

IA 605 Homework 1

Home Internet Service Provider

In the rural town of Rehoboth, MA, there are essentially two options for an Internet Service Provider (ISP):

- (a) Verizon Digital Subscriber Line (DSL) or
- (b) Comcast Coaxial Cable.

A decade ago, we used Verizon's Digital Subscriber Line (DSL) for Internet access; however, we terminated that service in 2012 when we disconnected our home phone number.

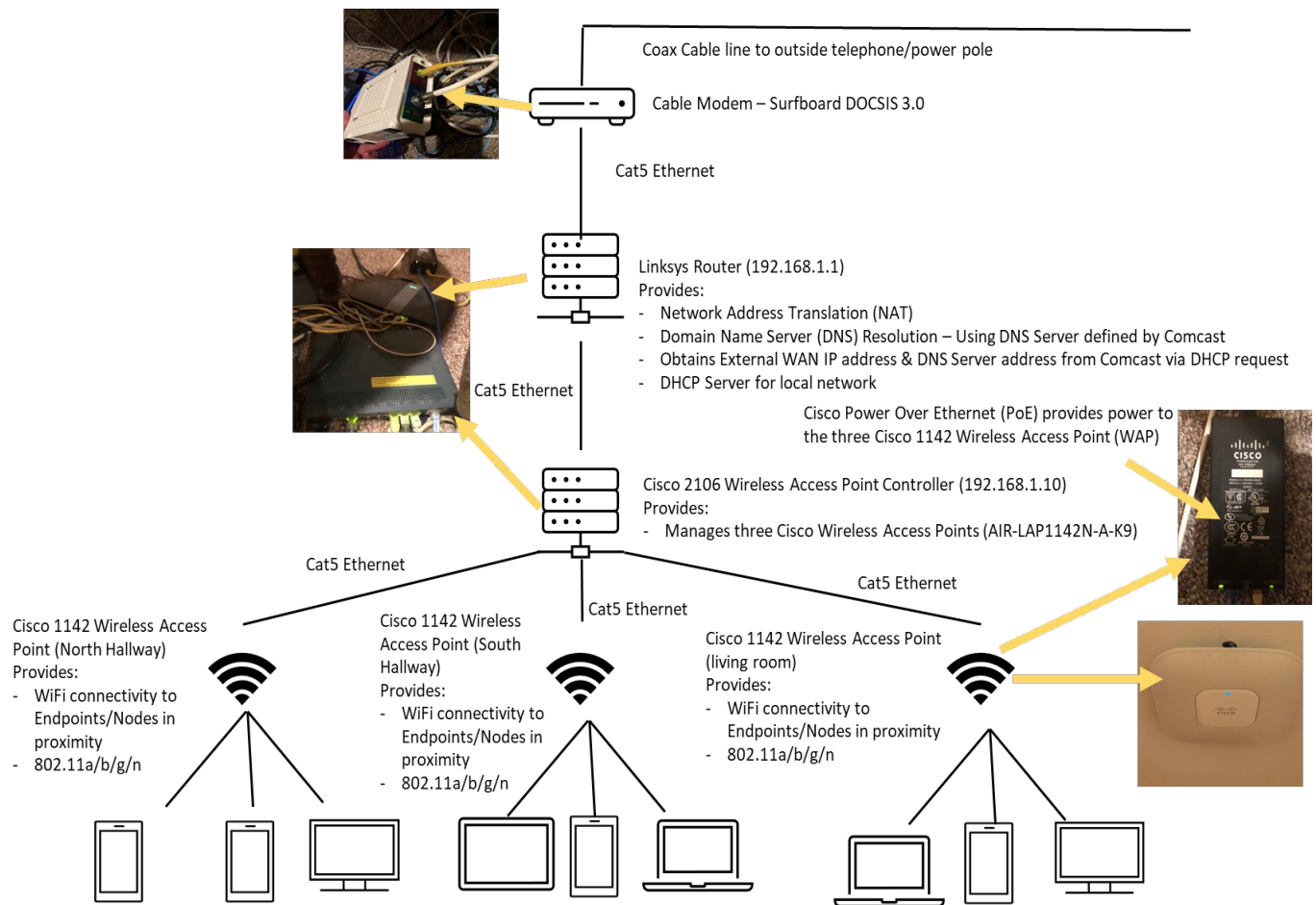
We now use Comcast and purchased a DOCSIS 3.0 cable modem. Even though we purchased the modem, the Media Access Control (MAC) address for the cable modem had to be registered with Comcast for service to be activated at the house.

Transmission over the Comcast cable lines is a shared broadcast medium and any noise on the lines can impede service. In April 2020, a Comcast technician was troubleshooting the cable network in my neighborhood determined my house was the source of noise on the coaxial cable line and installed a filter outside the house to reduce impact to other users.

