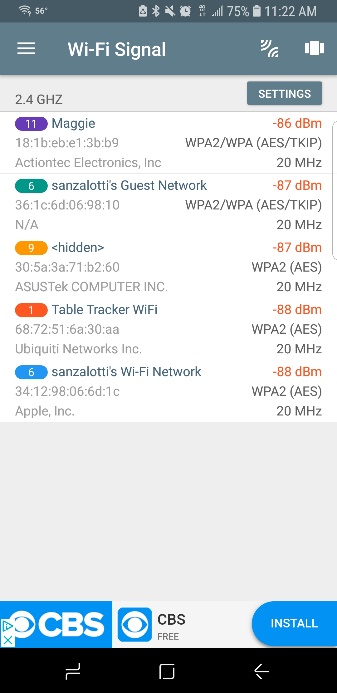
Group 1 (Ayers Lead)

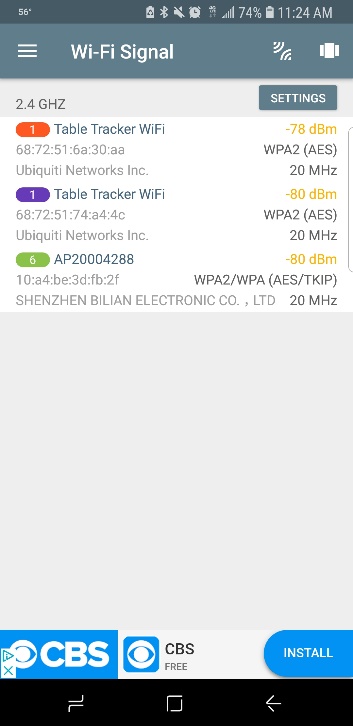
10/22/2018

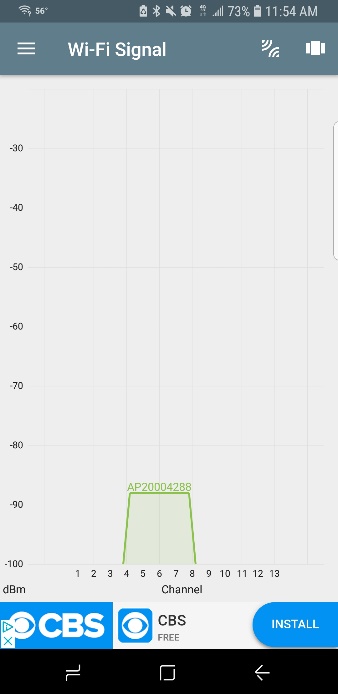
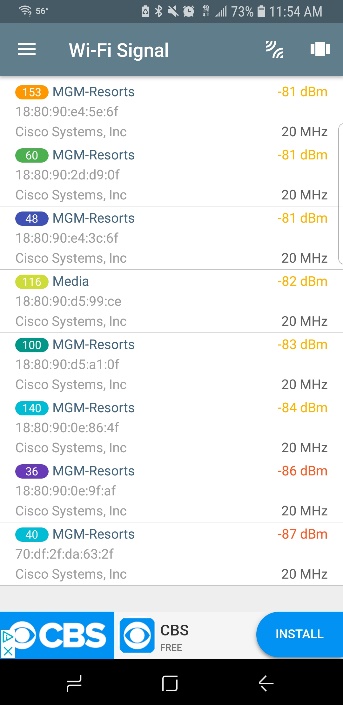
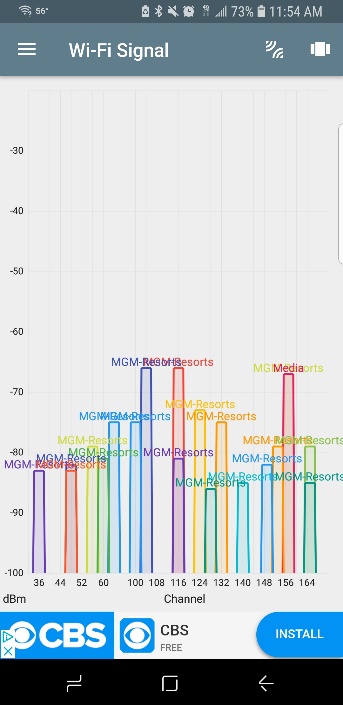
IT 320 – 41

