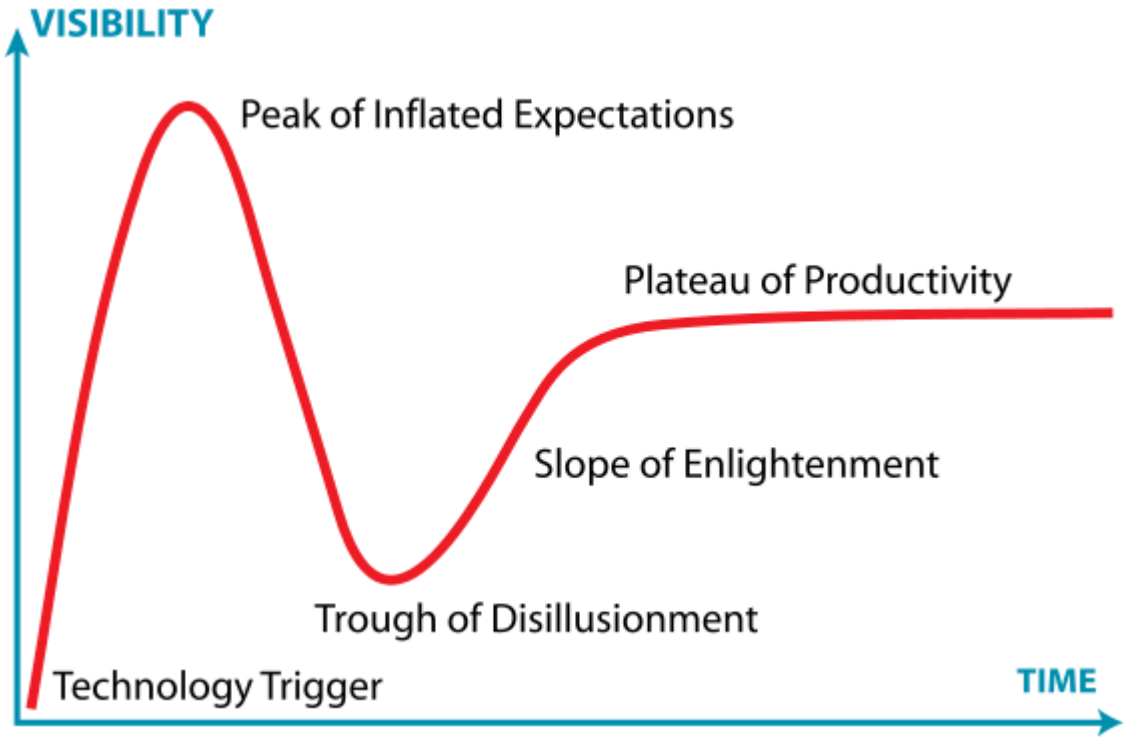
DNS Consideration

- Replicate DNS locally
- Excessive DNS requests appear like DoS attack.
- Personal vs Corporate licensing
- First line of Defense

Provider	Primary DNS Server	Secondary DNS Server
Level3[1]	209.244.0.3	209.244.0.4
Verisign[2]	64.6.64.6	64.6.65.6
Google[3]	8.8.8.8	8.8.4.4
DNS.WATCH[4]	84.200.69.80	84.200.70.40
Comodo Secure DNS	8.26.56.26	8.20.247.20
OpenDNS Home[5]	208.67.222.222	208.67.220.220
DNS Advantage	156.154.70.1	156.154.71.1
Norton ConnectSafe[6]	199.85.126.10	199.85.127.10
GreenTeamDNS[7]	81.218.119.11	209.88.198.133
SafeDNS[8]	195.46.39.39	195.46.39.40
OpenNIC[9]	162.211.64.20	199.195.249.174
SmartViper	208.76.50.50	208.76.51.51
Dyn	216.146.35.35	216.146.36.36
FreeDNS[10]	37.235.1.174	37.235.1.177
Alternate DNS[11]	198.101.242.72	23.253.163.53
Yandex.DNS[12]	77.88.8.8	77.88.8.1
censurfridns.dk[13]	91.239.100.100	89.233.43.71
Hurricane Electric[14]	74.82.42.42	
puntCAT[15]	109.69.8.51	

Bluetooth Low Energy

- BLE operates in the 2.4 GHz ISM band.
- Unlike classic Bluetooth, BLE remains in sleep mode constantly except for when a connection is initiated. (The actual connection times are only a few mS)
- Leveraging Beacons for context awareness.
- “Where am I” vs “How Close am I”?
- Battery and smartphone friendly.
- Increased focus on engagement applications.



*Gartner Hype Cycle

Mobility Strategy

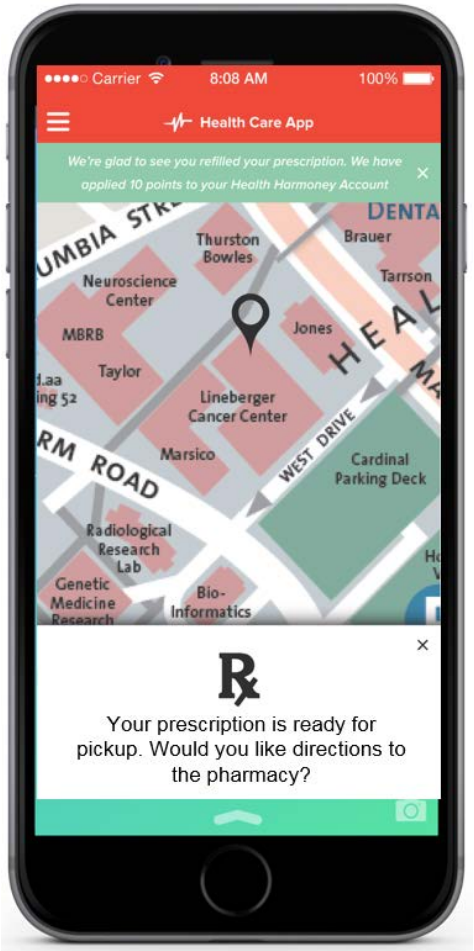
- Mobility encompasses much more than Wi-Fi
- As the number of RF devices increases so does the chance and risk of interference.
- Availability and roadmap of spectrum shapes our mobility strategy including direction with DAS, LTE-U, Wayfinding, RTLS, etc. Using DECT is a good example.
- Options for smartphone and tablet indoor connectivity
- Trend towards Mobility teams.