Infrastructure offerings from Comcast are limited to e-mail accounts for all family members, with some limited anti-virus filtering. In the past, Comcast offered McAfee antivirus software for laptops and desktops; however, that support has now been discontinued as well.

Essentially, our ISP in this case simply offers e-mail, route to the Internet with a single IP address provided by their Dynamic Host Configuration Protocol (DHCP) server, and Domain Name Service (DNS) support.

Home Network Architecture



The above diagram illustrates the high-level architecture of the home network.

A DOCSIS 3.0 cable modem is connected to the coaxial cable that serves as the physical link for communications and connects to Comcast infrastructure on the telephone/power pole outside the house.

An End-of-Life Linksys router (Model # EA6350) is statically assigned an IP address 192.168.1.1 and is connected to the DOCSIS 3.0 cable modem. This router also implements a WiFi capability, but that capability has been disabled in favor of the Cisco Wireless architecture that is now used in the house. The Linksys router implements Network Address Translation (NAT) to allow nodes on the local network to use the 192.168.1.x subnet. The Linksys router also

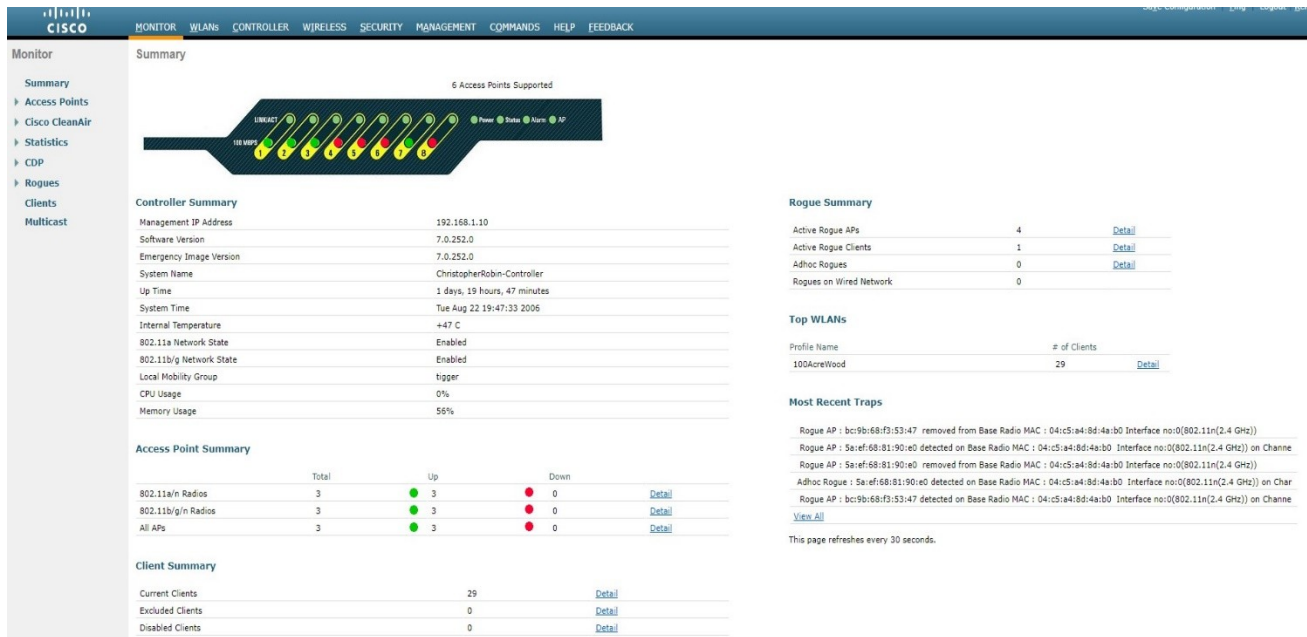
implements a local DHCP service for all Endpoints/Nodes that connect to the network in the house. The range of IP addresses that are assigned include 192.168.1.100 through 192.168.1.255.

The Linksys router connects directly to the Cisco 2106 Wireless Access Point (WAP) Controller, which is also End-of-Life and no longer supported by Cisco. The WAP Controller is statically assigned the IP address of 192.16.1.10. The WAP Controller has three ethernet cables that connect to three Cisco Power Over Ethernet (POE) injectors that deliver DC power to three Cisco Wireless Access Points (Model AIR-LAP1142N-A-K9), allowing their deployment to anyplace without electrical outlets (e.g., ceiling).

Three Cisco 1142 Wireless Access Points (APs) are installed in the ceilings of the house at strategic locations to maximize WiFi coverage (i.e., North Hallway, South Hallway, Living Room). They are connected by ethernet wiring that runs through the attic and connects back to the Cisco WAP Controller 2106. These three Wireless APs are used to connect all network EndPoints/Nodes in the house to the Internet. The three Wireless APs obtain an IP address from the DHCP service running on the Linksys router.