Assignment 2

Group1\_assign2.pdf

**WIFI Scan #1**



**General findings**

For the WIFI scan portion of the assignment, I decided to do a walkthrough of the new MGM Springfield. I chose this area for two reasons; to examine how a brand-new resort casino would handle their WIFI infrastructure and to see if any loopholes/over looked security issues exist. From the scans in and around the casino, it seems that MGM has decided to exclusively uses Cisco access points. As I was doing the scans, I noticed that I would get a massive amount of 5ghz readings that changed as I walked throughout the property. Although the IPv6 numbers changed, the number of scans stayed consistent. At first, I wondered what these connections could be used for, then I realized that if I walked closer to the gaming machines, the number of scanned items increased. This led me to believe that each of the slot machines had some sort of access point attached (A reasonable assumption is that the machines require access to customer rewards information when a loyalty/rewards card is used by players, which is transmitted via WIFI). Oddly, the scanned items didn’t have encryption attached to the description lists, unlike 2.4GHZ. This may be due to the enterprise suite used my MGM or the fact that it’s all 5GHZ signals.

**Security**

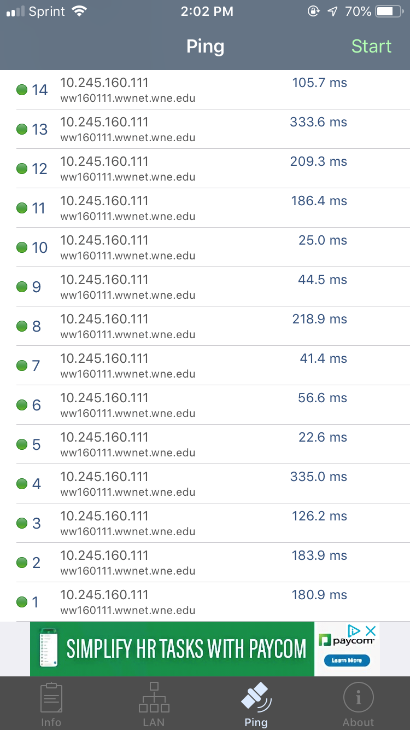
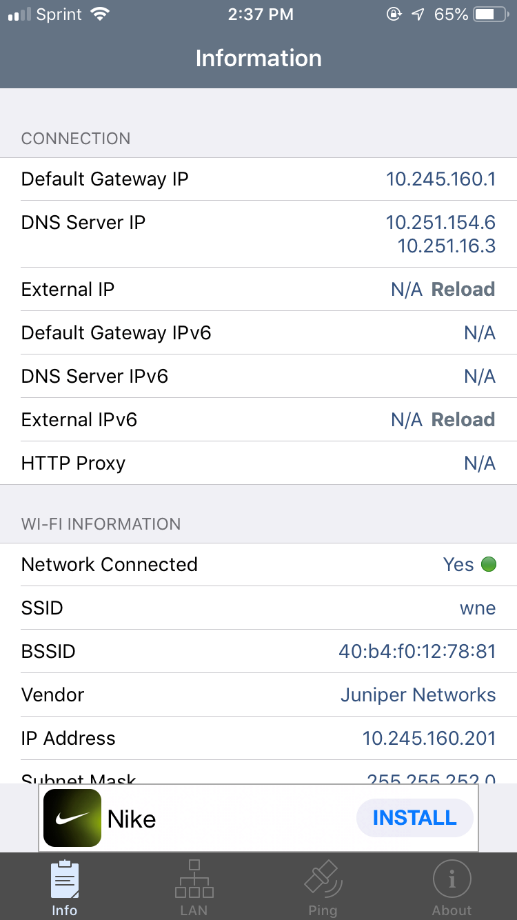
