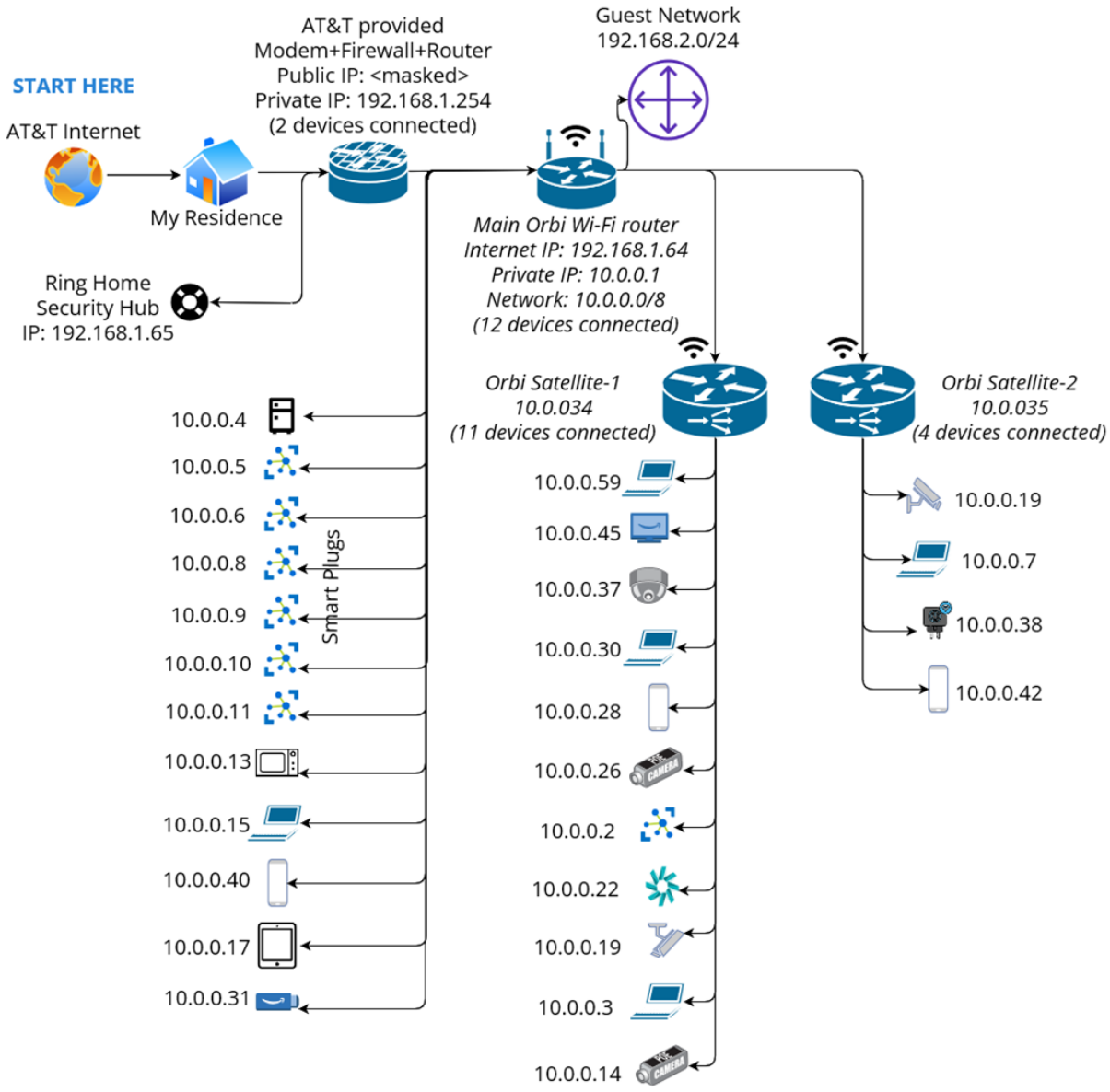
Viswanath Srinivasan Chirravuri
D.Eng. | DC7 | G34657239 | September 8th, 2024
THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

CSCI 6015: Homework-3: Collecting Network Evidence

My Home Network Architecture Diagram

(created on https://online.visual-paradigm.com/app/diagrams/#diagram:proj=0&type=NetworkDiagram)



A node to investigate on the home network

I decided to investigate my personal laptop, which has the IP address **10.0.0.3** and is connected to the Orbi satellite-1 Wi-Fi extender. I chose this device because it's a Windows laptop, and I can easily install Wireshark GUI on it to capture network packets. Plus, since this is my D.Eng. laptop, checking it won't affect the other devices on the network. I also run the nmap tool on this for hosts discovery (**nmap -sn 192.168.1.0/24 10.0.0.0/8**).

Which tool to use and Why

I plan to use **Wireshark** because I want to apply what I learned in class (from the YouTube video shown) and also use my existing knowledge of the tool on my home network. I've often used Wireshark to analyze pcap files from corporate networks, but never on my home network. So, this is a good chance for me to analyze my home network using the Wireshark tool. I also used **nmap** because I am skilled in using it.

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

Viswanath Srinivasan Chirravuri
D.Eng. | DC7 | G34657239 | September 8th, 2024

Summary of Results of packet dump obtained from Wireshark

Here're the details of packets captured on Wireshark (Statistics -> Capture File Properties):

File

Name:	C:\Users\vchir\Desktop\D.Eng\2. CSCI6015 Cyber Forensics\Assignments\Packet_Dump_10.0.0.3_Sep_7_2024.pcap
Length:	26 kB
Hash (SHA256):	d89bf778708d46b0330a98edbd08f73b71f591f73daf288ab3e73c2cecd00fcd
Hash (SHA1):	0bfe20b4fd7e4843680bed48e26f68ac222a3a30
Format:	Wireshark/tcpdump/... - pcap
Encapsulation:	Ethernet
Snapshot length:	262144

Time

First packet:	2024-09-07 14:51:49
Last packet:	2024-09-07 14:52:08
Elapsed:	00:00:18

Capture

Hardware:	Unknown
OS:	Unknown
Application:	Unknown

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Unknown	Unknown	Unknown	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	142	142 (100.0%)	—
Time span, s	18.253	18.253	—
Average pps	7.8	7.8	—
Average packet size, B	167	167	—
Bytes	23765	23765 (100.0%)	0
Average bytes/s	1301	1301	—
Average bits/s	10 k	10 k	—

Summary of packets captured:

During the Wireshark analysis of my home network, I discovered a total of **39 hosts** actively communicating. The captured data primarily consisted of IP and TCP packets, as HTTP data was not visible due to encryption provided by TLS. Additionally, I observed that **IPv6** is in use within the network. Although I initially missed including **printers** in my network diagram, Wireshark was able to detect them during the packet capture, highlighting their presence in the network.

Difference between home network diagram and Wireshark obtained results

The differences between the home network diagram I initially provided and the Wireshark results can be attributed to a few factors. First, the network diagram was based on my understanding and manual observation of devices connected to the network, which may have overlooked certain devices like printers or temporary connections. Wireshark, on the other hand, provides a more detailed and real-time view of all active hosts, capturing even those devices that may not be immediately apparent, such as those using dynamic IP addresses or intermittently connecting devices like IoT gadgets (ring cameras, washing machine, etc.). Also, Wireshark revealed network traffic at a packet level, which provided insight into the protocols and services in use, such as IPv6, that may not have been considered in the manual network diagram. This deeper, automated discovery contributes to the differences observed between the two representations.

***** END OF DOCUMENT *****