The Cisco WAP Controller and three APs were deployed in our house because the walls contain a mixture of concrete which reduces ability for the wireless radio signals to travel between rooms. We had implemented WiFi repeaters in the past, but they ultimately weren't reliable because of the concrete issue. By deploying the three Wireless APs at locations across the house with Ethernet connectivity to the controller, all end points can keep a reliable network connection. The picture below depicts the web-based console for administering the Cisco 2106

WAP controller with the three access points listed.



Home Network EndPoints/Nodes

Our house contains numerous Endpoints/Nodes, including at least seven iPhones, seven iPads, three smart TVs, GE refrigerator (with Keurig Coffee maker), Bosch dishwasher, four Alexa speakers, Amazon SmartPlugs, laptops, smartlock on front door, WiFi enabled HP printer, Apple TVs, and an Anova Precision Oven. IP addresses for these endpoints are assigned by the DHCP server running on the Linksys Router. The DNS server IP address provided to all nodes is 192.168.1.1 which allows the Linksys Router to route to the DNS server identified by Comcast. The listing below contains the current leased IP addresses for all endpoints as of Jan 22, 2022.

Device Name	IP v4 Address
iPad	192.168.1.146
iPad	192.168.1.204
Abigail's iPad (2)	192.168.1.179
Abigail's iPad (2)	192.168.1.111
AmazonPlug20DG	192.168.1.157
AmazonPlug1144	192.168.1.253
Abigail's iPad (2)	192.168.1.188

Erin's iPad	192.168.1.252
ESP_730F33	192.168.1.137
Erin's iPhone	192.168.1.176
LAPTOP-ENJERFVG	192.168.1.104
Abigail's iPad (2)	192.168.1.249
Apple TV (2)	192.168.1.117
ESP-BB25DE	192.168.1.238
Abigail's iPad (2)	192.168.1.178
Apple TV (2)	192.168.1.135
TABLET-28QJDOOR	192.168.1.236
US1LTFJYX5M2	192.168.1.155
Network Device	192.168.1.136
Apple TV (2)	192.168.1.166
iPad	192.168.1.220
ANOVA?Oven	192.168.1.148
Network Device	192.168.1.128
MM269407-PC	192.168.1.108
[LG] webOS TV UP7670PUC	192.168.1.223
iPad (7)	192.168.1.239
iPad (7)	192.168.1.121
Erin's iPad (3)	192.168.1.168
Jeffrey's iPad	192.168.1.163
Apple TV (2)	192.168.1.245
iPad (4)	192.168.1.158
Network Device	192.168.1.246
LAPTOP-DV8VSPM8	192.168.1.221
iRobot- 21D593E5A722464D9EAB7D87B04D6178	192.168.1.114
c74eca1c-9b6b-4cfc-bc86-047095b97711	192.168.1.199
HP9F0254	192.168.1.219
[LG] webOS TV UN7300AUD	192.168.1.105
PS5-AF38F5	192.168.1.224
South-Hallway-AP	192.168.1.234
living-room-ap	192.168.1.170
North-Hallway-AP	192.168.1.142
Network Device	192.168.1.173
LAPTOP-ENJERFVG	192.168.1.138
Toniebox	192.168.1.162
Abigail's iPad (2)	192.168.1.222
[TV] Samsung 6 Series (49)	192.168.1.123

The Cisco 2106 WAP Controller also allows the ability to view the nodes that are connected to specific APs (e.g., North Hallway, South Hallway). Each node accesses the network through an AP in the ceiling back to the controller, which sends packets back to the router for either external routing or internal routing to another node on the network.

Bluetooth usage is limited to Air pods and other wireless headphones that are use on conjunctions with iPad, cell phones and laptop computers for participating in telecons, listening to music, and watching videos.

Home Network Security

Security on the home network is mostly nonexistent. We have enabled Wi-Fi Protected Access II (WPA2) on the Cisco network controller; however, the password is not rotated. Likewise, the administrator password for the Linksys router and the Cisco 2106 are trivial but have at least been changed from the default values. The router and Cisco 2106 offer some ability to log network traffic, but it would be overwhelmingly to review and maintain.

Most security on the network is the responsibility of the endpoints. This includes automatic Operating System updates and the use of malware detection software on laptops. For Apple devices, we rely on iCloud backup and for work devices (e.g., laptop) we rely on corporate security offerings (e.g., VPN, encrypted backup, intrusion detection).

Years ago, we had a Linux server that served as a firewall to the network, placed between the cable modem and the wireless router; however, it became burdensome to manage for those without a computer networking background. It would be a good practice to add that again.

Given the number of “Internet of Things” devices that reside on the network, there are multiple opportunities an adversary could use to penetrate the network.