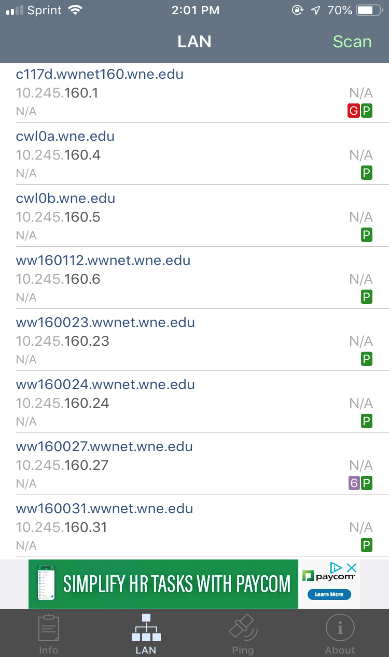
Network security, specifically WIFI security seems to be very good at MGM. Although there are hundreds of scan hits around the property, accessing the connections through conventional means seems improbable. The 5GHZ connections do not even provide encryption details, and although general names of the AP are given along with the IPV6 addresses, the lack of a description can hinder possible threats; by not giving out that information, attackers will need to try a broad range of attacks, rather than using a focused toolset. As the for names, they are general and give no indication to what the purpose of the connection is for. “MGM-Resorts” is used throughout the property for each AP and provides anonymity in function. There were a few exceptions to the theme of MGM’s WIFI networks. The Table Tracker WIFI were running on 2.4 and clearly stated what the purpose of the AP (running Table Tracker). Despite this, the connection is protected by WPA2 AES encryption, which is one of the most powerful ciphers available. There was a rogue access point that was easily discovered (given away by it’s naming convention) within the casino. These manufacturers were not consistent with the exclusive use of Cisco products within MGM, but considering the overall security of the property, I don’t feel it would be an issue. It’s probably worth locating and discovering regardless.