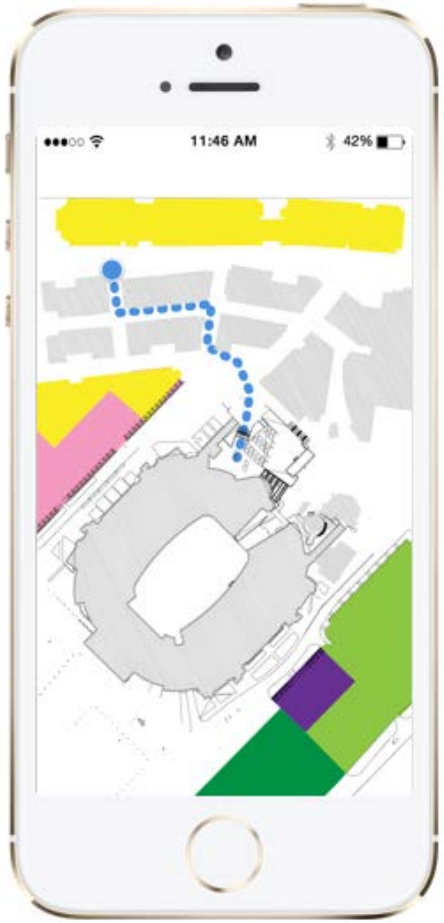
“Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.”

-Sun Tsu

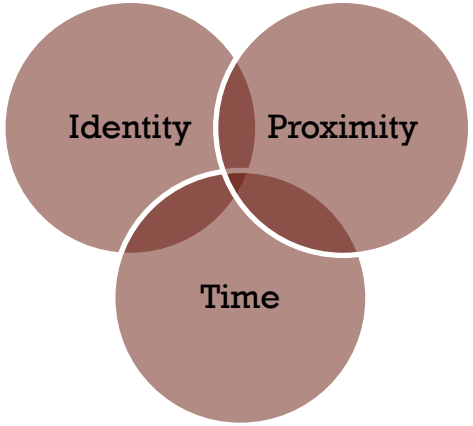
Wayfinding

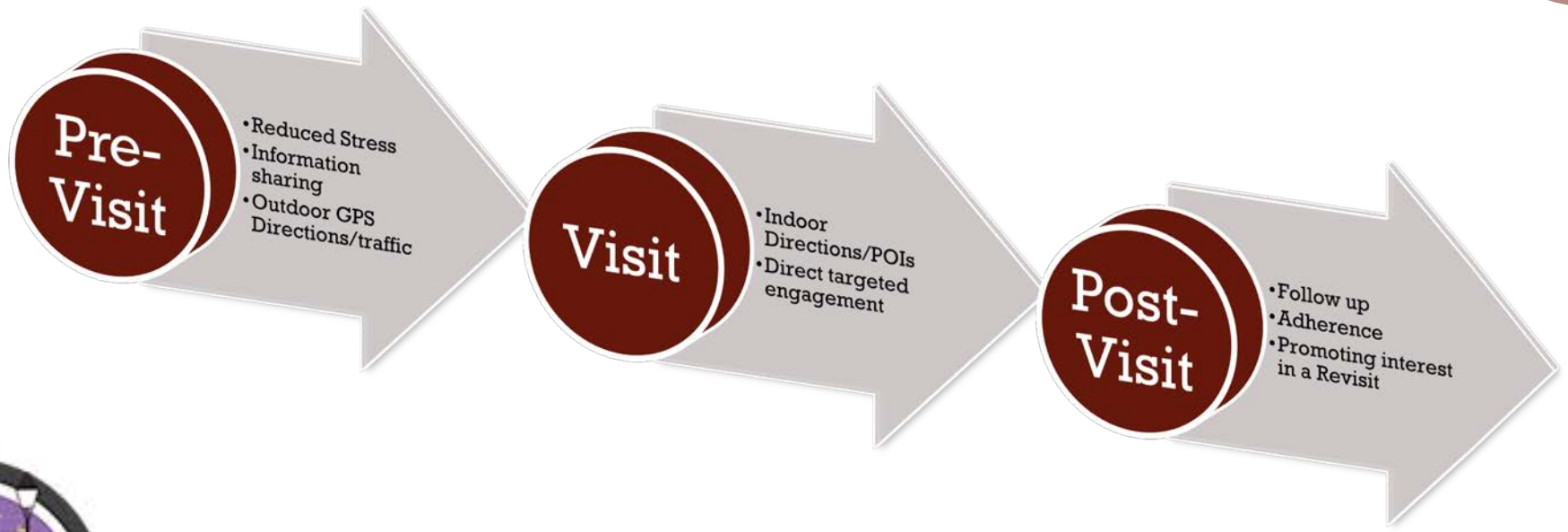
- Indoor Turn by Turn navigation
- Key points of interest
- GPS, BLE, and Wi-Fi Triangulation.
- Guest engagement is the immediate intent not RTLS.





The Future: End to end engagement





Q & A