Physical security is good. I was actually approached by security as I was preforming my scans. Although I was not exactly discrete in scanning, it was surprising that it was brought to the floor security’s attention. Due to the nature of the property, and the fact it’s a casino, it’s unsurprising that personnel are monitoring cameras attentively. I was scanning for roughly 20-25 minutes before I was approached, and on a busy Saturday it was impressive.

**Final thoughts and recommended fixes**

Overall, MGM seems to be living up to the “New construction, new technology”. The use of 5GHZ WIFI permits the use of hundreds of AP’s attached to gaming machines, business use, and customer use. The use of 23 channels is clearly used to prevent multichannel interference among the property and is carefully laid out to reflect such. Even though the MGM-Resorts WIFI AP’s did not display encryption methods, the 2.4 signals are using the best form of encryption available. Rouge AP’s seem to be an issue but it’s unknown if they have posed any threat to MGM’s WIFI infrastructure. Physical security is apparently doing their jobs very well, considering being approached by personnel for my phone scanning.

**Wifi Scan #1**

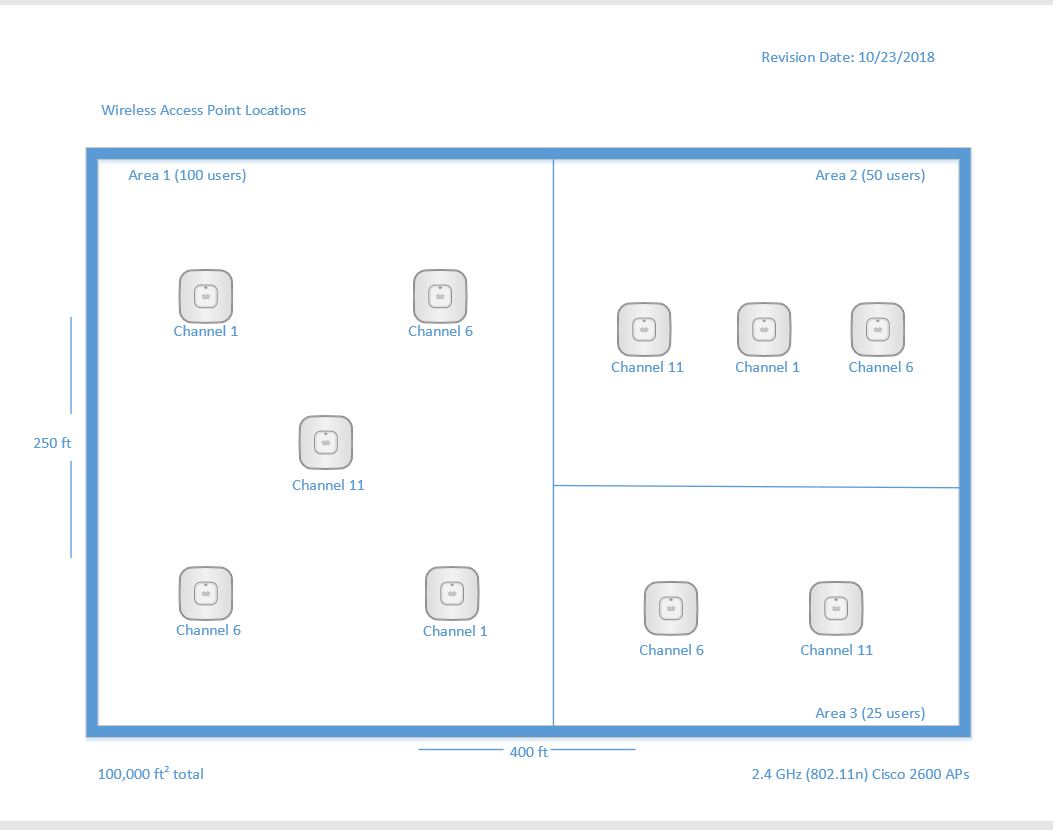


**General and Security thoughts**

For the Wi-Fi scan, I did it from the OIT room at work. I was able to come up with around 860 different IPv6 addresses that were all unique showing that they were all different devices connected to the WNE guest Wi-Fi. I even was able to ping a few of these repeatedly with a simple press of a button which shows that the ability to DDOS an individual on the WNE guest Wi-Fi is as simple as having a free app and pressing one button. Most of these were phones and laptops as most school desktops around campus are plugged in through Ethernet capabilities to the wne.local domain. I do not know if the school keeps track of WNE guest security wise, but it did not seem as if anyone was aware of the face that I was one tracking hundreds of IP addresses as well as simultaneously pinging multiple of these addresses constantly for a few minutes.

I came up with over 1,000 IP addresses when using WNE Wi-Fi. These are usually loaner laptops that professors and other staff can use, I authenticated with the actual Wi-Fi with my ID and password. If the pinging constantly disrupted anything I may get a call or something from my supervisors about all the pinging I had done to multiple different devices as shown in the screenshots(for both WNE and WNE guest). The encryption was not displayed by the app I had found yet it seemed as if all these devices connected to various access points were very accessible and findable through very simple means. Rouge AP’s were nonexistent throughout campus as it is a policy here that you cannot set up your own routers or other means of creating AP’s and can be tracked and shut down by campus police “peacefully”.

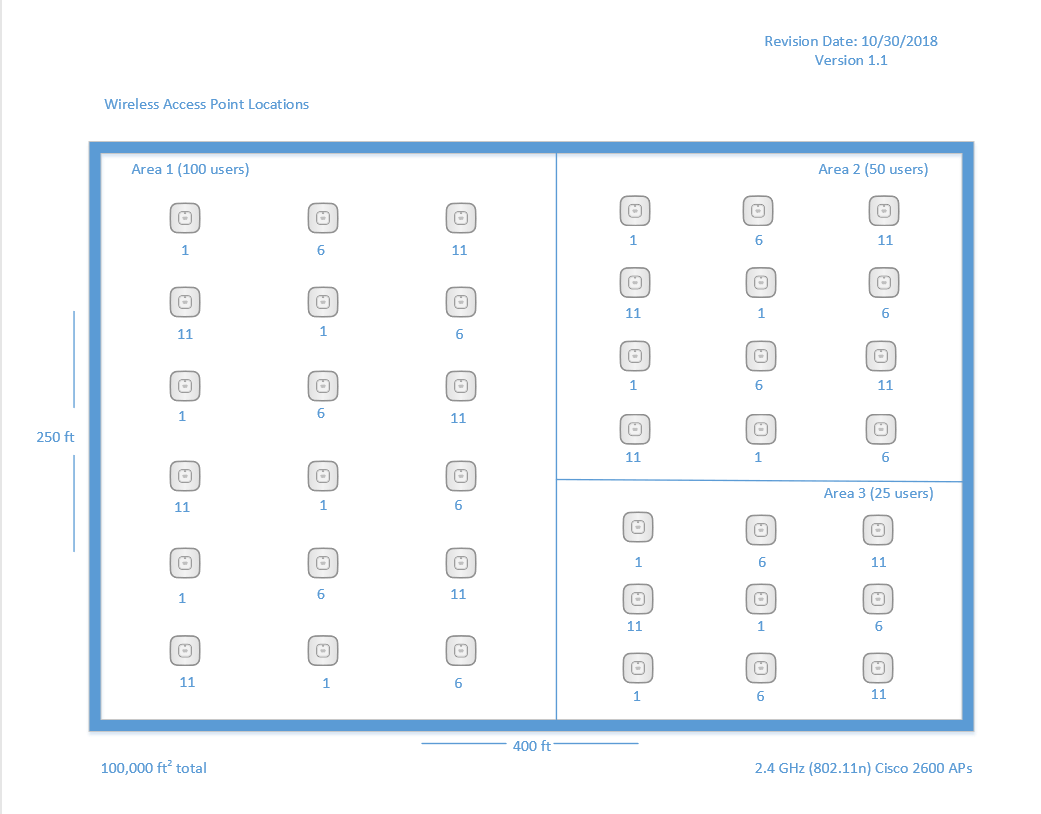
**AP Diagram Version 1 10/23/2018**



**Brief rationale of AP diagram :**

The building is 100,000 ft2 on the inside, with dimensions of 250 feet by 400 feet. Not only did the physical range of the wireless network need to be accounted for, but also the number of hosts connected to each AP. The latest wireless standard to support 2.4 GHz is 802.11n, which is used in the diagram. This standard, with an enterprise-grade AP, theoretically has a range of over 200 feet. However, since the interior structure and organization of the building is unknown, I kept the physical range estimates conservative to ensure dead-zones were kept to a minimum. Regarding the number of hosts using each access point, I found the generally accepted rule of thumb in the industry to be a maximum of 25 hosts per AP for general use. But since our three segmented areas have 100, 50, and 25 concurrent users respectively, I wanted to allow a buffer in case the users require a lot of bandwidth. Thus, I’ve elected to install 1 additional AP over the rule of thumb in each segmented area. For example, the areas should be able to support 125, 75, and 50 hosts for general use respectively. This buffer accounts for growth, potential hardware failure of APs, and rigorous bandwidth demands. With regard to wireless channels, channels 1, 6, and 11 were utilized to mitigate wireless interference. I used the “graph coloring” principle of graph theory to choose which APs were assigned to certain channels to prevent overlap as best as possible.

**AP Diagram Revision 2, Version 1.1 10/30/2018**



**Rationale for Revision (ver. 1.1)**

An expert networking consultant analyzed our site diagram and explained that we would have weak coverage at best, given the square footage of the building. Also, that if any of the APs were to fail, we’d have major dead zones and would struggle to handle the load of the users. Upon further research, the average coverage in square feet for the Cisco 2600 AP (our chosen model) has a rule of thumb coverage of 5,000 ft2 for data only, and 3,000 ft2 for VoIP and location services as well, according to Cisco documentation linked below. Based on a rectangular grid pattern to position the APs evenly across the space, the total number is now 36, up from 10 access points. Dividing 100,000 by 36 gives each access point an area of roughly 2,800 ft2, which is significantly below the data-only coverage number, and comfortably below the VoIP number.

https://www.cisco.com/c/en/us/td/docs/wireless/technology/apdeploy/7-5/Cisco\_Aironet75.html